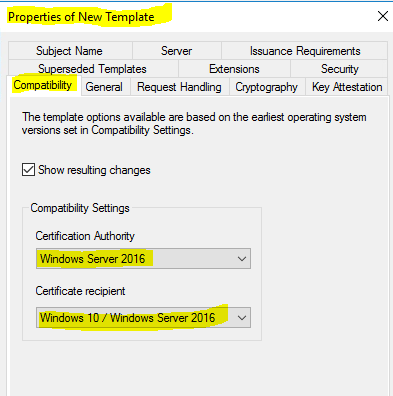
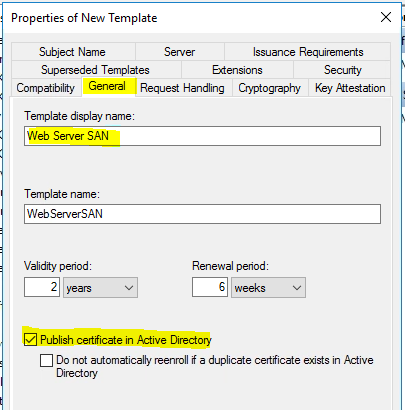
Lab 3 – Certificates & IIS

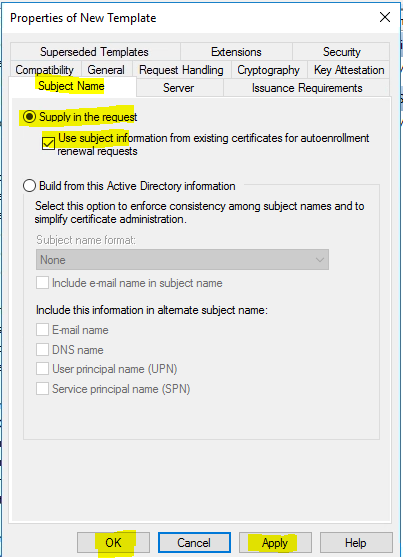
Make sure SRV1, SRV2, SRV3, and CLIENT1 are on

# Part 1 - IIS and SSL

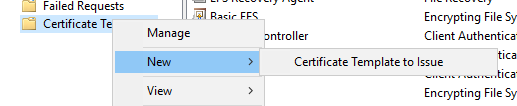
1. Sign-In to **SRV3** with your PDA (Password16)
2. Server Manager -> Dashboard -> Add Roles & Features -> install the **Web Server IIS** role with all defaults.
3. While this role is installing, **Sign-In to SRV2** -> Server manager -> Tools -> Certification Authority
4. Right Click on Certificate Templates and Select manage
5. Locate the **Web Server Template**, right click and select **duplicate template**
6. Update the [Compatibility] tab to the following

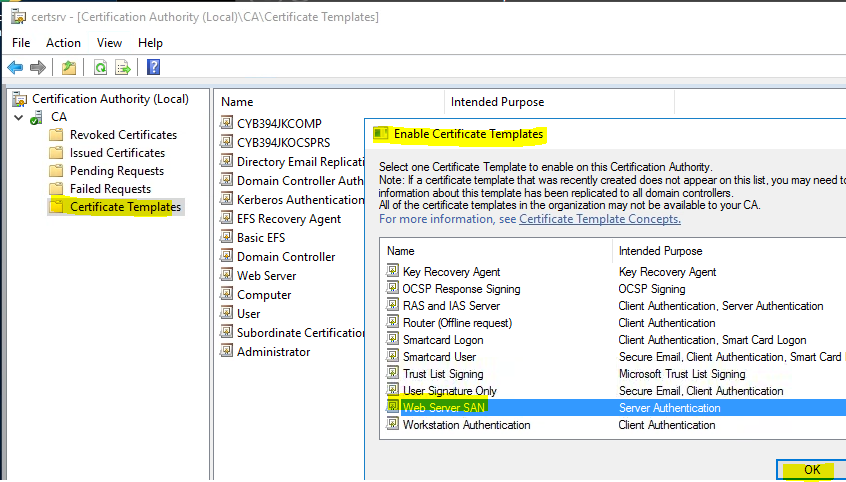
 **DO NOT click [Apply] or [OK]**

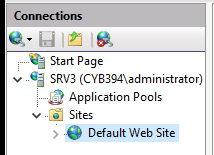
1. In the [General] tab name, the template **Web Server SAN  
   \*Ensure [V] Publish certificate in Active Directory is ON\*\*** **DO NOT click [Apply] or [OK]**
2. Under [**Subject** *Alternate* **Name**] make sure the following is selected.

