I have trouble connecting or the connection drops frequently: Changing Ports

Travis - 2021-05-14 - Change Ports

If you experience issues connecting or staying connected to any of our servers, you might want to try using a different port to connect to or a different protocol altogether.

Reason for connection Drops

There are multiple reasons why this could be happening:

- You are using UDP (default) behind one or multiple NAT routers that doesn't support hole punching;
- You are connecting from a public network (such as a school, library, mall, coffee shop, hotel, etc) or a corporate network that filters or restrict Internet usage (typically to prevent abuse and piracy);
- Your Internet Service Provider (ISP) filters some traffic for filtering, quality of service or restrictive measures;
  Your ISP is actively blocking or trying to restrict usage of VPN services due to national bans;
- A firewall device on your network is blocking the connection;
- You are using a mobile network with frequently changing IP addresses or service restrictions;
- Your connection is not reliable enough to maintain the connection active for extended periods of time (such as unstable/crowded WiFi access).

In these situations, using a different port or protocol to masquerade as another kind of application typically resolve the issue. For instructions on how to change the ports on our application please review the following guides:

- Windows - Change Ports
- MacOS - Change Ports
- Linux (systemd) - Change Ports
- iOS - Change Ports
- Android- Change Ports

Protocols and Ports

Try the following combinations of protocols and ports using the above steps until you find one that provides you with satisfactory connectivity:

Connection type	Remote port	Local port	Explanation
UDP	1194, 1197, 1198	*(empty)*	This is the default ports used by OpenVPN
UDP	8080	*(empty)*	Uses the often open port 8080 (http alternate) using UDP
UDP	9201	*(empty)*	(no particular signification)
UDP	53	*(empty)*	Mimics traffic to DNS servers
UDP	53	53	Mimics traffic to DNS servers coming back
TCP	80	*(empty)*	Mimics traffic to standard, unencrypted web (http) servers
TCP	110	*(empty)*	Mimics traffic to Email servers (pop3)
TCP	443	*(empty)*	Mimics traffic to secure web servers (https). Typically the most compatible option due to the technical challenge involved into filtering this port without causing every website to display an error

Related solutions:

- I can connect to the VPN, but my speeds are really slow using Windows

Tags

connection

Ports

Related Content

- I can connect to the VPN, but my speeds are really slow using Windows
- What ports are used by your VPN service?