Overview

Compliance & SIEM

Evidence pack

The **Compliance** screen assembles an auditor-ready evidence pack for any period: the policies in force (MCP default + rules, detector actions), risk sensitivity, capture settings, top models/tools/MCP servers, and activity summaries. Export and hand it to your auditor — this is the artifact the EU AI Act's transparency expectations (August 2026) map onto.

SIEM export

Pull or push your audit events into your own SIEM:

- **Pull**: an OCSF-formatted API your collector polls with a scoped credential.
- **Push**: the platform delivers events to your HTTPS endpoint.

Either way the data is yours — Sentilai's audit trail is designed to feed your existing security operations, not replace them.

Retention

Audit metadata retention is per-tenant (default 14 days) with automated purge; device logs are fixed 14-day; captured prompts (opt-in) follow the same tenant retention. Support tickets persist for the support relationship. Deletion on offboarding is contractual and scripted.

Egress blocklist

The Policy page generates a network **egress blocklist** from what's actually configured for your tenant — the direct provider hosts to block and the one Gateway host to allow — so your network team can enforce "AI only via Sentilai" at the firewall.

Revision #1
Created 2026-08-01 13:06:30 UTC by Sentilai Docs

Updated 2026-08-01 13:06:30 UTC by Sentilai Docs