

Procedure to setup IIT Delhi VPN in various Operating Systems:

1. Windows Configuration
2. Linux Configuration
3. Mac OS Configuration
4. Android Configuration
5. Apple IO

- For getting VPN credentials, there are two methods:
 1. Faculty can create VPN credentials for themselves and their advisee using the following link.
<https://ldapweb.iitd.ac.in/usermanage/newvpn.php>
(Site can be accessed from the IITD campus only).
 2. Users can also drop an email at sysadm@cc.iitd.ac.in to get VPN credentials.
- In both cases, the user will get an email with instructions for setup and use.
- Download the yourID.ovpn file and client based on your operating system.

Recommended Versions of VPN Applications:-

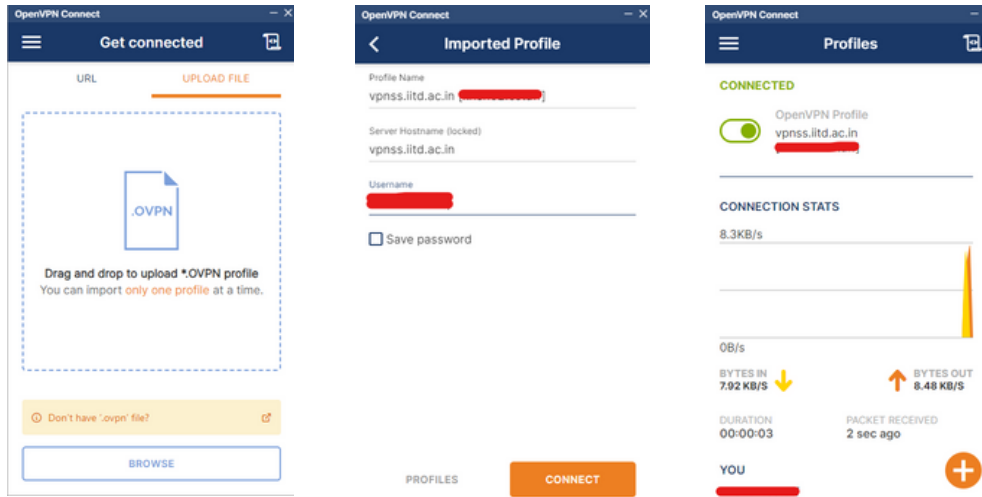
- a. **Windows:** OpenVPN Connect (3.6.x ver & above) / OpenVPN Application (2.6.x ver & above)
- b. **Linux:** OpenVPN client. (2.6.x version and above)
- c. **Mac OS:** Use TunnelBlick (4.0.1 version and above)
- d. **Android OS:** OpenVPN
- e. **Apple IOS:** OpenVPN

Download the client software of your choice from the link provided in the email or from the developer's site.



Windows Configuration: (Option 1 with OpenVPN Connect Client)

- After installation of windows client software (shared on mail), download the file yourID.ovpn from the following site <https://newcert.iitd.ac.in/usermanage/vpn3cert.html> into any folder and name it as VPN or any name to find it later.
- Install the OpenVPN Connect client software, Import Profile > Upload File > Browse and select the yourID.ovpn file to import.
- Click the button on left of profile to connect. Enter Your id, and select “Connect” to enter password.



