

IPsec VPN Server User's Guide

Rev F
March, 2021

All Rights Reserved

Table of Content

IPsec VPN Server User's Guide	1
Table of Content	2
List of Figures	3
1. Introduction.....	4
2. Connect VPN Server to Wireless Router.....	5
3. Access VPN Server Configuration Web UI.....	6
3.1. Access Web UI by Built-in WiFi Hotspot	6
3.2. Access Web UI by LAN Ethernet Port	7
3.3. Access Web UI by http://Router IP:1234.....	7
3.4. Access Web UI by VPN Server IP.....	7
4. Configure VPN Client on Smart Phone	8
4.1. Configure VPN Client on iPhone.....	8
4.1.1. Test Your iPhone VPN Client.....	9
4.2. Configure VPN Client on Android Phone.....	10
4.2.1. Set up Android VPN Profile	10
4.2.2. Test Android VPN Profile	14
5. Configure IPsec VPN Client on Windows.....	16
5.1. Windows 10: Use built-in IKEv2 VPN Client.....	16
5.1.1. Test Windows 10 IKEv2 VPN Client.....	19
5.2. Windows 7: Use Free ShrewVPN Client Software.....	20
5.2.1. Setup Shrew VPN Client Profile.....	20
5.2.2. Test Shrew VPN Client Profile.....	21
6. Configure IPsec VPN Client on MacBook	23
7. Change Default Keys & Username/Password on VPN Server.....	23
8. Advanced Settings	24
8.1. About Product	26
9. Quick Troubleshoot	27

List of Figures

Figure 1 Overall VPN Working Model	4
Figure 2 Connect VPN Server to Wireless Router	5
Figure 3 Find vpneveryone.ddns.net WiFi hotspot.....	6
Figure 4 Access VPN Server Web UI by Built-in WiFi Hotspot	7
Figure 5 Access VPN Server Web UI by Router IP:1234.....	7
Figure 6 Access VPN Server Web UI by VPN server IP	8
Figure 7 Access VPN Client Profile Prepared by VPN Server	8
Figure 8 iPhone Screenshots of Installing VPN profile	9
Figure 9 Test iPhone VPN Connection.....	10
Figure 10 Andoid App Screen.....	10
Figure 11 Android Settings	11
Figure 12 Android VPN Add Profile.....	11
Figure 13 Edit VPN Profile.....	12
Figure 14 VPN Server Public IP.....	12
Figure 15 Enter IPsec pre-shared key	13
Figure 16 Android VPN Profile List.....	13
Figure 17 Enter VPN Username and Password	14
Figure 18 VPN Tunnel Created Successfully	15
Figure 19 VPN Client Profile	16
Figure 20 Windows 10 IKEv2 Configuration PowerScript.....	17
Figure 21 Find Windows 10 PowerShell app and Run as Administrator	18
Figure 22 IKEv2 VPN Configuration Commands Successfully Run in Windows 10 PowerShell	18
Figure 23 VPN Profile	20
Figure 24 Shrew VPN Access Manager	21
Figure 25 Test Shrew VPN Profile	21
Figure 26 Shrew VPN Client Successfully Connects.....	22
Figure 27 IPsec VPN Server Configuration UI	23
Figure 28 VPN Device Advanced Settings.....	24
Figure 29 Router Port Forwarding Info	25
Figure 30 Product Info	26
Figure 31 Router Info UI Page.....	27

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.

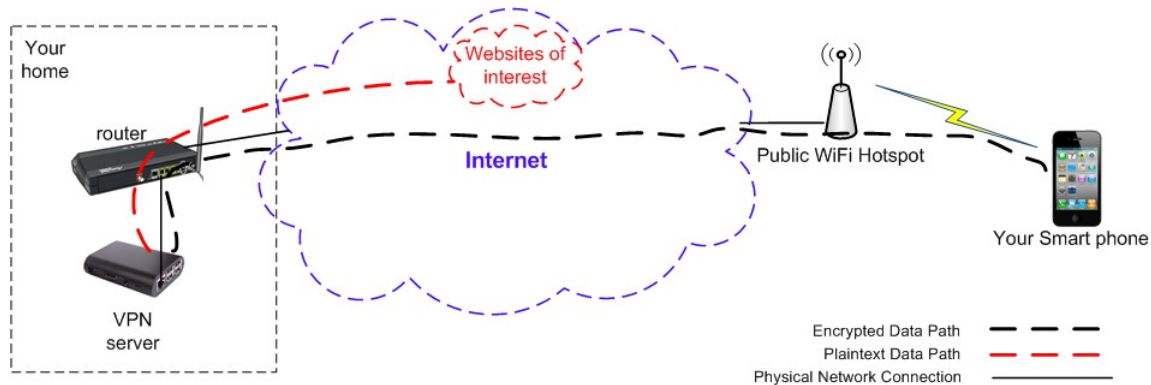


Figure 1 Overall VPN Working Model

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)

