Advantech AE Technical Share Document

Date	2018/11/30	**SR#**	1-3613369991
Category	■FAQ □SOP	**Related OS**	N/A
Abstract	How to set up OpenVPN		
Keyword	VPN		
Related Product	ADAM-3600, ECU-1152, ECU-1251		

- **Problem Description**:

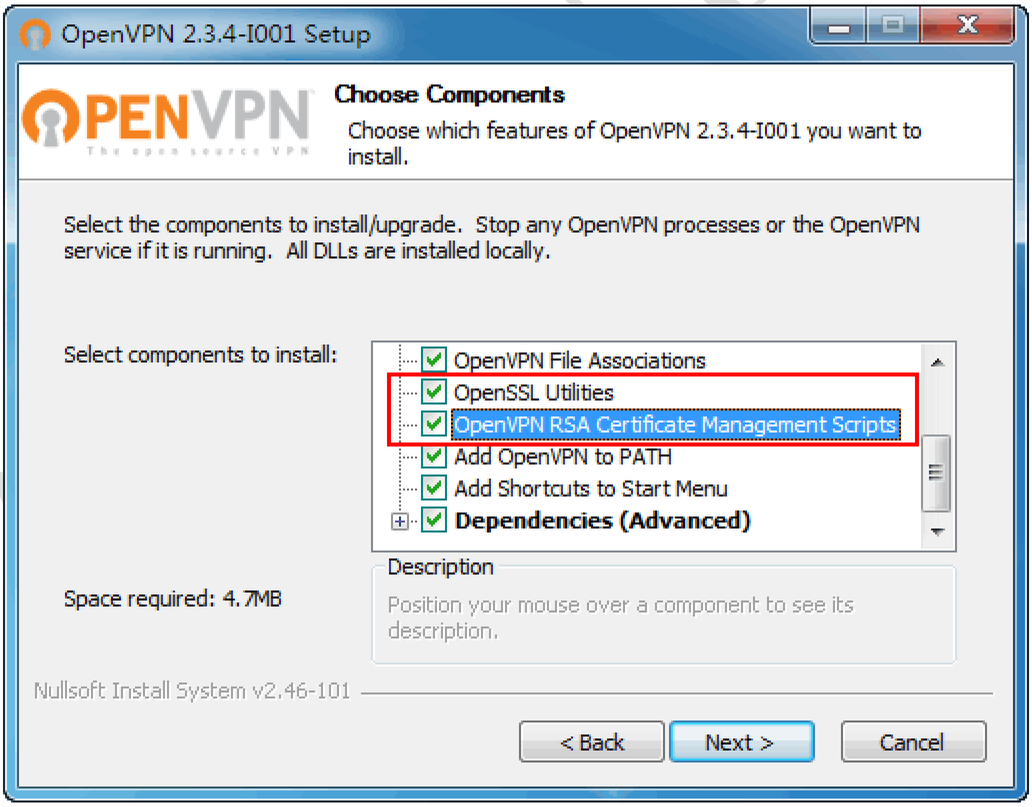
  This document explains how to set up OpenVPN. User could set up VPN for iRTU devices to access private network domain.

- **Answer**:

1. Please download OpenVPN GUI for Windows OS.

https://openvpn.net/index.php/open-source/downloads.html

2. Choose to install "OpenSSL Utilities" and "RSA Certificate Management Scripts" components. (Some OpenVPN version may not be chosen by default.)



OpenVPN 2.3.4-I001 Setup

Choose Components

Choose which features of OpenVPN 2.3.4-I001 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

- ☑ OpenVPN File Associations
- ☑ OpenSSL Utilities
- ☑ OpenVPN RSA Certificate Management Scripts
- ☑ Add OpenVPN to PATH
- ☑ Add Shortcuts to Start Menu
- ☑ **Dependencies (Advanced)**

Space required: 4.7MB

Description

Position your mouse over a component to see its description.