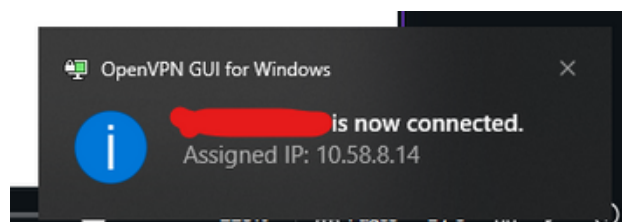
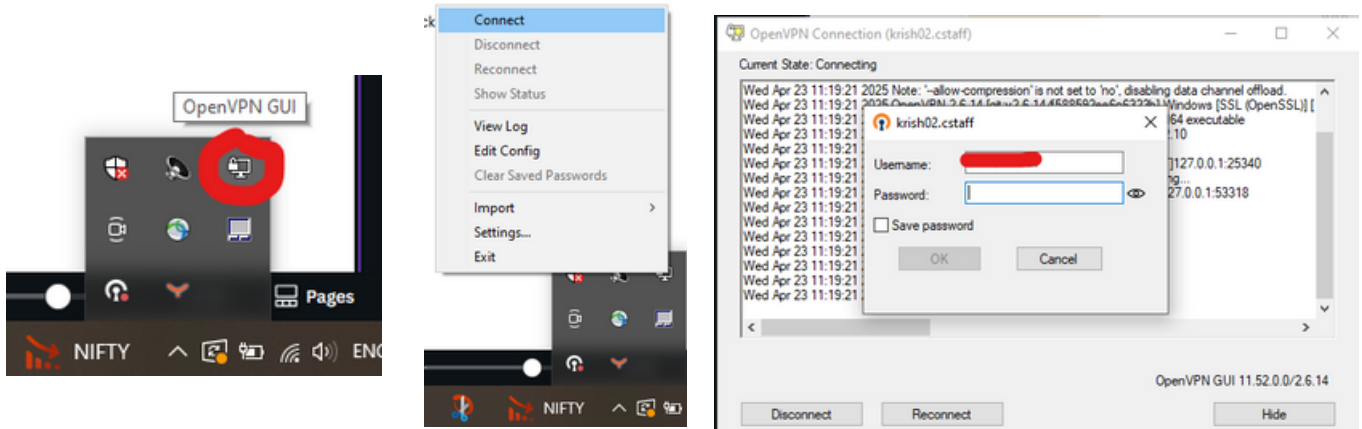
Test your connection by visiting internal IITD sites like:

<https://internal.iitd.ac.in>



Windows Configuration: (Option 2 with OpenVPN application)

- After installation of windows client software, download the file yourID.ovpn from the following site <https://newcert.iitd.ac.in/usermanage/vpn3cert.html> into "c:\ProgramFiles\OpenVPN\config" folder.
- Right-click on OpenVPN GUI and run as administrator; right-click on ovpn client and click connect. Enter your credentials (user id, password), and you are done.



Test your connection by visiting internal IITD sites like:

<https://internal.iitd.ac.in>

Linux Configuration:

Download yourID.ovpn from the following site

<https://newcert.iitd.ac.in/usermanage/vpn3cert.html>

- Put this file inside a folder
- On the same folder, right-click and open terminal

Run the following command:

```
$ sudo apt install openvpn
```

```
$ sudo wget https://csc.iitd.ac.in/uploads/update-systemd-resolved -P /etc/openvpn
```

```
$ sudo chmod 777 /etc/openvpn/update-systemd-resolved
```

```
$ sudo nano yourID.ovpn
```

Add the following two lines at the end:-

```
up /etc/openvpn/update-systemd-resolved
```

```
down /etc/openvpn/update-systemd-resolved
```

```
$ sudo openvpn --script-security 2 --config yourID.ovpn
```

