Prompt capture

Off by default, and the setting that deserves the most thought before you turn it on.

What it does

Stores the actual content of conversations — what developers typed and what the model replied — so you can read them later on the **Conversations** screen.

Without it you still get everything else: who, when, which tool, which model, what the policy decided, what the detectors found. What you do not get is the text.

Before you turn it on

Tell your team. Not because the law necessarily requires a specific notice in your jurisdiction, but because discovering afterwards that their prompts were being stored is the fastest way to lose your developers' cooperation — and a governance programme that your engineers are working around is worse than none.

What protects the content

- **Redaction happens before storage.** Secrets found by the detectors are replaced with a marker naming the kind, so the stored transcript contains `[REDACTED:aws_access_key_id]` rather than the key. In the console these render as amber shield badges.
- **It follows your retention setting** and is purged with everything else.
- **Sentilai support cannot read it.** Support can see that a request happened and what the policy decided. The content is yours.

Turning it on

Policy ? Prompt capture. Conversations then start appearing on the Conversations screen. Until then that screen shows an explicit "Prompt capture is off" state with a link back to Policy, rather than an empty list that looks like a bug.

Revision #8
Created 2026-08-01 13:06:39 UTC by Sentilai Docs
Updated 2026-09-29 14:39:38 UTC by Sentilai Docs