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.

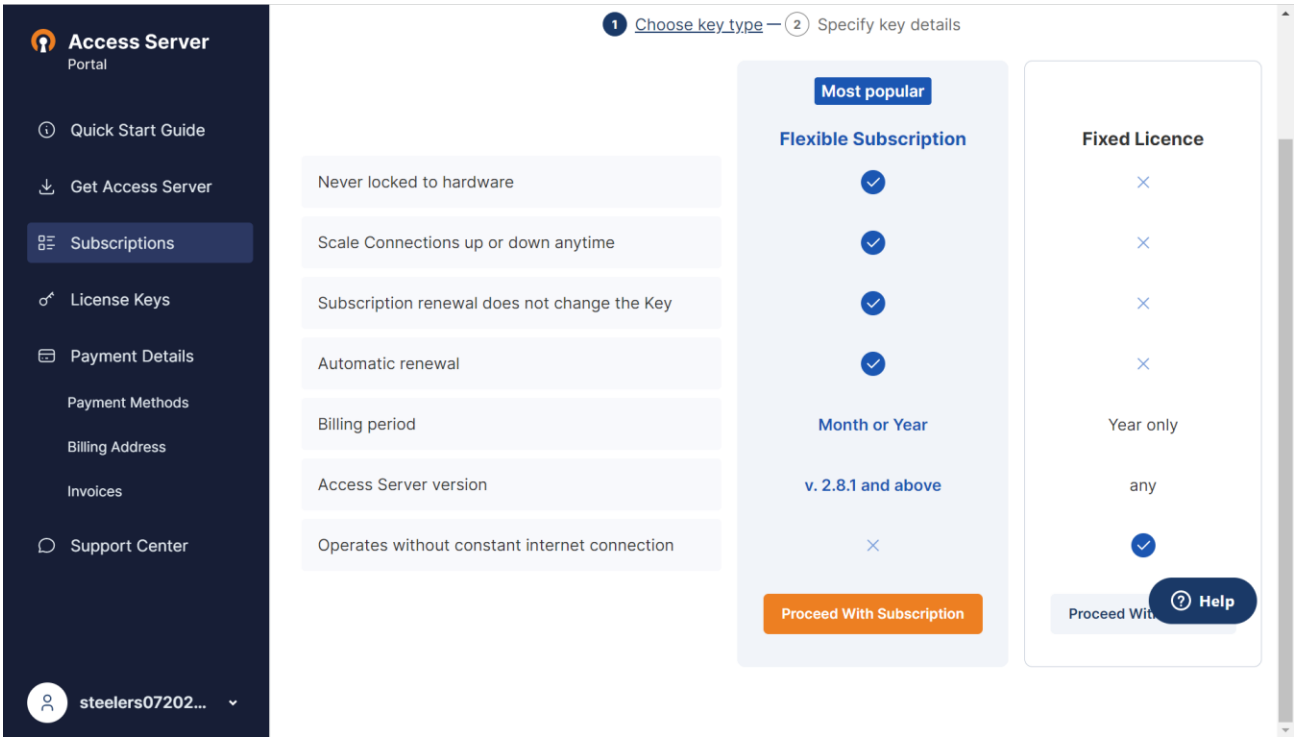
Keep in mind that OpenVPN tunneling protocol is a separate/different protocol than the other encryption protocols used such as PPTP, L2TP, IPsec, SSTP, SSL & TLS, and IKEv2. (And SSH).

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

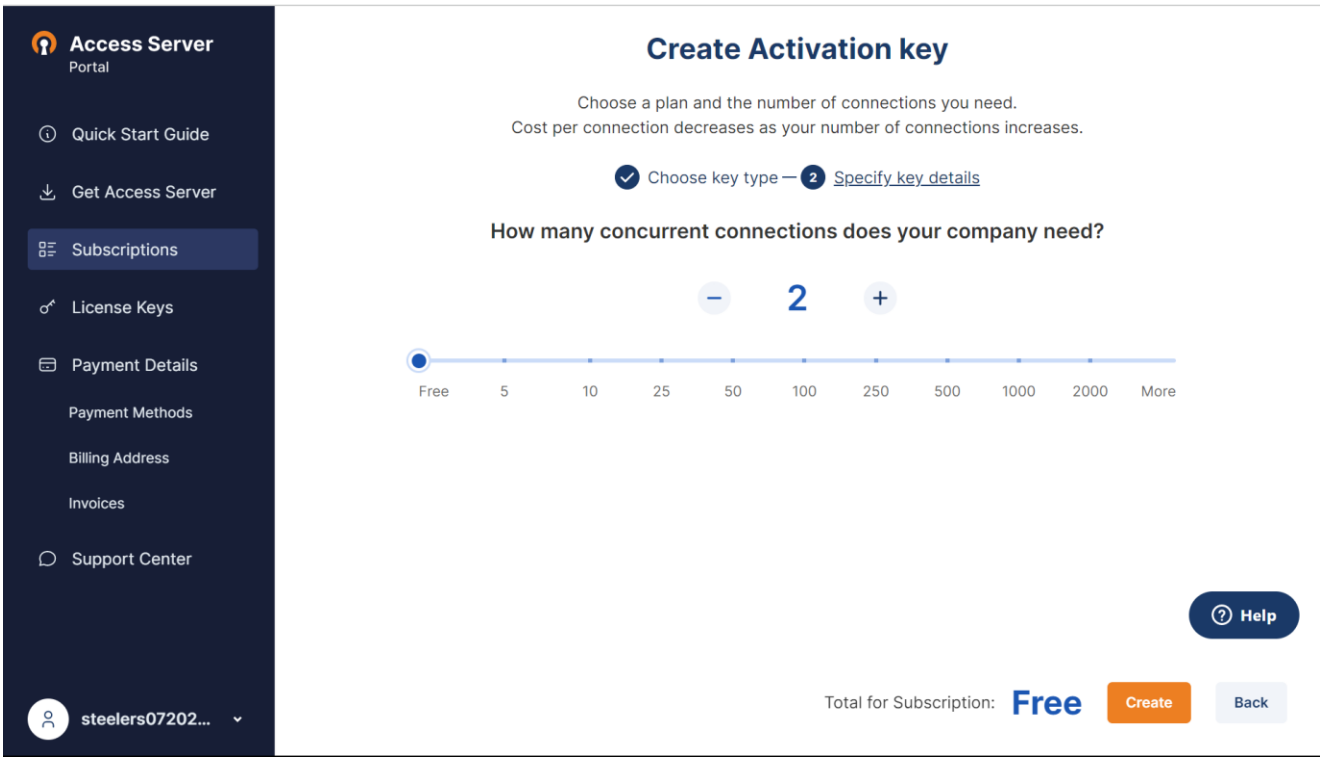
That way the OpenVPN client will be the app and can transmit traffic to encrypted tunnel where that traffic is then encrypted, and then it goes to the OpenVPN server (on access point in this scenario) where it is decrypted and then the traffic goes back in the reverse direction. The OpenVPN server can 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/

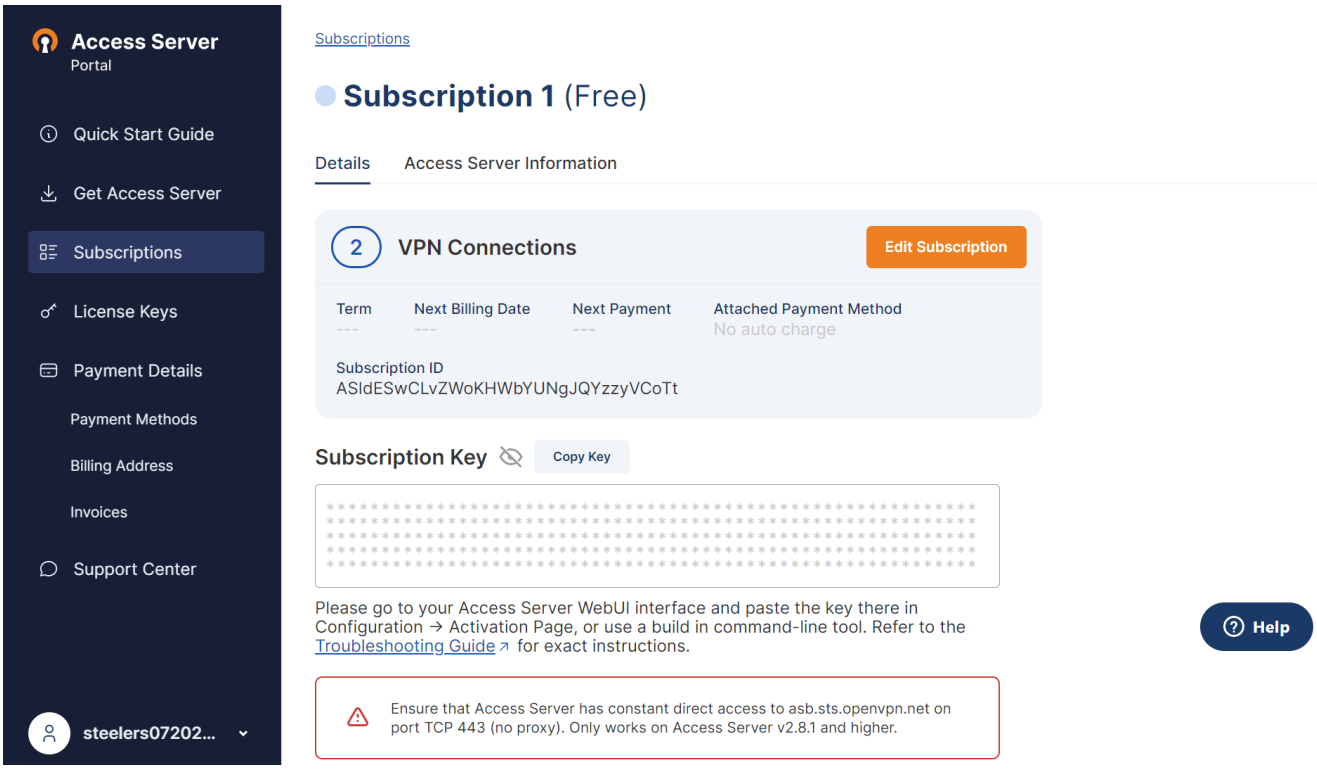
Go to your Access Server.



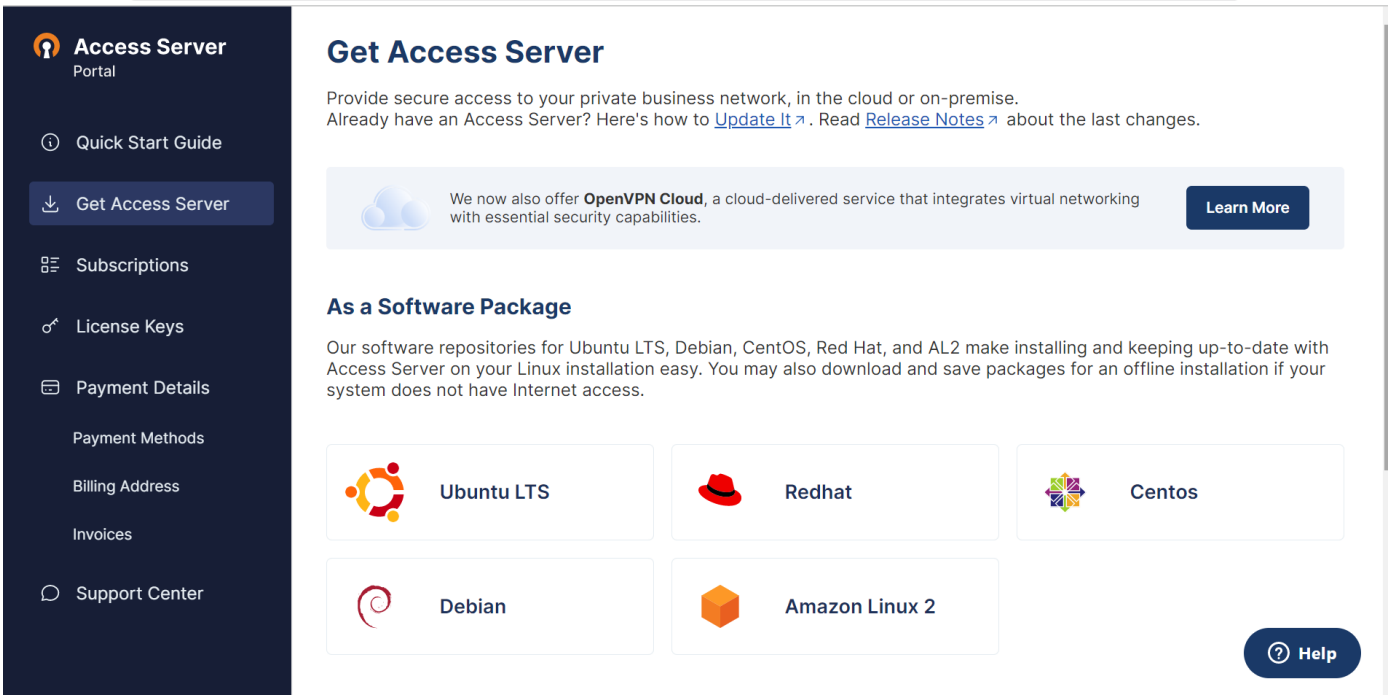
Click on “Subscriptions” on the left side column. Then choose “Flexible Subscriptions” and click on “Proceed with Subscription”.



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



Copy subscription key.

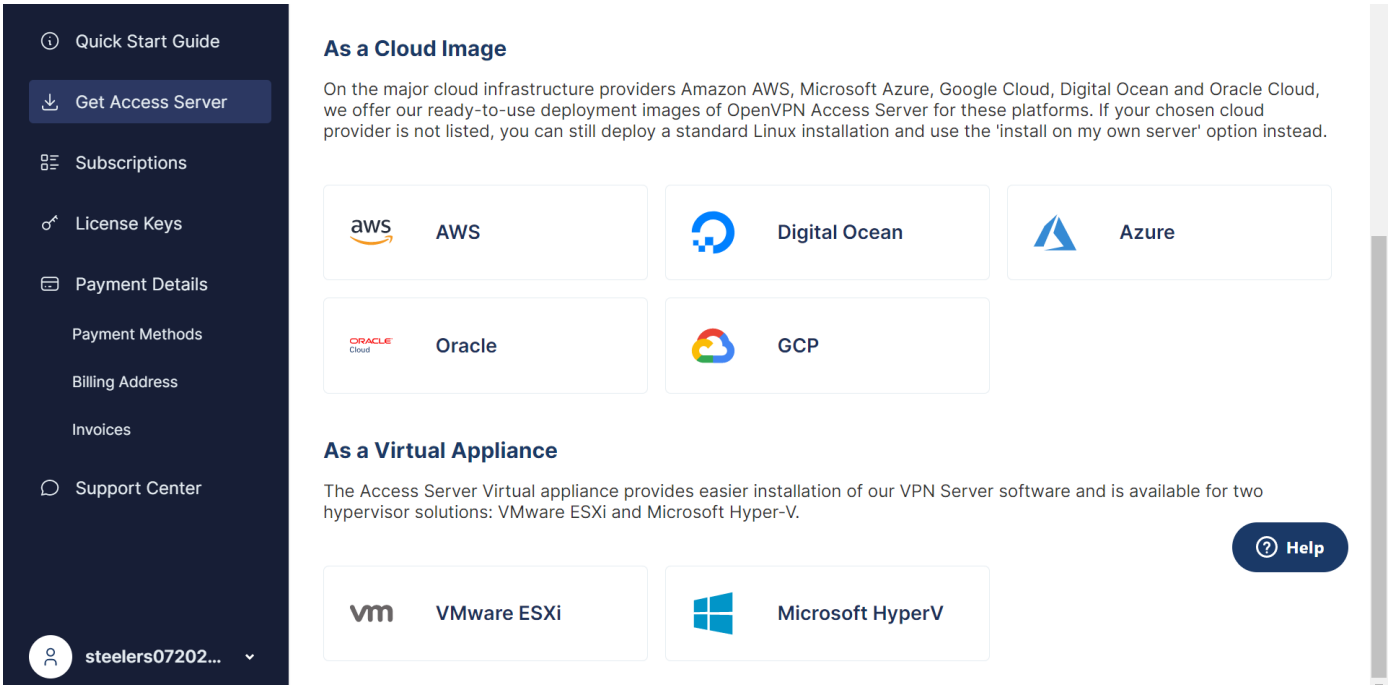


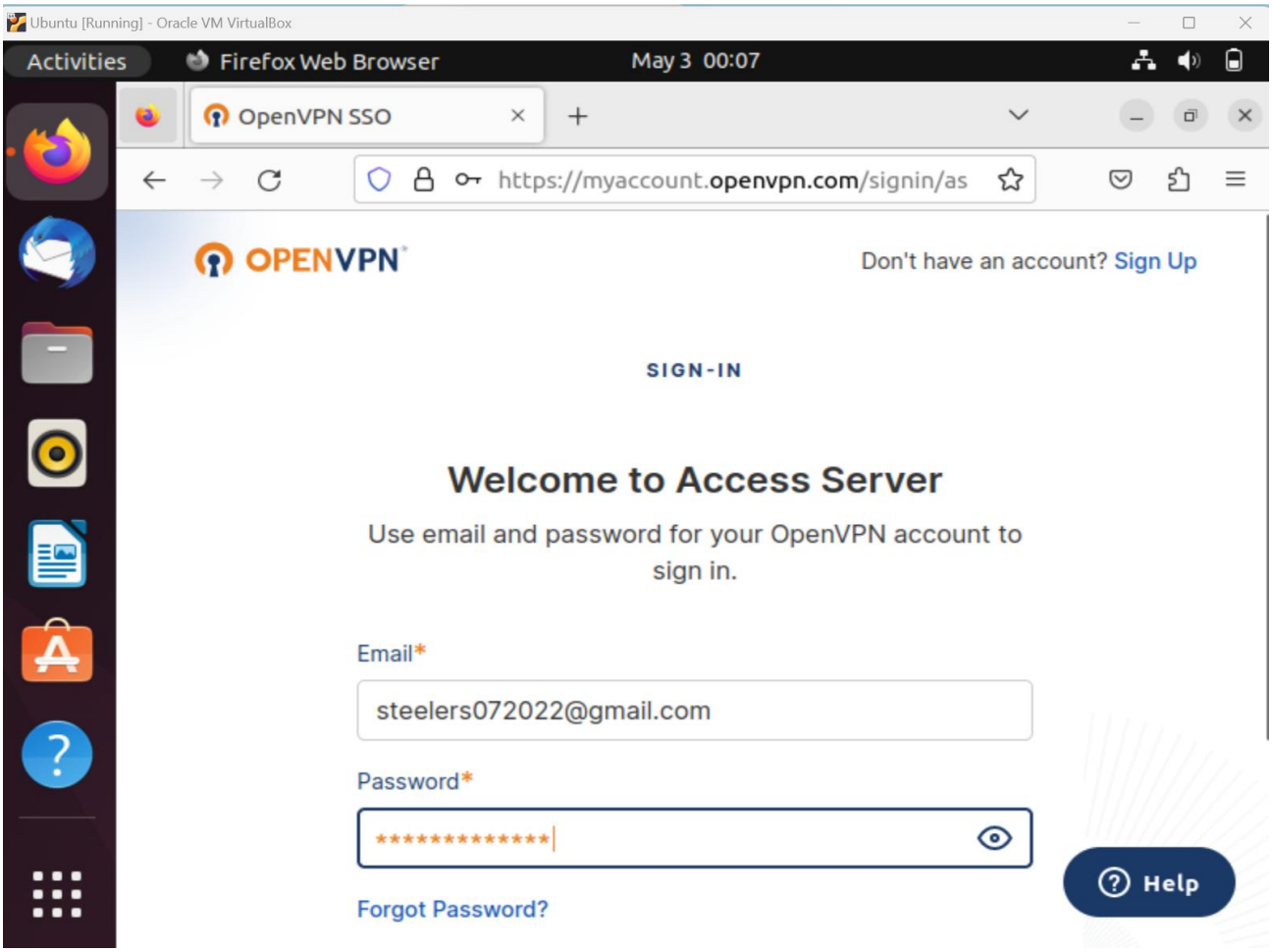
Then go to “Get Access Server” on the left side of the column.

