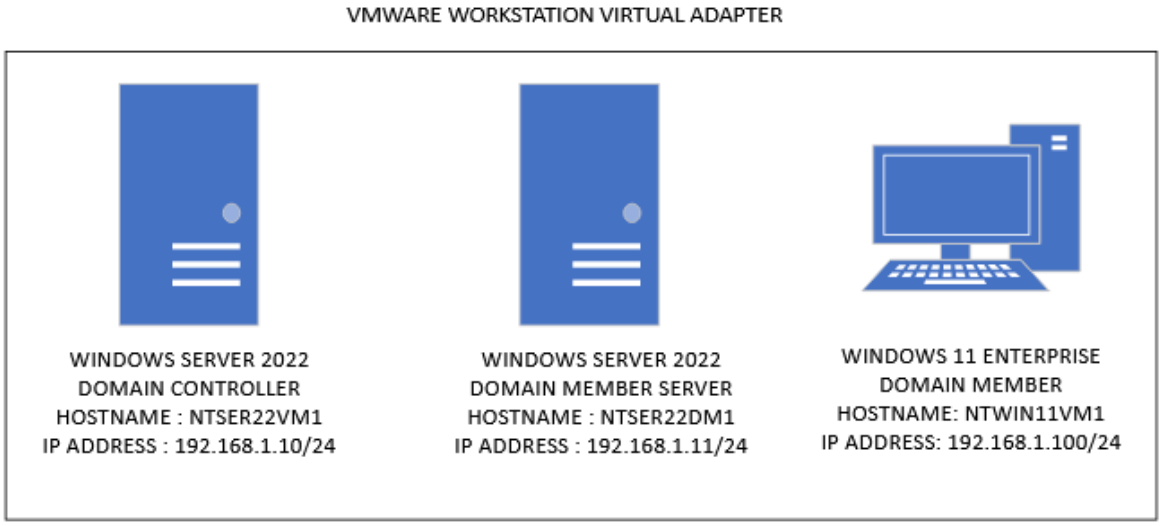
Exercise 1 - Configure Certificate Auto Enrollment

In a small business, the certificates request wizard in the Microsoft Management Console (MMC) can be used to manually enroll a machine or user certificate. Certificate enrollment can be expedited for large enterprises with hundreds of network users by customizing a certificate template. Using Group Policy Objects, you may set properties like auto enrollment and simplify certificate deployment to domain users using a customized certificate template.

In this exercise, learn how to handle certificates by configuring various attributes for a custom template, such as security, which specifies which user or security group has access to the certificate, timeline, which depicts the validity of a given certificate, and other features.

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: Configure a Customized Certificate Template

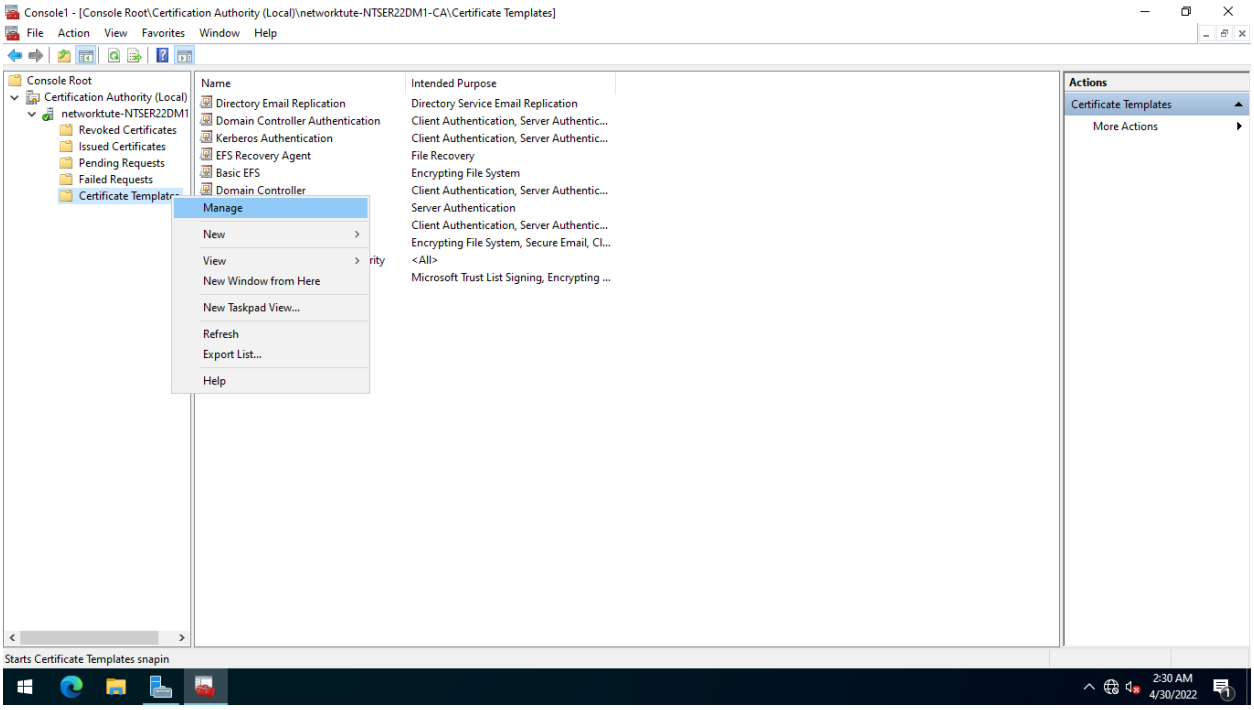
You can also make a certificate template that is unique to you. You can adapt an existing template to meet the needs of your organization.

Follow these steps to create a personalized certificate template:

Step 1:

On **NTSER22DM1**, the **Certification Authority** console window is open.

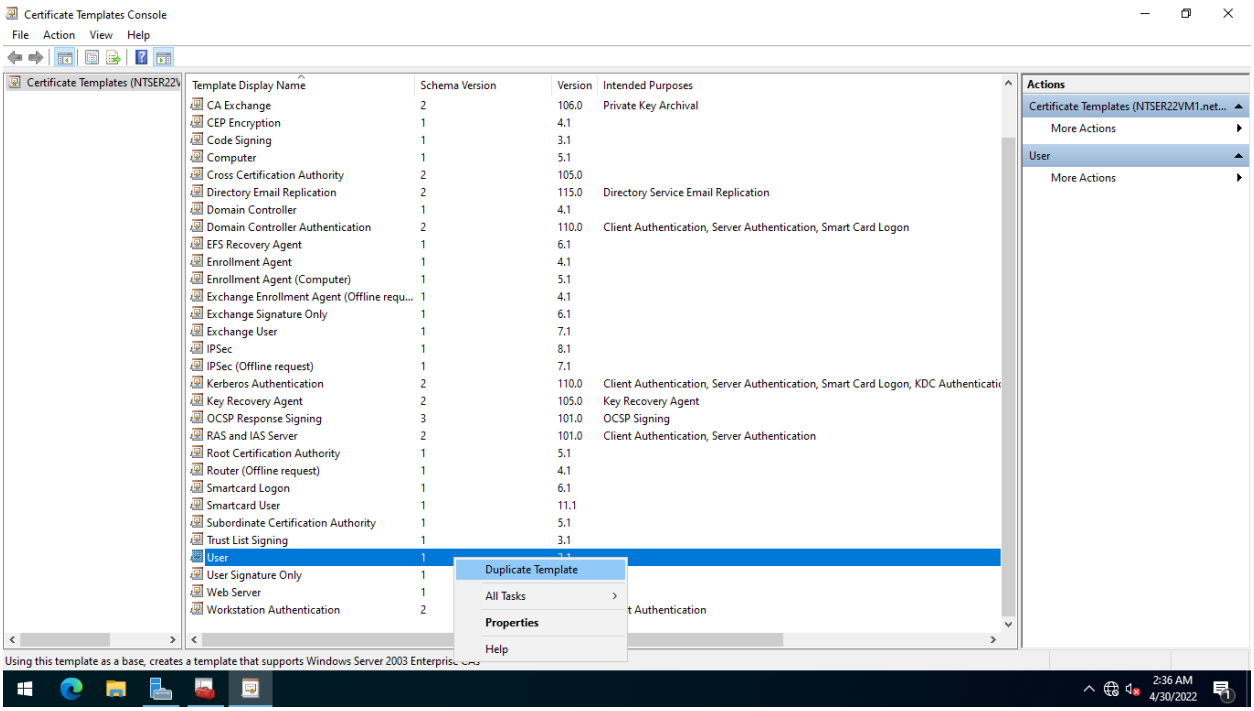
Right-click the **Certificate Templates** folder and select **Manage**.



Step 2:

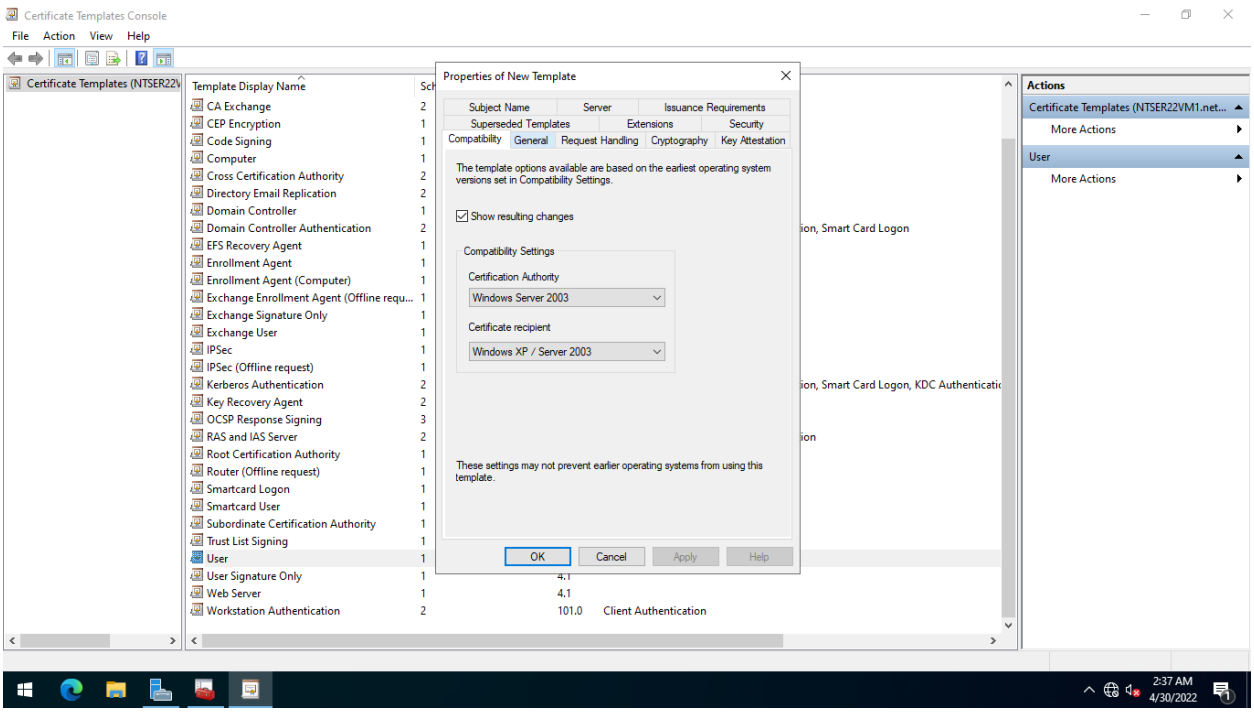
The **Certificate Templates Console** window opens.

Scroll down the templates list and right-click on **User**, and then select **Duplicate Template.**



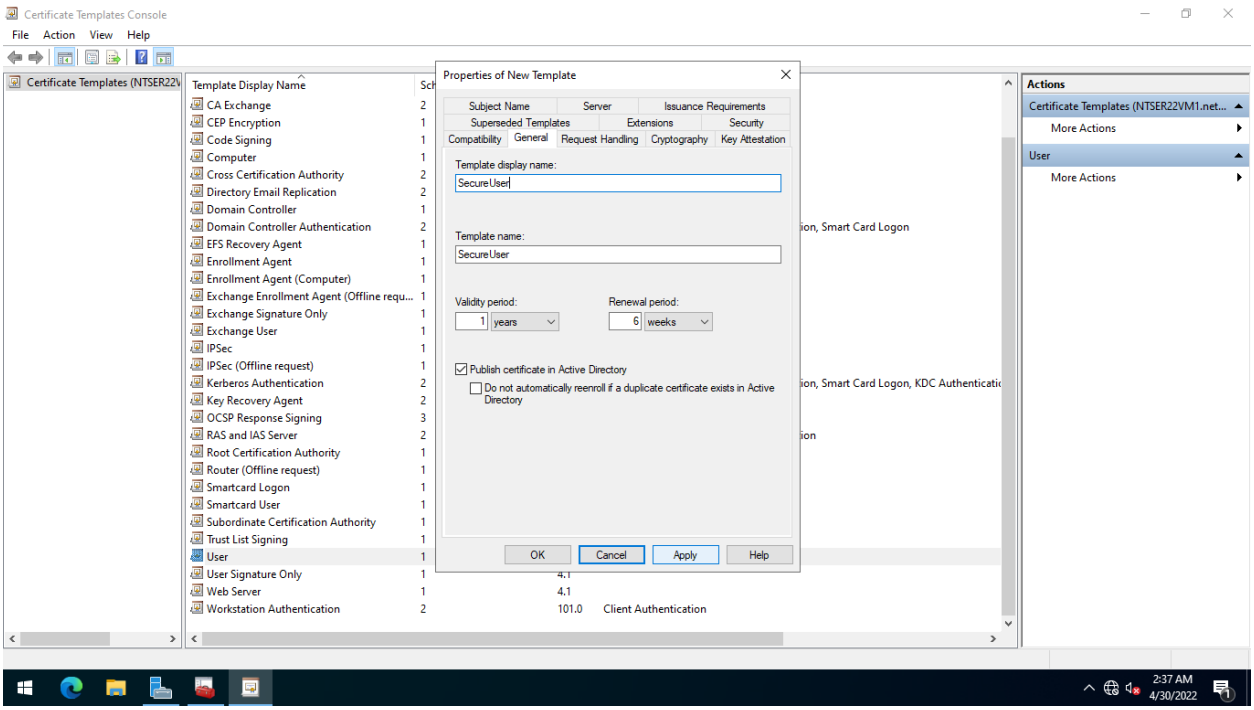
Step 3:

On the **Properties of New Template** dialog box, click the **General** tab.



