TEPS Sentinel — Complete Setup Guide

TEPS Sentinel is the caretaker for your studio Macs. It activates and tracks your TEPS licenses, keeps your photo apps running and up to date, restarts machines on a schedule, cleans out old job folders, keeps network shares mounted, and reports every machine's health back to one place — so you find out a kiosk is in trouble before an event does.

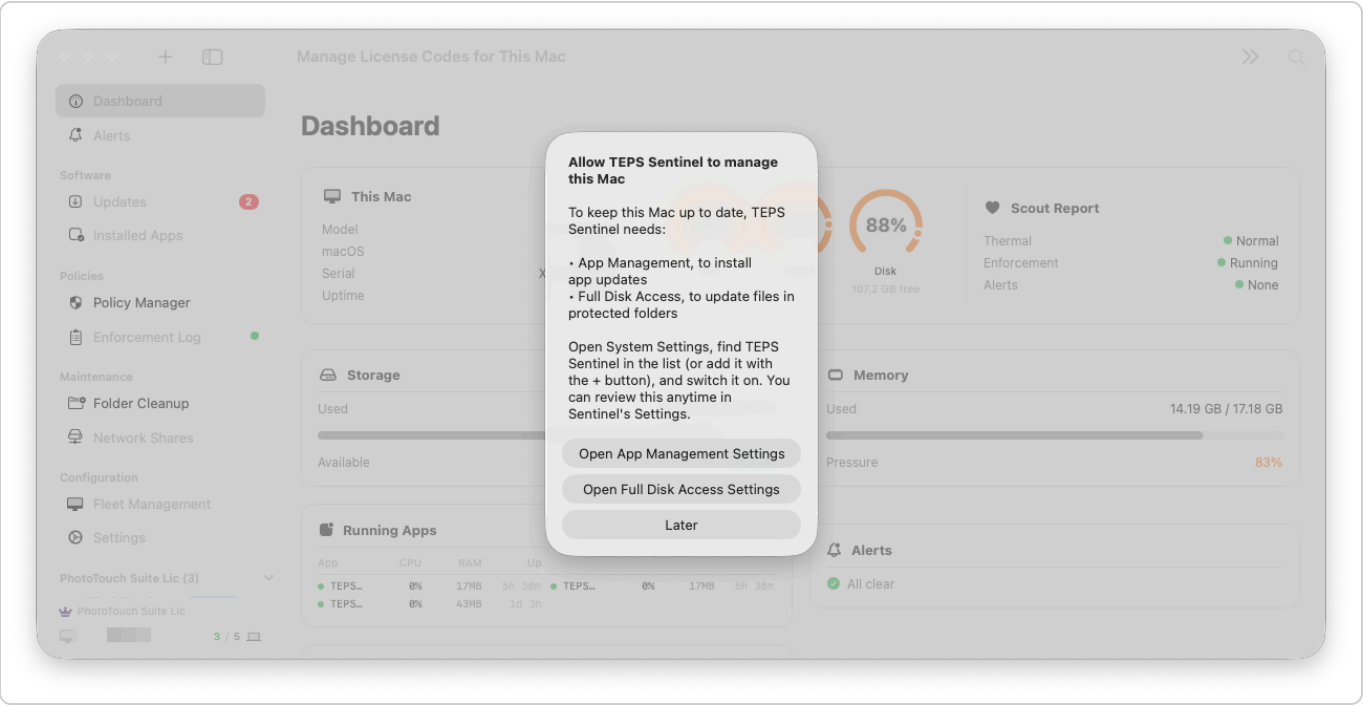
This guide takes one new Mac from first launch to fully managed, then covers the fleet features you'll use day to day. Sensitive values (serials, license keys, IP addresses, account codes) are pixelated in the screenshots.

Contents

---

1. First launch — the two macOS permissions

The first time Sentinel opens, it asks for the two permissions it needs to do its job:



Permission	Why Sentinel needs it
App Management	To install and update TEPS apps by replacing them in the Applications folder
Full Disk Access	To update files in protected folders, and to run folder cleanup anywhere on the disk

Click **Open App Management Settings** — macOS opens System Settings to the right pane. Find **TEPS Sentinel** in the list (if it isn't there, add it with the **+** button) and switch it on. Come back and repeat with **Open Full Disk Access Settings**.

You can press **Later** and grant them any time. Until both are granted, Sentinel reminds you in the menu bar (⚠ **Grant Full Disk Access…**) and shows the live status of each permission under **Settings** → **General** → **macOS Permissions**, where a green **Granted** badge confirms each one:

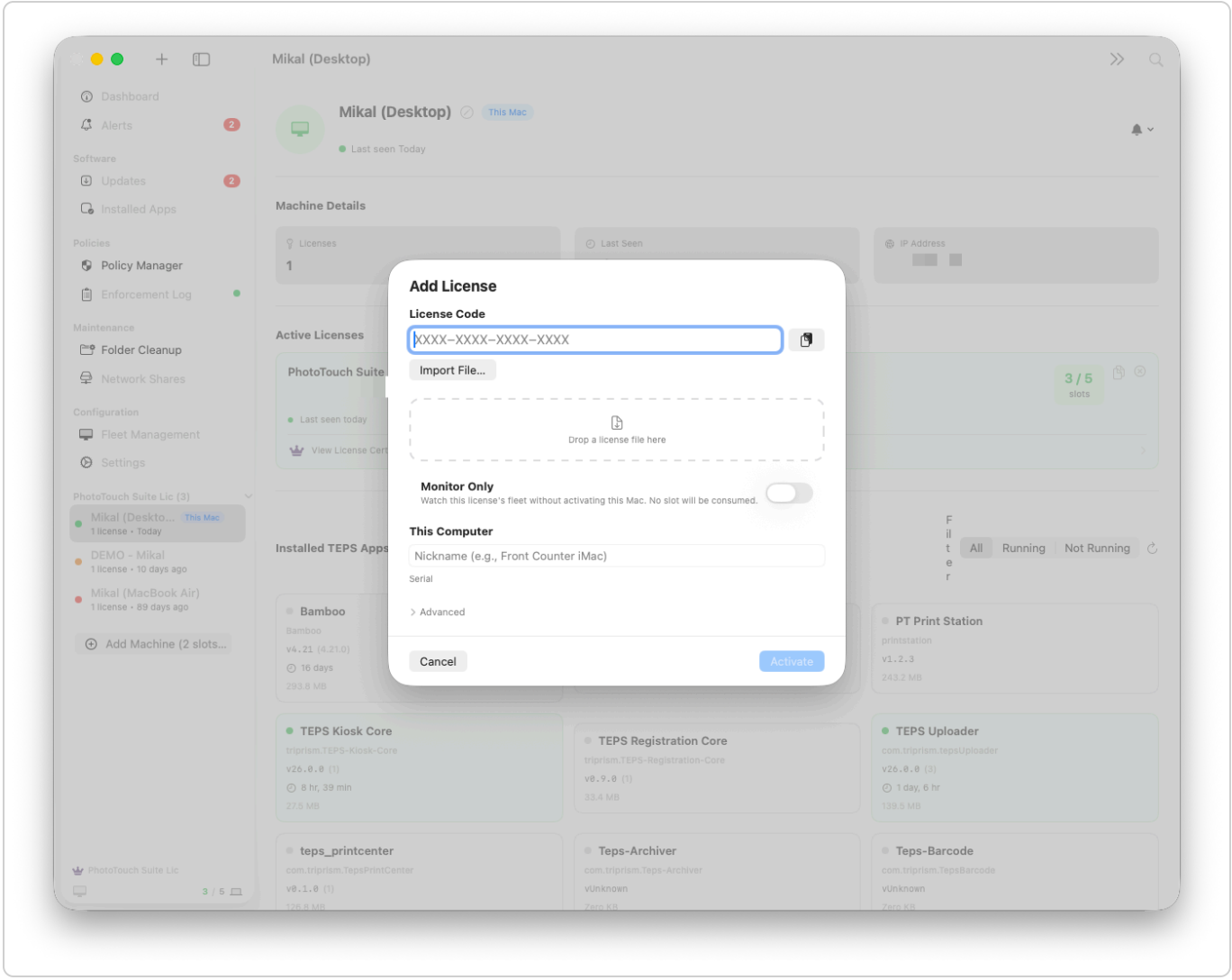
(see the bottom of the Settings → General screenshot in section 4)

One macOS quirk worth knowing: the App Management prompt only appears the first time Sentinel actually tries to update another app. Full Disk Access never prompts on its own — it must be switched on by hand in System Settings, which is why the app walks you there.

---

2. Activate a license

Choose **File** → **Add License…** or press ⌘**N**:



Three ways to get the license in:

1. **Type or paste the code** — the `XXXX–XXXX–XXXX–XXXX` code from your license email. The clipboard button to the right of the field pastes it in one click.
2. **Import File…** — pick the license file you were sent.
3. **Drag and drop** — drop the license file straight onto the dashed target.

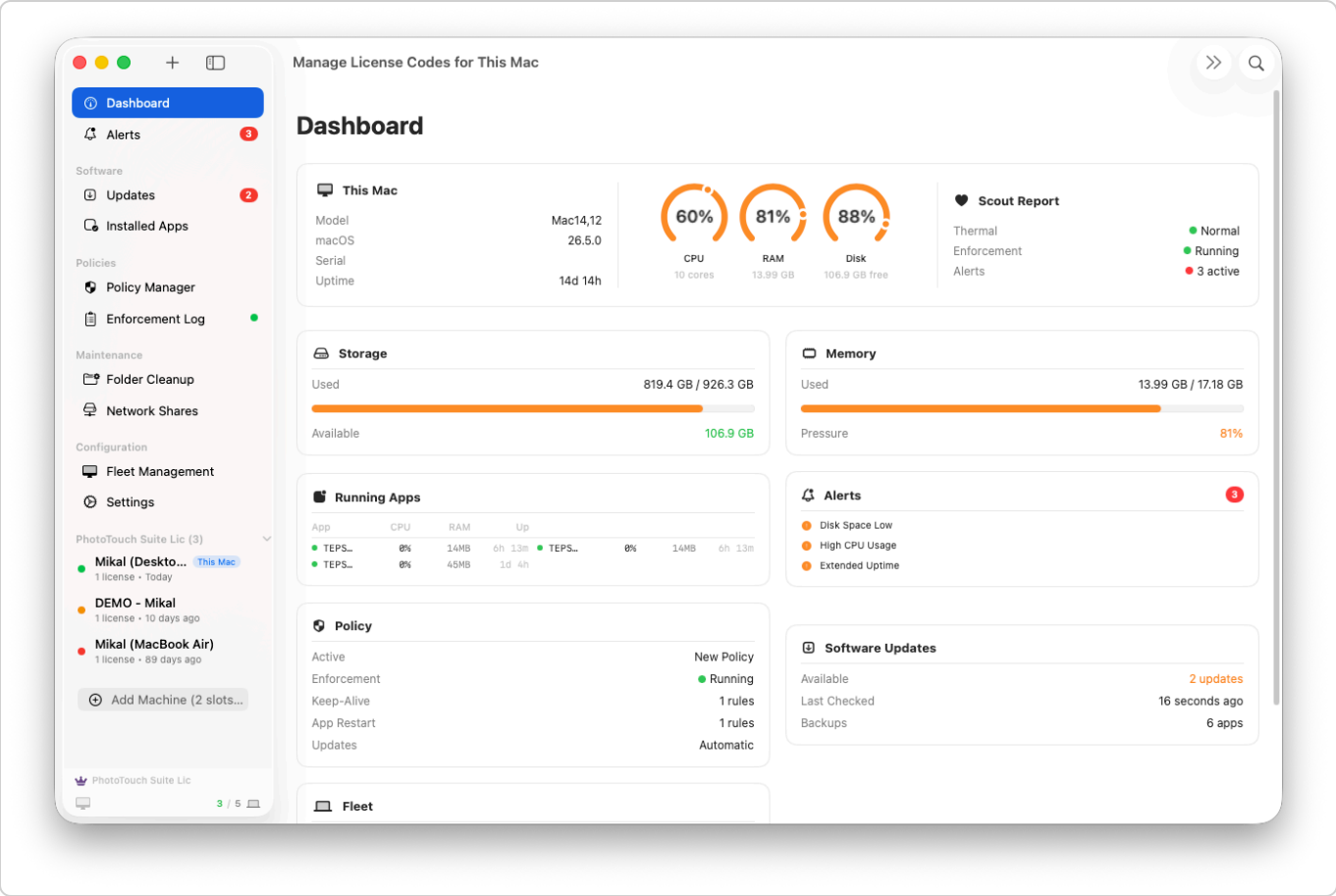
Under **This Computer**, give the Mac a **nickname** you'll recognize from across the room — "Front Counter iMac", "Kiosk 3" — because that's the name that shows up in the fleet list and in alerts. The serial number is read automatically.

Monitor Only deserves a callout: switch it on and this Mac *watches* the license's fleet — every machine, alert, and app — **without consuming a license slot**. That's the mode for your own office Mac when the slots belong to the venue machines doing the work.

Click **Activate**. The license appears at the bottom of the sidebar with its machines under it (section 13).

---

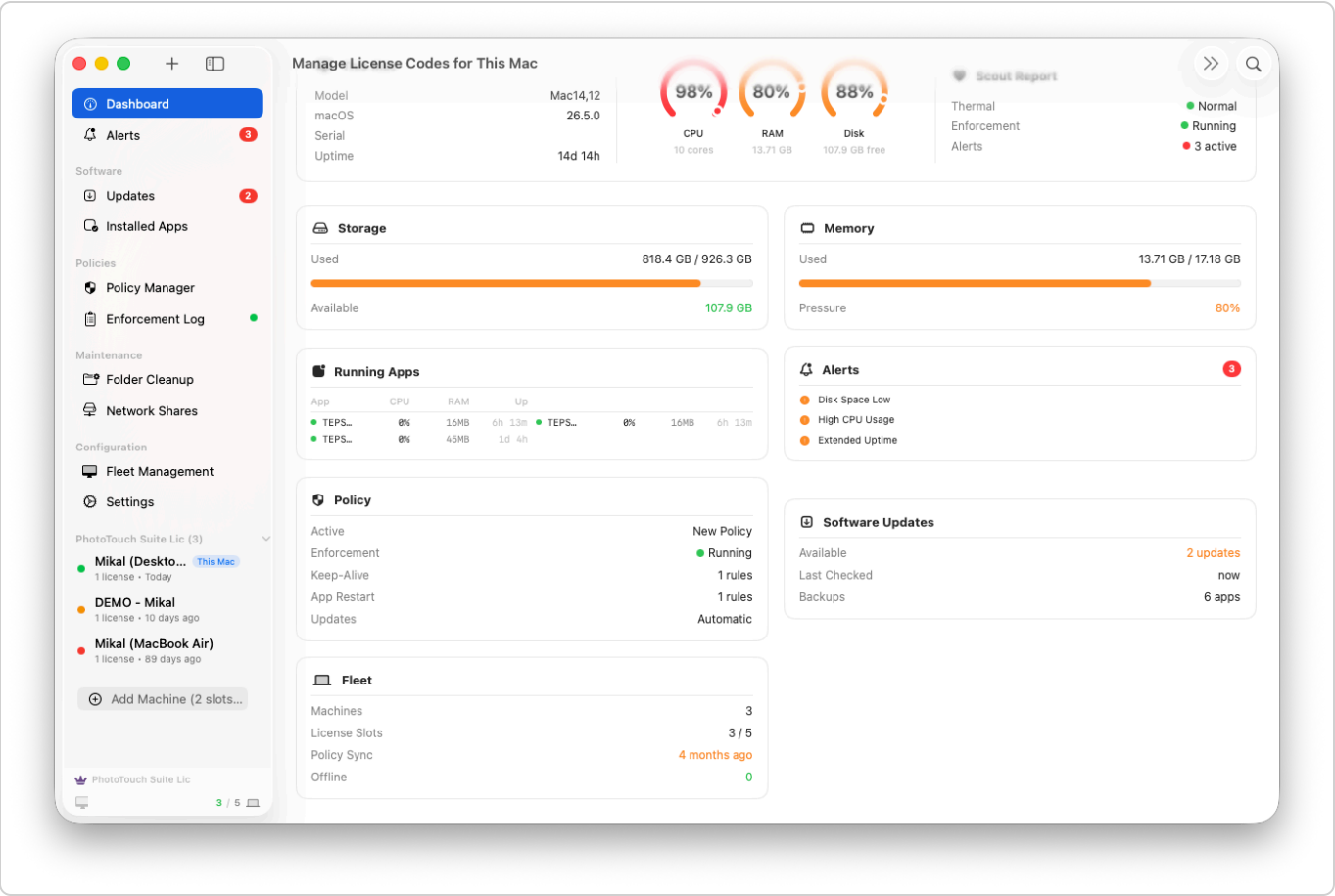
3. The Dashboard — reading a machine at a glance



The top half is the machine's vital signs:

- **This Mac** — model, macOS version, serial, and uptime. Uptime matters: machines that run for weeks without a restart drift, and Sentinel raises an *Extended Uptime* alert when one goes too long (you can see one in the Alerts card here — the machine's been up 14 days).
- **CPU / RAM / Disk gauges** — current load, memory in use, and disk free. They go orange as they climb.
- **Scout Report** — the summary this Mac sends to the fleet: thermal state, whether enforcement is running, and how many alerts are active.
- **Storage and Memory** — the same disk and RAM numbers in detail, including **memory pressure**, which is the better "is this Mac struggling" signal than raw usage.
- **Running Apps** — every TEPS app currently running, with its CPU, RAM, and how long it's been up.
- **Alerts** — the active alerts, duplicated from the Alerts view so you don't have to leave the Dashboard to see them.

