What the evidence pack contains

Compliance produces a point-in-time record for a date range you choose, as a printable report and as JSON.

The four parts

Traffic — AI requests, how many were blocked by policy, how many developers were active, and the split between subscription and API-key usage.

Active policy configuration — the MCP default action, your retention setting, per-tool connection modes, and the **rules in force**: every risk-detector rule and every MCP server rule. If you have changed nothing, it says "code defaults only", which is itself an honest and useful statement.

Enforcement and detections — what was blocked and why, risk findings by detector, requests by tool, and the top models.

Access inventory — seats used against your cap, how many devices are registered, and a table of every admin and developer with their role and enrolment date.

Two formats

Print / Save as PDF produces a report with a proper header and footer, for attaching to something. **Download JSON** gives you the same data as `senticons-evidence-<date>.json` for your own tooling.

What it is not

The report says so itself: it supports **the AI section of a security questionnaire** (SIG, CAIQ, SOC 2 evidence requests) and, from December 2027, AI Act deployer documentation where that applies — but it is **not a certification and not a legal assessment**. It is evidence that you have controls and that they were operating. Whether that satisfies a particular obligation is a question for your counsel.

We would rather say this plainly than let a customer discover it in an audit.

Revision #7
Created 2026-08-02 10:19:36 UTC by Sentilai Docs
Updated 2026-09-29 14:39:17 UTC by Sentilai Docs