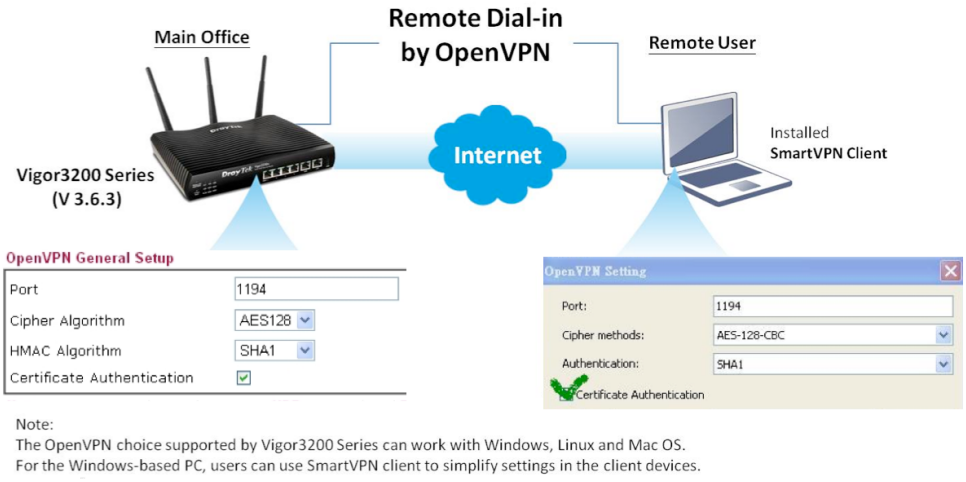
How to Establish OpenVPN Tunnels (Authenticate with CA) via SmartVPN Client?

OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchanges. It is capable of traversing network address translators (NATs) and firewalls.

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority.



Following is the step-by-step setting.

**Before setting, please make sure SmartVPN Client 4.1.0.1 is installed on the PC, and the firmware of the router is the latest version. Also please install XCA on the PC to utilize the CA Server feature.

**We define the network diagram as below :

PC------Internet------Vigor 3200------LAN

Settings of PC :

- IP address = 188.188.188.188

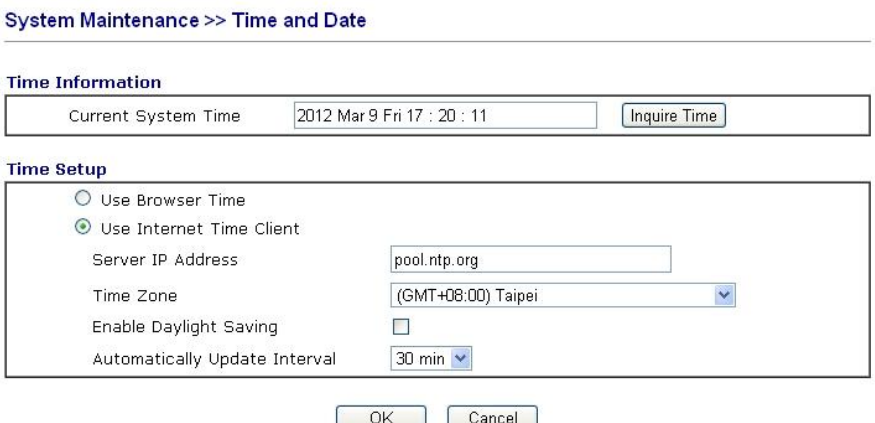
Settings of Vigor 3200 :

- WAN IP address = 200.200.200.200
- LAN: IP address = 192.168.1.1/24

XCA is a freeware for the CA Server. This article describes making the CA (Certificate Authentication) for Vigor users**.**

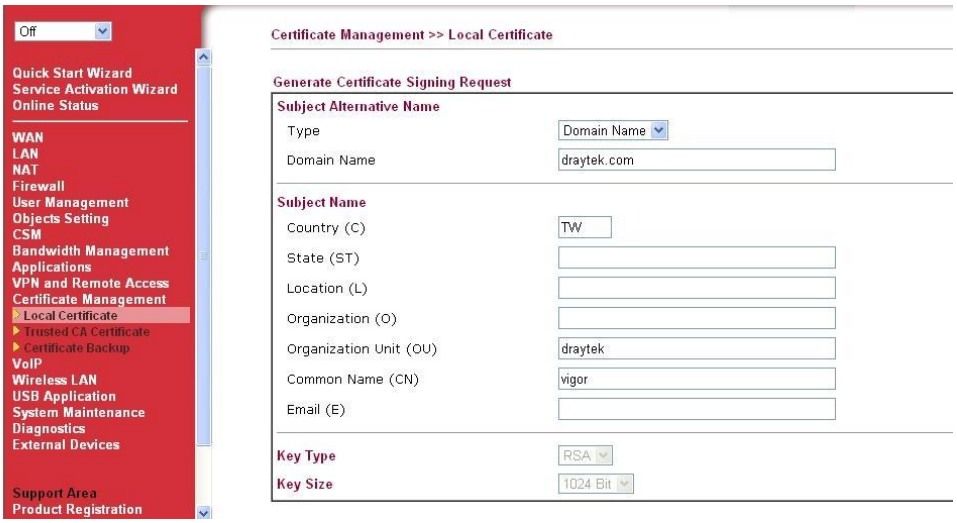
Part A : Time Setup

Please make sure the router is using **Internet Time Client**.



Part B : Making a Local Certificate and Trusted CA Certificate

Please go to **Certificate Management >> Local Certificate** to generate a Certificate Signing Request, and type related information in the **Subject Alternative Name** and **Subject Name** sections.