Use your credentials to log in.

```
expedition@expedition-virtual-machine:~/Downloads/VPN$ sudo wget https://csc.iitd.ac.in/uploads/update-systemd-resolved -P /etc/openvpn
--no-check-certificate
--2025-04-23 03:20:42-- https://csc.iitd.ac.in/uploads/update-systemd-resolved
Resolving csc.iitd.ac.in (csc.iitd.ac.in)... 103.27.8.173, 2001:df4:e000:29::211
Connecting to csc.iitd.ac.in (csc.iitd.ac.in)|103.27.8.173|:443... connected.
WARNING: cannot verify csc.iitd.ac.in's certificate, issued by 'CN=GlobalSign RSA OV SSL CA 2018,O=GlobalSign nv-sa,C=BE':
Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: 11978 (12K)
Saving to: '/etc/openvpn/update-systemd-resolved.1'

update-systemd-resolved.1 100%[=====] 11.70K --.-KB/s
in 0.007s

2025-04-23 03:20:43 (1.53 MB/s) - '/etc/openvpn/update-systemd-resolved.1' saved [11978/11978]

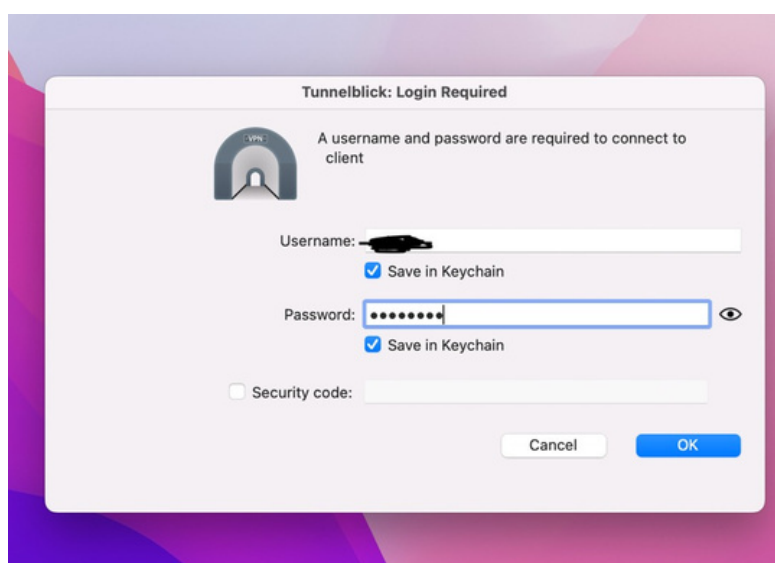
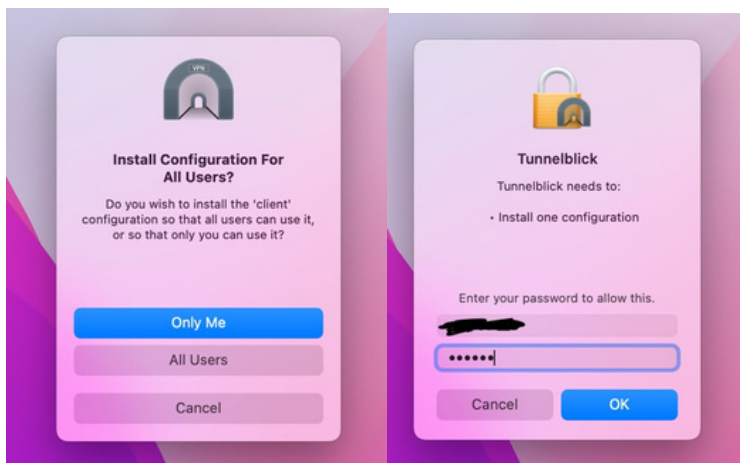
expedition@expedition-virtual-machine:~/Downloads/VPN$
expedition@expedition-virtual-machine:~/Downloads/VPN$
expedition@expedition-virtual-machine:~/Downloads/VPN$ sudo openvpn --script-security 2 --config yourID.ovpn
Wed Apr 23 03:21:24 2025 OpenVPN 2.4.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jun
27 2024
Wed Apr 23 03:21:24 2025 library versions: OpenSSL 1.1.1f 31 Mar 2020, LZO 2.10
Enter Auth Username:
Enter Auth Password: *****
Wed Apr 23 03:21:35 2025 WARNING: --ns-cert-type is DEPRECATED. Use --remote-cert-tls instead.
Wed Apr 23 03:21:35 2025 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
Wed Apr 23 03:21:35 2025 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Wed Apr 23 03:21:35 2025 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Wed Apr 23 03:21:35 2025 TCP/UDP: Preserving recently used remote address: [AF_INET]103.27.9.160:1194
Wed Apr 23 03:21:35 2025 Socket Buffers: R=[212992->212992] S=[212992->212992]
Wed Apr 23 03:21:35 2025 UDP link local: (not bound)
Wed Apr 23 03:21:35 2025 UDP link remote: [AF_INET]103.27.9.160:1194
Wed Apr 23 03:21:35 2025 TLS: Initial packet from [AF_INET]103.27.9.160:1194, sid=bc2c625 29f53747
Wed Apr 23 03:21:35 2025 VERIFY OK: depth=2, C=IN, ST=Delhi, L=New Delhi, O=Indian Institute of Technology, Delhi, OU=Computer Services C
enter, IITD, CN=csc.iitd.ac.in, emailAddress=sysadm@csc.iitd.ac.in
Wed Apr 23 03:21:35 2025 VERIFY OK: depth=1, C=IN, ST=Delhi, O=Indian Institute of Technology, Delhi, OU=Computer Services Center, IITD,
CN=csc.iitd.ac.in, emailAddress=sysadm@csc.iitd.ac.in
Wed Apr 23 03:21:35 2025 VERIFY OK: nsCertType=SERVER
Wed Apr 23 03:21:35 2025 Validating certificate extended key usage
Wed Apr 23 03:21:35 2025 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication

<1>Apr 23 03:21:37 update-systemd-resolved: Mounting DNS domain iitd.ac.in
<1>Apr 23 03:21:37 update-systemd-resolved: Adding DNS Domain iitd.ernet.in
<1>Apr 23 03:21:37 update-systemd-resolved: SetLinkDNS(3 2 2 4 10 10 1 4 2 4 10 10 1 5)
<1>Apr 23 03:21:37 update-systemd-resolved: SetLinkDomains(3 2 iitd.ac.in false iitd.ernet.in false)
Wed Apr 23 03:21:40 2025 /sbin/route add 10.0.0.0/11 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.10.1.2/32 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.10.2.2/32 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.87.2.2/32 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.176.0.0/12 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.192.0.0/10 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.113.0.0/16 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.123.0.0/16 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.143.0.0/16 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.144.0.0/13 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.170.0.0/16 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.171.0.0/16 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 172.19.0.0/16 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 172.20.0.0/16 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.172.4.0/24 via 10.58.8.13
Wed Apr 23 03:21:40 2025 /sbin/route add 10.20.0.0/16 via 172.161.161.2
Wed Apr 23 03:21:40 2025 /sbin/route add 10.38.0.0/16 via 172.161.161.2
Wed Apr 23 03:21:40 2025 /sbin/route add 10.40.0.0/16 via 172.161.161.2
Wed Apr 23 03:21:40 2025 /sbin/route add 10.147.0.0/16 via 172.161.161.2
Wed Apr 23 03:21:40 2025 /sbin/route add 10.148.0.0/16 via 172.161.161.2
Wed Apr 23 03:21:40 2025 /sbin/route add 10.149.0.0/16 via 172.161.161.2
Wed Apr 23 03:21:40 2025 /sbin/route add 10.58.8.1/32 via 10.58.8.13
Wed Apr 23 03:21:40 2025 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Wed Apr 23 03:21:40 2025 Initialization Sequence Completed
```

