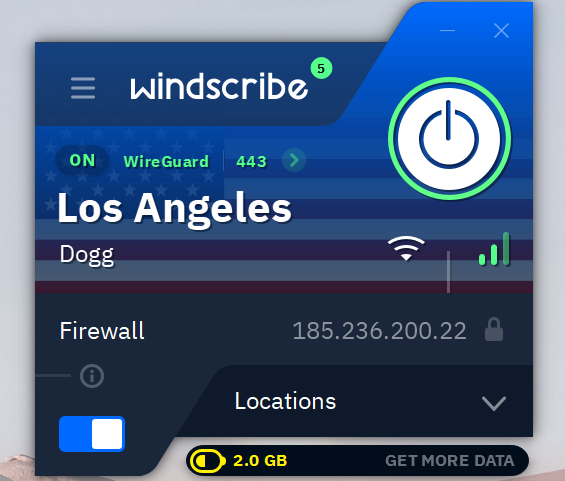
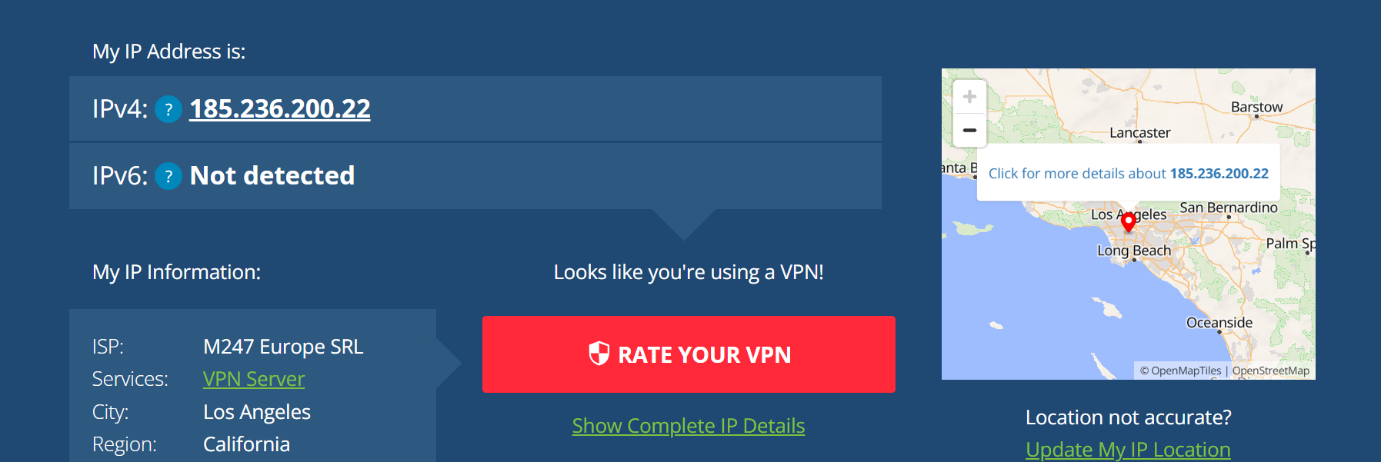
1. **VPN connection**



1. **Verifying the connection**



1. **VPN encryption and privacy features**

**1. Strong Encryption**

Windscribe uses:

* **AES-256 bit encryption** — the same standard used by banks and governments.
* Paired with **SHA-512** for authentication and **4096-bit RSA keys** for handshakes.

This ensures your data cannot be easily intercepted or decrypted.

**2. Tunneling Protocols**

Windscribe supports multiple secure protocols:

* **WireGuard** – Fast and secure, modern standard
* **OpenVPN (UDP/TCP)** – Highly secure and widely used
* **IKEv2/IPSec** – Default for mobile devices, stable and fast

These protocols establish a secure tunnel between your device and the VPN server.

**3. IP and DNS Leak Protection**

* Windscribe hides your **real IP address** by replacing it with a VPN server’s IP.
* It prevents **DNS leaks**, meaning your ISP can’t see what websites you're visiting.

This protects your privacy from being monitored by your ISP or public Wi-Fi providers.

**4. No-Logs Policy**

* Windscribe states it **does not log your browsing activity**, connection timestamps, or IP addresses.
* Only minimal information (like bandwidth usage) is stored temporarily to enforce free plan limits.

-> Note: Free VPNs that *do* log your data can compromise your privacy — Windscribe is among the few that respect privacy.

**5. Ad and Tracker Blocking (R.O.B.E.R.T)**

* Windscribe offers a unique tool called **R.O.B.E.R.T**, which:
  + Blocks ads and trackers
  + Stops known malware domains
  + Can be customized for specific blocking (like gambling or adult sites)

This helps improve privacy and browsing speed.

**6. Kill Switch / Firewall**

* Windscribe has a **built-in firewall** (kill switch).
* If the VPN disconnects suddenly, it blocks all internet traffic to prevent data leaks.

**7. Multi-Hop (Double VPN)**

* You can route your traffic through **two VPN servers** instead of one.
* This adds another layer of anonymity and security.

1. **VPN benefits and limitations**

**Benefits of Using a VPN**

1. **Encrypts Your Internet Traffic**
   * Prevents hackers, ISPs, and governments from viewing your activity.
   * Especially useful on public Wi-Fi networks.
2. **Hides Your IP Address**
   * Replaces your real IP with the VPN server's IP, masking your location and identity.
3. **Bypasses Geo-Restrictions**
   * Allows access to websites, apps, or streaming content blocked in your region.
4. **Protects Privacy**
   * Prevents ISPs from tracking and selling your browsing habits.
5. **Avoids Bandwidth Throttling**
   * Stops ISPs from slowing down your connection based on your online activity.
6. **Blocks Trackers and Ads** *(with VPNs like Windscribe)*
   * Features like Windscribe's R.O.B.E.R.T block malware, ads, and trackers automatically.

**Limitations of a VPN**

1. **Slower Internet Speeds**
   * Encryption and rerouting traffic can reduce speed slightly, especially on distant servers.
2. **Does Not Protect Against Malware**
   * A VPN encrypts your connection but does not block viruses or phishing attacks. You still need antivirus software.
3. **Free VPNs May Be Limited**
   * Some free VPNs have bandwidth limits, fewer servers, or weaker privacy policies.
4. **Doesn’t Make You 100% Anonymous**
   * If you log in to websites (e.g., Gmail), your identity can still be tracked regardless of VPN usage.
5. **Not a Replacement for Security Awareness**
   * VPNs can't protect against weak passwords, fake websites, or unsafe downloads.
6. **May Be Blocked by Some Services**
   * Certain websites or platforms (e.g., Netflix, banking sites) may block known VPN traffic.

**Conclusion**

While VPNs like Windscribe greatly enhance privacy and security, they should be used **alongside other best practices** like using strong passwords, avoiding suspicious links, and using antivirus tools for full protection.