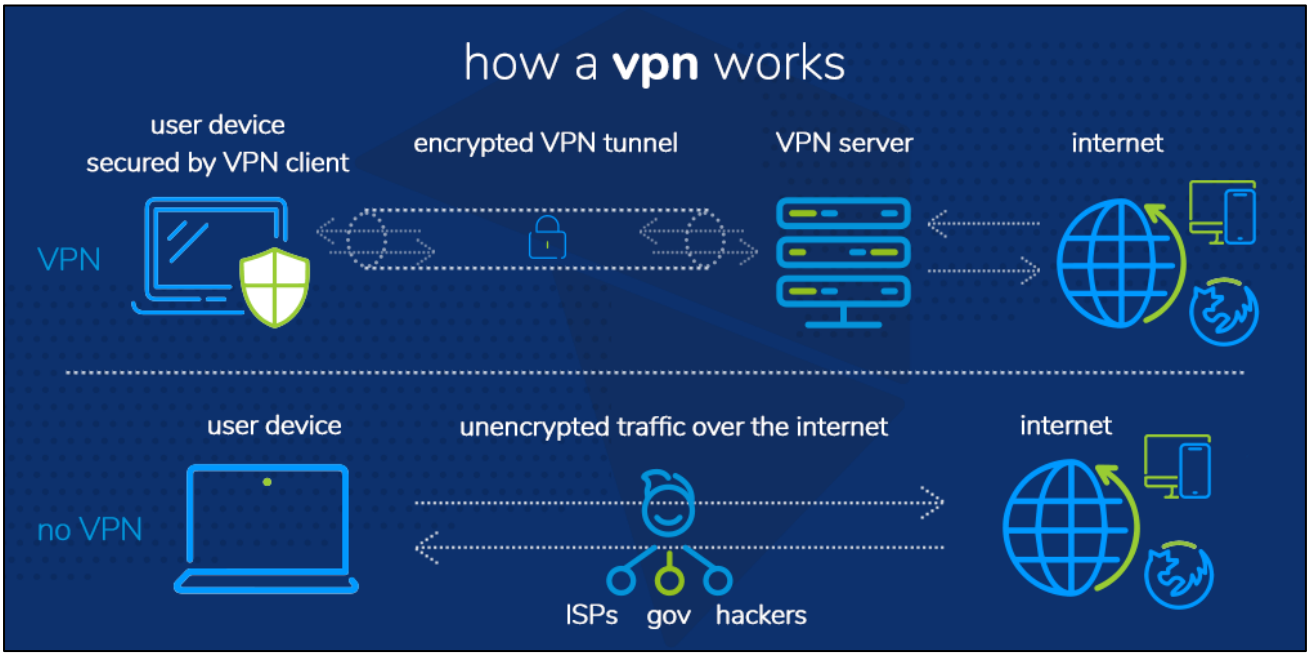
CREATE YOUR OWN VPN

What is a VPN?

A **VPN (Virtual Private Network)** is a service that encrypts your internet connection and routes it through a remote server, hiding your IP address and securing your online activity.

How It Works

1. **Encryption:** Your device encrypts internet traffic before sending it to the VPN server.
2. **Tunneling:** The encrypted data is transmitted through a secure tunnel to the VPN server.
3. **IP Masking:** The VPN server assigns you a new IP address, hiding your real location.
4. **Decryption & Forwarding:** The server decrypts the data and forwards it to the destination (website/service).
5. **Response Reversal:** The website's response goes back through the VPN, encrypting it again before reaching you.



Benefits

- **Privacy:** Hides your IP and location.
- **Security:** Protects data from hackers on public Wi-Fi.
- **Bypass Censorship & Geo-Restrictions:** Access content restricted in your region.
- **Anonymity:** Prevents ISP tracking.

