HTTPS VPN Server & Client Quick Start Guide

Rev B
January, 2019

All Rights Reserved

Table of Content

List of Figures

1. Introduction

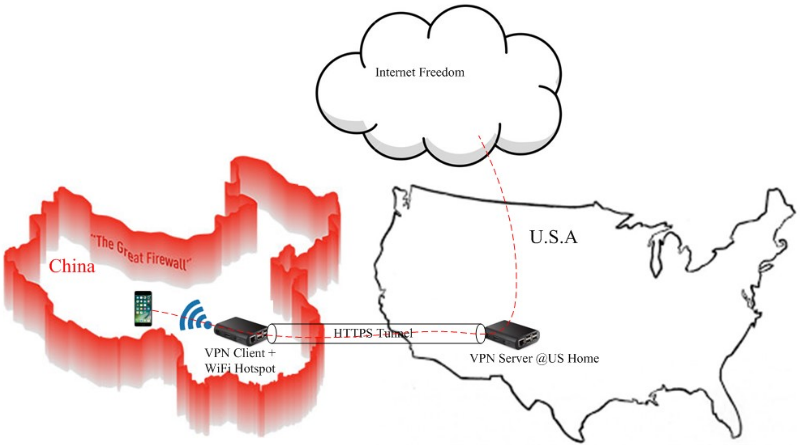


Figure 1 How HTTPS VPN works

How It Works

- Plug in HTTPS VPN server at your router at home.
- Bring the HTTPS VPN client device with you when you travel to China.
- Simply connect your smart phone / PC to the WiFi hotspot created by the HTTPS VPN client device.
- All smart phone/PC traffic would be encrypted in HTTPS format and forwarded to VPN server in US home which access internet for you.

For questions, comments, supports, please contact us by email.
vpn.everyone@gmail.com

1.1. Connect HTTPS VPN Device to Wireless Router

1) Connect VPN server to wireless router by Ethernet cable
2) Connect USB cable to power up VPN server (Figure 2)

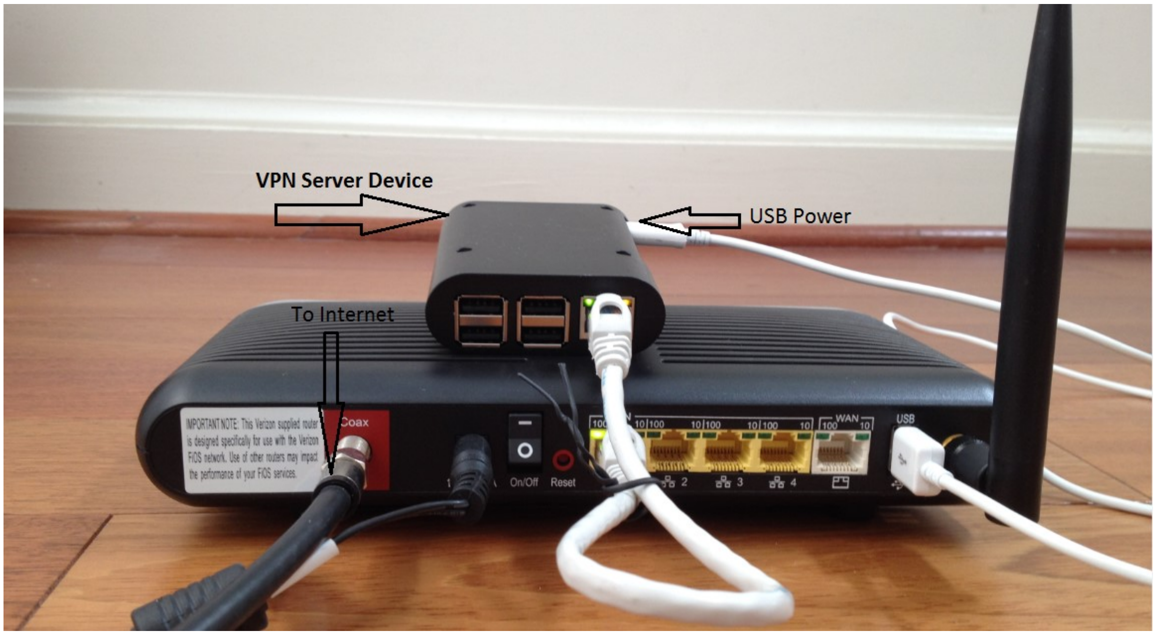


Figure 2 Connect VPN Server to Wireless Router

Most wireless routers come with a USB interface. This USB interface on your wireless router can provide enough power for the VPN server. Connect VPN server to your router by USB data sync cable (Figure 2).

NOTE:
The figure above is for ***wiring*** illustration purpose**.** Do NOT put VPN server on top (or close to the grill) of your router. Otherwise, the heat generated by your router may drive VPN server to overheat.

Note 1: Ethernet cable is an optional accessory.

Note 2: USB data sync cable is an optional accessory. Please re-use your USB cable for your old Android phones. Nowadays, every household has one or more retired Android phones, therefore USB cables. To save environment, we don't ship USB cables.

