



# Red.One

PRIVACY. SECURITY. DISCRETION.

## QUICK START GUIDE

# SET UP YOUR RED.ONE VPN

A secure internet connection with encrypted traffic, protected DNS, and privacy-focused filtering.

### PRIVATE CREDENTIAL

#### Protect the supplied configuration

The file or QR code is a private access credential. Do not share it or reuse it on another device. If it is exposed or lost, ask Red.One to replace it.

## DOWNLOAD THE VPN APP

Choose the official download for your device. The store page may display the name of the underlying VPN client; this is expected.

| DEVICE        | OFFICIAL DOWNLOAD                         |
|---------------|-------------------------------------------|
| iPhone / iPad | <a href="#">Apple App Store</a>           |
| Android       | <a href="#">Google Play</a>               |
| Windows PC    | <a href="#">Official Windows download</a> |
| Mac           | <a href="#">Mac App Store</a>             |

## ADD YOUR RED.ONE CONFIGURATION

- 1. Open the VPN app.** Tap the plus sign on mobile, or select Add Tunnel / Import Tunnel(s) from File on a computer.
- 2. Import the configuration.** Choose the supplied .conf file, or scan the supplied QR code on a supported mobile device.
- 3. Approve the VPN request.** Allow the device to add a VPN configuration and authenticate if prompted.
- 4. Confirm the name.** Rename the tunnel Red.One if supported; otherwise, leave the supplied name in place.
- 5. Turn it on.** Enable the toggle or select Activate. Confirm the tunnel shows Active before browsing.

### CONNECTION CHECK

#### Look for Active

The app should show an active tunnel, and its sent and received traffic counters should increase as the device uses the internet.

## PROTECTION

# WHAT THE RED.ONE VPN DOES

Red.One protects traffic in transit and applies secure DNS filtering whenever the tunnel is active.

### FULL-TRAFFIC PROTECTION

#### Encrypted traffic

Web, app, email, and DNS traffic leaving the device is routed through an encrypted tunnel to the Red.One gateway. This helps prevent local networks, public Wi-Fi providers, and nearby observers from reading or altering it in transit.

### ENCRYPTED NAME RESOLUTION

#### Protected DNS

DNS requests travel through the encrypted connection and a secure filtering layer, reducing local monitoring, manipulation, and common DNS leaks.

### SECURITY FILTERING

#### Threat blocking

Known phishing, malware, command-and-control, and other high-risk domains can be blocked before the device connects.

### PRIVACY FILTERING

#### Ad and tracker reduction

Many advertising, tracking, telemetry, and unnecessary data-collection domains are blocked. Online services generally see the Red.One gateway's public IP instead of the current network's public IP.

## EVERYDAY USE

### QUICK CONTROL

#### Turn protection on or off quickly

Open the VPN app and use the switch beside Red.One. On a computer, select Red.One and choose Activate or Deactivate. Confirm the app shows Active before browsing.

### AUTOMATIC RECONNECTION

#### Optional on-demand protection

On Apple devices, enable On-Demand Activation for Wi-Fi, cellular data, or both. On Android, enable Always-on VPN in system VPN settings. The stronger block-without-VPN option stops internet access if the tunnel cannot connect. On Windows, leave Red.One activated for continuous protection.

## PUBLIC NETWORKS

# HOTEL, AIRCRAFT & OTHER WI-FI

Some networks require a local login or terms page that cannot open while the VPN is active.

1. **Pause automatic reconnection.** Temporarily pause on-demand or always-on protection if Red.One immediately reconnects.
2. **Join the Wi-Fi.** Switch Red.One off and complete only the required login, payment, or acceptance page.
3. **Turn Red.One back on.** Reactivate it immediately, before browsing, opening apps, checking email, or entering sensitive information.
4. **Confirm protection.** Restore on-demand or always-on protection and verify that Red.One shows Active.

## CRITICAL

**Turn it back on immediately**

While Red.One is off, traffic returns to the normal network and Red.One protected DNS may no longer apply.

## IF A TRUSTED LINK IS BLOCKED

## AD AND TRACKER BLOCKING

**Filtering can block legitimate tracking-wrapped links**

This commonly affects sponsored results, marketing emails, and shortened URLs. First, navigate directly to the known website. If you are confident the link and destination are safe, briefly switch Red.One off, open the link, and turn Red.One back on immediately. Do not enter credentials, payment details, or sensitive information while protection is off.

## KEEP PROTECTION ACTIVE

- Leave Red.One on whenever practical, especially on hotel, airport, conference, cafe, and other public Wi-Fi.
- Only one device-level VPN normally operates at a time. Disable conflicting VPN connections if Red.One will not activate.
- If protection is temporarily disabled, reactivate it as soon as the required task is complete.

## PRIVACY BY DESIGN

# NO USER-ATTRIBUTABLE ACTIVITY LOGS

Red.One is designed to protect network activity without building a browsing history tied to the user.

## DNS &amp; VPN PRIVACY

**Your VPN and DNS activity is not retained**

Red.One does not maintain logs of individual DNS queries or VPN browsing activity. It does not retain DNS request content, browsing destinations, resolver histories, originating IP addresses associated with activity, connection histories, session timestamps, bandwidth histories, or other personally identifiable network-activity records.

- **Aggregate statistics only:** Red.One may maintain numerical totals for DNS requests processed and blocked. These totals do not contain domain names, destinations, timestamps, browsing histories, or information identifying the underlying activity.
- **Limited operational data:** Only technical information necessary to operate and secure the service is maintained, such as an account email address, randomly generated authentication tokens, encryption or authentication keys, and device notification tokens.
- **No advertising use:** Red.One does not sell or share browsing histories or VPN activity, and it does not monetize, redirect, alter, or manipulate traffic for advertising or commercial purposes.
- **Account control:** Users may manage available account and privacy information and may request deletion of eligible personal information, subject to legal, security, fraud-prevention, and operational requirements.

FULL PRIVACY POLICY / [red-one.info/privacy](https://red-one.info/privacy)

## TROUBLESHOOTING

- **Nothing loads:** Switch the tunnel off and back on. Confirm the internet works without the VPN, try another network, and restart the device if needed.
- **A site or app will not work:** A domain may be filtered or the service may restrict VPNs. Report it to Red.One. Do not edit DNS, keys, server, or routing fields unless instructed.
- **The tunnel will not activate:** Approve VPN permission, set date and time automatically, close another VPN, and re-import the current configuration. Do not reuse one configuration on several devices.

## IMPORTANT SECURITY LIMITS

## KNOW THE LIMIT

**A VPN protects data in transit**

It does not make a device anonymous or repair a compromised device. Websites and apps may still identify the user through sign-ins, cookies, device identifiers, or browser fingerprinting. Keep the device updated, use strong authentication, and treat unexpected links, files, and login requests cautiously.