How to connect to SFL's VPN

The following article describes the VPN client setup on various platforms.

We are using the OpenVPN server to allow remote users to connect SFL's infrastructure out of the office perimeter.

To be able to connect to the office, the user needs to have installed on the PC VPN client application. VPN client application uses a certificate signed by the SFL's certificate authority system and user's credentials to establish a connection to the office.

All necessary components (client application, certificate) you can download from here ONLY connected to the office's WiFi. Please make sure that selected VPN server is itremote. If the user already outside of the office's perimeter, he/she must contact with ops/DevOps team.

As a VPN client application credentials, we are using SFL's Active Directory username and password, which is the same credentials as for your PC login or SFL_Employees WiFi SSID connection credentials, or https://jira.sflpro.com/'s credentials.

Additional information:

As a MAC(OsX) user, you can use Tunnelblick as an OpenVPN client.

As a Windows user, you can use pure OpenVPN client.

As a Linux user you can install the OpenVPN client application via apt or snap

APT

```
apt install openvpn network-manager-openvpn
network-manager-openvpn-gnome
```

After the installation, you need to import the *.ovpn configuration file, which you can download from here or a request from the ops/DevOps team.