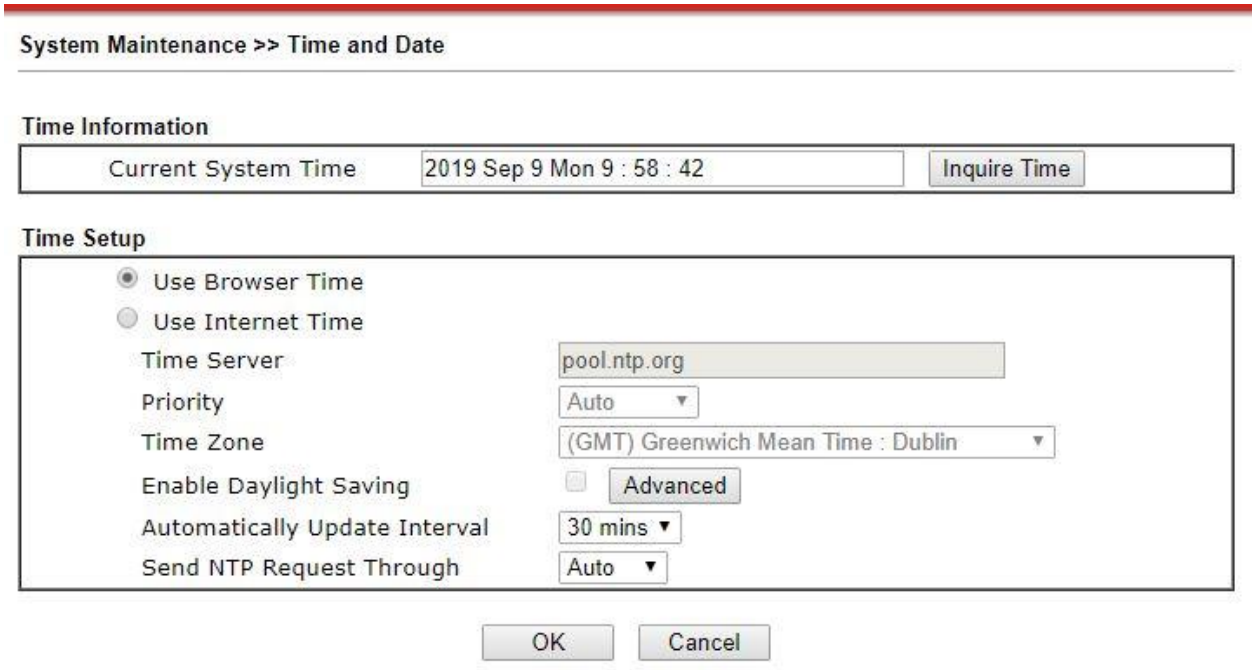
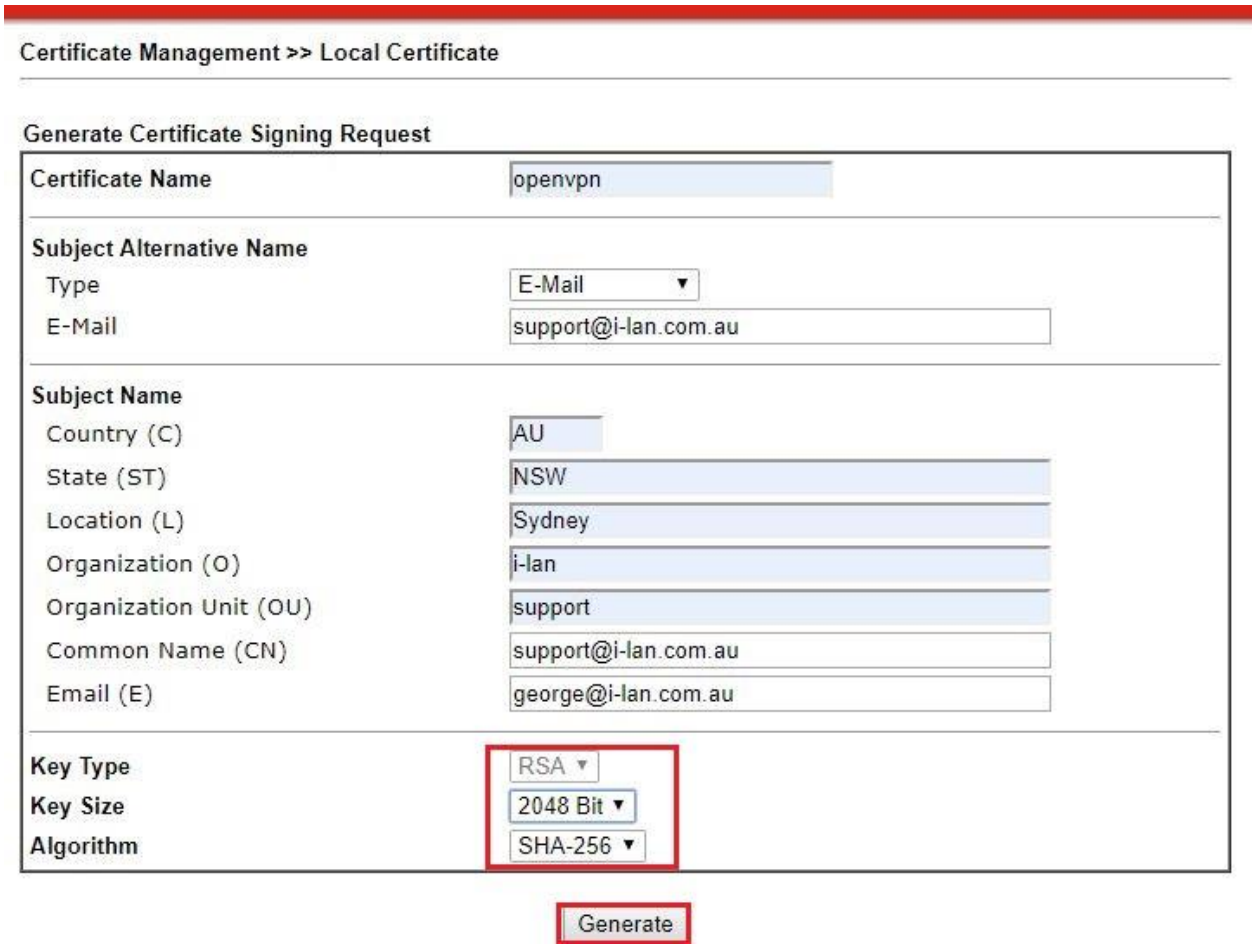
# How to configure OpenVPN in Vigor Router using XCA certificate and key management.

## *I. Create local certificate in the Vigor Router.*

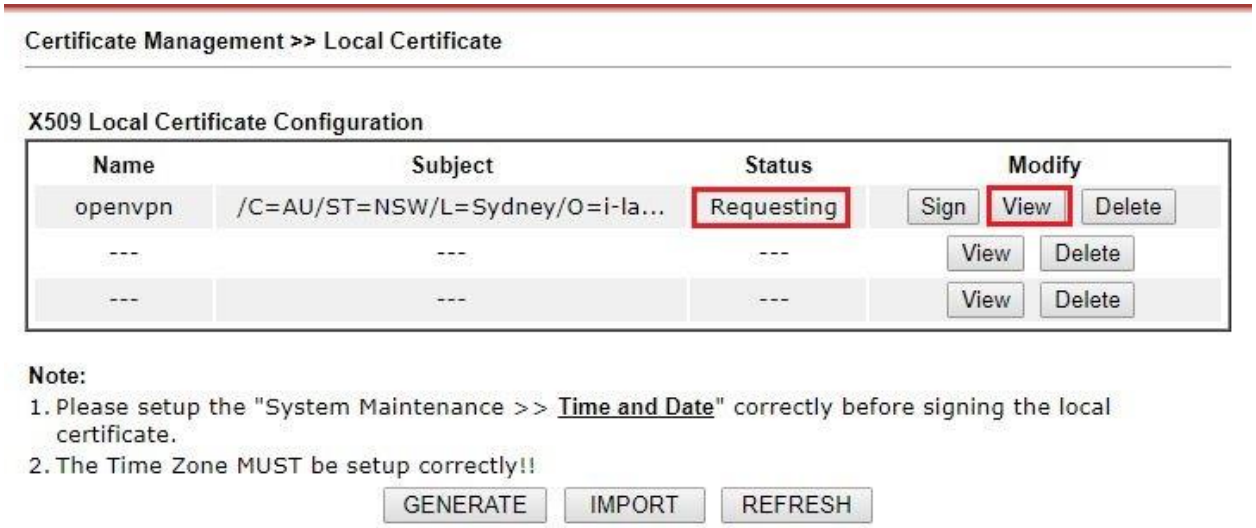
1.1 Since the certificate has a valid period, please make sure the time settings of the router is correct, by going to **System Maintenance >> Time and Date**.

