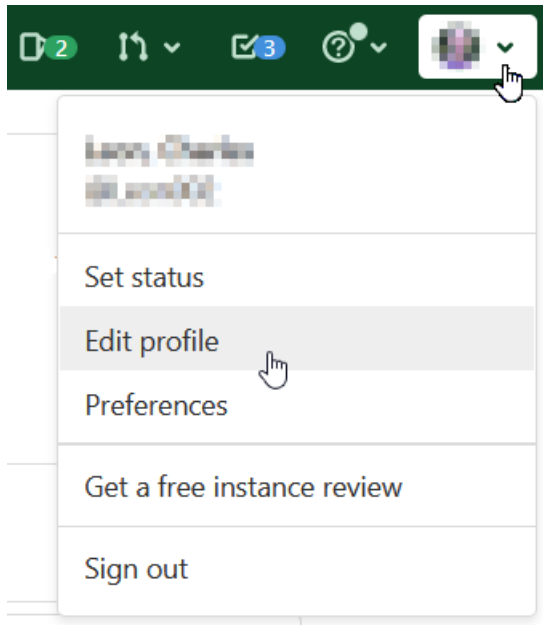


Authenticating over HTTPS against git.wur.nl with two-factor authentication enabled

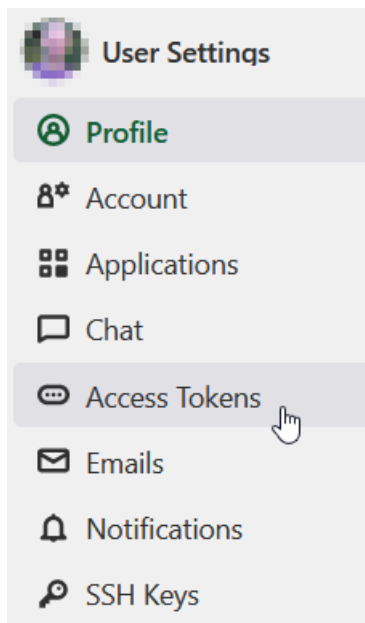
You have to authenticate with a personal access token in place of your password when two-factor authentication is enabled.

Creating a personal access token

1. Navigate directly to [User Settings](#) > [Access Tokens](#) or by selecting the option Edit profile below your avatar



2. Click Access Tokens at the left side of the screen



3. In the form Personal Access Tokens, fill in a token name and tick the boxes read_repository and write_repository. Press the button Create personal access token.

Personal Access Tokens

You can generate a personal access token for each application you use that needs access to the GitLab API.

You can also use personal access tokens to authenticate against Git over HTTP. They are the only accepted password when you have Two-Factor Authentication (2FA) enabled.

Add a personal access token

Enter the name of your application, and we'll return a unique personal access token.

Token name

For example, the application using the token or the purpose of the token.

Expiration date

Select scopes

Scopes set the permission levels granted to the token. [Learn more.](#)

api

Grants complete read/write access to the API, including all groups and projects, the container registry, and the package registry.

read_user

Grants read-only access to the authenticated user's profile through the /user API endpoint, which includes username, public email, and full name. Also grants access to read-only API endpoints under /users.

read_api

Grants read access to the API, including all groups and projects, the container registry, and the package registry.

read_repository

Grants read-only access to repositories on private projects using Git-over-HTTP or the Repository Files API.

write_repository

Grants read-write access to repositories on private projects using Git-over-HTTP (not using the API).

read_registry

Grants read-only access to container registry images on private projects.

write_registry

Grants write access to container registry images on private projects.

sudo

Grants permission to perform API actions as any user in the system, when authenticated as an admin user.

Create personal access token

4. Save your new personal access token at a secure location like a password manager.

User Settings > Access Tokens

Your new personal access token has been created.

Search settings

Personal Access Tokens

You can generate a personal access token for each application you use that needs access to the GitLab API.

Your new personal access token

Y5iIawSfP9zD7a5WRZ_f

Copy personal access token

Make sure you save it - you won't be able to access it again.

Using the Personal Access Token at the CLI

You will use the Personal Access Token as the password for the fictional "oauth2" user in CLI commands.

For example, to clone your repository:

```
$ git clone https://oauth2:Y5iiawSfP9zD7a5WRZ_F@git.wur.nl/User001/example-project.git example-project.git
```

For example, use the personal access token with HTTPS as authentication method for an existing checked out project (stored in your git project in the .git/config file):

```
git remote set-url origin https://oauth2:Y5iiawSfP9zD7a5WRZ_F@git.wur.nl/User001/example-project.git
```