Exercise 1 - Installing and Configuring iSCSI Storage

The Encrypting File System (EFS) is a Windows security feature that encrypts certain folders and files on a hard drive. This differs from BitLocker Drive Encryption, which encrypts the entire disk. Users can encrypt their files in EFS on a domain by simply selecting the option in the document properties. This file system filter that provides filesystem-level encryption and was introduced in version 3.0 of NTFs.

An EFS recovery agent for the domain is configured on the group policy to recover the encrypted documents. A privileged account that the Root CA authorizes by granting it an EFS recovery agent certificate is known as an EFS recovery agent. The certificate is subsequently added to the group policy and then attached to the decrypted file.

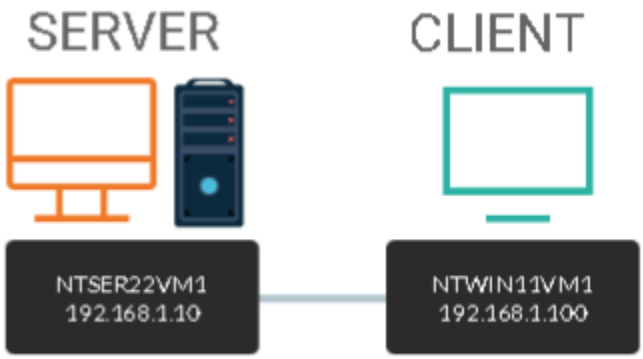
A Certification Authority (CA) is a Windows Server service that generates certificates (digital IDs) for requesters such as users, computers, and network services. The purpose of a certificate is specified, such as secure e-mail, file encryption, and so on. The certificate also checks the identity of the requester with the CA server and the organization.

A user certificate includes EFS. To safeguard personal folders and files from other users, a user can encrypt them. Users should first appoint an EFS recovery agent before utilizing EFS to secure their folders and files. A privileged user with an EFS Recovery Agent certificate is known as an EFS recovery agent. The Active Directory of the company has access to information about the EFS Recovery Agent thanks to Group Policy Objects.

In this exercise,

1. we will configure an EFS recovery agent
2. This agent will then decrypt an encrypted document.
3. Enable EFS on domain-joined Windows computers

Topology



DOMAIN = networktute.com

NTSER22VM1 = Windows Server 2022 – Domain Controller

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: I Install Root CA

A certificate is issued by a Certification Authority (CA) server to a requesting user, computer, or service. CA servers are usually arranged in a hierarchy, with the Root CA at the top, which has complete authority to issue certificates. As a result, the Root CA is the most crucial CA server in the hierarchy and must be adequately safeguarded.

The Root CA is usually kept secure, while a Subordinate CA is used to issue certificates. All certificates issued by the Root CA, as well as any servers under its control, are invalidated if it is hacked.

In this task, we will use Windows PowerShell commandlets to install a Root CA server on NTSER22VM1. This server will issue a certificate to the Administrator account.

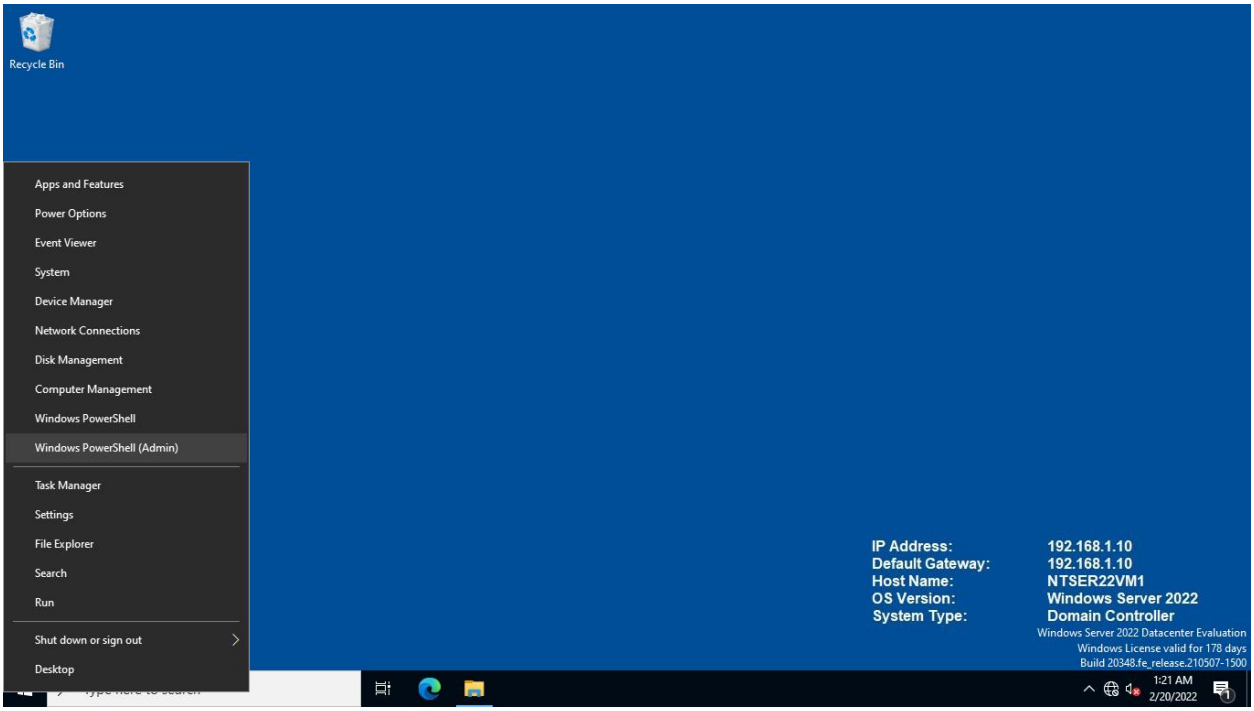
Step 1:

Make sure all of the devices listed in the exercise introduction are turned on.

Right now, let’s work with the NTSER22VM1

Since we are using the **PowerShell** for configuration

Right-click the Start icon and select **Windows PowerShell (Admin)**

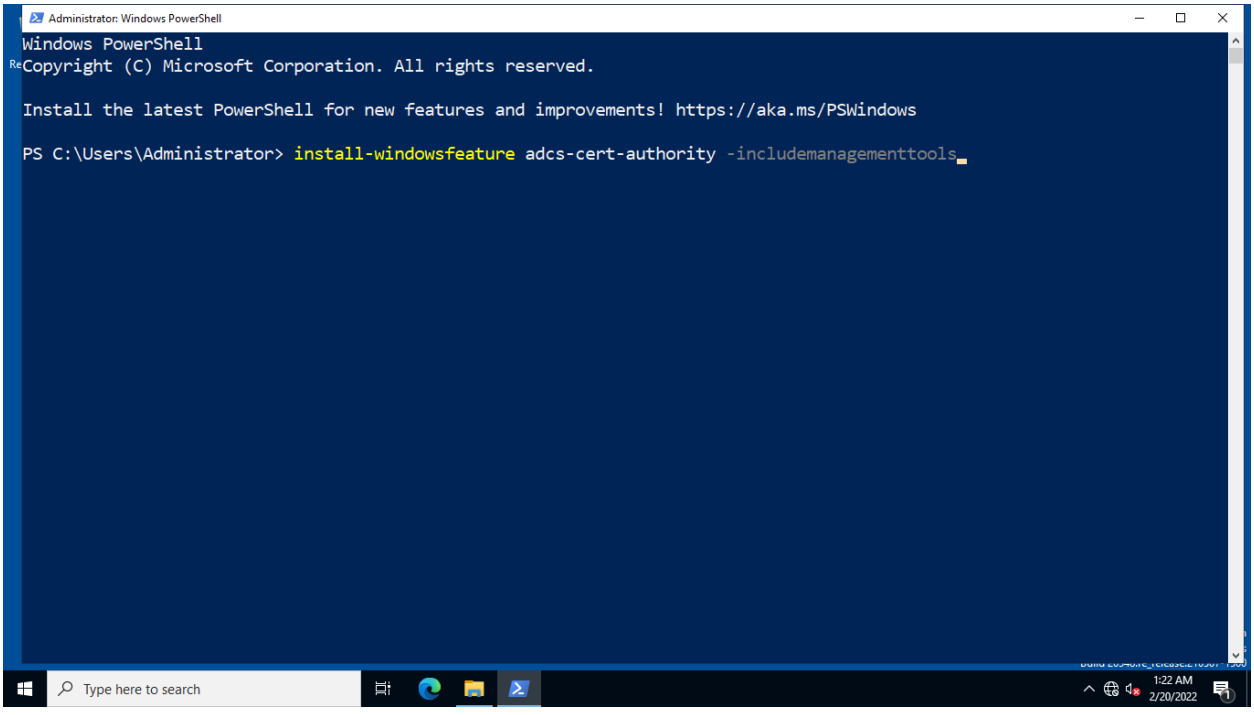


Step 2:

To install the **Active Directory Certificate Services**, type the following command:

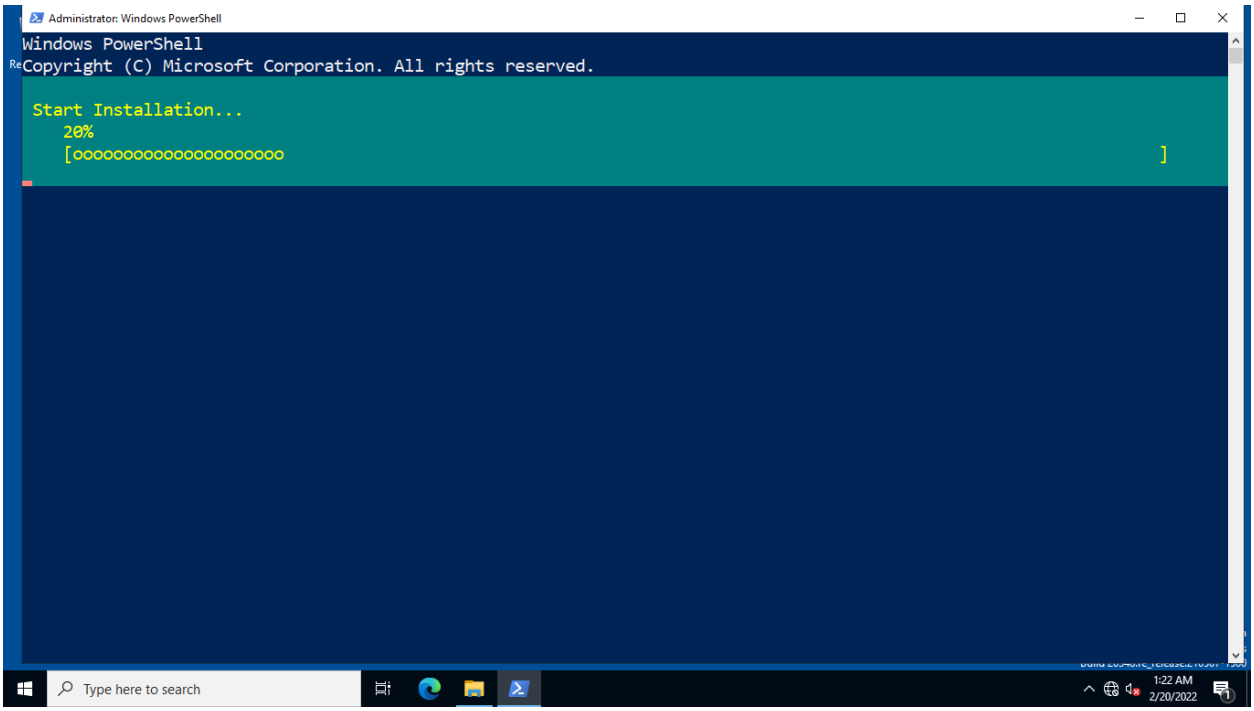
```
install-windowsfeature adcs-cert-authority -includemanagementtools
```

Press **Enter**.



Step 3:

Please wait while the **Active Directory Certificate Services** support files are installed.



Step 4:

Make sure the installation of the **Active Directory Certificate Services** is successfully completed.

Next, to install and configure the **Enterprise Root Certification Authority (CA)** role service since **Active Directory (AD)** is installed on **NTSER22VM1**. This **CA** type is integrated with **AD** that enable users, devices and network service to request certificates.

This **CA** type similarly supports **Certificate Templates. Certificate Templates** describe the usage and purpose of a certificate.

Type the following command:

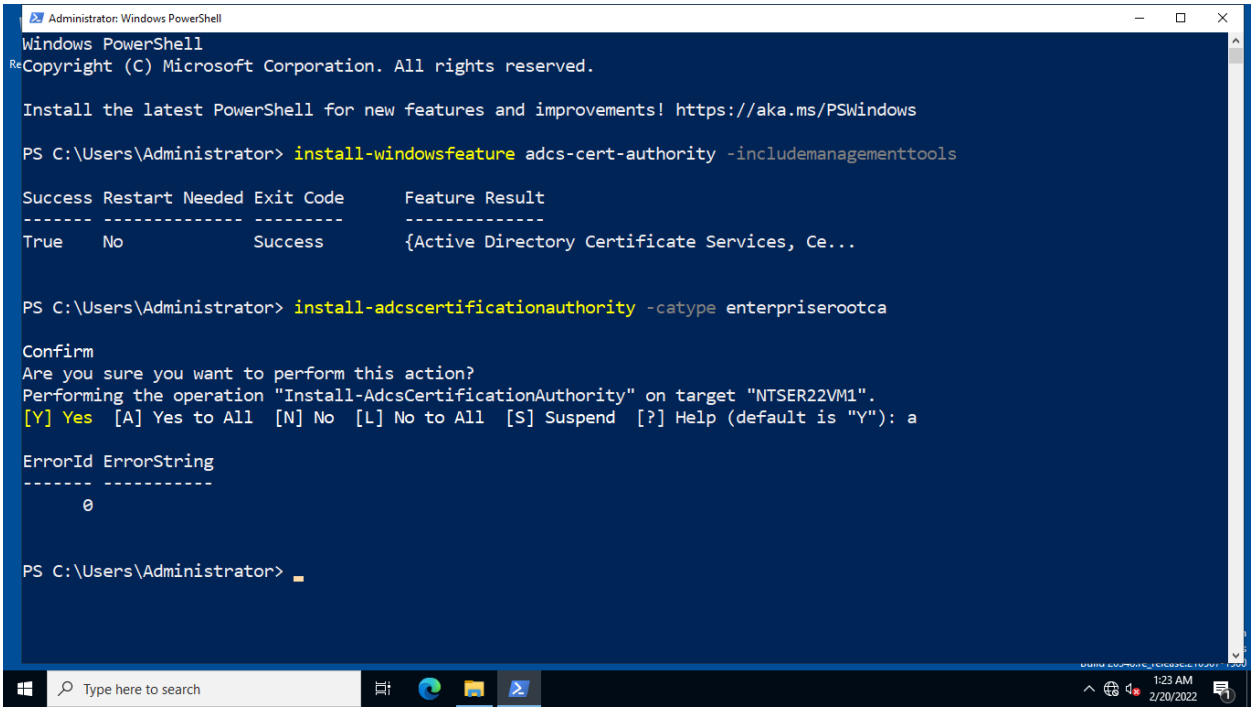
```
install-adcscertificationauthority -catype enterpriserootca
```

On the **Confirm** prompt, type:

```
a
```

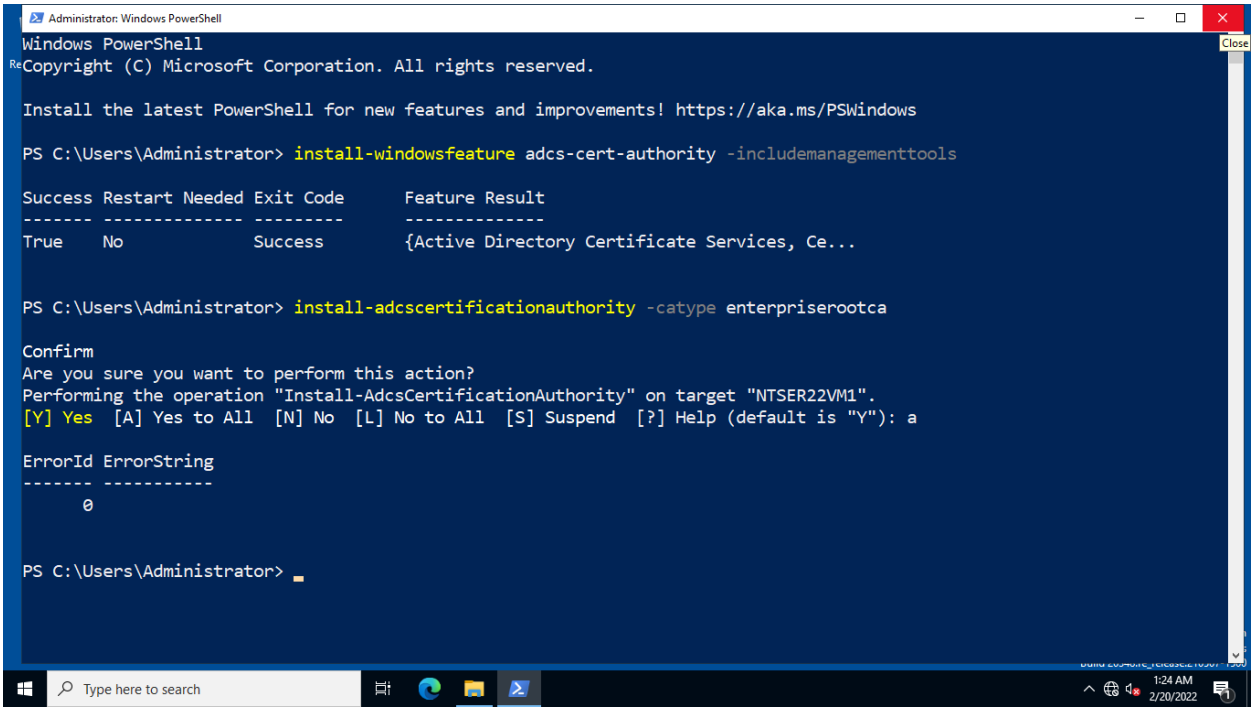
Press Enter.

A "**0**" in the **ErrorId** field indicates successful operation.



Step 5:

Close **Windows PowerShell.**



Task 2: Request EFS Recovery Agent Certificate

EFS Recovery Agent is a user account that can retrieve files that have been encrypted by other users.

The EFS recovery agent certificate was issued by the Certification Authority (CA) server to this user account.

Before allowing users to create encrypted files on their devices, corporate networks that use Active Directory Domain Services must first install an EFS recovery agent.

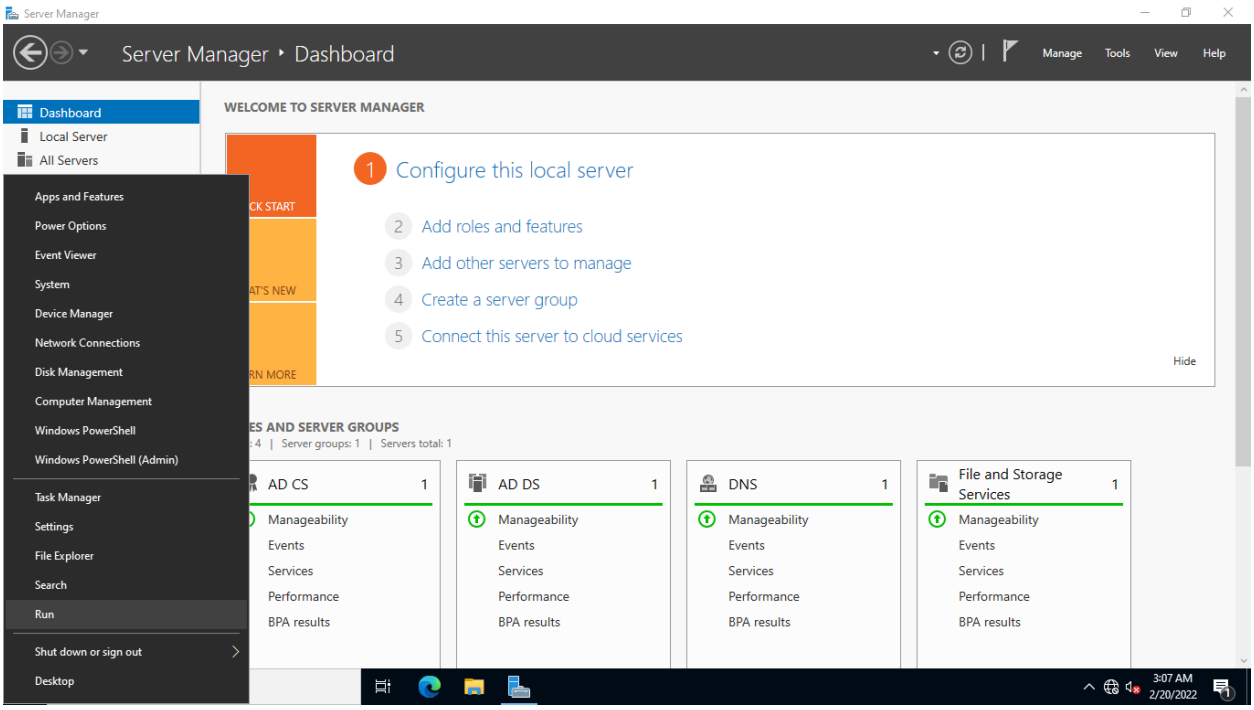
In this task, we will request for an EFS recovery agent certificate as NETWORKTUTE\administrator.

Step 1:

You are signed-in as NETWORKTUTE\administrator using NTSER22VM1.

Step 2:

Right-click **Start** and then select **Run.**

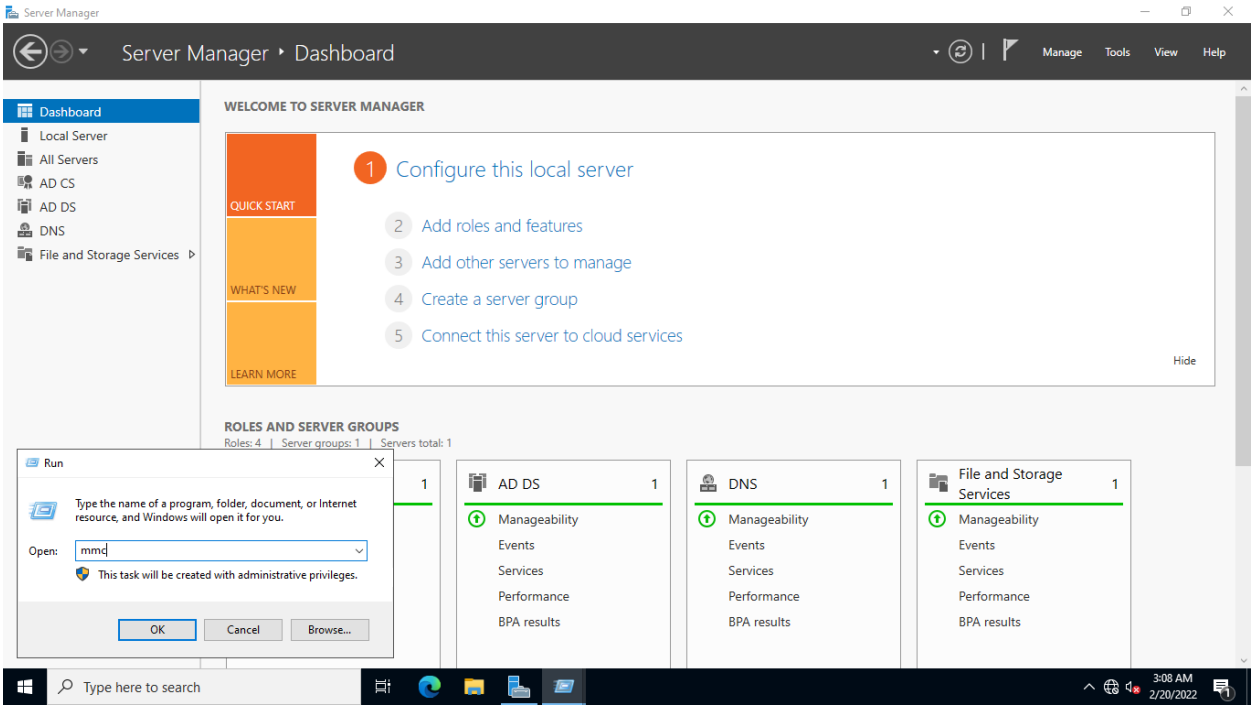


Step 3:

In the **Run** dialog box, type:

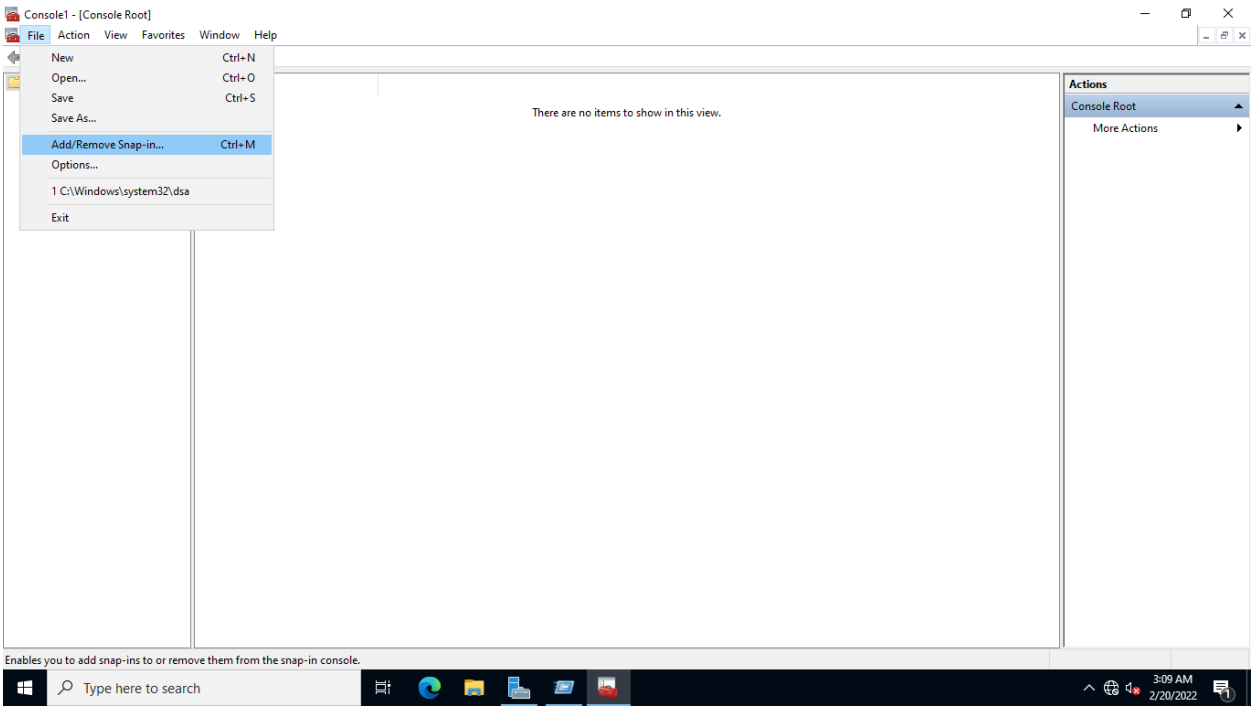
mmc

Press **OK.**



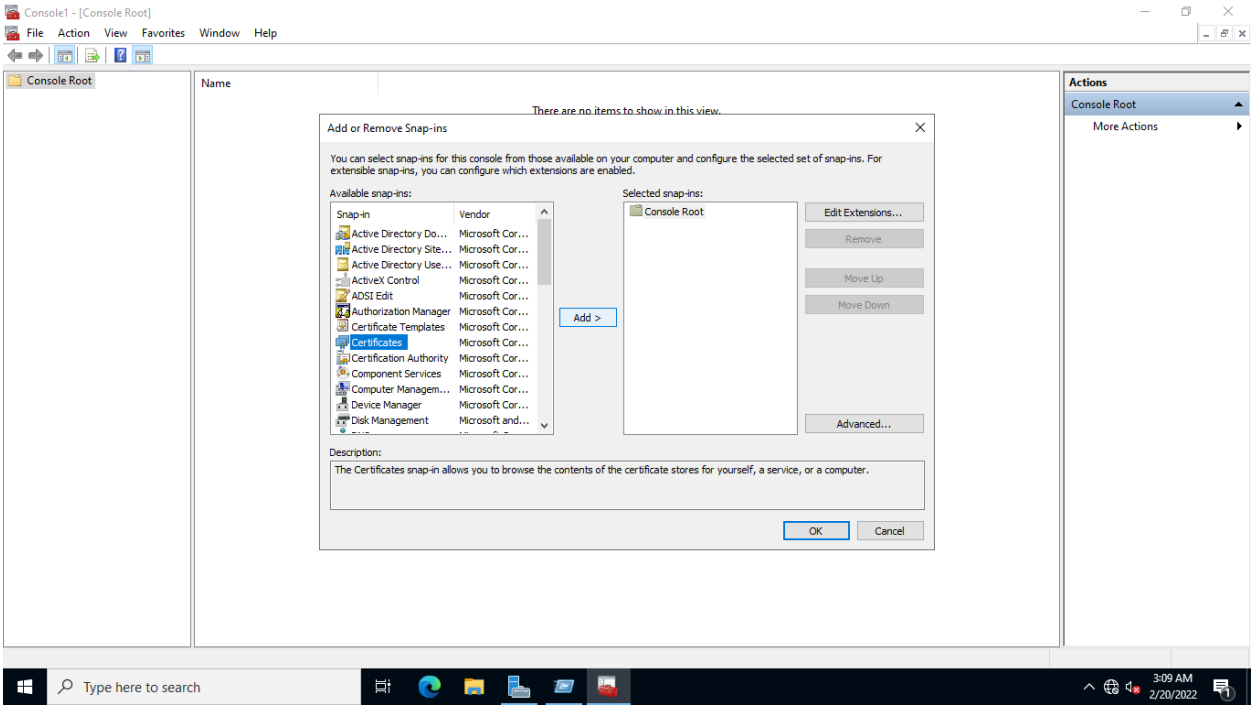
Step 4:

On the **Console1** window, click **File** and select **Add/Remove Snap-in**.



