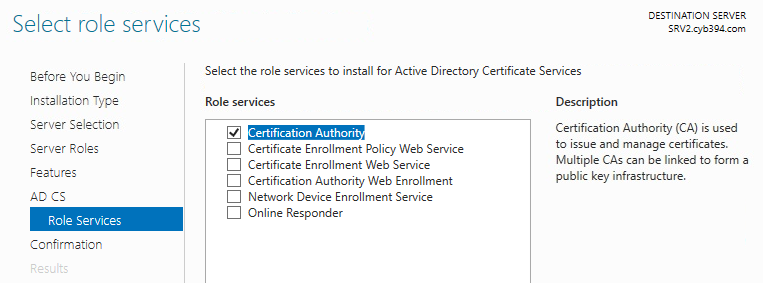
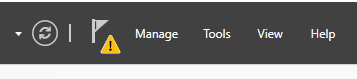
# **\*\*\*Attention – You MUST Perform Part 1 -> steps 1 – 21 EXACTLY CORRECT\*\*\***

# Part 1 Install Certificate Services

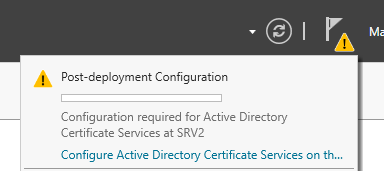
1. Power on SRV1 and SRV2
2. **Sign-In to SRV2** with your Personal Domain Admin Account (Password16)
3. From Server Manager -> Dashboard -> Add Roles and Features -> **Active Directory Certificate Services**
4. Select Add Features if prompted
5. Click Next
6. When you get to the **Role Services Page** and ensure **Certification Authority is checked.**



1. Complete the wizard to Install AD CS
2. Click Close when the installation is complete
3. In the **Server Manger Notifications Area click on the yellow triangle.**



1. Then Click on the **Configure Active Directory Certificate Services** Link



12. Specify Credentials Page click [Next]

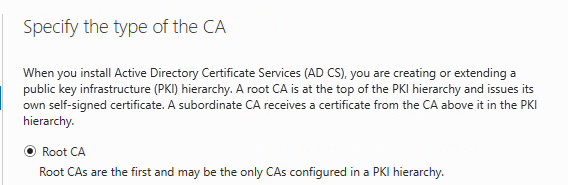
13. Check Mark **[X] Certification Authority**

14. Choose **(\*) Enterprise CA** -> [Next]

\*Note since we are in deploying to a small lab environment we can choose Enterprise CA then root. In larger and medium organizations, you will want to plan a PKI hierarchy. See

<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786436(v=ws.11)>

15. Select **(\*) Root CA** -> [Next]



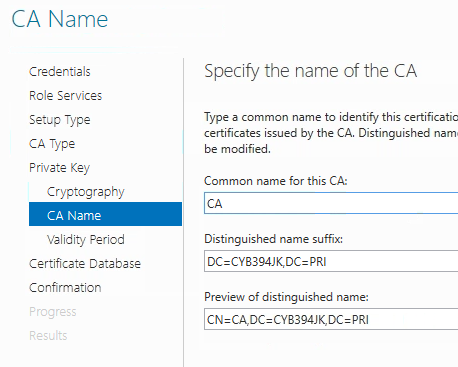
16. Select **(\*) Create a new private key** -> [Next]

17. Under Cryptography Select [**RSA#MSKey Storage Provider]\_[2048]; [SHA256]** and Check Mark the following:



[Next]

18. In CA name Change the common name to be simply **CA**



19. Review the options for the rest of the install but keep the defaults.

20. Click **[Configure]** on the Confirmation Page

|  |
| --- |
| Screenshot Configuration Success page: |

21. Click **[Close]** on the Configuration succeeded page

# Part 2 Examine the Certificate services console

1. From SRV2 Server Manager -> Tools -> Certification Authority
2. Right click Certification Authority (Local) -> Retarget CA

Here you should see that you can retarget the certification authority. This means that you can use this tool to manage other CA’s that you have access to. **[Finish]**

1. Right-Click -> CA -> Properties

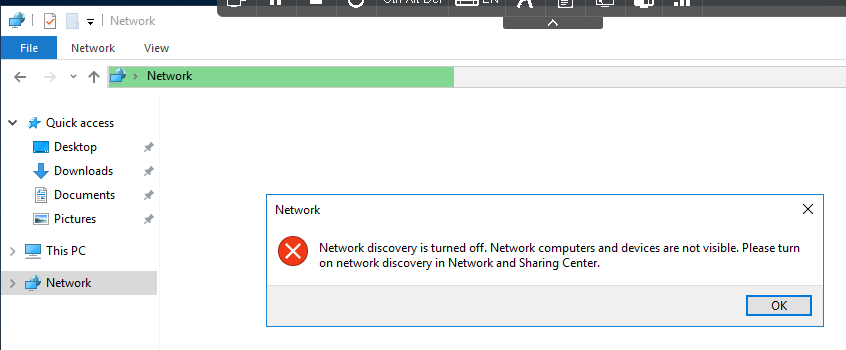
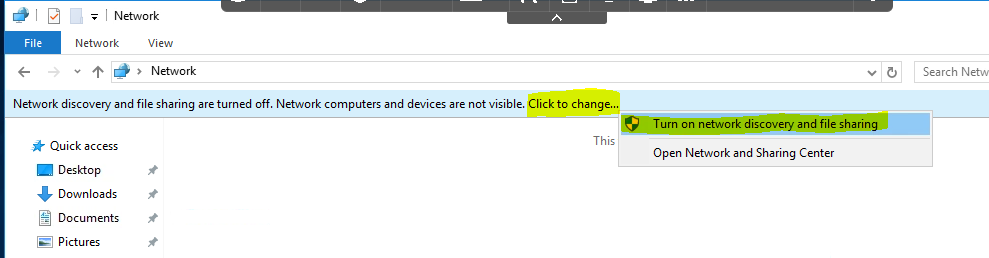
Here you will see the general properties of your CA. Click on the **[View Certificate].** Here you will see the CAs self-signed certificate and its validity period.

