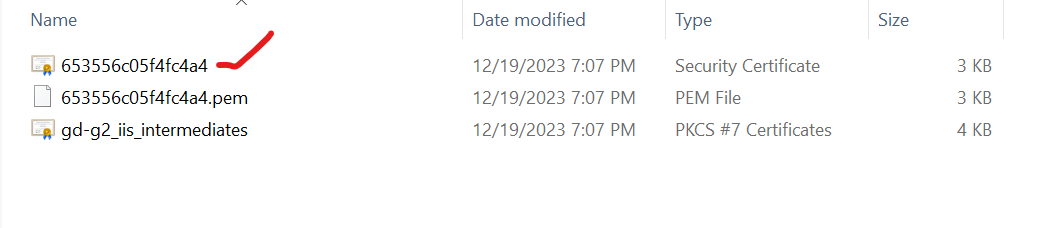
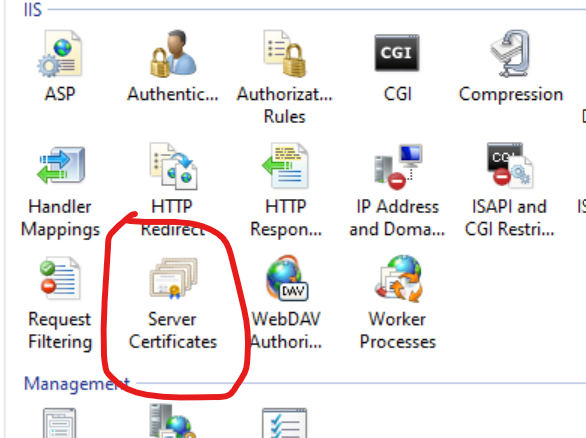
**Steps to Set Up SSL Certification**

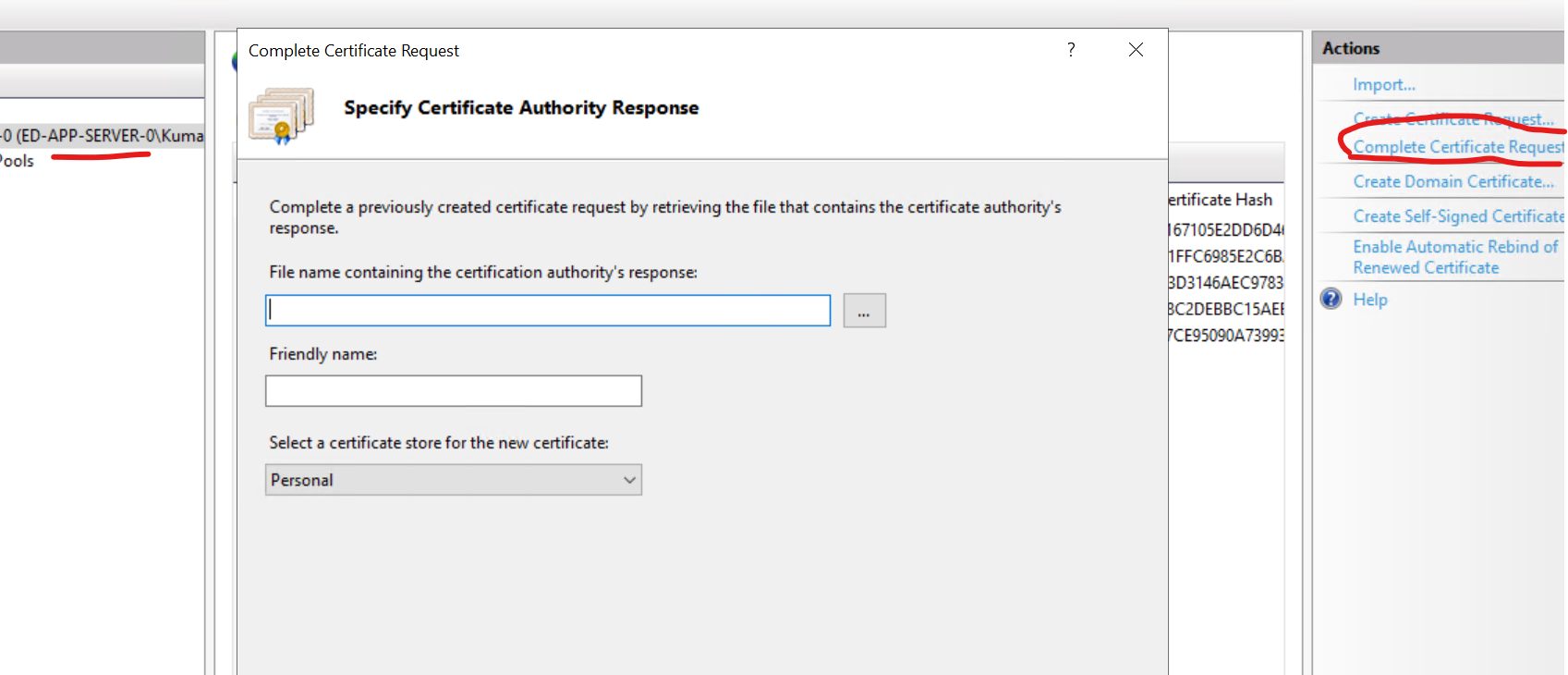
**"The attached image shows the certifications required."**