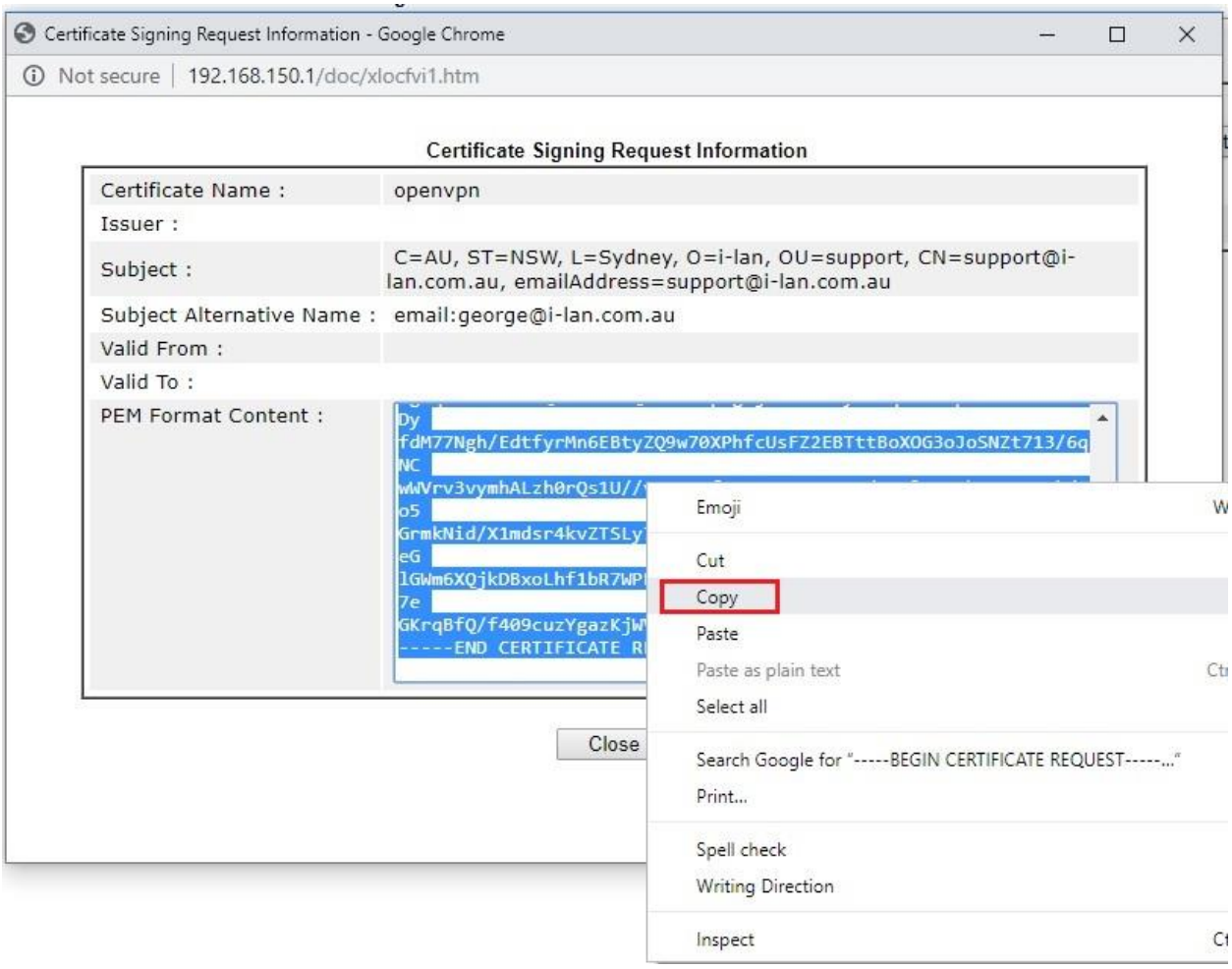


1.2 To generate a new certificate, go to **Certificate Management>>Local Certificate**. Type the information below and select Key size as ***2048 Bit*** and Algorithm as ***SHA-256*** and then click **Generate**.



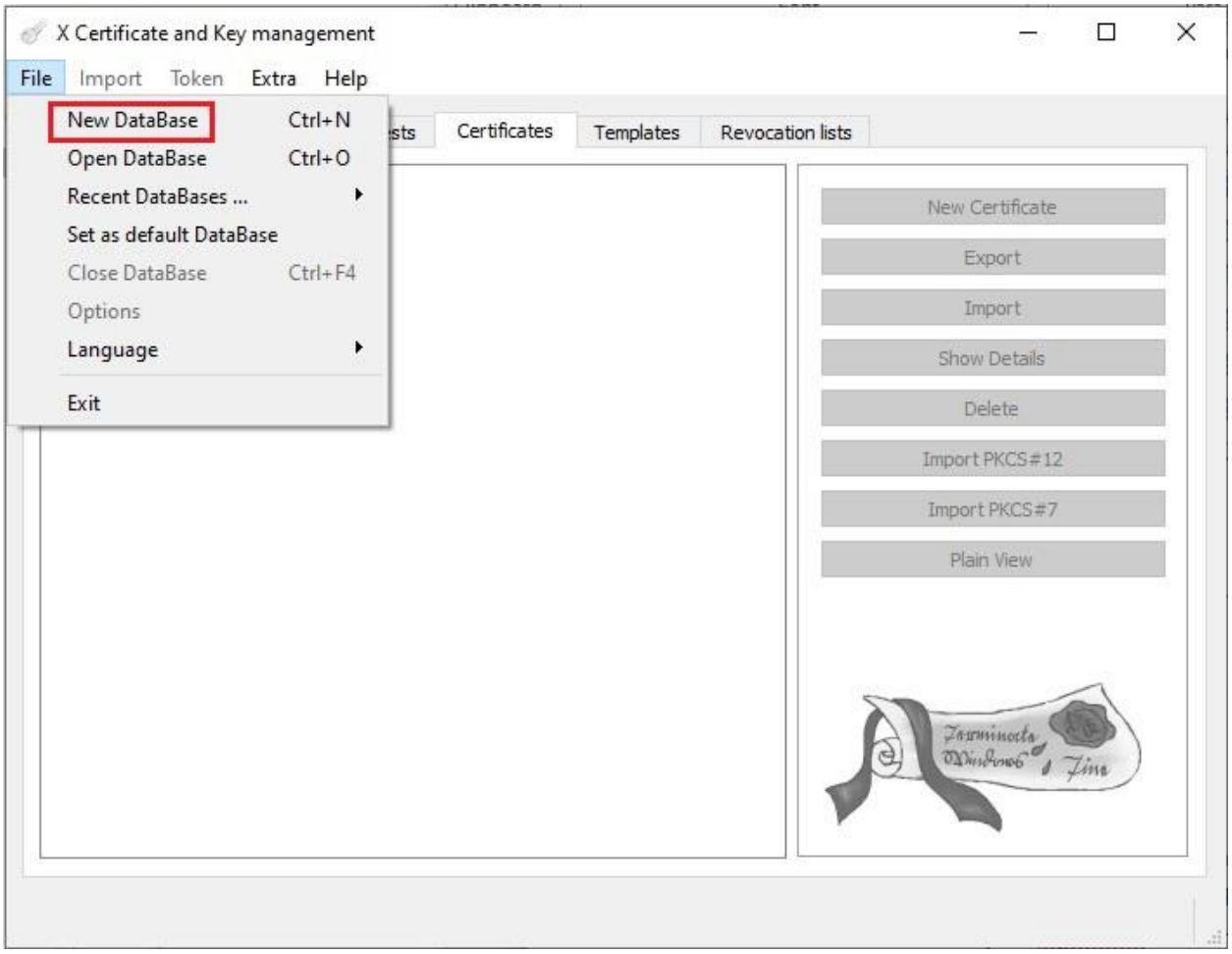
1.3 After generating, you will see the Certificate Signing Status as ***Requesting***, which needs to be signed by a CA. Click ***View*** and highlight the content inside the **PEM Format Content** and then right-click and select copy.