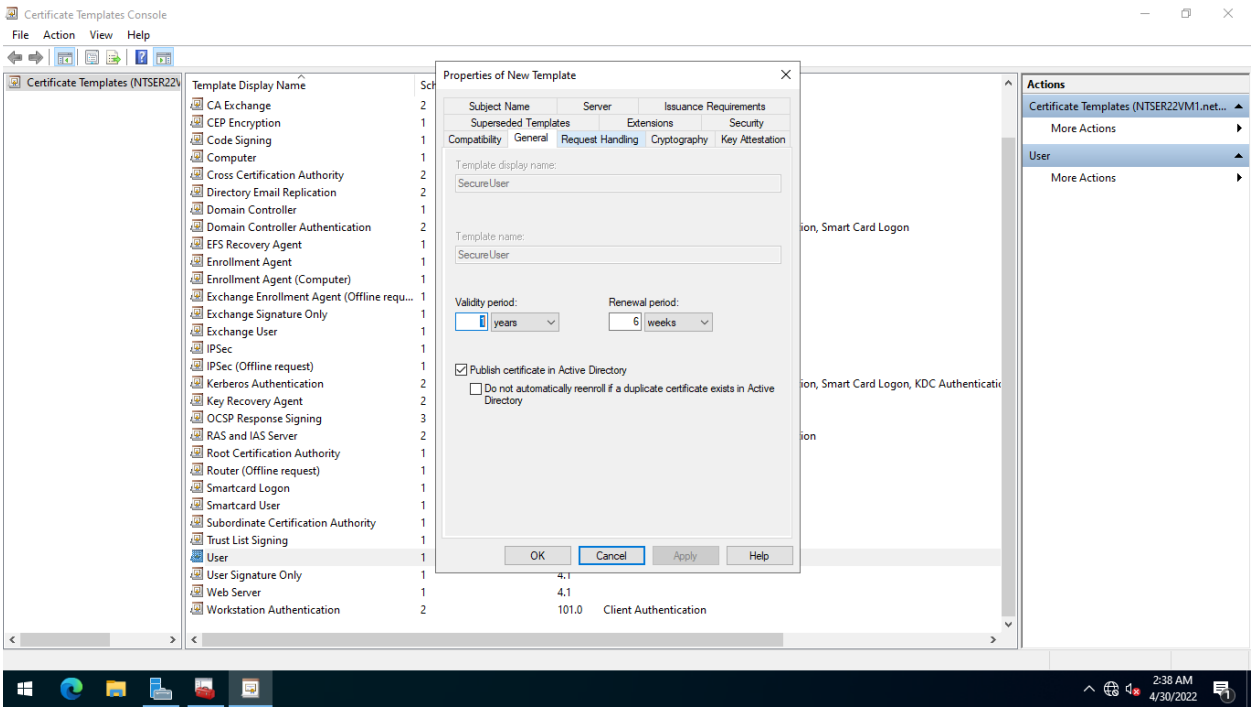
Step 4:

In the General tab, click inside the Template display name text box and type-over the existing text with the following and then click Apply. ***SecureUser***



Step 5:

Then, click the **Request Handling** tab.

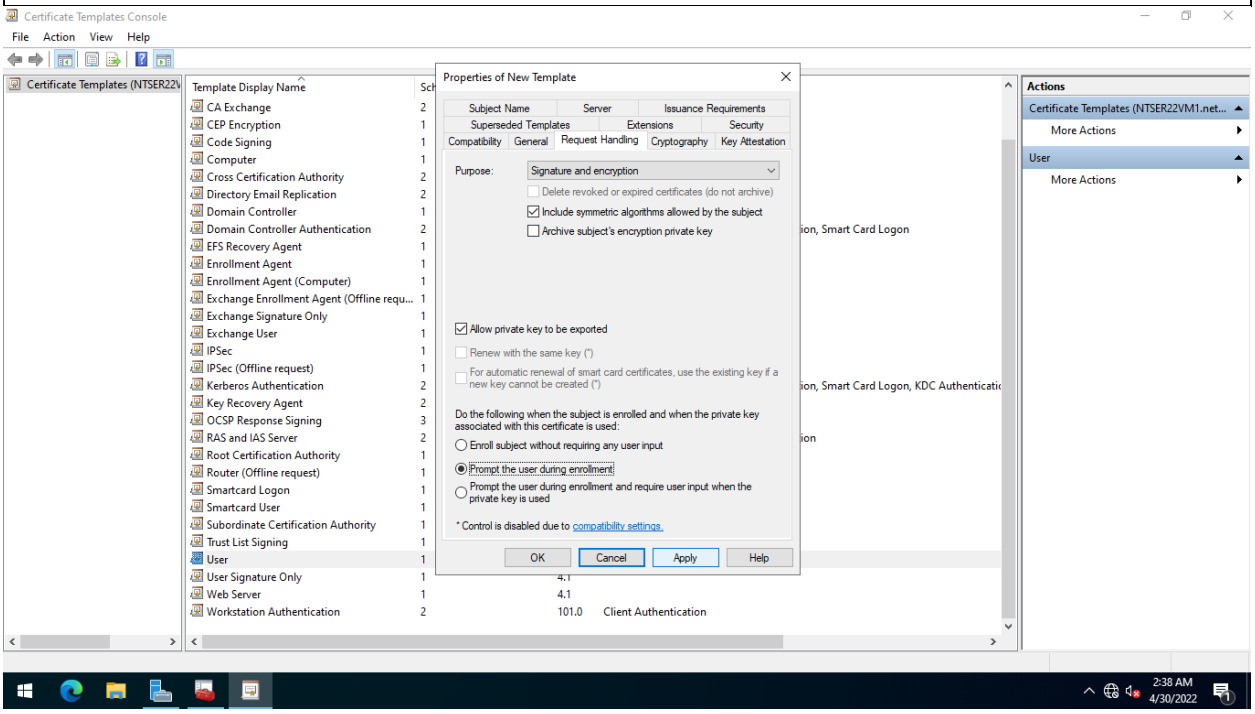


Step 6:

In the **Request Handling** tab, select **Prompt the user during enrollment** option.

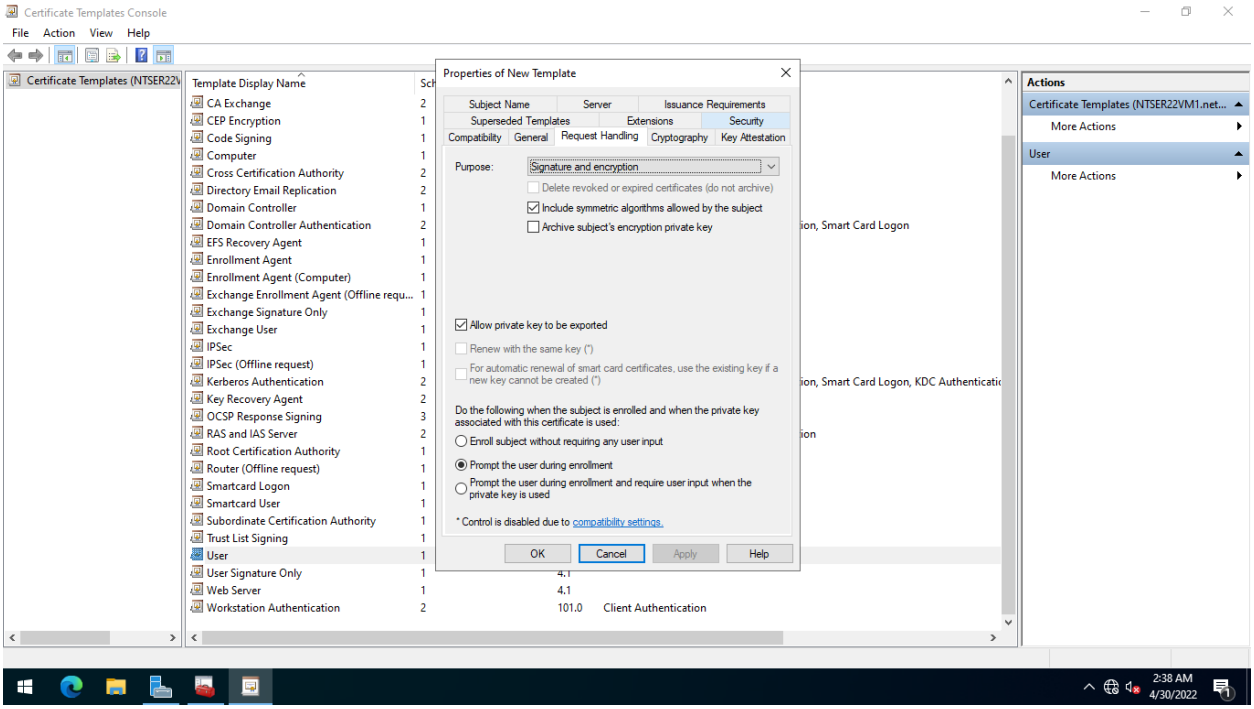
Click **Apply**.

NOTE: This option will be used to prompt the user during enrolment in this lab. When users are automatically registered for a certificate in a real deployment, they are not prompted by any notification.



Step 7:

Then, click the **Security** tab.

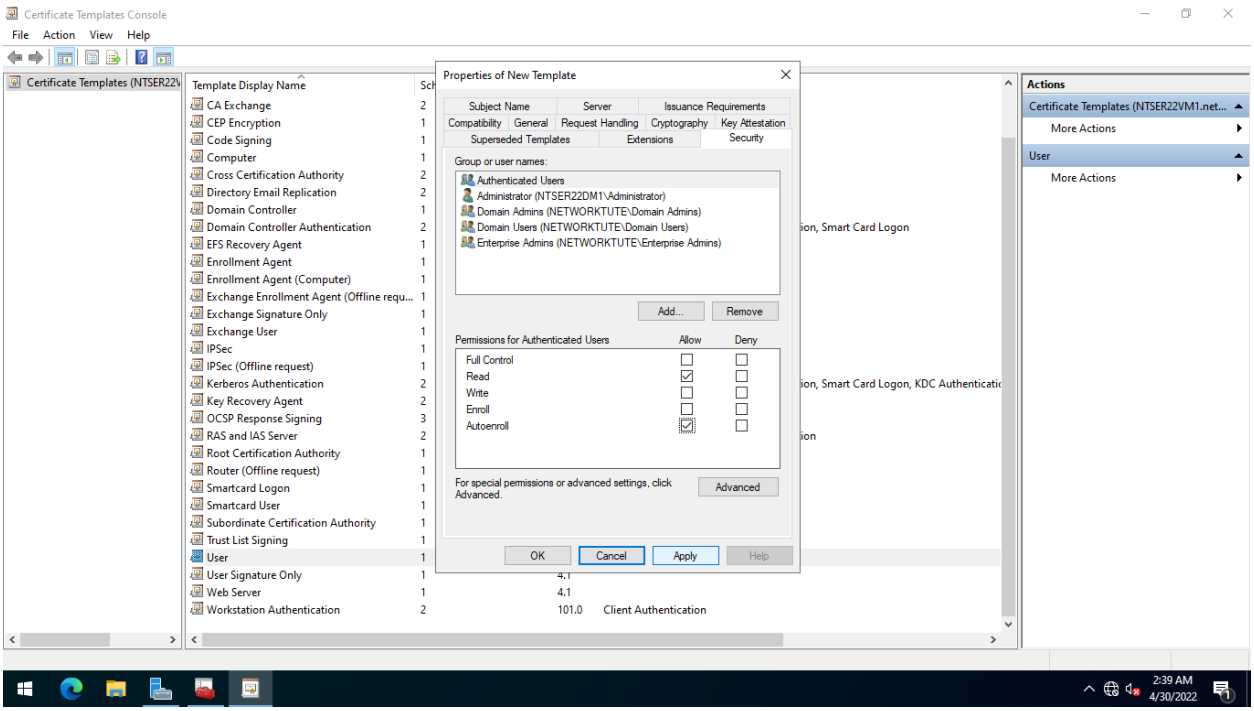


Step 8:

In the **Security** tab, ensure that the **Authenticated Users** security group is selected.