Nullsoft Install System v2.46-101

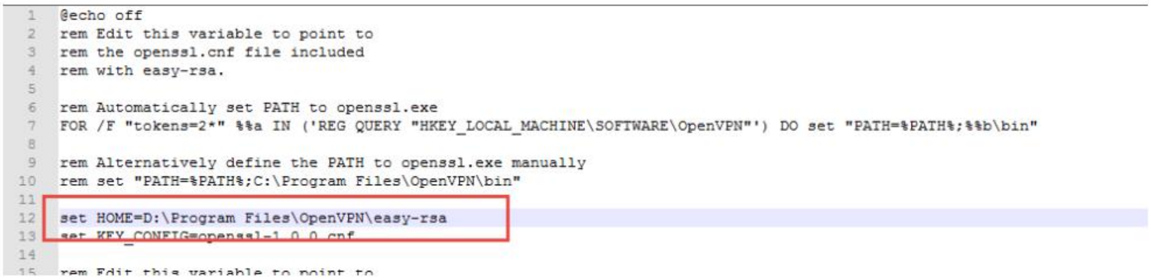
3. Open the directory where OpenVPN installed. (For example, D:\Program Files\OpenVPN)

4. Back up “easy-rsa” and “sample-config” directories.
   (Need to select above RSA package to install in step 2. Otherwise, there is no easy-rsa directory)

5. Edit vars.bat.sample
   Change it to the correct path.

----

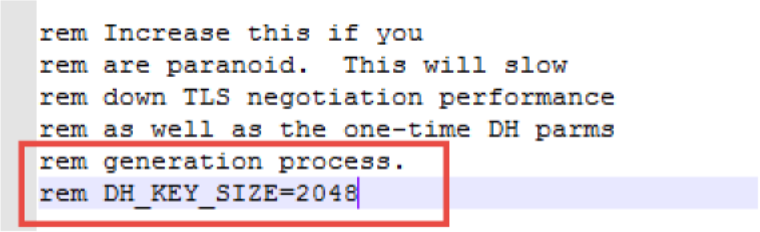
set HOME=D:\Program Files\OpenVPN\easy-rsa



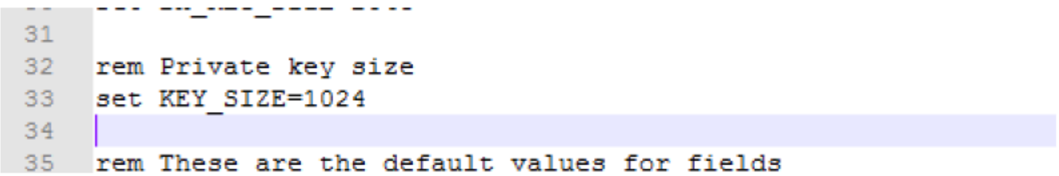
```
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.

rem Automatically set PATH to openssl.exe
FOR /F "tokens=2*" %%a IN ('REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN"') DO set "PATH=%PATH%;%%b\bin"

rem Alternatively define the PATH to openssl.exe manually
rem set "PATH=%PATH%;C:\Program Files\OpenVPN\bin"

set HOME=D:\Program Files\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
```

rem can choose 1024 or 2048 key length. (Choosing 2048 coding takes a long time.)

set KEY_SIZE=1024



```
rem Increase this if you
rem are paranoid.  This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
rem DH_KEY_SIZE=2048
```



```

rem Private key size
set KEY_SIZE=1024

rem These are the default values for fields
```

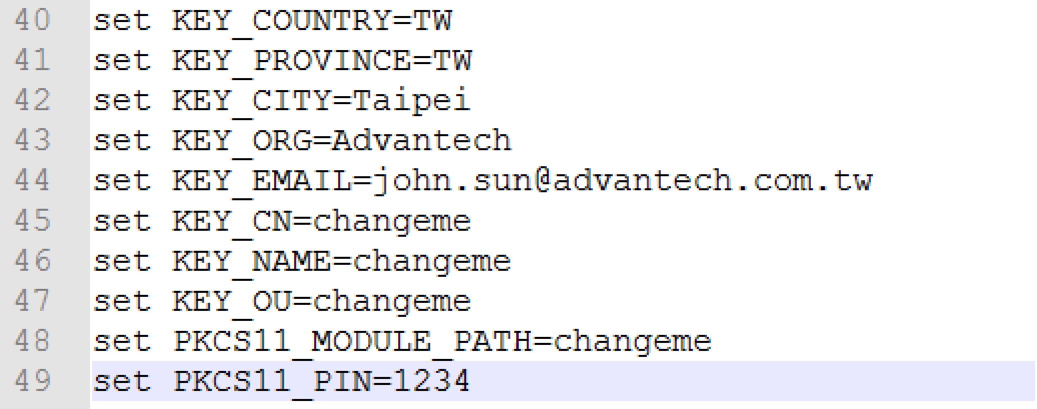
Modify the parametes under rem.

