Keycloak

Your people sign in to Gebo.ai with the accounts of a Keycloak realm. Add Gebo.ai as a client of the realm, then enter it in Setup.

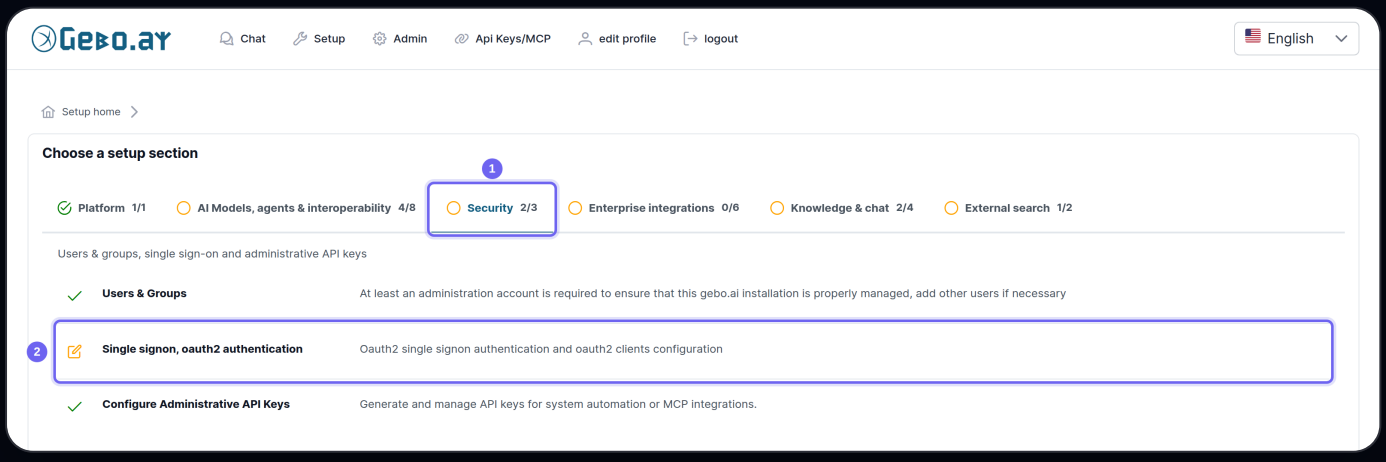
TIME	10 minutes.
YOU NEED	An administrator of the Keycloak realm, the address Keycloak is published at, and Gebo.ai open at the address your users use.

1 Add Gebo.ai to the realm

1. In the Keycloak admin console choose the realm, open **Clients** and click **Create client**.
2. **Client type** *OpenID Connect*, **Client ID** `gebo-ai`, then **Next**.
3. Turn on **Client authentication**, keep **Standard flow**, then **Next** and **Save**. The redirect address comes later.
4. In the **Credentials** tab copy the **Client secret**.