Step 5:

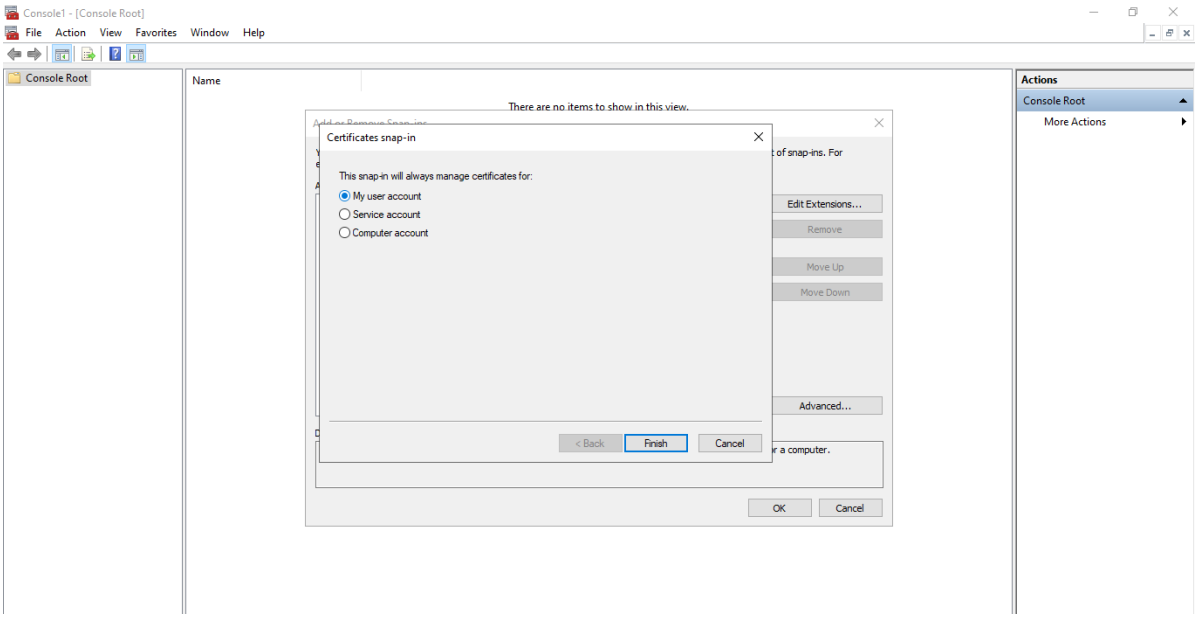
On the **Add or Remove Snap-ins** dialog box, under **Available snap-ins**, select **Certificates** and click **Add**



Step 6:

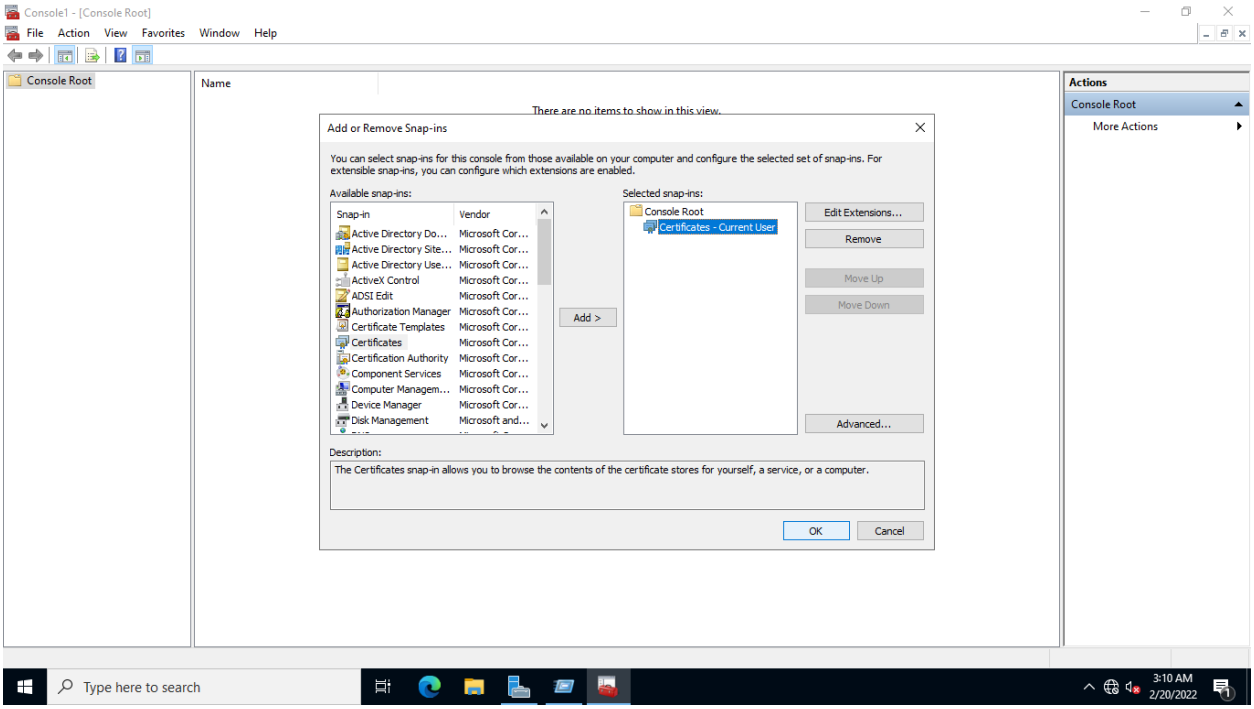
On the **Certificates snap-in** dialog box, ensure the option **My user account** is selected.

Click **Finish**.



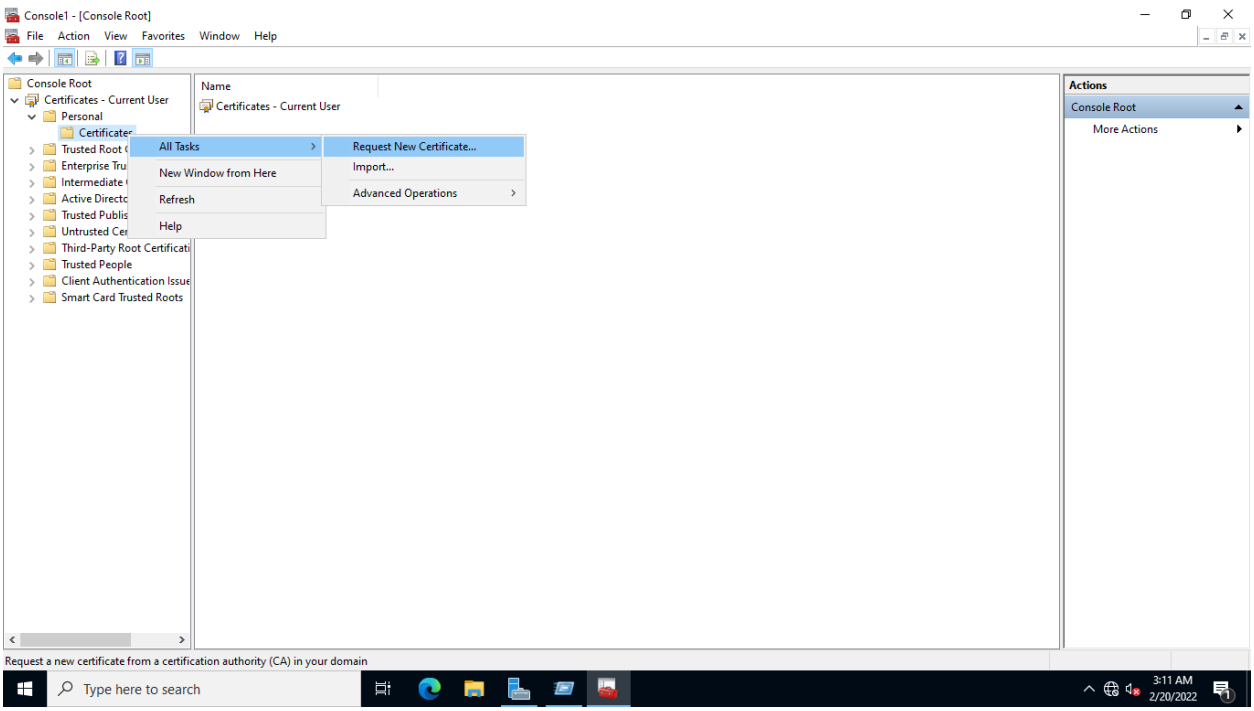
Step 7:

Back on the **Add or Remove Snap-ins** dialog box, click **OK** to close.



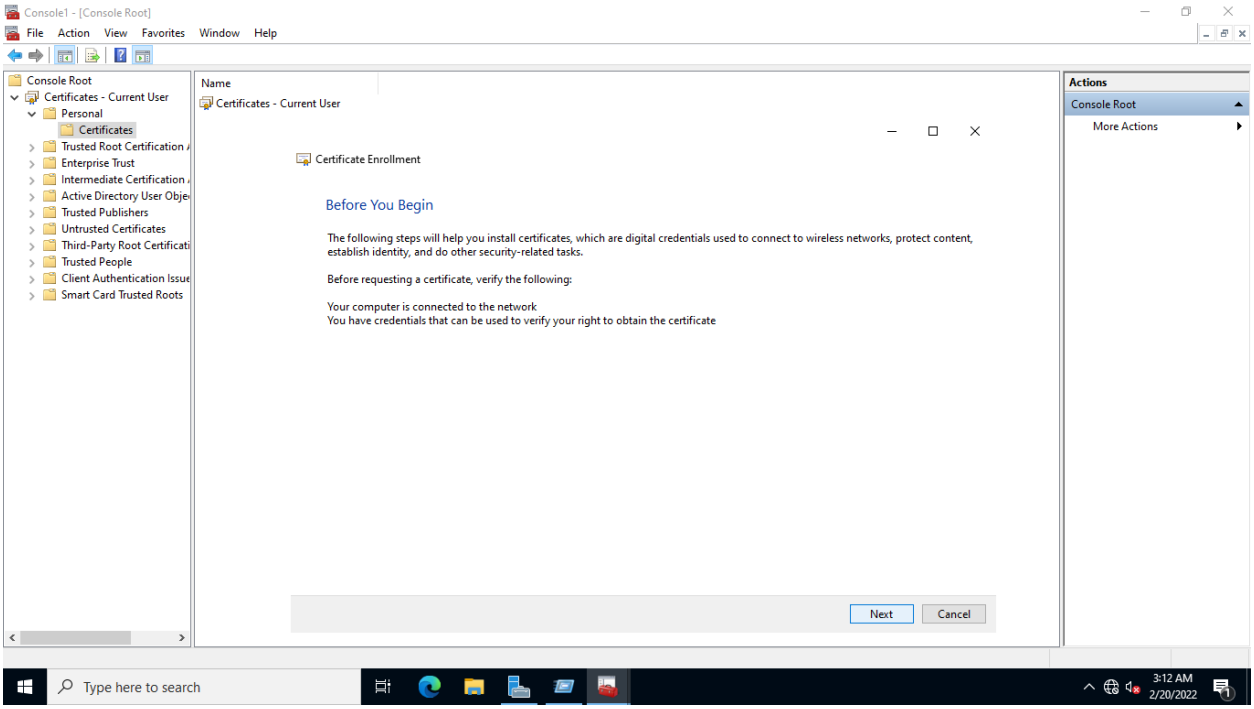
Step 8:

Back in **Console1** window, expand **Certificates** - **Current User** > **Personal**.
Right-click **Certificates**, point to **All Tasks** and select **Request New Certificate….**



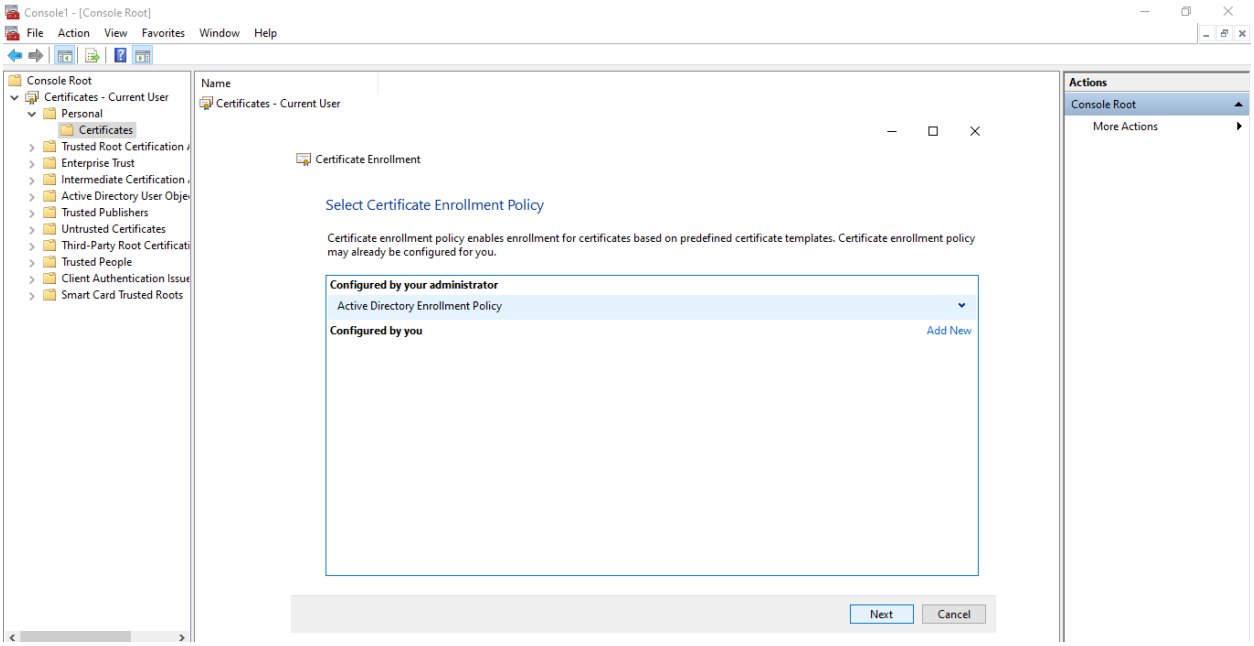
Step 9:

On the **Before You Begin** page, click **Next.**



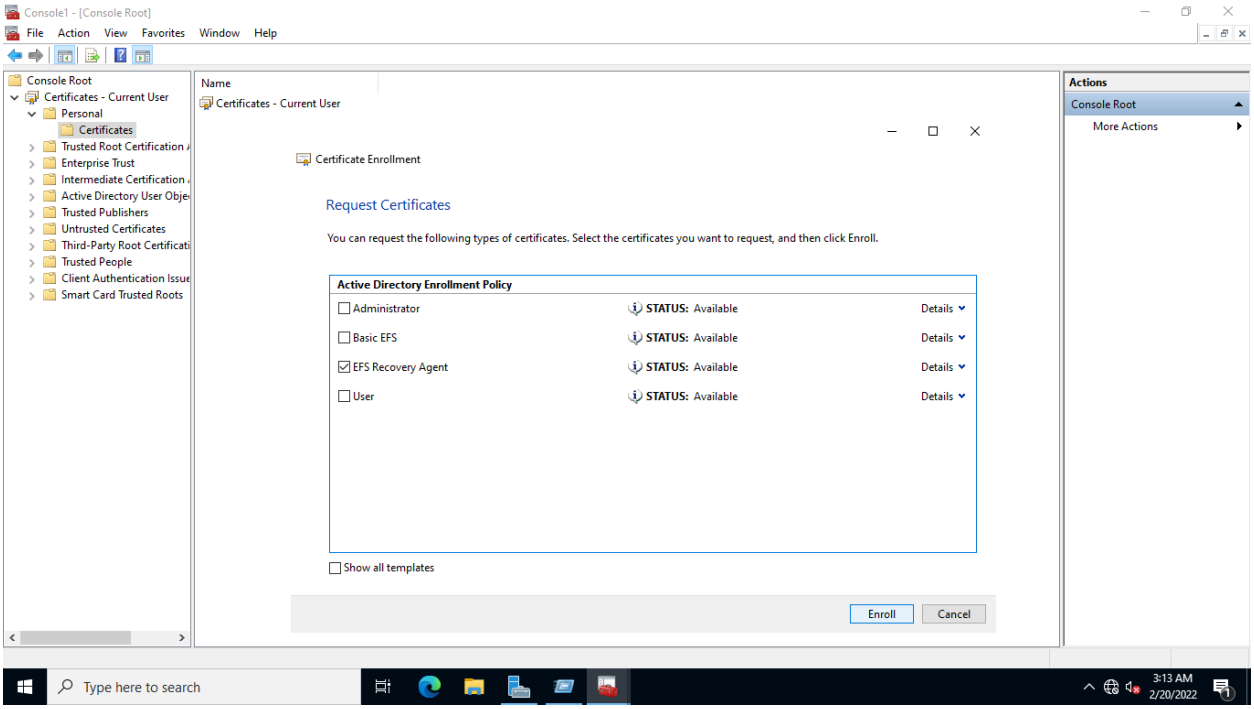
Step 10:

On the **Select Certificate Enrollment Policy** page, click **Next**.



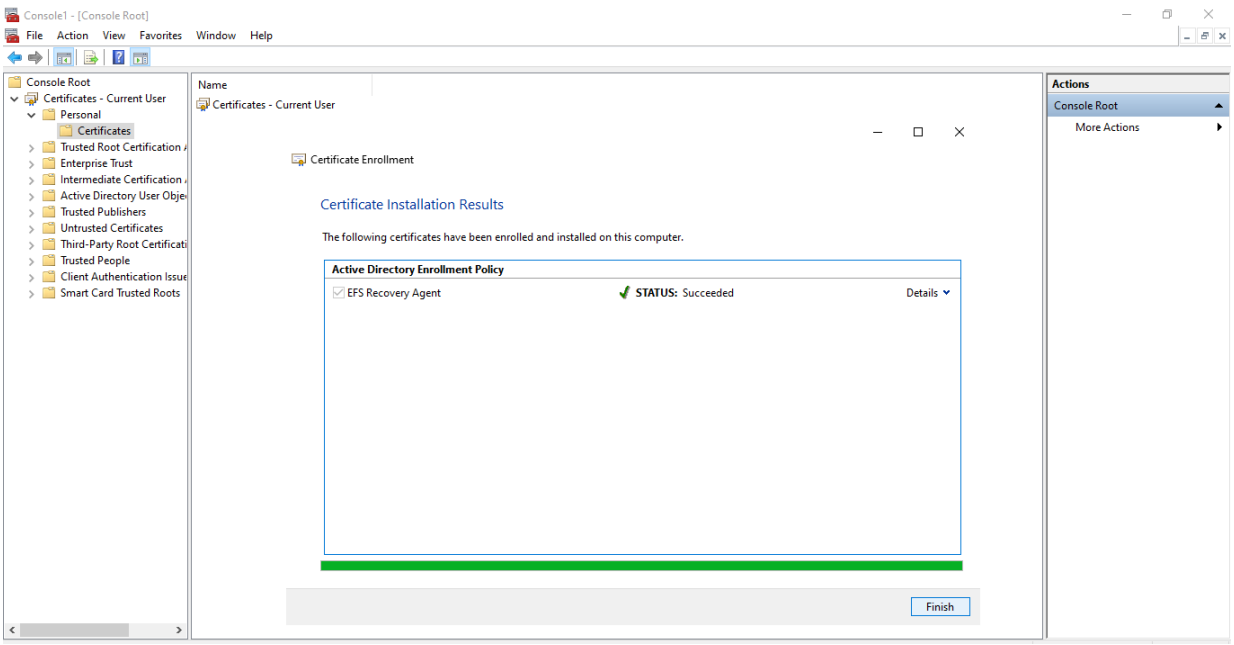
Step 11:

On the **Request Certificates** page, tick the **EFS Recovery Agent** option and click **Enroll**.



Step 12:

When the certificate enrolment is successfully completed, click **Finish** to close the **Certificate Installation Results** page.



Keep the Console1 window open.

Task 3: Export Certificate as .cer and .pfx

Certificates issued by a Windows Server Certification Authority are exportable to two formats namely .cer and .pfx

- The.cer (DER encoded binary or Base-64 encoded binary) file type contains a certificate that can be linked to a Group Policy for Encrypting File System.
- A certificate and a private key are included in the.pfx (Personal Information Exchange) format for unlocking EFS-encrypted files.

When a certificate is exported to a file, it becomes portable since the EFS recovery agent can access user devices and retrieve encrypted files. In addition, the certificate can be used by the administrator when setting an EFS recovery policy for the Active Directory domain.

In this task, we will export the File Recovery Certificate to support both formats.

Step 1:

Make sure you are connected to NTSER22VM1.

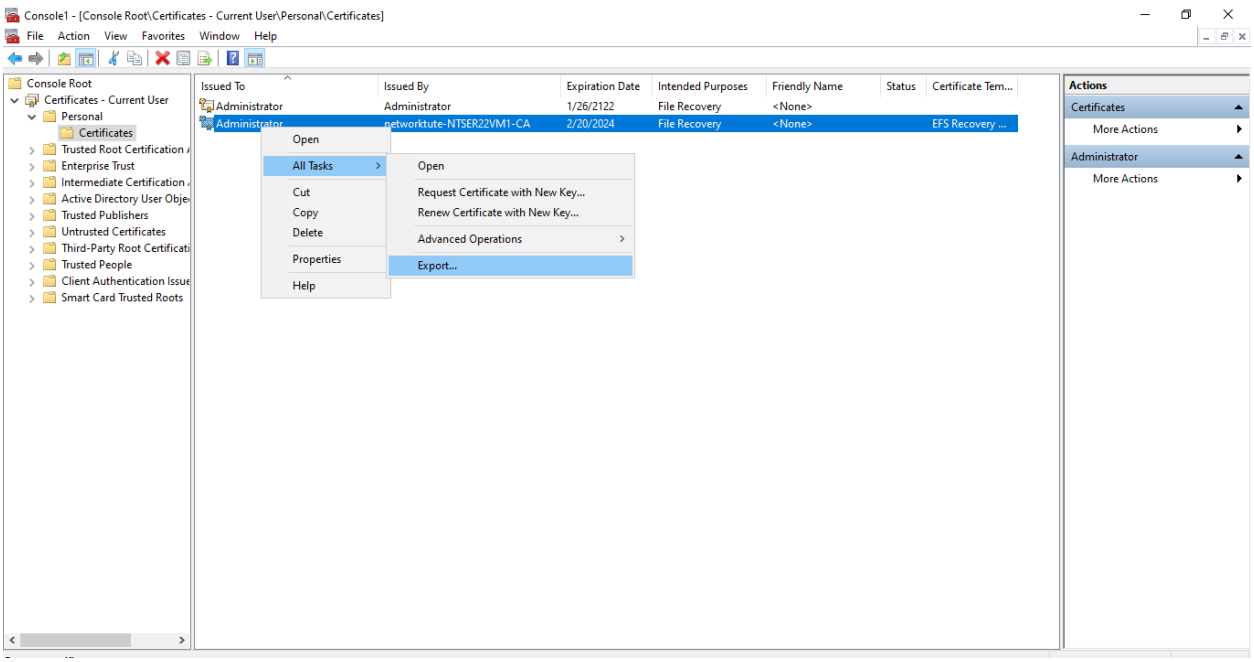
Back in the **Console1** window, check you are in the **Console Root > Certificates - Current User > Personal.**

Click on the **Certificates** folder.

