# IPsec VPN Server User's Guide

Rev E
January, 2019

# Table of Content

# List of Figures

# 1. Introduction

This IPsec VPN Server is designed to enforce the strongest security level while very easy to use. The goal is to help those not-so-tech-savvy users to use internet securely while on the go. With easy-to-use in mind, the complicated VPN security settings are automatically configured. User only needs to configure/change keys and passwords. This VPN server can be plug-n-play out of box if you don't mind using factory default keys and passwords.

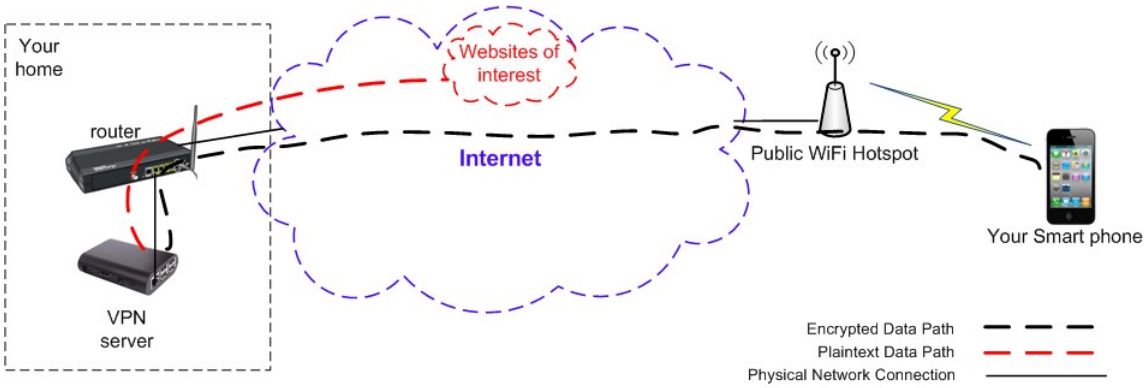


**Figure 1 Overall VPN Working Model**

## How It Works

- Plug in this IPsec VPN server to your wireless router at home.
- Configure VPN client on your smart phones or PC on the go.
- All traffic from your smart phones or PC on the go will be encrypted and sent to VPN server which decrypts the traffic and accesses the internet for your smart phone. The return traffic is then encrypted by VPN server before it sends to your smart phone.

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

## 2. Connect VPN Server to Wireless Router

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

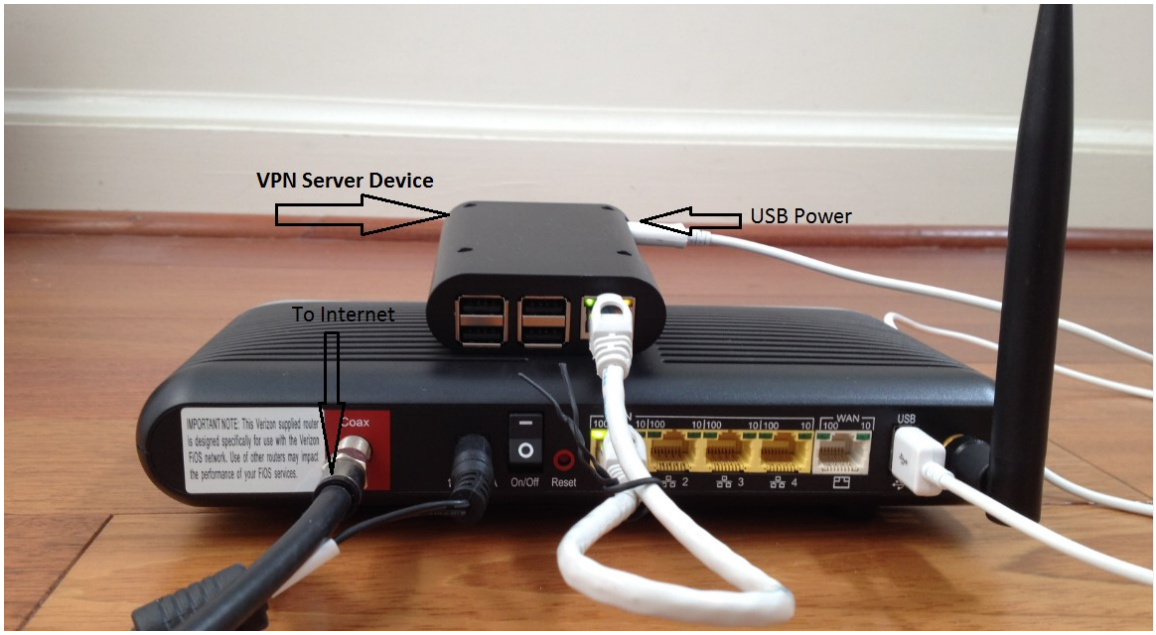


**Figure 2 Connect VPN Server to Wireless Router**

**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 VPN server 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.