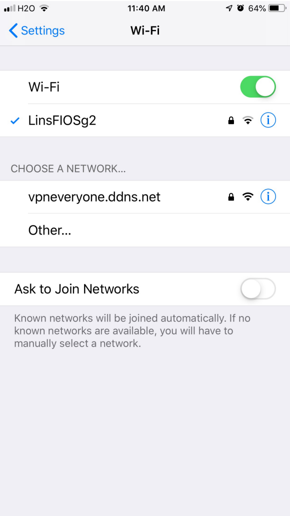
Note 3: The software only runs on the MicroSD card shipped.

Tip: Each VPN server device is pre-configured with default shared-key and a set of user&password. The device can be plug-n-play. We suggest that you try the default VPN setting first. Make sure your VPN client works well with default server configuration first.

2. Access VPN Device Configuration Web UI

2.1. Access Web UI by Built-in WiFi Hotspot

Your VPN device may be equipped with a short-range WiFi hotspot. Go to your iPhone WiFi setting screen. If you see "*vpneveryone.ddns.net*" in your network list, tap it to connect. The default password is *00000000*



Wi-Fi

✓ LinsFIOSg2

CHOOSE A NETWORK...

vpneveryone.ddns.net

Other...

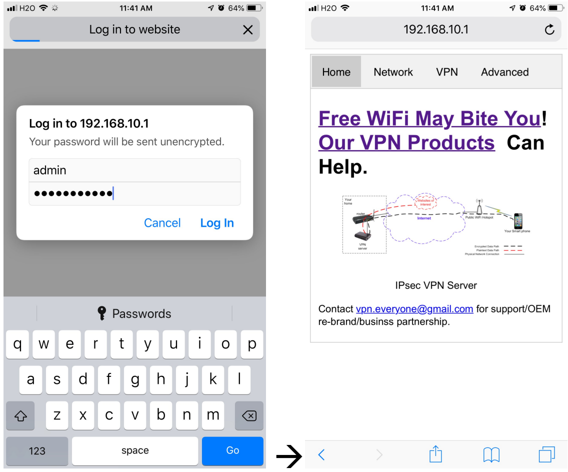
Ask to Join Networks

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

Figure 3 Find vpneveryone.ddns.net WiFi hotspot

Note: The hotspot may complain about incorrect password. It may take up to 3 times to connect the WiFi hotspot. That is by design to avoid hacker guessing WiFi password.

After your iPhone successfully connects to "vpneveryone.ddns.net" WiFi hotspot, start web browser to access http://192.168.10.1 web page. Use "admin" & "vpneveryone" without quote sign as username and password to login to VPN device web UI.



Log in to 192.168.10.1

Your password will be sent unencrypted.

admin

•••••••••••

Cancel Log In

Free WiFi May Bite You! Our VPN Products Can Help.

IPsec VPN Server

Contact vpn.everyone@gmail.com for support/OEM re-brand/businss partnership.

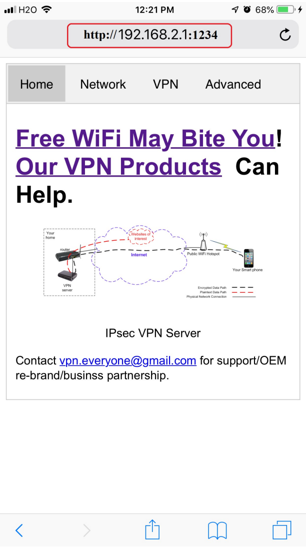
Figure 4 Access VPN Device Web UI by Built-in WiFi Hotspot

Note: The WiFi hotspot from VPN server is for convenience for out-of-box configuration. It is never meant to replace your regular WiFi at home. After you finish configuring your VPN settings, you may disable hotspot to avoid WiFi interference to your regular WiFi. You can always configure VPN server by VPN server IP directly. See below.

2.2. Access Web UI by http://Router IP:1234

If your VPN server is not equipped with WiFi hotspot or you are out of range, your iPhone can connect to your own wireless router where VPN server is attached. Then use your router IP with port 1234 to access VPN server web GUI.

Assume that your wireless router IP address 192.168.2.1. Open the Safari web browser, use http://192.168.2.1:1234 to access the web page on VPN device.



Free WiFi May Bite You! Our VPN Products Can Help.

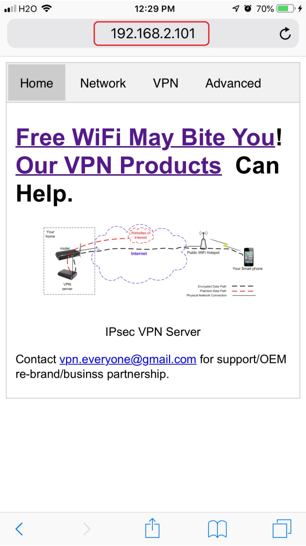
IPsec VPN Server

Contact vpn.everyone@gmail.com for support/OEM re-brand/businss partnership.

Figure 5 Access VPN Server Web UI by Router IP:1234

2.3. Access Web UI by VPN Server IP

Some router models don't support LAN port forwarding. In this case, http://routerip:1234 will not work. You will have to login to your router to find out what IP address is allocated to the VPN server (e.g. 192.168.2.101). Then use that IP address (http://192.168.2.101) to access VPN device web page.