Notice that two certificates are shown in the right-hand details pane.

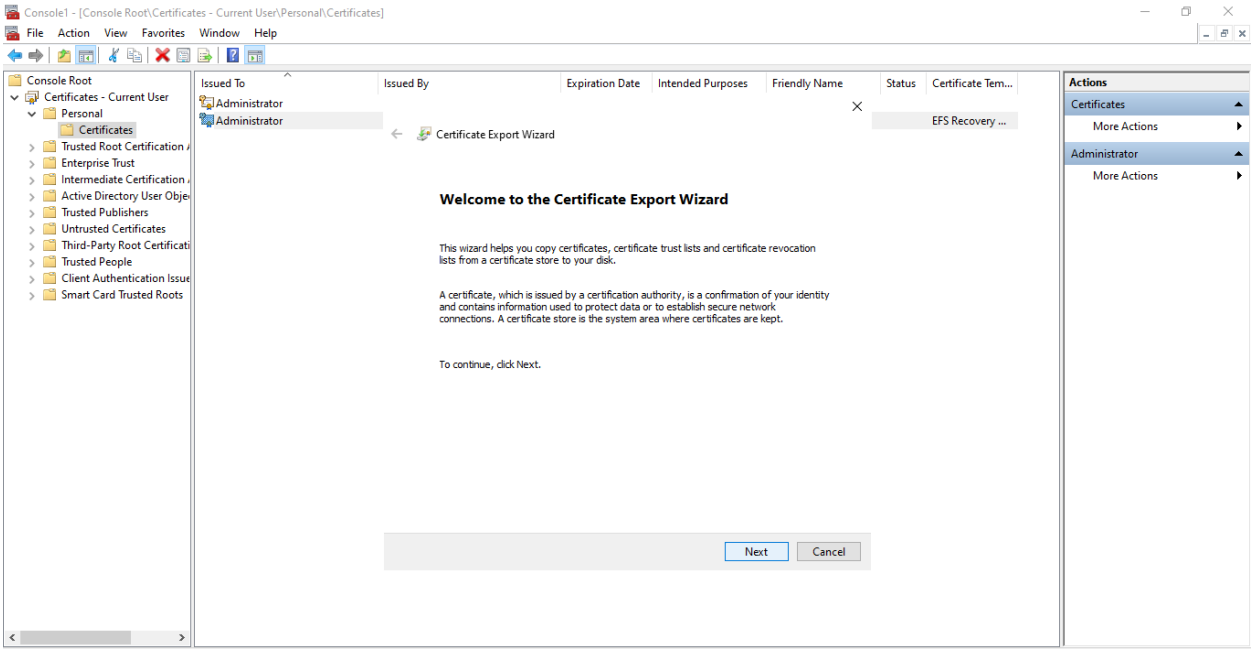
Right-click the certificate with **NETWORKTUTE-NTSER22VM1-CA** in the **Issued By** column.

Point to **All Tasks** and select **Export….**



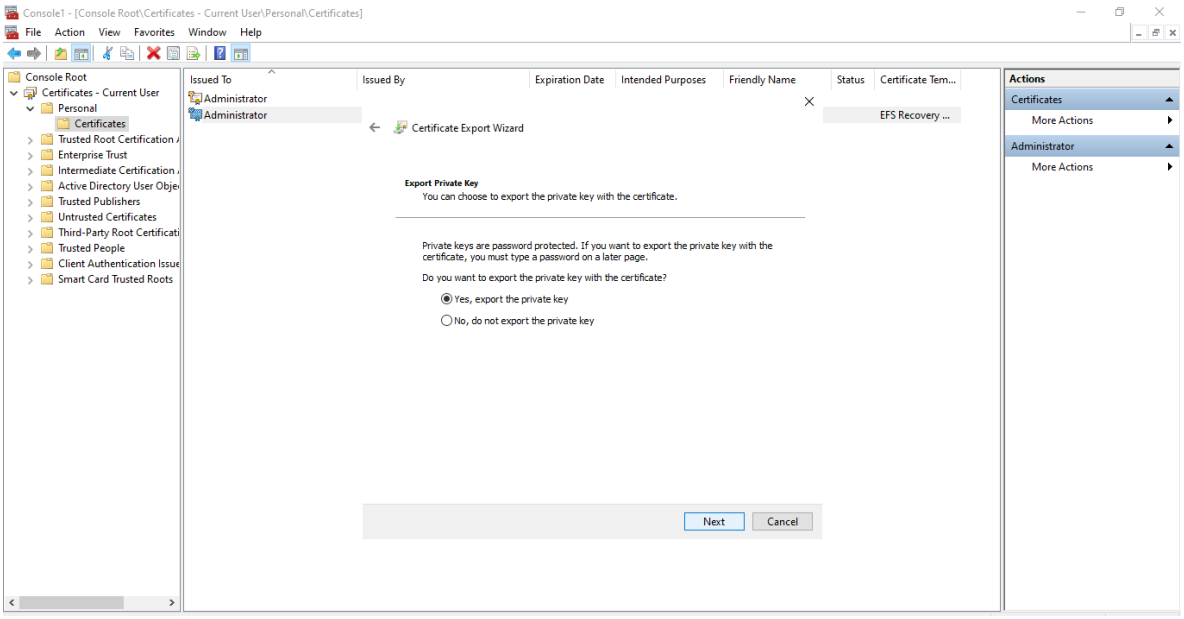
Step 2:

On the **Welcome to the Certificate Export Wizard** page, click **Next.**



Step 3:

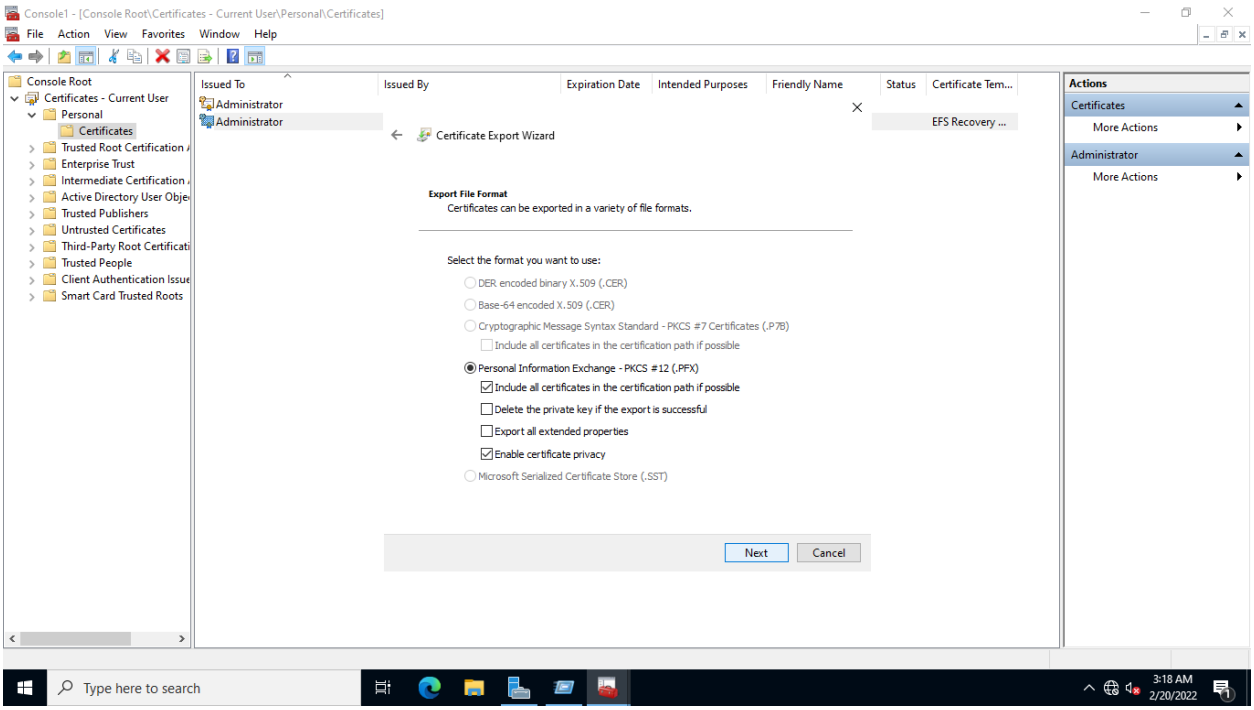
On the **Export Private Key** page, select **Yes, export the private key**, and click **Next**.



Step 4:

On the **Export File Format** page, notice that the **.pfx** format is selected by default.

Click **Next.**



Step 5:

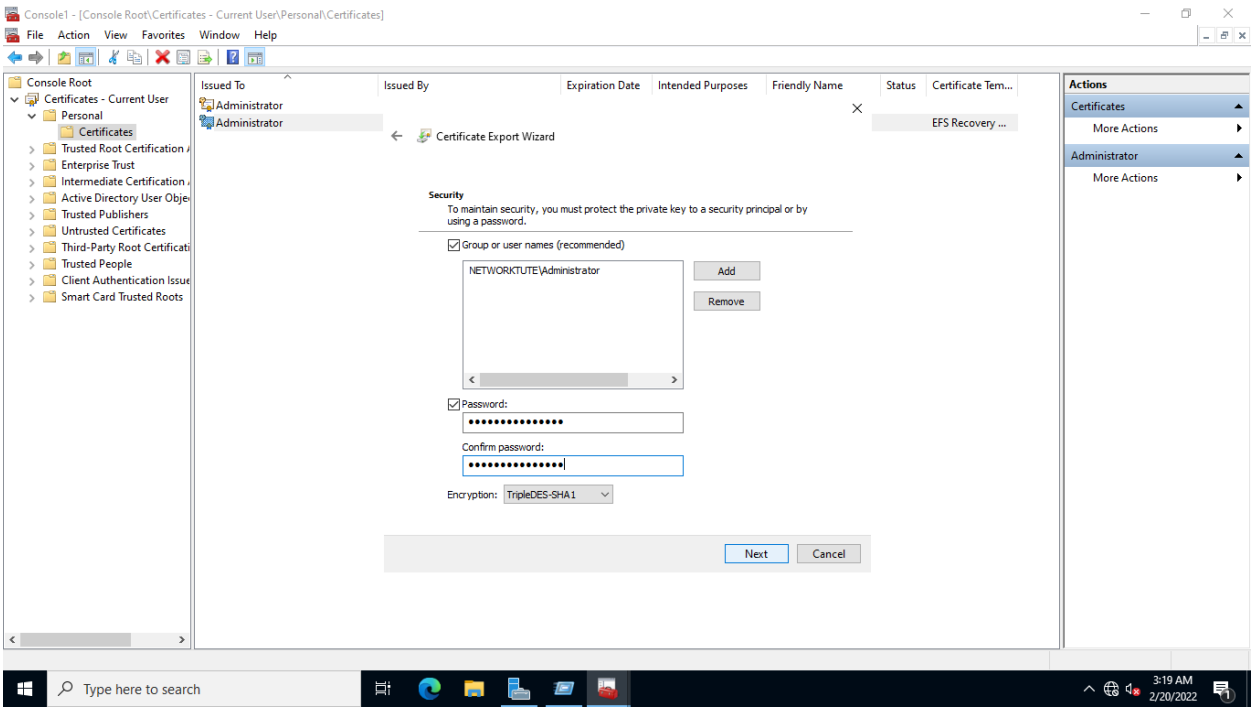
On the **Security** page, tick the **Group or user names (recommended)** checkbox.

The user account NETWORKTUTE**Administrator** appears.

Tick the Password checkbox, in the Password and Confirm password textboxes, type:

Networktute@123

Click **Next**.

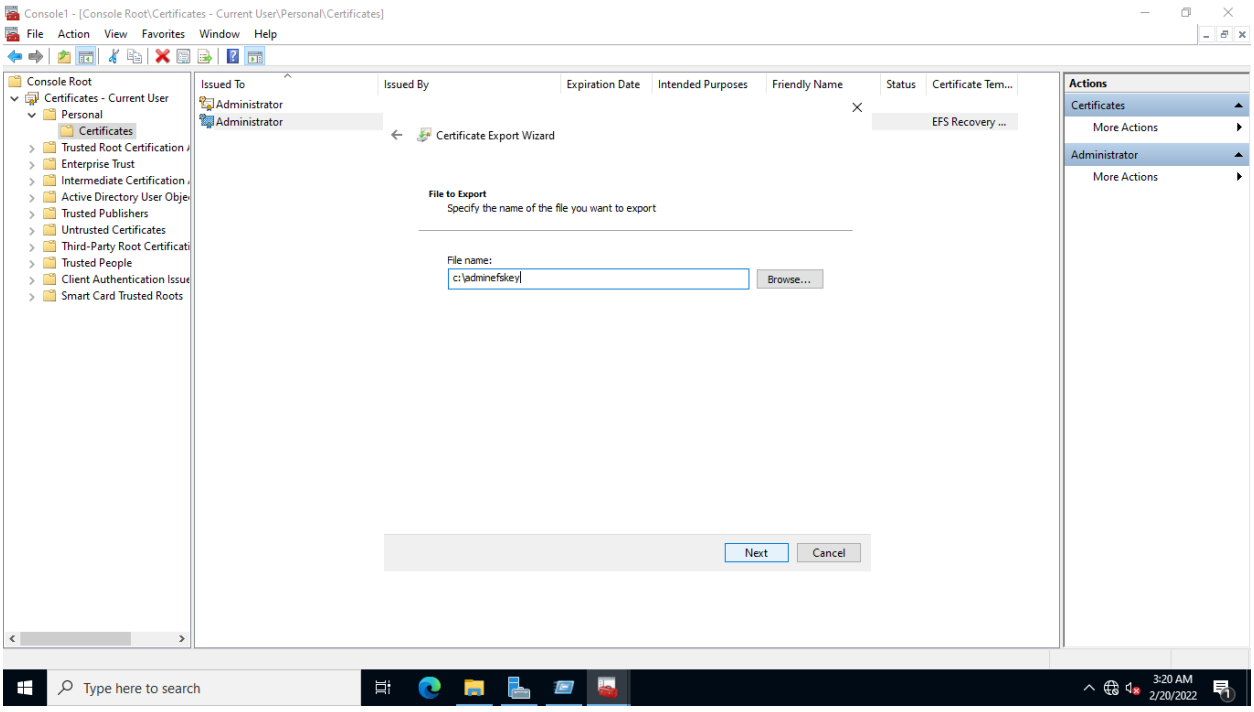


Step 6:

On the **File to Export** page, type the following in the **File name** textbox:

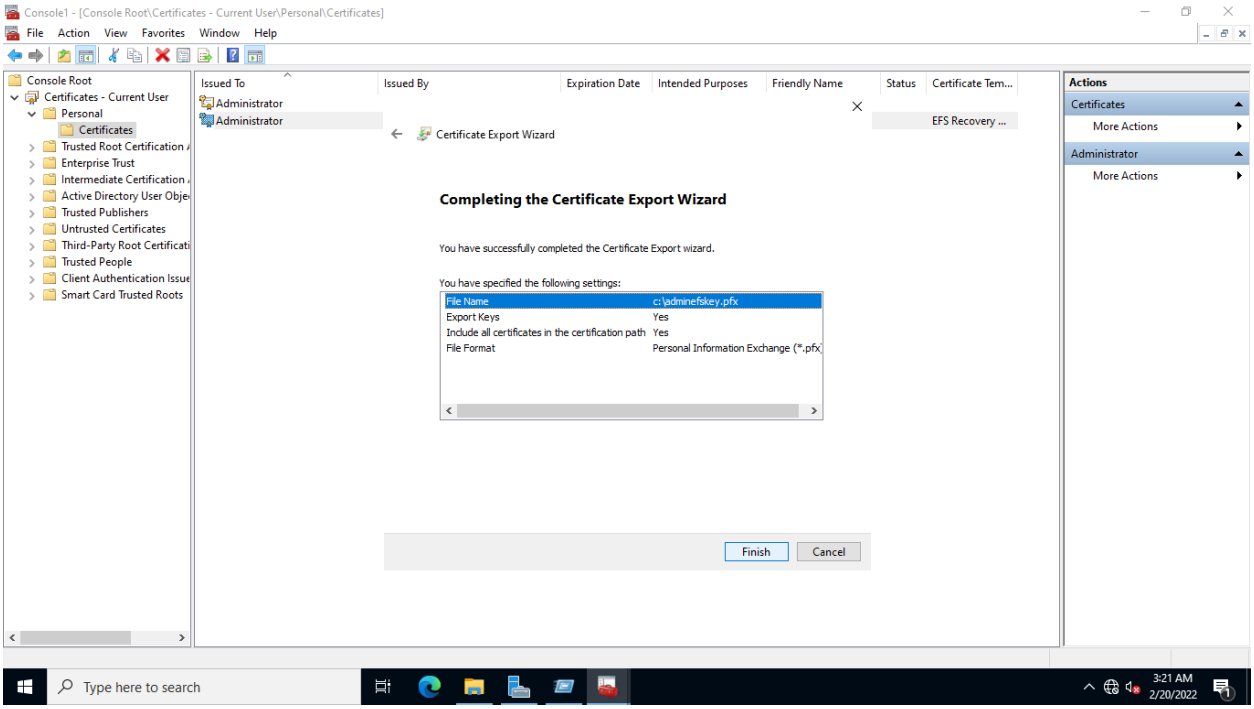
c:\adminefskey

Click **Next.**



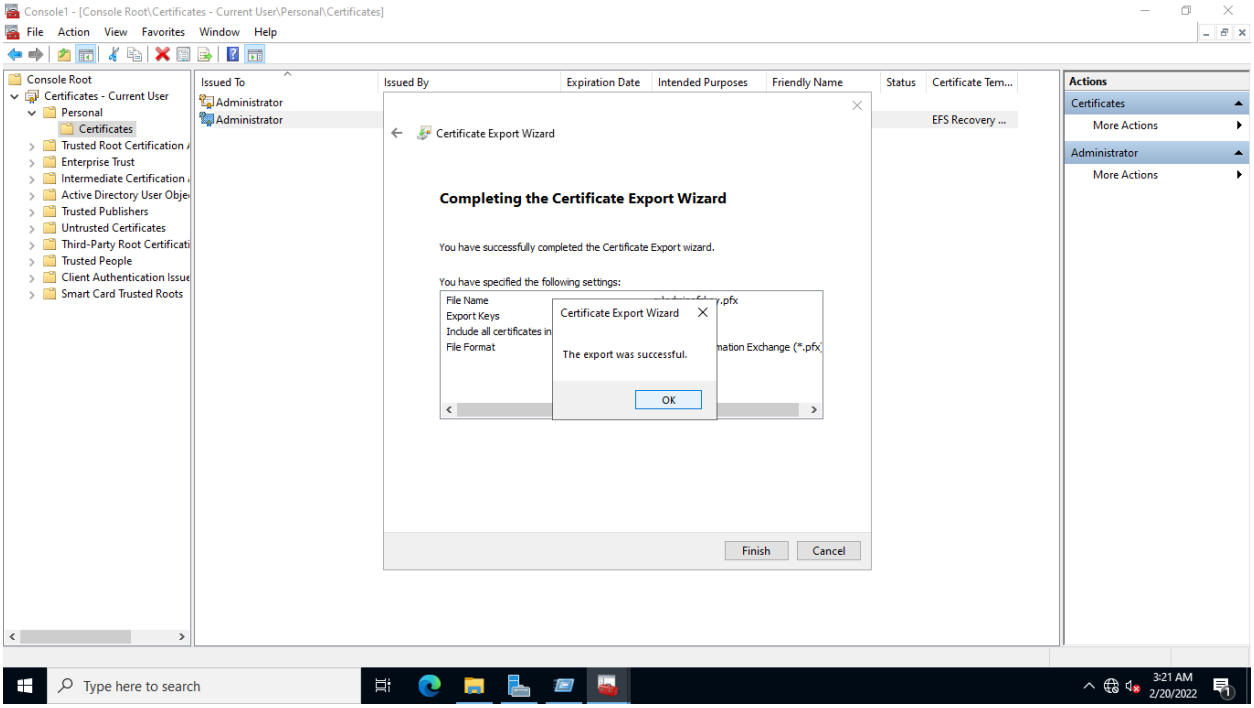
Step 7:

On the **Completing the Certificate Export Wizard** page, click **Finish**.



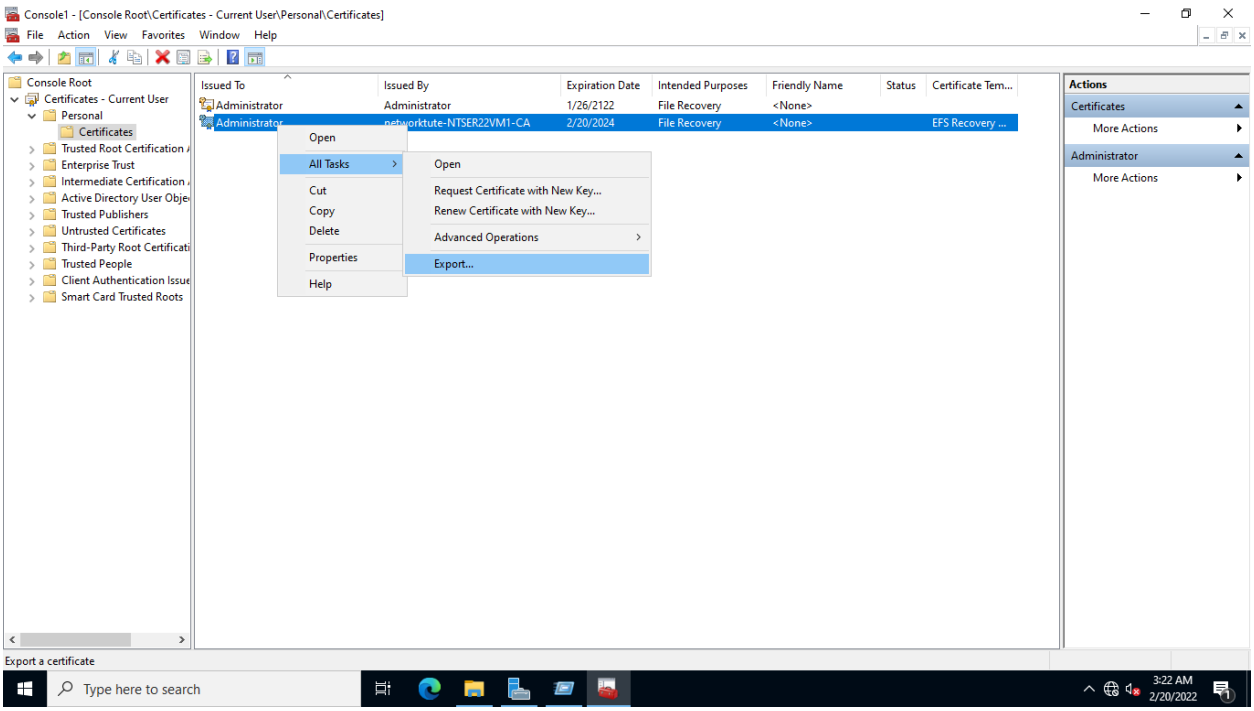
Step 8:

Click **OK** when prompted that the export was successful.



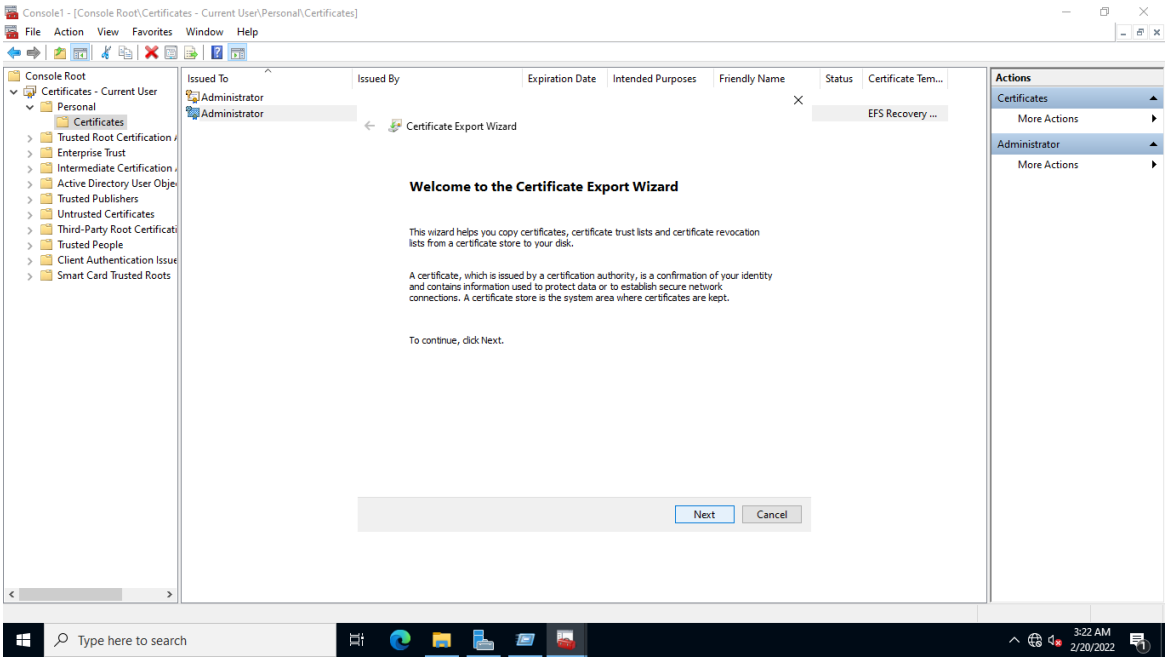
Back in the **Console1** window, again, export the certificate, but without the private key this time.