Step 1: Open IIS and navigate to "Server Certificates"

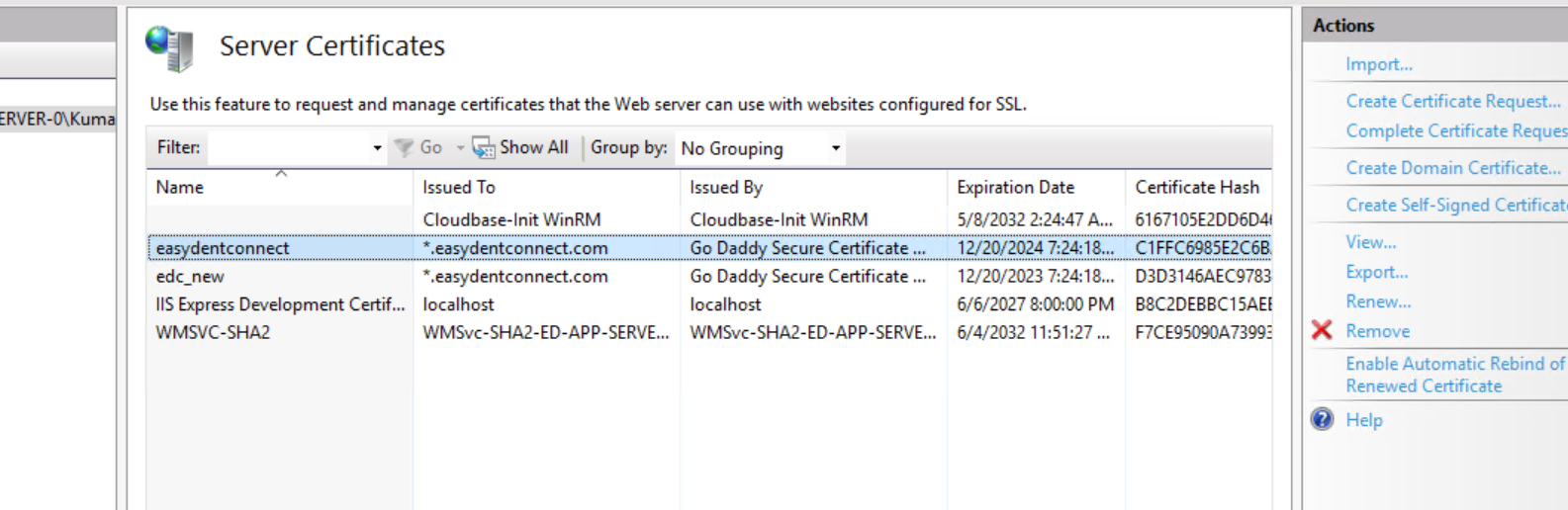


Step 2: Click "Complete Certificate Request" and provide the path where the certification file is located on the server. Enter any name in the "Friendly Name" field. Once you click "OK," it will prompt for a password. Enter the password and click "OK."



