TozID Powered OIDC Implicit Flow Third Party SSO

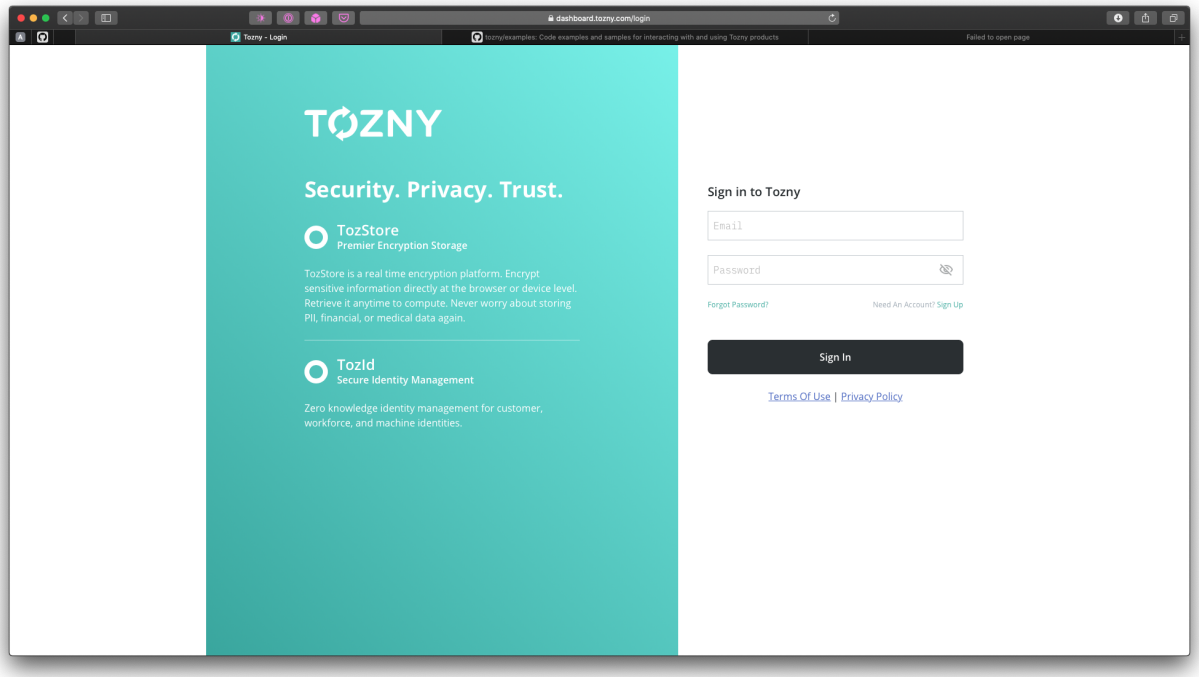
Purpose

The purpose of this document is to walk through how to use TozID to provide Single Sign On to a website using the OIDC implicit flow.

Create / Sign into Tozny Dashboard

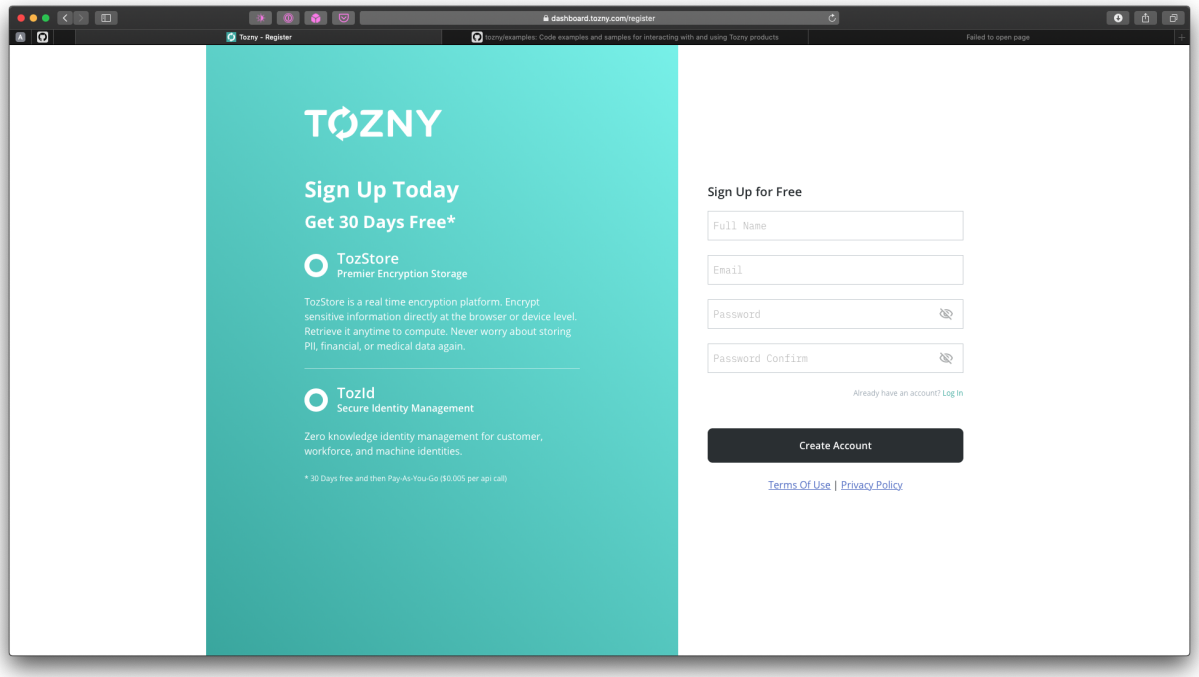
To get started, you will either need to create a Tozny account, or sign into your existing account.

Navigate to https://dashboard.tozny.com



If you have an existing account, use your username and password to login.

Otherwise, click ‘Sign Up’, enter your account name, email (which will serve as your username for login purposes) and choose a strong password to protect your account.



After filling out valid information and clicking ‘Create Account’ you will be presented with a paper key, which can be used to recover access to your account and associated data in the event you have lost your password. Make sure to store this paper key somewhere private and durable such as a password manager.

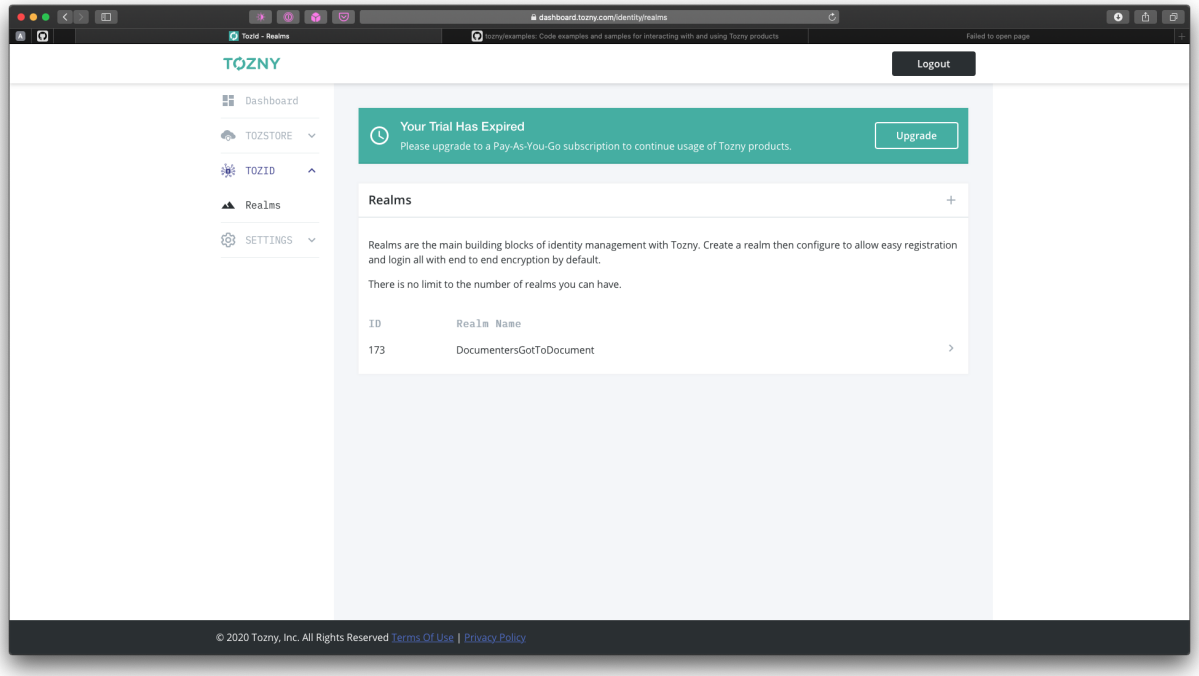
Once you’ve created or logged into your existing account, you will receive an email to verify your account.

Open that email and click the verification link.