# 3. Access VPN Server Configuration Web UI

## *3.1. 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*

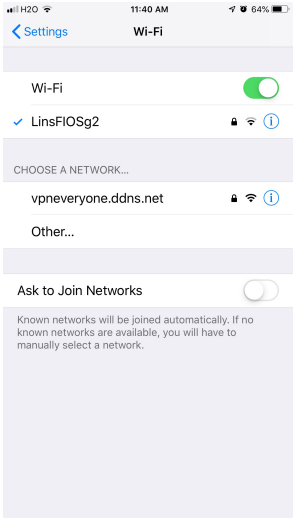


**Figure 3 Find vpneveryone.ddns.net WiFi hotspot**

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 server web UI.

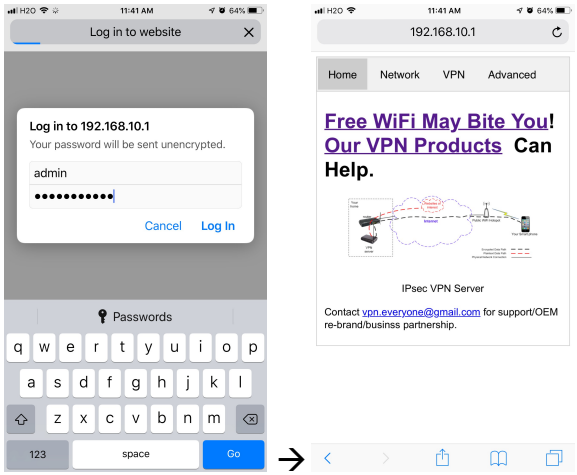

**Figure 4 Access VPN Server Web UI by Built-in WiFi Hotspot**

**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.

## 3.2. 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.


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

## 3.3. Access Web UI by VPN Server IP

Some router models don't support internal 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.


**Figure 6 Access VPN Server Web UI by VPN server IP**

# 4. Configure VPN Client on Smart Phone

## 4.1. Configure VPN Client on iPhone

This procedure is based iOS 9.0 or later. The VPN server automatically generates a few "*.mobileconfig*" profile for iOS. This profile is available on the download web page on VPN server device.

After you successfully login to VPN server Web UI, click "VPN" tab on the screen top. Then click **+VPN Client Profile …** on the screen bottom

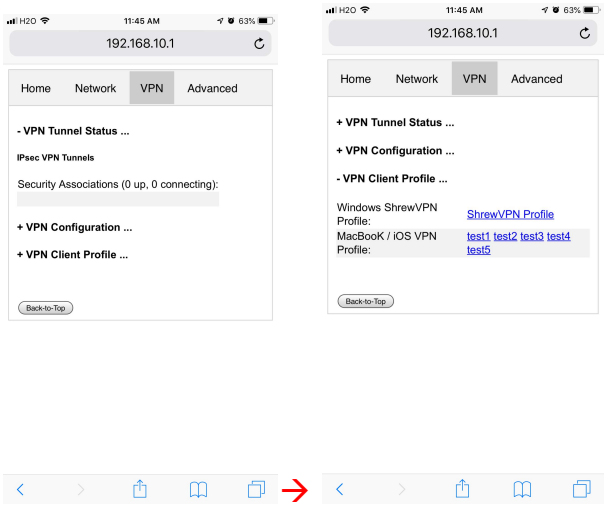


**Figure 7 Access VPN Client Profile Prepared by VPN Server**

Tap one of the 5* links (test1, …, test5) on the screen bottom. Follow what iOS device says to install the VPN profile. The screenshots are like below.

