

Justin Linder

VPN Project

OpenVPN and Proton VPN

Virtual Private Networks (VPNs)

VPNs or Virtual Private Networks can either be free/open-source or are paid for as a service provided by an outside company that will usually provide resources like VPN servers and added features/services with VPN. Open-source VPNs are available to the public for free. These require that a user provides VPN server for their VPN clients.

OpenVPN is a very popular one, and it utilizes its own OpenVPN tunneling protocol.

The OpenVPN protocol is in Proton third party VPN servers can also be used in OpenVPN protocol on a router (as the VPN server) or you can download an OpenVPN server from their website.

The **OpenVPN tunnelling protocol** uses SSL/TLS protocol in tunneling protocol.

SSL or secure socket layer protocol uses AES-256 encryption algorithm. Good connection speeds. Communication through firewalls. OpenSSL and TSL key exchange.

All OpenSSL authentication, certification, and encryption are compatible with OpenVPN.

All key exchange types for TLS are compatible with OpenVPN.

OpenVPN protocol via the OpenVPN Cloud has more options like IDS/IPS, remote VPN connection that are protected, filtering content with DNS, end to end encryption, and more advanced routing options. It uses OpenVPN tunneling protocol.

Free version of OpenVPN cloud available via <https://openvpn.net/cloud-vpn/pricing/>

The **OpenVPN client** needs to be downloaded from OpenVPN as well since OpenVPN protocol does not come preinstalled on systems like Windows. This will be able to communicate with OpenVPN server or Access Server.

OpenVPN has a client application software called “**OpenVPN Connect**”. Compatible with Linux, Windows, macOS, iOS, and Android.

OpenVPN connect has kill switch too to mitigate man in the middle styled attacked.

OpenVPN can tunnel via UDP or TCP for virtual ethernet adapters any sub netted IP network including ones utilizing NAT.

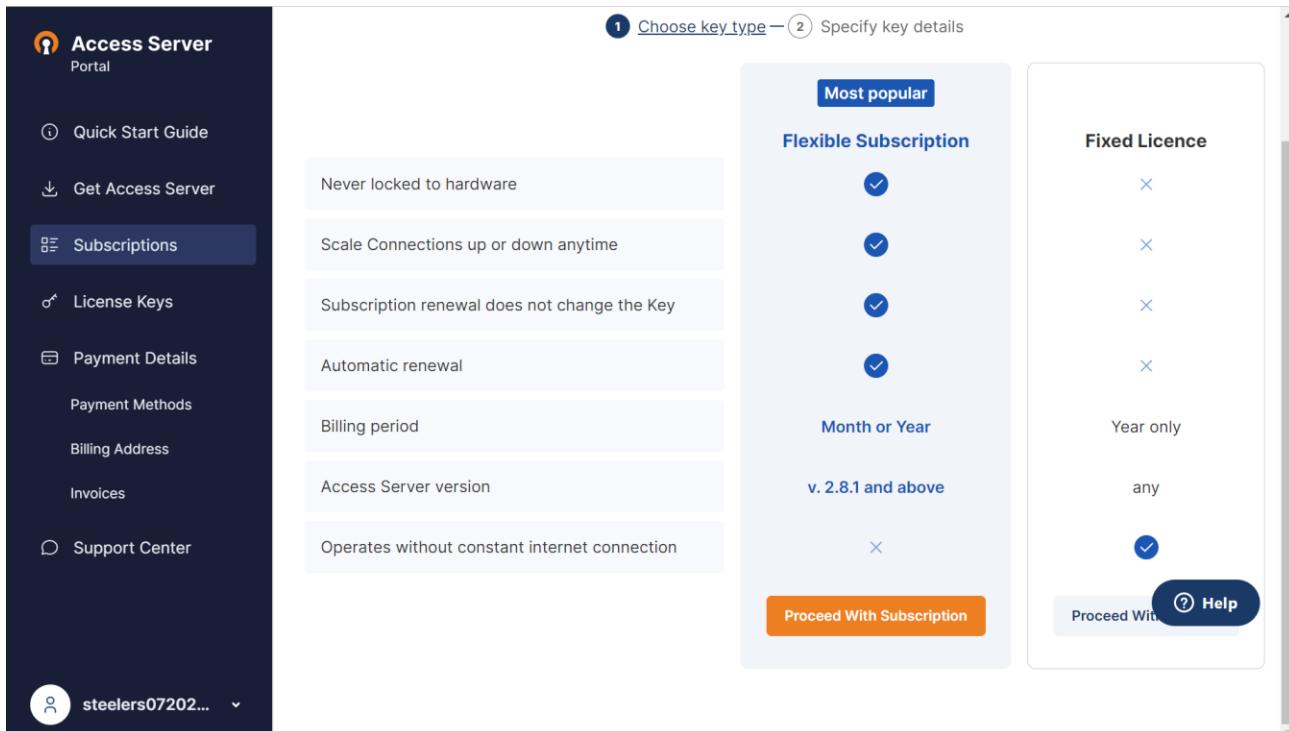
Keep in mind that OpenVPN tunneling protocol is a separate/different protocol than the other encryption protocols used such as PPTP, L2TP, IPsec, SSTP, SSL & TLS, and IKEv2. (And SSH).

Need an OpenVPN client (and it does not have to be through OpenVPN Connect).

That way the OpenVPN client will be the app and can transmit traffic to encrypted tunnel where that traffic is then encrypted, and then it goes to the OpenVPN server (on access point in this scenario) where it is decrypted and then the traffic goes back in the reverse direction. The OpenVPN server can be an access point/WAP, router or another wireless device with OpenVPN server. The OpenVPN server could also be referred to as the “Access Server”.

Free version of OpenVPN Access Server available for download via
<https://openvpn.net/access-server/pricing/>

Go to your Access Server.



The screenshot shows the 'Access Server Portal' interface. On the left sidebar, 'Subscriptions' is selected. The main area displays a two-step process: 'Choose key type' (step 1) and 'Specify key details' (step 2). Step 1 is titled 'Most popular' and includes options: 'Never locked to hardware' (checked), 'Scale Connections up or down anytime' (checked), 'Subscription renewal does not change the Key' (checked), and 'Automatic renewal' (checked). Step 2 includes 'Month or Year' (Year only checked), 'v. 2.8.1 and above' (any checked), and 'Operates without constant internet connection' (unchecked). At the bottom are 'Proceed With Subscription' and 'Help' buttons.

Click on “Subscriptions” on the left side column. Then choose “Flexible Subscriptions” and click on “Proceed with Subscription”.

The screenshot shows the Access Server Portal interface. On the left, a sidebar menu includes 'Quick Start Guide', 'Get Access Server', 'Subscriptions' (which is selected and highlighted in blue), 'License Keys', 'Payment Details', 'Payment Methods', 'Billing Address', 'Invoices', and 'Support Center'. A user profile icon for 'steelers07202...' is at the bottom. The main content area is titled 'Create Activation key' with the sub-instruction 'Choose a plan and the number of connections you need. Cost per connection decreases as your number of connections increases.' A checked checkbox says 'Choose key type — 2 Specify key details'. Below is a question 'How many concurrent connections does your company need?' with a slider set to '2'. The slider scale ranges from 'Free' to 'More' with increments of 5, 10, 25, 50, 100, 250, 500, 1000, and 2000. At the bottom right are 'Help', 'Total for Subscription: Free', 'Create' (in orange), and 'Back' buttons.

Choose 2 connections since that is the only free option and click on “Create”.

The screenshot shows the 'Subscription 1 (Free)' details page. The sidebar is identical to the previous screenshot. The main content shows 'Subscription 1 (Free)' with tabs for 'Details' (selected) and 'Access Server Information'. Under 'VPN Connections', there is a table with columns 'Term', 'Next Billing Date', 'Next Payment', and 'Attached Payment Method'. The 'Attached Payment Method' row shows 'No auto charge'. Below is a 'Subscription ID' field containing 'ASIdESwCLvZWoKHWbYUNGJQYzzyVCoTt'. A 'Subscription Key' field contains a long string of asterisks (*). A 'Copy Key' button is next to it. A note at the bottom says: 'Please go to your Access Server WebUI interface and paste the key there in Configuration → Activation Page, or use a build in command-line tool. Refer to the [Troubleshooting Guide](#) for exact instructions.' A warning message in a red box at the bottom states: '⚠ Ensure that Access Server has constant direct access to asb.sts.openvpn.net on port TCP 443 (no proxy). Only works on Access Server v2.8.1 and higher.'

Copy subscription key.

Access Server
Portal

- Quick Start Guide
- [Get Access Server](#)
- Subscriptions
- License Keys
- Payment Details
- Payment Methods
- Billing Address
- Invoices
- Support Center

Get Access Server

Provide secure access to your private business network, in the cloud or on-premise. Already have an Access Server? Here's how to [Update It](#). Read [Release Notes](#) about the last changes.

We now also offer **OpenVPN Cloud**, a cloud-delivered service that integrates virtual networking with essential security capabilities. [Learn More](#)

As a Software Package

Our software repositories for Ubuntu LTS, Debian, CentOS, Red Hat, and AL2 make installing and keeping up-to-date with Access Server on your Linux installation easy. You may also download and save packages for an offline installation if your system does not have Internet access.

 Ubuntu LTS
 Redhat
 Centos
 Debian
 Amazon Linux 2

[Help](#)

Then go to “Get Access Server” on the left side of the column.

You can either install it as a software package on Linux systems like CentOS, Redhat, Ubuntu LTS, Debian, and Amazon Linux 2.

Or you can install it as a Cloud image if using cloud services for your Access Server.

Or you can download it for a VM or hypervisor.

Quick Start Guide

[Get Access Server](#)

Subscriptions

License Keys

Payment Details

Payment Methods

Billing Address

Invoices

Support Center

steelers07202... ▾

As a Cloud Image

On the major cloud infrastructure providers Amazon AWS, Microsoft Azure, Google Cloud, Digital Ocean and Oracle Cloud, we offer our ready-to-use deployment images of OpenVPN Access Server for these platforms. If your chosen cloud provider is not listed, you can still deploy a standard Linux installation and use the 'install on my own server' option instead.

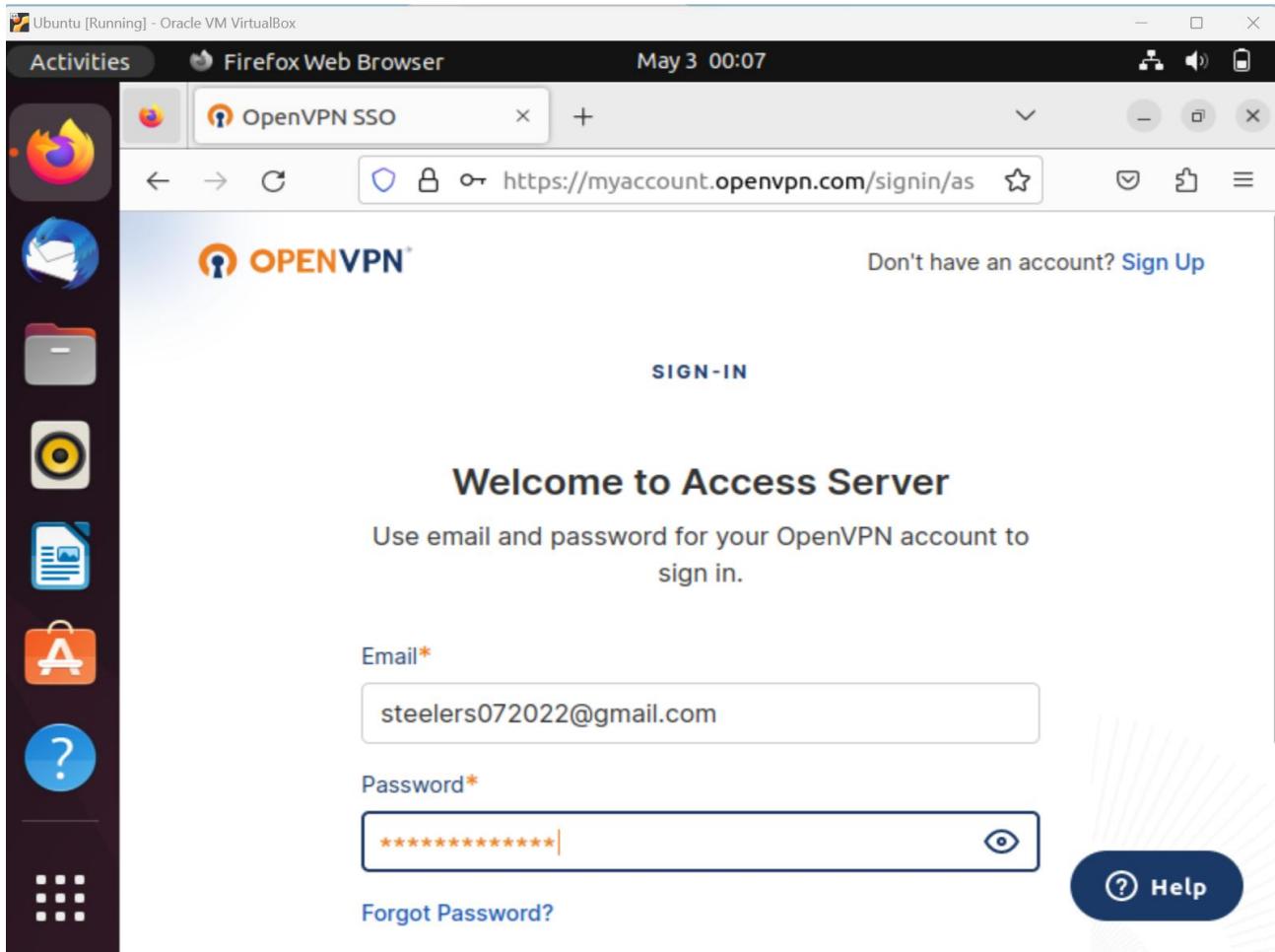
 AWS
 Digital Ocean
 Azure
 Oracle
 GCP

As a Virtual Appliance

The Access Server Virtual appliance provides easier installation of our VPN Server software and is available for two hypervisor solutions: VMware ESXi and Microsoft Hyper-V.

 VMware ESXi
 Microsoft HyperV

[Help](#)



Login to Access Server.

Open a command line in your environment.

```
jay@jay-VirtualBox:~$ sudo nano /etc/sudoers  
jay@jay-VirtualBox:~$ sudo visudo
```

Run these commands to first check and then edit sudoers list if your user needs root privileges.

```
GNU nano 6.2                               /etc/sudoers.tmp *
# Per-user preferences; root won't have sensible values for them.
Defaults: %sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
Rhythmbox sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
Defaults: %sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
jay     ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:
```

```
jay@jay-VirtualBox:~$ sudo usermod -a -G sudo jay
jay@jay-VirtualBox:~$ groups
jay adm cdrom sudo dip plugdev lpadmin lxd sambashare
```

Or can add user to sudo group for root privileges.

```
jay@jay-VirtualBox:~$ sudo apt update
[sudo] password for jay:
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
```

Then update.

```
jay@jay-VirtualBox:~$ sudo apt update && apt -y install ca-certificates wget net-tools gnupg  
[sudo] password for jay:  
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease  
Hit:2 http://us.archive.ubuntu.com/ubuntu jammy InRelease  
Hit:3 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease  
Hit:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
All packages are up to date.
```

Run this command first.

```
jay@jay-VirtualBox:/$ sudo wget https://as-repository.openvpn.net/as-repo-public.asc -qO /etc/apt/trusted.gpg.d/as-repository.asc  
jay@jay-VirtualBox:/$ sudo echo "deb [arch=amd64 signed-by=/etc/apt/trusted.gpg.d/as-repository.asc] http://as-repository.openvpn.net/as/debian jammy main">/etc/apt/sources.list.d/openvpn-as-repo.list
```

Then run these 2 commands.

```
total 0  
jay@jay-VirtualBox:/$ sudo apt update && apt -y install openvpn-as  
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease  
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease  
Hit:3 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease  
Hit:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done
```

This is the first way to do it but if there is another way if it doesn't work.

