

Advantech AE Technical Share Document

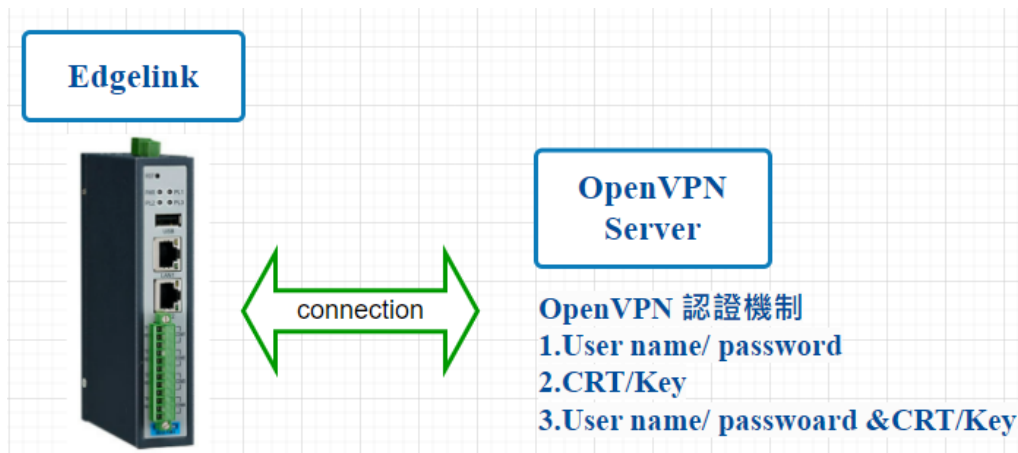
Date	2023/09/07	Release Note	<input type="checkbox"/> Internal <input checked="" type="checkbox"/> External
Category	<input checked="" type="checkbox"/> FAQ <input type="checkbox"/> SOP	Related OS	Win10, Win7
Abstract	How to set up dual certification for OpenVPN in Edgelinek		
Keyword	Edgelinek OpenVPN		
Related Product	ECU-1051 , ECU-1251 、 ADAM-3600		

■ **Description:**

Edgelinek 針對 OpenVPN 連線設定，目前提供 2 種認證機制(二擇一)。

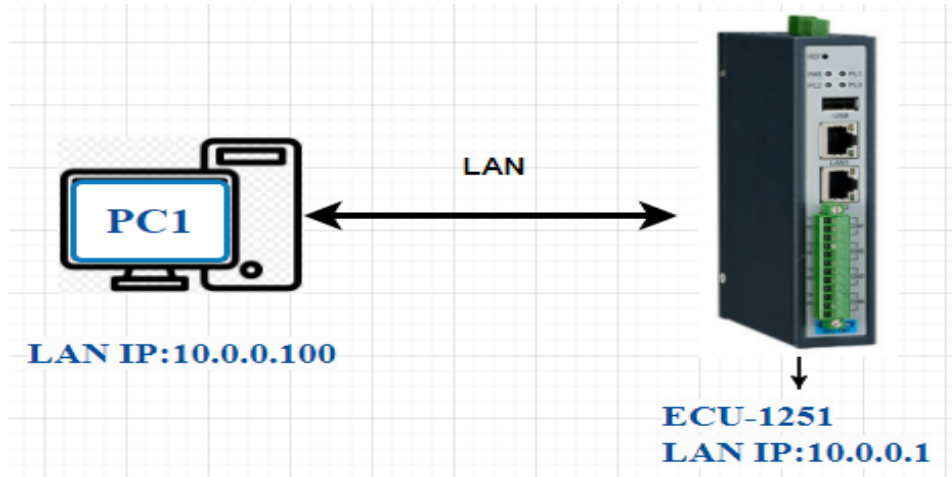
- ◆ 帳密認證 User name/password
- ◆ 金鑰憑證 Crt/Key