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.





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 ne
t-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.ope
nvpn.net/as/debian jammy main">/etc/apt/sources.list.d/openvpn-as-repo.list
```

Then run these 2 commands.

```
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 liblzo2-2
 libmariadb3 libpcap0.8 libssl3 libstdc++6 libsasl2-2 libsqlite3-0 net-tools python3-pkg-resources python3-migrate python3-sq
lalchemy python3-mysqldb python3-ldap3 sqlite3 zlib1g python3-netaddr python3-arrow python3-lxml python3-constantly python3-h
yperlink python3-automat python3-service-identity python3-cffi python3-defusedxml
```

NOTE:

```
jay@jay-VirtualBox:~/Downloads$ sudo apt --fix-broken install
```

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.

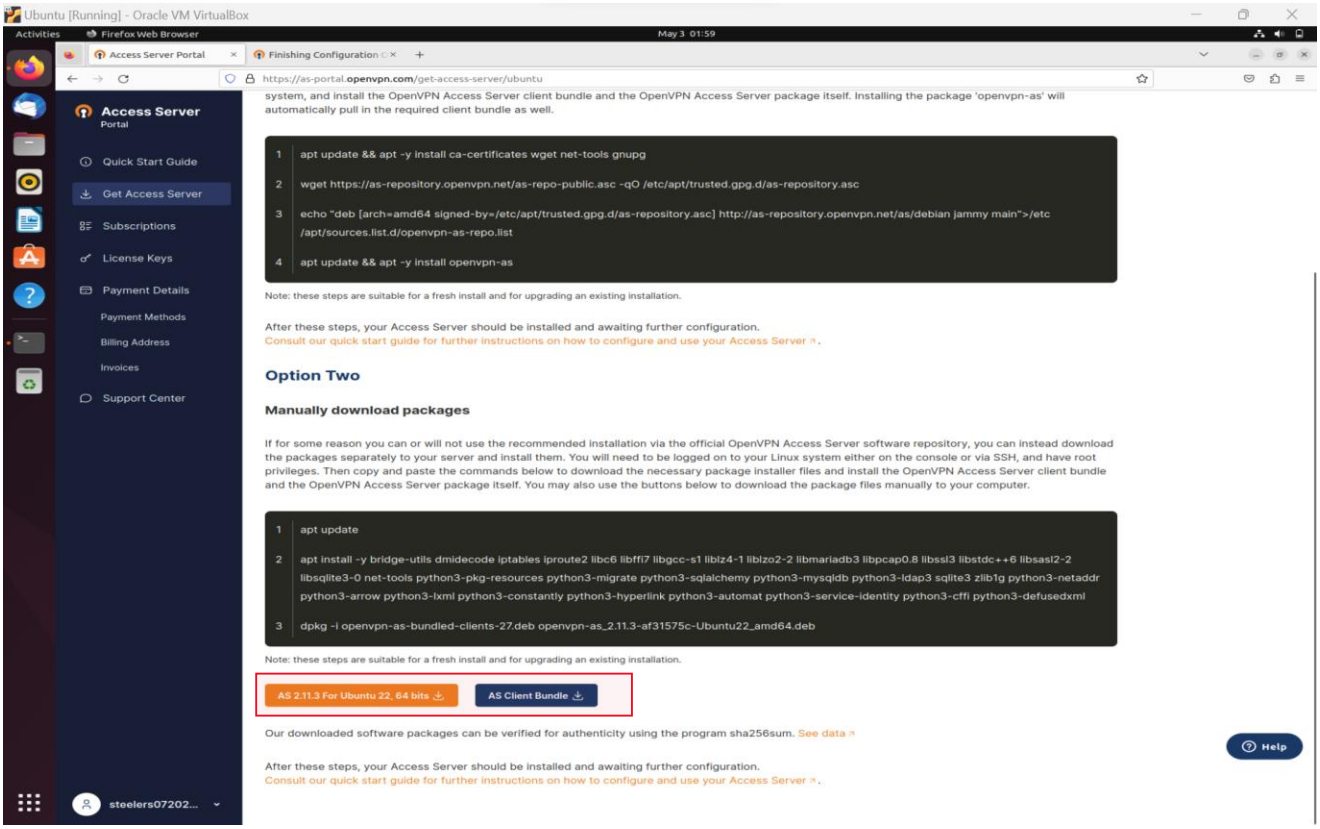
Go to the web URL for admin “https://10.0.2.15:943/admin”

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

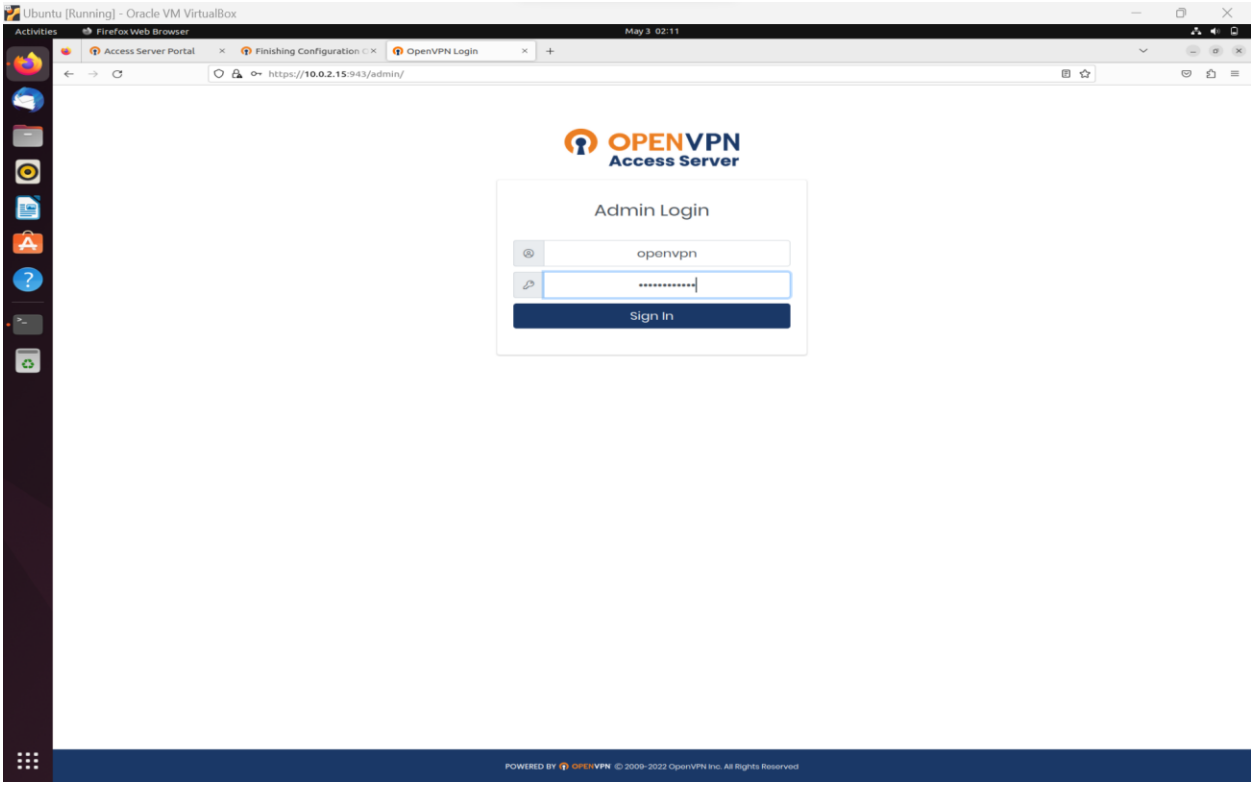
Run this command after downloading the 2 packages from Access Server.

```
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$
```

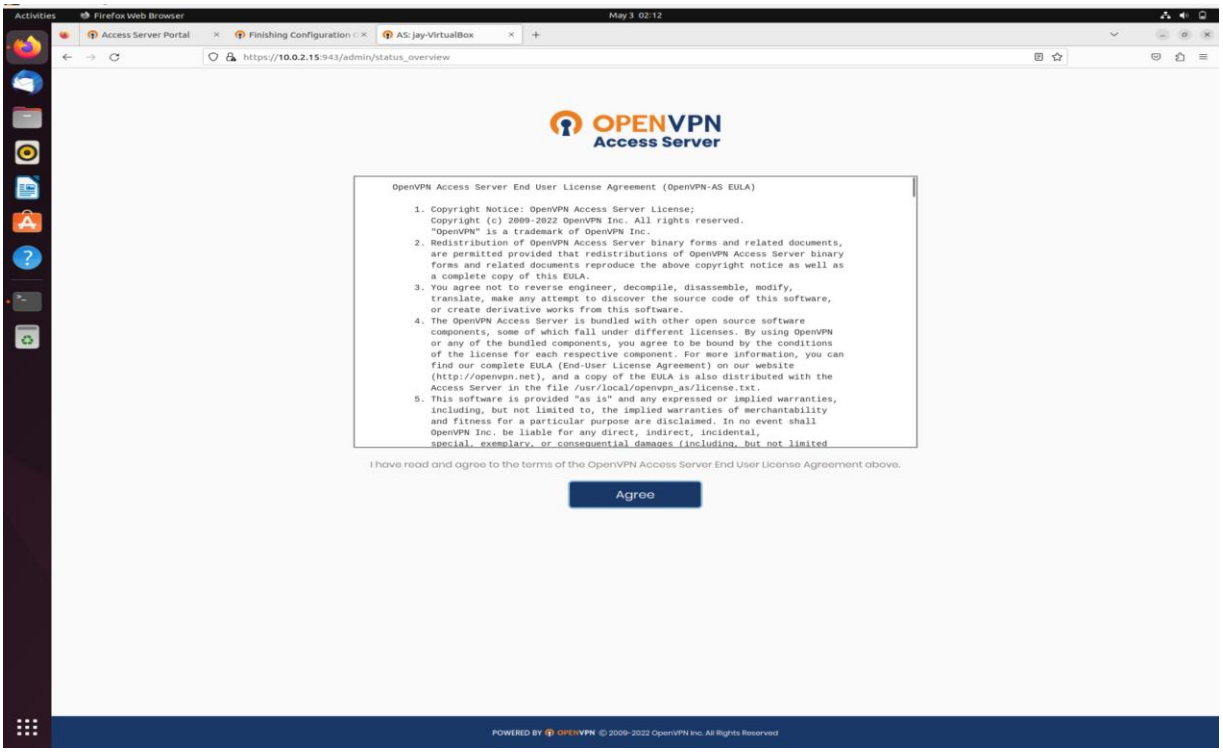
Can either use full file path or do it like this by switching to directory first to install packages that were downloaded.



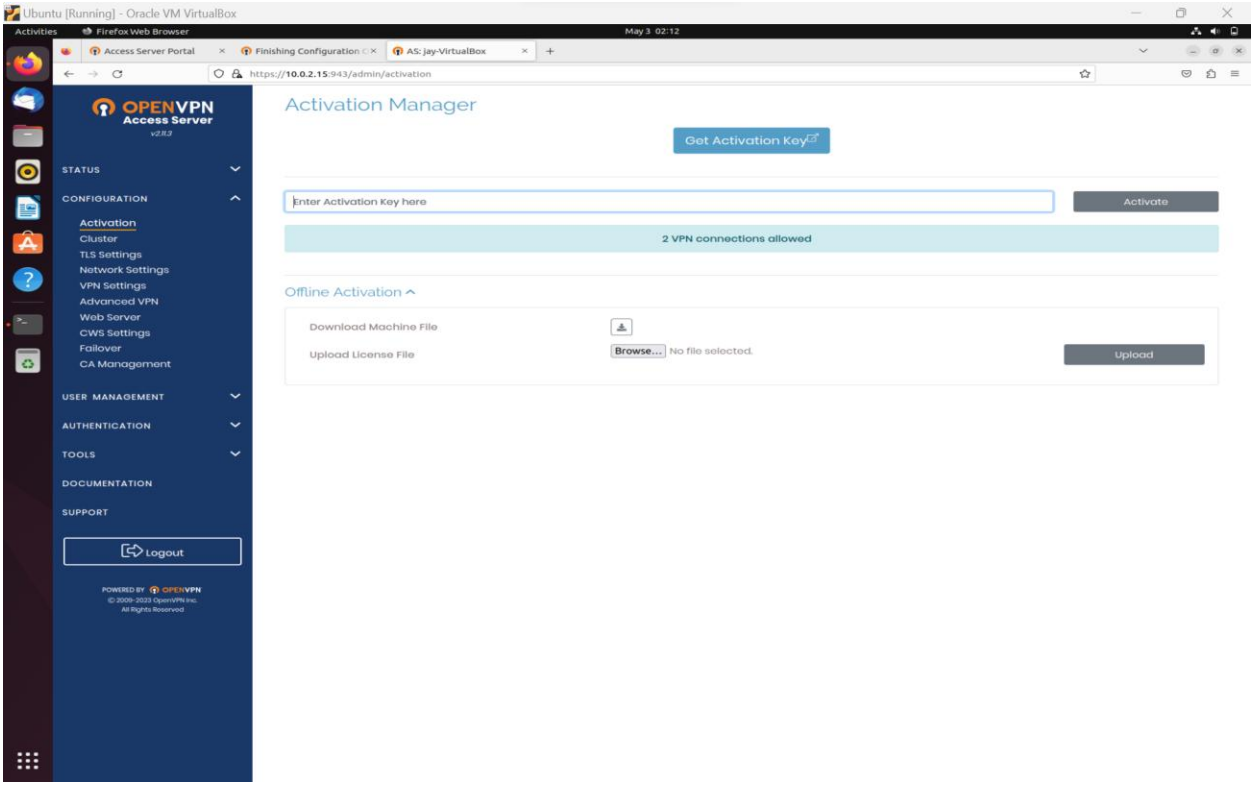
The 2 packages are right here on the Access Server portal.



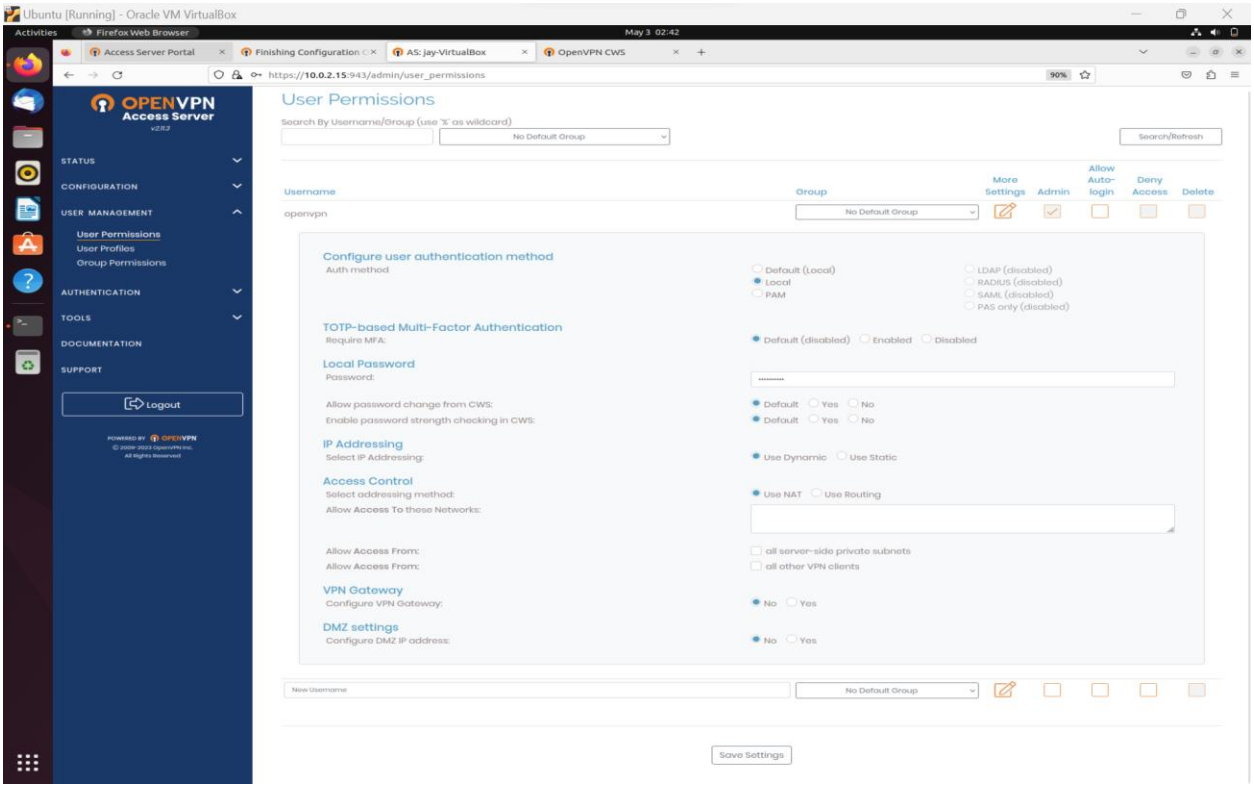
Login to “admin” Access Server interface.