Free WiFi May Bite You! Our VPN Products Can Help.

IPsec VPN Server

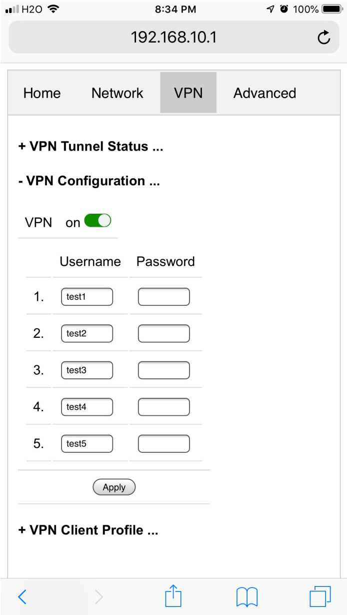
Contact vpn.everyone@gmail.com for support/OEM re-brand/businss partnership.

Figure 6 Access VPN Server Web UI by VPN server IP

3. Change Default Configuration on HTTPS VPN Server

Tip: Each server device is pre-configured with a set of shared-key and password. The device can be plug-n-play. We suggest that you try the default VPN setting first. Make sure your VPN client works with default server configuration first.

In case you want to pick your own username and password, here is the detail procedure.



+ VPN Tunnel Status ...

- VPN Configuration ...

VPN on

	Username	Password
1.	test1	
2.	test2	
3.	test3	
4.	test4	
5.	test5	

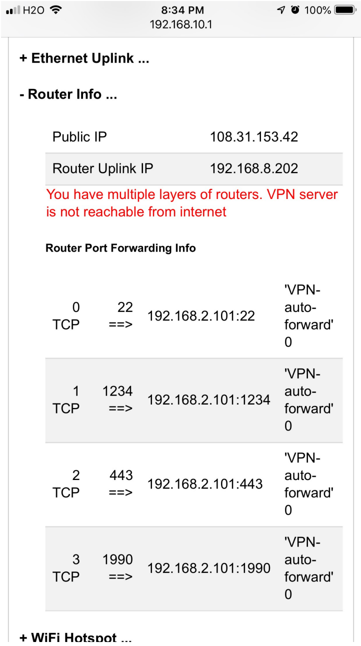
+ VPN Client Profile ...

Figure 7 HTTPS VPN Server Configuration UI

- Login to VPN server web UI.
- Click “VPN” tab
- Click “VPN Configuration”
- Enter 5 pairs of Username & password
- Click Apply

That’s it! Isn’t that easy? You don’t need to understand anything about VPN.

On HTTPS VPN server device web UI, click ***Network*** tab. Then click ***+ Router Info …*** You will see the public IP which is needed to configure HTTPS VPN client device.



+ Ethernet Uplink ...

- Router Info ...

Public IP	108.31.153.42
Router Uplink IP	192.168.8.202

You have multiple layers of routers. VPN server is not reachable from internet

Router Port Forwarding Info

0 TCP	22 ==>	192.168.2.101:22	'VPN-auto-forward' 0
1 TCP	1234 ==>	192.168.2.101:1234	'VPN-auto-forward' 0
2 TCP	443 ==>	192.168.2.101:443	'VPN-auto-forward' 0
3 TCP	1990 ==>	192.168.2.101:1990	'VPN-auto-forward' 0

+ WiFi Hotspot ...

Figure 8 Public IP of HTTPS VPN Server

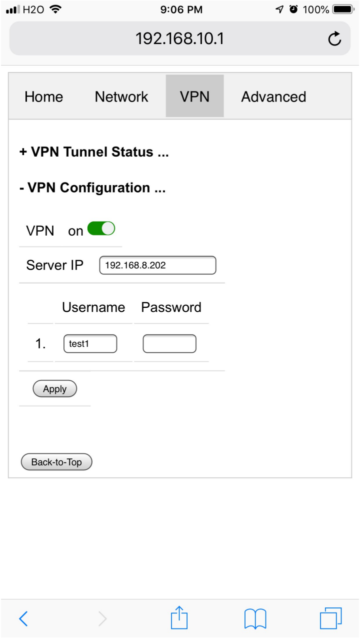
4. Configure HTTPS VPN Client Device

Configuring HTTPS VPN client device is very similar to configuring the server device except for the following.

a. You need the VPN server IP
b. You only need one username & password pair.

HTTPS-VPN client device always comes with WiFi hotspot. Connect to its WiFi hotspot to access device web UI.

- Login to VPN server web UI.
- Click "***VPN***" tab
- Click ***"+VPN Configuration …"***
- Click to enable VPN
- Enter HTTPS-VPN server public IP (Figure 8)
- Enter Username & password
- Click Apply



+ VPN Tunnel Status ...

- VPN Configuration ...