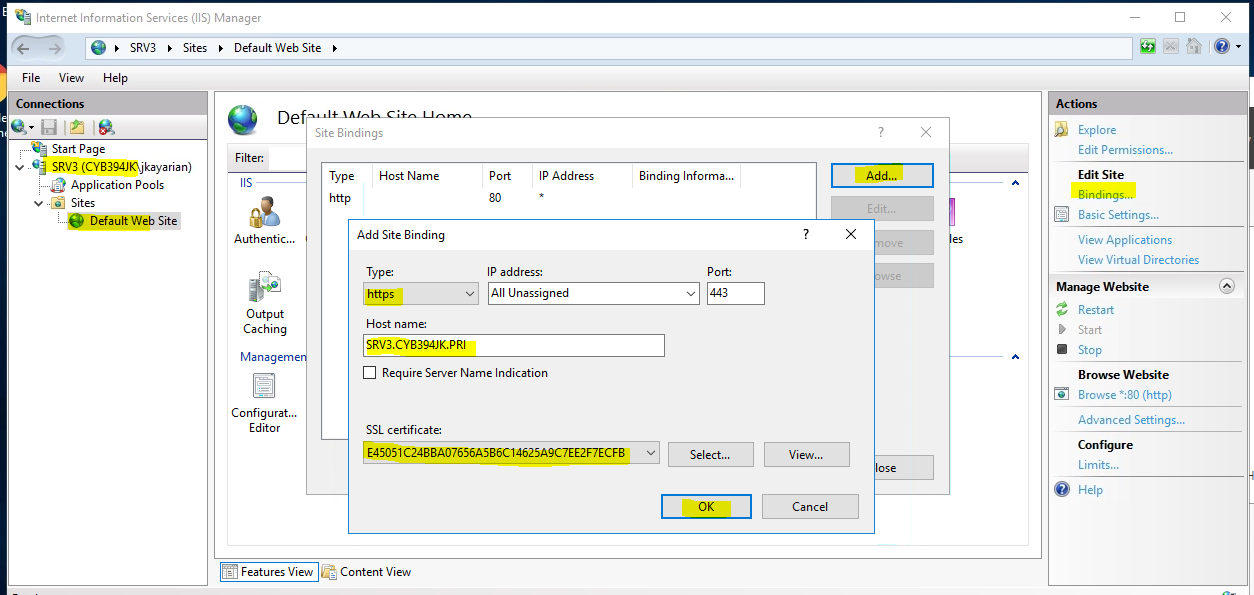


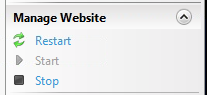
1. **Click [Apply] then [OK]. Close the Certificate Template Console**
2. Right click on the Certificate Templates -> Certificate Template to Issue -> and choose