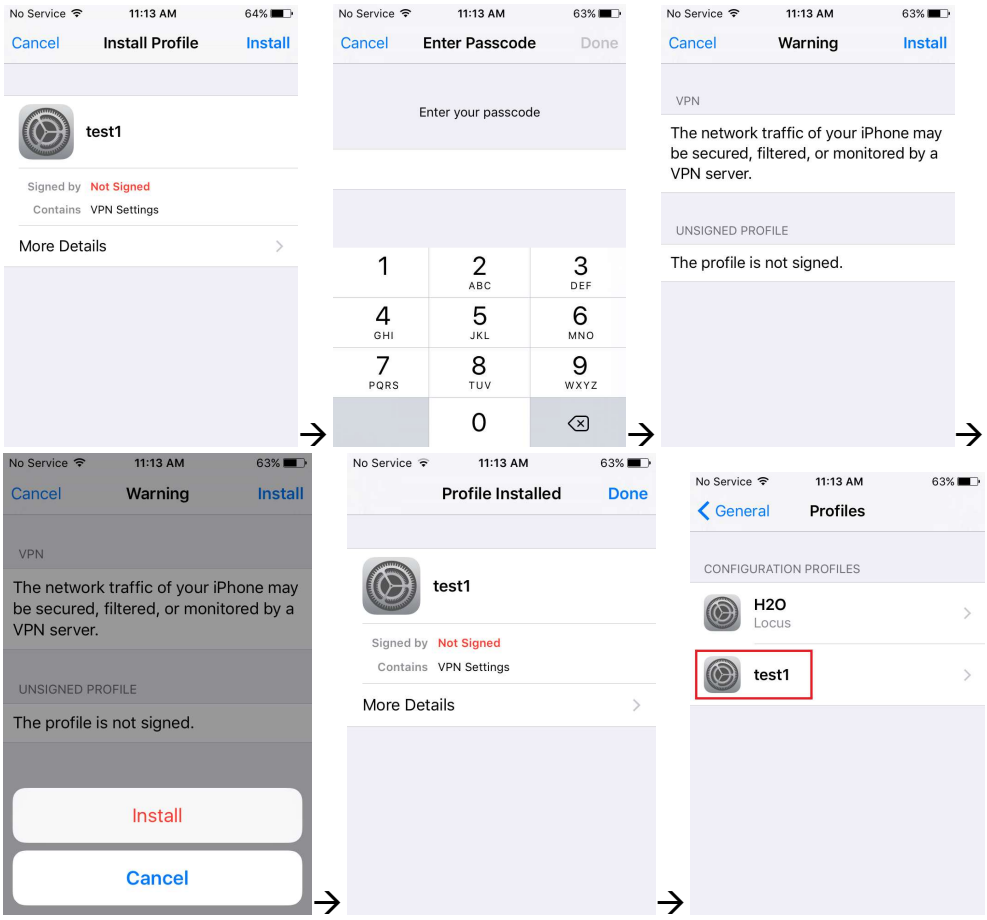


**Figure 8 iPhone Screenhots of Installing VPN profile**

### 4.1.1. Test Your iPhone VPN Client

**Note**: You cannot test VPN connection from the same LAN where VPN server is. You need to use your smart phone data plan to test VPN. Or use your neighbor's WiFi if they give you guest access.

To connect VPN, go to iPhone "Settings", slide the button beside the "VPN". Or go to iPhone "Settings" → "General" → "VPN", slide the button beside the "Status"

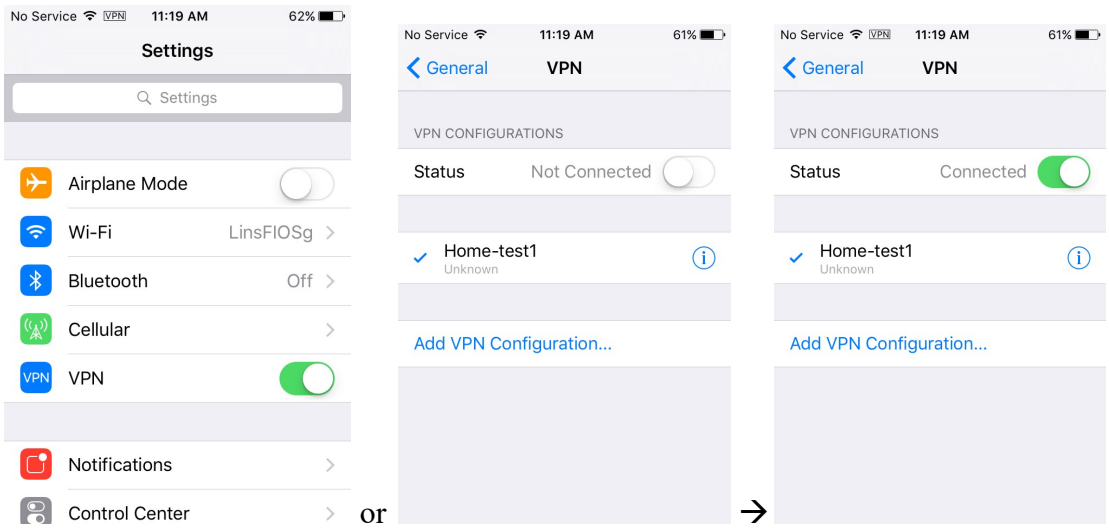


**Figure 9 Test iPhone VPN Connection**

## 4.2. Configure VPN Client on Android Phone

Android phone does not provide a way to load profile like iOS device as installation option. You have to do it step by step. The good thing is the procedure is very straightforward.