Create TozID Realm

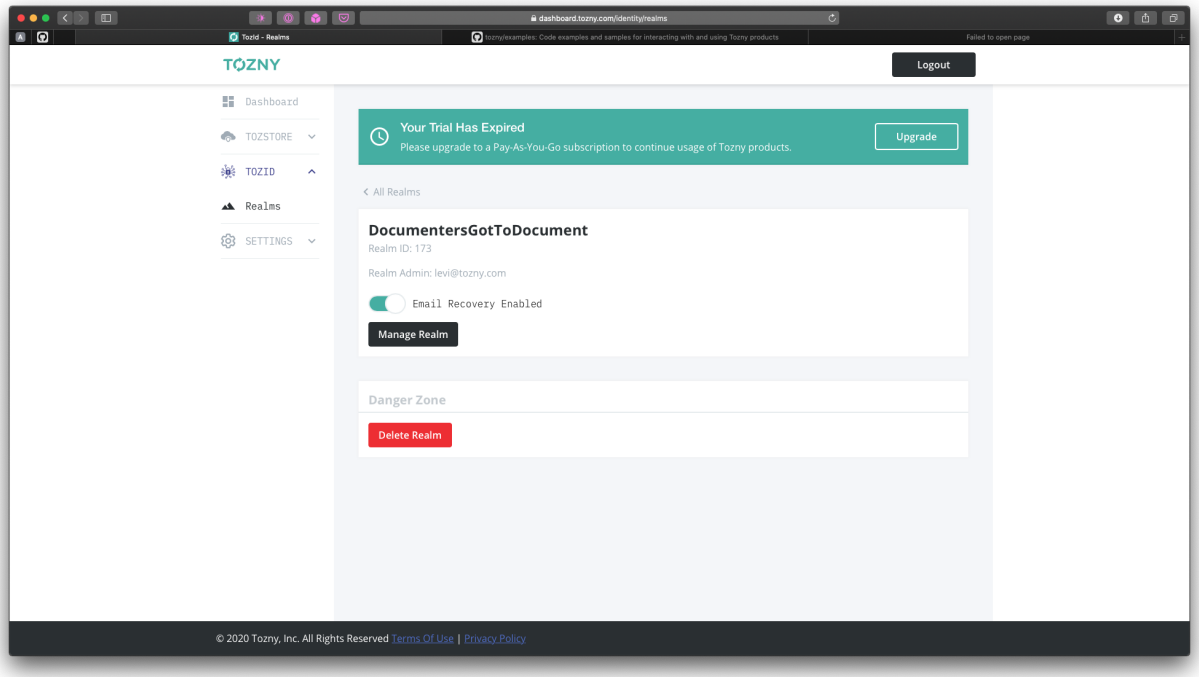
Now that your account has been verified, you can proceed to creating a realm. A realm is a virtual container for identities (users or devices) and applications (such as a web site or API service) that allows you to manage settings, authentication and authorization for identities and applications that are a part of the realm.

Select TozID from the side left menu bar, and click on realms.

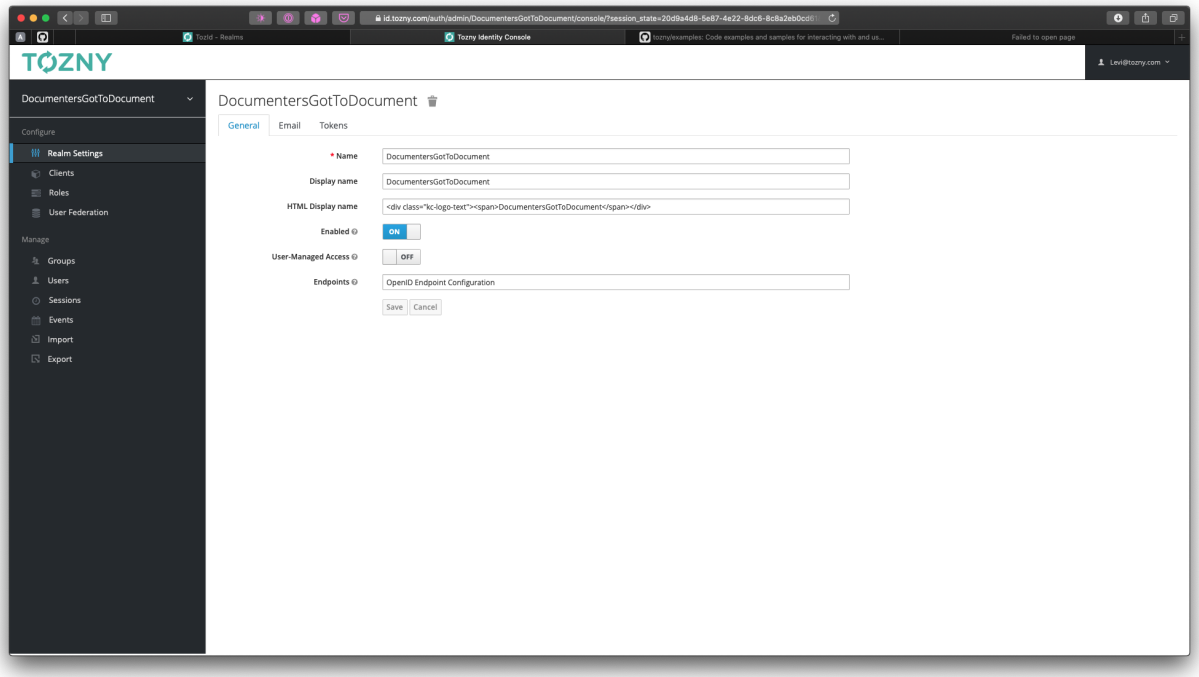


Click the `+` icon in the middle left of the screen, and enter a unique realm name (using lowercase characters a-z or digits 0-9 only), then click ‘Create Realm’. After a few seconds, your realm will be created.

Select the realm you created from the list of realms

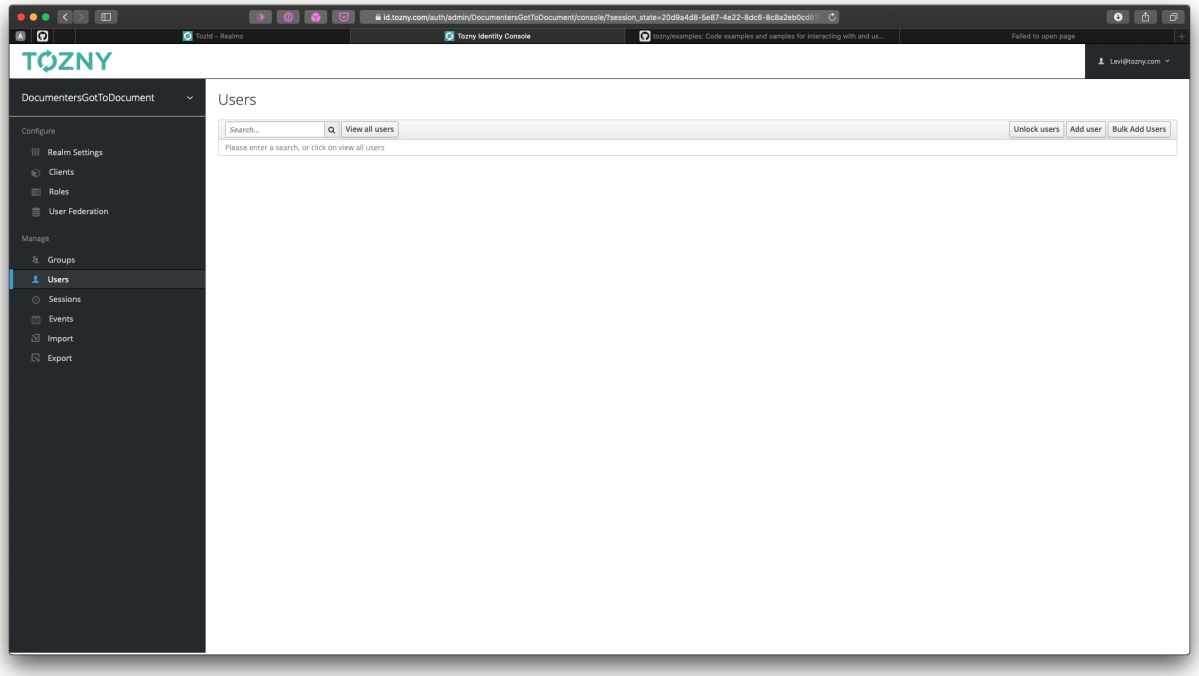


Click ‘Manage Realm’ to be taken to the Realm Admin Portal for the given realm.

