Microsoft Entra ID

Your people sign in to Gebo.ai with their Microsoft work account. Register Gebo.ai as an application of your Entra tenant, then enter it in Setup.

TIME	15 minutes.
YOU NEED	A Microsoft Entra administrator who can register applications, and Gebo.ai open at the address your users use.

1 Register Gebo.ai in Entra

1. In the Microsoft Entra admin center open **App registrations** and click **New registration**.
2. Name it *Gebo.ai*, choose **Accounts in this organizational directory only** and click **Register**. The redirect address comes later.
3. On the **Overview** copy the **Application (client) ID** and the **Directory (tenant) ID**.
4. In **Certificates & secrets** click **New client secret** and copy its **Value** at once: Entra shows it only now.

Secrets expire

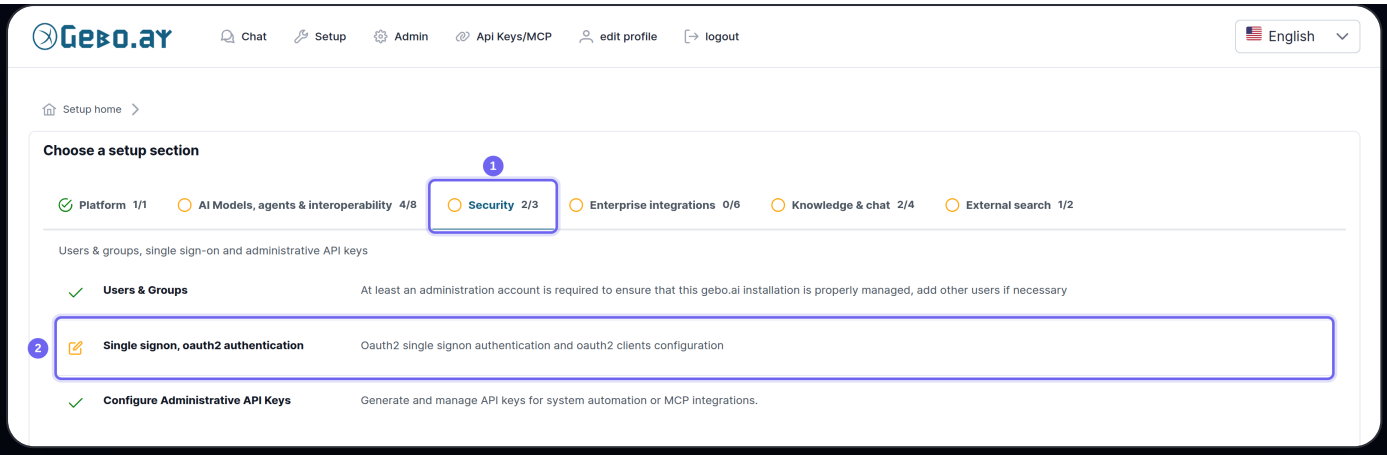
Note the expiry date of the secret. Before it, create a new one and enter it in the configuration, or the sign-in stops working.

Personal accounts or several organizations?

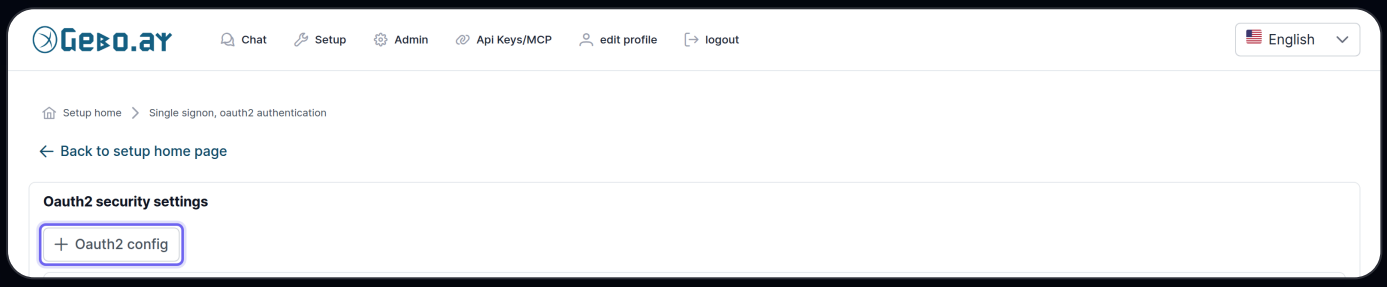
Page 24b lets in personal Microsoft accounts and the people of the organizations you list, with one configuration.