To export the certificate, again right-click the certificate issued by **NETWORKTUTE-NTSER22VM1-CA**, point to **All Tasks** and select **Export…**



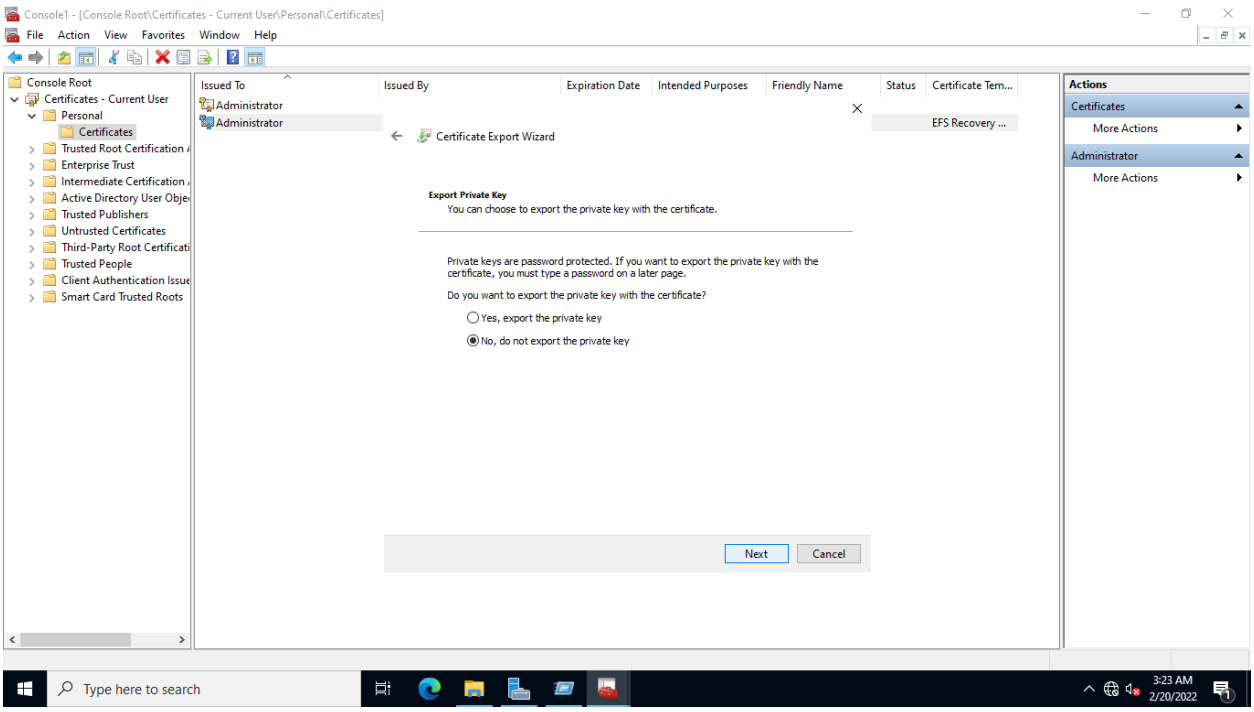
Step 9:

On the **Welcome to the Certificate Export Wizard** page, click **Next.**



Step 10:

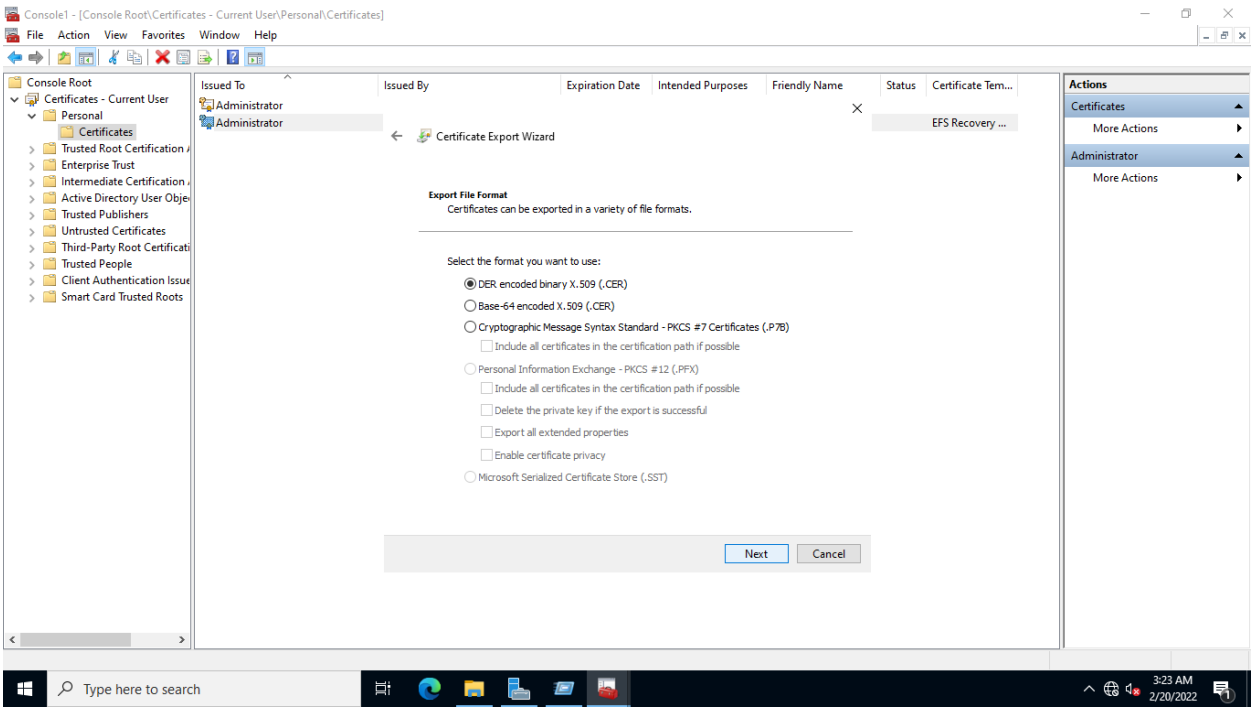
On the **Export Private Key** page, ensure that **No, do not export the private key** is selected and click **Next.**



Step 11:

On the **Export File Format** page, notice that the **.cer** format is selected by default.

Click **Next.**

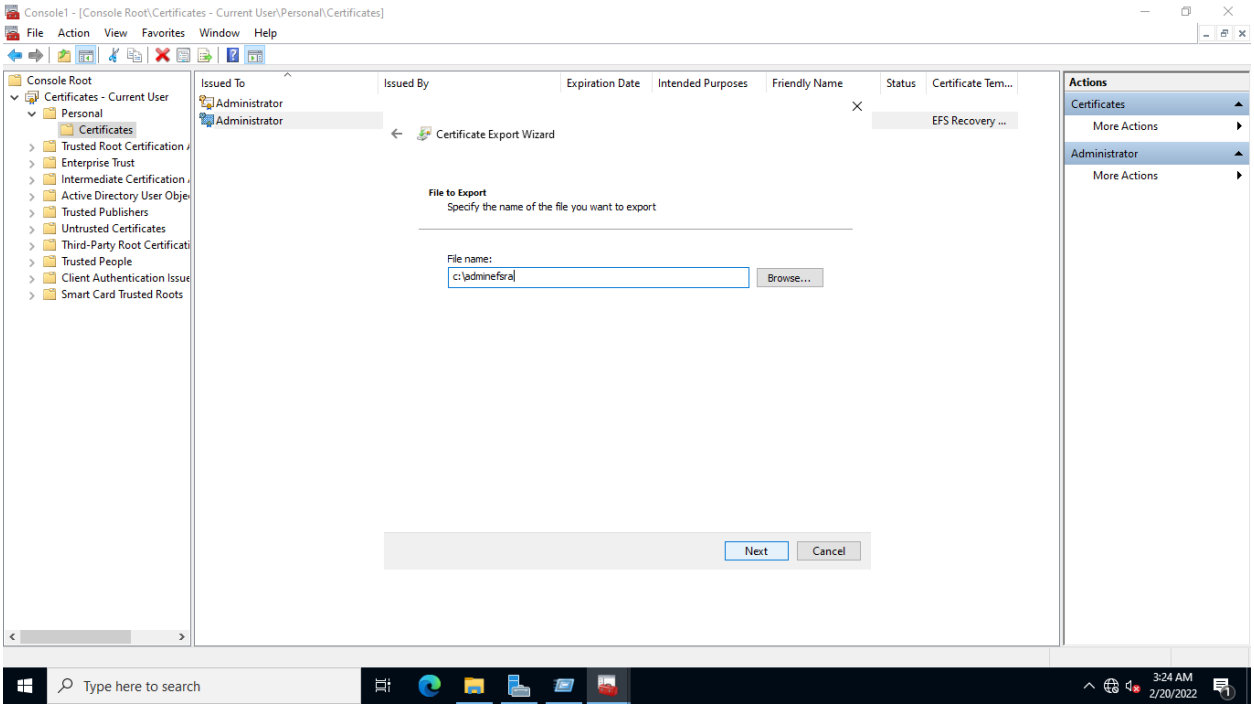


Step 12:

On the **File to Export** page, type the following:

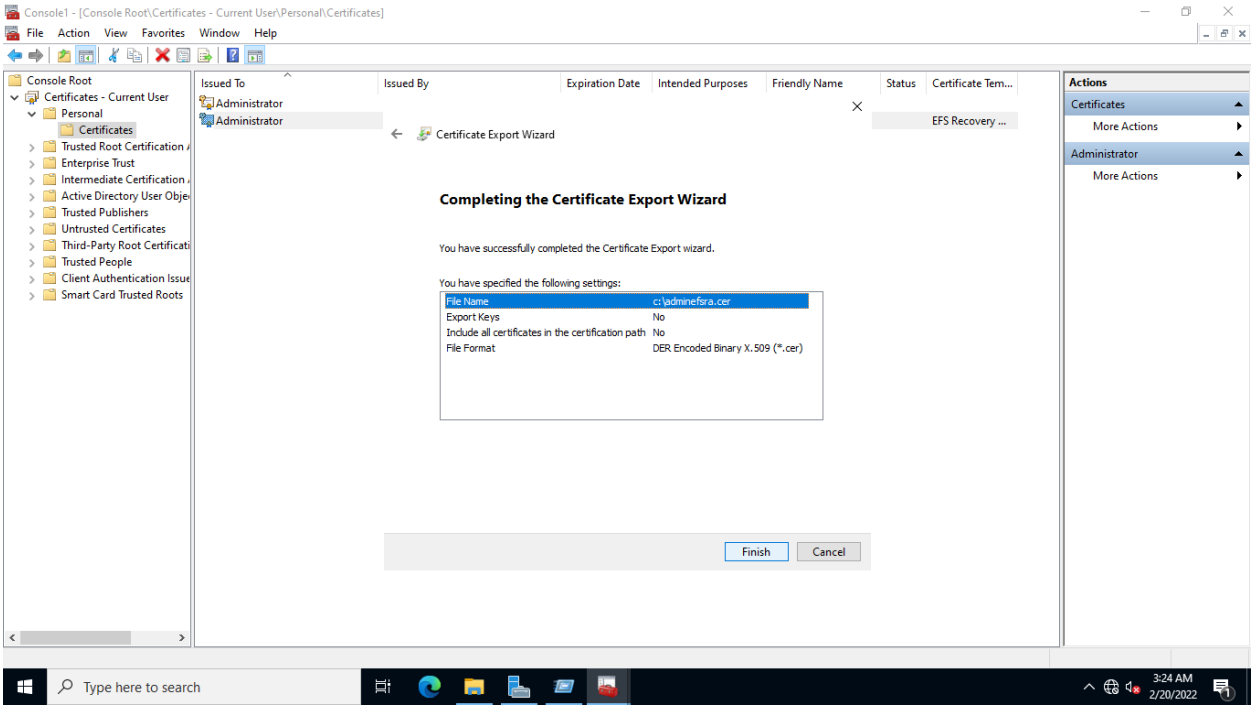
c:\adminefsra

Click **Next.**



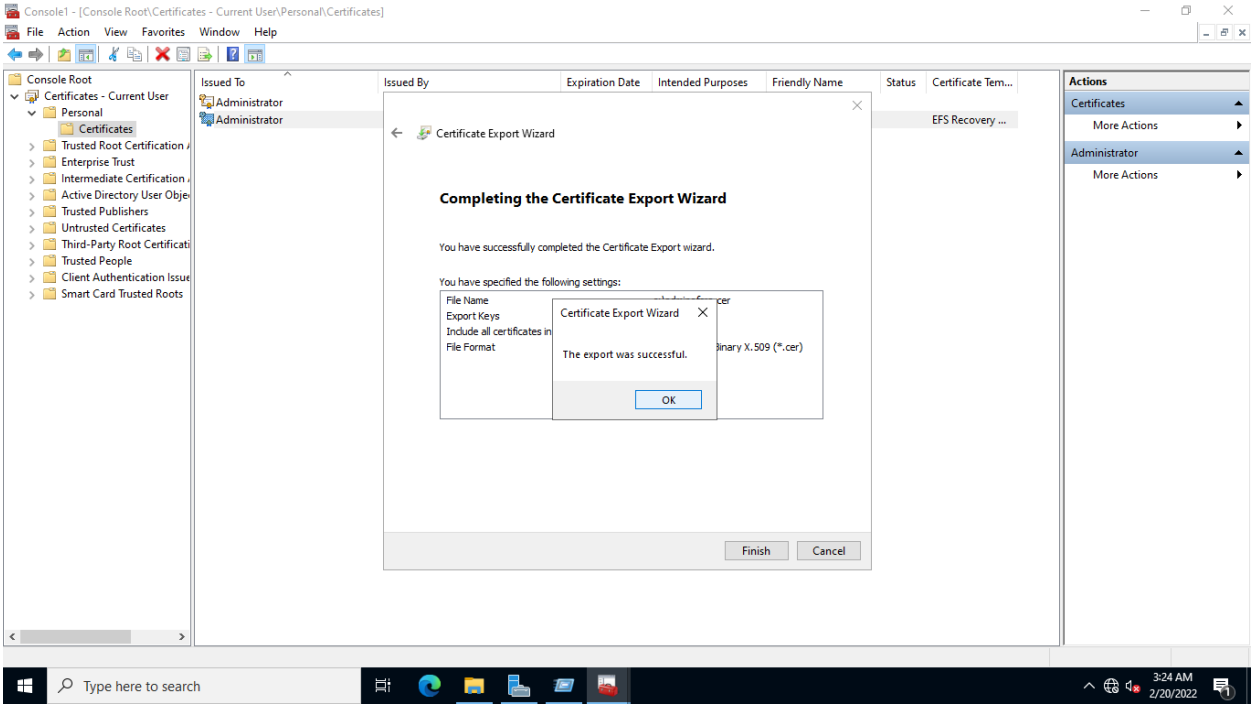
Step 13:

On the **Completing the Certificate Export Wizard** page, click **Finish.**



Step 14:

Click **OK** when prompted that the export was successful.



Minimize the Console1 window.

Task 4: Configure Group Policy for EFS Recovery

After an administrator account has been assigned an EFS recovery agent certificate, the next step is to define an EFS recovery policy for a local machine or an Active Directory Domain network.

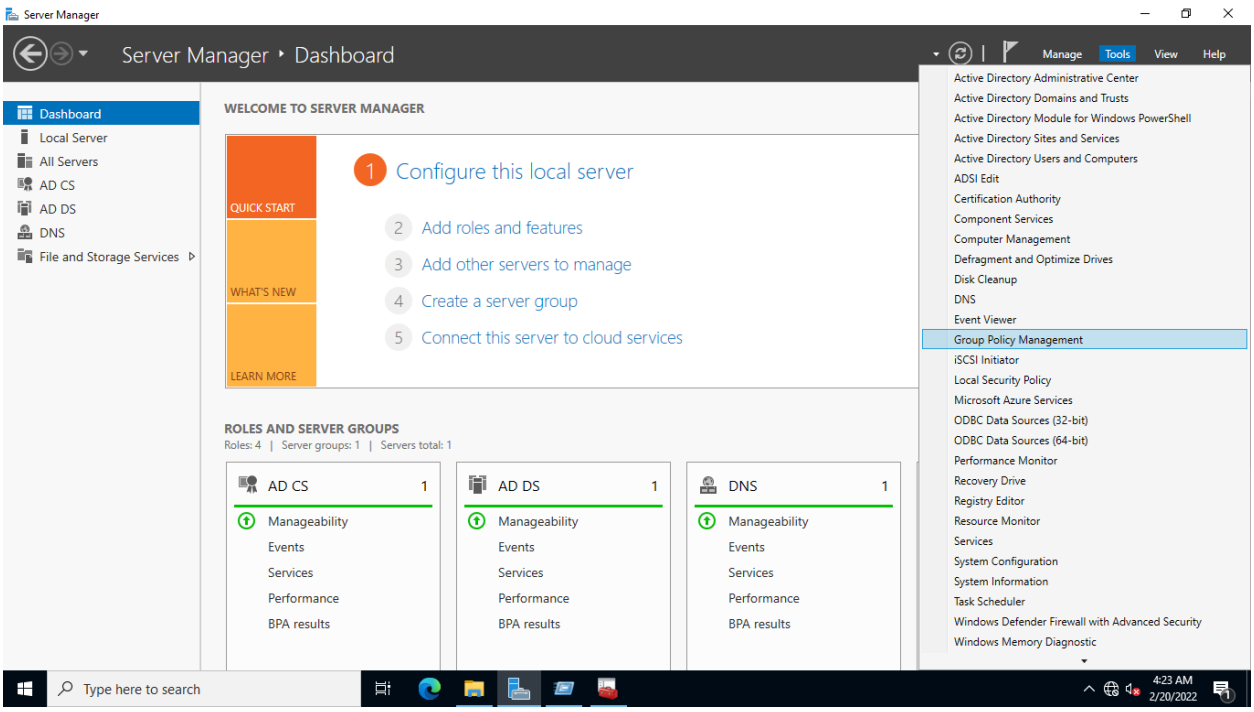
In this task, we will add a data recovery agent to the Group Policy. After that, the newly configured policy will be changed in order to propagate it. After that, the computer will be restarted in order for the policy to take effect.

Step 1:

You are connected to NTSER22VM1.

Click **Server Manager** on the taskbar, if it isn't already open.

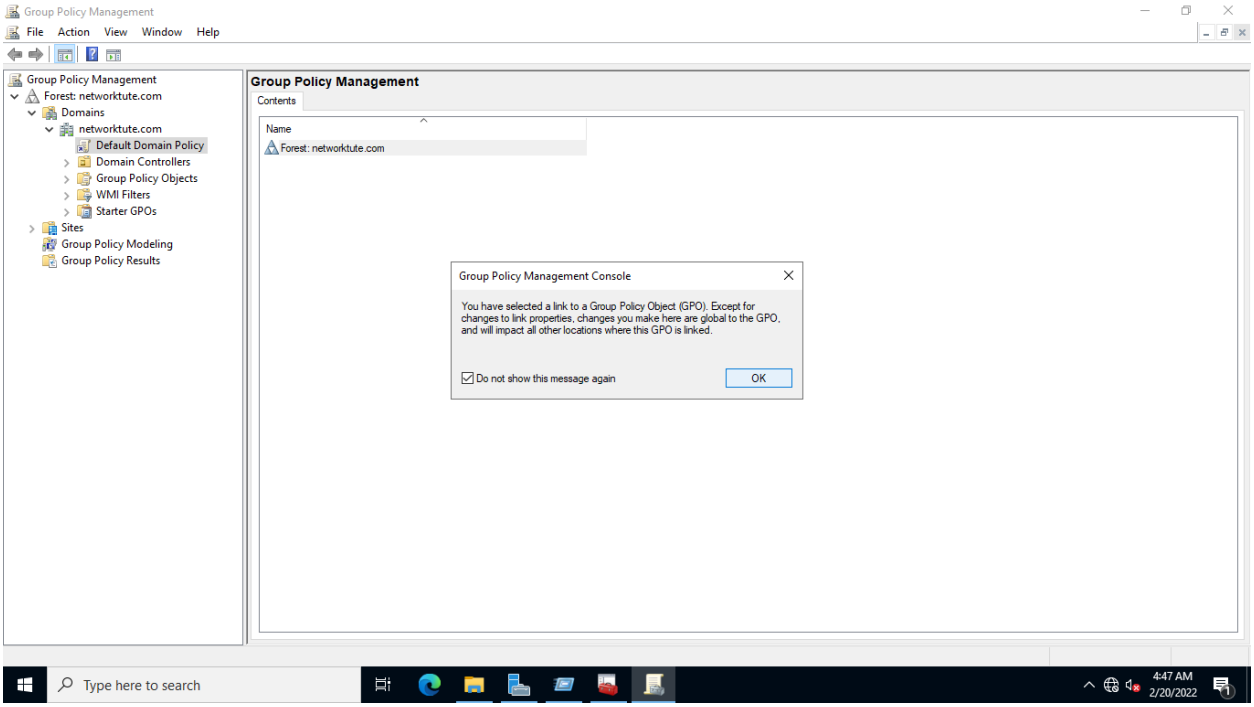
On the **Server Manager** > **Dashboard**, click **Tools** > **Group Policy Management.**



Step 2:

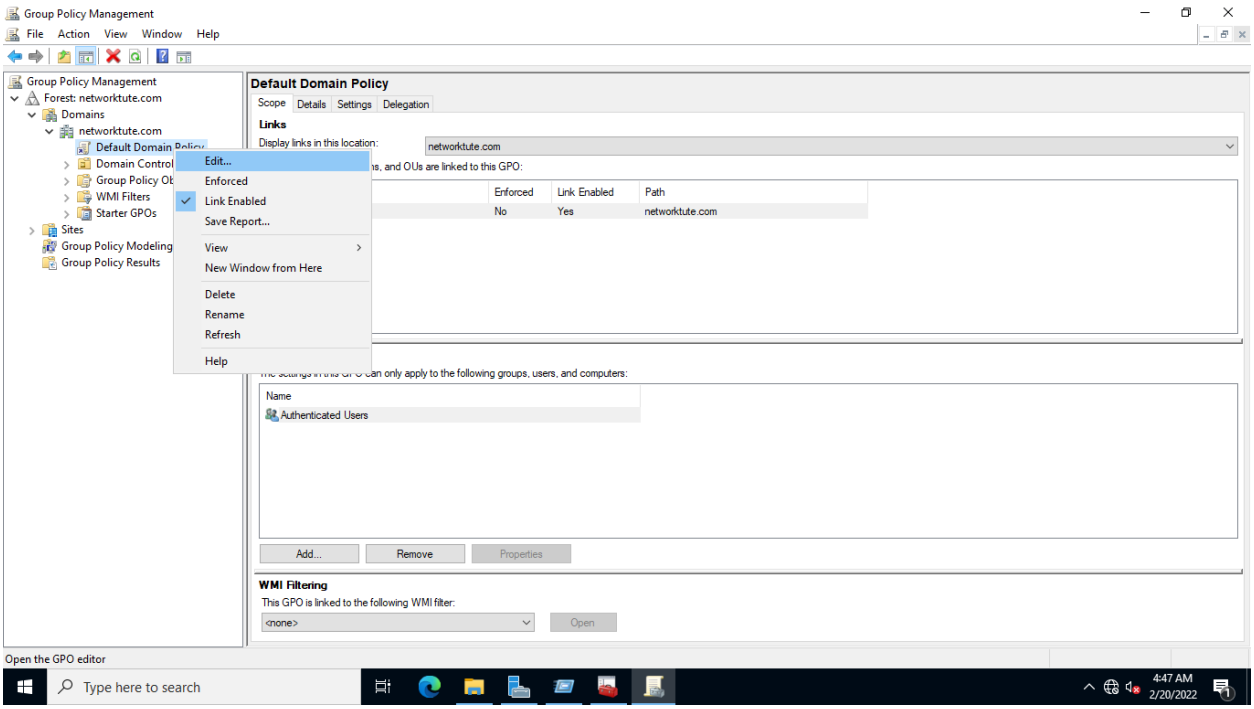
On the **Group Policy Management** console, expand **Forest: Networktute.com** > **Domains** > **Networktute.com** then click **Default Domain Policy.**

Note: If the **Group Policy Management Console** message box, appears, tick **Do not show this message again** box and click **OK**.



Step 3:

Right-click **Default Domain Policy** and select **Edit….**

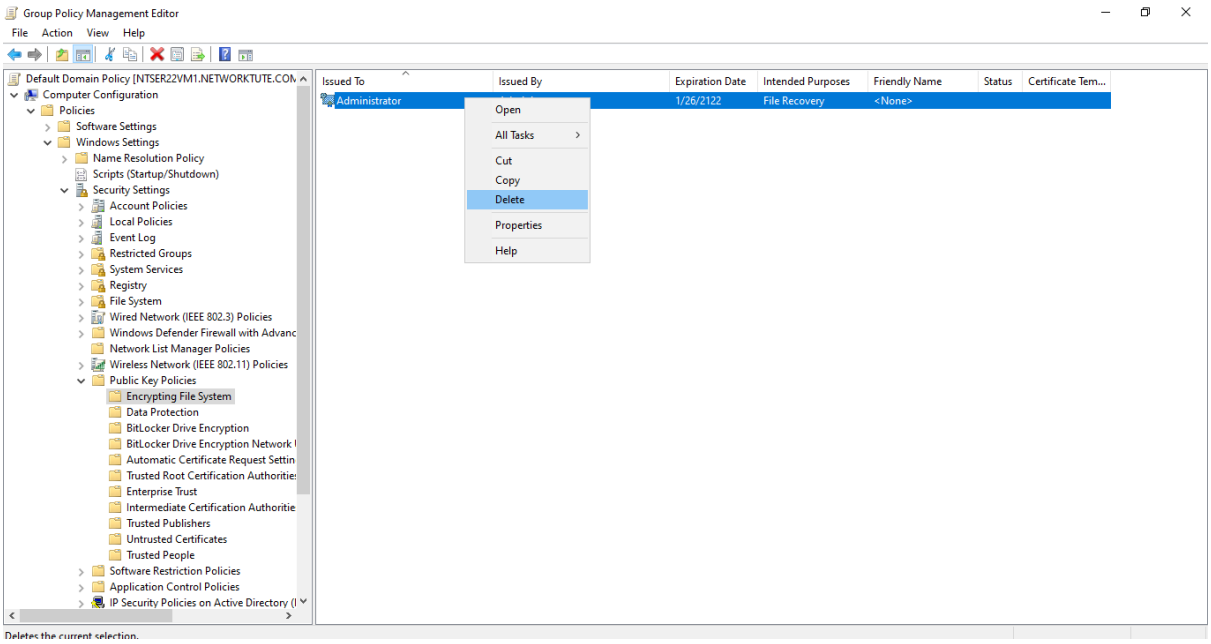


Step 4:

On the **Group Policy Management Editor**, expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** then click **Encrypting File System.**

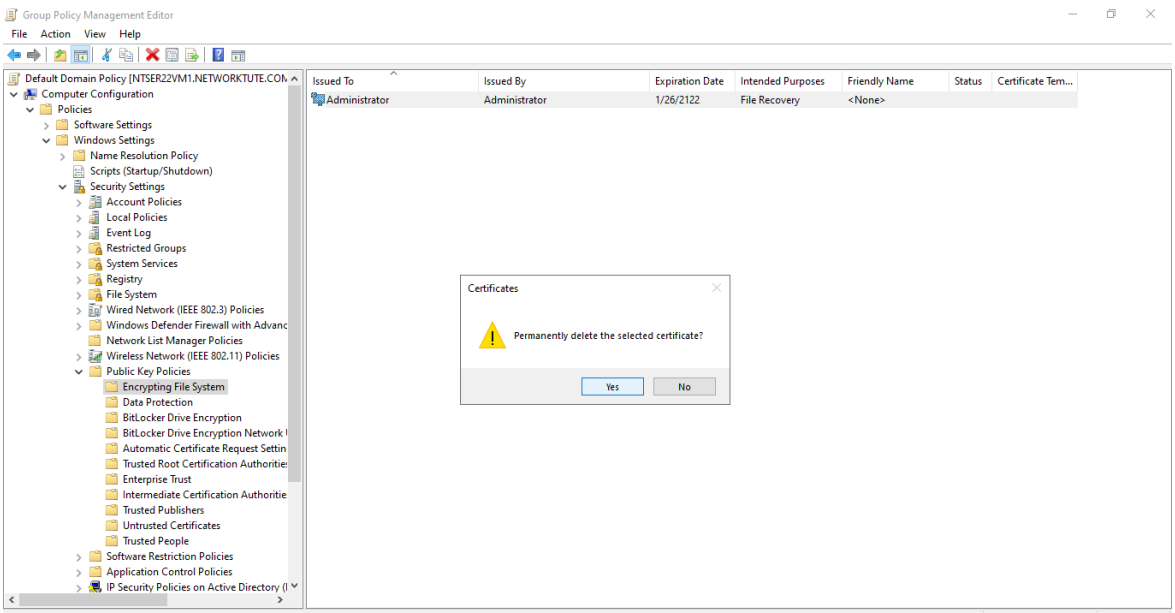
Notice that an Administrator self-issued certificate is present. You will not be using this one as a **NTSER22VM1**-issued certificate was requested earlier.