Risk associated with using third party VPN-

Using a third-party VPN server has some risks, including:

1. Privacy Risks – Some VPN providers log user data, defeating the purpose of anonymity.
2. Trust Issues – You must trust the provider not to sell or leak your data.
3. Speed Reduction – VPN encryption and rerouting can cause latency and slow speeds.
4. Limited Security – If the provider has weak security, your data can be exposed.
5. Potential Data Leaks – Some VPNs suffer from DNS, WebRTC, or IP leaks, revealing your real identity.
6. Blocked Services – Some platforms (e.g., Netflix, banks) detect and block VPNs.
7. Legal & Compliance Issues – Using a VPN in some countries violates laws or terms of service.
8. Cost – Reliable VPNs require paid subscriptions, while free ones may sell user data.

How to create your own VPN

There are different trustworthy methods of creating your own VPN, each satisfying a specific need of user. Some of the commonly used are –

- For speed & simplicity: **WireGuard**
- For maximum security & flexibility: **OpenVPN**
- For cloud hosting: **Algo VPN**
- For a home setup: **PiVPN**

We will be using the Open Vpn for building our VPN in the following sections.

Open VPN

OpenVPN is an open-source VPN protocol and software that provides **secure, encrypted communication** over the internet. It uses **SSL/TLS** for encryption and supports multiple authentication methods, such as passwords, certificates, and two-factor authentication.

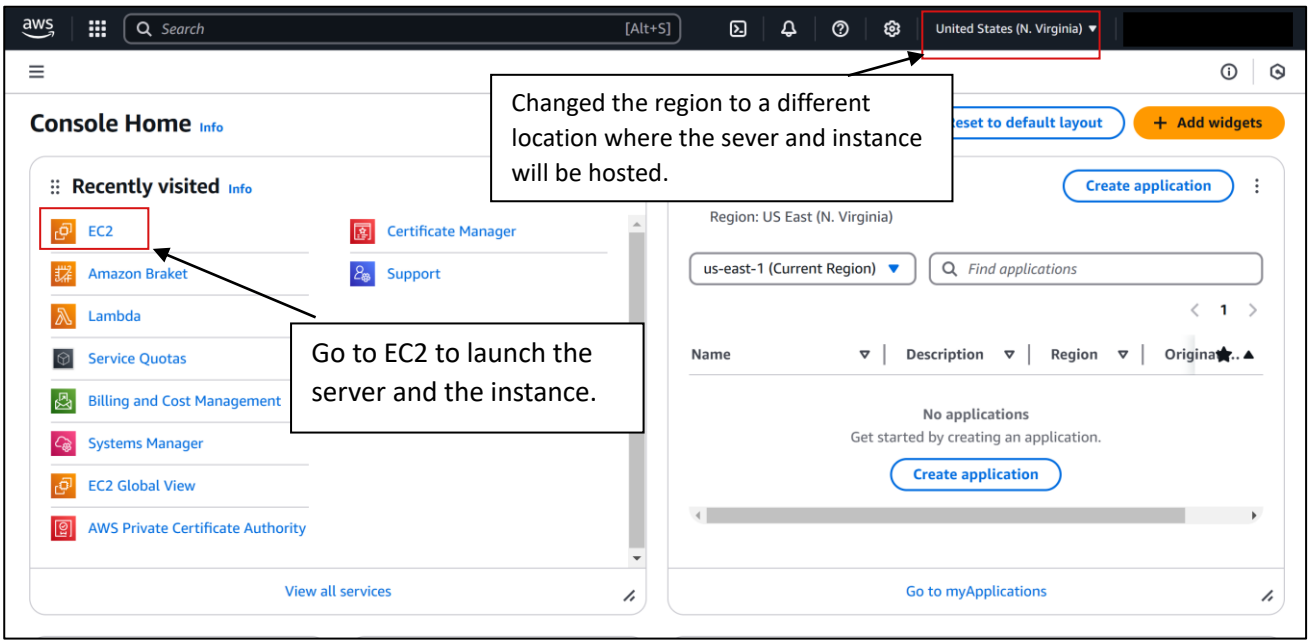
Key Features:

- **Strong Encryption:** Uses **AES-256**, RSA, and TLS for security.
- **Cross-Platform:** Works on Windows, Linux, macOS, Android, and iOS.
- **Tunneling Protocols:** Supports **TCP and UDP** for flexibility.
- **Firewall Bypass:** Can run on **port 443** (HTTPS) to avoid detection.
- **Highly Configurable:** Supports split tunneling, site-to-site VPNs, and more.

