OpenVPN client configuration for Windows Systems

ONCELL G3150A-LTE

Shayne Harris

ECS LTD Hamilton, New Zealand

Intended Audience

This guide assumes that the reader is familiar with the basics of IP addresses, cellular networks and the concepts of VPN and private networks.

OpenVPN Types

This guide is specifically written for the software OpenVPN client, that resides on Windows, and terminates to a Moxa OnCell G3150A-LTE device. There are several different scenarios that the G3150A-LTE can support, however those topics are beyond the scope of this guide. (Once built, the **ovpnclient.ovpn** file can be sent to an iOS device, once the OpenVPN client application is installed, the remote network can be access from your iOS device!)

Additionally, OpenVPN can be configured to TAP & TUN modes. TAP mode, is ethernet bridging and is not discussed in this guide. TUN is IP routing, this is what we will be configuring.

A note on networks and routing.

There are many ways networks can be configured, and it is impossible to be aware of each nuance when writing this guide. I will refer to the network that the G3150A is installed at, to be the **remote** network, the network you are controlling from will be the **local** network. When OpenVPN is running, it creates a route in the Windows routing table, a route instructs Windows to send packets destined for a network, out the correct interface (in this case, the OpenVPN interface). It is best practice, for the remote network e.g. 192.168.127.0 /24 to be unique from your local network e.g.: 10.10.100.0 /24. Windows will choose by default, the shortest path to a given network, so if your local network and the remote network are on the same subnet – Windows will not route to the remote network (because logically it is local).

So, when designing your remote locations, be sure to choose a unique network, e.g. 192.168.254.0 /24 or 192.168.133.0 /24 etc… that is not used by your or your customer, local networks.

Typical Setup

Moxa G3150A-LTE – OpenVPN Server to OpenVPN Client Configuration.

Pre-requisites

- An account with DynDns (or similar provider) is mandatory. Please setup your login credentials and hostname before attempting this guide.
- A working SIM card, with credit, and the correct APN to allow the G3150A-LTE to be publicly accessed.
- The G3150A-LTE, OpenVPN client scripts and driver package.
- DO NOT change the default export file names for the certificates and .ovpn configuration file.

Pre-installation of the OpenVPN Client (Windows 7 or greater)

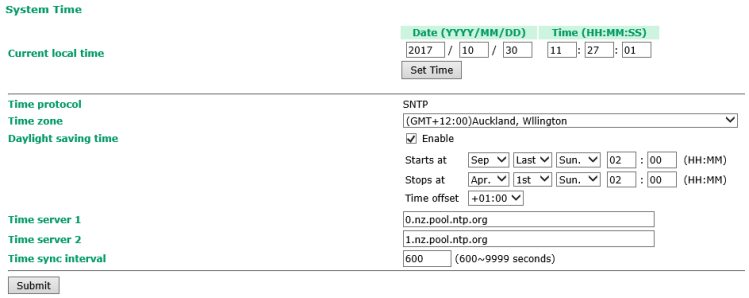
- Unzip the OpenVPN scripts folder to My Documents.
- Open an administrator command prompt or, administrator PowerShell session.
- Change to where the scripts folder is located. **cd c:\users\moxa\Documents\OpenVPN_Scripts**
- Execute the scripts in this order:
  1) **1_Install_OpenVPN_v1.vbs** *[detects 32bit/64bit OS and installs correct version)*
  2) **2_Create_Auth_File.vbs** *[prompts for the username/password for authorised OpenVPN server clients - saves entering credentials each time) - please retain for the steps further down.*
  3) **3_OpenVPN_ChangeAdapterName.vbs** *[TAP OpenVPN looks for the Windows ethernet adapter by name - this ensures consistency, only used in TAP mode.]*
  4) **4_Install_OpenSSL.vbs** *[Installs OpenSSL certificate tools]*
  5) Exit the command prompt.

OpenVPN must be installed and run with Administrator privileges.
This is because the OpenVPN server 'pushes' routes to Windows.
Windows requires Administrator privileges to add or modify routes.