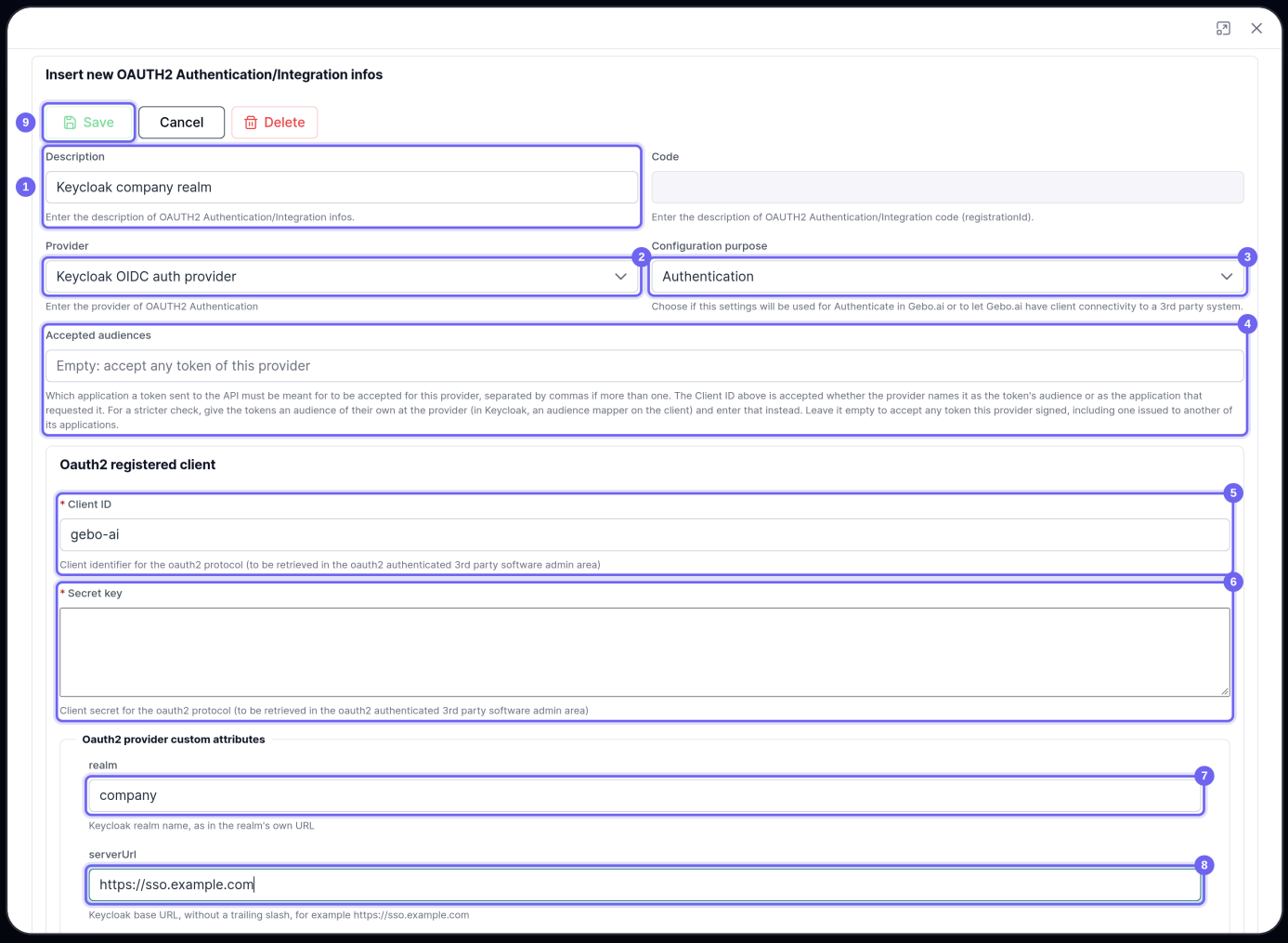
2 Open the single sign-on settings

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



The Security tab of Setup.

3 Enter the client



A new configuration for Keycloak. The secret is still to be entered.

1. **Description:** the name on the login button, for example *Keycloak company realm*.
2. **Provider:** *Keycloak OIDC auth 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 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. **realm:** the name of the realm, as in its address.
8. **serverUrl:** the address Keycloak is published at, without the final `/`, for example `https://sso.example.com`.
9. Click **Save**.

The address Keycloak publishes

Gebo.ai checks that the sign-in comes from `<serverUrl>/realms/<realm>`, exactly as Keycloak writes it in its tokens: use the public address configured in Keycloak, reachable from the Gebo.ai server too. For Keycloak versions before 17 it ends in `/auth`.

