

# 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**.

---

### System Maintenance >> Time and Date

#### Time Information

Current System Time	2019 Sep 9 Mon 9 : 58 : 42	Inquire Time
---------------------	----------------------------	--------------

#### Time Setup

<input checked="" type="radio"/> Use Browser Time	
<input type="radio"/> Use Internet Time	
Time Server	pool.ntp.org
Priority	Auto
Time Zone	(GMT) Greenwich Mean Time : Dublin
Enable Daylight Saving	<input type="checkbox"/> Advanced
Automatically Update Interval	30 mins
Send NTP Request Through	Auto

OK

Cancel

- 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**.

Certificate Management >> Local Certificate

Generate Certificate Signing Request

Certificate Name	openvpn
Subject Alternative Name	
Type	E-Mail ▼
E-Mail	support@i-lan.com.au
Subject Name	
Country (C)	AU
State (ST)	NSW
Location (L)	Sydney
Organization (O)	i-lan
Organization Unit (OU)	support
Common Name (CN)	support@i-lan.com.au
Email (E)	george@i-lan.com.au
Key Type	RSA ▼
Key Size	2048 Bit ▼
Algorithm	SHA-256 ▼

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.

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
openvpn	/C=AU/ST=NSW/L=Sydney/O=i-la...	Requesting	Sign	View
---	---	---	View	Delete
---	---	---	View	Delete

Note:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before signing the local certificate.
2. The Time Zone **MUST** be setup correctly!!

Certificate Signing Request Information

Certificate Name : openvpn

Issuer :

Subject : C=AU, ST=NSW, L=Sydney, O=i-lan, OU=support, CN=support@i-lan.com.au, emailAddress=support@i-lan.com.au

Subject Alternative Name : email:george@i-lan.com.au

Valid From :

Valid To :

PEM Format Content :

```

Dy
FdM77Ngh/EdtFYrMn6EBtyZQ9w70XPhfcUsFZ2EBTttBoXOG3oJoSNZt713/6q
NC
wVrv3vymhALzh0rQs1U//
o5
GrmkNid/X1mdsr4kvZTSLy
eG
lGwm6XQjkDBxoLhf1br7WP
7e
GKrqbFQ/f409cuzYgazKjW
-----END CERTIFICATE REQUEST-----

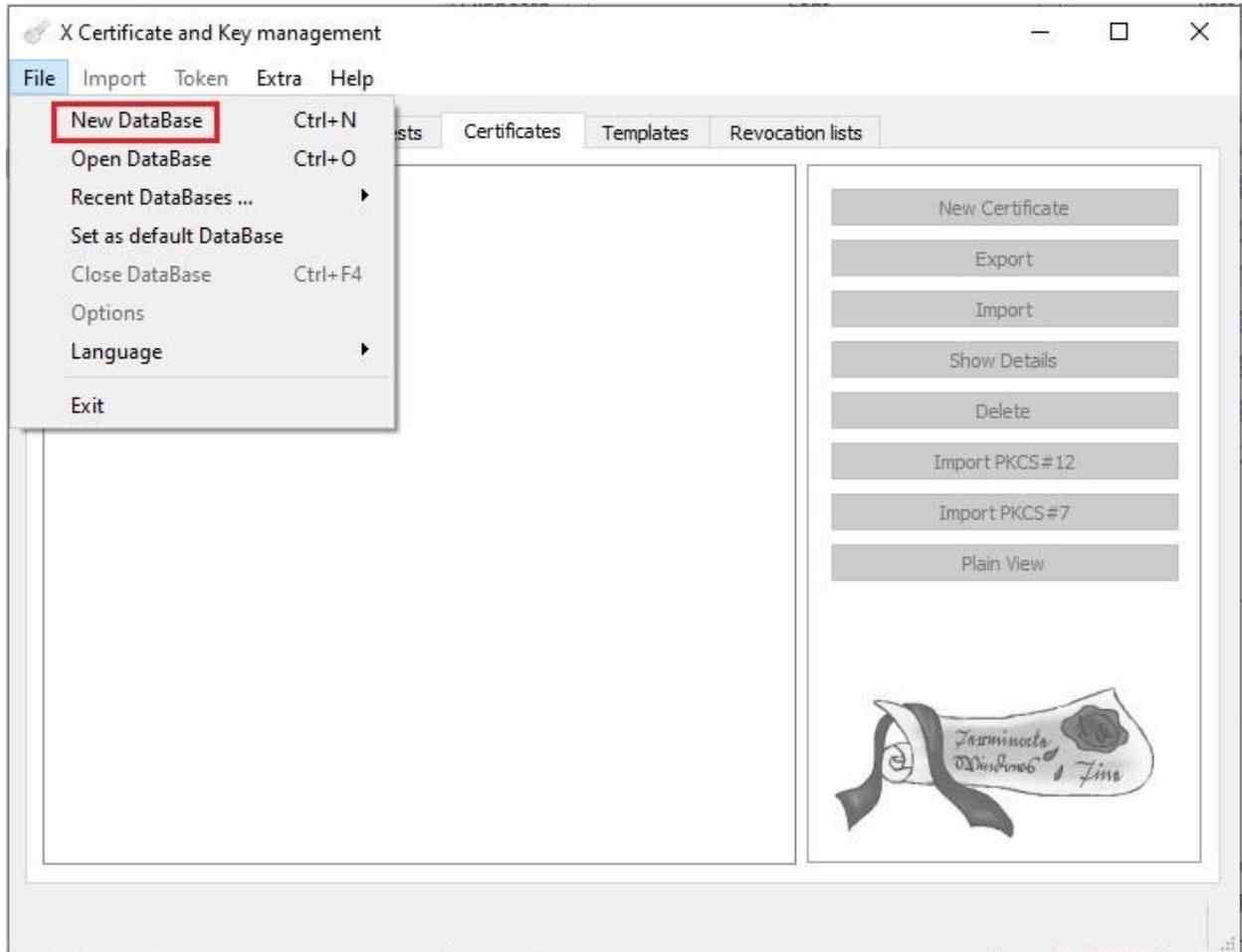
```