If that does not work then run this command below.

```
jay@jay-VirtualBox:/$ sudo apt install -y bridge-utils dmidecode iptables iproute2 libc6 libffi7 libgcc-s1 liblz4-1 liblz4-2 libmariadb3 libpcap0.8 libssl3 libstdc++6 libsasl2-2 libsqlite3-0 net-tools python3-pkg-resources python3-migrate python3-sqlalchemy python3-mysqldb python3-ldap3 sqlite3 zlib1g python3-netaddr python3-arrow python3-lxml python3-constantly python3-hyperlink python3-automat python3-service-identity python3-cffi python3-defusedxml
```

NOTE:

```
jay@jay-VirtualBox:~/Downloads$ sudo apt --fix-broken install  
Reading package lists... Done
```

If still having trouble, run this command.

```
To reconfigure manually, use the /usr/local/openvpn_as/bin/ovpn-init tool.  
+++++  
Access Server 2.11.3 has been successfully installed in /usr/local/openvpn_as  
Configuration log file has been written to /usr/local/openvpn_as/init.log  
  
Access Server Web UIs are available here:  
Admin UI: https://10.0.2.15:943/admin  
Client UI: https://10.0.2.15:943/  
To login please use the "openvpn" account with "nJdwFLWj0kDc" password.  
(password can be changed on Admin UI)  
+++++
```

This should be displayed afterwards for login credentials.

Go to the web URL for admin “<https://10.0.2.15:943/admin>”

```
jay@jay-VirtualBox:~$ sudo dpkg -i ~/Downloads/openvpn-as-bundled-clients-27.deb ~/Downloads/openvpn-as_2.11.3-af31575c-Ubuntu22_amd64.deb
```

Run this command after downloading the 2 packages from Access Server.

```
jay@jay-VirtualBox:~/Downloads$ sudo dpkg -i openvpn-as-bundled-clients-27.deb openvpn-as_2.11.3-af31575c-Ubuntu22_amd64.deb
(Reading database ... 202752 files and directories currently installed.)
Preparing to unpack openvpn-as-bundled-clients-27.deb ...
Unpacking openvpn-as-bundled-clients (27) over (27) ...
Preparing to unpack openvpn-as_2.11.3-af31575c-Ubuntu22_amd64.deb ...
Upgrade detected (debian)...
Unpacking openvpn-as (2.11.3-af31575c-Ubuntu22) over (2.11.3-af31575c-Ubuntu22) ...
Setting up openvpn-as-bundled-clients (27) ...
Setting up openvpn-as (2.11.3-af31575c-Ubuntu22) ...
Backing up configuration and DB files to /usr/local/openvpn_as/etc/backup/2023-05-03T01:35:43-04:00 before update.
jay@jay-VirtualBox:~/Downloads$
```

Can either use full file path or do it like this by switching to directory first to install packages that were downloaded.

The screenshot shows the Access Server Portal interface on an Ubuntu desktop. The main window title is "Finishing Configuration". The left sidebar lists "Access Server Portal" with sections: Quick Start Guide, Get Access Server, Subscriptions, License Keys, Payment Details, Payment Methods, Billing Address, Invoices, and Support Center. The central content area has two large code blocks:

Option One

```
1 apt update && apt -y install ca-certificates wget net-tools gnupg
2 wget https://as-repository.openvpn.net/as-repo-public.ssc -qO /etc/apt/trusted.gpg.d/as-repository.asc
3 echo "deb [arch=amd64 signed-by=/etc/apt/trusted.gpg.d/as-repository.asc] http://as-repository.openvpn.net/as/debian jammy main">/etc
   /apt/sources.list.d/openvpn-as-repo.list
4 apt update && apt -y install openvpn-as
```

Note: these steps are suitable for a fresh install and for upgrading an existing installation.

After these steps, your Access Server should be installed and awaiting further configuration.
Consult our quick start guide for further instructions on how to configure and use your Access Server.

Option Two

Manually download packages

If for some reason you can or will not use the recommended installation via the official OpenVPN Access Server software repository, you can instead download the packages separately to your server and install them. You will need to be logged on to your Linux system either on the console or via SSH, and have root privileges. Then copy and paste the commands below to download the necessary package installer files and install the OpenVPN Access Server client bundle and the OpenVPN Access Server package itself. You may also use the buttons below to download the package files manually to your computer.

```
1 apt update
2 apt install -y bridge-utils dmidecode iptables iproute2 libcurl libffi7 libgcc-s1 liblzo2-1 liblzo2-2 libmariadb3 libpcap0.8 libssl13 libstdc++6 libsqlite3-0 net-tools python3-pkg-resources python3-migrate python3-sqlalchemy python3-mysqldb python3-ldap3 sqlite3 zlib1g python3-netaddr
   python3-arrow python3-lxml python3-constantly python3-hyperlink python3-automat python3-service-identity python3-cffi python3-defusedxml
3 dpkg -i openvpn-as-bundled-clients-27.deb openvpn-as_2.11.3-af31575c-Ubuntu22_amd64.deb
```

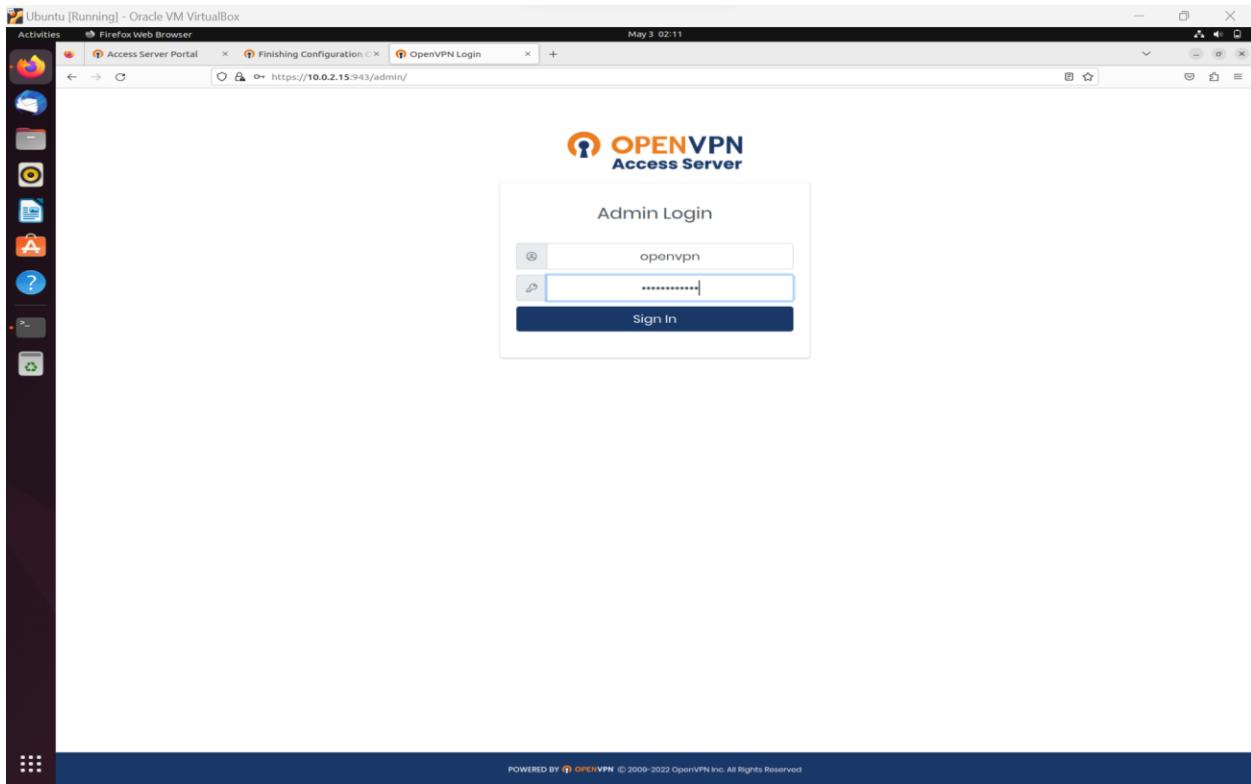
Note: these steps are suitable for a fresh install and for upgrading an existing installation.

[AS 2.11.3 For Ubuntu 22, 64 bits](#) [AS Client Bundle](#)

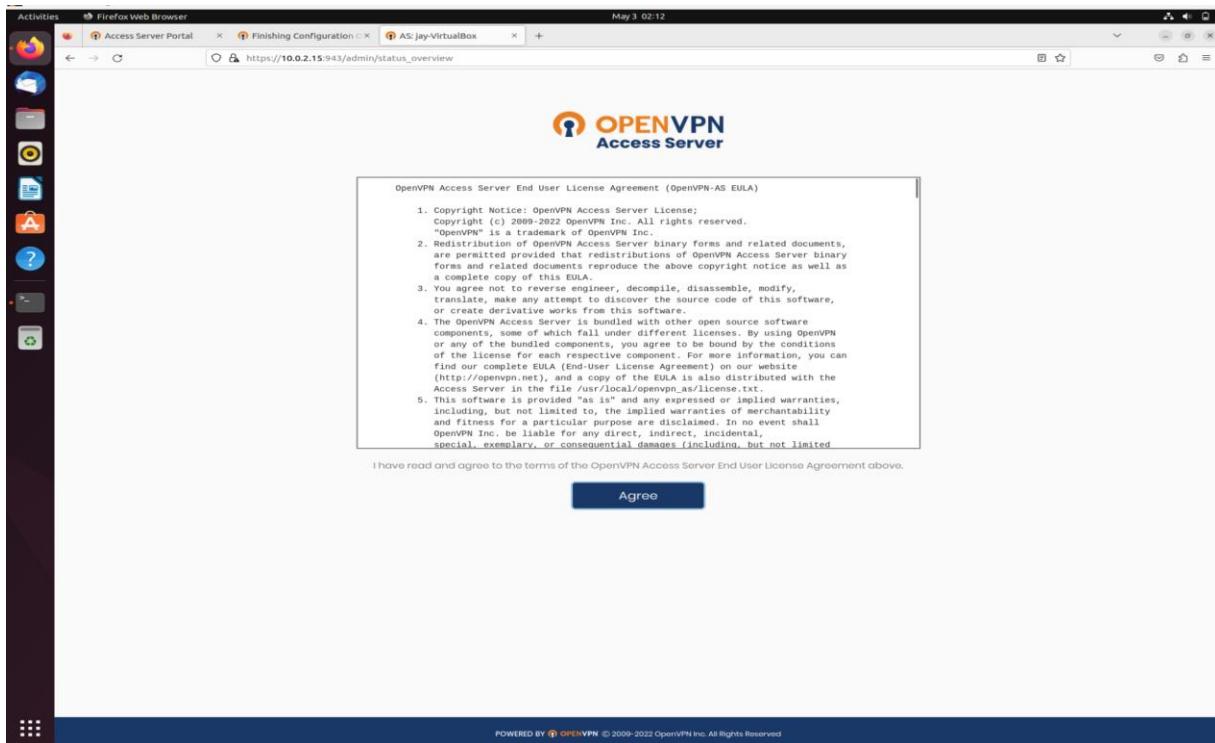
Our downloaded software packages can be verified for authenticity using the program sha256sum. See data.

After these steps, your Access Server should be installed and awaiting further configuration.
Consult our quick start guide for further instructions on how to configure and use your Access Server.

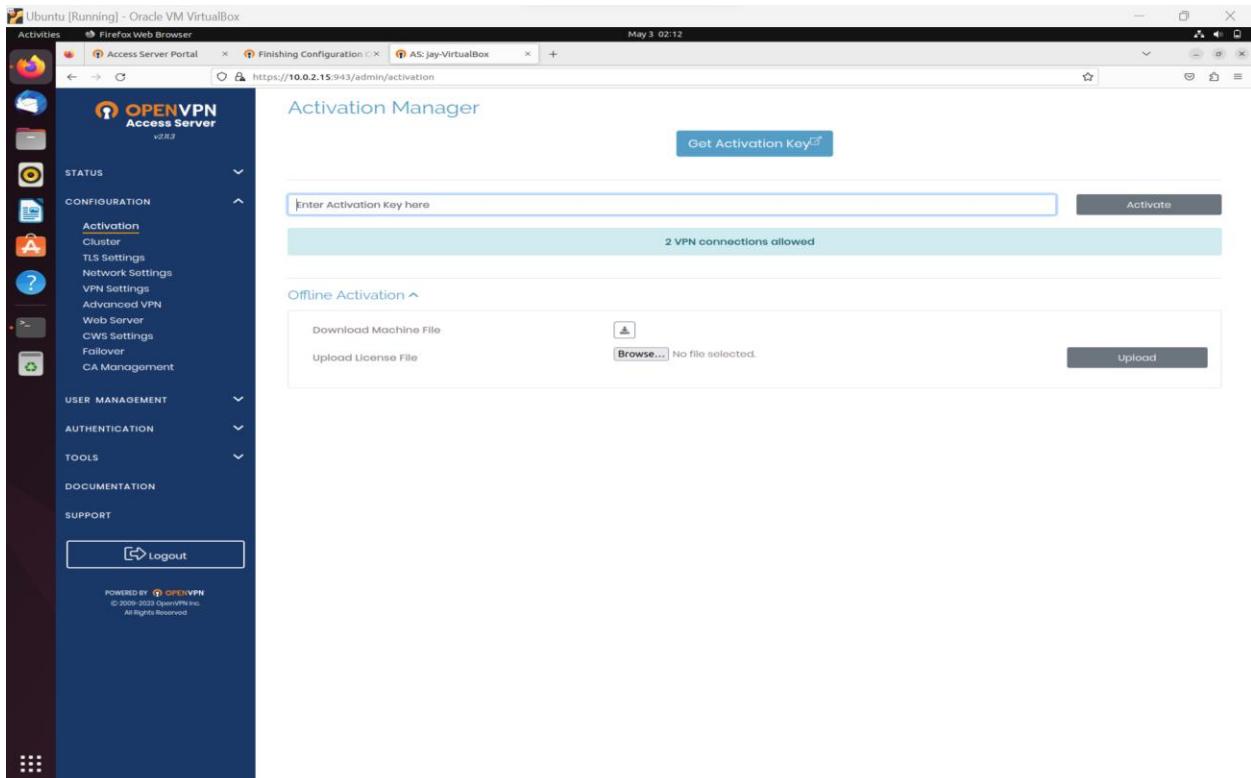
The 2 packages are right here on the Access Server portal.