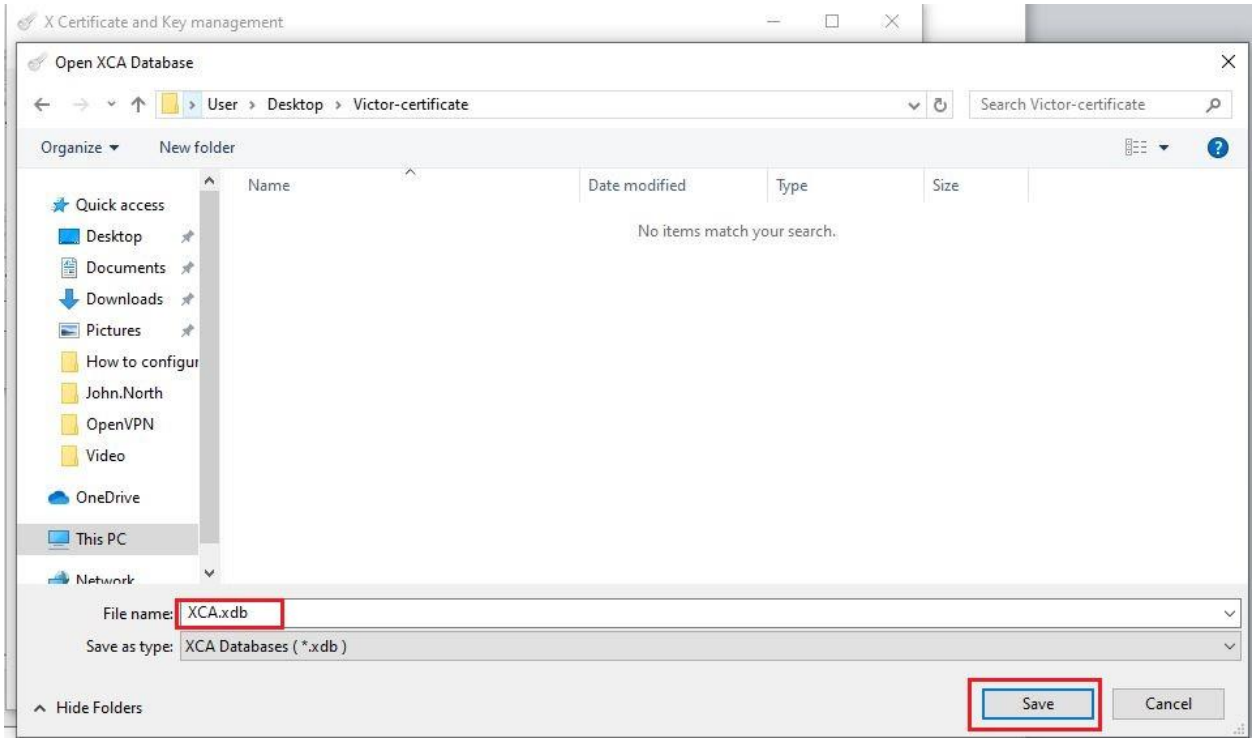



## *II. Create a new CA using XCA.*

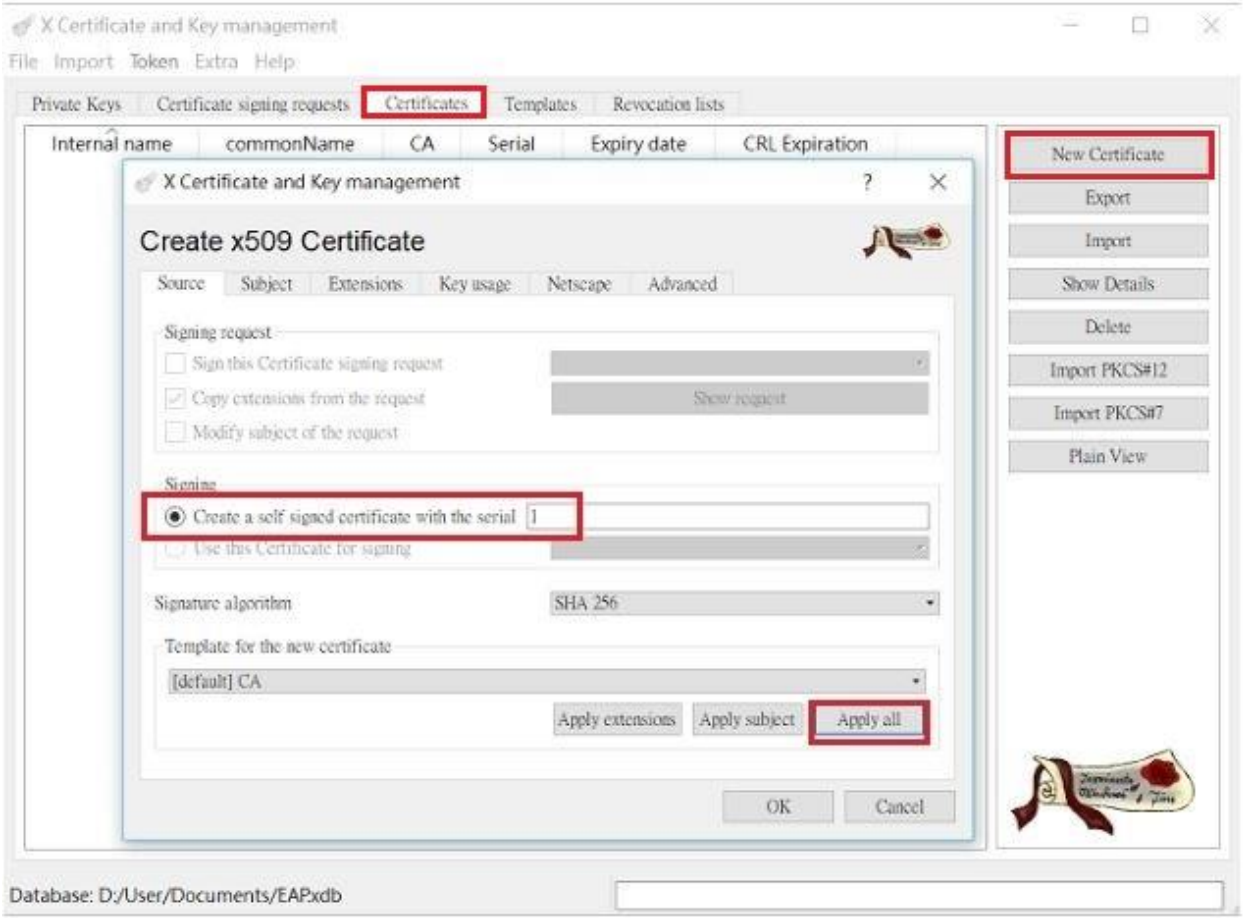
2.1 Launch XCA, go to File and click New Database.



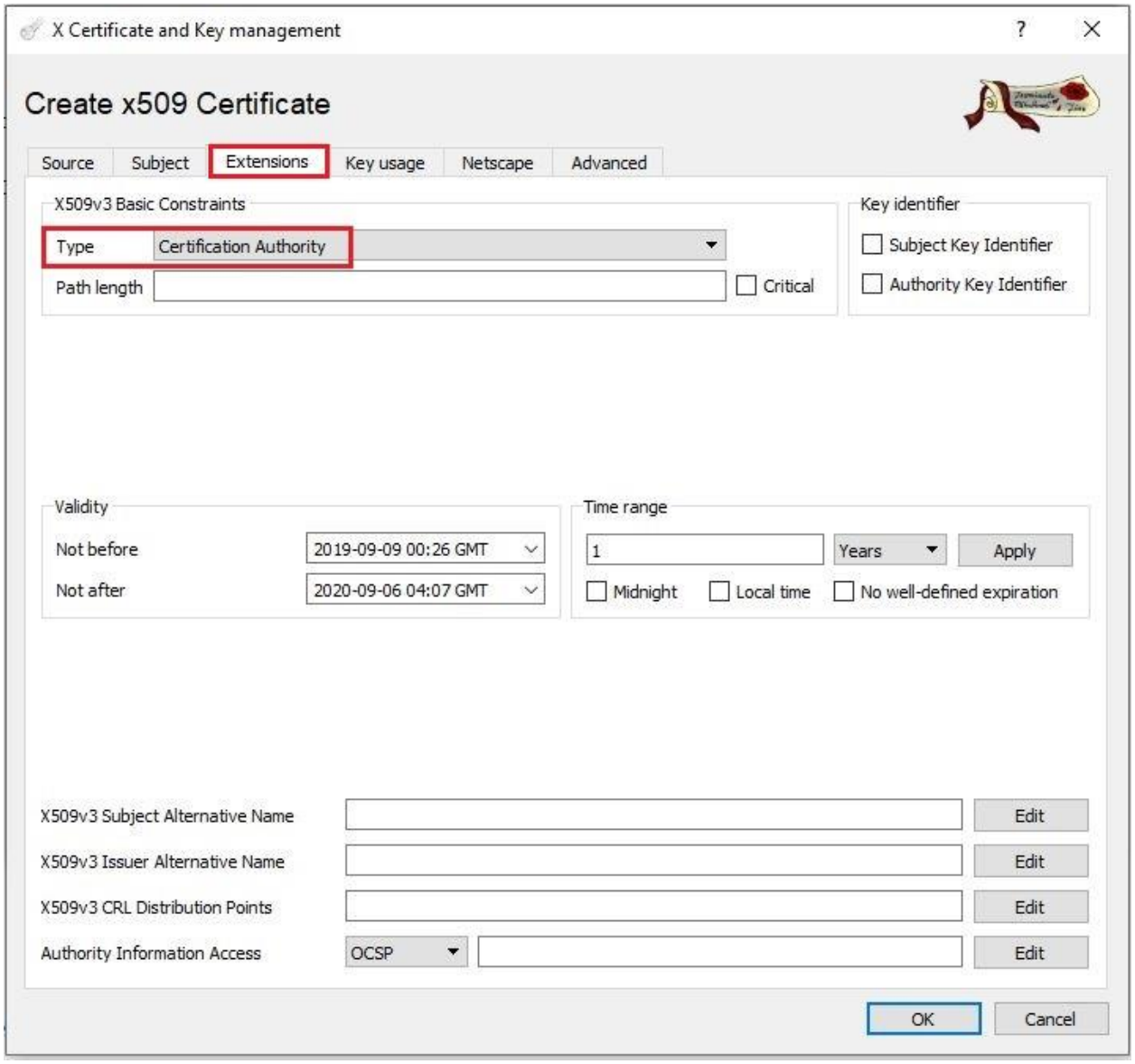
2.2 Name your database as e.g XCA.xdb and click ***save***.



2.3 Go to the ***Certificates tab***, click ***New Certificate***. Select ***Create a self-signed Certificate with the serial.*** Click ***Apply all*** to apply the CA Template.

