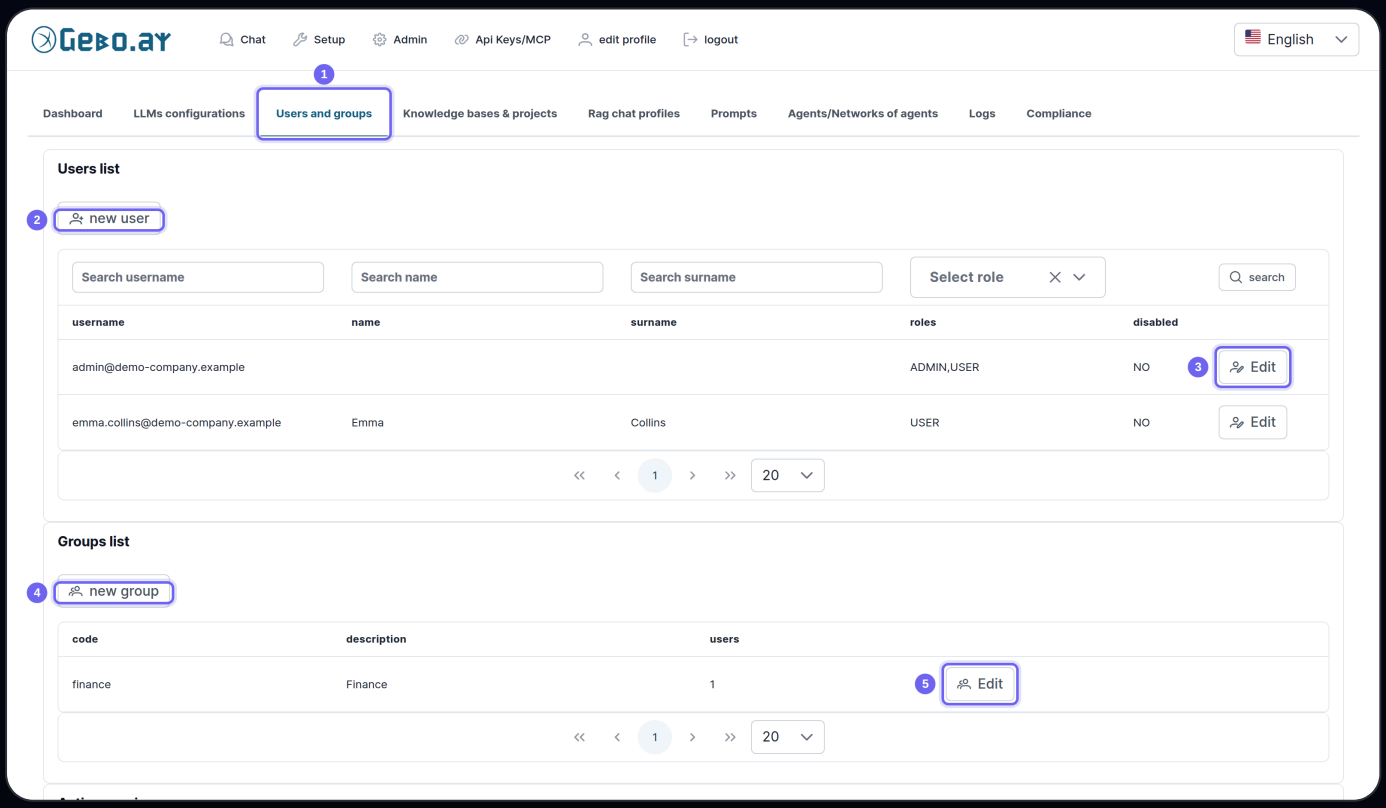
Users and groups

Who can sign in and how: the accounts Gebo.ai keeps itself and those of the single sign-on providers, gathered in groups that open knowledge bases and projects to some people only.

WHERE	Admin → Users and groups.
YOU NEED	An administrator account; for single sign-on, a configuration of pages 24 to 28.