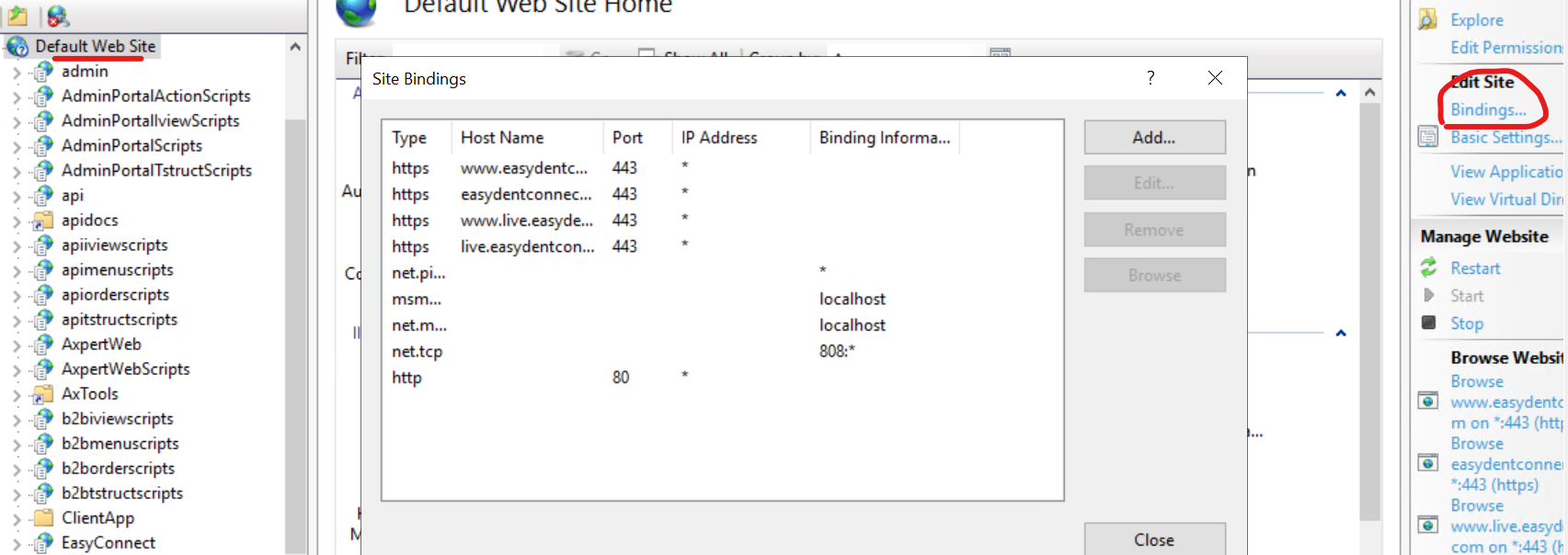
Step 3: After completing the above, exit IIS and return to the server certificates settings. You'll find the new SSL certification added with the name you provided. Verify the validity date.

