csiPass Companion Manual

This guide is for someone who already has a csiPass device and wants to use the **optional** companion on a computer. The companion lists passkeys, enrols OATH accounts, changes Display preferences, and guides erase. It never signs for you and never presses Confirm.

The device screen is still the trust surface. Anything that changes security state or destroys data waits for a press on the glass.

For everyday use of the key itself, see the User Manual.

What the companion is

The companion is a local program: a Go service on loopback and a native window (or a browser tab in headless mode). It talks to the device over a **management** USB channel that is separate from FIDO HID.

It **cannot**:

- export private keys, PINs, seeds, or decrypted vault records
- approve a registration or assertion
- show an OATH code (codes stay on the device glass)

It **can**:

- unlock a management session with the device PIN
- list resident passkeys, site-held journal rows, and OATH accounts
- change Display settings and PIN / UV policy (after Confirm on the device)
- enrol, edit, reveal-on-glass, and delete OATH accounts (after Confirm)
- erase everything through management (after Confirm)

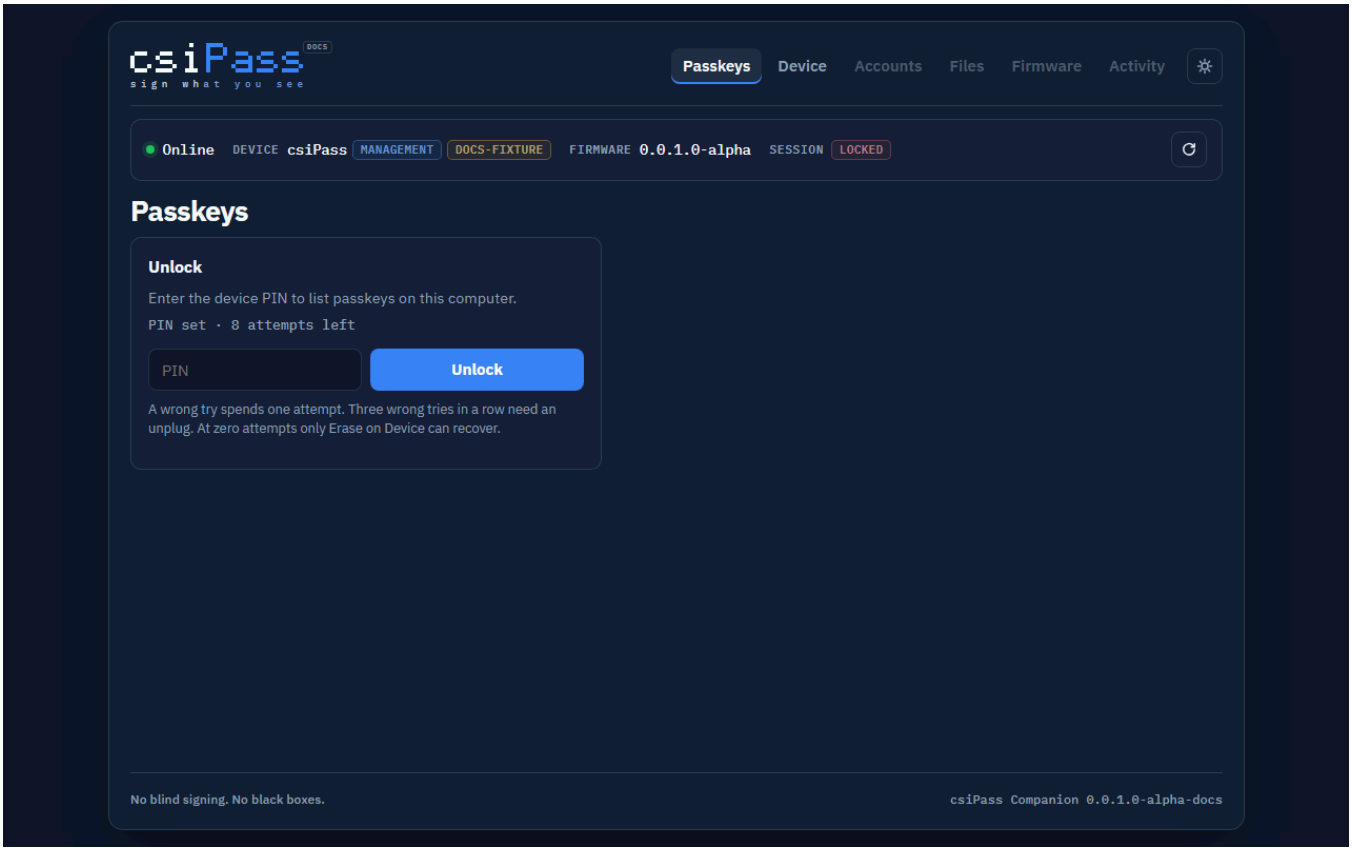
Footer claim, same as the site: **No blind signing. No black boxes.**

