

# **Lab 8: Implementing AD Certificate Services**

By: Ethan Holmes

## Table of Contents

Lab 8: Implementing AD Certificate Services.....	1
Introduction:.....	3
Activity 8-2:.....	3
Activity 8-3:.....	6
Activity 8-4:.....	7
Activity 8-5:.....	8
Activity 8-6:.....	9
Activity 8-7:.....	11
Activity 8-8:.....	13
Activity 8-9:.....	16
Activity 8-10:.....	18
Activity 8-11:.....	21

### Introduction:

In this lab we will learn about creating a certificate authority machine that can assign certifications to other machines and users on the network, as well as backing up these certifications and private keys and restoring them from deletion.

### Activity 8-2:

To start this lab, we must first install the AD CS role on our DM1 server, we can install the CA role as well as adding on the Web Enrollment roll so we can get access to IIS and dealing with certificate renewal and retrieval.

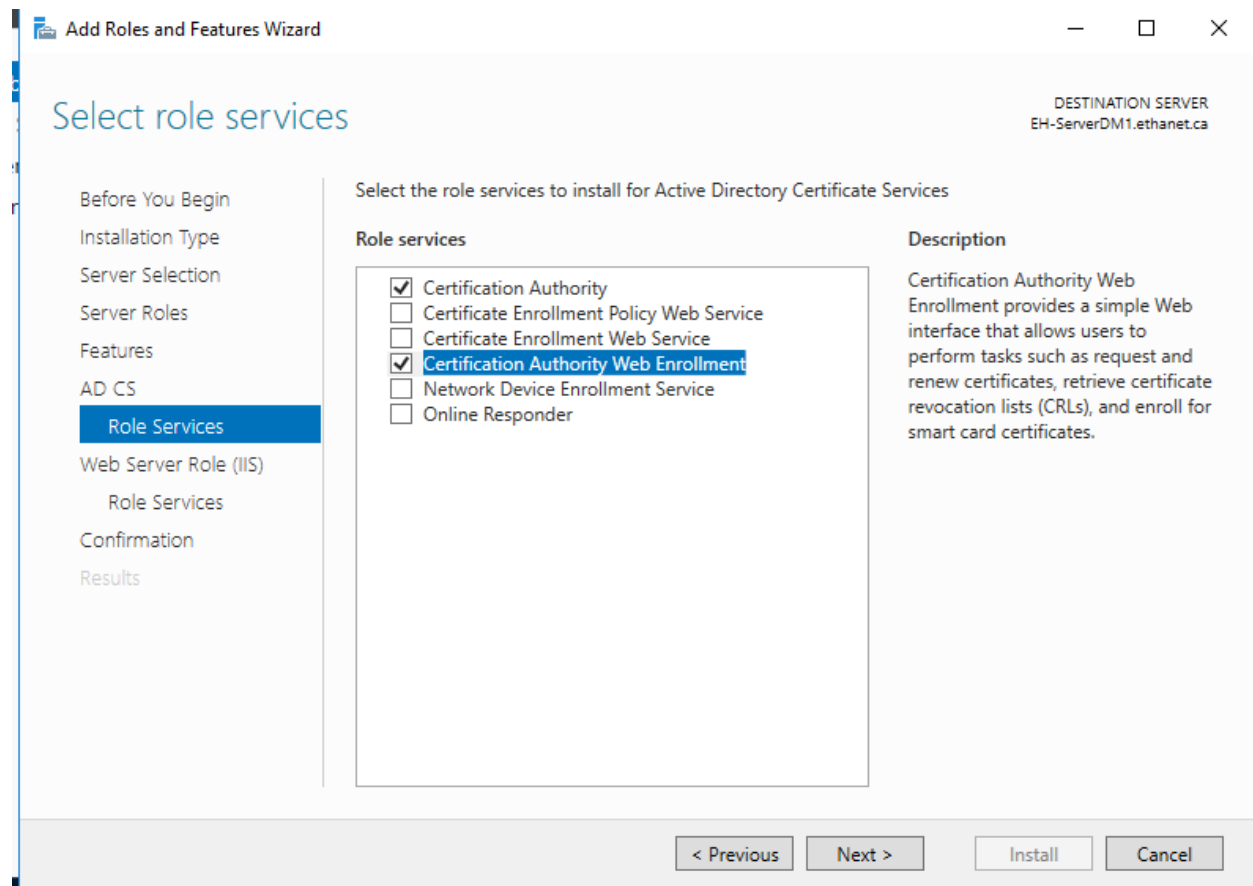


Figure 1: Installing role services

Once this has finished, we can then set up the Certification Services, making the machine an Enterprise certificate authority.

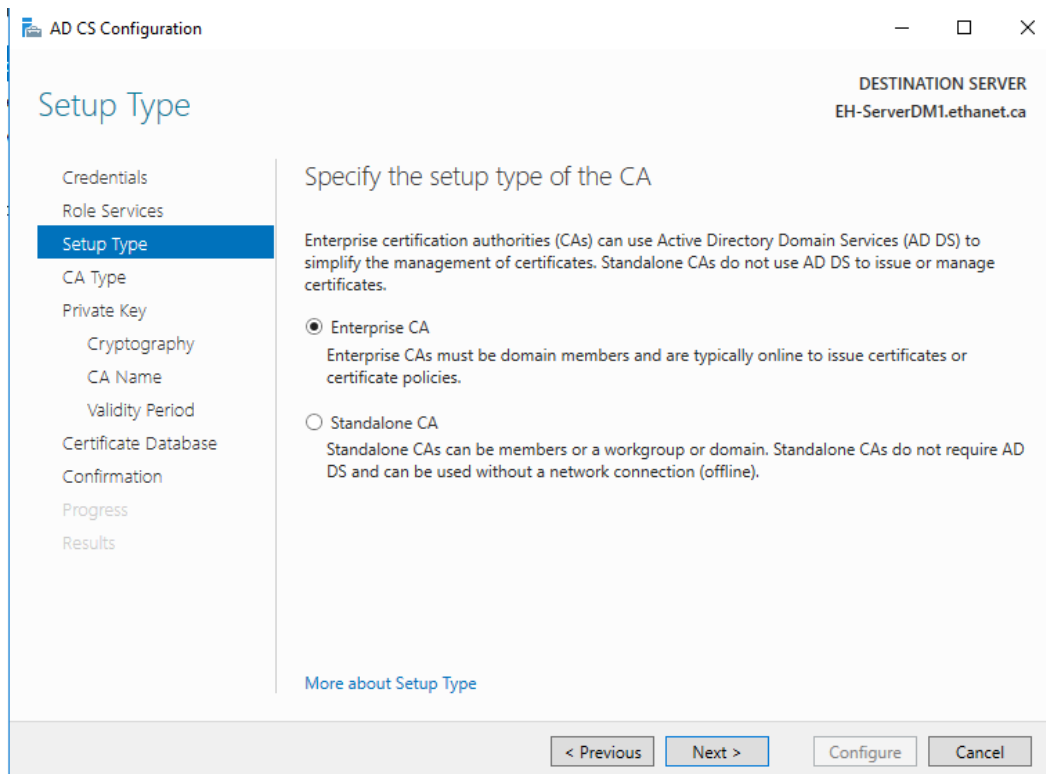


Figure 2: Setting up an Enterprise CA

From this point forward, we can accept the defaults for the machine. Once done, we can run a `certutil -viewstore` and see the created cert

