

How to setup OpenVPN on Tomato Router

Configuring a PureVPN tunnel on your router is a great way to ensure the safety and security of all the devices in your home. This method is especially beneficial if you have devices that don't have VPN compatibility or you want to protect all the Wi-Fi-connected devices in your home.

It is very easy to configure VPN on Tomato Router. The following guide will help you setup PureVPN on your Tomato router.

Things to Consider:

1. You have a working internet connection
2. VPN Supported Router.
3. A Premium PureVPN account (If you haven't bought yet click [here](#) to buy)

Note: Dedicated IP addon can be only be connected with Ras protocol i.e PPTP/L2TP/SSTP/IKEV.

Find your VPN credentials for manual configuration.

To find your VPN credentials log into the PureVPN members area. Click ? [here](#) to visit member area.

- Login to the **Member area** using your PureVPN registered email address and password.

PureVPN Support

Solution of Your Problems

• From manage account section, go to the **Subscriptions tab**.

<https://support.purevpn.com>

Super Upgrade Offer. Get **88%** off on upgrading your PureVPN plan today. [Upgrade Now](#) ×

PUREVPN

GET STARTED

- PureVPN
- PureKeep

Manage account

- Subscriptions
- Upgrade Plan
- Downloads
- Help desk
- Refer a friend
- Affiliates

Manage Account

Manage your account details and preferences at one place.

Name:

Email: **fahadtesting5@gmail.com**

Password: ********* [Change password](#)

Subscriptions: **1** [See all subscriptions](#)

We value feedback and suggestions from our customers. Join our Slack group to directly contribute to improve our product experience. [Join us on Slack group](#)

Please check the box if you do not wish to receive email offers and other marketing emails relevant to PureVPN.

[Logout](#)

Earn Free Credit

Invite your friend and get \$10 on each invite.

[Invite now](#)

- On Subscription tab scroll down to be able to view your **VPN credentials**

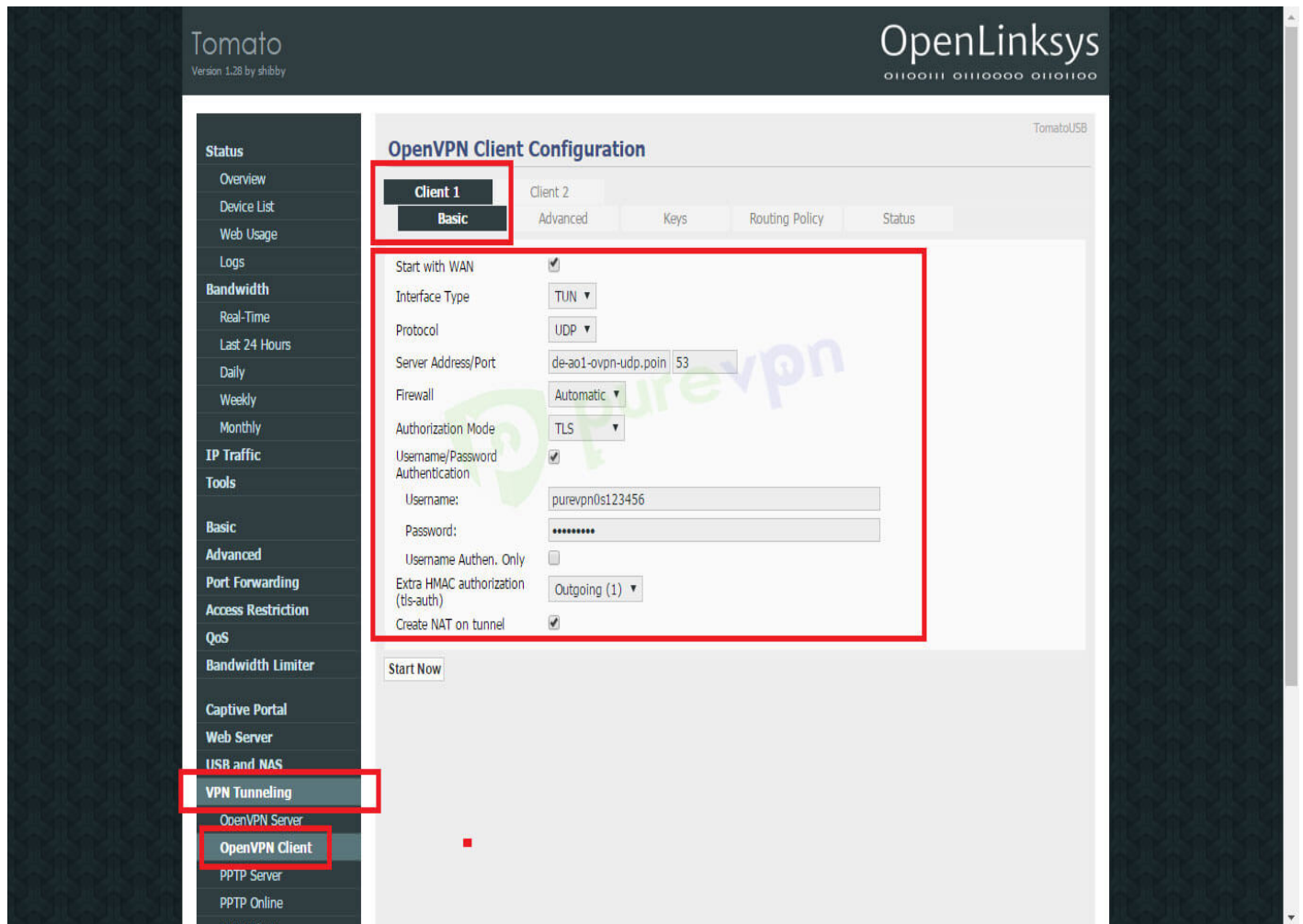
- You will be able to see and copy your VPN credentials.
- Note down your PureVPN username and click the **Eye icon** to make your password visible and use it in the manual configuration.