但有些 OpenVPN server 要求帳密和金鑰憑證同時認證。所以此文件說明如何設定 Edgelinek，同時提供帳密和金鑰憑證同時認證。此範例使用 ECU-1251 硬體

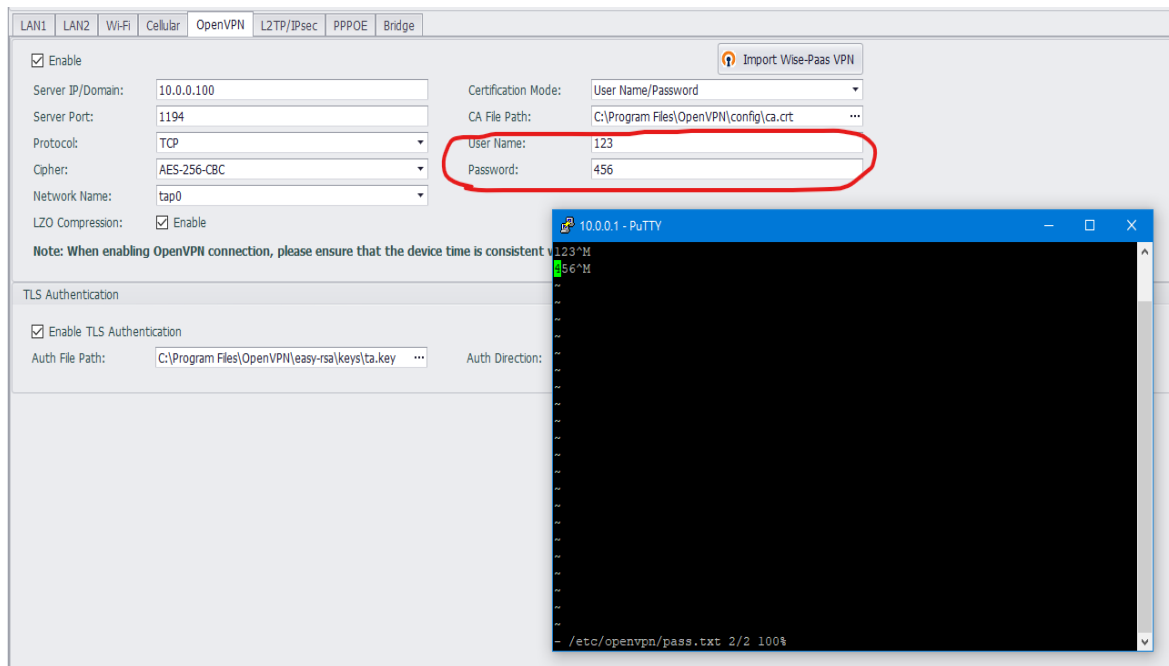


■ Brief Solution - Step by Step:

- ◆ 請先將電腦 IP 設定和 ECU-1251 的 IP 相同網域並直接連線。此範例架構如下
目前 ECU-1051 LAN1 IP:10.0.0.1
電腦 IP:10.0.0.100



- ◆ 電腦執行 Edgeline Studio 開啟專案，請將 OpenVPN 認證切為 user name/password 模式設定 user name/password 後，將專案下載至 ECU 目的是讓 pass.txt 內容有帳密