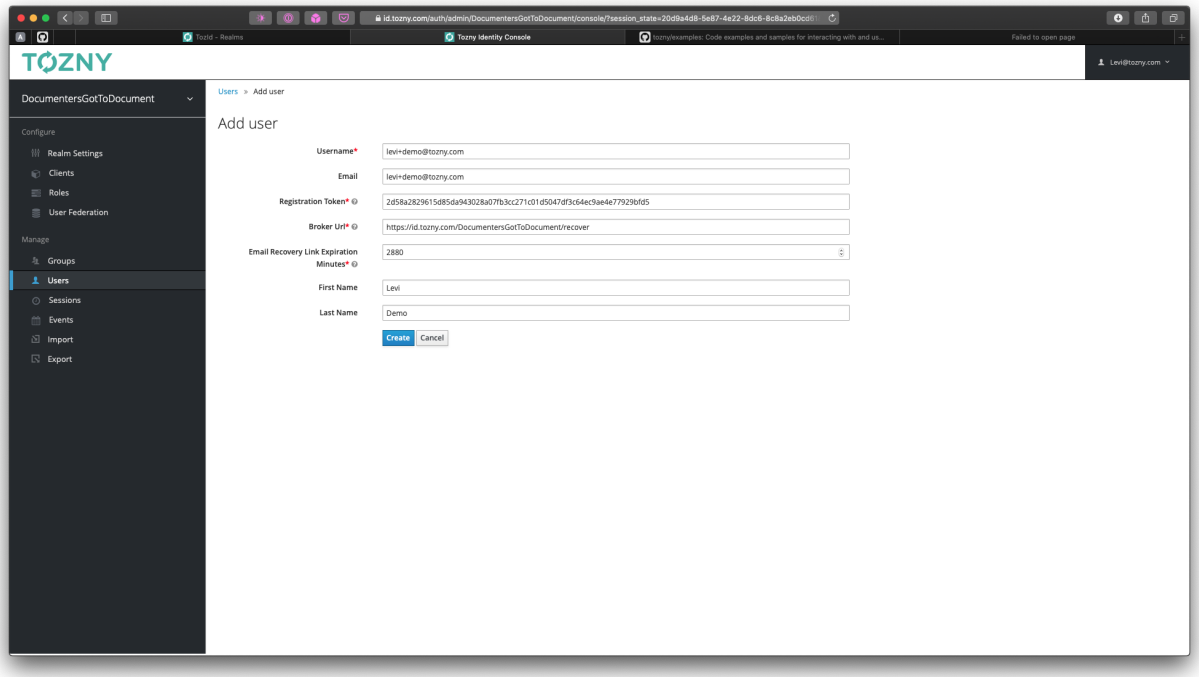


Create Realm Identity

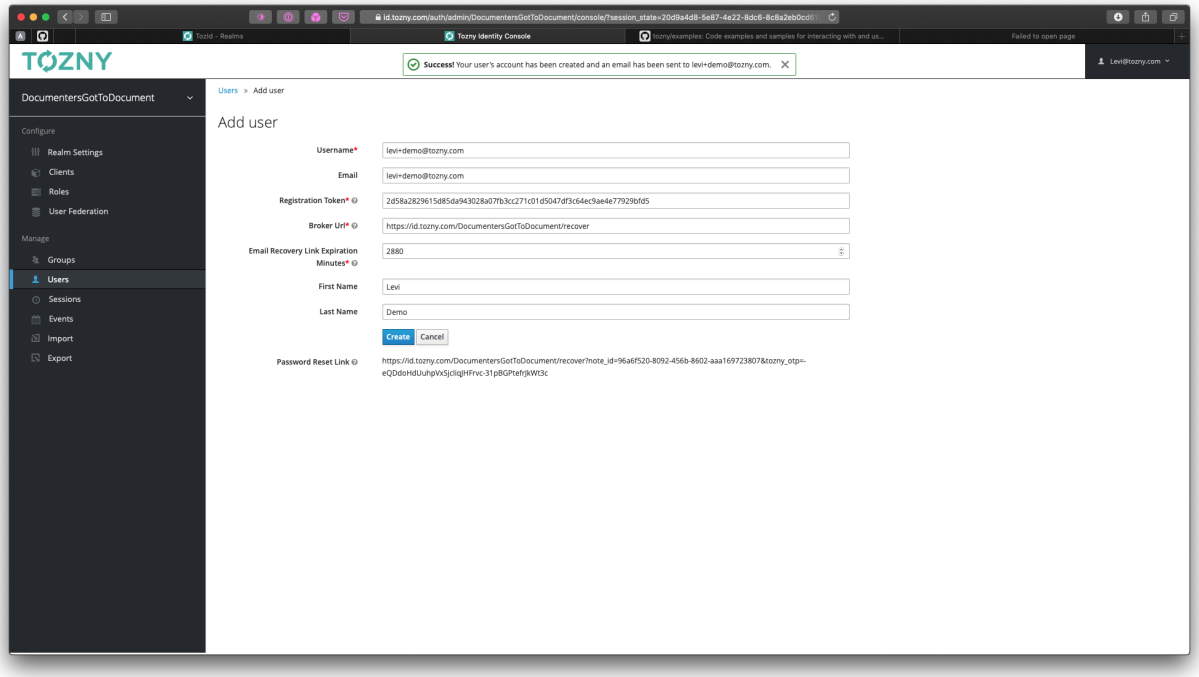
From the lower left menu bar, click on ‘Users’



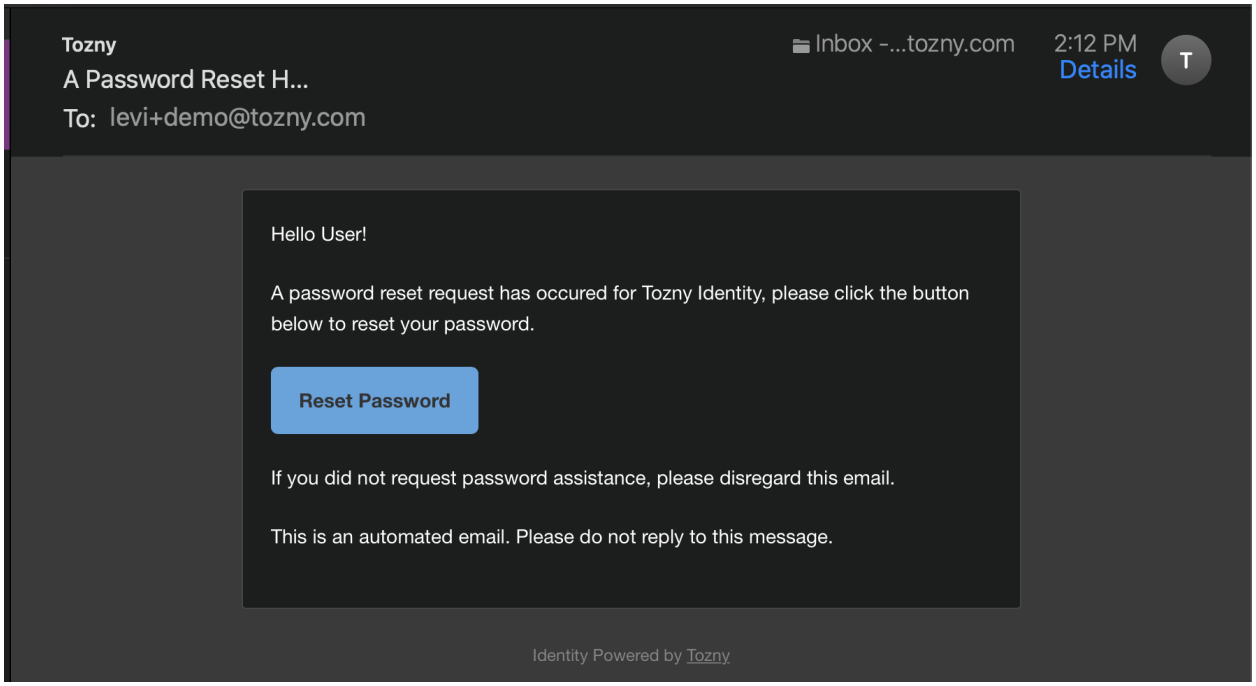
On the upper right side of the screen click on ‘Add user’, and enter information for the new identity.