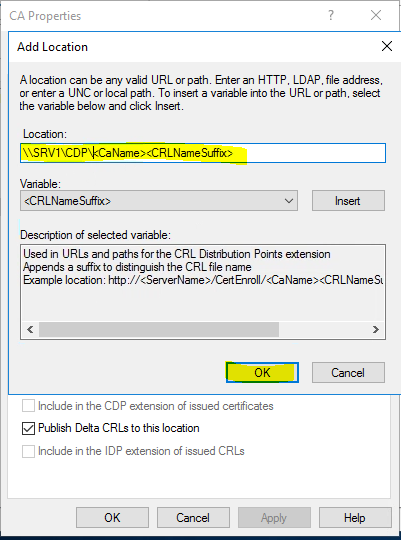
|  |
| --- |
| Screenshot of Certificate Validity property dates |

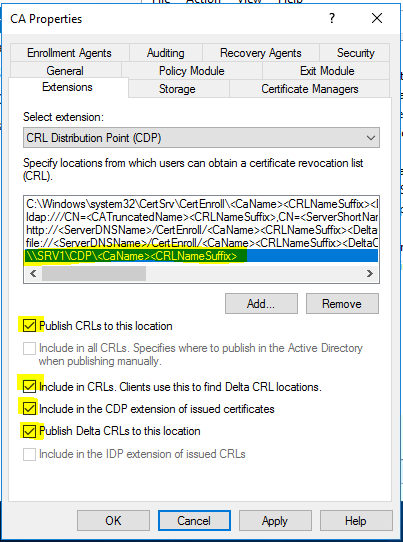
1. Explore the other tabs on your own then **close the properties dialog box.**
2. Explorer each one of the folders under the CA. Each folder is self-explanatory.
3. Click on **Certificate Templates** folder to see what templates are active by default. The Templates will show on the right-hand side.
4. To manage templates, you can right click on the Certificate Templates -> Manage. Do so now to view what is available then close the Certificate Templates Console.

# Part 3 CRL Distribution Points (CDPs)

1. Sign-In to SRV1 and create a folder on the C: drive called CDP (C:\CDP)
2. CDP <- Right-Click -> Properties -> Sharing use the **[Advanced Sharing]** tool to set the folder so Everyone has Full Control
3. **Sign-In to SRV2** with your PDA (Password16)
4. ~~Open File Explorer, browse the Network and turn ON Network discovery and file sharing.~~

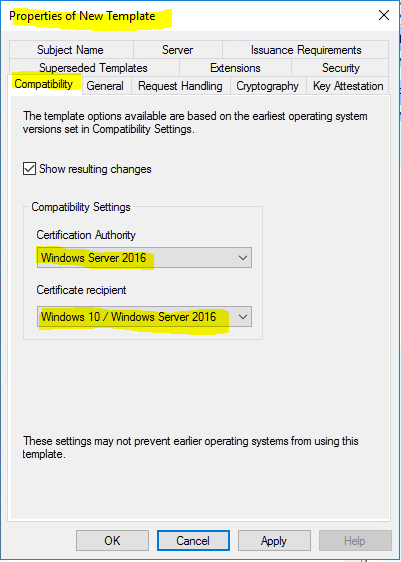
~~  
~~

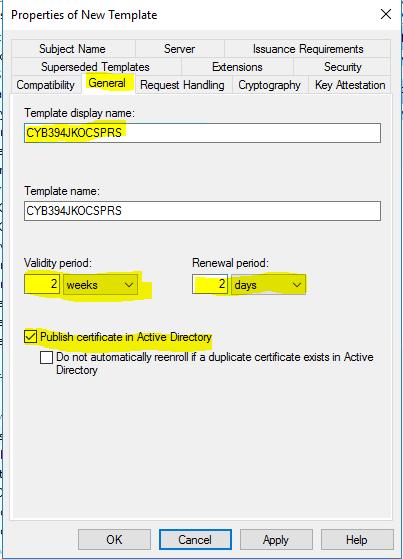
1. Server Manager -> Tools -> Certification Authority Tool
2. CA <- Right-Click -> Properties -> **[Extensions]**
3. Location: [ \\SRV1\CDP\]
4. Now, from the **Variable drop-down** select **<CaName>** and click **[Insert] and again,** from the **Variable drop-down** list, select **<CRLNameSuffix>** and click [Insert] to complete the following location.  
   