How to setup OpenVPN on Tomato Router

- Go to the Control Panel and select VPN Tunneling. Click on **OpenVPN Client** and select **Client 1** to enter the following details under the Basic Tab:
 1. From Drop Down in Interface Type select TUN
 2. In Protocol Drop down, select UDP
 3. To fill the Server Address Details, open the [downloaded .ovpn file](#) on notepad, copy the address of your desired server and paste it in the field
 4. Insert 53 for UDP in the port field
 5. Select Automatic in firewall
 6. Select TLS in Authorization Mode
 7. Select on Username/ Password Authentication
 8. Enter your Username and Password provided to you by PureVPN

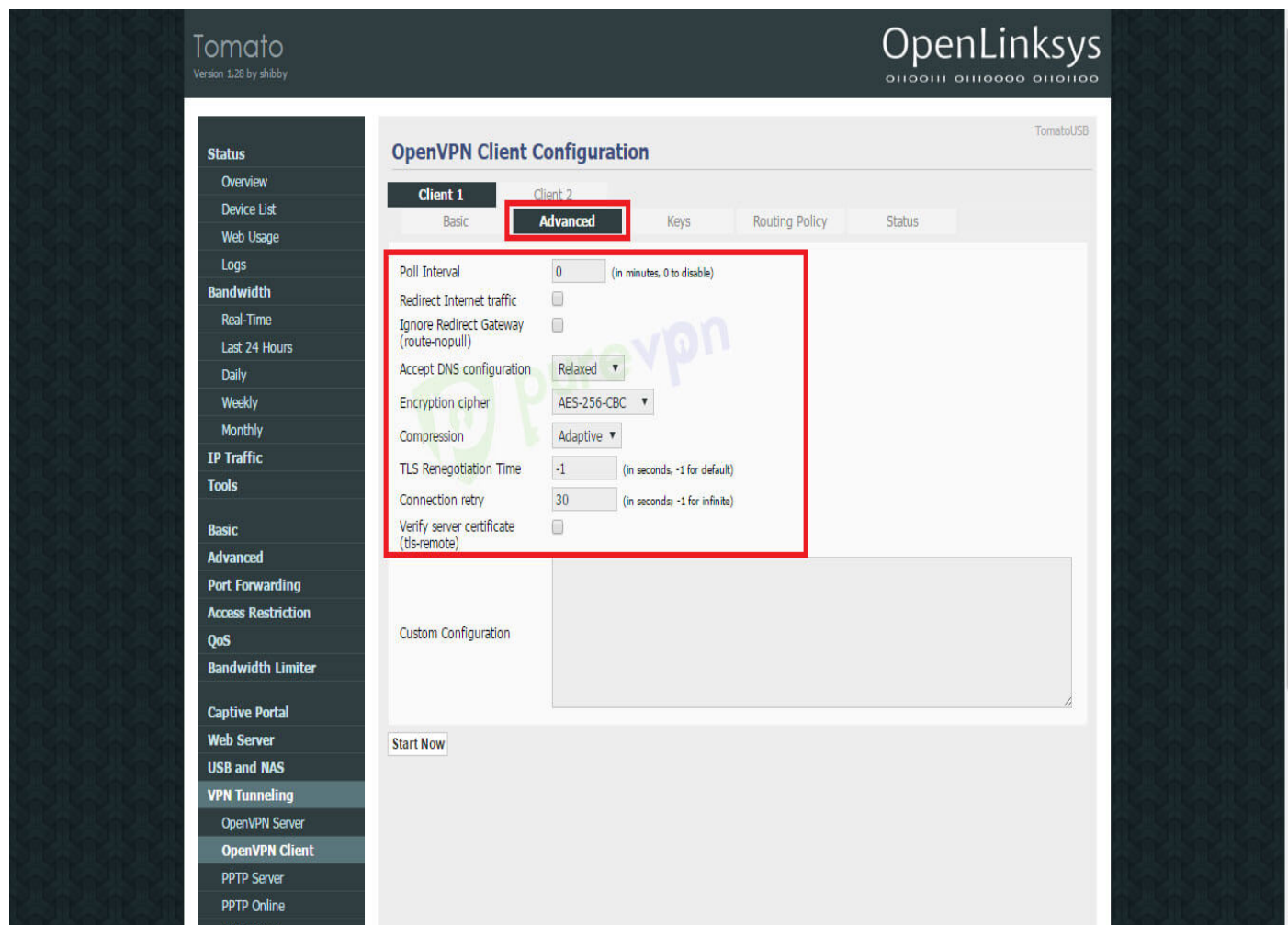
9. Uncheck the Username Authen. Only
10. Select Outgoing (1) in the drop down of Extra HMAC authorization (tls-auth-)
11. Check Create NAT on tunnel

Note: For TCP port, you need to change the port from UDP to TCP and select 80 instead 53 in the port field..



- **Go to Advance Tab and do as follows:**
 1. Enter 0 in the field Poll Interval
 2. Uncheck Redirect Internet Traffic