When you see the above output, then the vpn is connected, leave the tab open and do your work on other tab

MAC OS configuration:

- Download the latest stable version of the TunnelBlick client from the developer site.
- Post installation, create a folder, and name it VPN or any other.
- Download the file yourID.ovpn from the following site
<https://newcert.iitd.ac.in/usermanage/vpn3cert.html>
- Put this file inside a folder. Go to the folder and invoke the yourID.ovpn with TunnelBlick.
- It will ask for your Mac credentials to install the software.
- After installation from the TunnelBlick icon, select connect client. It will ask for your Kerberos credentials for the first time (save them). You are now connected.
- Visit any internal site to verify the same.



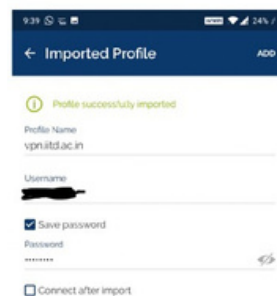
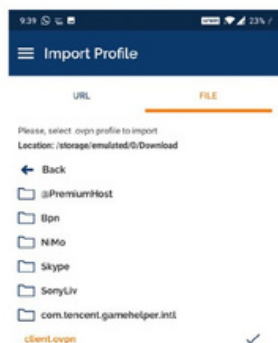
Android Configuration:

- Install the OpenVPN app from Play Store.
- Download yourID.ovpn, from the following site

<https://newcert.iitd.ac.in/usermanage/vpn3cert.html>

- Put this file inside a folder.
- Go to OpenVPN > Import Profile > File > Select yourID.ovpn.
- In the case of faculty, the profile name will be vpnfac.iitd.ac.in.

Use your Kerberos credentials to log in.



Apple IOS Configuration:

- Install the OpenVPN app from App Store on your IOS device. Now you need to
- use a separate system, preferably Mac OS-based system, to download certificate files in this system.
- Download the file yourID.ovpn from the following site
<https://newcert.iitd.ac.in/usermanage/vpn3cert.html>
- Put this file inside a folder.
- Now connect your Apple IOS device through a USB cable to this system.
- On the IOS device, trust the accessing device.
- Go to the finder and browse the IOS Device.
- Go to files, and you will see OpenVPN App.
- Drag all five files from your Mac OS system and put them in OpenVPN Folder.
- Go to OpenVPN > Import Profile > File > Select yourID.ovpn (IOS Device)
- Use your Kerberos credentials to log in.