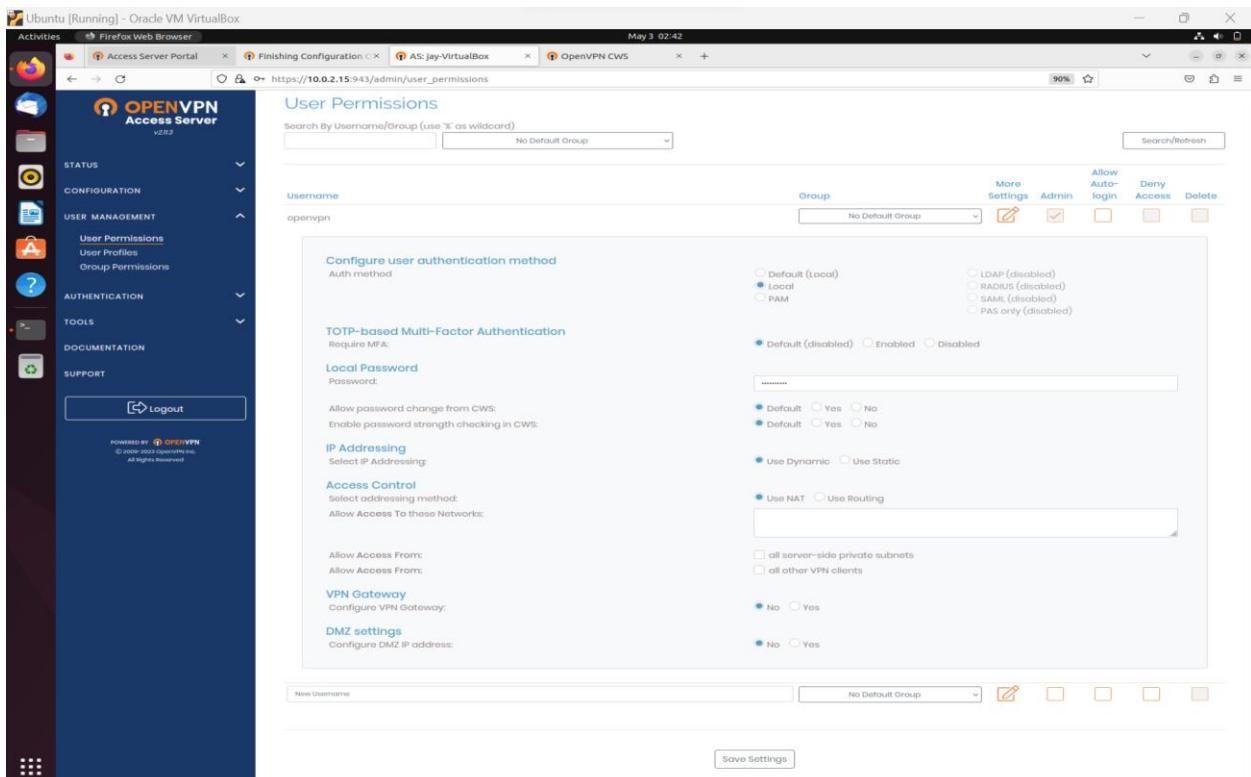
Login to “admin” Access Server interface.



Click on “Agree”.



On left side column click on “Activation” underneath “Configuration”.



Can change the password in “User Permissions” under “User Management”.

The screenshot shows the OpenVPN Access Server interface at the URL https://10.0.2.15:943/admin/user_permissions. A green success message box at the top right says "User Permissions Changed" and "Changed permissions for 1 user: openvpn". It includes a button to "Update Running Server". Below this, the "User Permissions" section lists a single user "openvpn" under "No Default Group". The user has "Admin" checked in the "More Settings" column and "Allow Auto-login" checked in the "Allow Auto-login" column. Buttons for "Save Settings" and "Logout" are visible.

Click on “Update Running Server” when done to make sure changes are applied.

This screenshot shows the "User Permissions" page for the "openvpn" user. A large configuration dialog is overlaid on the main table. The "Auth method" section shows "Local" selected. The "TOTP-based Multi-Factor Authentication" section has "Default (disabled)" selected. Under "Local Password", "Default" is selected. In the "IP Addressing" section, "Use Dynamic" is selected. The "Access Control" section shows "Allow Access To these Networks:" and "Allow Access From:" fields. The "VPN Gateway" section has "No" selected. The "DMZ settings" section also has "No" selected. At the bottom of the dialog, there is a "Save Settings" button.

Can also add another user to server on the bottom with its own password.

The screenshot shows the 'User Permissions' section of the OpenVPN Access Server administration interface. At the top, a green success message states 'User Permissions Changed' and 'User 'jayvpn' added.' Below this, a button says 'Press the button below to propagate the changes to the running server.' A large green button labeled 'Update Running Server' is visible. The main table lists a single user entry:

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
New Username	No Default Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

At the bottom right of the table area is a 'Save Settings' button.

Make sure to Update Running Sever again.

The screenshot shows the 'Activation Manager' section of the OpenVPN Access Server administration interface. The left sidebar includes 'Activation' under 'Configuration'. The main area displays an activation key in a text input field: 'skdfQVNjZEVTd9NmldpXbdrIV2JzVUSnslFZenzpSVkNVvHR0TYSMWZhnjhjzeyNWU2YjBjNmzjODNNTc4Zt13NjfhOWfjNWiz2MyisCIAgimhhdCigOixaNjgzMDc5Mjlk2Ch0=|. The 'Activate' button is located to the right of the key field. Below the key field, a message says '2 VPN connections allowed'. At the bottom, there is an 'Offline Activation' section.

Go to "Activation" under "Configuration" on left side column.

Then, click “Get Activation Key”.

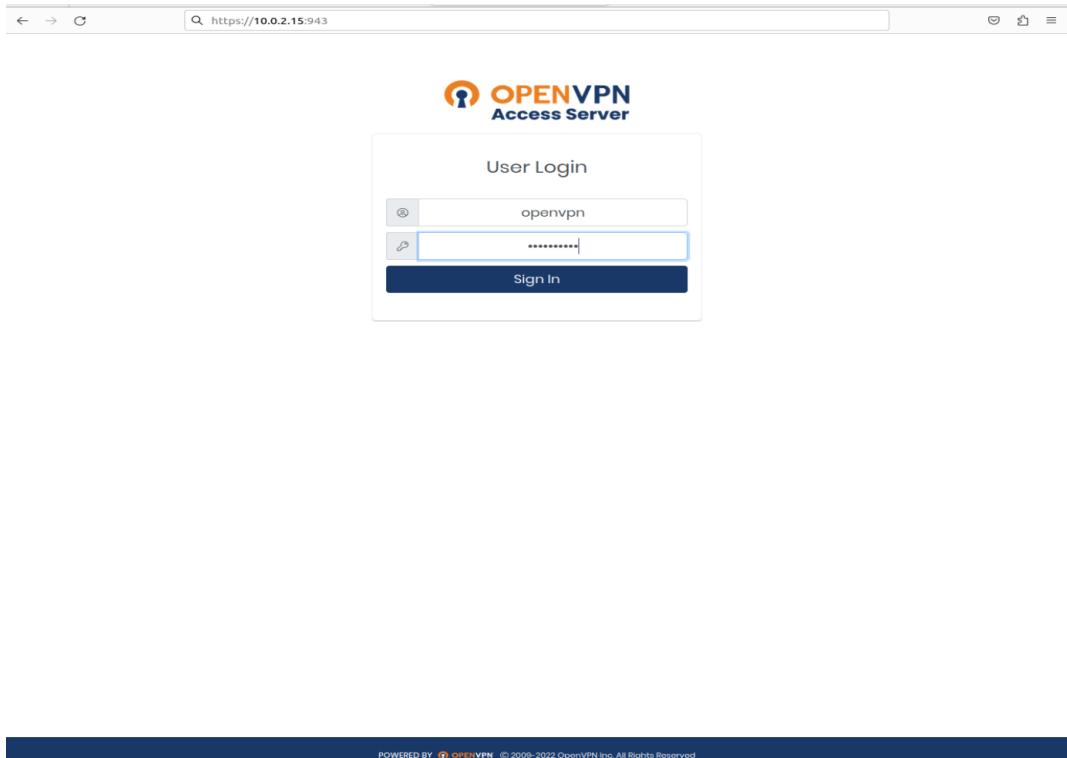
The screenshot shows the Activation Manager interface of the OpenVPN Access Server. On the left, a dark sidebar lists various configuration options under 'CONFIGURATION' such as Activation, Cluster, TLS Settings, Network Settings, VPN Settings, Advanced VPN, Web Server, CWS Settings, Follower, and CA Management. The main content area is titled 'Activation Manager' and contains a green banner with the text 'Subscription is active and operating normally'. Below this, there is a text input field labeled 'Enter Activation key here' and a 'Replace' button. At the top right, there is a 'Get Activation Key' button. The status bar at the bottom indicates '90%'.

Should get message that it is active and operating normally.

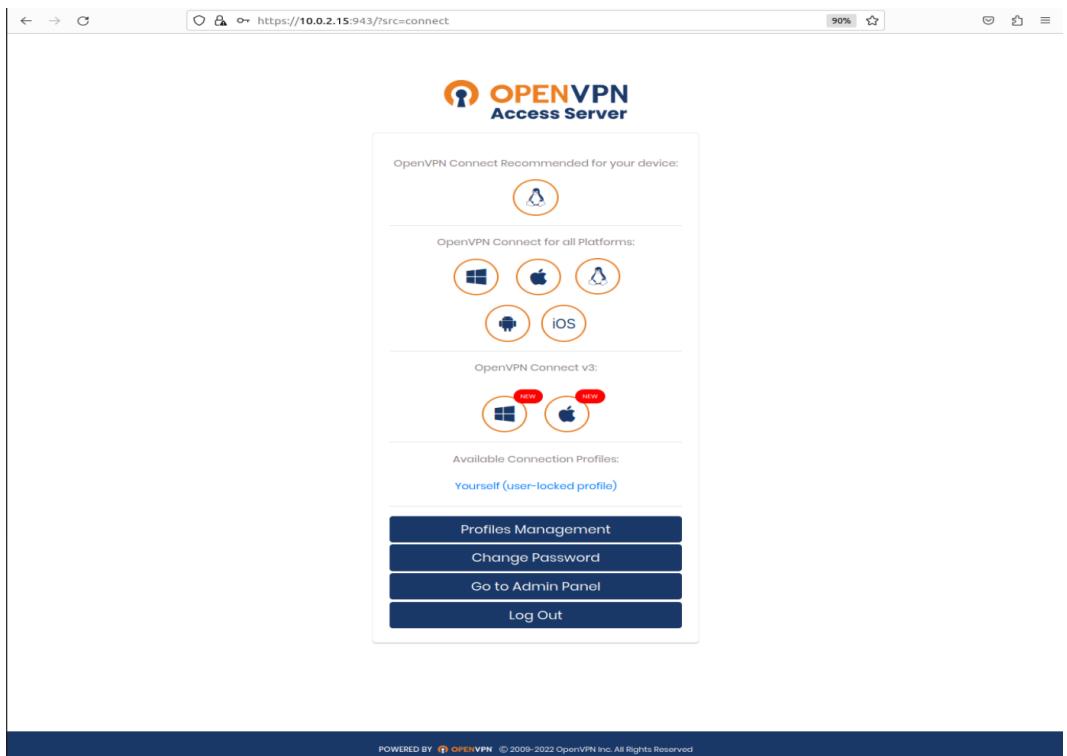
The screenshot shows the 'Server Network Settings' page of the OpenVPN Access Server. The left sidebar highlights 'Network Settings' under 'CONFIGURATION'. The main content area includes sections for 'VPN Server' (warning about changing hostnames), 'Interface and IP Address' (set to 'Listen on all interfaces' with 'enp0s3: 10.0.2.15'), 'Protocol' (TCP, UDP, Both), and 'Multi-Daemon Mode' (TCP and UDP daemons set to 2). There are also 'Web Service forwarding settings' for Admin and Client Web servers. The status bar at the bottom indicates '90%'.

Can change the Hostname/IP address under “Network Settings” which is under “Configuration” on the left side column.

Now go to client VPN interface which for me is" <https://10.0.2.15:943>"



Sign in as client. (Can be done on mobile devices like smartphones too with compatible O.S)

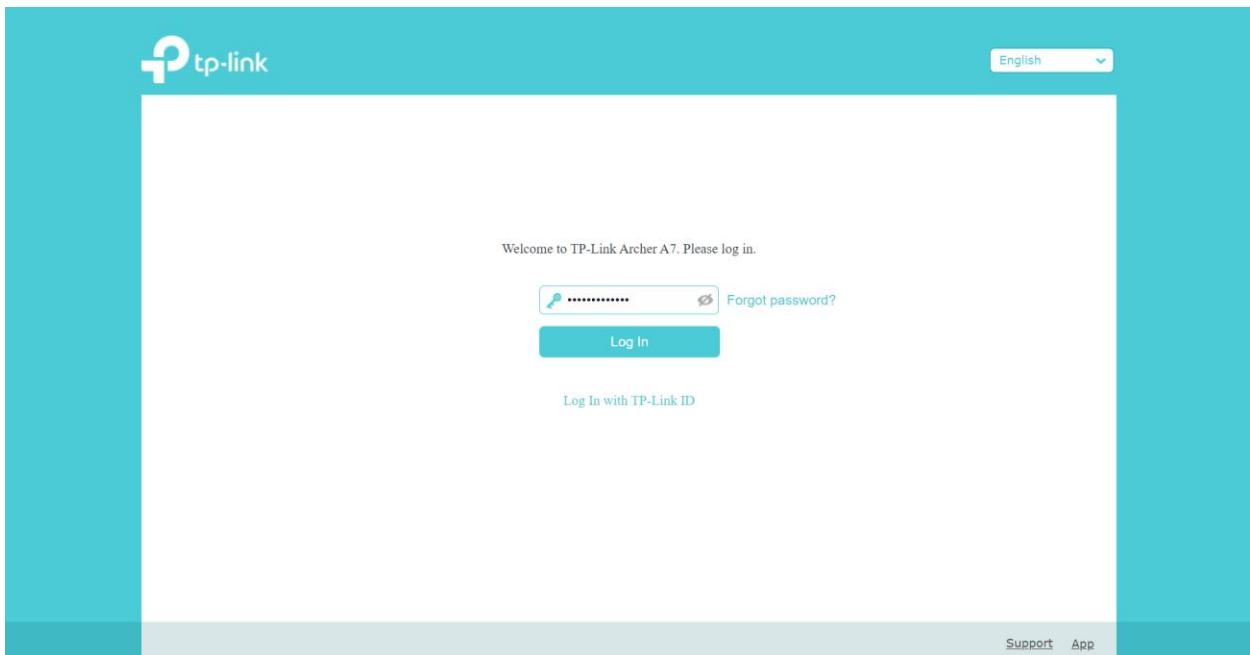


Now the client can download the OpenVPN connect to use OpenVPN via OpenVPN tunnelling protocol.