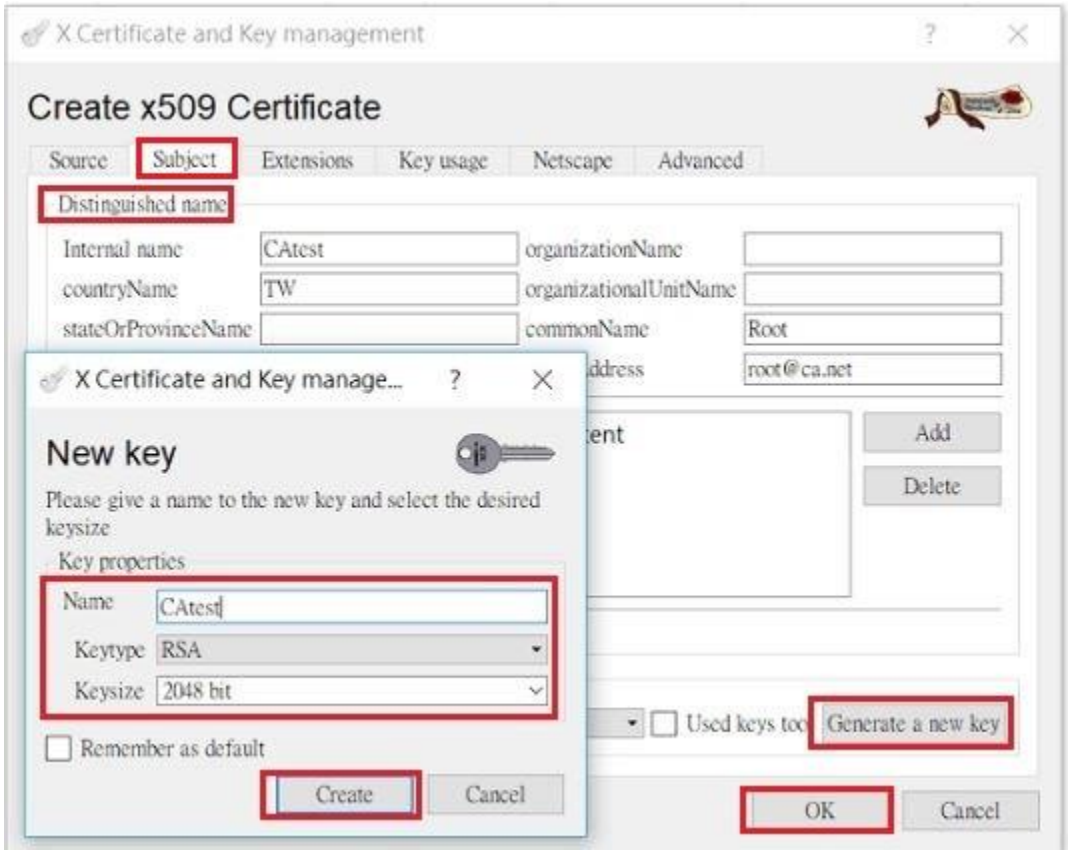


2.4 Go to the ***Extensions tab*** and select type as ***Certificate Authority***.



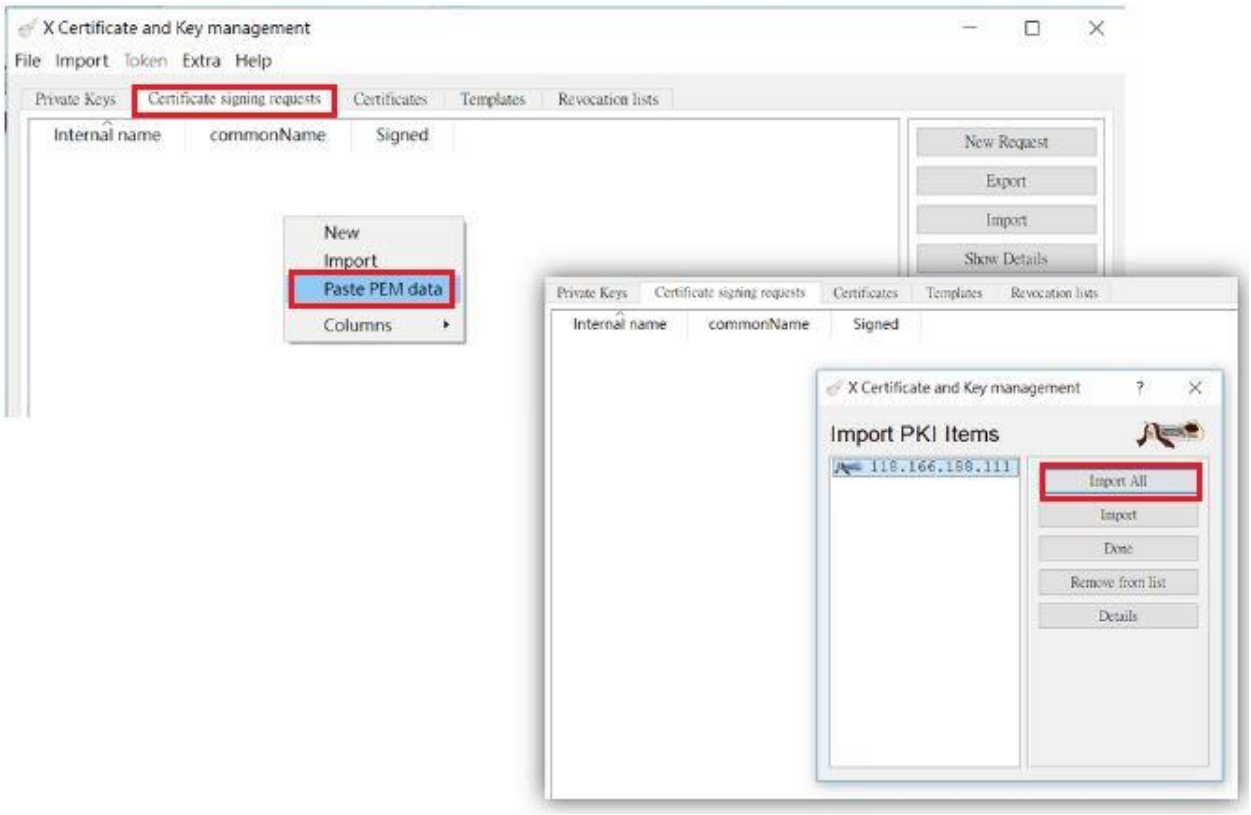
2.5 Go to the Subject tab.

- Enter certificate information under ***Distinguished name***, then click ***Generate a new key***.
- Select "RSA" for Keytype and "2048 bit" for Keysize, then click ***Create***.
- Click ***OK*** to generate the CA Certificate. Now we have the Trusted CA Certificate to sign the server certificate and client certificate.

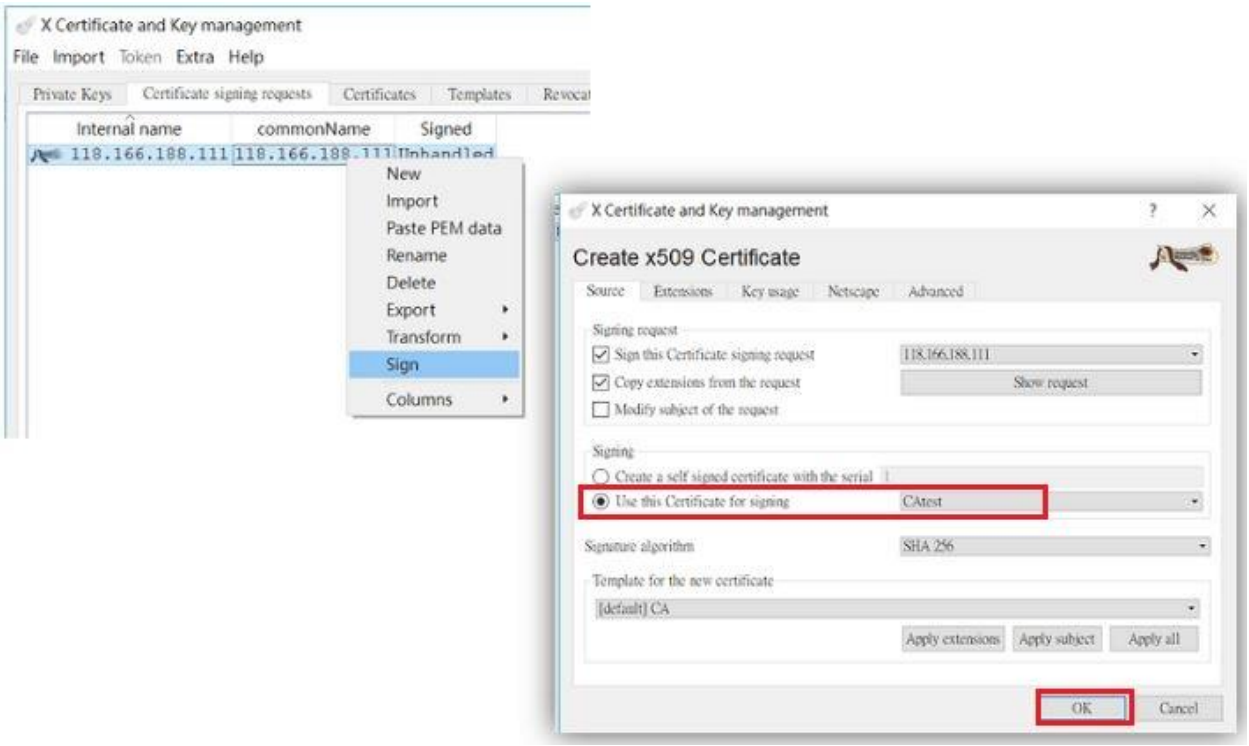


### *III. Importing Signed Server Certificate and CA Certificate to the Router.*

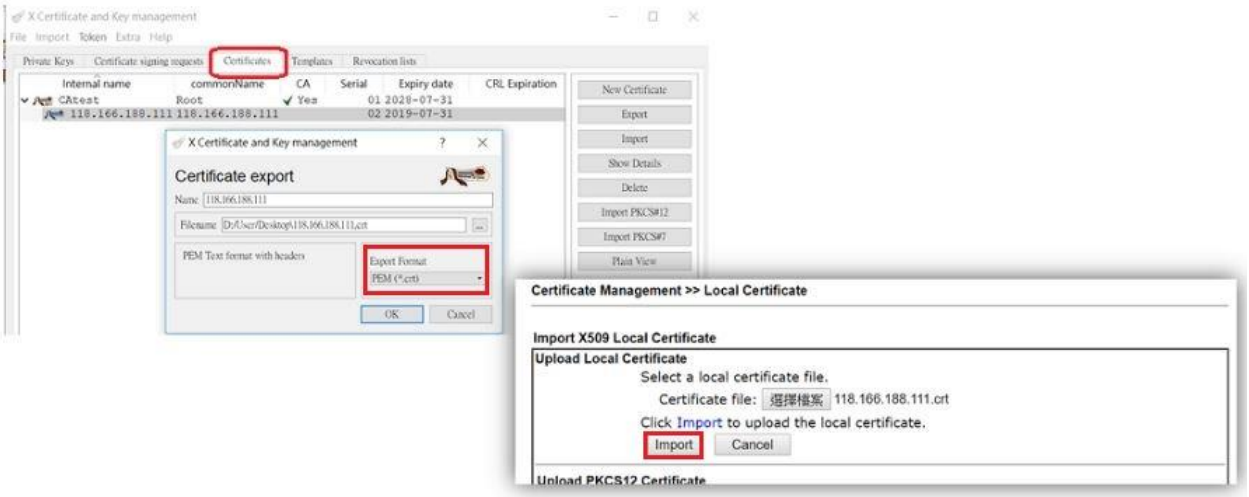
3.1 Go to ***Certificate signing requests***, right-click and select ***Paste PEM data*** and paste the PEM Format Content copied from the Vigor router in procedure 1.3. and then click ***Import All.***



