

## Advantech AE Technical Share Document

Date	2019/7/20	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:**

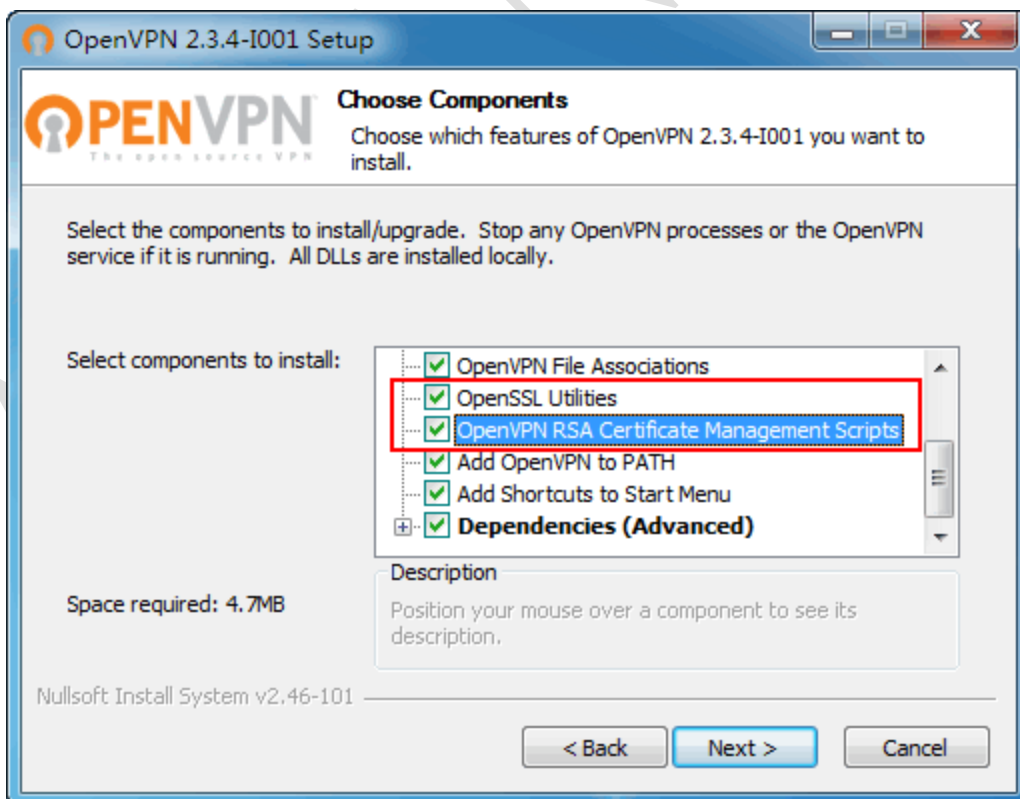
1. Please download OpenVPN GUI for Windows OS.

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

Note: Please use OpenVPN version 2.3.x, instead of 2.4.x or newer.

(Because iRTU uses 2.3 version, so VPN server needs to install 2.3 as well.)

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



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 /easy-rsa/vars.bat.sample  
Set Home to the path of folder easy-rsa.

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

```

1 @echo off
2 rem Edit this variable to point to
3 rem the openssl.cnf file included
4 rem with easy-rsa.
5
6 rem Automatically set PATH to openssl.exe
7 FOR /F "tokens=2*" %a IN ('REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN"') DO set "PATH=%PATH%;%a\bin"
8
9 rem Alternatively define the PATH to openssl.exe manually
10 rem set "PATH=%PATH%;C:\Program Files\OpenVPN\bin"
11
12 set HOME=D:\Program Files\OpenVPN\easy-rsa
13 set KEY_CONFIG=openssl-1.0.0.cnf
14
15 rem Edit this variable to point to

```

You can choose 1024 or 2048 for Key length. (Choosing 2048 coding takes a long time.)

set KEY\_SIZE=1024

```

31
32 rem Private key size
33 set KEY_SIZE=1024
34
35 rem These are the default values for fields

```

6. Use cmd line and move to easy-rsa directory.  
Execute the following commands in turn to complete the initialization

```

init-config
vars
clean-all

```

```

D:\OpenUPN\easy-rsa>init-config
D:\OpenUPN\easy-rsa>copy vars.bat.sample vars.bat
已复制      1 个文件。
D:\OpenUPN\easy-rsa>vars
D:\OpenUPN\easy-rsa>clean-all
系统找不到指定的文件。
已复制      1 个文件。
已复制      1 个文件。
D:\OpenUPN\easy-rsa>

```

“init-config.bat” would copy 2 files if there is no error message.