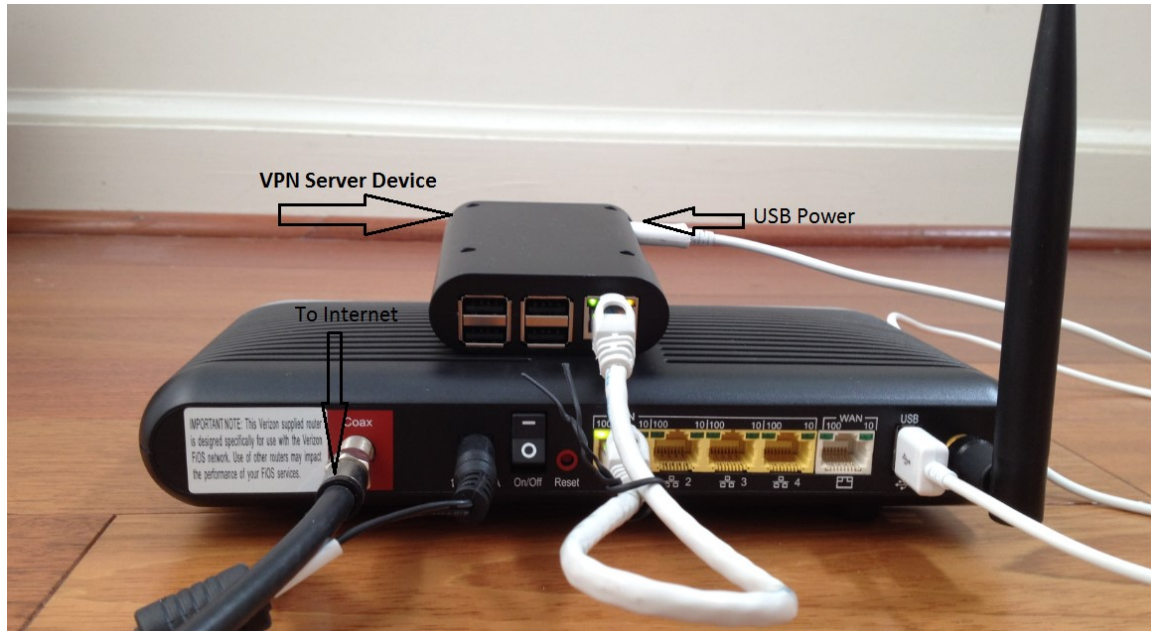


Figure 2 Connect VPN Server to Wireless Router

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*

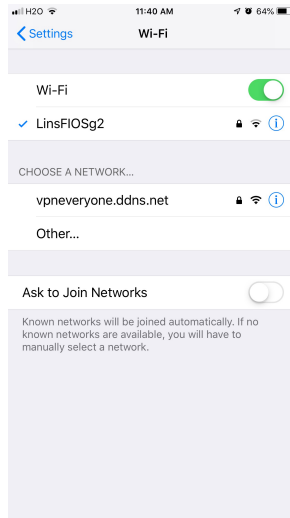


Figure 3 Find *vpneveryone.ddns.net* WiFi hotspot

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.

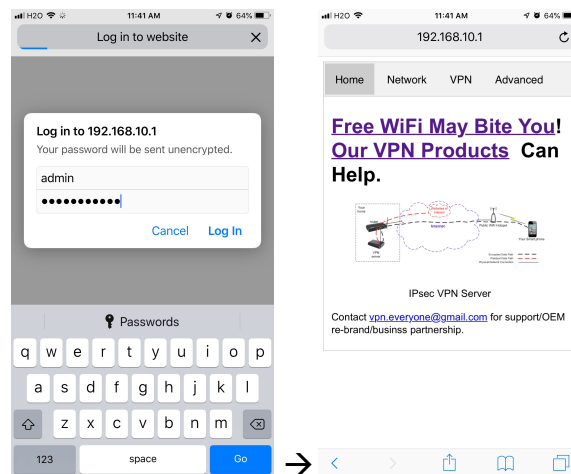


Figure 4 Access VPN Server Web UI by Built-in WiFi Hotspot

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 LAN Ethernet Port

If your VPN device comes with **TWO** Ethernet ports, plug in your PC to the port labeled “LAN”. Your PC should get an IP 192.168.10.x.

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.

3.3. 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

3.4. 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

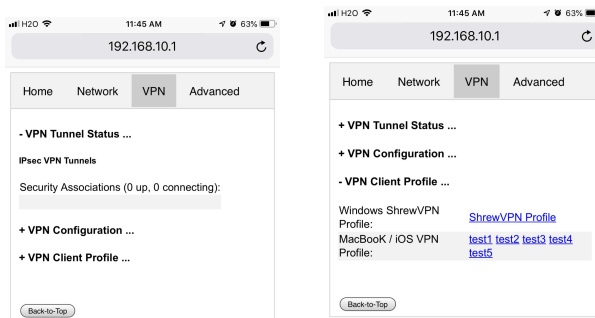


Figure 7 Access VPN Client Profile Prepared by VPN Server

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.

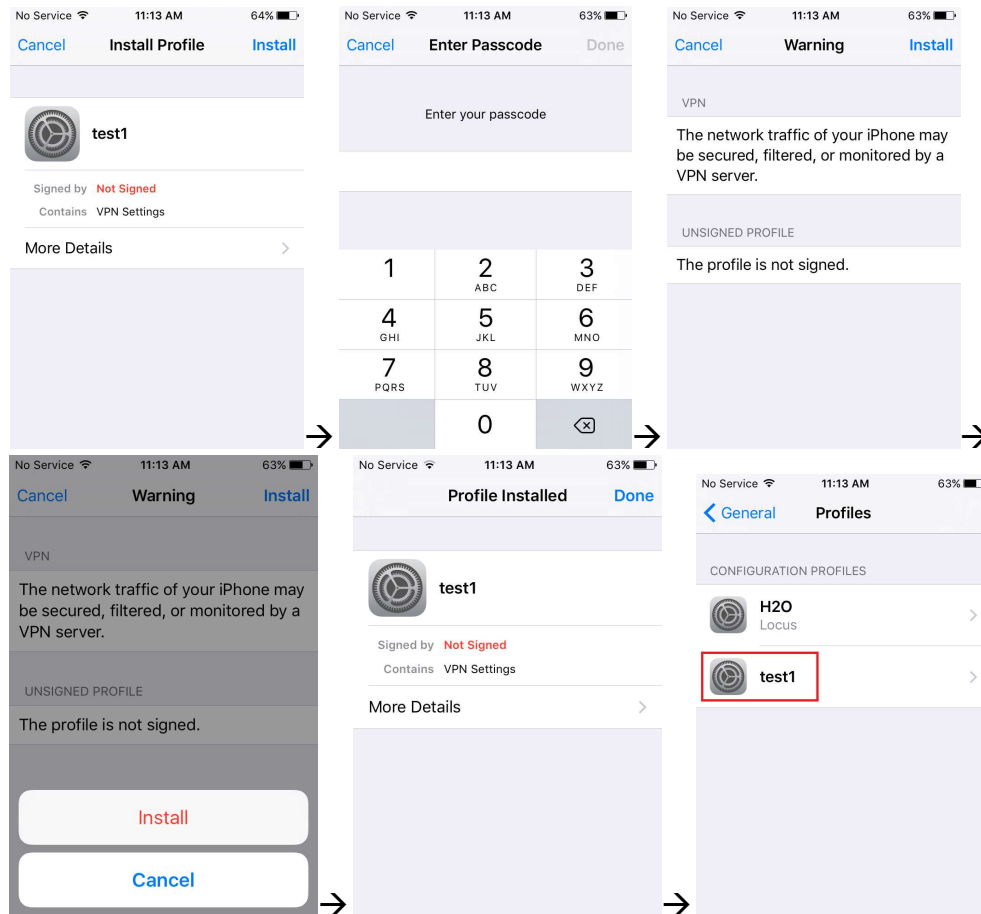


Figure 8 iPhone Screenshots of Installing VPN profile

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”