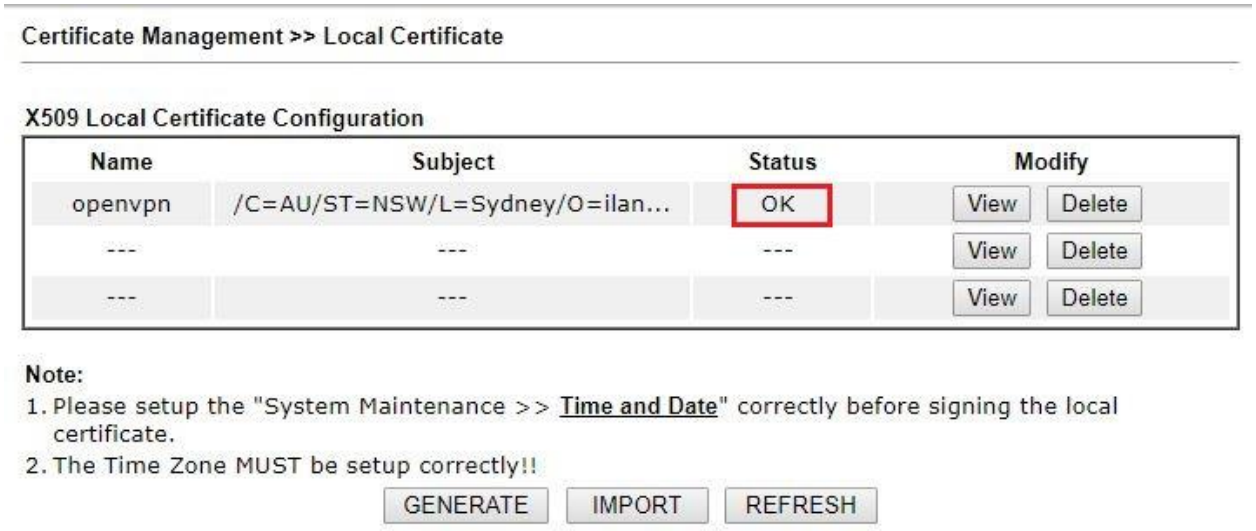
3.2 Right-click on the imported certificate and select **Sign**. Use the CA created in procedure 2 to sign the imported certificate and then click ***OK.***



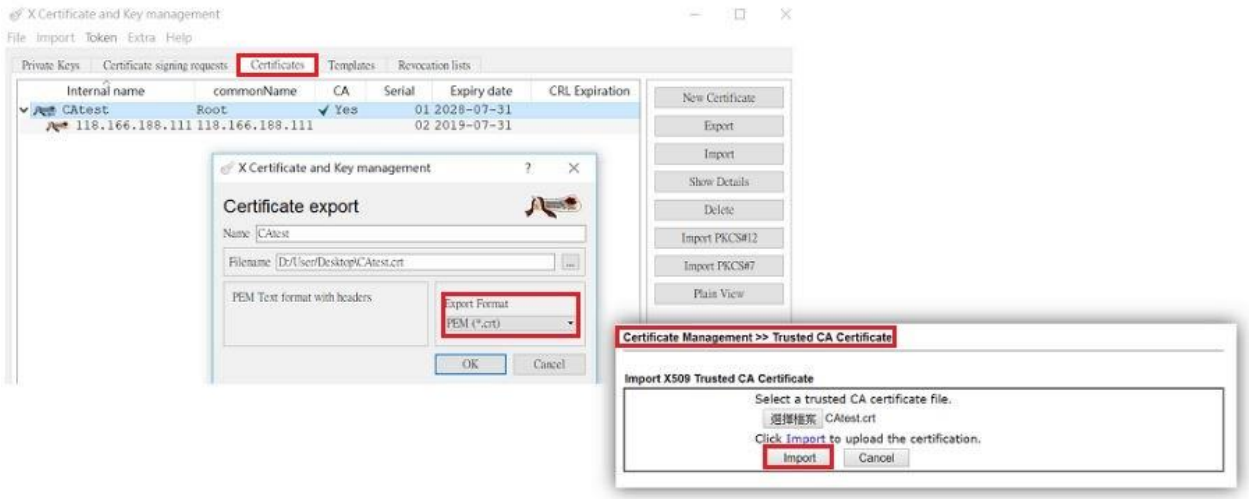

3.3 Under ***Certificate tab***, export the Singed Local Certificate as ***.crt*** format. Go back to the Vigor router's GUI and import it to the Vigor router by going to **Certificate Management >> Local Certificate >>Import**



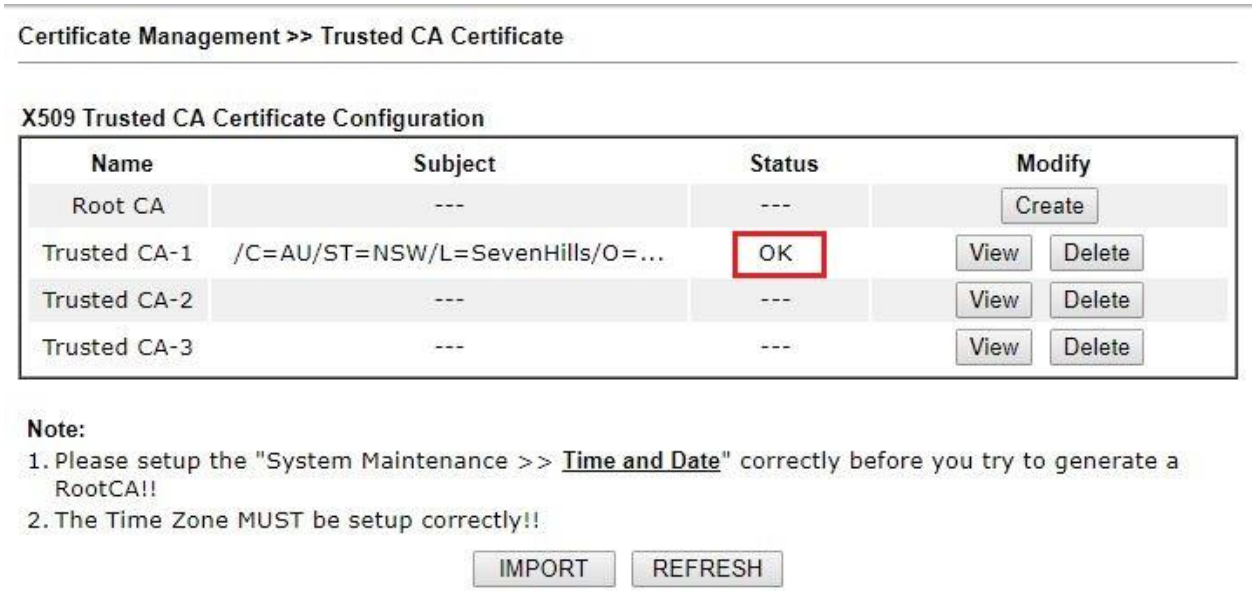
3.4 Make sure that the status of the certificate imported is ***OK***.




3.5 In XCA, go to ***Certificate***, choose the CA certificate and export it as ***.crt*** format, and then import the CA certificate to the Vigor router, by going to **Certificate Management >> Trusted CA Certificate**.

