Other OpenID Connect providers

Any identity provider that speaks OpenID Connect, such as Okta, Auth0, Authentik or Zitadel: you enter its addresses yourself, from its discovery document.

TIME	15 minutes.
YOU NEED	An administrator of the provider, the provider's issuer address, and Gebo.ai open at the address your users use.

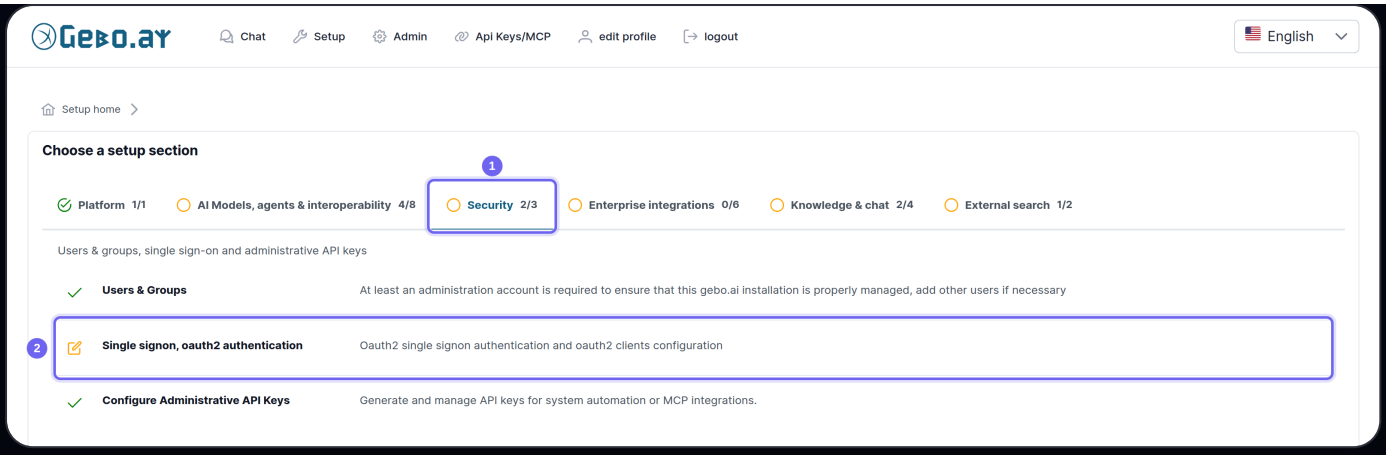
1 Register Gebo.ai at the provider

Create a web application (a confidential client) with the authorization code flow and the `openid`, `profile` and `email` scopes, and copy its client ID and client secret. The redirect address comes later. The provider must send the e-mail address of the person: Gebo.ai recognizes people by it.

Then open the provider's discovery document, `<issuer>/.well-known/openid-configuration`: it lists the addresses to enter.

