

Audit trail and export

DOCUMENT	VERSION	STATUS
SB-GD-114	1.0, October 2026	Public. Checked against the product, October 2026

Who this is for

Workspace owners and admins who need to review what happened in their workspace and copy audit records into their own tools.

Before you start

- You need the Admin or Owner role. Members who open the page see a message that the full audit trail is for admins and owners only.
- The plan entitlements list the Audit trail from the Pro plan up, and the signed export and SIEM streaming from the Business plan up.
- SIEM streaming is Beta.
- The audit trail is designed to hold counts and metadata about activity, not the text of prompts or responses.

Where to find audit information

SynapBridge has three audit views. They cover different event families, so check the one that matches your question.

- 1 Governance > Audit trail. Security, redaction, policy and cost events for your workspace.
- 2 Admin center > Identity & access > Audit logs. Administrative actions: users, groups, roles, SSO, directory sync, DLP, BYO-K, SIEM streaming, cost caps, conditional access, MFA policy and access reviews.
- 3 Admin center > Identity & access > Sign-in logs. Sign-in events by method and outcome.

Note The Audit trail page itself says that automated control-execution and audit-log records are tracked separately, under Compliance > Evidence.

What a record contains

Each row in Governance > Audit trail shows these columns: Time, Kind, Action, Source and Actor. The kinds are SecurityEvent, RedactionEvent, PolicyDecisionEvent and CostEvent.

Select a row, or use its row menu, to open Event detail. It has three tabs:

- Summary: kind, action, source, actor, time and the Event ID.
- Detail: any extra fields the producing feature recorded.
- Raw: the full event as JSON.

Some events have no durable event ID. Those can still be copied and exported, but they cannot be used to draft a workflow or agent.

What a record does not contain

Raw content is stripped from audit events when they are ingested, and the page says "Counts and metadata only." Fields with these names are removed, including inside nested objects: prompt, response, content, message, body, query, sample, completion, input and output. The page footer lists the first six of these. The stripping works on field names, so it is a safeguard, and text could still appear under other field names.

Filter the Governance > Audit trail

- Category chips (multi-select): Onboarding, Workspace state, Query, Retrieval, LLM invocation, Content policy, IP defense, Hallucination, Workflow and Connector.
- Date: Any time, Last 7 days, Last 30 days, or a start and end date. With Any time, the page shows the last 7 days.
- Source: a substring match on the source name.
- Search: matches actor, event type, resource or summary.
- Event type: an exact event type.
- Kind: All kinds or one of the four kinds above.
- User: filter by user ID, or choose Just me.
- Limit: 25, 50 or 100 rows per page. Choose Load older events to page back.

The page shows the window it queried ("Showing events from ... to ..."). Set a date range to look further back. Use Clear all filters to reset. You can switch between a Table view and a List view.

Filter the Admin center audit logs

Filters: From, To, Actor, Category, Action and Target. Categories include User, Group, Role, SSO, Directory sync, DLP, BYO-K, SIEM streaming, Cost cap, Conditional access, MFA policy, Access review, Workflow anomaly and Other. Actions include Create, Update, Delete, Assign, Revoke,

Enable, Disable, Test, Rotate and Trigger. Select a row to see the change detail.

Export

Export as evidence (JSON)

On Governance > Audit trail, choose Export page as evidence to download the rows currently shown. For one row, choose Export as evidence. To export several, select the rows and choose Export selected as evidence. The file is JSON with the export time, the exporting user, the event count, the event IDs and the events. It is built in your browser from the rows already loaded.

Signed audit export (NDJSON)

- 1 Open Governance > Audit trail as an admin or owner.
- 2 Open the page's overflow menu and choose Export audit log (SIEM / signed export).
- 3 A file named audit-export-(timestamp).jsonl downloads.

Details:

- The format is newline-delimited JSON (NDJSON). Each line holds one event and a signature (an HMAC-SHA256 of the event).
- Each call returns up to 1000 events, newest first. When a page is full, the API returns a cursor for the next page in the x-audit-export-cursor response header. The menu item does not send your on-screen filters or a cursor, so it downloads one page.
- The API route (GET /api/v1/audit/export) accepts since, until, event_type, user_id and cursor.
- The export is built from administrative audit events, the same family as Admin center > Identity & access > Audit logs. Each event carries its ID, tenant, category, actor, target, action, outcome and time, with extra detail such as target type, actor email and the change diff where available. It does not carry the Governance > Audit trail kinds listed above.
- If the export is not set up for your workspace, the page says "Signed export is not available for your workspace yet. Contact SynapBridge support to enable it." If nothing matches, it reports that there is nothing to export.

CSV export of admin audit logs

On Admin center > Identity & access > Audit logs, choose Export CSV. The download keeps the filters you have set.

Scheduled reports for FinOps saved views

This is not an audit report. In Insights > FinOps, the Saved views and scheduled reports panel lets you save a date range and grouping as a named view, then choose Schedule to email it.

- Cadence: weekly only. You choose the day and the hour (UTC).
- Format: CSV or PDF.
- The report is emailed to you.

SIEM streaming (Beta)

Admin center > Security & compliance > SIEM streaming sends admin audit events, sign-in events and DLP detections to your own SIEM. It is owner only and requires the Business plan.

- 1 Choose Add destination.
- 2 Pick a provider: Splunk HEC, Datadog, Sumo Logic, Microsoft Sentinel, Elastic, Generic HTTPS or Syslog (TCP).
- 3 Enter a display name, the endpoint URL and the auth token or API key. The secret is stored in AWS Secrets Manager and is not shown again after you save.
- 4 Choose the event categories to forward. The defaults are admin, signin and dlp. Other categories include llm_activity, policy_decision, cost, security, workflow, connector and tenant_state. Higher-volume categories can raise your SIEM ingest costs.
- 5 Save, then choose Test to send a test event. Each destination shows its last delivery status and has an enable toggle, so you can pause it without deleting it.

If streaming is not turned on for your workspace, the page says so and tells you to contact SynapBridge support.

Retention

- Governance > Audit trail reads a recent-events store that keeps events for 90 days by default. With no date range set, the page shows the last 7 days. The page tells you the window it queried.
- This document does not state any retention period beyond that recent-events store. Ask SynapBridge support for the retention that applies to your workspace.

Limits and notes

- The audit trail is a record of activity. It is not a substitute for your own review process, and it is not offered as proof of any certification. SynapBridge is architected to align with the SOC 2 Trust Services Criteria, and a HIPAA BAA program is planned.
- The signed export is built for feeding your own SIEM. SynapBridge does not provide SIEM search, correlation or alerting.
- Some product actions may not produce audit events yet, so do not treat the trail as a complete list of everything that changed.

- The Audit trail page and the signed export read from different sources and cover different event families.
- The Notifications action on the Audit trail page shows a 90-day delivery log and lets you save your own view preferences.