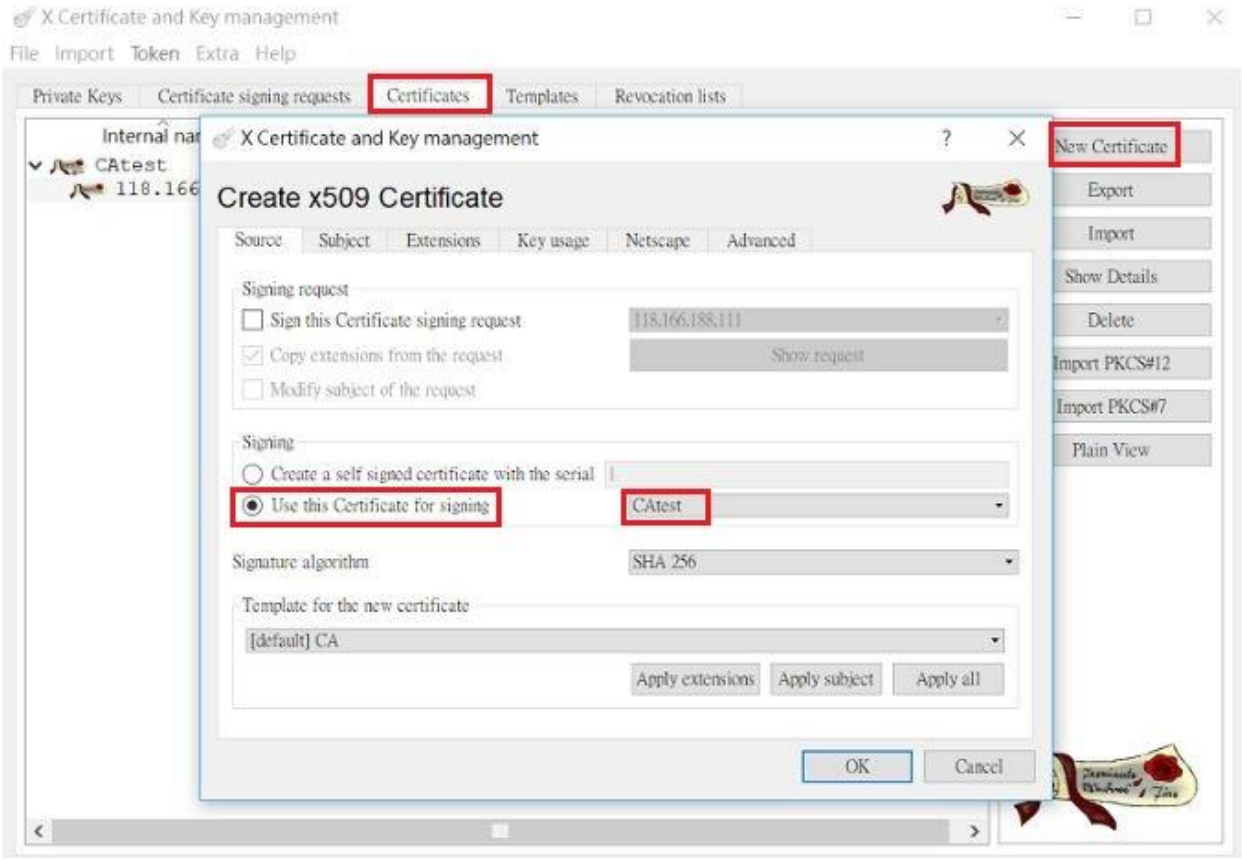


3.6 Make sure that the status of the Trusted CA imported is ***OK***.



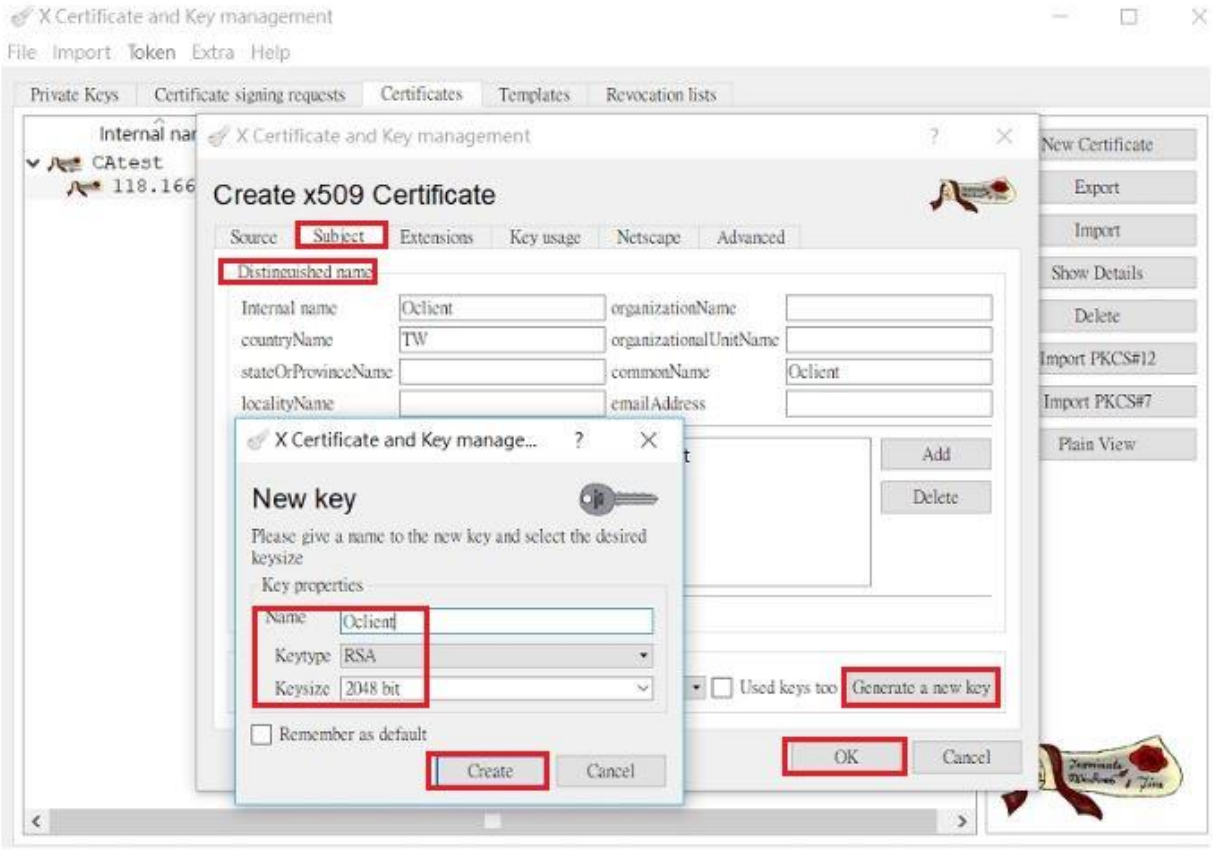

## *IV. Making a Private Certificate and Private Key for VPN Client.*

4.1 In XCA, go to **Certificates**, click **New Certificate**. Under ***Signing***, select ***Use this Certificate for singing***.

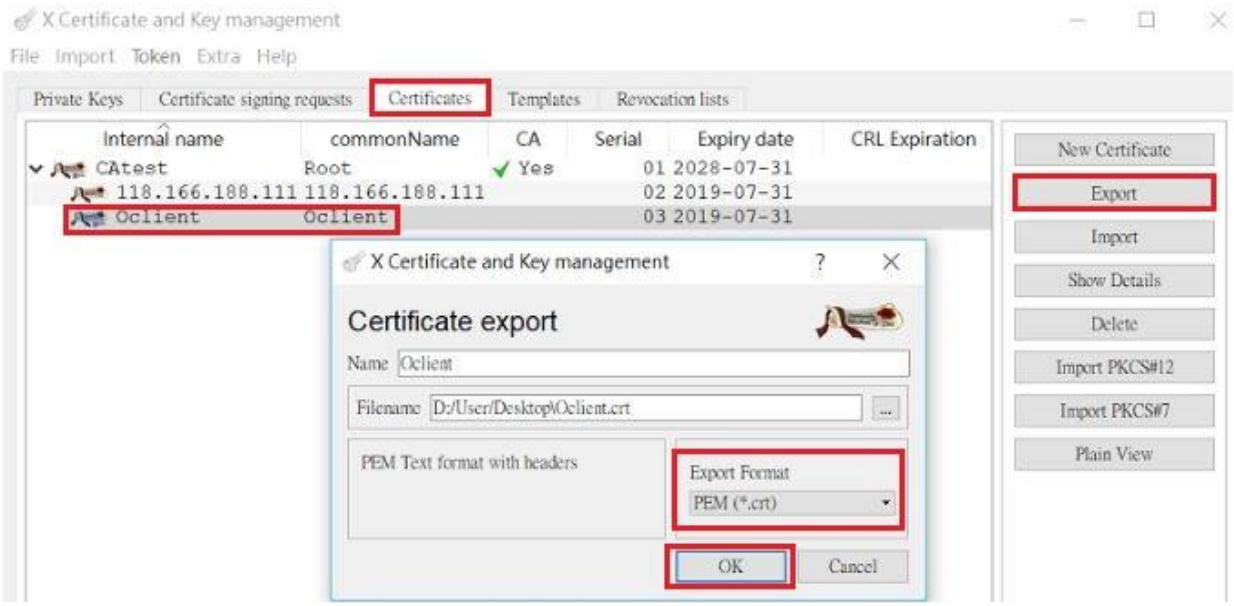


4.2 Go to the Subject tab.

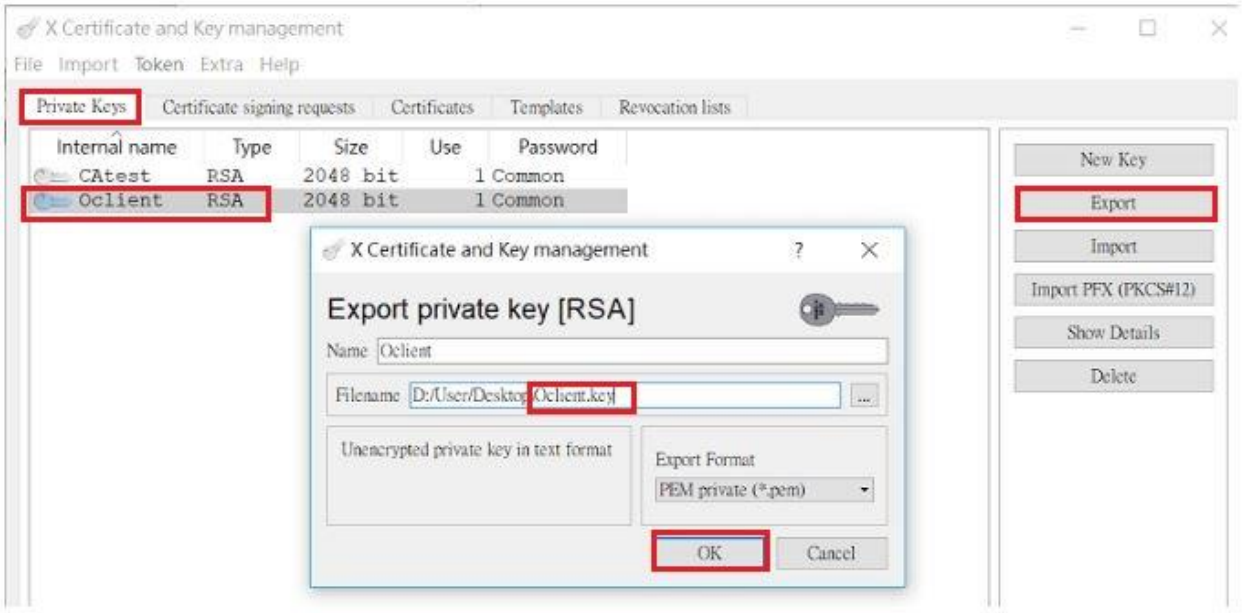
- Enter certificate information under ***Distinguished name***, then click ***Generate a new key***. Select ***"RSA"*** for Keytype and ***"2048 bit"*** for Keysize, then click ***Create***.
- Click ***OK*** to generate the certificate.