Scroll down for the management summary:



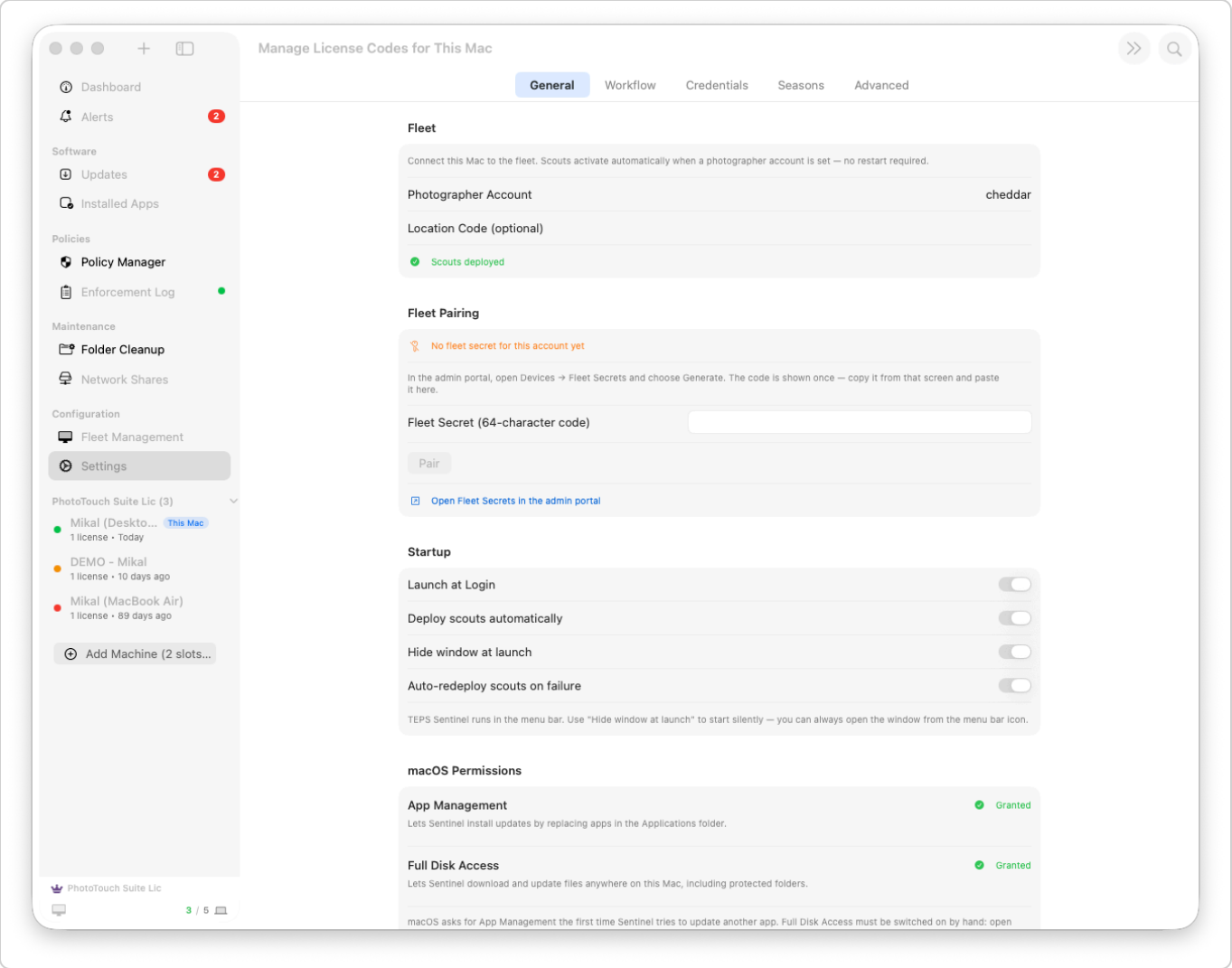
- **Policy** — which policy governs this Mac, whether enforcement is **Running**, and how many keep-alive and app-restart rules are live, plus the update mode (here: Automatic).
- **Software Updates** — how many updates are waiting, when Sentinel last checked, and how many app backups it's holding for rollback.
- **Fleet** — the whole fleet in four numbers: machines, license slots used, when policies last synced, and how many machines are offline.

If a card reads wrong — enforcement not running, policy sync months old, offline > 0 — the card names the view to go fix it in.

---

4. Connect to your fleet (Settings → General)

Open **Settings** in the sidebar. The **General** tab is where a machine joins the fleet:



Fleet — set the **Photographer Account** this Mac works under, and optionally a **Location Code** if you use location-based rules. Scouts activate automatically the moment the photographer account is set; no restart needed. The green **Scouts deployed** badge confirms it.

Fleet Pairing — this is the one step that needs the admin portal:

1. In the admin portal, open **Devices** → **Fleet Secrets** and choose **Generate**.
2. The 64-character code is shown **once** — copy it from that screen.
3. Paste it into the **Fleet Secret** field here and click **Pair**.

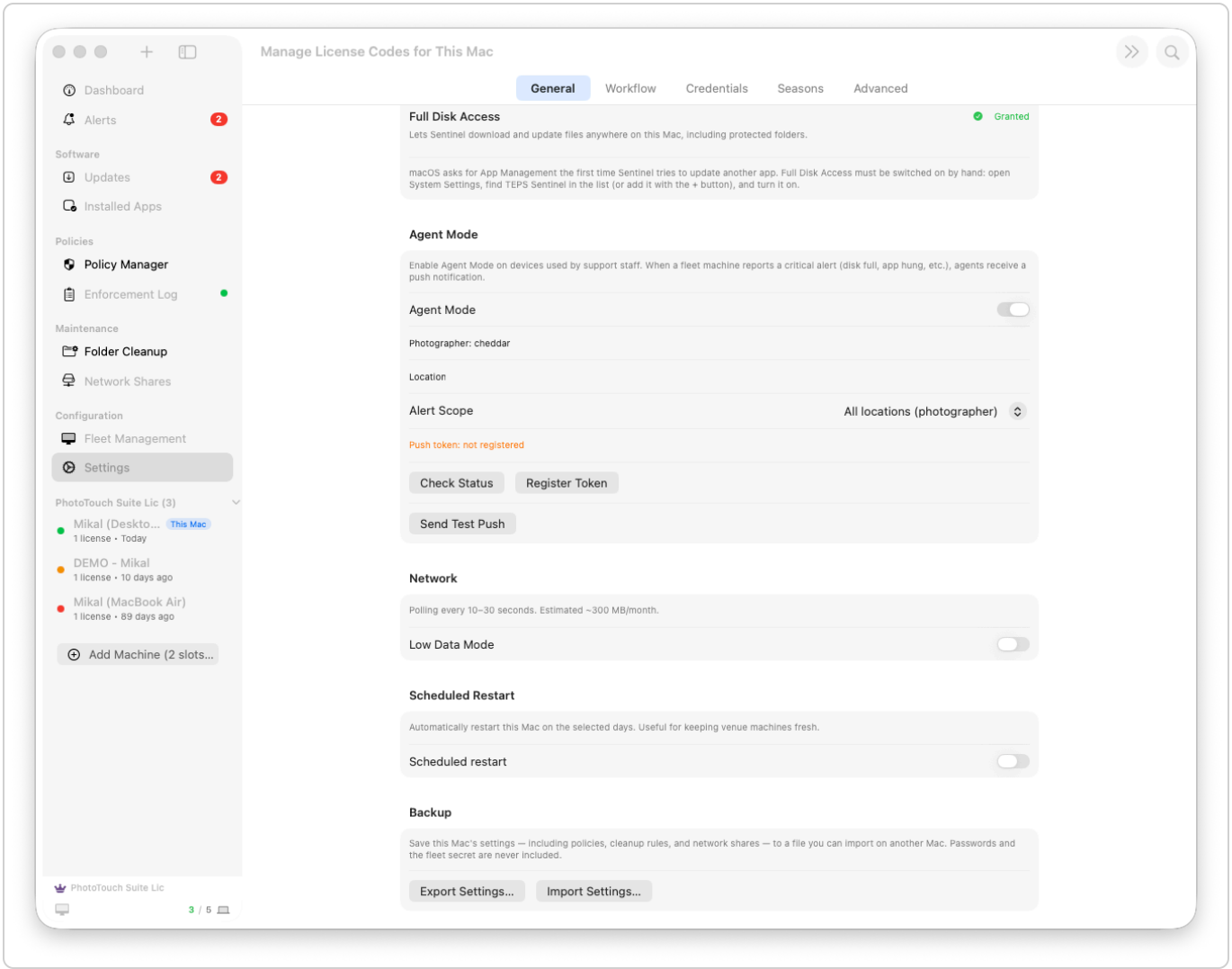
The **Open Fleet Secrets in the admin portal** link takes you straight to the right page. Until you pair, the orange "No fleet secret for this account yet" notice stays put.

Startup — four switches that decide how Sentinel behaves on login:

Switch	What it does
Launch at Login	Starts Sentinel automatically — turn this on for any managed machine
Deploy scouts automatically	Re-arms fleet reporting on every launch
Hide window at launch	Starts silently in the menu bar — right for kiosks; the window is always one menu-bar click away
Auto-redeploy scouts on failure	If a scout dies, put it back without waiting for someone to notice

macOS Permissions — the live status of App Management and Full Disk Access from section 1, each with a **Granted** badge when it's in place.

Scroll down for the rest of General:



Agent Mode — for Macs used by *support staff* rather than venue machines. When any fleet machine reports a critical alert (disk full, app hung, machine offline), agents get a **push notification**. Set the photographer and location it watches, choose the **Alert Scope** (all locations or just one), then **Register Token** and **Send Test Push** to prove the pipe works before you rely on it. **Check Status** shows whether the push token is registered.

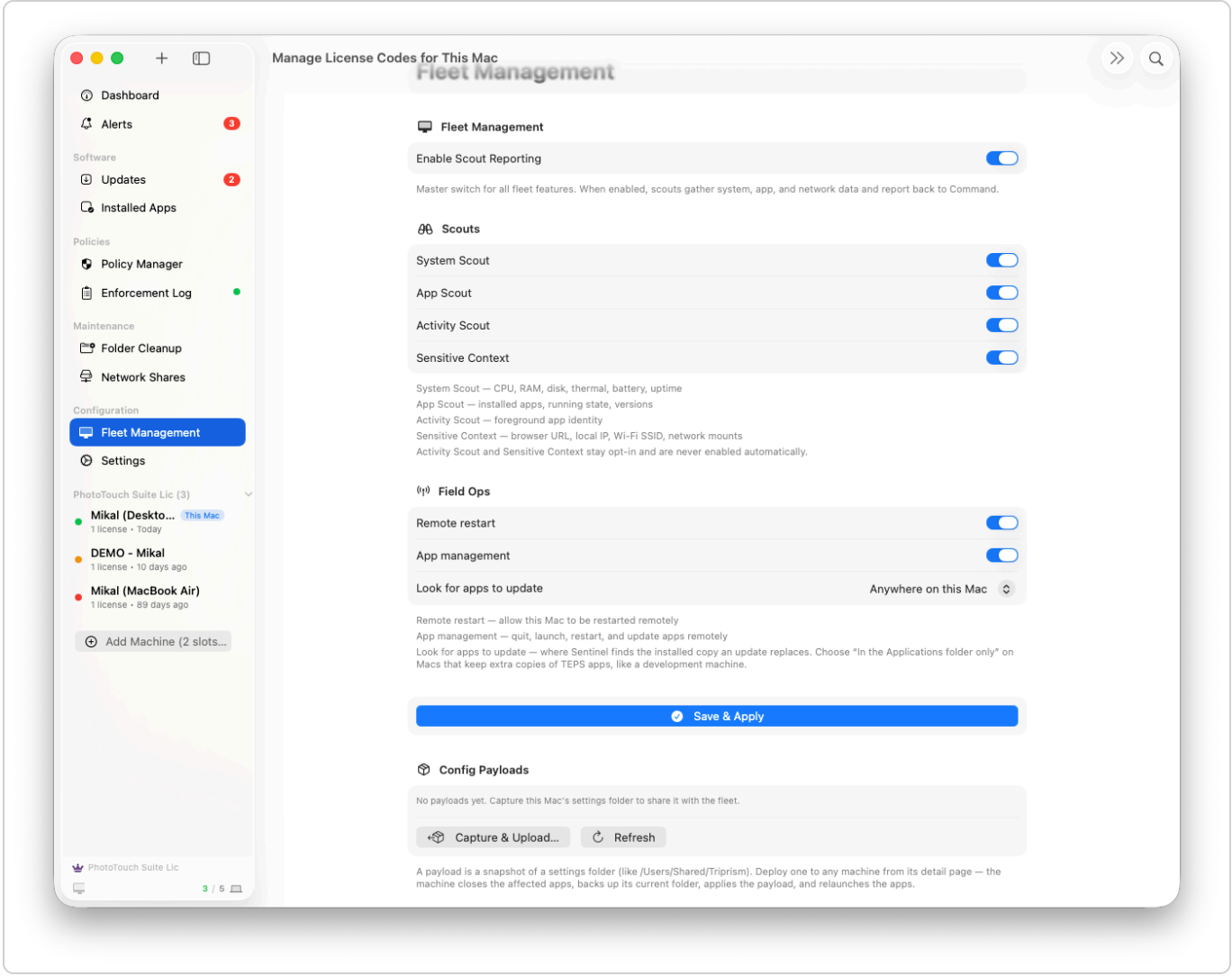
Network — Sentinel polls every 10–30 seconds (roughly 300 MB/month). **Low Data Mode** stretches the interval for machines on metered or weak connections.

Scheduled Restart — restart *this* Mac on selected days. (Fleet-wide restart schedules belong in a policy — section 6. This local switch is for a one-off machine.)