Process

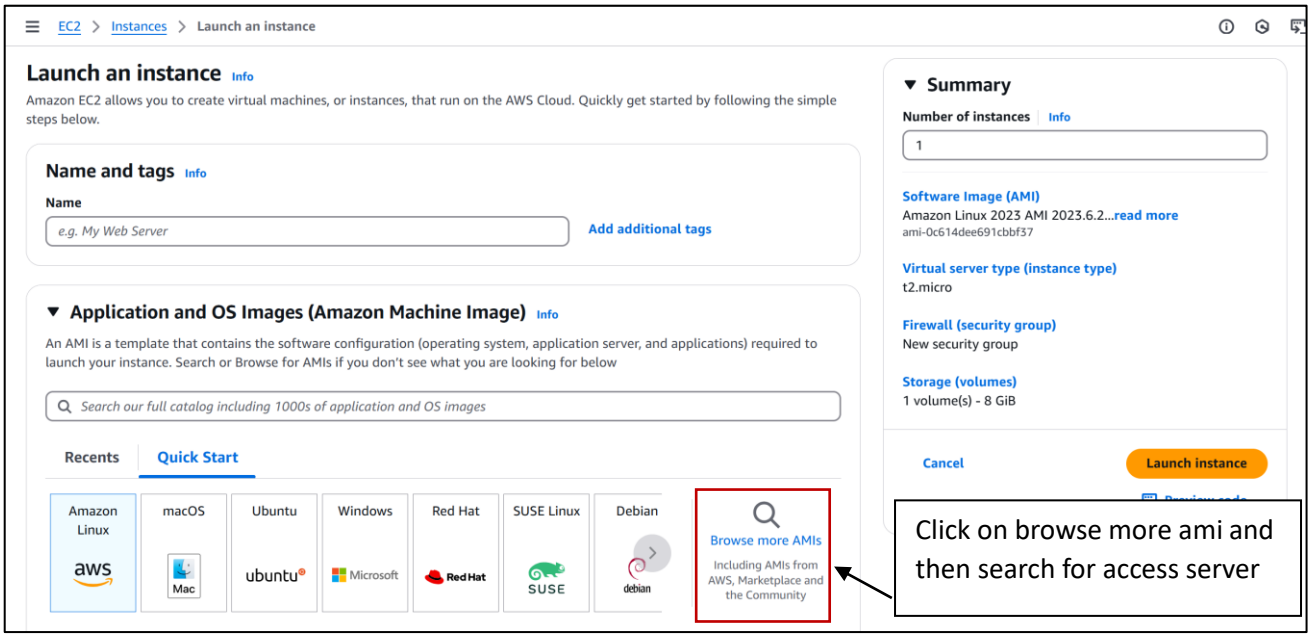
- We will be using the Open VPN access server, for this open your aws account or create a free tier account and go to the launch instances section.