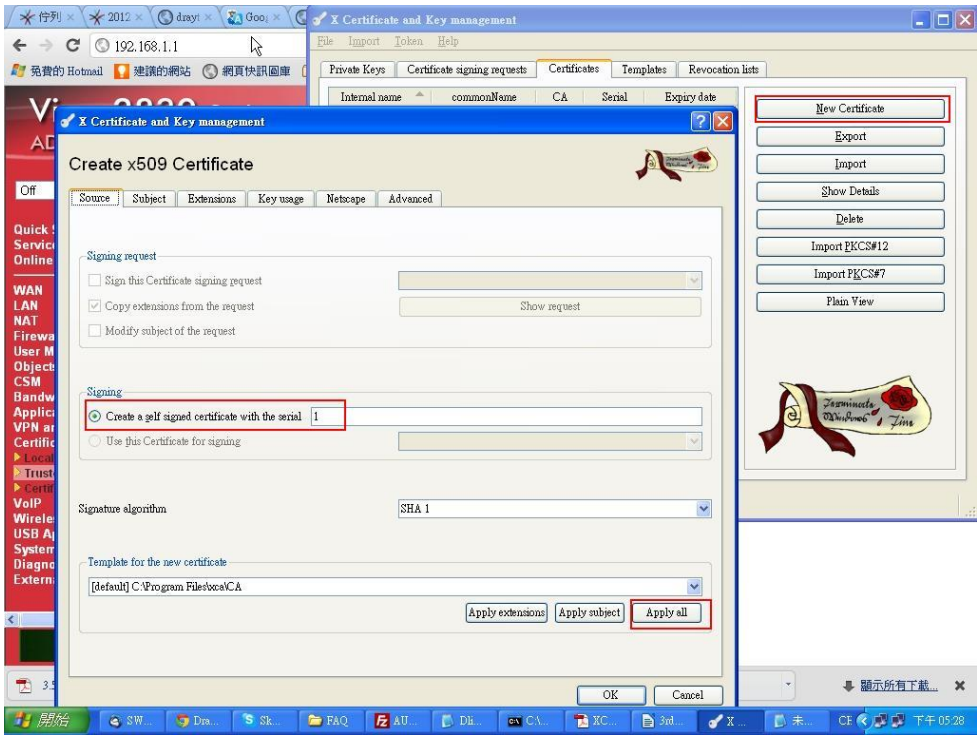


After clicking **Generate**, you will see the following screenshot.

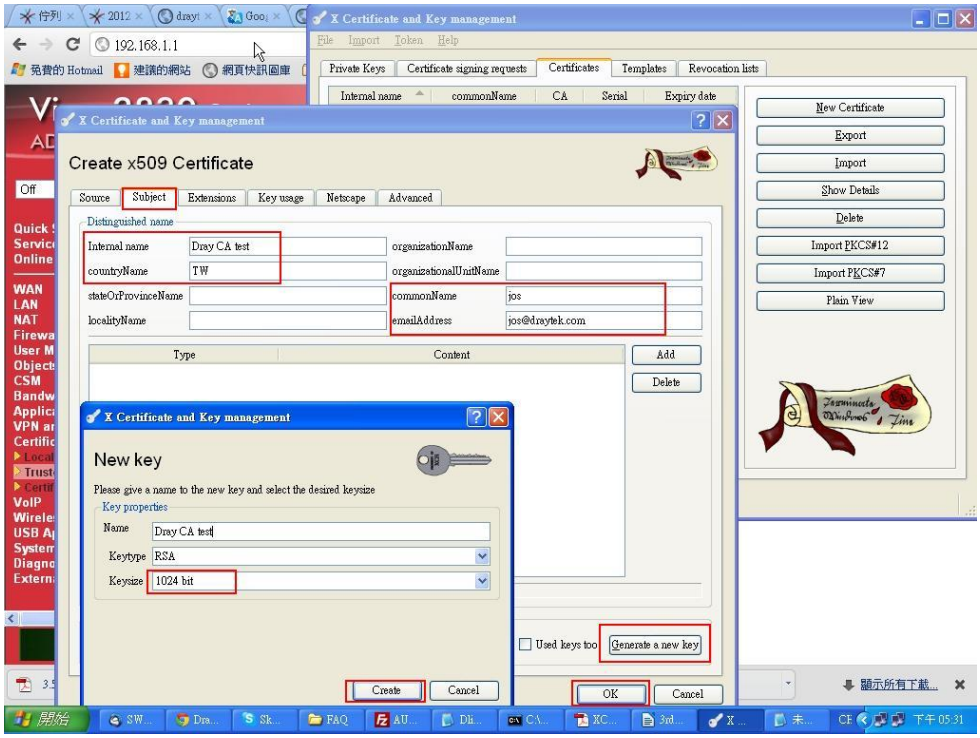
Launch XCA as CA Server

1. Click **New Certificate**.
2. Choose **Create a self signed Certificate with the serial** in the signing section.
3. Click **Apply All** to apply the CA Template.

3. Click **Apply All** to apply the CA Template.



4. In Subject page, type a distinguishable or preferred name.
5. Click **Generate a new key** to create a **RSA 1024 bit** for this Certificate.
6. Click **OK**, and we have generated a Trusted CA Certificate well.



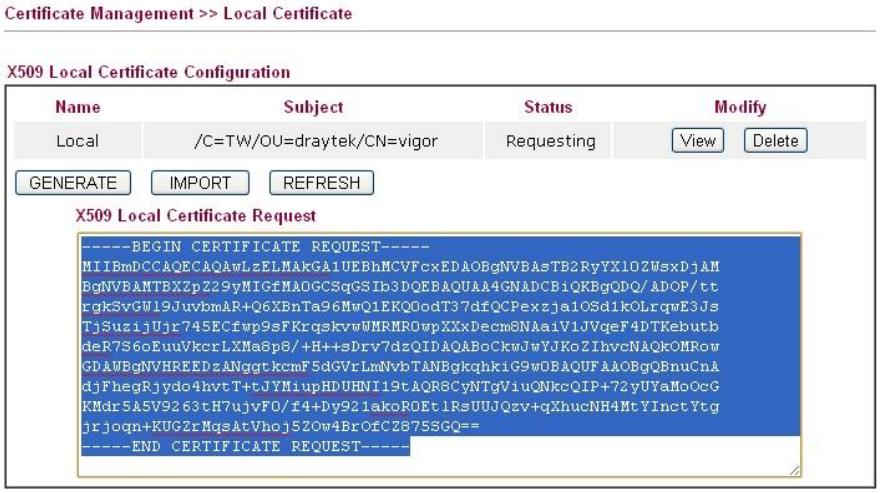
From **Certificate Management >> Local Certificate**, we copy the **X509 Local Certificate Request** and paste to the XCA.