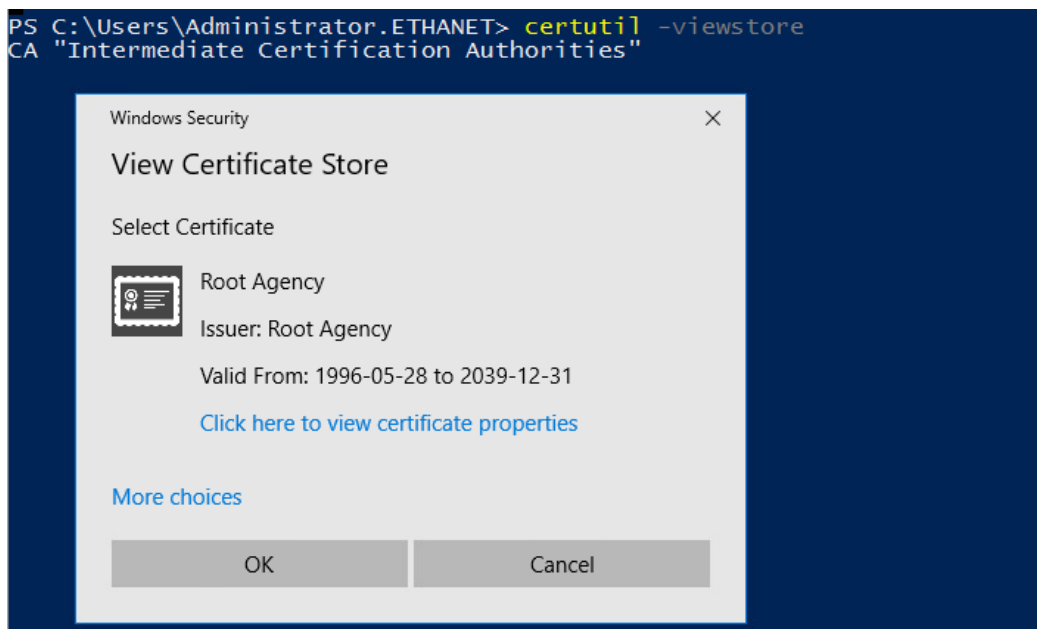


Figure 3: Viewing the Certificate Agency

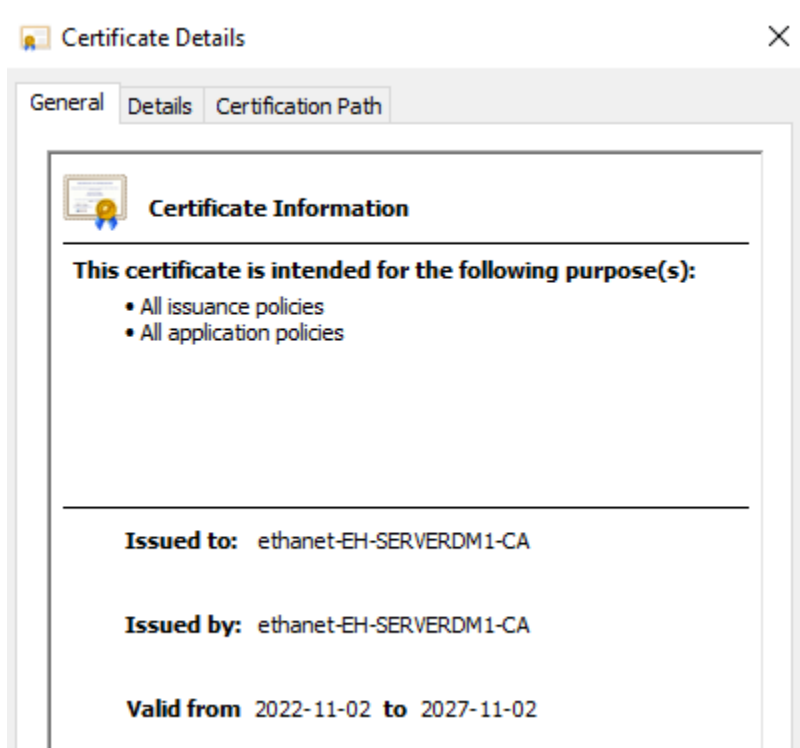


Figure 4: Details of certificate

## Activity 8-3:

In this part, we will create an EFS Certification template. In the Certificate Templates Console we can right click the “Basic EFS” Certificate and create a new template from this as seen in the figure below

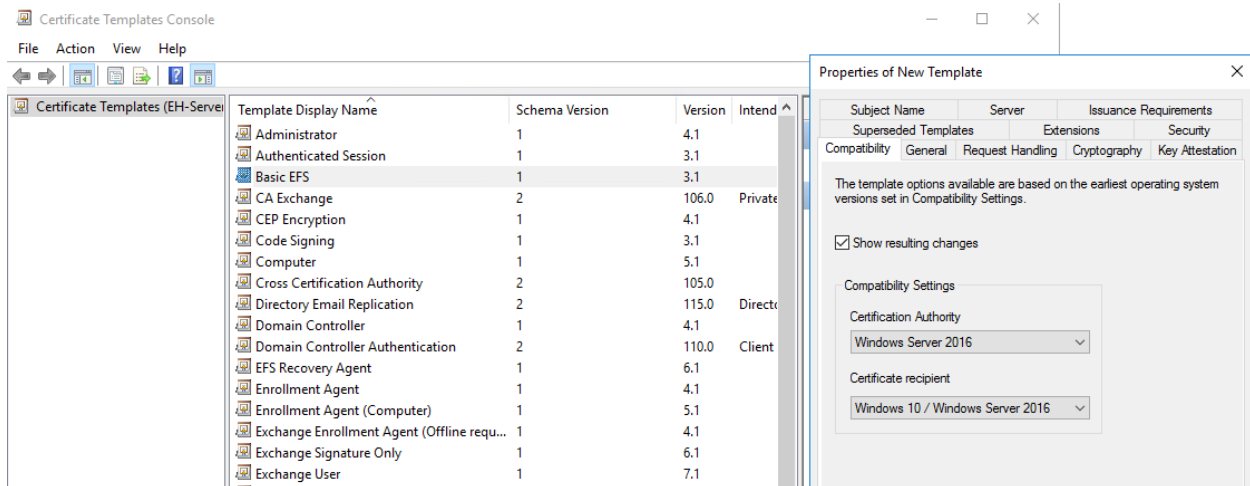


Figure 5: Cloning the Basic EFS template

After creating this template, we can suspend the default “Basic EFS” certificate to make sure that our newly created EFS-2016 certificate is the only one being issued.

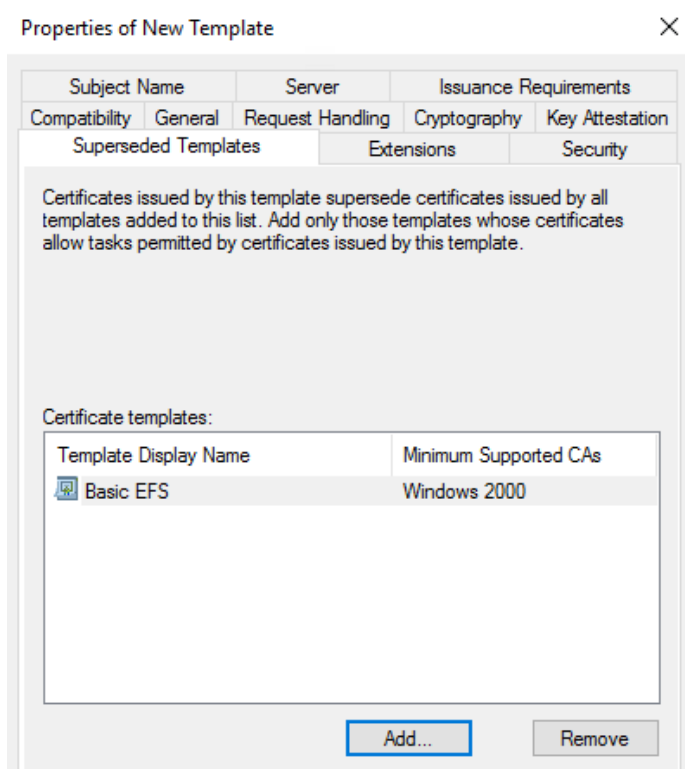


Figure 6: Suspending the Basic EFS template for the newly created one

## Activity 8-4:

In this Activity, we will configure autoenrollment for EFS, we can create a GPO for AutoEnrollment in the Group Policy Management Editor, we can create the GPO, and then under “Public Key Policies” turn on the Auto-Enrollment service.