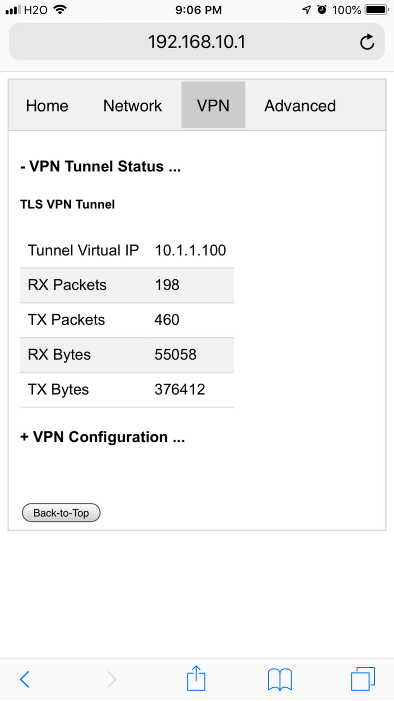
VPN on

Server IP 192.168.8.202

	Username	Password
1.	test1	

Figure 9 HTTPS-VPN Client Configuration

The HTTPS-VPN client device should connect to server shortly. Click ***<u>+ VPN Tunnel Status …</u>*** to check the status.



- VPN Tunnel Status ...

TLS VPN Tunnel

Tunnel Virtual IP	10.1.1.100
RX Packets	198
TX Packets	460
RX Bytes	55058
TX Bytes	376412

+ VPN Configuration ...

Figure 10 HTTPS-VPN Client Device VPN Status

Now you can take HTTPS-VPN client device with you when you travel overseas. Just plug it in any network that has internet access. The HTTPS-VPN tunnel should be automatically created on power up. All traffic to/from WiFi hotspot of the HTTPS-VPN client device will route to/from this HTTPS-VPN tunnel.

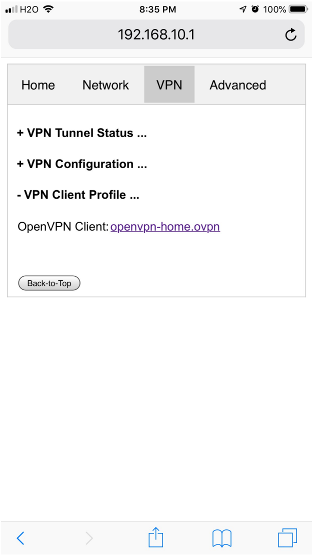
5. Configure OpenVPN VPN Clients

The HTTPS-VPN server supports OpenVPN protocol, too. One of the 5 users is used for HTTPS-VPN client device w/ WiFi. You can use the rest 4 users for OpenVPN clients. This section shows you how to configure OpenVPN clients. It is super easy. In one sentence, import in your device, the OpenVpn configuration file generated by HTTPS-VPN server.

5.1. Configure TLS VPN Client on Windows 7 PC

The commercial of-the-shelf free **OpenVPN client** can be used to create TLS VPN tunnel to TLS VPN server. Google "openvpn download" to find the software and install it on your PC.

VPN server prepares the OpenVPN configuration file. You can download it from web UI page. Click ***VPN*** tab. Then click ***+VPN Client Profile …***



+ VPN Tunnel Status ...

+ VPN Configuration ...

- VPN Client Profile ...

OpenVPN Client: openvpn-home.ovpn

Figure 11 OpenVPN Client Configuration Prepared by VPN Server

Right click openvpn-home.ovpn link and save it at OpenVPN configuration directory ***C:\Program Files\OpenVPN\config\.***

Note 1: C:\Program Files\OpenVPN\config\ may need administrator privilege to save file.
Note 2: This openvpn-home.ovpn file is good for OpenVPN clients of all platforms (Windows, iOS, Android, MacBook)

1. From windows start menu, find "OpenVPN GUI" icon. Right click it and click "Run as administrator". (Figure 12).

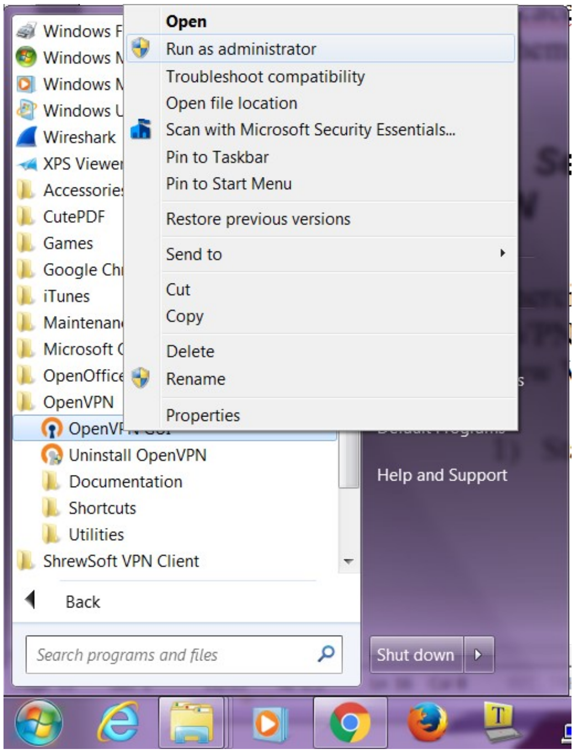


Figure 12 Run OpenVPN GUI as administrator

2. There will be an icon that looks like a lock at bottom right corner of screen. (Figure 13)

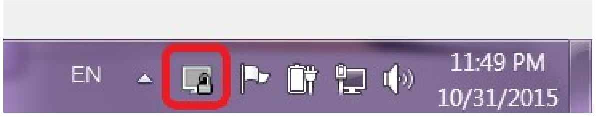


Figure 13 OpenVPN Icon in Task Bar

3. Right click on this lock-like icon and click “connect” on the menu. You will be asked for user name and password. Use one of the users you created on VPN server.