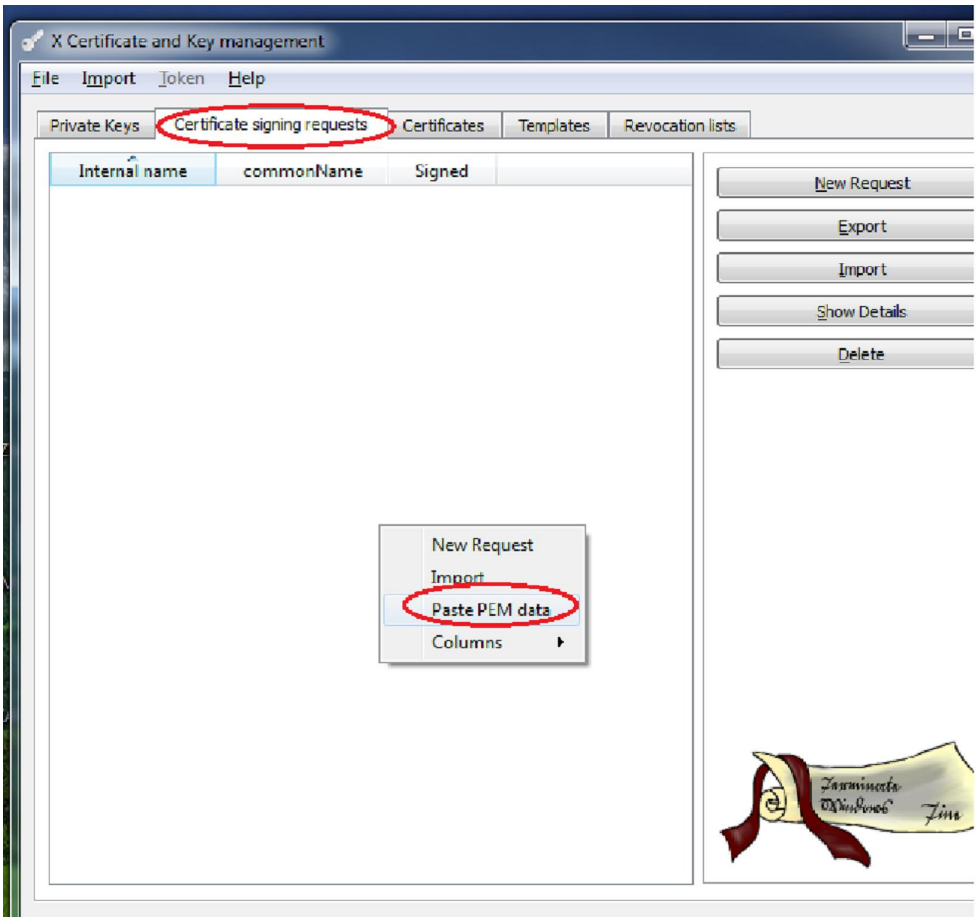
Certificate Management >> Local Certificate

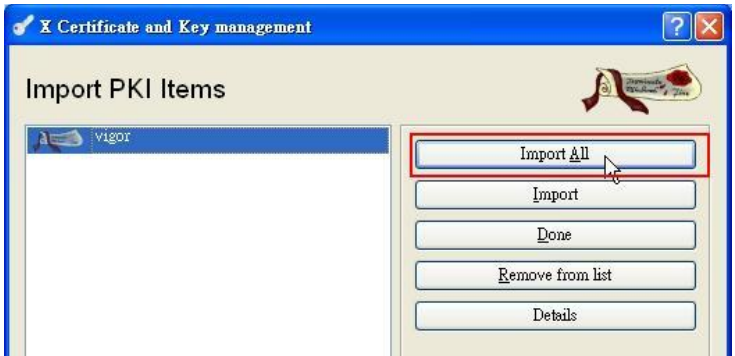
X509 Local Certificate Configuration

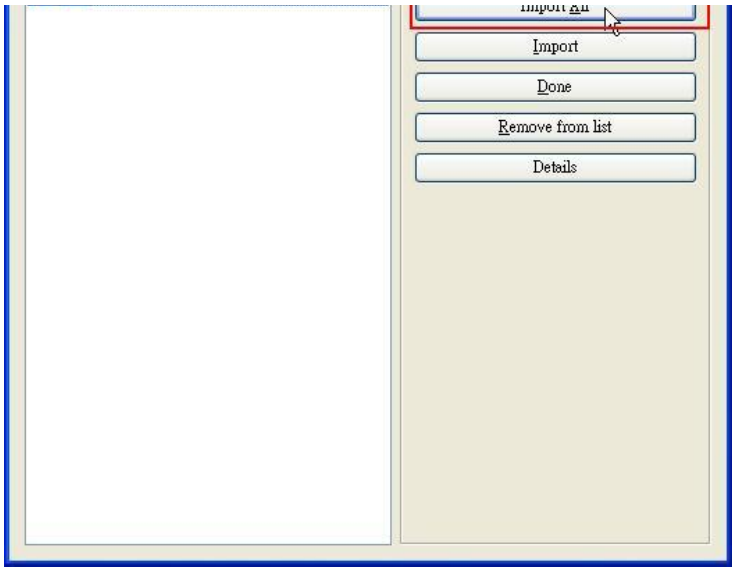
Name	Subject	Status	Modify

From **Certificate Management >> Local Certificate**, we copy the **X509 Local Certificate Request** and paste to the XCA.