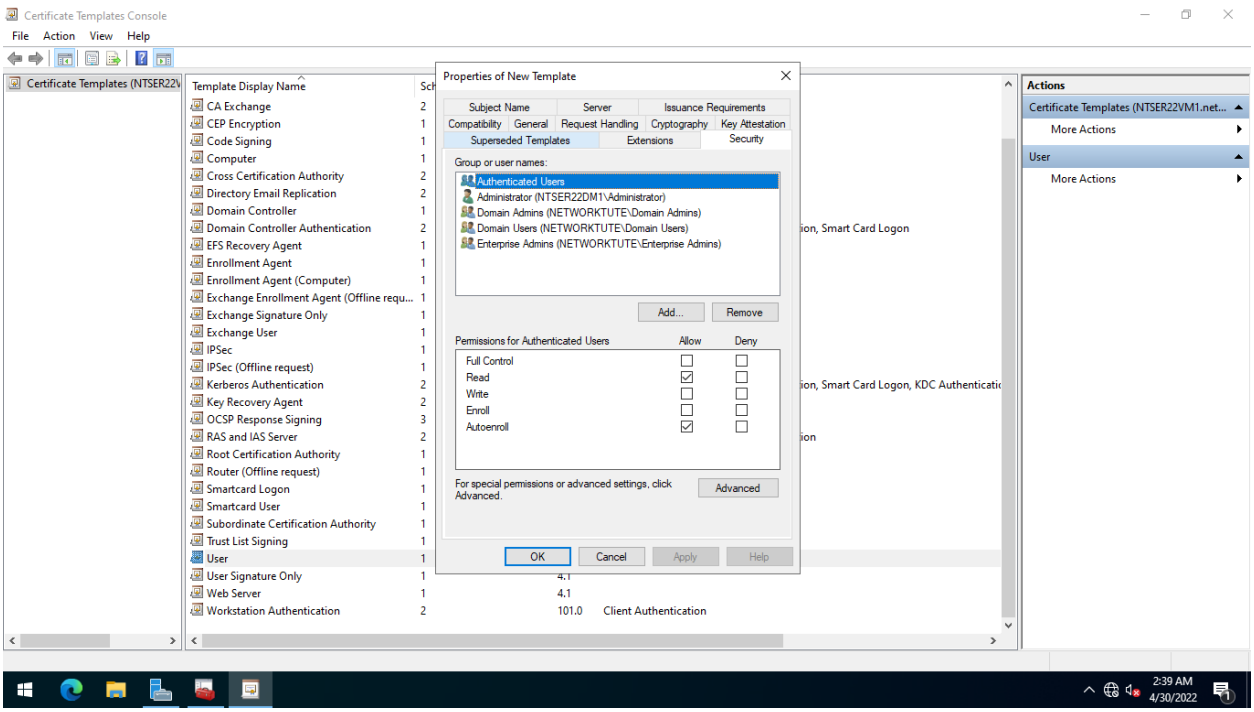
Under the **Permissions for Authenticated Users** section, select the **Autoenroll** checkbox.

Click **Apply**.



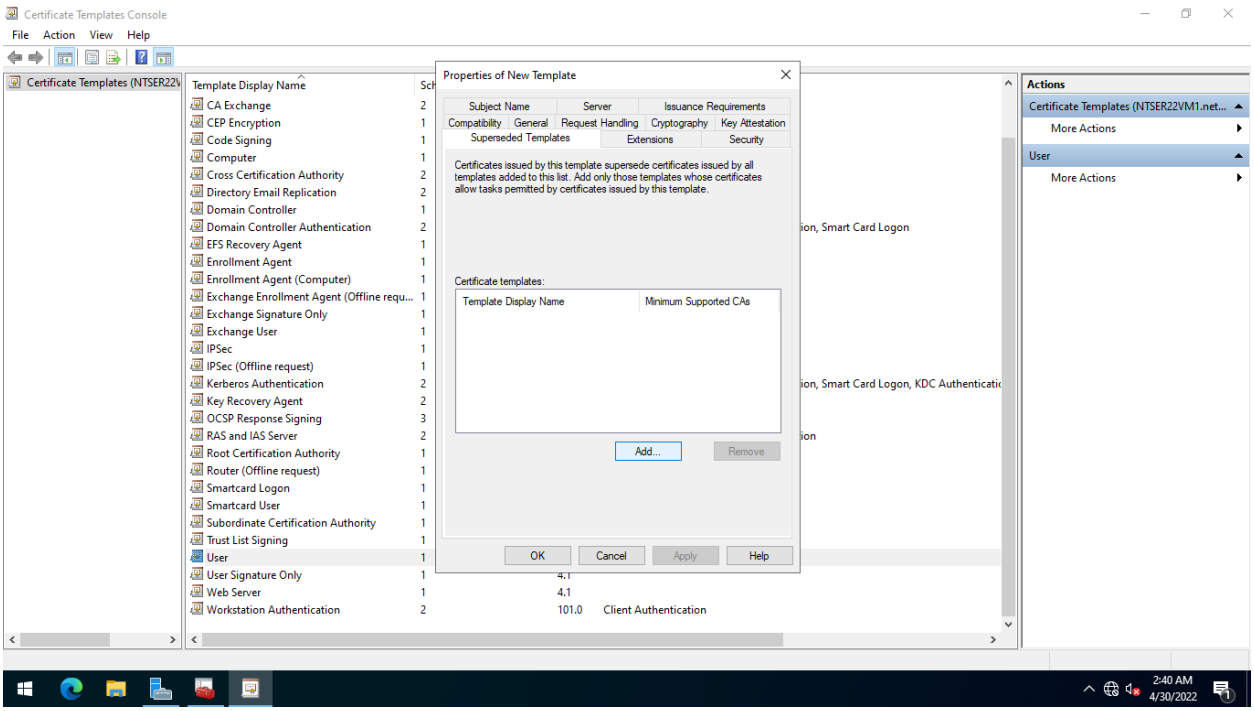
Step 9:

Then, select the **Superseded Templates** tab.



Step 10:

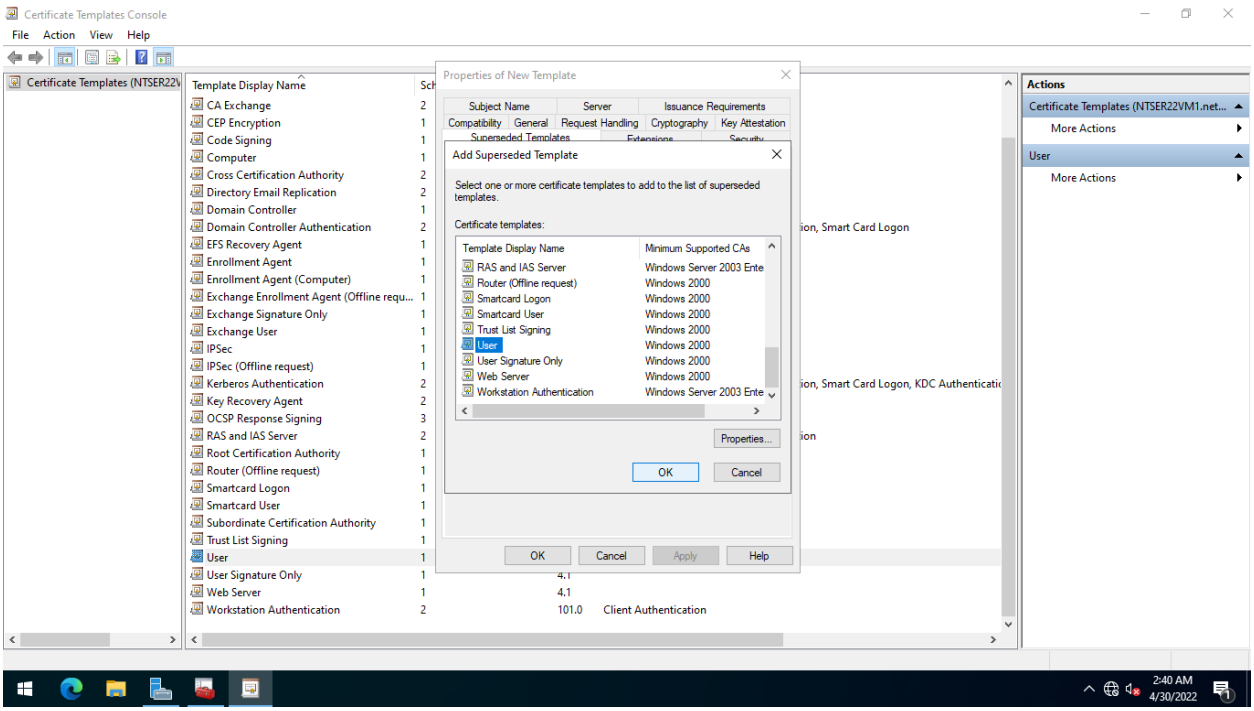
In the **Superseded Templates** folder tab, click **Add**.



Step 11:

In the **Add Superseded Template** dialog box, scroll down the list of certificate templates and select **User**.

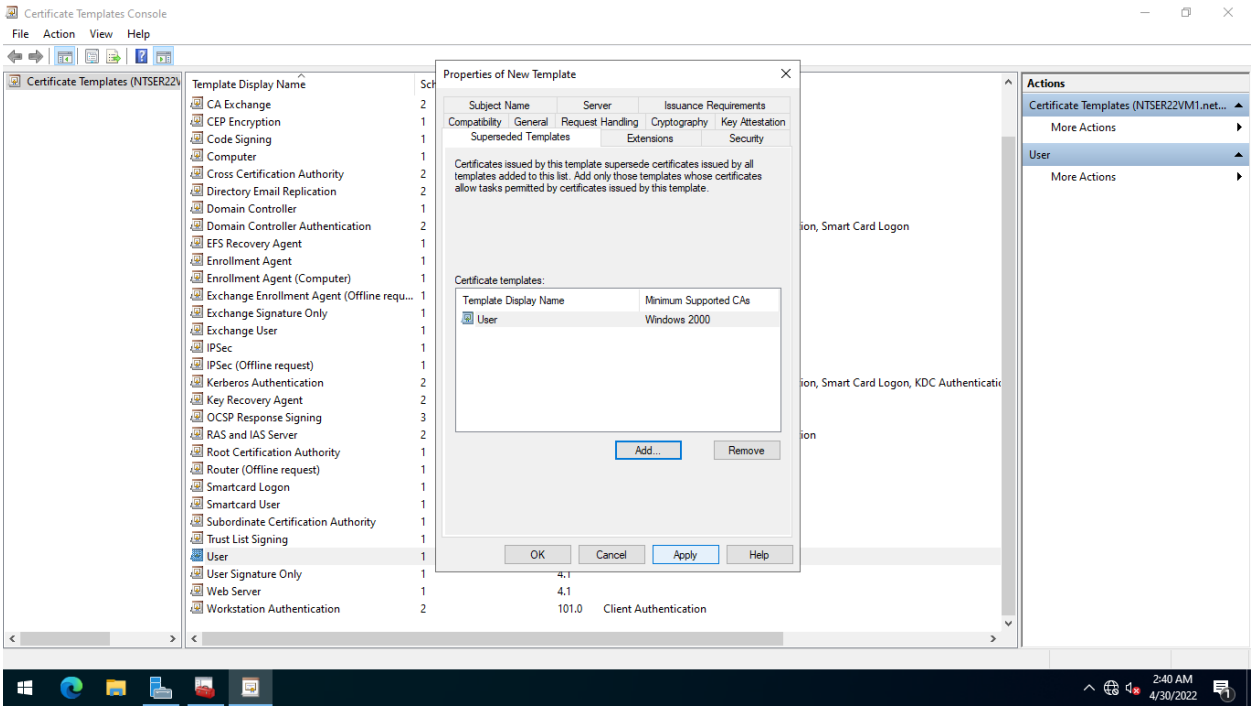
Click **OK.**



Step 12:

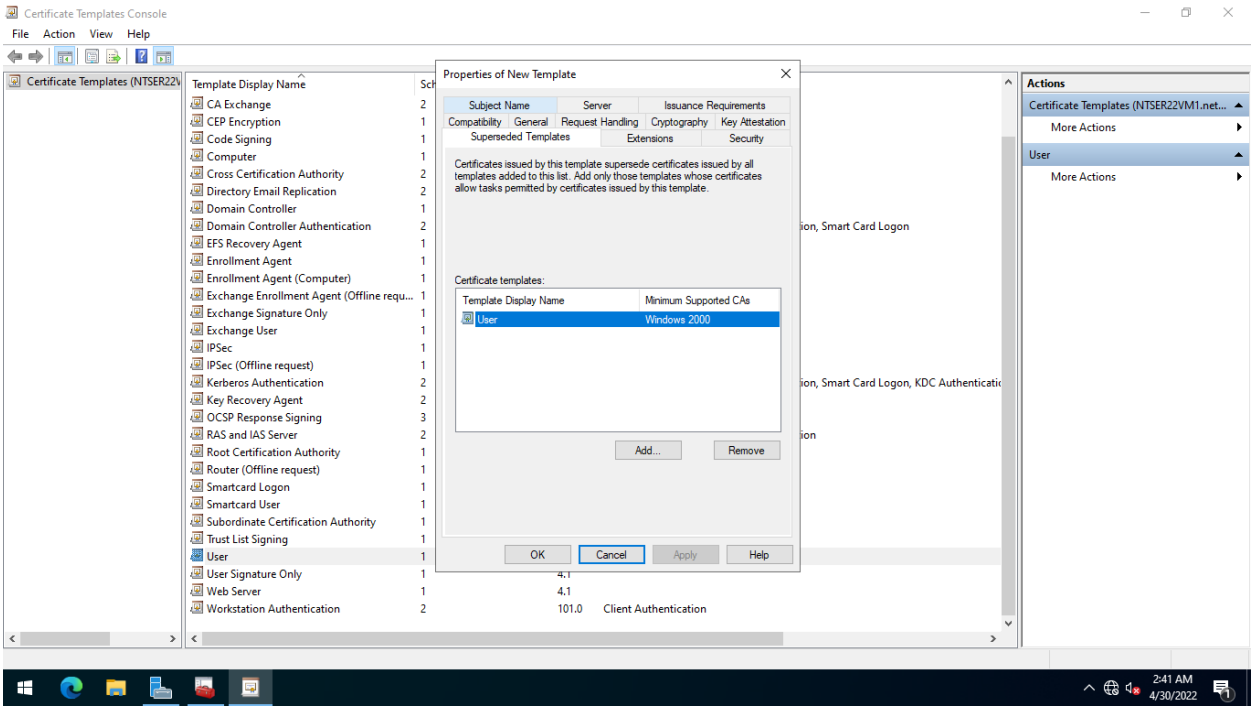
Back in the **Superseded Templates** tab, the **User** template is now added.