### 4.2.1. Set up Android VPN Profile

1) Go to Android "Settings" (Figure 10)

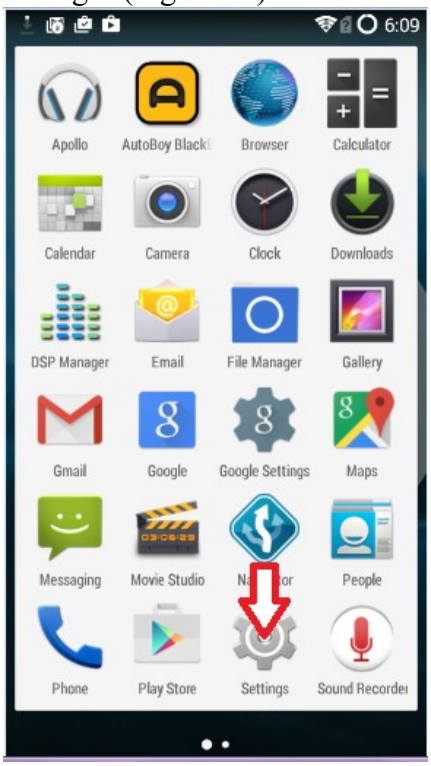


**Figure 10 Andoid App Screeen**

2) Select "Settings", then select "More…"

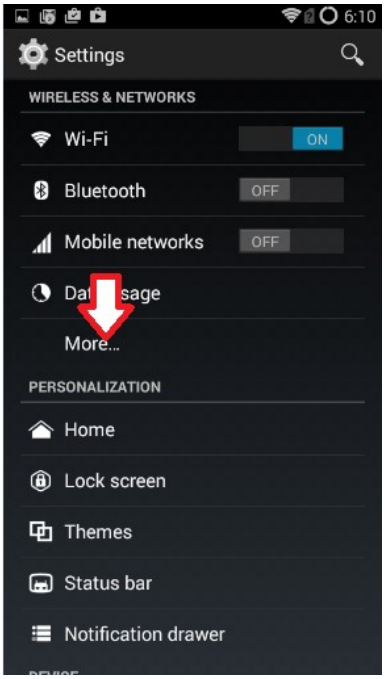


**Figure 11 Android Settings**

3) Select “VPN”, then select “+”

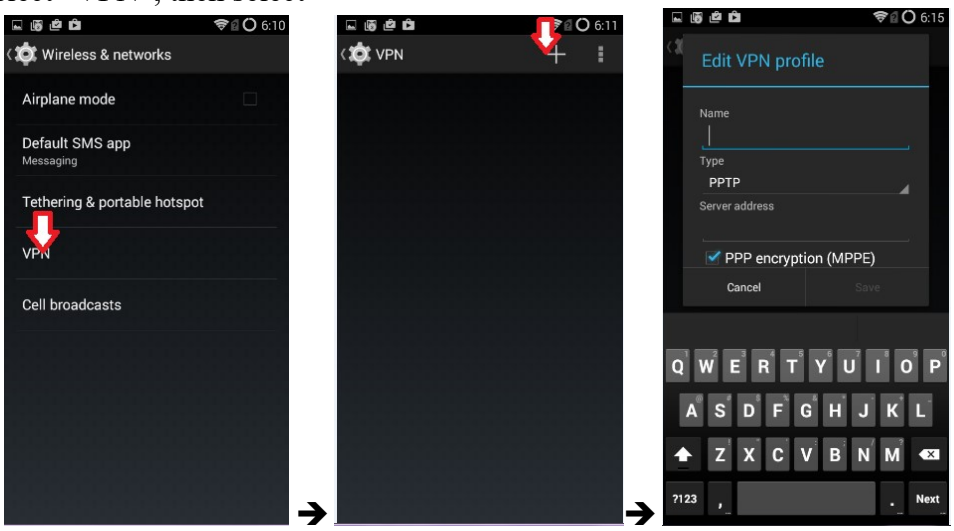


**Figure 12 Android VPN Add Profile**

4) Enter any name in “Name” field, select “IPSec Xauth PSK” in “Type” field, enter public IP of VPN server in “Service address” field. (Figure 13)

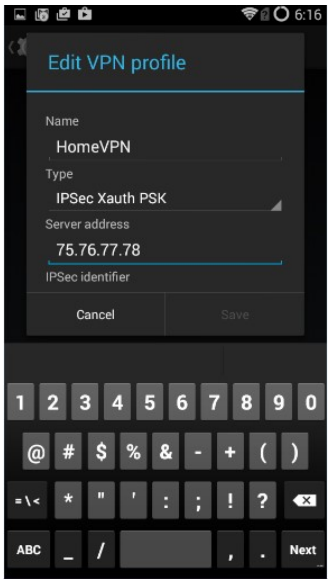


**Figure 13 Edit VPN Profile**

**Note 1**: The "Name" here is NOT the VPN user name you configured on VPN server side. It is just a name to identify this VPN profile.