5. Click **[OK]**
6. With the new location highlighted;  
   [X] Publish CRLs to this location  
   [X] Include in CRLs. Clients use this to find Delta CRL locations  
   [X] Include in the CDP extension of issued certificates.  
   [X] Publish Delta CRLs to this location  
   (See Screenshot)

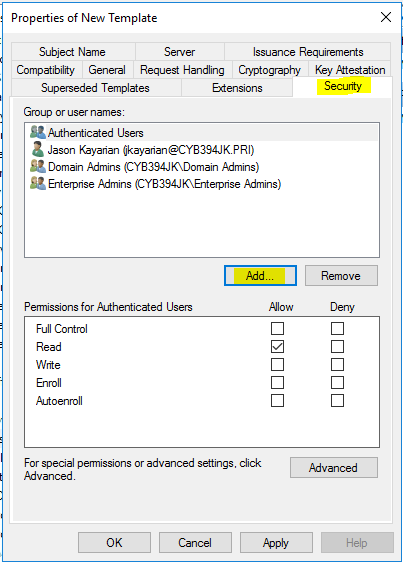
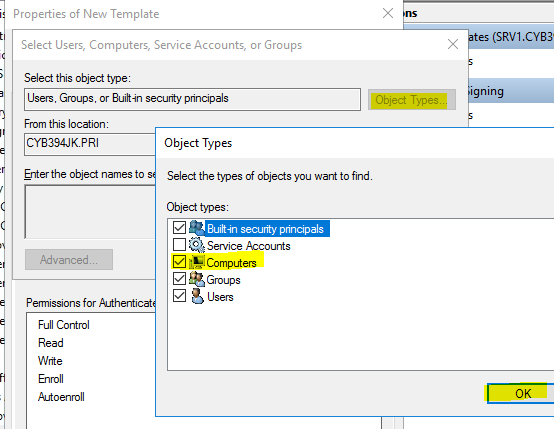


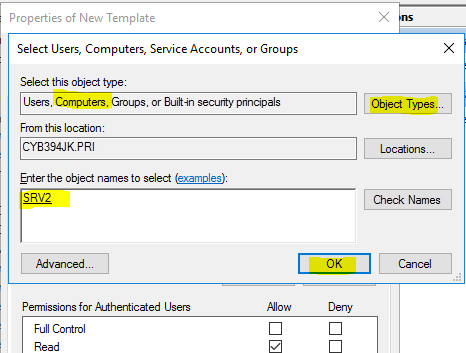
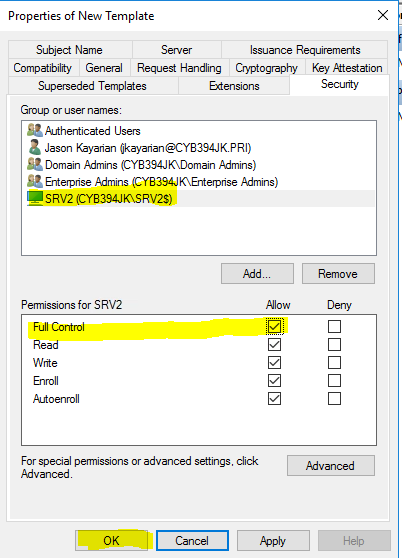
1. Click Apply then OK -> Restart AD Cert Services? [Yes]

# Part 4 Online Responder

1. Server Manager -> Tools -> Certification Authority
2. Right-Click on the Certificate Templates folder -> Manage
3. Locate OCSP Response Signing -> Right-click -> Duplicate Template and change the following compatibility settings.  
   ATTENTION: \*\***Make each tab changes BEFORE clicking Apply or OK.\*\***  
    **Do Not Click [Apply] or [OK]**
4. On the [General] tab name the template CYB394XXOCSPRS and make the following changes and [v] Publish cert in AD.

 Do Not click [Apply] or [OK]

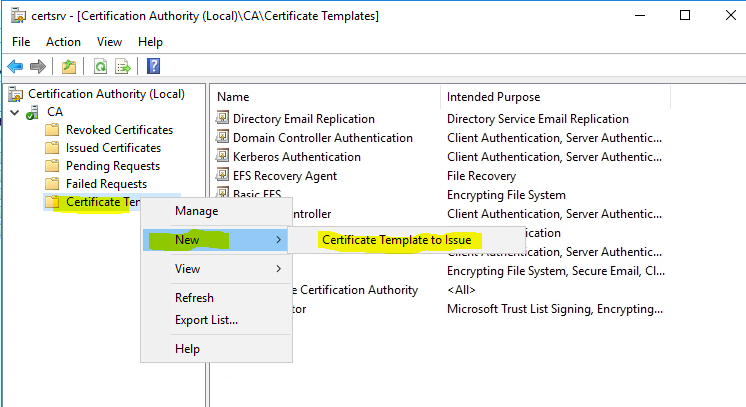
1. On the [Security] tab Add SRV2 server with Full Control  
    -> 