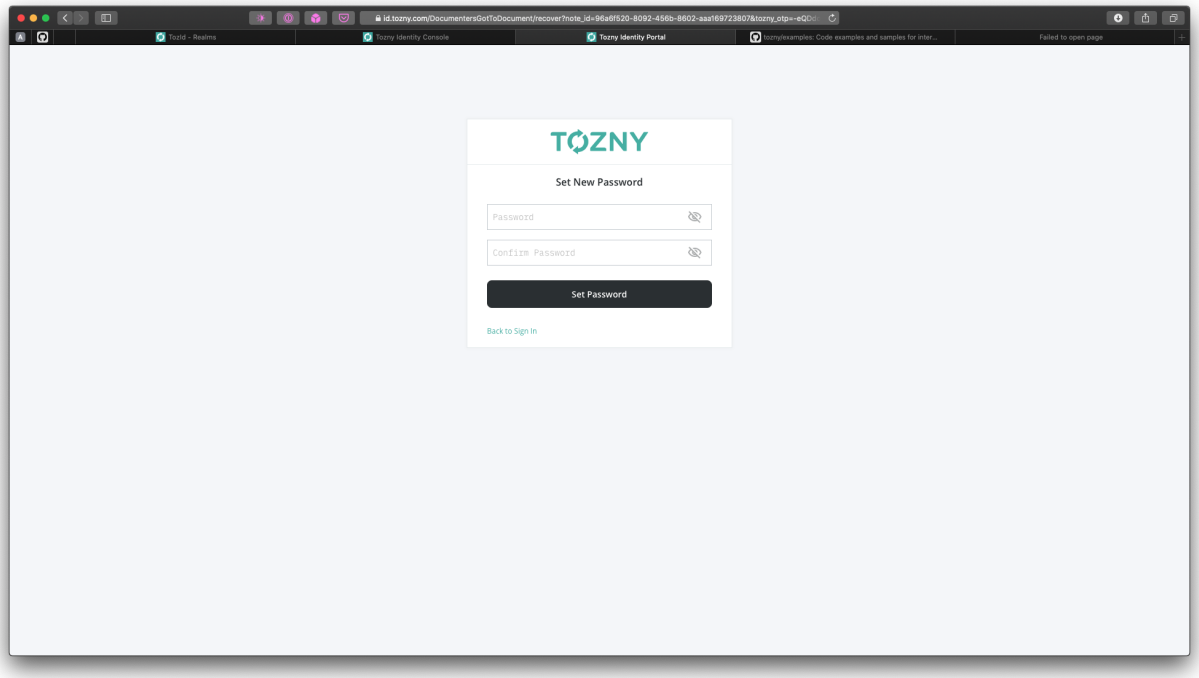
Click create, and after a few seconds the new identity will be created.



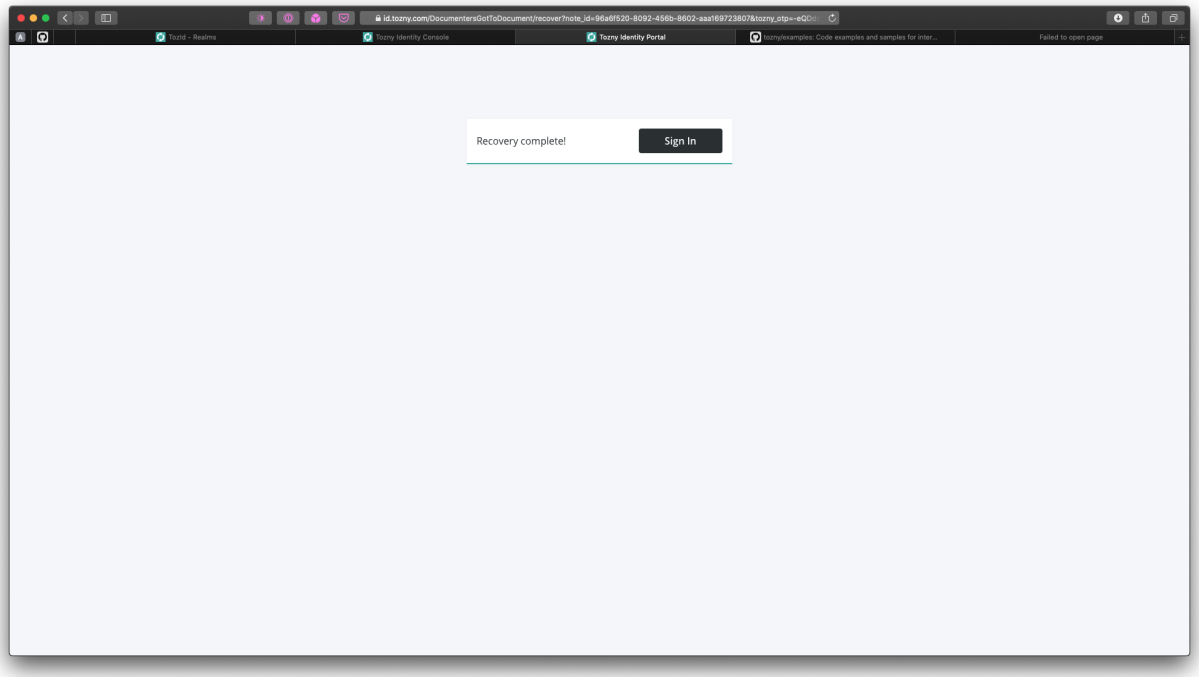
An email will be sent to the specified email address containing a link for the new identity to set their password, or you can also use the ‘Password Reset Link’ value (which will only be shown on initial identity creation, but a password reset can be triggered at a later time as well) to give to the user over another secure channel.



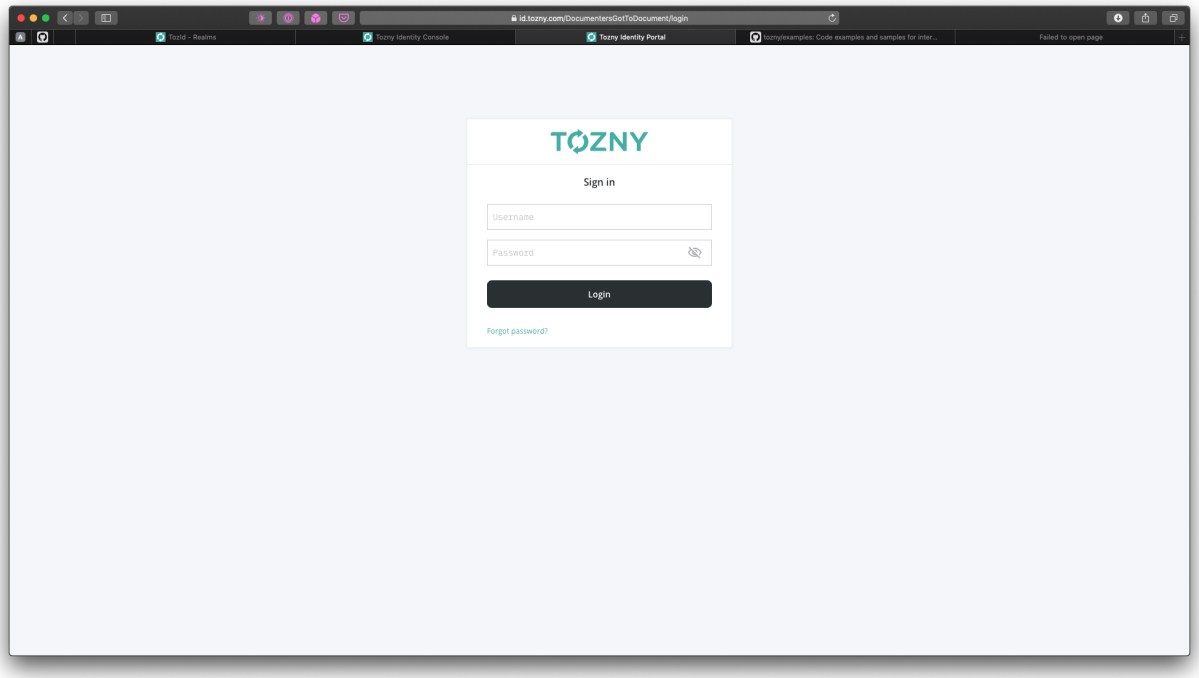
To finish setting up the identity, either click the ‘Reset Password’ button in the email or navigate to the url specified by the ‘Password Reset Link’ .



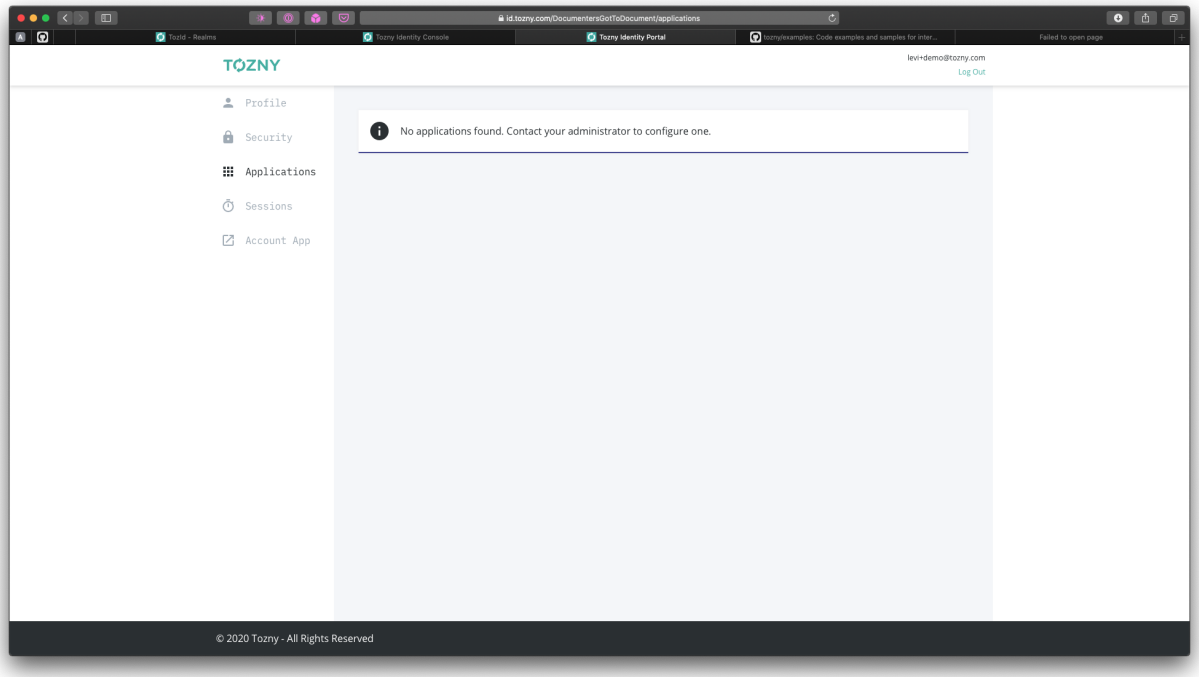
Enter a strong password and click `Set Password`. Upon success the following screen will be shown:



Click `Sign In` and enter the username and password associated with the identity

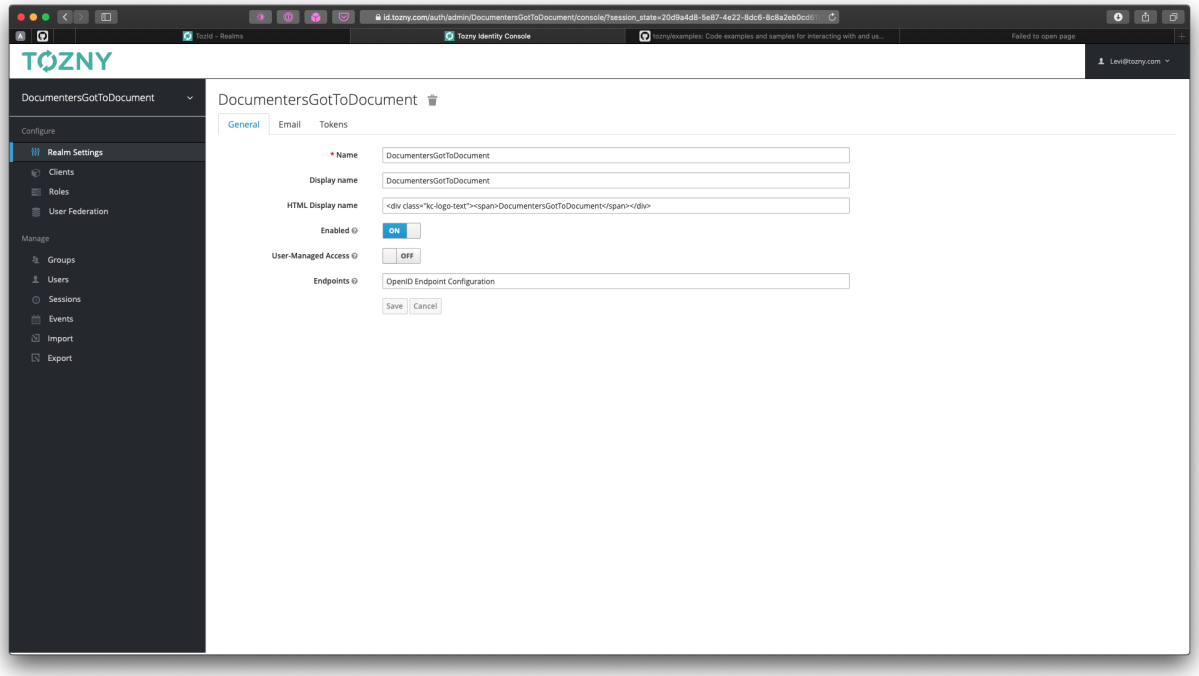


Click ‘Login’ and you will be taken to the Identity Portal page, at this time the identity will have no applications associated with them.

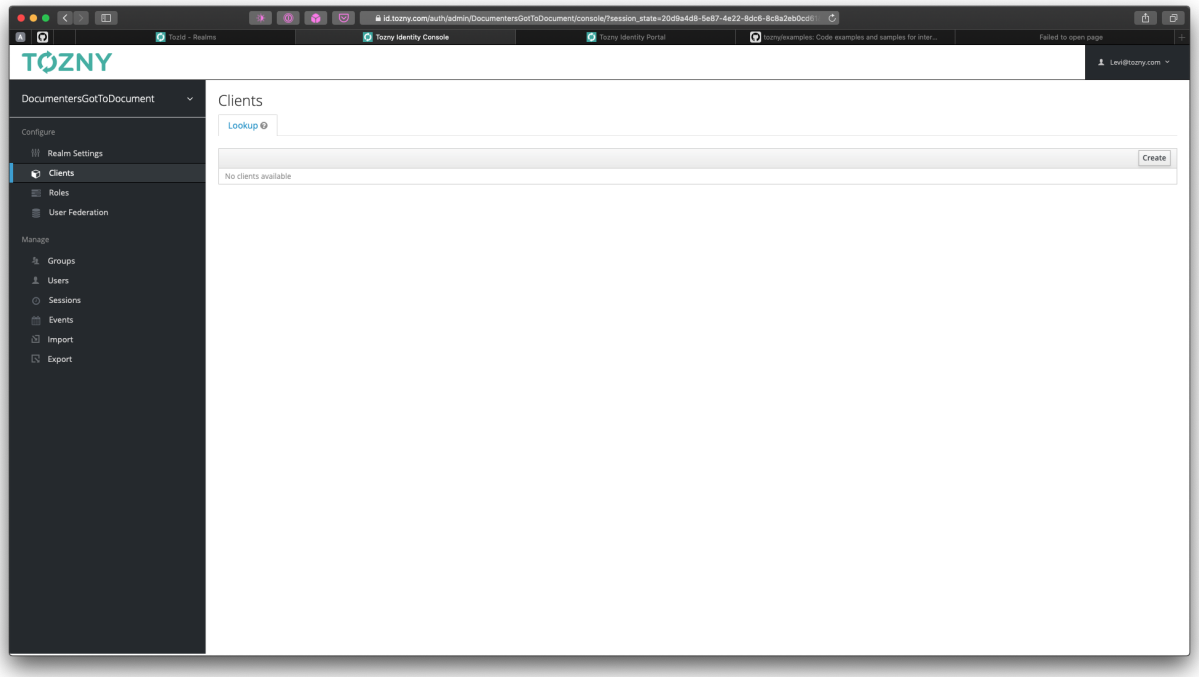


Create Realm Client Application

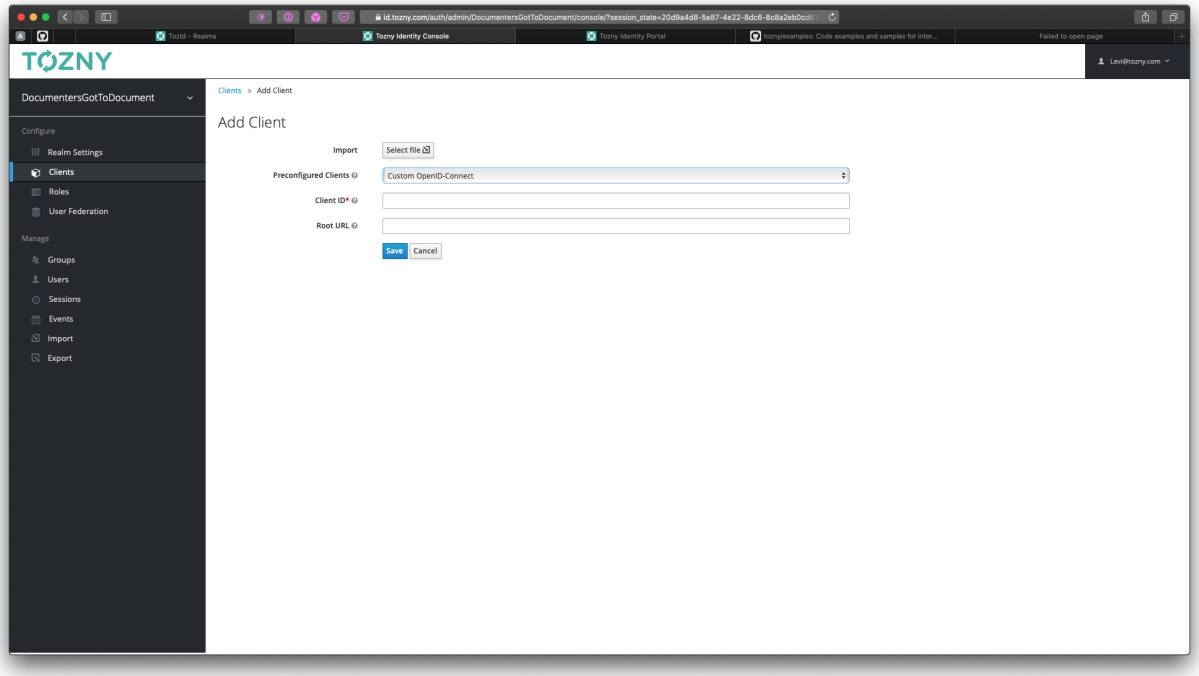
Next you will create an application for the identity to be able to log in to. Navigate back to the Realm Admin Portal for the previously created realm.