Close

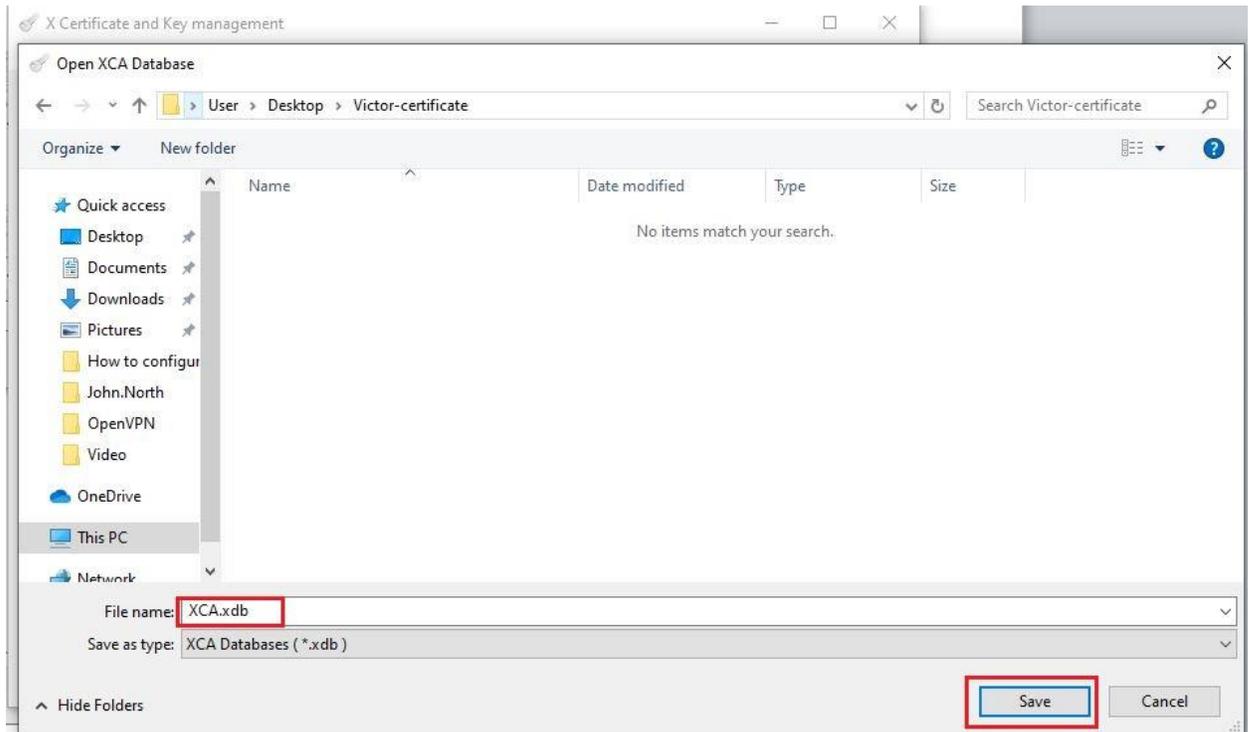
Copy

## II. Create a new CA using XCA.

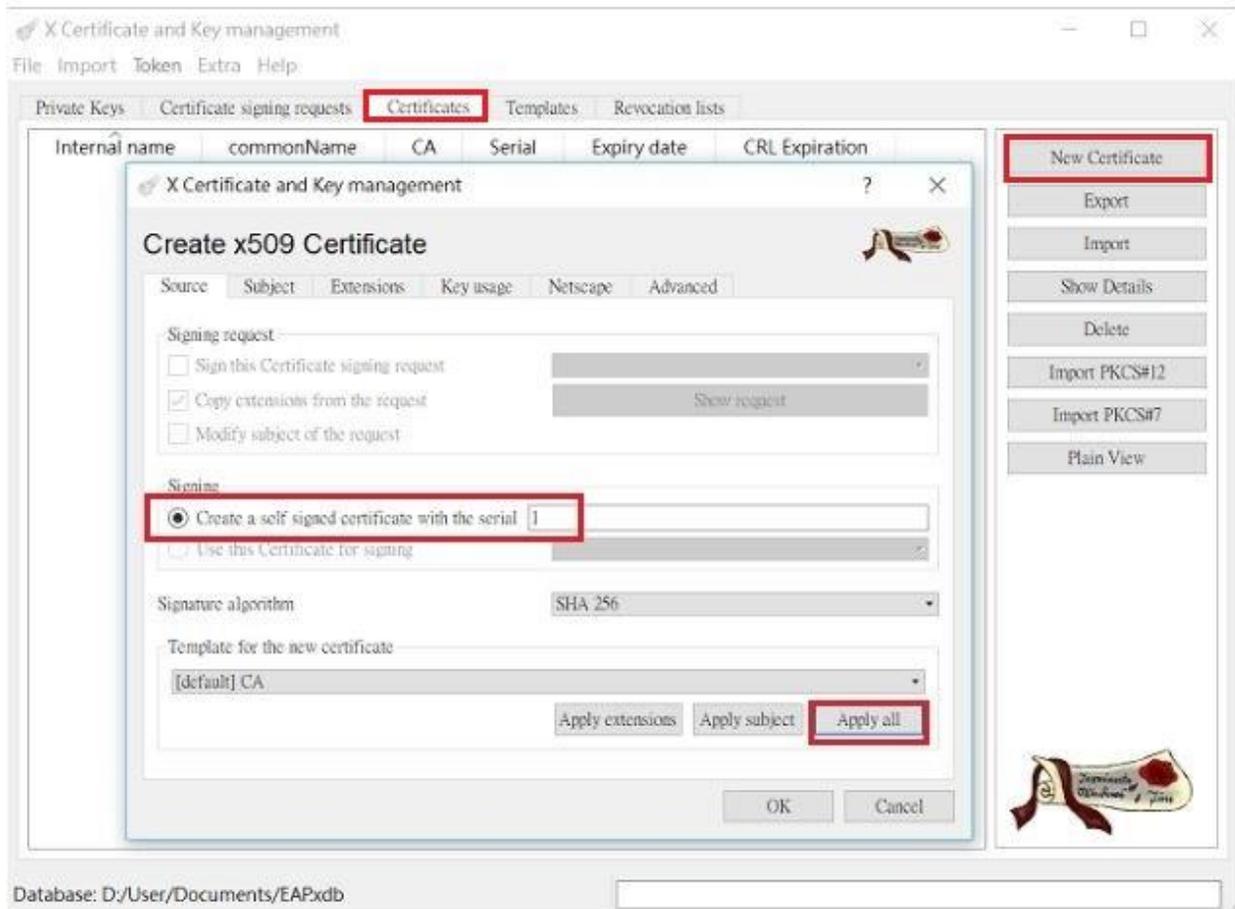
2.1 Launch XCA, go to File and click New Database.



## 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**.

The screenshot shows a window titled "X Certificate and Key management" with a close button (X) and a help button (?). The main title is "Create x509 Certificate". There are five tabs: "Source", "Subject", "Extensions" (which is selected and highlighted with a red box), "Key usage", "Netscape", and "Advanced".