set KEY_COUNTRY=TW

set KEY_PROVINCE=TW

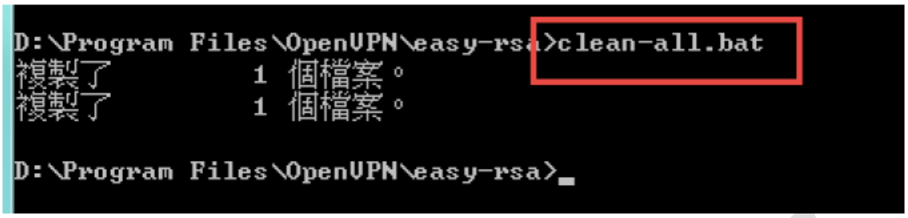
set KEY_CITY=Taipei set KEY_ORG=home

set KEY_EMAIL=john.sun@advantech.com



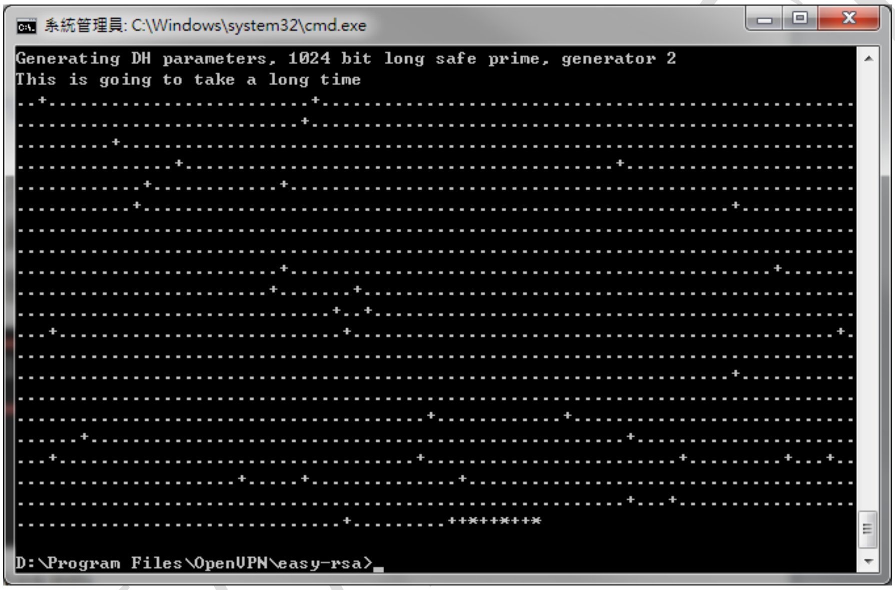
```
set KEY_COUNTRY=TW
set KEY_PROVINCE=TW
set KEY_CITY=Taipei
set KEY_ORG=Advantech
set KEY_EMAIL=john.sun@advantech.com.tw
set KEY_CN=changeme
set KEY_NAME=changeme
set KEY_OU=changeme
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

6. Use cmd line and move to easy-rsa directory.
   Execute “init-config.bat” file, and it would copy 2 files if there is no error message.
7. Execute “vars.bat” to initialize the environment variables.
8. Execute “clean-all.bat” to clean “keys” directory.
   It would copy 2 files if there is no error message.



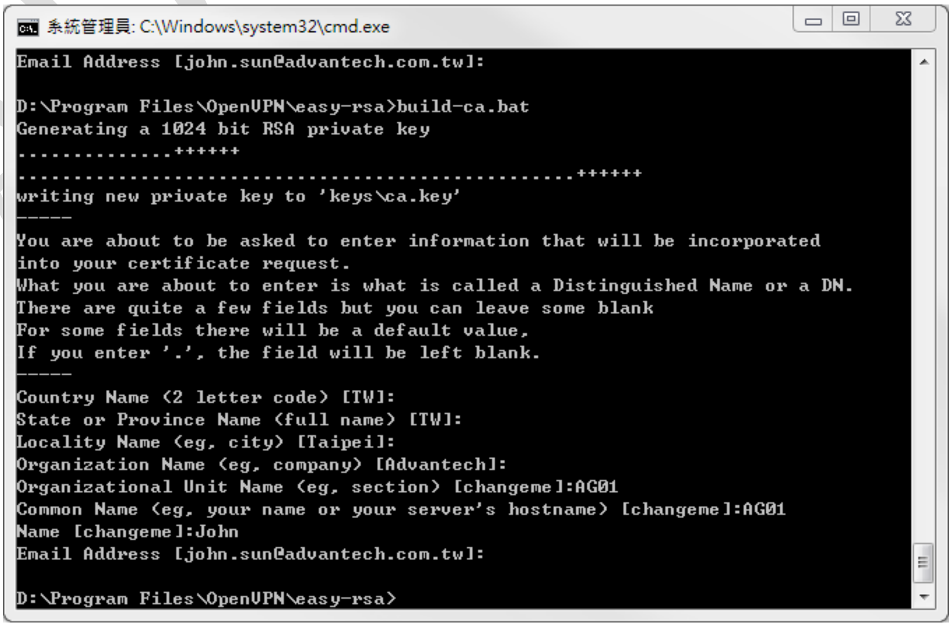
```
D:\Program Files\OpenVPN\easy-rsa>clean-all.bat
複製了         1 個檔案。
複製了         1 個檔案。