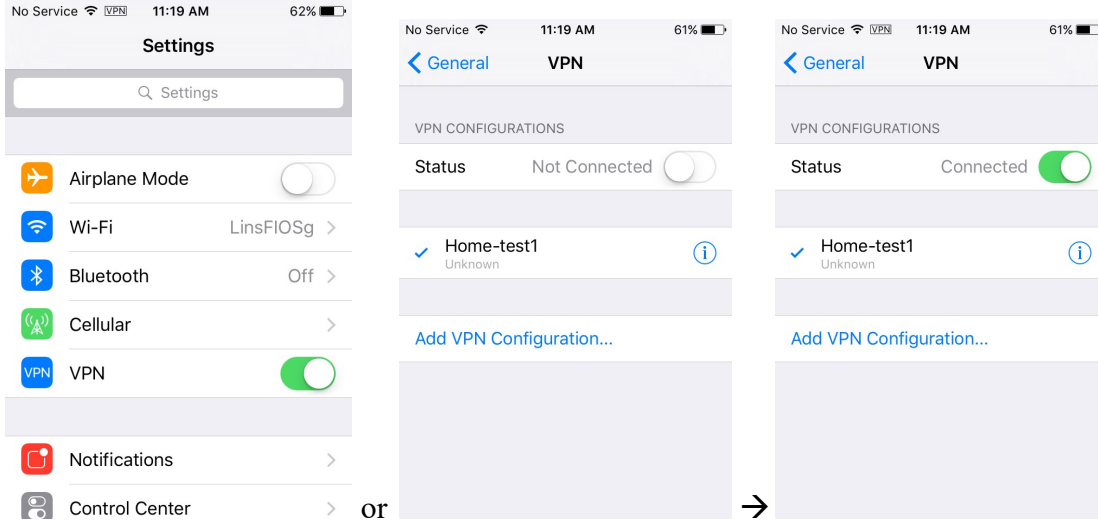


Figure 9 Test iPhone VPN Connection

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)

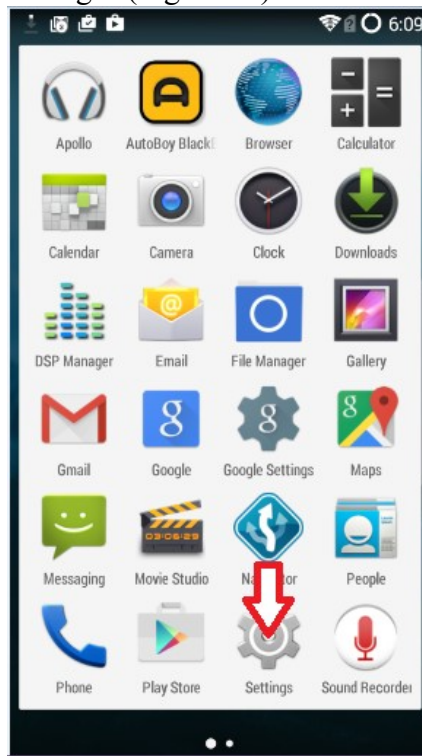


Figure 10 Andoid App Screen

- 2) Select “Settings”, then select “More...”

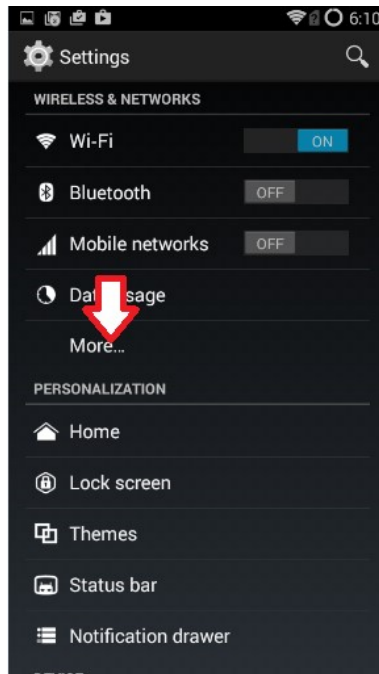


Figure 11 Android Settings

3) Select “VPN”, then select “+”

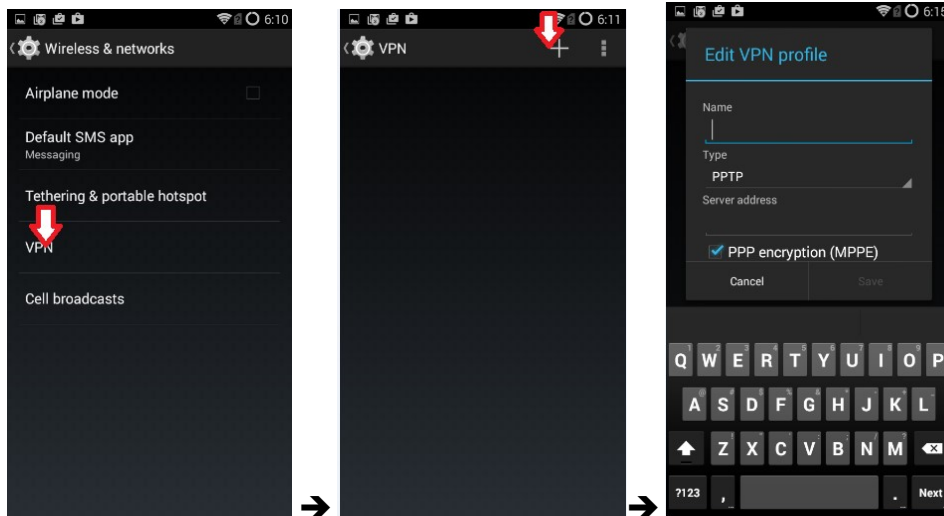


Figure 12 Android VPN Add Profile

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)