Under the "Extensions" tab, there are two main sections:

- X509v3 Basic Constraints:** A dropdown menu for "Type" is set to "Certification Authority" (highlighted with a red box). Below it is a "Path length" input field and a "Critical" checkbox.
- Key identifier:** Two checkboxes: "Subject Key Identifier" and "Authority Key Identifier".

Below these sections are two more sections:

- Validity:** "Not before" is set to "2019-09-09 00:26 GMT" and "Not after" is set to "2020-09-06 04:07 GMT".
- Time range:** A dropdown is set to "Years", with a value of "1" in the input field. There are checkboxes for "Midnight", "Local time", and "No well-defined expiration", and an "Apply" button.

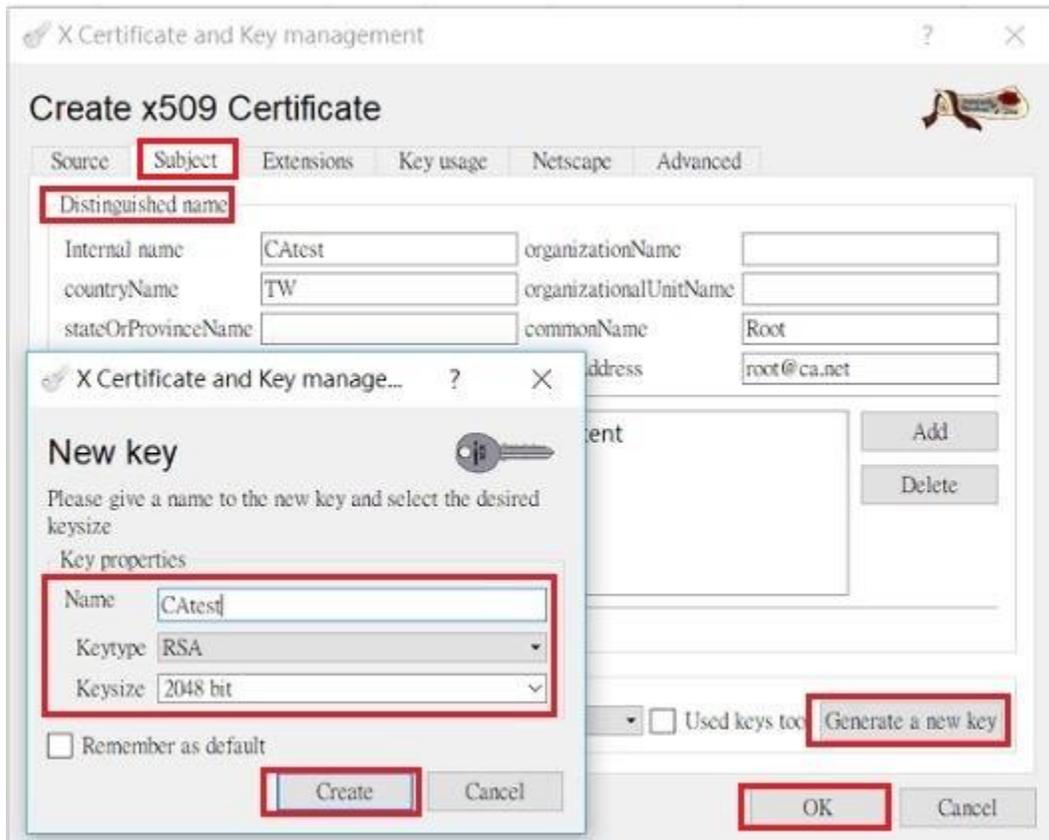
At the bottom, there are four rows of fields for X509v3 extensions:

- X509v3 Subject Alternative Name: [Empty field] [Edit]
- X509v3 Issuer Alternative Name: [Empty field] [Edit]
- X509v3 CRL Distribution Points: [Empty field] [Edit]
- Authority Information Access: [OCSP dropdown] [Empty field] [Edit]

At the bottom right, there are "OK" and "Cancel" buttons.

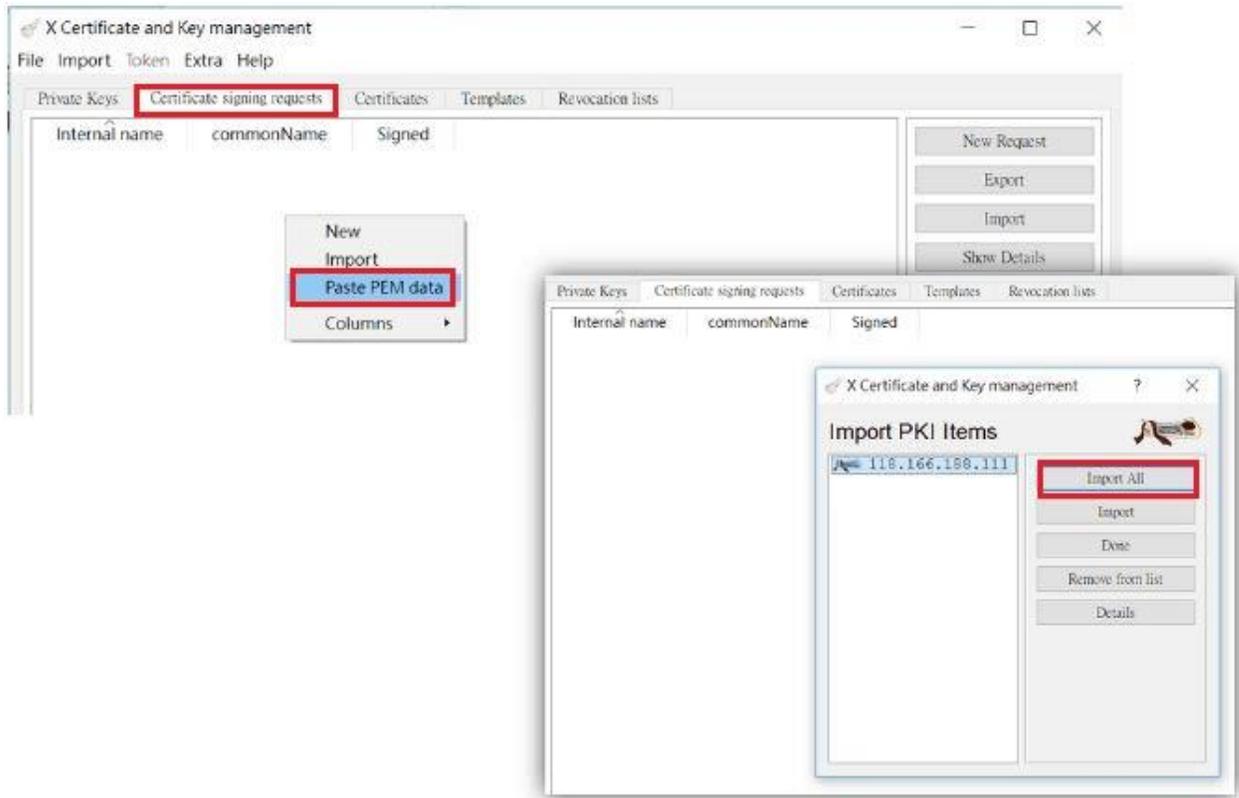
2.5 Go to the Subject tab.