Right-click the **Administrator** self-issued certificate and click **Delete.**



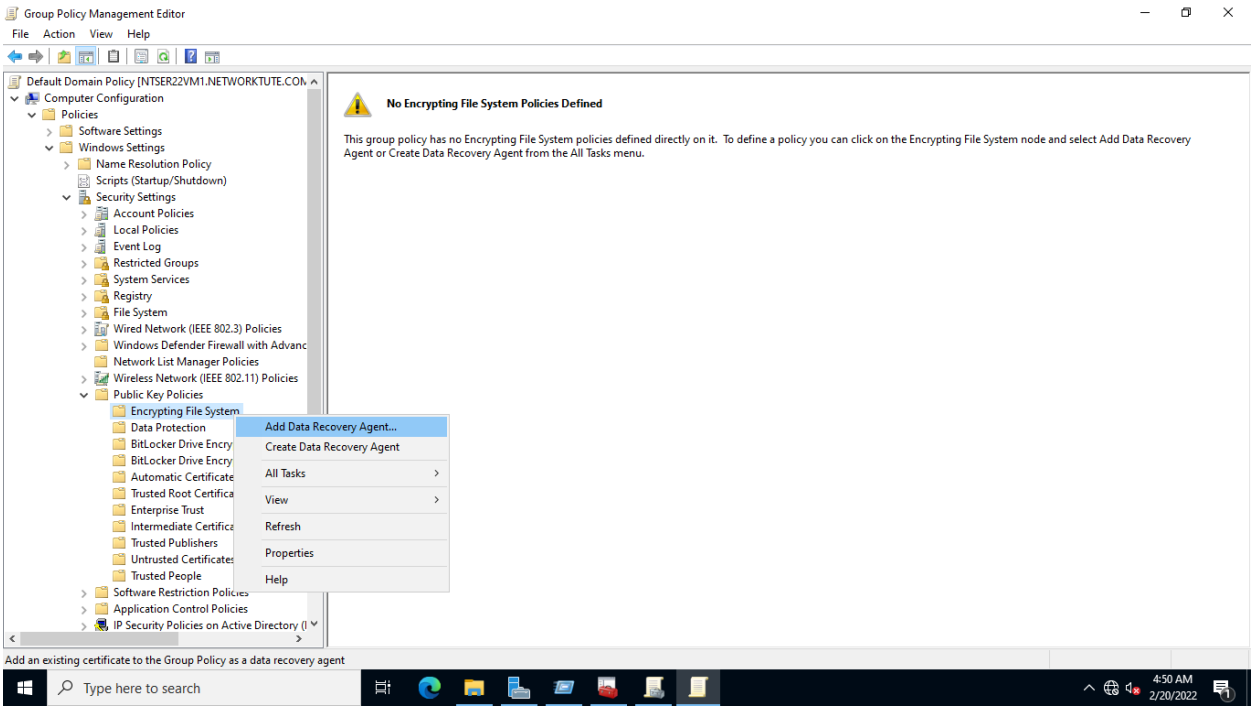
Step 5:

Click **Yes** to continue.



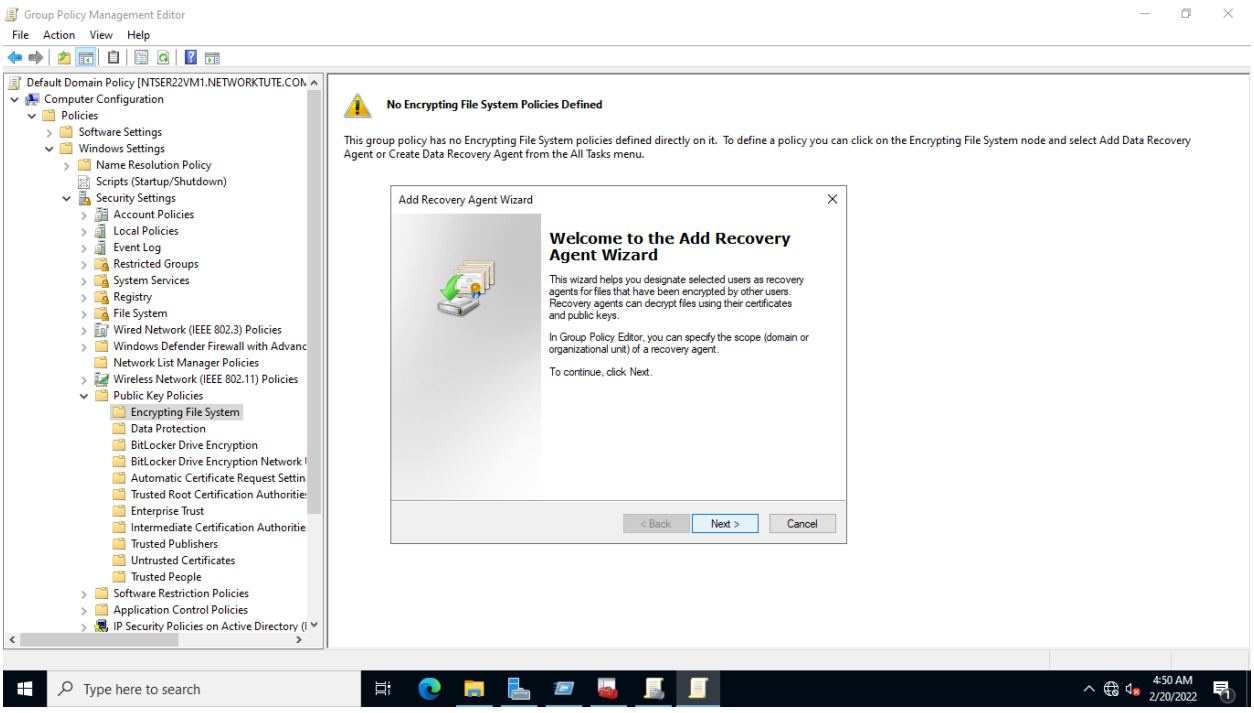
Step 6:

Right-click **Encrypting File System** folder and select **Add Data Recovery Agent….**



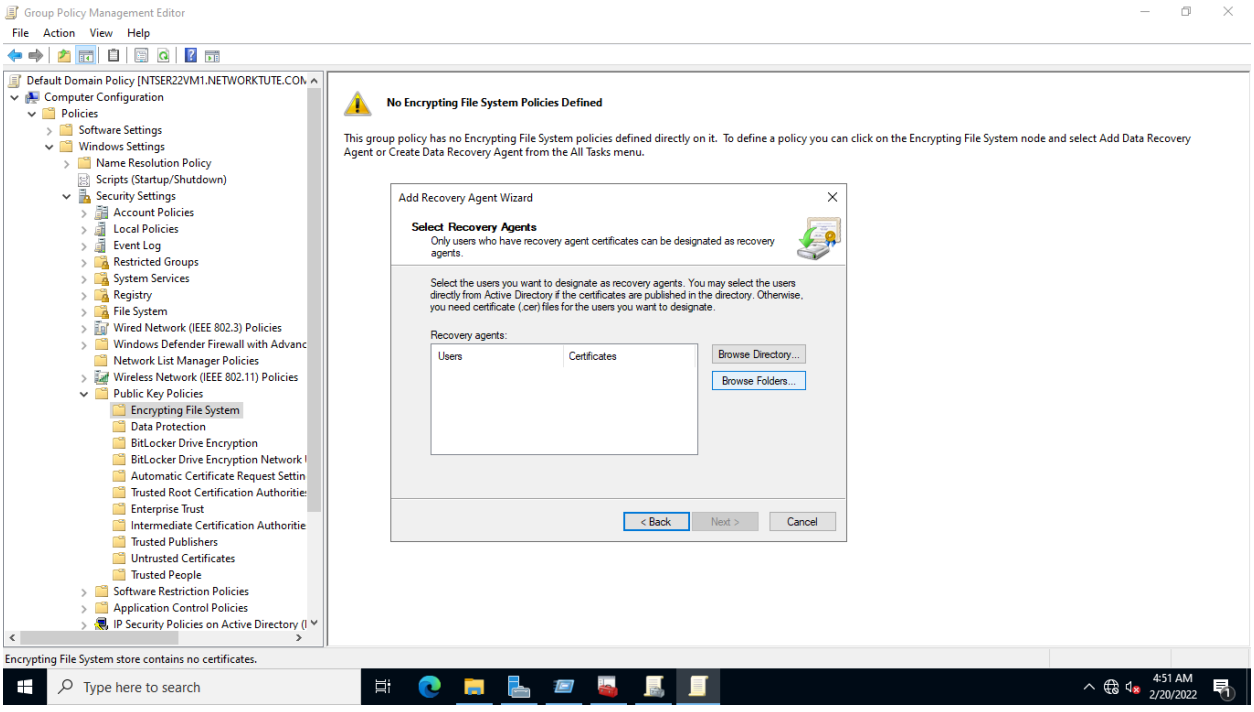
Step 7:

On the **Welcome to the Add Recovery Agent Wizard** page, click **Next.**



Step 8:

On the **Select Recovery Agents** page, click **Browse Folders….**

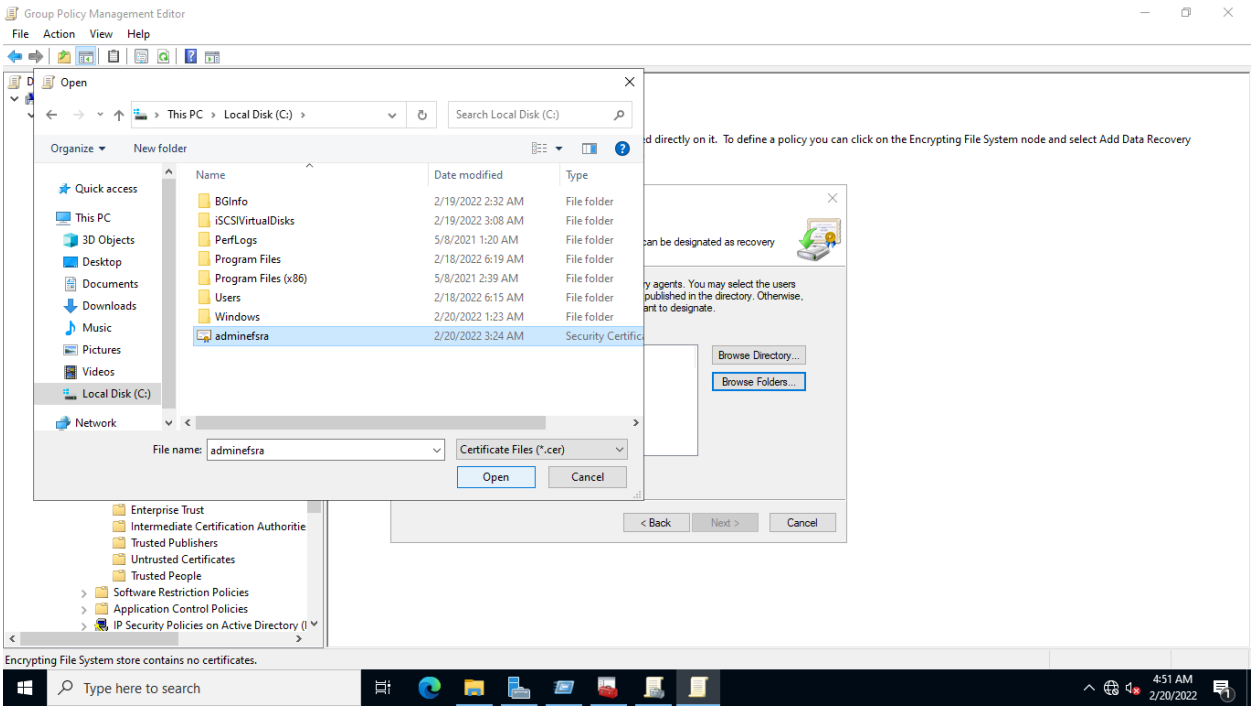


Step 9:

On the **Open** dialog box, navigate to **This PC** > **Local Disk (C:)** path. Then select **adminefsra.**

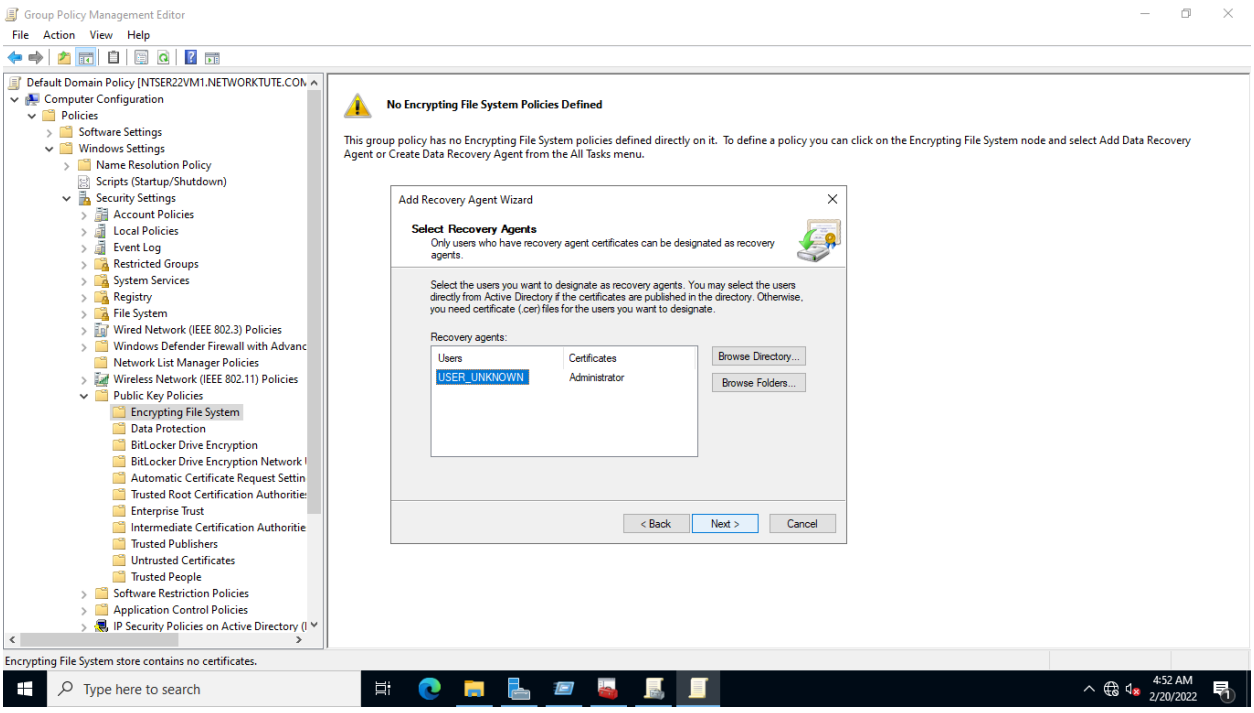
Notice only the **.cer** format - the format to associate with a policy - is listed here.

Click **Open.**



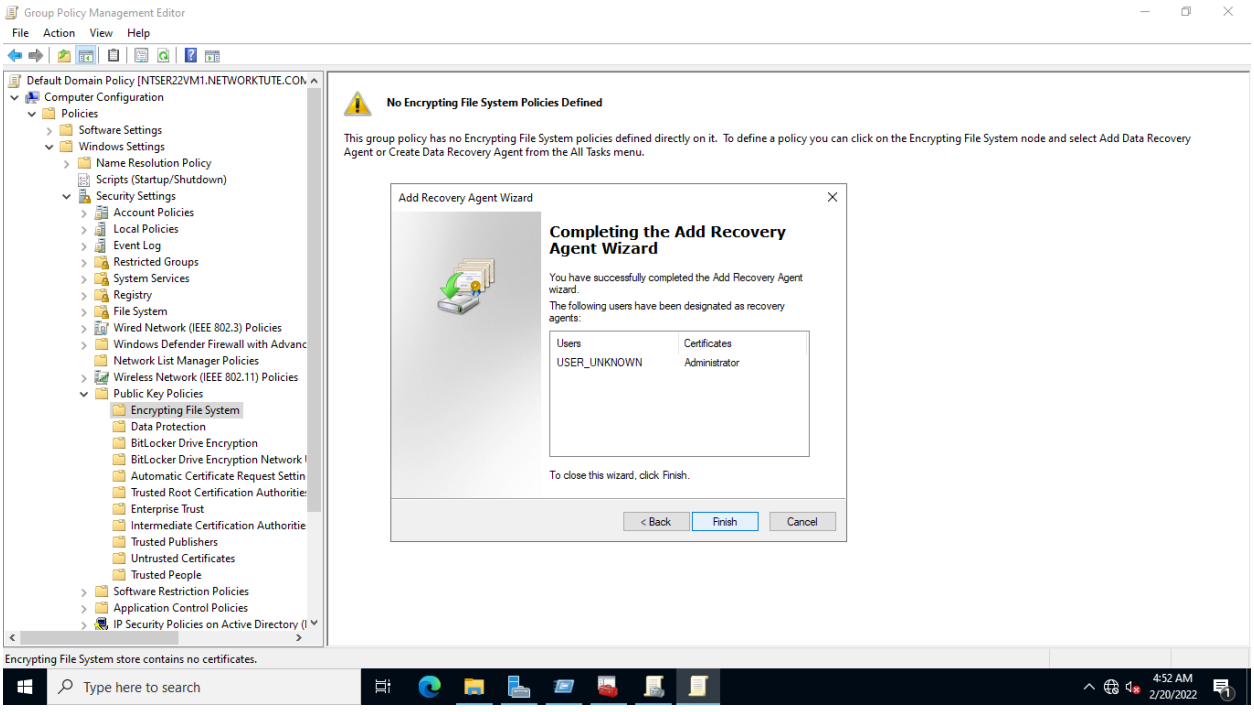
Step 10:

On the **Select Recovery Agents** page, click **Next.**



Step 11:

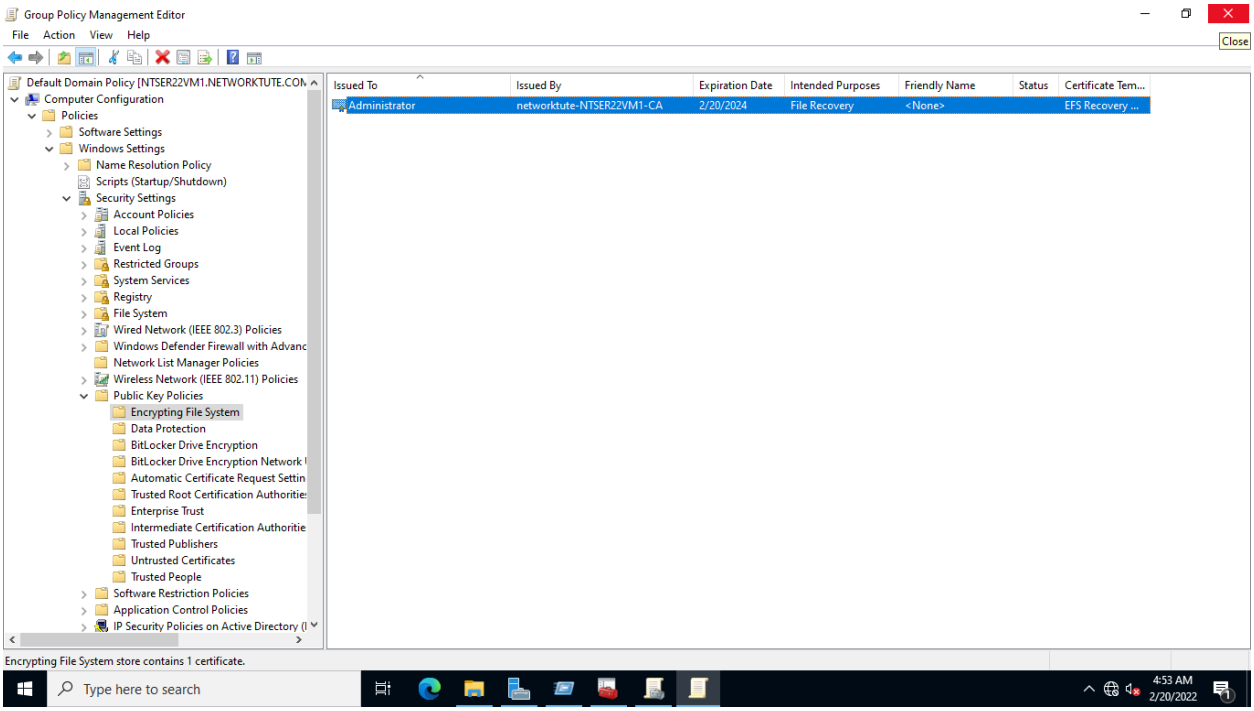
On the **Completing the Add Recovery Agent Wizard** page, click **Finish**.



Step 12:

Back on the **Group Policy Management Editor** window, notice the newly associated certificate - **NETWORKTUTE-NTSER22VM1-CA** is listed.

Close both the **Group Policy Management Editor** and **Group Policy Management** console windows



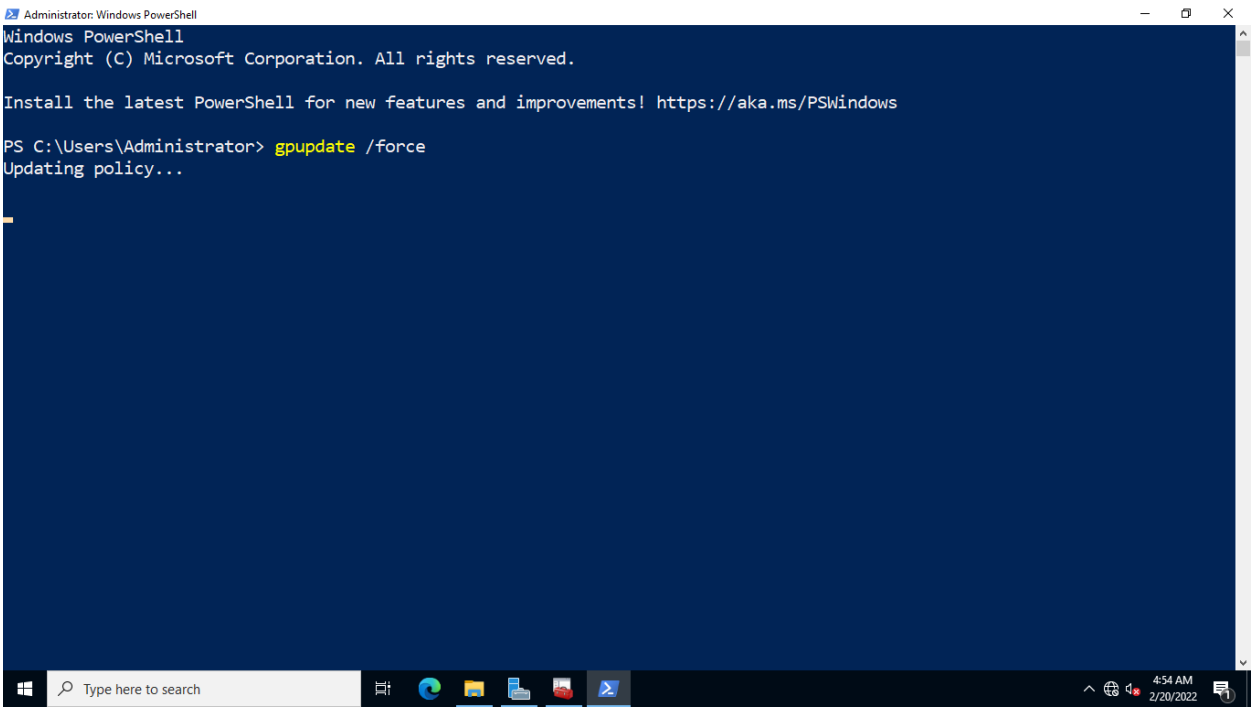
Step 13:

Launch **Windows PowerShell.**

Type the following command to propagate the updated policy:

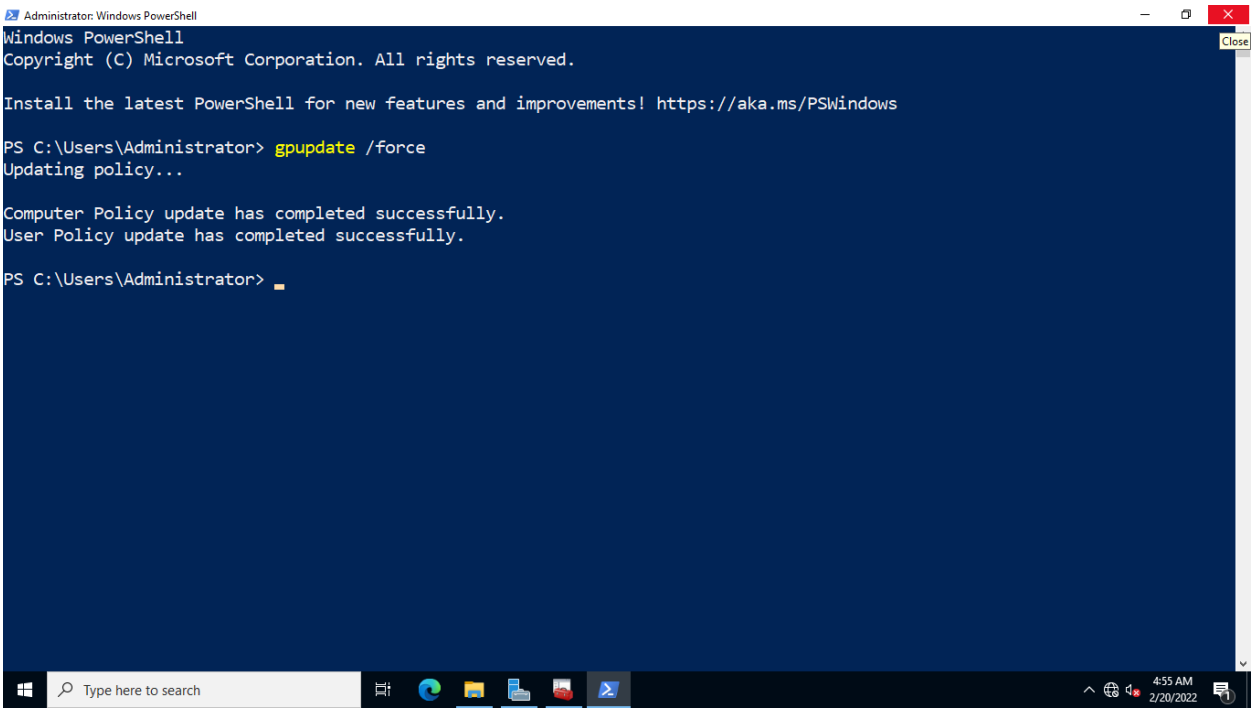
```
gpupdate /force
```

Press **Enter.**



Step 14:

Close **Windows PowerShell** when **Computer Policy** and **User Policy** are successfully updated.