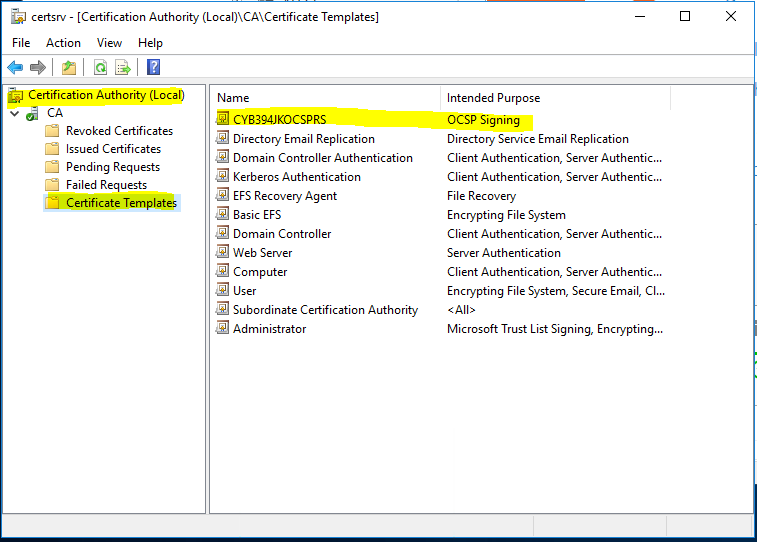
-> 

**Once All of these changes have been made click [Apply] then [OK]**

Now, Issue the new Certificate. This will make it available for access.

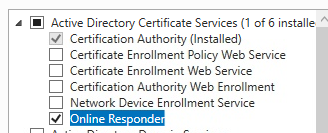
Right-click on Certificate Templates -> New -> Certificate Template to Issue





|  |
| --- |
| Screenshot of Certificate Templates -> CYB394XXOCSPRS cert listed |

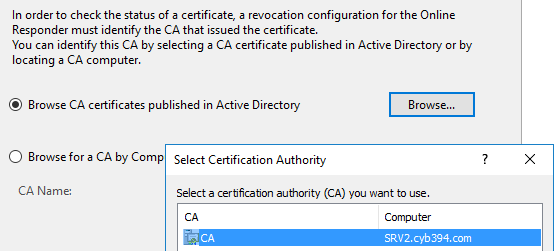
1. Server Manager -> Dashboard -> Add Roles and Features -> Role based or feature-based installation -> [Next] -> [Next]
2. Expand the AD CS node and select Online Responder -> [Next]

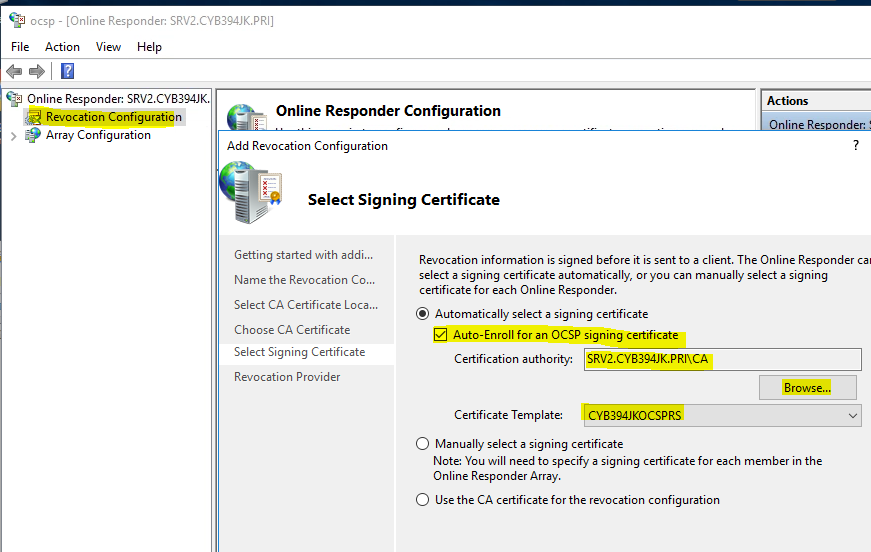


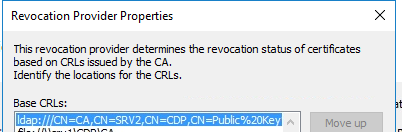
1. Click [Add Features].
2. Keep the defaults, clicking [Next] -> [Install]
3. Click **[Close]** once the install completes

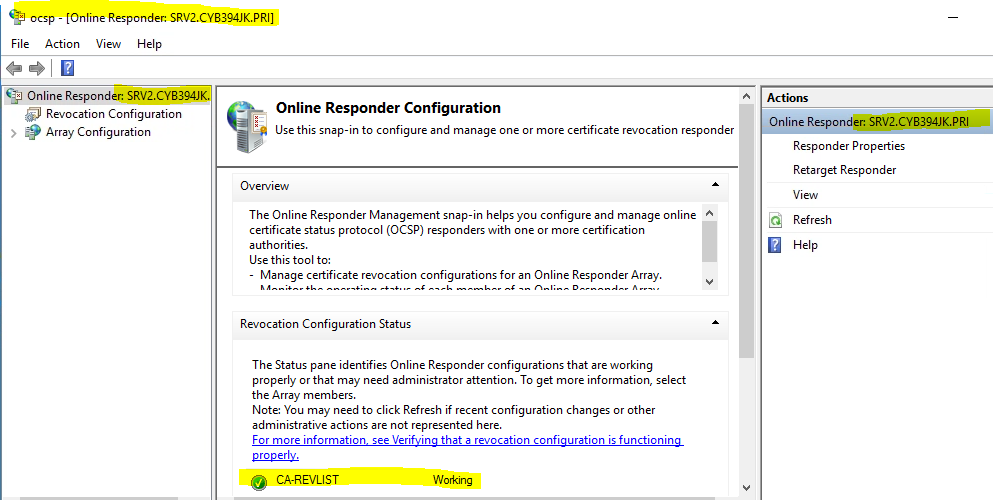
Once an Online Responder has been installed, you must **create a revocation configuration**. A new configuration must be created for each certificate being revoked.\*