**Note 2**: If you don't know what your public IP is, go to VPN server web UI. Click ***Network*** tab, then click ***+ Router Info …,*** you will see the public IP

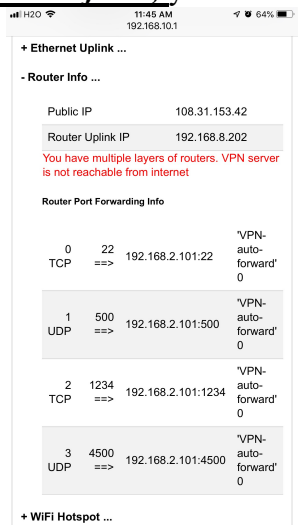


**Figure 14 VPN Server Public IP**

5) Scroll up screen a little bit and fill in the preshared-key (Figure 15).

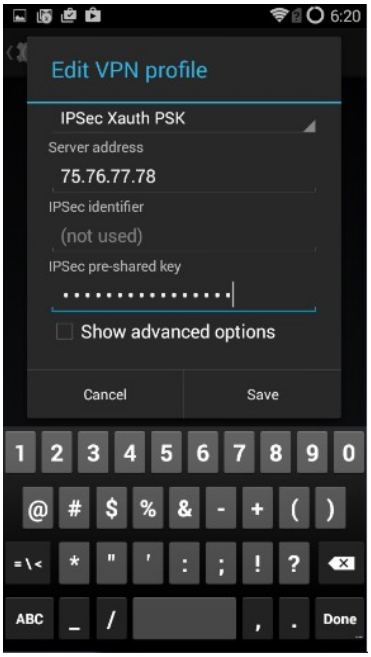


**Figure 15 Enter IPSec pre-shared key**

**Note**: Use the pre-shared key you configured on VPN server
*Factory default preshared-key is "1234567890" without quote sign.*

6) Select "Save", now you have successfully created a VPN profile (Figure 16).

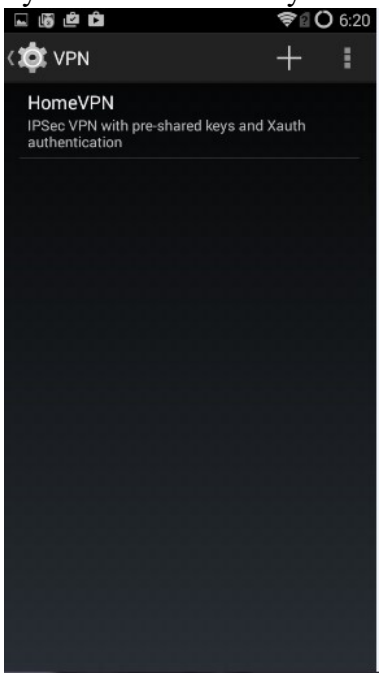


**Figure 16 Android VPN Profile List**

7) Click VPN profile just created to fill in username and password. Then click "Connect".

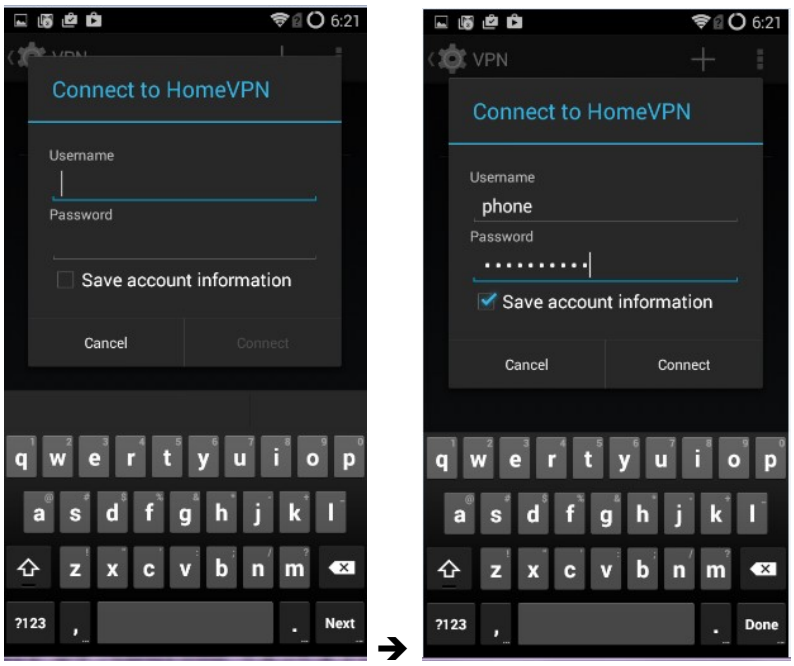


**Figure 17 Enter VPN Username and Password**

**Notes**:

**a.** Use the username and password you configured on VPN server. You may select "Save account information" so that you don't need to enter username and password again every time you connect VPN.
Factory default user is "test1" with password "vpneveryone".

**b.** VPN connect **would fail** if you are using home WiFi of the same router where VPN server is attached. But it's OK. You have finished configuring Android VPN profile.

### 4.2.2. Test Android VPN Profile

If you are at home, you may temporarily disable WiFi on your Android phone and turn on your cell phone data plan. Then click on the VPN profile created at section 4.2.1

Alternatively, you can use your neighbor's WiFi just to test VPN profile created at section 4.2.1.

