Configure your identity provider

What step 3 of the wizard needs, by provider.

Google Workspace

Client ID and client secret from a Google Cloud OAuth client. Roughly ten minutes if you already have a project.

Microsoft Entra ID

Client ID and client secret, plus two decisions:

- **Account types** — organizations only, or also personal Microsoft accounts. Almost everyone wants organizations only.
- **Treat emails from Microsoft as verified** — whether to trust the email claim Entra returns without further checking. Correct for a tenant you control; think twice if you have allowed personal accounts.

Generic OIDC

Issuer URL, client ID, client secret, and the scopes to request. The issuer must serve a standard discovery document — the validate step fetches it and tells you precisely what is missing.

Generic SAML

Metadata URL only. Sentilai does not accept a pasted certificate or hand-entered endpoints; if your provider cannot publish metadata at a URL, SAML will not work here today.

Editing later

Leaving the client secret **blank** when editing keeps the stored one. You never have to find the original secret again just to change an unrelated field.

A display name

Whatever you put here is what your developers see on the sign-in screen. "Acme SSO" is kinder than "oidc-prod-2".

Revision #5
Created 2026-08-02 10:20:16 UTC by Sentilai Docs
Updated 2026-08-02 16:29:40 UTC by Sentilai Docs