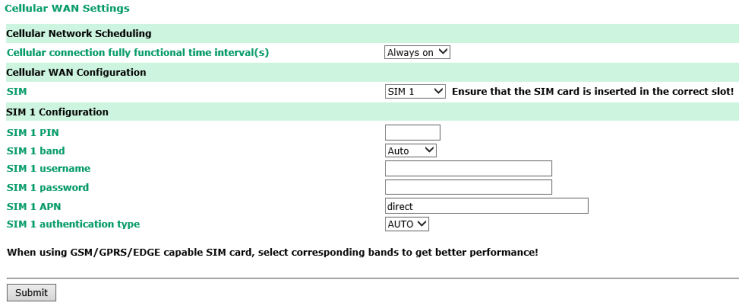
G3150A-LTE Setup

- Login using the web console (default IP : 192.168.127.254, Username: admin, Password: moxa)

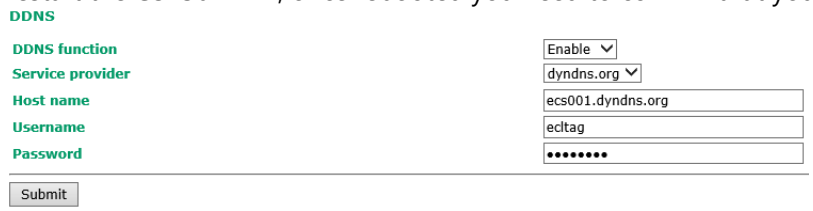
- **General Setup/System Time** - Setup the time and location and daylight savings. This is a crucial step, *OpenVPN will disconnect with large time differences*. Additionally, the SSL certificates will have the wrong date and/or time – making connections impossible. Once set, restart the G3150A and check the time again, if necessary re-adjust the time save and reset. (The time can advance when daylight saving is set).



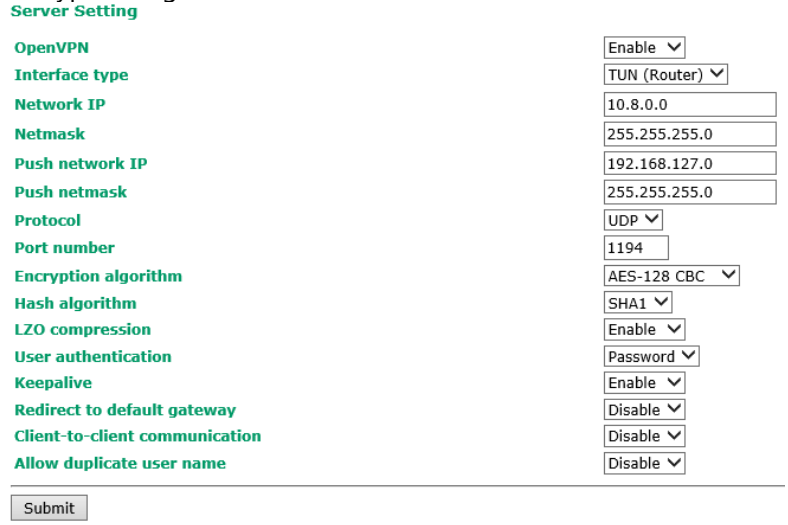
- **Cellular Settings/Cellular WAN Settings -** Set the APN according to your service provider. The Username, Password and PIN are dependent on the carrier.



- **Advanced Setup/DDNS -** Enable the service, set the provider, hostname, username & password. e.g. DynDNS, moxa001.dyndns.org, myusername, mypassword. At this stage, it would be prudent to save and restart the G3150A-LTE, once rebooted you need to confirm that you can ping the DDNS hostname.

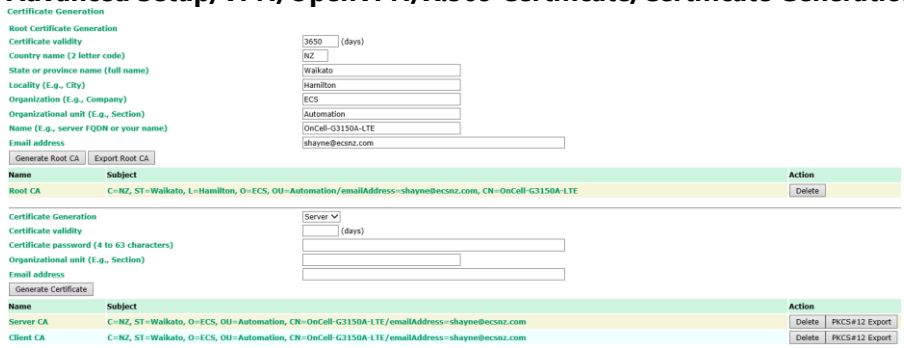


- **Advanced Setup/VPN/OpenVPN/Server Settings/Server Setting** - Enable the service, change the Encryption Algorithm to AES-128-CBC, otherwise leave the default settings.