2 Open the single sign-on settings

In **Setup** open **Security** (1) and click **Single signon, oauth2 authentication** (2), then **+ Oauth2 config**.

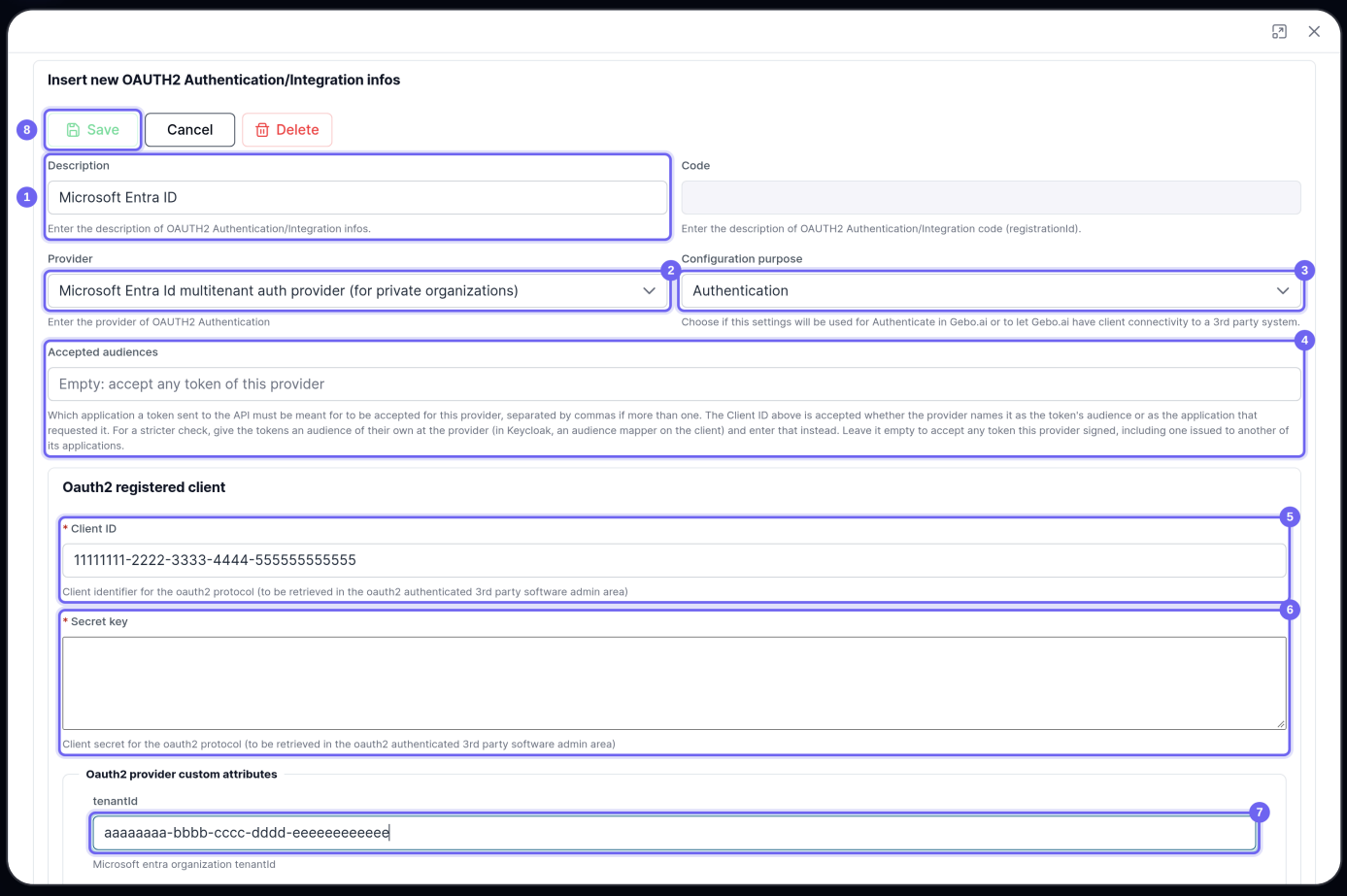


The Security tab of Setup.



The single sign-on configurations, still none, and **+ Oauth2 config**.

3 Enter the application



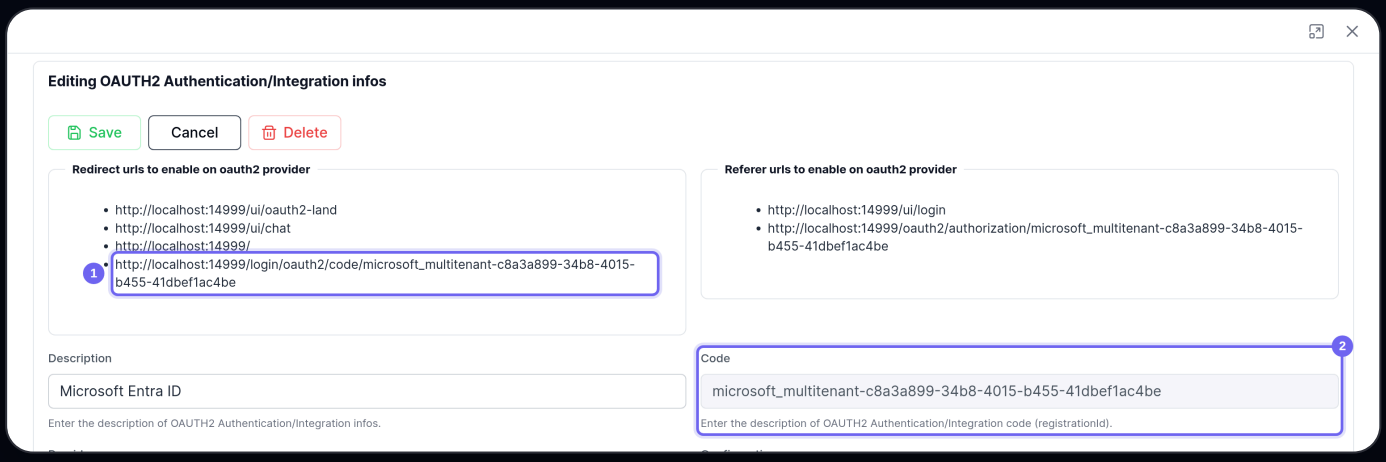
A new configuration for Microsoft Entra ID. The secret is still to be entered.

1. **Description:** the name on the login button, for example *Microsoft Entra ID*.
2. **Provider:** *Microsoft Entra Id multitenant auth provider (for private organizations)*.
3. **Configuration purpose:** *Authentication*.
4. **Accepted audiences:** only for tools that call the Gebo.ai API with tokens of this provider (page 28b). Enter the **Client ID** of item 5 to accept only tokens meant for Gebo.ai; empty, any token this provider signed is accepted. Signing in with the button does not depend on it.
5. **Client ID:** the identifier the provider gave Gebo.ai.
6. **Secret key:** the client secret the provider gave Gebo.ai.
7. **tenantId:** the **Directory (tenant) ID** of the application.
8. Click **Save**.

---

4 Give the provider the redirect address

Save closes the dialog. Click **Modify** next to the new configuration: Gebo.ai has given it a **Code** (2) and lists the addresses to enable at the provider. The redirect address to register is the one ending in `/login/oauth2/code/` followed by the code (1).