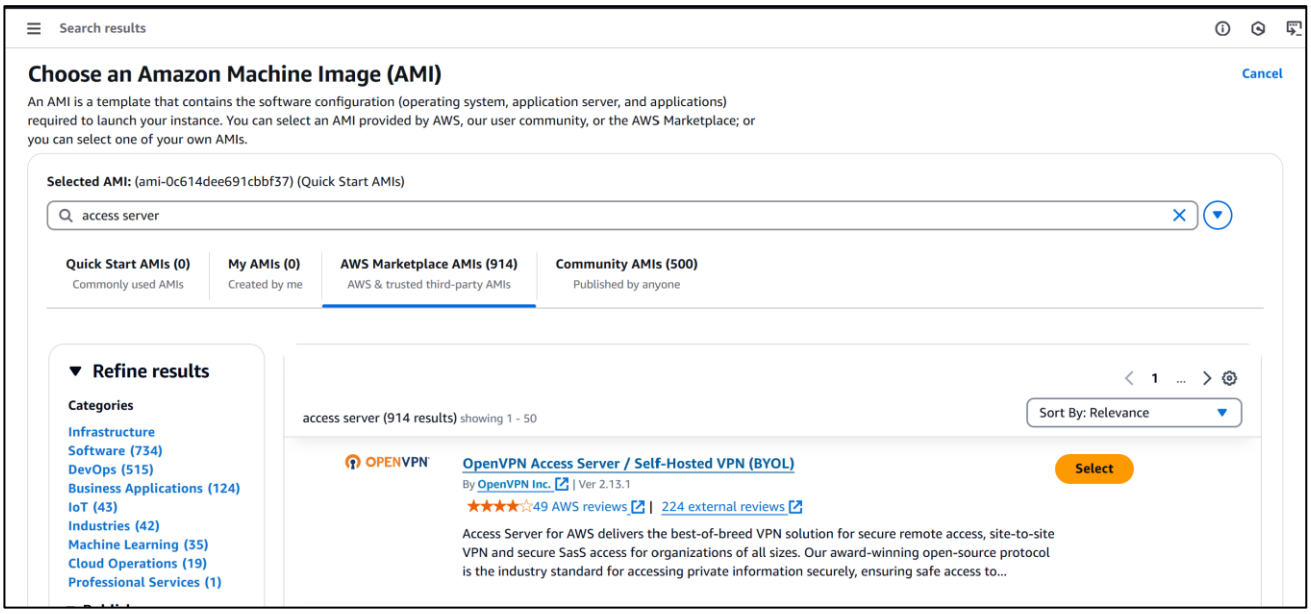
- Before launching any instance you must select a region different from your physical region on the aws webpage in the manage region section. **If the region is not selected properly the vpn server will not work.**



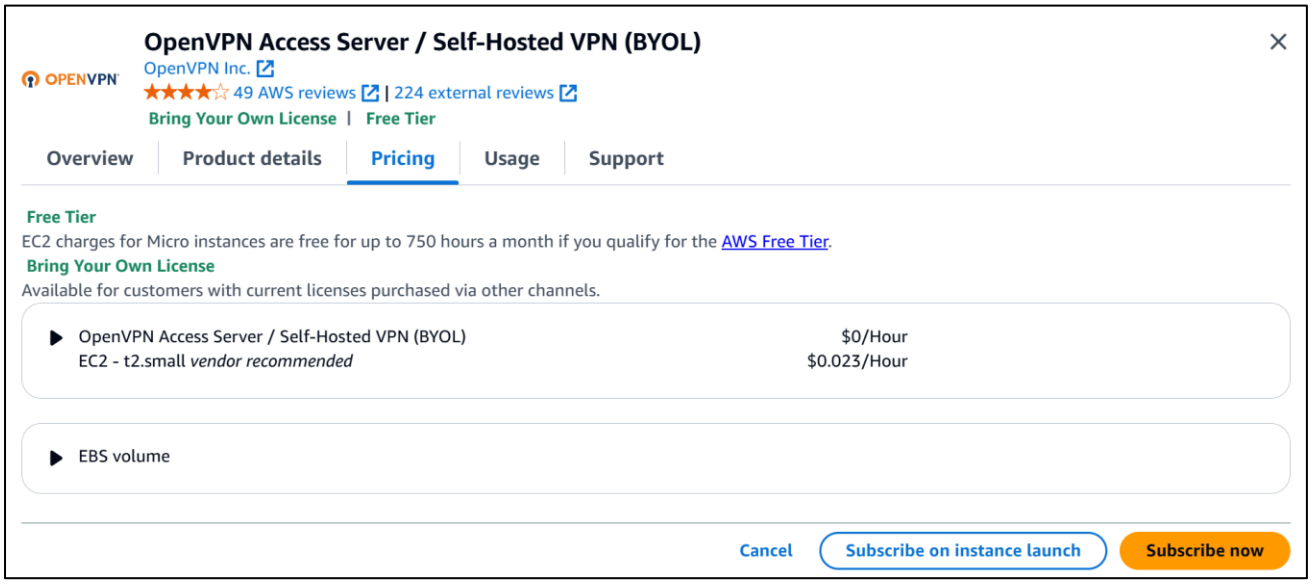
- There you shall search for Open VPN access server in the AMI section and choose the server as per your need.

- Also select the instance type you want in addition to the server.