Backup — **Export Settings…** writes this Mac's whole setup — policies, cleanup rules, network shares — to a file you can **Import** on the next Mac you set up. Passwords and the fleet secret are deliberately never included, so the file is safe to keep on a shared drive.

---

5. Choose what this Mac reports (Fleet Management)



Enable Scout Reporting is the master switch — off means this Mac reports nothing.

Scouts are the four reporters, each with its own switch:

Scout	Reports	Notes
System Scout	CPU, RAM, disk, thermal, battery, uptime	The basics — leave it on
App Scout	Installed apps, running state, versions	Feeds the fleet app views
Activity Scout	Which app is in the foreground	**Opt-in, never auto-enabled**
Sensitive Context	Browser URL, local IP, Wi-Fi SSID, network mounts	**Opt-in, never auto-enabled**

Turn the last two on only where that visibility is appropriate — kiosks and venue machines, not staff laptops.

Field Ops — what the fleet is allowed to do *to* this Mac remotely:

- **Remote restart** — allow this Mac to be restarted from the fleet.
- **App management** — quit, launch, restart, and update apps remotely.
- **Look for apps to update** — where Sentinel searches for the installed copy an update replaces. **Anywhere on this Mac** is the default; choose **In the Applications folder only** on Macs that keep extra copies of TEPS apps around — like a development machine — so an update never touches a build product.

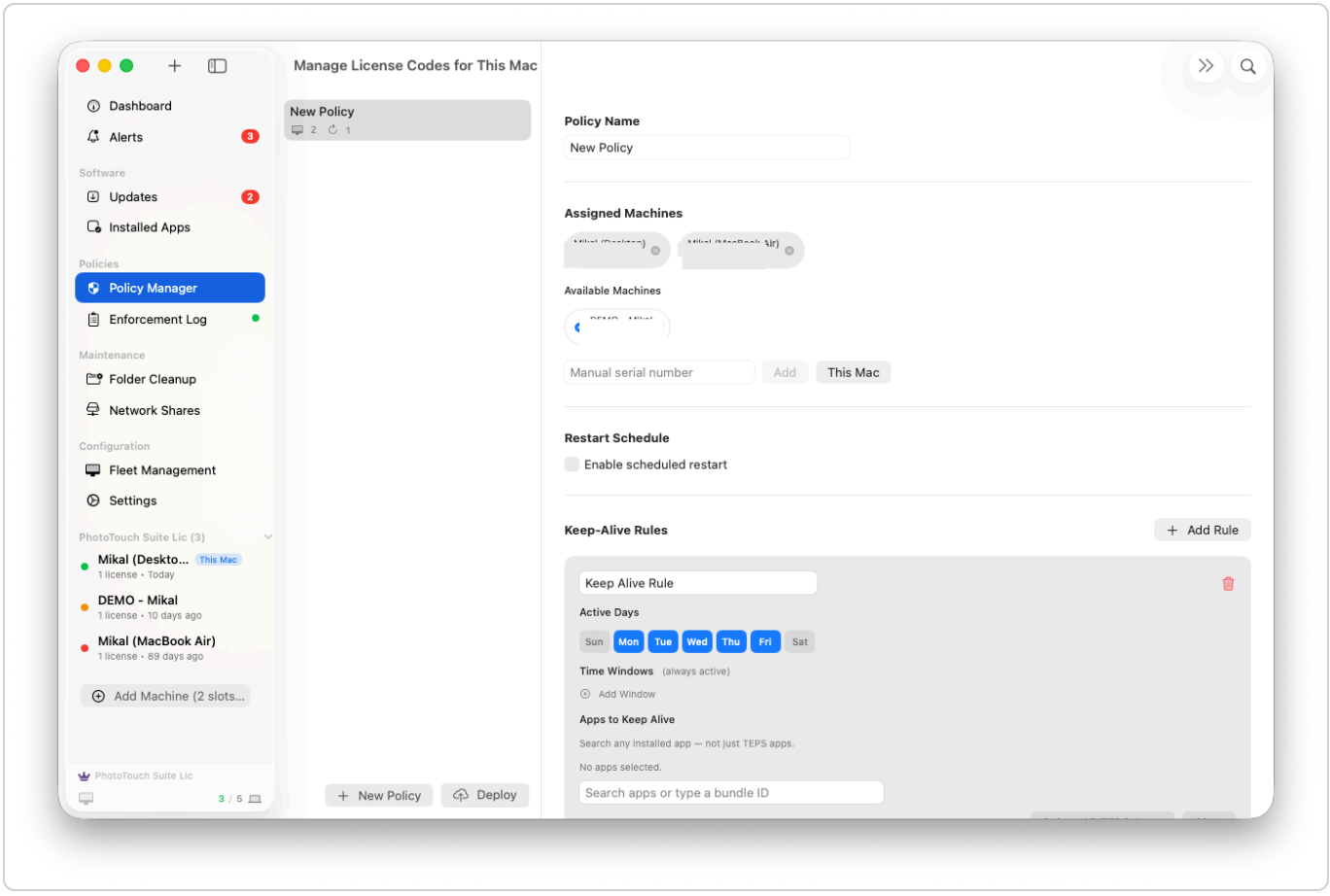
Press **Save & Apply** after changing anything here.

Config Payloads — a payload is a snapshot of this Mac's settings stored with the fleet. **Capture & Upload** saves the current state; **Reload** pulls the stored one back down. It's the mechanism behind "set up one machine, push it to the rest."

---

6. Build a policy (Policy Manager)

Policies are the heart of Sentinel: one set of rules, enforced identically on every machine you assign. You configure them once, press Deploy, and stop touching individual Macs.



The left column lists your policies with **+ New Policy** and **Deploy** at the bottom. The editor fills the right side, top to bottom:

Policy Name — name it for what it governs ("Venue Kiosks", "Print Stations").

Assigned Machines — the chips are machines this policy governs; click the ⊗ on a chip to unassign. Below, **Available Machines** lists fleet machines not yet assigned — click one to assign it. You can also type a **manual serial number** for a machine that hasn't enrolled yet, or press **This Mac** to assign the machine you're sitting at.

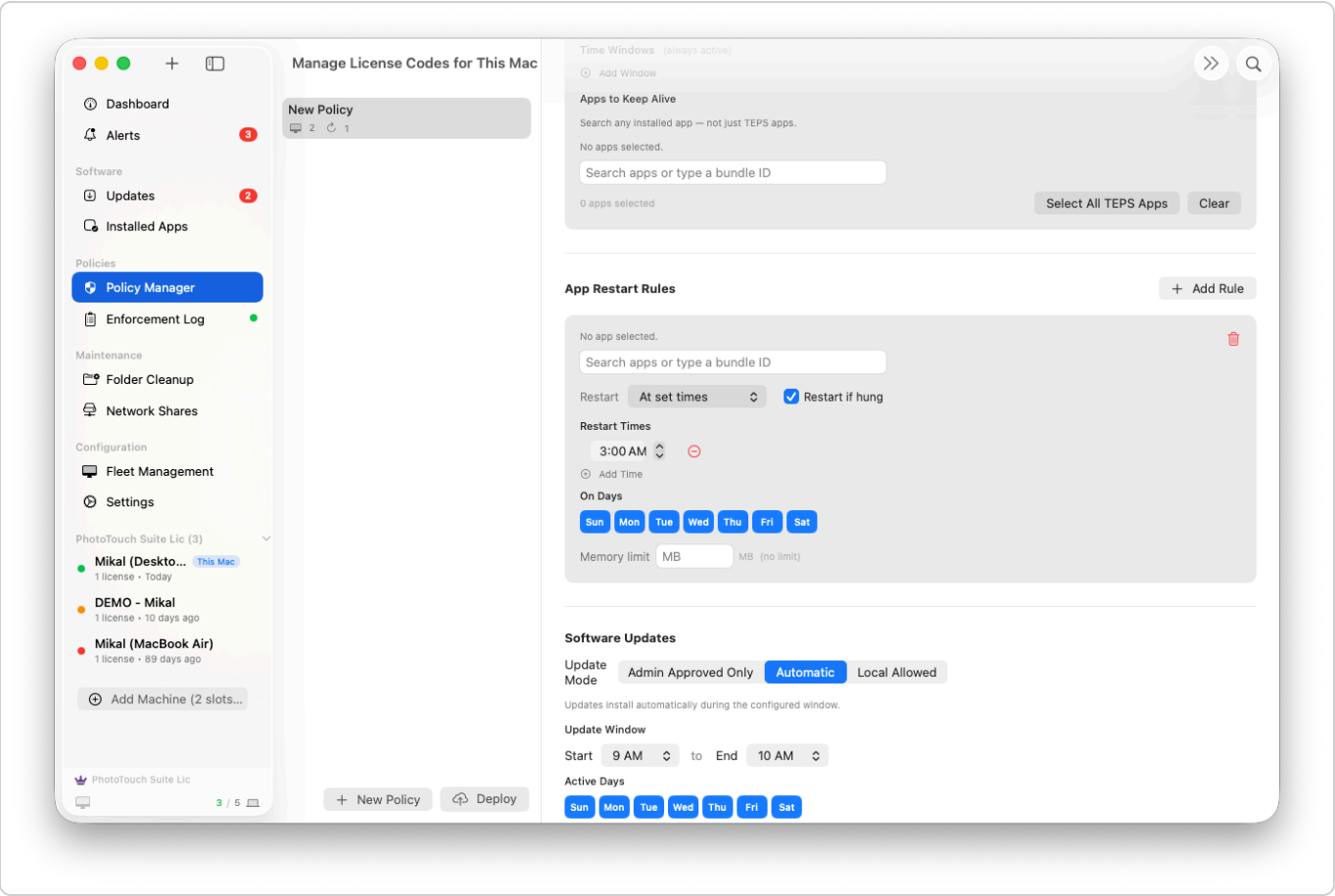
Restart Schedule — tick **Enable scheduled restart** to restart every assigned machine at set times on chosen days. Venue machines stay fresh without anyone remembering to bounce them.

Keep-Alive Rules — the "this app must always be running" rules. **+ Add Rule**, then per rule:

- **Active Days** — which days the rule enforces (the blue chips).
- **Time Windows** — *always active* by default, or ⊕ **Add Window** to enforce only during show hours.
- **Apps to Keep Alive** — search **any installed app, not just TEPS apps**, or press **Select All TEPS Apps** to cover the whole suite in one click.

If the app quits — crash, accidental ⌘Q, whatever — Sentinel relaunches it within the rule's window and writes what it did to the Enforcement Log.

Scroll down for the next sections:



App Restart Rules — different from keep-alive: these *proactively restart* an app to keep it healthy. Per rule:

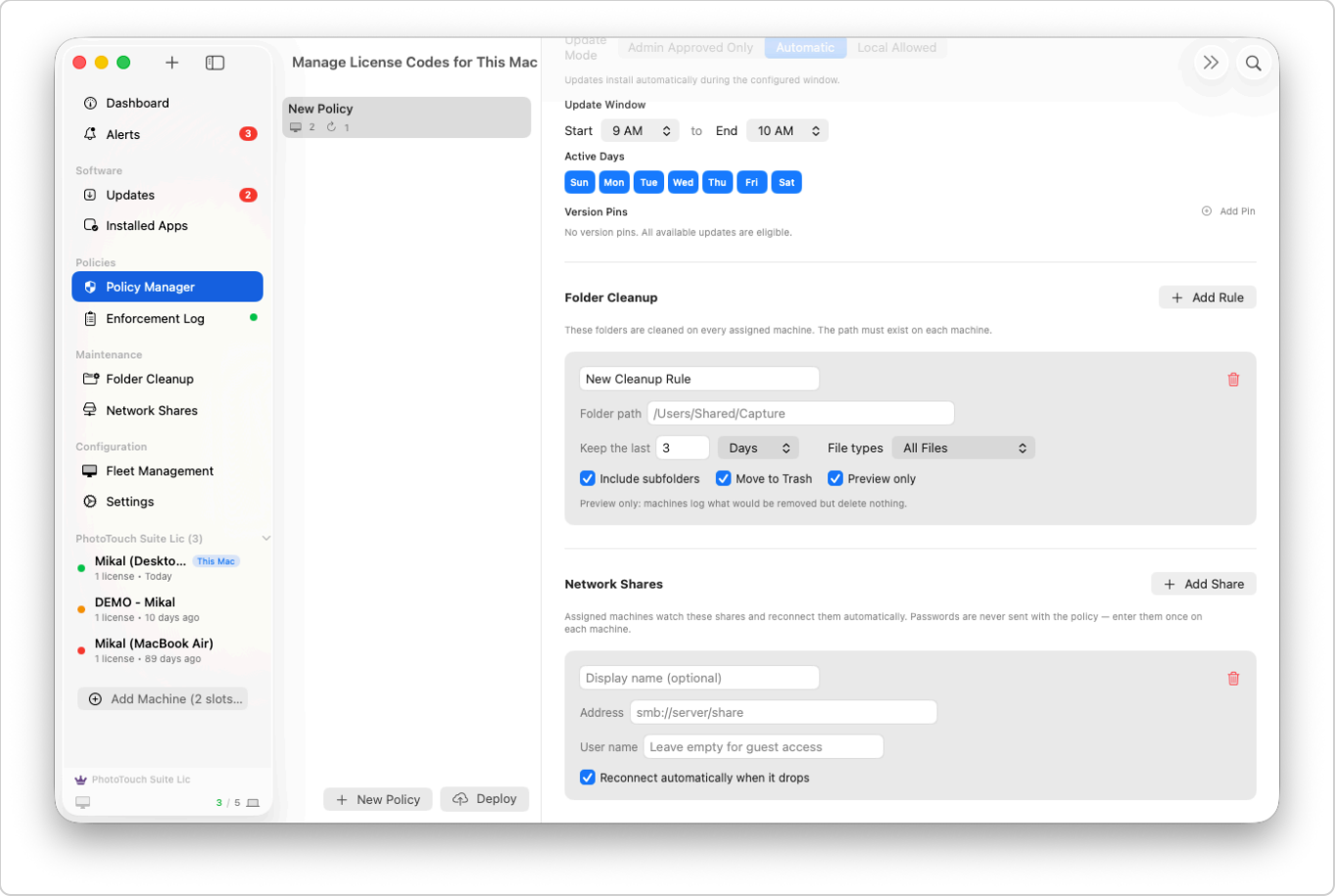
- Pick the app (same search), then choose when: **At set times** (here 3:00 AM, and ⊕ **Add Time** for more) on the chosen **days**.
- **Restart if hung** — restart the app whenever it stops responding, independent of the schedule.
- **Memory limit** — restart the app if it grows past this many MB. Long-running photo apps that leak memory get bounced before they take the machine down.

Software Updates — how updates install on assigned machines:

Mode	Meaning
Admin Approved Only	Nothing installs until you approve it from the fleet
Automatic	Updates install on their own during the window below
Local Allowed	Someone at the machine may also install updates

The **Update Window** (here 9–10 AM on all days) confines automatic installs to hours when a restart of an app won't interrupt a job.

Version Pins — ⊕ **Add Pin** to freeze an app at a version. Pinned machines ignore newer releases until you remove the pin; unpinned, every available update is eligible.



