RED.ONE CLIENT DEVICE GUIDE

YOUR PRIVATE & SECURE DEVICE

Purpose, configuration, applications, and operating habits for reducing digital exposure.

WHY THIS DEVICE EXISTS

A separate device for a separate risk profile

Red.One provides privacy-focused devices, connectivity, applications, and operational solutions for executives, high-profile individuals, protective teams, travelers, and others with elevated privacy or security concerns.

CORE OBJECTIVE Reduce unnecessary tracking, attribution, telemetry, and digital exposure while preserving the functionality needed for communication, travel, safety, and work.

Attribution	Telemetry	Network exposure	Operational exposure
Limit direct links between the device, its accounts, its service, and the end user's personal identity.	Reduce background analytics, advertising identifiers, unnecessary permissions, and routine data collection.	Encrypt traffic, apply protective DNS policies, and reduce visibility to local networks and destination services.	Support safer communications, travel, navigation, tracking detection, and team coordination.

Red.One solutions may include hardened Apple or Android devices, privacy-focused mobile or eSIM service, secure hotspots, encrypted communications, VPN and DNS protection, a strategic app suite, and turnkey provisioning for individuals or teams.

PRIVACY BY DESIGN

Configured to collect less, reveal less, and expose less

Exact settings vary by platform, mission, and client requirements. Typical provisioning includes the controls below.

Identity and device controls

- Separate, purpose-built accounts configured to minimize attribution to the end user.
- No personal phone number, email address, payment method, contact book, cloud profile, or recovery channel unless specifically authorized.
- Strong passcode, short auto-lock, hidden notification previews, and restricted lock-screen access.
- Biometric unlock enabled or withheld based on the user's legal, travel, and operational risk profile.
- Advertising personalization, analytics, diagnostic sharing, and unnecessary background activity disabled or minimized.

Network and management controls

- App permissions limited to what each approved application needs, including location, microphone, camera, photos, contacts, and nearby-device access.
- Always-on or persistent encrypted tunnel and protective DNS settings where supported.
- Automatic Wi-Fi joining disabled; private or randomized network addressing enabled where available.
- Operating-system and approved-app updates enabled, with installation limited to trusted sources.
- Remote management, mobile threat defense, backup, recovery, remote lock, and remote wipe configured according to the deployment model.

IMPORTANT Hardened does not mean invulnerable. A secure configuration can be defeated by unsafe account choices, repeated co-location, personal-network use, oversharing, or unapproved applications.

APPROVED CAPABILITIES

Privacy, communication, and productivity

Encrypted VPN No-log, ad-free encrypted traffic with private DNS resolution.	**Private DNS / Tunnel** Lightweight DNS privacy and an encrypted network tunnel.	**Custom Secure DNS** Policy-based blocking for malicious, risky, tracking, and unnecessary data-sharing domains.
Private Browser Blocks ads and trackers and automatically erases browsing history.	**App Privacy Analyzer** Reviews installed apps for trackers, permissions, and privacy concerns.	**Cellular Security Monitor** Identifies potentially suspicious towers or insecure mobile-network conditions.
Remote Security Camera Motion detection, live viewing, alerts, and optional remote recording.	**Encrypted Messaging Platform**** End-to-end encrypted messaging, calls, video, and file sharing.	**Privacy-Focused Messenger**** Private messages and calls designed to minimize user-data collection.
Encrypted Email Privacy-focused email with encrypted communications and enhanced account security.	**Group Communication Platform**** Efficient text, voice, video, and group communications.	**Push-to-Talk Application**** Group voice over cellular or Wi-Fi without radio line-of-sight limits.
Remote Desktop Secure remote access and control across computers and mobile devices.	**Privacy Productivity Suite** Secure storage, calendar, password manager, and multi-factor authentication.	**Optional Cloud Suite*** Email, documents, spreadsheets, presentations, storage, and collaboration.
Encrypted Notes Cross-platform notes with encrypted storage and synchronization.	**Private AI Assistant** Research, writing, summarization, and problem-solving with minimized logging and retention.	

* Requires a proprietary mobile service framework. ** May rely on associated push-notification infrastructure for reliable background notifications.

FIELD AND TRAVEL CAPABILITIES

Navigation, safety, awareness, and language

Primary Navigation Platform*

Routing, traffic, local search, and downloadable offline maps.

Privacy-Focused Offline Maps

Navigation without an active connection or persistent user tracking.

Temporary Location Sharing*

Time-limited live location sharing without requiring recipient accounts.

Group Location & Safety*

Location sharing, geofences, arrival alerts, crash detection, and safety tools.

Ride-Hailing Applications*

On-demand transportation, with prepaid or gift-card funding where available.

Weather Radar

Live radar, alerts, forecasts, and storm visualization.

Emergency Room Locator

Uses device location to identify nearby emergency medical facilities.

Offline First Aid Guide

Step-by-step medical and safety information available without connectivity.

