

# TozID Powered OIDC Implicit Flow Third Party SSO

## Purpose

[Create / Sign into Tozny Dashboard](#)

[Create TozID Realm](#)

[Create Realm Identity](#)

[Create Realm Client Application](#)

[Create SSO Application](#)

[Login to SSO Application using TozID](#)

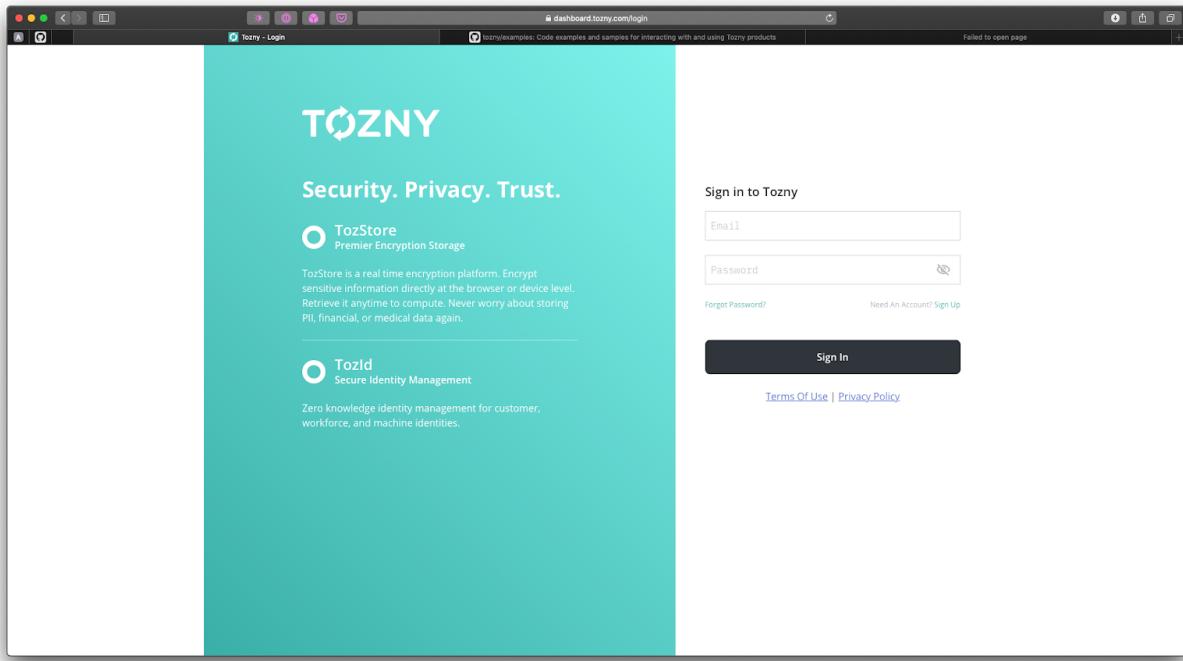
## Purpose

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

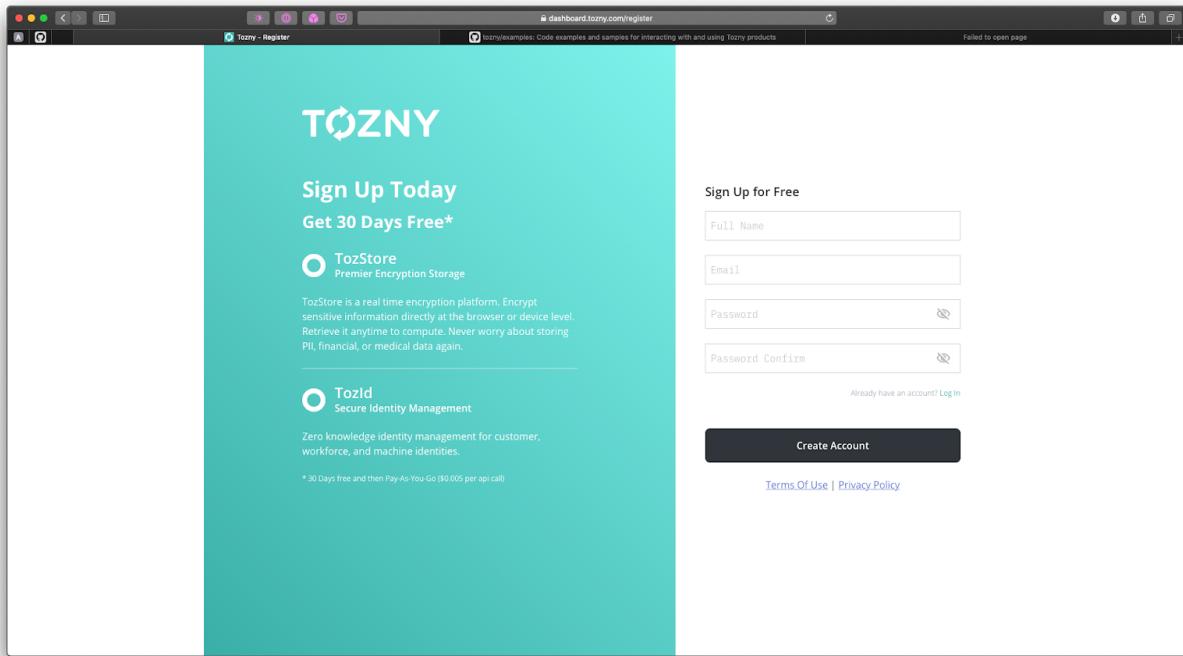
To get started, you will either need to create a Tozny account, or sign into your existing account.

