User Guide

Using the Synapse-Vanguard dashboard

Audience: Security Analysts and Read-Only Auditors

Version 0.3.0

Self-hosted, data-sovereign Security Information & Event Management

1. Introduction

Synapse-Vanguard is a self-hosted, data-sovereign SIEM. It collects security events from your hosts and network, normalizes them, and lets you search, triage and alert on them from a single web dashboard. All data stays on your own infrastructure.

This guide covers day-to-day use of the dashboard. Administrative setup (deployment, agents, API keys, alert rules) is covered in the separate *Administrator Guide*.

2. Signing in

Open the dashboard in a browser:

```
http://<VANGUARD-HOST>:5500/
```

Enter your username and password. Sessions are short-lived JSON Web Tokens that refresh automatically while you work. Your role determines what you can see and do:

Role	What you can do
Read-Only Auditor	Search and export events; read-only. No tuning or admin.
Security Analyst	Everything above, plus tune out false positives and run triage.
System Administrator	Everything, plus the Admin menu (users, agents, alerts, API, webhooks).

3. The dashboard at a glance

The main screen is an event search. From top to bottom:

- **Header** - the Synapse-Vanguard wordmark, your username and role, and (for admins) the **Admin** menu.
- **Filters bar** - narrow events by source type, host, minimum severity, or message text.
- **Toolbar** - the result count, a live **events/sec** meter (server receive rate), a **Live tail** toggle, and - for Analysts/Admins - the **Tuning** button (bell icon).
- **Events table** - the matching events, newest first.
- **Agents** - a panel of enrolled log-shipping agents and their status.

4. Searching events

Use the filters bar, then press **Search** (or toggle Live tail for a rolling view). Filters combine together:

Filter	Effect
Source type	Limit to one source, e.g. winlog, journald, syslog, auditd, ironnode.
Host	Exact hostname match.
Min severity	Show events at or above a severity (Emergency is most severe).
Message contains	Free-text substring match on the event message.
Limit	Maximum rows returned (100-1000).

Reset clears the filters. **Live tail** re-runs the search every 5 seconds so new events appear automatically; the pulsing dot shows it is active.

5. Reading an event

Each row shows the timestamp (UTC), severity, source, host, event ID and message. Chips inside the message column add context:

- **Severity tag** - colour-coded (see the table below). Emergency and Critical events pulse red and highlight the whole row so they stand out.
- **Source chip** (cyan) - the log source type.
- **ATT&CK chip** (violet) - the MITRE ATT&CK technique, when Vanguard recognises the event (e.g. T1110 for brute force).
- **Alert chip** (amber, bell icon) - a named keyword Alert (see section 7).

6. Severity levels

Vanguard uses the standard syslog severity scale (0 = most severe). Colours make the important ones jump out:

Level	Name	Appearance
0	EMERGENCY	Red - pulses, whole row flashes
1	ALERT	Rose
2	CRITICAL	Red - pulses, whole row flashes
3	ERROR	Orange
4	WARNING	Amber
5	NOTICE	Blue
6	INFO	Slate (muted)
7	DEBUG	Dim grey

7. Alerts (named keyword detections)

Administrators can define **Alert rules** that watch for keyword(s) in event messages. When an event matches, Vanguard re-tags it as a named Alert (for example "Ransomware" or "Brute Force") at a chosen severity. These appear in the events table with an amber Alert chip carrying the alert name, and can be filtered like any other event. You do not configure these yourself unless you are an administrator - see the Administrator Guide.

8. The Agents panel

Below the events table, the Agents panel lists the log-shipping agents installed on your hosts. For each agent you can see the hostname, its source IP, the last sequence number it shipped, and whether it is active or revoked. A live dot indicates a healthy, active agent. (Managing agents requires an administrator.)

9. Tuning out false positives

If a benign event is being alerted on, an Analyst or Administrator can **tune it out** so it stops triggering in future. Tuning does not delete anything - the event is still logged; it just stops being escalated (no severity bump, no alert, no webhook).

Two ways to create a suppression:

- **From an event** - click the bell (Tuning) icon on an alerted row. A form opens pre-filled with that event's details. Adjust and save.
- **From the toolbar** - click **Tuning** to open the suppressions manager and add one manually.

A suppression can match on any combination of **alert type**, **host**, **source type** and **message text** - all conditions you set must match. The more fields you set, the narrower the suppression.

> **TIP** Prefer narrow suppressions. Setting a host and a message substring targets one noisy source without hiding genuine alerts elsewhere.

In the Tuning manager you can enable/disable a suppression with its toggle (disabling immediately resumes alerting) or select and delete suppressions you no longer need. The "Suppressed" column shows how many events each one has muted.

10. Roles & permissions

Capability	Auditor	Analyst	Admin
Search / export events	Yes	Yes	Yes
Tune out false positives	No	Yes	Yes
Manage alert rules / webhooks / API	No	No	Yes
Manage users / agents / system	No	No	Yes

11. Getting help

- If the dashboard will not load, confirm the server is running and reachable on port 5500 (your admin can check `/healthz`).
- If you are signed out unexpectedly, your session expired - sign in again.
- For anything requiring the Admin menu (new alert rules, agents, users), contact your Synapse-Vanguard administrator.