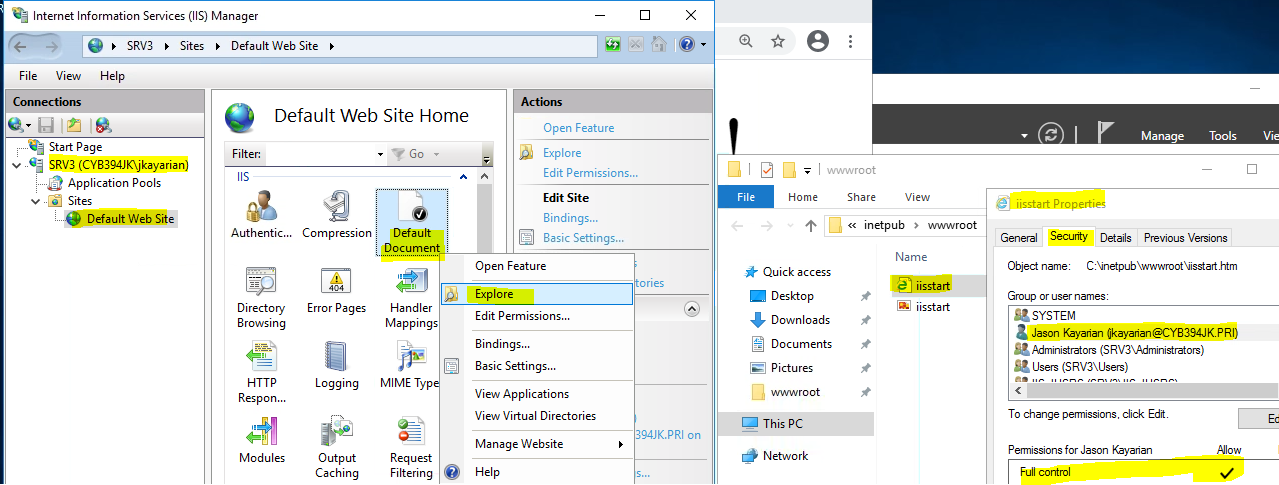
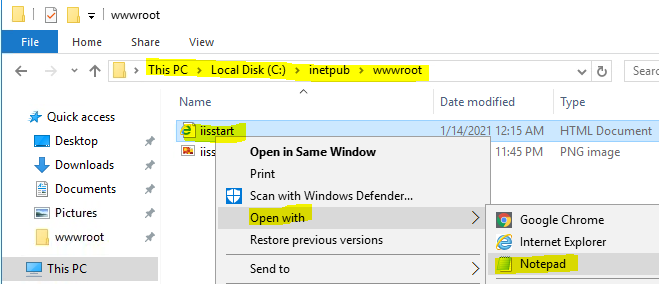


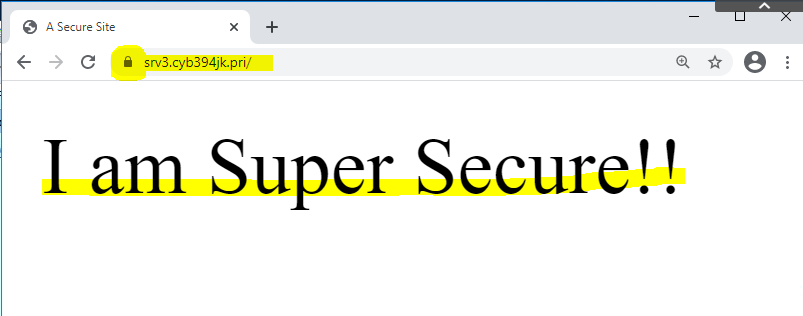
1. Choose **Web Server SAN** click [OK]  
   
2. On **SRV3** -> Restart the Server
3. **SRV3** -> Server Manager -> Tools -> Internet Information Services (IIS) Manager. May need to restart for Tools -> IIS menu option to appear.
4. Navigate the left pane **SRV3** -> Sites -> Default Web Site



1. On the right-hand side pane choose **Bindings** then click Add
2. Select **Type: https** and give the host name **SRV3.CYB394XX.PRI**
3. In the SSL drop down choose the default certificate and select OK  
   
4. Restart IIS under Manage Website



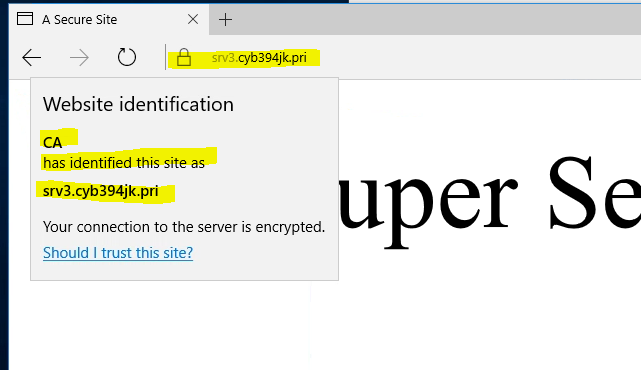
1. Right-click the Default Document -> Explore and edit the [Security] of the iisstart file to give your PDA full control; then edit the iisstart document. Modify the default HTML page to say *your name* and I’m super secure.  
     