1. From Server Manager -> Tools -> Online Responder Management
2. In the left-hand navigation pane, **right-click Revocation Configuration and select Add Revocation Configuration.**
3. The Add Revocation Configuration Wizard launches. Click Next.
4. Type a **CA-REVLIST** in the name for the configuration. It is recommended to include the name of the CA in the configuration name to help identify it. Click Next.
5. **(\*) Select a certificate for an Existing enterprise CA**: As the signing CA is an enterprise CA on the domain we choose this option to find the certificate from the CA.
6. Select **[Browse]** then choose your **CA SRV2.CYB394XX.PRI** [OK] (See Screenshot below)



1. Click [Next]
2. **(\*) Automatically select a signing certificate** -> [Next]  
   
3. Click **[Provider]**
4. Select the **ldap://CN=CA,CN=SRV2…** Provider then click [OK]



1. Then click [Finish]  
   

|  |
| --- |
| Screenshot: |

Continued on next page….

# Part 5 using CA for EFS and Prepare the Issuing CA for EFS

At this point in the exercise you have created a Root CA and a process of actually using your certificate systems requires several more steps. You will also create a Group Policy Object to set certificate policies. Finally, you will have an account obtain a certificate. To make things simpler we will use auto enrollment for our example.

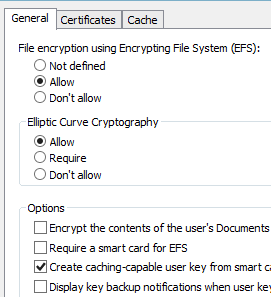
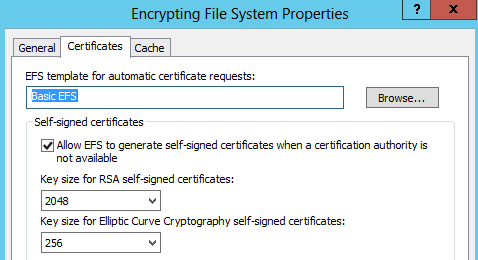
Now your CAs are set up. The next step is to create GPOs for an EFS policy.

First you will create a Computer policy.

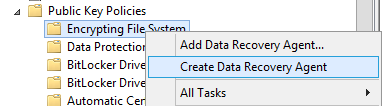
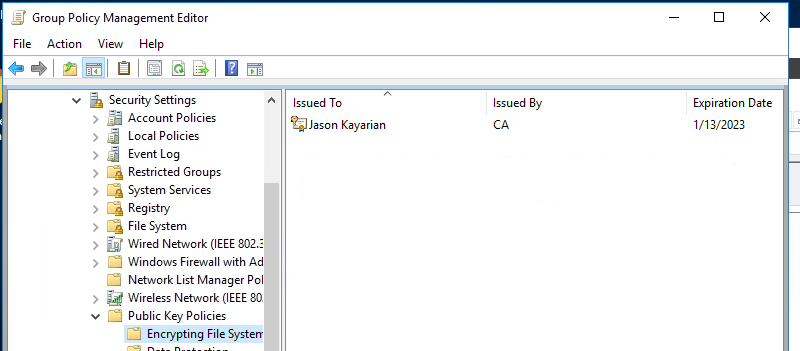
1. Sign-In to SRV1 with your PDA
2. Server Manager -> Tools -> Group Policy Management -> create a new GPO called EFS Certificate Policy and link it to (create it under) the **CYB394XX.PRI** Domain container.
3. Edit the new policy and navigate to the Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Public Key Policies -> Encrypting File System. You will note that this section is empty since this is a new blank GPO.