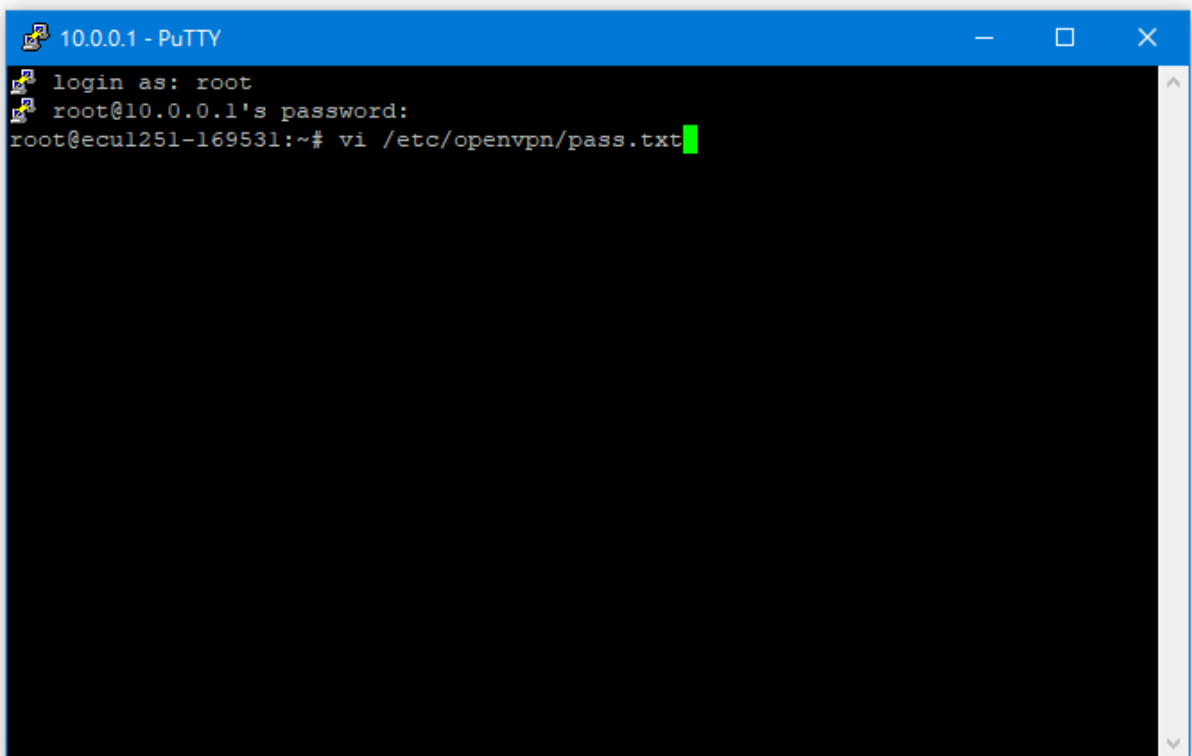
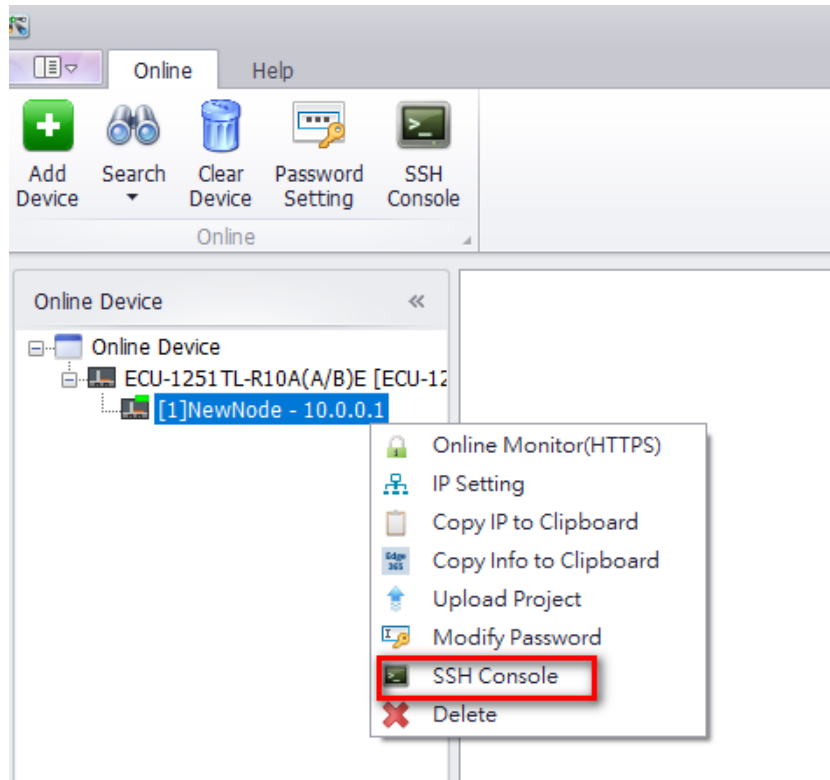