Bluetooth Tracker Detection

Identifies potentially unwanted or hidden Bluetooth-based trackers.

Bluetooth Device Scanner

Surveys nearby Bluetooth and low-energy devices for identification or troubleshooting.

Wi-Fi Analyzer

Shows nearby networks, signal strength, channels, and local wireless conditions.

Translation Application*

Text, speech, image, and conversation translation, including offline languages where supported.

USE SELECTIVELY Location, Bluetooth, Wi-Fi scanning, ride-hailing, and translation tools may require permissions or proprietary services. Enable them only when needed, use the minimum necessary permissions, and disable them after the task.

* Application or service that requires a proprietary mobile service framework to operate properly.

LAYERED PROTECTION

Encrypted transport plus policy-driven DNS defense

Connections are routed through an encrypted tunnel designed to protect traffic on untrusted networks, reduce ISP visibility into destination activity, and present a protected exit address to internet services. A custom DNS layer then applies real-time policies before domains are reached.

1 DEVICE	2 ENCRYPTED TUNNEL	3 SECURE DNS	4 INTERNET
Approved apps and hardened settings	Protected transit and source-IP separation	Real-time policy and threat filtering	Reduced exposure to risky destinations

Known-threat blocking

Threat-intelligence feeds, AI-driven DNS detection, Google Safe Browsing, and command-and-control blocking.

Deception defense

Protection against phishing, IDN homographs, typosquatting, DNS rebinding, and algorithmically generated domains.

High-risk domain controls

Blocking for newly registered domains, risky dynamic DNS hosts, parked domains, selected top-level domains, and known CSAM-hosting domains.

Resource abuse defense

Cryptojacking protection helps prevent unauthorized use of device resources for cryptocurrency mining.

Policy control

Configurable categories allow the deployment to block domains that are risky, unnecessary, or inconsistent with the mission.

Continuously updated

Protective categories and reputable data sources are updated as threats and infrastructure change.

Network defenses materially reduce exposure but cannot eliminate all malicious content, endpoint compromise, traffic correlation, or user error.

CONTINUOUS DEVICE AWARENESS

Protection across apps, files, networks, and device integrity

Comprehensive coverage Monitors application, file, network, operating-system, rooting, jailbreaking, and device-integrity risks.	**Malware prevention** Detects and blocks malicious apps and files in real time before they can affect the user or enterprise.	**Phishing and network defense** Identifies phishing, unsafe Wi-Fi, man-in-the-middle conditions, and other network-based threats.	**Conditional access** Can restrict corporate resources when a device becomes risky, compromised, or non-compliant.
Enterprise integration Supports major UEM and MDM platforms, including Microsoft Intune, VMware Workspace ONE, and Samsung Knox.	**Zero-touch deployment** Supports streamlined enrollment and consistent security-policy application across managed devices.	**Low user impact** Designed to operate transparently with low performance overhead and privacy protection for end users.	**Unified visibility** Centralized management supports monitoring, policy enforcement, BYOD, and corporate-owned iOS and Android devices.

If the device reports a threat

Do

- Stop the affected activity and note what happened immediately before the alert.
- Disconnect from untrusted Wi-Fi and follow the organization's support or incident-reporting procedure.
- Preserve the device and alert details for review.

Do not

- Dismiss, override, or repeatedly retry a blocked action.
- Factory-reset, delete evidence, or install unapproved security tools unless directed.
- Move sensitive work to another unapproved device.

THE MOST IMPORTANT RULE

Keep the device unassociated with your personal identity

PRIVACY IS OPERATIONAL The device is provisioned to minimize attribution. Your habits determine whether that separation lasts.

1 Do not sign in to personal Apple, Google, Microsoft, social-media, banking, shopping, loyalty, cloud-storage, or messaging accounts.	**2** Do not use personal phone numbers, email addresses, physical addresses, payment cards, contacts, or trusted devices for account recovery.
3 Do not import personal contacts, photos, calendars, browser history, passwords, backups, or SIM profiles.	**4** Do not connect to your home Wi-Fi, personal hotspot, vehicle infotainment system, smartwatch, earbuds, printer, or other personally associated device unless specifically approved.
5 Avoid routinely carrying or operating the Red.One device beside your primary phone. Repeated co-location and synchronized movement can create a behavioral association.	**6** Do not add personal payment methods or use routine delivery addresses. Use approved funding and fulfillment methods where available.
7 Do not publish the device number, alias, screenshots, distinctive configuration, or account identifiers in a way that connects them to you.	**8** Keep the device's purpose narrow. Do not gradually convert it into a second personal phone.

When operational requirements conflict with these rules, obtain specific guidance before proceeding. One convenience-based exception can create a lasting link.