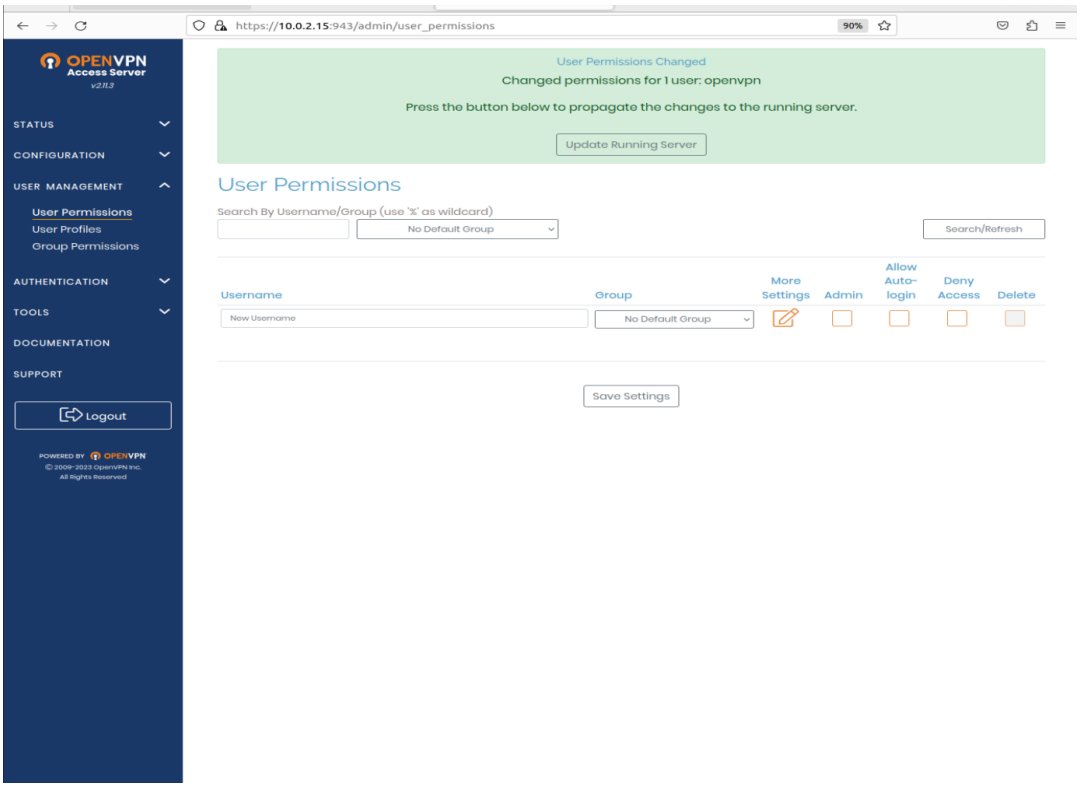
Click on “Agree”.



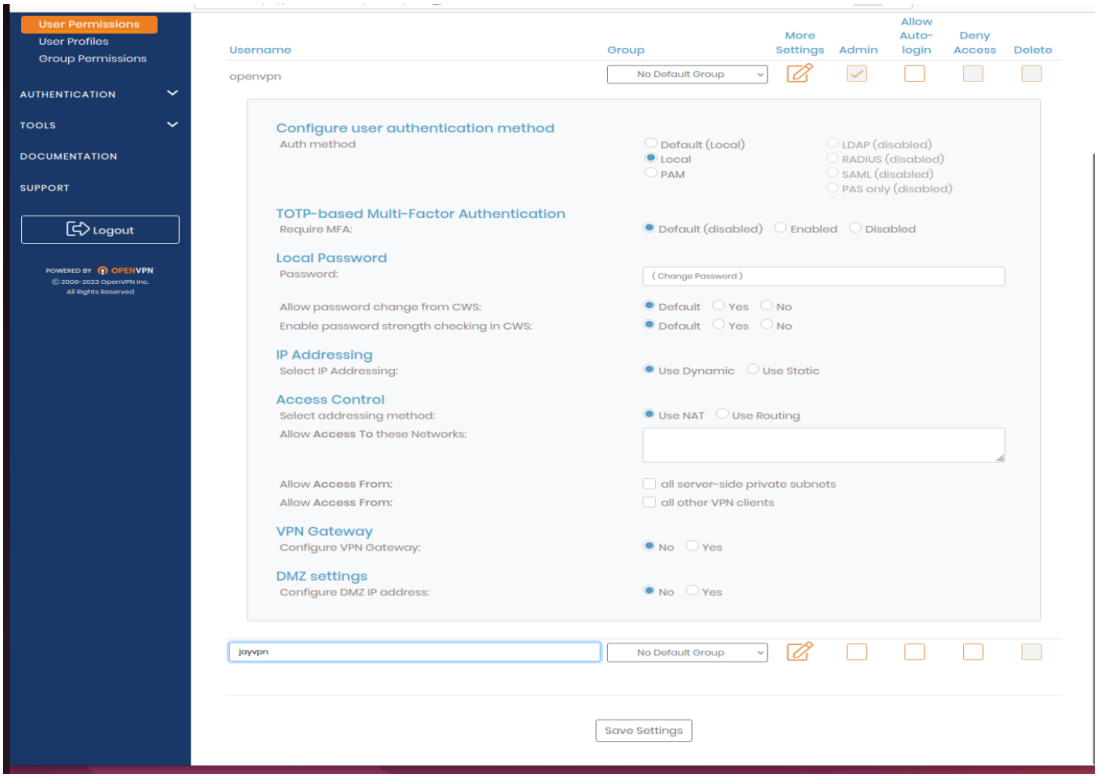
On left side column click on “Activation” underneath “Configuration”.



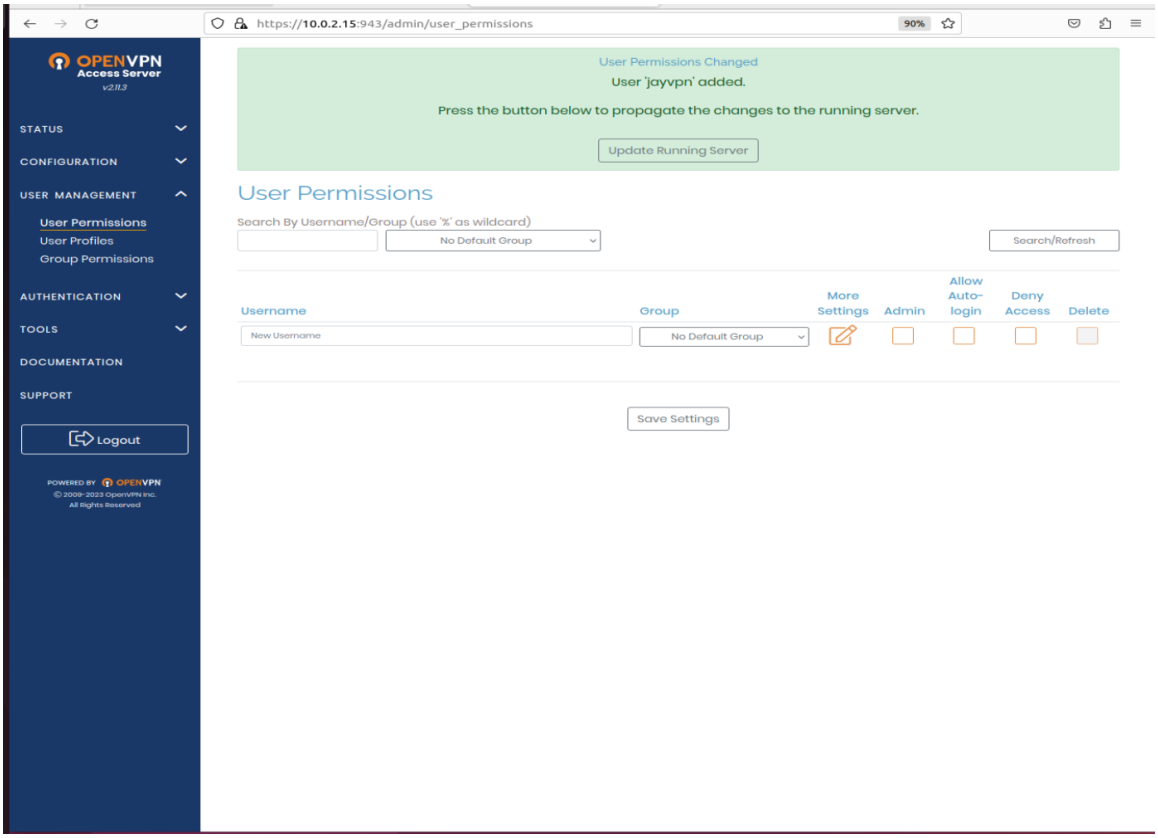
Can change the password in “User Permissions” under “User Management”.



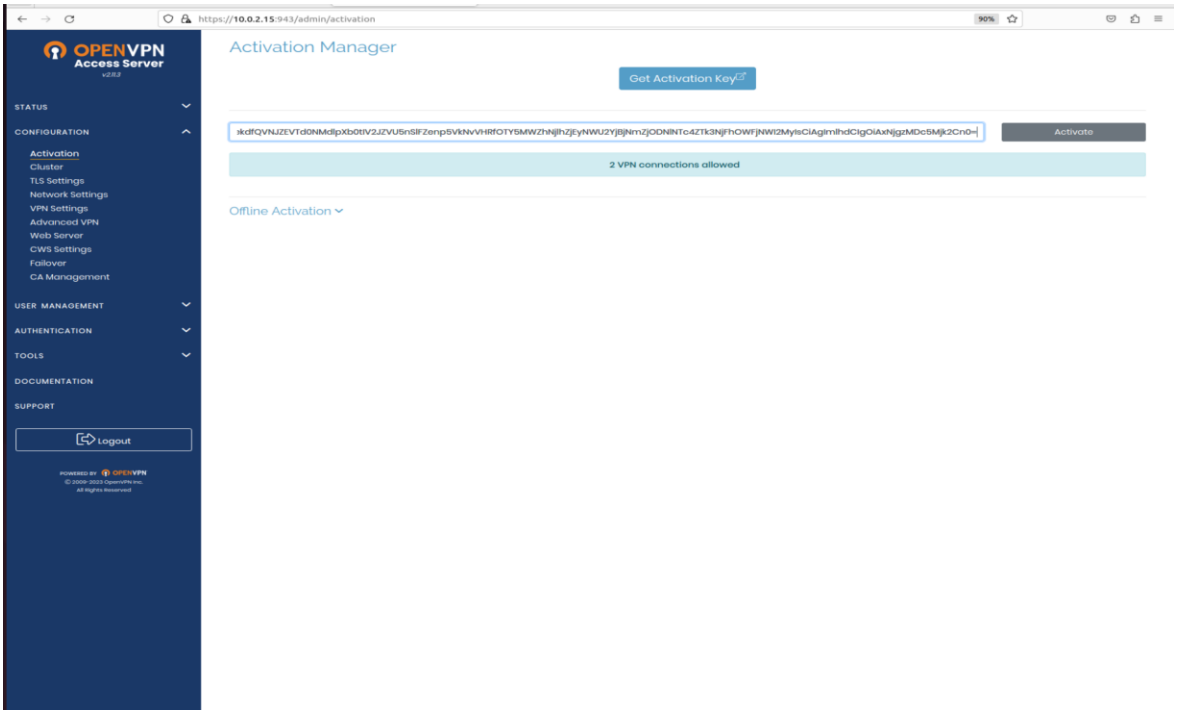
Click on “Update Running Server” when done to make sure changes are applied.



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

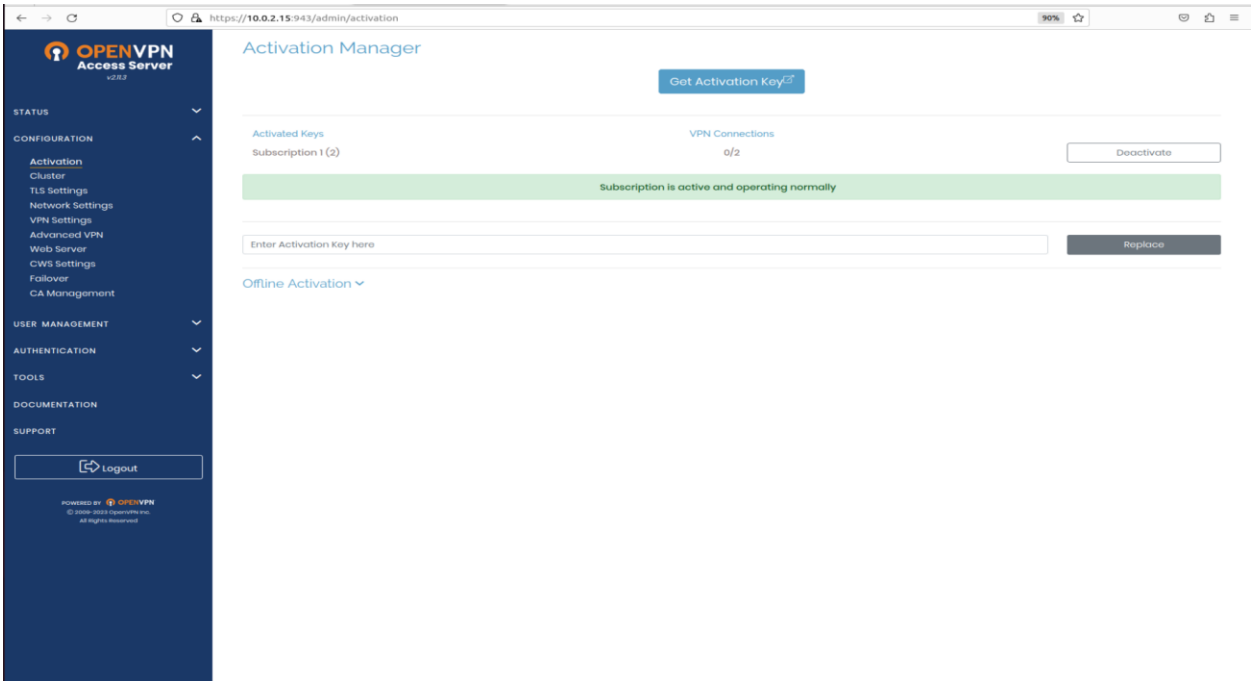


Make sure to Update Running Sever again.

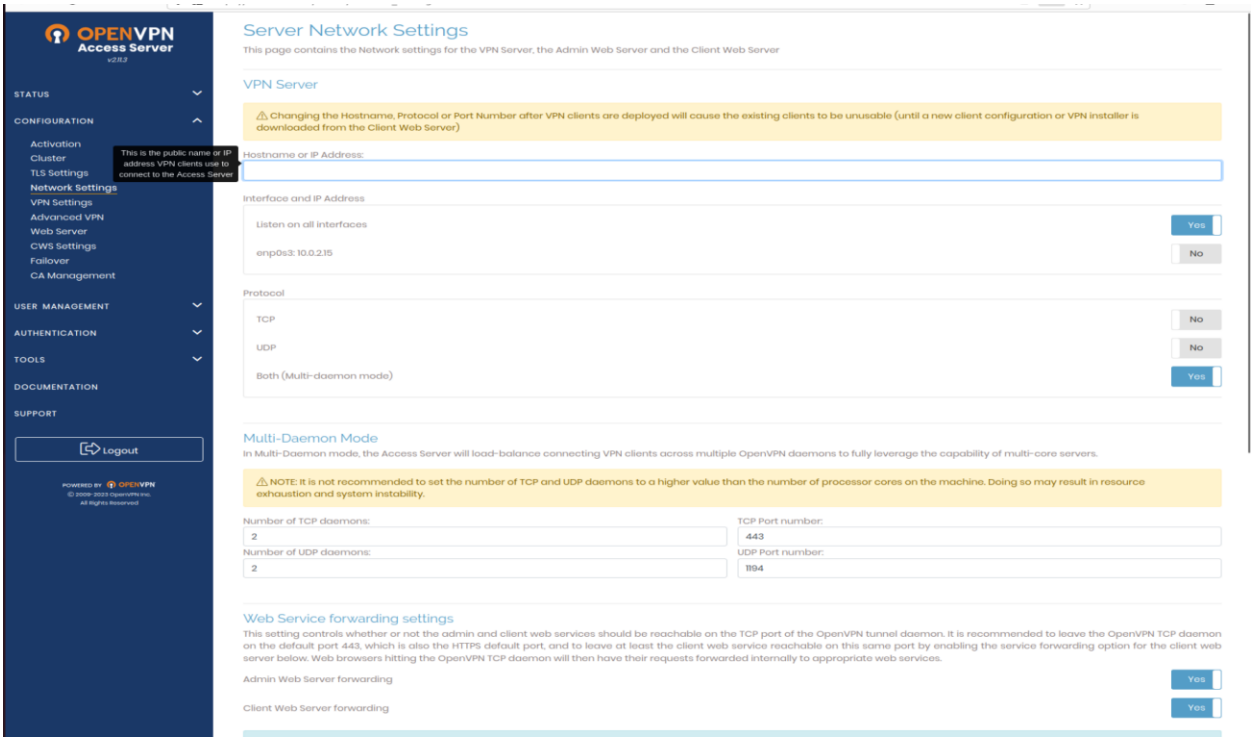


Go to “Activation” under “Configuration” on left side column.

Then, click “Get Activation Key”.

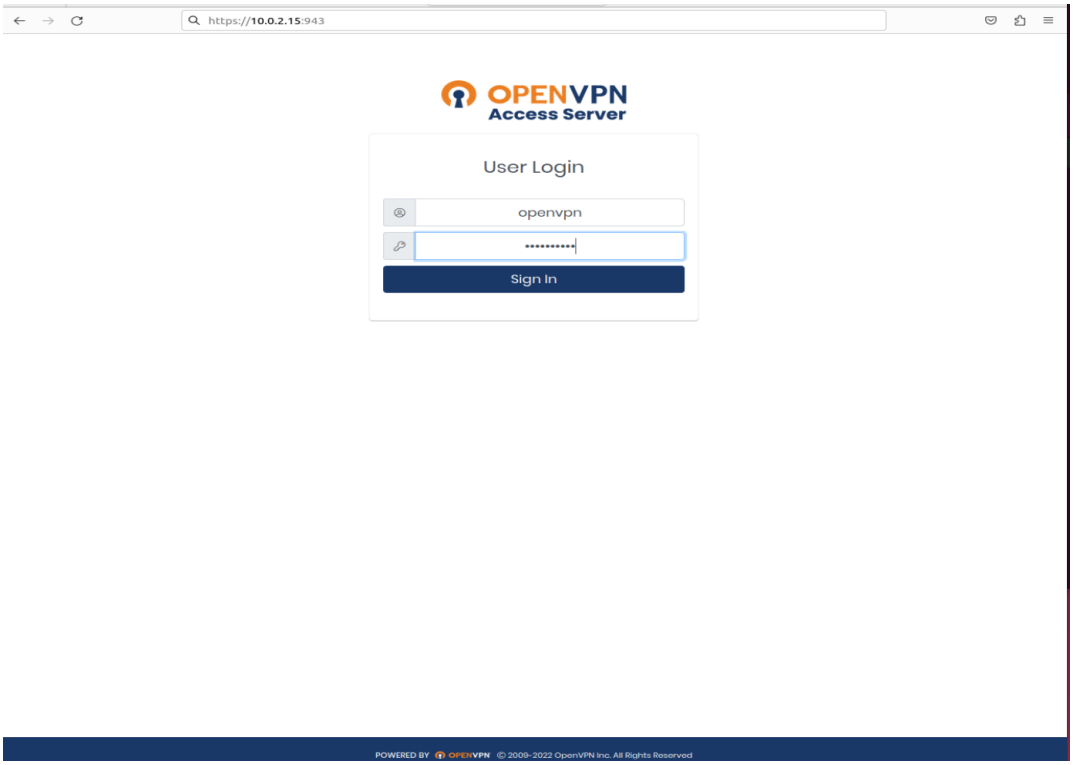


Should get message that it is active and operating normally.