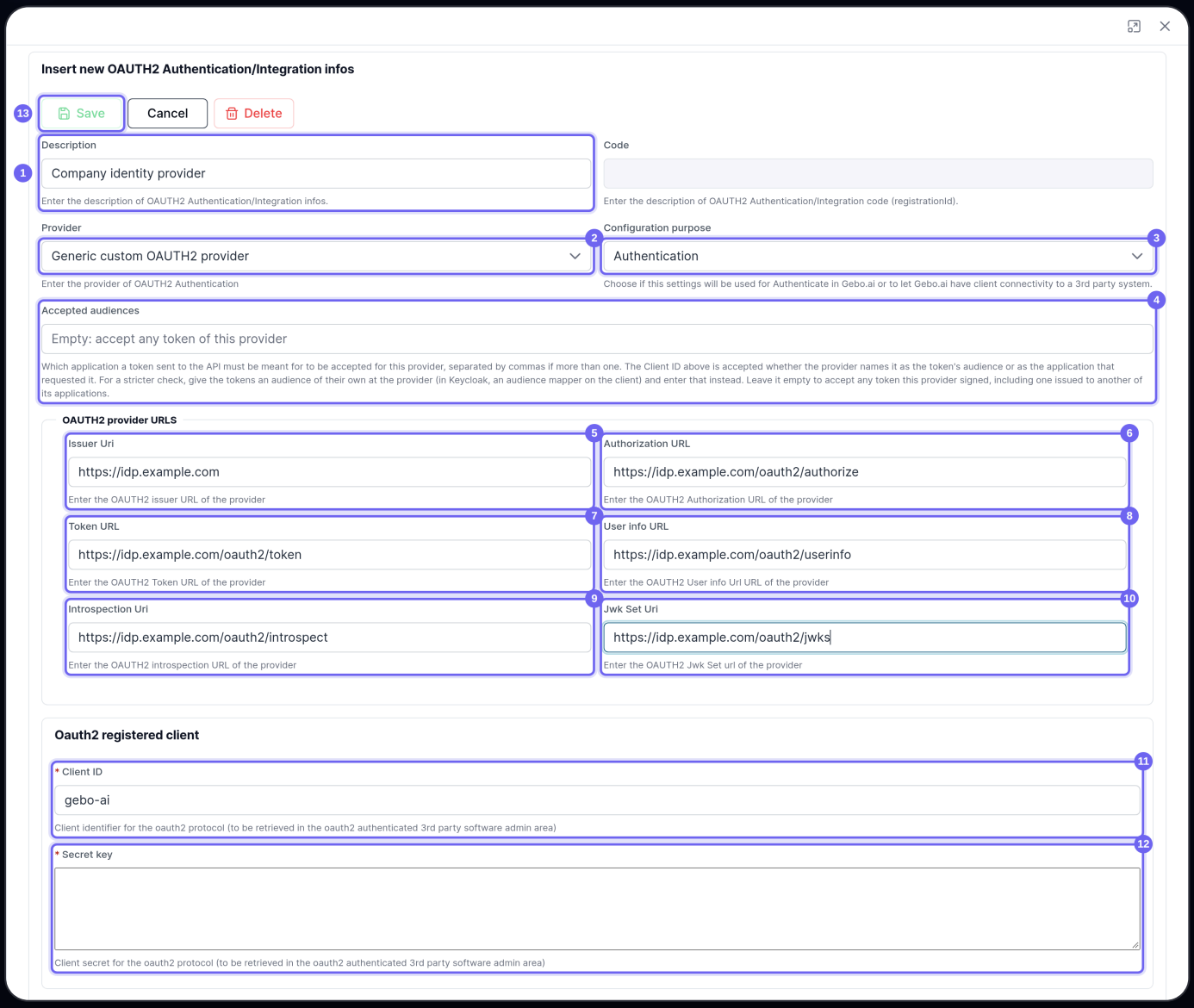
2 Open the single sign-on settings

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



The Security tab of Setup.

3 Enter the provider



A new configuration for another OpenID Connect provider. The secret is still to be entered.

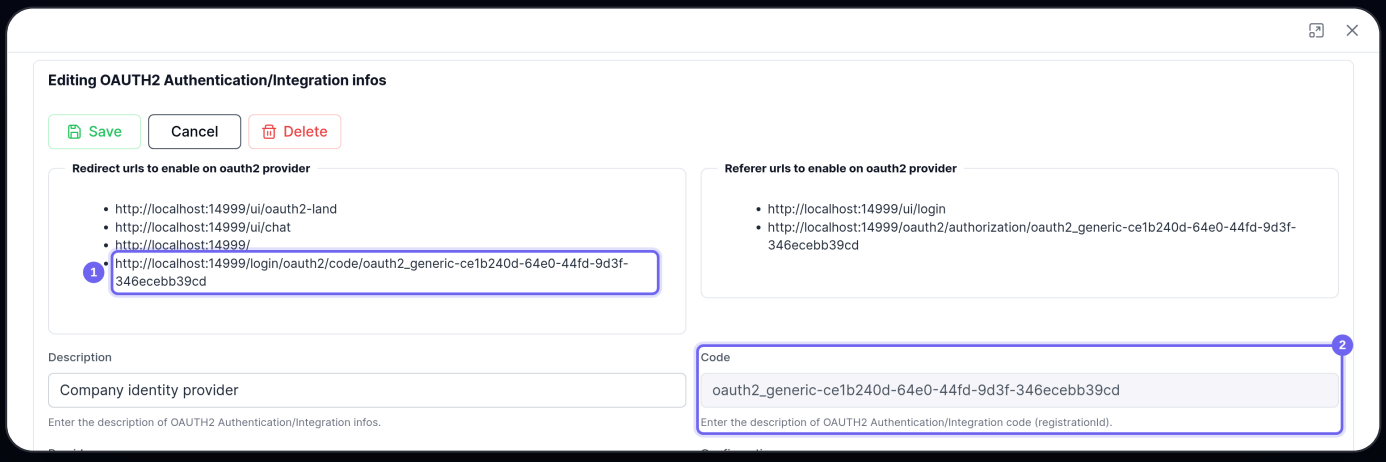
1. **Description:** the name on the login button, for example *Company identity provider*.