SIMPLE ROUTINES

Use the device deliberately

BEFORE USE

- Confirm the device is updated and shows no security warnings.
- Confirm the VPN or encrypted tunnel and secure DNS are active.
- Disable Wi-Fi, Bluetooth, location, and nearby-device scanning unless needed.
- Use the secure hotspot or approved connectivity plan for sensitive activity.

DURING USE

- Use approved apps only and grant the minimum permission needed.
- Prefer encrypted messaging and calls; verify contacts through a separate trusted channel for sensitive exchanges.
- Use offline maps when practical and temporary location sharing only for the required period.
- Avoid public charging ports; use an AC adapter, power bank, or data blocker.

AFTER / WEEKLY

- End temporary location sharing and disable permissions no longer needed.
- Clear sensitive downloads, screenshots, clipboard content, and browser data according to policy.
- Review installed apps, permissions, VPN/DNS status, storage, and security alerts.
- Store the device securely and power it down when it is not required for the mission.

Communication discipline

Verify

Confirm sensitive contacts and key changes through a separate trusted channel.

Minimize

Share only the information needed and use disappearing or retention-limited options when appropriate.

Separate

Keep personal and Red.One conversations, groups, aliases, files, and contact paths distinct.

Report

Treat unexpected login prompts, codes, warnings, or account changes as possible compromise indicators.

BEFORE, DURING, AND AFTER TRAVEL

Expect hostile networks, inspection, loss, and observation

Prepare

- Confirm local laws, border-search considerations, and organizational travel policy.
- Remove data and applications not needed for the trip; use the minimum-data principle.
- Download offline maps, language packs, medical guides, and essential documents in advance.
- Confirm roaming, eSIM, hotspot, VPN, DNS, remote lock, and recovery methods before departure.
- Record support procedures separately; do not store every recovery secret on the same device.

Operate and return

- Treat hotel, airport, aircraft, event, and public Wi-Fi as untrusted.
- Do not surrender an unlocked device or disclose credentials unless required and addressed by policy.
- Use a privacy screen, maintain physical control, and avoid leaving the device unattended in vehicles or rooms.
- Run tracker or local wireless-environment checks when justified, understanding they are screening tools rather than full technical surveillance countermeasures.
- After travel, review alerts, accounts, apps, permissions, and device integrity before reconnecting to sensitive resources.

PHYSICAL SECURITY A private configuration cannot protect information displayed to an observer, spoken within listening range, photographed from the screen, or extracted from an unlocked device.

For higher-risk travel, a clean travel profile, dedicated temporary service, reduced data load, and post-travel technical review may be appropriate.

IF SOMETHING DOES NOT LOOK RIGHT

Contain first. Preserve evidence. Escalate quickly.

LOST OR STOLEN Use the approved reporting path immediately. Initiate remote lock or wipe only in accordance with the deployment policy and support direction.	**SUSPICIOUS LOGIN** Do not approve unexpected prompts or codes. Record the details, disconnect from untrusted networks, and report the event.	**PHISHING OR MALWARE** Stop interacting with the content. Do not revisit the link, download additional tools, or forward the suspicious item outside the approved reporting process.
NETWORK WARNING Leave the network, disable automatic reconnection, retain the alert details, and move to approved connectivity.	**TRACKER ALERT** Move to a safe location, preserve screenshots and timing, inspect belongings and vehicles only when safe, and involve security or law enforcement as appropriate.	**BORDER OR DEVICE SEARCH** Follow applicable law and the organization's travel protocol. Report the access or inspection before resuming sensitive use.

Do not destroy evidence

Do not factory-reset the device, delete messages, clear security alerts, rotate every account, or install new security software unless directed. Those actions can remove information needed to understand the event and may complicate recovery.

SAFETY FIRST If the event creates an immediate physical threat, move to safety and contact emergency services or the responsible protective team before performing technical steps.

BEFORE FIRST OPERATIONAL USE

Confirm the device is ready - and keep it separate

[ ] I understand the device's approved purpose and who to contact for support.	[ ] I have not added personal accounts, recovery details, contacts, payment methods, networks, vehicles, wearables, or backups.
[ ] The device uses a strong passcode, short auto-lock, and hidden lock-screen previews.	[ ] The encrypted tunnel, protective DNS, mobile threat defense, and required management profiles are active.
[ ] Wi-Fi auto-join is off, private addressing is enabled where supported, and radios or permissions are disabled when unnecessary.	[ ] Only approved applications are installed, and each has the minimum required permissions.
[ ] Offline maps, language resources, medical references, and travel content are loaded if needed.	[ ] I know how to report loss, compromise, suspicious towers or networks, tracker alerts, and unexpected account activity.

Privacy. Security. Discretion.

The strongest protection comes from combining a hardened device, protected connectivity, carefully selected applications, and disciplined user behavior.

red-one.info

Important limitation: Red.One solutions are designed to reduce exposure and attribution risk, not to guarantee anonymity, immunity from lawful process, or protection against every technical or operational threat. Configuration and capabilities vary by device, service, jurisdiction, and client policy.