SIEM: push over syslog

The push option: Sentilai sends events to your collector as they happen.

Configuring

SIEM Export ? push:

- **Enable delivery**
- **Host** and **Port** (6514 by default)
- **Protocol** — TLS encrypted, or TCP plaintext
- **Sender hostname** — how the events identify themselves in your SIEM

Use TLS. Plaintext exists for collectors inside a network you already trust; audit events describing your AI traffic are not something to put on the wire in the clear.

Restrictions

One destination per organization. Private and internal hostnames are rejected — the collector must be reachable from Sentilai, so a `10.x` address will not work. Terminate TLS on something with a public name, or use the pull API from inside your network instead.

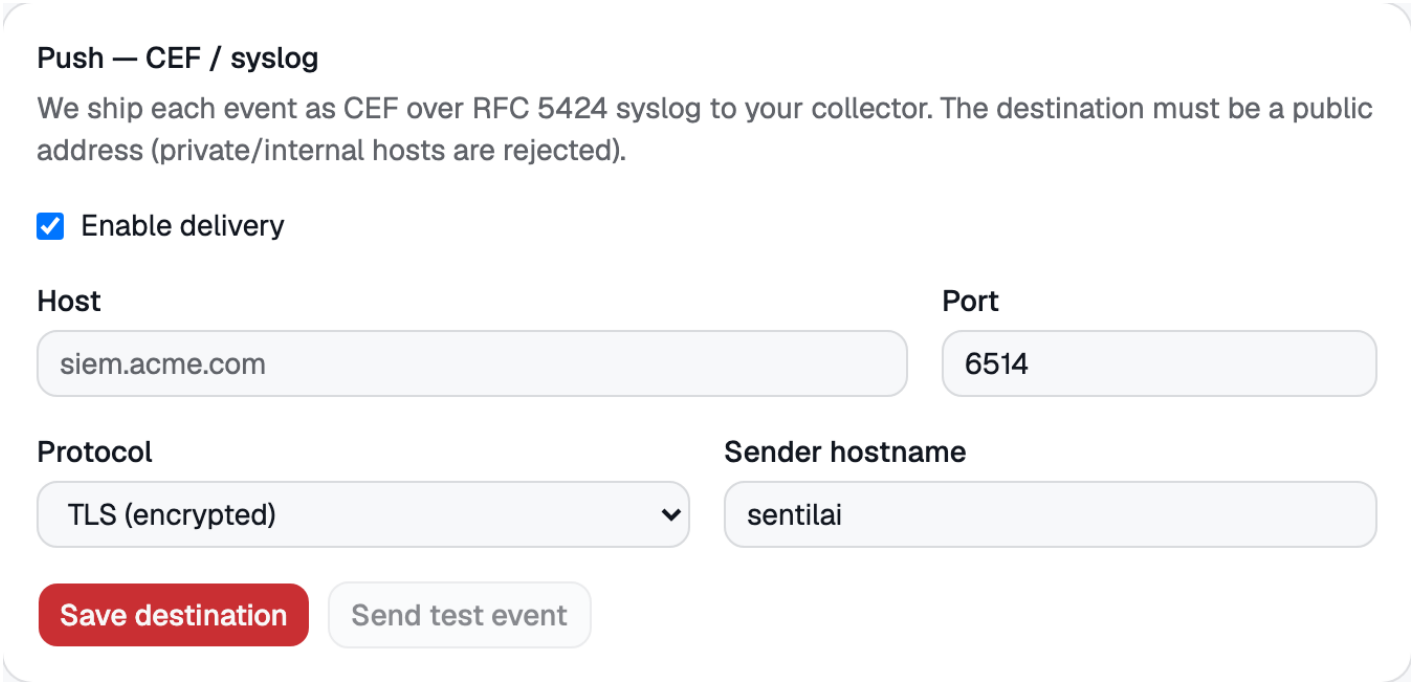
Test it

Send test event delivers a `siem_push_test` event. Look for it in your SIEM before assuming the integration works.

Delivery status

The panel shows the delivered count, last success, last attempt, and the last error. When push stops working — an expired certificate, a moved collector — this is where it shows up. The status badge reads **Active** or **Paused**.

Check it occasionally. Silent failure of an audit pipeline is the failure mode that matters most and announces itself least.



The push card on SIEM Export — syslog destination, TLS, and live delivery status with the last error if one occurred.

Revision #11
Created 2026-08-02 10:19:37 UTC by Sentilai Docs
Updated 2026-08-06 04:31:44 UTC by Sentilai Docs