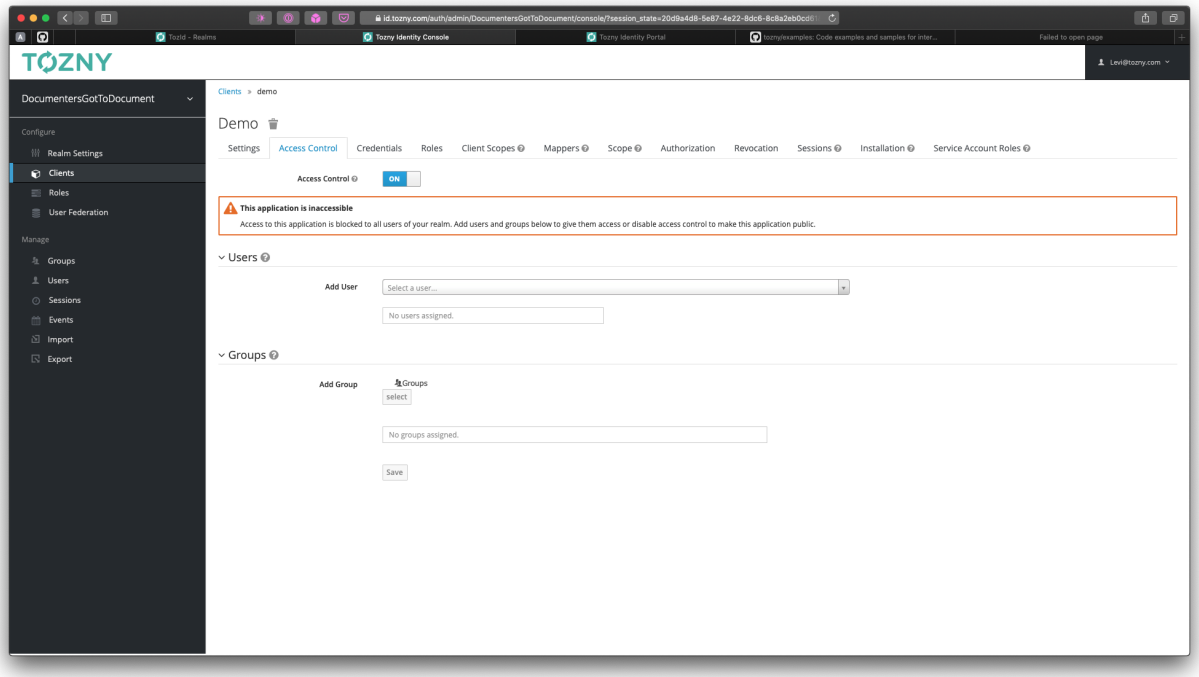
On the upper left menu, click on ‘Clients’



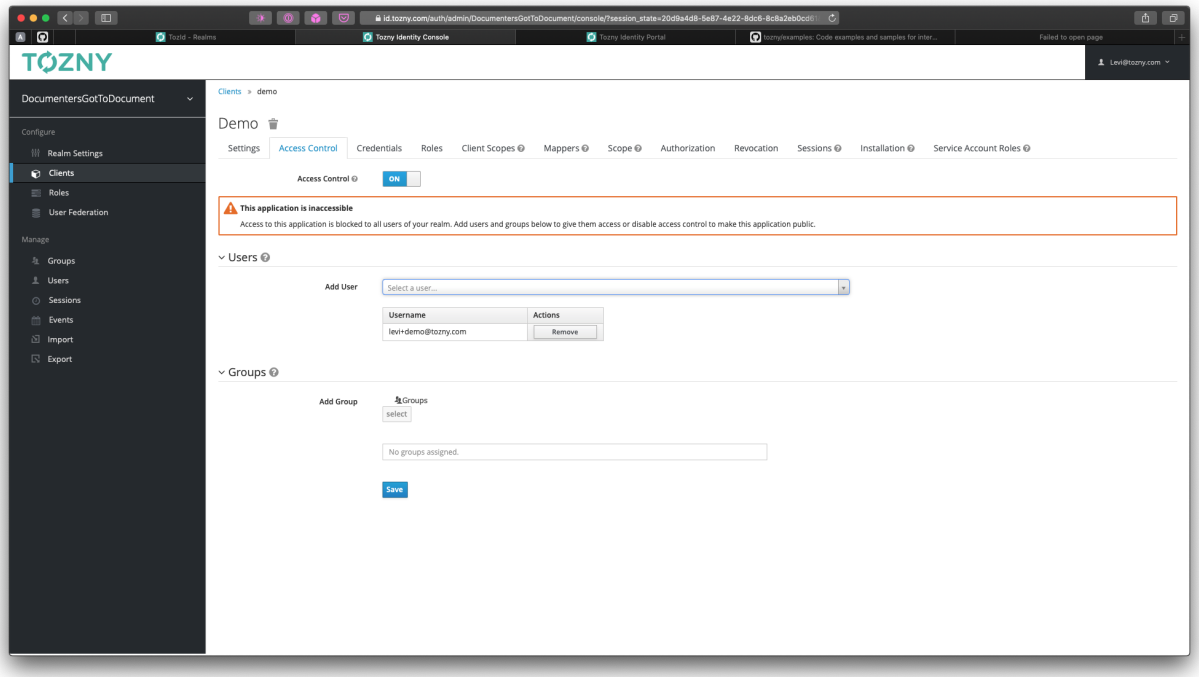
Click ‘Create’ on the right side of the screen



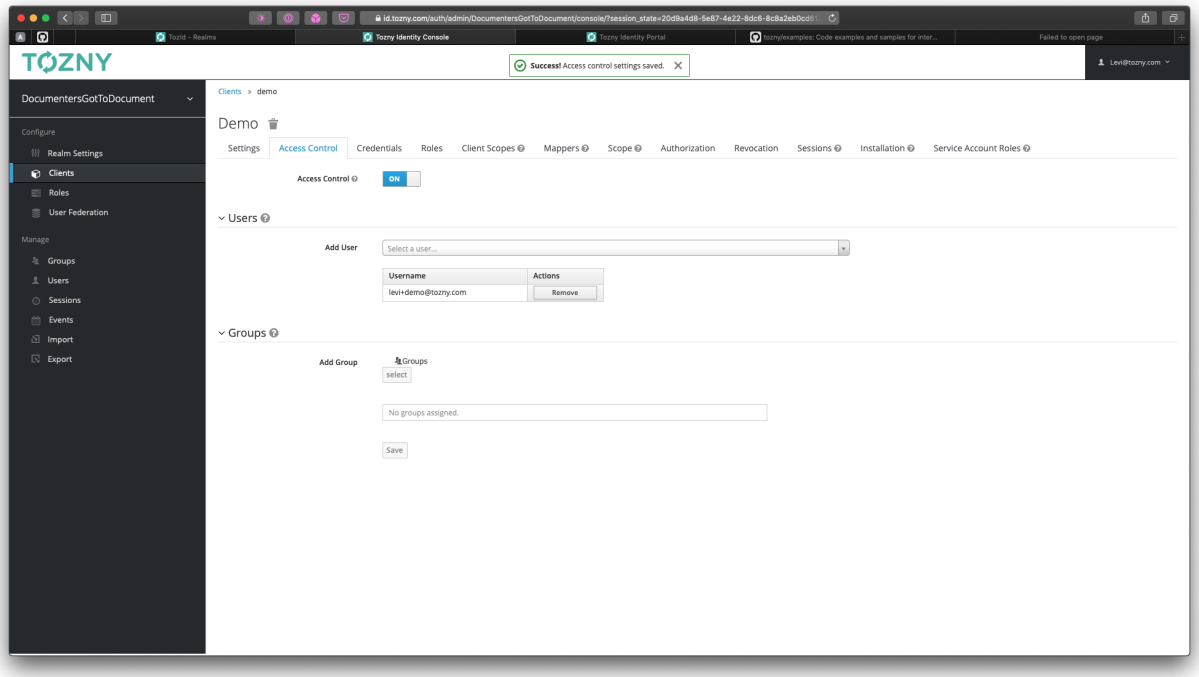
Select `Custom OpenID-Connect` for `Preconfigured Clients`, choose a meaningful and unique name, leave the `Root URL` blank, and select `Save`.