On successful VPN connection, you will see a key sign on top left of the phone screen and see "connected" on the VPN profile (Figure 18).

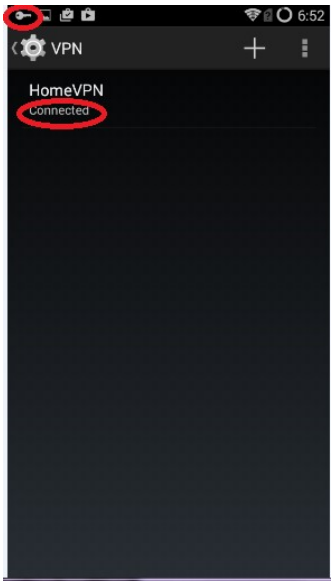


**Figure 18 VPN Tunnel Created Successfully**

# 5. Configure IPsec VPN Client on Windows 7/10

## *5.1. Setup Shrew VPN Client Profile*

The easiest way to use IPsec VPN on windows 7 is to use shrew VPN client. The standard version is free. Google "ShrewVPN" to download it for free.

After you install shrew VPN client, from Windows PC, login to VPN server device. Click ***VPN*** tab, click ***+VPN Client Profile*** to see UI like below. Right click on ***ShrewVPN Profile*** link to download the ShrewVPN profile

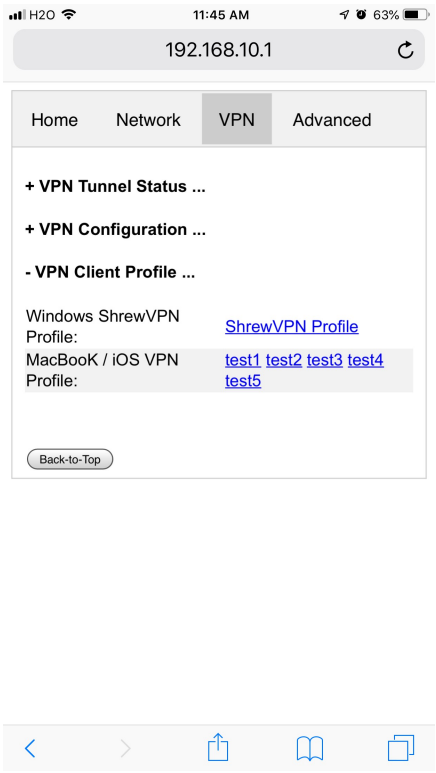


**Figure 19 VPN Profile**

Start Shrew VPN Access Manager, click ***File*** menu and then click ***Import***, then select the profile saved in last step.

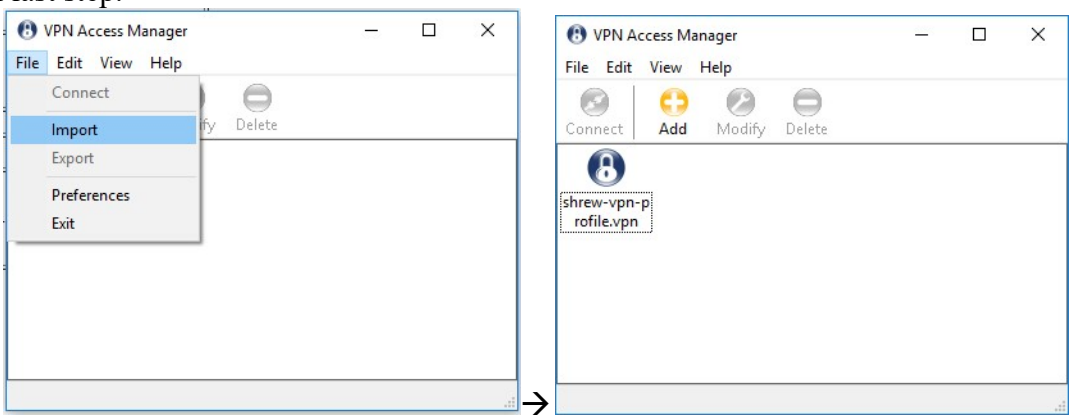

**Figure 20 Shrew VPN Access Manager**

## 5.2. Test Shrew VPN Client Profile

VPN connect would fail if you are in the same local network where VPN server is attached.

If your neighbor allows you to use their WiFi guest, you can connect your Windows 7 laptop to their WiFi to test VPN. Or you can bring laptop to your work place to try.

Double click the VPN profile just created. Enter the username and password you configured* on VPN server. Then click "Connect" button (Figure 21).