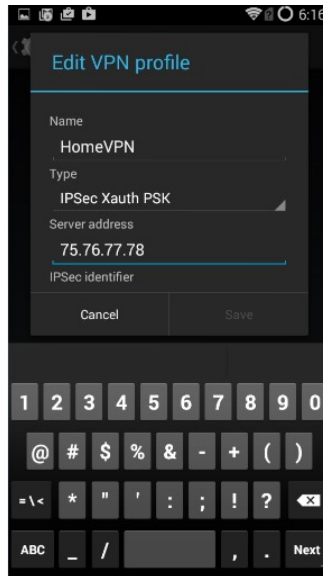


Figure 13 Edit VPN Profile

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

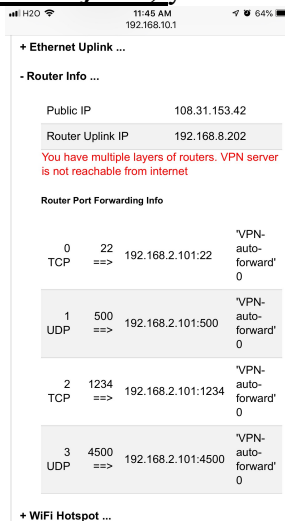


Figure 14 VPN Server Public IP

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

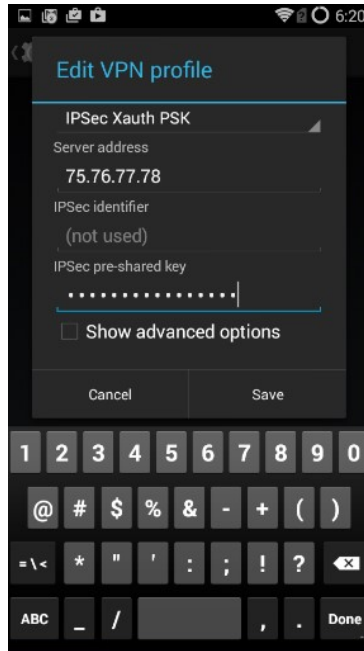


Figure 15 Enter IPSec pre-shared key

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).

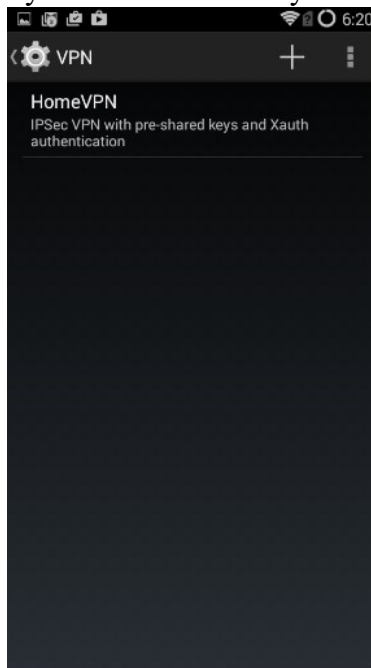


Figure 16 Android VPN Profile List

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

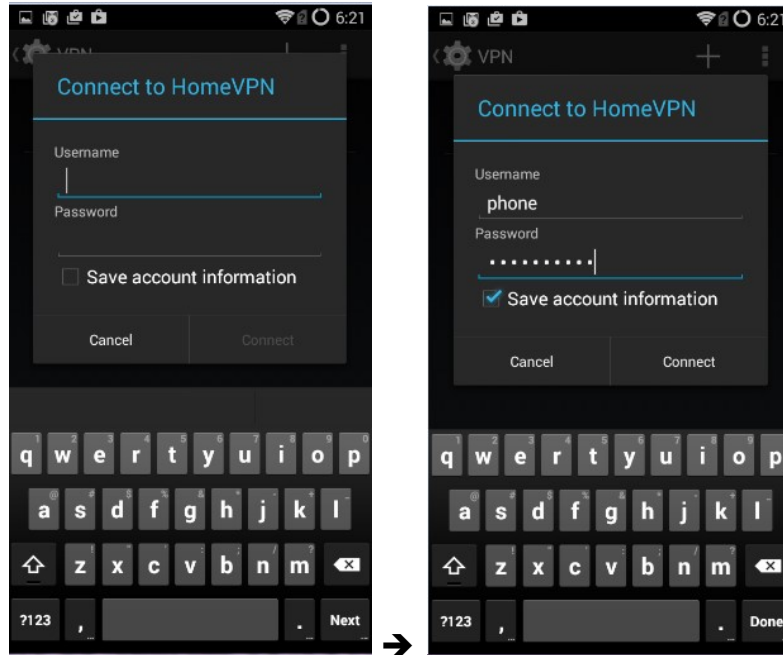


Figure 17 Enter VPN Username and Password

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).

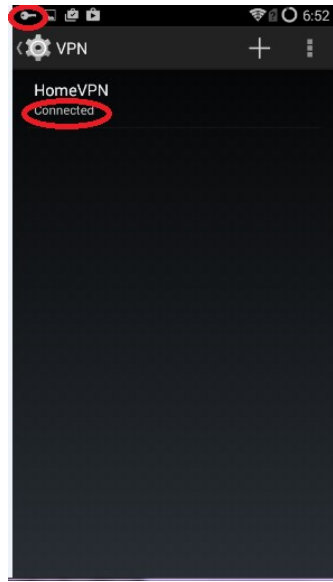


Figure 18 VPN Tunnel Created Successfully

5. Configure IPsec VPN Client on Windows

5.1. Windows 10: Use built-in IKEv2 VPN Client

Windows 10 comes with IKEv2 VPN client built-in. The VPN server automatically generates a script for windows 10. Copy & Paste the script and run it in Windows 10 PowerShell. That's it.

Here is the detail.

Assume you use Windows 10 PC to access VPN server web UI page, VPN tab. Click “+VPN Client Profile ...” You will see UI like below.