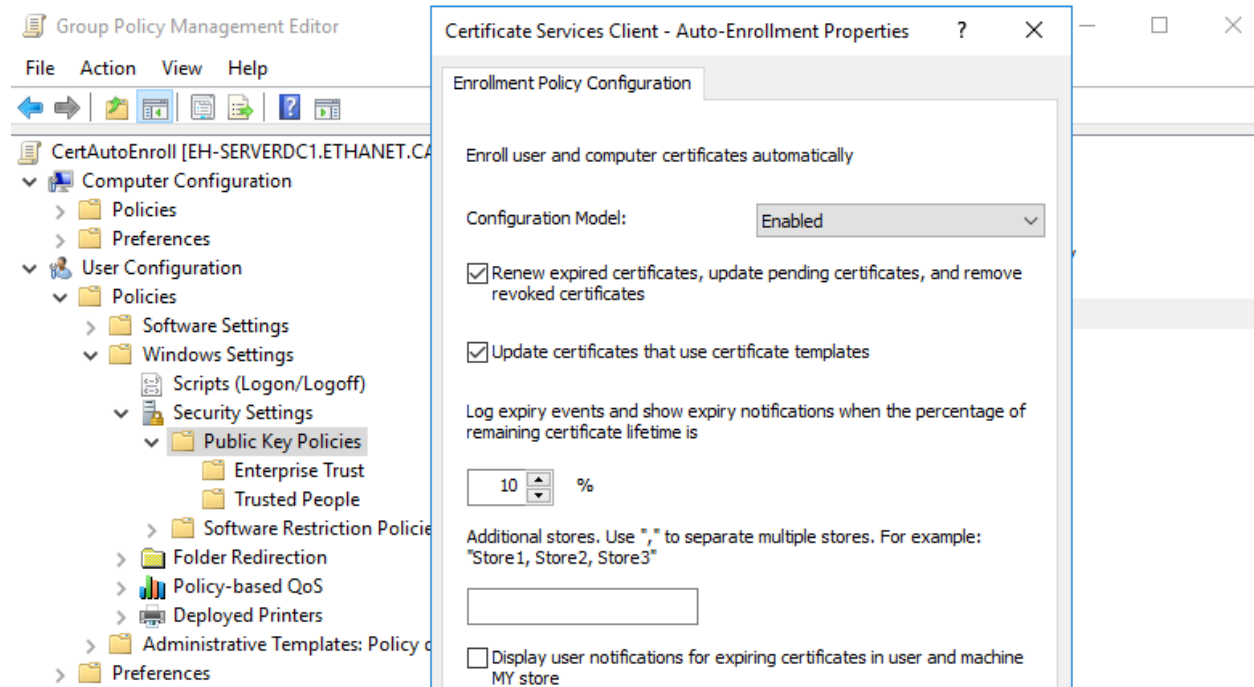


Figure 7: Configuring the autoenrollment property

We can link this GPO to our domain after its creation. We can then go back to our DM1 Machine and go to our Certificate Template Console, which we can then Allow domain users to use the Autoenroll permission.

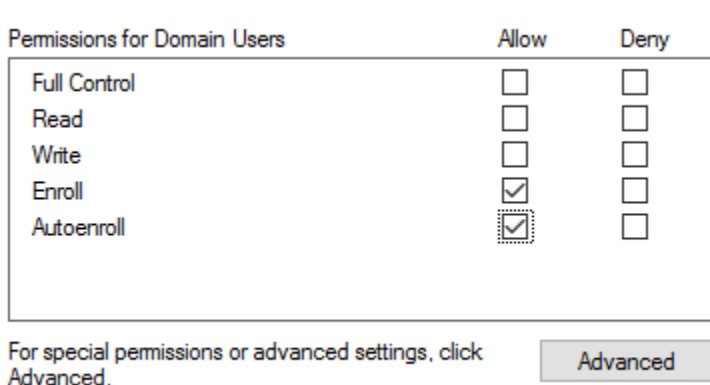


Figure 8: Setting up Autoenroll for domain users

Once this is done, we can go back and right-click the Certificate Templates folder, click Certificate template to issue, and issue our EFS-2016 certificate to our domain.

### Activity 8-5:

In this step, we will test our certificate. After signing into our domuser1 account on the DM1 server, we can open the MMC and add a snap-in for Certificates. Under the Personal section, we can see our domuser1 has been issued a certificate from DM1 with the EFS-2016 template

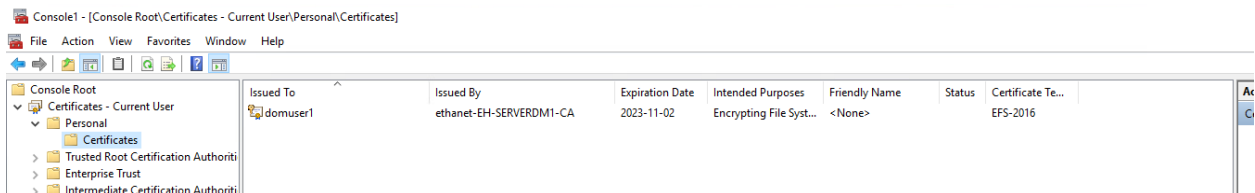


Figure 9: domuser1 certificate issued

Underneath the “Trusted Root Certification Authorities” folder, we can see that server DM1 has been added as a trusted CA

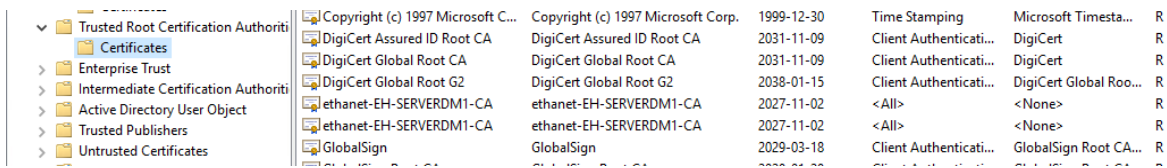


Figure 10: DM1 is a certified authority



### Activity 8-6:

In this activity, we will finish the installation of IIS and request a certificate from our CA machine. Once IIS has been properly installed, we can then create a new domain certificate on IIS, which should look something like this:

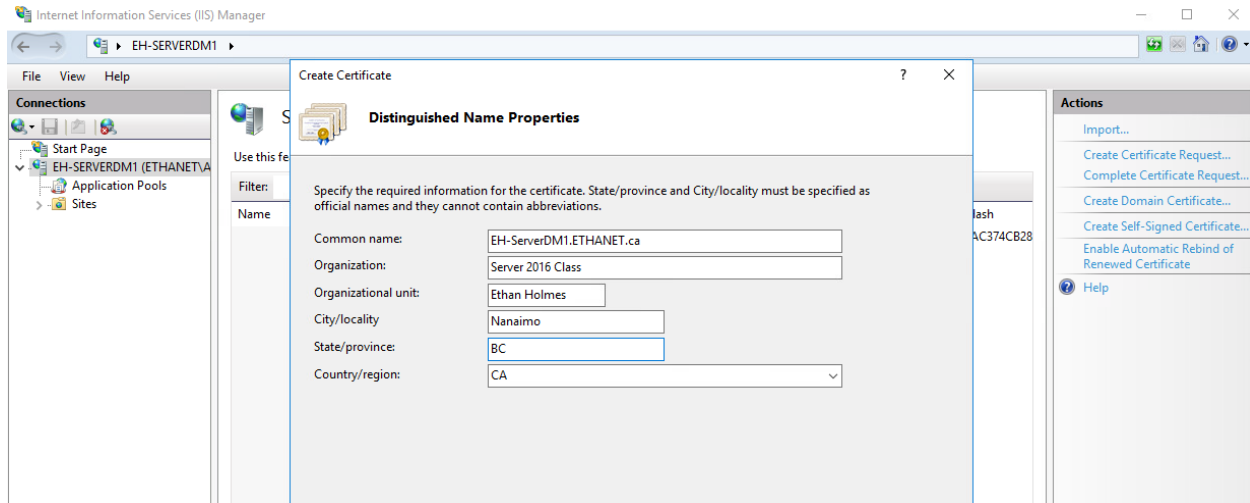


Figure 11: Creating a domain certificate

On the following page, we can specify our DM1 machine as the CA for certificate, give it a friendly name and then finish the creation. We can then next configure the default site to require our Certificate as well as give it a binding to our CA