     
     
   
2. Browse to the website using HTTPS://SRV3.CYB394XX.PRI

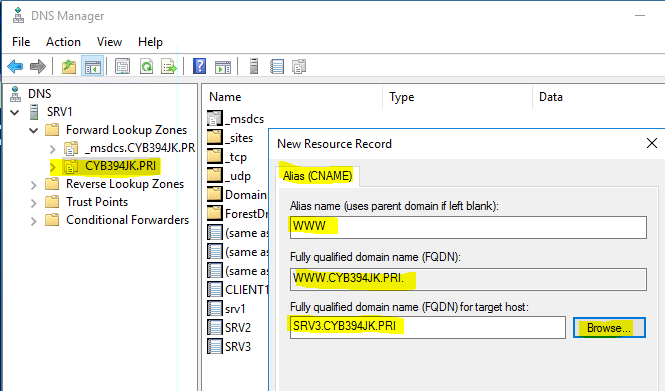


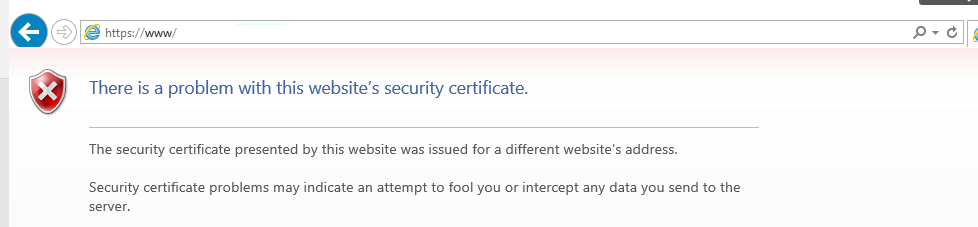
|  |
| --- |
| Screenshot of your Secure (Lock enabled) Default Document |

**Part 2**

1. Sign-In to CLIENT1 with your PDAA
2. Install Chrome
3. Within Chrome open <https://srv3.cyb394xx.com>
4. You should be taken to the page setup previously.
5. Click on t he lock symbol next to the Internet Explorer refresh bar.



1. SRV1 -> Server Manager -> Tools -> DNS create a CNAME record with an alias name **www** that points back to SRV3.CYB394JK.PRI as the target host.  
   
2. Once the CNAME is created open a Command Prompt on CLIENT1 and ping www  
   We are not concerned that the request times out. Here we are checking for name resolution. You should see that the www resolves to srv3.cyb394.com
3. Close Chrome
4. ~~Open a new Internet Explorer session and type in~~ [~~https://www~~](https://www)
5. ~~You should get a warning about a problem with this websites security certificate.~~