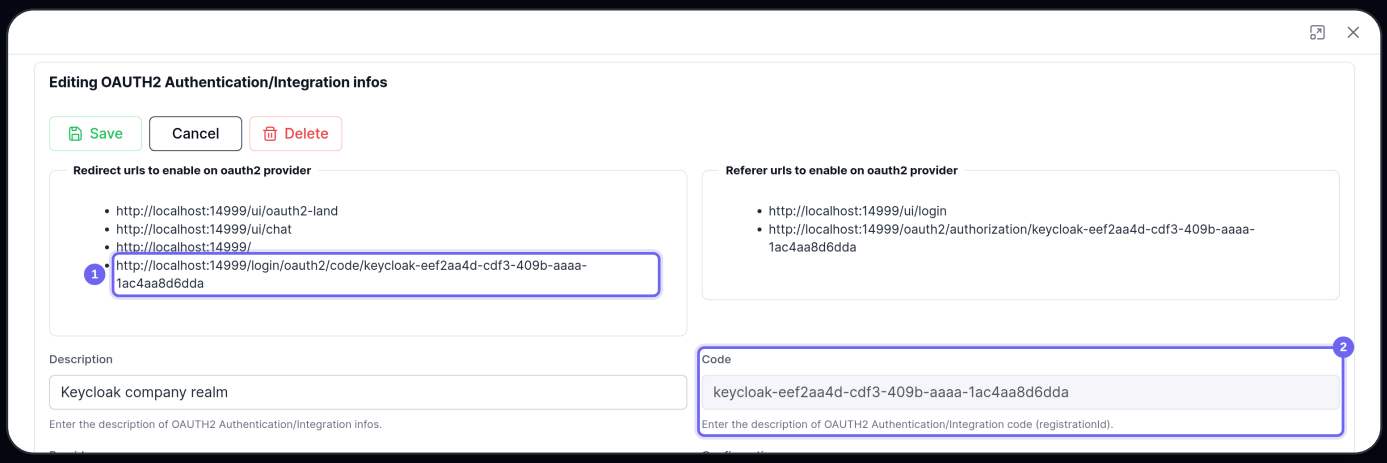
Tokens for the API

Keycloak addresses its tokens to `account` and names the requesting client apart: with the **Client ID** among the **Accepted audiences**, the tokens of the `gebo-ai` client are accepted and those of the other clients refused. For a stricter check, add an audience mapper to the client and enter its audience instead.

---

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).

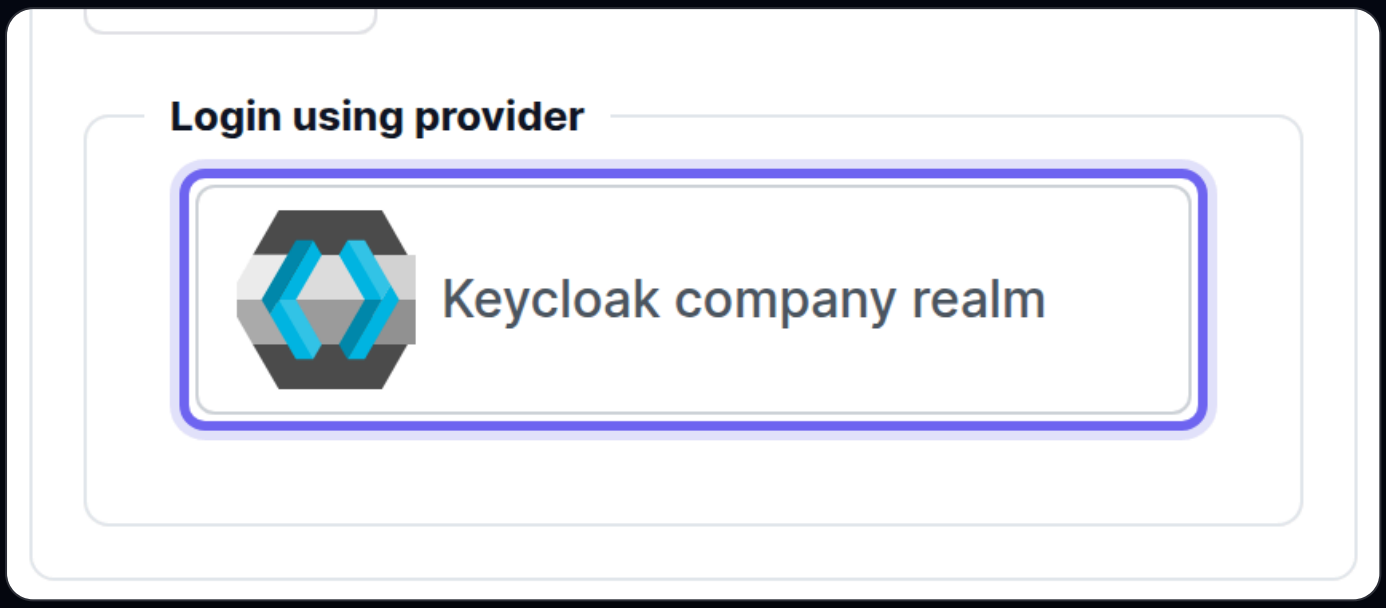
In Keycloak open the `gebo-ai` client, paste the address among the **Valid redirect URIs** of its **Settings** and click **Save**.

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 Keycloak 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 of their Keycloak account 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.

← AWS Cognito

Next: Other OpenID Connect providers →