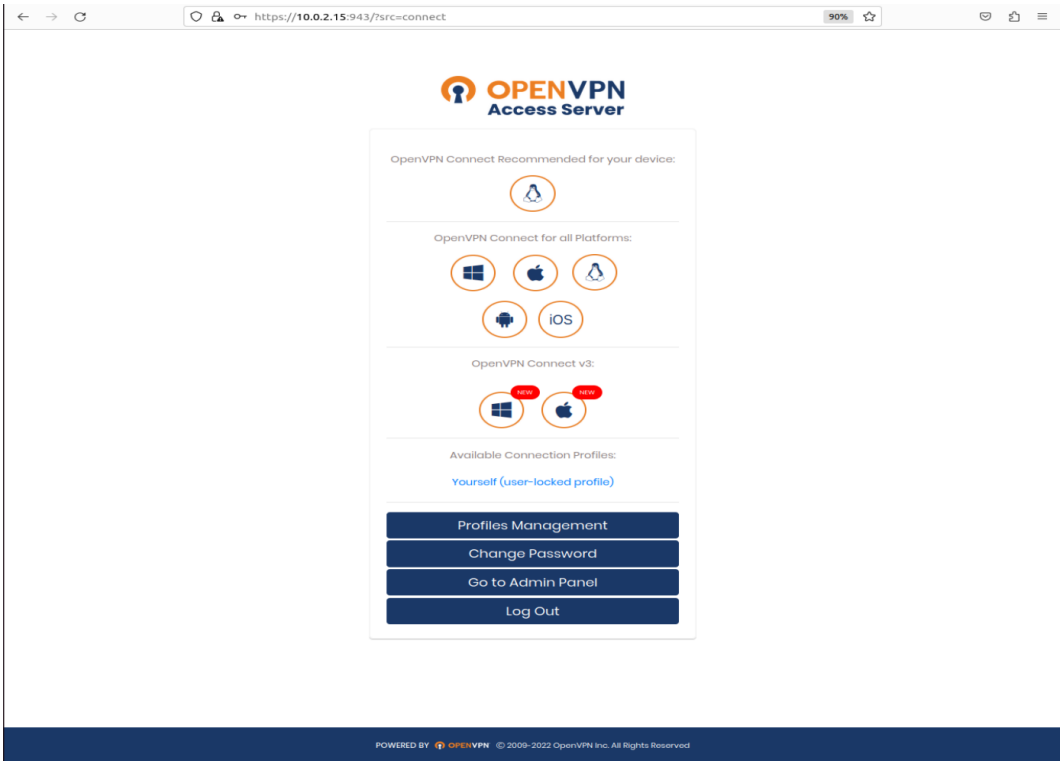


Can change the Hostname/IP address under “Network Settings” which is under “Configuration” on the left side column.

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)

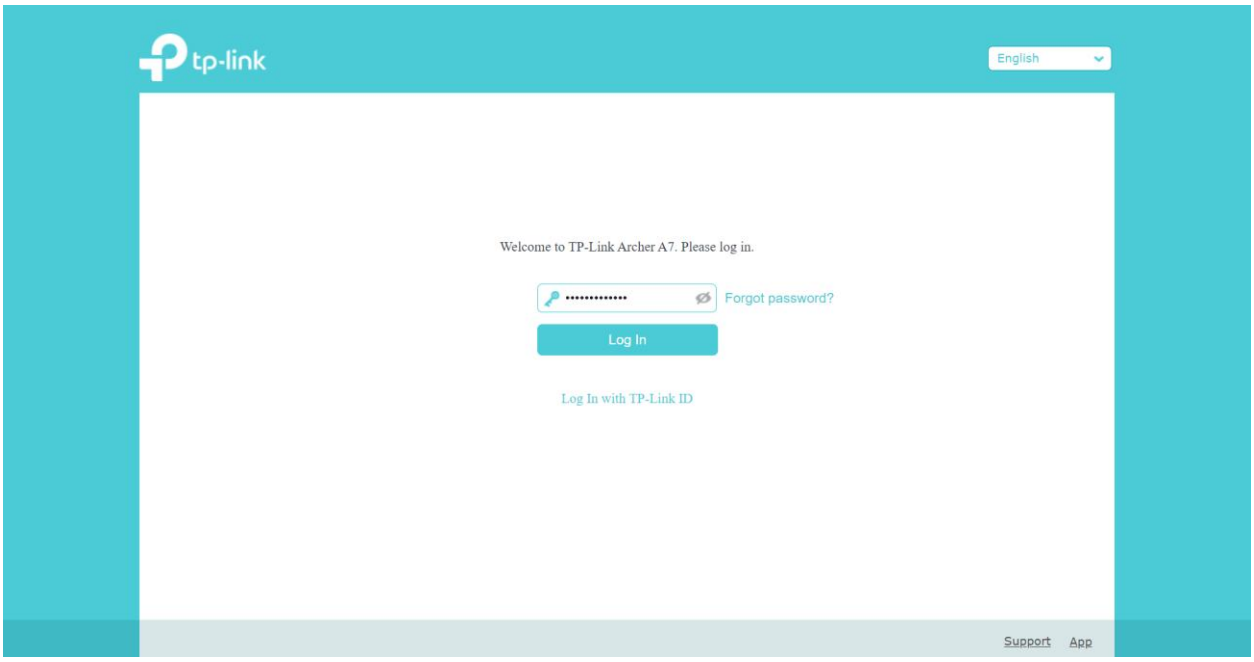


Now the client can download the OpenVPN connect to use OpenVPN via OpenVPN tunnelling protocol.

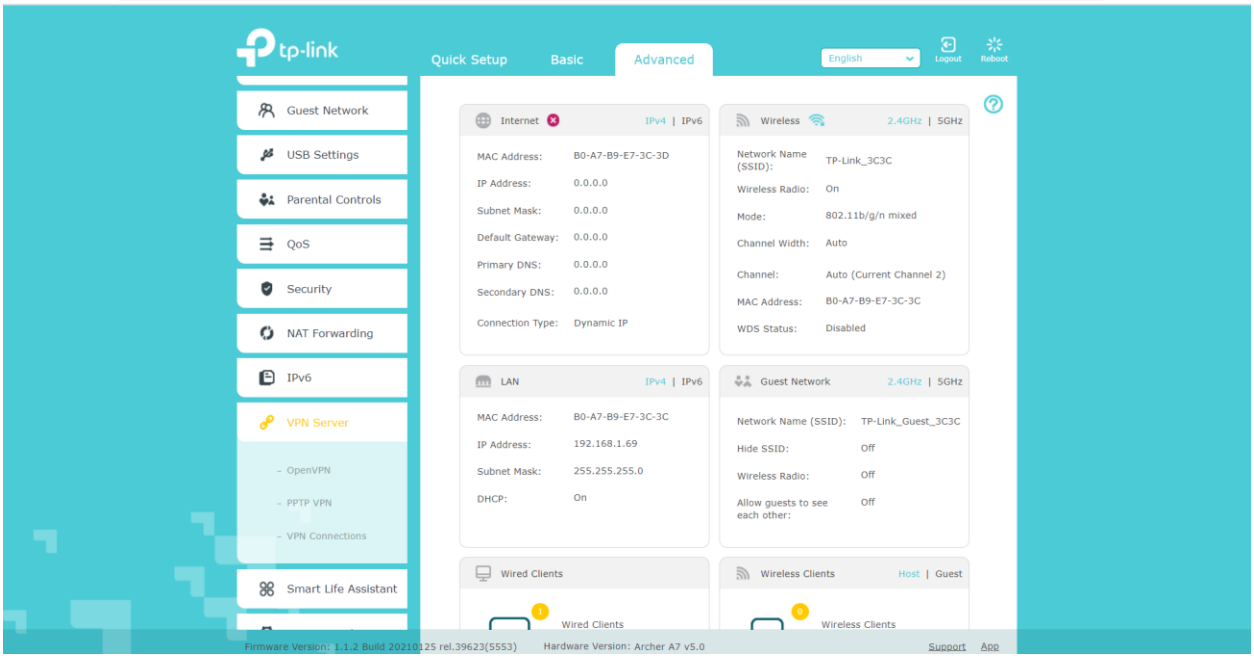
Linux requires a few commands which it walks you through.

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

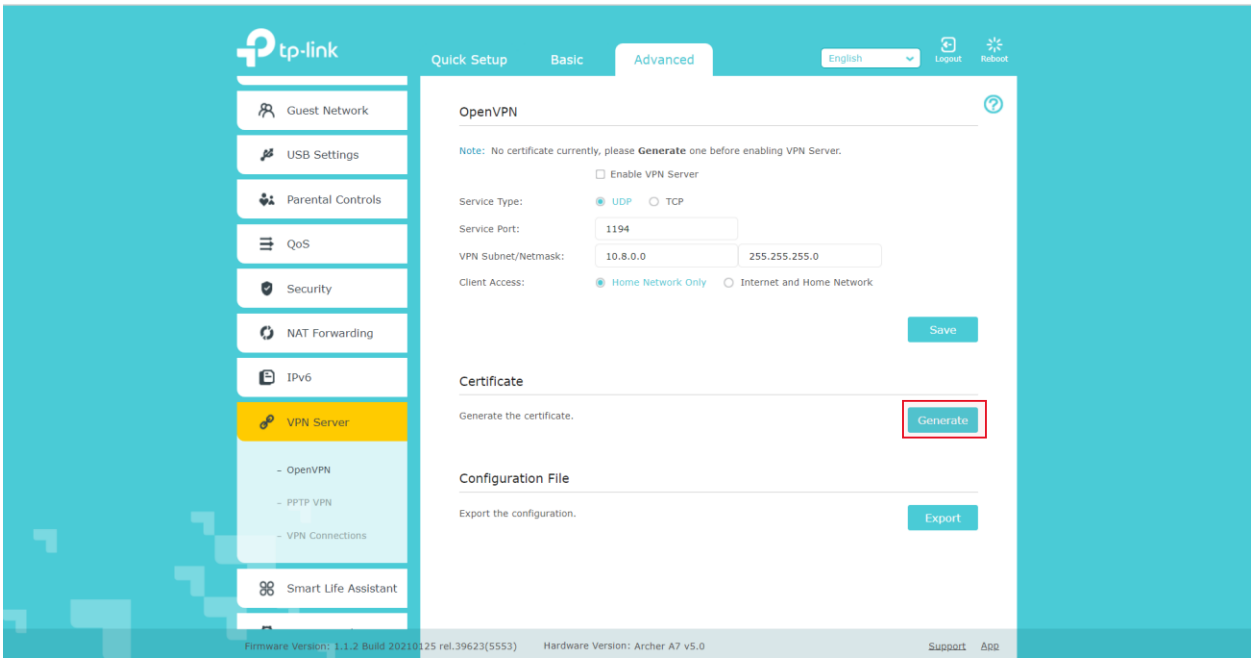
Aside from configurating an OpenVPN server on your computer it can also be done a wireless device like a router or Wireless Access Point.



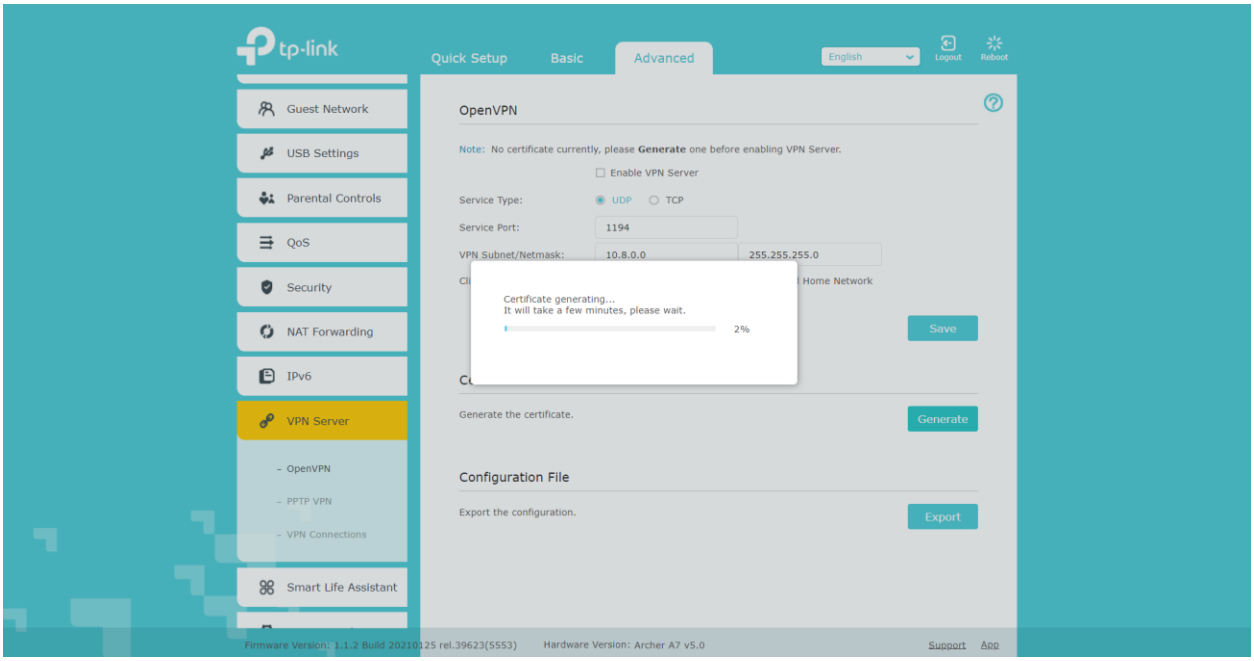
Login to your router/access point.



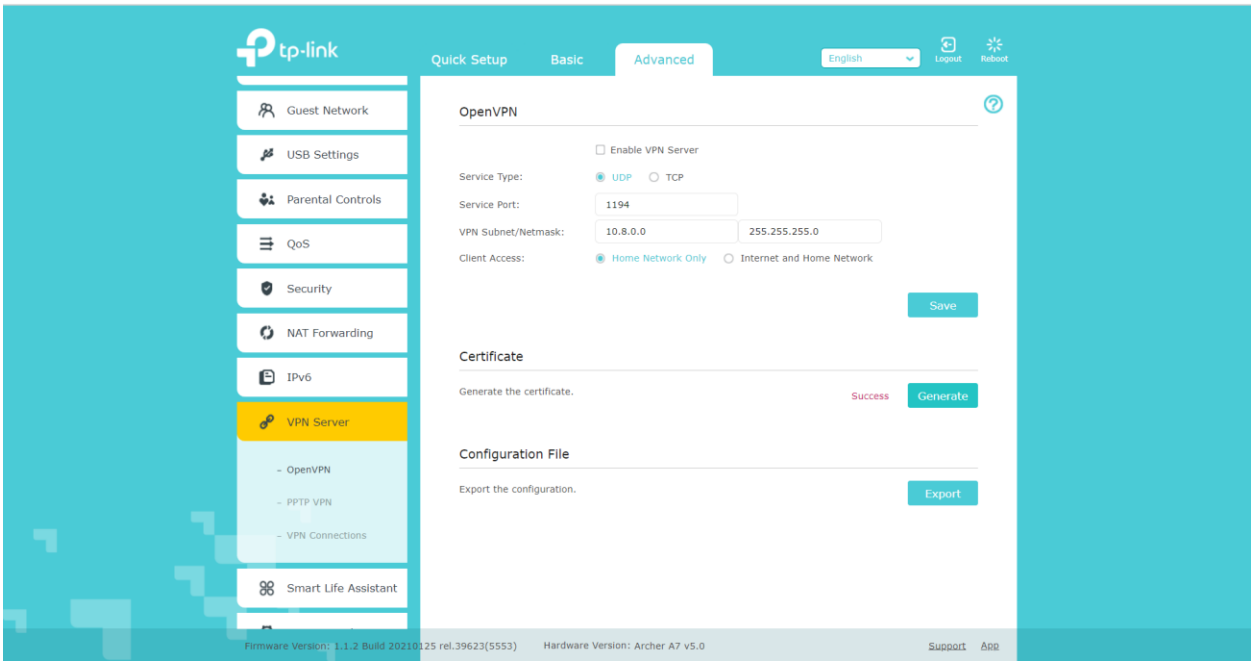
Navigate to your VPN Server settings and look for “OpenVPN” and click on it.



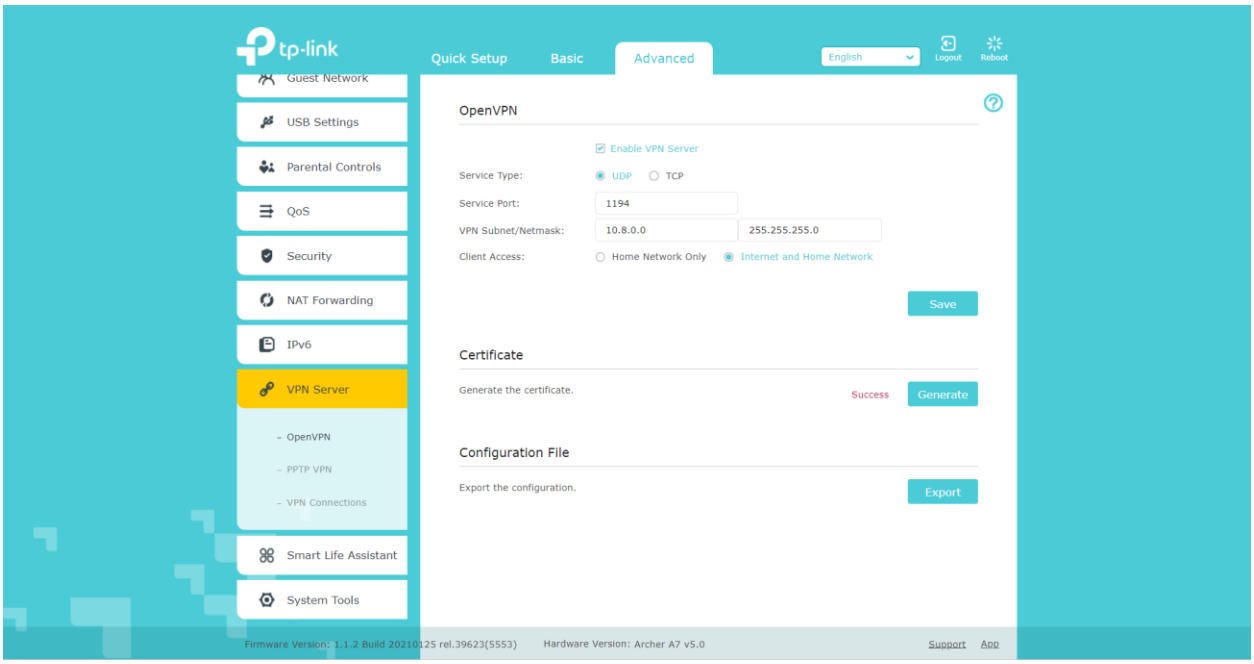
Click on “Generate” under “Certificate”.