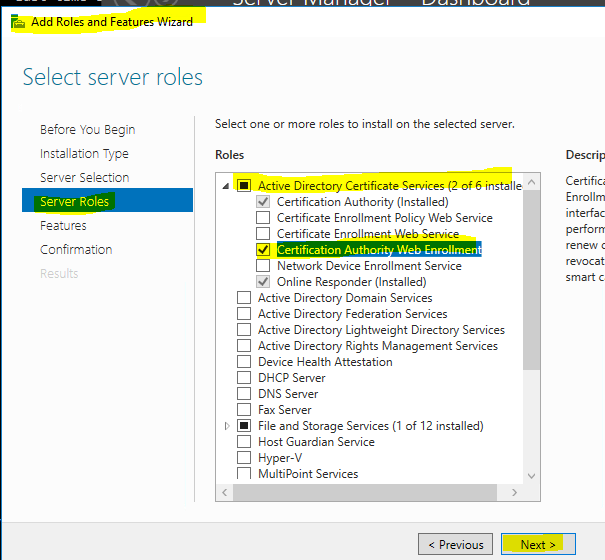
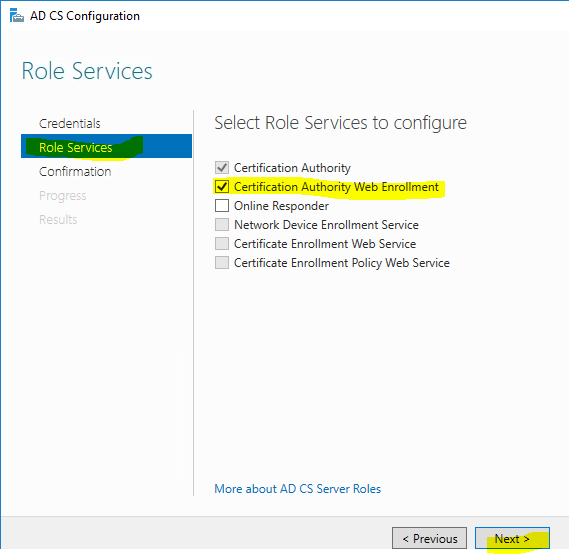
~~~~

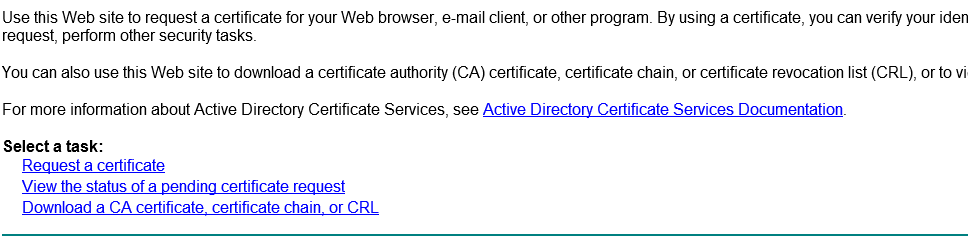
1. ~~Close out the browser and try it once again but this time put in~~ [~~https://www.cyb394.com~~](https://www.cyb394.com)

~~You should get presented with the same warning.~~

1. ~~Why is there a certificate warning? Type down your answer on a piece of paper and give it to the professor before proceeding.~~

# Part 2 Installing AD CS Certification Authority Web Enrollment Role

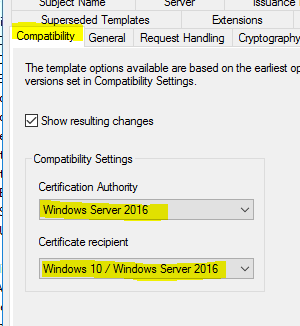
1. On **SRV2** -> Server Manager -> Add Roles and Features -> expand the Active Directory Certificate Services -> add the **Certification Authority Web Enrollment Role**.  
   
2. Once the install is complete Reboot SRV2.
3. SRV2 -> Server Manager -> Click on the  and finish configuring the **Certification Authority Web Enrollment Role using All default entries.**  
     
     
    -> [Configure] -> Do Not Configure Additional Roles.
4. SRV2 -> open Chrome and navigate to [http://srv2/certsrv](http://srv2.cyb394.com/certsrv)
5. You should get a web page with three options



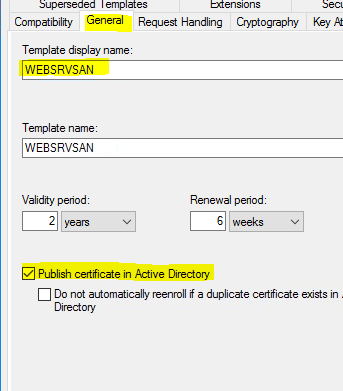
1. This web form is useful for devices that do not have a tool built in to request certificates or for out external domain certificate requests.

# Part 3 Generating a new certificate for SRV3

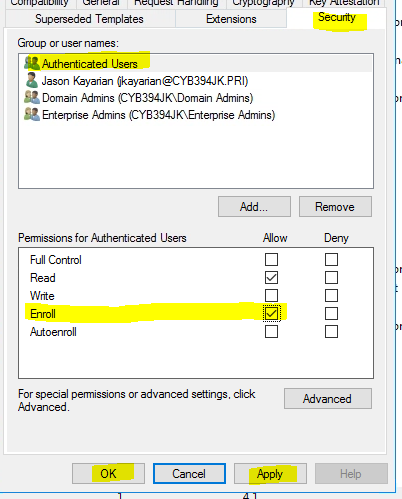
1. SRV2 -> Server Manager -> Tools -> Certification Authority -> CA -> Certificate Templates folder <- right click -> Manage.
2. Locate the Web Server template <- right click -> Duplicate Template.
