

Stream events to your SIEM

SIEM Export pushes Sentilai events to your security monitoring stack as they happen.

1. Enter the destination host and port, and pick the protocol (`tcp` or `tls`).
2. **Save destination.**
3. **Send test event** and confirm it lands in your SIEM.

Destinations must be publicly resolvable addresses — an internal-only host will be rejected, since our Gateway has to reach it.

Prefer `tls` unless the destination genuinely cannot terminate it: these events describe your developers' AI usage and shouldn't cross the internet in the clear.

SIEM Export ⓘ
Stream your audit trail to your SIEM. Two options, both live: pull the OCSF JSON API with an audit:read API credential, or push CEF over syslog to the destination below.

Pull — OCSF JSON API
Point your SIEM's HTTP/JSON collector (Splunk, Microsoft Sentinel, Elastic, QRadar...) at the cursor-paginated OCSF endpoint below, authenticated with an API credential carrying the audit:read scope (create one under API Credentials).

```
GET /api/siem/v1/events?cursor=&limit=1000
```

Push — CEF / syslog
We ship each event as CEF over RFC 5424 syslog to your collector. The destination must be a public address (private/internal hosts are rejected).
☒ Enable delivery
Host: Port:
Protocol: Sender hostname:

SIEM Export — the OCSF pull API and the CEF/syslog push destination, with live delivery status.

Revision #11

Created 2026-08-01 13:06:45 UTC by Sentilai Docs

Updated 2026-08-05 06:29:37 UTC by Sentilai Docs