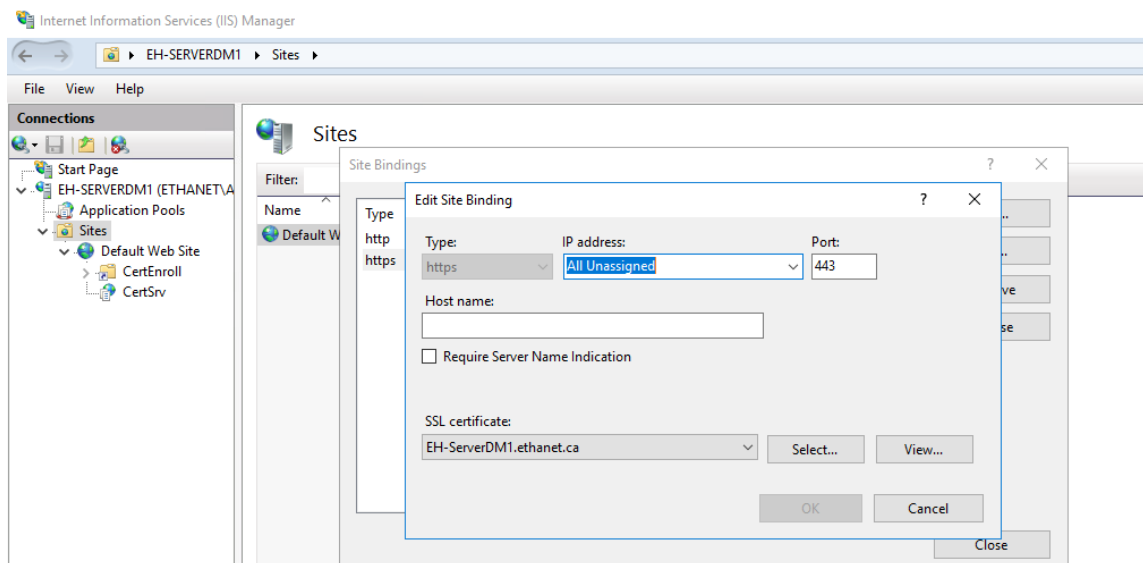


Figure 12: Making a site binding for IIS

Once configured, we can navigate to the URL of our certsrv (this can be seen in the figure below) and then we should be prompted to enter a username and password to go any further, we will enter domuser1 as that is the user that has a certificate generated for it already. We should then be created with the following screen:

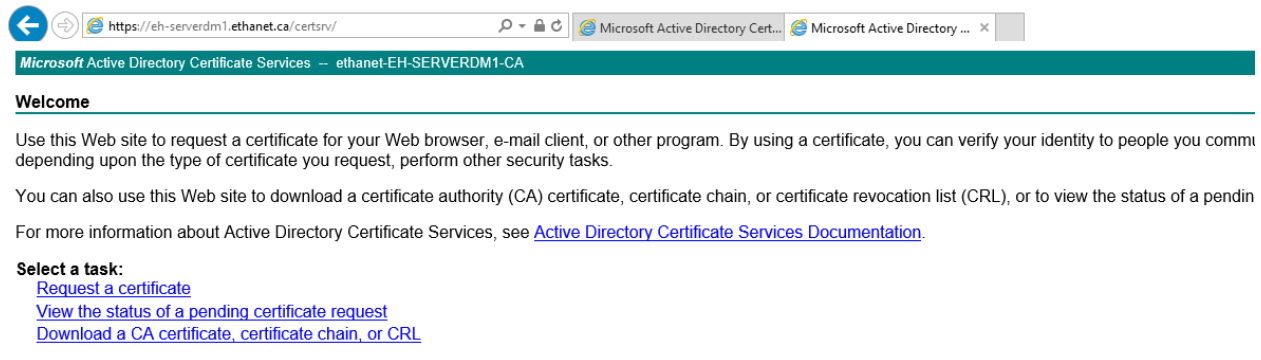


Figure 13: Certificate Service through IIS created

We can click “Request a certificate” and on the next page click “User Certificate” and then click yes to the following Web Access Confirmation popup.

#### Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

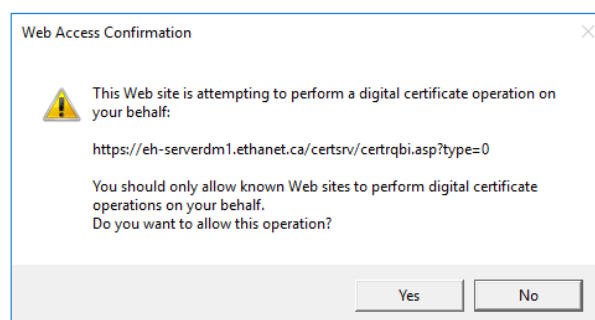


Figure 14: User certificate created

Click submit to generate the request, and then once again click yes on the following box

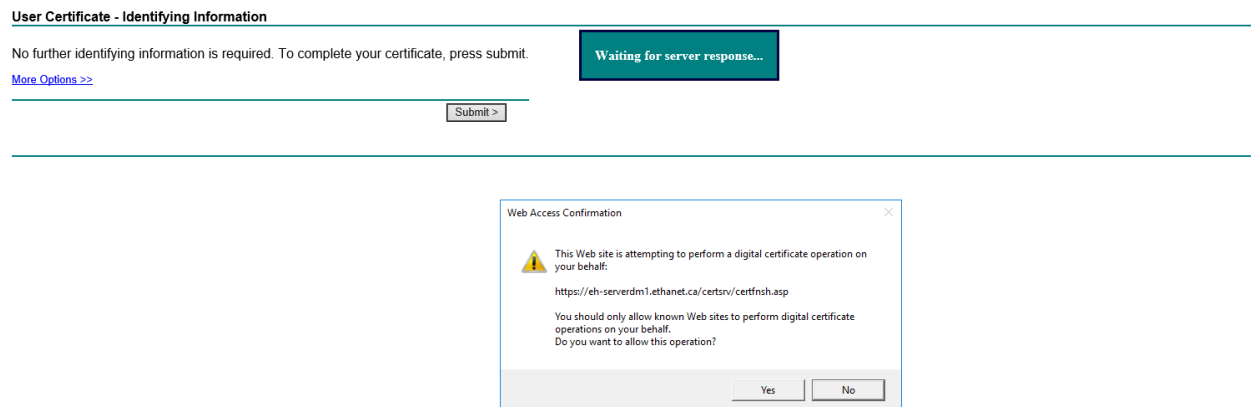


Figure 15: Submitting and waiting for server response

You will then be given a link to install your certificate, click it and after a few second you will see a page telling you that your certificate has been installed.

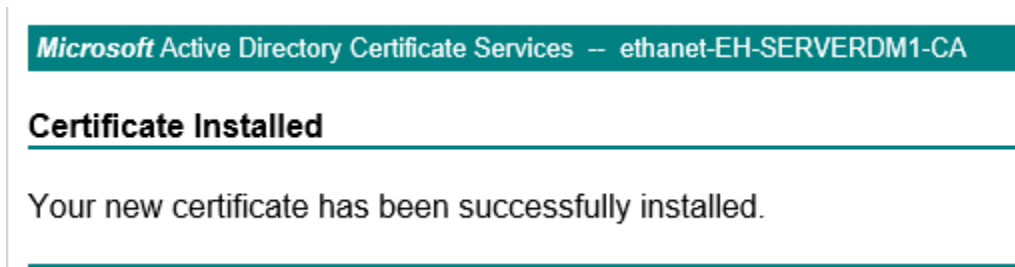


Figure 16: Successful certificate installation

#### Activity 8-7:

In this activity, we will configure the online response for certificates. To start, we will duplicate the OCSP Response signing, like what we did in the previous activity with the ERS certificate. This time we will make sure to select the "Publish certificate in Active Directory" box and in the Security tab, we will add a computer object and add DM1 to our permissions list with Enroll and Autoenroll selected.

