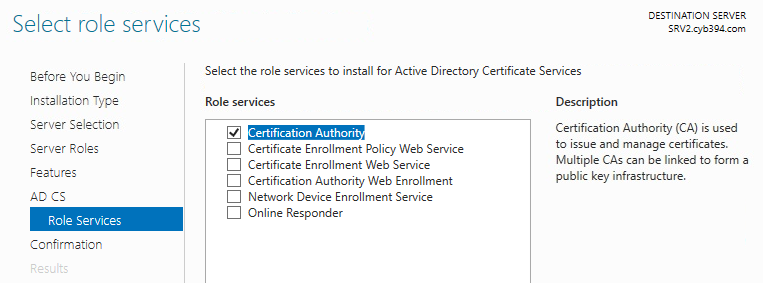
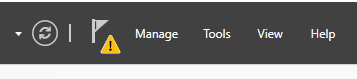
# Part 1 Install Certificate Services

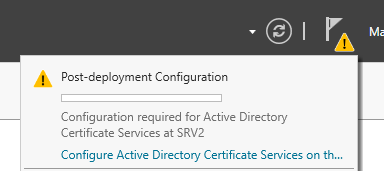
1. Power on SRV1 and SRV2
2. Log on to SRV2 with your personal Domain Admin Account
3. From Server Manager go to Manage and Add Roles and Features
4. On the Server Roles Page Select Active Directory Certificate Services
5. Select Add Features if prompted
6. Click Next
7. When you get to the Role Services Page make sure Certification Authority is checked.



1. Complete the wizard to Install AD CS
2. Click Close one 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. Click Next on the Specify Credentials Page

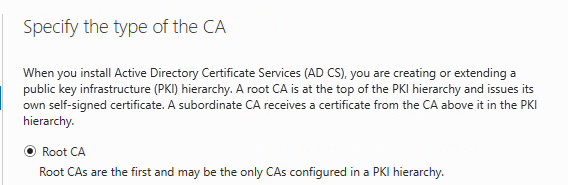
13. Check Mark Certification Authority

14. Choose Enterprise CA\*

\*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

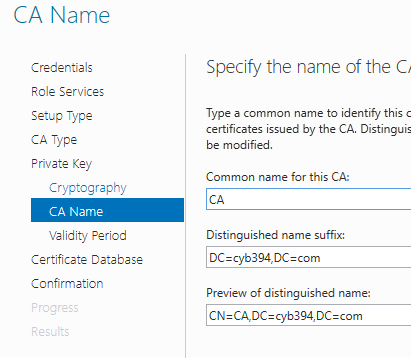


16. Select create a new private key

17. Under Cryptography Select SHA256 and Check Mark the following.



18. In CA name update the common name to be CA



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

20. Click Configure on the Confirmation Page

21. Click Close on the Configuration succeeded page

# Part 2 Examine the Certificate services console

1. From SRV2 Server Manager go to Tools the Certification Authority
2. Right click on Certification Authority (Local)

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.

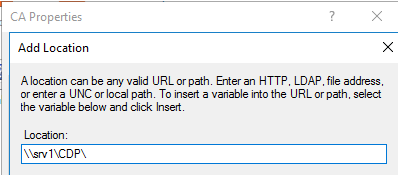
1. Click on CA and then right click and select properties

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.

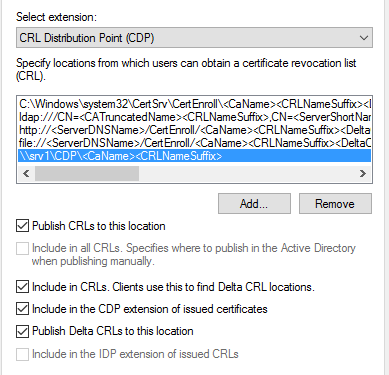
1. Explore the other tabs on your own then close the properties dialog box.
2. Explorer each one of the folders under the CA. Each folder is self-explanatory.
3. Click on Certificate templates to see what templates are active by default. The Templates will show on the right hand side.
4. To manage templates,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

# Part 3 CRL Distribution Points (CDPs)

1. Create a folder called CDP on SRV1 C:
2. Share the folder so everyone has full control
3. Start Server Manager from either the Start Menu or the Taskbar on SRV2
4. Open the Certification Authority Tool
5. Right Click on the CA and select properties
6. Go to the extensions tab
7. Click Add then input the following in the location



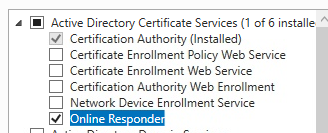
1. From the Variable drop-down list, select <CaName> and click Insert.
2. From the Variable drop-down list, select <CRLNameSuffix> and click Insert.
3. Click OK
4. With the new location highlighted, check the boxes labeled Publish CRLs to this location, Publish Delta CRLs to this location, Include in CRLs. Clients use this to find Delta CRL locations, and include in the CDP extension of issued certificates. (See Screenshot)