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



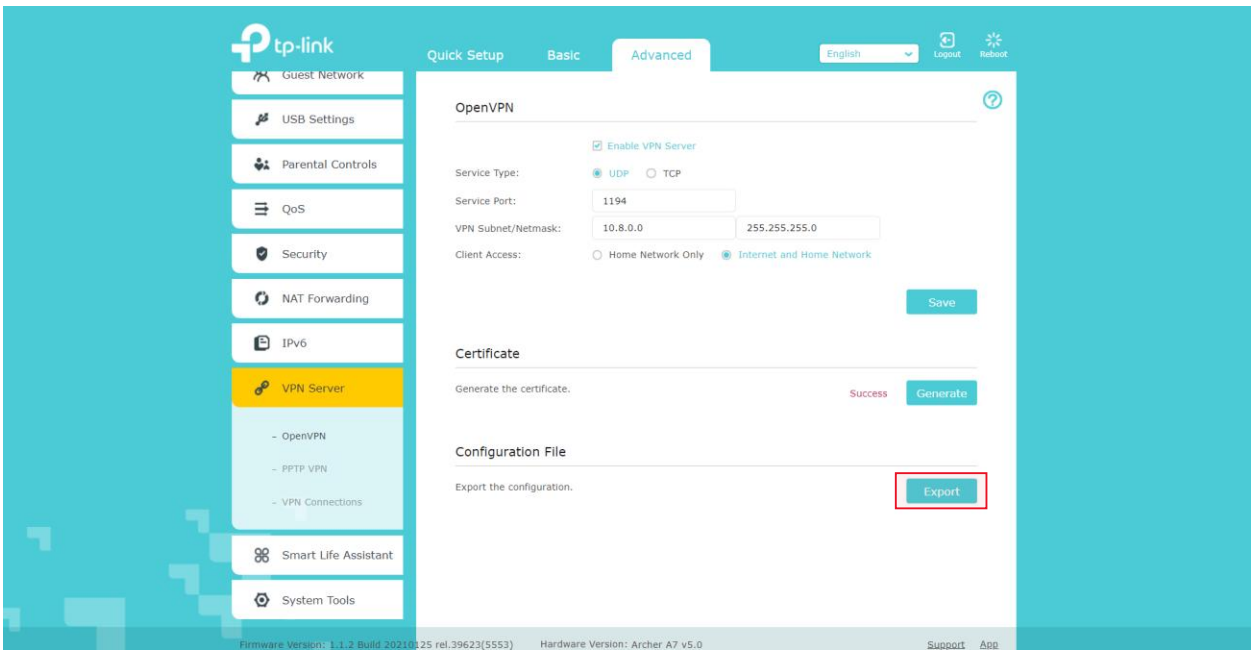
Should then get a “Success” message in red after completion.



Click on the “Enable VPN Server” checkbox.

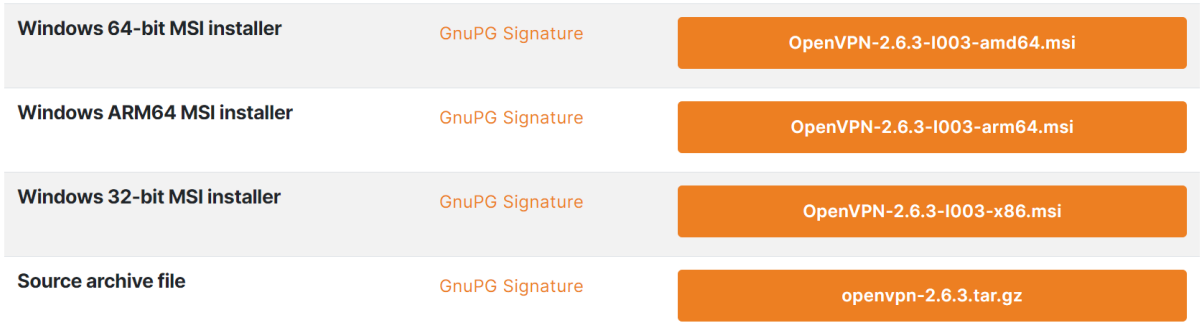
The “Check Access” portion can either be “Home Network Only” or the “Internet and Home Network” if you want to have internet access too.

Click on “Save” when you are done.



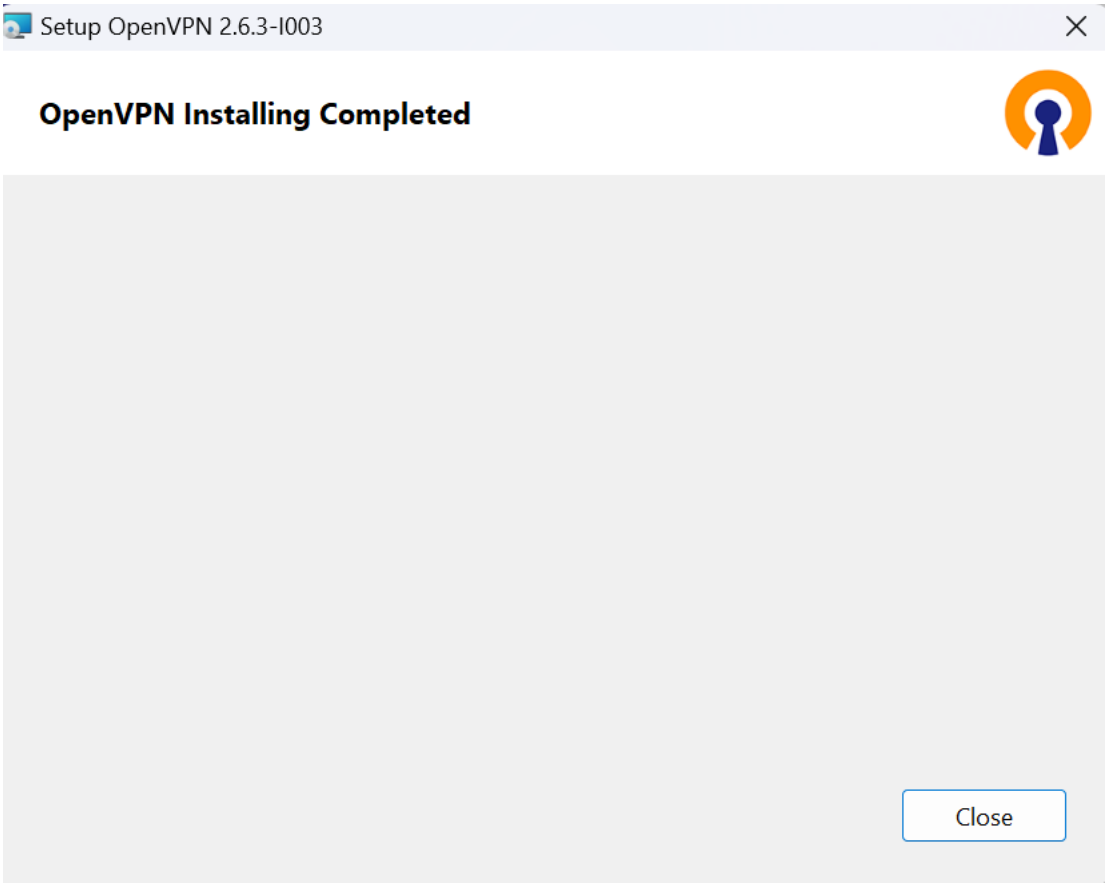
Click on “Export”.

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

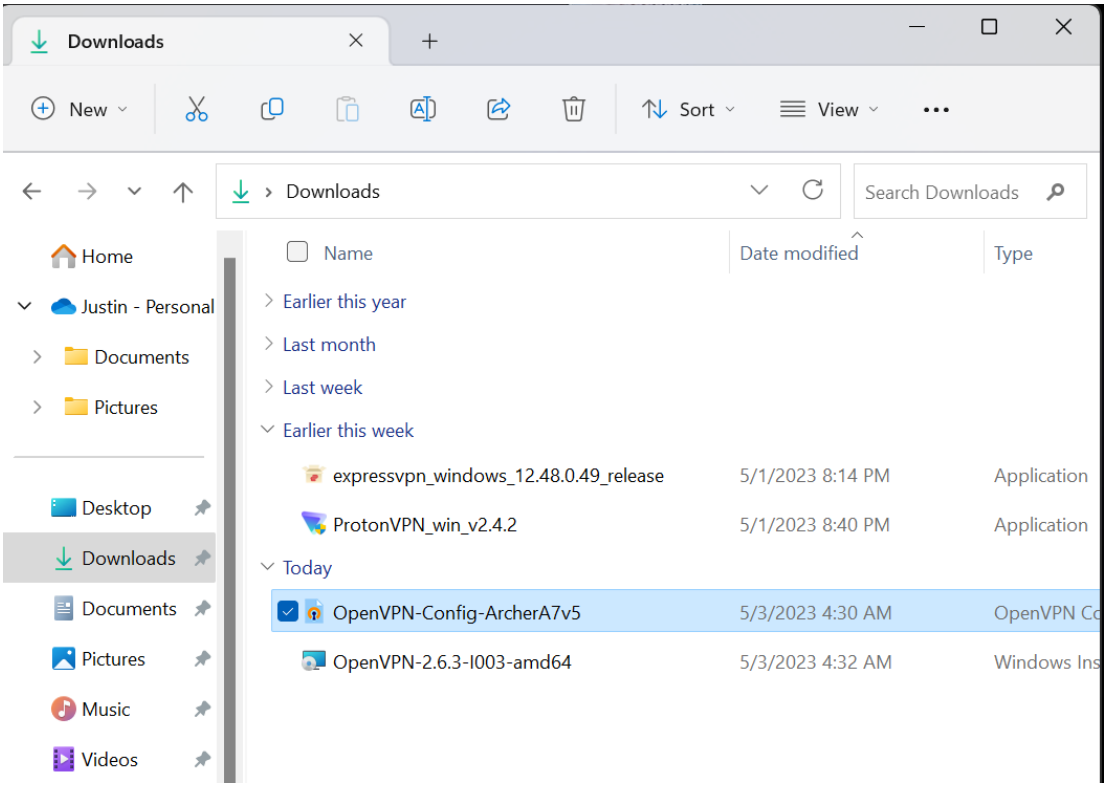


Choose download type on your client device.

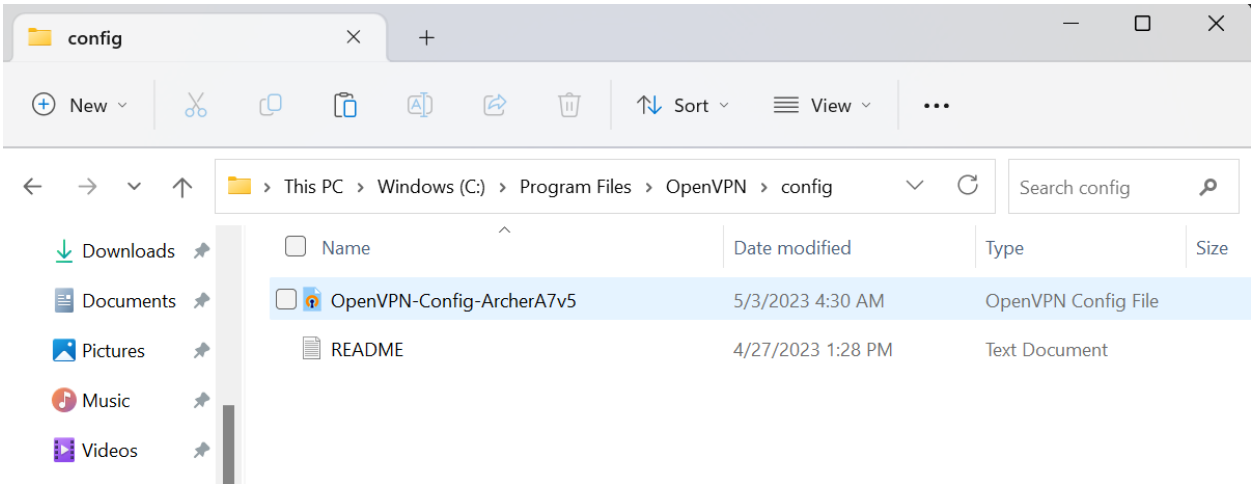
After download is complete click on the file.



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

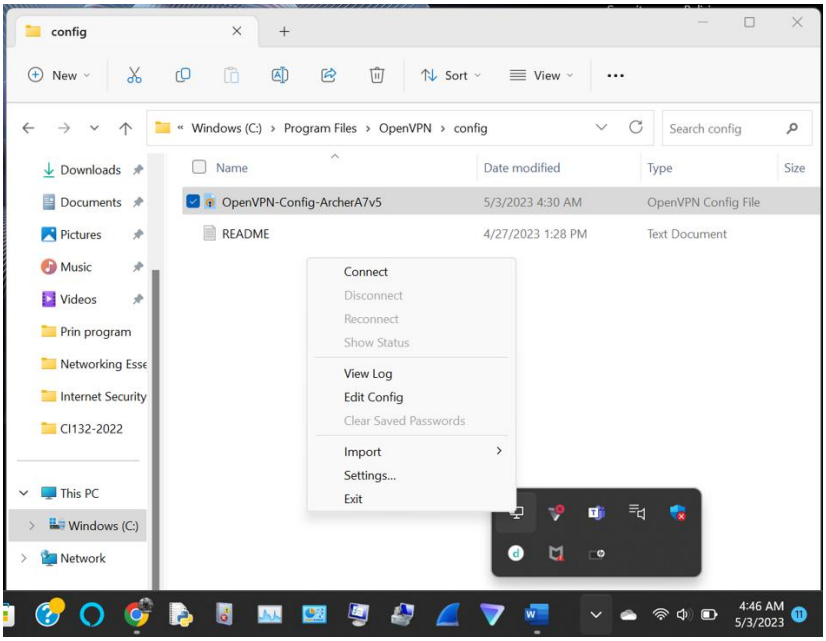


Go to the copy of the OpenVPN server file that was exported from your router/access point, and make a copy of it.



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”.

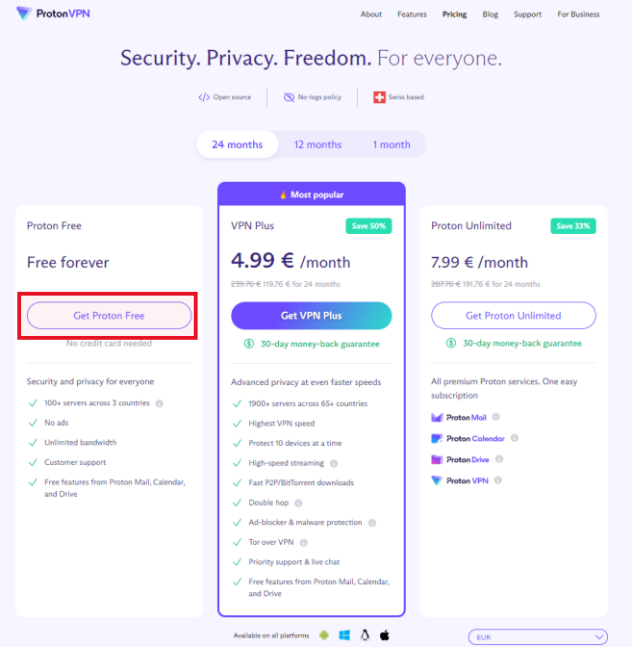
OpenVPN is open-source and free but there are other VPN services too.

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)

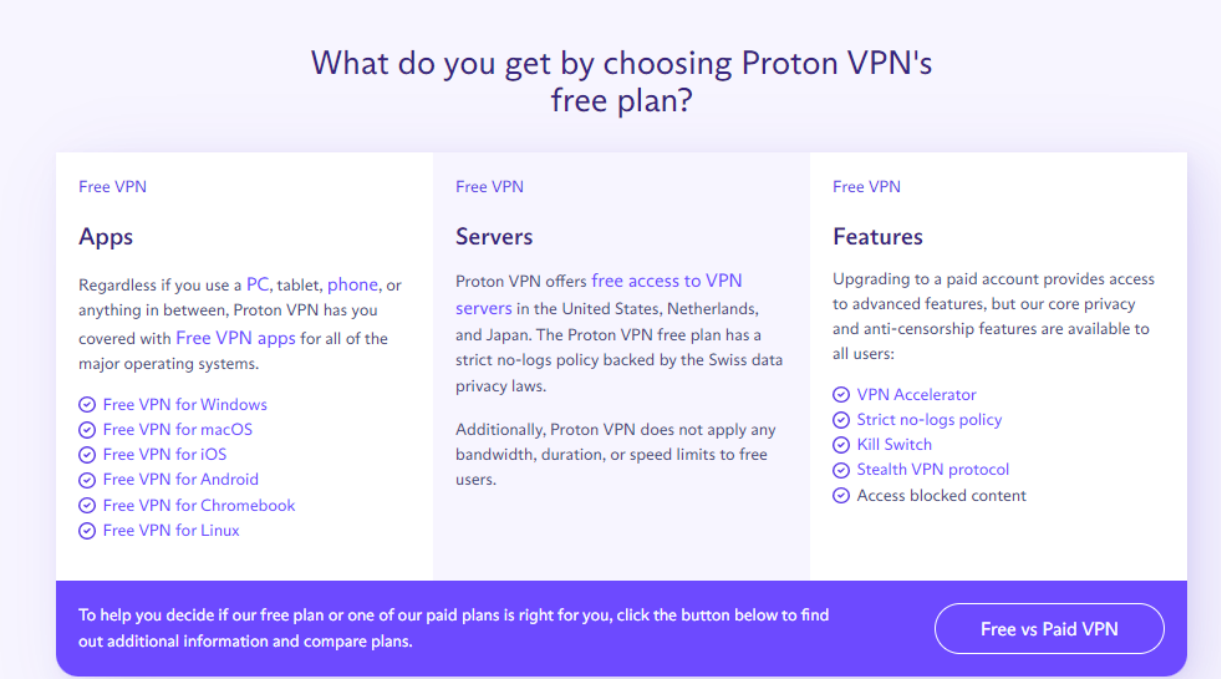
- Unlimited bandwidth.
- NO Advertisements.
- And features from their Mail, Calendar, and Drive for free along with their VPN services.
- Free customer support too.

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.

