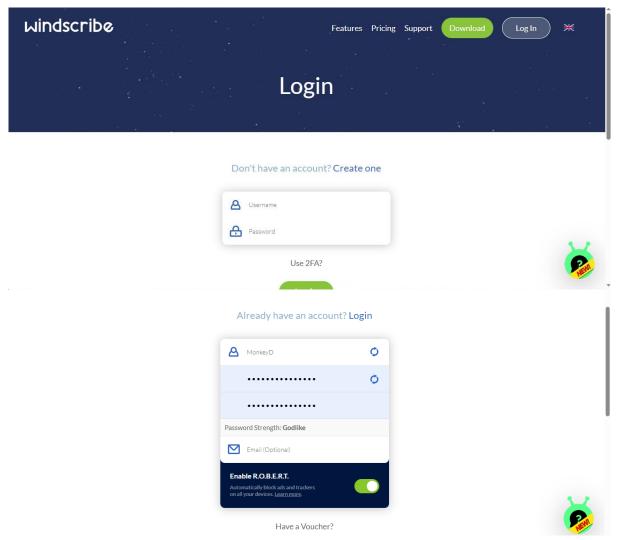
Task 8: Working with VPNs.

Note:

- Only install VPN software from the official provider site.
- Use throwaway credentials or a dedicated test account
- If you need to check potentially sensitive traffic, use an isolated VM.

1. Pick a provider and sign up

Windscribe (Free) — feature rich, free tier with limited monthly data (can increase by verifying email), native apps and CLI available. Good for flexibility.



- https://windscribe.com/login

2. Install client — Kali Linux

add windscribe repo (check Windscribe docs for current repo steps)

\$echo 'deb https://repo.windscribe.com/ubuntu/ bionic main' | sudo tee
 /etc/apt/sources.list.d/windscribe-repo.list

update and install

- \$sudo apt update
- \$sudo apt install -y windscribe-cli

usage

- \$windscribe login
- \$windscribe connect # connect to best/last or `windscribe connect US`
 etc.
- \$windscribe status
- \$windscribe disconnect

3. Connect, verify IP change & check encryption

show just the IP

\$curl -s ipinfo.io/ip

or get full info

- \$curl -s ipinfo.io

These endpoints return your public IP (and details). Compare before/after connecting to confirm the IP changed.

Browser check

Open browser → visit https://whatismyipaddress.com or https://ipinfo.io.
 Confirm the displayed IP & country match the VPN endpoint.

Check HTTPS encryption

\$curl -I https://example.com

4. Disconnect & compare

- \$windscribe disconnect

Verify your IP reverted by rerunning curl ipinfo.io/ip.

5. Extra checks (privacy / leaks)

- **DNS leak test:** visit https://www.dnsleaktest.com or https://ipleak.net from your browser while connected. If DNS servers shown belong to the VPN provider, DNS is protected; if your ISP DNS shows, you have a DNS leak.
- WebRTC leak (browsers): use browser test sites (e.g., browserleaks.com/webrtc). If WebRTC shows your real IP, consider disabling WebRTC or using browser extension/privacy settings.

(These are interactive web checks — perform in an isolated/test environment.)