- 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.

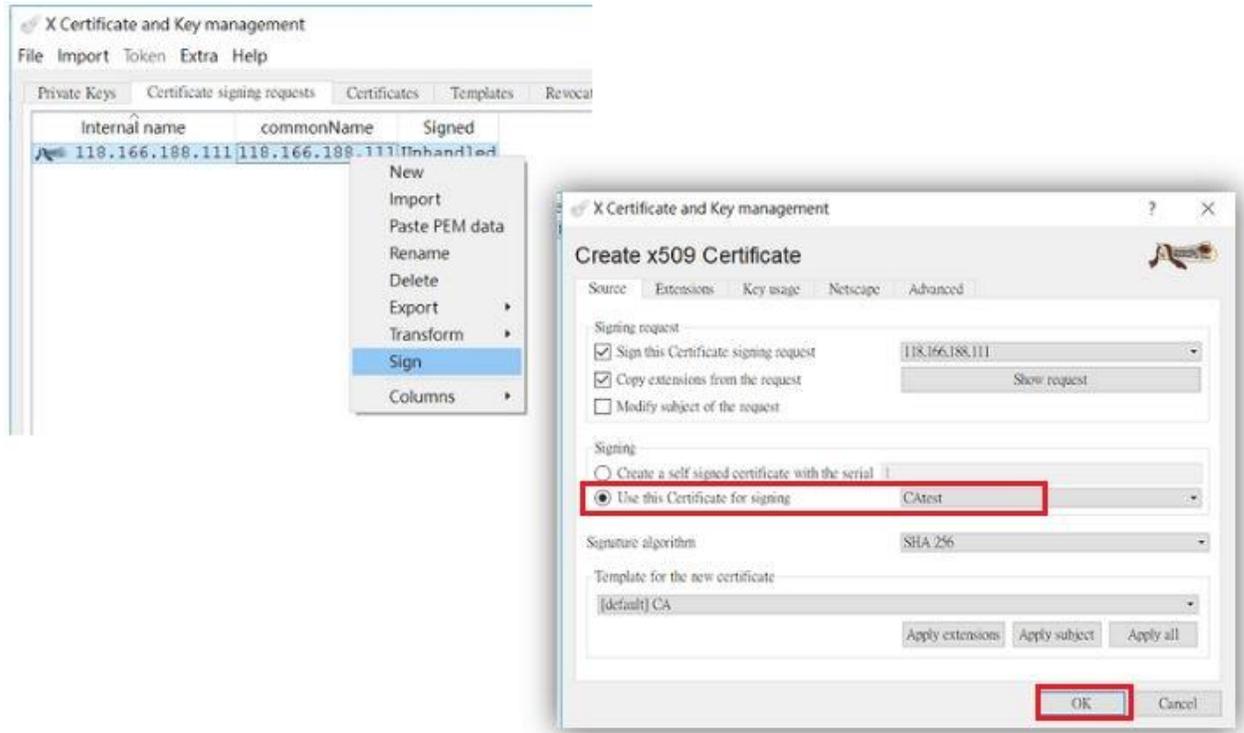


### III. **Importing Signed Server Certificate and CA Certificate to the Router.**

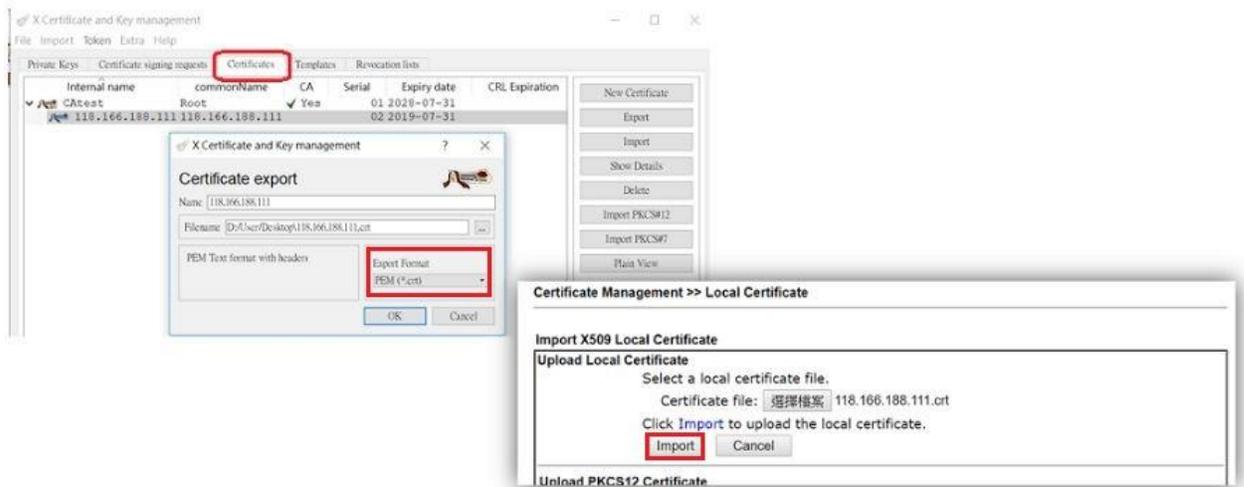
3.1 Go to **Certificate signing requests**, right-click and select **Paste PEM data** and paste the PEM Format Content copied from the Vigor router in procedure 1.3. and then click **Import All**.



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 Signed 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**.