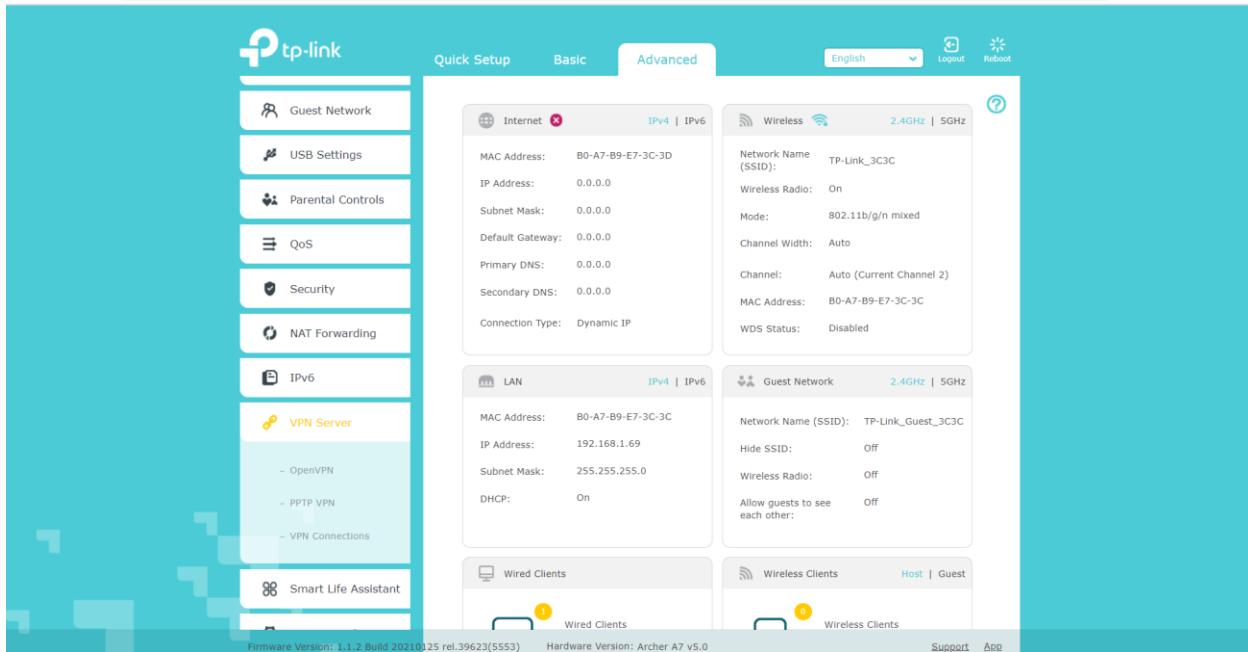
Linux requires a few commands which it walks you through.

Windows and MacOS “OpenVPN Connect v3” are the BEST one to use and is the newest versions (quickest usually).

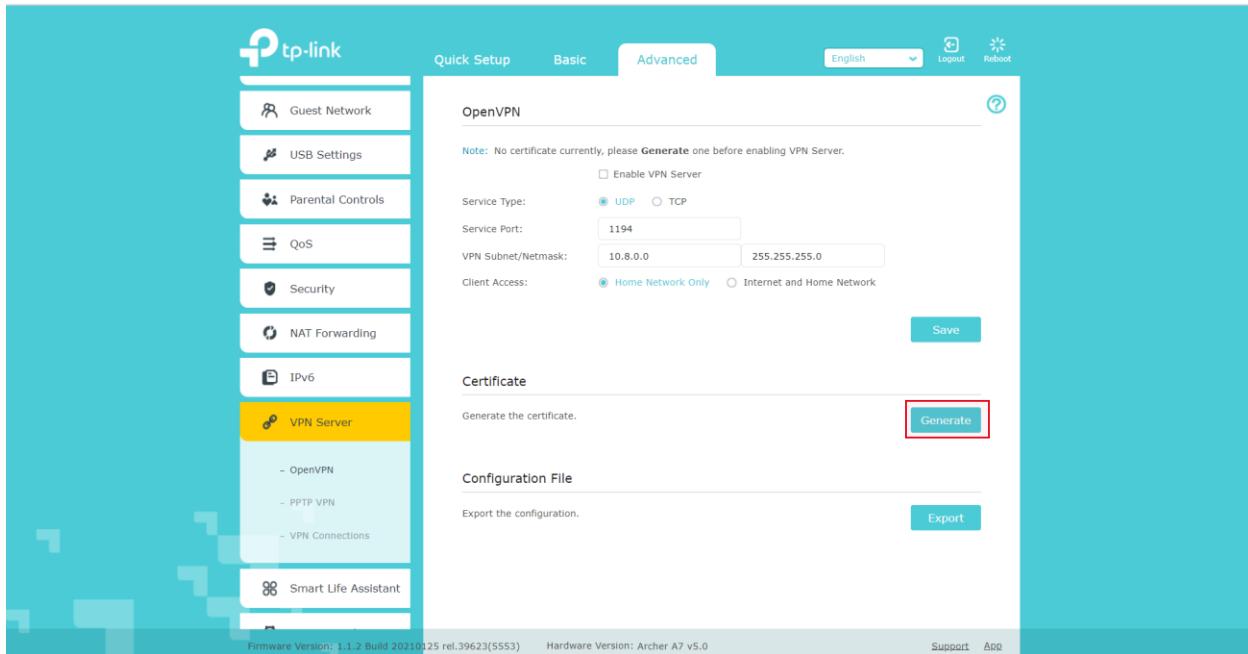
Aside from configuring an OpenVPN server on your computer it can also be done a wireless device like a router or Wireless Access Point.



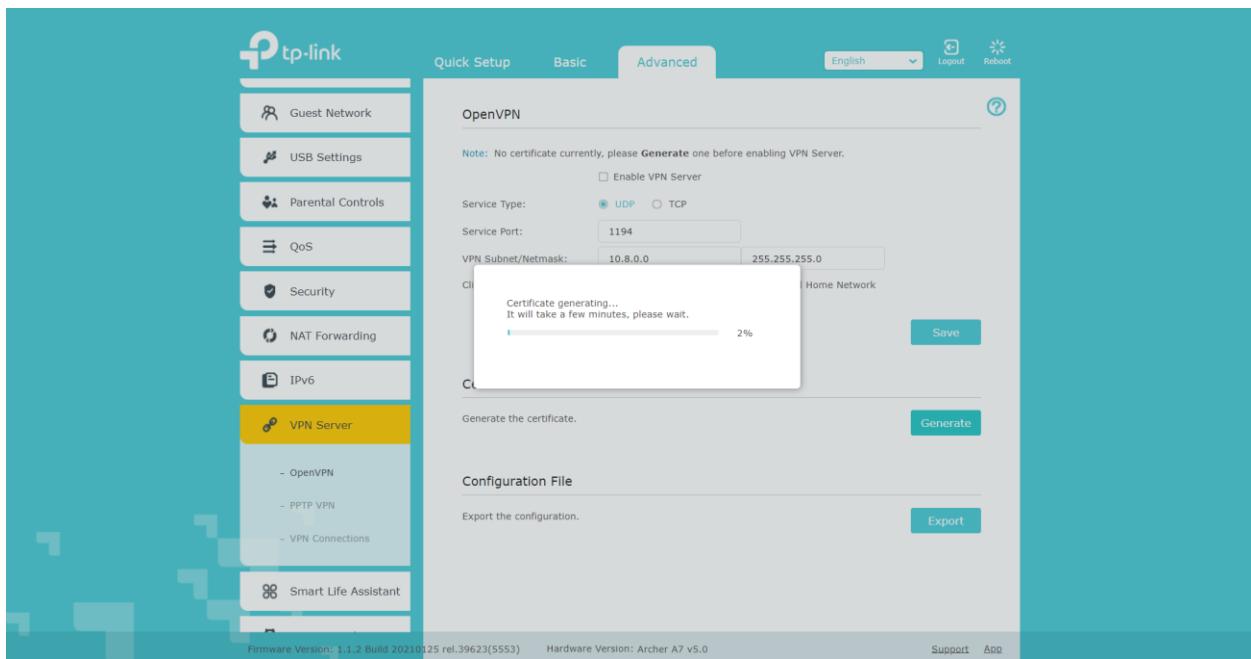
Login to your router/access point.



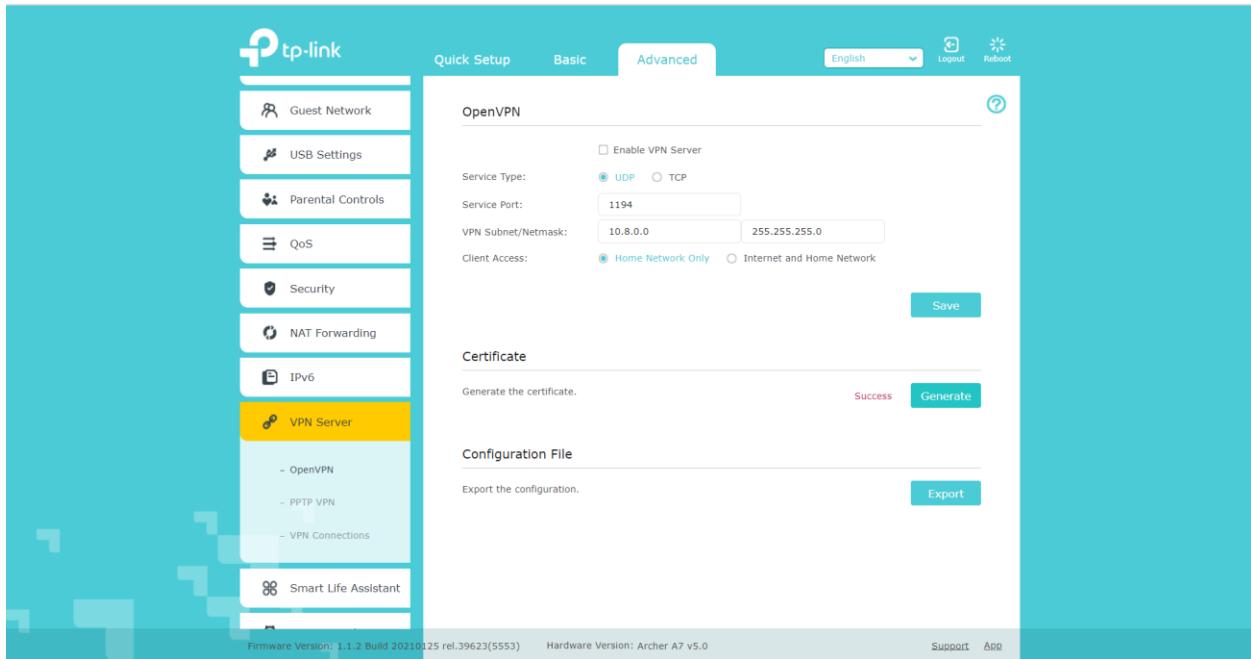
Navigate to your VPN Server settings and look for “OpenVPN” and click on it.



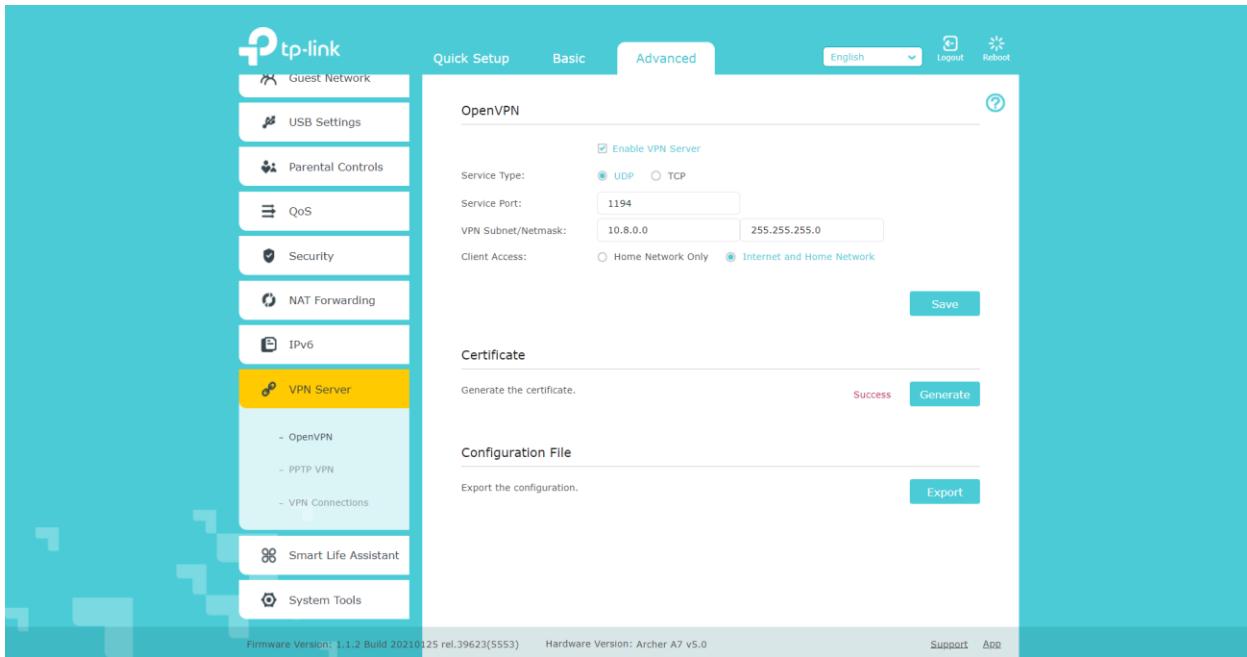
Click on “Generate” under “Certificate”.



It will take 3-5 minutes for the certificate generation to be complete.



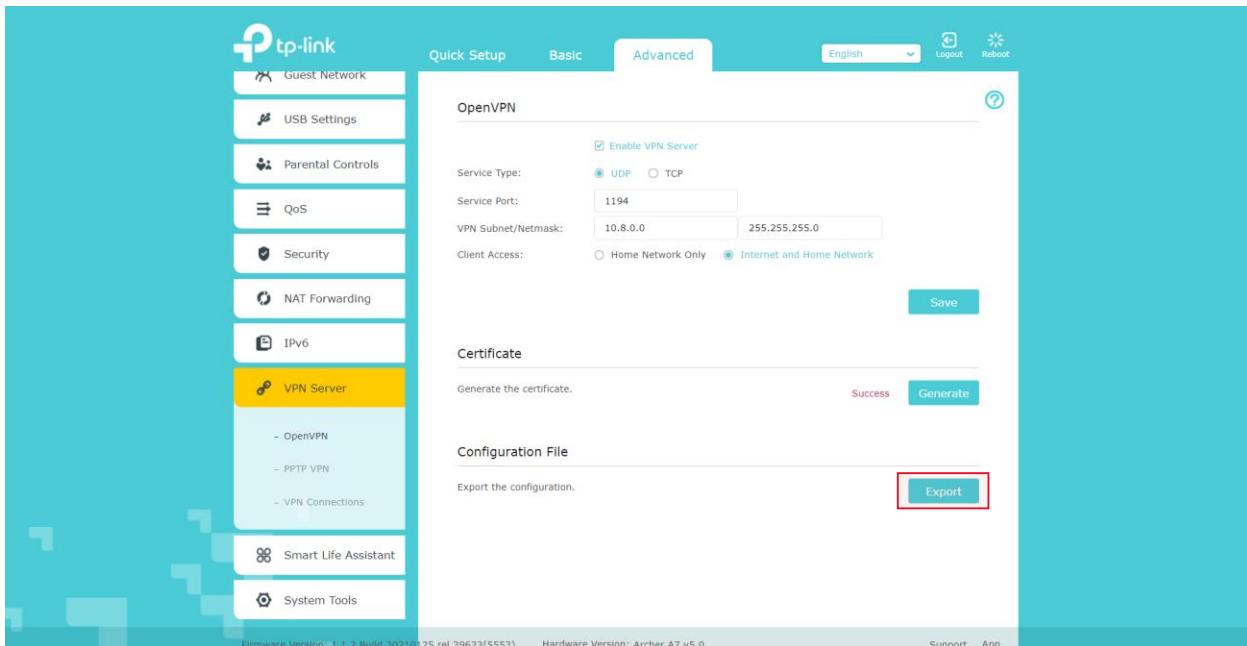
Should then get a “Success” message in red after completion.