1. Click Apply then OK.

# Part 4 Online Responder

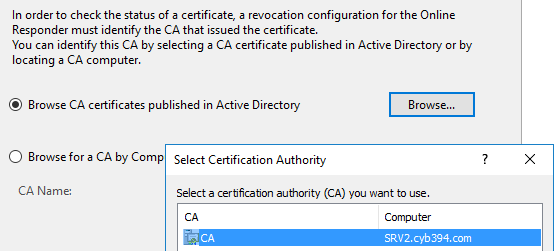
1. On SRV2 Start Server Manager from either the Start Menu or the Taskbar
2. Click Manage > Add Roles and Features
3. Select Role-based or feature-based installation and click Next.
4. Click Next again
5. Expand the AD CS node and select Online Responder; then click Next.



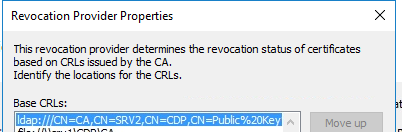
1. If Prompted Click add features.
2. Keep the defaults then click next to install
3. Click Close once the install completes

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 click Tools, then 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 CAREVLIST 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: If the signing CA is an enterprise CA on the domain, choose this option to find the certificate from the CA.
6. Select Browse then choose your CA (See Screenshot)



1. Click Next to choose automatically select a signing certificate.
2. Click Provider.
3. Select a valid CRL from the list provided. The provider uses this CRL to determine the status of the certificate.
4. Select the following provider then click OK.



1. Then click finish.

Continued on next page….

# Part 5 using CA for EFS 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.

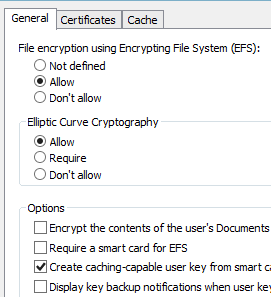
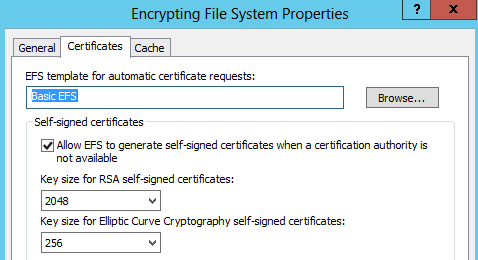
Now your CAs are set up. The next step is to create GPOs for an EFS policy.

First you will create a Computer policy.

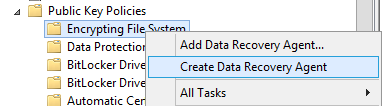
1. On SRV1 create a new GPO called EFS Certificate Policy and link it to the Domain container.
2. Edit the new policy and navigate to the Computer Configuration / Policies / Windows Settings / Security Settings / Public Key Policies / Encrypting File System. You will note that this section is empty since this is a new blank GPO.



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



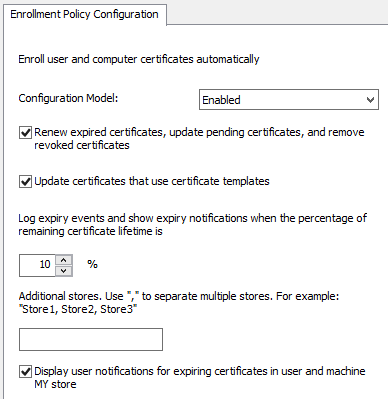
1. Right click on Encrypting File System and select Create Data Recovery Agent. After a few seconds you should see a certificate for your account in the right hand pane.



1. Close the GPEDIT window
2. Now create another new GPO. Call this one EFS User Policy and also link it to the Domain container.
3. Edit the policy and drill down in the **User Configuration** node through 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 Method Enable the policy. Then check all three check boxes, then click OK. This is done so an administrator doesn’t have to manually approve every EFS certificate: the CA will issue it directly to the user.

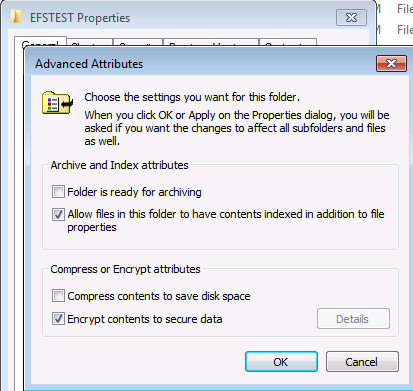


1. Run GPUPDATE on SRV2
2. Run gpresult on SRV2 to verify the policies have applied there as well.
3. Return to Certification Authority snap-in on SRV2 and left click on Issued Certificates.
4. Record any certificates you see. You should see at least one certificate. (If you don't see any issued certificates after clicking the Refresh button, restart SRV1).