4.3 Go to ***Certificates***; select the certificate we just created. Export it as ***.crt*** format.

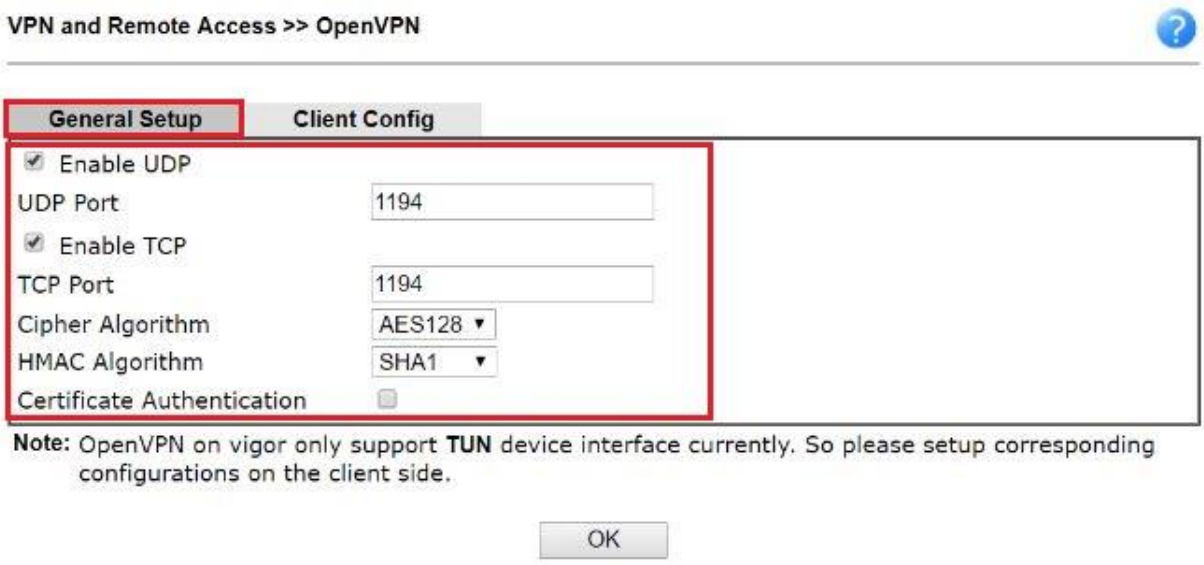



4.4 Go to ***Private Keys***, export the Private Key (***Oclient.key***), and manually change extension name to ***.key*** and then click ***Ok***.

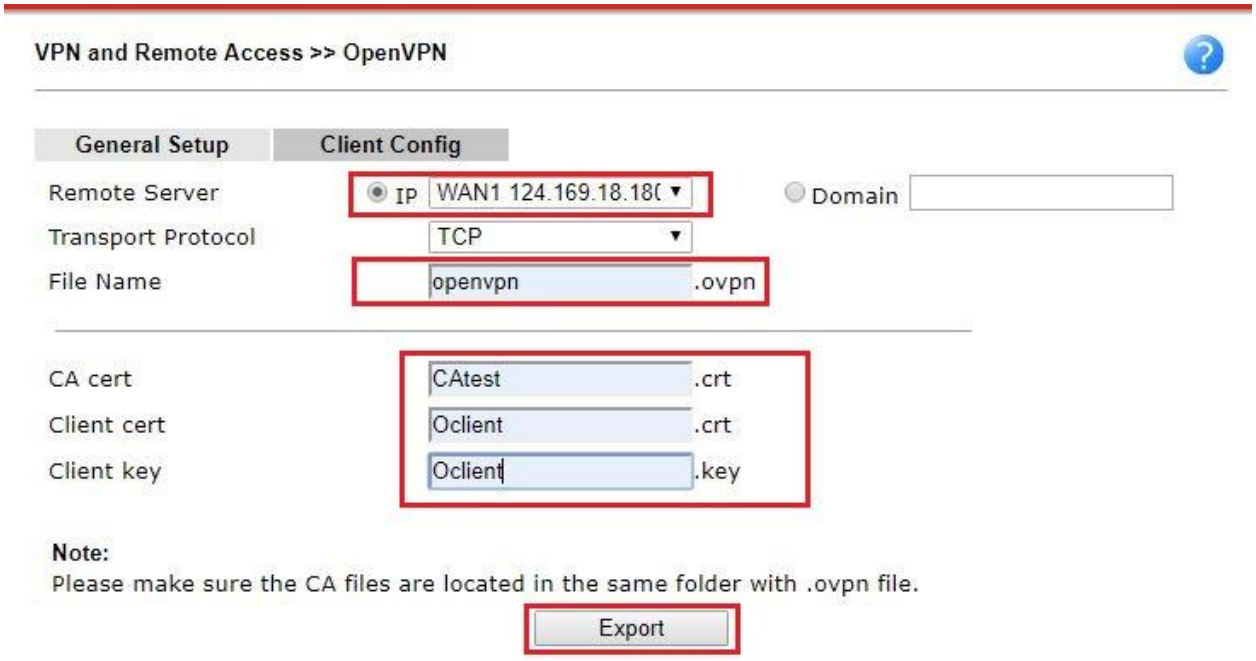


## *V. Setup the Vigor router as OpenVPN Server.*

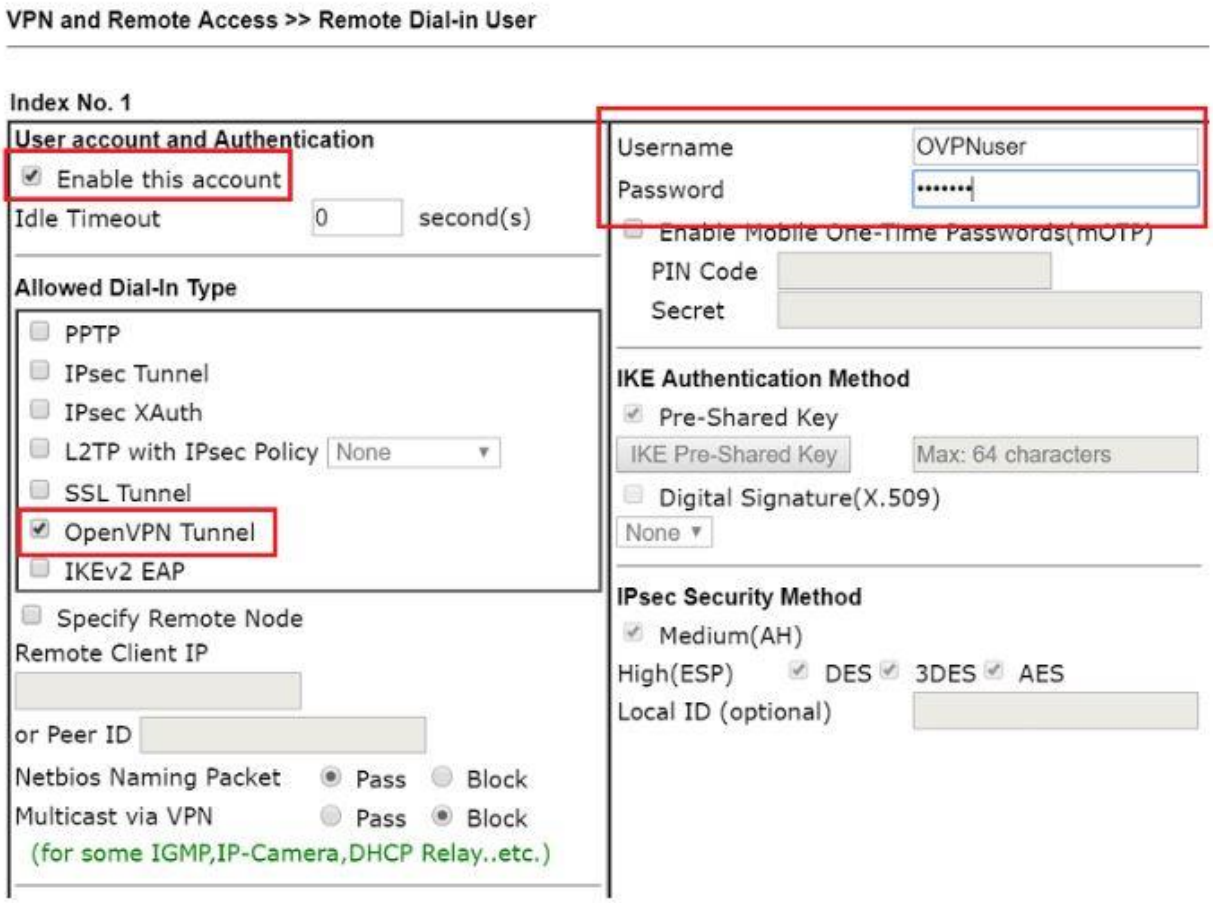
5.1 Go to **VPN and Remote Access >> OpenVPN, General Setup**, and follow the settings below.



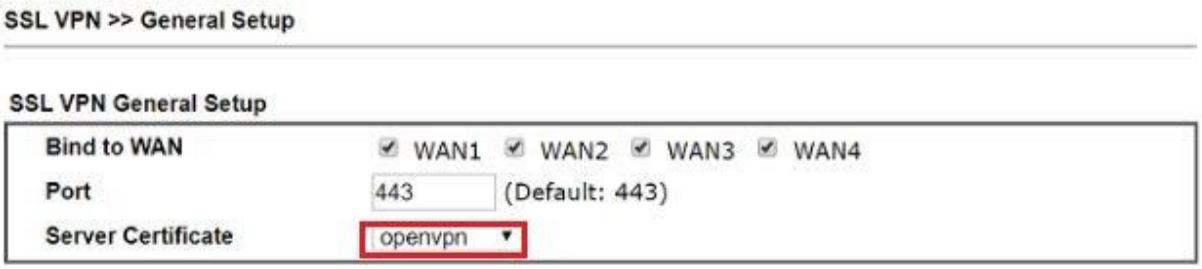

5.2 Go to the ***Client Config*** tab, specify the file name of **CA Certificate**, **Client Certificate**, and **Client Key** and then click **Export**. Please make sure that your WAN is up before exporting .ovpn file.



5.3 Go to **VPN and Remote Access >> Remote Dial-in User** and create user profiles for OpenVPN Dial-in users. Select **Enable this account**, enter **Username/Password**, and select **OpenVPN Tunnel** under ***Allowed Dial-In Type***.