Click **Apply**.



Step 13:

Then, select the **Subject Name** tab.



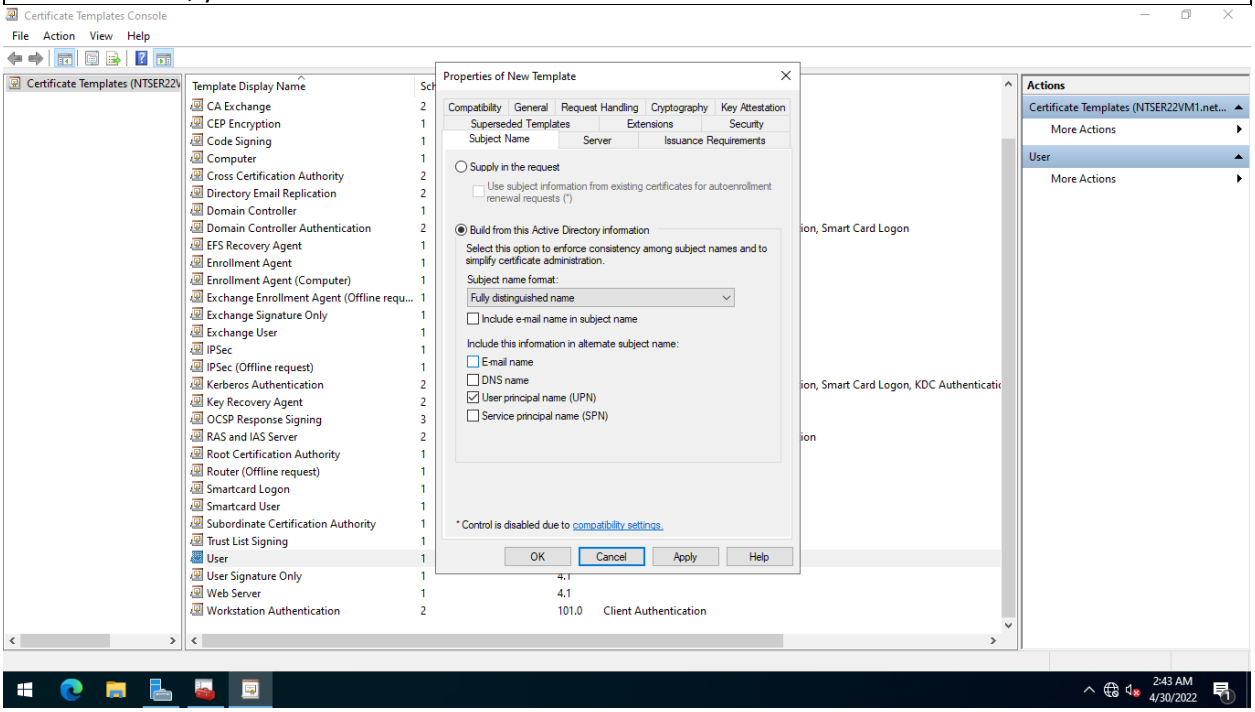
Step 14:

In the **Subject Name** tab, clear the following checkboxes:

- **Include e-mail name in subject name**
- **E-mail name**

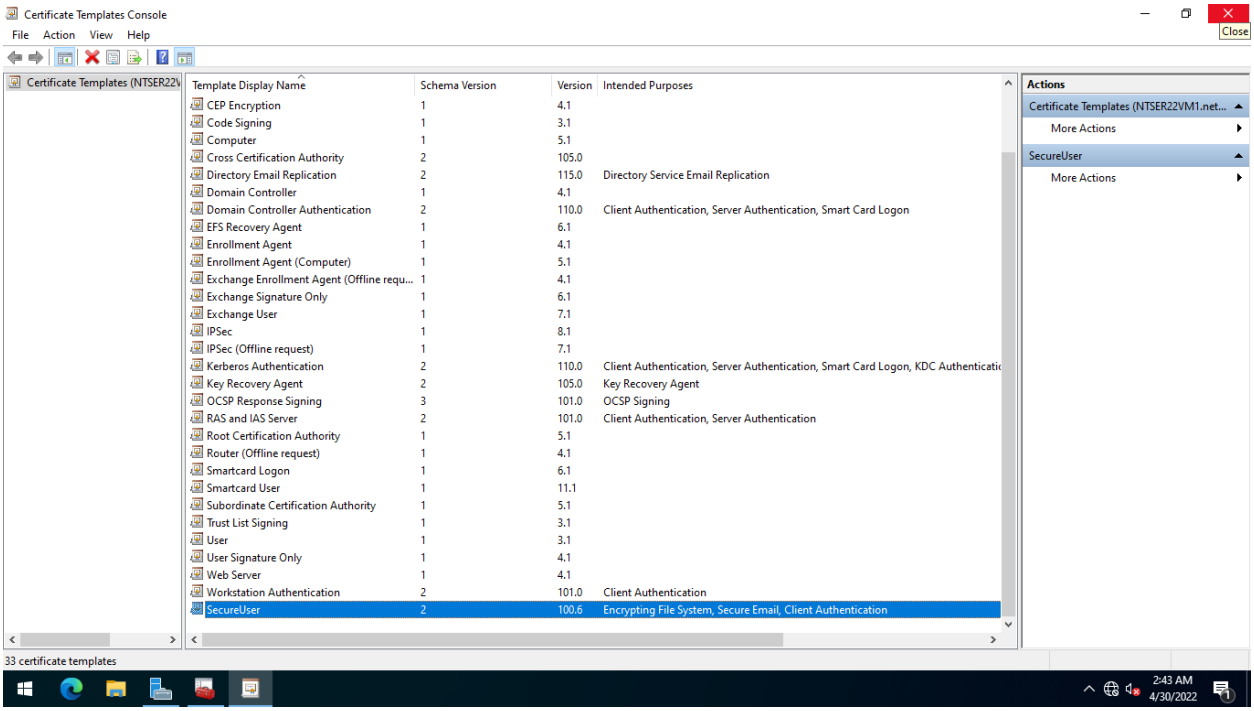
Click **OK**.

NOTE: Because AD users in the Networktute Labs domain do not have such properties configured in their accounts, you cleared the two checkboxes.



Step 15:

Close the **Certificate Templates Console** window.

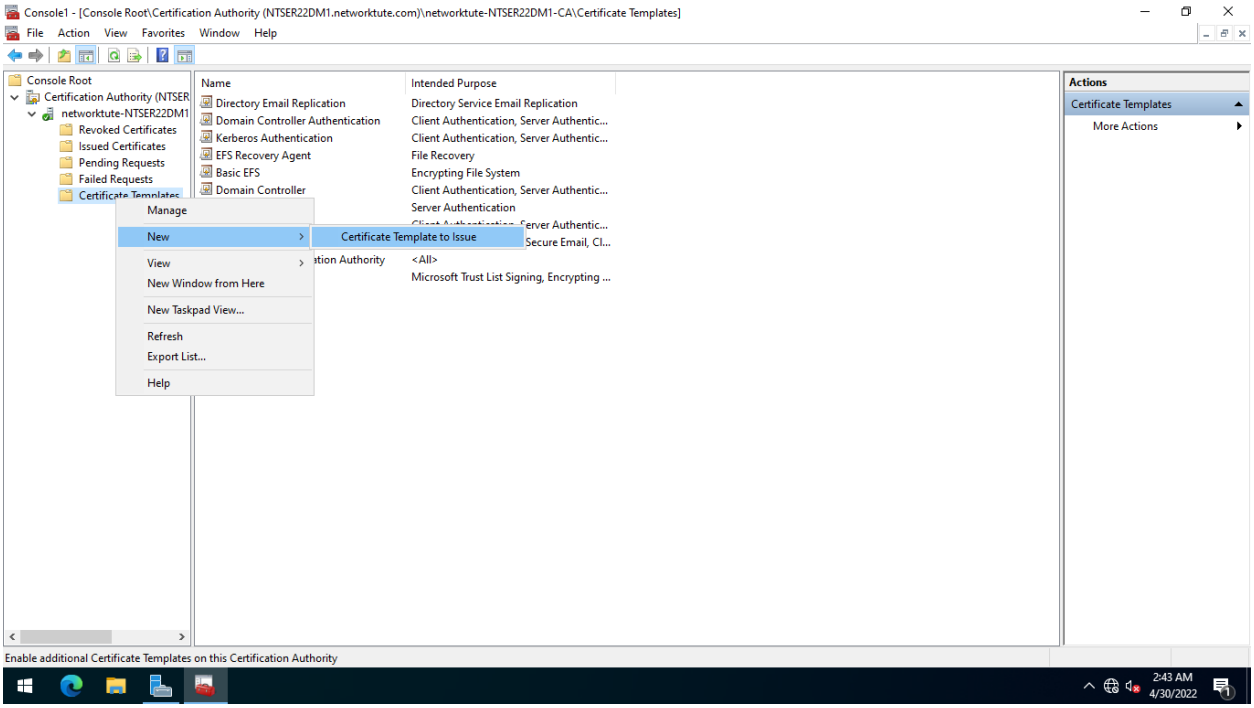


Step 16:

Next, you need to include the **SecureUser** certificate template in the list of certificates issued by **NTSER22DM1**.

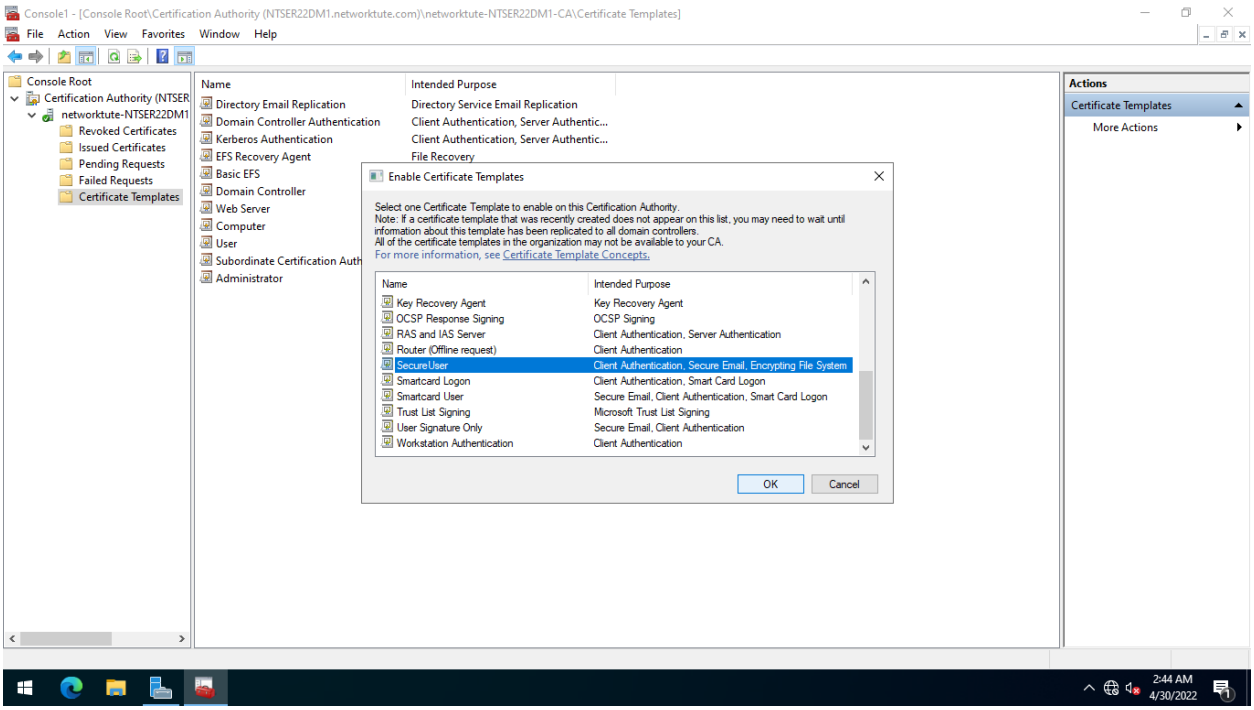
Ensure that you are back on the **Certification Authority** console window.

Right-click the **Certificate Templates** folder, select **New** and then select **Certificate Template to Issue**



Step 17:

In the **Enable Certificate Templates** dialog box, scroll down the list of templates, select **SecureUser** and then click **OK**.