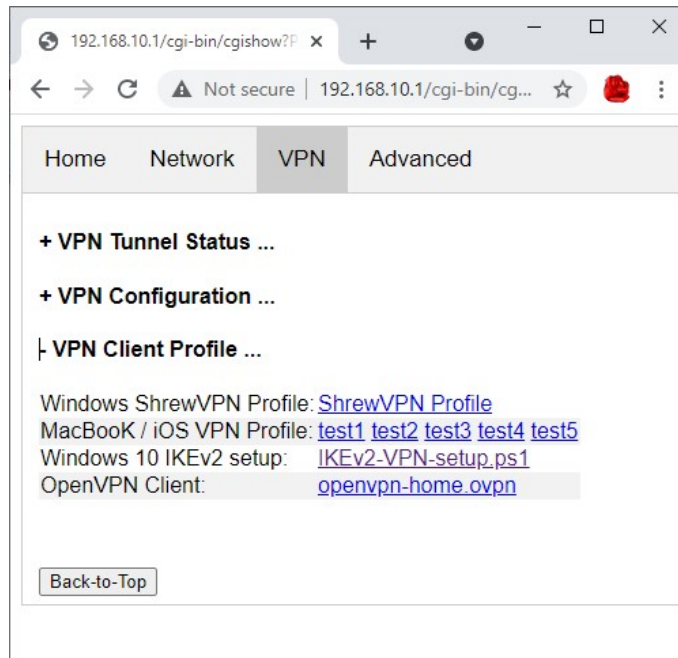


Figure 19 VPN Client Profile

Click “*IKEv2-VPN-setup.ps1*” link. The web browser will open it in text format like below. Press “*Ctrl + A*” to select all texts. Then press “*Ctrl + C*” to copy all texts in clipboard.


```

VQQG6WJVOZERMA8GA1UECBPLTWfYerXNDMjQXEZARBgNVBACILKNS YXJFZ2Jlcmcx
FDASBgNVBAoTC3ZwbmV2ZXJ5b251MQwwCgYDVQQLLEwNWUE4xDALBgNVBAMTBHJv
b3QxJTAjBgkqhkiG9w0BCQEFnZwbi51dmVyeW9uZUBnbWFPbC5jb20wHhcNMTYx
MDA4MDMxNDM2WhcNMzYxMDAzMDMxNDM2WjCBjzELMAKGA1UEBHMCMVVMxETAPBgNV
BAGTCE1hcn1sYw5kMRMwEQYDVQQLLEwpcDdGfya3NiZXNMRQwEgYDVQQKEwt2cG51
dmVyeW9uZEMMAoGA1UECXMMDVlBOMQ0wCwYDVQQDEwRyb290MSUwIwYJKoZIhvcN
AQkBFH2cG4uZXZlcnlvbmVAZ21haWwvY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCA
Q8AMIIBCGkCAQEAqK35t4ByavKcsZ6SnRiXSMXE1Dc0Y45tJQpzTkk317iKtyZ3
QXKMOs5IU4EAY+rSjTDD4EYokbXbnASU2qwc0XkMJJ2903B3gd8jngBigrVvqWIS
1w7sbQ56FGItuBmkqk0m1DUkG2cX6yDGg8062Vkh0oBdo1tbz19jCD1e3TUaxu0H
n1UUMB6G6Scfj5DQIEJ2gZAsnsp6PtNt88CYwSocXpE7e1Zb/kdNUcjCHKIp7bVv
h35JcNIkvtm5ksG7MNavhdD5DtqDix/GxBGATPaeUGwvm8XS4buqDuxdHbaDPsJ0
uyHX2kcPaj6Y3JU0mcUu92y4bQ7DHP6Z93a82QIDAQABo4IBBTCCAQEWHQYDVR00
BBYEFNhrMwR6taNvo1kJg1xP9CQn1SMIHEBgNVHSMGbwgmbAFNhrMwR6ta
Nvo1kJg1xP9CQn1SoYGVpIGSMIGPMQswCQYDVQGEwJVUzERMA8GA1UECBMITWfY
erXNDMjQXEZARBgNVBACILKNS YXJFZ2JlcmcxFDASBgNVBAoTC3ZwbmV2ZXJ5b251
MQwwCgYDVQQLLEwNWUE4xDALBgNVBAMTBHJvbn3QxJTAjBgkqhkiG9w0BCQEFnZw
bi51dmVyeW9uZUBnbWFPbC5jb22CCQD699cMcu1V1zAMBGNVHRMEBTADAQH/MA5G
A1UdDwQEAwIBBjANBgkqhkiG9w0BAQUFAAOCAQEATJcT/QbJ216Hfz08S4RQ0gso
rJAAd+kVC5yUheU0PZtzvc5nn+f+tXe2B0oti3f0LeikUeUz6HYvg/RE65gRvsCd
xjEoeYGemIOu04JanhdhqRzWDB4afZyzeFbqIsZG+svdx9wATP9L6DG500pCQEp
OS+Ha1j0c8sMIouaaRrAhD9Ss+6SWyaCtQGemH2gZENznmZ08bJ5iVHTBwInWg
5PcFkRKJsov8FCPhvRSihwEuFF4pIwhWrL5VkfjHtWvrKtIs5r8x+MB3mOM937TU
Zaz+0/4W+Wcgjx2iebRppICRmnaVeXnRalyzPta8KVI+zgBeh44ME5Lids6Cmg==
"
$Cert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate
$Cert.Import([Convert]::FromBase64String($CertBlob))
$store = new-object
System.Security.Cryptography.X509Certificates.X509Store([System.S
ecurity.Cryptography.X509Certificates.StoreName]::Root,
"localmachine")
$store.open("MaxAllowed")
$store.add($Cert)
$store.close()

$hostsFile = "$($env:windir)\system32\Drivers\etc\hosts"
$hostsEntry = '192.168.8.202 C20210319130929-1850d'
Add-Content -Path $hostsFile -Value ' '
Add-Content -Path $hostsFile -Value $hostsEntry

Add-VpnConnection -Name "C20210319130929-1850d" -ServerAddress
"C20210319130929-1850d" -TunnelType "IKEv2" -EncryptionLevel
"Max" -AuthenticationMethod ESP -AllUseConnection

```

Figure 20 Windows 10 IKEv2 Configuration PowerShell

In Window 10, right click the “Start” located at bottom left of the screen. Then click “Windows PowerShell (Admin)”. Click “Yes” when “User Access Control” window pops up. See figures below.