◆ Edgelinek 切換至線上監控模式，使用 SSH console 連線至 ECU-1251

1) 帳號:root 密碼:無

2) 輸入:vi /etc/openvpn/pass.txt

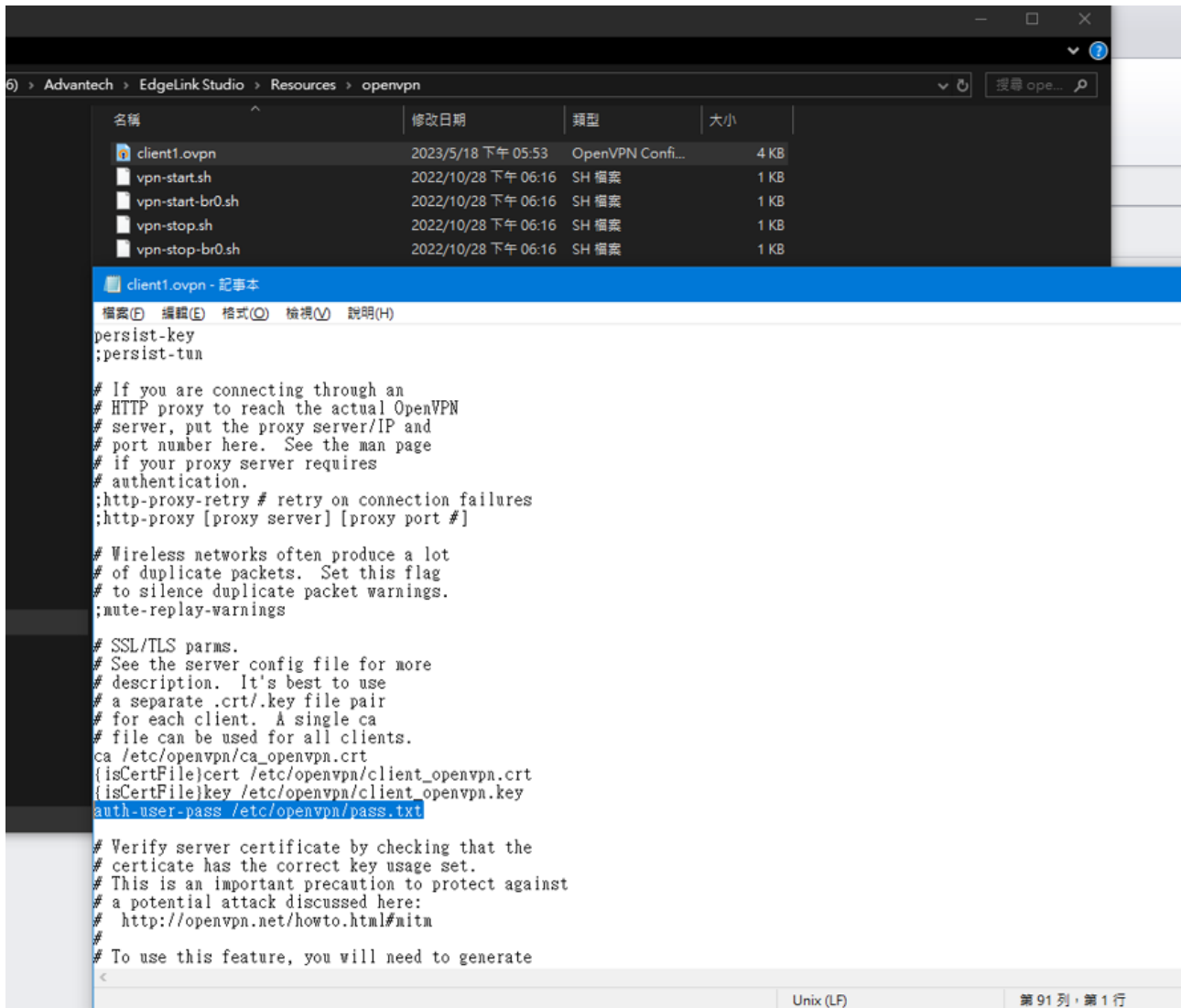
可以確認在 Edgelinek 設定的帳密有無寫入 pass.txt



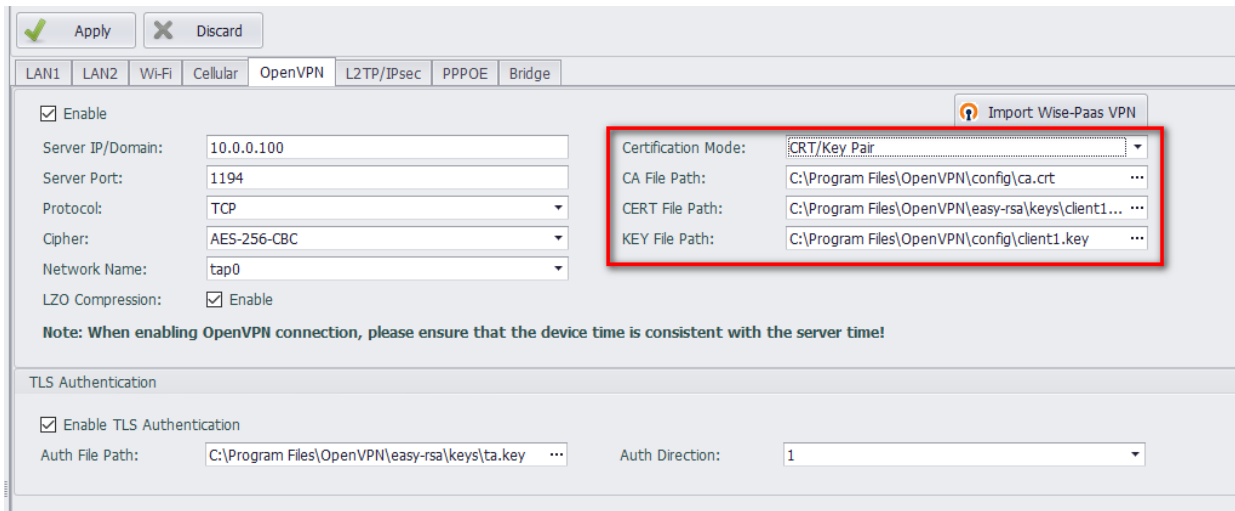
- ◆ 請到電腦下列路徑，找到 client1.ovpn 檔案

C:\Program Files (x86)\Advantech\EdgeLink Studio\Resources\openvpn\client1.ovpn

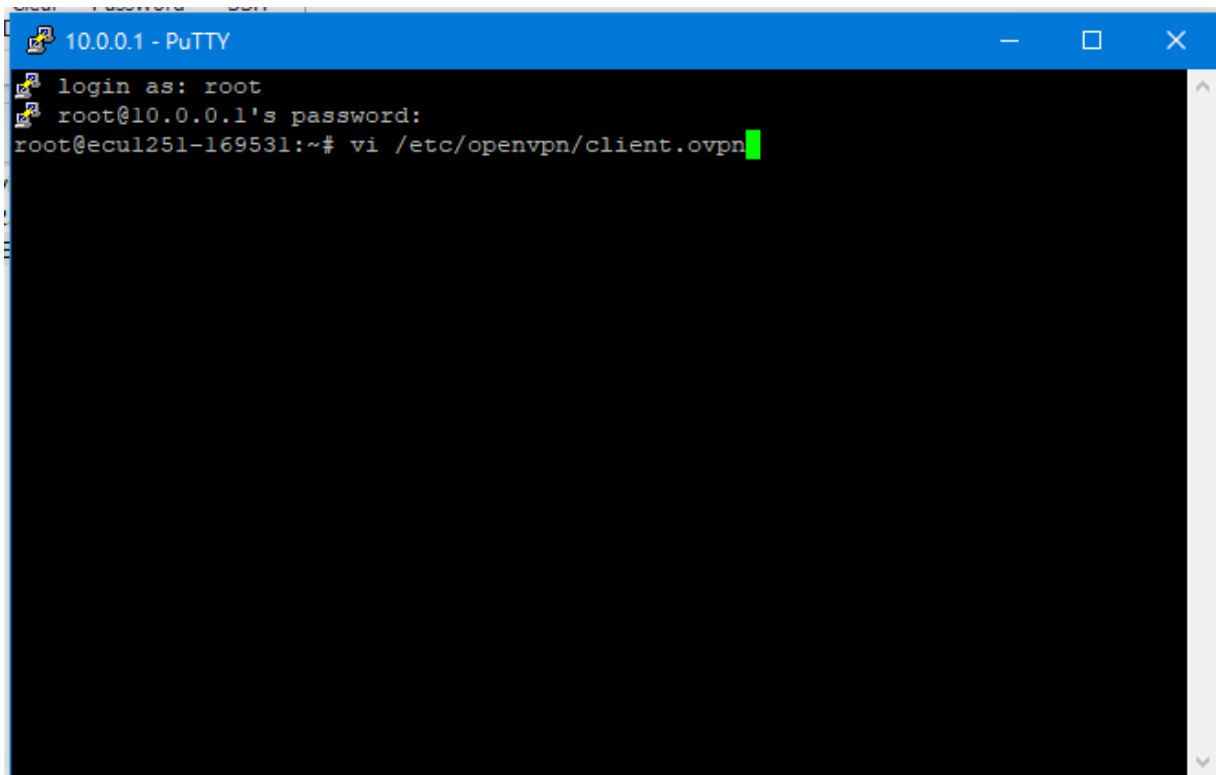
修改如下藍框並儲存。



- ◆ 電腦重啟 Edgeline Studio，開啟專案 OpenVPN 認證切為 CRT/Key Pair 模式
選擇 CA/CERT/Key 檔案所放置本機路徑後，將專案下載至 ECU。



- ◆ Edgeline studio 切換至線上監控模式，使用 SSH console 連線至 ECU-1251
 - 1) 帳號:root 密碼:無
 - 2) 輸入:vi /etc/openvpn/client.ovpn 內容。有順利修改完成，系統會吃 CA/CERT/Key 和 pass.txt 後續系統就會依據此 client.ovpn 連線 open server。



```
10.0.0.1 - PuTTY
# on machines which are not permanently connected
# to the internet such as laptops.
# resolv-retry infinite
# Most clients don't need to bind to
# a specific local port number.
# nobind
# Downgrade privileges after initialization (non-Windows only)
# ;user nobody
# ;group nobody
# Try to preserve some state across restarts.
# persist-key
# ;persist-tun
# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here. See the man page
# if your proxy server requires
# authentication.
# ;http-proxy-retry # retry on connection failures
# ;http-proxy [proxy server] [proxy port #]
# Wireless networks often produce a lot
# of duplicate packets. Set this flag
# to silence duplicate packet warnings.
# ;mute-replay-warnings
# SSL/TLS parms.
# See the server config file for more
# description. It's best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
ca /etc/openvpn/ca_openvpn.crt
cert /etc/openvpn/client_openvpn.crt
key /etc/openvpn/client_openvpn.key
auth-user-pass /etc/openvpn/pass.txt
# Verify server certificate by checking that the
# certificate has the correct key usage set.
# This is an important precaution to protect against
# a potential attack discussed here:
# - /etc/openvpn/client.ovpn 96/131 73%
```

■ **Contact Window and File Link:**

If you have any questions, please contact Stanley.Huang #6035