Generate an evidence pack

Compliance produces a point-in-time record of how AI is governed in your organization: the active policy, who had access, and what the Gateway actually enforced.

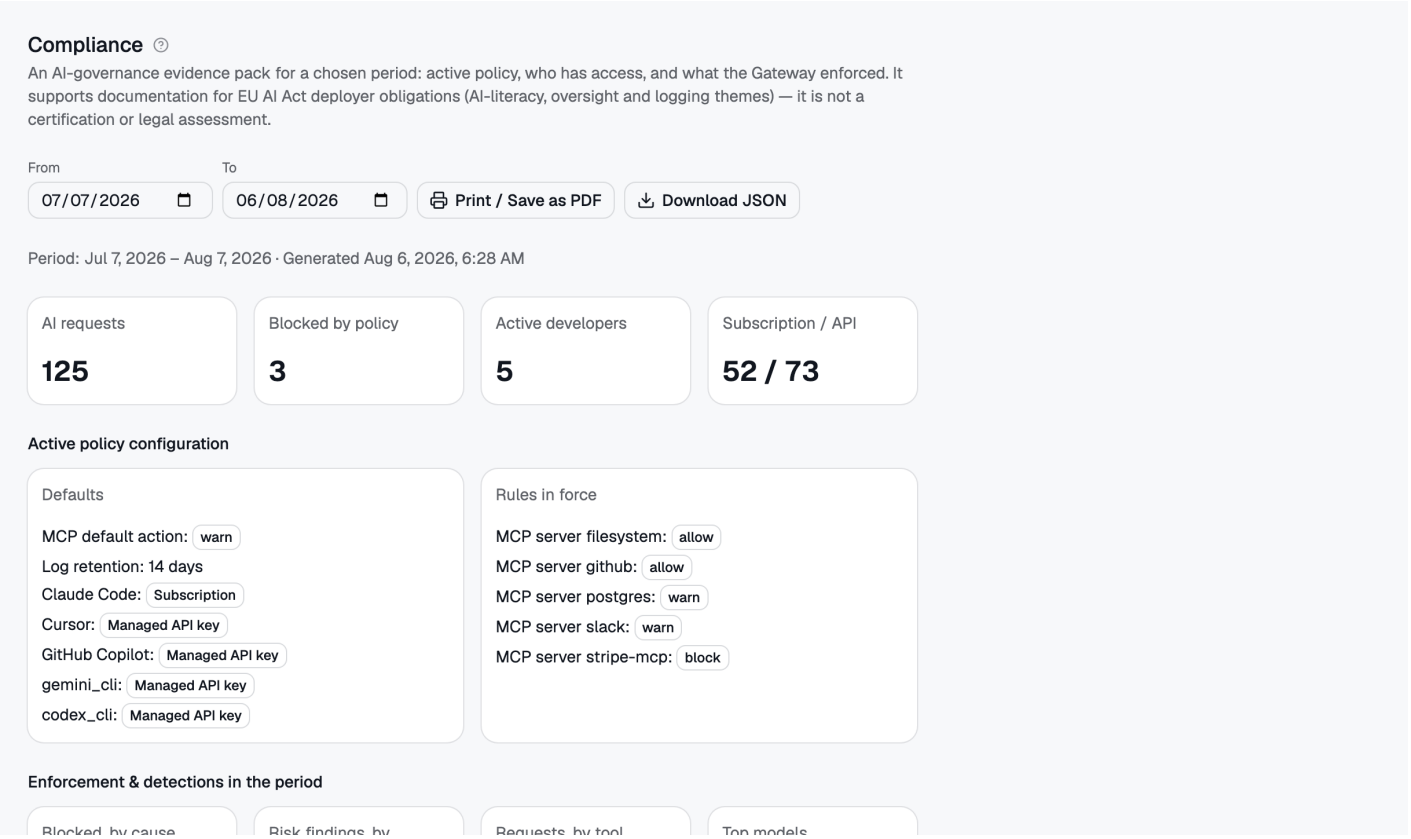
1. Pick a **From** and **To** date.
2. **Print / Save as PDF** for a document to hand over, or **Download JSON** for a machine-readable copy.

What it contains

- **Totals** for the period: AI requests, blocked by policy, active developers, and the subscription/API split.
- **Active policy configuration** — defaults, retention, per-tool connection modes, and every MCP rule in force.
- **Enforcement and detections** — blocks by cause, risk findings by detector, requests by tool, top models.
- **Access inventory** — seats, admins, developers, and registered devices.

What it is, and isn't

It is built for the AI section of a customer's security questionnaire (SIG, CAIQ) and for the evidence requests of a SOC 2 audit — by showing what you actually did. Where the EU AI Act's deployer obligations apply to you (for most teams using coding assistants they do not, and the high-risk ones start in December 2027), it supports that documentation too. It is **not** a certification, and it is not a legal assessment. Treat it as evidence you can hand to an auditor, not as an answer to whether you comply.



The Compliance evidence pack: totals, active policy, enforcement and access inventory for a period.

Revision #19
Created 2026-08-01 13:06:45 UTC by Sentilai Docs
Updated 2026-09-29 14:39:15 UTC by Sentilai Docs