Click on the “Enable VPN Server” checkbox.

The “Check Access” portion can either be “Home Network Only” or the “Internet and Home Network” if you want to have internet access too.

Click on “Save” when you are done.



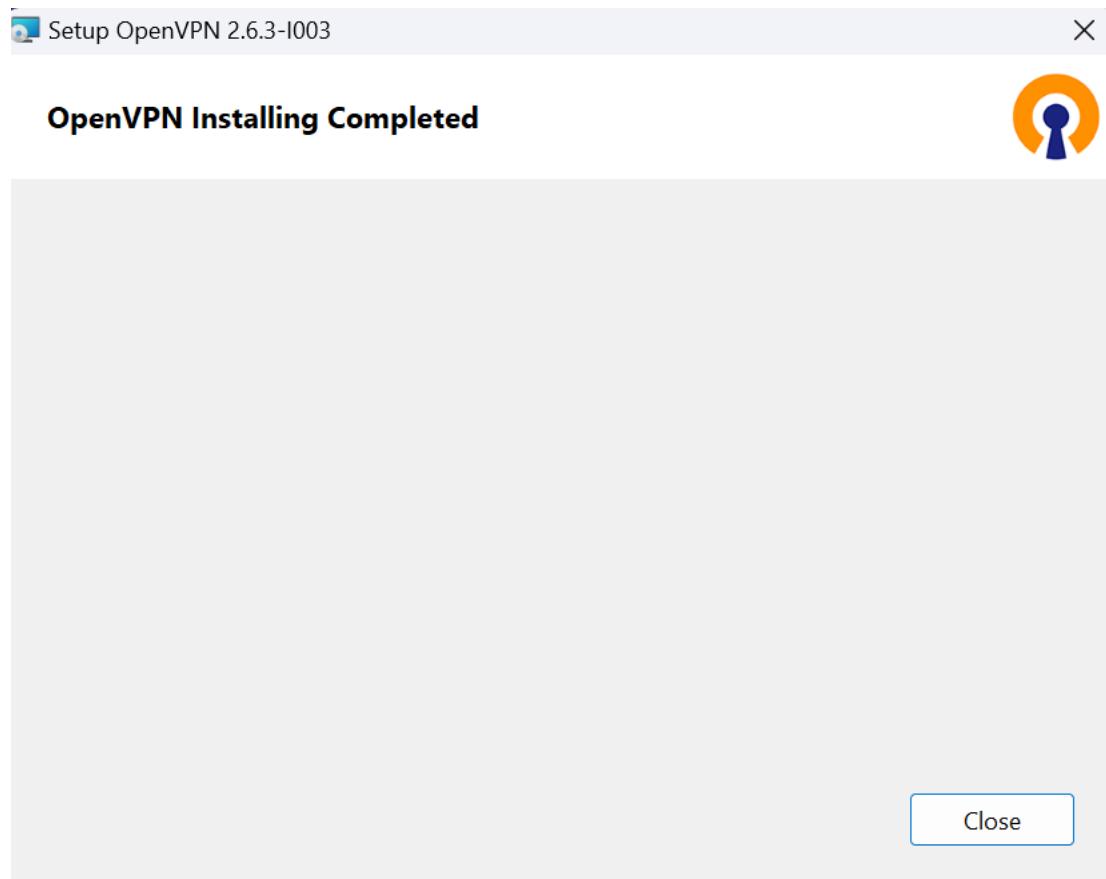
Click on “Export”.

Go to <https://openvpn.net/community-downloads/>

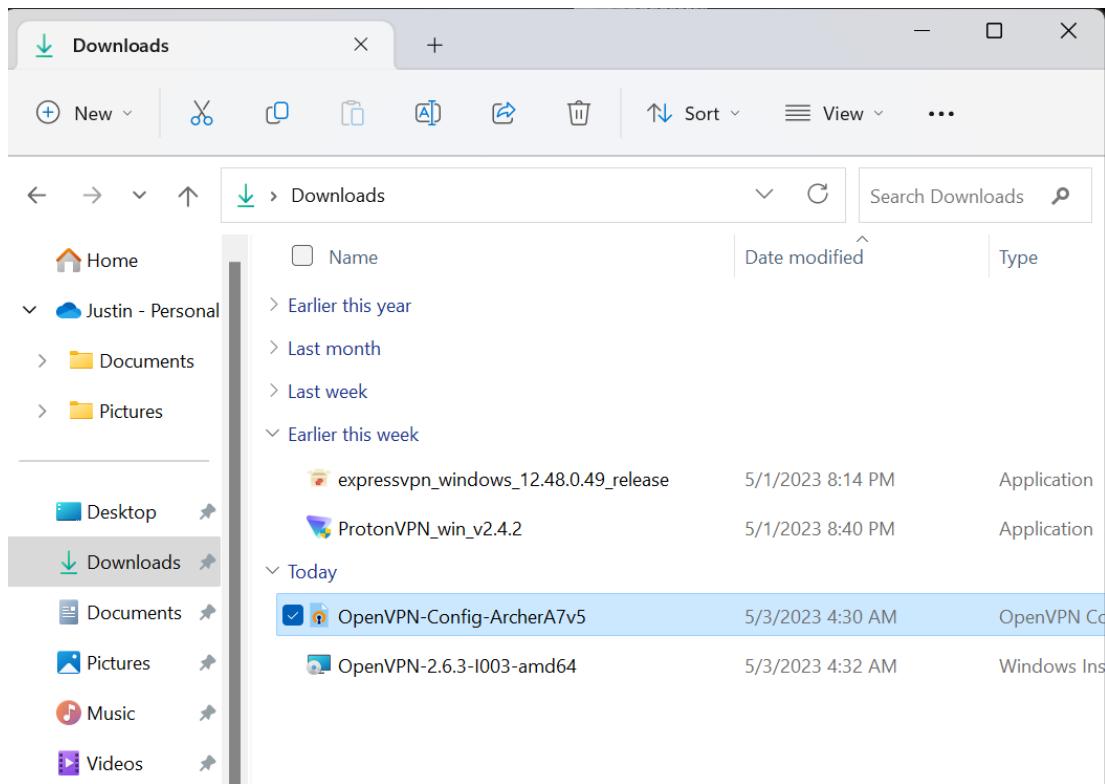
Windows 64-bit MSI installer	GnuPG Signature	OpenVPN-2.6.3-I003-amd64.msi
Windows ARM64 MSI installer	GnuPG Signature	OpenVPN-2.6.3-I003-arm64.msi
Windows 32-bit MSI installer	GnuPG Signature	OpenVPN-2.6.3-I003-x86.msi
Source archive file	GnuPG Signature	openvpn-2.6.3.tar.gz

Choose download type on your client device.

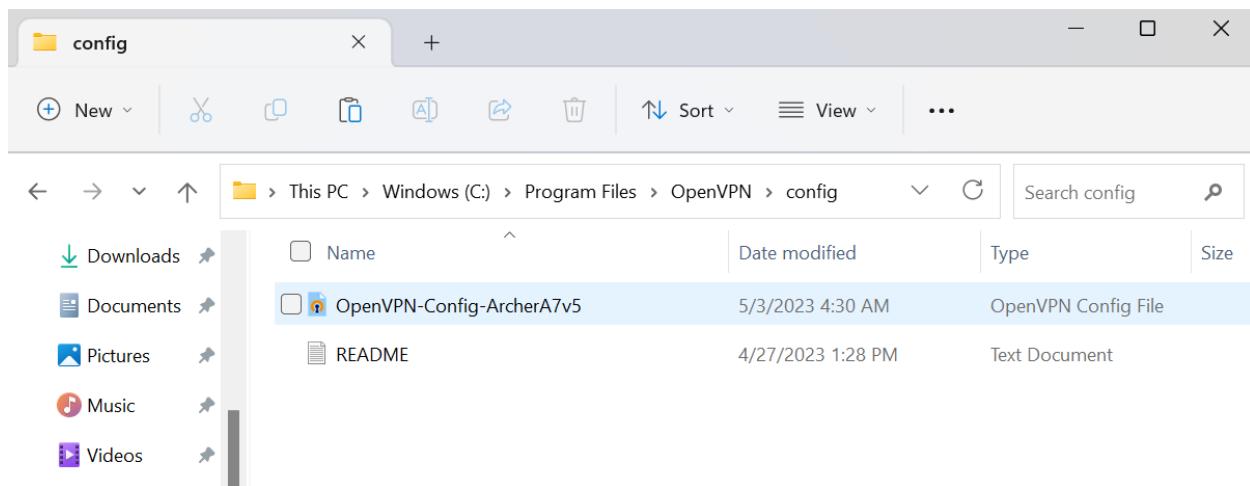
After download is complete click on the file.



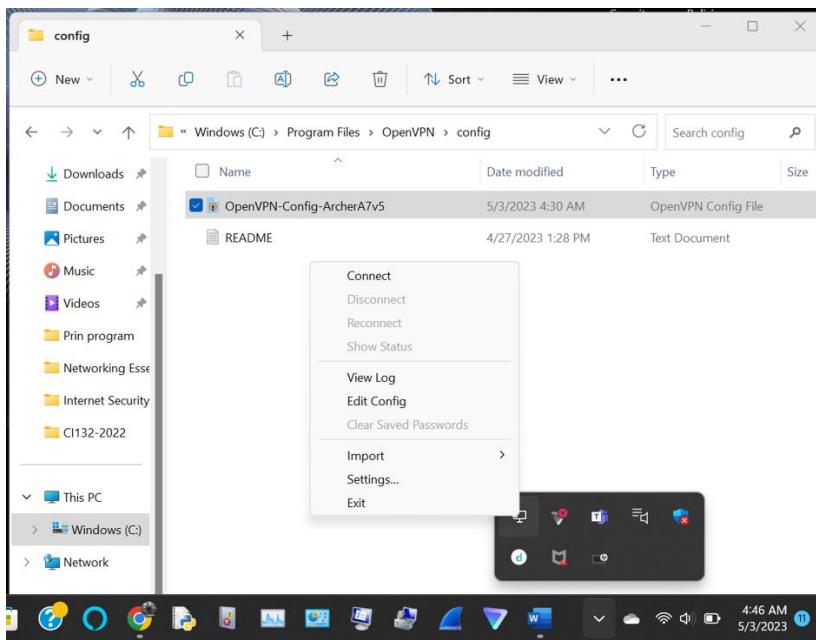
Then it will be installed on client device and click "Close" when it is finished.



Go to the copy of the OpenVPN server file that was exported from your router/access point, and make a copy of it.



Paste it in the folder/directory in Windows (C drive) > Program Files > OpenVPN > config.
(OpenVPN directory gets created in the download)



Then right click on OpenVPN click “Connect”.

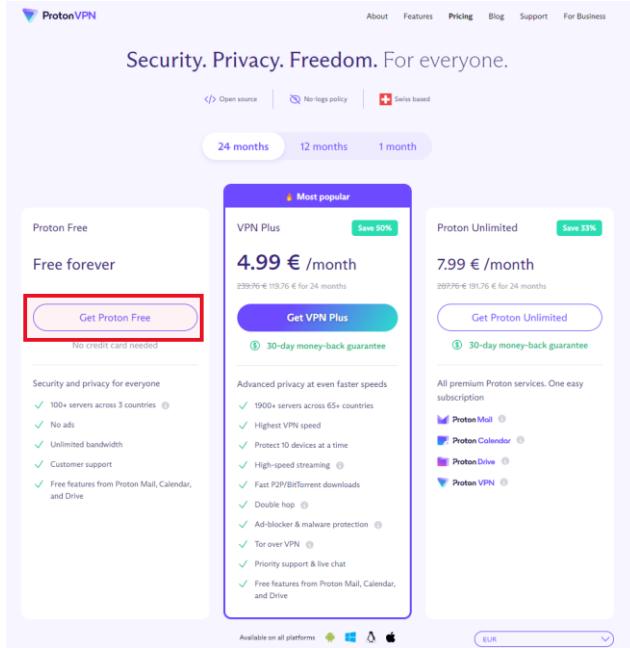
OpenVPN is open-source and free but there are other VPN services too.

VPN service providers offer subscriptions and usually will offer some sort of free trial so customers can test it out first.

ProtonVPN is a VPN service created by a Switzerland company called AG and has servers in over 110 countries. ProtonVPN has a free version and a couple of paid versions too with more advanced features.

ProtonVPN (free version):

This VPN application uses a 3rd party service provider's for VPN server to simplify VPN services so that everybody is able to understand how to use one.



ProtonVPN open-source version offers over 100 servers across 3 countries (United States, Netherlands, and Japan)

- Unlimited bandwidth.
- NO Advertisements.
- And features from their Mail, Calendar, and Drive for free along with their VPN services.
- Free customer support too.

There is then the “VPN Plus” Version which comes with lots of more features like double hop, tor, ad blockers, malware protection, over a thousand VPN servers in over 65 different countries, and more.

The 3rd version of ProtonVPN is the “Proton Unlimited” version which comes with all of their services without any restrictions as they are all unlimited.

The plans for the paid versions can be chosen between 1 month, 12 months, and 24 months. The 24 months plan has the best deals.

Getting the monthly plan is 9.99 euro/10.98 USD for Proton's VPN plus and 11.99 euro/13.18 USD for Proton Unlimited.

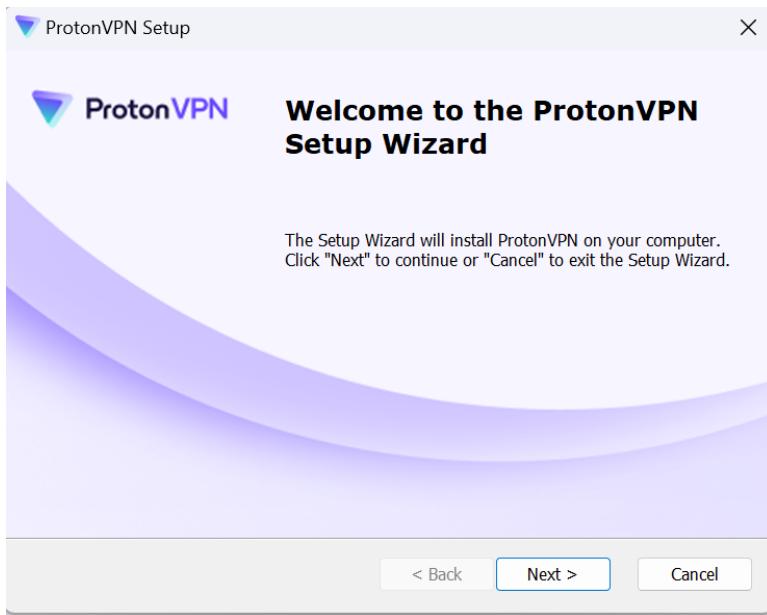
What do you get by choosing Proton VPN's free plan?