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.

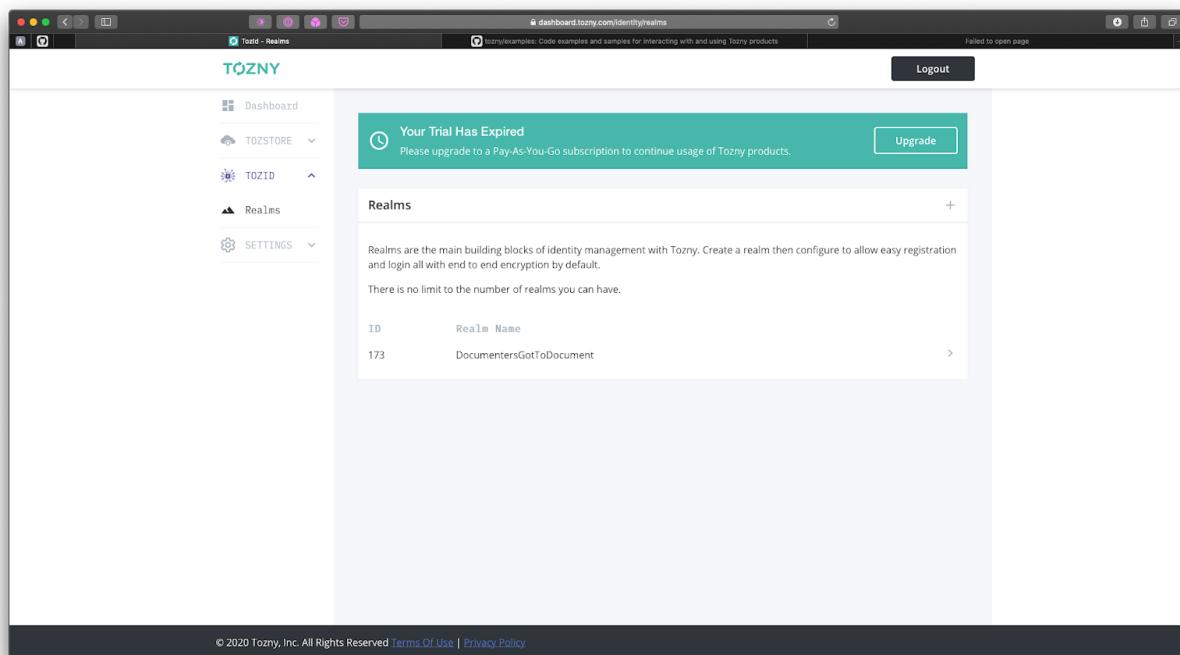
Once you've created or logged into your existing account, you will receive an email to verify your account.

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 menubar, and click on realms.



The screenshot shows the Tozny dashboard interface. On the left, there is a sidebar with navigation links: Dashboard, TOZSTORE, TOZID (which is currently selected), and Realms. Below the sidebar, there is a 'SETTINGS' dropdown. The main content area is titled 'Realms'. At the top of this section, there is a teal-colored banner with the text 'Your Trial Has Expired' and 'Please upgrade to a Pay-As-You-Go subscription to continue usage of Tozny products.' with a 'Upgrade' button. Below the banner, the text 'Realms are the main building blocks of identity management with Tozny. Create a realm then configure to allow easy registration and login all with end to end encryption by default.' is displayed. Underneath this text, it says 'There is no limit to the number of realms you can have.' A table lists one realm: ID 173, Realm Name DocumentersGotToDocument. At the bottom of the page, there is a footer bar with the text '© 2020 Tozny, Inc. All Rights Reserved [Terms Of Use](#) | [Privacy Policy](#)'.