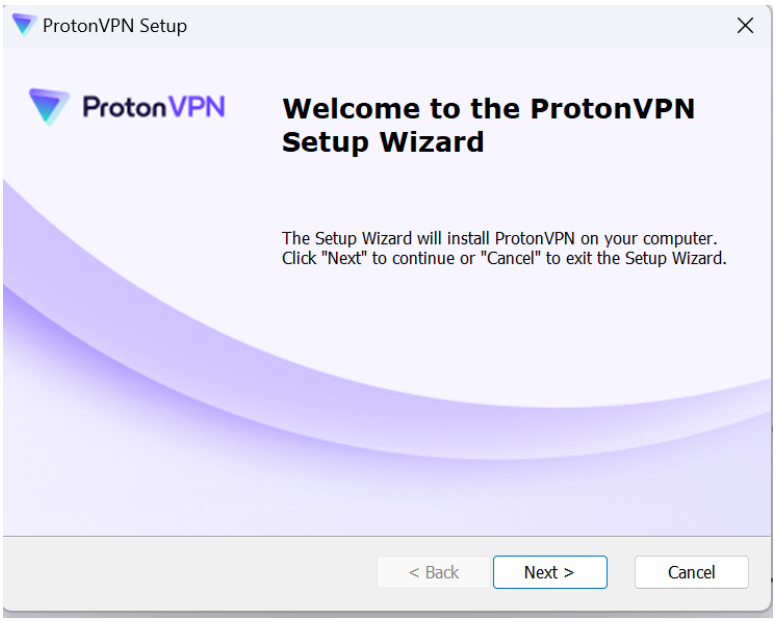
The 3rd version of ProtonVPN is the "Proton Unlimited" version which comes with all of their services without any restrictions as they are all unlimited.

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.

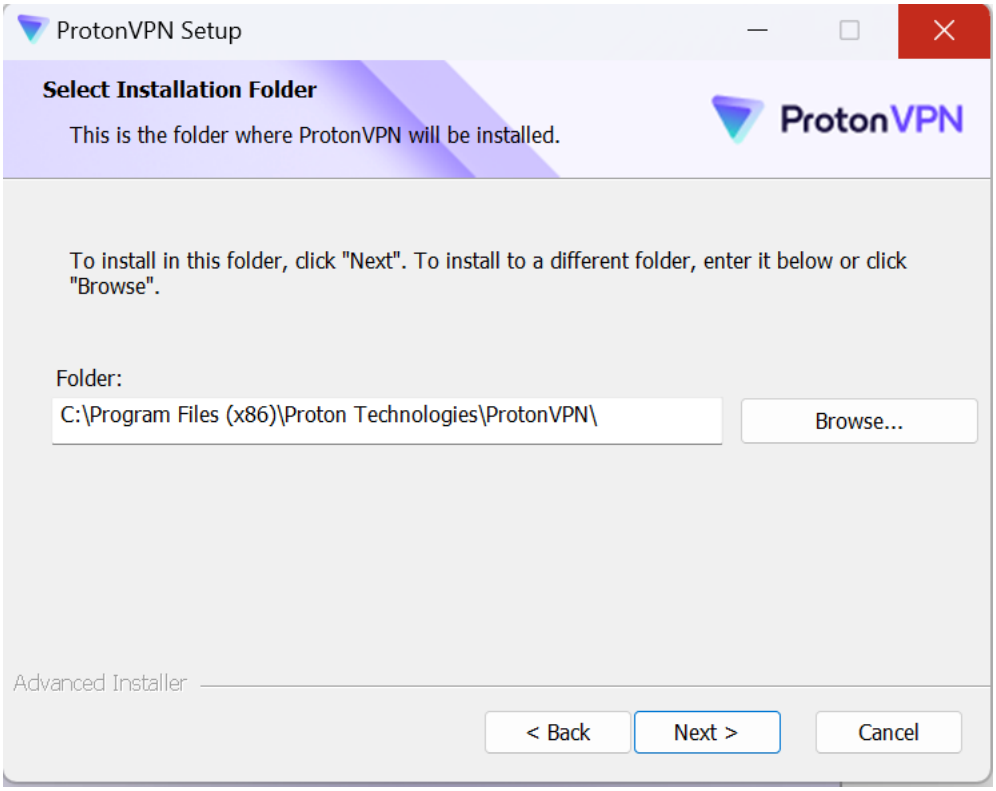
Getting the monthly plan is 9.99 euro/10.98 USD for Proton's VPN plus and 11.99 euro/13.18 USD for Proton Unlimited.



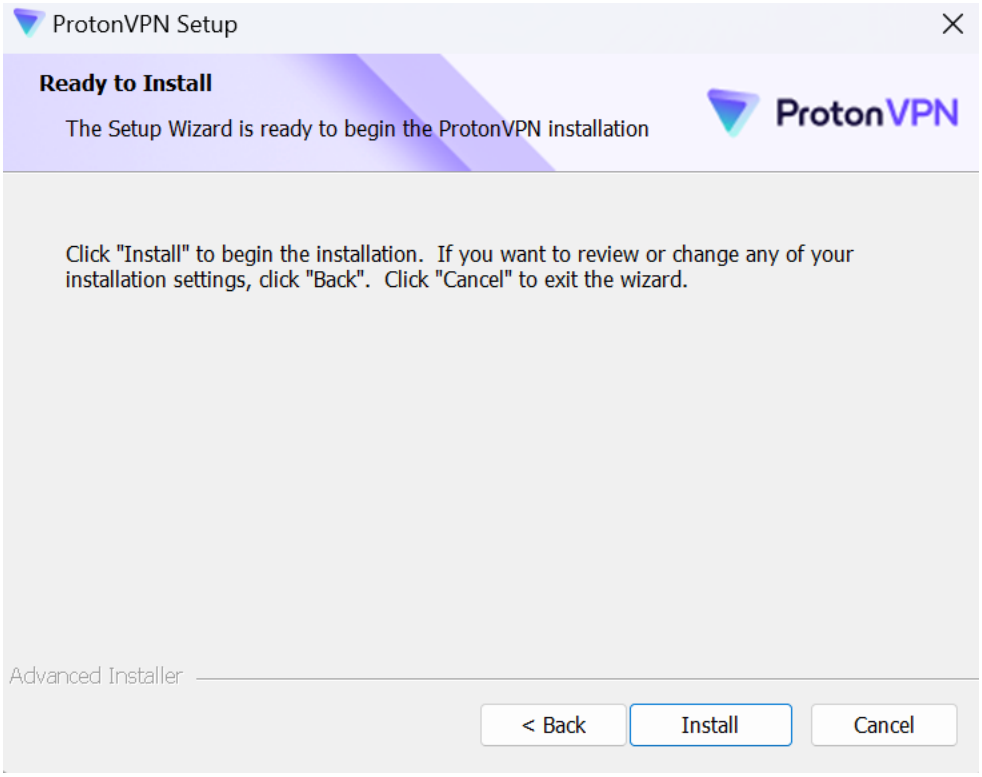
Anyone can download this free/open-source Proton VPN on a variety of systems such as Windows, macOS, iOS, Android, Chromebook, and Linux.



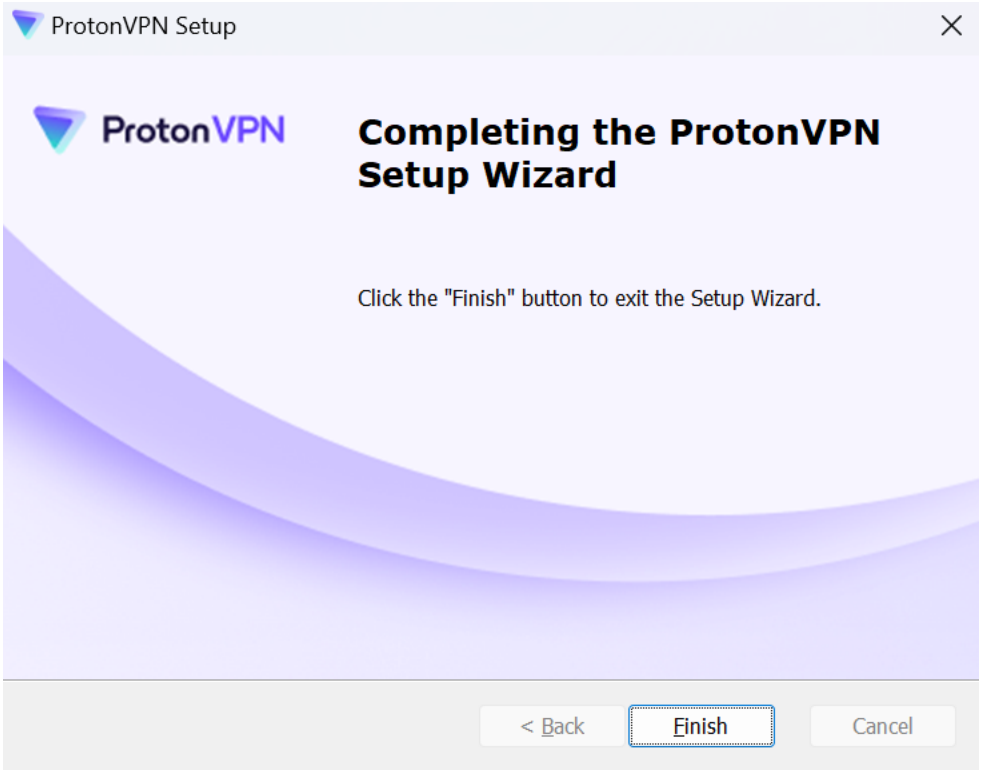
After installing the free version of ProtonVPN, click on "Next".



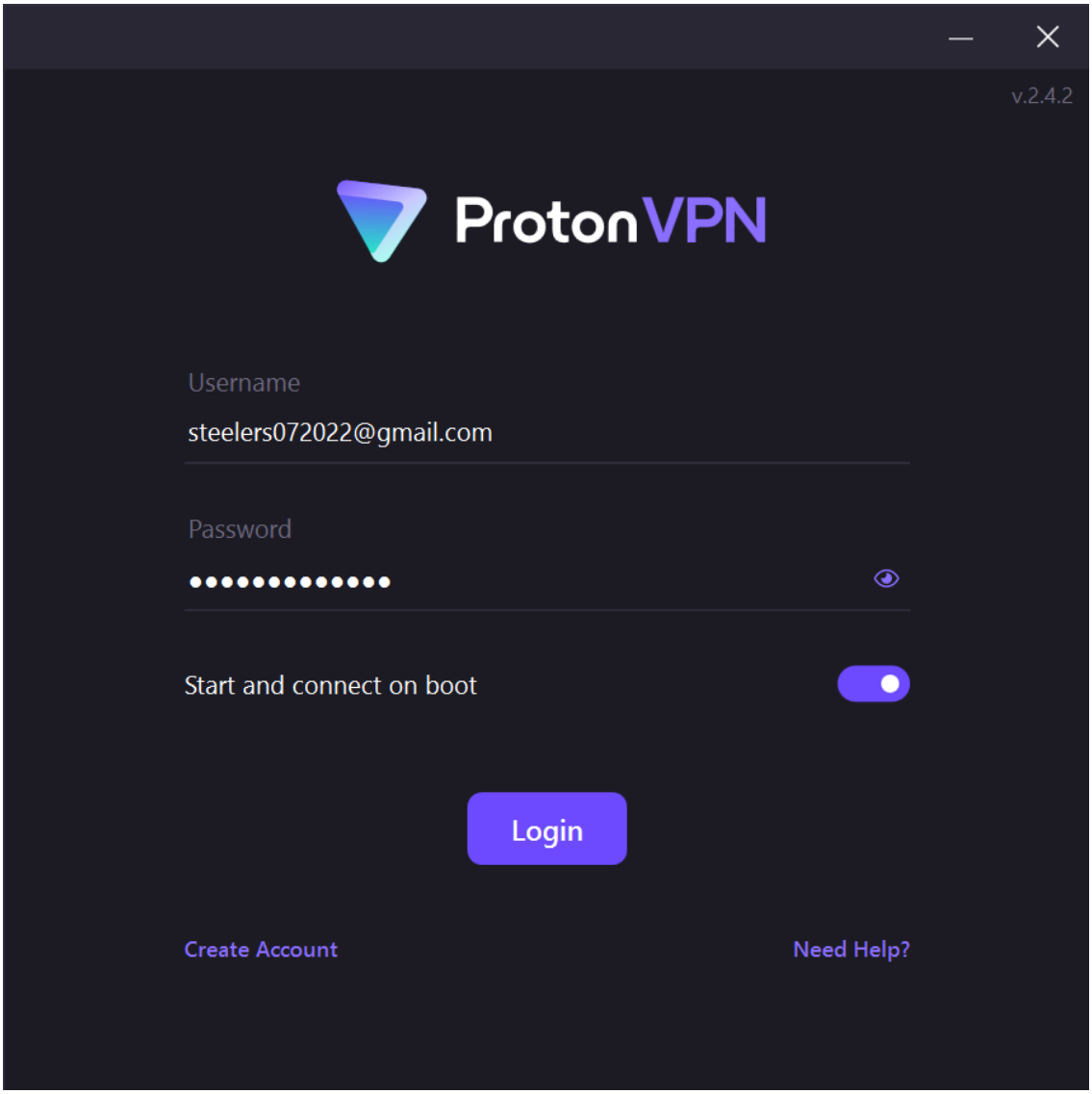
Choose folder/directory path.



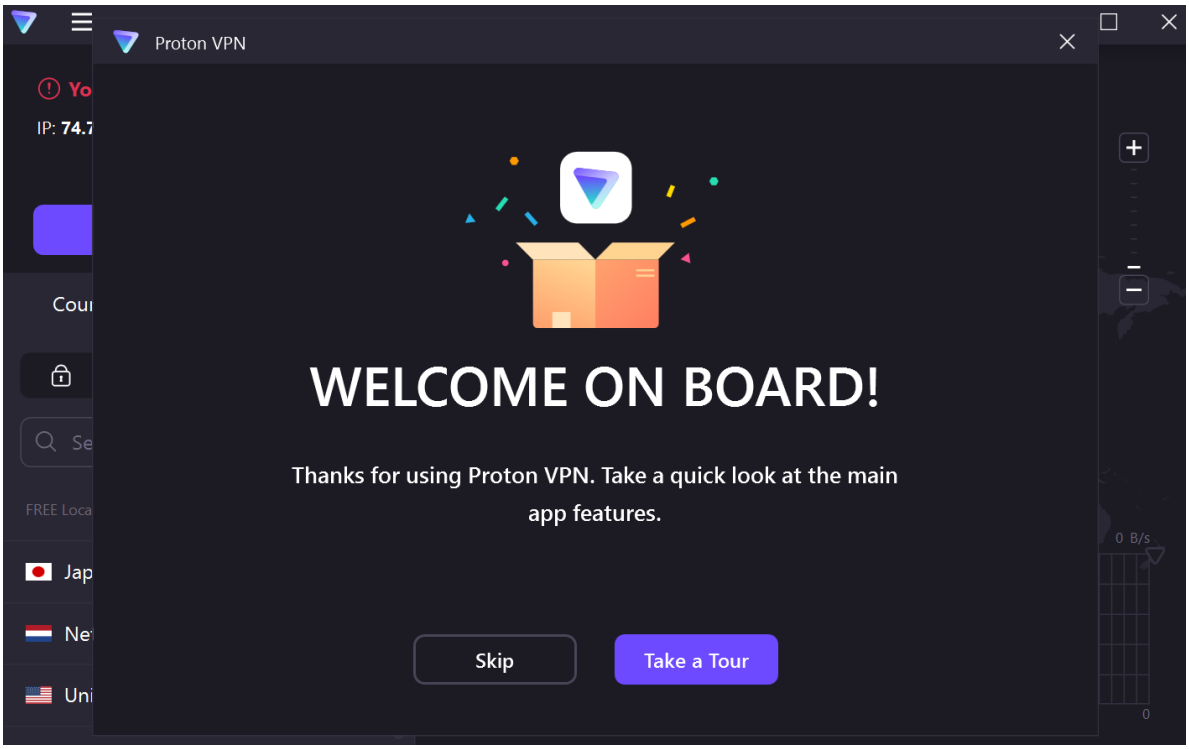
Click on “Install”.



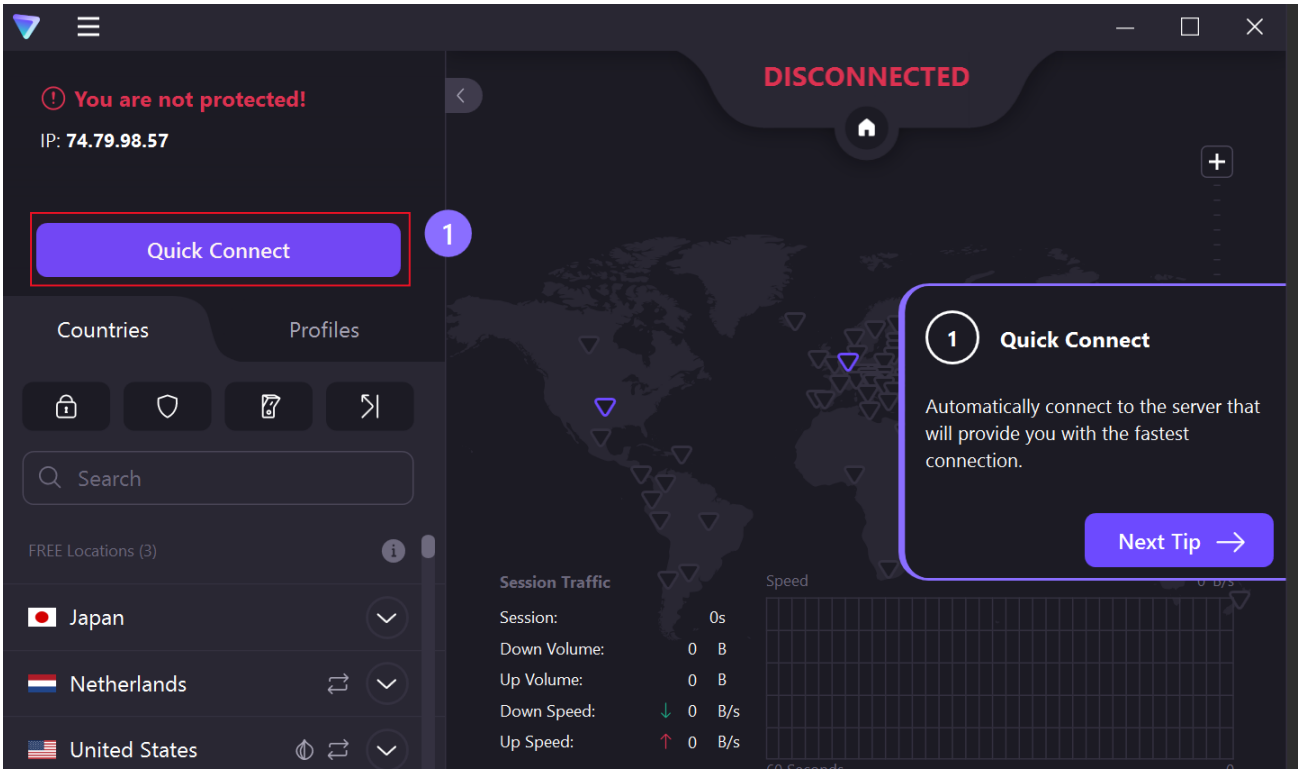
Click on “Finish” after the installation has completed.