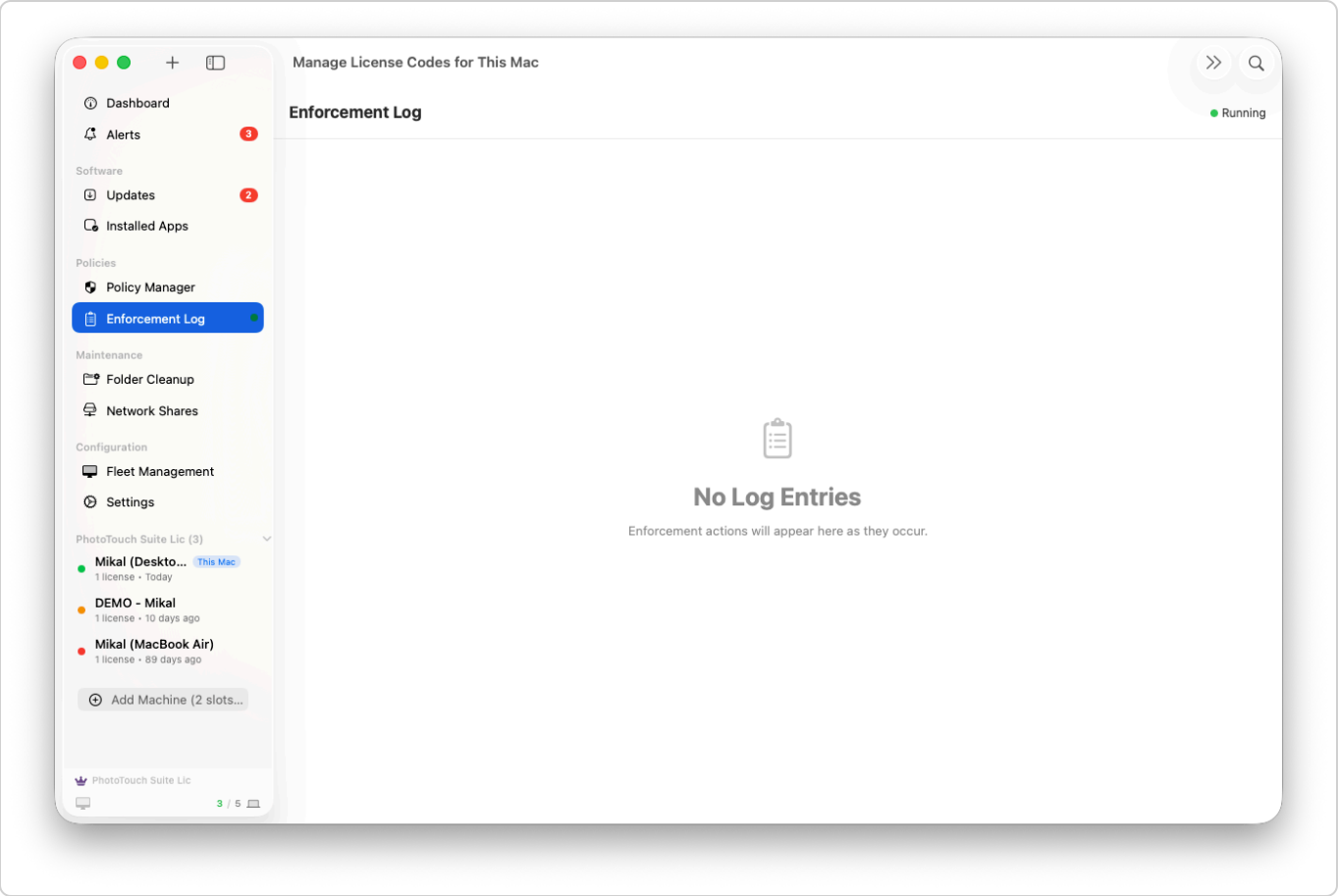
Folder Cleanup (policy-level) — cleanup rules that run **on every assigned machine**. The path must exist on each machine. Per rule: the folder path, **keep the last N days**, **file types**, **include subfolders**, **move to Trash** (vs. delete), and — important — **Preview only**, which logs what *would* be removed without deleting anything. Deploy new cleanup rules in preview, read the logs for a few days, then turn preview off.

Network Shares (policy-level) — shares every assigned machine should keep mounted: display name, address (`smb://server/share`), user name (leave empty for guest access), and **reconnect automatically when it drops**. **Passwords are never sent with the policy** — you enter them once on each machine, and only the address and user name travel.

When the policy reads right, press **Deploy** to push it to the fleet.

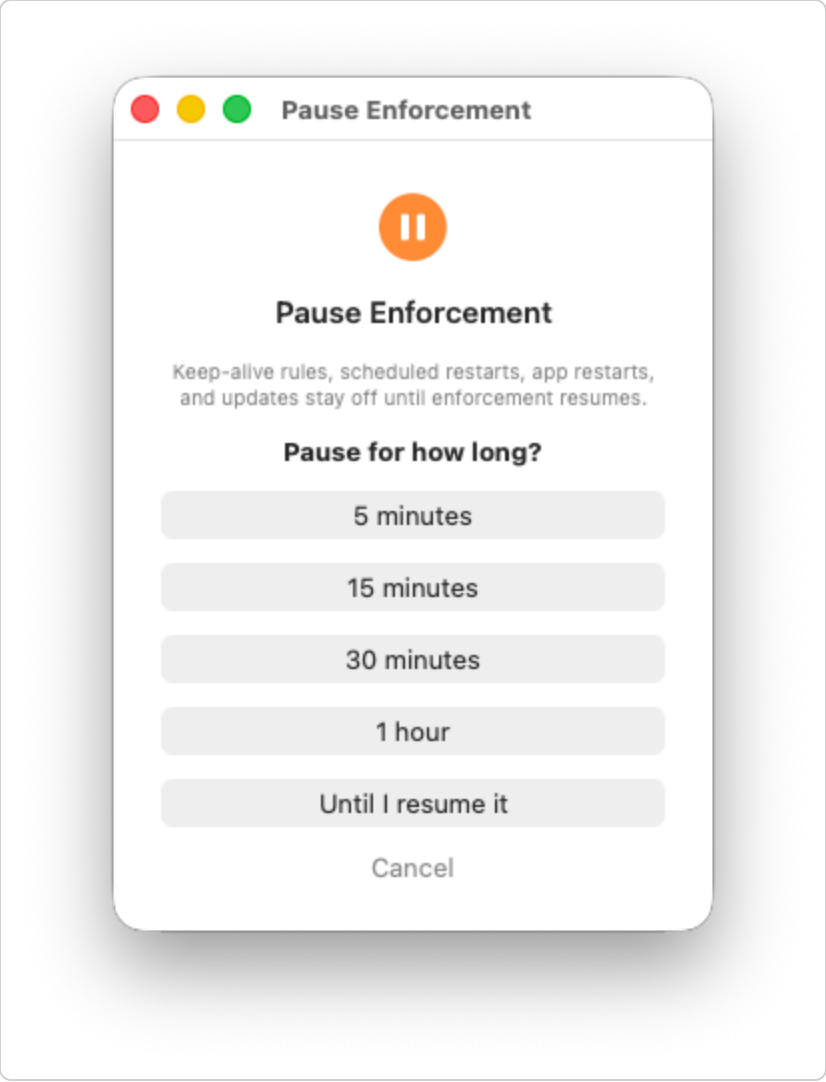
---

7. The Enforcement Log and pausing enforcement



Every action a policy takes — an app relaunched, a scheduled restart, a hung app bounced — lands here with a timestamp. A fresh machine shows *No Log Entries*; the green **Running** badge in the corner is the thing to check — it means enforcement is alive.

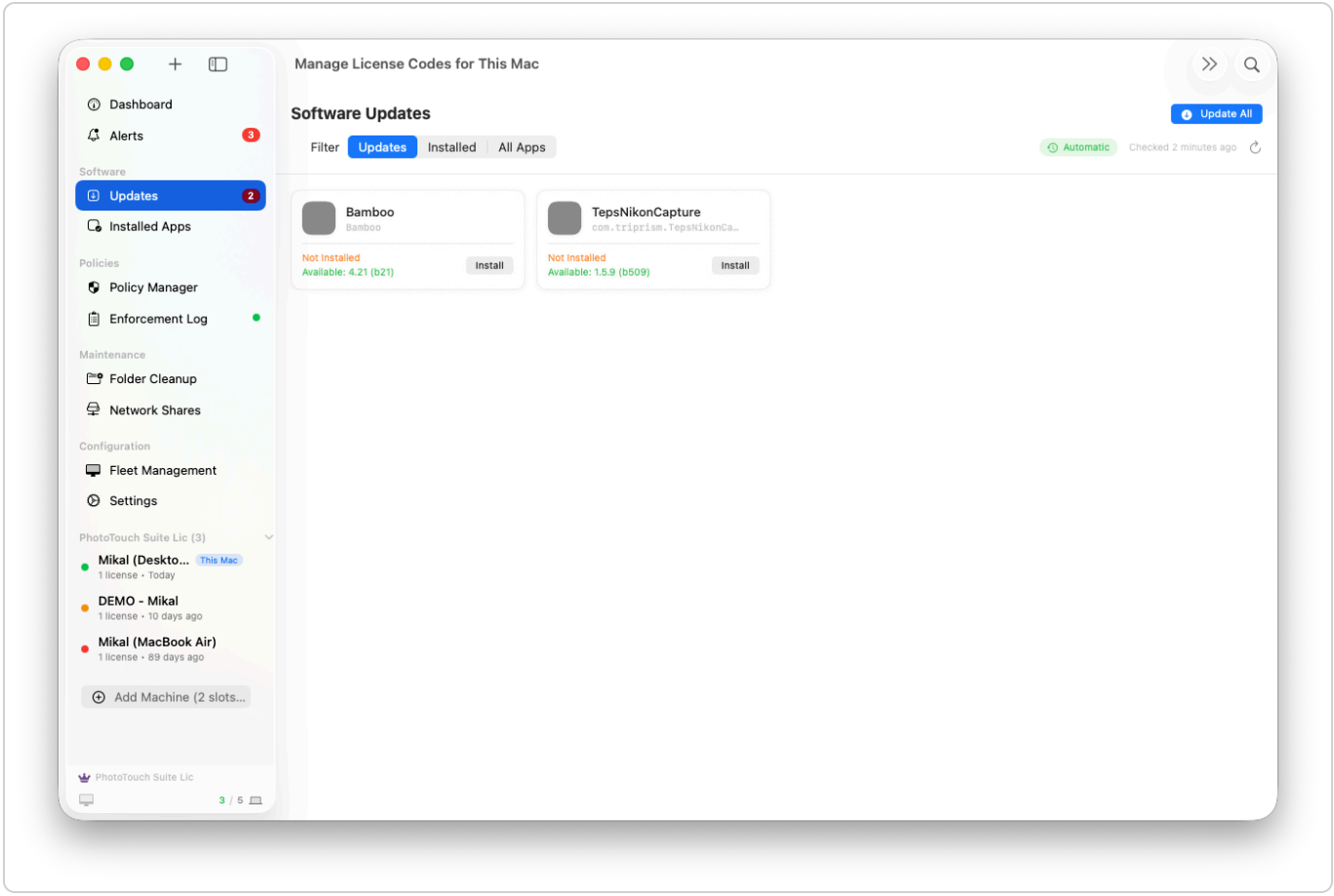
When you need enforcement out of the way — training someone on a kiosk, debugging a machine — don't turn rules off. Use **Enforcement** → **Pause Enforcement…** (also in the menu bar icon):



Keep-alive rules, scheduled restarts, app restarts, and updates all stay off until the pause ends — and every duration except *Until I resume it* resumes **by itself**, so a pause can't quietly become "enforcement has been off for a month." The durations offered here are configurable (Settings → Advanced → Pause Durations, section 15), and you can require a password to pause at all.

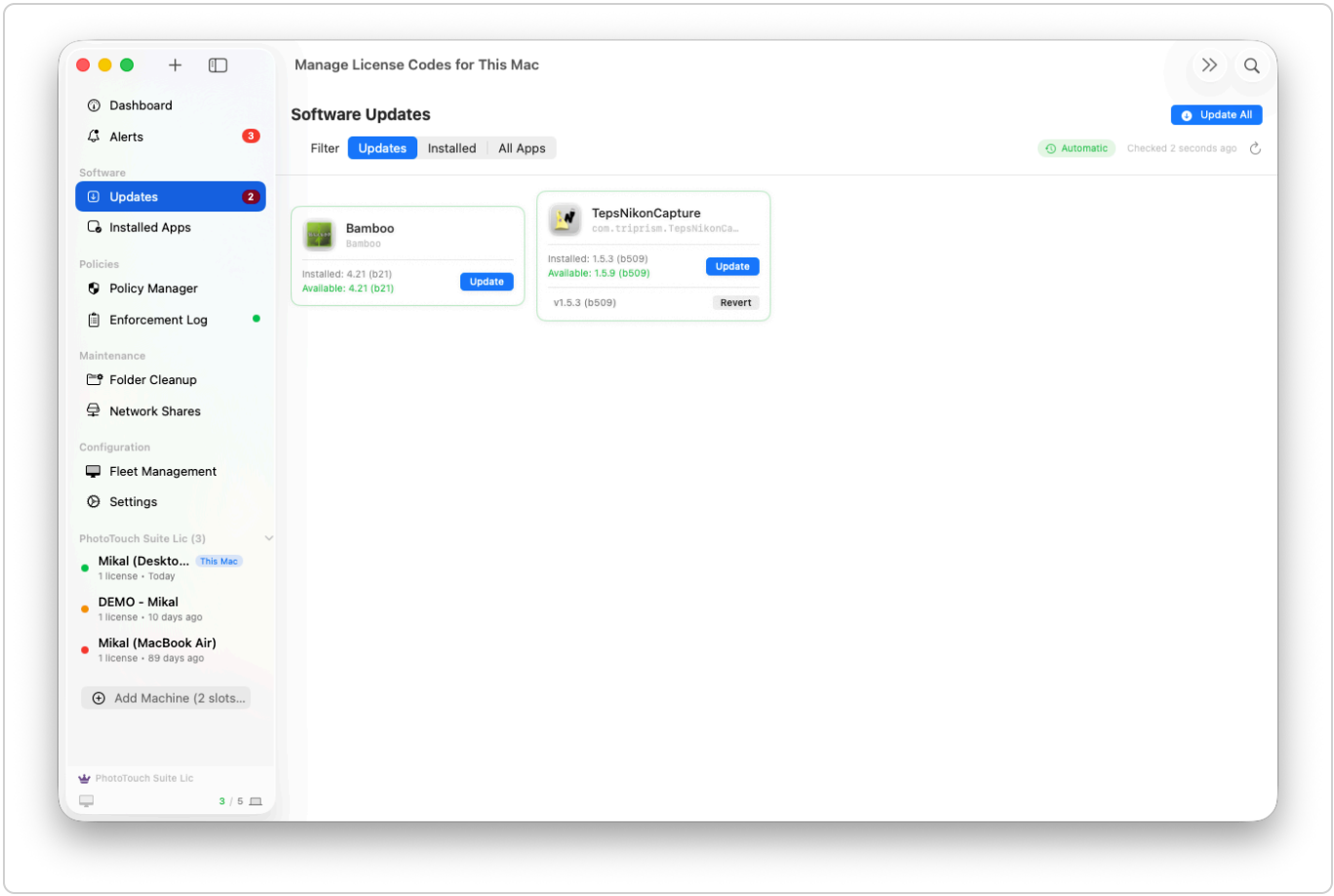
---

8. Software Updates



The **Updates** filter shows what needs action: apps with a newer version available, and apps that *should* be installed on this Mac but aren't (marked **Not Installed** in orange). **Install** / **Update** handles one app; **Update All** does the lot. The **Automatic** badge next to the checked-time confirms this Mac installs updates on its own (that mode comes from the policy — section 6).