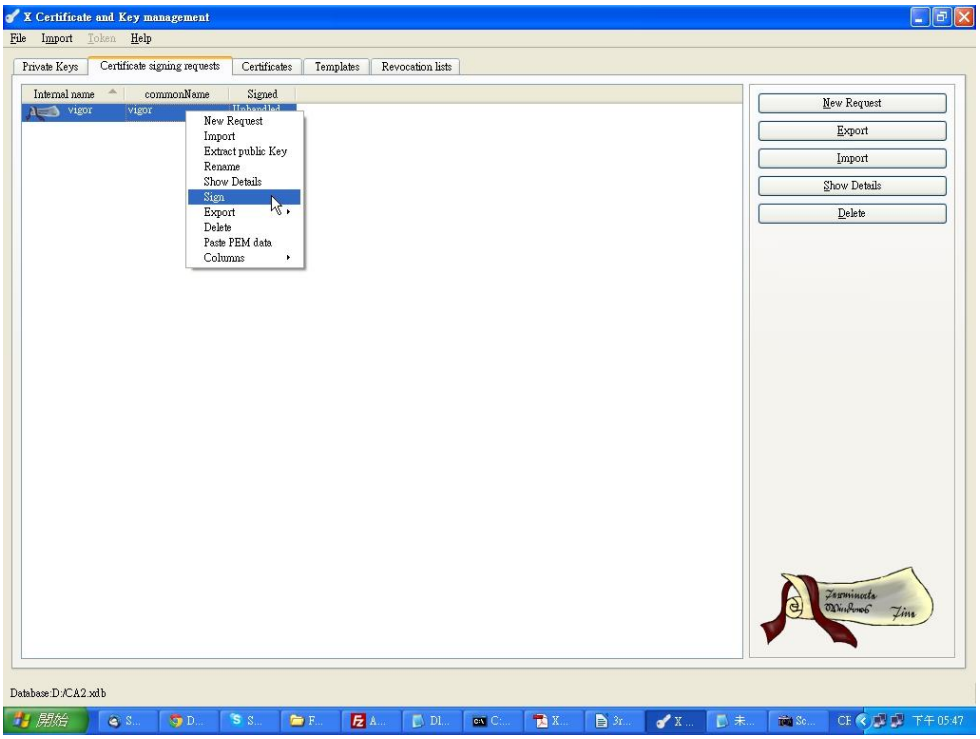


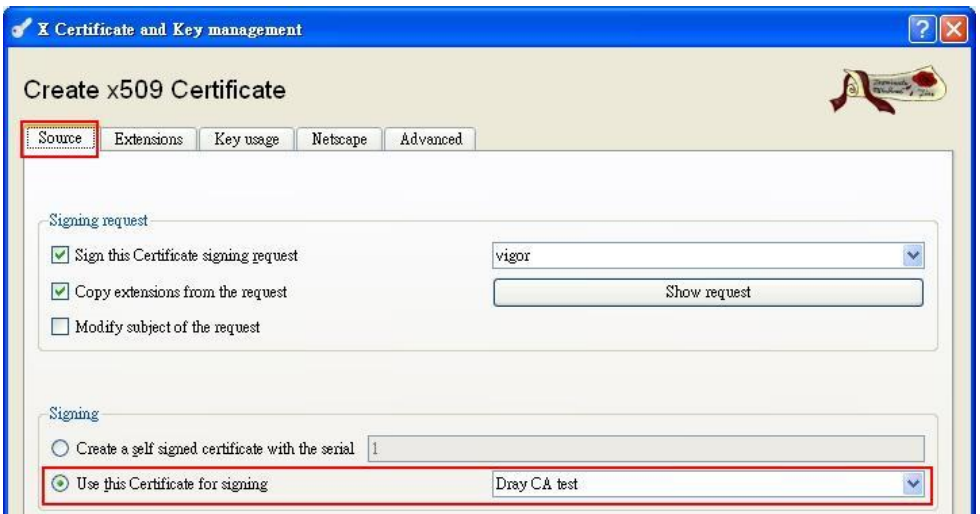




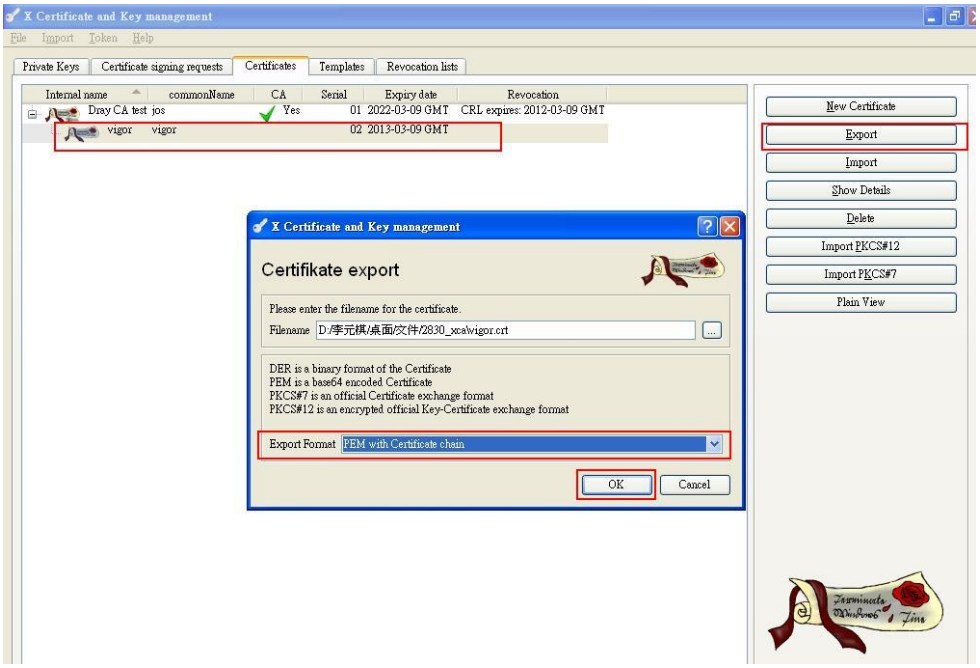


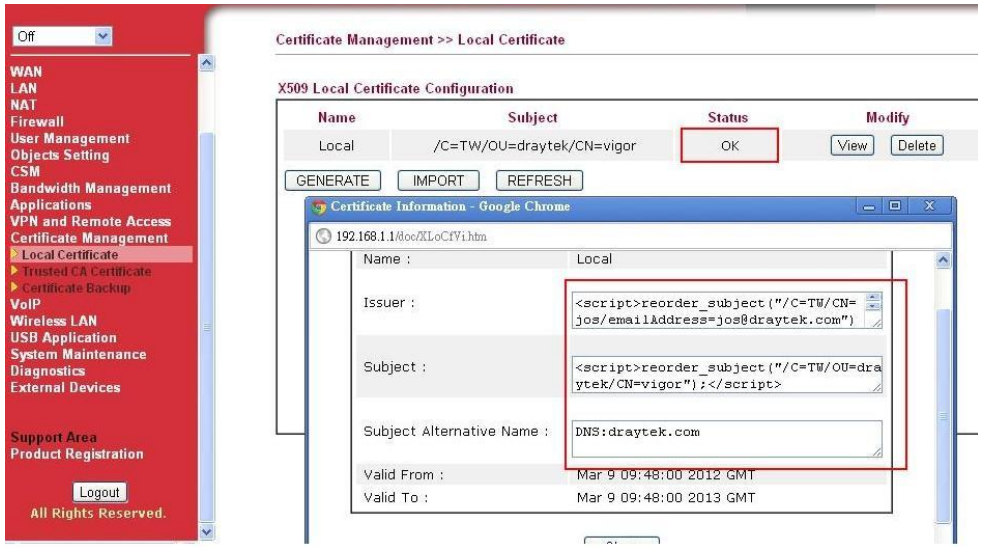
7. Sign Certificate with right click and choose the **Sign** option.