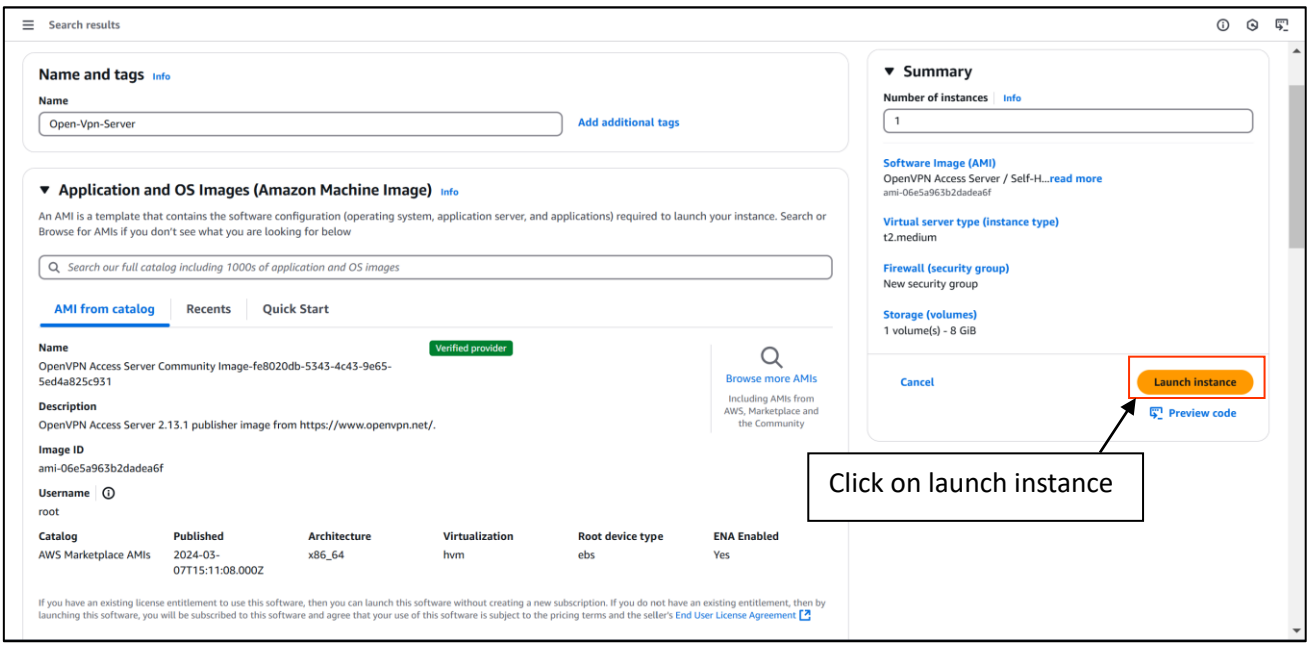




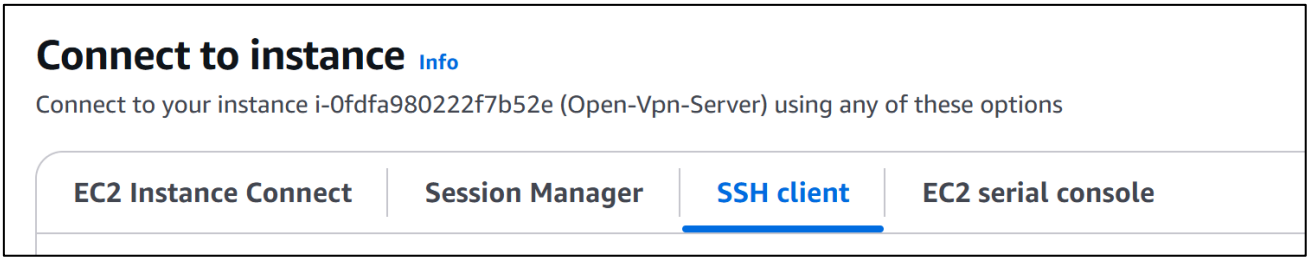
- For testing purpose, you can always select the free server and instance type offered by AWS.



- Click on subscribe now and then configure any necessary changes like adding the name to the instance. Do add the key pair to ensure security.



