Lab 2 Part 2

# Part 1

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

1. Logon to client1 and launch Internet Explorer.
2. In the address bar type: <https://srv3.cyb394.com>
3. You should be taken to the page setup previously.
4. Click on the lock symbol next to the Internet Explorer refresh bar.

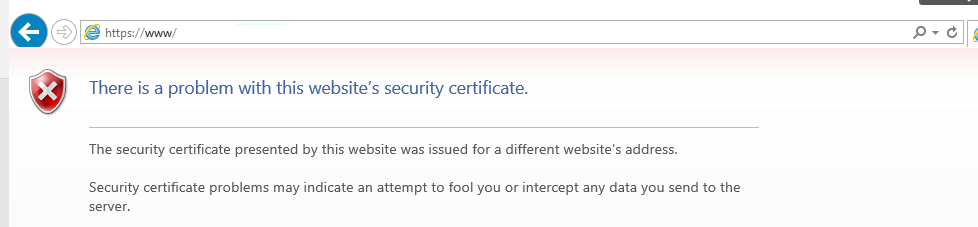


1. Click on view certificates.

\*You should notice that your Enterprise CA has issued this certificate. It has identified the server as srv3.cyb394.com

Normally Organizations will not access an intranet page by using the server fqdn. It will usually be a shorter name like **www** or something that identifies the web servers’ function.

1. In DNS create a CNAME record with an alias name **www** that points back to srv3.cyb394.com 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 any open Internet Explorer windows.
4. Open a new Internet Explorer session and type in <https://www>
5. You should get a warning about a problem with this websites security certificate.



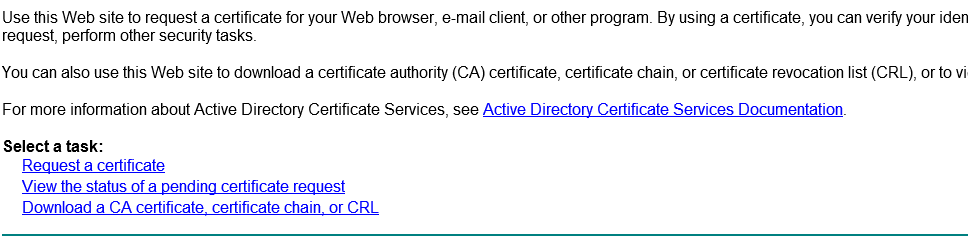
1. Close out the browser and try it once again but this time put in <https://www.cyb394.com>

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

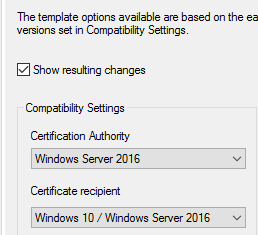
1. On SRV2 go to the Add Roles and Features wizard and then add the Certification Authority Web Enrollment Role.
2. Once the install is complete additional configuration is required. Click on the  and finish configuring the Certification Authority Web Enrollment Role.
3. Once the installation is complete open Internet Explorer on SRV2 and navigate to [http://srv2/certsrv](http://srv2.cyb394.com/certsrv).
4. You should get a web page with three options



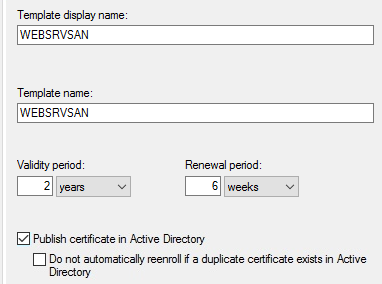
1. This web form is useful for devices that do not have a tool built in to request certificates or for out of off domain certificate requests.

# Part 3 Generating a new certificate for SRV3

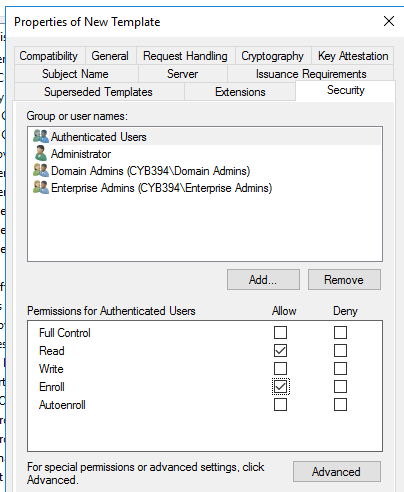
1. On SRV2 open the Certification Authority tool and navigate to the certificate templates folder.
2. Right click and select Manage.
3. Locate the Web Server template and right click to select duplicate template.
4. Set the Certification Authority and the recipient to the following:



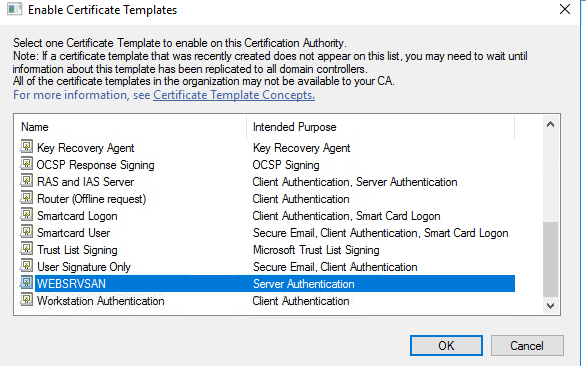
1. Under the general tab name the template WEBSRVSAN and check mark publish in Active Directory:



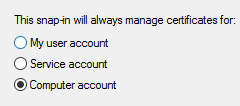
1. Under Security tab permissions make sure authenticated users have enroll checked.