Before you start

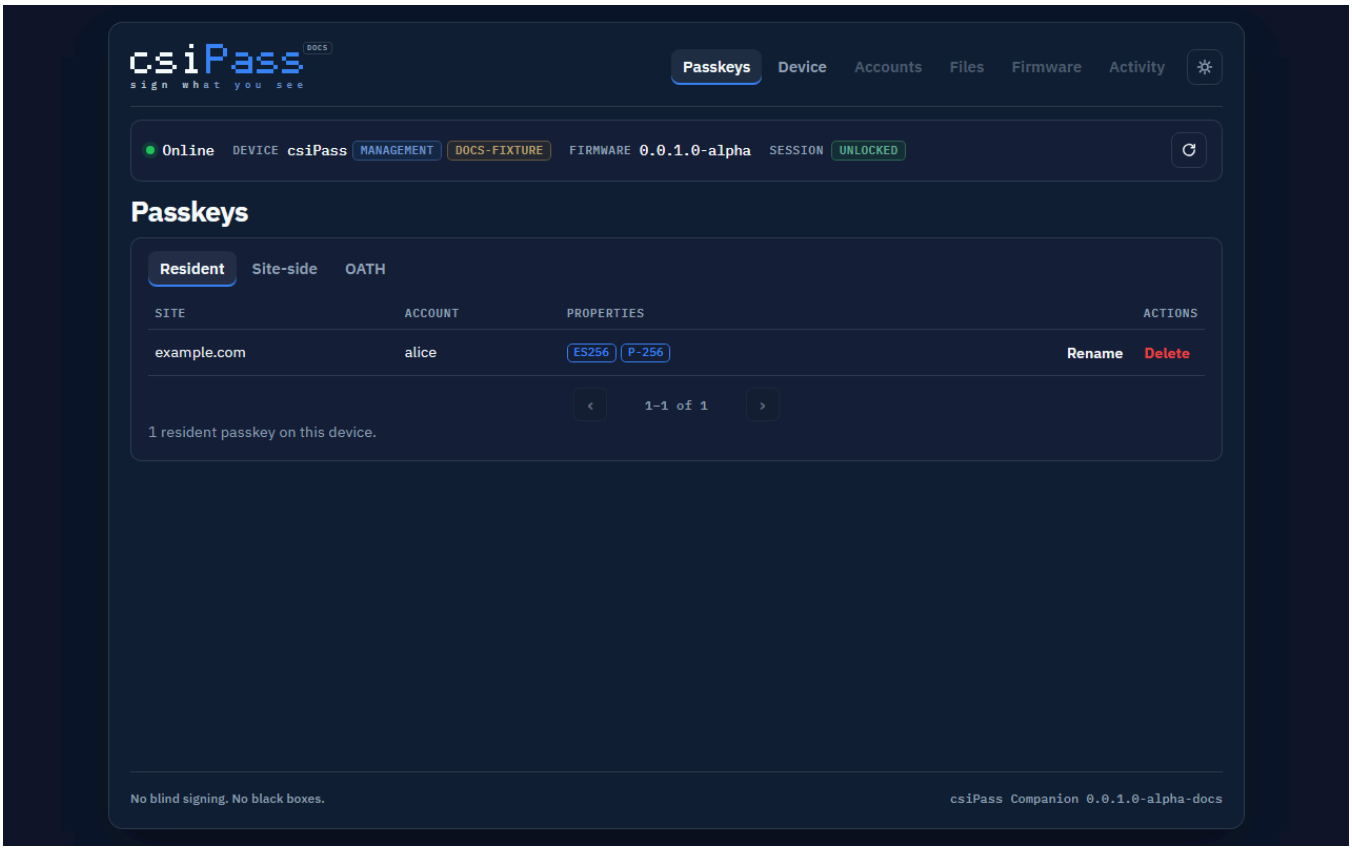
1. Flash a current firmware build and plug the key in.
2. Run the companion for your OS (`cmd/csipass`). On Windows the desktop shell opens a WebView; `-headless` serves the UI for a local browser.
3. Use **test accounts only**. The product is still a development prototype.

