Real-time alerts

Slack, Teams and webhook notifications for high-severity events.

Overview

Real-time alerts

Don't watch dashboards — get paged. Sentilai posts to your channels the moment a qualifying governance event fires.

Channels

- **Slack** — an incoming-webhook URL; alerts arrive as formatted messages.
- **Microsoft Teams** — an incoming-webhook URL; alerts arrive as cards.
- **Generic webhook** — a JSON payload for anything else (SIEM hooks, PagerDuty ingestion, custom automation).

What fires

An alert is sent when an event's severity reaches the channel's **floor** (default: high only), or whenever a request is **blocked** — a block is always alert-worthy. Severity comes from the risk detectors and the AI classifier.

Setting up

On the **Policy** page, under **Real-time alerts**: pick the channel type, name it, paste the webhook URL, choose the severity floor, and use **Send test** to verify delivery before saving. The destination URL is stored encrypted and never displayed again — treat it like a credential, because anyone holding it can post into your channel.

Behavior

Delivery is fire-and-forget with a short timeout: alerting can never slow down or fail a developer's AI request. Each qualifying event posts once per matching channel.

Set up an alert channel

Nobody watches a dashboard. Alerts put the findings that matter into the place your team already looks.

Adding a channel

Policy ? Real-time alerts ? add a channel:

- **Kind** — Slack, Microsoft Teams, or a generic JSON webhook.
- **Name** — how it appears in the list. Name it after the destination, not the event: "#security-alerts" tells you more later than "high severity".
- **Fires on** — the minimum severity: **High only**, **Medium and up**, or **Low and up (all)**.
- **Webhook URL** — must be `https`.

Test it immediately

Send test posts a message to the channel. It reports "? Sent", or tells you the destination did not accept it. Do this before you rely on it — a mistyped webhook URL fails silently forever otherwise.

The URL is write-only

Once saved, the webhook URL is never shown again. A Slack or Teams webhook URL is a credential — anyone holding it can post into your channel — so it is stored the same way a provider key is. To change it, remove the channel and add it again.

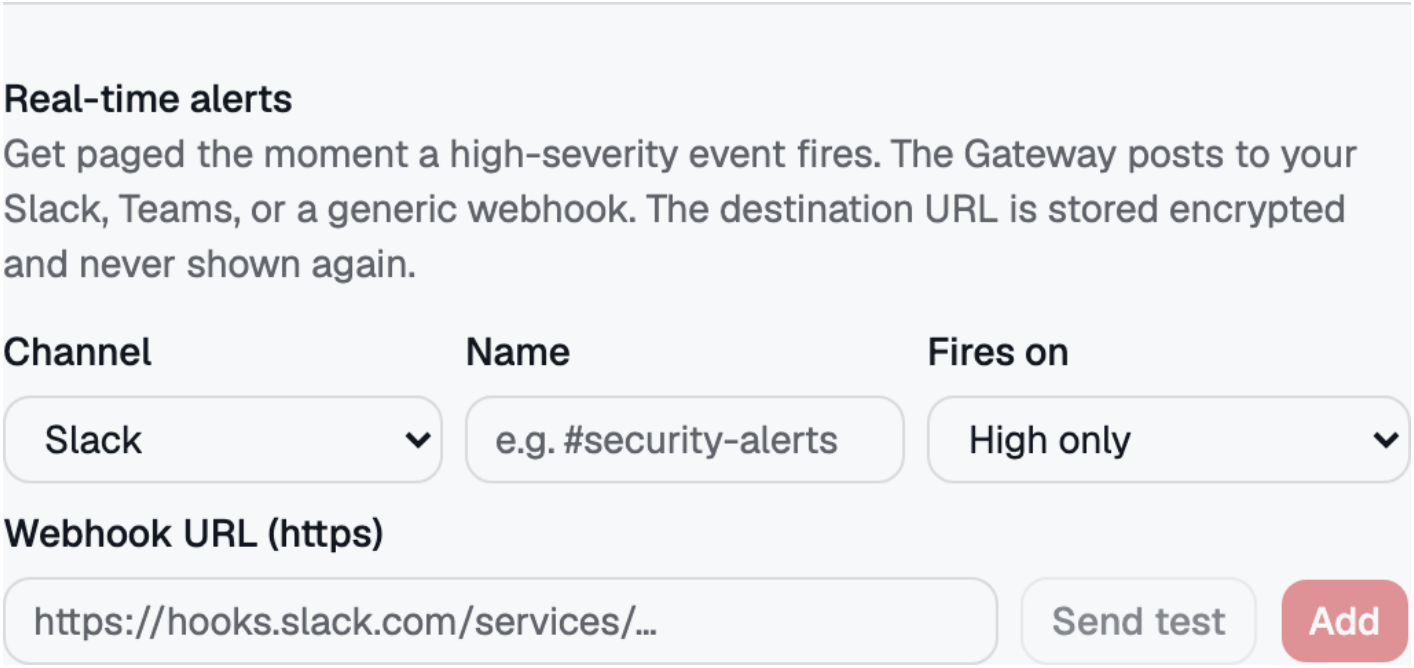
Enable, disable, remove

Each channel can be disabled without losing its configuration — useful during a noisy migration — and removed permanently.

Choosing a severity

Start at **High only**. A security channel that fires constantly is a channel people mute, and a muted channel is worse than no channel because you believe you are covered.

Widen to Medium once you know what High actually produces in your organization.



Alert channels — Slack, Teams or a plain webhook, with a test send before you save.

What alerts are for

The delivery guarantee

Alerts are **fire-and-forget**. Delivery is attempted alongside the request, never in front of it: a Slack outage cannot slow down or fail your developers' AI traffic. The trade-off is that an alert can be lost if the destination is unreachable, so alerts are a notification mechanism and not an audit trail.

The audit trail is Activity, Compliance and your SIEM. If you need guaranteed delivery of every event, use Stream events to your SIEM — that path is built for completeness. Alerts are built for attention.

What to route where

- **Slack or Teams** for the things a human should look at today: high-severity classifier verdicts, secrets blocked, a lethal-trifecta block.
- **A generic webhook** when you want to drive something automatic — open a ticket, page someone, tag a device in your own tooling.

Multiple channels

You can have several, each with its own severity threshold. A common arrangement is a noisy engineering channel at "Medium and up" and a quiet security channel at "High only".

What not to do

Do not use alerts as your compliance evidence. When an auditor asks what happened in March, the answer comes from the evidence pack on **Compliance**, not from a Slack channel with a 90-day history and no guarantee of completeness.