

Anleitung für System-Admins (SA)

Technischer Betrieb: Nutzerkonten, Audit-Log, Monitoring, API

Rollen-Abgrenzung (seit 07.07.2026): Der SA arbeitet „technisch, ohne Dateninhalt“ — kein Zugriff auf Auswertung/Einzelauswertung, keine Klarnamen, keine Ergebnisdaten über die API. Verwaltung (Erhebungen, Fragebögen, Nutzer, Audit-Log, Monitoring) bleibt vollständig.

1. Nutzer:innen & API-Keys

Menü **Administration** → **Nutzer:innen**: Konten anlegen/deaktivieren, Rollen und Einrichtung zuordnen. Der **Aktiv-Schalter** sperrt sofort Login und API.

PAL Kompetenzmess

 **ES**

 Dashboard

 Erhebungen

 Erhebungen

 Fragebögen

 Fragebögen

 Kohorten

 Auswertung

 Auswertung

 Einzelauswertung (T1-T3)

 Administration

 **Nutzer:innen**

 Audit-Log

Nutzer:innen > Übersicht

Nutzer:innen

Erstellen

 0

☐	Name ▾	E-Mail	Rolle	Einrichtung	Aktiv	Letz
☐	PAL Super-Admin	admin@pal.hszg.de	super_admin	Hochschule Zittau/Görlitz (HSZG)	✓	—
☐	Demo Einrichtungs-Admin	ea@demo.de	einrichtungs_admin	Demo-Einrichtung	✓	—
☐	Demo Fachnutzer	fn@demo.de	fachnutzer	Demo-Einrichtung	✓	—
☐	E2E SUP	e2e-sup@test.de	super_admin	—	✓	—
☐	E2E SA	e2e-sa@test.de	system_admin	—	✓	—
☐	E2E EA	e2e-ea@test.de	einrichtungs_admin	E2E Testfirma	✓	—
☐	E2E FN	e2e-fn@test.de	fachnutzer	E2E Testfirma	✓	—

pro Seite 10 ▾

Nutzerverwaltung: Rollen, Status, API-Key-Aktion je Zeile.

API-Key erzeugen (Aktion in der Nutzerzeile): Der Schlüssel wird **einmalig** angezeigt — gespeichert wird nur ein Hash. Verlorener Key = neuen erzeugen (der alte wird ungültig).

2. Audit-Log

Menü **Administration** → **Audit-Log** (nur lesbar): Logins/Logouts, Änderungen an Stammobjekten, **jeder Export** (wer, was, Format, Zeilen), API-Zugriffe, Consent-Widerrufe, Retention-Läufe.

Dashboard

Erhebungen

Erhebungen

Fragebögen

Fragebögen

Kohorten

Auswertung

Auswertung

Einzelauswertung (T1-T3)

Administration

Nutzer:innen

Audit-Log

Audit-Log > Übersicht

Audit-Log

Suche

Zeit	Bereich	Ereignis	Nutzer	Objekt	
07.07.2026 10:52:13	auth	Login	E2E FN		Anzeigen
07.07.2026 10:52:11	auth	Login	E2E EA		Anzeigen
07.07.2026 10:52:09	auth	Login	E2E SA		Anzeigen
07.07.2026 10:52:07	auth	Login	E2E SUP		Anzeigen
07.07.2026 10:52:02	default	created	System	Cohort	Anzeigen
07.07.2026 10:52:02	default	created	System	Questionnaire	Anzeigen
07.07.2026 10:52:02	default	created	System	Survey	Anzeigen
07.07.2026 10:29:49	auth	Login	E2E FN		Anzeigen
07.07.2026 10:29:47	auth	Login	E2E EA		Anzeigen

Revisionssicheres Audit-Log mit Filter nach Ereignistyp.

3. Monitoring

Werkzeug	Zweck
<code>/horizon</code>	Queue-Zustand, fehlgeschlagene Jobs (Retry direkt dort)
<code>/telescope</code> (nur SA/SUP)	Fehler, langsame Queries, Schedule, Mail-Vorschau — in Prod nur Fehler/Slow/Failed
<code>/metrics</code> (mit METRICS_TOKEN)	Prometheus-Kennzahlen (<code>pal_up</code> , <code>pal_queue_size</code> ...); optional Compose-Profil <code>monitoring</code> (Prometheus+Grafana)

/up	Healthcheck für externe Uptime-Überwachung
-----	--

4. Wiederkehrende Jobs

Zeit	Job	Prüfen
03:00	<code>retention:enforce</code> — Klardaten-Anonymisierung	Audit-Log „retention“; Probelauf mit <code>--dry-run</code>
08:00	<code>reminders:dispatch</code> — Kohorten-Erinnerungen	Horizon (Mail-Jobs)

`php artisan schedule:list` zeigt die Registrierung; der `scheduler`-Container muss laufen.

5. REST-API

- Auth: Header `X-API-Key: <key>` oder `Authorization: Bearer <key>`
- Lesend: `GET /api/v1/me`, `/surveys`, `/surveys/{id}/results` (pseudonymisiert + Aggregat), `/cohorts`
- Schreibend: `POST /api/v1/surveys/{id}/participants` mit `{"count": 10}` und/oder `{"persons": [...]}` — Antwort enthält die Zugangs-Tokens
- RBAC gilt auch hier; jeder Zugriff wird auditiert. Details: `docs/spec/rest-api.md`

6. Störungen

Playbooks im Betriebs-Runbook (`docs/RUNBOOK.md`, Abschnitt 8): Admin-500 (intl), unstyled Survey (Vite-Assets), fehlende Ergebnisse (Worker), PDF-Fehler (Gotenberg), RLS (DB-Rolle), Traefik/Session.

[← Zurück zur Übersicht aller Anleitungen](#)