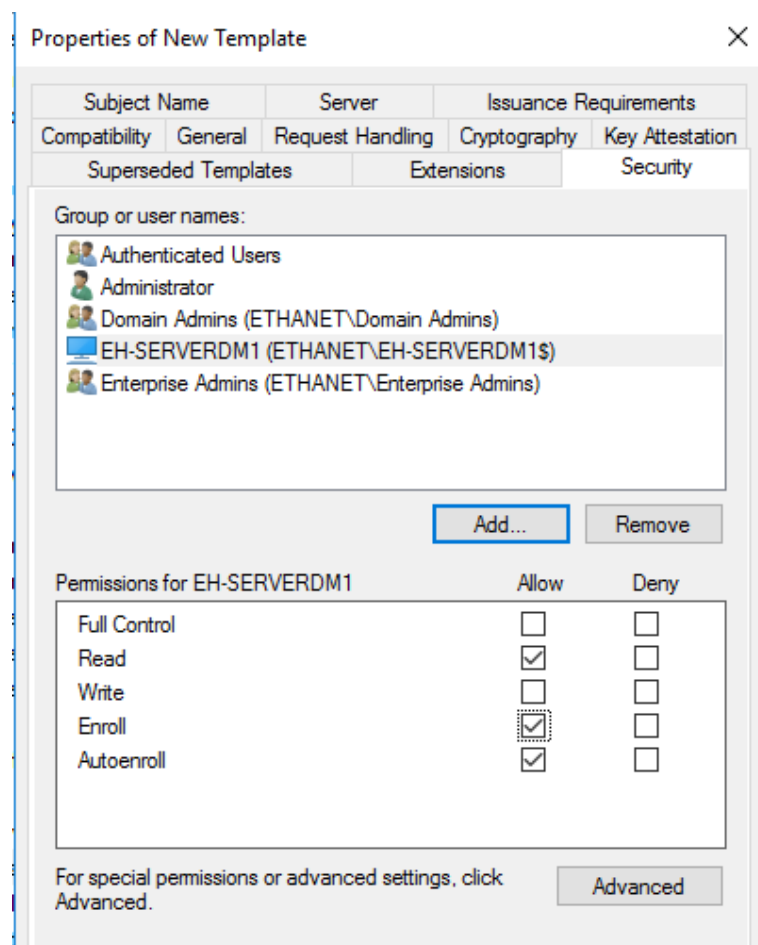


Figure 17: Adding serverDM1 as an autoenroll machine

After this, we must then inform our CA of the location of the online responder. Which after issuing the template, we can right-click the node, and under extensions change to an AIA extension and then select the HTTP option. Restart the AD CS when it asks.

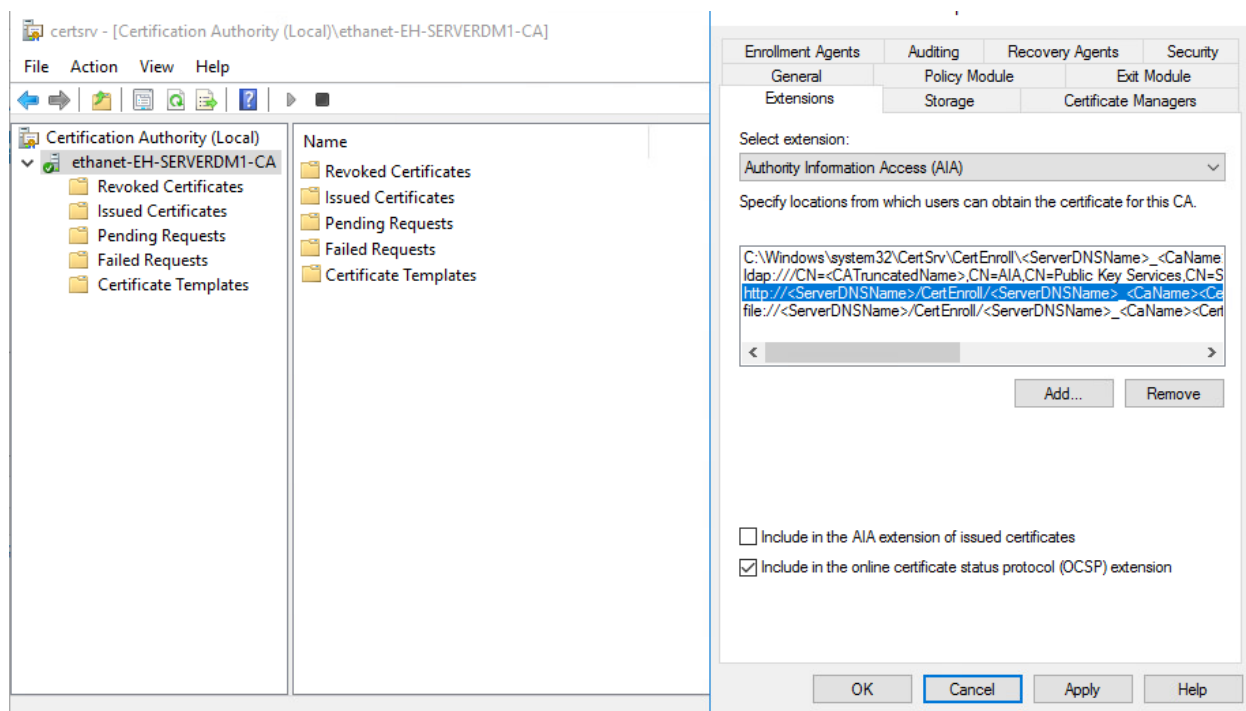


Figure 18: Adding the HTTP location to obtain certificates

#### Activity 8-8:

In this step, we will request the ocsp certificate to be signed in order to avoid restarting the machine. Inside MMC, we can add the certificates (Local Computer) snap-in, and under personal, then right click the certificates folder and select "Request New Certificate"

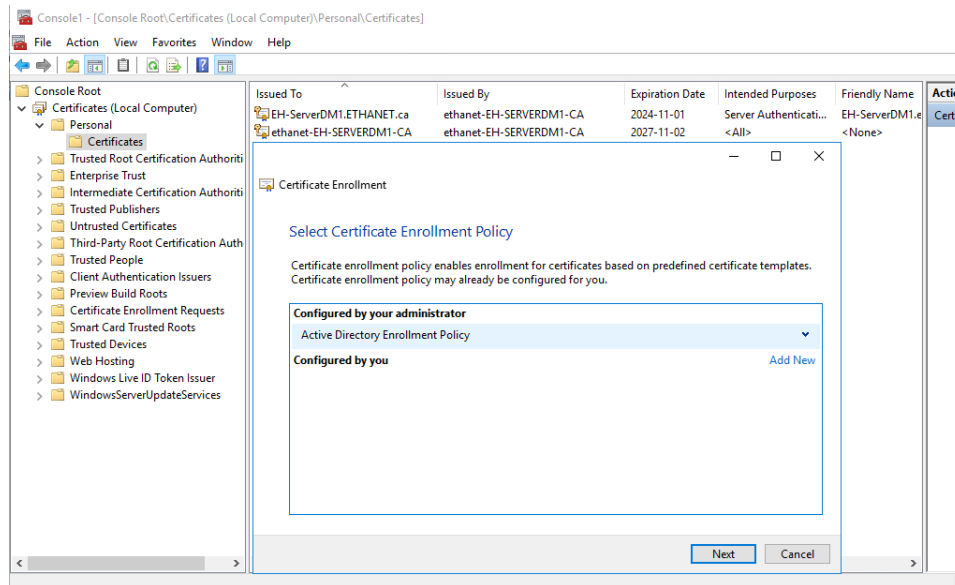


Figure 19: Creating certificate enrollments for OCSP

Click next, and on the Request page, request the OCSP-2016 certificate and enroll it