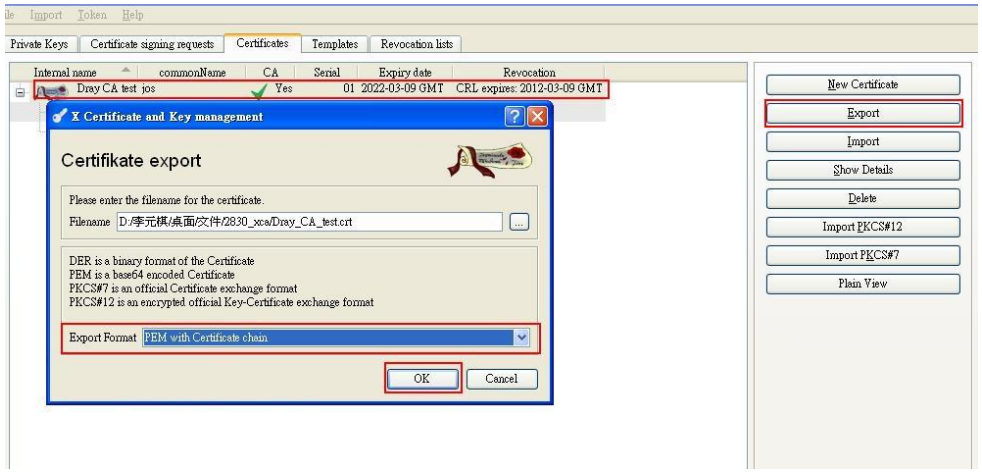


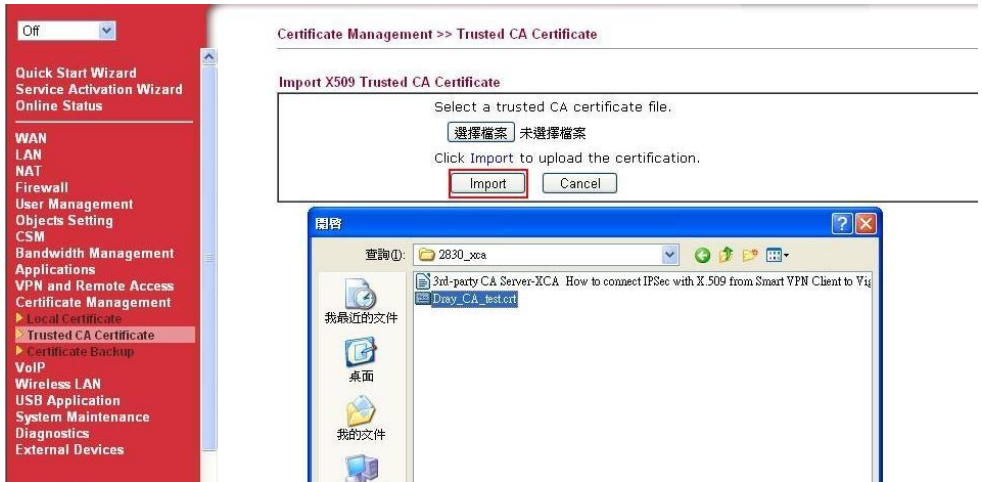
8. Export the Local Certificate to Vigor.