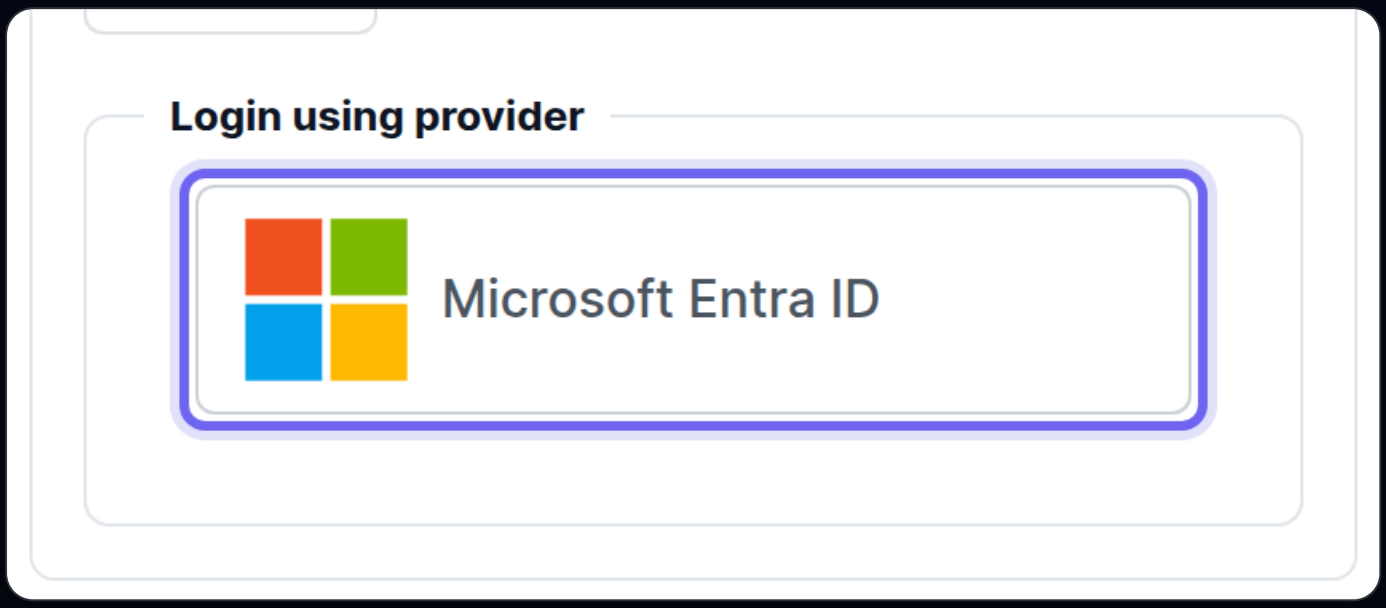
The saved configuration: its redirect address (1) and its code (2).

In Entra open the application, **Authentication** → **Add a platform** → **Web**, paste the address as **Redirect URI** and click **Configure**.

> **Open Gebo.ai at its real address first**
> The addresses are built from the address your browser has Gebo.ai open at. Open Gebo.ai at the address your users use, for example `https://gebo.company.com`, before copying it: an address with `localhost` works only on the server itself.

5 Let people in

The login page now shows a button with the **Description** of the configuration.



The Microsoft Entra ID button on the login page.

By default Gebo.ai lets in the people an administrator has created: for each of them create a user whose **Username** is their e-mail address in Entra and whose **Authentication provider** is this provider, as described in page 29. To make every person the provider recognizes a user on their own, see page 28b.

6 If someone cannot get in

- Gebo.ai recognizes people by the e-mail address Entra sends: make sure each account has one (the **Email** of the user in Entra).
- If Microsoft asks for a consent the person cannot give, an administrator grants it in the application's **API permissions** with **Grant admin consent**.

← Active sessions

Next: Microsoft accounts →