   The factory default user is “**test1**” with password “**vpneveryone**” (without quote sign)

   In a short moment, OpenVPN successfully creates VPN tunnel and assign the PC a virtual IP.

   Now all your internet access will be through this OpenVPN tunnel.

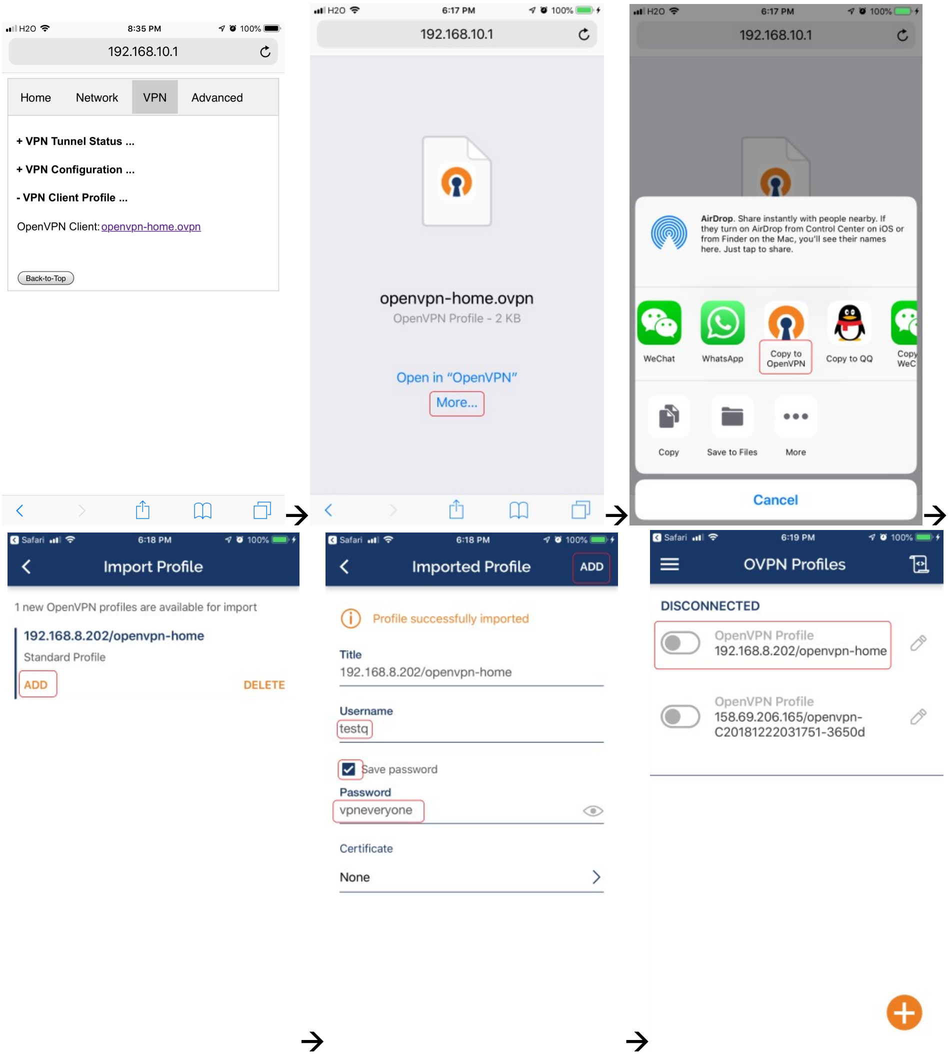
5.2. Configure TLS VPN Client on iOS

First you need to install OpenVPN app on your iPhone/iPad.

After that, use your iPhone/iPad to access VPN server web UI.

- Tap ***VPN*** tab.

- Then tap ***+VPN Client Profile ….***
- Then tap openvpn-home.ovpn link.
- Then follow red marks in the screenshots below



