Log retention

How long Sentilai keeps your audit events, findings and any captured prompt content.

Where it is

Policy shows it as a read-only card. It is currently set by Sentilai support rather than by you — open a ticket from **Support** and tell us the number of days you need.

What retention covers

Everything time-bounded: audit events behind Activity, risk findings, captured conversations, and the blocked-conversation list. When the window passes, the data is purged rather than archived.

Choosing a number

Two forces pull in opposite directions.

Longer helps you investigate. An incident discovered in June is much easier to understand if you can see April.

Shorter reduces what a breach could expose and what a legal request could reach. If prompt capture is on, this argument gets stronger — captured conversations are the most sensitive thing in the system.

Compliance frameworks rarely mandate a specific number for this kind of telemetry. Pick what you can justify, write down why, and keep the evidence pack from **Compliance** as the record.

If you need longer-term retention

Stream events to your own SIEM — see Stream events to your SIEM. Your retention rules then apply to your copy, independently of Sentilai's window.

Revision #12
Created 2026-08-02 10:20:05 UTC by Sentilai Docs
Updated 2026-09-29 14:40:27 UTC by Sentilai Docs