After an update installs, the card keeps the previous version on hand:

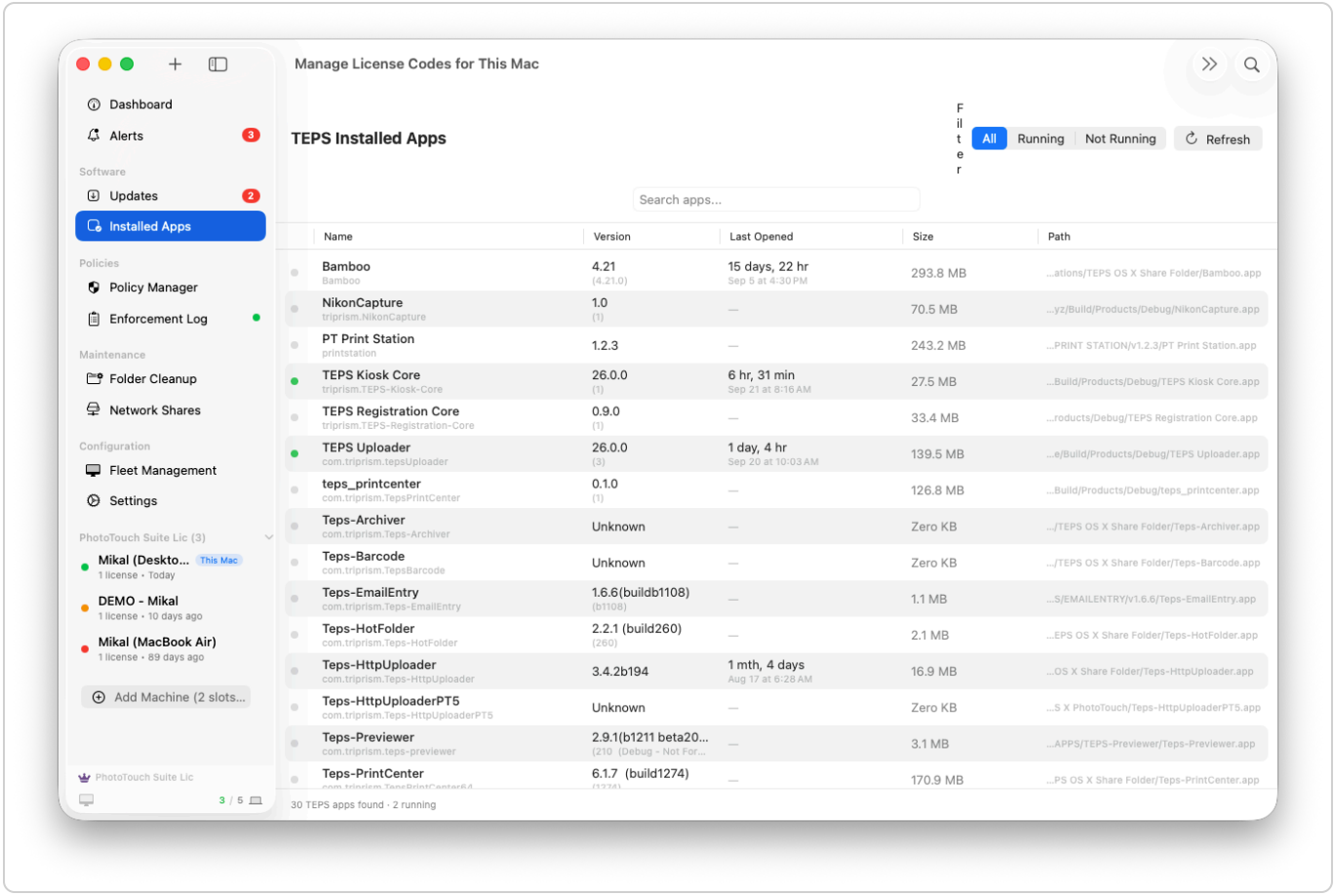


Revert rolls the app back to the version you were on before — the escape hatch when a new release misbehaves mid-season. The **Backups** count on the Dashboard's Software Updates card tells you how many of these rollback copies Sentinel is holding.

The **Installed** and **All Apps** filters show the same cards for everything already current, and everything Sentinel knows about, respectively.

---

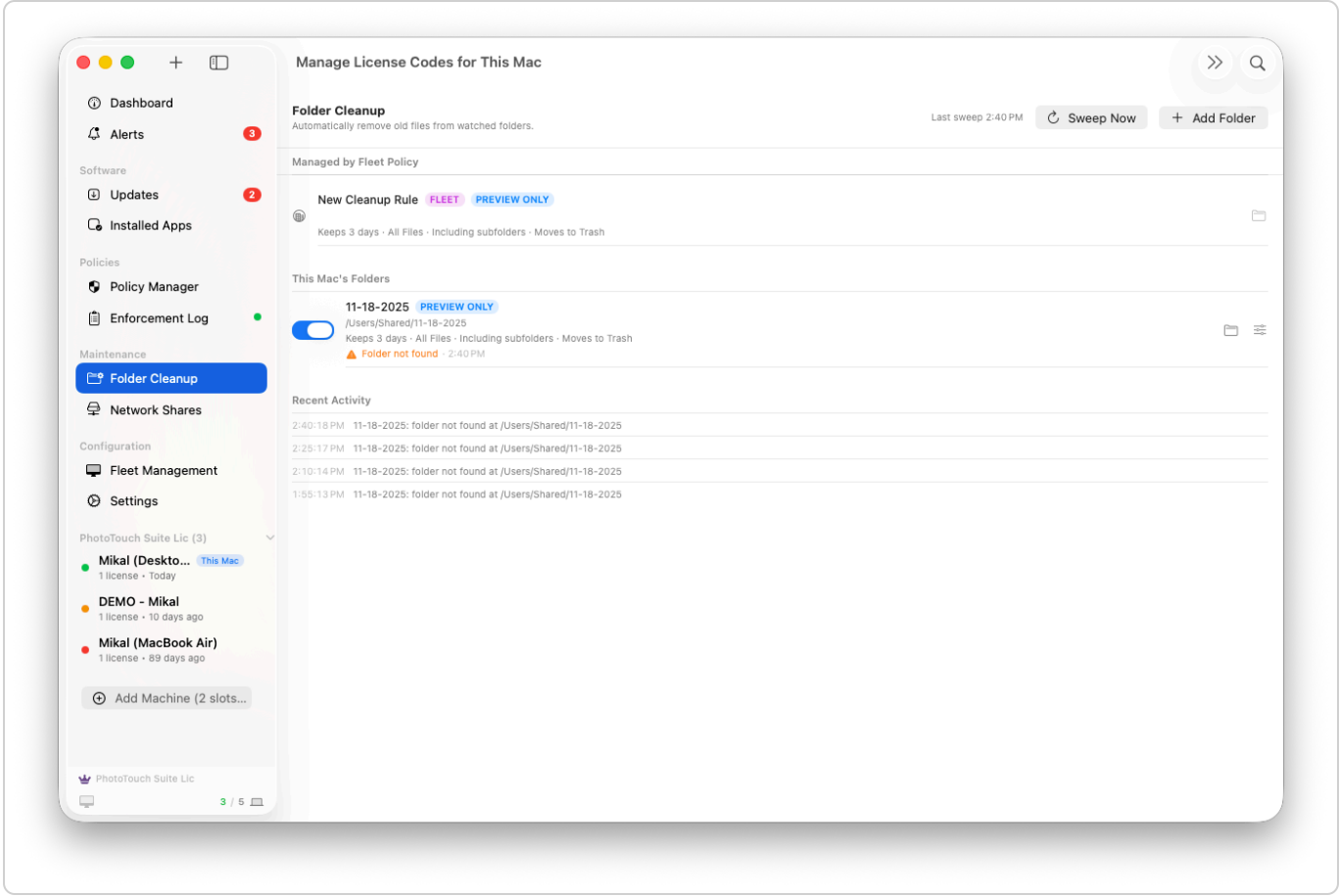
9. Installed Apps



Every TEPS app on this Mac in one table: **version**, **last opened**, **size**, and the **install path** (the path column is how you spot a copy running out of a build folder or a share instead of Applications). A green dot means running right now. Filter by **All / Running / Not Running**, search by name, and **Refresh** to rescan.

---

10. Folder Cleanup on this Mac



Two groups of rules:

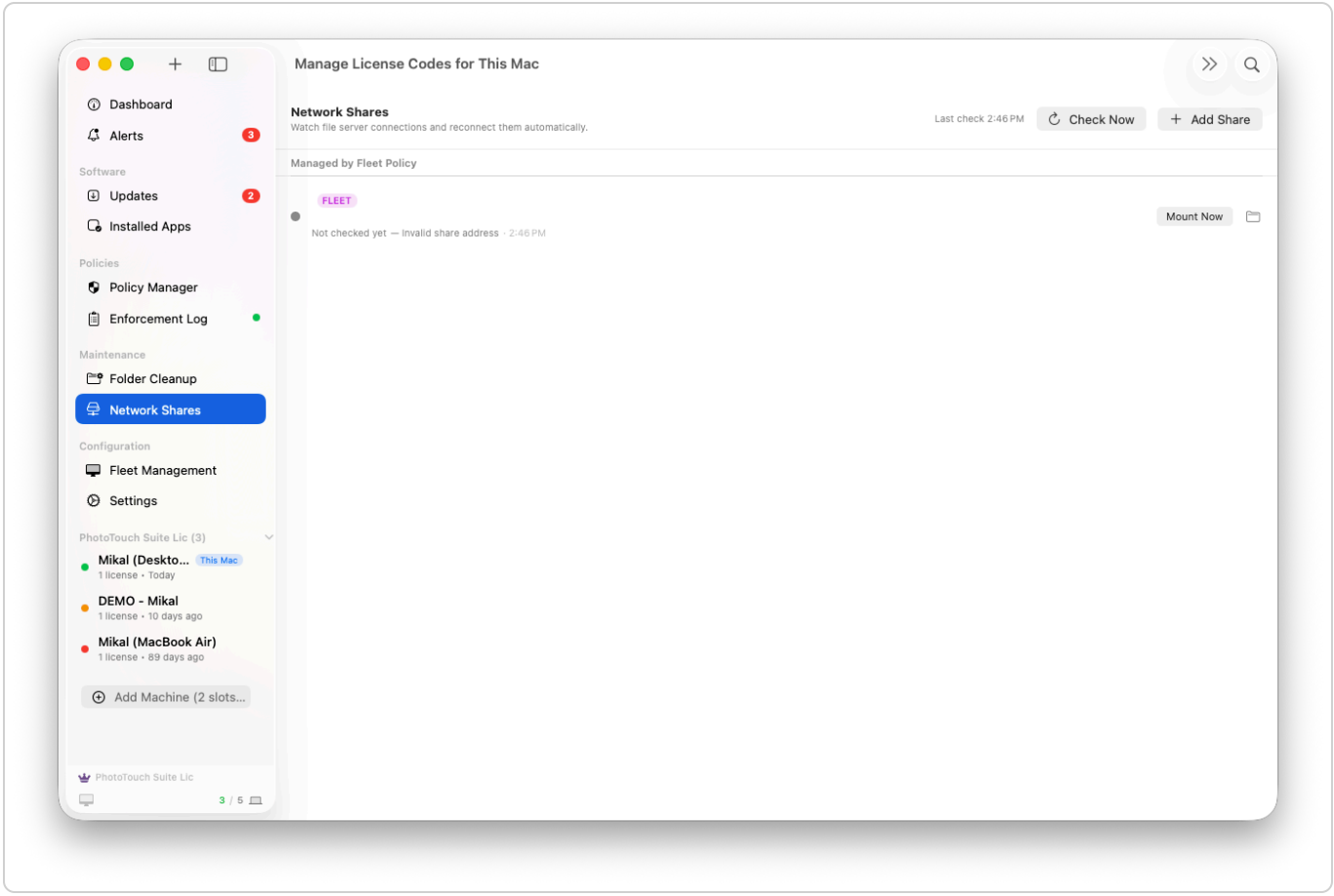
- **Managed by Fleet Policy** — rules that arrived with the policy, marked **FLEET**. You can read them here but they're edited in the Policy Manager.
- **This Mac's Folders** — local rules, added with **+ Add Folder**: pick the folder, how many days to keep files, file types, whether subfolders count, and Trash vs. delete.

Each rule shows its settings on one line and has an on/off toggle, an open-in-Finder button, and an options menu. The **PREVIEW ONLY** badge means the rule logs what it would remove but deletes nothing — the safe way to run a new rule until you trust it.

Sweep Now runs all rules immediately instead of waiting for the schedule. **Recent Activity** is the receipt: every sweep, what it removed (or would have), and warnings — here the orange *Folder not found* tells you the target path doesn't exist on this Mac.

---

11. Network Shares on this Mac

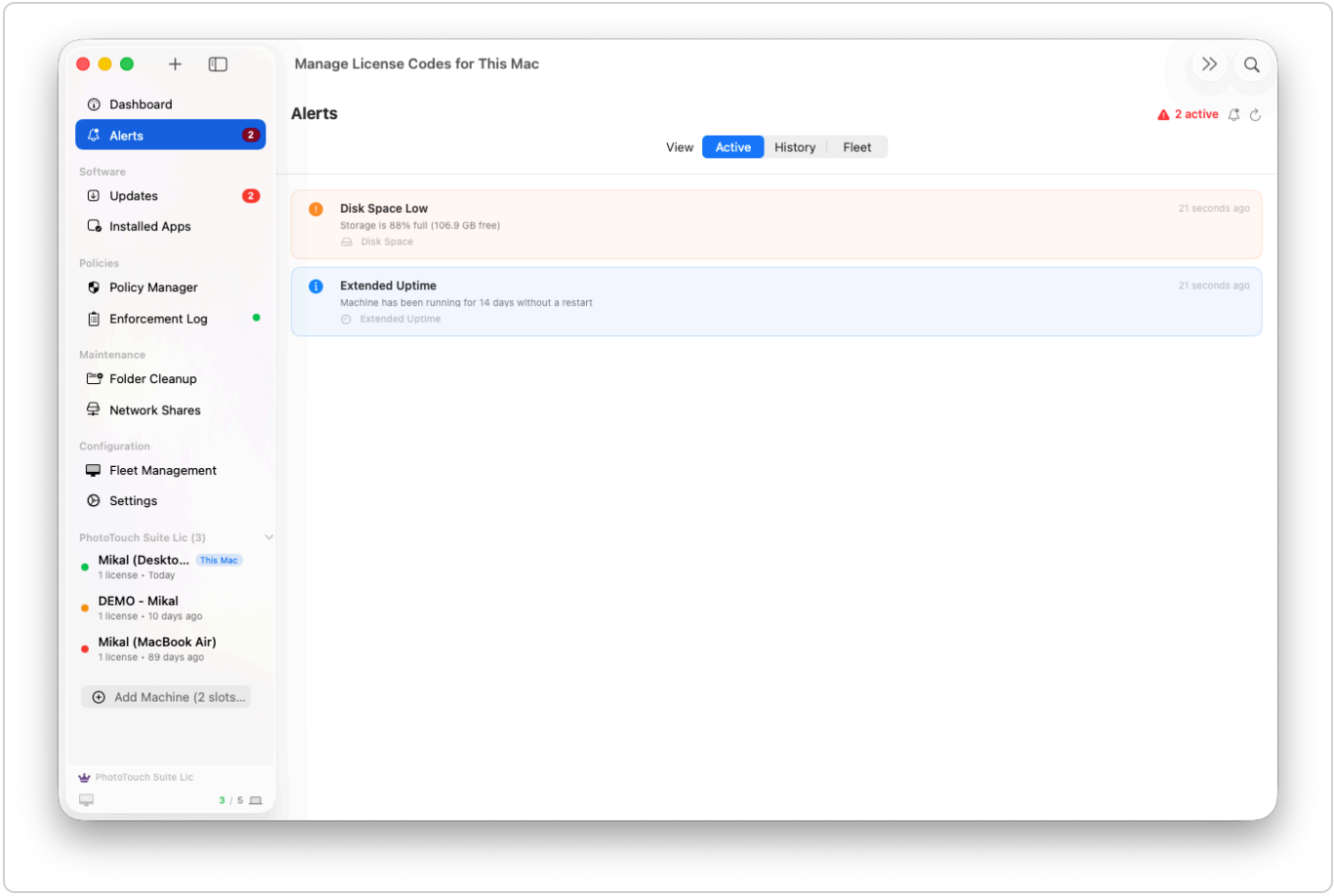


The shares this Mac depends on. Policy-managed shares show the **FLEET** badge; local ones you add with **+ Add Share**. Sentinel watches each share and remounts it when it drops (per-share **Reconnect automatically** setting). **Check Now** verifies everything immediately; **Mount Now** forces one share to reconnect. Status text under each share tells you the last check result — the one in this screenshot has an invalid address, which is exactly how a typo'd `smb://` path shows up.

