

Single sign-on (SSO)

From the SourceLace manual: Have your people sign in to SourceLace through your own identity provider (Okta, Microsoft Entra ID, Google Workspace, OneLogin, Ping, JumpCloud or any OpenID Connect provider), add them automatically on their first sign-in, require SSO for your domains, and sync their gr

SourceLace version 0.1.0 · Made October 4, 2026

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

Single sign-on (SSO)

Have your people sign in to SourceLace through your own identity provider (Okta, Microsoft Entra ID, Google Workspace, OneLogin, Ping, JumpCloud or any OpenID Connect provider), add them automatically on their first sign-in, require SSO for your domains, and sync their groups.

Single sign-on is part of the Business and Enterprise plans (see [Plans and limits](#)).

Status: in testing. Single sign-on is built to the OpenID Connect standard and covered by automated tests; tell support@sourcelace.com when you set it up so we can help with your first sign-in.

SAML-only identity providers are not supported yet; SAML support is planned. Almost every modern identity provider, including all of those above, offers OpenID Connect, so use that.

What it does

- **Sign-in.** The SourceLace sign-in page, and the page an MCP client opens, offers **Continue with SSO / work email** next to Google and Microsoft. The person types their work email; if its domain belongs to an organization with SSO, they are sent to that organization's identity provider, sign in as they do every day, and come back signed in to SourceLace.
- **New people are added automatically.** The first time someone signs in through SSO, SourceLace adds them to your organization as a **member**. Admins can make them admins on the Team page. The Team page shows them as joined by "Single sign-on".
- **Require SSO (optional).** People at your chosen domains can no longer sign in with Google or Microsoft: they are sent to SSO instead. Sessions they already had that did not come through SSO, in the SourceLace app and in MCP clients, stop working at once, so they sign in again through SSO.
- **Group sync (optional).** At every SSO sign-in, SourceLace reads the person's groups from your identity provider, puts them into the matching SourceLace groups, and takes them out of groups they are no longer in. See [Group sync](#).
- **Audit.** Every sign-in (including refused SSO sign-ins, and Google or Microsoft sign-ins that were sent to SSO) and every change to the SSO settings is recorded in your audit trail: who, when, how, and which groups changed. Never secrets or tokens.

How SourceLace checks a sign-in

SourceLace uses the OpenID Connect **authorization code flow with PKCE**, plus state and nonce. It reads your provider's addresses from `<issuer>/.well-known/openid-configuration` and checks the ID token in full: its **signature** against your provider's published keys (only public-key algorithms such as RS256, never "none" or shared-secret ones), the **issuer**, the **audience** (your client id), the **expiry** and the **nonce**. It then takes the person's address from the email claim, requires it to be at one of the domains you chose for SSO, and, when the provider sends `email_verified`, requires that to be true.

Your client secret is encrypted with your organization's own key before it is stored. It is never shown again, never logged and never returned by any API: the settings screen only says it is set.

A saved secret is only ever sent to the identity provider it was saved for: changing the issuer URL or client id needs the secret to be entered again.

Before you start

1. On the **Team** page, make sure your email domains (for example corvanta.com) are listed under **Email domains**. SSO can only cover domains your organization already has.
2. Note the **redirect URL** to register in your identity provider. It is shown at the top of **Settings → Single sign-on (SSO)** in the SourceLace app. On this server it is:

`https://sourcelace.onrender.com/login/callback`

If the screen lists more than one address, register all of them.

Set up Okta

1. Sign in to the **Okta Admin Console**.
2. Go to **Applications → Applications → Create App Integration**.
3. Choose **OIDC - OpenID Connect**, then **Web Application**, and click **Next**.
4. Fill in:
 - **App integration name:** SourceLace
 - **Grant type:** leave **Authorization Code** ticked.
 - **Sign-in redirect URIs:** the redirect URL from [Before you start](#). Remove the example sign-out URI, or leave it empty.
 - **Assignments:** choose who may use SourceLace (everyone, or selected groups).
5. Click **Save**.
6. On the app's **General** tab, copy the **Client ID** and the **Client secret** (under *Client Credentials*; client authentication "Client secret"). You may tick **Require PKCE as additional verification**: SourceLace always uses PKCE.
7. **Issuer URL.** Your Okta domain, such as `https://corvanta.okta.com` (shown at the top right of the Admin Console, or under **Security → API**). If you use a custom authorization server instead, the issuer is its address, such as `https://corvanta.okta.com/oauth2/default`.
8. **Email.** Nothing to do: Okta sends email and email_verified with the email scope SourceLace asks for.
9. **Groups (only for group sync).**
 - With the Okta domain as issuer: open the app's **Sign On** tab → **OpenID Connect ID Token** → **Edit**. Set **Groups claim type** to **Filter**, the claim name to groups, and the filter to **Matches regex** `.*` (or, to send only some groups, **Starts with** SourceLace-). Click **Save**. SourceLace asks for the groups scope itself when group sync is on.
 - With a custom authorization server: **Security → API → Authorization Servers** → your server → **Claims** → **Add Claim**: name groups, include in **ID Token** (Always), value type **Groups**, filter **Matches regex** `.*`.
 - Okta sends **group names**. In SourceLace, set each group's **external id** to the Okta group's name exactly as it appears in Okta (case does not matter).

