

Admin guide

From the SourceLace manual: For your organization's SourceLace admins: who can sign in, single sign-on, groups and access by group, sources, turning on changes, AI settings, the audit trail and how long things are kept.

SourceLace version 0.1.0 · Made October 4, 2026

The latest version is at <https://sourcelace.onrender.com/docs>

Admin guide

For your organization's SourceLace admins: who can sign in, single sign-on, groups and access by group, sources, turning on changes, AI settings, the audit trail and how long things are kept.

Everything here is done in the [SourceLace app](#) by someone with the **admin** role. Most of it can also be done by asking an MCP client in plain words, which calls SourceLace's admin tools (`admin_people`, `admin_sources` and `admin_groups`). Single sign-on is set up in the app only, so a client secret never has to be typed into a chat. Every admin change is recorded in your organization's audit trail.

Roles

Role	Can
Member	Connect sources with their own logins, ask questions, propose changes (where allowed), keep their own skills, chats and projects.
Admin	Everything a member can, plus manage people, email domains, sources, groups, single sign-on, settings, shared skills, and read the audit trail, usage and invoices.

Every organization always keeps at least one admin: SourceLace refuses to remove or demote the last one.

What your organization can use (seats, connectors, AI questions, and features such as access by group) depends on its plan. See [Plans and limits](#).

People and sign-in

People sign in to SourceLace with **Google**, **Microsoft**, or your organization's own identity provider through [single sign-on](#). SourceLace never sees their password: it receives a confirmed email address from the identity provider and checks it against your organization's people.

There are two ways someone gets in:

- **Invited.** On the **Team** page, under **Invite someone**, enter their email address and choose **member** or **admin**. From chat: "Add bo@corvanta.com to SourceLace as a member". Invited people stay in even if you later remove the email domain they are at.
- **By email domain.** Under **Email domains**, list your domains (such as `corvanta.com`). Anyone who signs in with a verified address at one of them joins as a **member**. Public domains such as `gmail.com` are refused. If you remove a domain, the people who joined through it lose access.

Each person is one seat. The Team page shows how many seats are used of your plan's maximum; on Starter and Team, nobody new can join once it is reached (see [Seats](#)).

The Team page shows each person's role, how they joined (invite, domain or single sign-on) and when they last signed in. To change a role, pick it next to the person; to remove someone, remove them there. **Removing someone ends their SourceLace sign-in at once and deletes their sign-ins to every source.**

A few details about how sign-in works:

- **Microsoft accounts.** For a work or school account, SourceLace uses the person's Microsoft sign-in name (such as ana@corvanta.com), not the free-text email field, because only sign-in names are tied to domains your company has proved it owns. Add people by the address they sign in to Microsoft with. Guest accounts (someone from another company added to your directory) are refused; they sign in with their own company's account. Personal Microsoft accounts that sign in with a phone number cannot sign in.
- **One organization per person.** An email address belongs to one SourceLace organization.
- **How long sign-ins last.** In an MCP client, SourceLace's token lasts 1 hour and renews itself for up to 30 days; after that the person signs in again. In the SourceLace app, a session lasts 7 days.
- **People added by SourceLace's own server settings** (shown as joined by "settings") are managed by whoever runs your SourceLace server and cannot be changed on the Team page.

Single sign-on

Single sign-on is part of the Business and Enterprise plans. Your people can sign in through Okta, Microsoft Entra ID, Google Workspace, OneLogin, Ping, JumpCloud or any OpenID Connect provider, be added automatically on their first sign-in, and have their groups kept in step with your identity provider. You can also require single sign-on for your domains. See [Single sign-on \(SSO\)](#) for every step.

Sources

A **source** is one system your people can connect to, such as your production Salesforce org or a reporting database. Admins add sources on **Manage sources** (or from chat: "Add a SourceLace source salesforce:prod, kind salesforce, label Corvanta Salesforce").

Each source has:

Field	What it is
Kind	Which system it is, such as salesforce, snowflake or database. See Connecting your systems for every kind.
Name	The source's id, written kind:name, such as salesforce:prod or database:sales. Lowercase letters, numbers, dashes and underscores. People and their AI use this id. It cannot be renamed; add a new source instead.
Label	The name people see, such as "Corvanta Salesforce".
Options	Settings for that kind, such as a Salesforce login address or a Snowflake account. Each kind's page lists every option.
Allow changes and Objects that can be changed	Off by default. See Turning on changes .