3. Set [Compatibility] to the following:

 **DO NOT click [Apply] or [OK]**

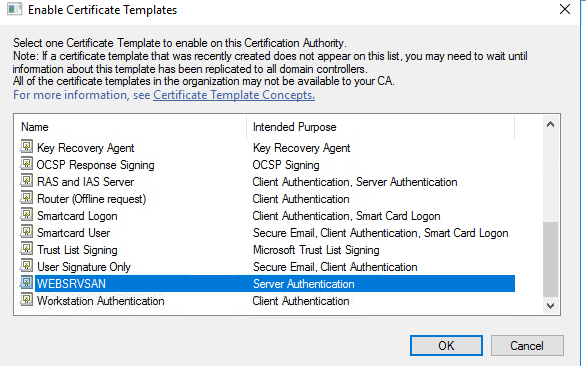
1. Set [General] tab Template display name to WEBSRVSAN **\*\* Ensure to [V] Publish in Active Directory:**

 **DO NOT click [Apply] or [OK]**

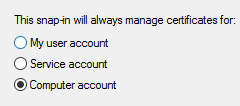
1. Set [Security] tab permissions make sure **Authenticated Users have Enroll** permissions.



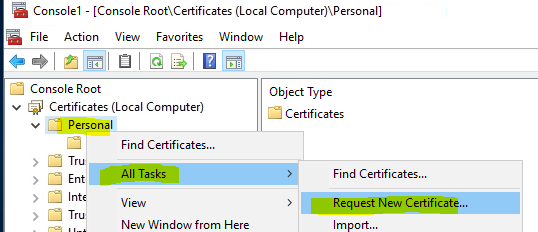
1. Click [Apply] then [OK].
2. Close the Certificate Template Console.
3. Certificate Templates <- right click -> New Certificate Template to issue.
4. Locate WEBSRVSAN in the list and select OK.

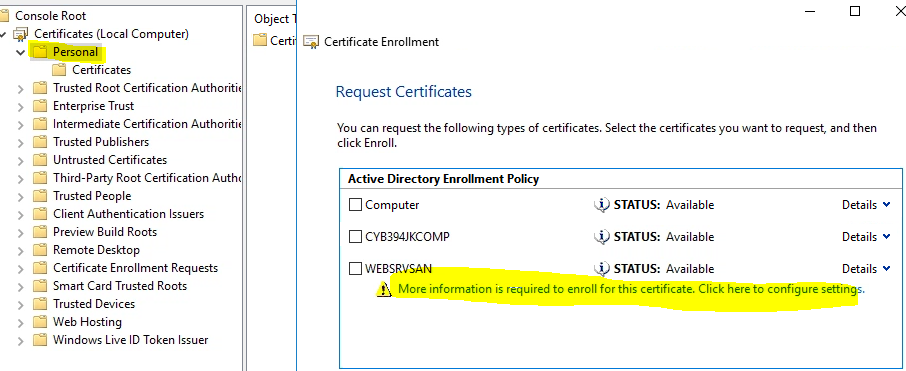


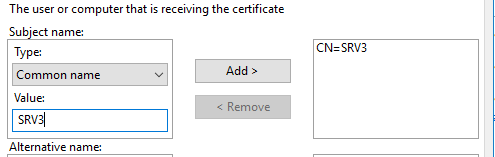
1. On SRV3 launch the mmc console by typing mmc in the run bar.
2. Go to, File 🡪 Add/Remove snap-ins -> Certificates then click Add.
3. Select the following and Click Next.



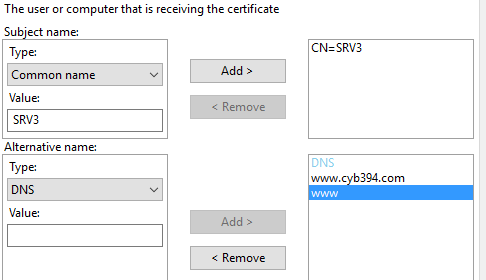
1. Add the Certificate **Local Computer** (the computer this console is running on) then click [Finish].
2. Then click [OK]
3. Click on the Personal Folder within the snap in and then Right click 🡪 All Tasks 🡪Request New Certificate.

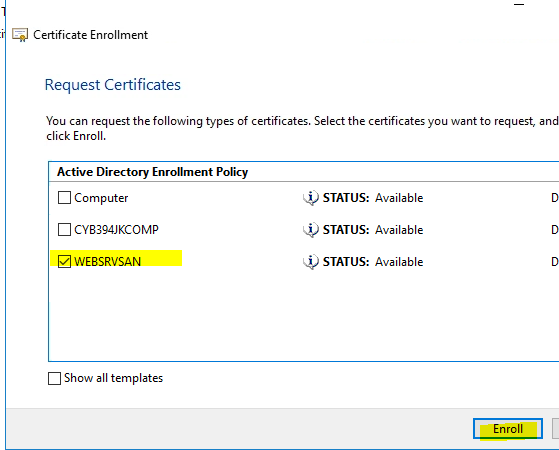
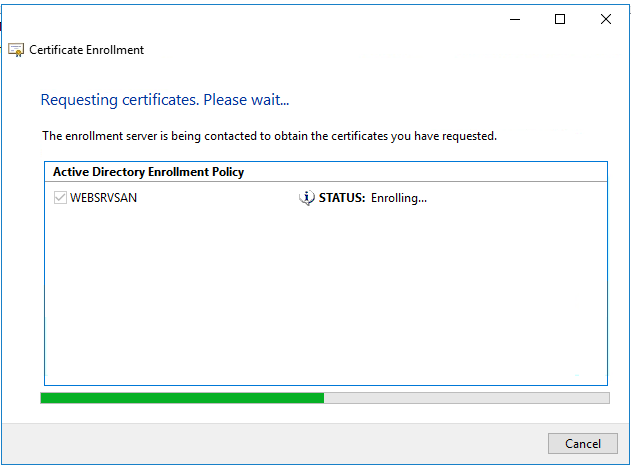


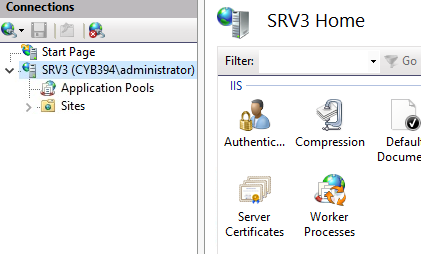
1. Click [Next] until you see the list of available templates under the Active Directory Enrollment Policy.
2. Under the WEBSRVSAN template Click on the blue text that says more information is required....  
   