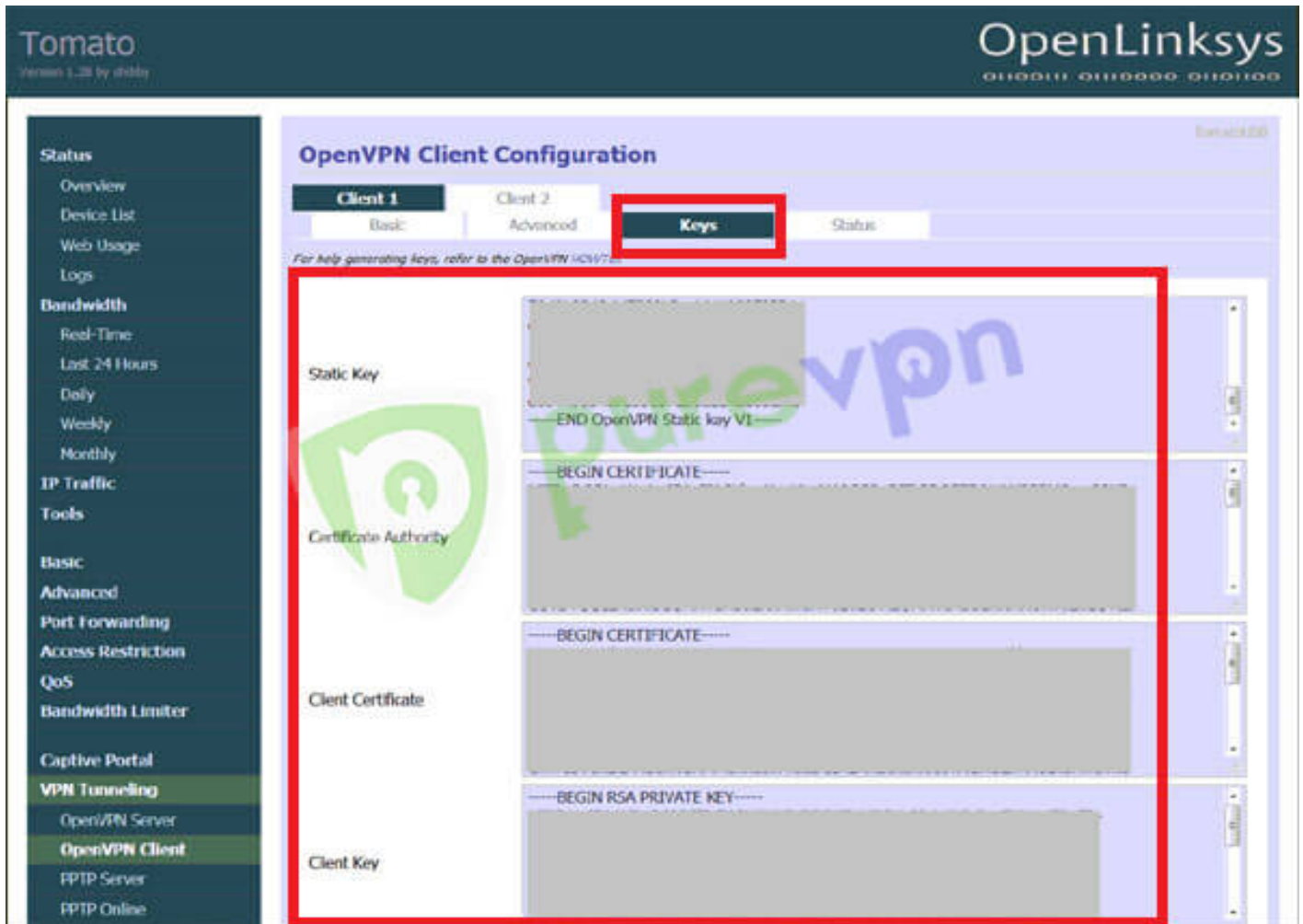
3. Select Relaxed in the drop down of Accept DNS Configuration
4. Select AES-256-CBC in the drop down of Encryption Cipher
5. Select Adaptive in Compression
6. Enter -1 in TLS Renegotiation
7. Enter 30 in Connection Retry
8. Uncheck the option Verify server certificate (tls-remote)



- **Go to the tab titled Keys and do as follows:**

1. For Static Key open the WDC.key in a notepad, copy all content and paste the content in the field.
2. For Certificate Authority, open CA.crt in a notepad, copy all its content and paste the content in the field.
3. For Client Certificate, open Client.crt in a notepad, copy all of the content and paste the content in the field.
4. For Certificate Key, open Client.key in a notepad, copy all its content and paste the

content in the field.



- Click on the **Save button** and then click on the **Start Now** button. After a few seconds, your VPN connection will be established. You can verify the VPN connection status by clicking on the **Status Tab**.

