GEBO.AI SETUP GUIDE · SECURITY · PAGE 28B

Single sign-on: platform settings

Two settings of the platform's configuration file shape single sign-on: whether the people your provider recognizes become users on their own, and how your own applications call Gebo.ai with the tokens of your provider.

TIME	10 minutes.
YOU NEED	Access to the server, and a provider configured as on pages 24-28.

1 The configuration file

The settings go in the `ai.gebo.security` block of the configuration file of the installation, and apply when Gebo.ai restarts.

- **Docker Compose:** in the folder of `docker-compose.yml`, copy out the `application.yml` the image ships, change it, and mount it in `docker-compose.override.yml` (step 5); `docker compose up -d` applies it.
- **Linux service** (`.deb`): `/etc/gebo-ai/application.properties`, then `sudo systemctl restart gebo-ai`.
- **Windows** (`.msi`): `config\application.properties` in the instance folder of the installation, then restart the **Gebo.ai Service**.

With Docker Compose, copy the file out:

```
docker compose cp gebo.ai:/opt/gebo.ai/config/application.yml ./application.yml
```

and mount your copy: add its line to the `volumes` of the `gebo.ai` service in `docker-compose.override.yml`, or create the file with:

```
services:
  gebo.ai:
    volumes:
      - "./application.yml:/opt/gebo.ai/config/application.yml:ro"
```

When you upgrade Gebo.ai, copy the file of the new image again and add your lines back.

---

2 Let in the people your provider recognizes

By default Gebo.ai lets in the users an administrator created (page 29). To make every person your provider signs in a user of Gebo.ai, add `loginPolicy` to the `ai.gebo.security` block, indented like the lines below it:

```
ai.gebo.security:
  loginPolicy: TRUST_EVERY_OAUTH_IDENTITY
  auth:
    ...
```

In an `application.properties` file the same setting is one line:

```
ai.gebo.security.loginPolicy=TRUST_EVERY_OAUTH_IDENTITY
```

- The first time a person signs in through a configured provider, Gebo.ai creates their user, with their e-mail address as **Username** and the role **USER**; every later sign-in updates it. The same happens the first time one of your applications calls the API with that person's token.
- Give the new users their groups and roles as on page 29; to keep someone out, tick **User disabled** on their user.
- Choose it for providers whose accounts all belong to your organization, since every account they recognize becomes a user. `REQUIRE_INVITATION` brings back the default.

---

3 Applications that call Gebo.ai with OAuth2 tokens

Your own applications, on the client or on the server side, can call the Gebo.ai API with the access tokens of a configured provider, next to the tokens Gebo.ai issues itself: `oauth2ResourceServerEnabled` is `true` by default.

```
ai.gebo.security:
  oauth2ResourceServerEnabled: true
  auth:
    ...
```

- In each provider configuration, list the client IDs of your applications among the **Accepted audiences** (pages 24-28): Gebo.ai then accepts the tokens issued to them.

- With `loginPolicy: TRUST_EVERY_OAUTH_IDENTITY` the people behind the tokens become users at their first call; otherwise create them as on page 29.

← Other OpenID Connect providers

Next: Users and groups →