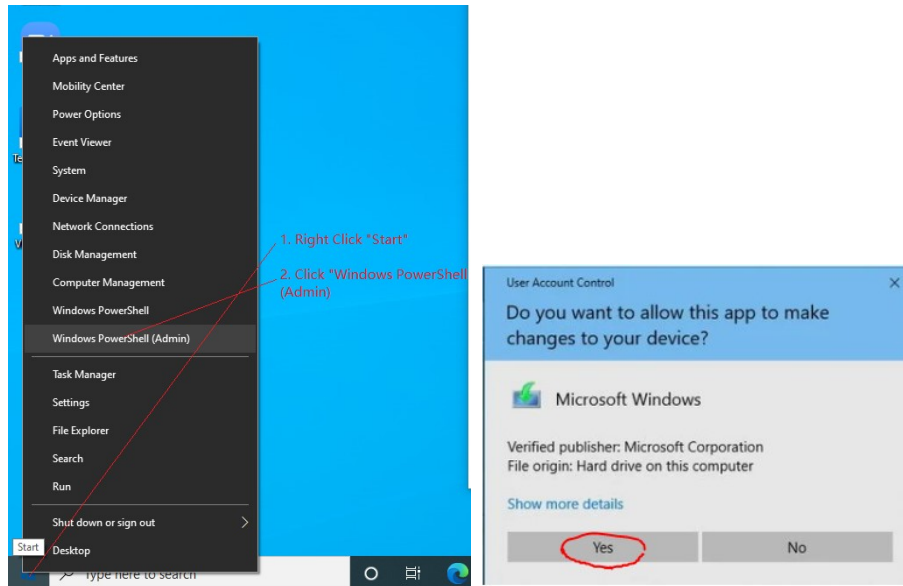


Figure 21 Find Windows 10 PowerShell app and Run as Administrator

A blue color PowerShell window starts. **Right Click** mouse inside of PowerShell window to paste the commands in clipboard. See figure below.

```

Administrator: Windows PowerShell
>> uyHMA2kcPaJ6Y3JU0mcUu92y4B07DHP6Z93a02Q1DAQABo4I88TCCAQEwHQYDVVR00
>> BBYEFNhxRrMwR6taNvo1k3g1xP9CQn1SMIEHBgNVHSMEgbwgbwAFNhxRrMwR6ta
>> Nvo1k3g1xP9CQn1SoYGVpIGSMIGPMQswCQYDVQGEw3VuzERMA8GA1UECBMTWFY
>> eKXhbmQxExARBgNVBAcTckNsYXJzY2JlcmcxZDASBgNVBAoTC3ZwbmV2ZXJ5b251
>> MQwwCgYDVQQLZWwVUE4xDTALBgNVBAMTBHJvb3QxJTAjBgkqhkiG9w0BCQEFn2w
>> b151dmVyeW9uZUBnbWVpbC5jb22CCQD699cMcu1V1zAMBglNHRMEBTADAQH/MASG
>> A1UdMwEAWIBBjANBgkqhkiG9w0BAQUFAAOCAQEATjct/QbJ216HFz08S4RQ0gso
>> rJAAd+kVC5yUheU0PZtzvc5nn++tXe2B0ot13f0Le1KueUZ6HYvg/RE65gRvscD
>> xJEoeYGemIOu04JanhdhgRzWDBB4afZyzeFbqIsZG+svdx9wATP9L6DG50OpCQEp
>> 05+Ha1j0c8sMtouaaRrAhD9Ss+6SmYaCtQGEMH2gZENzrmZ08bJ5iVHTBwINWg
>> 5PcFkRkJs0v8FCPhvRSiHwEuFF4pIwhWrl5VkfJHtwVrKtIs5r8x+MB3mOM937TU
>> Zaz+04W+Wcgjx2iebRppICRmaVeXnRalyzPta8KVI+zgBeh44ME5LIdS6Cmg==
>>
PS C:\WINDOWS\system32> $Cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate
PS C:\WINDOWS\system32> $Cert.Import([Convert]::FromBase64String($CertBlob))
PS C:\WINDOWS\system32> $store = new-object System.Security.Cryptography.X509Certificates.X509Store((System.Security.Cry
ptography.X509Certificates.StoreName)::Root, "localmachine")
PS C:\WINDOWS\system32> $store.open("MaxAllowed")
PS C:\WINDOWS\system32> $store.add($Cert)
PS C:\WINDOWS\system32> $store.close()
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> $hostsFile = "$($env:windir)\system32\Drivers\etc\hosts"
PS C:\WINDOWS\system32> $hostsEntry = '192.168.8.202 C20210319130929-1850d'
PS C:\WINDOWS\system32> Add-Content -Path $hostsFile -Value '$$'
PS C:\WINDOWS\system32> Add-Content -Path $hostsFile -Value $hostsEntry
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Add-VpnConnection -Name "C20210319130929-1850d" -ServerAddress "C20210319130929-1850d" -TunnelTy
pe "IKEv2" -EncryptionLevel "Maximum" -AuthenticationMethod EAP -AllUserConnection -RememberCredential -PassThru

Name                : C20210319130929-1850d
ServerAddress       : C20210319130929-1850d
AllUserConnection  : True
Guid                : {34C8393A-675D-4D5C-97CF-E27580915610}
TunnelType         : Ikev2
AuthenticationMethod : {Eap}
EncryptionLevel    : Maximum
L2tpIPsecAuth     :
UseWinlogonCredential : False
EapConfigXmlStream : #document
ConnectionStatus   : Disconnected
RememberCredential : True
SplitTunneling     : False
DnsSuffix          :
IdleDisconnectSeconds : 0
PS C:\WINDOWS\system32>

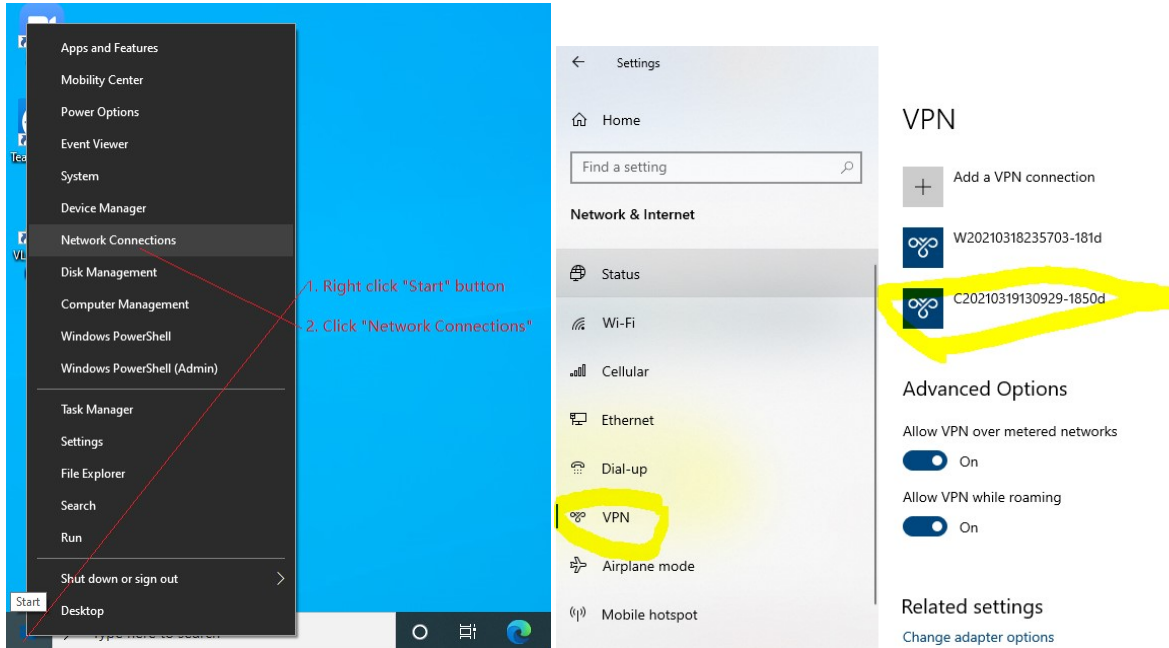
```

Figure 22 IKEv2 VPN Configuration Commands Successfully Run in Windows 10 PowerShell

Congratulations! You have successfully configured Windows 10 IKEv2 VPN client.

