OHMPORT DOCUMENTATION

Security Overview

Written for the people who have to approve software: exactly what OhmPort does and doesn't do with your network, your data and your evidence.

APPLIES TO OHMPORT 2.0 · UPDATED AUGUST 2026

At a glance

OhmPort is built on one principle: **"we don't send your data anywhere" should be a property you can verify, not a promise you have to trust.** The desktop edition makes it structural — the binary contains no networking code — and the web edition keeps all of your data inside your browser's storage on your own computer.

PROPERTY	DESKTOP	WEB
Outbound connections	None — no HTTP client exists in the binary	App code loads from our host; your data makes zero requests
Account / sign-in	None	None
Telemetry & analytics	None	None — no cookies, no third-party requests of any kind
Where data lives	One SQLite file in your user profile	Same SQLite format, in the browser's private storage on your computer
Automatic updates	None — updates are deliberate manual installs	Only on page reload, never mid-session
Licence verification	Entirely offline, inside the app (Ed25519 signatures)	
Works air-gapped	Yes — designed for it	After first visit (installable, offline-capable)

Network behaviour

Desktop: structurally offline

- There is **no HTTP client in the application or its dependency tree** — the app is incapable of making a network request, rather than configured not to.
- No auto-updater, no crash reporting, no analytics, no telemetry, no licence "phone home".
- Everything that would normally be fetched ships inside the installer: reverse-geocoding data, licence verification keys, release notes.
- The embedded webview runs under a `default-src 'self'` Content-Security-Policy, so even the UI layer cannot load remote content.
- The Windows installer bundles the WebView2 runtime as an offline installer — installation itself needs no network.

Verify it yourself: run OhmPort on an air-gapped machine, or watch it under a firewall or packet capture — you will observe no traffic, at install time or at runtime.

Web: data-local, code-served

- The web edition is a static site — there is **no application server**, no API, and no account system. The only network activity is your browser downloading the app's own code from our host.
- Your detector talks directly to the browser tab over Web Serial; records are written to the browser's origin-private storage on your computer and are never transmitted.
- The site sets no cookies and makes no third-party requests — fonts, scripts and map data are all served from the same origin.
- One honest caveat: the app's code is delivered by our host each visit (cached for offline use thereafter). If your threat model requires that nothing is ever fetched, use the desktop edition.

Enforced browser policy (web edition)

The web edition's promises are enforced by response headers, not just kept by convention — the deployed policy prevents the app from talking to third parties even if its code tried:

- **Content-Security-Policy**: `default-src 'none'` with `connect-src 'self'` — the page cannot make requests to any other host. Scripts are same-origin only, with no `unsafe-inline` or `unsafe-eval` (only `wasm-unsafe-eval`, required to instantiate the app's own WebAssembly modules).

- **Permissions-Policy**: `serial=(self)` — Web Serial for this origin only; geolocation, camera, microphone and USB are explicitly disabled.
- **Framing**: `frame-ancestors 'none'` and `X-Frame-Options: DENY` — the app cannot be embedded in another site.
- **Referrer-Policy**: `no-referrer`.

Data handling & sovereignty

- **One file, yours** — all records, notes, projects, custody logs, watchlists and settings live in a single SQLite database: in your OS user profile (`com.ohmsense.yorkipro`) on desktop, or the browser's private storage in the web edition. There are no cloud copies, caches or shadow databases.
- **Backups under your control** — backups are ordinary `.sqlite` files written where you choose, interchangeable between editions. Before a new desktop version first touches your database it takes an automatic local backup (ten most recent kept).
- **Retention is yours to manage** — delete individual records or all data from the app; separately, erase the detector's own on-device memory when required by your handling procedures.
- **At-rest encryption** — OhmPort does not add its own file encryption; protect data at rest with your standard operating-environment controls (e.g. BitLocker, FileVault), which cover the database like any other user file.

Evidence integrity

- **Hash-chained custody log** — every project keeps a chain-of-custody log in which each event cryptographically commits to the events before it. The app verifies the chain and displays its status; any subsequent alteration or deletion breaks the chain and is flagged.
- **Operator attribution** — custody events record the operator/investigator name configured in Settings.
- **Copies, not references** — adding a record to a project copies the evidence into the case file, so later changes to the working set don't silently change the case record.

Licensing security

- Licences are JSON payloads signed with **Ed25519**; the app embeds only the public key and verifies signatures locally. The private signing key never ships with the product.
- Licences are bound to device serials and carry version and expiry constraints, all evaluated offline.
- Activation is deliberately out-of-band: you obtain the licence in your own web browser on the Ohmsense portal and paste it into the app. The app itself never contacts the portal — the "Activate online" button simply opens your system browser.

Update model

- **Desktop** — no self-update mechanism exists. New versions are installed deliberately, by you, from installers supplied by Ohmsense; this keeps change control in your hands and suits managed SOEs. Your database is untouched by reinstalls and automatically backed up before first open by a newer version.
- **Web** — new versions apply only when you reload the page, never mid-session, and offline use continues on the version you last loaded.

Deployment notes for security teams

- **No firewall exceptions, proxy configuration or TLS-inspection allowances are needed** for the desktop app — it makes no connections to allow.
- Suitable for **air-gapped networks and evidence-handling machines**; installation is fully offline.
- Installed per-machine on Windows (NSIS); data is per-user, in the user's profile.
- The application requests no elevated privileges at runtime and accesses the detector via the operating system's serial interface.
- For the web edition, host access can be restricted to your network's allowlist; after first load the app runs offline as an installed PWA.

Reporting a security issue

If you believe you've found a security issue in OhmPort, contact info@ohmsense.com.au with details and we will respond promptly. Please don't publish details until we've had a reasonable opportunity to address the issue.

More

- OhmPort overview — features, editions and screenshots.
- User guide — installation, day-to-day use and troubleshooting.