Task 5: Create an EFS Protected File

The domain controller has now propagated the newly defined EFS recovery policy to the domain. You must restart the clients to verify that the policy is identified and executed by the domain members.

You'll need to log in as a regular domain user to see how the policy impacts encrypted documents. After that, you'll build an encrypted file and examine its properties.

Step 1:

On the **NETWORKTUTE** web application, mouse-over the NTWIN11VM1 device.

Click **Reboot.**

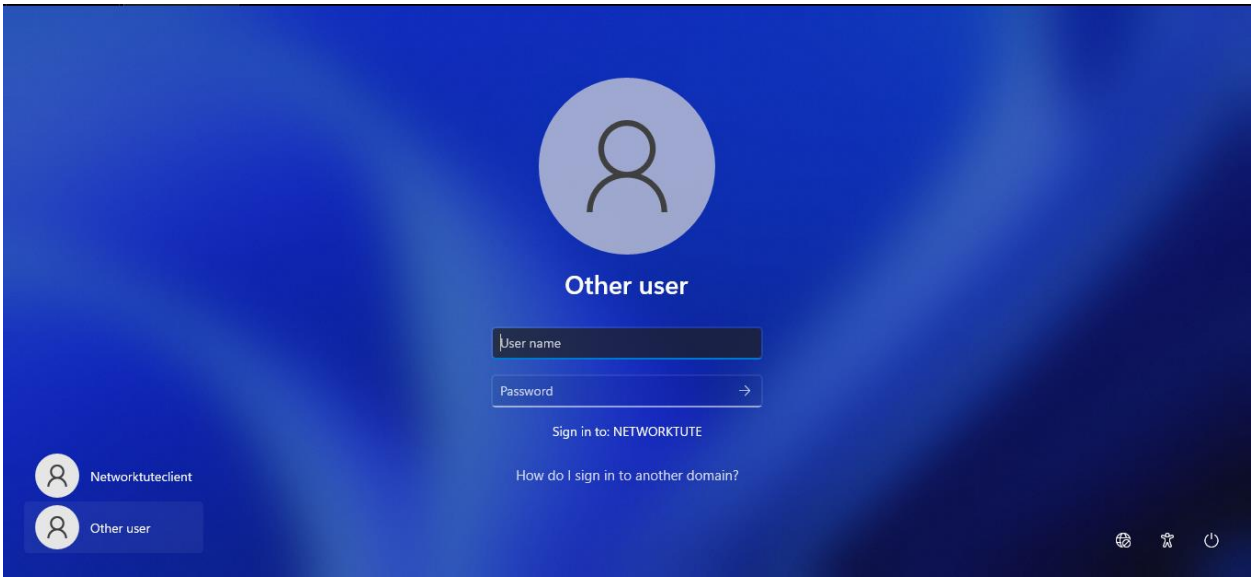
This step is important to enable the **Windows 11** client to become aware of the updated group policy.

For this step, you will also need to ensure your **Server auto login** feature is **disabled** under the Settings and customization tab.

Please see our **help and support > Personal Settings > Settings Tabs** section for more information on how to do this.

After a few minutes, reconnect to **NTWIN11VM1**.

On the sign-in page, click "**Other user**".



Step 2:

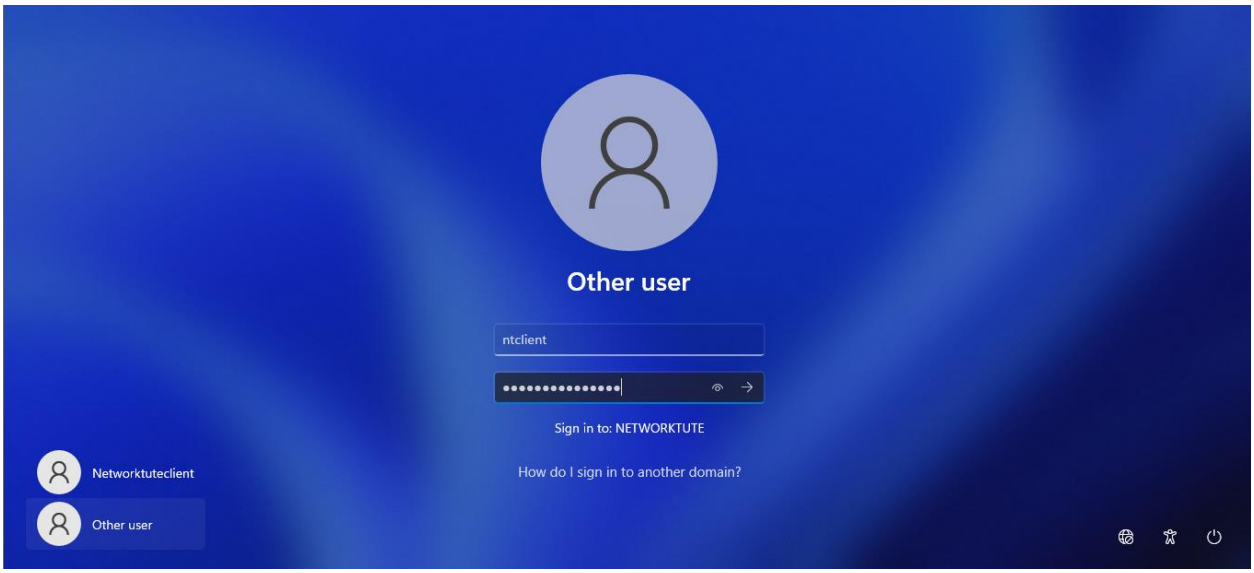
In the **Username** text box, type:

Ntclient

In the Password text box, type:

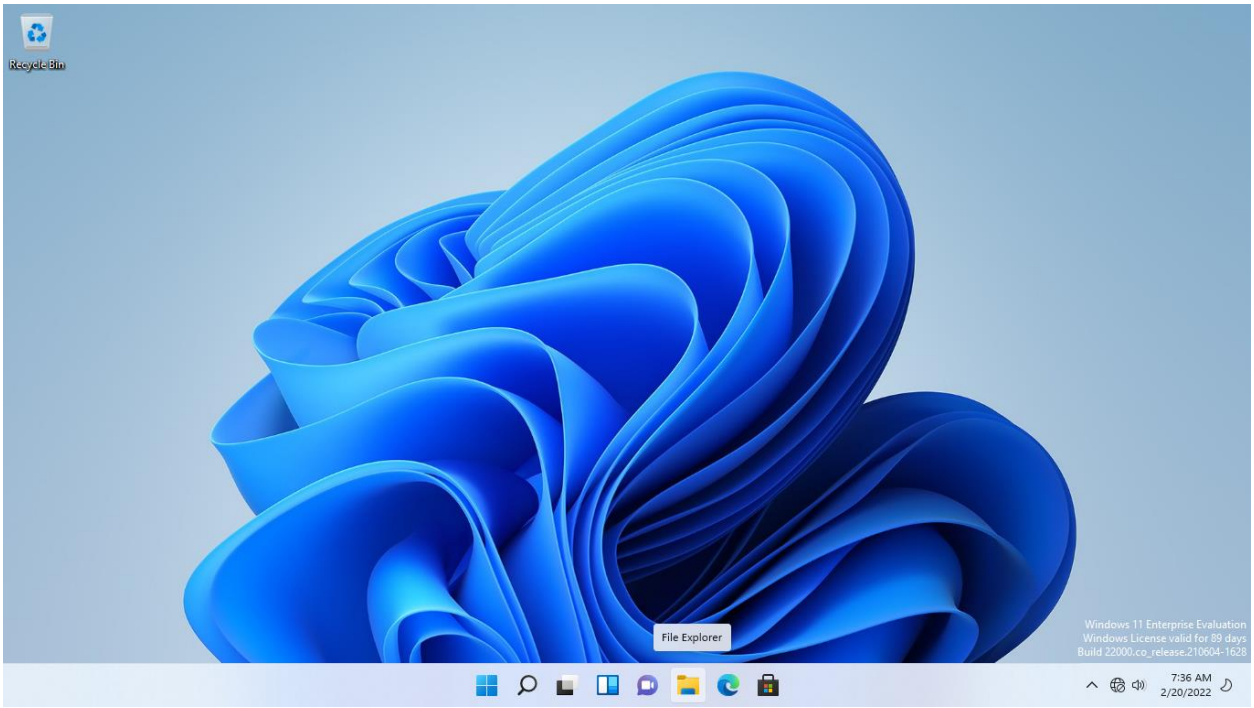
Networktute@123

Press **Enter.**



Step 3:

When logged in, click the **File Explorer** on the Taskbar.

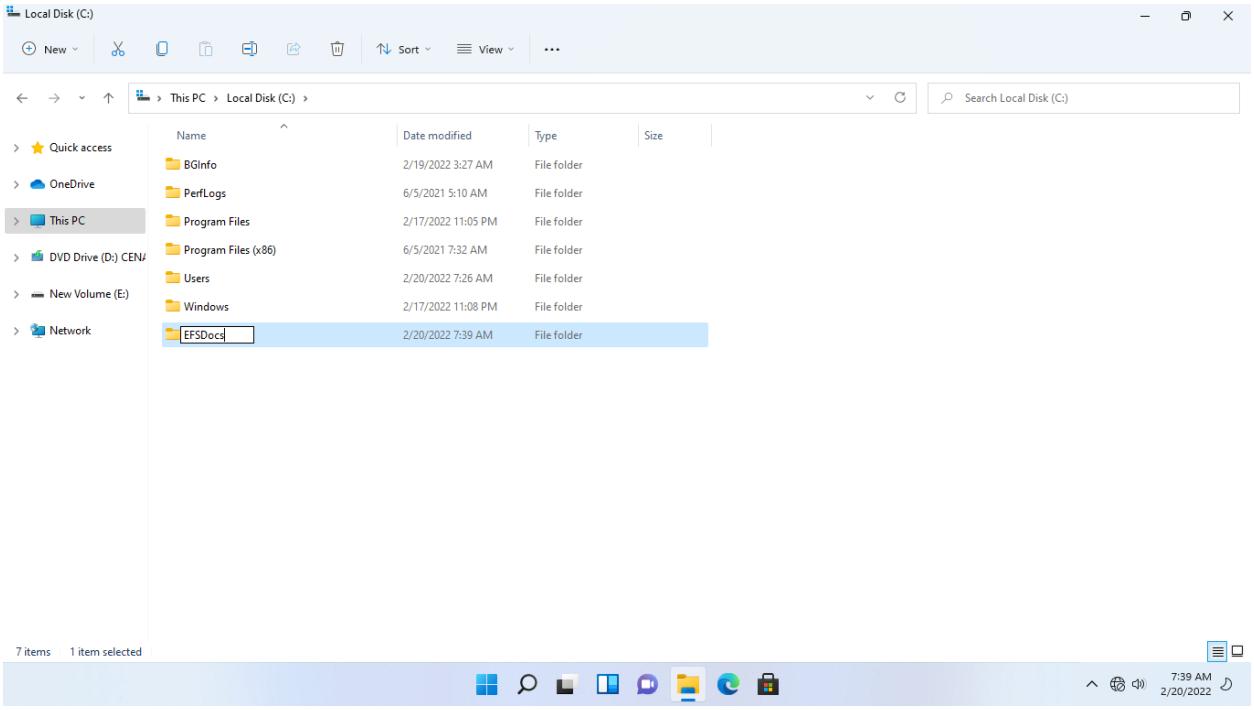


Step 4:

On the **File Explorer** window, expand **This PC** > **Local Disk (C:)** drive.

Right-click **Local Disk (C:)** drive point to **New** and select **Folder.**

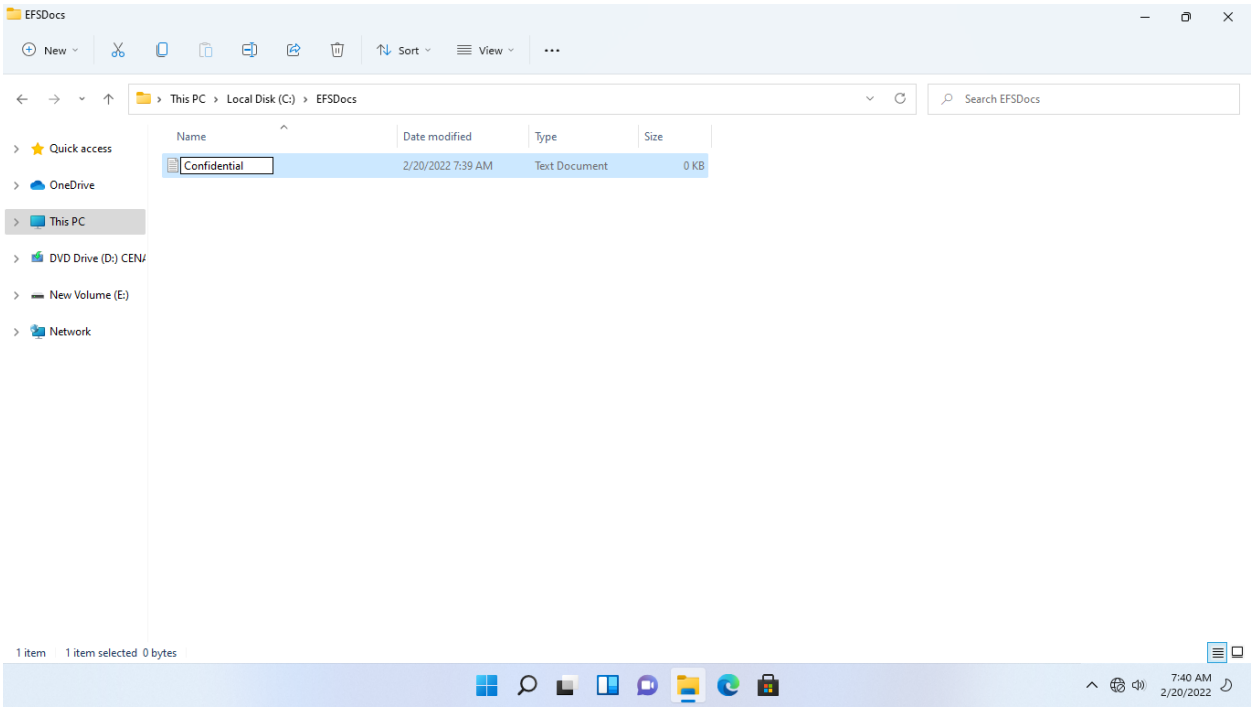
Name the folder as **EFSDocs.**



Step 5:

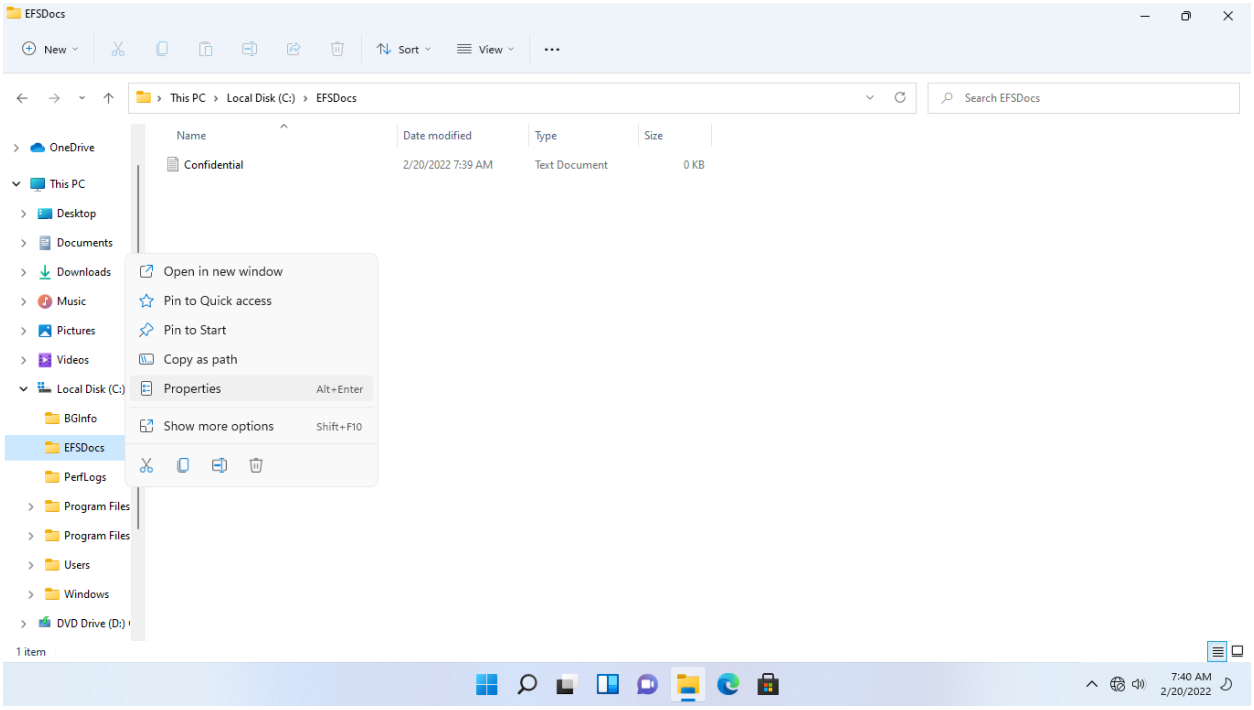
With **EFSDocs** folder selected, go to the details pane at right. Right-click in the blank space and select **New** > **Text Document.**

Name the document as **Confidential.**



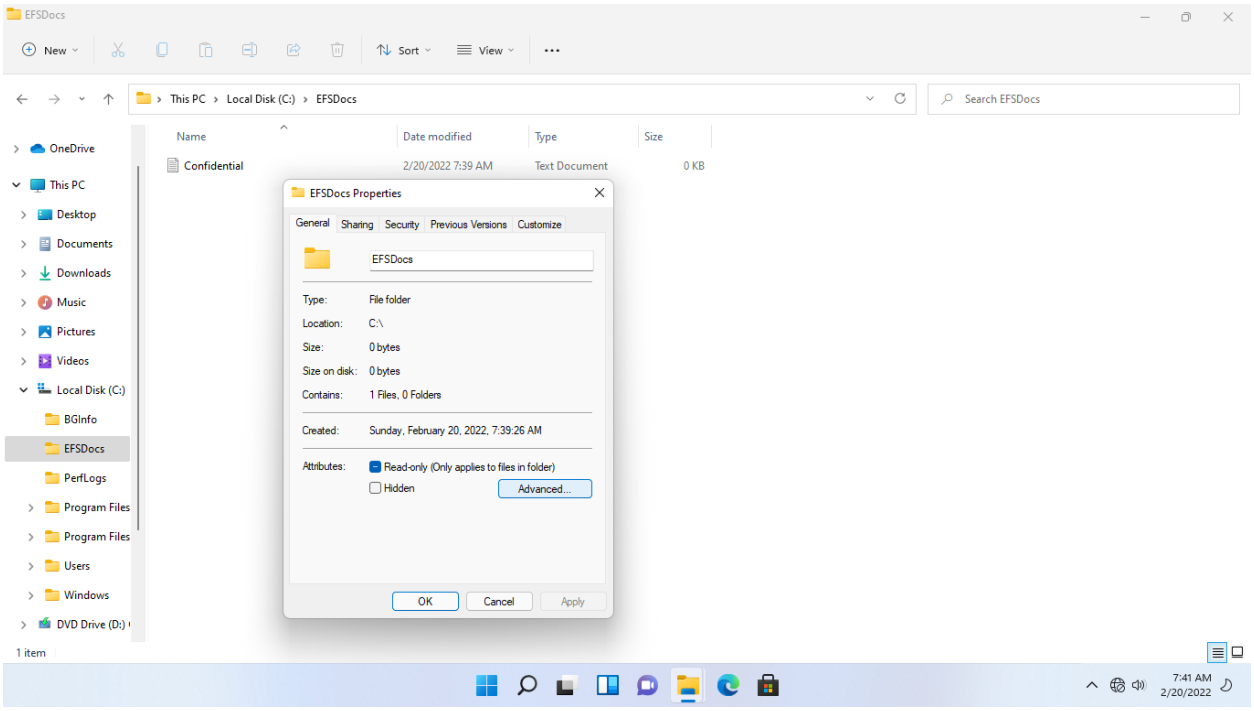
Step 6:

Right-click **EFSDocs** folder and select **Properties.**



Step 7:

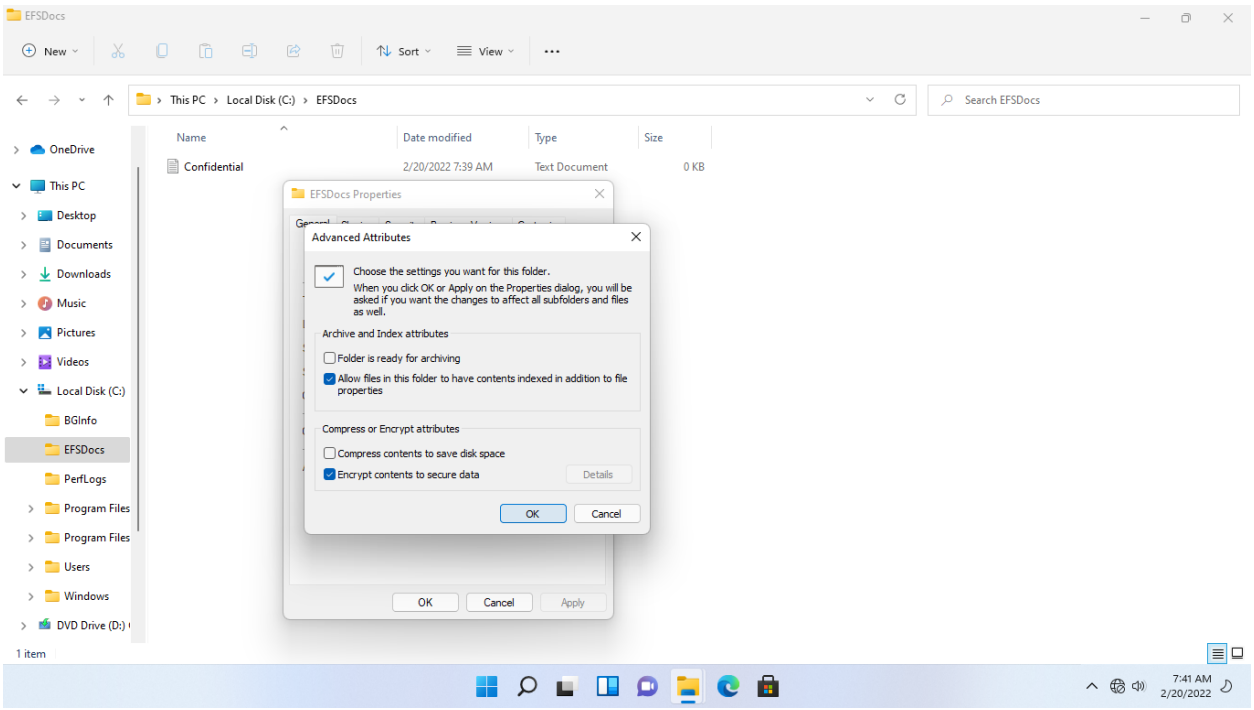
On the **EFSDocs Properties** dialog box, click **Advanced.**



Step 8:

On the **Advanced Attributes** dialog box, tick the **Encrypt contents to secure data** checkbox.