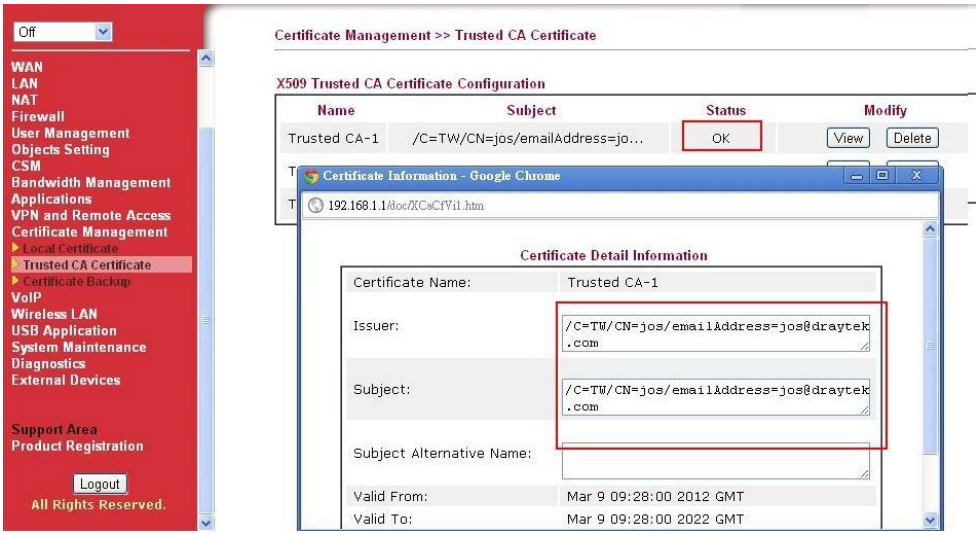




9. Export the Trusted CA Certificate (Dray_CA_test.crt) to Vigor.

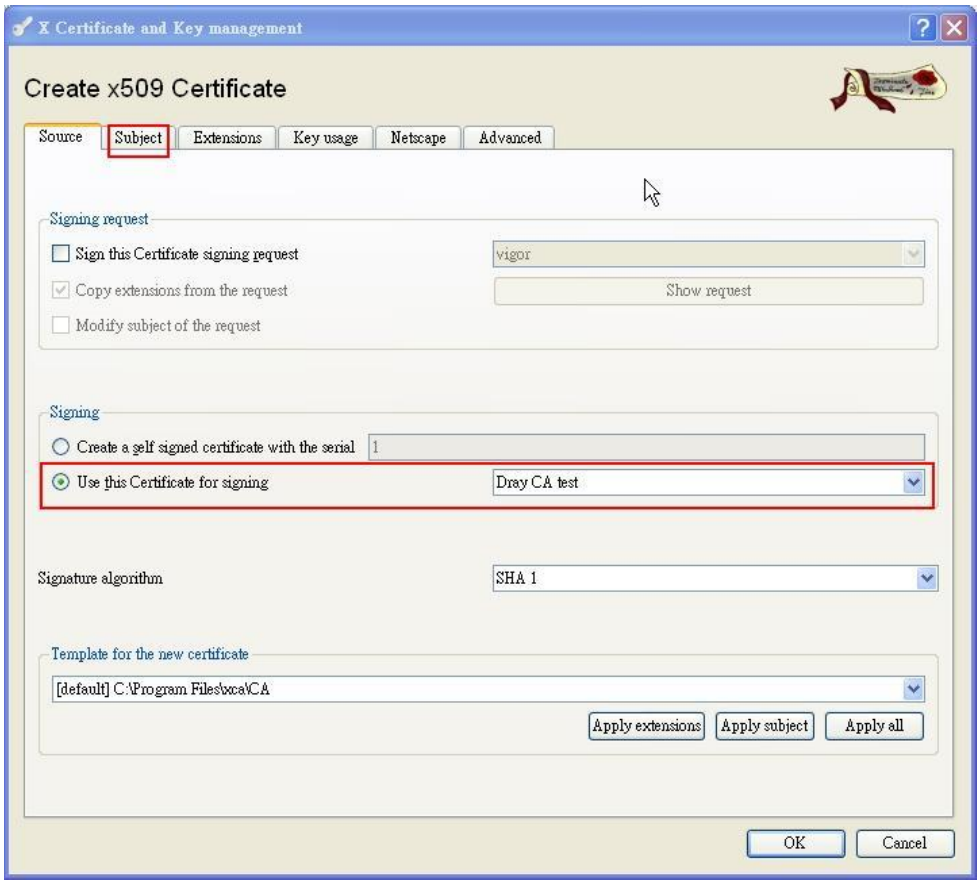




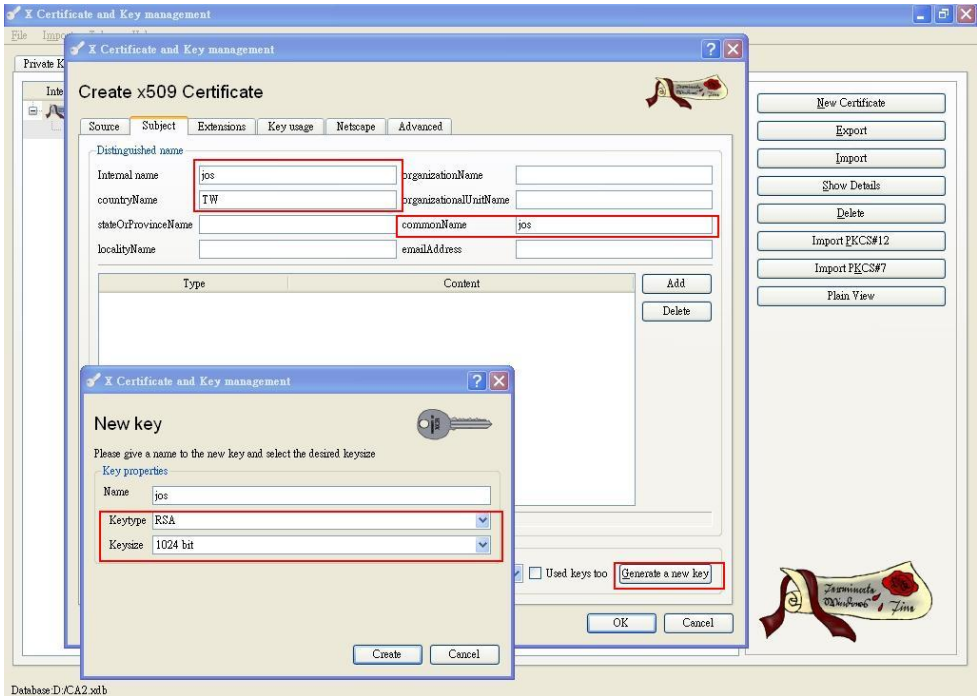


Part C : Making a Private Certificate and Private key for the PC

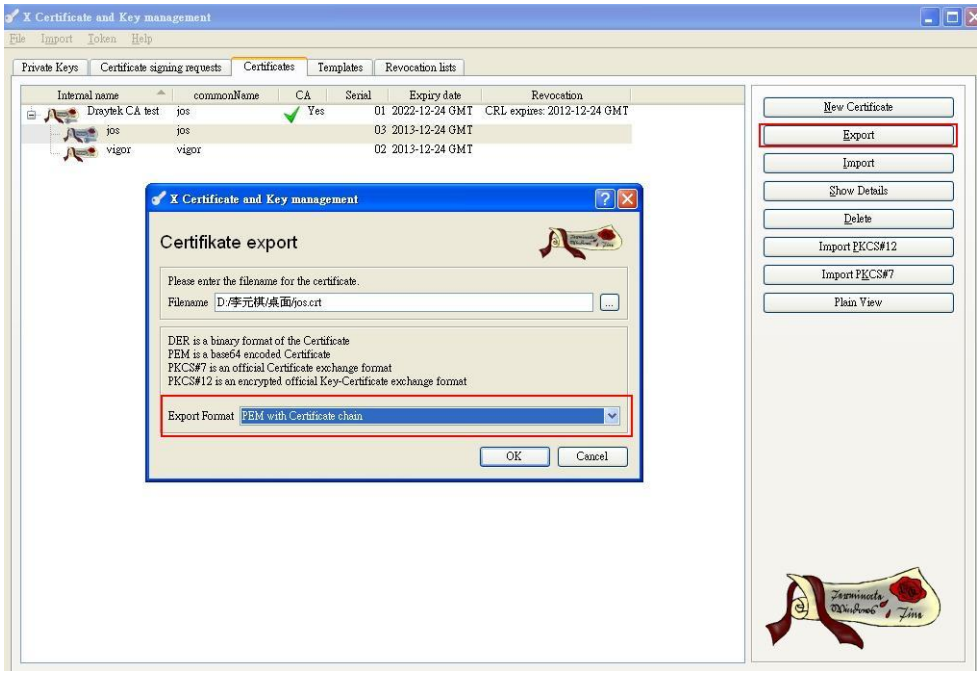
1. Click **New Certificate** button on XCA.
2. Sign with the Trusted Certificate, and go to the **Subject** tab.



3. In Subject page, type a distinguishable or preferred name.
4. Click **Generate a new key** and create a **RSA 1024 bit** key for this Certificate.
5. Click **OK**, and we have generated the Trusted CA Certificate well.