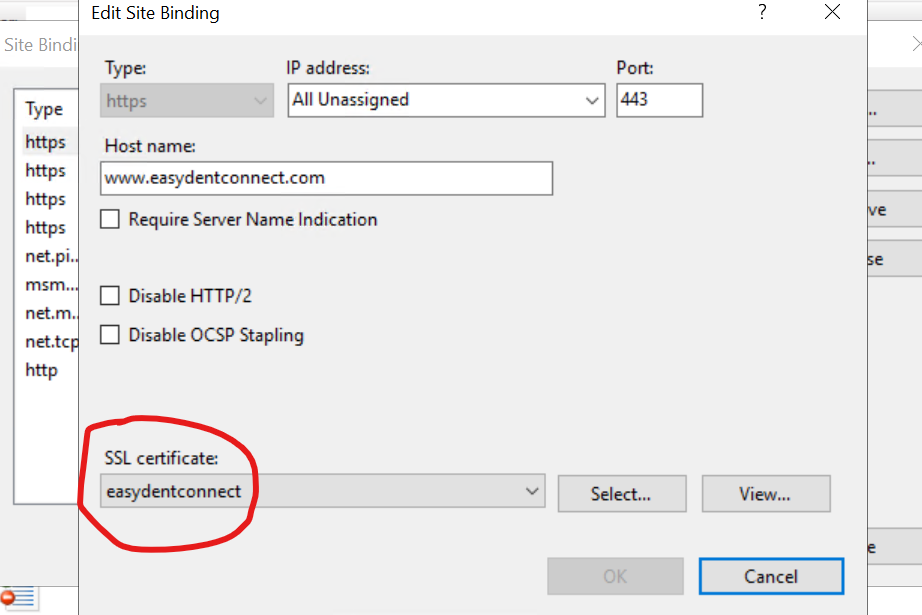
Step 4: Navigate to server certificate settings and click on the new SSL certificate. Choose to export the services and paste them somewhere accessible.



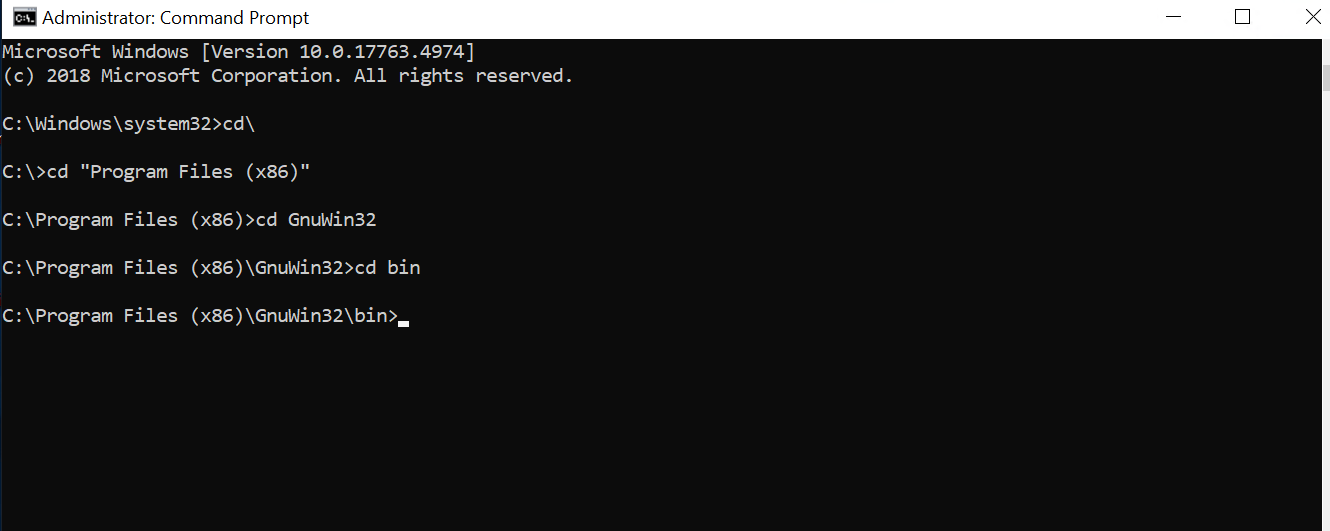
Step 5: Access "Program Files (x86) -> GnuWin32 -> bin." Delete the old server SSL file and replace it with the new server file.

Step 6: Go to the default website and click on "Bindings." In the all HTTPS services, select the new SSL certificate you created in the SSL certificate area.