Remember: passwords are entered **once per machine** (they never travel with a policy), so a brand-new machine will ask for each share's password the first time.

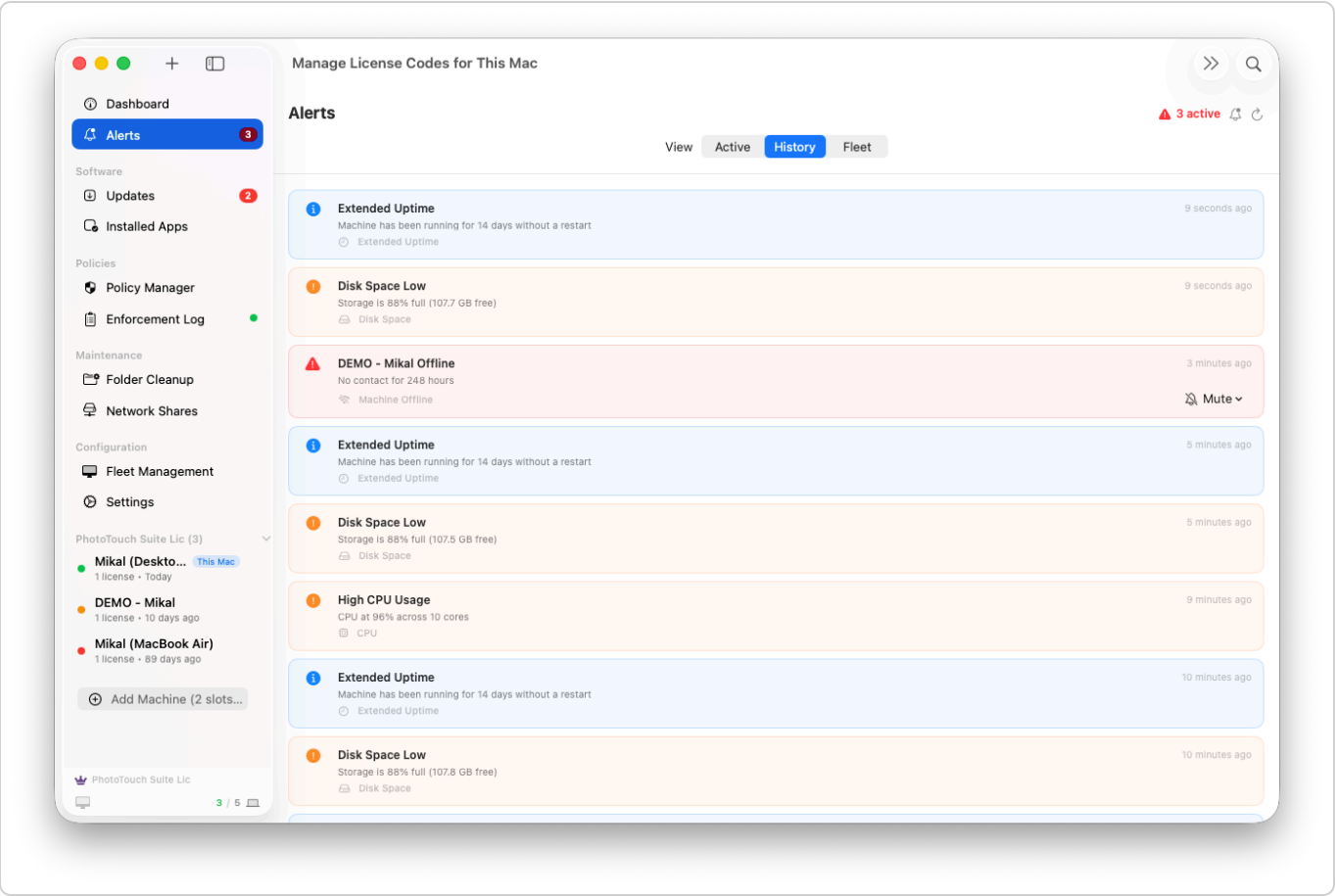
---

12. Alerts — Active, History, and Fleet

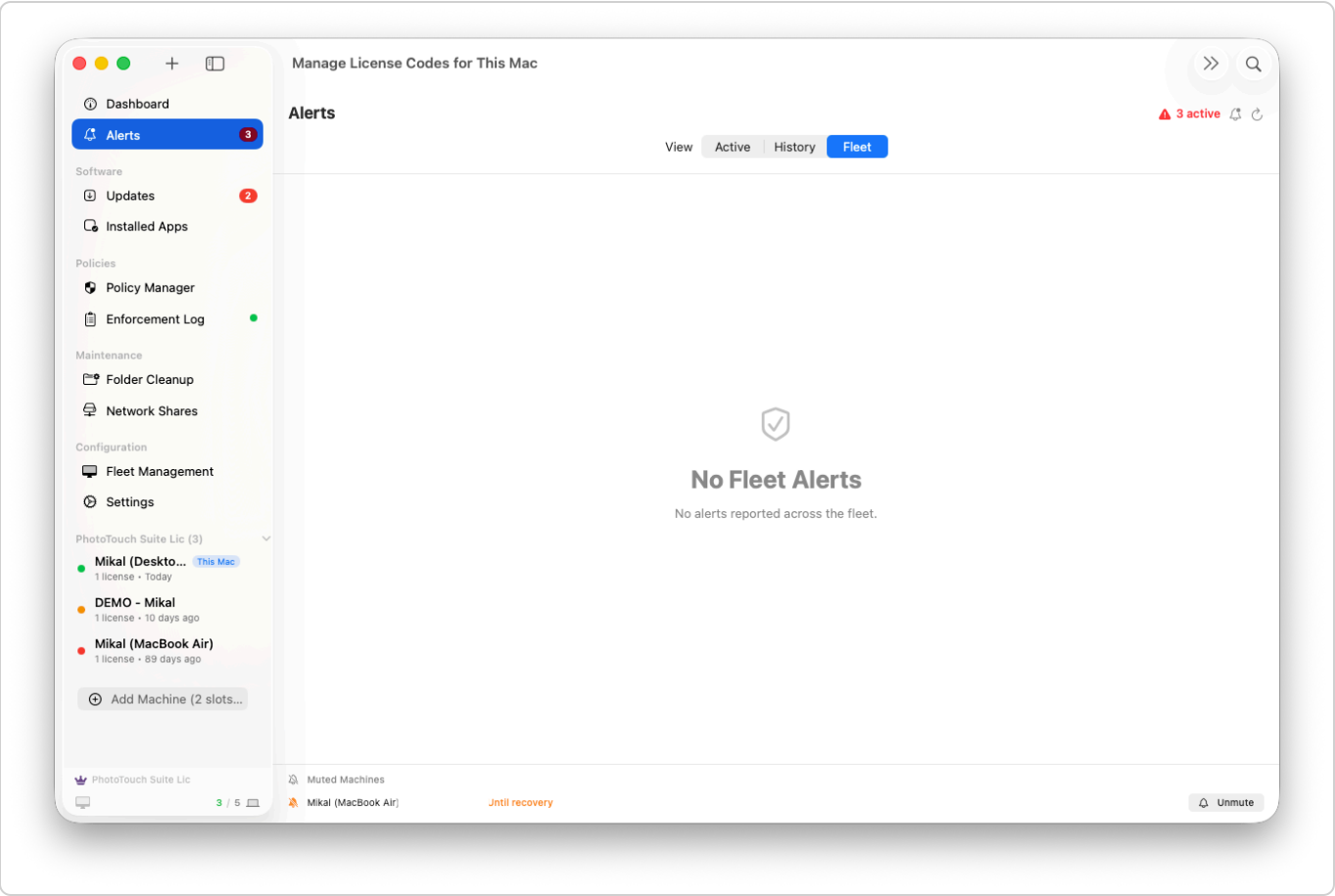


The **Active** tab is what needs attention now, newest first. Each alert names the machine it came from, and the ones you'll see most:

- **Disk Space Low** — the disk is filling (fires around 88% here).
- **Extended Uptime** — the machine has run too long without a restart.
- **High CPU Usage** — sustained load.
- **Machine Offline** — a fleet machine hasn't checked in (here: no contact for 248 hours). The **Mute** ▾ menu on the alert silences that machine's alerts, with *until recovery* as an option — muted machines are listed at the bottom of the Fleet tab with an **Unmute** button, so a mute can't be forgotten.



History shows alerts that have come and gone — the pattern-spotting view. The same machine raising *Disk Space Low* every Friday is a workflow problem, not a disk problem, and this is the tab that shows it. It's also where you can see the **Mute** ▾ menu on a fleet alert in action.



Fleet shows alerts from *other* machines on your licenses — the tab that makes one office Mac a monitoring station for every venue. *No Fleet Alerts* is the state you want. Note the **Muted Machines** strip at the bottom: this fleet has one machine muted *until recovery*.

The red badge on **Alerts** in the sidebar and on the menu bar icon (section 16) carries the active count everywhere.

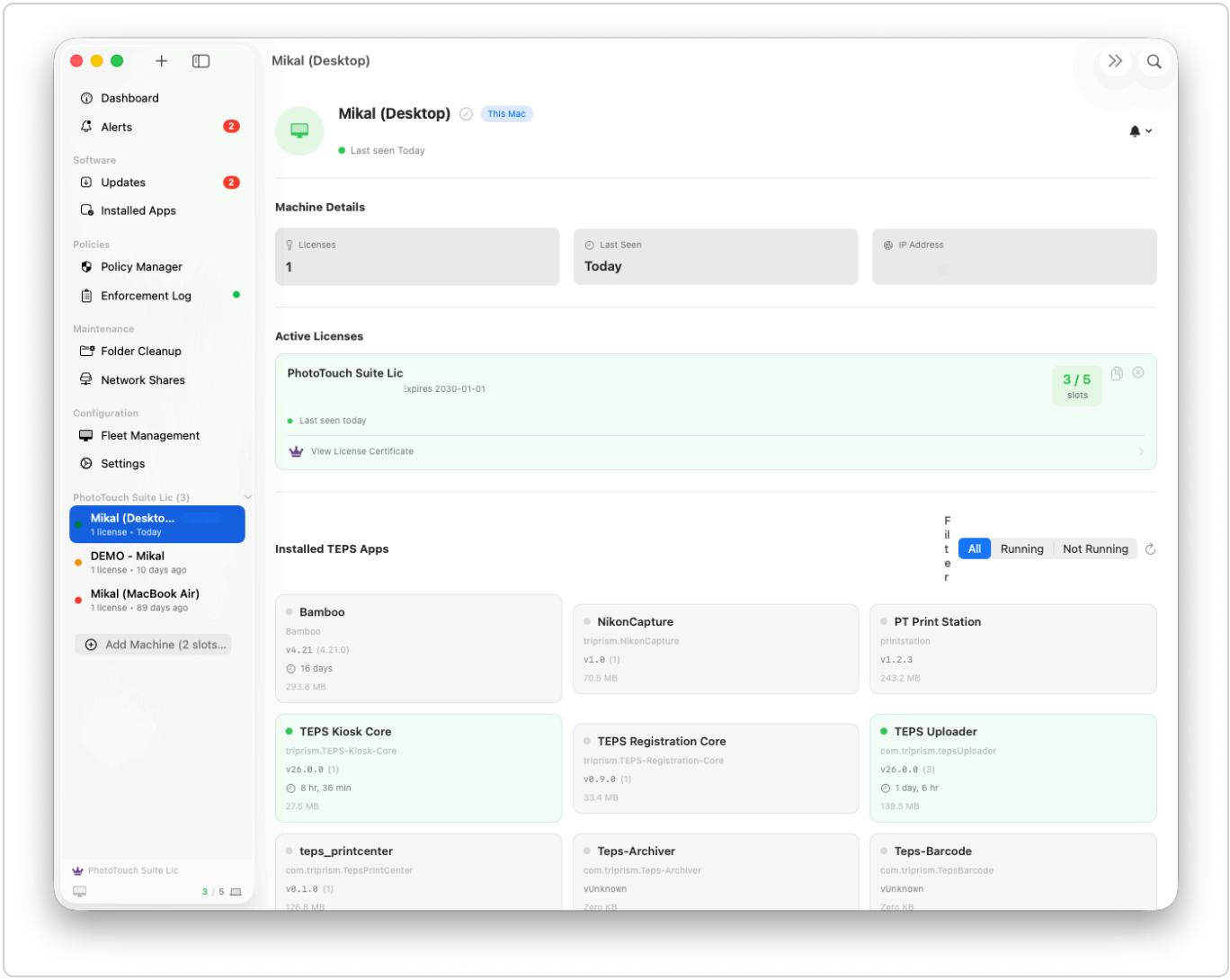
---

13. Machines and licenses in the sidebar

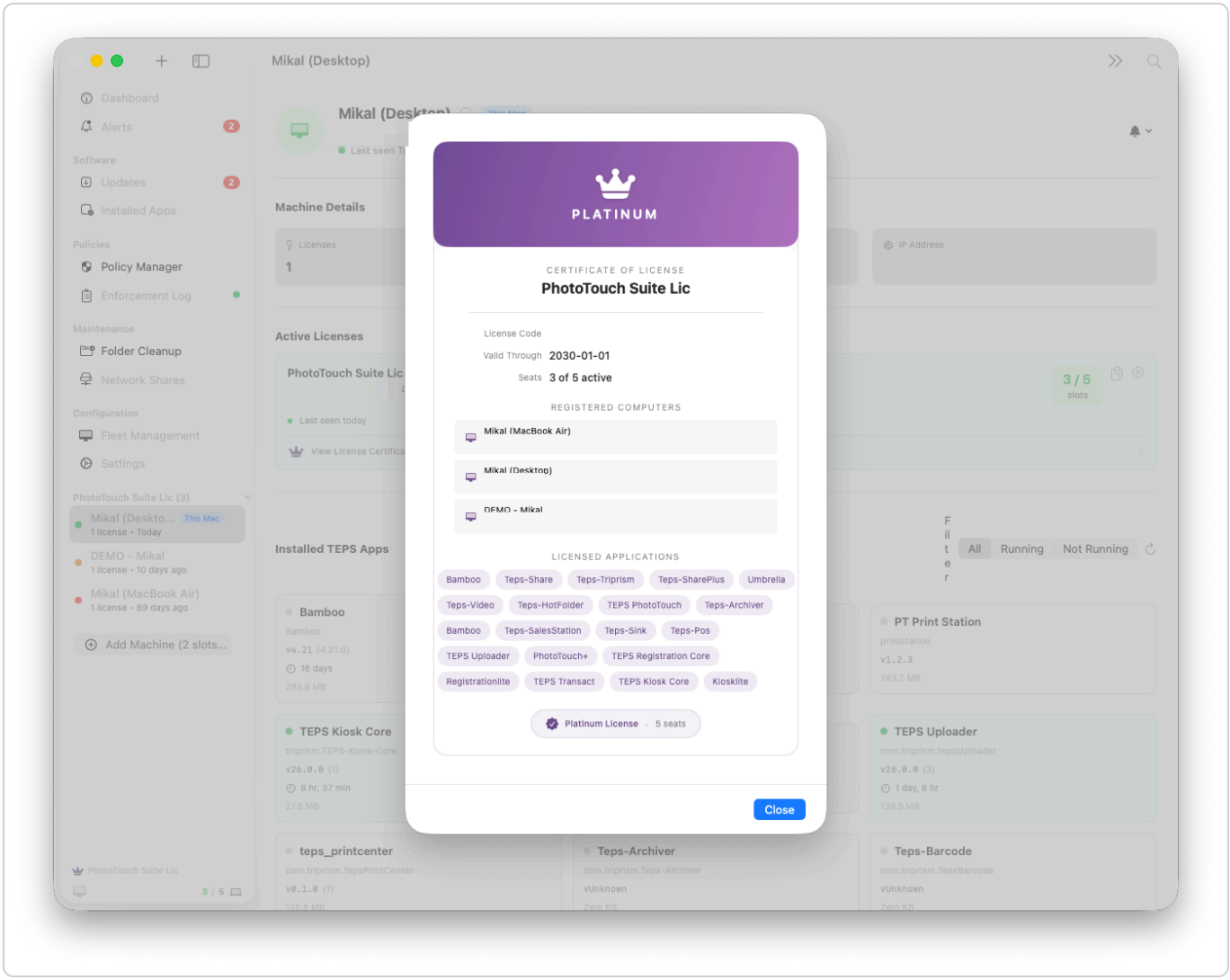
The bottom of the sidebar lists each license with its machines:

- A colored dot per machine — green (seen recently), orange (getting stale), red (not seen in a long time; the "89 days ago" machine here has earned its red dot).
- **This Mac** badge on the machine you're sitting at.
- The footer shows the license summary — **3 / 5** slots used.