5.1.1. Test Windows 10 IKEv2 VPN Client

In Window 10, right click “**Start**” button on bottom left of the screen. Then click “**Network Connection**”

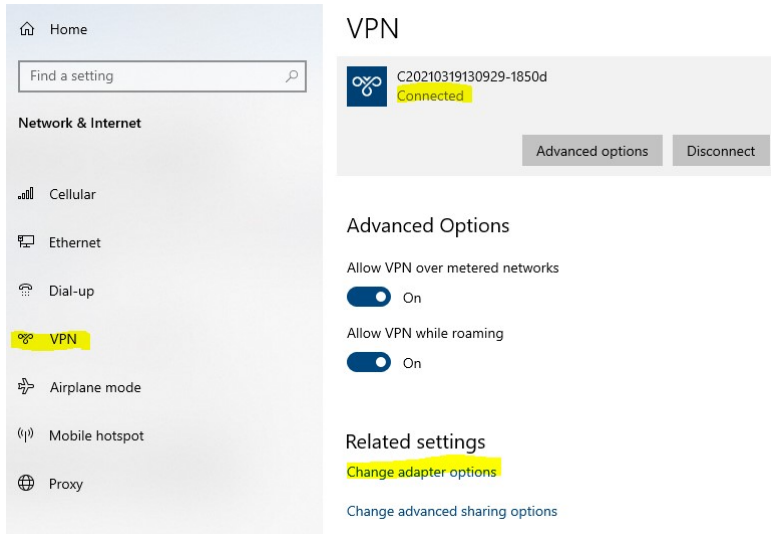


Click “**VPN**” on left. Then click VPN Connection **C20210319130919-1850d**.
When your Windows PC is away from home, click “**Connect**” button of VPN Connection **C20210319130919-1850d** to connect.



You will be asked for username & password. Input one of the 5 users you configured earlier. If you have not changed the default setting on VPN server, you can use “**test1**” & “**vpneveryone**” as username & password, respectively.

The VPN connection should connect successfully.



5.2. Windows 7: Use Free ShrewVPN Client Software

5.2.1. 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

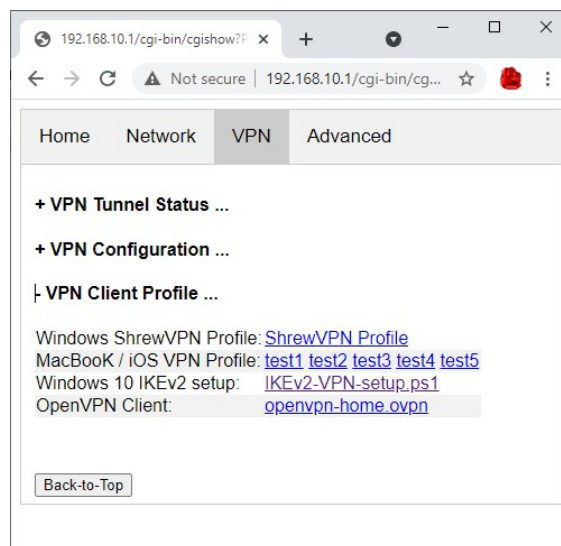


Figure 23 VPN Profile

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

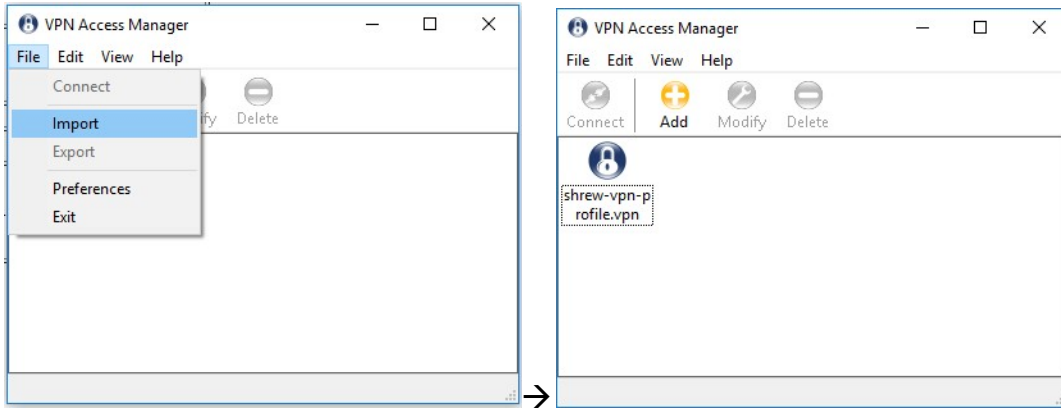


Figure 24 Shrew VPN Access Manager

5.2.2. 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 25).

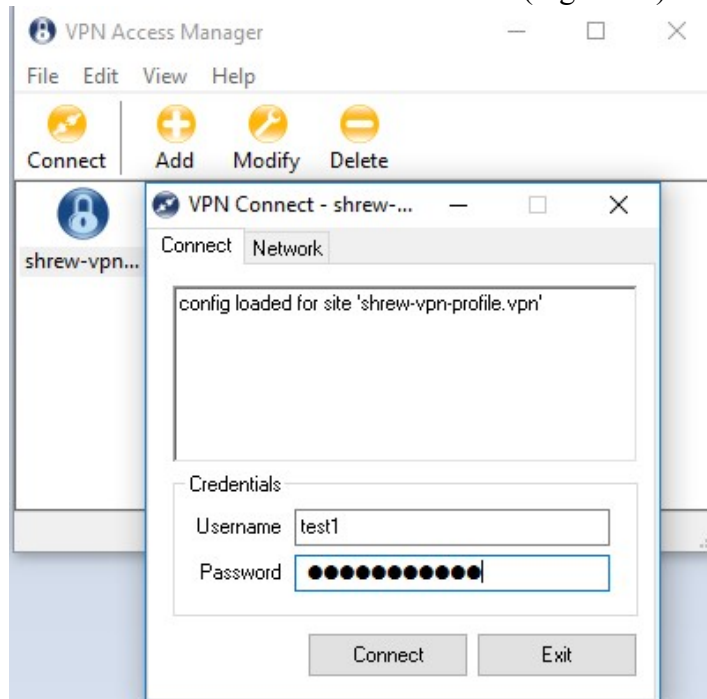


Figure 25 Test Shrew VPN Profile

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

VPN Tunnel Created Successfully (Figure 26)



Figure 26 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.