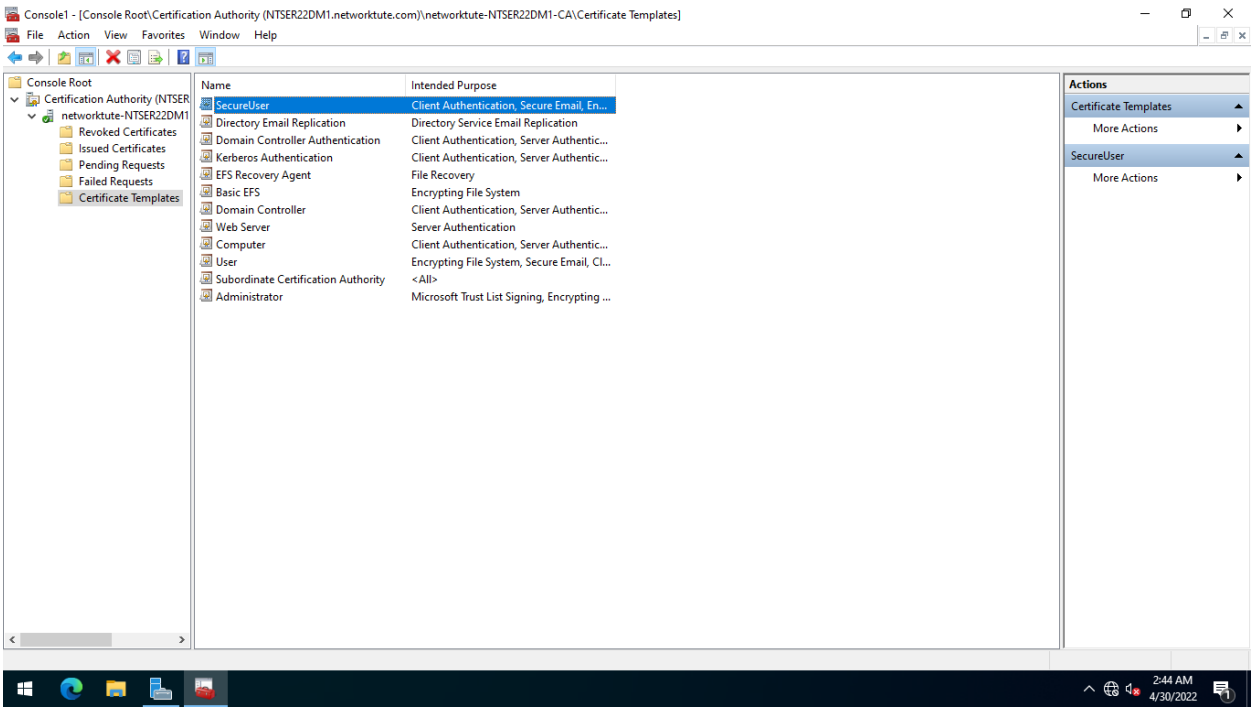


Step 18:

You have just added the **SecureUser** template as one of the certificate templates that can be issued.

Minimize the **Certification Authority** window as you will need this application in a later task

NOTE: If a system message appears stating that the certificate could not be added at this time, select Cancel. This can happen if the Certification Authority Server experiences some system delays. To add the new certificate template, repeat Step 16 from the beginning.



Task 2: Create a Group Policy for Certificate Auto Enrollment

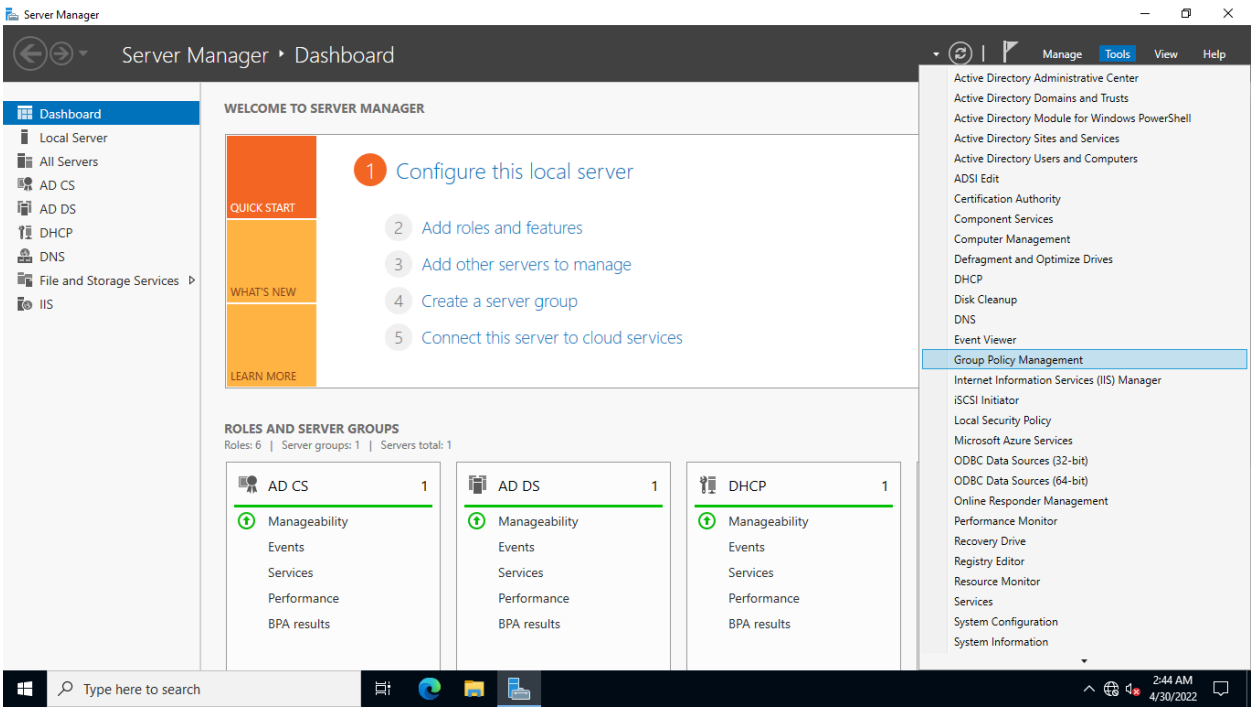
You must configure Group Policy for certificate auto enrollment in the Windows domain. When Group Policy is enabled, certificate enrollment is automated, and users and devices receive their certificates without the need for manual intervention.

We will create a Group Policy Object to automate the deployment of user certificates to domain network users.

Step 1:

Connect to **NTSER22VM1**..

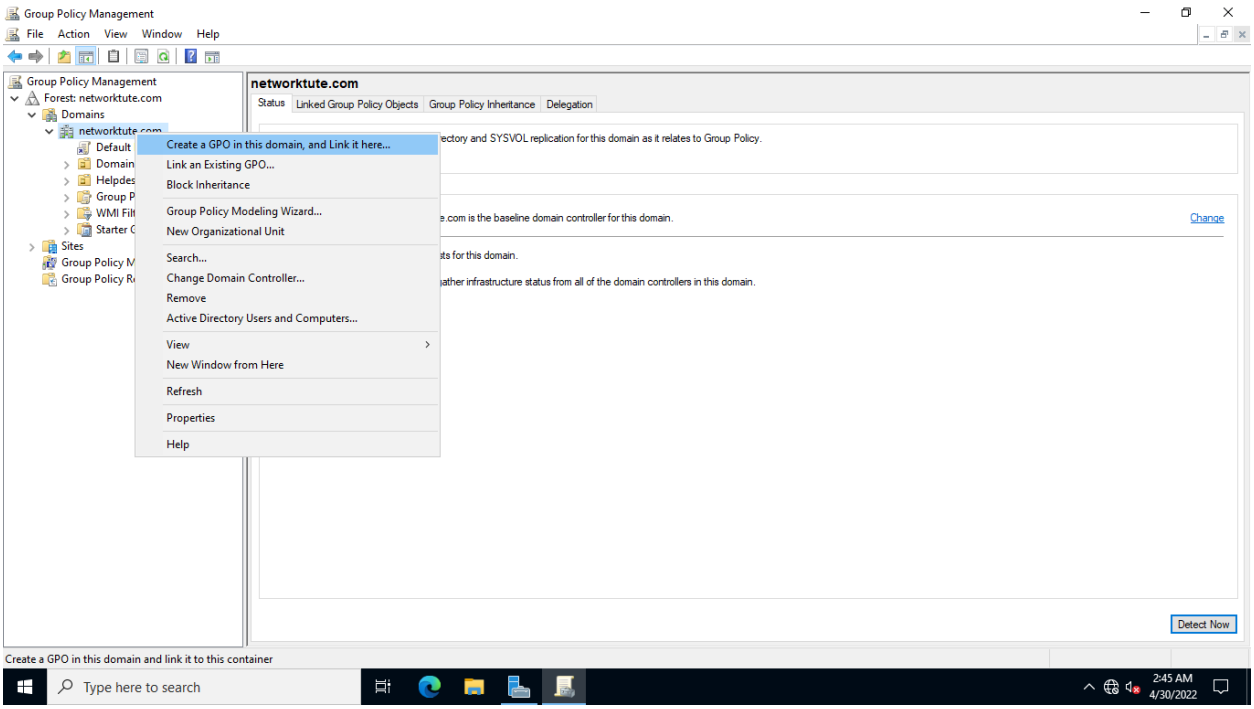
In the **Server Manager** > **Dashboard** window, click the **Tools** menu and select **Group Policy Management.**



Step 2:

In the **Group Policy Management** console window, expand **Forest**: **networktute.com** > **Domains** > **networktute.com**.

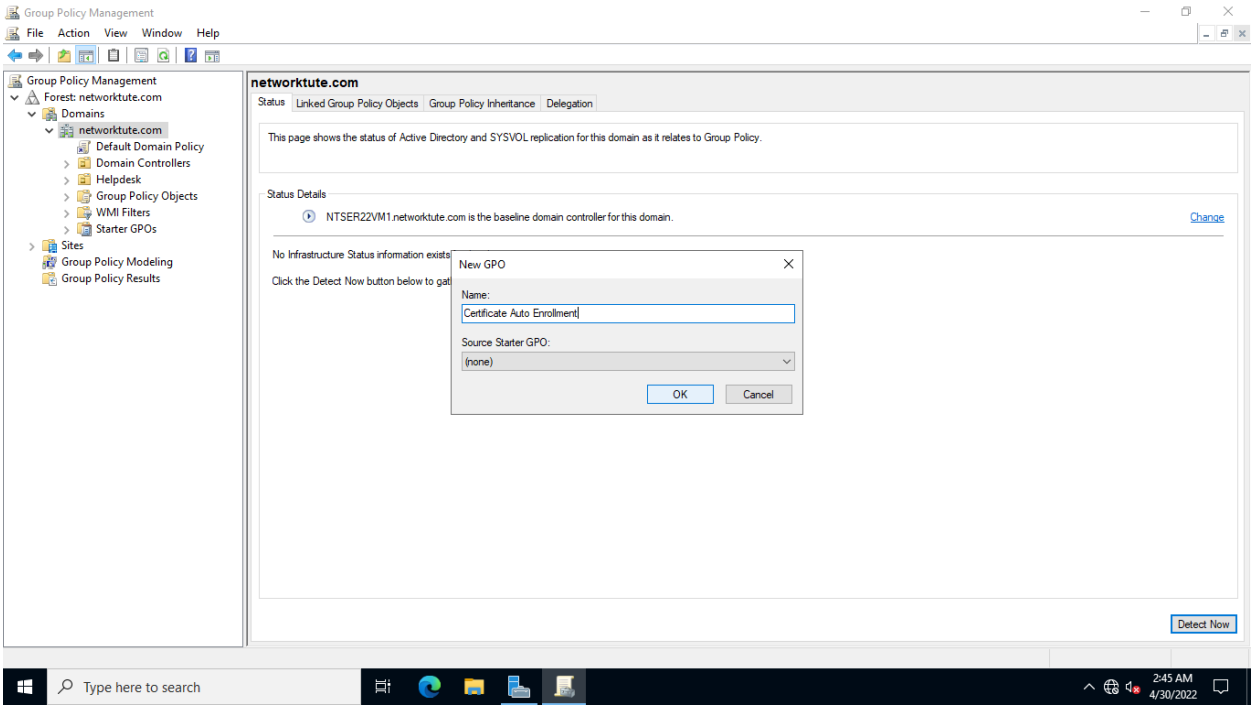
Right-click the **networktute.com** domain and select **Create a GPO in this domain, and link it here.**



Step 3:

In the **New GPO** dialog box, type the following name: ***Certificate Auto Enrollment***

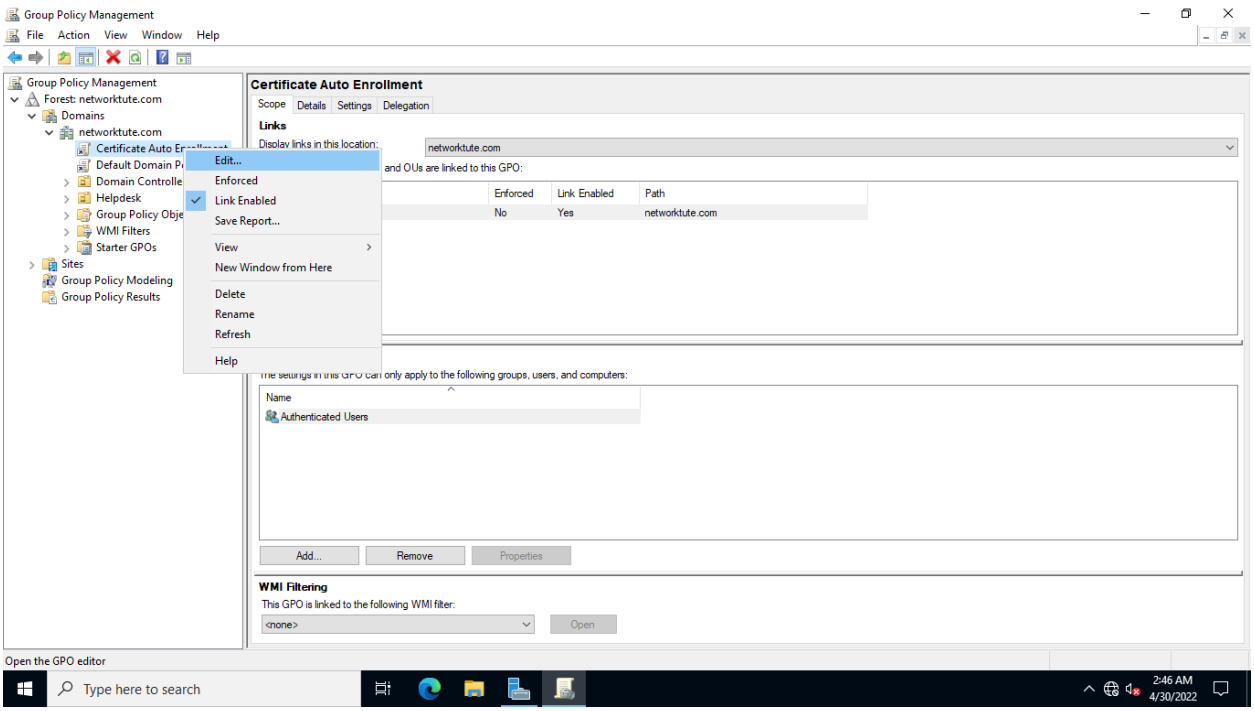
Click **OK**.