Free VPN	Free VPN	Free VPN
Apps	Servers	Features
Regardless if you use a PC , tablet, phone , or anything in between, Proton VPN has you covered with Free VPN apps for all of the major operating systems. <input checked="" type="checkbox"/> Free VPN for Windows <input checked="" type="checkbox"/> Free VPN for macOS <input checked="" type="checkbox"/> Free VPN for iOS <input checked="" type="checkbox"/> Free VPN for Android <input checked="" type="checkbox"/> Free VPN for Chromebook <input checked="" type="checkbox"/> Free VPN for Linux	Proton VPN offers free access to VPN servers in the United States, Netherlands, and Japan. The Proton VPN free plan has a strict no-logs policy backed by the Swiss data privacy laws. Additionally, Proton VPN does not apply any bandwidth, duration, or speed limits to free users.	Upgrading to a paid account provides access to advanced features, but our core privacy and anti-censorship features are available to all users: <input checked="" type="checkbox"/> VPN Accelerator <input checked="" type="checkbox"/> Strict no-logs policy <input checked="" type="checkbox"/> Kill Switch <input checked="" type="checkbox"/> Stealth VPN protocol <input checked="" type="checkbox"/> Access blocked content

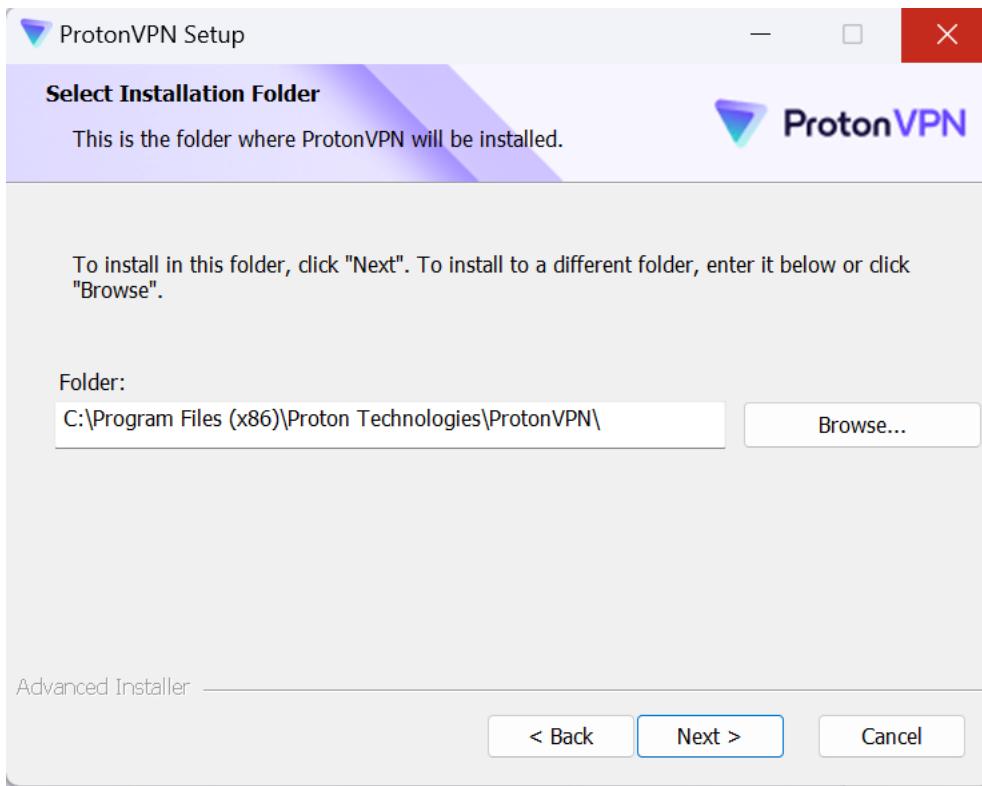
To help you decide if our free plan or one of our paid plans is right for you, click the button below to find out additional information and compare plans.

[Free vs Paid VPN](#)

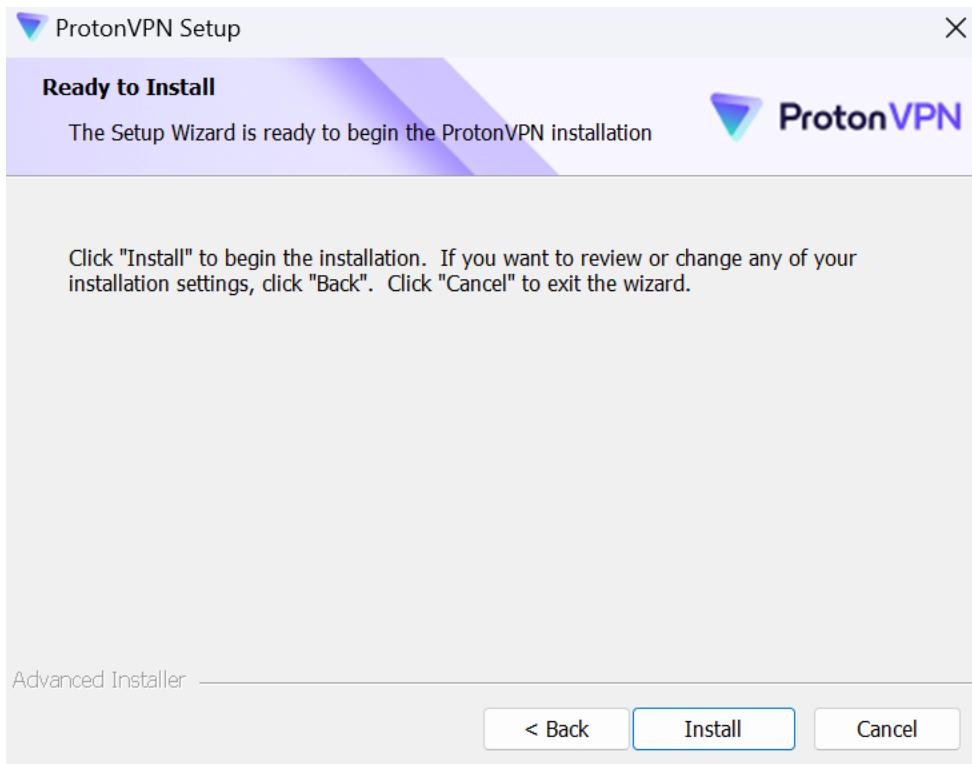
Anyone can download this free/open-source Proton VPN on a variety of systems such as Windows, macOS, iOS, Android, Chromebook, and Linux.



After installing the free version of ProtonVPN, click on "Next".



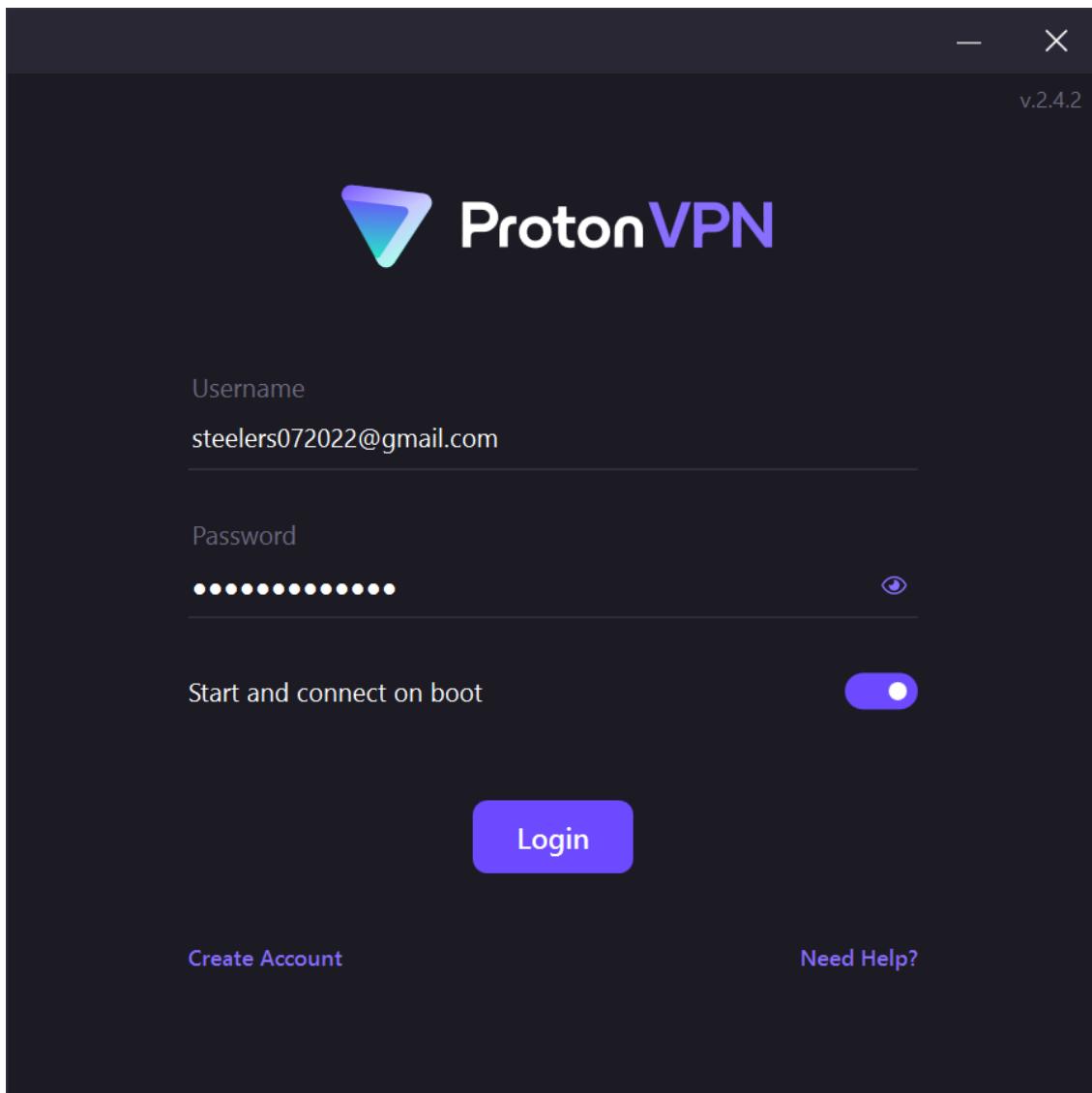
Choose folder/directory path.



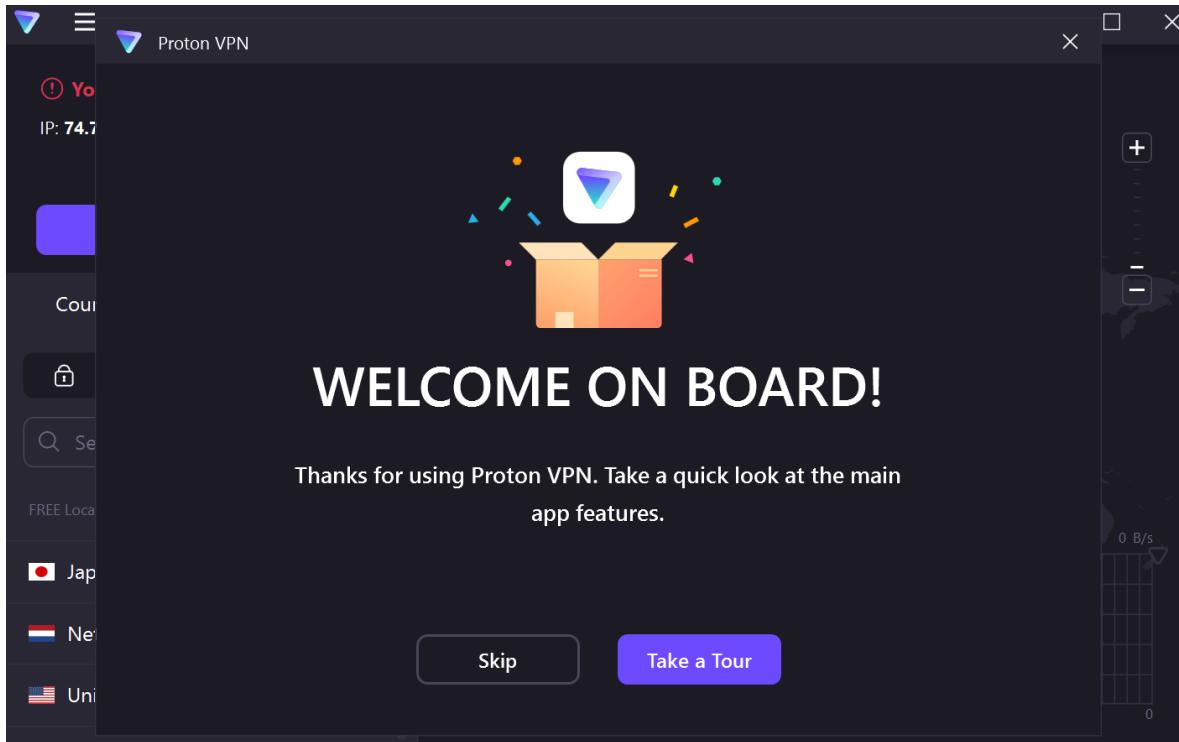
Click on "Install".



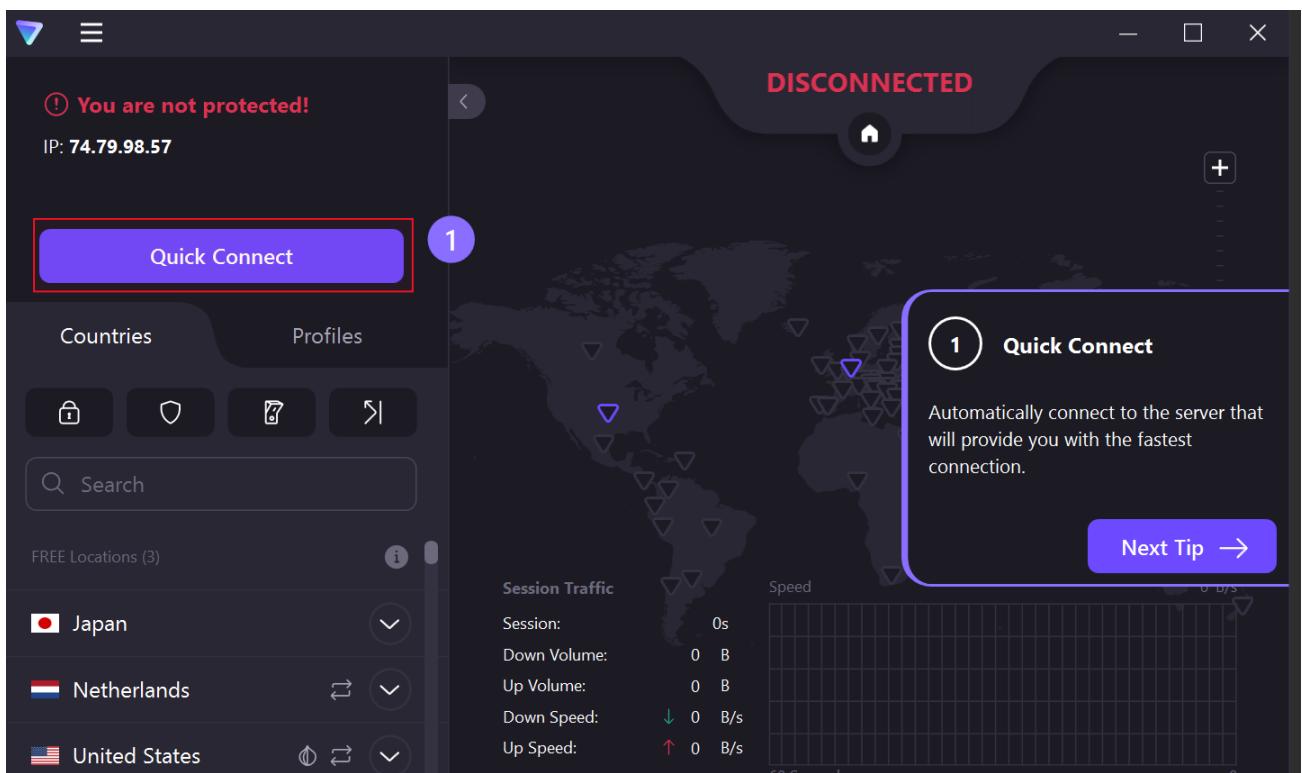
Click on “Finish” after the installation has completed.