- Now after launching the instance connect to your instance using your preferred method. Here we will be using the ssh client for connecting to our instance. Remember while using the ssh client use the username as **openvpnas**.



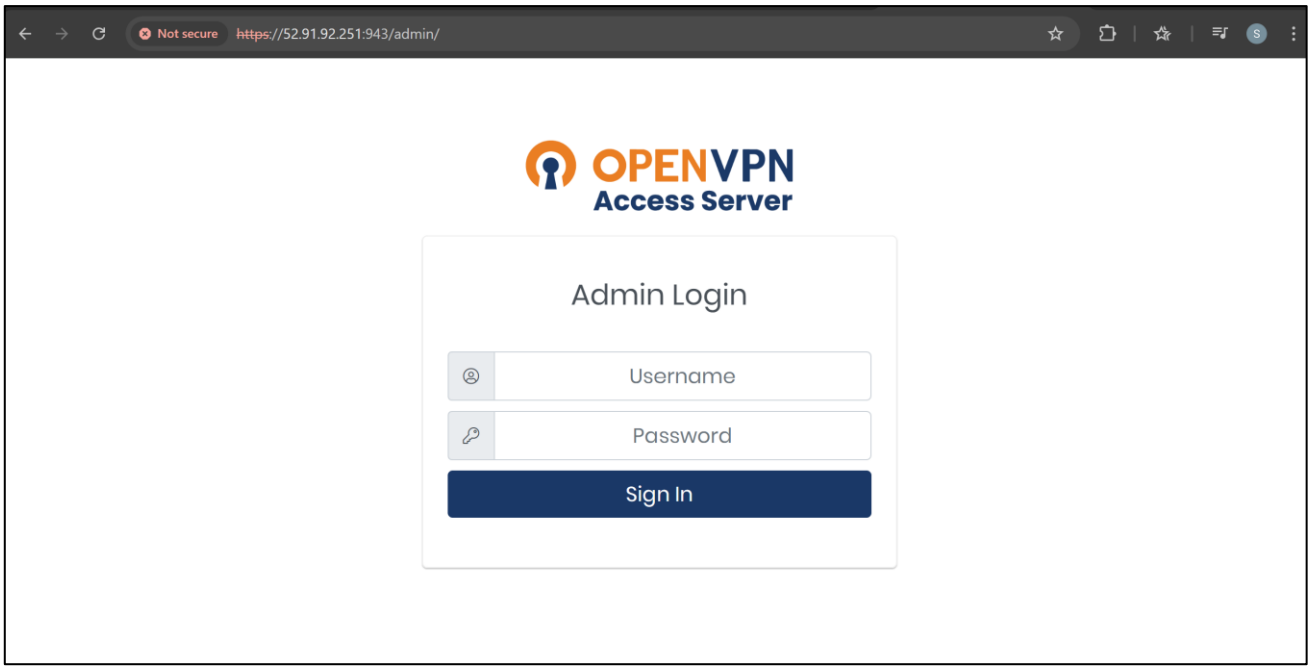
- Now after connecting to your instance apply the settings as per your need but better performance keep some settings as mentioned below.

```
rsa       - maximum compatibility
secp384r1 - elliptic curve, higher security than rsa, allows faster connection setup and smaller user profile files
showall   - shows all options including non-recommended algorithms.
> Press ENTER for default [secp384r1]:

Please specify the port number for the Admin Web UI.
> Press ENTER for default [943]:

Please specify the TCP port number for the OpenVPN Daemon
> Press ENTER for default [443]:

Should client traffic be routed by default through the VPN?
> Press ENTER for default [no]: yes

Should client DNS traffic be routed by default through the VPN?
> Press ENTER for default [no]: yes
Admin user authentication will be  local

Private subnets detected: ['172.31.0.0/16']

Should private subnets be accessible to clients by default?
> Press ENTER for EC2 default [yes]: yes
```