Step 4:

Right-click **Certificate Auto Enrollment** and select **Edit**.

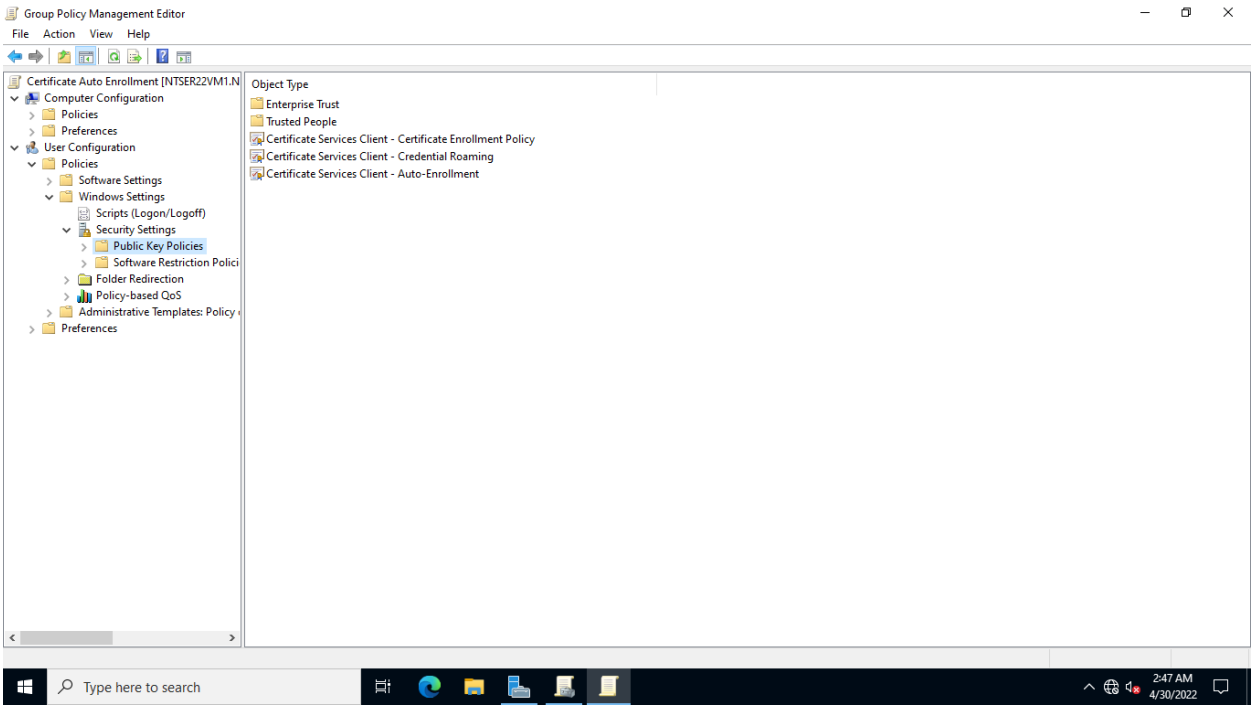
NOTE: If a message box displays in the Group Policy Management Console indicating that you have selected a link to a Group Policy Object (GPO), choose the Do not show this message again checkbox and then click OK.



Step 5:

The **Group Policy Management** Editor window opens.

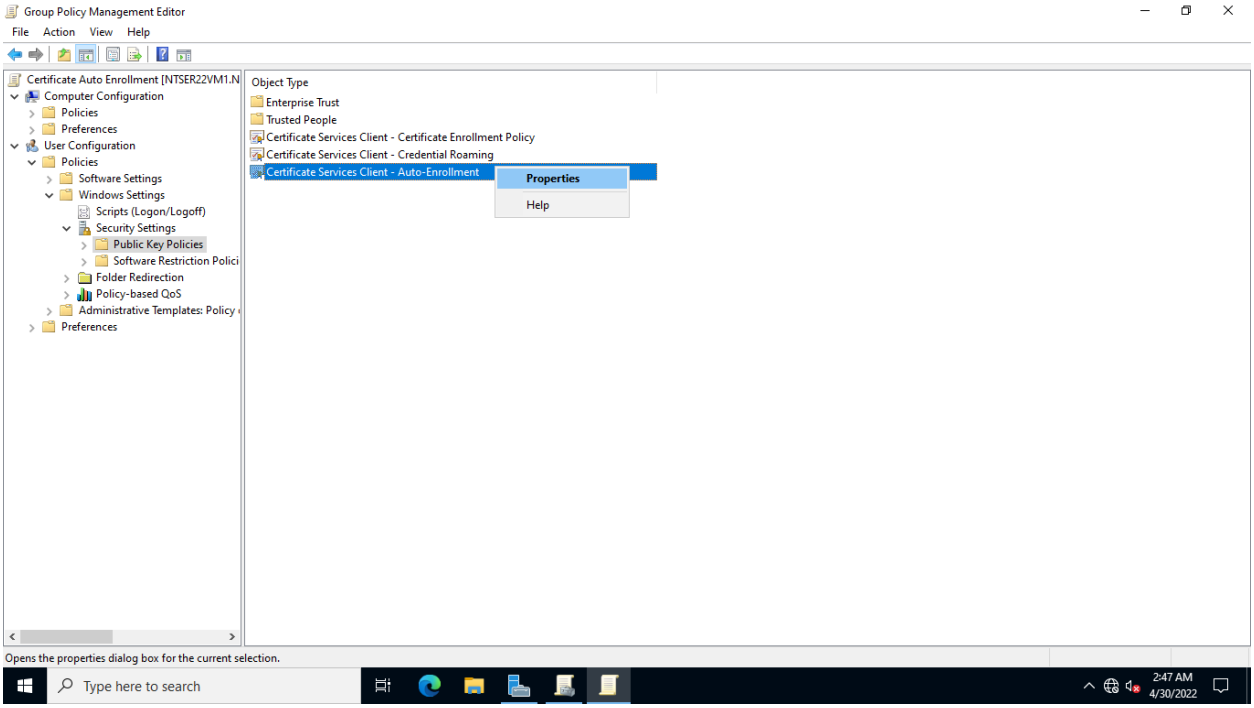
Expand **User Configuration** > **Policies** > **Windows Settings** > **Security Settings**, then click **Public Key Policies**



Step 6:

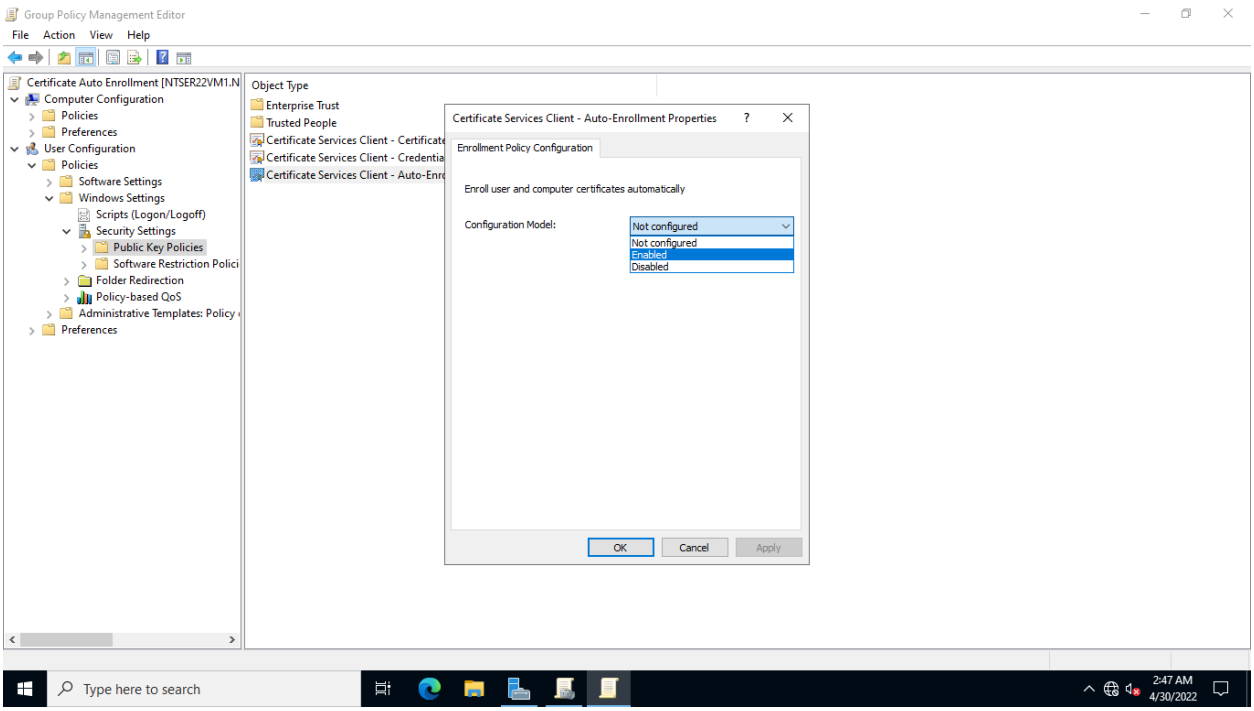
Observe the **Public Key Policies** details in the right pane.

Then, right-click **Certificate Services Client** - **Auto-Enrollment** and select **Properties**.



Step 7:

In the **Certificate Services Client-Auto-Enrollment Properties** dialog box, change the **Configuration Model** drop-down list to **Enabled**

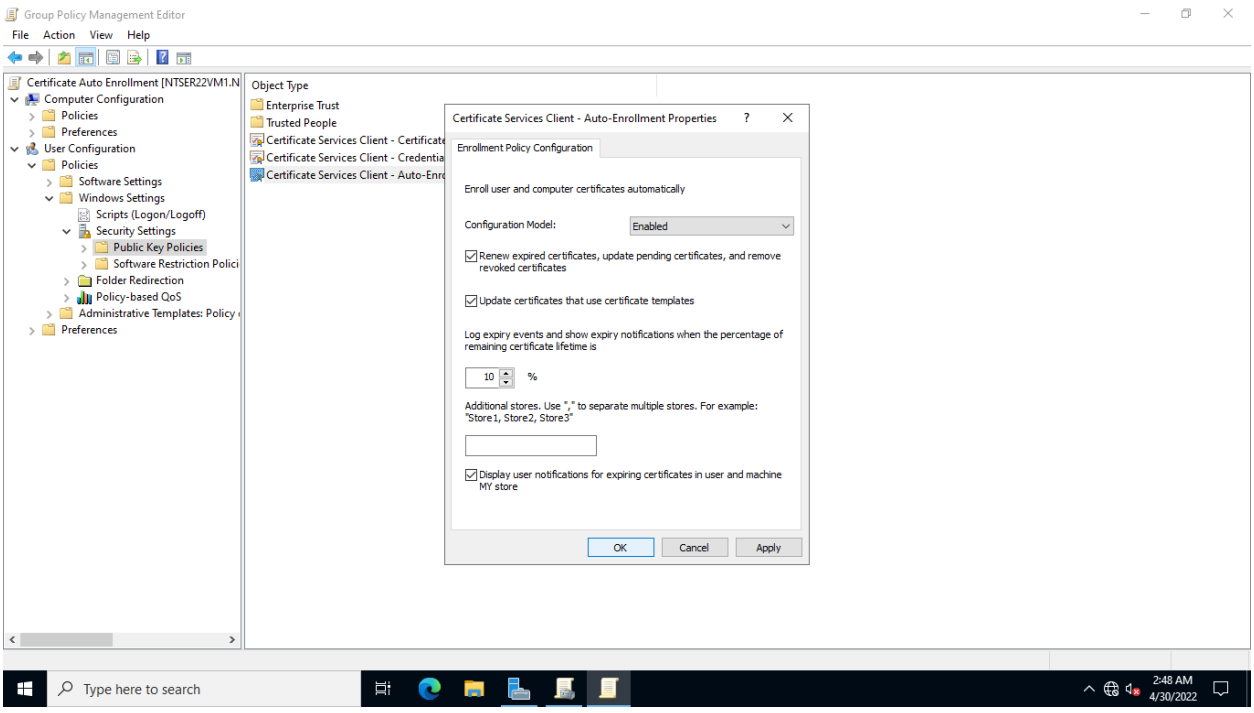


Step 8:

Select the following checkboxes:

- Renew expired certificates, update pending certificates, and remove revoked certificates
- Update certificates that use certificate templates
- Display user notifications for expiring certificates in user and machine MY store

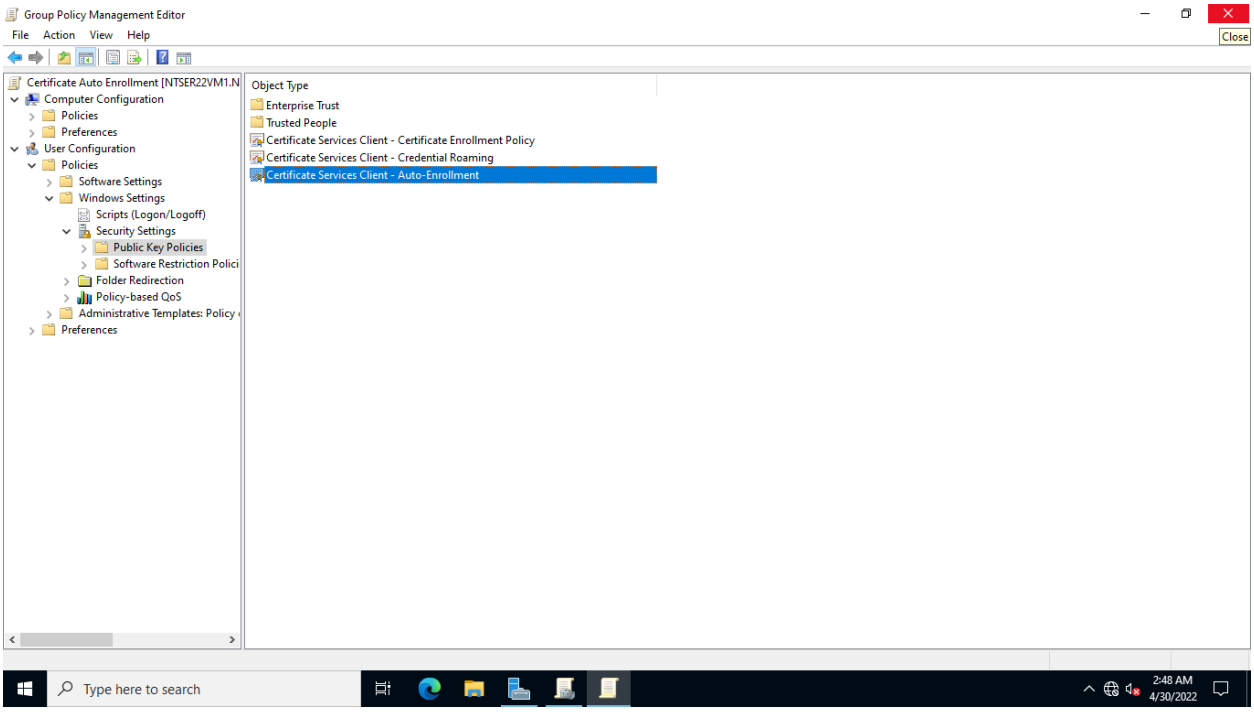
Several checkboxes will become enabled as a result and Click **OK**.



Step 9:

Close **Group Policy Management** Editor application window.

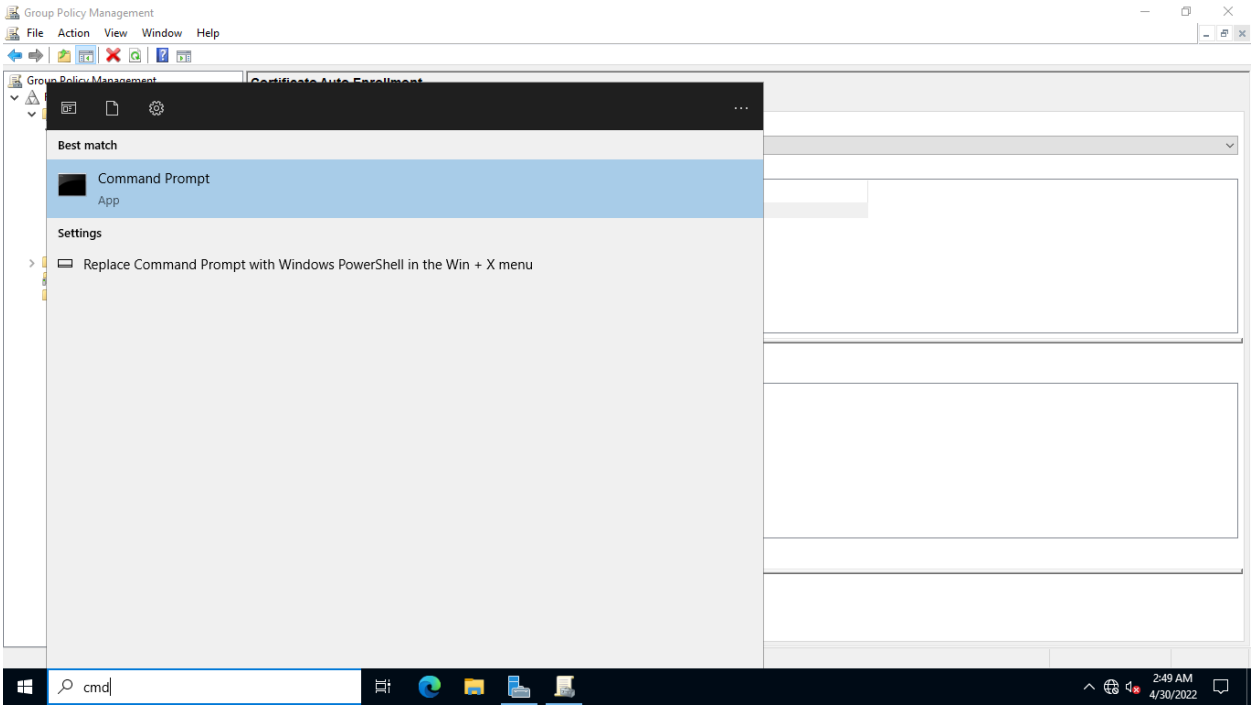
Similarly, exit from the **Group Policy Management** console window.



Step 10:

Click **Start** and type the following: ***cmd***

Click **Command Prompt**.



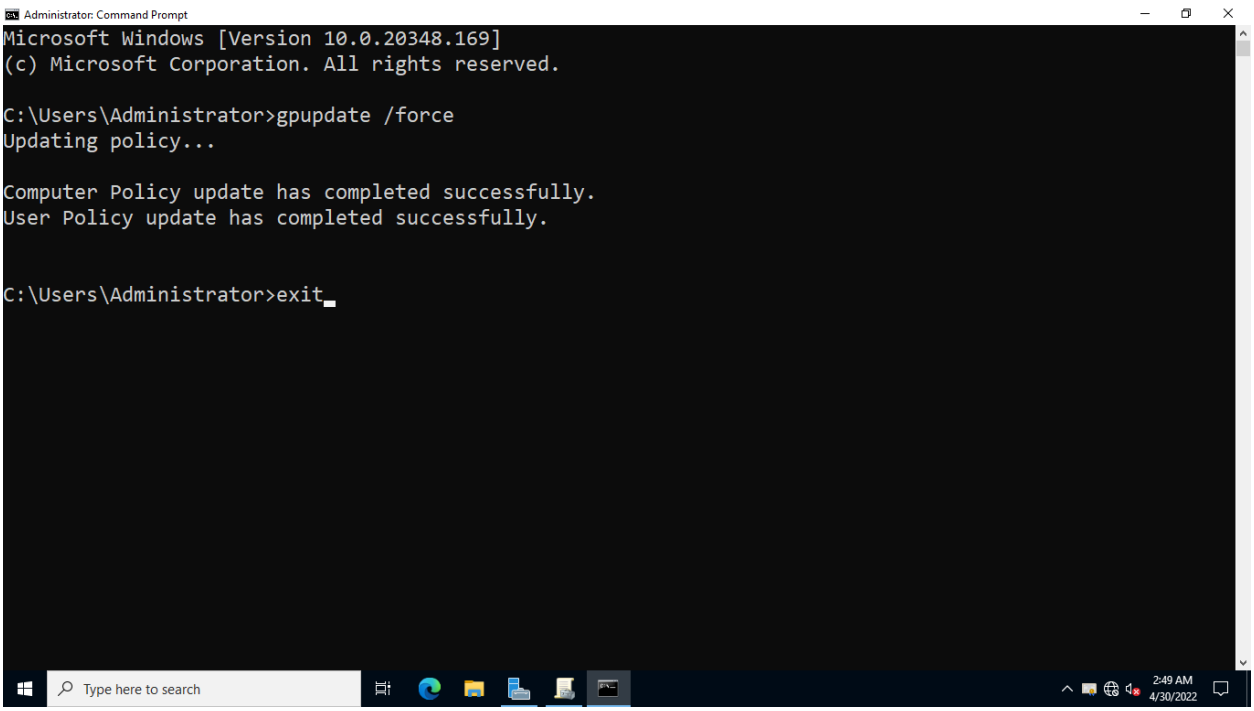
Step 11:

To propagate the new user Group Policy settings to the domain, type the following command: ***gpupdate /force***

Press **Enter**.

On the next prompt, type the following command: ***exit***

Press **Enter**.



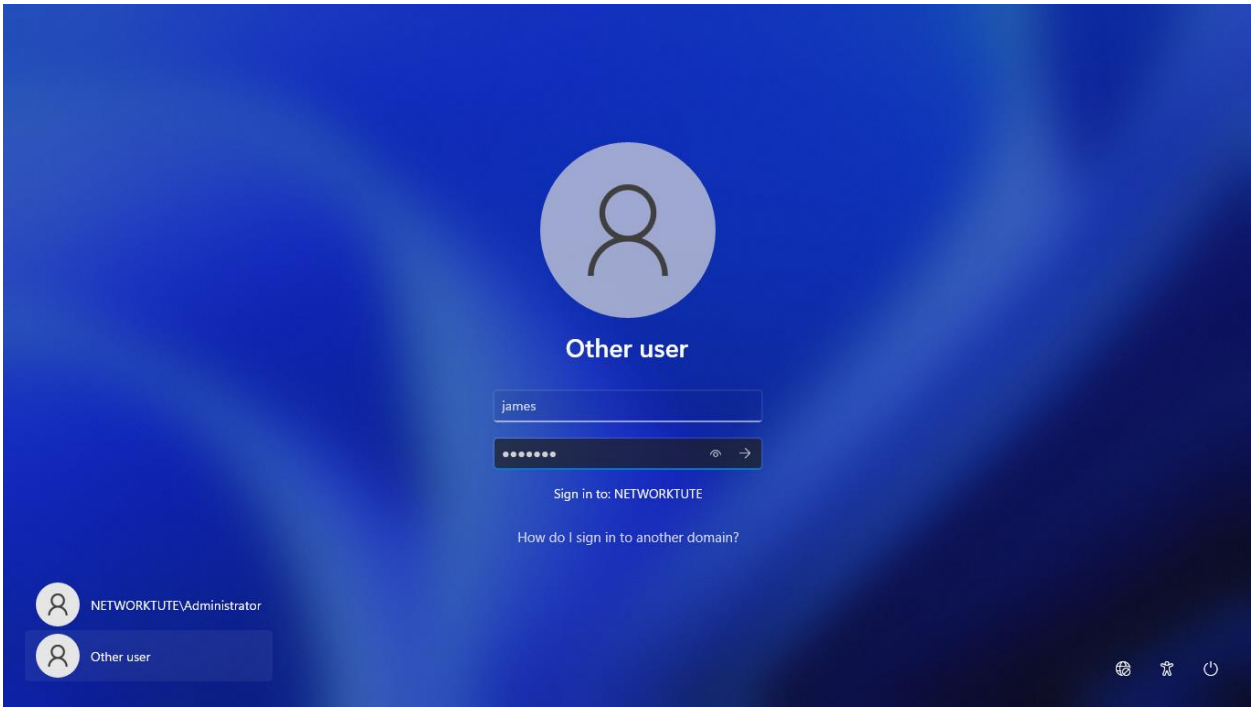
Task 3: Verify the Certificate Issuance

After creating the certificate auto enrolment policy in the preceding process, sign on as a domain user in the IT organizational unit and verify that the user has received a certificate.