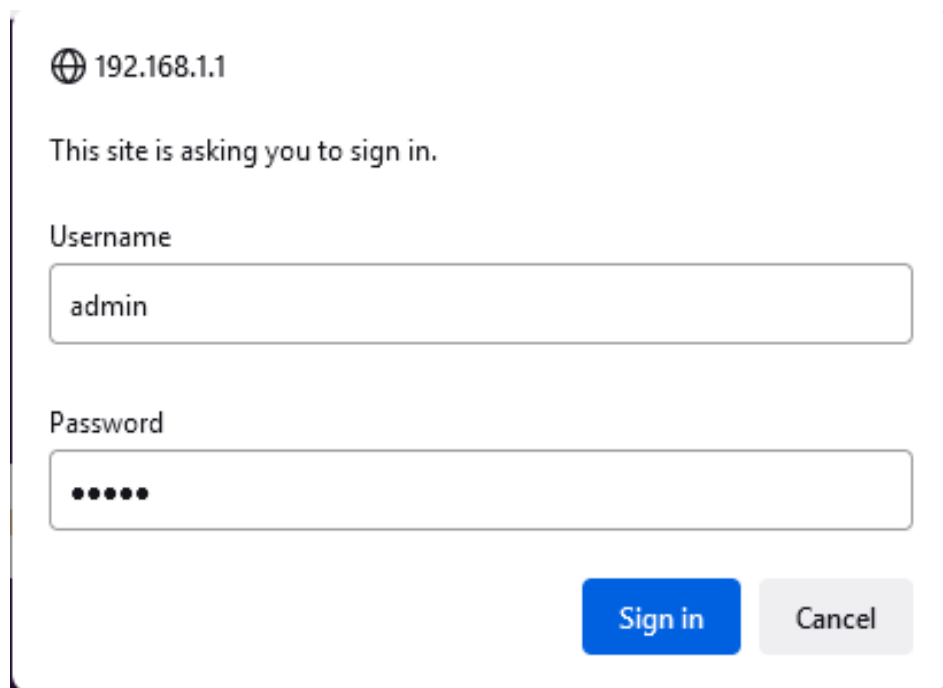


Note: Dedicated IP addon can be only be connected with Ras protocol i.e PPTP/L2TP/SSTP.

How to setup OpenVPN Connection Setup for Advanced Tomato v3.5

This article will guide you through the steps involved in setting up PureVPN OpenVPN on an Advanced Tomato firmware router. We have used the Netgear R7000 router flashed with the latest Advanced Tomato firmware version 3.5 to prepare this article:

- Log in to the router control panel by entering the router's default IP address 192.168.1.1 in the address bar of your preferred browser. (If you have changed your router's default IP address, enter that in your browser tab instead). Enter the admin name and password for your router, then click **Sign In**.



The screenshot shows a browser window with the address bar containing a globe icon and the IP address 192.168.1.1. Below the address bar, the text "This site is asking you to sign in." is displayed. There are two input fields: "Username" with the text "admin" and "Password" with six dots. At the bottom right, there are two buttons: a blue "Sign in" button and a grey "Cancel" button.

- In order to configure OpenVPN on Adv. Tomato, first download the required OpenVPN Files from [this](#) link.
- Now go to the **VPN** tab and select the **OpenVPN Client** option.

The screenshot shows the AdvancedTomato Status Overview page. The left sidebar has a dark background with a red box around the 'VPN' menu item, and a red arrow pointing to the 'OpenVPN Client' sub-item. The main content area is divided into three panels: System, LAN, and Wireless (5 GHz / eth2). A yellow attention banner at the top contains a warning icon and the text: 'Attention: You did not configure TomatoAnon project setting. Please go to [TomatoAnon configuration page](#) and make a choice.'

System	
Name	TomatoUSB
Model	Netgear R7000
Chipset	ARMv7 Processor rev 0 (v7l)
CPU Freq	1000 MHz (dual-core)
Flash Size	128MB
Time	Mon, 01 Nov 2021 11:05:58 +0100
Uptime	0 days, 00:18:01
CPU Usage	1.77%
CPU Load (1 / 5 / 15 mins)	0.04 / 0.05 / 0.05
Memory Usage	22.09 MB / 249.70 MB (8.85%)
NVRAM Usage	30.63 KB / 64.00 KB (47.85%)

LAN	
Router MAC Address	b0:39:56:cfa4:7e
Router IP Addresses	br0 (LAN) - 192.168.1.1/24
DHCP	br0 (LAN) - 192.168.1.2 - 192.168.1.51

Wireless (5 GHz / eth2)	
MAC Address	B0:39:56:CF:A4:81
Wireless Mode	Access Point
Wireless Network Mode	Auto
Interface Status	Up (LAN)
Radio	Enabled ✓
SSID	Tomato50

- **Now configure your OpenVPN client as shown below.**
- Under basic tab
 1. Start with WAN: Check
 2. Interface Type: TUN
 3. Protocol: Choose either UDP or TCP and keep it in mind as this will be important later on
 4. Server Address/Port: Enter your desired location's OpenVPN address. You can get your desired server address from [this](#) link.
 5. Enter port number 80 for TCP or port number 53 for UDP.
 6. Firewall: Automatic
 7. Authentication Mode: TLS
 8. Enter your PureVPN credentials. Here is how you can find your [VPN credentials](#).
 9. Extra HMAC authorization (tls-auth): Outgoing(1)
 10. Create NAT on tunnel: Check
- Click the **Save** button.