How many sources of each kind you can add depends on your plan's connector classes and add-ons; connectors you cannot add are marked locked with the reason. See [Connectors](#).

Adding a source does not give anyone access to the data in it. **Each person still connects the source with their own login**, and sees only what that login can see.

Secrets in options. A few kinds take a secret as an option (the client secret for Oracle Fusion and Workday, and the shared secret for a custom connector). It is stored encrypted with your organization's own key, never shown again (the page shows (saved)), and never returned by any API or tool. To keep it while editing the source, leave the field as it is; to change it, type the new one. Type secrets on the Manage sources page, not into a chat with an AI.

Removing a source also removes everyone's sign-in to it and every group's access settings for it. Adding a source with the same name later starts afresh.

Turning on changes

SourceLace is read-only until you say otherwise. To let people create or update records in a source:

1. On **Manage sources**, edit the source and turn on **Allow changes**.
2. Under **Objects that can be changed**, list the objects, separated by commas, such as Opportunity, Case for Salesforce, deals for HubSpot, incident for ServiceNow, customer for NetSuite, invoices for Oracle Fusion, businessTitleChange for Workday or drafts for mail. * allows every object the source supports changes to.
3. Save. From chat: "Allow writes to Account and Opportunity on salesforce:prod".

Even then, every change is previewed first and applied only after the person confirms it, the person's own permissions in the system still apply, and, with access by group on, their groups must give them **read & write** on that object.

Some sources never accept changes through SourceLace, whatever this setting says: they are marked read-only on their pages and on the Manage sources page.

HubSpot, Zendesk and Jira: after you turn changes on or off, or change the objects, people connect that source again, so the system gives their sign-in the matching write permission. Until they do, the system refuses the change and SourceLace tells them to reconnect.

Access by group

Access by group lets you decide which people can use which sources, and which objects inside a source. For example: Sales can read Salesforce and change Opportunities; Finance can read SAP but not Salesforce.

It is **off** until you turn it on. While it is off, everyone in your organization can use every source. Access by group is part of the Business and Enterprise plans.

How it works:

- You create **groups** (such as "Sales") and add **people** to them. Only people already on the Team page can be added.
- Each group gets an **access level** per source: **no access**, **read**, or **read & write**.
- A group can also get a level for **one object** in a source, such as Opportunity. That replaces the group's whole-source level for that object: for example "read all of Salesforce, but no access to Opportunity", or "no access to Salesforce, except read on Account".
- Someone in several groups gets the **most** any of their groups gives, object by object.

- **Once it is on, someone in no group sees no sources at all.** That includes admins: admins can always manage groups, people and sources, but their own data access follows their groups. Put admins in a group if they also use the data.

To set it up, open **Groups**: create the groups, add people, set each group's access per source (and per object where needed), then turn **Access by group** on. From chat, the `admin_groups` tool does the same.

It only narrows access, never widens it. People still sign in to each source with their own account, so they see a record only if both their groups and the system itself allow it. **Read & write** does not by itself let anyone change data: the source must also allow changes to that object, and each change is confirmed. Groups are checked again when a change is applied, so taking access away also stops changes that were previewed but not yet applied.

Which objects a query reads. SourceLace works this out from the query before anything is sent: the object after `FROM` in SOQL, every table after `FROM` and `JOIN` in SQL, the entity set in OData, the object in JSON queries. When a query may reach objects it does not name (related fields such as `Account.Name`, subqueries, joins in some languages, `$expand`), it needs read access to the **whole source**. Someone with only object-level access gets a message asking them to query one object at a time.

Groups from your identity provider. Each group can carry an **external id**: the Okta group name, or the Microsoft Entra group's object id. With single sign-on and group sync on, every sign-in puts the person into the groups their identity provider lists and takes them out of the others that have an external id. Groups without an external id are managed by hand. See [Group sync](#).

Removing someone from the organization takes them out of every group. Chats saved before access was taken away keep what they already show; new questions follow the current groups.

AI settings

These apply to the assistant in the SourceLace app only. MCP clients use their own AI model, which SourceLace does not choose.