Unlock

When a device is connected and a PIN is set, Passkeys opens behind an unlock gate. Enter the PIN. Three wrong tries in a row require unplugging the key before further attempts spend retries.



After a successful unlock the session stays open until you quit or the device leaves. The rail shows **Unlocked**.

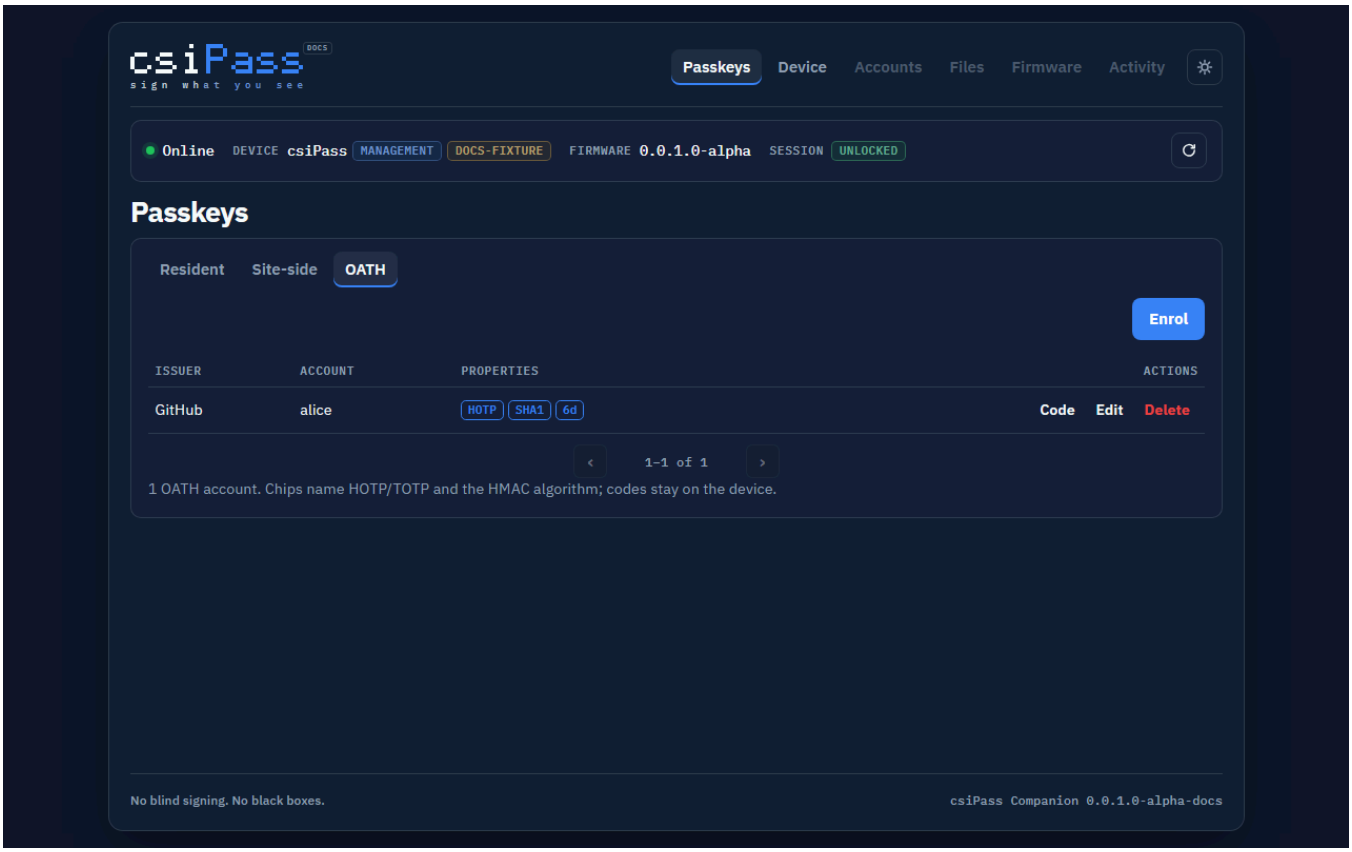


Passkeys, Site-held, and OATH

Three lists share the Passkeys view:

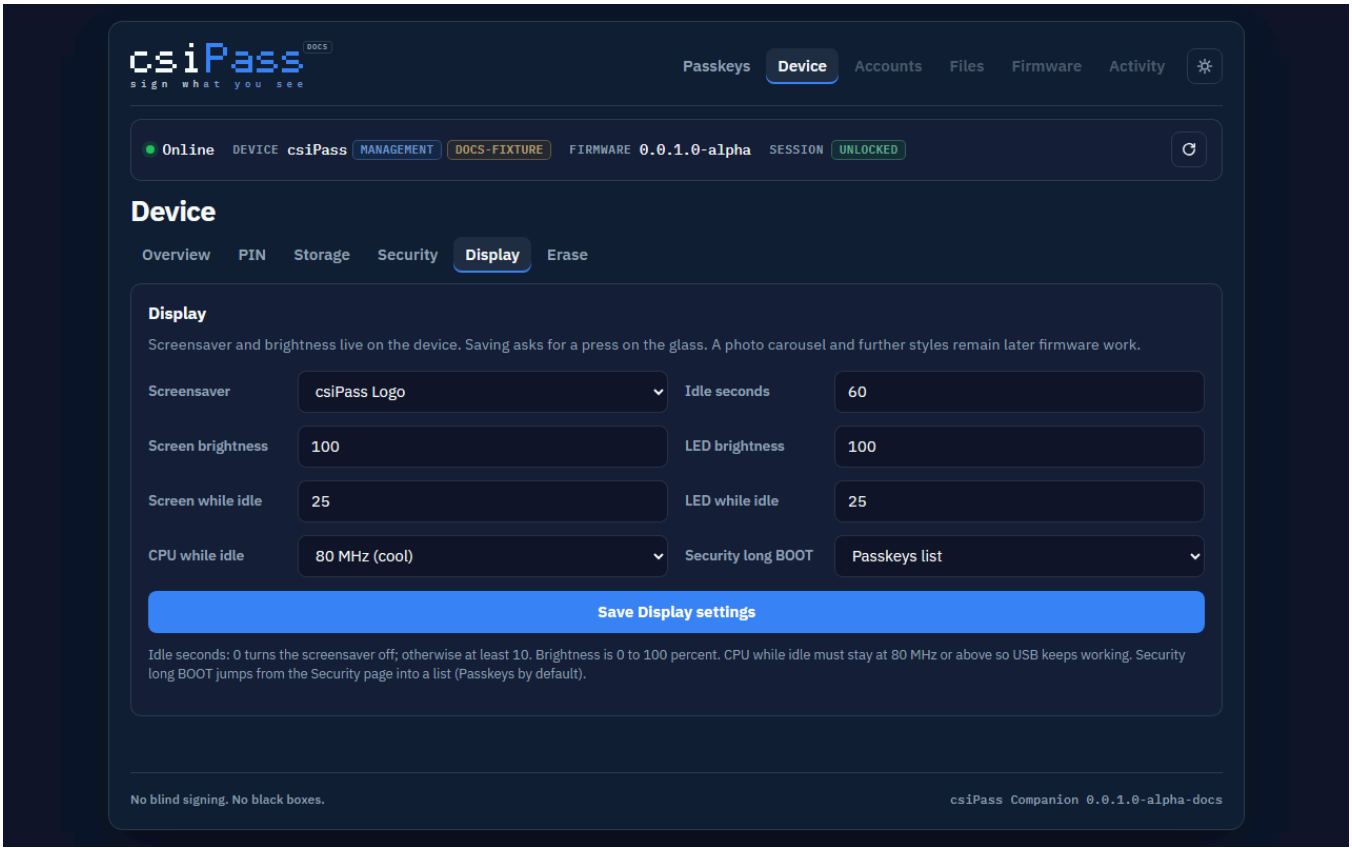
List	What it shows
Passkeys	Resident credentials stored in the vault
Site-held	Metadata for non-discoverable (derived) registrations
OATH	HOTP (and later TOTP) accounts; codes never leave the glass

Rename and delete for passkeys, and enrol / edit / reveal / delete for OATH, each wait for **Confirm on the device**. Cancel in the companion aborts the wait and clears the Confirm screen.



