https://app.titra.io/try

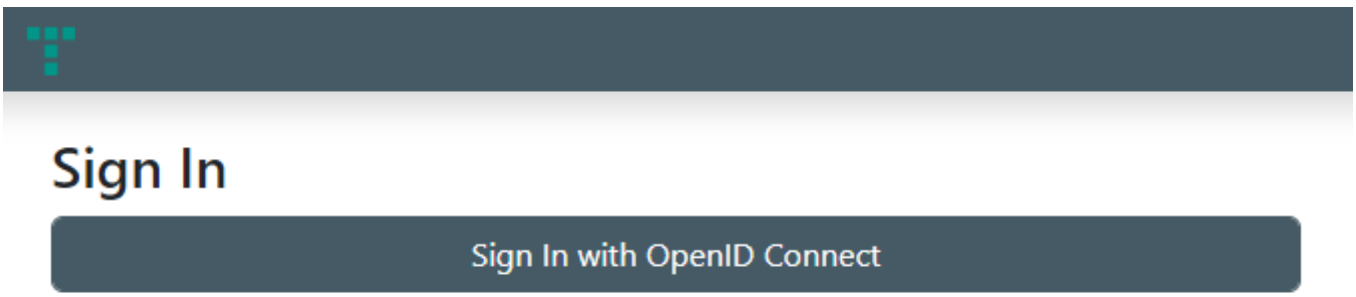
OpenID Connect (OIDC) Authentication

1. Configure your OIDC client for **Authorization Code Flow**
2. Set the relevant fields in titra

223077004-e6451fd7-7198-4a6a-a009-8b02d0ed07e6.png

- **Client ID**: Client ID as per your OIDC App Configuration
- **Client Secret**: As per your OIDC App Configuration
- **OIDC Server Url**: Your auth domain e.g. http://auth.your.domain
- **Authorization Endpoint**: /your/auth/endpoint *Note the prepended slash*
- **Token Endpoint**: /your/token/endpoint *Note the prepended slash*
- **UserInfo Endpoint**: /your/userinfo/endpoint *Note the prepended slash*
- **Id Token Fields**: Extra fields to be grabbed from your token and appended to the user. In my case my server returns an opaque access token which it grabs first (not the id token) so make sure that these fields are on the relevant token.
- **Request Permissions**: These permissions will be requested from your OIDC server, it defaults to openid,profile,email.

You can disable the default login form to prevent password based logins entirely:



Gitlab OpenID Provider

Example configuration provided by Github user Rishats in issue 171.
Screenshot from 2023-04-28 13-33-08

Screenshot from 2023-04-28 13-33-35

> All credit goes to @iamscottcab who has authored this documentation and provided two pull requests to improve the OIDC integration. Also a shoutout to @Rishats for providing the Gitlab example configuration!

Revision #4
Created 2023-03-07 08:23:56 UTC by Fabian Kromer
Updated 2023-05-04 08:27:46 UTC by Fabian Kromer