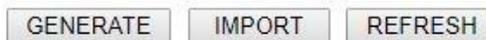
#### Certificate Management >> Local Certificate

##### X509 Local Certificate Configuration

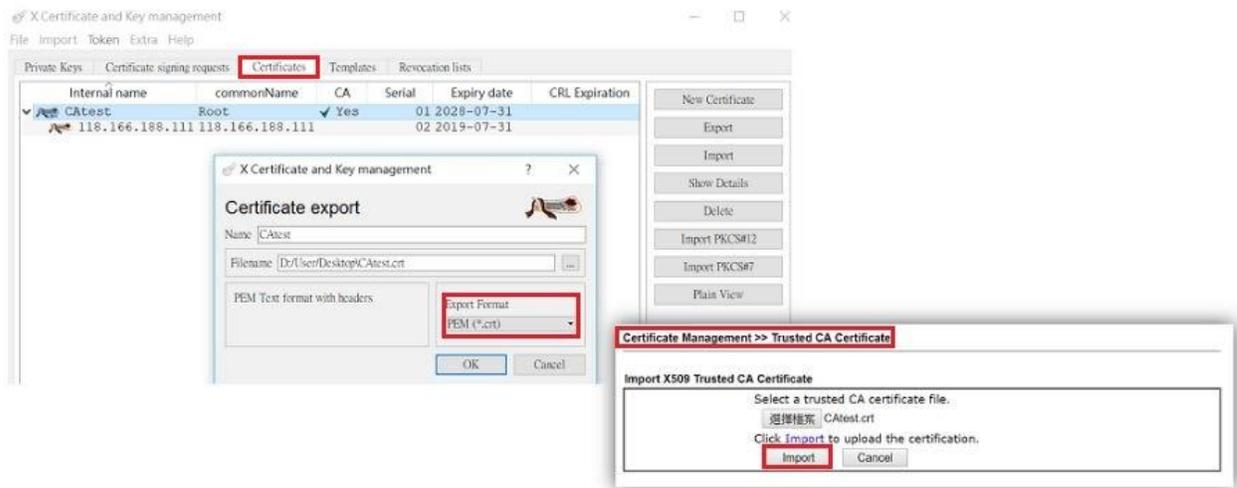
Name	Subject	Status	Modify	
openvpn	/C=AU/ST=NSW/L=Sydney/O=ilan...	OK	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete

##### Note:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before signing the local certificate.
2. The Time Zone MUST be setup correctly!!



### 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**.

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	---	---	Create
Trusted CA-1	/C=AU/ST=NSW/L=SevenHills/O=...	OK	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

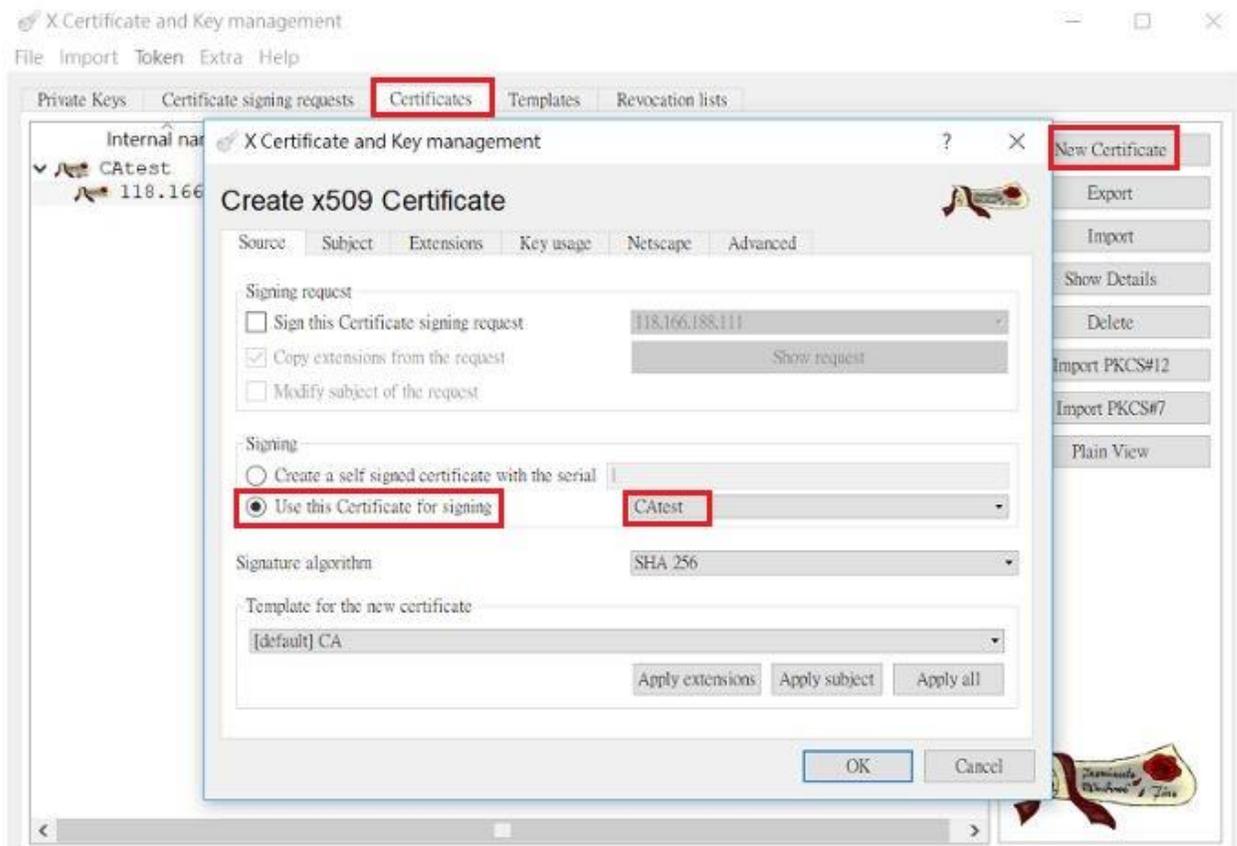
Note:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before you try to generate a RootCA!!
2. The Time Zone MUST be setup correctly!!