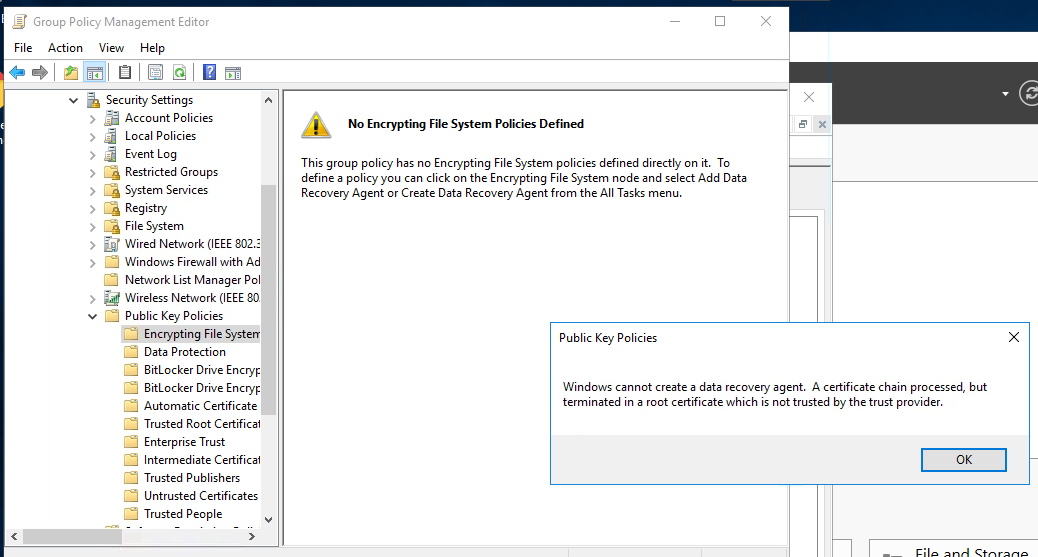
1. Right click on Encrypting File System folder and select Properties.
2. From the [General] tab, select  
   (\*) Allow radio button
3. Then use the [Certificates] tab (Browse… button if necessary) to select the Basic EFS template, then click OK



1. Right click on Encrypting File System and select Create Data Recovery Agent. After a few seconds you should see a certificate for your account in the right hand pane.

 ->

If you receive the error below, simply wait a few minutes and try again.

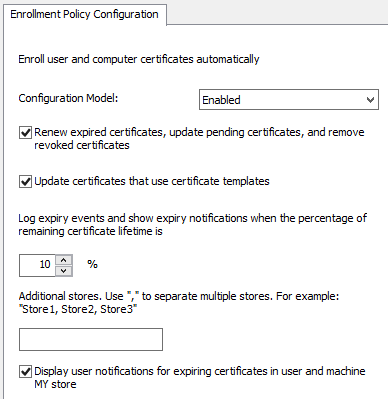


1. Close the Group Policy Management Editor window
2. Now create another new GPO linked to CYB394XX.PRI and name it EFS User Policy
3. Edit the policy and drill down in the **User Configuration** -> Policies -> Windows Settings -> Security Settings -> Public Key Policies
4. Highlight Public Key Policies (left pane) then right-click on Certificate Services Client – Auto-Enrollment (right pane) and select Properties



1. Click on the drop down menu for Configuration Model -> Enabled. Then check all three check boxes, then click [OK].

This EFS policy is enabled so an administrator doesn’t have to manually approve every EFS certificate: the CA will issue it directly to the user.



1. Switch to SRV2 -> Elevated CMD prompt -> GPUPDATE /force
2. Run **gpresult /r** on SRV2 to verify the policies have applied there as well.

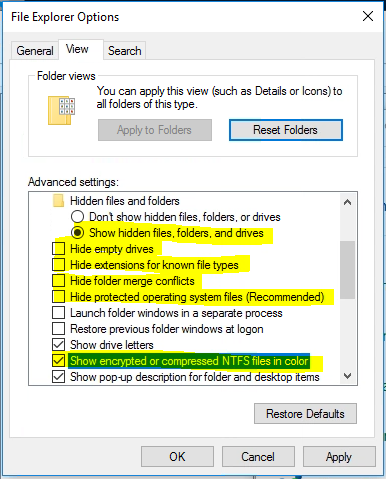
|  |
| --- |
| Screenshot of gpresult /r showing EFS User Policy. |

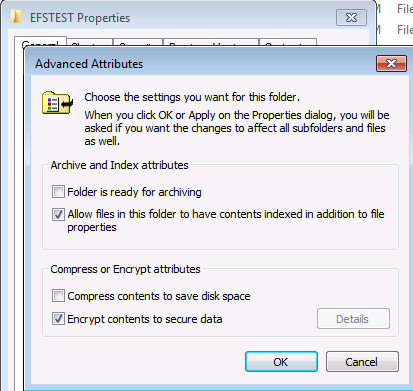
1. SRV2 -> Tools -> Certification Authority and left click on Issued Certificates.

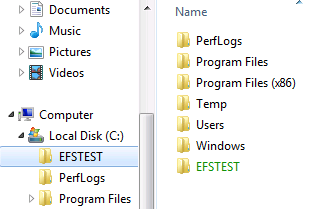
|  |
| --- |
| Screenshot of Issued Certificates |

# Part 6: Test your policies and templates.

In this section you will see what happens when a user uses EFS to encrypt something.