Title: 192.168.8.202/openvpn-home

Username: testq

☑ Save password

Password: vpneveryone

Certificate: None

OpenVPN Profile 192.168.8.202/openvpn-home

OpenVPN Profile 158.69.206.165/openvpn-C20181222031751-3650d

Figure 14 OpenVPN iPhone Client Screenshots

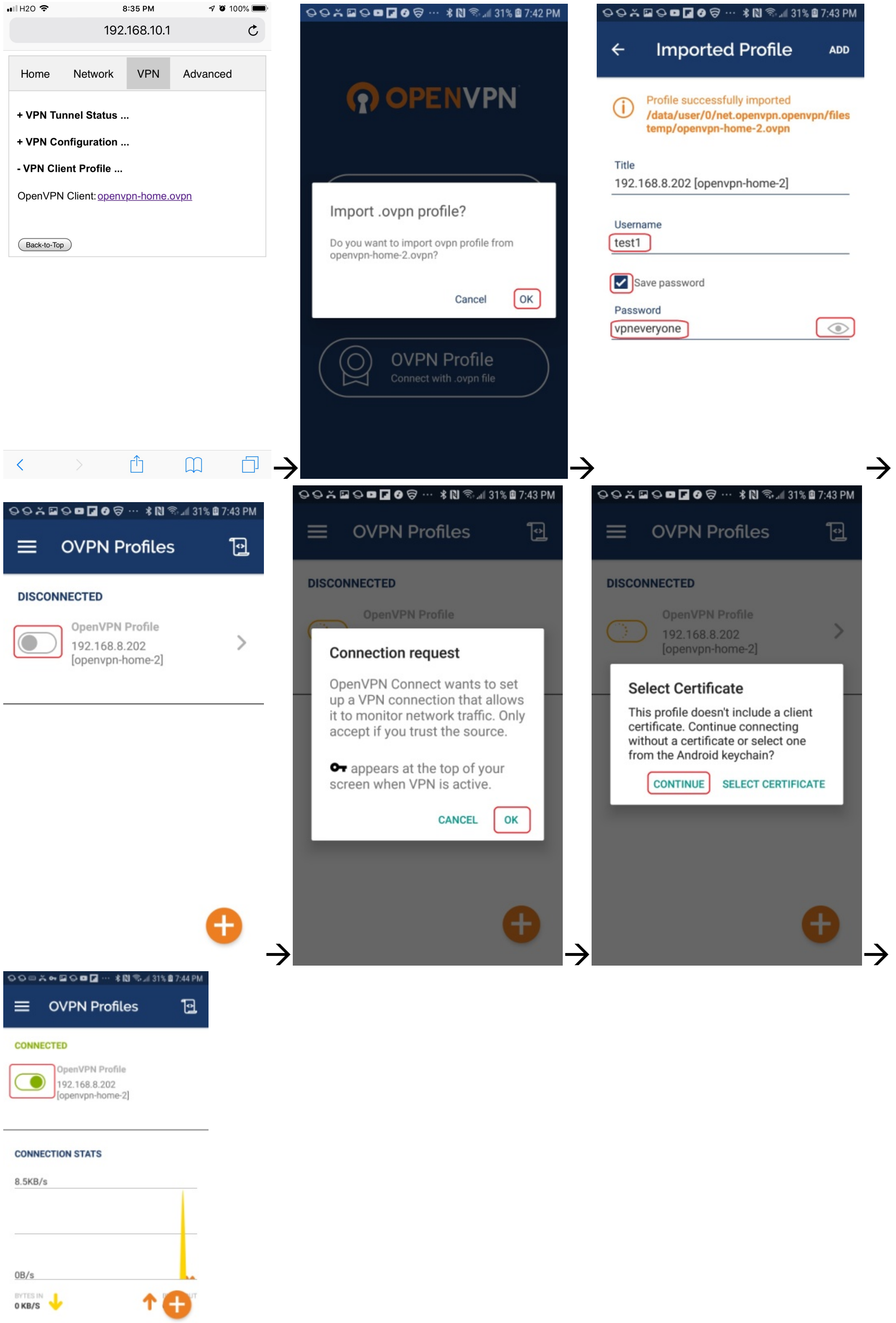
Note: Use the right username & password you set on HTTP server.

5.3. Configure TLS VPN Client on Android

It is pretty much the same as TLS VPN client setup in iOS.

First you need to install OpenVPN on Android phone/tablet.
After that, use your Android device to access VPN server web UI.

- Tap ***VPN*** tab.
- Then tap ***+VPN Client Profile ….***
- Then tap openvpn-home.ovpn link.
- Then follow red marks in the screenshots below



192.168.10.1

Home Network VPN Advanced

+ VPN Tunnel Status ...

+ VPN Configuration ...

- VPN Client Profile ...

OpenVPN Client: openvpn-home.ovpn

Back-to-Top

Import .ovpn profile?

Do you want to import ovpn profile from openvpn-home-2.ovpn?

Cancel OK

OVPN Profile
Connect with .ovpn file

Imported Profile ADD

Profile successfully imported /data/user/0/net.openvpn.openvpn/files temp/openvpn-home-2.ovpn

Title: 192.168.8.202 [openvpn-home-2]

Username: test1

☑ Save password

Password: vpneveryone

OVPN Profiles

DISCONNECTED

OpenVPN Profile
192.168.8.202 [openvpn-home-2]

Connection request

OpenVPN Connect wants to set up a VPN connection that allows it to monitor network traffic. Only accept if you trust the source.

appears at the top of your screen when VPN is active.

CANCEL OK

Select Certificate

This profile doesn't include a client certificate. Continue connecting without a certificate or select one from the Android keychain?