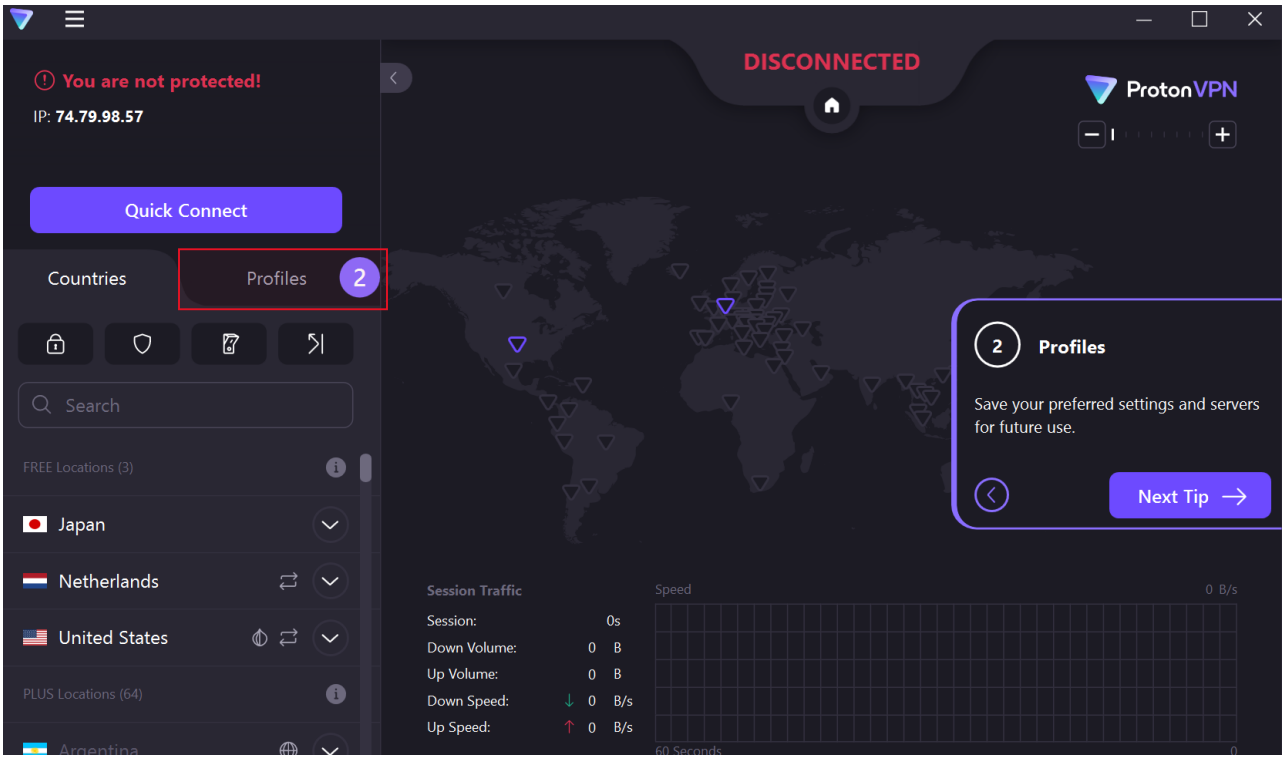
Login or create an account and then login.



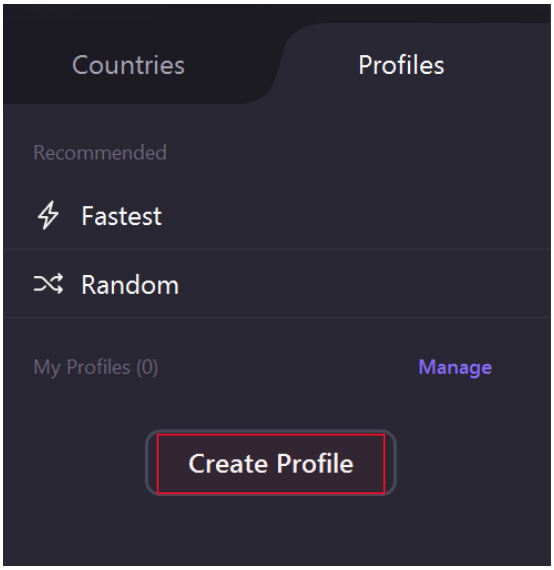
Click on “Take a Tour”.



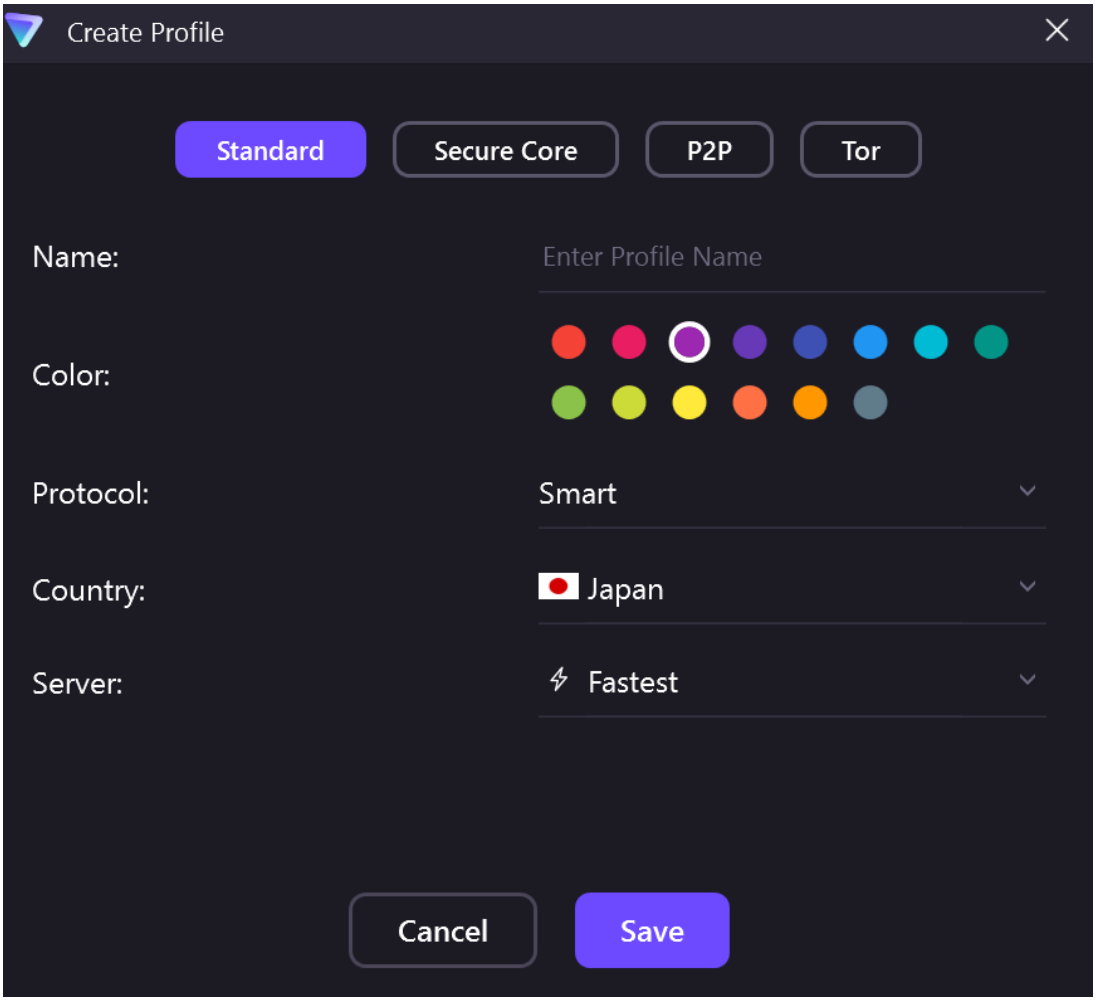
The “Quick Connect” option is what I will be using to connect to a free server quickly and automatically.



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”.



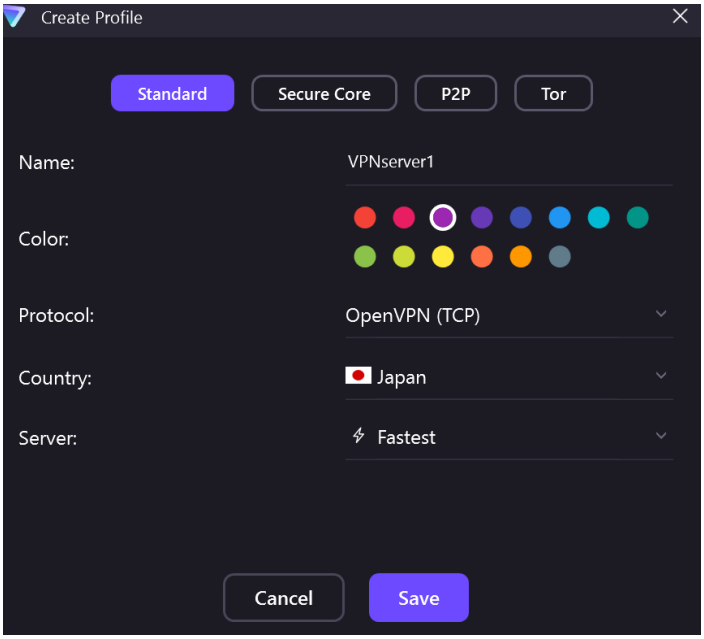
Can choose between a “Standard, Secure Core, P2P, or Tor” connection type.

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.

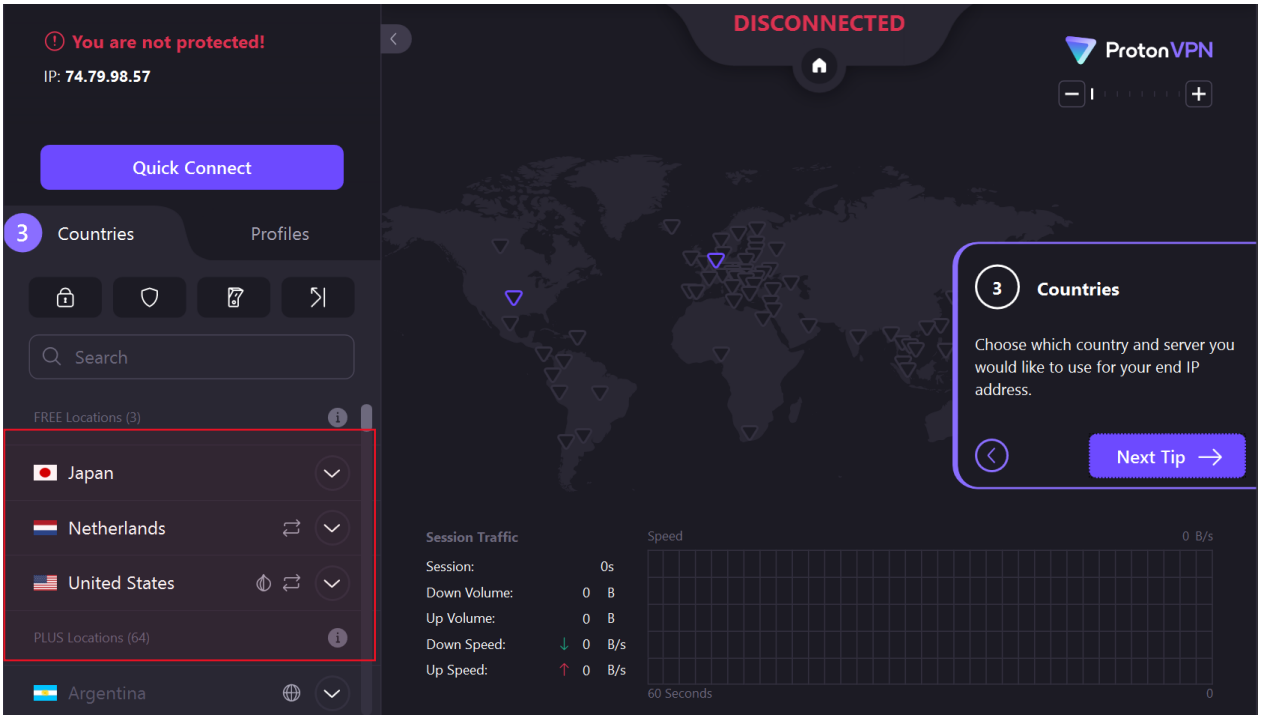
“Smart” will do it automatically, and “WireGuard” protocol is a newer/faster VPN protocol. This is what is mostly used since it has faster speeds while still being secure.



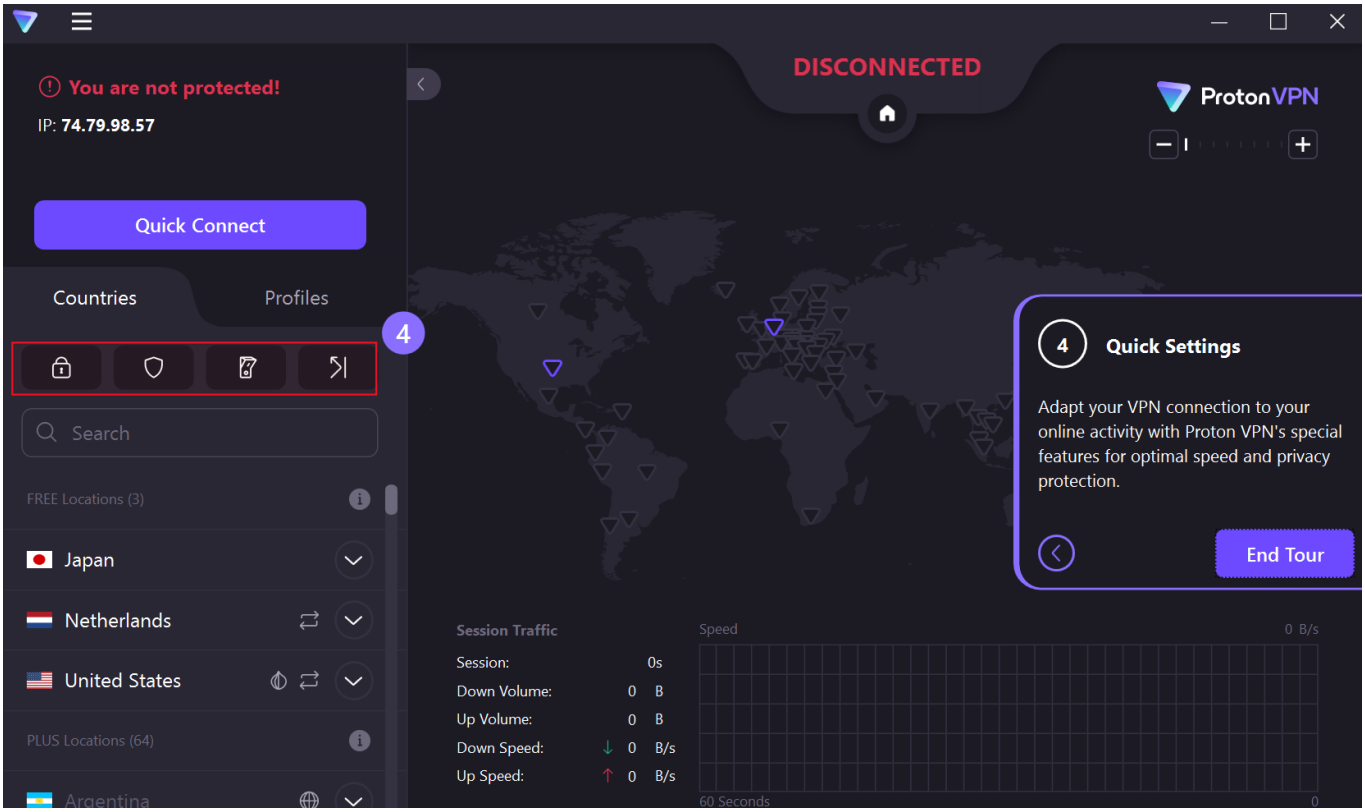
After choosing a Name and Color click on “Save”.

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

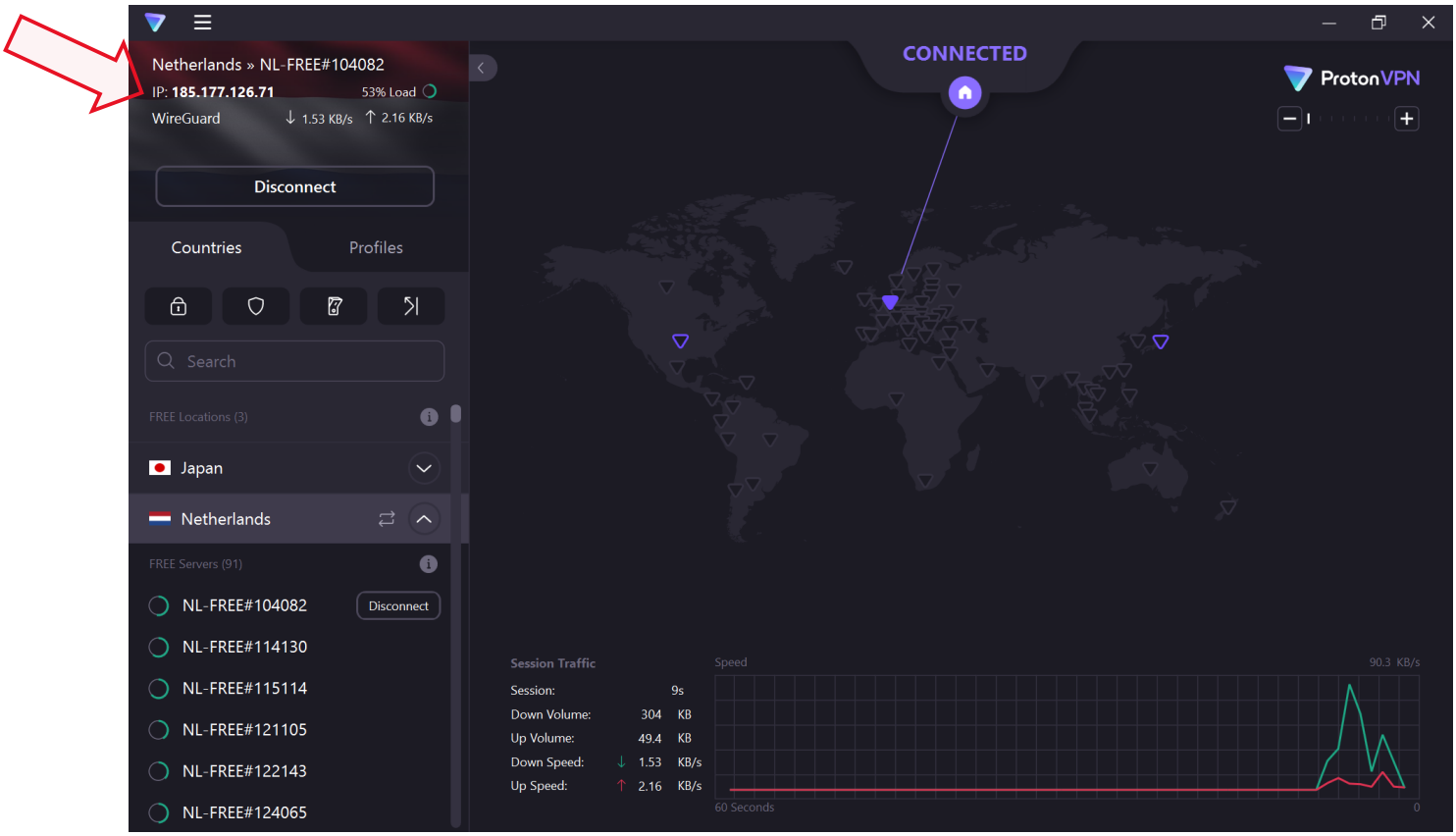
Instead of creating a Profile you can just choose VPN server from the 3 choices on left hand side and click “Quick Connect”, and can then save it to a server profile later if chosen to do so.