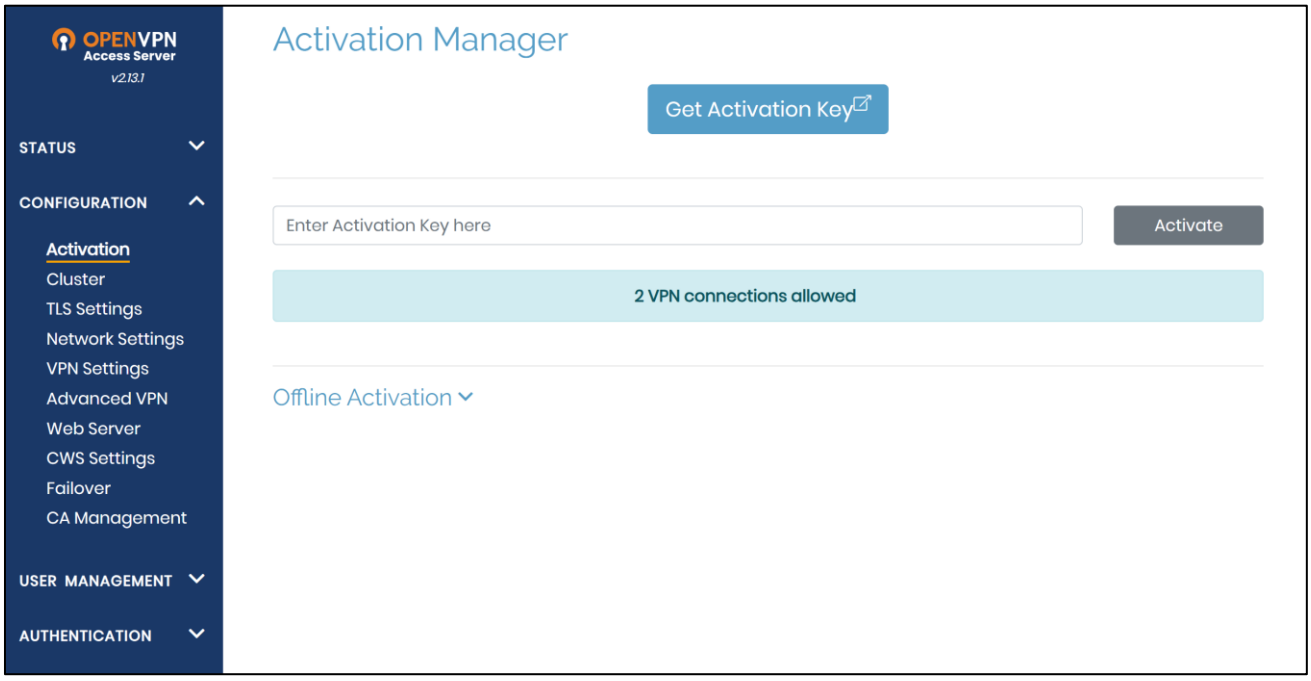
- After configuring the settings, give password for your server then you will be connected to your server and you will have details regarding the admin and the client.

```
During normal operation, OpenVPN AS can be accessed via these URLs:
Admin  UI: https://52.91.92.251:943/admin
Client UI: https://52.91.92.251:943/
To login please use the "openvpn" account with  the password you specified during the setup.

See the Release Notes for this release at:
   https://openvpn.net/vpn-server-resources/release-notes/
```