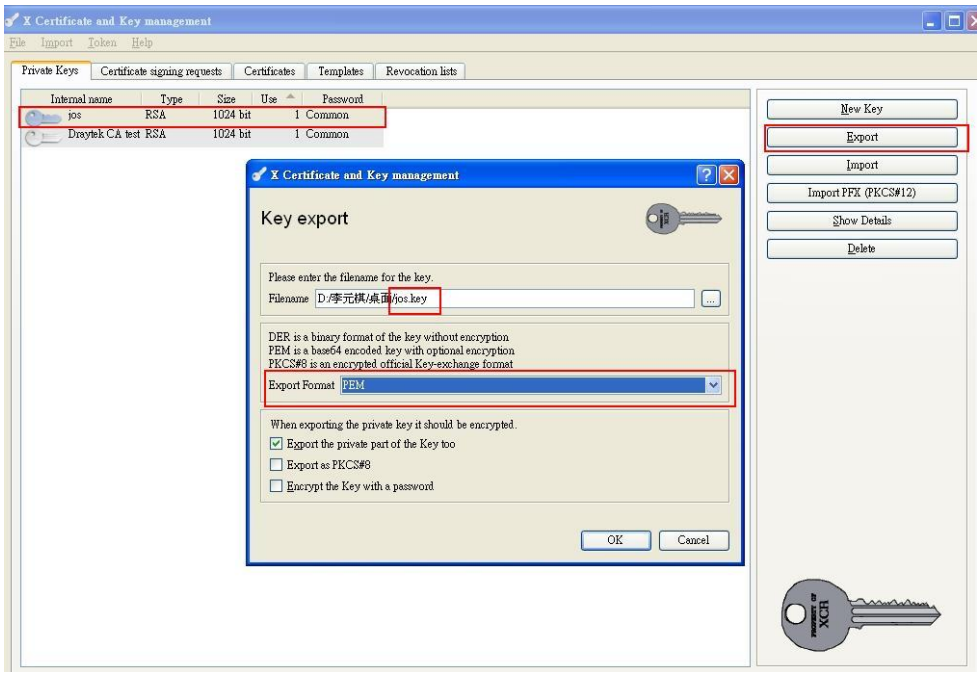


6. Export the Private Certificate (jos.crt) to PC.



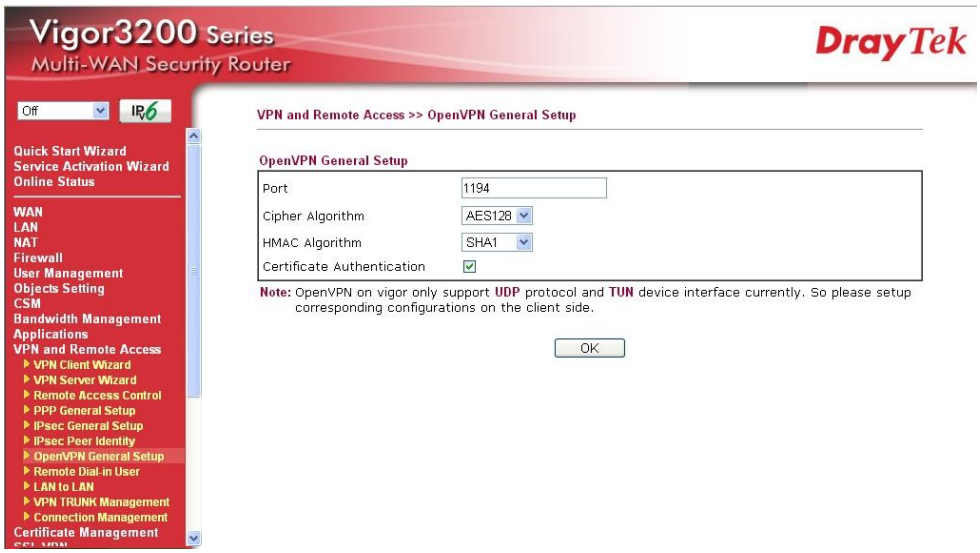
7. Export the Private Key (jos.key) to PC.

7. Export the Private Key (jos.key) to PC.

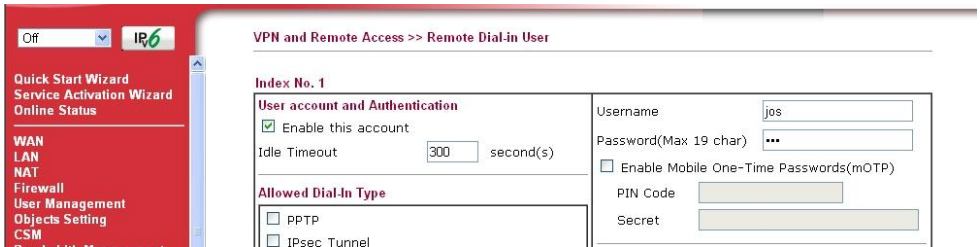


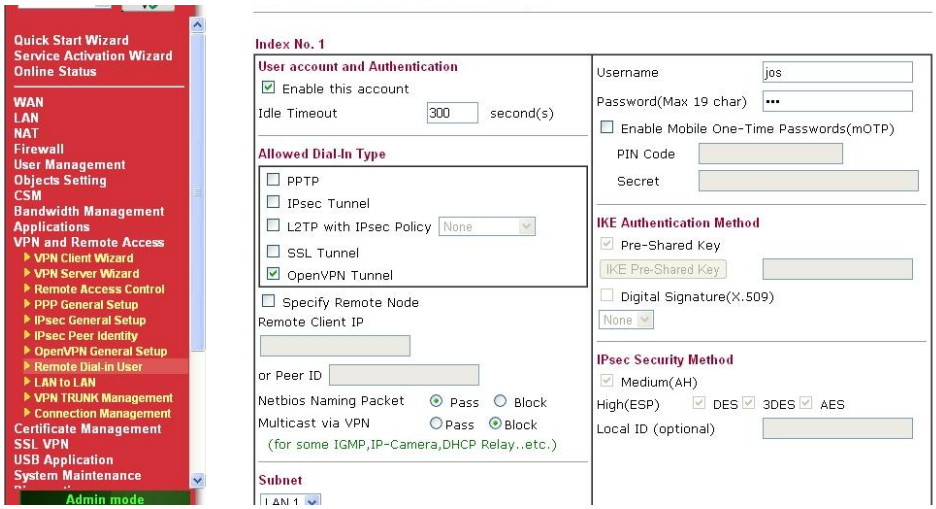
Part D : Setup for OpenVPN Dial-In User on the Router

1. Please go to **VPN and Remote Access >> OpenVPN General Setup**, and follow the OpenVPN setting as the screenshot below.