The screenshot displays the configuration page for 'VPN Client #1 (Stopped)'. At the top, there are navigation tabs: Basic, Advanced, Keys, Routing Policy, and Status. The configuration is organized into several rows, each with a label on the left and a control on the right. The controls include checkboxes, dropdown menus, and text input fields. The 'Save' button at the bottom left is highlighted with a red rectangular box.

Setting	Value
Start with WAN	<input checked="" type="checkbox"/>
Interface Type	TUN
Protocol	UDP
Server Address/Port	de2-auto-udp.ptoser 53
Firewall	Automatic
Authorization Mode	TLS
Username/Password Authentication	<input checked="" type="checkbox"/>
Username:	purevpn0
Password:	*****
Username Authen. Only	<input type="checkbox"/>
Extra HMAC authorization (tls-auth)	Outgoing (1)
Create NAT on tunnel	<input checked="" type="checkbox"/>

- **Under Advanced Tab:**
 1. Redirect Internet Traffic: Checked.
 2. Accept DNS configuration: Relaxed.
 3. Encryption Cipher: AES-256-CBC.
 4. Compression: Adaptive.
 5. TLS Renegotiation Time: -1
 6. Connection retry: 30
- Click the **Save** button.

The screenshot shows the configuration page for 'Client 1' in the 'Advanced' tab. The page title is 'VPN Client #1 (Stopped)'. The configuration options are as follows:

Option	Value	Notes
Poll Interval	0	(In minutes, 0 to disable)
Redirect Internet traffic	<input checked="" type="checkbox"/>	Highlighted with a red arrow
Accept DNS configuration	Relaxed	Dropdown menu
Encryption cipher	AES-256-CBC	Highlighted with a red box
Compression	Adaptive	Highlighted with a red box
TLS Renegotiation Time	-1	(In seconds, -1 for default)
Connection retry	30	(In seconds; -1 for infinite)
Verify server certificate (tls-remote)	<input type="checkbox"/>	
Custom Configuration		Text area

At the bottom, there are two buttons: 'Save ✓' (highlighted with a red box) and 'Cancel ×'.

- **Under Keys Tab:**
 1. For Static Key: Copy and paste all the content from the Wdc.key file you have from the previously downloaded the OpenVPN configuration files.
 2. For Certificate Authority: Copy and paste all the content from the ca.crt file.
 3. Client Certificate and Client Key: blank.
- Click the **Save button**.

Client 1 ✖ Client 2 ✖

Basic Advanced Keys Routing Policy Status

VPN Client #1 (Stopped)

For help generating keys, refer to the OpenVPN HOWTO.

Static Key

```
c737ad822f27e19057731f41e1e254cc  
9c95b7175c622422cde9f1f2cfd3510a  
dd94498b4d7133d3729dd214a16b27fb  
-----END OpenVPN Static key V1-----
```

Certificate Authority

```
xpeZQinof67nKrCsgz/xjktWFgcmPI4/POSsmqQD0fttWxGuRX+FzwwF2OCMCAJg  
p1RqjNik2g50/kBloJVPPCfjDFeDU5zGaWGSQ9+z1L6/z7VxjUIHL0ouOchWbiS  
4ZjTr9nMn6WdAHU2  
-----END CERTIFICATE-----
```

Client Certificate

Client Key

Save ✓ Cancel ✖

- Now under the **Status** tab.
- Click on **Start VPN Client** to establish/connect with the PureVPN OpenVPN connection.

Client 1 ✖ Client 2 ✖

Basic Advanced Keys Routing Policy Status

VPN Client #1 (Stopped)

Client is not running or status could not be read.

Start VPN Client 1

Refresh Status

Save ✓ Cancel ✖

You are connected to VPN now!!!

- In order to disconnect the OpenVPN connection, click on **Stop VPN Client** button.

Basic Advanced Keys Routing Policy **Status**

VPN Client #1 (Running)

Data current as of Mon Nov 1 12:14:59 2021.

General Statistics

Name	Value
TUN/TAP read bytes	457600
TUN/TAP write bytes	878789
TCP/UDP read bytes	937067
TCP/UDP write bytes	511418
Auth read bytes	878853
pre-compress bytes	0
post-compress bytes	0
pre-decompress bytes	0
post-decompress bytes	0

Refresh Status

Save ✓ Cancel ×

Stop VPN Client 1

Was this article helpful? Rate and share your comments below. Your input matters to us and everyone else in the Cyber Security Community.