Click a machine to open its page:

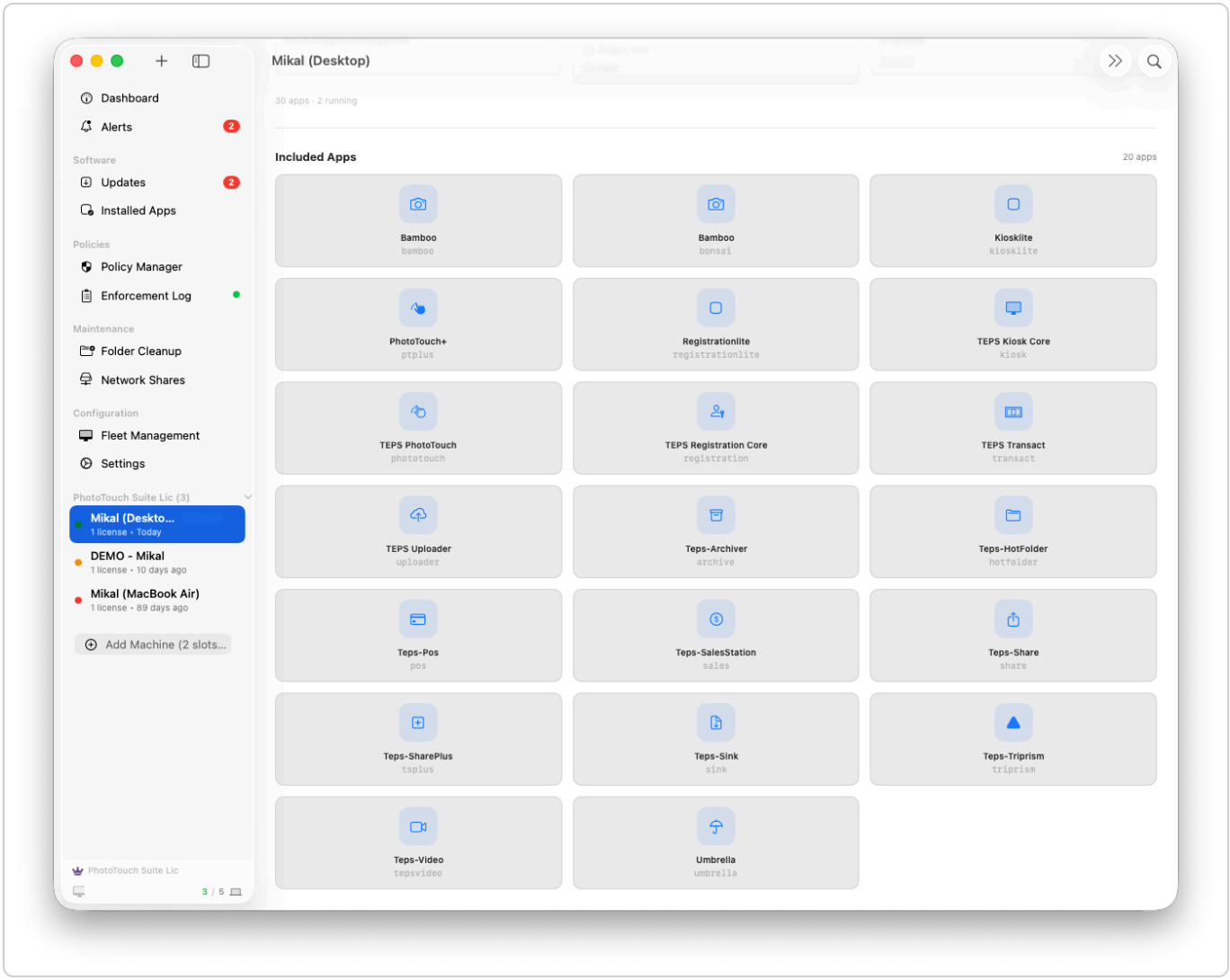


- **Header** — nickname, serial, last-seen, and a **bell menu** to choose which of this machine's alerts notify you.
- **Machine Details** — license count, last seen, and the machine's IP address.
- **Active Licenses** — the license activated on this machine: code, expiry, and the slots gauge (**3 / 5**). The copy button grabs the license code. **View License Certificate** opens the formal certificate:



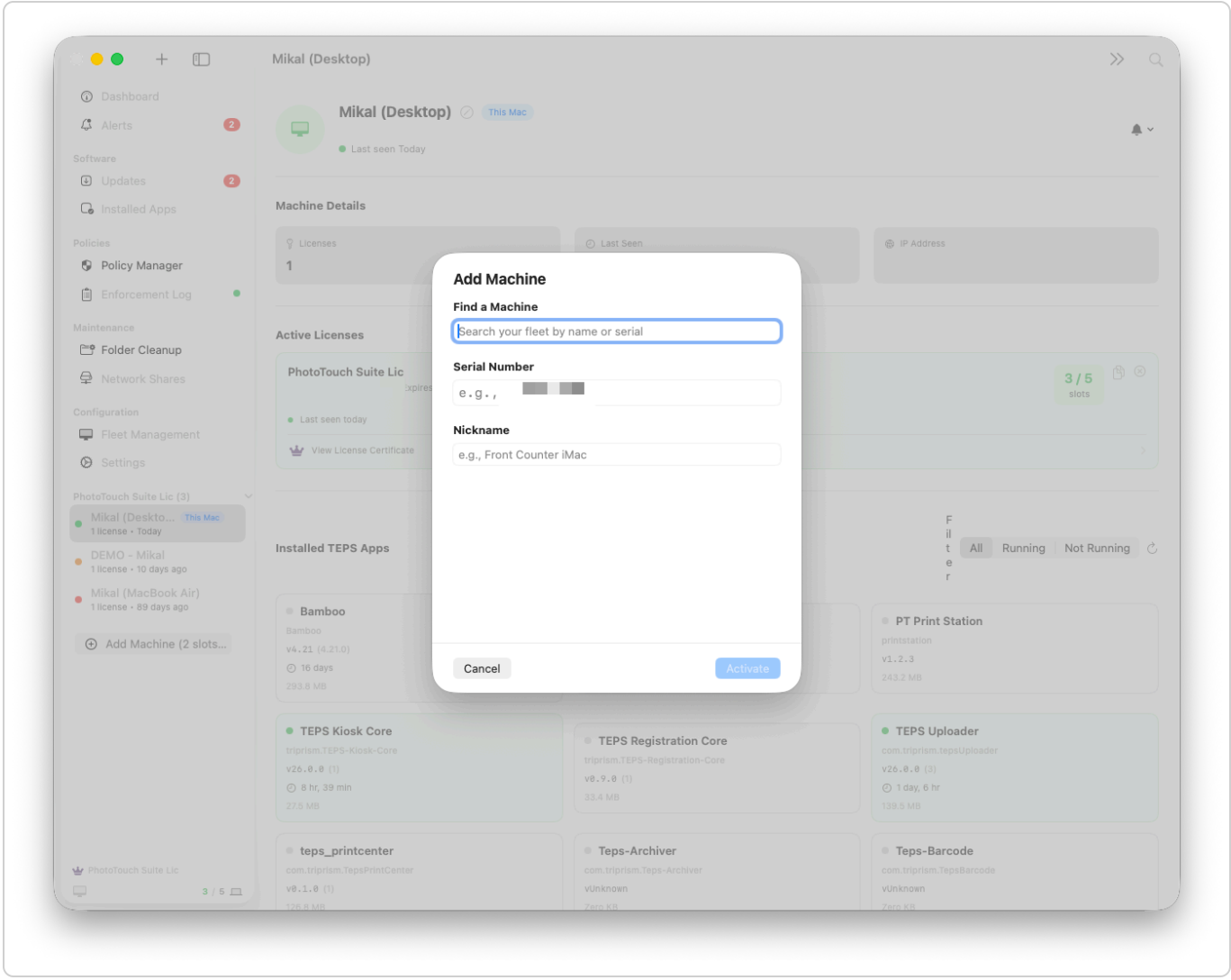
The certificate is the license in one card — tier (Platinum), license code, valid-through date, **every registered computer** on the license, and chips for **every application the license covers**. When a venue asks "what exactly are we licensed for," this is the screen you show them.

- **Installed TEPS Apps** — every TEPS app on that machine with version, how long it's been running (green = running now), and size. Filter All / Running / Not Running. This works for *remote* machines too — that's App Scout data.
- **Included Apps** — scroll down for the full grid of apps the license entitles the machine to run:



14. Activating other machines remotely (Add Machine)

You don't have to walk to a machine to put it on the license. Press **Add Machine (N slots…)** at the bottom of the sidebar:



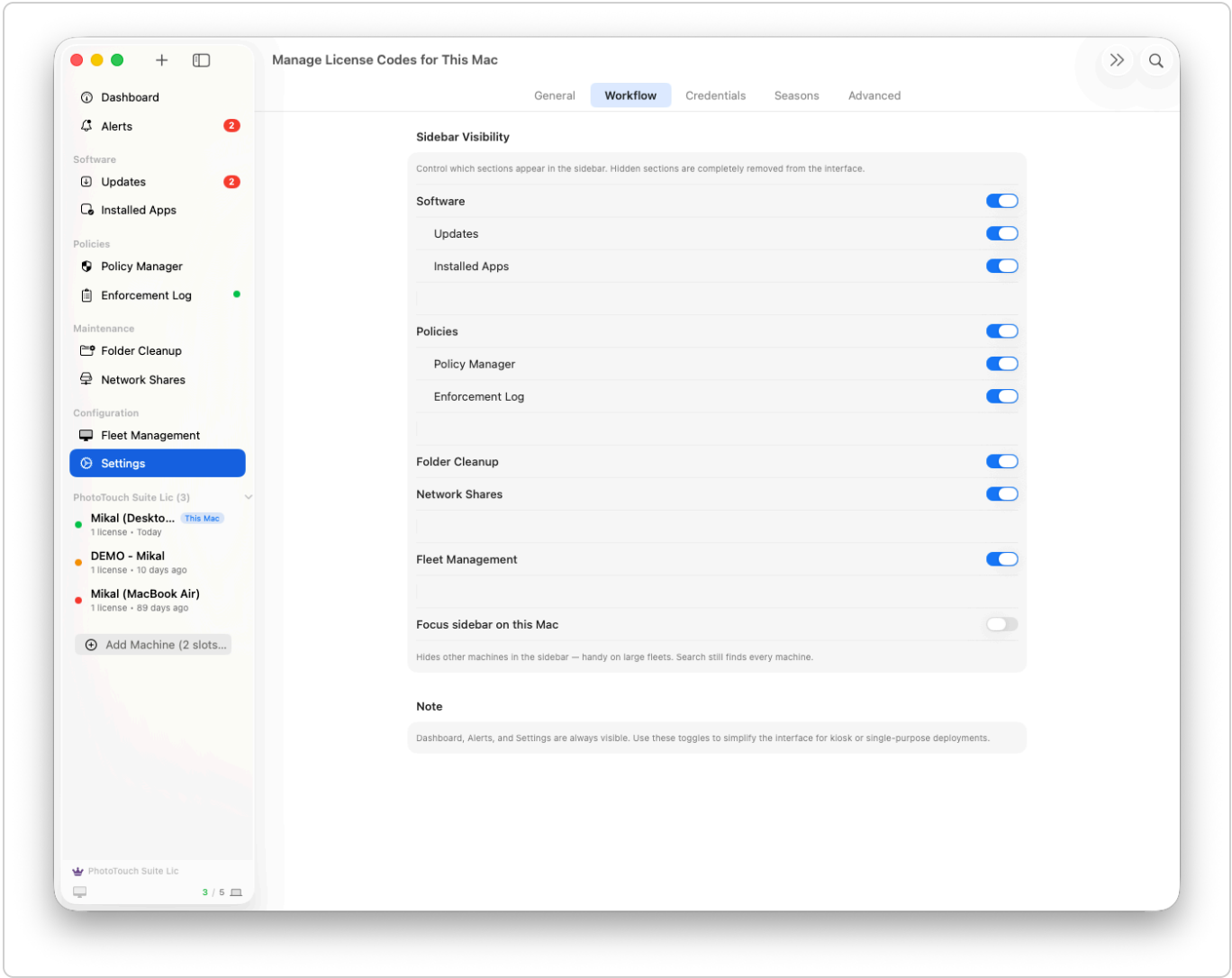
- **Find a Machine** — search your fleet by name or serial and pick it, or
- **Serial Number** — type the serial by hand (for a Mac that hasn't enrolled yet), plus a **Nickname**.

Activate uses one of the license's free slots for that machine. The button label tells you how many slots remain before you commit.

