Audit Log Export — Specification

Schema, retention, and integration options for SIEM and compliance teams.

Overview

ThermoCalc Enterprise emits an immutable audit trail for every security-relevant action. Logs are exportable on demand via the admin console or programmatically via a signed REST endpoint.

Event categories

- **auth.*** — sign-in, sign-out, SSO assertion, MFA challenge, failure.
- **session.*** — calculator session created, opened, modified, shared, deleted.
- **export.*** — PDF/CSV/Excel export with target hash.
- **admin.*** — user added/removed, role changed, SSO config changed, retention changed.
- **billing.*** — subscription change, seat add/remove, invoice generated.

Record schema (JSON Lines)

```
{
  "event_id": "evt_01HQ...",
  "occurred_at": "2026-05-19T14:23:01.482Z",
  "org_id": "org_abc123",
  "actor": { "user_id": "usr_...", "email": "jane@acme.com", "ip": "203.0.113.4" },
  "category": "export",
  "action": "export.pdf",
  "target": { "type": "session", "id": "sess_...", "name": "Psychrometric — AHU-3" },
  "meta": { "file_sha256": "...", "page_count": 4 },
  "request_id": "req_..."
}
```

Delivery options

- **On-demand export:** admin console → Audit → Export. CSV or JSONL. Date-range filter.
- **Scheduled S3 sync:** daily or hourly drop to a customer-owned bucket. We provide an IAM policy.
- **SIEM webhook:** signed POST to a customer endpoint. HMAC-SHA256 over the body with a rotating secret.
- **Splunk HEC / Datadog Logs:** direct forwarder available on request.

Retention

- Logs retained according to the org policy: 90 days, 1 year, or 7 years (audit-grade).
- Immutable: events are append-only, signed with a daily Merkle root for tamper evidence.
- Deletion: only via documented retention policy or on contract termination.

Integrity verification

Each daily batch is hashed; the Merkle root is published in the admin console and included in the export bundle. Auditors can independently verify that no events have been altered or removed.

Access control

- Only users with the **auditor** or **admin** role can read or export logs.
- Export events are themselves logged (**admin.audit_export**).

Sample CSV columns

```
occurred_at, event_id, category, action, actor_email, actor_ip, target_type, target_id, target_name,
meta_json, request_id
```