Using it in an audit

Some practical notes from what auditors actually ask.

Generate it at the time, not afterwards

Retention is finite. An evidence pack covering March, generated in March, keeps its detail; one generated in December may cover a window whose events have been purged.

Generate one per quarter and keep it. It takes a minute and it converts a perishable dataset into a durable document.

Answering the common questions

"How do you know which AI tools your developers use?" — Requests by tool, plus the device inventory.

"How do you control what data goes to AI providers?" — The risk-detector rules in force, with the detection counts showing they were operating rather than merely configured.

"Who has access?" — The access inventory, with roles and enrolment dates.

"What happens when someone leaves?" — Offboarding revokes devices and removes passkeys in one action; the device inventory across two consecutive packs shows it happened.

The gap to be honest about

The pack shows what happened **through Sentilai**. A developer using a personal API key on a personal machine does not appear, because they never touched the Gateway. If an auditor asks about coverage, the honest answer is that you govern the managed path and monitor for drift — and that the device inventory plus the non-compliant flag is how you detect machines slipping out of it.

Claiming complete coverage of something you cannot see is how organizations get into trouble with auditors, not out of it.

Revision #6
Created 2026-08-02 10:19:36 UTC by Sentilai Docs
Updated 2026-08-04 08:39:22 UTC by Sentilai Docs