IMPORT REFRESH

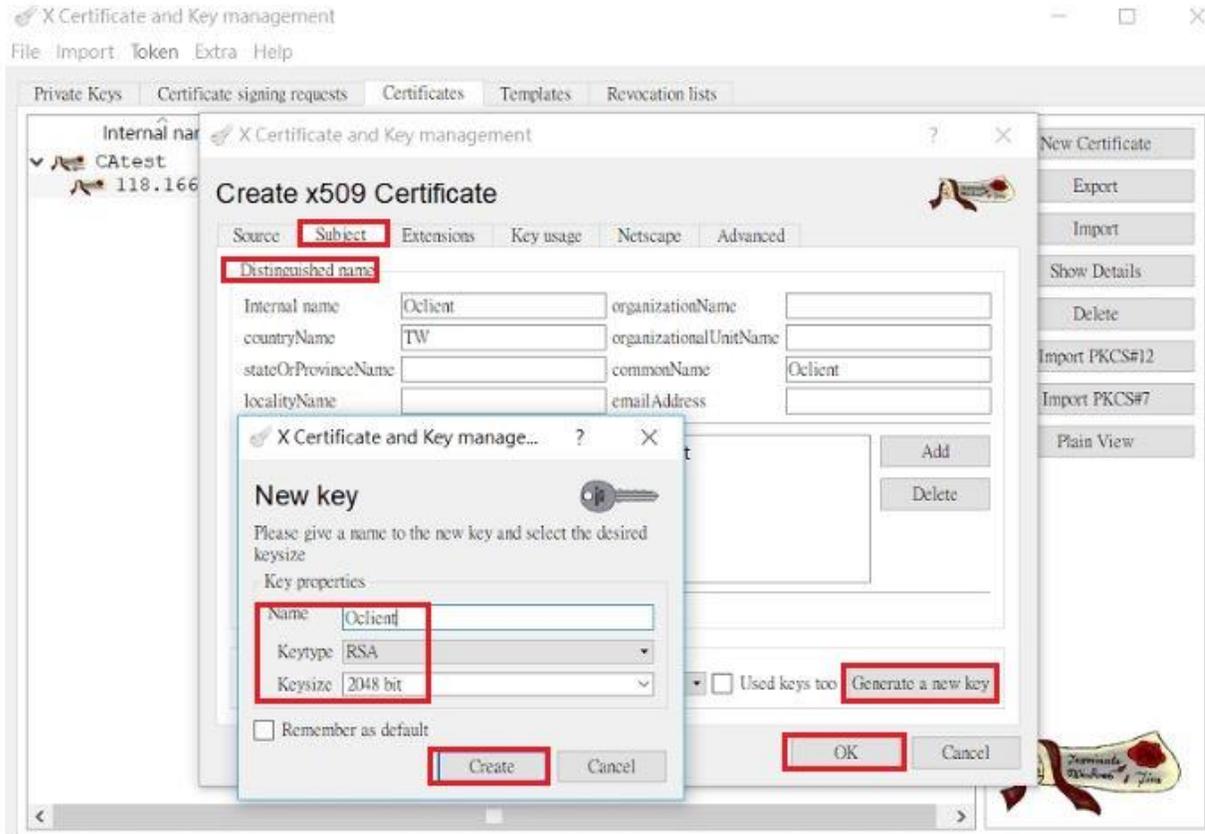
**IV. Making a Private Certificate and Private Key for VPN Client.**

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

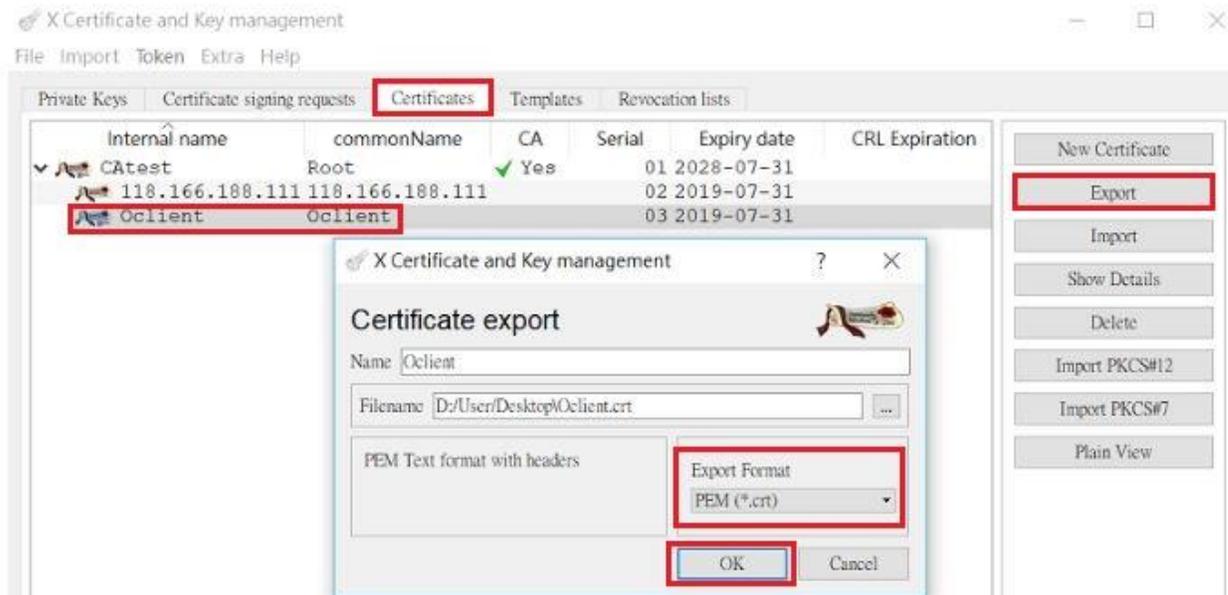


#### 4.2 Go to the Subject tab.

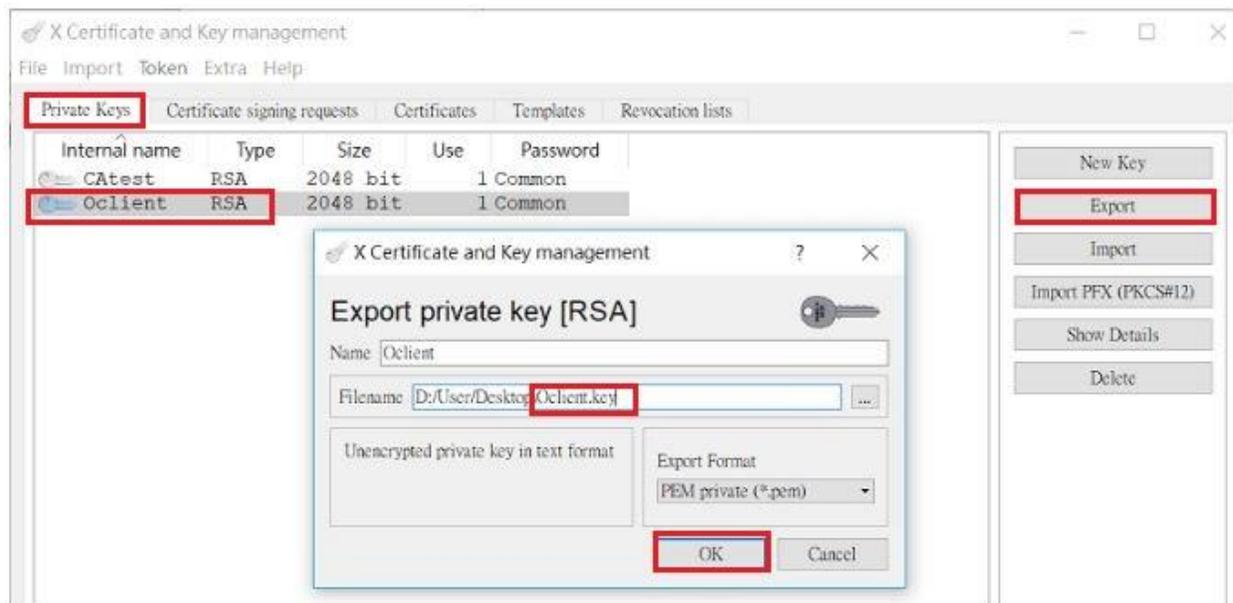
- Enter certificate information under **Distinguished name**, then click **Generate a new key**. Select **"RSA"** for Keytype and **"2048 bit"** for Keysize, then click **Create**.
- Click **OK** to generate the certificate.