Open **Settings** → **AI model**:

- **Included with SourceLace** (the default): the assistant uses Claude, through SourceLace's Anthropic account. Your plan includes a number of AI questions per seat a month, shared by the organization, counted in credits. After them come any prepaid questions, then extra use up to the maximum you set under **Settings** → **AI use** (0 turns it off). At that maximum, chat in the app pauses until the 1st of the next month, or until you raise the maximum or add your own key. See [AI use](#). The **Usage** and **Billing** pages show your organization's use.
- **Your own Anthropic key**: paste a key from your organization's Anthropic account. Anthropic then bills you directly and questions use no SourceLace credits. The key is encrypted with your organization's own key, never shown again, and never returned by any API. Send a new key only when you want to change it.
- **Your own OpenAI key**: paste a key from your organization's OpenAI account (create one under **API keys** in the OpenAI platform; it starts with `sk-`). OpenAI then bills you directly, and questions use no SourceLace credits. When you save, SourceLace makes one free call to

OpenAI to check that the key works and can use the chosen model, so a mistyped key or a model your account cannot use is caught straight away. The key is stored and protected exactly like an Anthropic key.

You can also choose which model the assistant uses: the Settings page lists the models available for each choice. A larger model gives better answers at a higher cost.

SourceLace keeps one key for your organization. To switch between your own Anthropic key and your own OpenAI key, paste the other provider's key. Switching to **Included with SourceLace** and back keeps your saved key. Saved chats continue with whichever model you choose.

The **Usage** and **Billing** pages show token counts and an estimated cost for every choice, at the provider's list prices. With your own key, your provider's bill is the real figure.

If the assistant cannot answer, chat says why: for example that the provider refused the key, that your OpenAI account has run out of credit or reached its spending limit, that the provider is busy (try again in a minute), or that your account cannot use the chosen model (choose another in Settings).

What the assistant sends to the AI model is described in [Security and privacy](#).

The audit trail

Every tool call is recorded in your organization's audit trail, whether it succeeded, was refused or failed: from the SourceLace app, from every MCP client, and from admins. Admins see it on the **Audit Log** page (on the Business and Enterprise plans), with filters by time, person, action, source, object and outcome, and a text search.

Each entry holds **metadata only**: when, who, which tool and source, the query text, the object, the record id, the names of changed fields, how many rows came back, the outcome, the error type if any, and how long it took. It never holds row values, field values, passwords or tokens.

Entries are chained by hashes: each entry includes the hash of the one before it, so an entry that was changed, removed or reordered breaks the chain and is detected. If SourceLace cannot write an entry, the call fails rather than returning data it could not record. Before a change is sent to a system, SourceLace records that it is starting.

Sign-ins (Google, Microsoft and single sign-on, including refused ones) and every change to people, sources, groups and single sign-on settings are recorded too.

The same entries are the usage meter: the **Usage** page counts calls and rows per person, action and source, and AI questions and their estimated cost.

How long things are kept

What	Kept for
Query results	In memory only, for at most 30 minutes, then gone. Never written to a database.

What	Kept for
Saved chats in the SourceLace app, with the files made in them and project pins to them	30 days after the chat was last used, by default. Admins set the period under Settings → Chats , from 1 day up to the plan's longest (30 days on Starter, 90 on Team, 1 year on Business, 10 years on Enterprise). Anyone can delete their own chats at any time. Old chats are deleted automatically, checked every hour.
Skills and projects	Until someone deletes them.
Each person's sign-ins to sources	Until they disconnect, are removed from the organization, the source is removed, or the system ends the sign-in.
The audit trail	Kept. It is not deleted automatically today. Your plan's audit history (90 days to 7 years) is the least it is kept for.

See [Security and privacy](#) for what is stored and how it is protected.

Status, usage and invoices

- **Status** (everyone) shows whether the AI assistant is ready and, for each source, whether you are connected and how your calls went in the last 24 hours.
- **Usage** (admins) shows calls, rows and AI use over any period, per person, model, action and source.
- **Usage** also shows this month's AI credits: included, prepaid and extra use.
- **Billing** (admins) shows how your organization pays, your prices and discounts, Stripe's invoices with PDF links, and AI use month by month with the "Extra AI questions" line. See [Billing](#).

Getting help

Email support@sourcelace.com. The **Support** page in the app starts an email with your organization and browser filled in. Please don't send passwords, keys or customer data. Security questions: security@sourcelace.com.