Overview

Devices & logs

Device registry

Every machine running the Sentilai Endpoint registers with its own credential (public-key identity). The **Devices** screen lists them with first/last seen, reported hostname, and compliance state. A device credential can be revoked instantly — its requests stop at the Gateway.

Compliance

The app reports whether every installed AI tool on the device is actually governed and whether local MCP servers are wrapped. Non-compliant devices are flagged so configuration drift surfaces.

Event logs

The app keeps a local, allowlisted event log (no prompt content) with fixed 14-day retention. From the console an admin can **request a device's logs**; the app uploads a bundle you can download — useful for troubleshooting a specific machine.

Sharing with support

A log bundle can be explicitly shared with Sentilai support from the console — nothing leaves your tenant without that explicit act, and the share is audited.

Revision #1
Created 2026-08-01 13:06:28 UTC by Sentilai Docs
Updated 2026-08-01 13:06:28 UTC by Sentilai Docs