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.

VPN and Remote Access >> OpenVPN ?

---

**General Setup**   Client Config

Enable UDP  
UDP Port:

Enable TCP  
TCP Port:

Cipher Algorithm:

HMAC Algorithm:

Certificate Authentication:

**Note:** OpenVPN on vigor only support TUN device interface currently. So please setup corresponding configurations on the client side.

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.

---

VPN and Remote Access >> OpenVPN ?

---

**General Setup**   **Client Config**

Remote Server:  IP   Domain

Transport Protocol:

File Name:  .ovpn

---

CA cert:  .cert

Client cert:  .cert

Client key:  .key

**Note:**  
Please make sure the CA files are located in the same folder with .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**.

**VPN and Remote Access >> Remote Dial-in User**

Index No. 1

**User account and Authentication**

Enable this account

Idle Timeout  second(s)

**Allowed Dial-In Type**

PPTP

IPsec Tunnel

IPsec XAuth

L2TP with IPsec Policy

SSL Tunnel

OpenVPN Tunnel

IKEv2 EAP

Specify Remote Node

Remote Client IP

or Peer ID

Netbios Naming Packet  Pass  Block

Multicast via VPN  Pass  Block  
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Username

Password

Enable Mobile One-Time Passwords(mOTP)

PIN Code

Secret

**IKE Authentication Method**

Pre-Shared Key

IKE Pre-Shared Key

Digital Signature(X.509)

**IPsec Security Method**

Medium(AH)

High(ESP)  DES  3DES  AES

Local ID (optional)

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

**SSL VPN >> General Setup**

**SSL VPN General Setup**

Bind to WAN  WAN1  WAN2  WAN3  WAN4

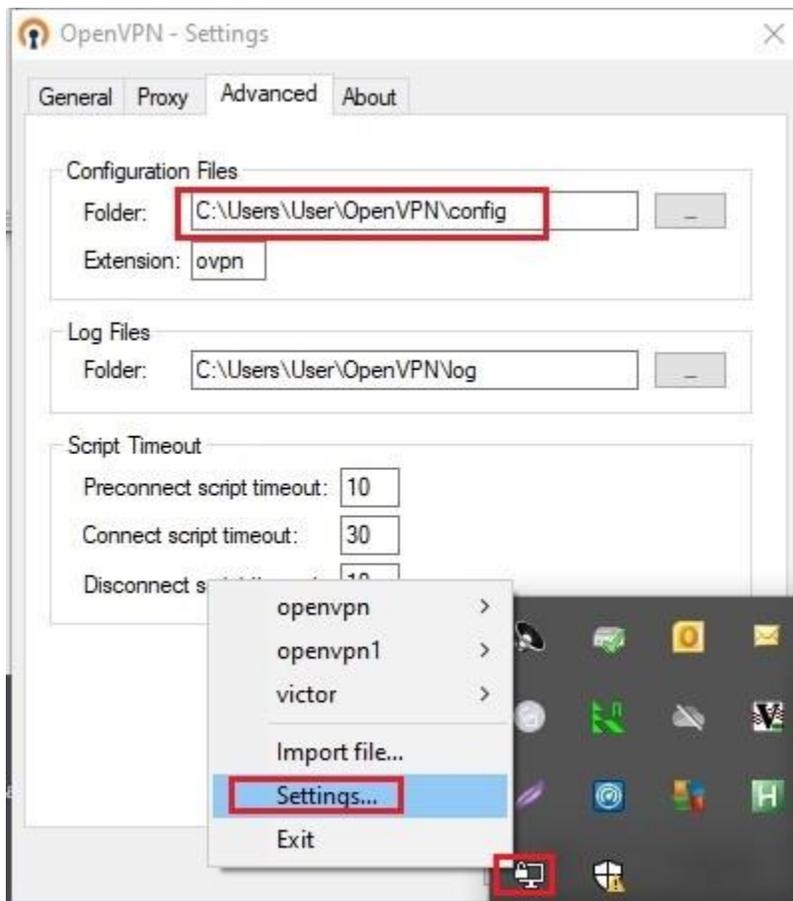
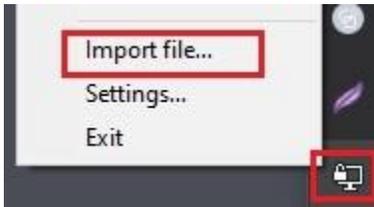
Port  (Default: 443)