Click **OK.**

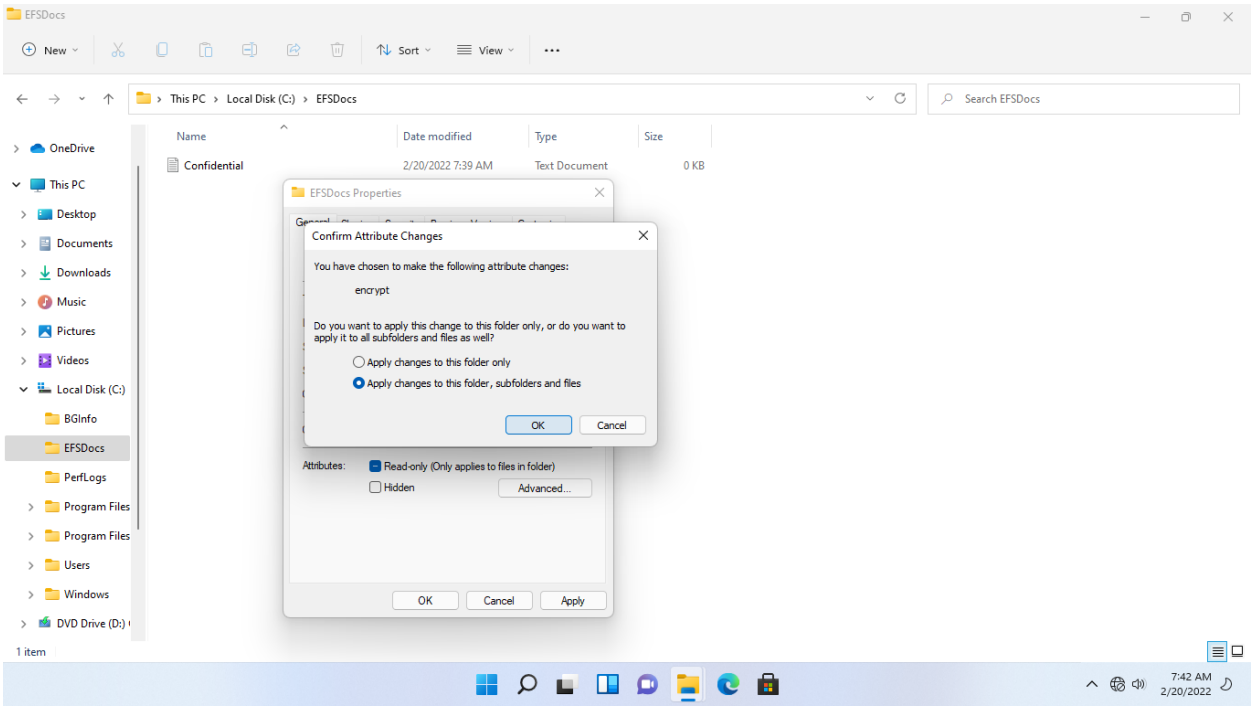


Step 9:

Click **OK** to close **EFSDocs Properties**

Similarly, click **OK** on the Confirm **Attribute Changes** message box.

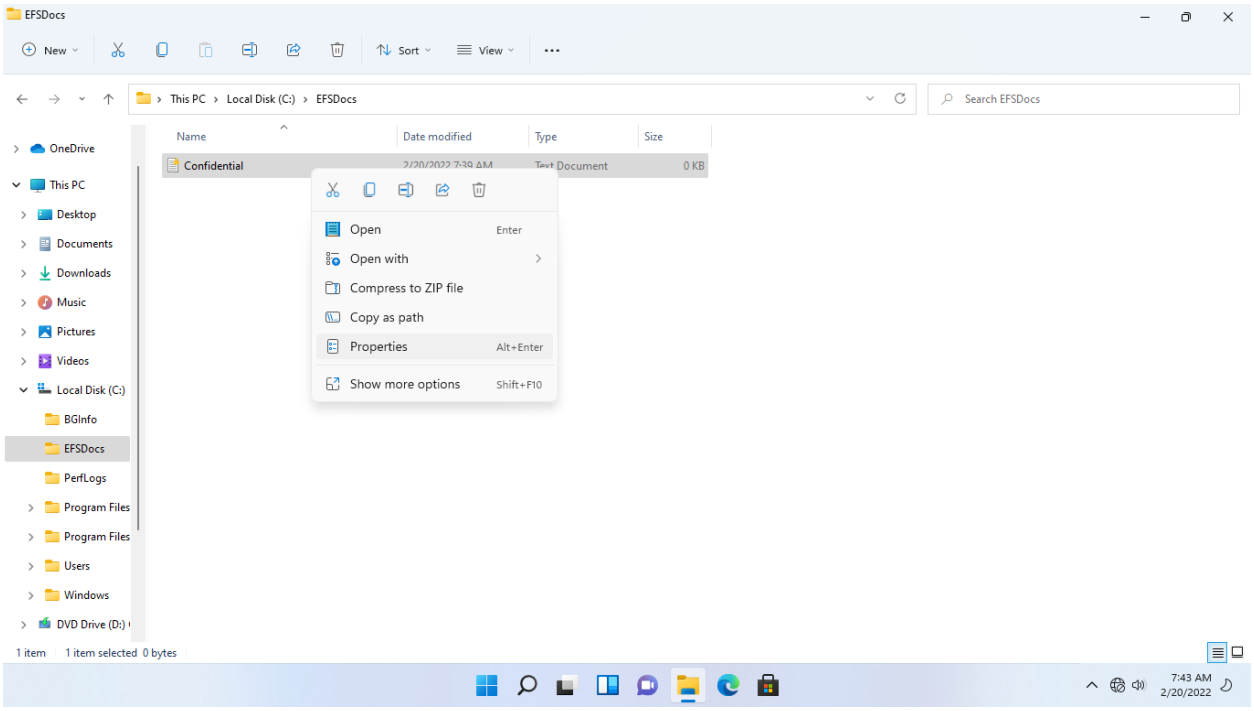
Note: There will be a momentary pause while the attributes are being applied.



Step 10:

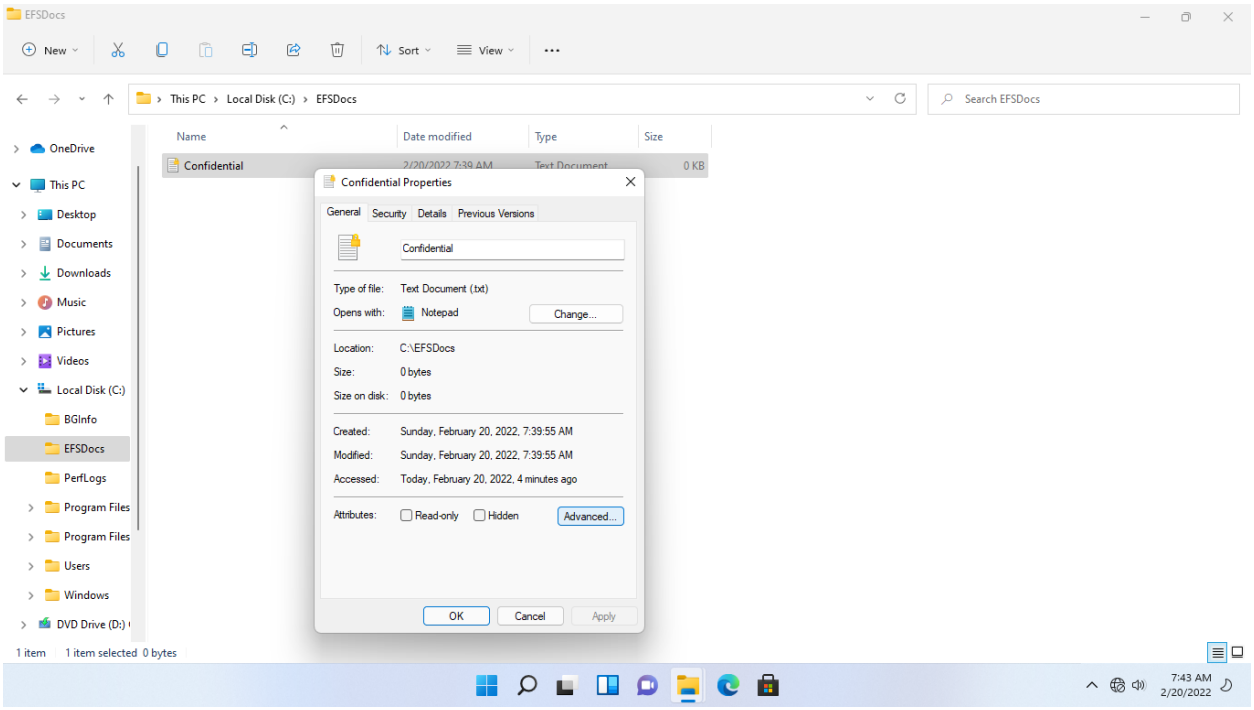
Back in **File Explorer** window, notice the small icon appended to the **Confidential** text document. This icon indicates the document is encrypted.

Right-click the **Confidential** document and select **Properties.**



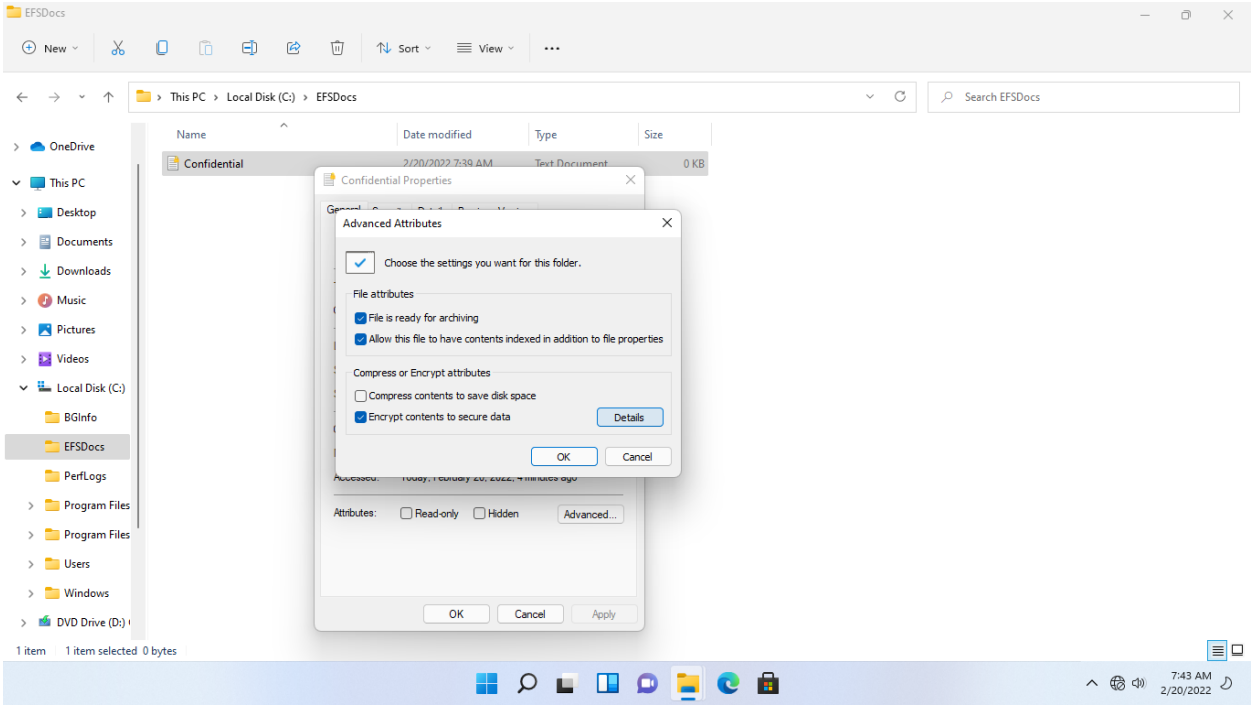
Step 11:

On the **Confidential Properties** dialog box, click **Advanced.**



Step 12:

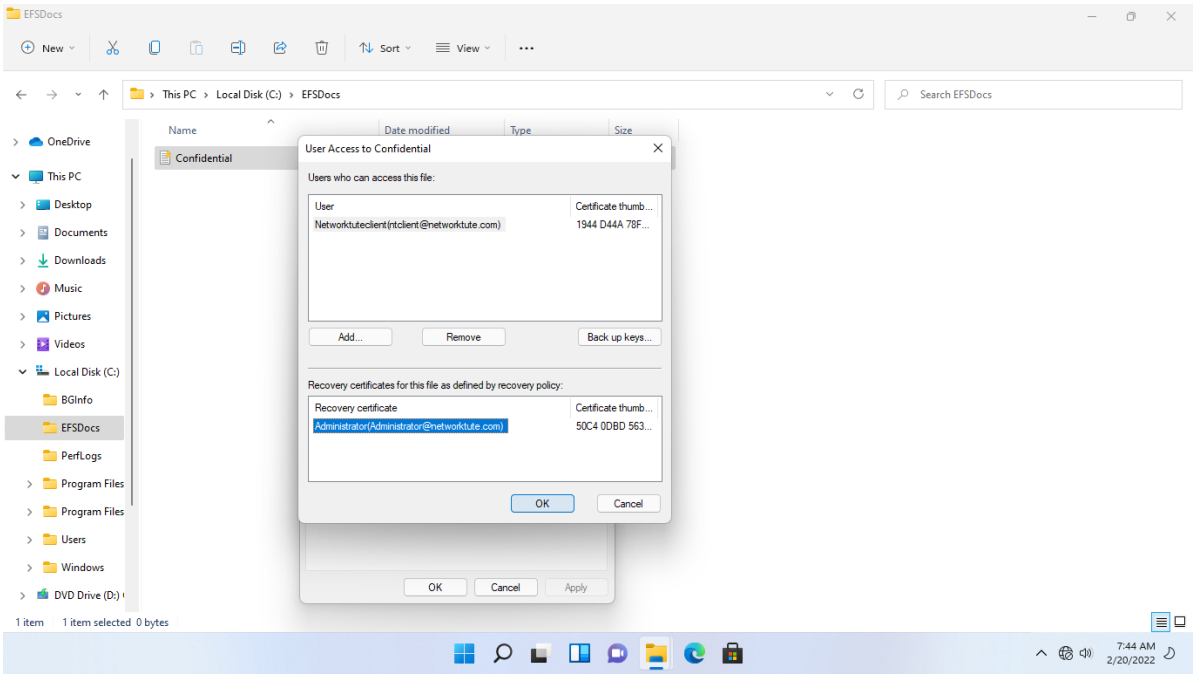
On the **Advanced Attributes** dialog box, click **Details.**



Step 13:

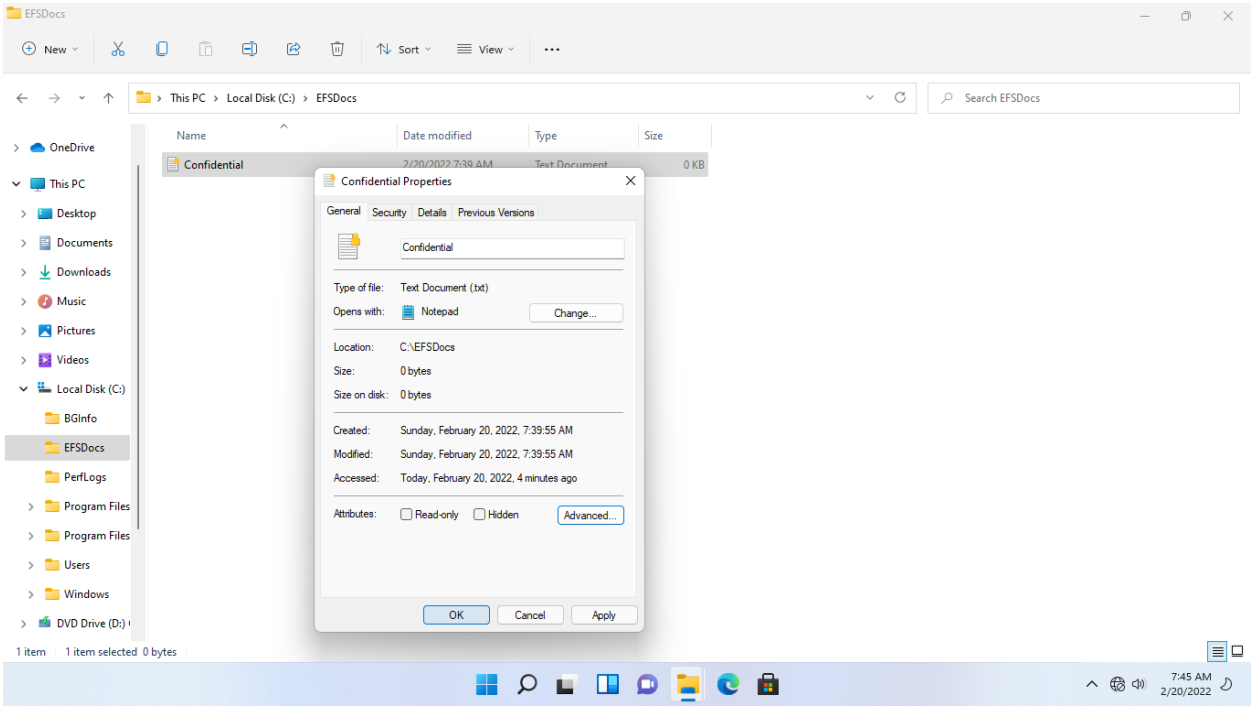
On the **User Access to Confidential** dialog box, in the **Recovery certificates for this file as defined by recovery policy** section, notice that the **Administrator (Administrator@NETWORKTUTE.COM)** is now listed.

Click **OK.**



Step 14:

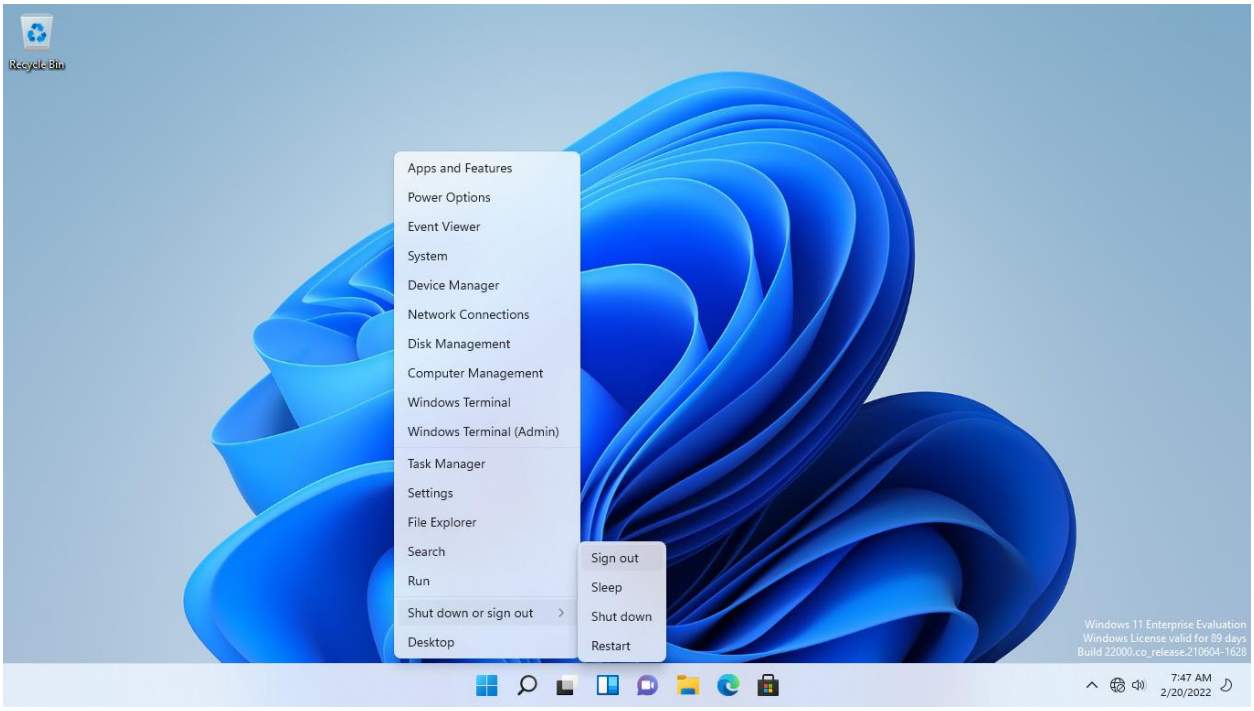
Similarly, click **OK** to close **Advanced Attributes** and **Confidential Properties.**



Step 15:

To verify that **NETWORKTUTE\Administrator** can recover encrypted files, you need to sign out the current user.

Right-click **Start**, point to **Shut down or sign out** and select **Sign out.**



Task 6: Recover an Encrypted File

The EFS recovery administrator certificate with the private keys - the.pfx file - must first be imported into the recovery agents account on the computer hosting the file in order to recover an encrypted file.

As a result, the.pfx file must be imported into NTWIN11VM1 in order for the NETWORKTUTE\Administrator to decrypt the Confidential text document in this assignment.

Let's now test the data recovery agent policy for recovering an encrypted file.

Step 1:

Connect to **NTWIN11VM1**.

In the **sign-in** page, ensure that **NETWORKTUTE\Administrator** is displayed.

In the **Password** box, type:

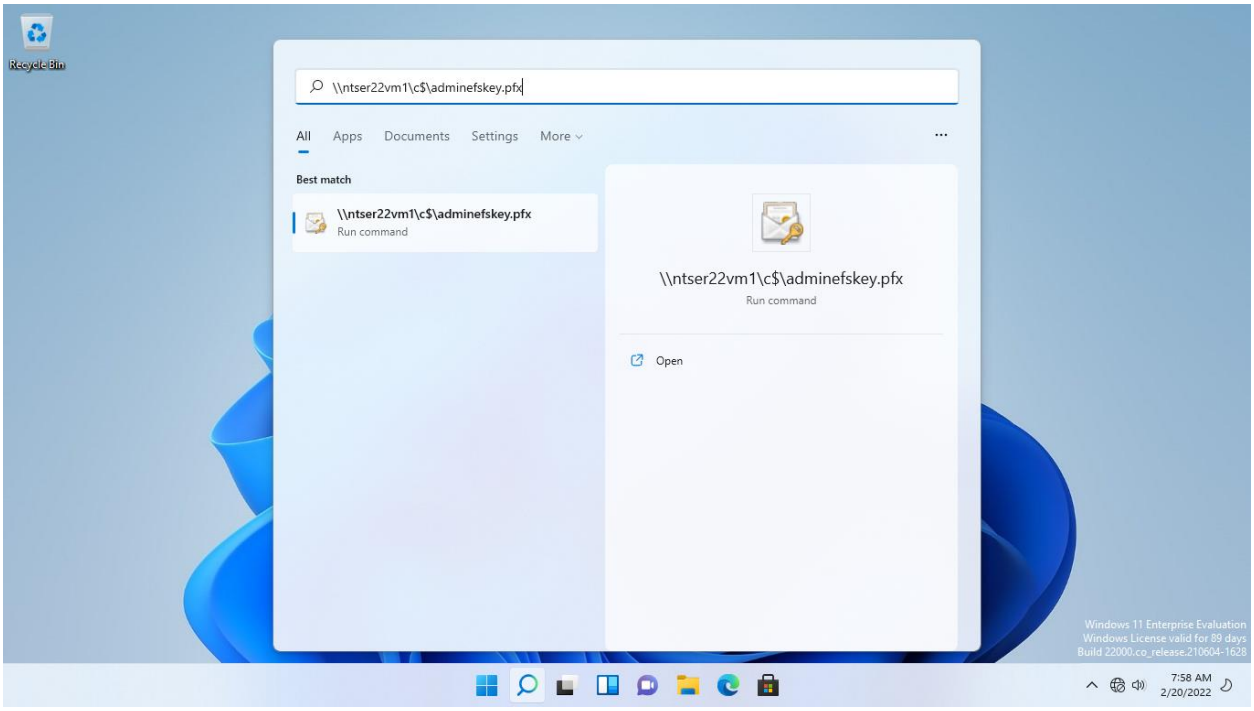
Networktute@123

Press **Enter.**

To import the .pfx file, click in the **Type here to search** box, type:

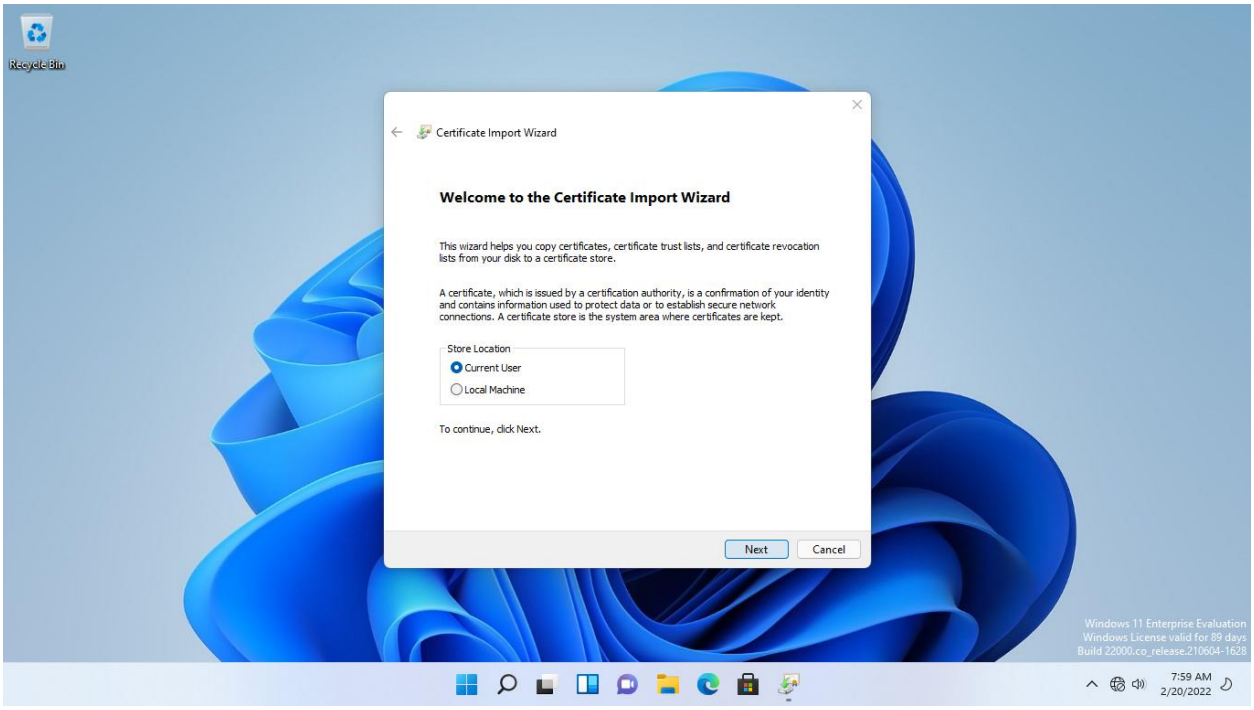
```
\\ntser22vm1\c$\adminefskey.pfx
```

As Windows auto-completes the network path, select **\\ntser22vm1\c$\adminefskey.pf**x in the menu.