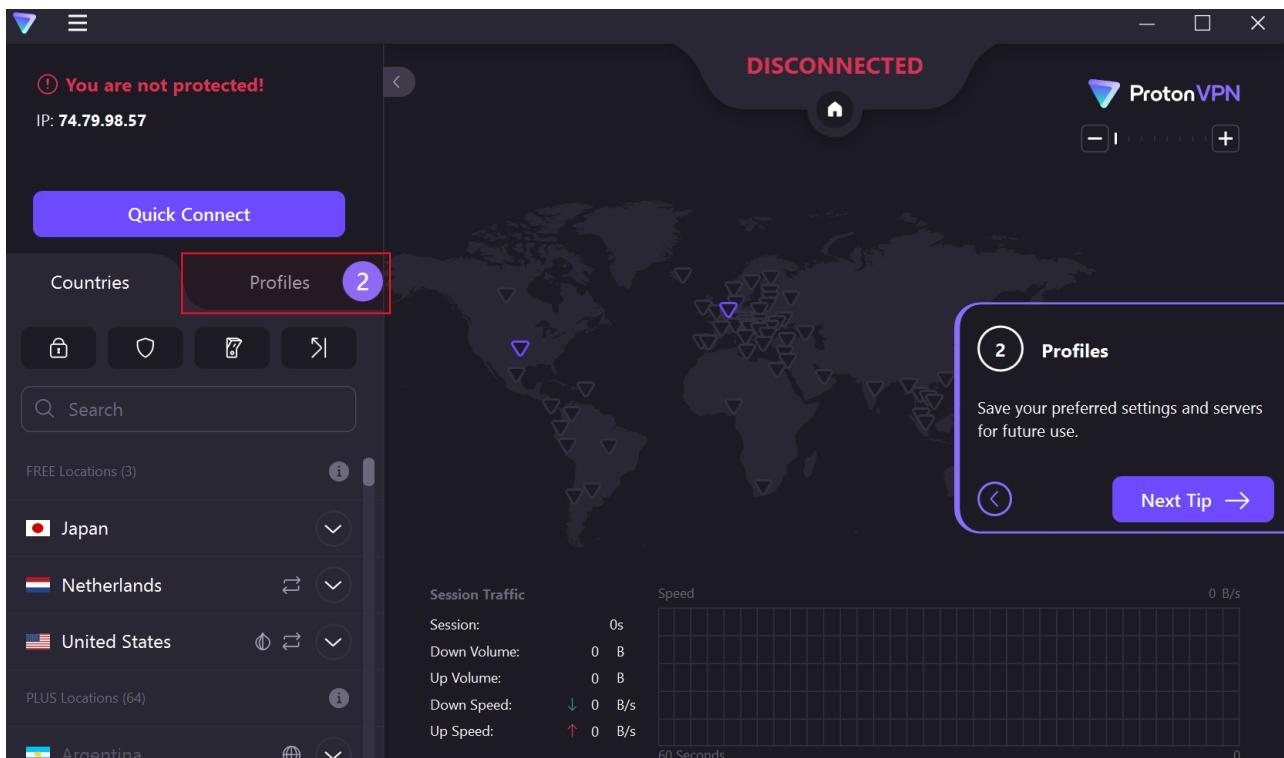
Login or create an account and then login.



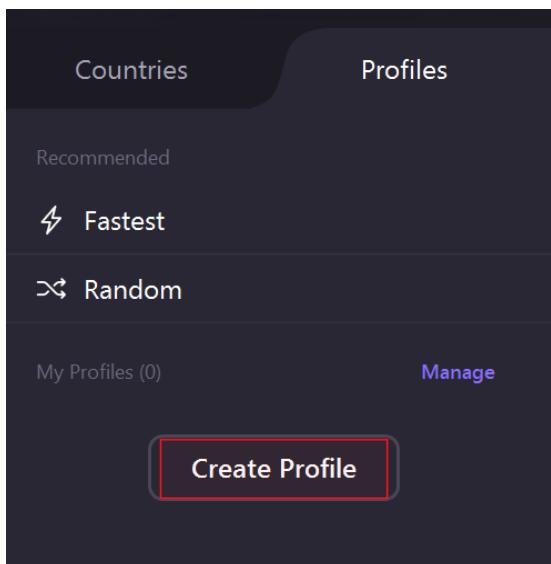
Click on “Take a Tour”.



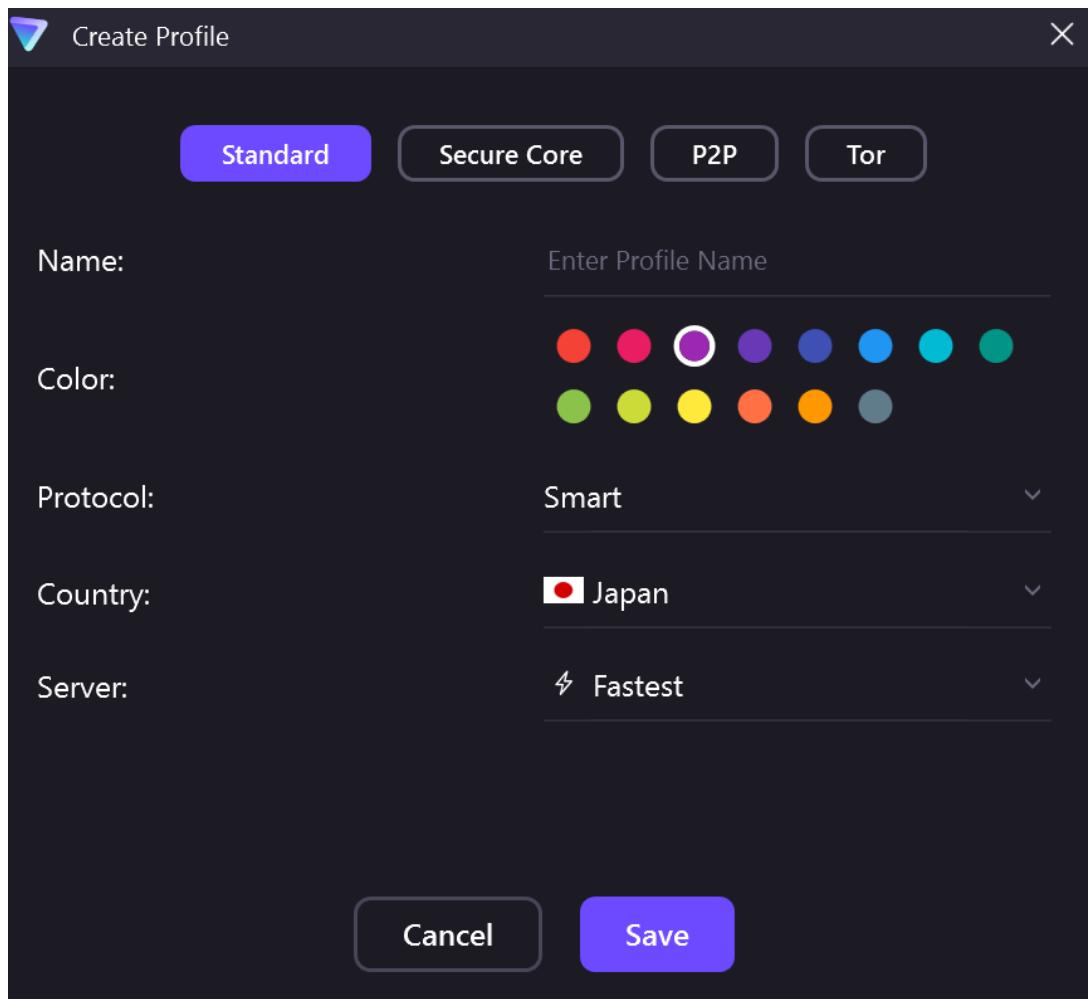
The “Quick Connect” option is what I will be using to connect to a free server quickly and automatically.



Can click on “Profiles” to save any VPN servers along with the setting you have configured.

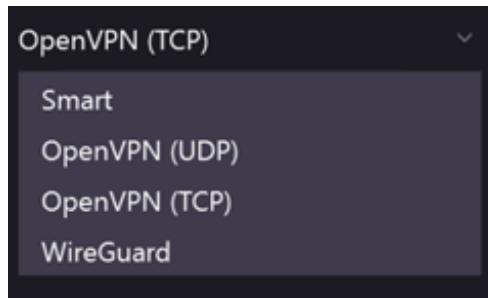


Can create a profile here by clicking on “Create Profile”.



Can choose between a “Standard, Secure Core, P2P, or Tor” connection type.

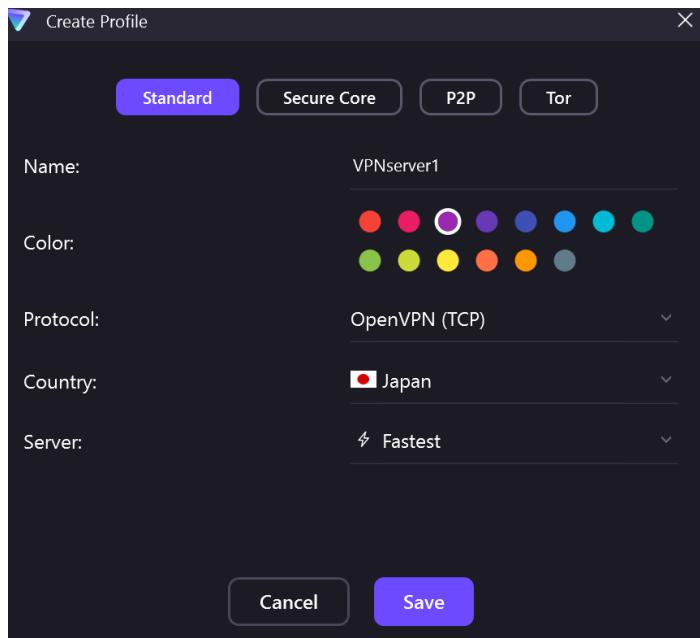
Here I select “Standard” and then click on the dropdown menu next to “Protocol”.



Click on “OpenVPN (UDP)” for faster connections.

Or click on “OpenVPN (TCP)” for safer and more reliable connections.

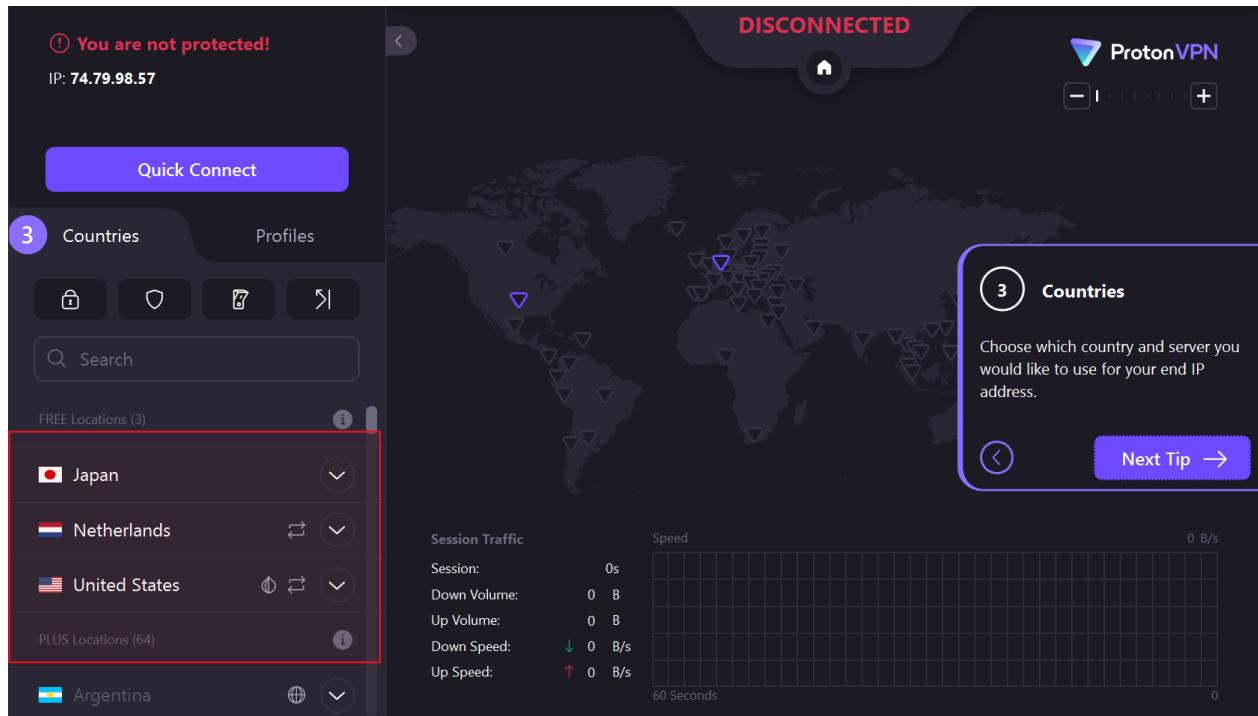
“Smart” will do it automatically, and “WireGuard” protocol is a newer/faster VPN protocol. This is what is mostly used since it has faster speeds while still being secure.