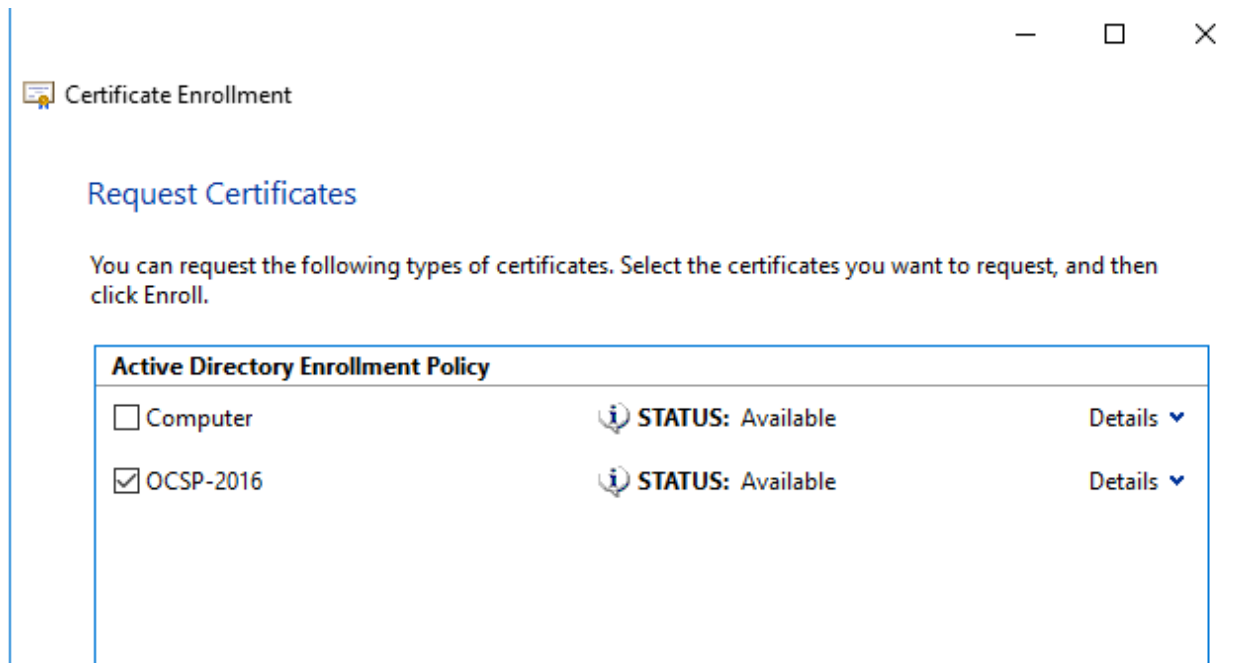


Figure 20: Adding OCSP to the enrollment

In the management console, find the key and right click it, click “Manage private keys” and add the NETWORK SERVICE user in Security

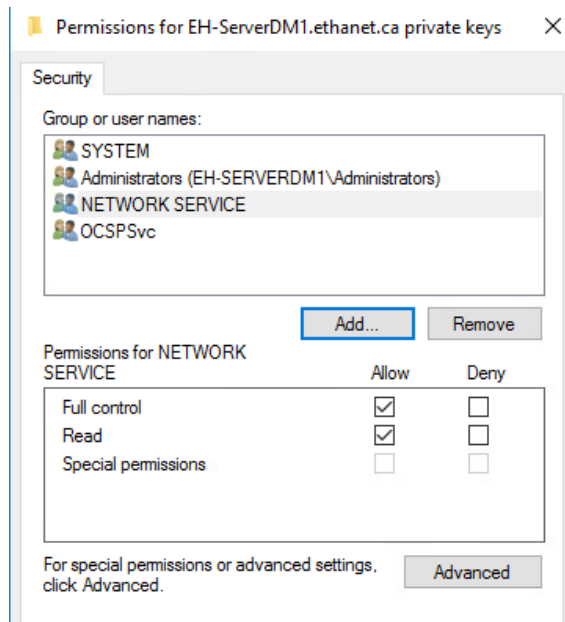


Figure 21: Network Services roll added to the Private Key

## Activity 8-9:

In this step, we will create the configuration for ocsf, we can right click Revocation Configuration, and click "Add Revocation Configuration", we can give a friendly name to the machine, and then select our CA of DM

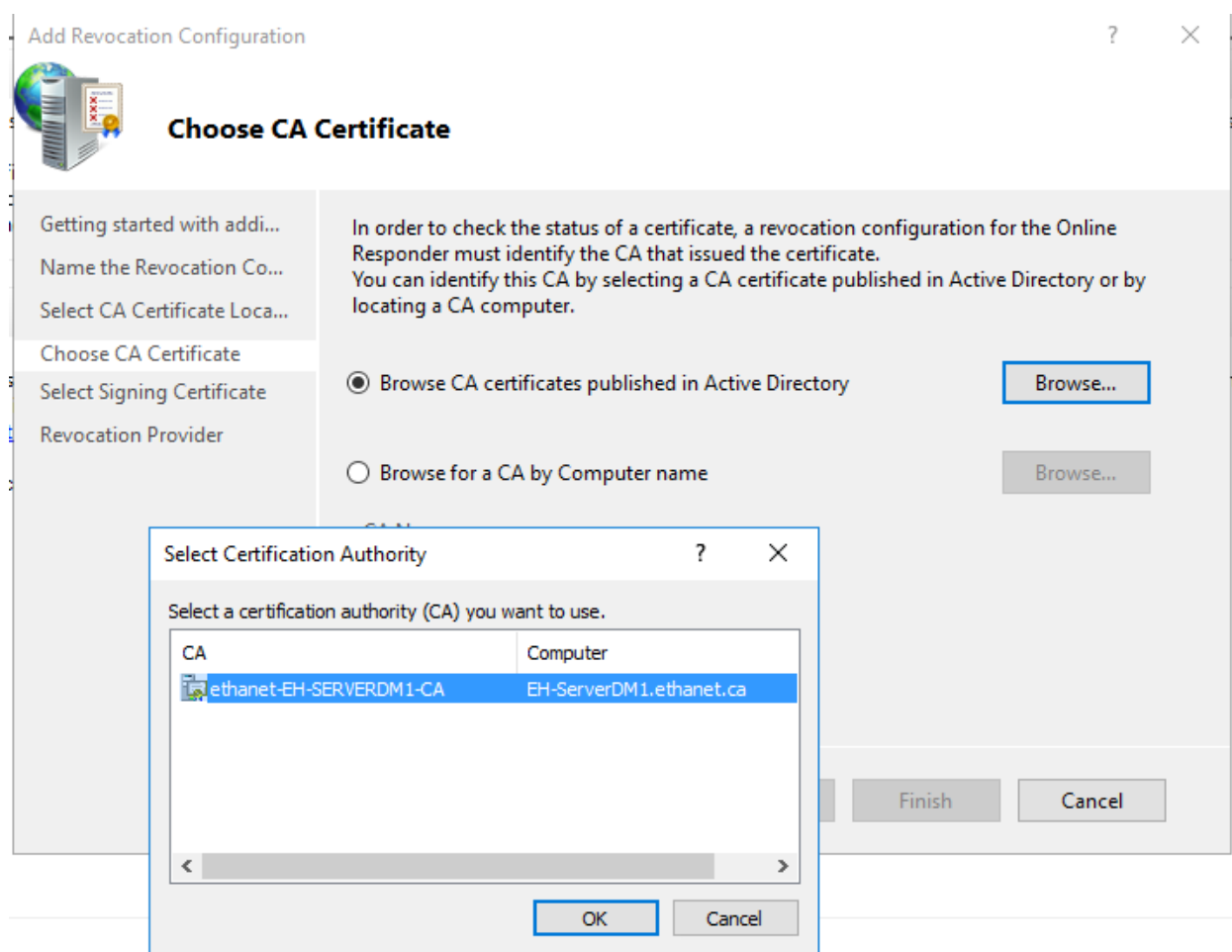



Figure 22: Using DM1 as our CA for Revocation



On the Select Signing Certificate page, we can leave the default options

Add Revocation Configuration ? X



### Select Signing Certificate

Getting started with addi...

Name the Revocation Co...

Select CA Certificate Loca...

Choose CA Certificate

Select Signing Certificate

Revocation Provider

Revocation information is signed before it is sent to a client. The Online Responder can select a signing certificate automatically, or you can manually select a signing certificate for each Online Responder.

☒ Automatically select a signing certificate

☒ Auto-Enroll for an OCSP signing certificate

Certification authority: EH-ServerDM1.ethanet.ca\ethanet-EH-SERVERDM1- Browse...

Certificate Template: OCSP-2016 ▼

☐ Manually select a signing certificate  
Note: You will need to specify a signing certificate for each member in the Online Responder Array.