- Create a temporary folder called temp-certificates, on your computer somewhere.

- **Advanced Setup/VPN/OpenVPN/X.509 Certificate/Certificate Generation**



- Click Generate Root CA

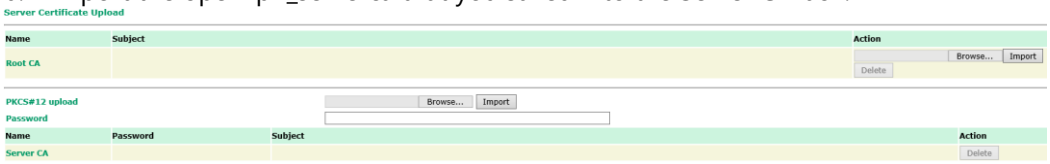
- Export the Root CA just made, to the temp-certificates folder above.

- In the section below, generate both a Server & Client certificate using the same defaults as the Root Certificate Generation. Enter a password to encrypt the file *(remember this password for later)*

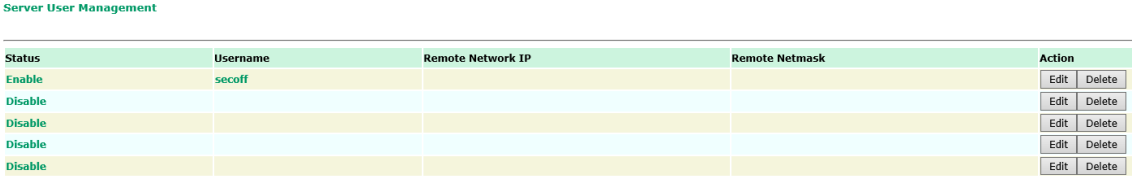
- Export both these certificates to the temp-certificates folder using the two PKCS#12 Export buttons.

- Save and restart the G3150A-LTE.

- **Advanced Setup/VPN/OpenVPN/Server Settings/Server Certificate**
    a. Import the openvpn_rootca that you saved into the Root CA box.
    b. Import the openvpn_serverca that you saved into the Server CA box.



- **Advanced Setup/VPN/OpenVPN/Server Settings/Server User Managements**
create a user here to access the OpenVPN network. (use identical credentials as step 3 when creating the credentials file above.)



- **Advanced Setup/VPN/OpenVPN/Server Settings/Server to User Config –** Export the configuration to the temp-certificates folder.

- Save & restart the G150A-LTE

OpenSSL certificate steps.

- Copy the ovpn_clientca.p12 certificate from temp-certificates to: **C:\Program Files\OpenVPN\certificates** - this requires Administrator privileges.
- Open an Administrator command prompt or PowerShell command prompt.
- Change directory to OpenSSL: **cd "C:\Program Files (x86)\GnuWin32\bin"**
- Enter these two commands:

.\openssl.exe pkcs12 -in "C:\Program Files\OpenVPN\certificates\ovpn_clientca.p12" -out "C:\Program Files\OpenVPN\certificates\ovpn_clientca_certificate.pem"

.\openssl.exe pkcs12 -in "C:\Program Files\OpenVPN\certificates\ovpn_clientca.p12" -out "C:\Program Files\OpenVPN\certificates\ovpn_clientca_private_key.pem" -nodes -nocerts

- *(You will be prompted for the certificate password 4 times in total, 3 for the first cert, 1 for the second)*

Client OVPN config file step.

- Copy the *ovpnclient.ovpn* config file from temp-certificates to: **C:\Program Files\OpenVPN\config\ -** this requires Administrator privileges.

- Open an administrator command prompt or, administrator PowerShell session.

- Change to where the scripts folder is located. **cd c:\users\moxa\Documents\OpenVPN_Scripts**

- Execute script: **5_Append_Client_Cert_PKey_To_Config.vbs** – when prompted, please enter the hostname for the G3150A-LTE **eg: remote.moxa.com** and press enter.

Summary

You should now have everything ready to test your OpenVPN configuration.
Save and restart the G3150A-LTE, unplug your PC from the ethernet port.
Wait a couple minutes and ping the hostname – then start the OpenVPN connection. When successfully connected the OpenVPN client icon will go green.