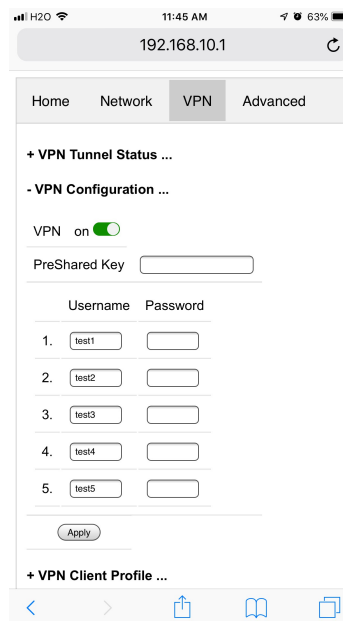


Figure 27 IPsec VPN Server Configuration UI

- 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.

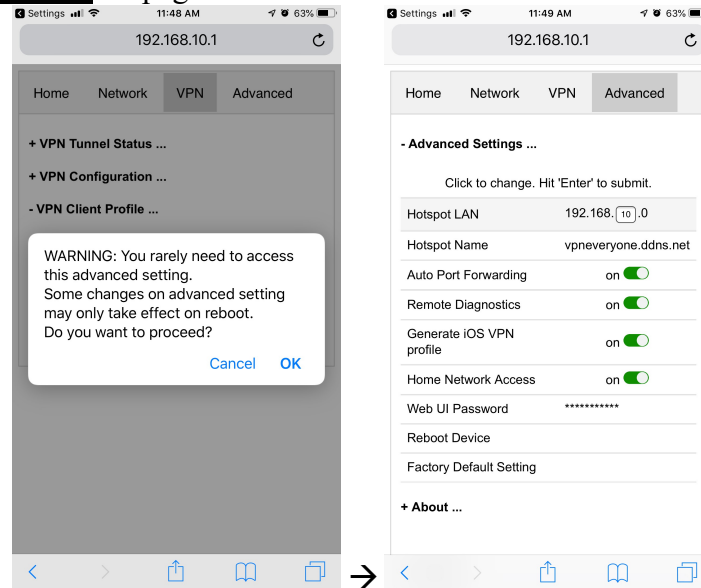


Figure 28 VPN Device Advanced Settings

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.

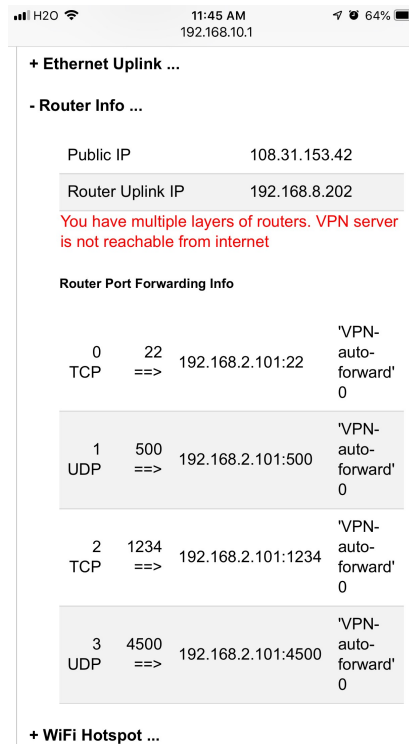


Figure 29 Router Port Forwarding Info

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

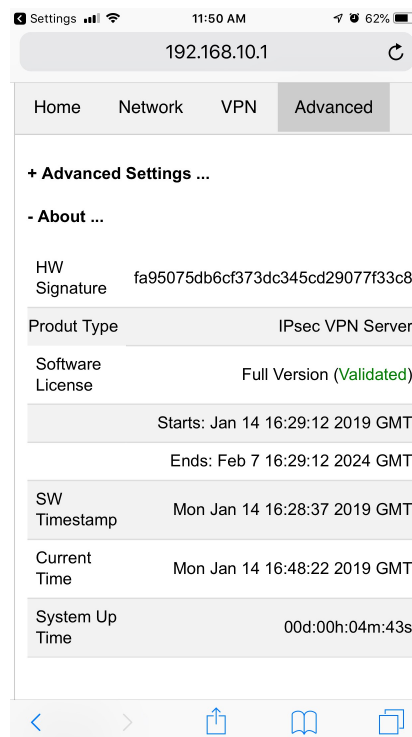


Figure 30 Product Info

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

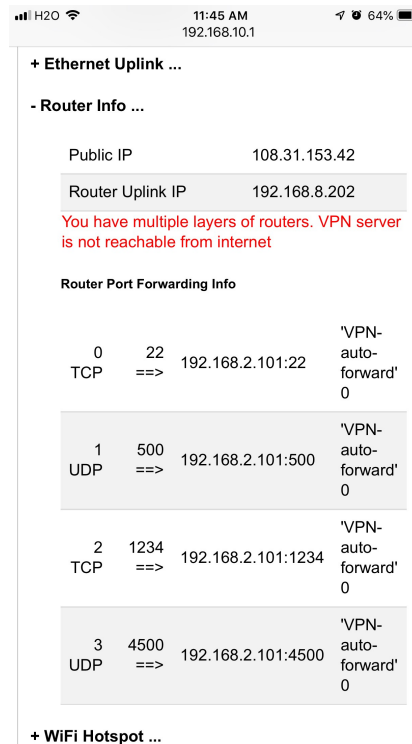


Figure 31 Router Info UI Page

- 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 31, you are good.

If you had disabled UPNP on your router, you need to enable it. Or manually forward ports like in Figure 31

If your router has *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"