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

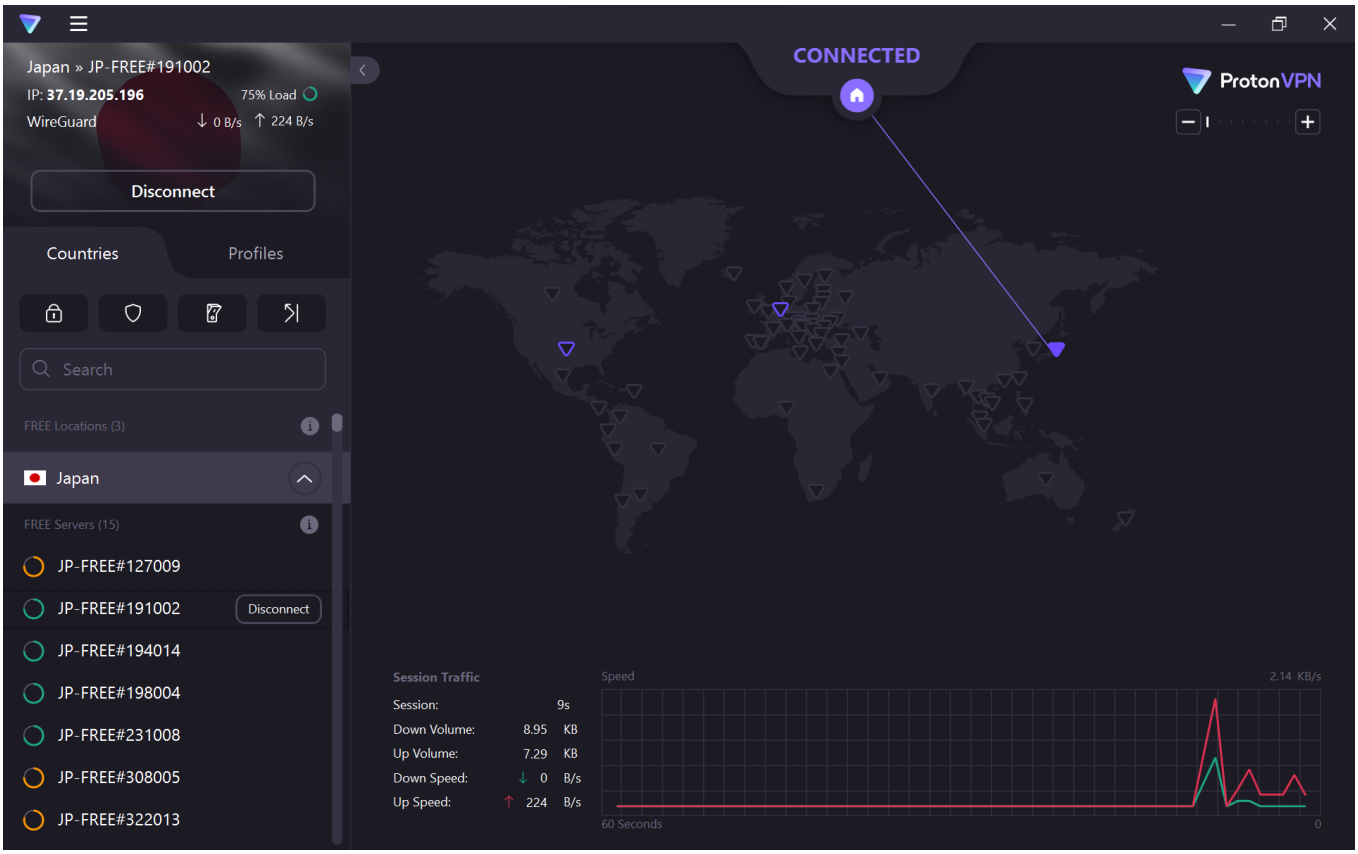


Can checking Privacy, Speed, and other ProtonVPN connection features via the “Quick Settings” option.

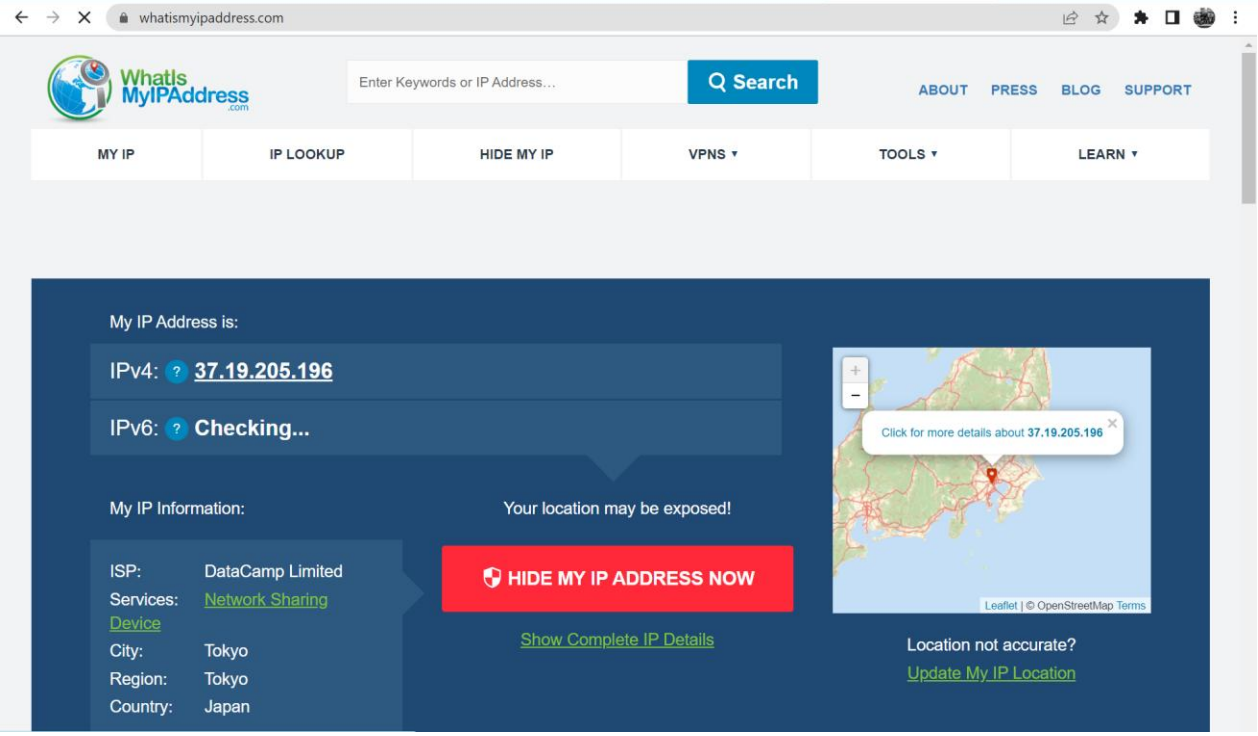


I am currently connected to a Netherlands ProtonVPN server.

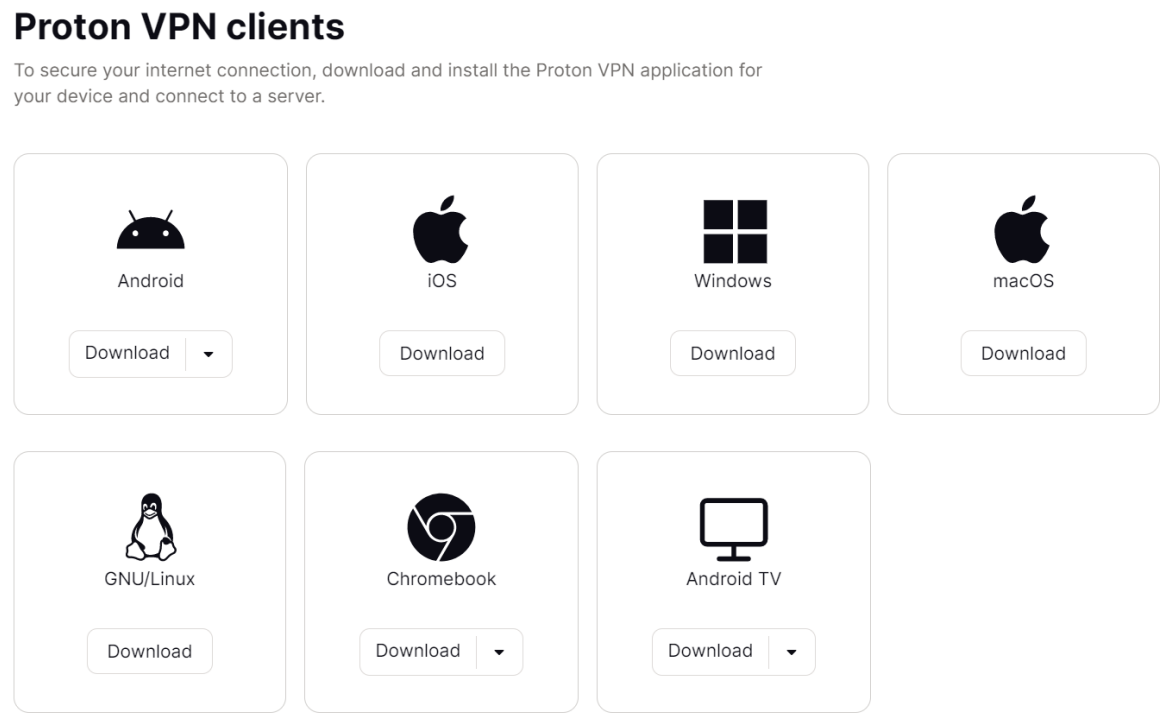
I can switch to a Japan ProtonVPN server as well to see the IP address change on the upper left of the screen.



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.

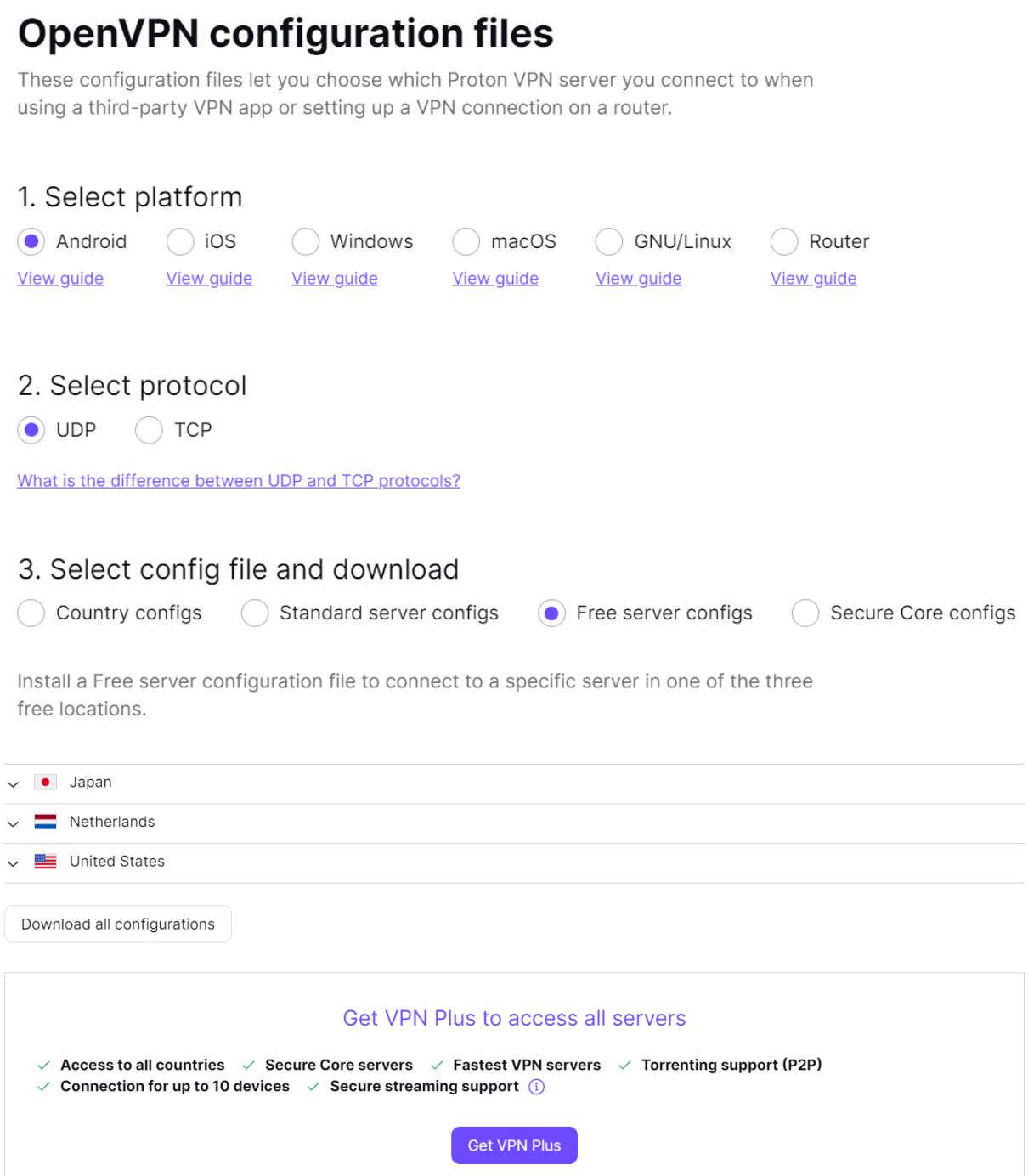


Now the IP address is masked with different IP address from Tokyo, Japan as shown on IP tracker website via https://whatismyipaddress.com/

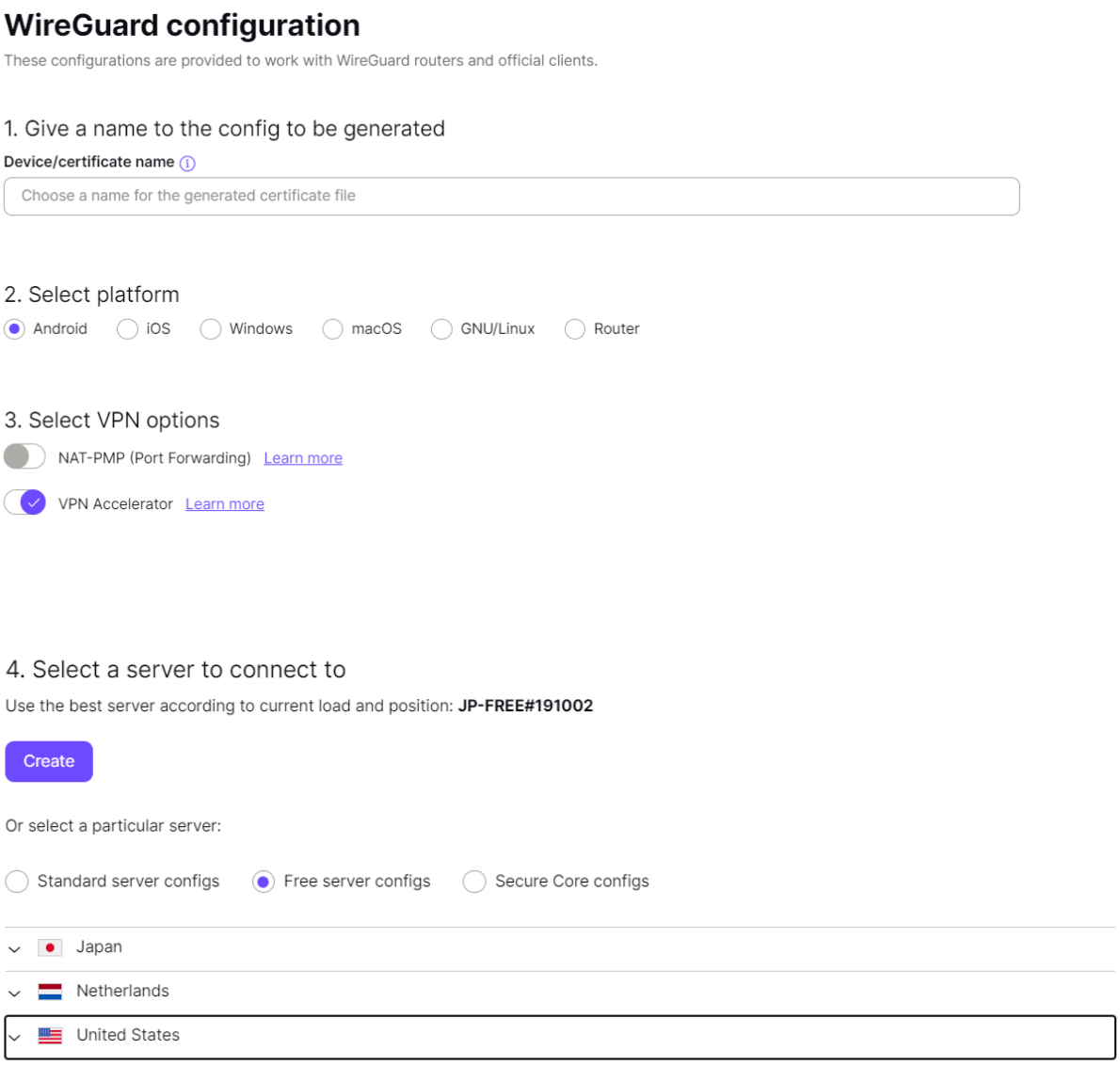


Proton VPN can be installed on the clients Android, iOS, Windows, macOS, GNU/Linux, Chromebook, and Android TV. (as shown above from their official website)

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



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 is a newer VPN protocol.

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