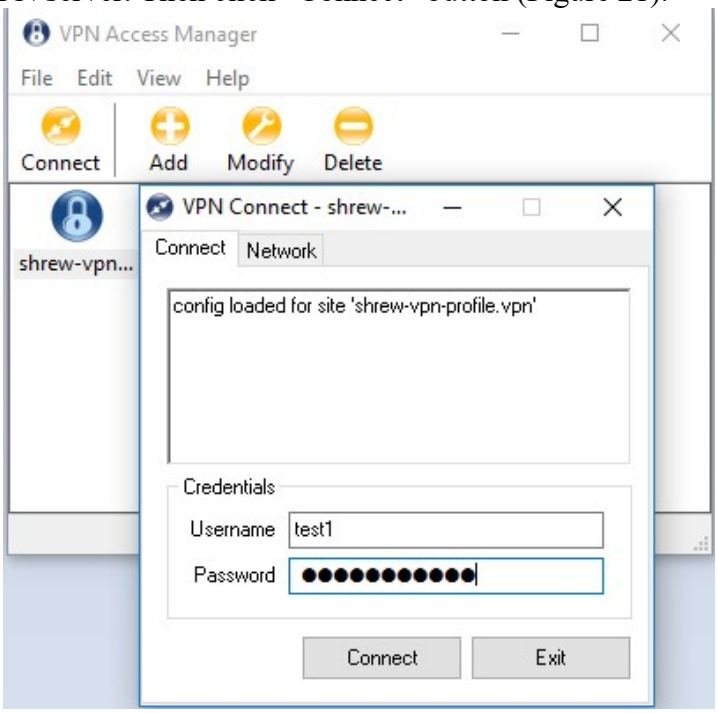


**Figure 21 Test Shrew VPN Profile**

*The factory default username is "test1" with password "vpneveryone" (without quote sign).

VPN Tunnel Created Successfully (Figure 22)

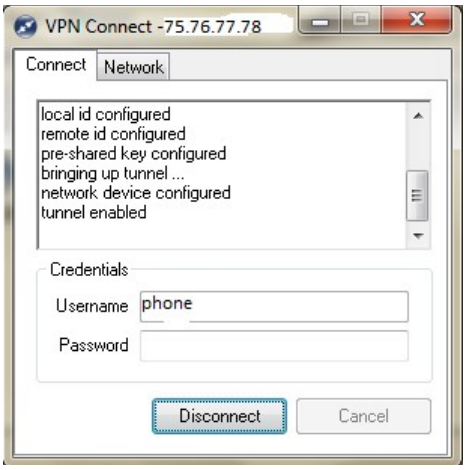


**Figure 22 Shrew VPN Client Successfully Connects**

# 6. Configure IPsec VPN Client on MacBook

MacBook has built-in IPsec VPN client. Follow exact the same procedure as in iOS in section 2 earlier. The ***mobileconfig*** profile generated by VPN device works for MacBook. Click any of the ***mobileconfig*** profile and simply follow what the direction your MacBook says. It's super easy!.

# 7. Change Default Keys & Username/Password on VPN Server

**Tip**: Each 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 shared-key and password, here is the detail procedure.

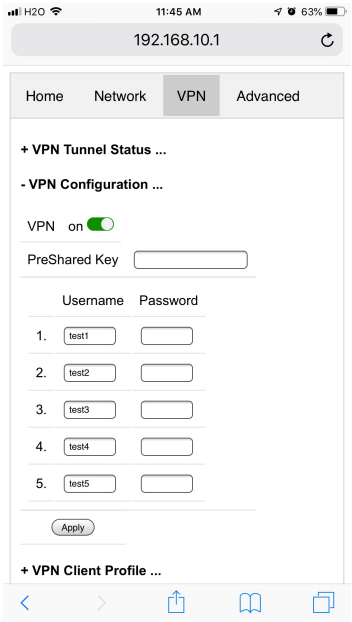


**Figure 23 IPsec VPN Server Configuration UI**

- Login to VPN server web UI.
- Click "VPN" tab
- Click "VPN Configuration"
- Enter 8 or more characters for ***PreShared Key***
- Enter 5 pairs of Username & password
- Click Apply

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

Note: If you change VPN settings, new ***VPN Client Profiles*** are automatically re-generated. You need to re-import them to your VPN clients (iOS or Windows).

