ROSTER

Privacy Policy

Effective: 19 May 2026 · Version 1.1 · Publisher: The Roster Project · Governing law: Commonwealth of Australia (does not displace your local mandatory consumer protections)

The short version

Roster does not collect, log, or transmit any information about you, the accounts you load into it, the games you launch, or how you use the app. The application would still work if you firewalled it from everything except Roblox.

By default there are three outbound destinations Roster ever contacts:

1. **Roblox's web API**, to refresh your accounts. Same hosts your browser would hit.
2. **The Roster update channel** (GitHub Releases), to check whether a newer version exists.
3. **The Roster licensing endpoint** (`api.accountroster.com`), only if you buy Plus: once to bind your licence to a machine, then once per day to re-issue a fresh signed licence file. After that, all licence verification is local.

Roster shows no ads at all - on any tier. There is no ad network, no banner, no pre-launch video, and no third-party advertising tag anywhere in the app. The Free tier is simply feature-limited; Plus unlocks the full app.

If you use the in-app cookie-capture sign-in flow, Roster also embeds Microsoft's WebView2 component to render Roblox's official login pages locally. WebView2 is a Microsoft-controlled rendering engine and is bound by Microsoft's own privacy disclosures for the embedded browser process. We use it only to load `roblox.com` and the OAuth pages it redirects to; we don't ship any analytics on top of it.

What stays on your machine

Everything that's "your data" lives in `%LOCALAPPDATA%\Roster` and never leaves it unless you explicitly export it:

- Your account list, usernames, aliases, notes, and per-account settings.
- The encrypted vault (DPAPI + optional Argon2id).
- The refresh log and audit log.
- Window-layout presets, group memberships, private-server links.
- Per-account playtime sessions.
- Your master password, only as an Argon2id-derived key, only in process memory, only while the vault is unlocked.

No cloud sync. No "anonymous usage statistics that turn out not to be anonymous." No crash pings. If Roster crashes, the crash dump is written to disk and you can mail it to us if you want; we don't pull it.

What touches the network

1 / Roblox APIs

For each account in the vault, Roster's refresh loop calls Roblox's web API on that account's behalf. These are the same authenticated endpoints the official site uses, with the cookie from the vault attached. We never proxy game-server traffic and never touch the game client's own sockets.

2 / Update channel

On an hourly cadence, Roster checks GitHub Releases for the project to see if a newer version is available. The request is unauthenticated. GitHub may log standard server-access information (IP, user-agent) under their own policy; we don't operate that endpoint and we don't see those logs.

3 / Licensing endpoint (Plus)

If you buy Plus, the desktop app talks to our licensing endpoint twice in distinct shapes:

- **Activation** - each time you paste your activation code on a machine. The call sends your code and a hardware fingerprint hash derived from stable Windows identifiers (a hash, not the raw values), and the server returns an Ed25519-signed licence token bound to that fingerprint. If your licence was previously bound to a different machine, the server rebinds it to the new one. The previous machine's daily refresh will then come back as `410 Gone`, and that machine drops to the free tier on its own.
- **Daily refresh** - once per day after activation, the app sends your customer ID plus the fingerprint hash and receives a re-issued licence token with a fresh expiry. This is what lets the app keep working through a renewal cycle without you doing anything.

Roster writes the signed token to `%LOCALAPPDATA%\Roster`. Between refreshes the app verifies the token entirely offline; you can take a machine off the network for a full renewal cycle and your licence keeps working. The fingerprint-binding is why copying the token to another machine doesn't work: the signature is over the fingerprint. Lifetime grants skip the daily refresh entirely.

If you pay for Plus

The billing system runs on Whop. Whop receives your payment details directly and is the merchant of record; Roster's servers never see card information. The information Roster's billing backend keeps in its own KV store is the minimum to make subscriptions work:

- Your email address (forwarded by Whop on successful checkout, so we can send the activation code).
- A Whop customer/membership ID (so renewals work).
- Subscription tier, status, and the next renewal date Whop reports.
- The hardware fingerprint hash of the machine you've bound your licence to, and the activation timestamp.

Notably absent: any Roblox account information (your Roblox usernames are not sent to the billing system), any usage data, and any device information beyond the opaque fingerprint hash.

Aggregate server-side counters

We keep daily aggregate counts of requests our own servers were going to receive anyway: how many machines pinged our lightweight first-party presence beacon when the app launched on a given day, how many paid licences performed their daily refresh, and how many times the installer was downloaded through this website's download button. This counting happens entirely on our servers; it adds nothing to what the app transmits, and the app remains telemetry-free.

To avoid counting the same machine twice in one day on the presence beacon, we hash the request's IP address and browser user-agent together with the current date. The hash rotates every day, cannot be reversed back into an IP address, and the raw IP is never stored. Paid refresh events are keyed by a one-way hash of the internal customer ID. No names, email addresses, Roblox accounts, or hardware fingerprints enter the metrics dataset, and nothing in it can reconstruct an individual's history.

What we will never do

- Add product analytics to the desktop app, even "anonymous" ones. The app sends nothing about how you use it; the only counting that exists is the aggregate server-side counters described above.
- Add crash telemetry that uploads automatically.
- Sell, share, or rent your email address.
- Phone home from a paid install for any reason after the one-time activation, beyond the daily licence refresh.
- Use cookies or third-party JavaScript on the marketing pages of this website. The pages you browse here set no cookies and load no third-party scripts.
- Bundle a third-party advertising, analytics, or bandwidth-sharing SDK in the desktop app. Roster ships no ad network and no advertising tag of any kind; the app shows no ads on any tier. (Microsoft's WebView2 is a Windows rendering component - it hosts the Roblox sign-in flow - and is not itself an advertising or analytics SDK.)

Your rights, briefly

For the Free tier, Roster doesn't hold personal data on its servers, so the rights you'd ordinarily exercise under GDPR, CCPA, or your local equivalent don't have much to attach to. The vault is on your machine; you delete it by uninstalling.

For Plus, the personal data we hold is your email address, your Whop customer/membership ID, and the hardware fingerprint hash of the machine you've bound your licence to. You can ask us to delete that record at any time (which will also deactivate the licence). Email support@accountroster.com. We'll do it within 30 days and confirm in writing.

Changes to this policy

If we ever change this policy in a way that affects what Roster does or does not transmit, we will announce the change in the next release's changelog, bump the major version of the application, and require explicit re-consent on first launch after the update. There is no scenario in which Roster begins transmitting new information about you without you noticing.

Contact

For anything privacy-related: security@accountroster.com. Read by one person, usually within 24 hours.