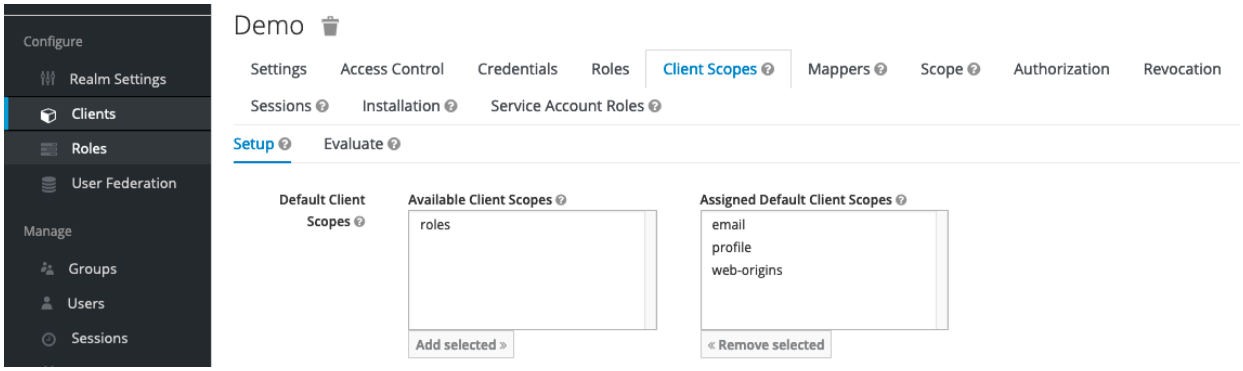
Under the `Users` section, type the username of the previously created identity.



Hit save and now that identity will be authorized to login to this application using TozID.



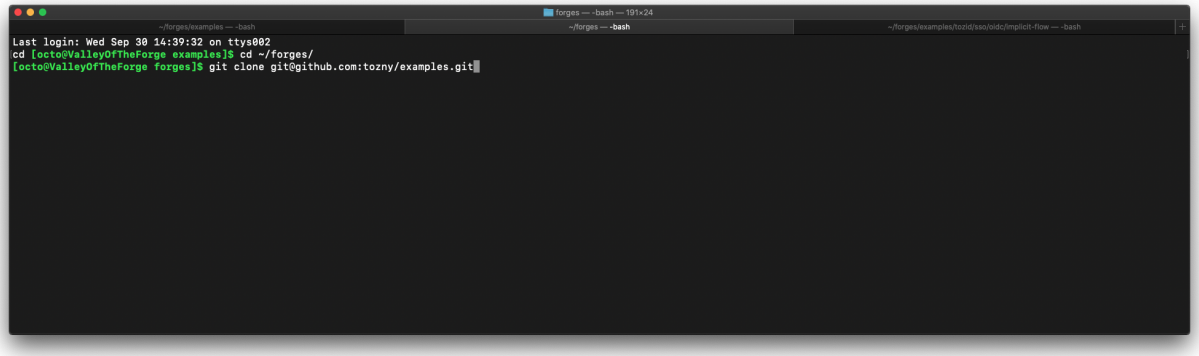
Finally, we must make the roles available in the client scope. This adds the roles to the token claims.
Under the ‘Client Scopes’ section, add ‘role` to the ‘Assigned Default Client Scopes. Hit save.



Create SSO Application

Next, we will set up and run a web server that will use TozId via the OIDC implicit flow to allow authorized identities to log into it. You can clone and run the example application provided via the Tozny `examples` GitHub repo: https://github.com/tozny/examples/tree/trunk/tozid/sso/oidc/implicit-flow

In a terminal, clone the Tozny examples repo



Change into that repo, and navigate to the `tozid/sso/oidc/implicit-flow` directory.

Open the `main.js` file in the `public/javascript` directory.

Update the values to match that of your created realm and client application, e.g.

```
const TOZID_REALM_NAME = 'DocumentersGotToDocument';
const TOZID_CLIENT_ID = 'demo';
const TOZID_HOSTNAME = 'https://id.tozny.com';
```

Save the file. Navigate back to the `tozid/sso/oidc/implicit-flow` directory.

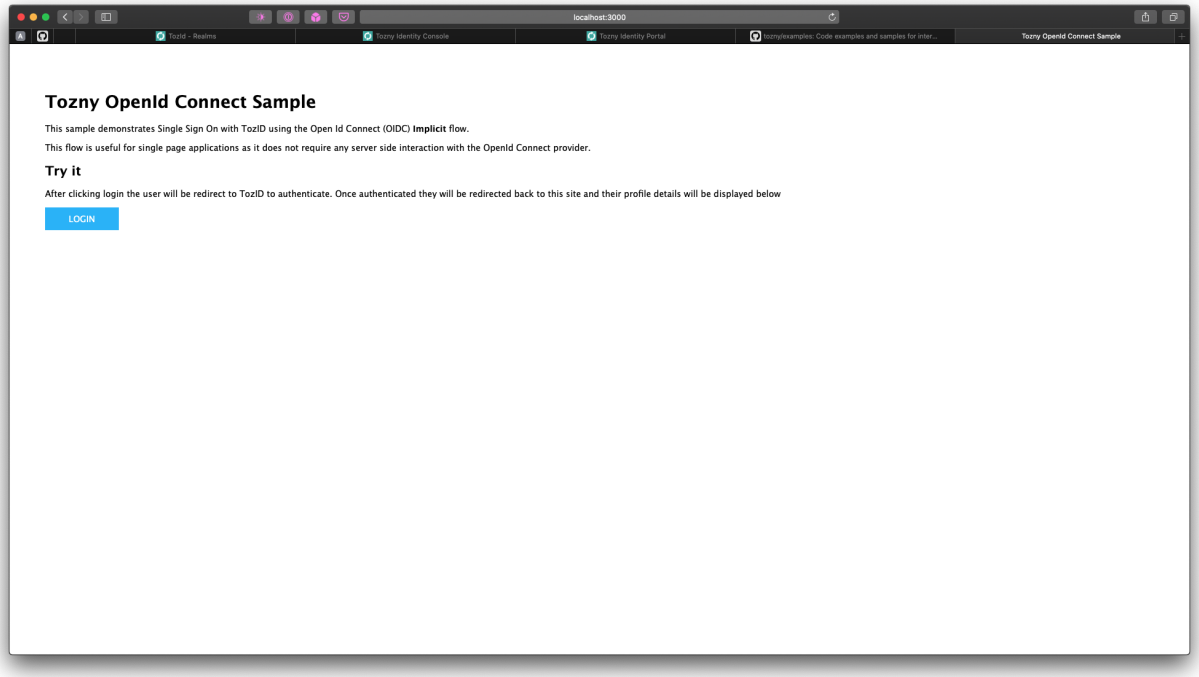
Install all dependencies for the project by running

```
npm install
```

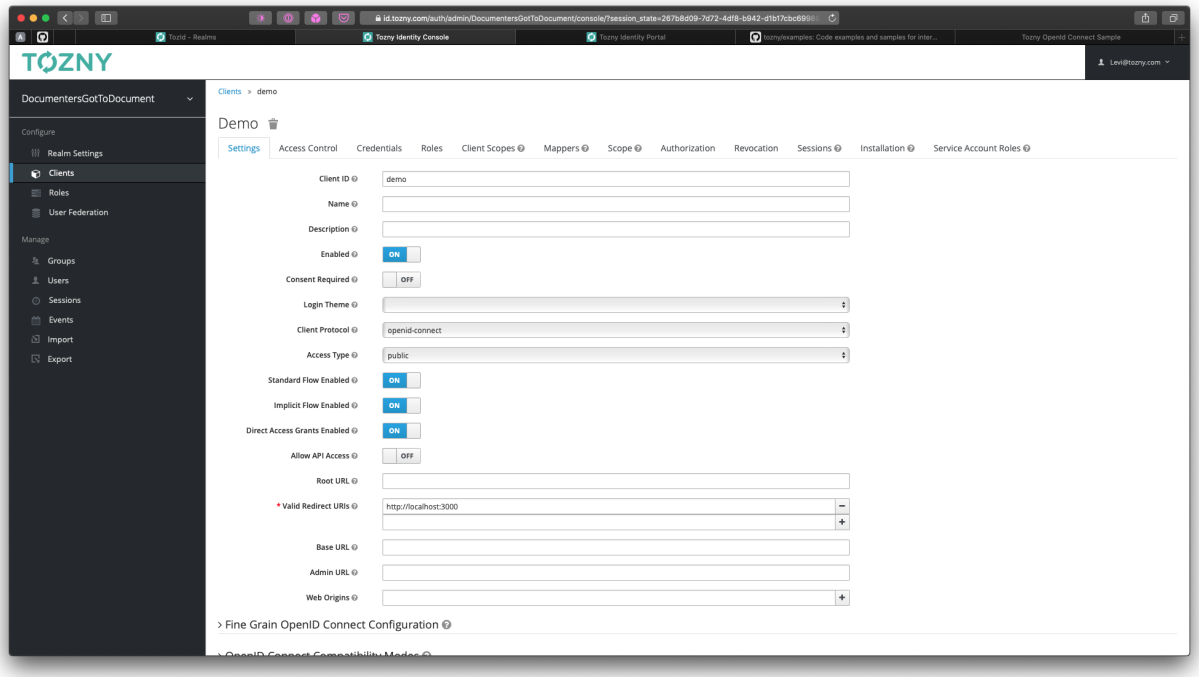
Start the web server by running

```
npm run start
```