D:\Program Files\OpenVPN\easy-rsa>_
```

9. Execute “build-dh.bat” to generate DH parameters. (It may take a while to generate.)



```
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
..+.........................+...................................................
...........................+....................................................
.........+......................................................................
...............+.........................................+......................
............+............+......................................................
...........+........................................................+...........
................................................................................
................................................................................
.........................+..............................................+.......
........................+.......+...............................................
..............................+..+..............................................
...+...........................+..............................................+.
................................................................................
....................................................................+...........
................................................................................
.......................................+............+...........................
......+...................................................+.....................
...+..................................+........................+.........+...+..
.....................+.....+..............+.....................................
..........................................................+...+.................
...............................+.........+++++++++

D:\Program Files\OpenVPN\easy-rsa>_
```

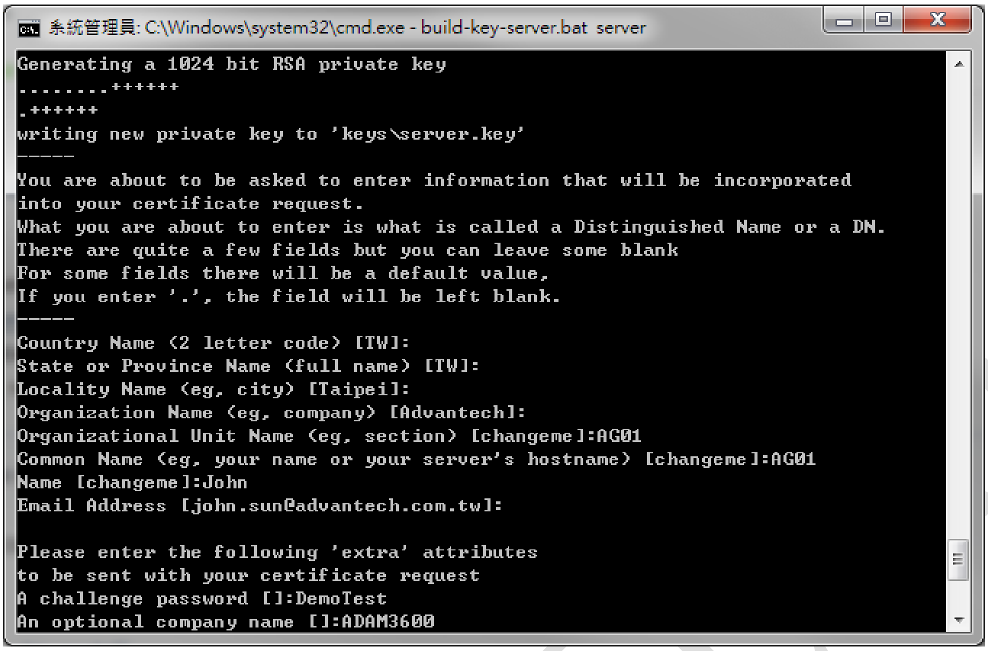
10. Execute “build-ca.bat” to generate certification of server. (keys\ca.key)
    Press “Enter” if there is value in []. (The value user set up in vars.bat.sample)



```
Email Address [john.sun@advantech.com.tw]:

D:\Program Files\OpenVPN\easy-rsa>build-ca.bat
Generating a 1024 bit RSA private key
..............++++++
.....................................................++++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [TW]:
State or Province Name (full name) [TW]:
Locality Name (eg, city) [Taipei]:
Organization Name (eg, company) [Advantech]:
Organizational Unit Name (eg, section) [changeme]:AG01
Common Name (eg, your name or your server's hostname) [changeme]:AG01
Name [changeme]:John
Email Address [john.sun@advantech.com.tw]:

D:\Program Files\OpenVPN\easy-rsa>
```

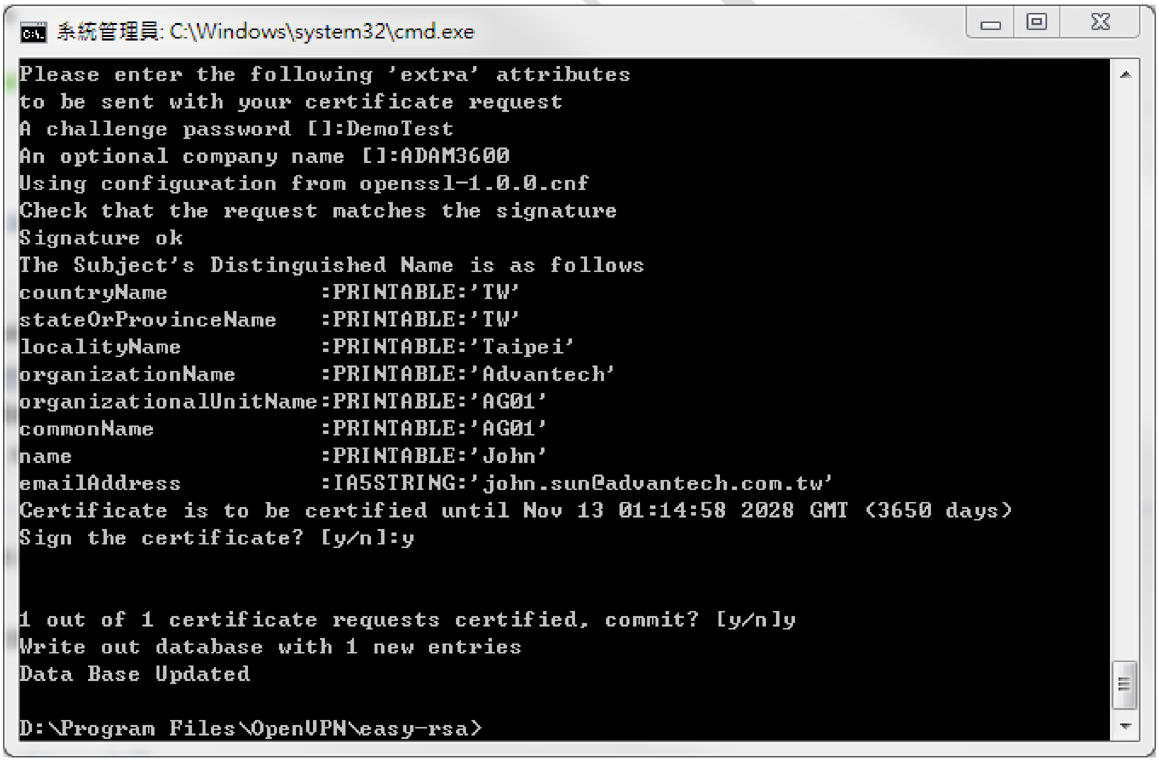
11. Execute “build-key-server.bat server” to generate server key. (keys\server.key)

    Please add space before variable “ server”.


系統管理員: C:\Windows\system32\cmd.exe - build-key-server.bat server

```
Generating a 1024 bit RSA private key
........++++++
.++++++
writing new private key to 'keys\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [TW]:
State or Province Name (full name) [TW]:
Locality Name (eg, city) [Taipei]:
Organization Name (eg, company) [Advantech]:
Organizational Unit Name (eg, section) [changeme]:AG01
Common Name (eg, your name or your server's hostname) [changeme]:AG01
Name [changeme]:John
Email Address [john.sun@advantech.com.tw]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:DemoTest
An optional company name []:ADAM3600
```

The information (section, host name, and so on) during generating server.key shall be the same in the next step of generating client.key.