Step 2:

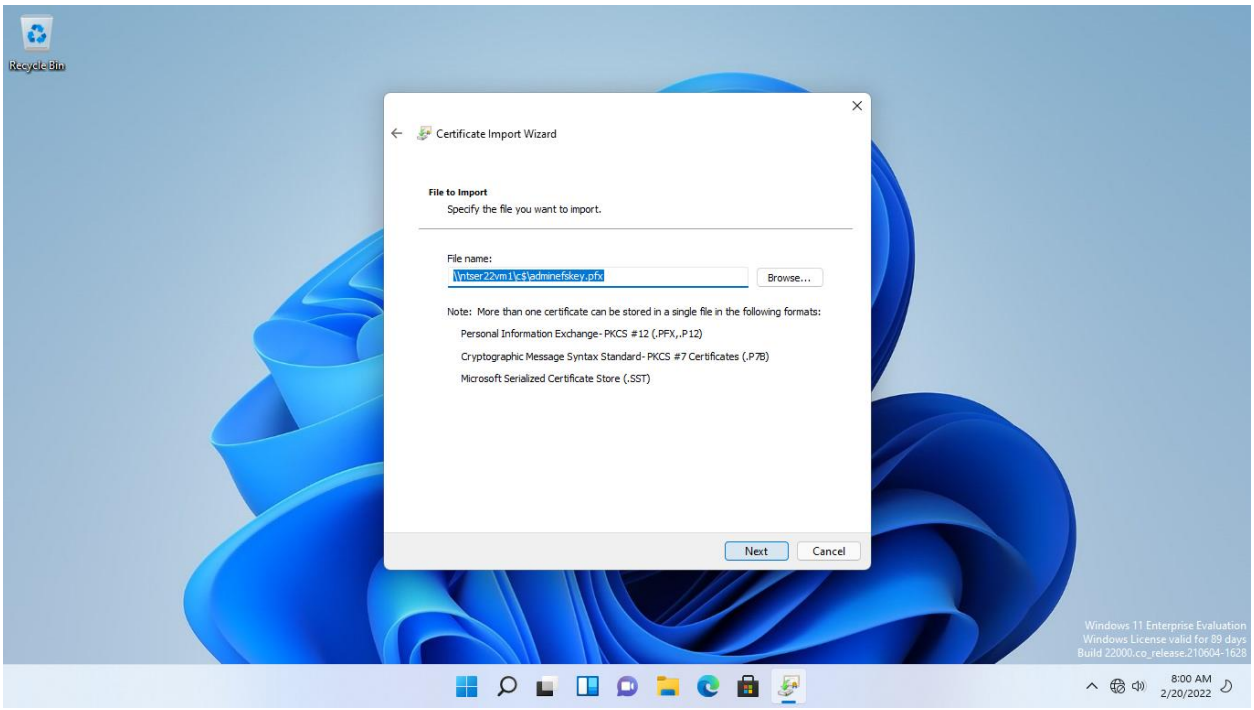
On the **Welcome to the Certificate Import Wizard** page, ensure **Current User** is selected, then click **Next.**



Step 3:

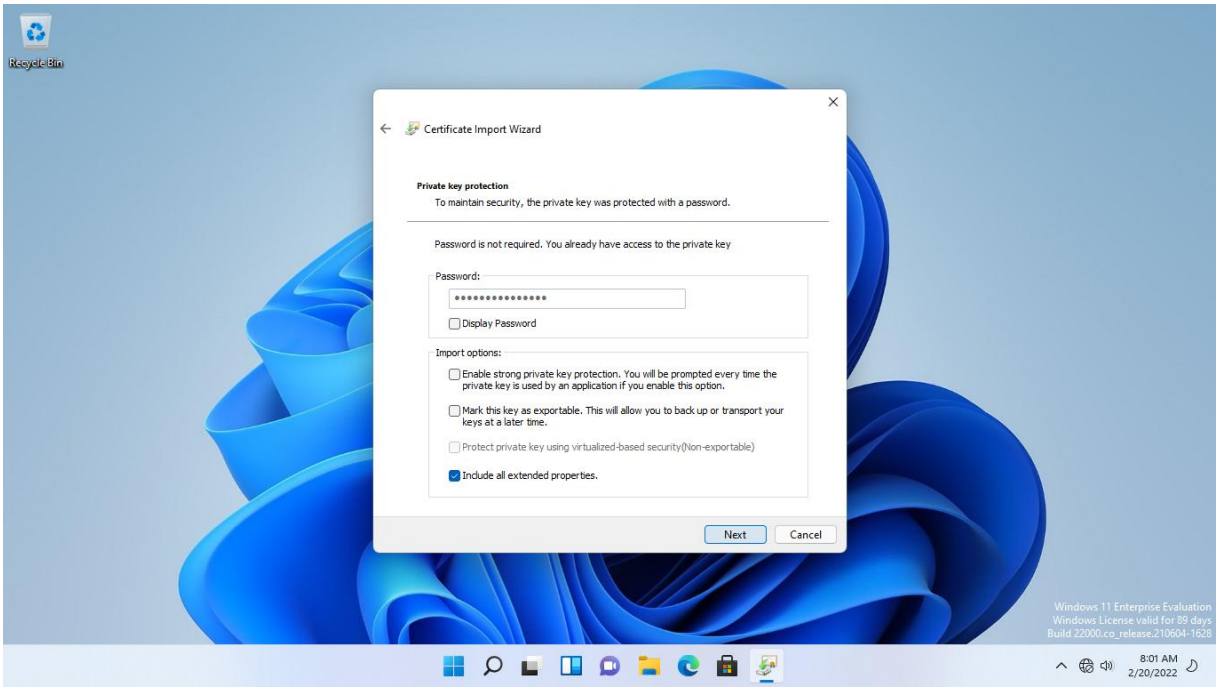
On the **File to Import** page, the **File name** path is displayed.

Click **Next.**



Step 4:

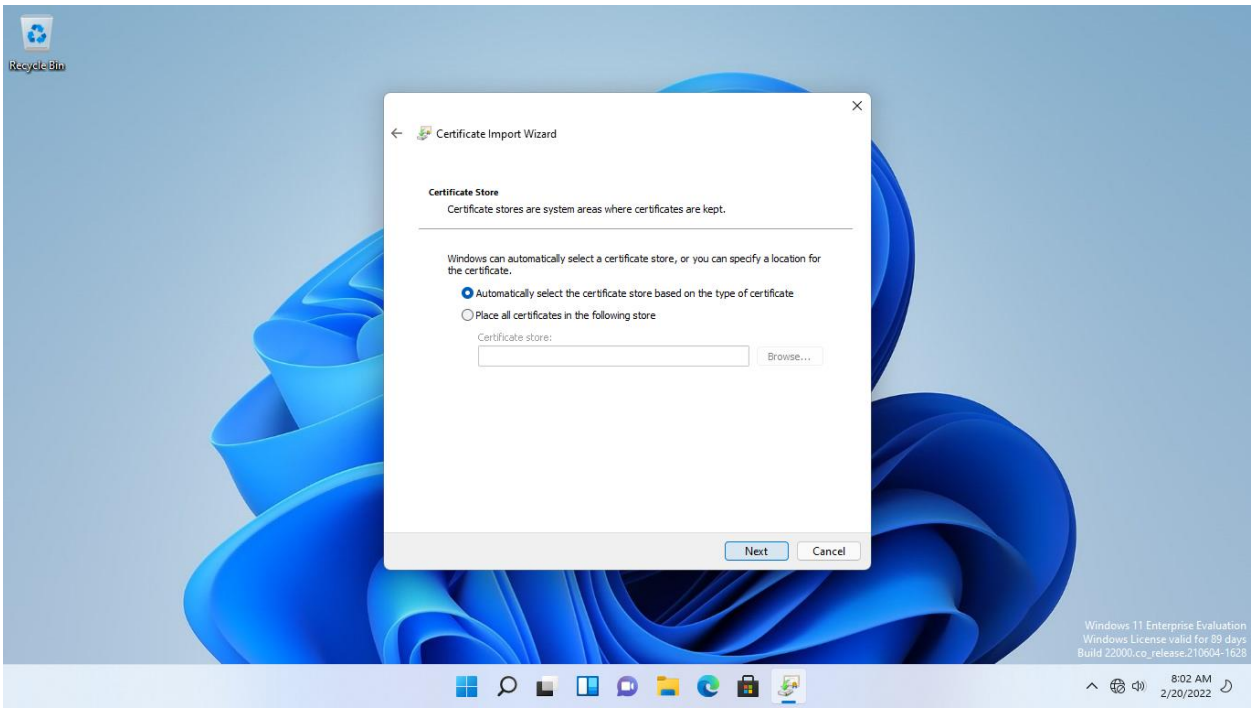
On the **Private key protection** page, click **Next.**



Step 5:

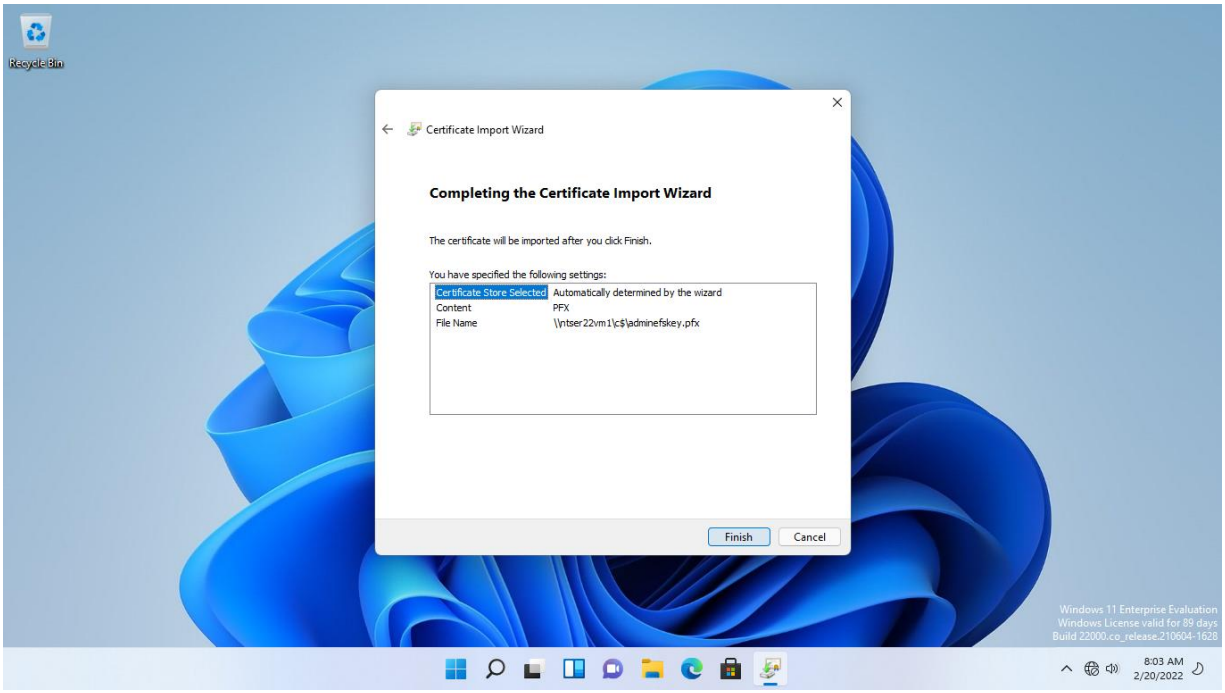
On the **Certificate Store** page, keep the default selection.

Click **Next.**



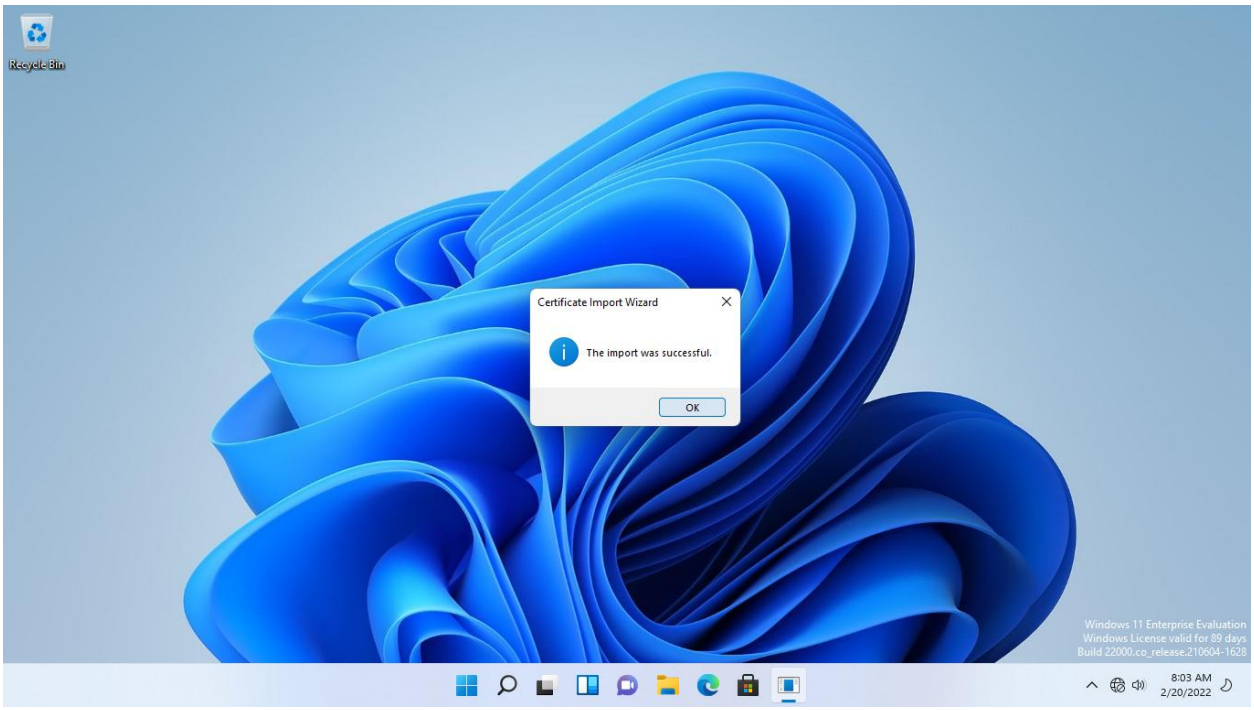
Step 6:

On the **Completing the Certificate Import** Wizard, click **Finish**.



Step 7:

Click **OK** when notified that the import was successful.

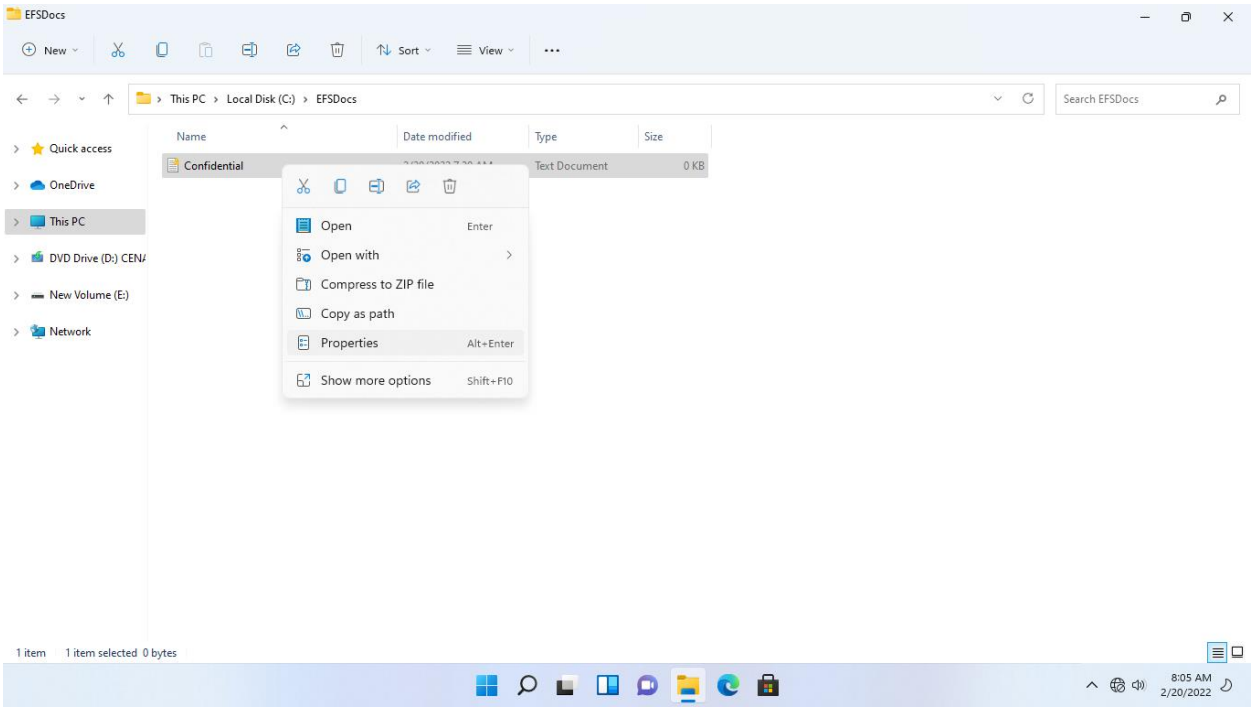


Step 8:

Click the **File Explorer** icon on the **Taskbar**.

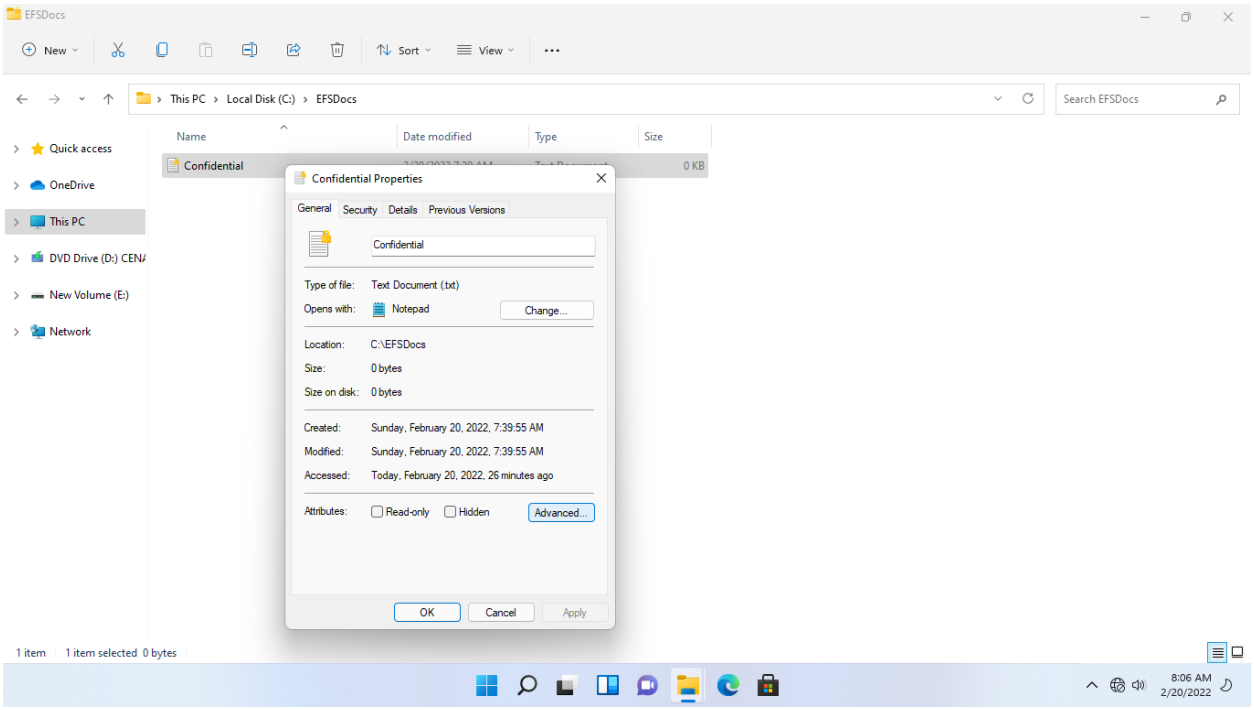
On the **File Explorer** window, expand the **This PC > Local Disk (C:)** nodes and then double-click the **EFSDocs** folder.

On the details pane at the right, right-click **Confidential** and select **Properties**.



Step 9:

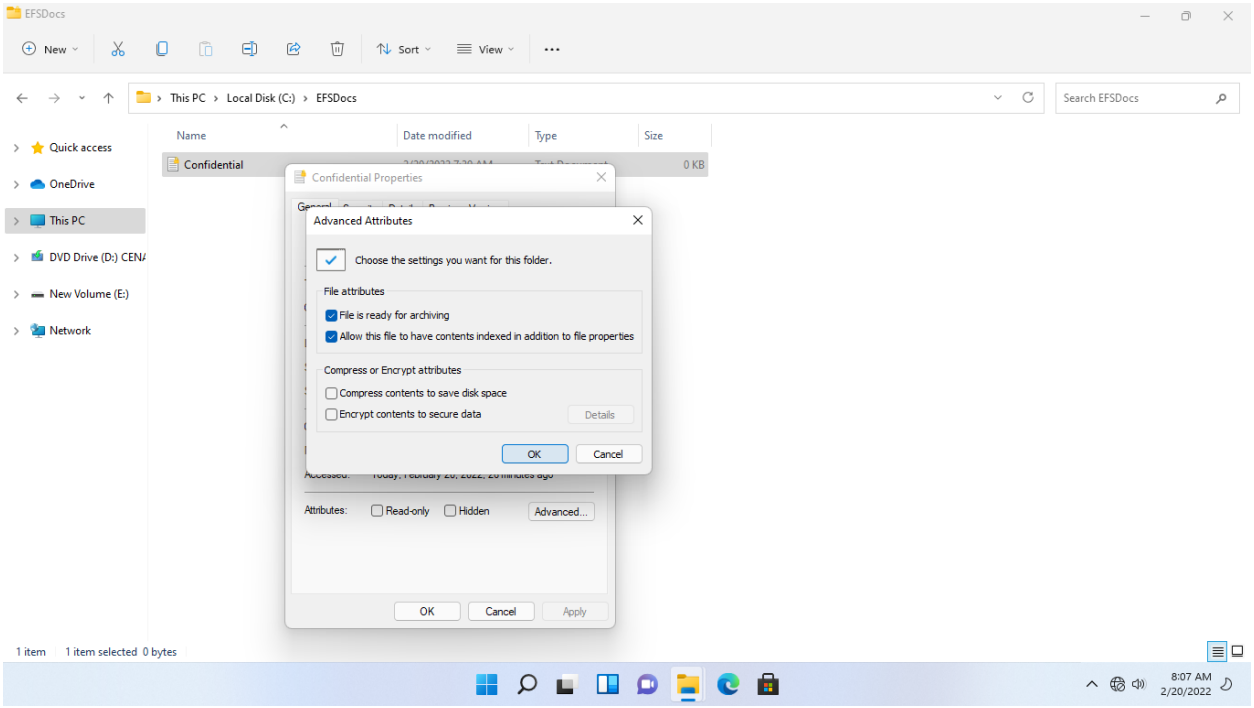
On the **Confidential Properties** dialog box, click **Advanced.**



Step 10:

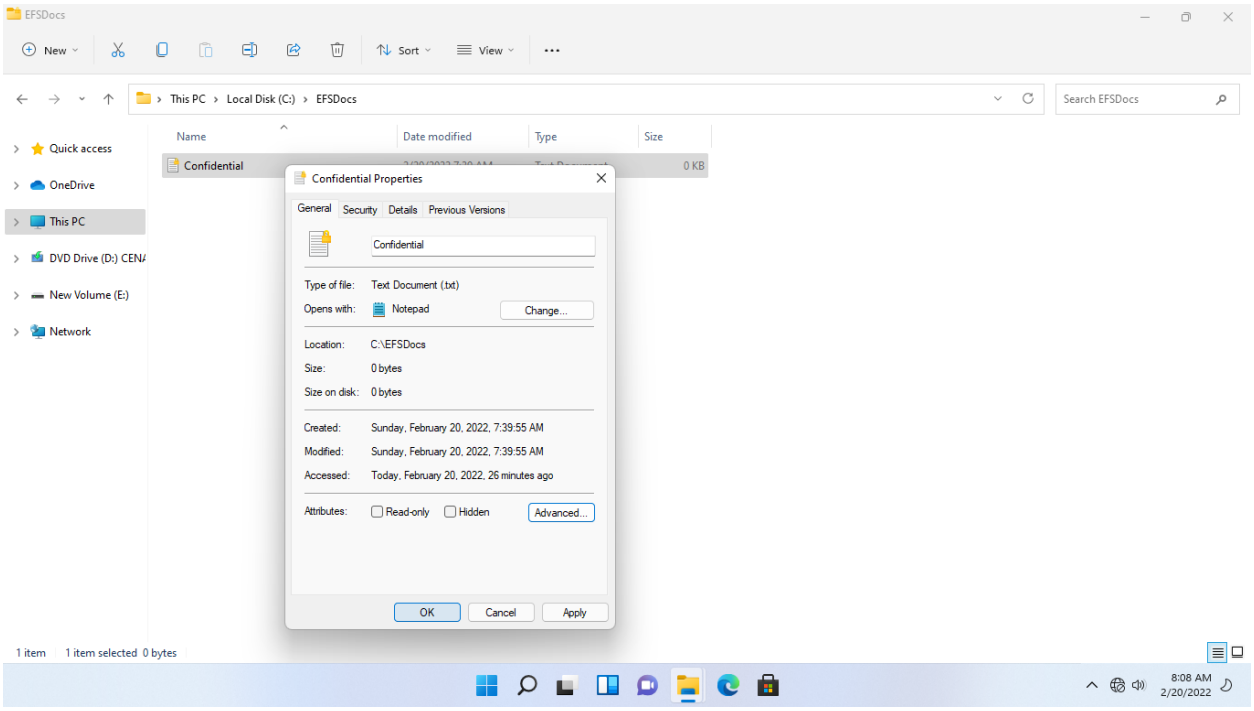
On the **Advanced Attributes**, untick the **Encrypt contents to secure data** checkbox.

Click **OK**.



Step 11:

On the **Confidential Properties** dialog box, click **OK**.



Step 12:

When you return to the **File Explorer** window, you'll notice that the little icon indicating document encryption has vanished. The **Confidential** text document has now been decoded, according to this.

Close **File Explorer.**