# 8. Advanced Settings

**Note**: In very rare case will you 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.

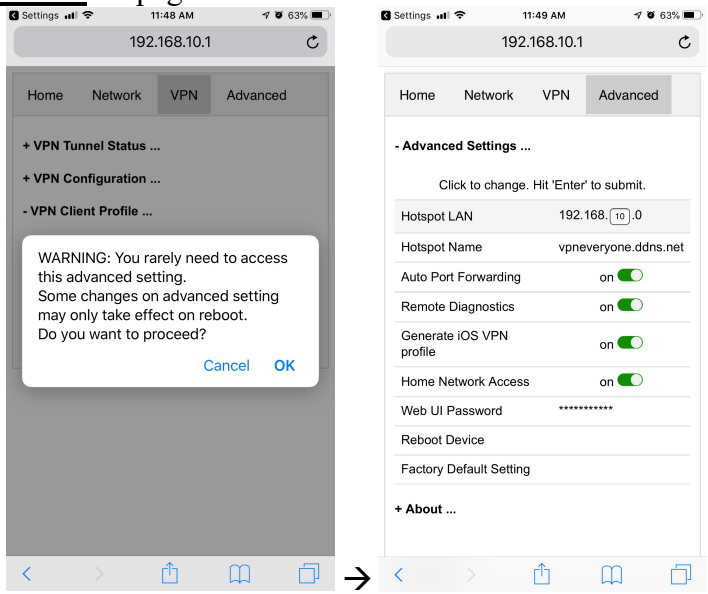


**Figure 24 VPN Device Advanced Settings**

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.

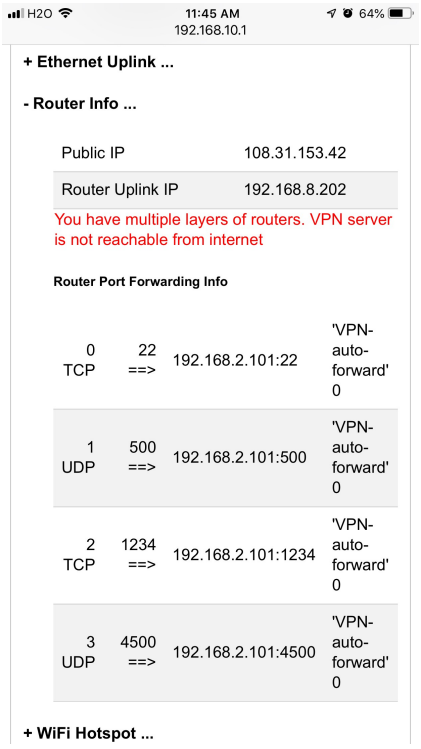


**Figure 25 Router Port Forwarding Info**

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) **Generate iOS VPN profile**
Disable this feature will tell VPN server NOT to generate .mobileconfig profiles for the 5 users you configured.
If you don't use iOS device at all, you may disable this feature.

6) **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***.

7) **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.

8) **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.

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

## *8.1. About Product*

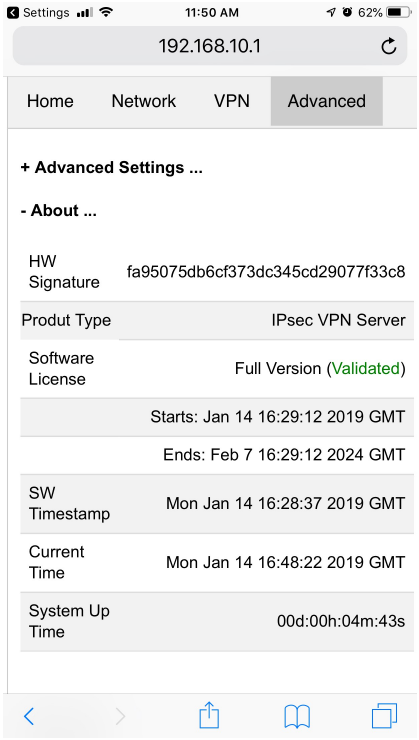


**Figure 26 Product Info**

Each VPN device runs the software programmed in the MicroSD card. The software is only licensed to run on the shipped MicroSD card.
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.

# 9. 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 27 below) will help you. If the ***Public IP*** does not match the ***Router Uplink IP***, it means you have multiple-layer router problem.

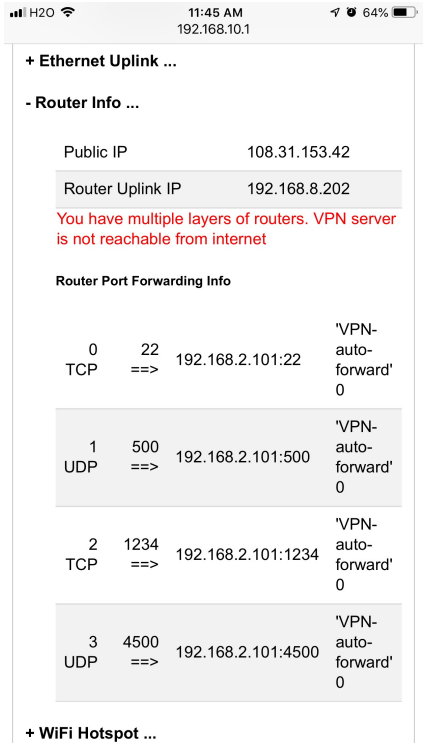


**Figure 27 Router Info UI Page**

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 27, you are good.

If you had disabled UPNP on your router, you need to enable it. Or manually forward ports like in Figure 27

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

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