☐ Use the CA certificate for the revocation configuration

< Previous Next > Finish Cancel

Figure 23: Creating the certificate auto signing

And on the Revocation Provider page, we can add the following url to both the base CRL and the Delta CRL

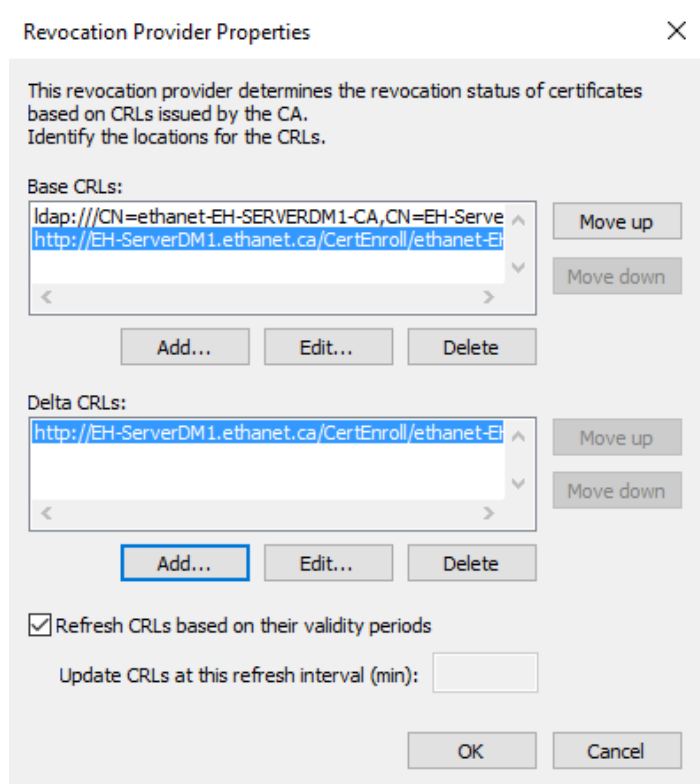


Figure 24: Adding the URL to Base and Delta CRL for the CA

#### Activity 8-10:

In this activity, we will be backing up our CA Server and archiving a key. We will start by creating a folder on our C: root called CABack. Then, in Certification Authority, we can right click our domain node and select "Backup CA" which gives us the "Certification Authority Backup Wizard"

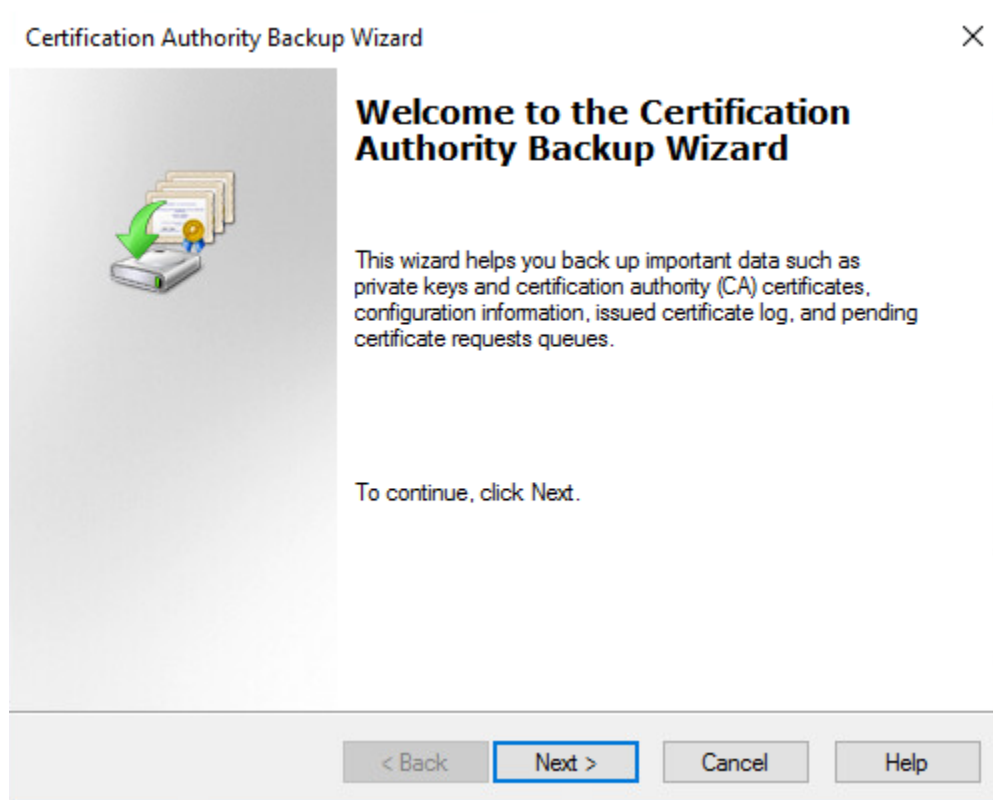


Figure 25: Backup wizard start

In the Items to Back Up window, Click both check boxes and then select the file path to the CABack folder

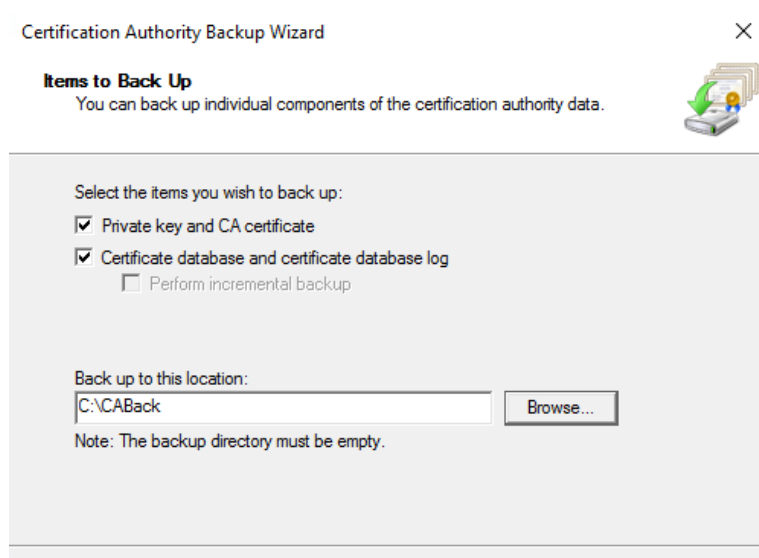


Figure 26: Telling what items to back up as well as where to back it up

Give the backup a password of your choice and finish the process. Next, we can once again add the Certificates snap-in in MMC, and right click the certificate of our choice, and export it

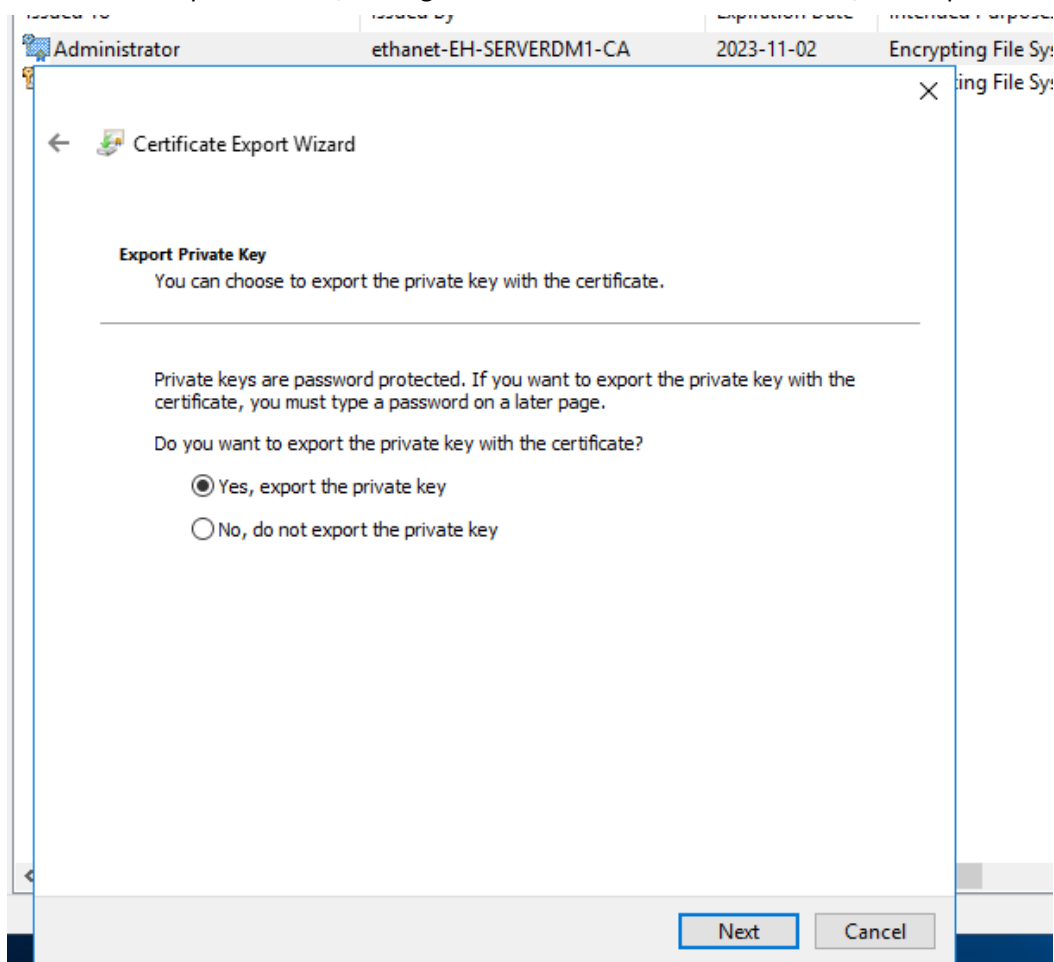


Figure 27: Exporting the private key

We can leave the defaults, except for the last step, we can give our Export a name and export it.