3. Under Subject Name choose Type: -> **Common name** and in the Value: **SRV3**Then click the Add> button.



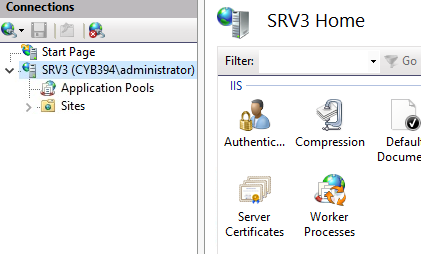
1. Under the Alternative name: Type: -> DNS. Then in the Value: [WWW.CYB394XX.PRI](http://WWW.CYB394XX.PRI) Then click add.
2. Add another value called WWW.

   
**DO NOT click [Apply] or [OK]**

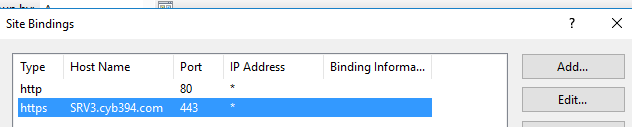
1. Under the [General] tab type WEBSRV for the friendly name.
2. Click [Apply] then [OK]
3. In the certificate templates dialog box Check mark WEBSRVSAN then click [Enroll] 
4. SRV3 -> Server Manager -> Tools -> Internet Information Services
5. Double Click on SRV3 then on the right-hand side double click Server Certificates.

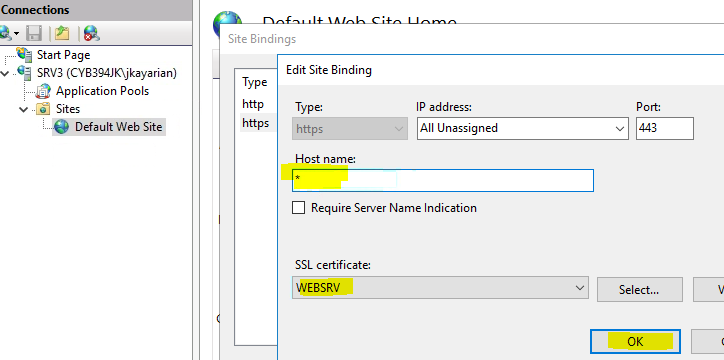


1. You should see the friendly name WEBSRV here.
2. Click on SRV3 again and drill down to find the default website.



1. In the right-hand Actions click on the Bindings and choose your https SRV3.CYB394XX.PRI site and select Edit.



1. Under SSL Certificate choose the friendly name WEBSRV Under hostname remove SRV3.cyb394.com and put a \*  
   
2. Restart SRV3 and allow a minute or so for it to start.
3. Client1 navigate to HTTPS://WWW.CYB394XX.PRI Then HTTPS://WWW

You should be able to reach each site without any certificate warnings.

|  |
| --- |
| Screenshot of both [www.cyb394xx.pri](http://www.cyb394xx.pri) and www |

1. Try to navigate to HTTPS://SRV3.CYB394XX.PRI you should receive a certificate warning. This is because we did not specify this name as an alternate name in the certificate request.