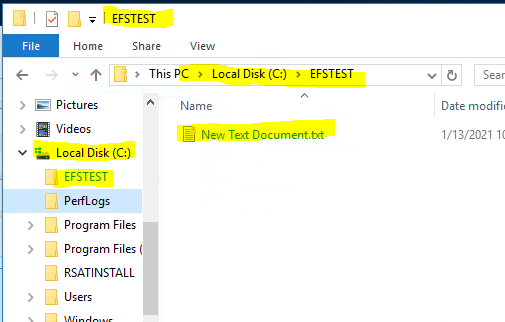
* SRV1 -> Server Manager -> Tools -> ADUC
* Create a new domain user account ~~that is only in the Domain Users security group~~. Use the following:
  + **First Name:** Cert **Last Name:** User
  + Logon Name:  **CertUser**
  + Password: **Password16**
  + Password Never Expires
* Start CLIENT1 and logon as CertUser.
* Control Panel -> File Explorer Options -> [View] tab:  
  
* As CertUser, create a folder on the C: drive of CLIENT1 called EFSTEST (C:\EFSTEST)
* Right click the EFSTEST folder -> Properties -> [General] tab -> [Advanced] button and then click the check box to [X] Encrypt contents to secure data. Then click OK twice.

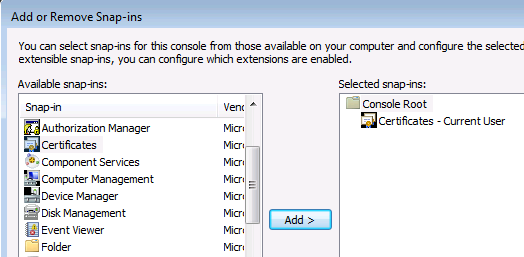


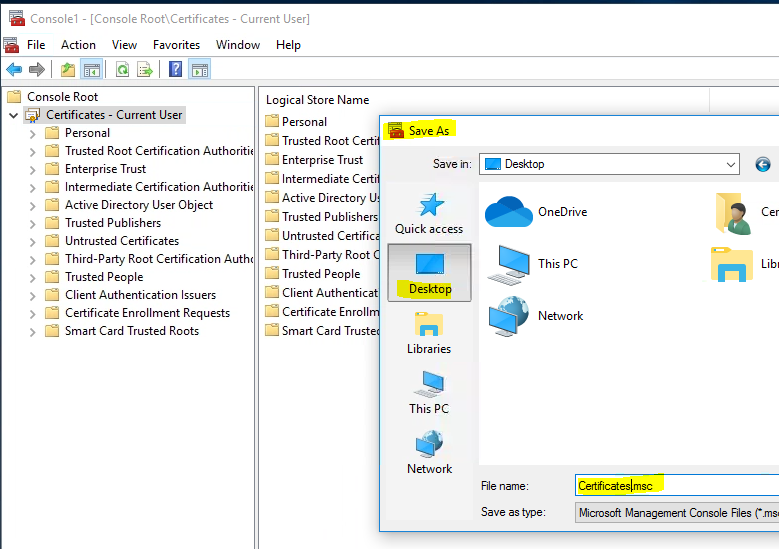
1. You should see that the folder name in the list has changed from black to green indicating that anything put into this folder will be encrypted.

The font color should be green.

1. Create a document within the EFSTEST folder



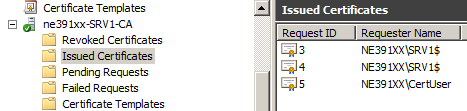
1. Still on Win10 (still logged on as CertUser) -> Search MMC and create a console -> File -> Add or Remove Snap-ins -> Certificates (Current User) snap-in.  
   Click [OK]
2. File -> Save and save the console to the desktop; name it Certificates.msc



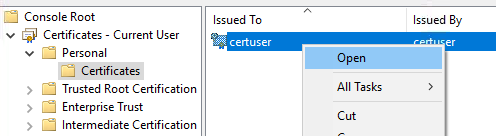
1. Once the MMC Console1 has been created click the Certificates – Current User and Examine the Personal -> Certificates. **There will be one certificate generated from the EFSTEST encryption option enable.** (It may take a couple minutes to appear - click the Refresh button)

|  |
| --- |
| Screenshot of Certificates -> Personal -> Certificates |

1. Leave the MMC running on CLIENT1
2. Switch back to SRV2.
3. Server Manager -> Tools -> Certification Authority
4. Highlight the Issued Certificates folder and click the Refresh button. You should now see the new certificate.



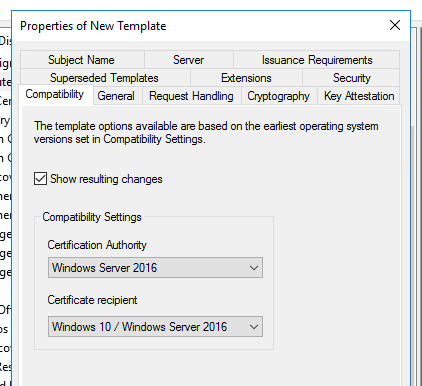
Switch back to CLIENT1, right click on the CertUser certificate and select **Open** as shown below (or double click on it)



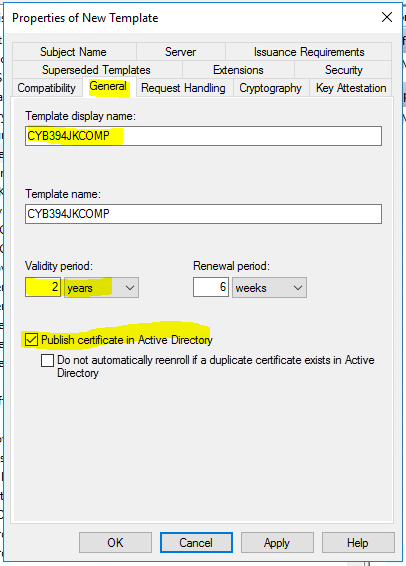
1. Click on the Certification Path tab. You should see a hierarchy since this certificate was issued by a subordinate CA, you need to be able to track the trust relationship back to the Root CA.
2. On CLIENT1 remove the check box for encryption on the C:\EFSTEST folder.

