

# Steps to Set Up Surfshark for Long-Term, Always-On Use

Configuring a VPN for continuous operation requires more than a quick connection toggle. Always-on VPN use means the service activates automatically on device startup, maintains stable tunnels across network changes, and includes fail-safes to prevent leaks during disruptions. Surfshark supports this through features like Auto-Connect, Kill Switch, and protocol optimizations, making it suitable for users prioritizing privacy over intermittent sessions. This guide outlines the steps to achieve reliable, long-term protection without platform-specific details, focusing on universal app-based configurations applicable across Surfshark's supported environments.

[Try Surfshark VPN >>](#) 

## Verify or Set Up Your Surfshark Subscription

Before installation, ensure you have an active Surfshark account. Long-term use benefits from a stable subscription, as it unlocks unlimited simultaneous connections and access to all servers—key for distributing load and avoiding single-point failures.

Start by visiting the official Surfshark site and selecting a plan that aligns with extended usage. Opt for annual or multi-year commitments for consistent access without renewal interruptions. After purchase, you'll receive login credentials via email. Store these securely, as they enable multi-device management.

Test account validity by logging into the member area online. Here, review server status and update payment methods preemptively to avoid lapses. Enable two-factor authentication (2FA) if available, adding a layer against unauthorized access during prolonged operation.

## Download and Install the Surfshark App

Obtain the app from Surfshark's official website or verified app stores to ensure integrity. Avoid third-party sources, which risk malware compromising your always-on setup.

During installation, grant necessary permissions for background operation, such as network access and notifications. These allow the app to monitor connections and reconnect silently. On first launch, the app prompts for login—enter your credentials promptly.

Post-installation, restart your device to verify the app integrates with system boot processes. This step confirms no conflicts with other software that could disrupt long-term VPN persistence.

## **Establish Initial Connection and Protocol Selection**

Log in and connect to a nearby server using the default WireGuard protocol, which Surfshark favors for its balance of speed and reliability. WireGuard typically offers lower overhead than OpenVPN, aiding battery efficiency in always-on scenarios.

Monitor the initial connection for stability: check for IP leaks via online tools and confirm DNS resolution works. If issues arise, switch to OpenVPN UDP for better handling of restrictive networks, though it may introduce slight latency.

Establish a baseline by running a session for 30 minutes, noting disconnects. This informs later optimizations, ensuring the setup withstands daily network fluctuations.

## **Enable Auto-Connect for Seamless Always-On Behavior**

Surfshark's Auto-Connect feature is central to long-term use, triggering VPN activation on boot, WiFi changes, or untrusted networks.

Access settings via the app menu:

- Toggle Auto-Connect on.
- Set triggers: always (for full-time protection), WiFi only, or mobile data.
- Prioritize trusted WiFi networks to exclude (e.g., home router) if split-tunneling applies later.

Pair this with "Connect on startup" if available, ensuring immediate tunnel establishment post-reboot. Test by rebooting multiple times—connection should restore within seconds without manual intervention.

## **Activate Kill Switch for Uninterrupted Protection**

No VPN is immune to drops, so the Kill Switch blocks all traffic during outages, preventing exposure.

In Surfshark settings:

- Enable "Kill Switch" (sometimes labeled Advanced Protection).
- Choose "Always On" mode over "On Untrusted Networks" for rigorous long-term enforcement.
- Verify app-level vs. system-wide options; system-wide is preferable for comprehensive coverage.

Test rigorously: disconnect the VPN manually or simulate network loss (airplane mode toggle). Internet should halt until reconnection. Adjust firewall rules if the Kill Switch conflicts with other apps.

## Optimize Server Selection and Multi-Hop

For sustained performance, select servers strategically. Surfshark's 3,200+ servers across 100 countries allow load balancing.

Criteria for long-term picks:

- Proximity to your location for minimal latency.
- High load capacity (check app's server list for real-time status).
- Countries with strong privacy laws (e.g., avoid Fourteen Eyes if paranoid).

Enable MultiHop (double VPN) for high-risk use, routing traffic through two servers. It enhances security but may reduce speeds—use judiciously. Rotate servers weekly via favorites list to prevent IP blacklisting.

## Configure Additional Stability Features

Enhance reliability with these targeted settings:

- NoBorders Mode: Activates obfuscation to bypass VPN blocks, ideal for restrictive ISPs or regions.
- CleanWeb: Blocks ads/trackers at the VPN level, reducing bandwidth waste over time.
- Bypasser (Split Tunneling): Exclude bandwidth-heavy apps (e.g., streaming) from VPN to preserve speeds.

Disable IPv6 leakage protection if your network supports it natively. Set custom DNS to Surfshark's or a trusted provider like 1.1.1.1 for leak prevention.

Update the app automatically—Surfshark pushes protocol improvements and bug fixes quarterly, crucial for long-term viability.

## Test and Validate the Full Setup

Rigorous testing ensures always-on integrity. Run these checks:

1. Reboot and confirm auto-connection.
2. Switch networks (WiFi to cellular) without drops.
3. Simulate outages; verify Kill Switch activation.
4. Use leak tests (ipleak.net, dnsleaktest.com) over hours.

Monitor logs in the app for errors. Generally, Surfshark maintains 99% uptime, but log patterns reveal ISP throttling.

## Perform Routine Maintenance

Long-term use demands upkeep. Weekly:

- Check app updates.
- Review connection logs for anomalies.
- Rotate servers or protocols if speeds degrade.
- Audit connected devices via account dashboard.

If performance dips, clear app cache or reinstall. Backup settings via app export if supported. Monitor data usage—VPNs add 5-15% overhead typically.

 [Try Surfshark VPN >>](#) 

## Final Thoughts

Setting up Surfshark for always-on, long-term use transforms it from a casual tool into a robust privacy shield. By prioritizing Auto-Connect, Kill Switch, and proactive optimizations, you minimize disruptions while maximizing protection. Expect occasional tweaks as networks evolve, but Surfshark's feature set generally handles extended sessions reliably. This configuration suits

remote workers, journalists, or anyone valuing persistent encryption without constant oversight. With disciplined maintenance, it delivers consistent results across varied conditions.

Disclosure: This is an unofficial guide created by our team and is not produced or endorsed by the VPN provider. This document may contain affiliate links; we may earn a commission at no extra cost to you.