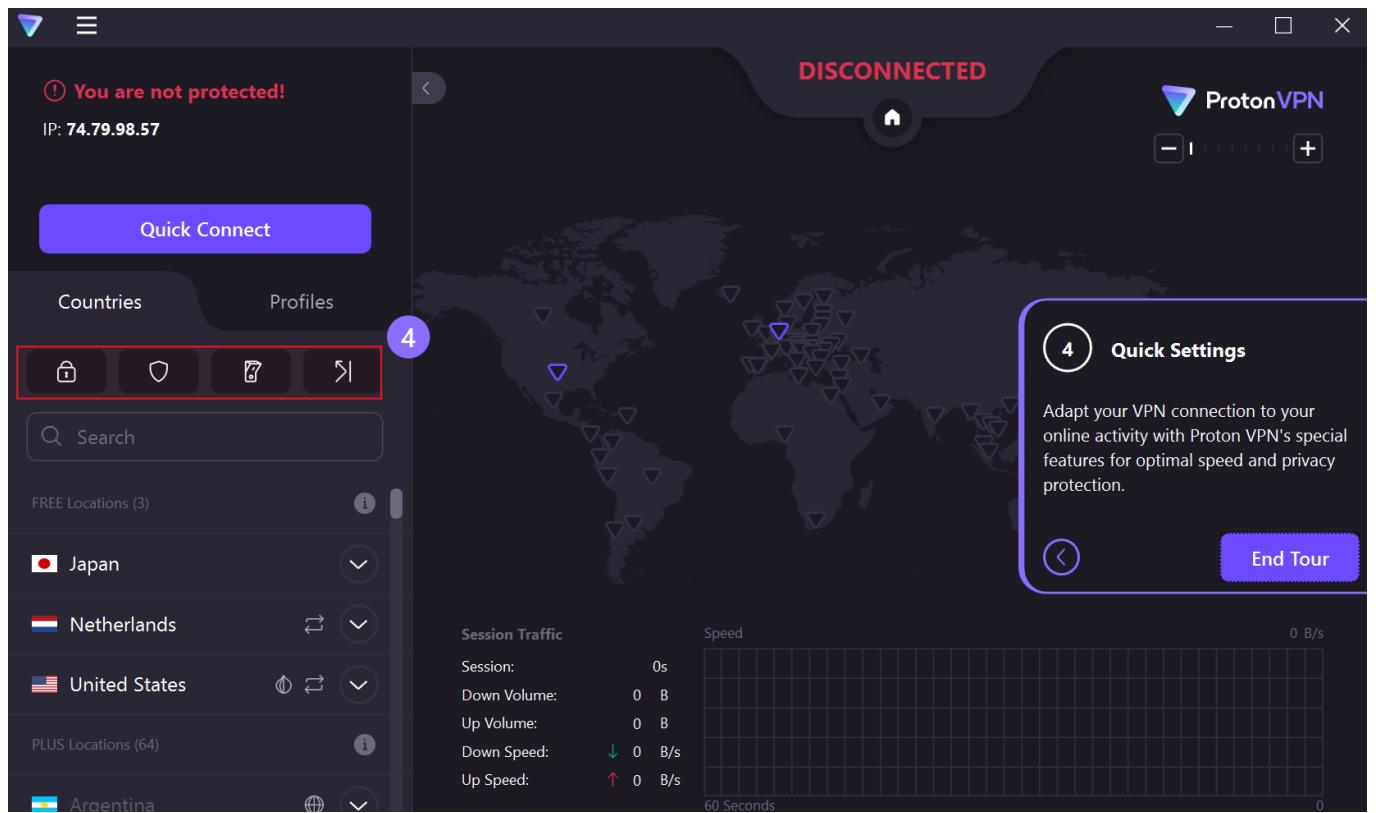
After choosing a Name and Color click on “Save”.

You could pick a specific server next to “Server”, but here I choose Fastest option.

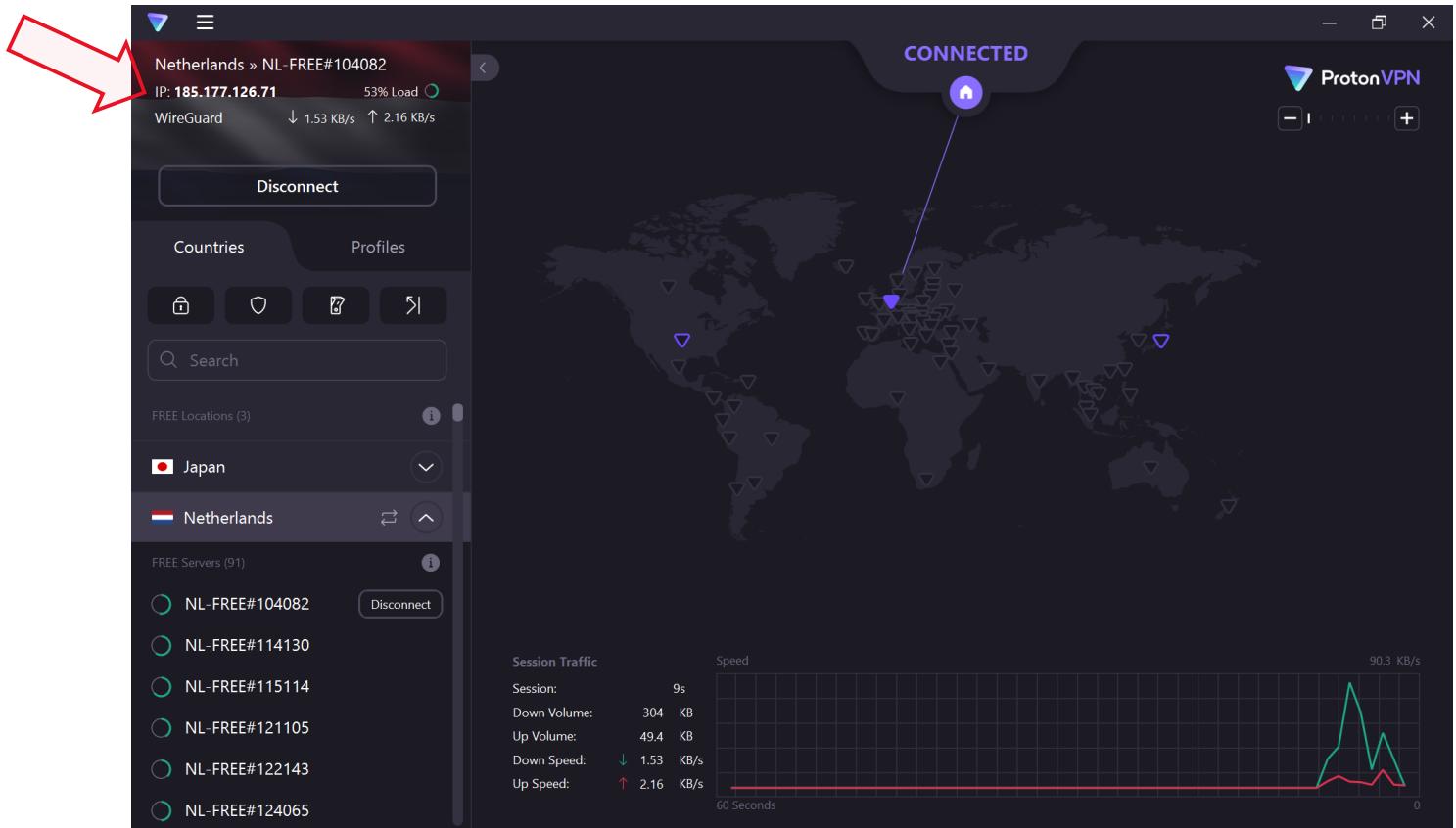
Instead of creating a Profile you can just choose VPN server from the 3 choices on left hand side and click “Quick Connect”, and can then save it to a server profile later if chosen to do so.



Can choose between US, Netherlands, or Japan as a location for your VPN server.

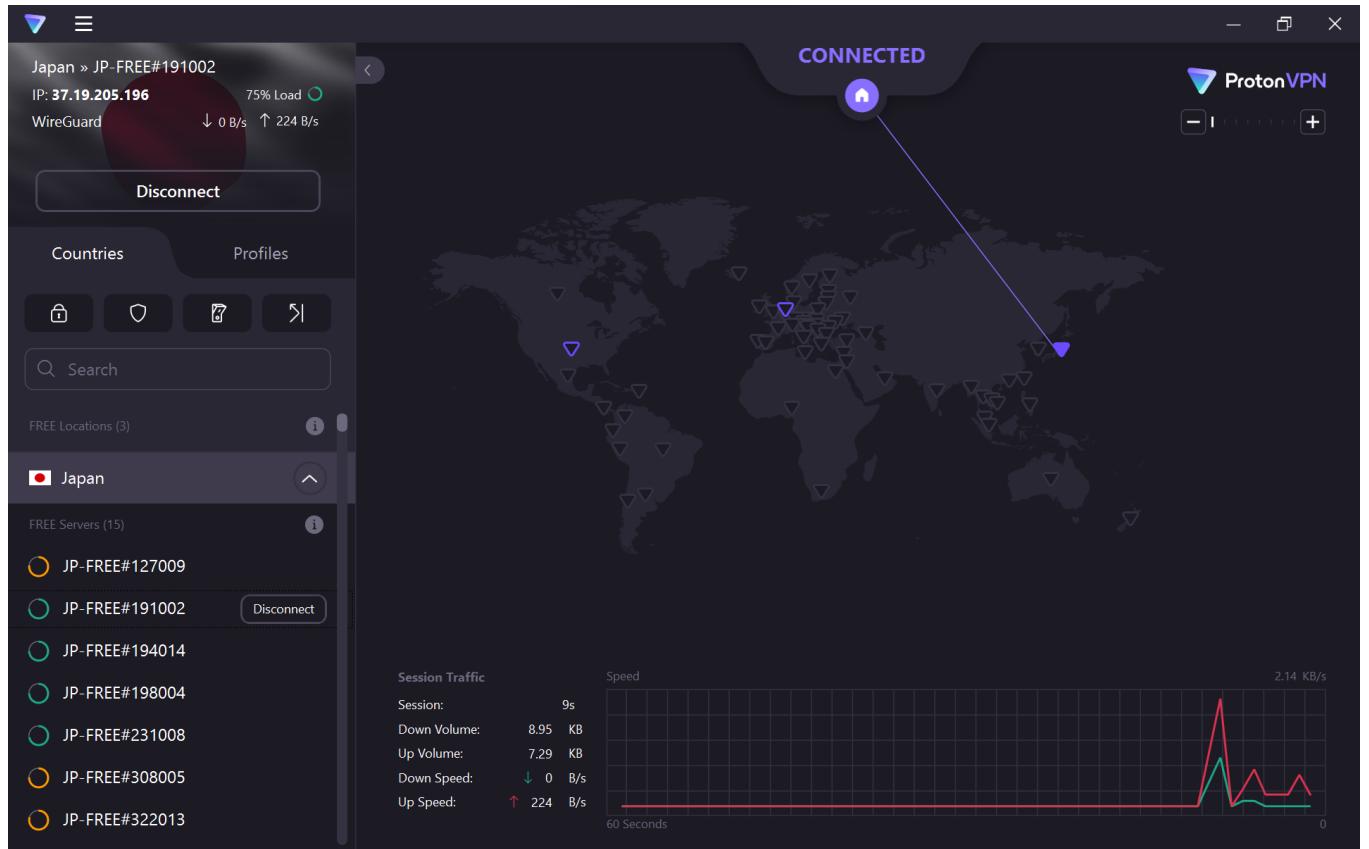


Can checking Privacy, Speed, and other ProtonVPN connection features via the “Quick Settings” option.



I am currently connected to a Netherlands ProtonVPN server.

I can switch to a Japan ProtonVPN server as well to see the IP address change on the upper left of the screen.



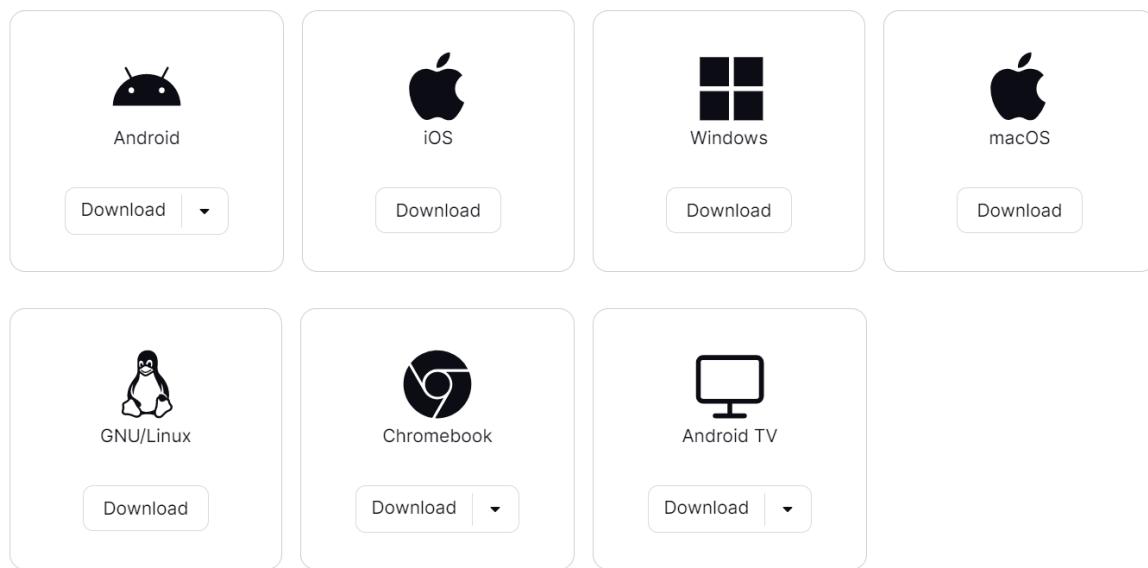
Now I am connected to a Japan ProtonVPN server, and I have a different IP address, as shown up above in the upper left-hand corner of the screen.

The screenshot shows the homepage of whatismyipaddress.com. At the top, there's a search bar with the placeholder "Enter Keywords or IP Address..." and a "Search" button. Below the search bar are navigation links for "ABOUT", "PRESS", "BLOG", and "SUPPORT". A horizontal menu bar includes "MY IP", "IP LOOKUP", "HIDE MY IP", "VPNS", "TOOLS", and "LEARN". The main content area displays "My IP Address is:" followed by "IPv4: 37.19.205.196" and "IPv6: Checking...". It also shows "My IP Information" with details: ISP: DataCamp Limited, Services: Network Sharing Device, City: Tokyo, Region: Tokyo, Country: Japan. There's a red button labeled "HIDE MY IP ADDRESS NOW" and a link to "Show Complete IP Details". To the right, a map of Japan with a pin indicates the location of the IP address. A tooltip says "Click for more details about 37.19.205.196". Below the map, it says "Location not accurate?" and "Update My IP Location".

Now the IP address is masked with different IP address from Tokyo, Japan as shown on IP tracker website via <https://whatismyipaddress.com/>

Proton VPN clients

To secure your internet connection, download and install the Proton VPN application for your device and connect to a server.



Proton VPN can be installed on the clients Android, iOS, Windows, macOS, GNU/Linux, Chromebook, and Android TV. (as shown above from their official website)

There are also some simple configurations files for the ProtonVPN server you want to set up.

OpenVPN configuration files

These configuration files let you choose which Proton VPN server you connect to when using a third-party VPN app or setting up a VPN connection on a router.

1. Select platform

- Android iOS Windows macOS GNU/Linux Router

[View guide](#)

[View guide](#)

[View guide](#)

[View guide](#)

[View guide](#)

[View guide](#)

2. Select protocol

- UDP TCP

[What is the difference between UDP and TCP protocols?](#)

3. Select config file and download

- Country configs Standard server configs Free server configs Secure Core configs

Install a Free server configuration file to connect to a specific server in one of the three free locations.

▼  Japan

▼  Netherlands

▼  United States

[Download all configurations](#)

[Get VPN Plus to access all servers](#)

- ✓ Access to all countries ✓ Secure Core servers ✓ Fastest VPN servers ✓ Torrenting support (P2P)
✓ Connection for up to 10 devices ✓ Secure streaming support ⓘ

[Get VPN Plus](#)

1. Choose “Platform” which is the system or operating system you want to configure.
2. Choose either “UDP” or “TCP” as your transfer protocol.
3. Choose Configuration file. (Select the “Free server configs” option)

WireGuard configuration

These configurations are provided to work with WireGuard routers and official clients.

1. Give a name to the config to be generated

Device/certificate name [\(i\)](#)

Choose a name for the generated certificate file

2. Select platform

Android iOS Windows macOS GNU/Linux Router

3. Select VPN options

NAT-PMP (Port Forwarding) [Learn more](#)

VPN Accelerator [Learn more](#)

4. Select a server to connect to

Use the best server according to current load and position: **JP-FREE#191002**

Create

Or select a particular server:

Standard server configs Free server configs Secure Core configs

▼  Japan

▼  Netherlands

▼  United States

WireGuard is a newer VPN protocol.

This is a configuration for a router that has WireGuard capabilities.