1 The lists

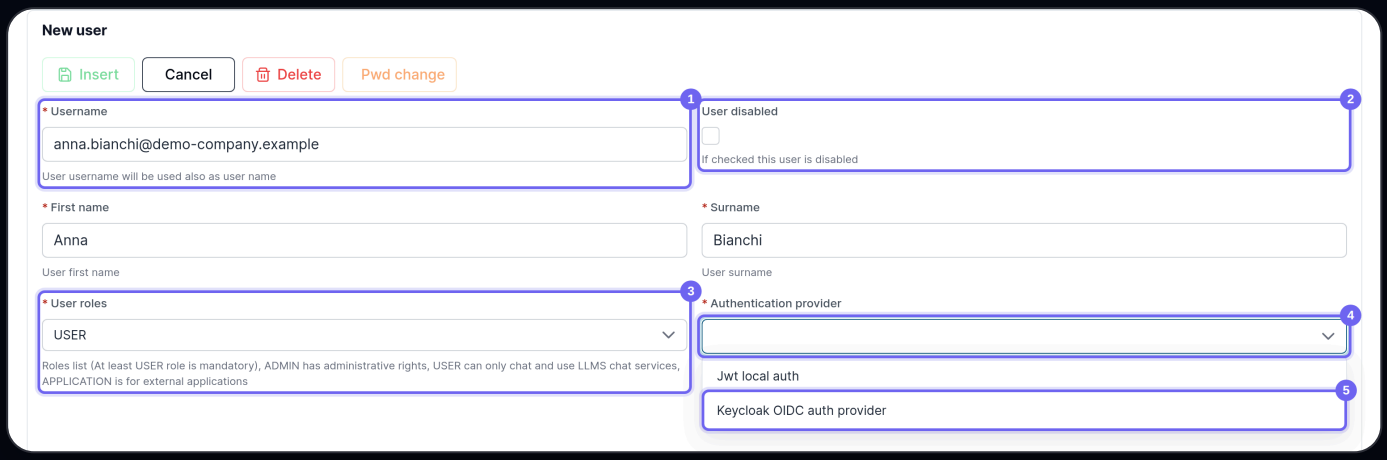
In **Admin** open **Users and groups** (1). **new user** (2) and **Modify** (3) create and change the users; **new group** (4) and **Modify** (5) the groups. The active sessions are further down (page 23).



The users and the groups.

2 A user who signs in with single sign-on

Click **new user**. A user with a password of Gebo.ai is described in step 7; for single sign-on:

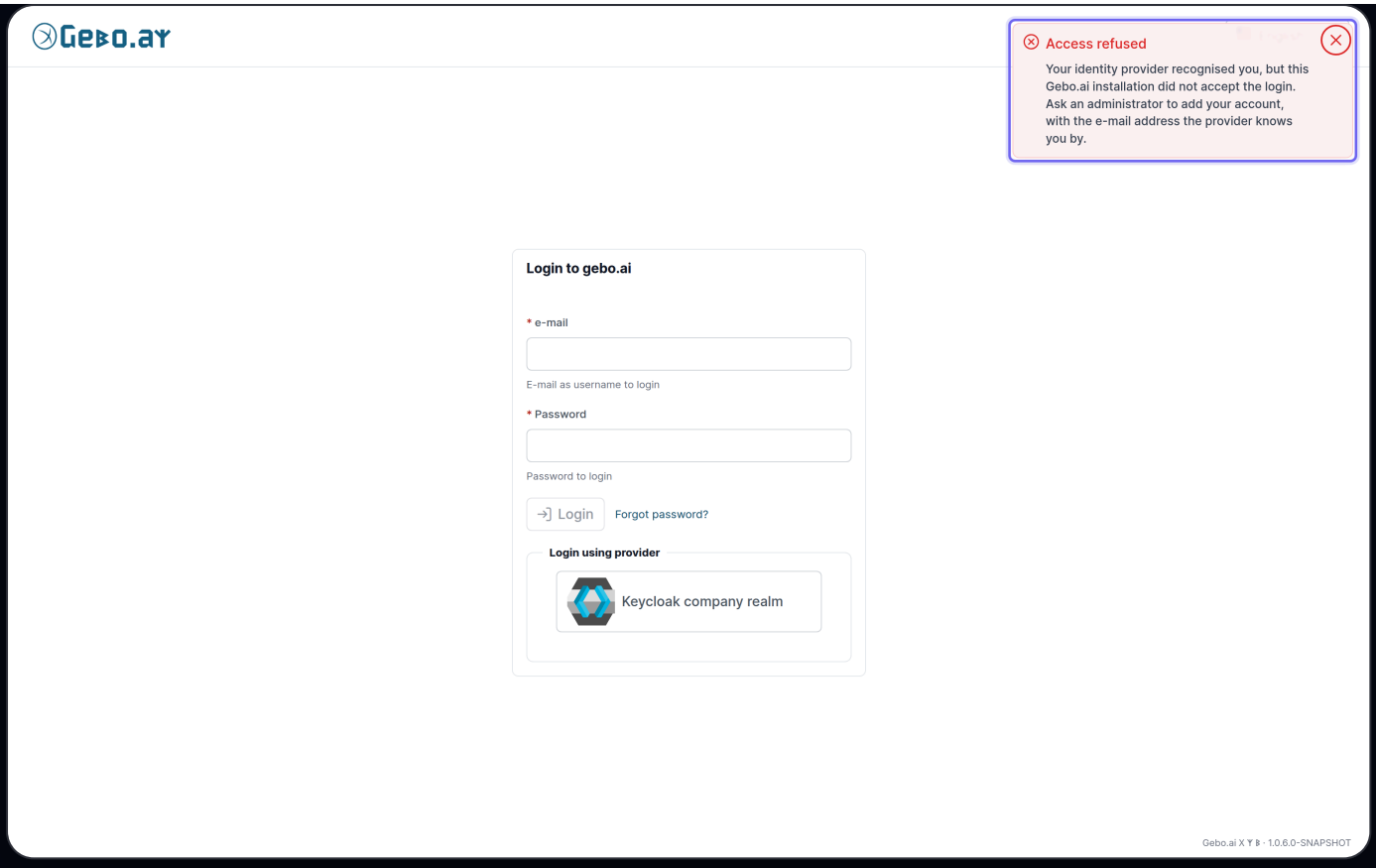


A new user who will sign in through Keycloak.

1. **Username:** the e-mail address the provider knows the person by.
2. **User disabled:** leave it unticked.
3. **User roles:** USER; ADMIN also opens the administration.
4. **Authentication provider:** the provider of the single sign-on configuration, not *Jwt local auth*.
5. Here, the Keycloak one.

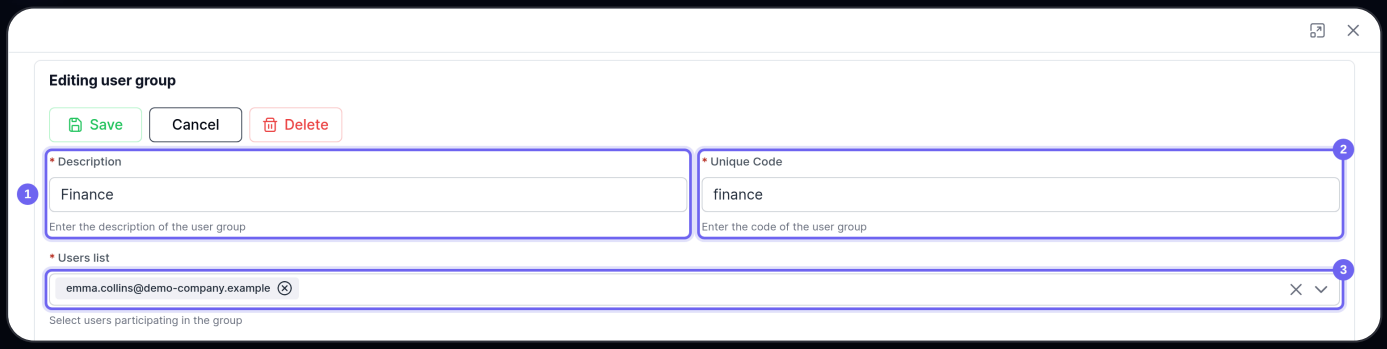
Fill in **First name** and **Surname** and click **Insert**. No password: the person signs in with the provider's button on the login page.

Gebo.ai lets in through single sign-on only the people created this way. Anyone else the provider recognizes, or a user created with another provider, gets this message:



A person the provider recognized, refused by Gebo.ai.

3 Groups



A group and its members.

A group has a **Description** (1), a **Unique Code** (2) and its members in **Users list** (3). The access settings of the knowledge bases (step 4), of the projects and of the MCP servers (page 16) choose among the groups: a group is the way to open them to a department.

← Single sign-on: platform settings

Next: Chat profiles →