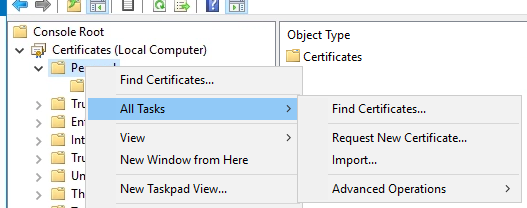
1. Click Apply then OK.
2. Close out of the Certificate Template Management windows.
3. Right click on the Certificate Templates folder and go to New Certificate Template to issue.
4. Locate WEBSRVSAN in the list and select OK.



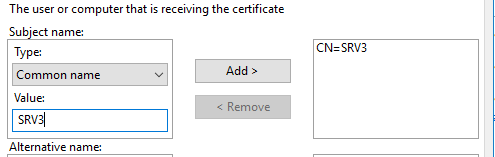
1. On SRV3 launch the mmc console by typing mmc in the run bar.
2. Go to, File 🡪 Add/Remove snap-in…. and the select certificates then click Add.
3. Select the following and Click Next.



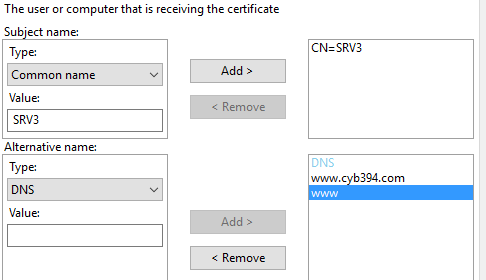
1. Add the Certificate Local Computer (the computer this console is running on) then click Finish.
2. Then click OK
3. Click on the Personal Folder within the snap in and then Right click 🡪 All Tasks 🡪Request New Certificate.



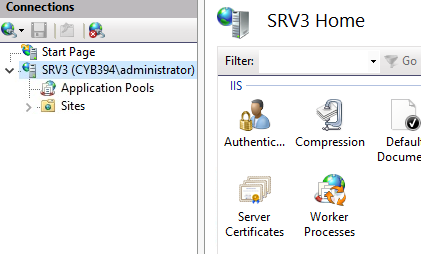
1. Click next until you see the list of available templates under the Active Directory Enrollment Policy.
2. Under the WEBSRVSAN template Click on the blue text that says more information is required....
3. Under Subject Name choose type Common name and in the value field put SRV3. Then click the Add> button.



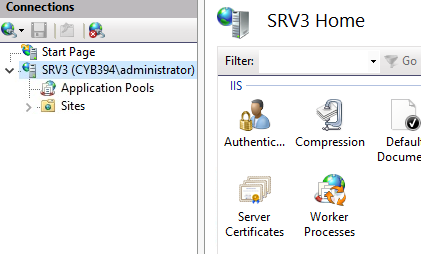
1. Under the Alternative name section choose DNS. Then in the value add [www.cyb394.com](http://www.cyb394.com) Then click add.
2. Add another value called www.



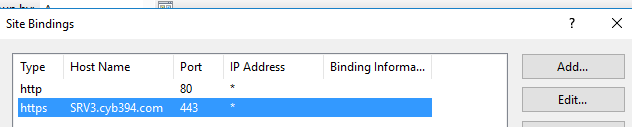
1. Under the general tab type websrv for the friendly name.
2. Click Apply then ok.
3. In the certificate templates dialog box Check mark WEBSRVSAN then click Next.
4. Launch Internet Information Services tool from SRV3.
5. Double Click on SRV3 then on the right-hand side double click server certificates.



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



1. Click on the bindings on the right-hand side choose your https 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
3. Once SRV3 is rebooted from client1 navigate to https://[www.cyb394.com](http://www.cyb394.com). Then <https://www>

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

1. Try to navigate to <https://srv3.cyb394.com> 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>

<https://srv3.cyb394.com>

<https://secure.cyb394.com>

<https://secure>

# Part 5

1. Power on SRV4 and change its name to SRV4.
2. Adjust the IP settings so that it has network connectivity with the other servers in the network
3. Try to navigate to <https://www.cyb394.com>
4. You should get a certificate warning.
5. Click continue to the site.
6. Then view the certificate information to identify why we are getting a cert warning. Inform your professor when you have the answer.
7. From SRV4 navigate to [http://srv2/certsrv](http://srv2.cyb394.com/certsrv)
8. Select Download a CA certificate, certificate chain, or CRL.
9. Select Download CA certificate.
10. Then Click Save.
11. Add the local computer certificate snap from mmc (You should be able to do this by now).
12. Navigate to Trusted Root Certification Authority then select certificates.
13. Right click Select All Tasks then import.
14. Browse to the CA cert you just downloaded.
15. Click next all the way through to complete the import.
16. Close IE and then browse to the website again. You should be able to reach the page without any warning.