### Activity 8-11:

In this step, we will recover a lost key, first we will delete the keys that we have made earlier

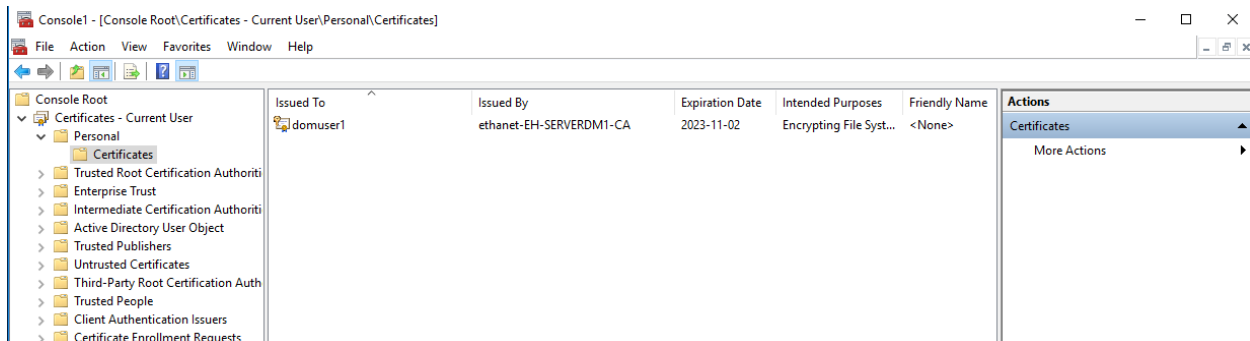


Figure 28: Deleting the Admin user

We can then right click the Certificates folder, and select import

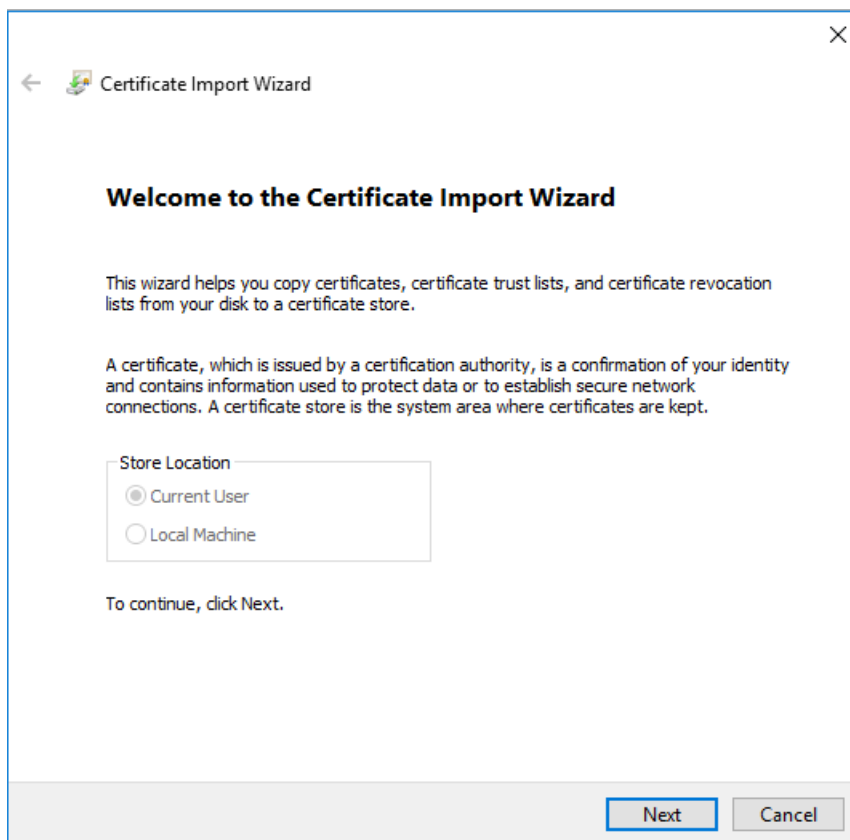


Figure 29: Location of the certificate you want to download

Select the location of the EFSCert that you saved

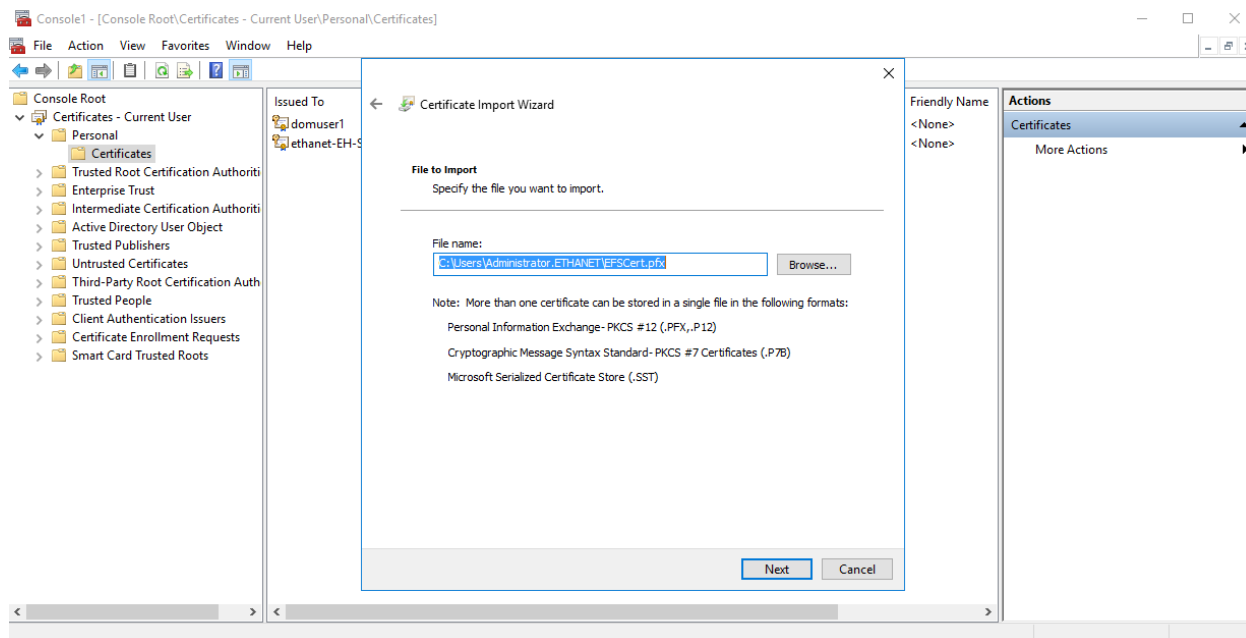


Figure 30: Importing the backup of the certificate

And on the following page, input the password and select the “Mark this key as exportable” box. Click next through the final boxes and you should see the deleted key reappear

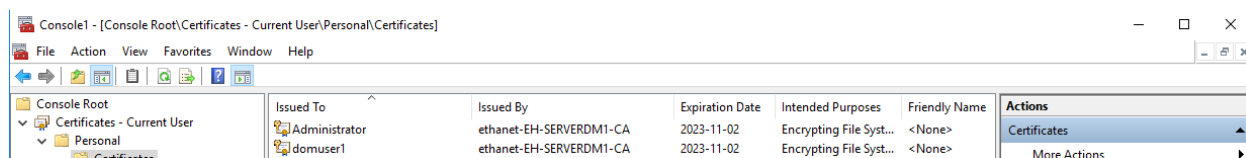


Figure 31: Certificate restored