2. **Provider:** *Generic custom OAUTH2 provider*.
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 11 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. **Issuer Uri:** `issuer` of the discovery document.
6. **Authorization URL:** `authorization_endpoint`.
7. **Token URL:** `token_endpoint`.
8. **User info URL:** `userinfo_endpoint`.
9. **Introspection Uri:** `introspection_endpoint`, when the provider has one. It only serves to check the opaque tokens that tools send to the API.
10. **Jwk Set Uri:** `jwks_uri`.
11. **Client ID:** the identifier the provider gave Gebo.ai.
12. **Secret key:** the client secret the provider gave Gebo.ai.
13. 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).

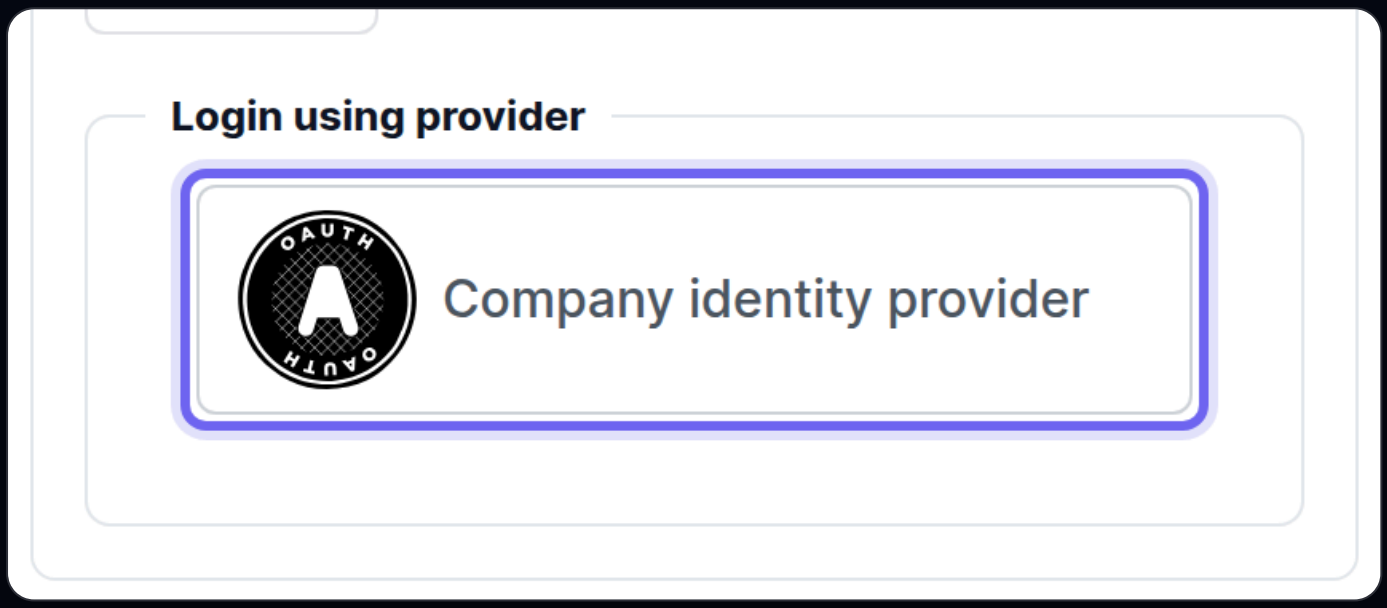
At the provider, add the address to the redirect (callback) addresses of the application.

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 provider 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 the e-mail address the provider sends 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.

← Keycloak

Next: Single sign-on: platform settings →