Navigate to the web server in your browser at `http://localhost:3000`



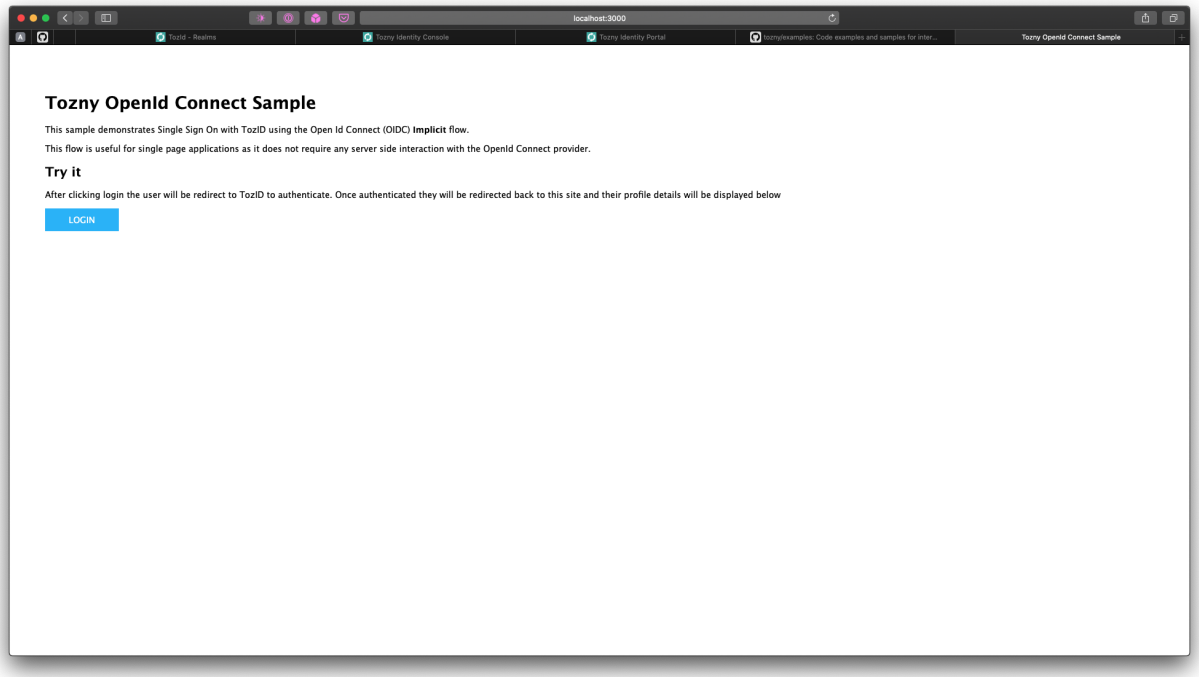
Navigate back to the realm client application, toggle the `Implicit Flow Enabled` to on and update the redirect URLS to include `http://localhost:3000`, otherwise the realm will not allow the user to be redirected back to the application once they have signed in or for the application to use the Implicit Flow to log the user in.



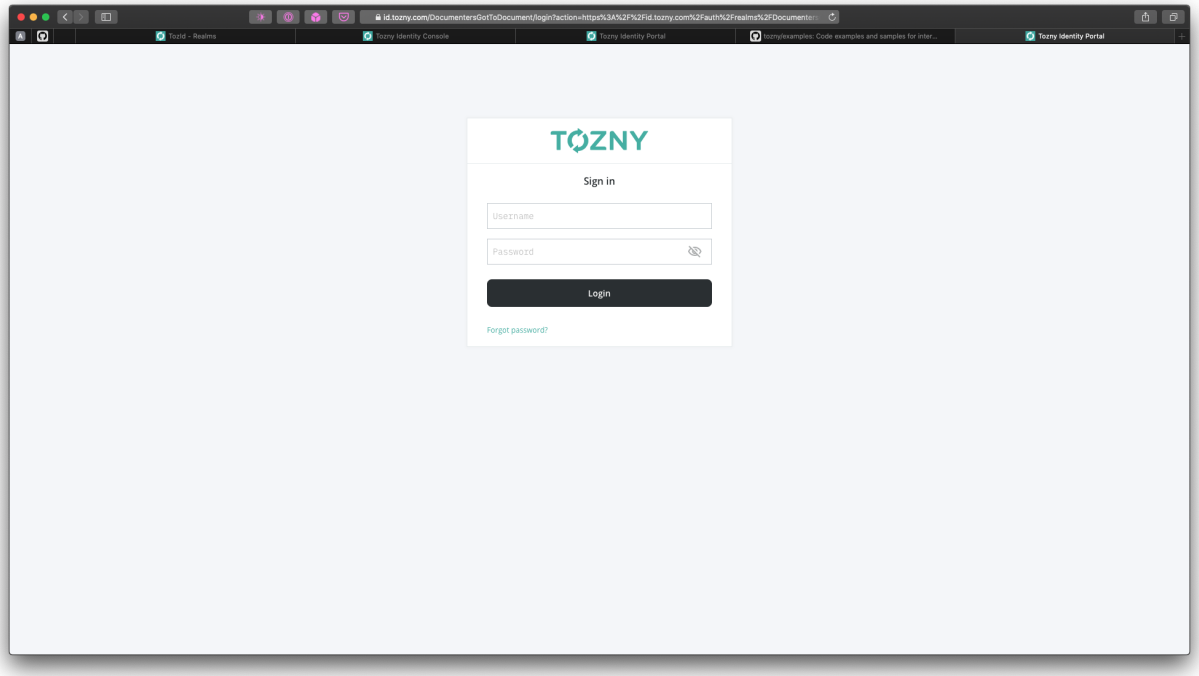
Click ‘Save’

Login to SSO Application using TozID

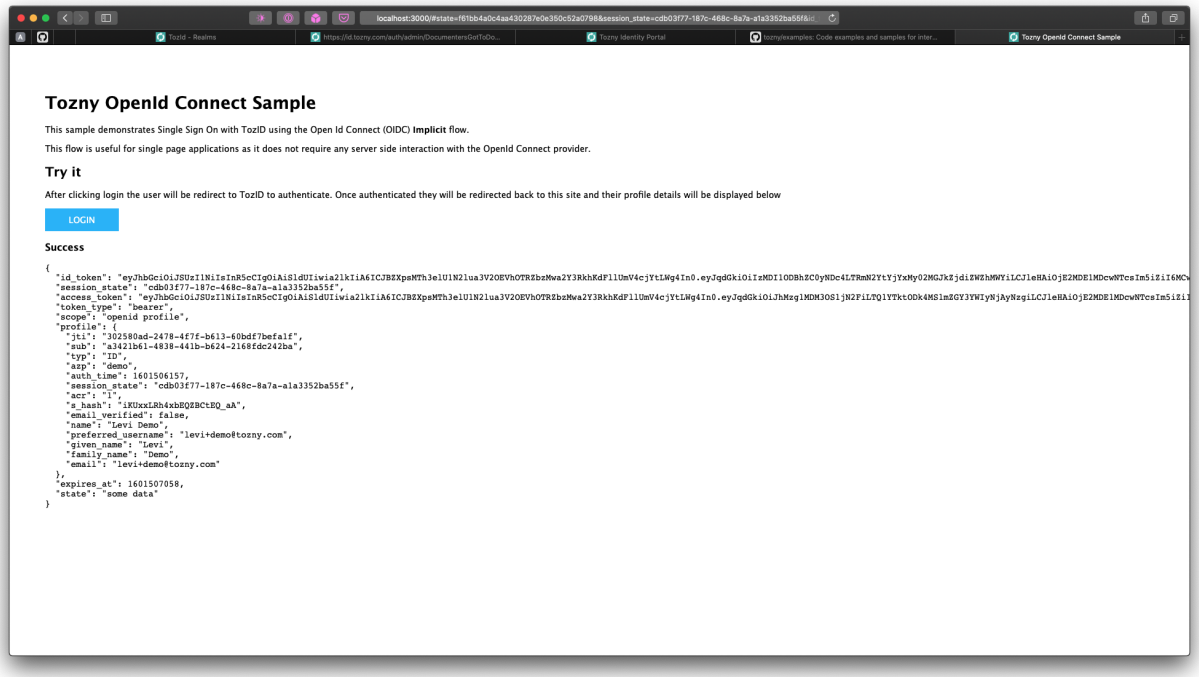
Navigate back to the local web server, and click ‘Login’.



Login to TozId using the username and password associated with the previously created and authorized identity



Upon success you will be redirected back to the local web server application.



Congratulations, you've just successfully set up a simple but powerful and flexible single sign on flow for your application.