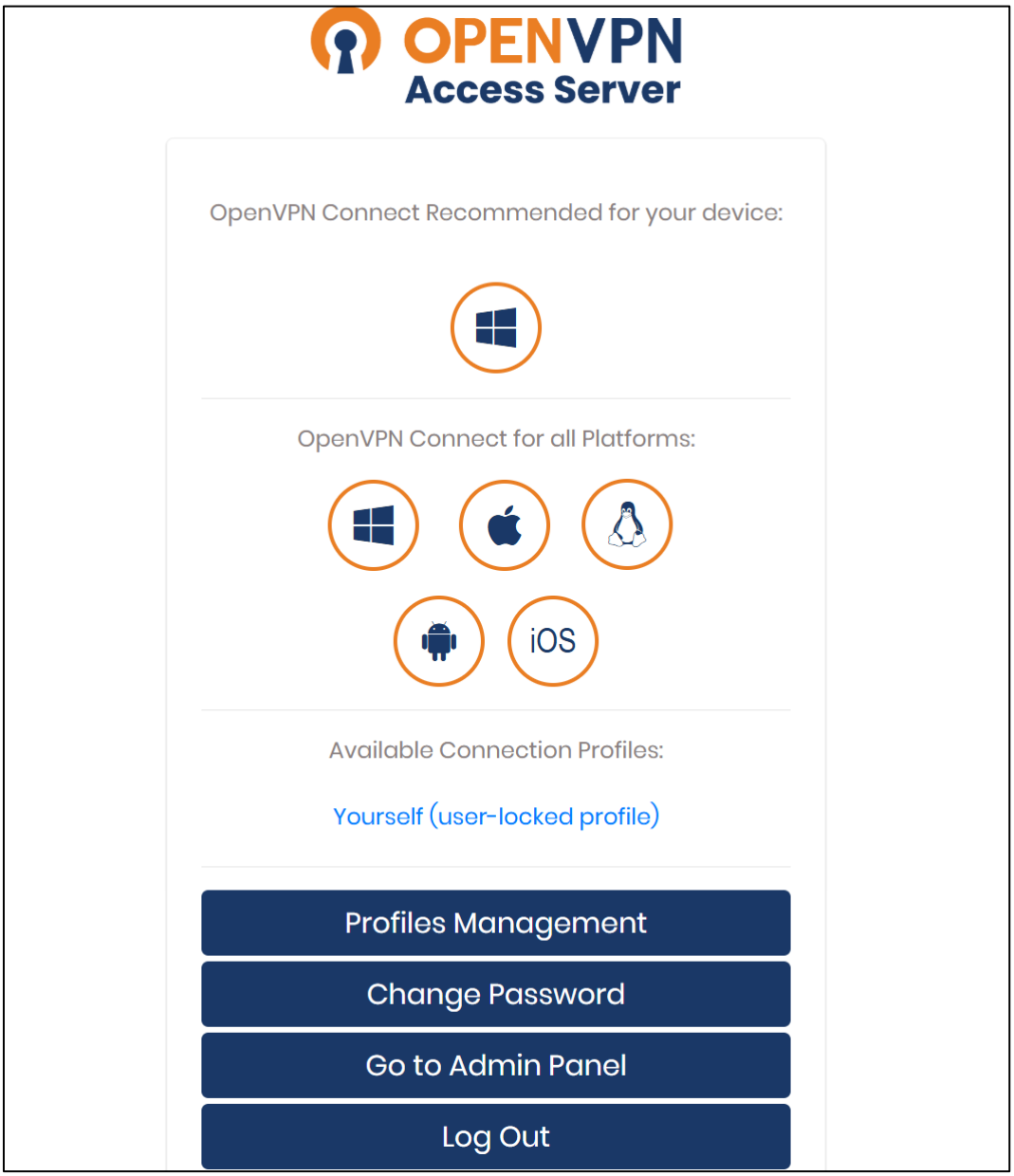
- Now click on the admin UI url to get logged into the admin server.



- Now use your username and password to log into the server.

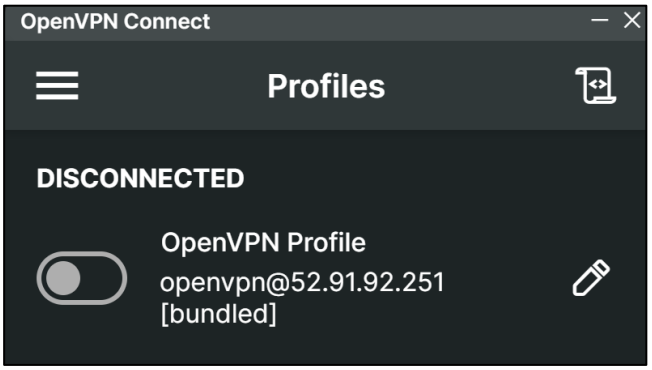


- Now log into your client url in the device you want to use the vpn to get the client connection file and download as per your Operating System.



- Now run the file you have downloaded, after the file get installed you will get a interface where you can connect to your vpn.

- To connect to the vpn now again you have to give the same password given during the client and admin login.



- After connecting you can see your vpn working and also data related to vpn being shown.