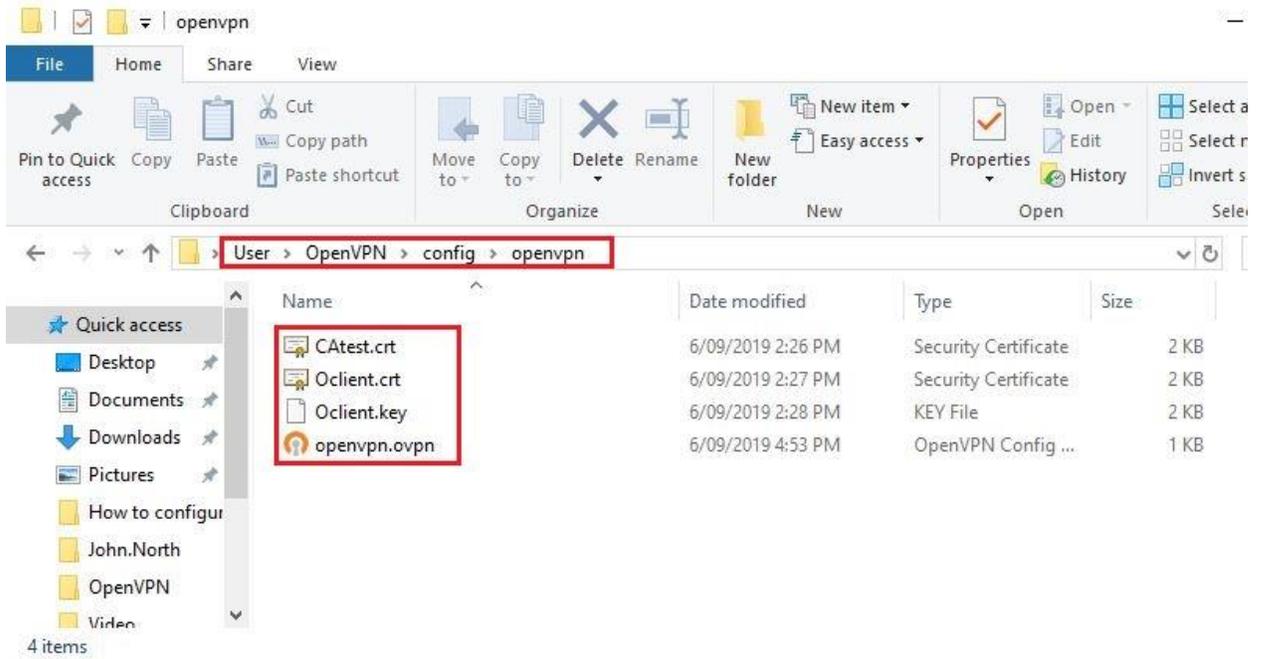
Server Certificate

## VI. OpenVPN Client setup.

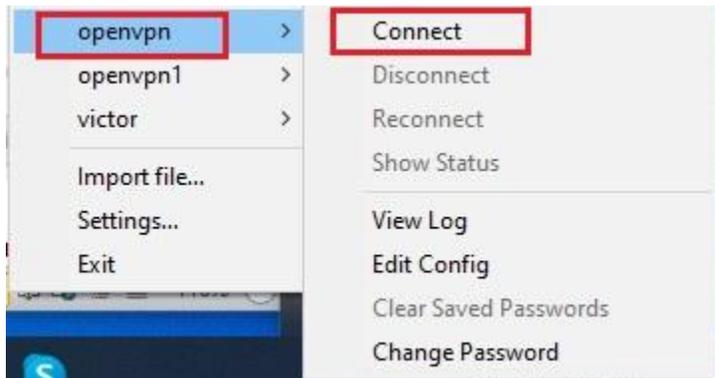
6.1 To import the openvpn.ovpn file to the OpenVPN client. Right click the OpenVPN icon, which is located on the bottom right of your taskbar. There are three files to put inside the OpenVPN config folder:

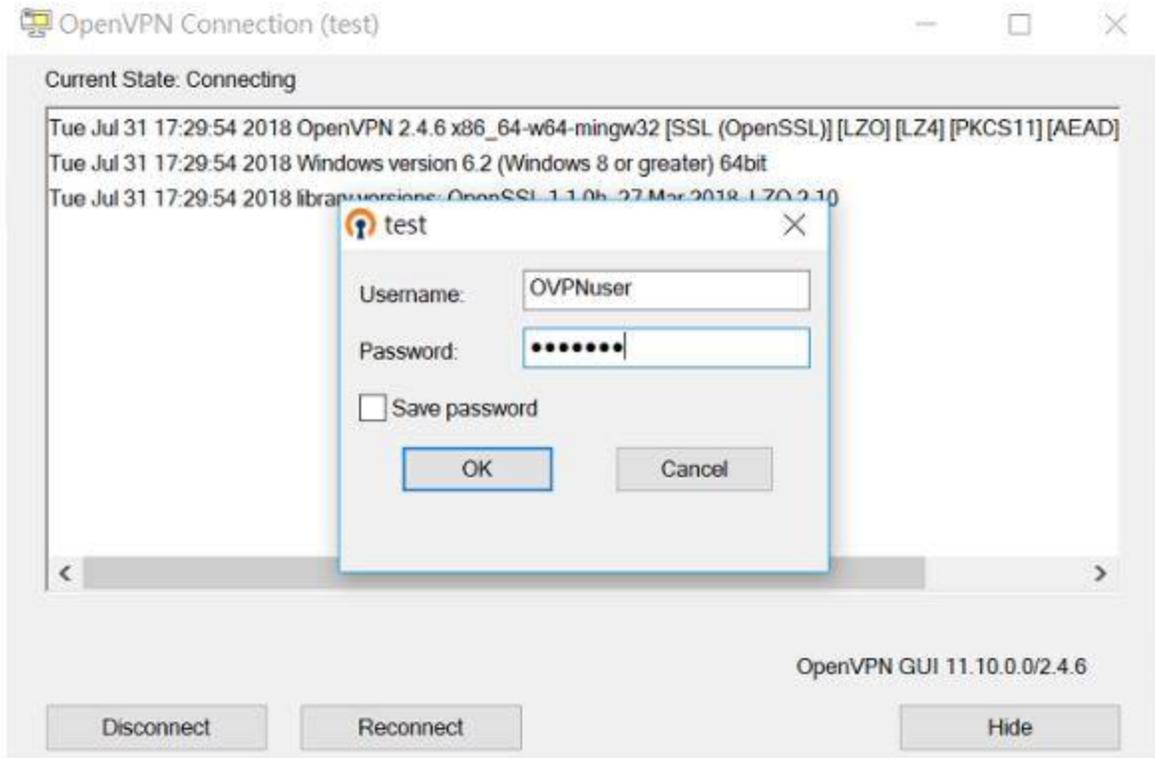
- Trusted CA Certificate (CAtest.crt)
- Private Certificate (Oclient.crt)
- Private Key (Oclient.key)





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.

#### VPN and Remote Access >> Connection Management

**Dial-out Tool** | [Refresh](#) |

General Mode:	<input type="text"/>	<input type="button" value="Dial"/>
Backup Mode:	<input type="text"/>	<input type="button" value="Dial"/>
Load Balance Mode:	<input type="text"/>	<input type="button" value="Dial"/>

#### VPN Connection Status

All VPN Status		LAN-to-LAN VPN Status		Remote Dial-in User Status				
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Kbps)	Rx Pkts	Rx Rate(Kbps)	UpTime
1 ( OVPNuser ) Local User Database	OpenVPN AES-SHA1 Auth	118.166.186.70 via WAN1	192.168.89.11/32	1048	438.40	947	56.10	0:3:56 <input type="button" value="Drop"/>

xxxxxxx : Data is encrypted.  
xxxxxxx : Data isn't encrypted.