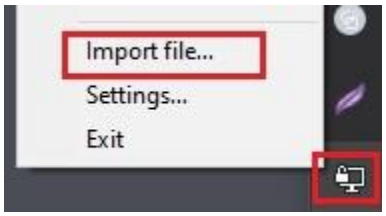

5.4 Go to **SSL VPN >> General Setup** to change the Server Certificate to the Local Certificate that we generated in procedure 2.

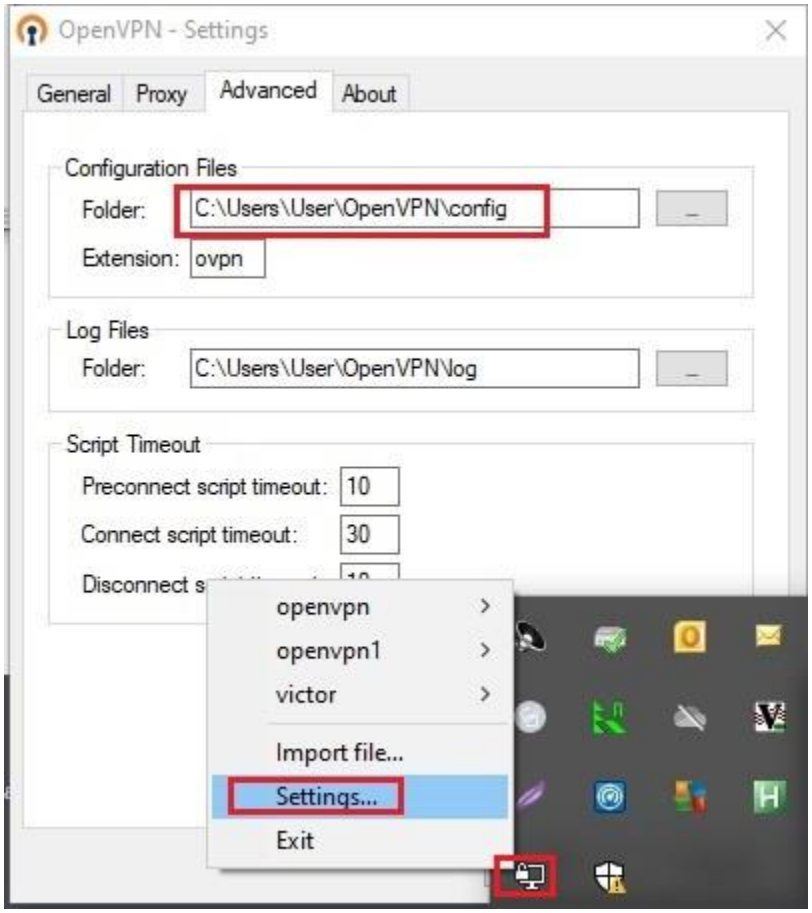


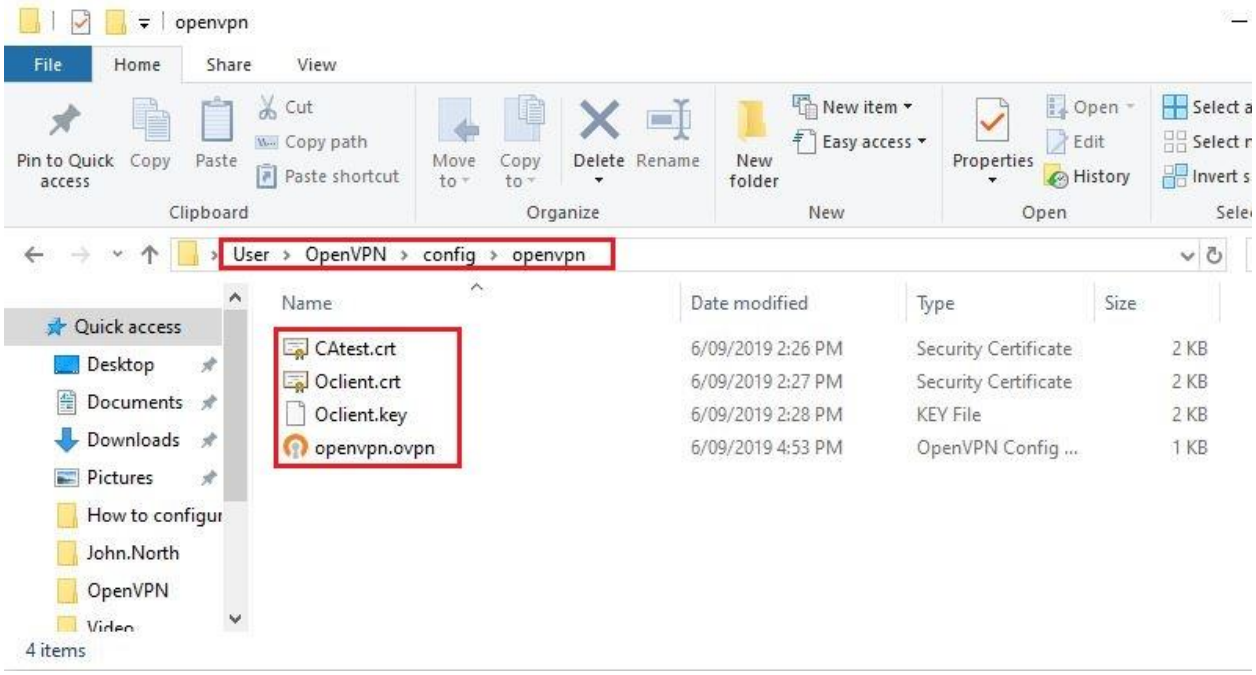
## *VI. OpenVPN Client setup.*

6.1 To import the openvpn.ovpn file to the OpenVPN client. Right click the OpenVPN icon, which is located on the bottom right of your taskbar. There are three files to put inside the OpenVPN config folder:

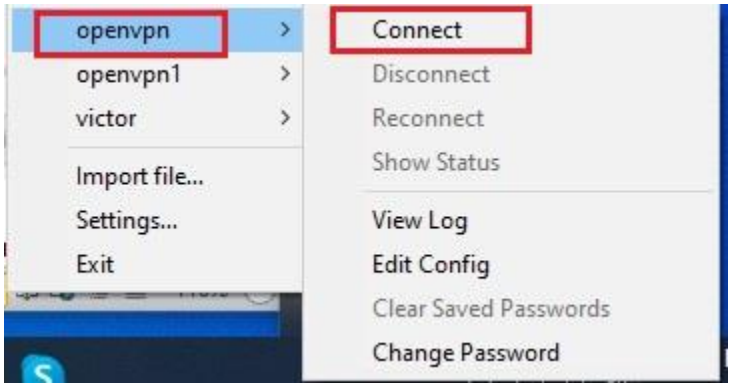
- Trusted CA Certificate (CAtest.crt)
- Private Certificate (Oclient.crt)
- Private Key (Oclient.key)

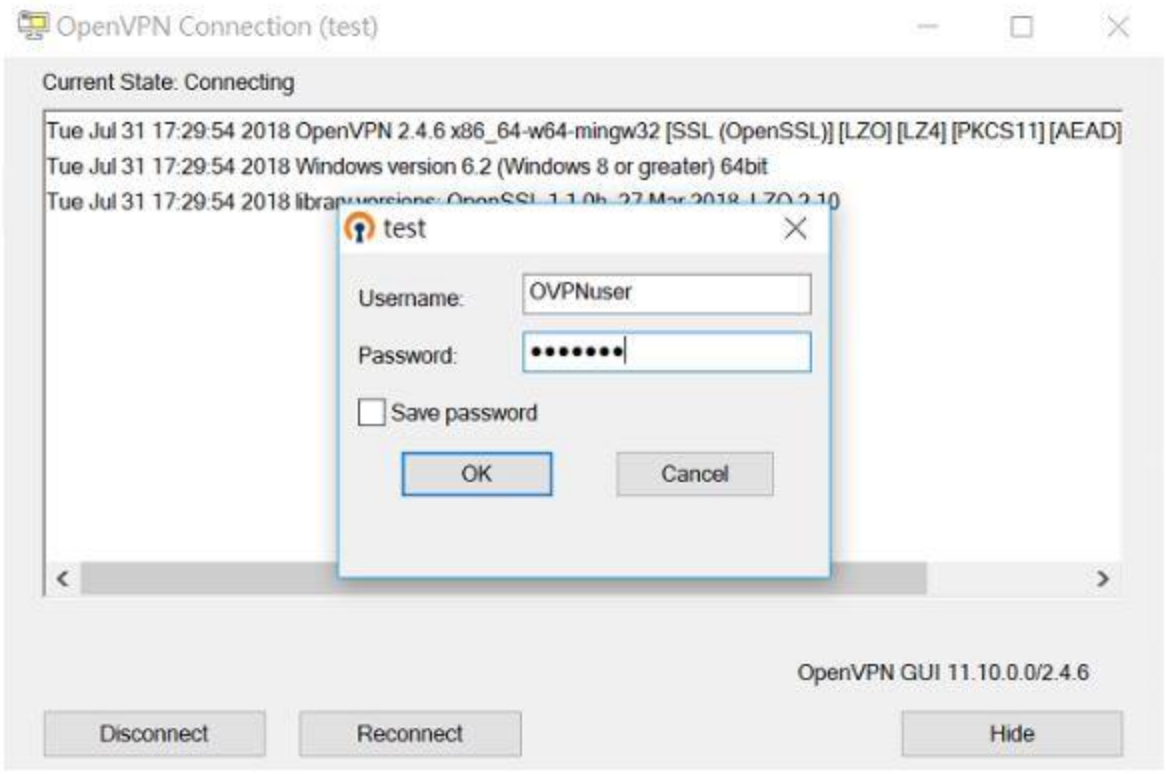





6.2 Click **Connect** and enter username/password configured in procedure 5.3.






6.3 After establishing the OpenVPN tunnel, go to **VPN and Remote Access >> Connection Management** in the Vigor router to verify the connection.