Device → Display

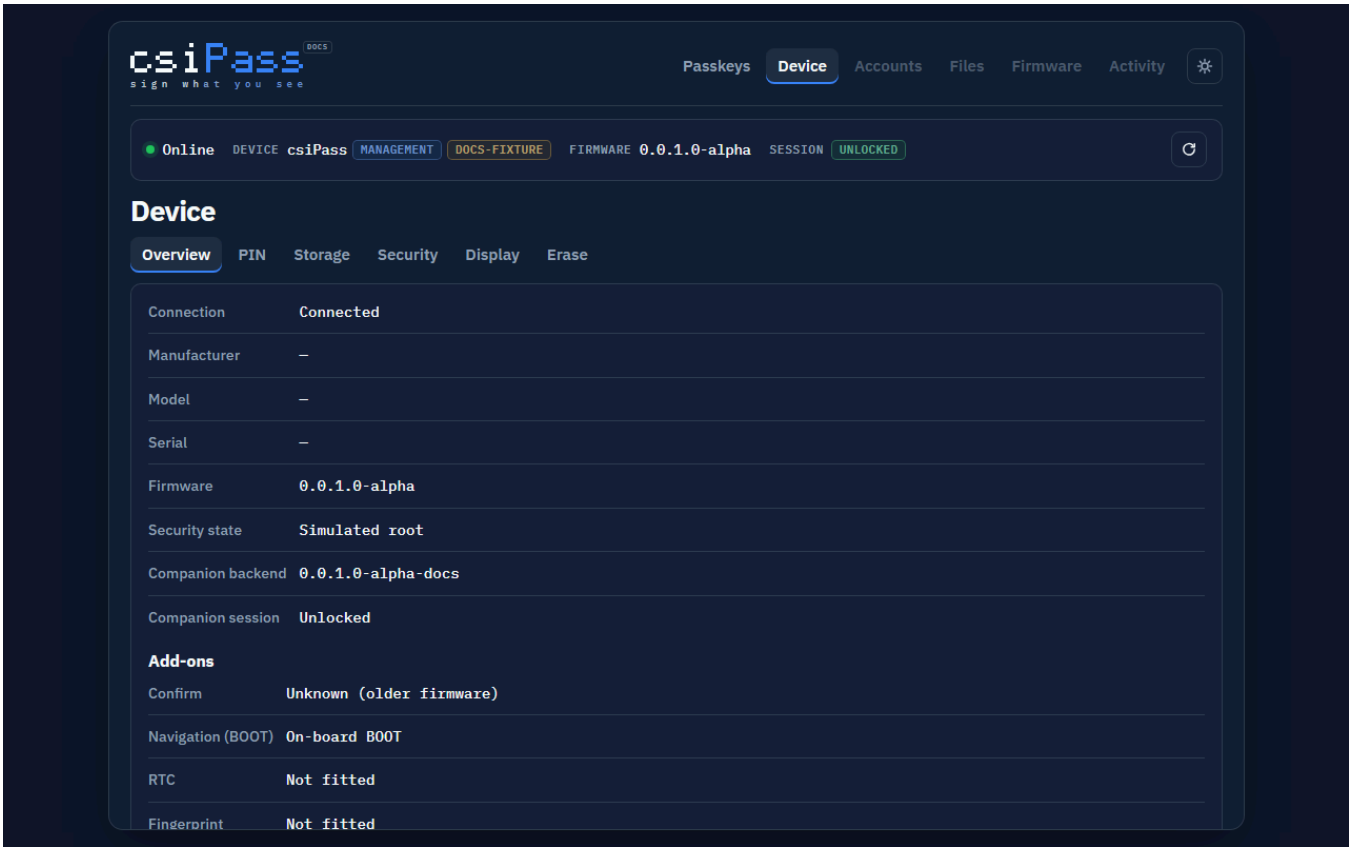
Unlock first. Open **Device** → **Display**. Saving asks for Confirm on the glass.