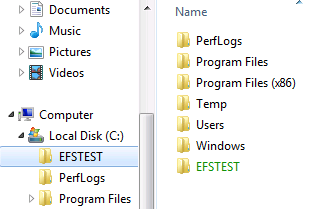
# Part 6: Test your policies and templates.

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

* On SRV1 create a new domain user account that is only in the Domain Users security group. Use the following:
  + Logon Name: CertUser
  + Password: Password1
  + Uncheck the box so that the user doesn’t have to change the password at next logon.
* Start WIN10 and logon as CertUser.
* As CertUser, create a folder on the C: drive of WIN10 called EFSTEST.
* Right click on the folder, select Properties, click on the Advanced button and then click the check box to encrypt the folder and contents. Then click OK twice.

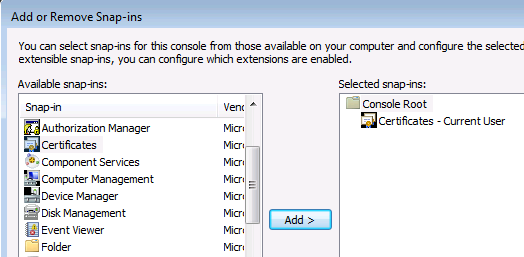


1. You should see that the folder name in the list has changed from black to green indicating that anything put into this folder will be encrypted.



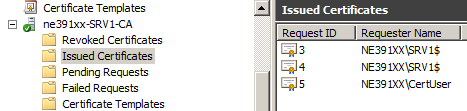
The font color should be green.

1. Still on Win10 (still logged on as CertUser) create a MMC and add the Certificates snap-in. When you click the Add> button select My user account.

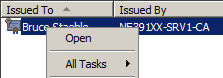


1. Examine the Personal folder. There should be one certificate in it. (It may take a couple minutes to appear - click the Refresh button)

Leave the MMC running on WIN10 and switch back to SRV2. Highlight the Issued Certificates folder and click the Refresh button. You should now see the new certificate.



Switch back to WIN10, right click on the certificate and select **Open** as shown below (or double click on it)

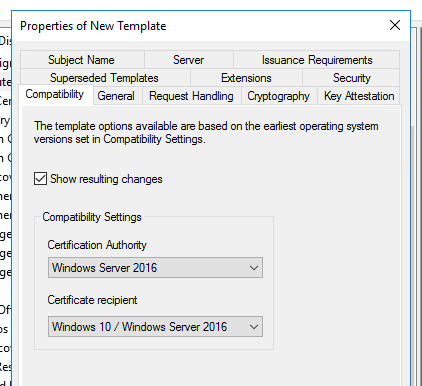


1. Click on the Certification Path tab. You should see a hierarchy since this certificate was issued by a subordinate CA, you need to be able to track the trust relationship back to the Root CA.
2. On WIN10, remove the check box for encryption on your folder.

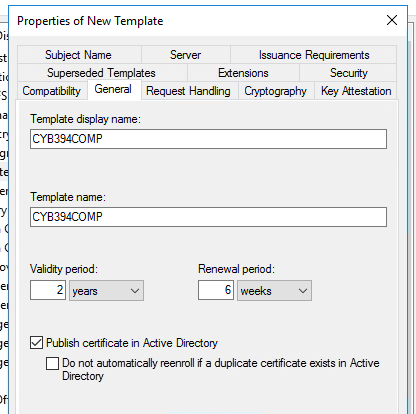
*(If you don’t have a certificate, encrypt a folder and put a file in it to force a certificate to be created.)*

# Part 7 Deploying Client Computer Certificates

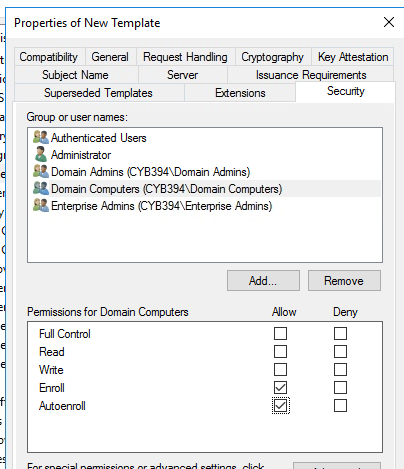
1. From Server Manager launch the Certification Authority tool
2. Click on the Certificate templates folder
3. Right Click on the Certificate Templates Folder and choose manage.
4. Locate the Computer Certificate Template and Click on it
5. Right click on the template and choose duplicate
6. Choose the following options under compatibility settings