---

15. Settings — Workflow, Credentials, Seasons, Advanced

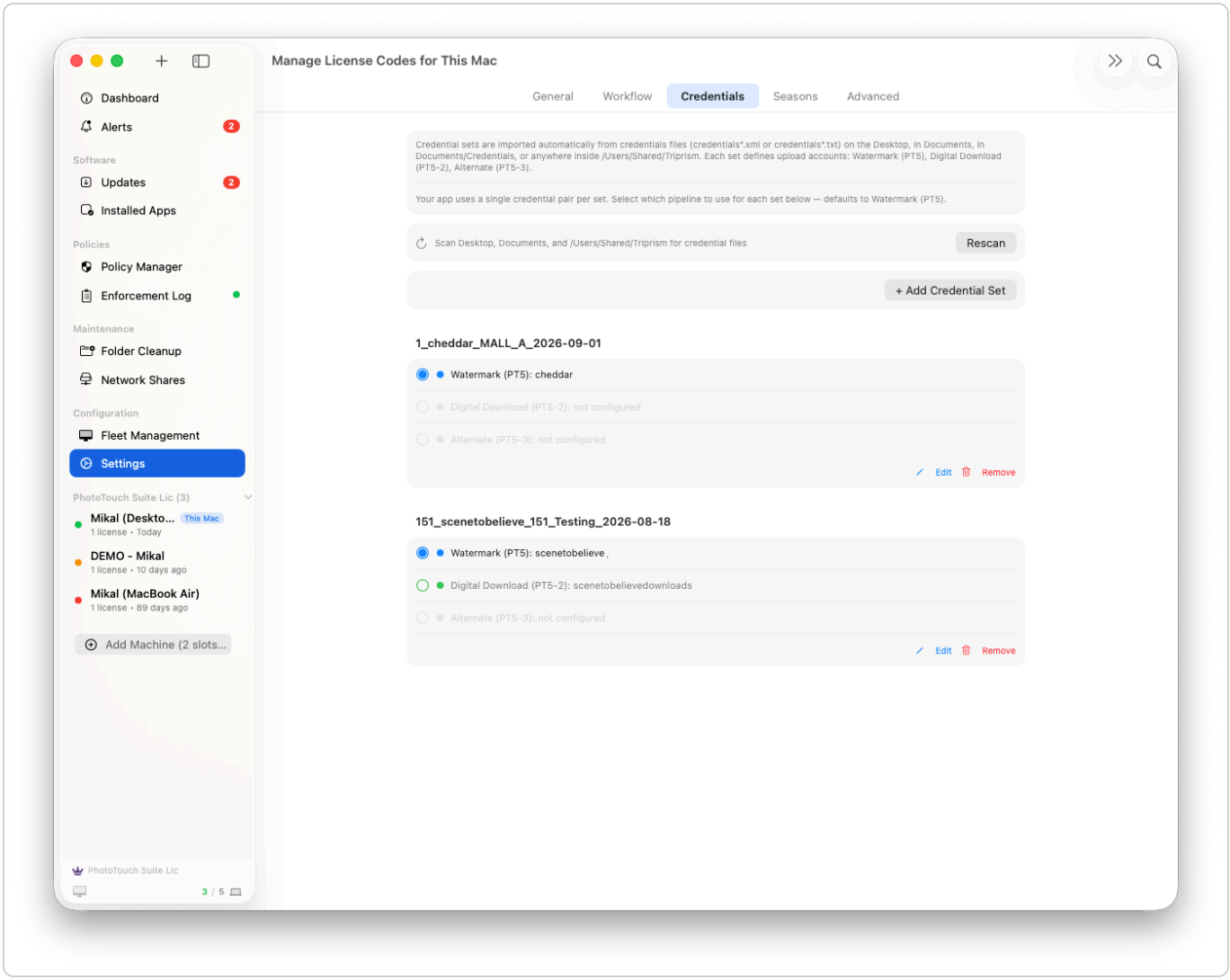
Workflow — shape the app for each machine



Every sidebar section has a visibility switch — a hidden section is **completely removed from the interface**, not just collapsed. A front-counter Mac that only needs license viewing can hide Policies, Maintenance, and Fleet Management entirely. Dashboard, Alerts, and Settings are always visible.

Focus sidebar on this Mac hides *other machines* from the sidebar — handy on large fleets where the machine list gets long. Search still finds every machine.

Credentials — upload accounts



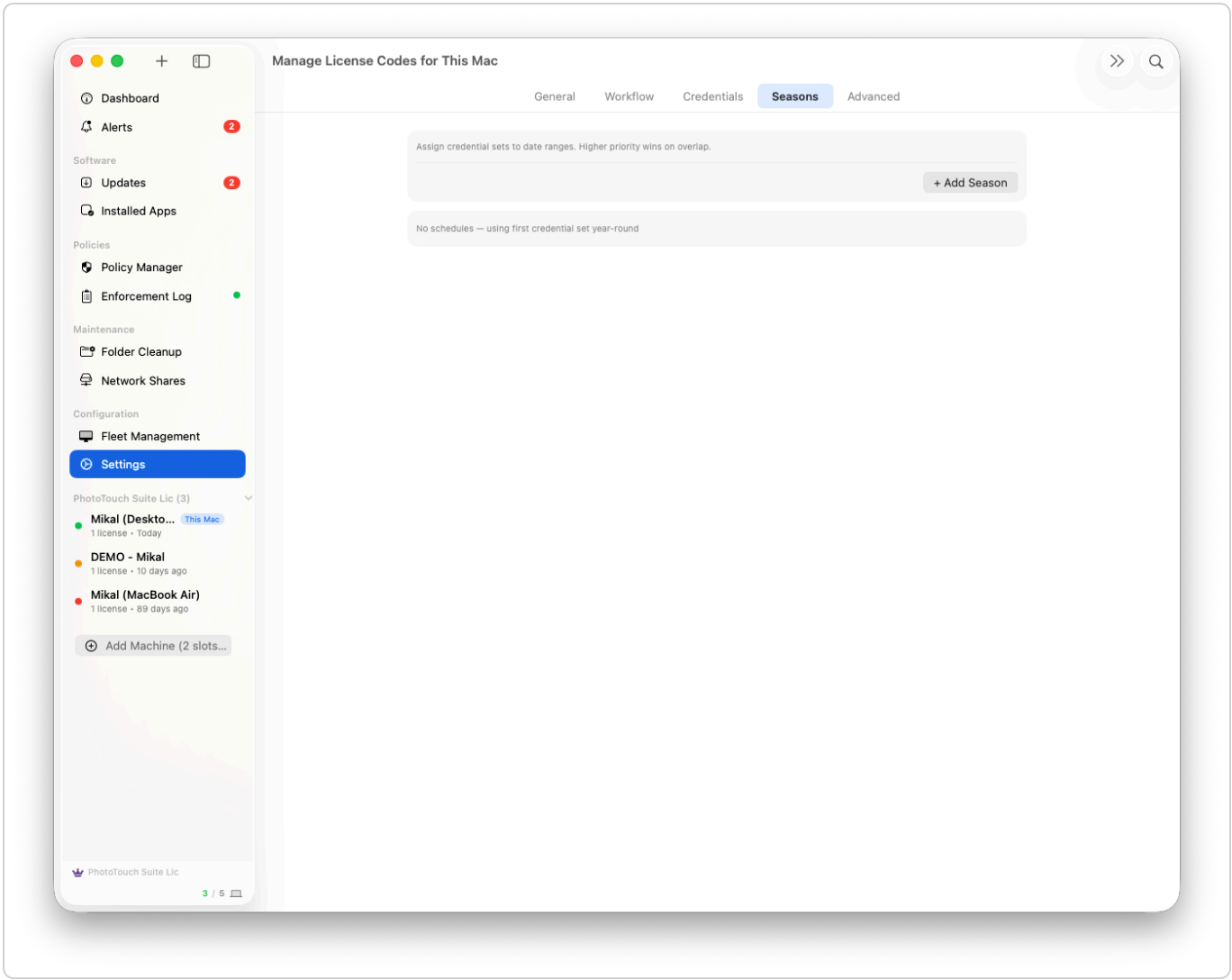
Credential sets are **imported automatically** from credential files (`credentials.xml` *or* `credentials.txt`) found on the Desktop, in Documents, in Documents/Credentials, or anywhere inside `/Users/Shared/Triprism`. Drop the file in one of those places and press **Rescan** — or add a set by hand with **+ Add Credential Set**.

Each set defines up to three upload accounts, and you pick which pipeline the app uses per set:

Pipeline	Account
Watermark (PT5)	The default
Digital Download (PT5-2)	If configured
Alternate (PT5-3)	If configured

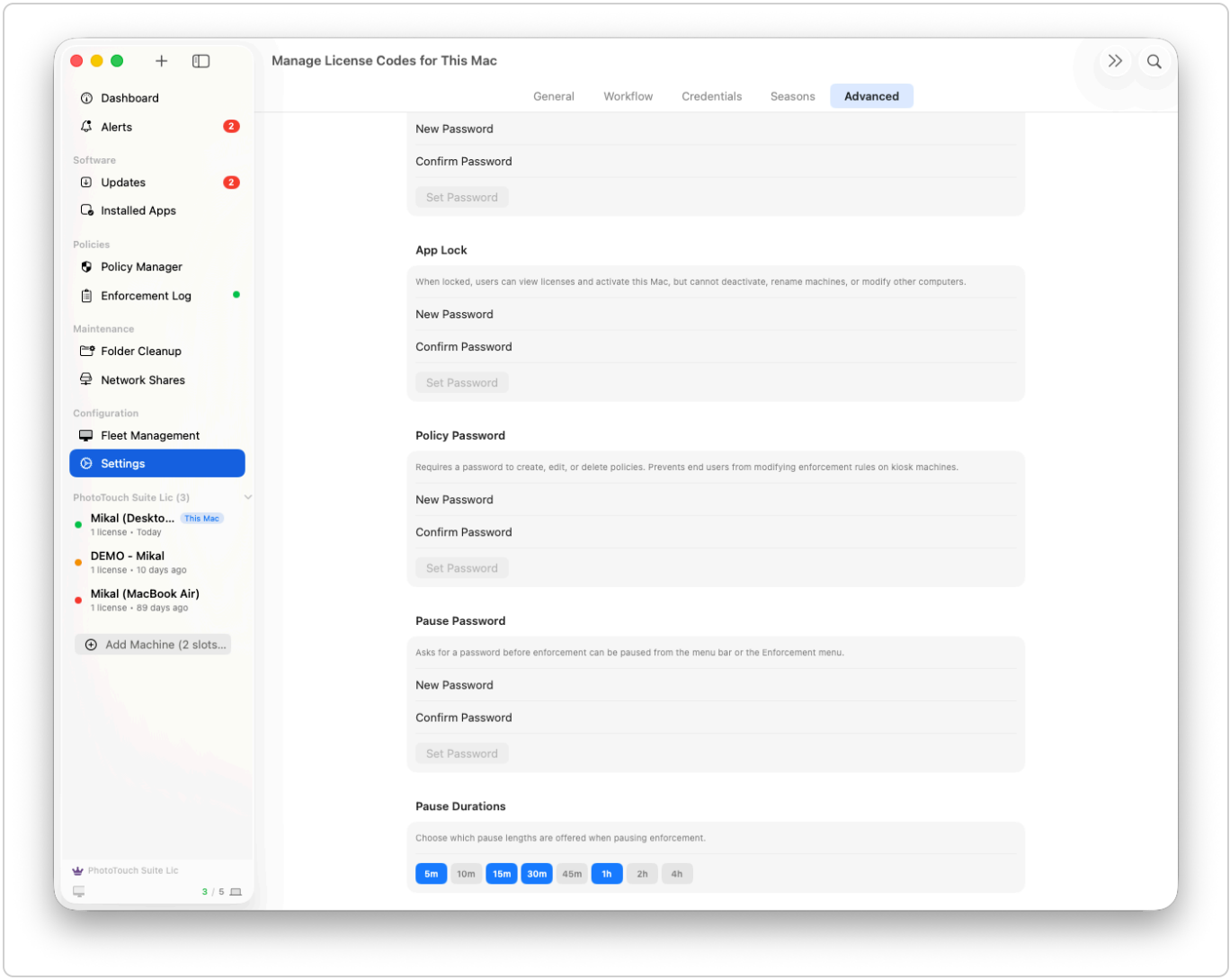
Unconfigured pipelines are greyed out. **Edit** and **Remove** per set.

Seasons — switch credentials by date



+ Add Season assigns a credential set to a date range — fall sports one set, spring another — and the switch happens on the calendar, not by someone remembering. Higher priority wins on overlap. With no schedules, the first credential set is used year-round.

Advanced — four locks and the pause menu



Four **separate** passwords, each guarding a different surface, so you can hand a kiosk password to staff without handing over the policies:

Lock	What it protects
Settings Lock	The Settings tabs. The Advanced tab stays reachable so you can always manage the passwords themselves
App Lock	Locked, users can view licenses and activate *this* Mac — but cannot deactivate, rename machines, or touch other computers
Policy Password	Required to create, edit, or delete policies — keeps enforcement rules safe on kiosk machines
Pause Password	Required before enforcement can be paused, from the menu bar or the Enforcement menu

Pause Durations — choose which pause lengths the pause dialog offers (the highlighted chips: here 5m, 15m, 30m, 1h). Trim it to short durations on kiosks so "pause" can never mean "off for the weekend."

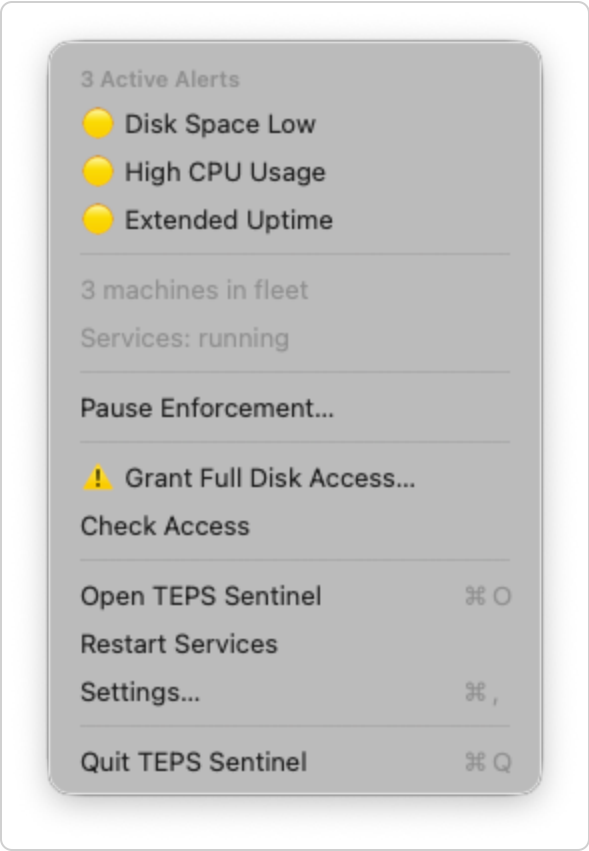
General

Covered in section 4 — fleet pairing, startup behavior, permissions status, Agent Mode, network polling, scheduled restart, and settings export/import.

---

16. The menu bar icon

Sentinel lives in the menu bar even when the window is closed (and starts there silently if *Hide window at launch* is on):



Top to bottom: the active alerts, the fleet summary (machines, services state), **Pause Enforcement…**, the permissions reminder (**Grant Full Disk Access… / Check Access**) until both permissions are granted, then **Open TEPS Sentinel** (⌘O), **Restart Services**, **Settings…** (⌘,), and **Quit** (⌘Q).

For day-to-day studio life this menu is the whole app: glance for alerts, pause when a tech needs a machine, open the window only when something needs fixing.

---

17. Quick-start checklist

For each new Mac, in order:

1. □ Launch Sentinel, grant **App Management** and **Full Disk Access** (§1) — verify both show **Granted** in Settings → General
2. □ **⌘N** — activate the license; nickname the machine; use **Monitor Only** on watch-only Macs (§2)
3. □ Settings → General: set **Photographer Account** (+ location code) and confirm **Scouts deployed** (§4)
4. □ Pair the **fleet secret** from the admin portal — shown once, paste and **Pair** (§4)
5. □ Settings → General → Startup: **Launch at Login** on; **Hide window at launch** on for kiosks (§4)
6. □ Fleet Management: confirm **Scout Reporting** on; set the opt-in scouts and Field Ops switches deliberately; **Save & Apply** (§5)

7. □ Assign the machine to a **policy** (or press **This Mac** inside the policy) and **Deploy** (§6)
8. □ Enter passwords for any policy-managed **network shares** — they never travel with the policy (§11)
9. □ New **folder-cleanup** rules run in **Preview only** until the Recent Activity log looks right (§10)
10. □ Set the **Advanced** passwords on any machine other people touch; trim **Pause Durations** on kiosks (§15)
11. □ **Export Settings** from the finished machine to seed the next one (§4)