Setting	Meaning
Screensaver	None, csiPass Logo, Breathing Dot, Cipher Text, Lissajous, Starfield, Floating Clock
Idle seconds	`0` disables; otherwise at least 10
Brightness	Screen / LED normal and while idle (0–100 %)
CPU while idle	`80`, `160`, or `240` MHz (USB stays up at 80+)
Security long BOOT	Long BOOT on the Security page opens Passkeys, Site-side, or OATH

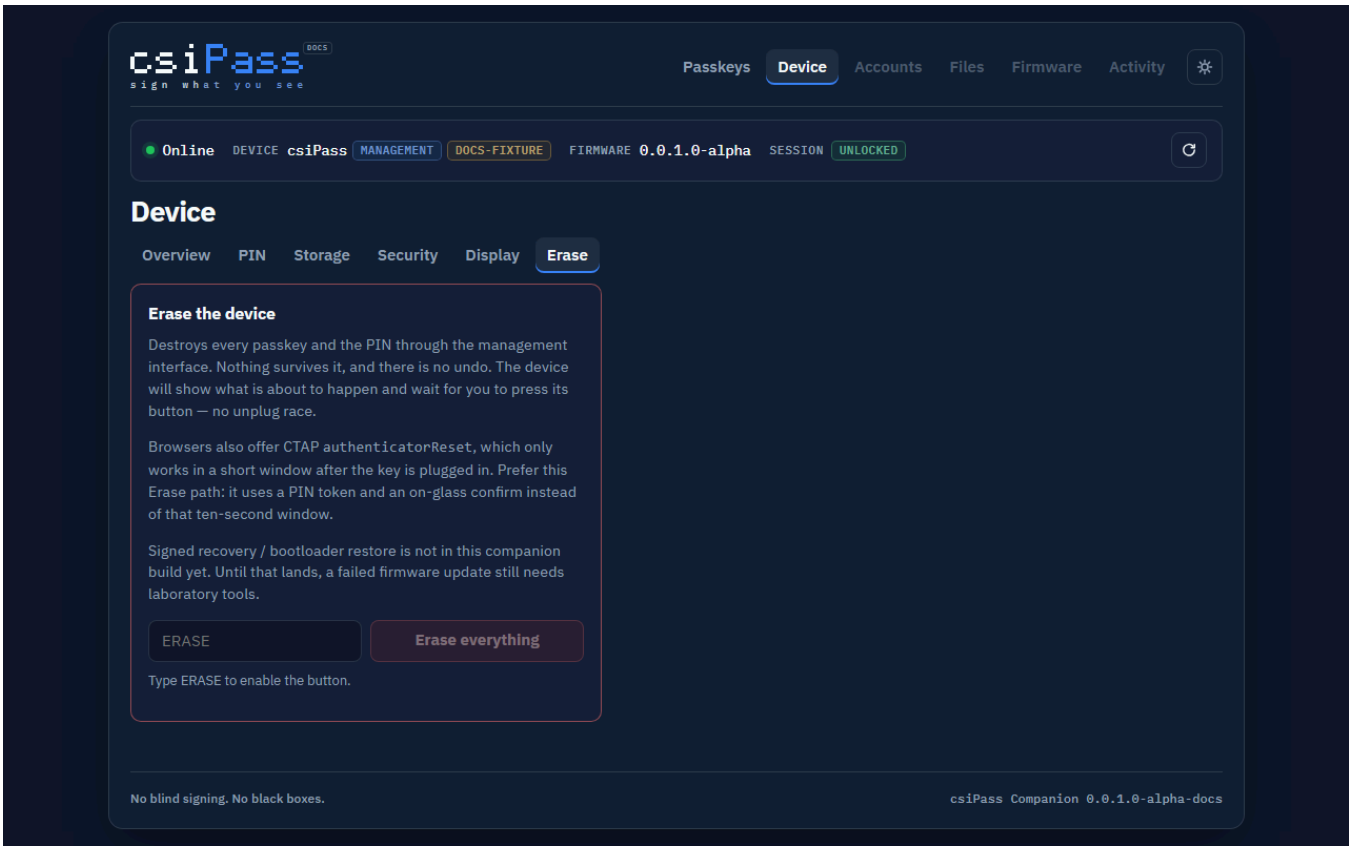
Device → Overview (PIN policy)

PIN / UV policy lives on Device overview: Always UV, minimum PIN length (may only rise), force PIN change, and the min-PIN RP allow-list. Saving waits for Confirm.



Erase

Device → **Erase** destroys every passkey and the PIN through management. Type `ERASE`, then Confirm on the glass. Prefer this path over CTAP `authenticatorReset` (the short plug-in window).



Regenerating these pictures

Companion screenshots are generated, never drawn by hand:

```
pwsh tools\companion-screenshot\companion-screenshot.ps1
```

The tool serves the real companion frontend against a fixture API (no USB key) and captures named scenes into `docs/images/companion/`.