```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:DemoTest
An optional company name []:ADAM3600
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'TW'
stateOrProvinceName   :PRINTABLE:'TW'
localityName          :PRINTABLE:'Taipei'
organizationName      :PRINTABLE:'Advantech'
organizationalUnitName:PRINTABLE:'AG01'
commonName            :PRINTABLE:'AG01'
name                  :PRINTABLE:'John'
emailAddress          :IA5STRING:'john.sun@advantech.com.tw'
Certificate is to be certified until Nov 13 01:14:58 2028 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

D:\Program Files\OpenVPN\easy-rsa>
```

Press “y” to commit for requesting certification.

The certification of server is established after finishing this step.

12. Now we create “Client key”. Execute “build-key.bat client1”

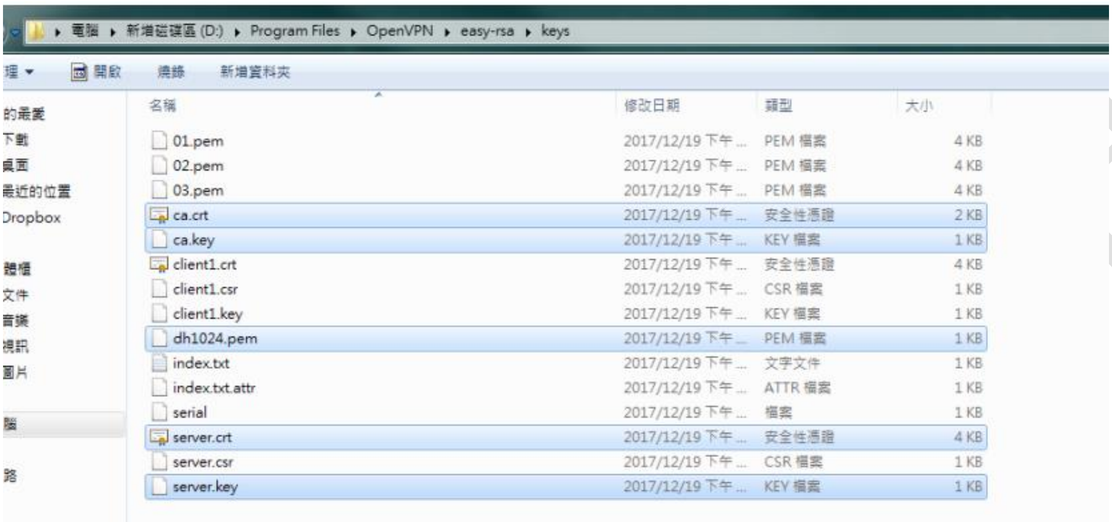
    Please add space before variable “ client1”.

(User could "build-key jack" or "build-key john")

Key in the same info as you created "server.key".

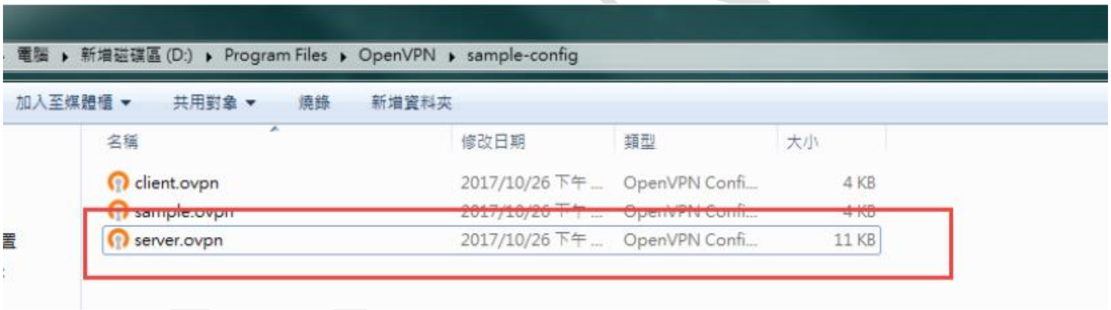
Note: User could create as many clients as he wants, but the name cannot be duplicated. Otherwise, there would be error message in .old file, and user needs to clean and make again.

13. Copy files for server (ca.crt、ca.key、dh1024.pem、server.crt、server.key) to config directory.



名稱	修改日期	類型	大小
01.pem	2017/12/19 下午 ...	PEM 檔案	4 KB
02.pem	2017/12/19 下午 ...	PEM 檔案	4 KB
03.pem	2017/12/19 下午 ...	PEM 檔案	4 KB
ca.crt	2017/12/19 下午 ...	安全性憑證	2 KB
ca.key	2017/12/19 下午 ...	KEY 檔案	1 KB
client1.crt	2017/12/19 下午 ...	安全性憑證	4 KB
client1.csr	2017/12/19 下午 ...	CSR 檔案	1 KB
client1.key	2017/12/19 下午 ...	KEY 檔案	1 KB
dh1024.pem	2017/12/19 下午 ...	PEM 檔案	1 KB
index.txt	2017/12/19 下午 ...	文字文件	1 KB
index.txt.attr	2017/12/19 下午 ...	ATTR 檔案	1 KB
serial	2017/12/19 下午 ...	檔案	1 KB
server.crt	2017/12/19 下午 ...	安全性憑證	4 KB
server.csr	2017/12/19 下午 ...	CSR 檔案	1 KB
server.key	2017/12/19 下午 ...	KEY 檔案	1 KB

14. Copy "server.ovpn" from sample-config directory to "config" directory.



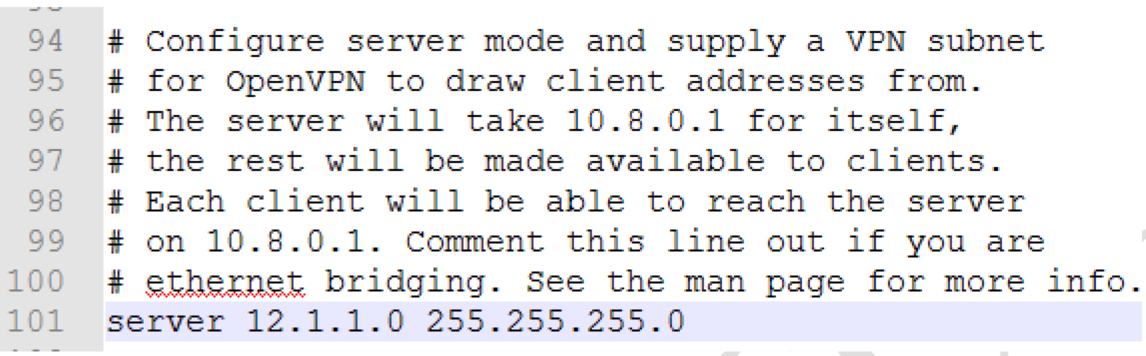
電腦 ▸ 新增磁碟區 (D:) ▸ Program Files ▸ OpenVPN ▸ sample-config
加入至媒體櫃 ▾
共用對象 ▾
燒錄
新增資料夾

名稱	修改日期	類型	大小
client.ovpn	2017/10/26 下午 ...	OpenVPN Confi...	4 KB
sample.ovpn	2017/10/26 下午 ...	OpenVPN Confi...	4 KB
server.ovpn	2017/10/26 下午 ...	OpenVPN Confi...	11 KB

15. Modify server.ovpn in config.