# Part 7 Deploying Client Computer Certificates

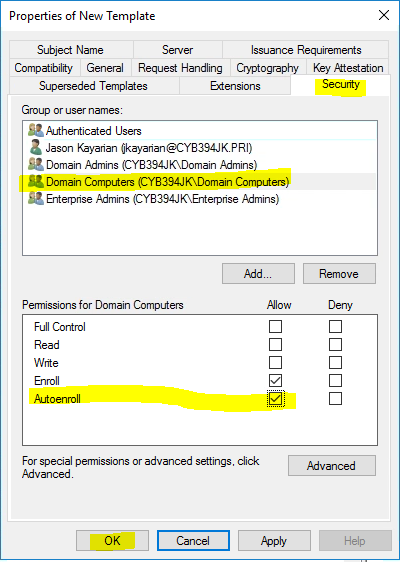
1. **SRV2** -> Server Manager -> Tools -> Certification Authority
2. Click on the Certificate Templates folder
3. Right Click on the Certificate Templates Folder -> Manage.
4. Locate the **Computer** template and Right- Click -> **Duplicate Template**
5. Choose the following options under [Compatibility] tab and **DO NOT click [Apply] or [OK] until all changes are made on each tab.**



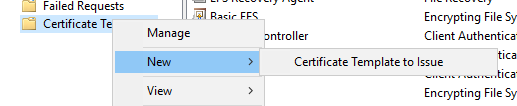
1. Click on the [General] tab and name the template CYB394XXCOMP
2. Change the validity period to **two years**
3. Check mark the [X ]Publish certificate in Active Directory

 DO NOT click [Apply] or [OK]

1. Navigate to the [Security] tab and view the permissions for Domain Computers. Check **Auto Enroll** allow.

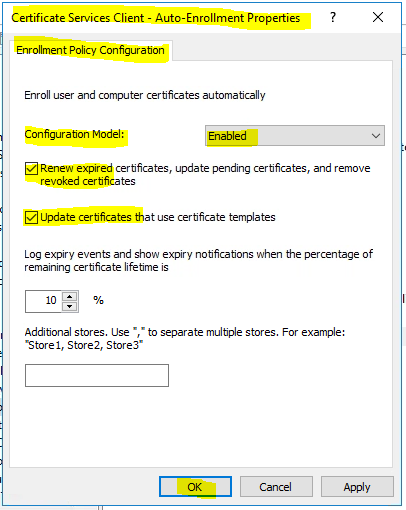


1. Click Apply Then Ok
2. Close this certificate template console
3. Right click on the Certificate Templates and choose

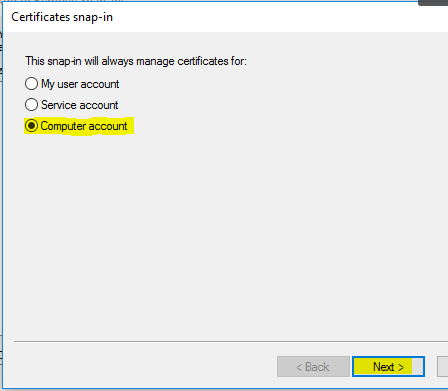


1. Choose CYB394XXCOMP then click Ok
2. Verify that the template is showing in the right pane

|  |
| --- |
| Screenshot of the Certificate Template showing CYB394XXCOMP |

1. Sign In to **SRV1** -> Server Manager -> Tools -> Group Policy Management
2. Create a new group policy linked to the CYB394XX.PRI domain container; name the policy **Computer Auto Enroll**
3. Edit the policy and navigate to Computer Configuration, Policies -> Windows Settings -> Security Settings -> Public Key Policies.
4. Right Click on **Certificate Services Client – Auto Enrollment** and choose properties
5. Configuration Model: Enabled
6. Select  
   [X] Renew expired certificates, update pending certificates, and remove revoked certificates check box  
   [X] Update Certificates that use Certificate templates check box
7. Click [OK]  
   
8. Restart CLIENT1 if it is already powered on. Power it on if it is powered off.
9. Sign-In to CLIENT1 with your PDA (Password16)
10. Open Eleveated Command Prompt -> **gpupdate /force**
11. **Gpresult /r** and verify **Computer Auto-Enroll Policy** is applied.

|  |
| --- |
| Screenshot of gpresult /r showing Computer Auto Enroll policy applied |

1. Right click on the start menu and select run (or use the Search tool)
2. Type in mmc
3. In MMC go to File Add/remove Snap-in…
4. Double click on certificates
5. Then choose **Computer account**
6. Click [Next] -> Local Computer is default -> [Finish] -> [OK]
7. Select Certificates (Local Computer) then ok
8. Drill into Certificates (Local Computer) -> Personal -> Certificates and verify that you have a certificate issued