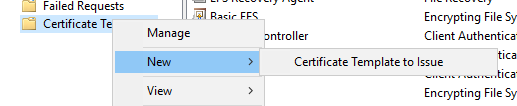
1. Click on the General tab and name the template CYB394COMP
2. Change the validity period to two years
3. Check mark the Publish certificate in Active Directory



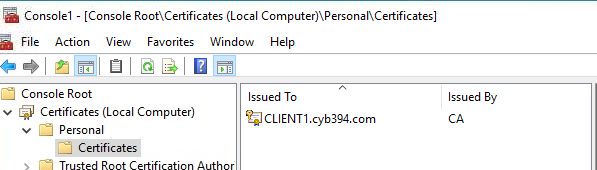
1. Navigate to the Security Tab and view the permissions for domain computers. Check auto enroll allow.



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



1. Choose CYB394COMP then click Ok
2. Verify that the template is showing in the right pane
3. Log on to SRV1 and launch the Group Policy Management tool
4. Create a new group policy linked to the domain container
5. Name the policy Computer Auto Enroll
6. Edit the policy and navigate to Computer Configuration, Policies, then Windows Settings, then Security Settings, and then Public Key Policies.
7. Select then right Click on Certificate Services Client – Auto Enrollment and choose properties
8. Next to the configuration model choose enabled
9. Select Renew expired certificates, update pending certificates, and remove revoked certificates check box
10. Select update Certificates that use Certificate templates check box
11. Reboot client 1 if it is already powered on. Power it on if it is powered off.
12. Logon with your personal administrator account
13. Right click on the start menu and select run
14. Type in mmc
15. In MMC go to File Add/remove Snap-in…
16. Double click on certificates
17. Then choose computer account
18. Click Finish Twice
19. Select Certificates (Local Computer) then ok
20. Drill into the following are and verify that you have a certificate issued

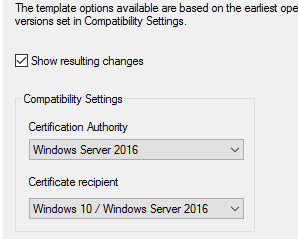


# Part 8 deploying a User Certificate (on your own)

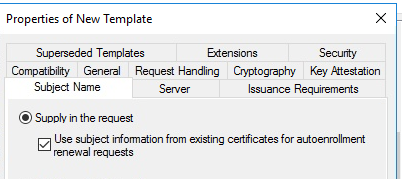
1. Use a similar procedure to auto enroll user certificates
2. Show the mmc console with the Current User Certificate Snap in and an issued certificate to your professor.

# Part 9 IIS and SSL

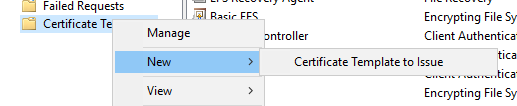
1. Power on SRV3 and install the Web Server IIS role
2. While the role is installing open the certification authority tool on SRV2
3. Right Click on Certificate Templates and Select manage
4. Locate the Web Server Template, right click and select duplicate template
5. Update the compatibility settings to the following



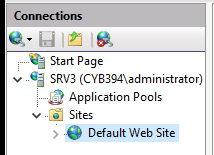
1. In the general tab name, the template Web Server SAN
2. Under Subject Name make sure the following is selected.



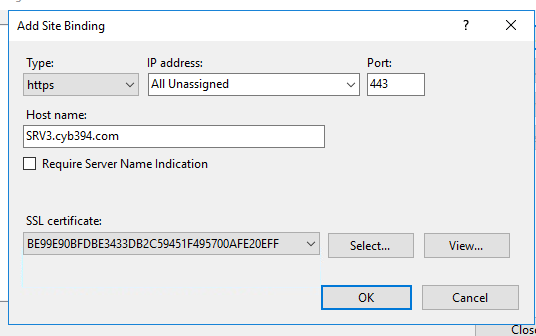
1. Click apply then ok. Then close the certificate template config tool
2. Right click on the Certificate Templates and choose



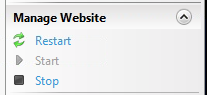
1. Choose Web Server SAN click OK
2. On SRV3 go to Tools and Launch IIS Manager
3. Navigate the left pane and choose default web site



1. On the right-hand side pane choose bindings then click Add
2. Select type https and give the host name srv3.cyb394.com
3. In the SSL drop down choose the default certificate and select OK



1. Restart IIS under Manage Website



1. Modify the default HTML page to say *your name* and I’m super secure
2. Browse to the website using <https://srv3.cyb394.com>