“vars.bat” is to initialize the environment variables. Every time opening command prompt

window, “vars” command must be executed before other commands can be executed.

“clean-all.bat” is to clean “keys” directory. (When cleaning-all is executed for the first time, it is normal to prompt “the system cannot find the specified file”. This command deletes all previously generated certificates and key files to avoid conflicting with the newly generated certificates and keys.)

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

```

系統管理員: C:\Windows\system32\cmd.exe
Email Address [john.sun@advantech.com.tw]:
D:\Program Files\OpenUPN\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\OpenUPN\easy-rsa>

```

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

```

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.



```
C:\Windows\system32\cmd.exe
D:\OpenVPN\easy-rsa>openvpn --genkey --secret keys/ta.key
D:\OpenVPN\easy-rsa>_
```

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



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



14. Modify server.ovpn in config.

You can also see the description in the server.ovpn.

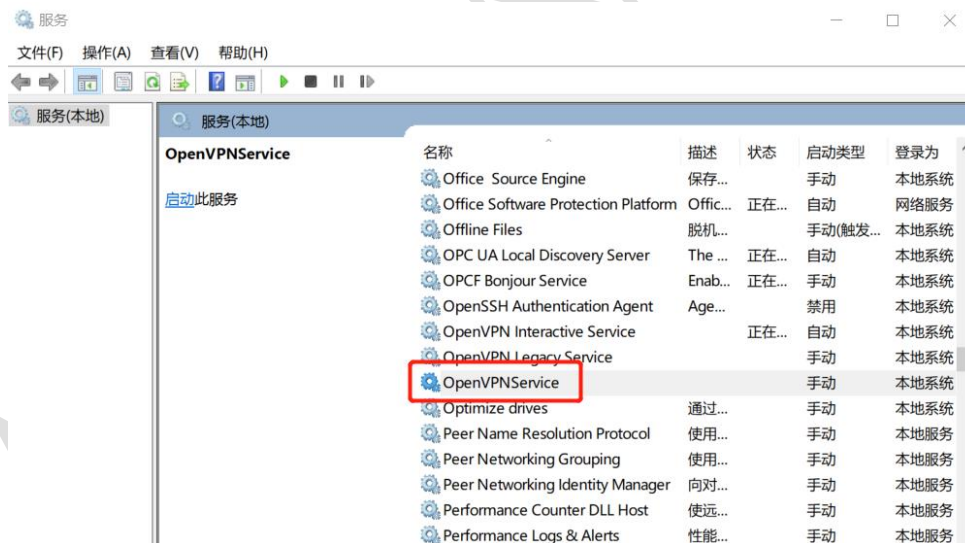
```
local 192.168.1.101 # Specify the native IP to listen on (because some computers
have multiple IP addresses), this command is optional and defaults to listen on all
IP addresses.
port 1194 # local port number to listen on
proto tcp # transport protocol
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 12.1.1.1 255.255.255.0 # IP address segments and subnet masks used in virtual
```

```

local area networks. In this example, the server occupy 10.0.0.1
ifconfig-pool-persist ip.txt
tls-auth ta.key 0 #Open TLS-auth, the second parameter should be '0' on the server
and '1' on the clients.
cipher AES-256-CBC #Cryptographic cipher.
keepalive 10 120
comp-lzo #Enable VPN connection compression. If the server is open, the
client must be open.
client-to-client # The client is allowed to connect to the client.
persist-key
persist-tun
status openvpn-status.log
verb 3
    
```

Save file.

15. Enter the Windows Service Interface of the Computer on the Server to open the service Openvpn. (cmd--- services.msc)



16. In EdgeLink, fill in the openvpn server's ip, port and choose the cipher, the path of files (ca.crt, client1.crt, client1.key).

For TLS, choose the ta.key and the auth direction should be 1 if server is 0.

Note: the gateway's time should be the same as openvpn server's time. You can do Time Calibration in online monitor.

Network Setting(Adam-3600) OpenVPN(Adam-3600) x

Apply Discard

Enable

Server IP/Domain: 10.0.0.100

Server Port: 1194

Protocol: TCP

Cipher: AES-256-CBC

Certification Mode: CRT/Key Pair

CA File Path: D:\Program Files\OpenVPN\easy-rsa\keys\ca.crt

CERT File Path: D:\Program Files\OpenVPN\easy-rsa\keys\adam360...

KEY File Path: D:\Program Files\OpenVPN\easy-rsa\keys\adam360...

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

TLS Authentication

Auth File Path: D:\Program Files\OpenVPN\config\ta.key

Auth Direction: 1

Download the project. The gateway will get the IP of openvpn.

Online Device

- [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