CONTINUE SELECT CERTIFICATE

CONNECTED

OpenVPN Profile
192.168.8.202 [openvpn-home-2]

CONNECTION STATS

Figure 15 Android OpenVPN Client Setup Screenshots

5.4. Configure TLS VPN Client on MacBook

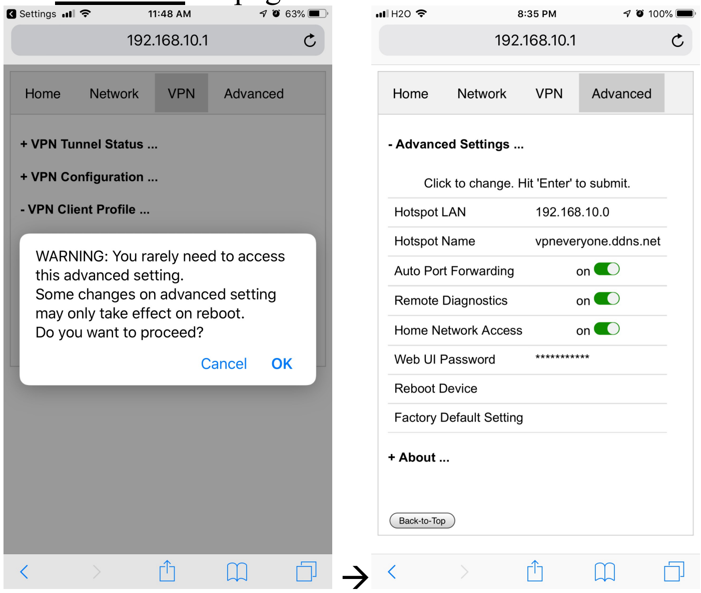
Download the Tunnelblick disk image file (a ".dmg" file) from https://tunnelblick.net

Tunnelblick is the popular OpenVPN client.
After installing tunnelblick, run it.
Download openvpn-home.ovpn prepared by VPN server device
Drag openvpn-home.ovpn to tunnelblick app. That's it!

6. Advanced Settings

Note: In very rare case that you will need to change advanced settings. If you are not very comfortable with computer networking, leave the setting as is.

After you login to the VPN server web UI, click ***Advanced*** tab to see the UI below. You can click ***OK*** to enter ***Advanced*** UI page.



WARNING: You rarely need to access this advanced setting.
Some changes on advanced setting may only take effect on reboot.
Do you want to proceed?

Click to change. Hit 'Enter' to submit.

Hotspot LAN	192.168.10.0
Hotspot Name	vpneveryone.ddns.net
Auto Port Forwarding	on
Remote Diagnostics	on
Home Network Access	on
Web UI Password	***********
Reboot Device	
Factory Default Setting	

Figure 16 VPN Device Advanced Settings

Each item except for ***Web UI Password*** on this Advanced UI is independent and will take effect on change.

1) **Hotspot LAN**

   Only when the router LAN happens to be 192.168.10.0, will you need to change hotspot LAN network.
   To change it, click the IP ***192.168.10.0***. Then the ***10*** part becomes editable. Enter any value between 0~254 and hit enter to change.

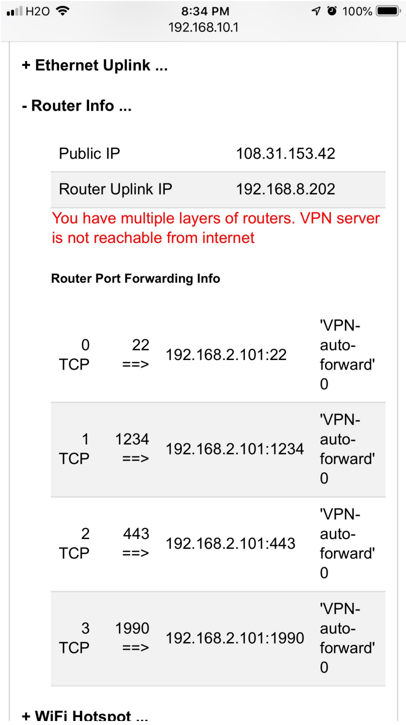
2) **Hotspot Name**

   The default hotspot network name "vpneveryone.ddns.net" should be unique enough identify itself. If you want to change it, click it. Then it becomes editable. Enter whatever name you like and hit enter to change.

3) Auto Port Forwarding

In order for VPN server to be reachable from internet, your router needs to forward a few ports to VPN server. This is done automatically by VPN server telling router to do port forwarding. You should never disable it.

If you have to disable this feature for whatever reason, you will have to set up your router to manually forward ports below to VPN server.



H2O 8:34 PM 100%
192.168.10.1

+ Ethernet Uplink ...

- Router Info ...

Public IP	108.31.153.42
Router Uplink IP	192.168.8.202

You have multiple layers of routers. VPN server is not reachable from internet

Router Port Forwarding Info

0 TCP	22 ==>	192.168.2.101:22	'VPN-auto-forward' 0
1 TCP	1234 ==>	192.168.2.101:1234	'VPN-auto-forward' 0
2 TCP	443 ==>	192.168.2.101:443	'VPN-auto-forward' 0
3 TCP	1990 ==>	192.168.2.101:1990	'VPN-auto-forward' 0

+ WiFi Hotspot ...

Figure 17 Router Port Forwarding Info

4) Remote Diagnostics

In case that you need remote help on troubleshooting VPN server, we may run diagnostics tools which use TCP port 22.

Disabling Remote Diagnostics only tell VPN server not to tell router to auto forward port 22 to VPN server.

5) Home Network Access

http://vpneveryone.ddns.net/reasons-for-vpn.html

One of the key use cases to VPN is to access home network. In some cases, you may not want VPN users to access home network at all. For example, you let your friends at oversea to use your VPN to access internet websites that are blocked by his country. You want your friends to access internet only, and disable his access to your home network.