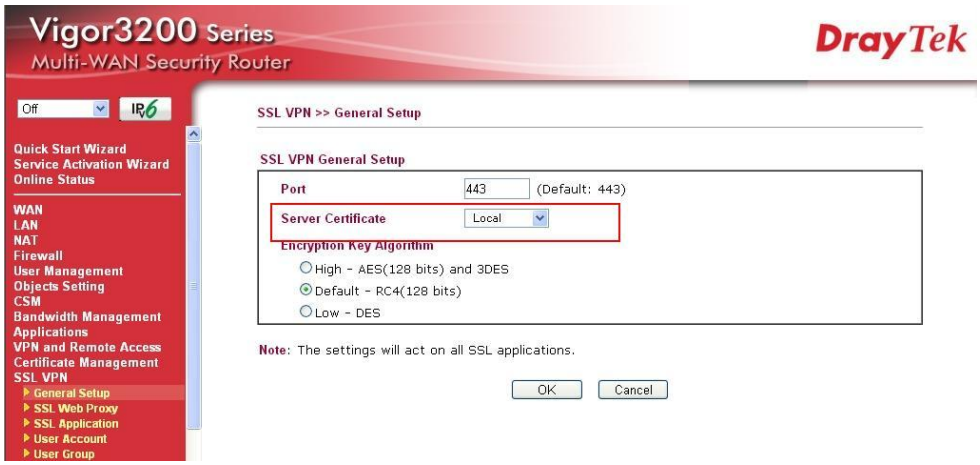


2. Go to **VPN and Remote Access >> Remote Dial-in User** to set up the profiles for Dial-in users. About the user name and password, we define jos/jos for OpenVPN.



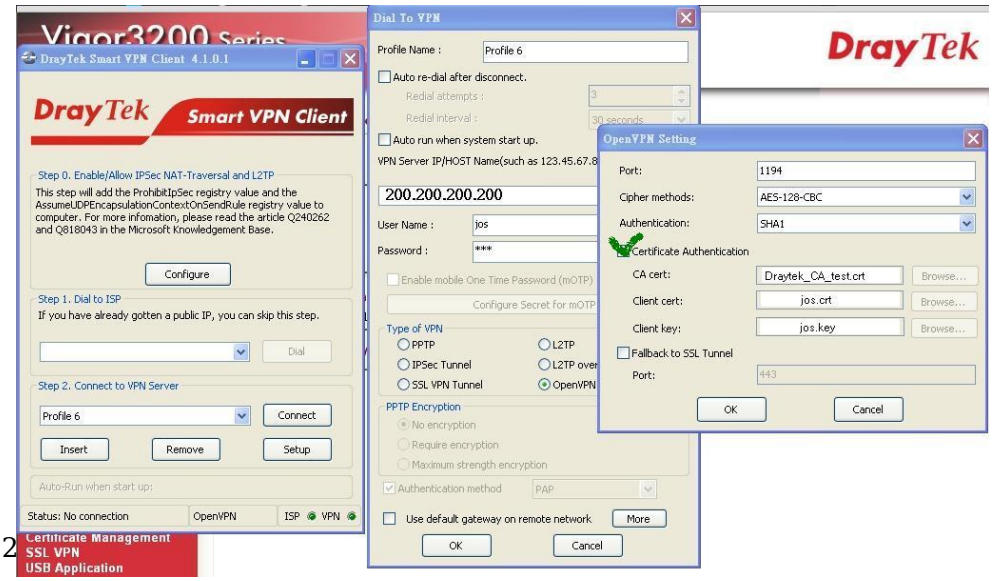


3. Go to **SSL VPN >> General Setup** to set up the Server Certificate Handshake Key for Dial-in users, and here for the **Server Certificate** we choose “Local”, which represents the Local Certificate for OpenVPN user we have generated in Part B.

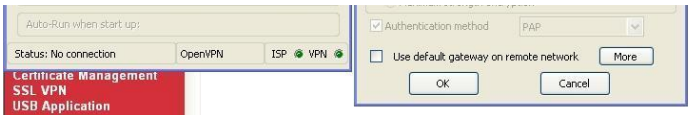


Part E : Setup for SmartVPN Client

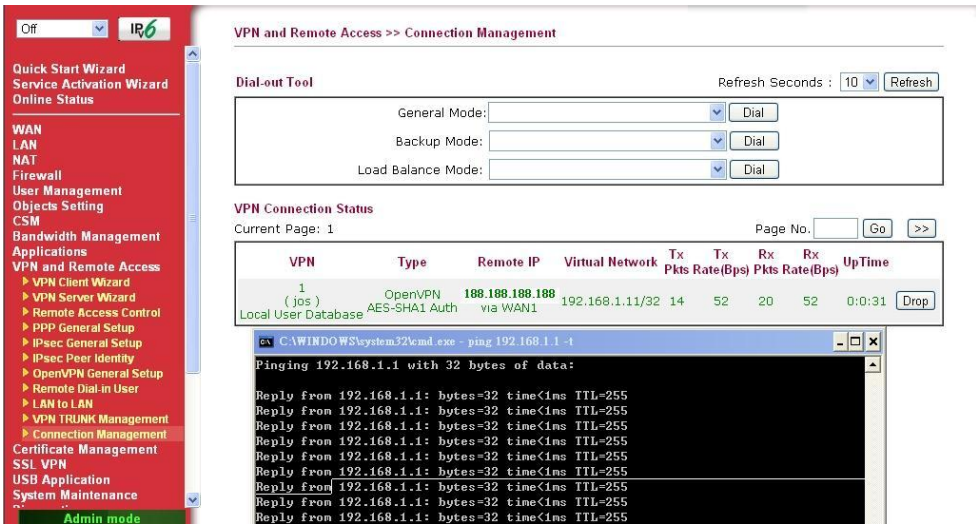
Now there are three files to import into the SmartVPN client**—Trusted CA Certificate (Draytek_CA_test.crt)**, **Private Certificate (jos.crt)**, and **Private Key (jos.key).**



After establishing the OpenVPN tunnels, the PC will be able to access the Vigor 3200's LAN successfully.



After establishing the OpenVPN tunnels, the PC will be able to access the Vigor 3200's LAN successfully.



Read **25** times

Last modified on Wednesday, 02 January 2013 12:21