# FAQ: Sign-in and single sign-on

From the SourceLace manual: How people sign in to SourceLace, single sign-on, automatic provisioning, and how long sessions last.

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

# Sign-in and single sign-on

How people sign in to SourceLace, single sign-on, automatic provisioning, and how long sessions last.

## How do people sign in to SourceLace?

With Google, Microsoft, or your organization's own single sign-on. SourceLace has no passwords of its own and never sees your people's passwords. It receives a confirmed email address from the identity provider and checks it against your organization's people.

Details: People and sign-in.

## Which identity providers do you support?

Any OpenID Connect or SAML 2.0 provider, such as Okta, Microsoft Entra ID, Auth0, Google Workspace, OneLogin, Ping, JumpCloud and ADFS. OpenID Connect is part of Business and Enterprise. SAML 2.0 is part of Enterprise.

Details: Single sign-on.

## Can we require single sign-on?

Yes. With **Require SSO** on, people at your domains can no longer sign in with Google or Microsoft, and sessions that did not come through single sign-on stop at once. SourceLace lets an admin turn it on only after signing in through single sign-on themselves, so a broken setting cannot lock you out.

Details: Turn it on in SourceLace.

## How do we switch to another identity provider?

An admin starts **Switch single sign-on provider** under **Changes**. It lists the steps in order: set up the new provider in SourceLace, sign in through it once, then remove SourceLace from the old provider. SourceLace ticks off the first two by itself when it sees them done. Your people keep their chats, groups and access, because SourceLace knows them by their email address, not by their provider.

Details: Switching to another identity provider.

## Do you support multi-factor authentication?

Through your identity provider. Because SourceLace has no passwords of its own, multi-factor authentication is whatever your Google, Microsoft or single sign-on setup requires. SourceLace has no separate MFA of its own.

Details: Do you support MFA?.

## Can our identity provider add and remove people automatically?

Yes, on Business and Enterprise: SCIM provisioning with Microsoft Entra ID, Okta or Ping Identity adds people, keeps their details and groups up to date, and removes their access the moment they leave, including their AI app connections and source sign-ins. It never makes anyone an admin unless you choose an admin group.

Details: SCIM provisioning.

## Can groups come from our identity provider?

Yes. Group sync updates people's groups at each single sign-on sign-in, and SCIM provisioning keeps them in step all the time. A group from your identity provider gives no access by itself: you decide what each group may use.

Details: Group sync and Groups and access.

## How long do sessions last?

A session in the SourceLace app lasts 7 days. An AI app's access lasts 1 hour and renews itself; if the AI app is not used for 30 days, the person signs in again. Admins can make these shorter on the **Limits** page. A removed person is refused at their next request, without waiting for anything to expire.

Details: How long do sessions and tokens last?.

## What if our identity provider is down while single sign-on is required?

Contact support@sourcelace.com. SourceLace can turn **Require SSO** off for your organization so people can sign in with Google or Microsoft. The reason is recorded in your audit trail, and your admins see who turned it off, when and why. Turn it back on yourself when your identity provider works again.

Details: Turn it on in SourceLace.

## Can one person belong to two organizations?

No. An email address belongs to one SourceLace organization. Microsoft guest accounts (someone from another company added to your directory) are refused; they sign in with their own company's account.

Details: People and sign-in.

## Why does SourceLace ask me to Allow when I connect my AI app?

Any AI app can ask to connect, so after you sign in SourceLace shows a page that names the app and the address it will send you back to, and waits for you. Choose **Allow** only if you just started connecting that app yourself. If a link or a message sent you there, or you do not recognize the address, choose **Cancel**: nothing is sent to the app. The page asks every time an app connects (an app not used for 30 days connects again), and only the browser that opened it can answer it.