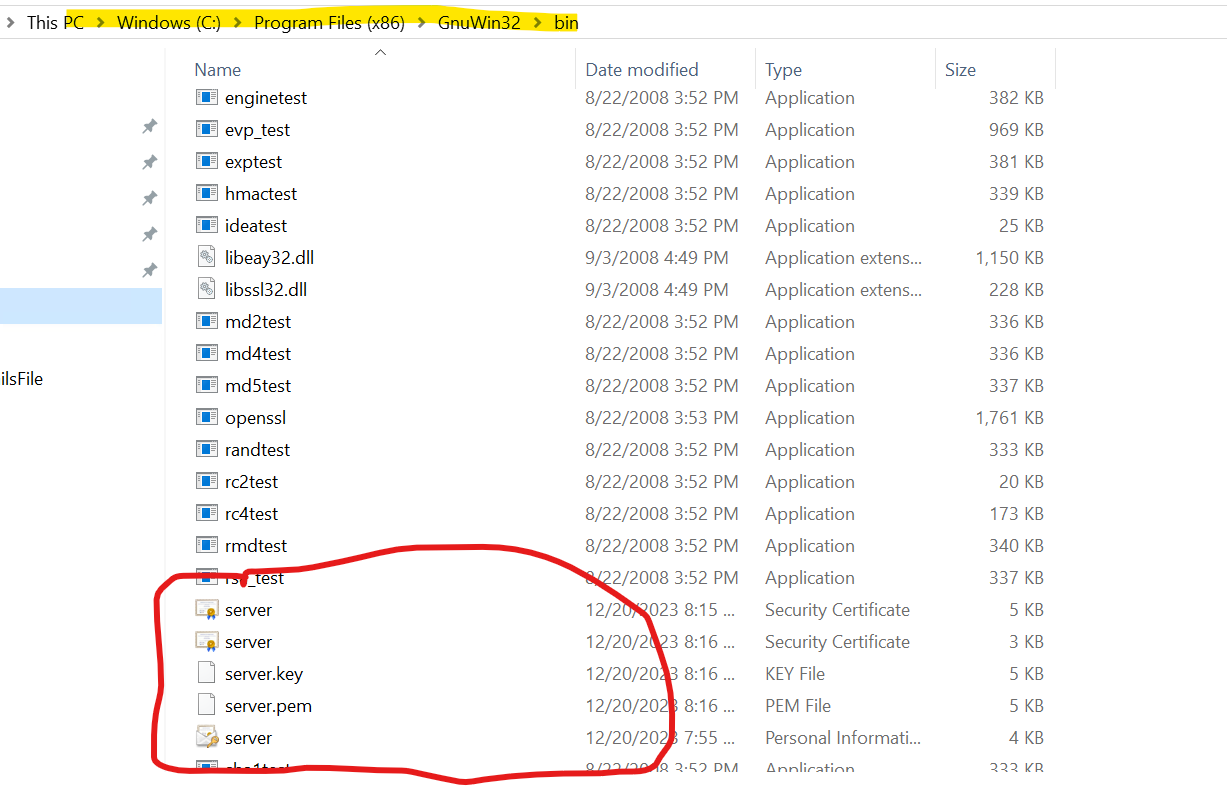
Step 7: Open CMD as an administrator and navigate to the folder mentioned below. Execute the three queries one by one. It will prompt you to enter a password. Please provide the password you used when creating the new SSL certificate; you'll need to enter that here.



openssl pkcs12 -in server.pfx -out server.cer -nodes  
openssl pkcs12 -in server.pfx -out server.pem -nodes  
openssl pkcs12 -in server.pfx -clcerts -nokeys -out server.crt

Step 8: Once the three queries are executed, below mentioned files will be generated.

Step 9: Make a copy of "server.pem" and paste it in the same folder. Rename the copy to "server.key".



Step 10: Copy all five server files and paste them into the node services folder under the certificate folder. Stop the node and restart the services.