Set up Microsoft Entra ID

1. Sign in to the **Microsoft Entra admin center** (entra.microsoft.com).
2. Go to **Identity → Applications → App registrations → New registration**.
3. Fill in:
 - **Name:** SourceLace SSO
 - **Supported account types:** **Accounts in this organizational directory only (single tenant)**.
 - **Redirect URI:** platform **Web**, and the redirect URL from [Before you start](#).
4. Click **Register**. On the **Overview** page, copy the **Application (client) ID** (the client id) and the **Directory (tenant) ID**.
5. **Client secret.** Go to **Certificates & secrets → Client secrets → New client secret**, choose an expiry, click **Add**, and copy the secret's **Value** (not its Secret ID) right away. Put a reminder in your calendar: when it expires, create a new one and paste it into SourceLace.
6. **Issuer URL.** [https://login.microsoftonline.com/<Directory \(tenant\) ID>/v2.0](https://login.microsoftonline.com/<Directory (tenant) ID>/v2.0). It must contain your directory's id: /common or /organizations will not work, because SourceLace only accepts people from your own directory.
7. **Email claim.** Go to **Token configuration → Add optional claim**, choose token type **ID**, tick **email**, and click **Add** (accept the prompt to turn on the Microsoft Graph email permission). Each person's **Email** field in Entra must hold their address at your domain. Entra does not send `email_verified`; SourceLace relies on the token coming from your own directory and the address being at one of your SSO domains.
8. **API permissions.** The defaults (User.Read, plus openid, email and profile) are enough. If your organization requires it, click **Grant admin consent**.
9. **Groups (only for group sync).**
 - Go to **Token configuration → Add groups claim**. Choose **Groups assigned to the application** (recommended) or **Security groups**. Under **ID**, keep **Group ID**. Click **Add**.
 - If you chose *Groups assigned to the application*, go to **Enterprise applications → SourceLace SSO → Users and groups** and add the groups SourceLace should see (this needs Entra ID P1 or higher).
 - Entra sends **group object ids** (such as 0f3a6c1e-...). In SourceLace, set each group's **external id** to the Entra group's **Object Id** (from **Groups → All groups → the group**).
 - If someone is in more than 200 groups, Entra leaves the groups out of the token ("group overage"). SourceLace then leaves that person's groups unchanged for that sign-in. Assigning only the needed groups to the application avoids this.

Other providers

For Google Workspace, OneLogin, Ping, JumpCloud and others: create an **OpenID Connect web application** in the provider's admin console with the redirect URL from [Before you start](#), and note its **issuer URL**, **client id** and **client secret**. The issuer URL is the address before `/.well-known/openid-configuration` in the provider's discovery URL. For Google Workspace it is `https://accounts.google.com` (create an OAuth client of type *Web application* in Google Cloud Console). Make sure the provider sends the `email` claim; for group sync, a claim listing the person's groups (set its name under **Group claim** in SourceLace if it is not groups).

Turn it on in SourceLace

1. In the SourceLace app, as an admin, open **Settings → Single sign-on (SSO)**.
2. Enter the **Issuer URL**, **Client id** and **Client secret** from your identity provider.
3. Tick the **email domains** that should sign in through SSO.
4. Leave **Require SSO** off for now, and click **Save SSO settings**. SourceLace checks the issuer URL by fetching its discovery document; if that fails, it tells you why.
5. **Test it:** sign out, choose **Continue with SSO / work email** on the sign-in page, and enter your work email. You should land in SourceLace, signed in. Try it from an MCP client too if you use one.
6. **Require SSO (optional):** back in **Settings → Single sign-on**, turn on **Require SSO** and save. SourceLace only lets you do this once you yourself are signed in through SSO, so a setting that does not work cannot lock you out.
7. **Group sync (optional):** see below.

To turn SSO off, click **Turn off SSO**. People then sign in with Google or Microsoft again.

If your identity provider stops working while **Require SSO** is on, your admins cannot sign in either. Contact support@sourcelace.com.

Group sync

1. On the **Groups** page, set each group's **External id**: the Okta group name, or the Entra group's object id.
2. In **Settings → Single sign-on**, turn on **Sync groups at each sign-in** (the group claim is usually groups) and save.

People's groups update the next time they sign in through SSO. Only groups with an external id are synced; groups without one are managed by hand and never touched. To use the synced groups for access, turn on [access by group](#).

When something goes wrong

What you see	What to do
"Enter the issuer URL your identity provider shows, such as <code>https://corvanta.okta.com</code> ."	The issuer URL is empty or not an <code>https://</code> address. Copy it from your identity provider.

What you see	What to do
"The identity provider's discovery document names a different issuer..."	Copy the issuer URL exactly as your provider shows it. For Entra, use the one with your directory's tenant id, not /common or /organizations.
"... does not sign in to SourceLace with single sign-on. Go back and sign in with Google or Microsoft..."	That email domain is not ticked under SSO, or the domain is not on your Team page.
"Your identity provider did not accept the sign-in..."	Check the client id, client secret and redirect URL in both your identity provider and SourceLace. An expired Entra client secret causes this too.
"Your identity provider did not send an email address..."	Add the email claim to the SourceLace app in your identity provider (for Entra, step 7 above).
"Your identity provider has not verified this email address."	The provider sent <code>email_verified: false</code> . Verify the address in your identity provider.
"... is not at a domain your organization signs in with through SSO."	The person's address in the identity provider is at a domain not ticked for SSO in SourceLace.
"... already uses SourceLace with another organization, so it cannot sign in here."	That address belongs to another SourceLace organization. Contact support.
"The sign-in was not meant for SourceLace. Ask your admin to check SSO."	The token's audience or issuer does not match the client id or issuer saved in SourceLace.
"Single sign-on is no longer set up for your organization."	SSO was turned off while the person was signing in. Sign in with Google or Microsoft, or turn SSO back on.
Someone's groups did not change	Group sync only runs at an SSO sign-in, and only for groups with an external id. For Entra, check the person is in fewer than 200 groups, or assign only the needed groups to the app.