Perform the following steps to confirm certificate issuance:

Step 1:

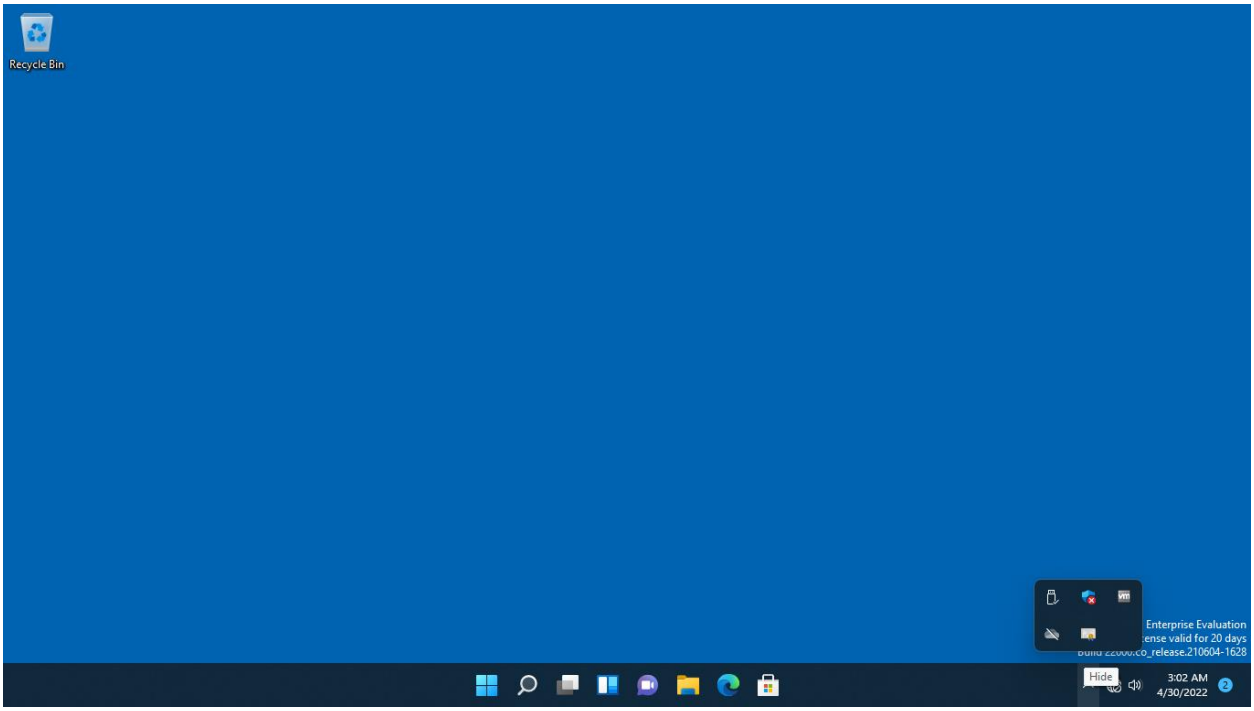
Connect to **NTWIN11VM1.** Use ***james*** account



Step 2:

When signed in, access the system tray and click the arrow to expand.

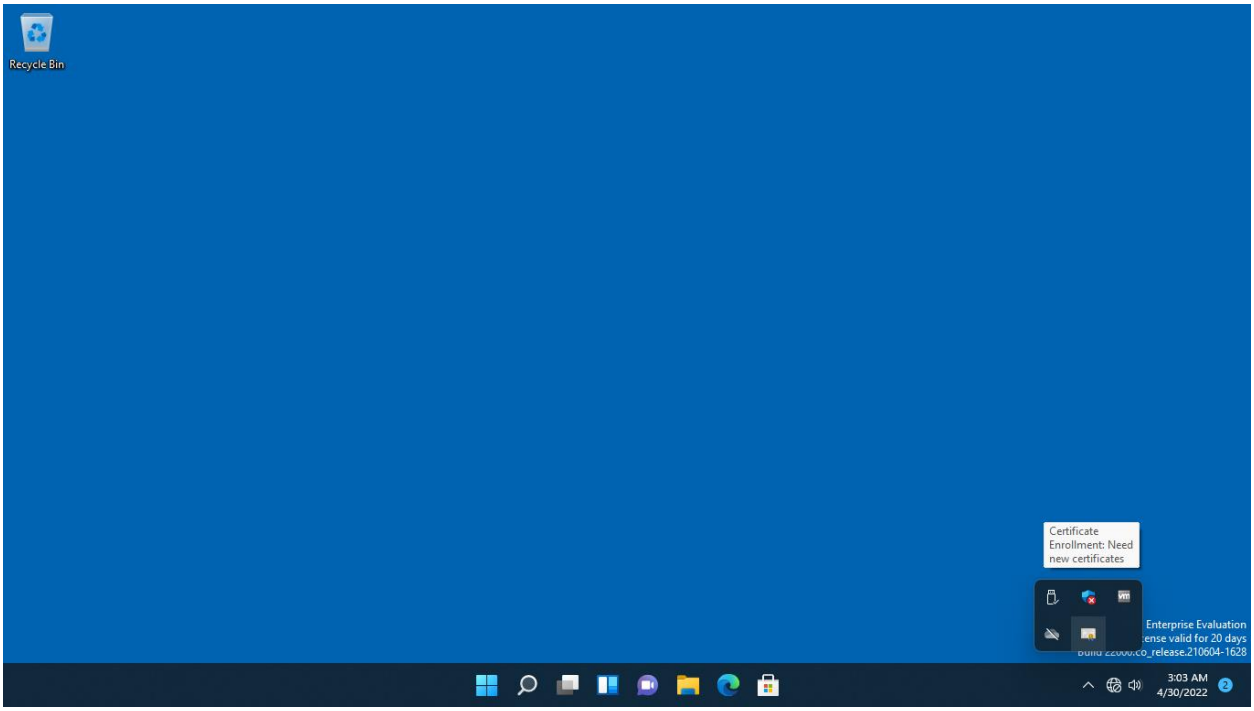
You should get a certificate icon.



Step 3:

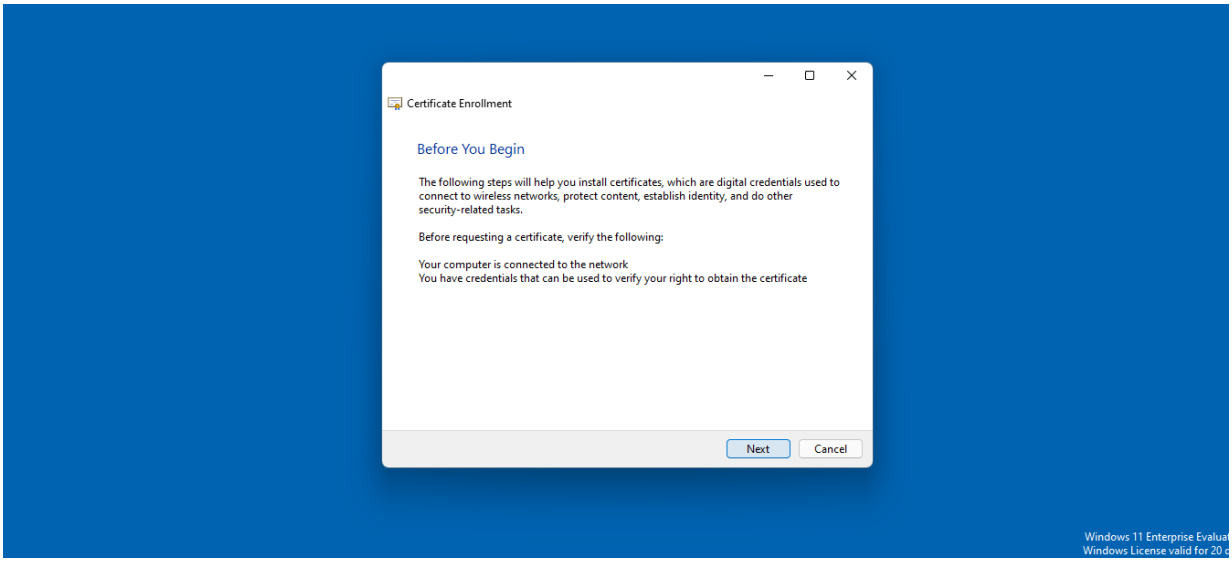
Then click on the certificate icon to proceed with the enrollment of the user certificate for ***james***

Important: The certificate symbol will display in the system tray after a brief delay of roughly 1 minute. If you don't get a certificate, use **gpupdate /force** at a command prompt. On the system tray, a certificate icon will display. Sign out and back in as **james** if no certificate icon shows.



Step 4:

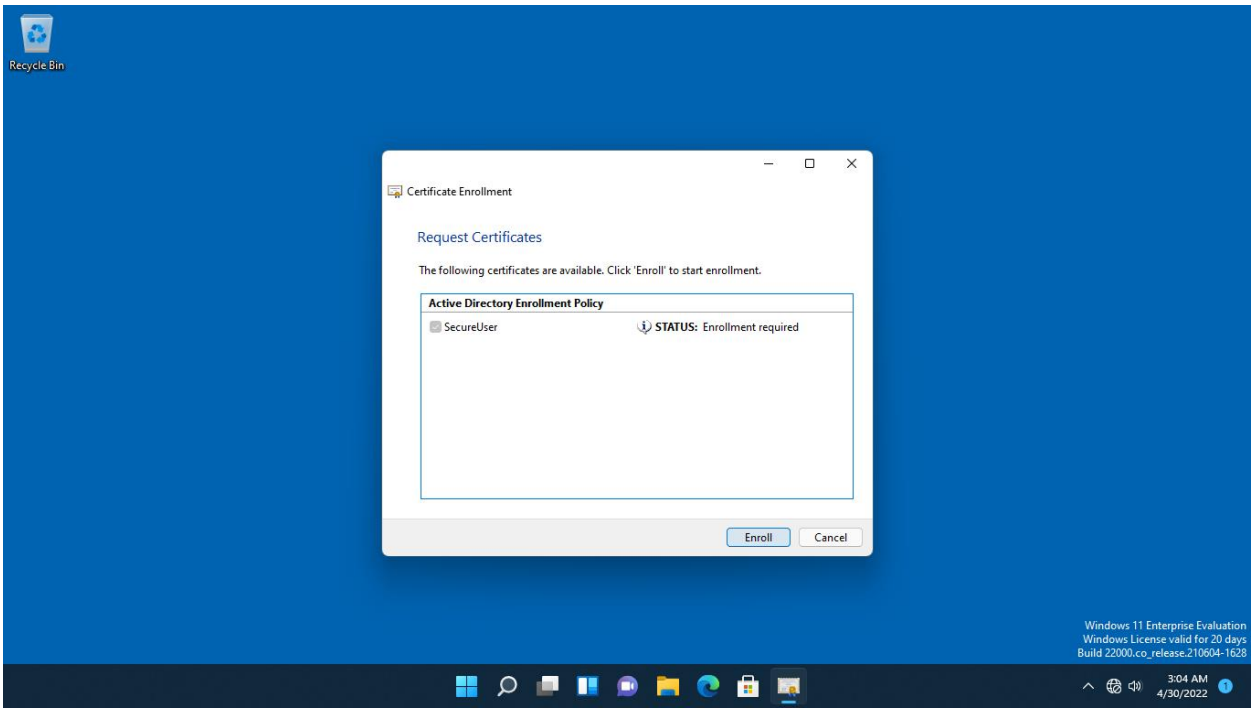
On the **Before you begin** page of the **Certificate Enrollment** wizard, click **Next**.



Step 5:

The **Request Certificates** page will display the **SecureUser** certificate template that you created earlier

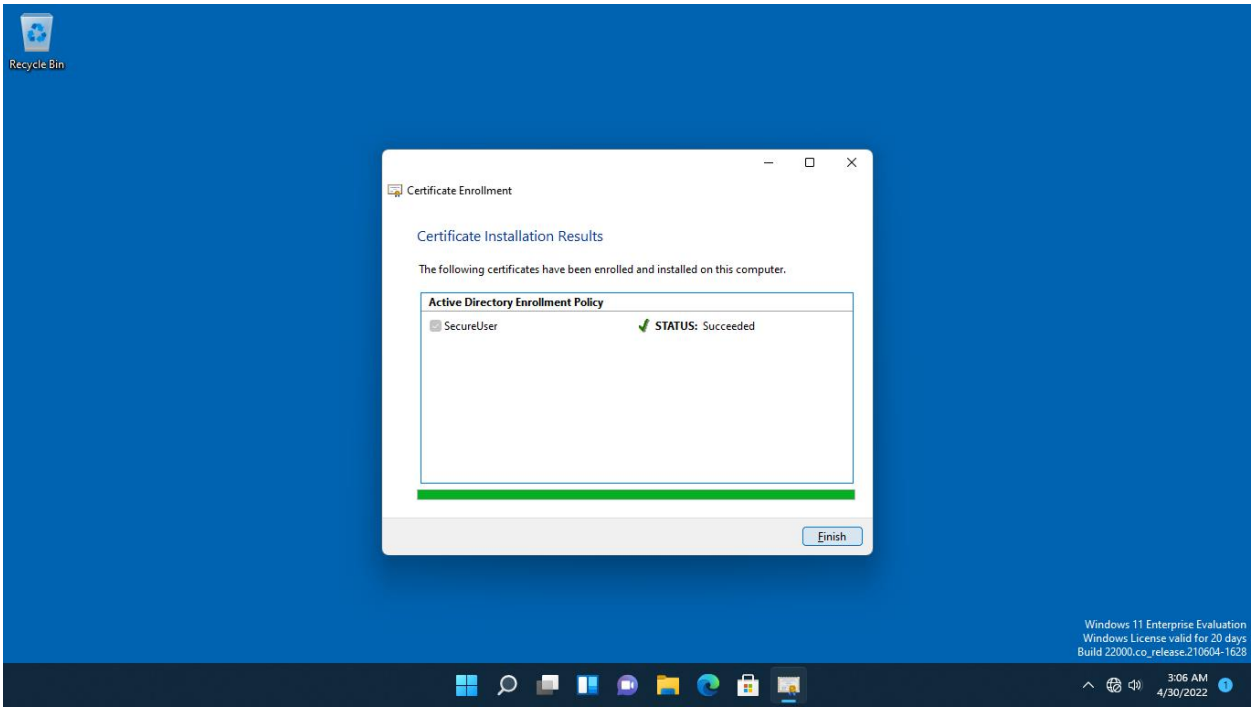
Click **Enroll**.



Step 6:

The **SecureUser** certificate template has been successfully enrolled for James. If there is an existing e-mail server on the network, the certificate granted to **James** can be used for a variety of tasks, including securing her data using **EFS** and sending encrypted e-mail messages.

Click **Finish**.



Step 7:

Right-click **Start** and mouse over **Shut down or sign out**.

Then, select **Sign out**.