FAQ: Audit and logging

From the SourceLace manual: What SourceLace's audit trail records, what it never records, who can read it, how it is protected, and how long it is kept.

SourceLace version 0.1.0 · Made November 22, 2026
The latest version is at https://sourcelace.ai/docs

Audit and logging

What SourceLace's audit trail records, what it never records, who can read it, how it is protected, and how long it is kept.

What does the audit trail record?

Every tool call, whether it succeeded, was refused or failed, from the SourceLace app, from every AI app and from admins. Also every sign-in (including refused ones), every change to people, sources, groups, single sign-on and settings, every AI agent run, step and approval, and each query result held and deleted. Each entry holds when, who, the action, the source, the query text, the object and record id, the names of changed fields, how many rows came back, the outcome and how long it took.

Details: The audit trail.

What is never in the audit trail?

Row values, field values, passwords, keys and tokens. One thing to know: the query text is kept as written, so a value typed into a question's filter (such as a customer name like "Corvanta") appears in the trail your admins read; the trail is stored encrypted with your organization's own key. Entries written before that was added are encrypted in the background; you do not need to do anything. For health record sources, only the names of search parameters are kept, not their values.

Details: The audit trail.

Who can see what my people asked?

Your admins, in the audit trail: who called which action on which source, the query text, and how many rows came back, never the rows themselves. Saved chats are private to the person who had them; admins do not read them.

Details: The audit trail.

Is everything audited, from every AI app?

Yes. The audit trail is the same whether someone asks from Claude, ChatGPT, any other AI app, the SourceLace app or an AI agent. If SourceLace cannot write an entry, the call fails rather than returning data that was not recorded. Before a change is sent to a system, SourceLace records that it is starting.

Details: The audit trail.

Where do admins read the audit trail?

On the **Audit log** page in the SourceLace app, on the Business and Enterprise plans. It filters by time, person, action, source, object and outcome, shows SourceLace staff's entries on their own with **SourceLace staff**, and has a text search of the person, action, source, object, record id and error (not the words inside a query's text). On every plan, every call is still recorded and counted on the **Usage** page.

Details: The audit trail and Locked features.

Is the audit trail tamper-evident?

Yes. Entries are chained together for each organization, so an entry that was changed, removed or reordered breaks the chain, and SourceLace detects it. SourceLace checks the audit trail automatically every day and alerts your admins if anything does not match. You can also check it yourself at any time and export it with its proof. The JSON export from the **Audit log** page says whether your whole trail still verifies, and carries each entry's hashes so your own reviewers can recheck them.

Details: Is the audit trail tamper-evident?.

How long is the audit trail kept?

For your plan's audit history: 90 days on Starter, 1 year on Team, 3 years on Business and 7 years on Enterprise. Older entries are deleted automatically, oldest first, and the entries kept can still be verified.

Details: The plans.

Can we export the audit trail or send it to our SIEM?

Yes, you can export it yourself. On the **Audit log** page (Business and Enterprise), **Export** downloads every entry matching your period and filters as CSV for a spreadsheet, or as JSON with each entry's hashes and a check of your whole trail for a security review. On other plans, ask support@sourcelace.com for an export.

Yes, you can also stream it to your SIEM (Business and Enterprise). On the **Audit log** page, under **Streaming**, an admin adds up to five destinations: a signed webhook, Splunk's HTTP Event Collector, or a bucket in Amazon S3, Google Cloud Storage or Azure Storage. New entries are sent within seconds, in batches, each with a hash proof that links it to the batch before, so your SIEM can check that nothing is missing or changed. A destination that is down is tried again until it takes the entries; nothing is skipped.

Details: Exporting the audit log, Streaming the audit trail and Can we see and export it?.

Are SourceLace staff actions recorded?

Yes. Every change SourceLace's staff make to your organization is recorded in your own audit trail under their name: your plan, discounts, credits, billing, contract, admins, single sign-on, features, setup help and more, from the moment your organization was created. So is every time they read or export your audit log, look at your setup readiness, or approve a setup change you allowed them to. Admins see all of it on its own with **SourceLace staff** on the **Audit log** page. Changes that apply to every organization at once, such as list prices, are not in your trail.

Details: What SourceLace staff did and Help from your SourceLace contact.

Can we prove that results were deleted?

Yes. Each held result writes an entry: which source, how many rows, how long and where it is held, and when it is deleted. An early deletion, such as a closed chat, writes its own entry with the reason. None of these entries hold row values.

Details: Data retention controls.

Are AI agents audited?

Yes. Creating, editing and turning an agent on or off, each run, each step and each approval are recorded. So are calls from other systems or agents that start an agent, and each large read an admin pre-approved for an agent.

Details: For admins.

Are data protection rules and masking audited?

Yes. Every rule change is in the audit trail, and each call's entry records how many fields were hidden and how many values masked, never the values themselves.

Details: Audit.

Are sign-in and provisioning changes audited?

Yes. Every sign-in, including refused single sign-on sign-ins, and every change to single sign-on settings is recorded. Every change your identity provider makes through automatic provisioning is listed too, with which token it came through and which details changed, never their values.

Details: What it does and SCIM provisioning.

Does SourceLace record our AI use?

Yes, as counts. For each question in the SourceLace app it records who, when, which model and how many tokens, never the question or the answer. The **Usage** page shows calls, rows and AI use per person, model, action and source.

Details: What SourceLace stores and Status, usage and invoices.

Do SourceLace's own system logs contain our data?

Not your records. SourceLace's own logs never contain tokens, passwords or query results. A runner's support bundle, which an admin may send to support, holds no tokens, keys, passwords, data or run results. The one thing to know: the servers in front of SourceLace record the web address of each request and keep those records for 365 days, and on some lists the words you type into the search box are part of that address (see Searching and sorting lists).

Details: What is never logged?.

How do I look at what happened in one hour of one day?

On the **Audit log** page, set **When** to **Custom range** and give a start and an end with the date and the time, for example Monday 9:00 AM to 11:30 AM. Times are in your own time zone, which is named under the control. The page starts on the last 7 days, **Clear filters** goes back to it, and the period is kept in the page's address so you can share the link (the Person, Action, Source and Object choices and the words typed in **Search** are not: they can be email addresses or names, so a refresh starts with none of them chosen). **Export** downloads exactly the entries in the period you set.

Details: Finding entries.