In this case, you can turn off ***Home Network Access***.

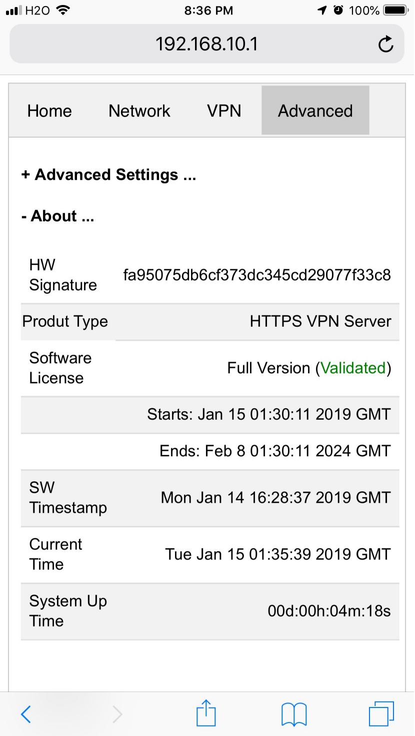
6) **Web UI Password**
By default, web UI password is vpneveryone
Although the VPN server web UI is not accessible from internet, you may not want everyone to know your VPN server UI password. You can change it. Click the ******. It will become editable. Enter your password and hit enter to change it.
Note: New UI password only take effect on next boot.

7) **Reboot Device**

In rare cases, you will need to reboot VPN server by web UI. If you are at home, power cycle VPN server device would be a better way to reboot it.

8) **Factory Default Setting**
Only when you think you don't know what you did and broke everything, should you do a factory default setting.

6.1. About Product



+ Advanced Settings ...

- About ...

HW Signature	fa95075db6cf373dc345cd29077f33c8
Produt Type	HTTPS VPN Server
Software License	Full Version (Validated)
	Starts: Jan 15 01:30:11 2019 GMT
	Ends: Feb 8 01:30:11 2024 GMT
SW Timestamp	Mon Jan 14 16:28:37 2019 GMT
Current Time	Tue Jan 15 01:35:39 2019 GMT
System Up Time	00d:00h:04m:18s

Figure 18 Product Info

Each VPN device runs the software programmed in the MicroSD card. The software is only licensed to run on the MicroSD card shipped.
For full version product, the software is ***licensed for 5 years***.

For trial/free version software image, it is only licensed for 30 days (subject to change without notice).

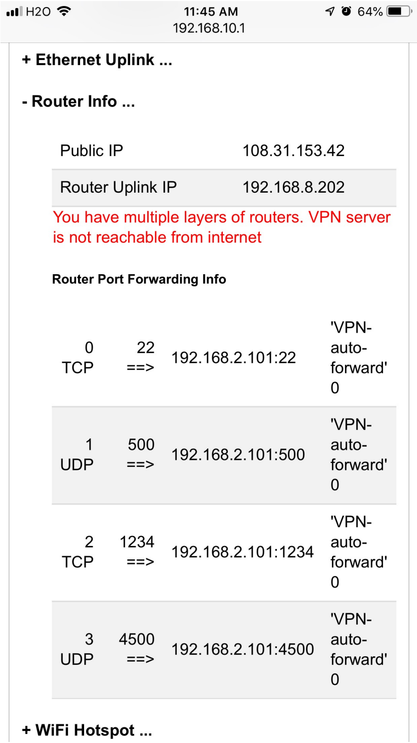
The **About** section in **Advanced** tab tells the license info. After software license expires, you still have access to web UI. But the VPN service is automatically shut down.

7. Quick Troubleshoot

1) Make sure you don't have multiple layers of router cascaded.

VPN server can only tell the router directly connected to auto forward ports. If you have multiple layers of router cascaded, the VPN server is not reachable from internet. Therefore, it will never work.

The ***Router Info*** section on ***Network*** web UI page (Figure 19 below) will help you. If the ***Public IP*** does not match the ***Router Uplink IP***, it means you have multiple-layer router problem.



192.168.10.1

+ Ethernet Uplink ...

- Router Info ...

Public IP	108.31.153.42
Router Uplink IP	192.168.8.202

You have multiple layers of routers. VPN server is not reachable from internet

Router Port Forwarding Info

0 TCP	22 ==>	192.168.2.101:22	'VPN-auto-forward' 0
1 UDP	500 ==>	192.168.2.101:500	'VPN-auto-forward' 0
2 TCP	1234 ==>	192.168.2.101:1234	'VPN-auto-forward' 0
3 UDP	4500 ==>	192.168.2.101:4500	'VPN-auto-forward' 0

+ WiFi Hotspot ...

Figure 19 Router Info UI Page

2) Make sure router port forwarding works correctly

99.99% of residential routers support UPNP and it is by default enabled. The auto port forwarding should work by default.
If you see port forwarding info like Figure 19, you are good.

If you had disabled UPNP on your router, you need to enable it. Or manually forward ports like in Figure 19

If you router have ***UPNP secure version*** enabled, it may not work well with VPN server. Please disable security on UPNP and run regular version UPNP.

3) Please be noted that all keys/passwords/usernames are case sensitive. “Password” is not the same as “password”