```
# Which local IP address should OpenVPN
# listen on? (optional)
;local 192.168.1.2

#   The port user connects. Please check firewall is open and set up well.
port 1194
#   To use TCP or UDP
proto tcp

# "dev tun" will create a routed IP tunnel, # "dev tap" will create an ethernet tunnel.
# choose tun to use existed IP as tunnel.
```

```
dev tun
# dh is the length of key. Modify it if you changed the default 1024.
dh dh1024.pem

# server is for setting your vpn network domain.
server 12.1.1.0 255.255.255.0
```



```
# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 12.1.1.0 255.255.255.0
```

```
#    Open push "route 192.168.2.0 255.255.255.0" for routing by vpn
push "route 12.1.1.0 255.255.255.0"
#    Open client-to-client to make client connects to other client.
client-to-client

#    Open duplicate-cn for client name duplicates.
# If many users use the same key with single connection file, after setting up “duplicate-cn”, each client IP would not be fixed.
duplicate-cn

#Please open comp-lzo because most users use 3G, and need to compress for packet traffic.
comp-lzo
# Notify the client that when the server restarts so it
# can automatically reconnect.
#explicit-exit-notify 1
```

Save file.

16. To check server is configured correctly, right-click on OpenGUI and choose “connect”. There would open another window, if there is no error, the window would close. OpenGUI would change from red light to green light and get one VPN IP.

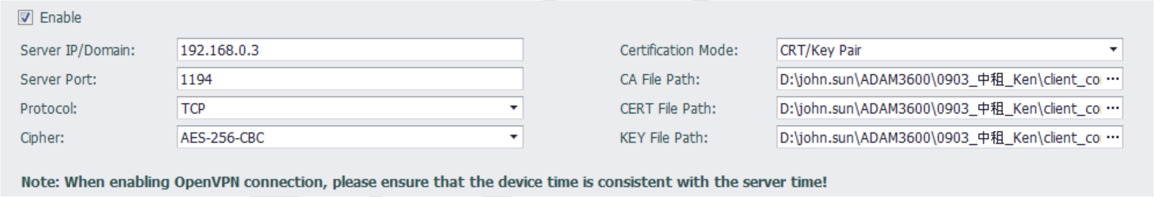
The files server needs:

```
ca.crt

ca.key

dh1024.pem

server.crt

server.key

ta.key (If there is TLS authentication.)
```

The files client needs:

```
ca.crt

client1.crt

client1.key (client1 name may be different based on previous configuration.)

ta.key (If there is TLS authentication.)
```

17. In EdgeLink, choose the path of files (ca.crt, client1.crt, client1.key).



☑ Enable

Server IP/Domain: 192.168.0.3

Server Port: 1194

Protocol: TCP

Cipher: AES-256-CBC

Certification Mode: CRT/Key Pair

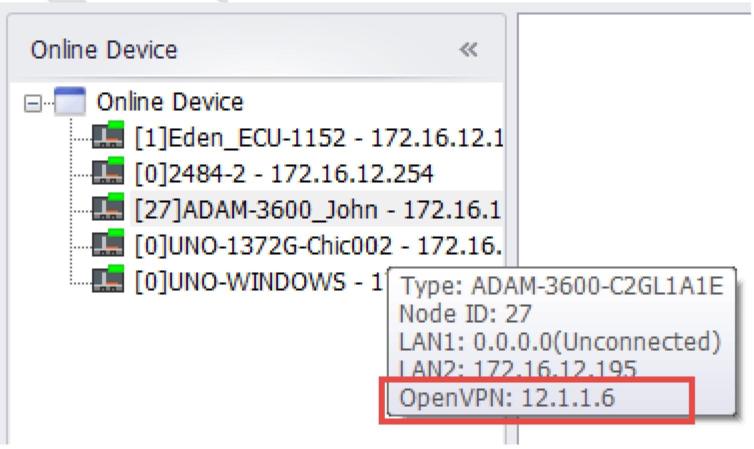
CA File Path: D:\john.sun\ADAM3600\0903_中租_Ken\client_co ···

CERT File Path: D:\john.sun\ADAM3600\0903_中租_Ken\client_co ···

KEY File Path: D:\john.sun\ADAM3600\0903_中租_Ken\client_co ···

Note: When enabling OpenVPN connection, please ensure that the device time is consistent with the server time!

Download the project and restart the service. The device may get VPN IP if successfully.



[1]Eden_ECU-1152 - 172.16.12.1

[0]2484-2 - 172.16.12.254

[27]ADAM-3600_John - 172.16.1

[0]UNO-1372G-Chic002 - 172.16.

[0]UNO-WINDOWS - 1

Type: ADAM-3600-C2GL1A1E

Node ID: 27

LAN1: 0.0.0.0(Unconnected)

LAN2: 172.16.12.195

OpenVPN: 12.1.1.6

18. Set Port Forwarding in the router if needed.

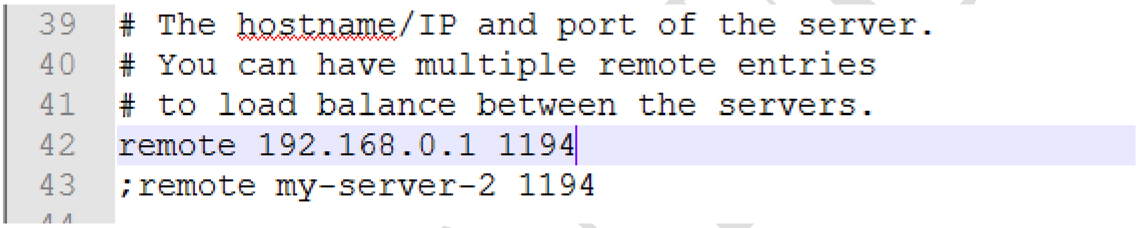
19. If user wants to use laptop as client, please do following steps.

    Copy ca.crt, client1.crt, client1.key in easy-rsa\keys to “config” directory.

    Copy Client.ovpn to “config” directory.

    Modify client.ovpn

```
# settings shall be coherent as in server.
dev tun
proto tcp
remote 192.168.0.1 1194
ca ca.crt
cert client1.crt
key client1.key
comp-lzo
```



```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 192.168.0.1 1194
;remote my-server-2 1194
```