2. ~~Delete all certificates in the computer personal certificate store. Then restart SRV3~~

# ~~Part 4 (Certs on your own)~~

1. ~~Make it so Client1 can reach the web site by browsing to the following URLS~~

[~~https://www.cyb394.com~~](https://www.cyb394.com)

[~~https://www~~](https://www)

[~~https://srv3.cyb394.com~~](https://srv3.cyb394.com)

[~~https://secure.cyb394.com~~](https://secure.cyb394.com)

[~~https://secure~~](https://secure)

# Part 5 – A Jesse style lab section 😉 See if you can do it & Enjoy!!

1. Power on SRV4 and change its name to SRV4.
2. Set the network stack:  
   IP: 10.0.0.40  
   Subnet: 255.255.255.0  
   Gateway: 10.0.0.254  
   Preferred DNS: 10.0.0.10
3. Install Chrome
4. Navigate to <https://www.cyb394.com>
5. You should get a certificate warning.
6. Click continue to the site.
7. Then view the certificate information to identify why we are getting a cert warning.
8. From SRV4 navigate to [http://srv2/certsrv](http://srv2.cyb394.com/certsrv)
9. Select Download a CA certificate, certificate chain, or CRL.
10. Select Download CA certificate.
11. Then Click Save.
12. Add the local computer certificate snap from mmc (You should be able to do this by now).
13. Navigate to Trusted Root Certification Authority then select certificates.
14. Right click Select All Tasks then import.
15. Browse to the CA cert you just downloaded.
16. Click next all the way through to complete the import.
17. Close Chrome and then browse to the website again. You should be able to reach the page without any warning.

|  |
| --- |
| Screenshot of successful site: |

End Lab3.