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

The screenshot shows a web browser window for the Tozny Identity Console. The URL is `dashboard.tozny.com/identity/realm`. A prominent green banner at the top states "Your Trial Has Expired" with a note to upgrade to a Pay-As-You-Go subscription. Below the banner, the page title is "DocumentersGotToDocument" and it shows "Realm ID: 173". The "Realm Admin" email is listed as "levi@tozny.com". A toggle switch indicates "Email Recovery Enabled". A "Manage Realm" button is present. A "Danger Zone" section contains a red "Delete Realm" button. The bottom of the page includes a copyright notice for Tozny, Inc. and links to Terms Of Use and Privacy Policy.

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

The screenshot shows the "DocumentersGotToDocument" realm settings in the Tozny Identity Console. The left sidebar has "Configure" selected, with "Realm Settings" highlighted. The main panel displays the "General" tab of the realm configuration. It shows the realm's name ("DocumentersGotToDocument"), display name ("DocumentersGotToDocument"), and an HTML display name containing a placeholder for the realm name. The "Enabled" switch is set to "ON". The "User-Managed Access" switch is set to "OFF". An "Endpoints" field is set to "OpenID Endpoint Configuration". There are "Save" and "Cancel" buttons at the bottom. The top navigation bar shows the URL `id.tozny.com/auth/admin/DocumentersGotToDocument/console?session_state=20d9a4d8-5e87-4e22-8dcd-8c8a2eb0cc01`.

## Create Realm Identity

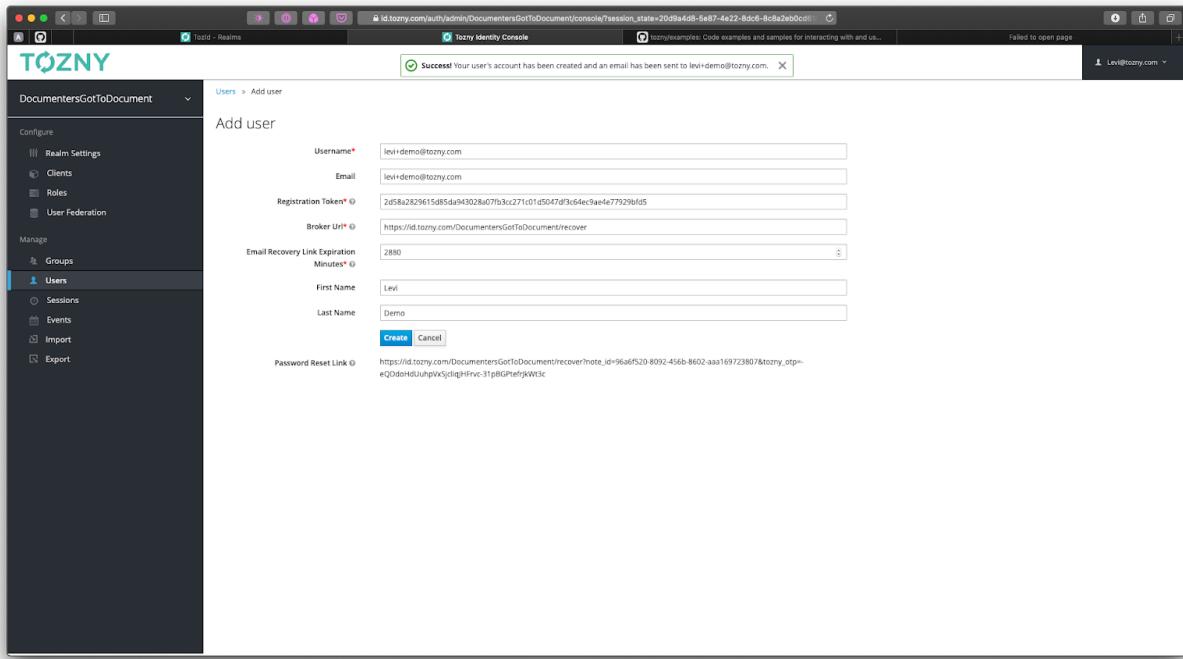
From the lower left menu bar, click on 'Users'

The screenshot shows the 'Users' page of the Tozny Identity Console. The left sidebar has 'Configure' and 'Manage' sections. Under 'Manage', 'Groups' is expanded, and 'Users' is selected. The main area has a search bar and buttons for 'Unlock users', 'Add user', and 'Bulk Add Users'. A message says 'Please enter a search, or click on view all users'.

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

The screenshot shows the 'Add user' form. The left sidebar shows 'Configure' and 'Manage' sections with 'Groups' and 'Users' selected. The form fields are: Username\* (levi+demo@tozny.com), Email (levi+demo@tozny.com), Registration Token\* (2d58a829615d85da943028a07fb3c27101d5047d3c64ec9ae77929bf05), Broker Uri\* (https://id.tozny.com/DocumentersGotToDocument/recover), Email Recovery Link Expiration Minutes\* (2880), First Name (Levi), and Last Name (Demo). There are 'Create' and 'Cancel' buttons at the bottom.

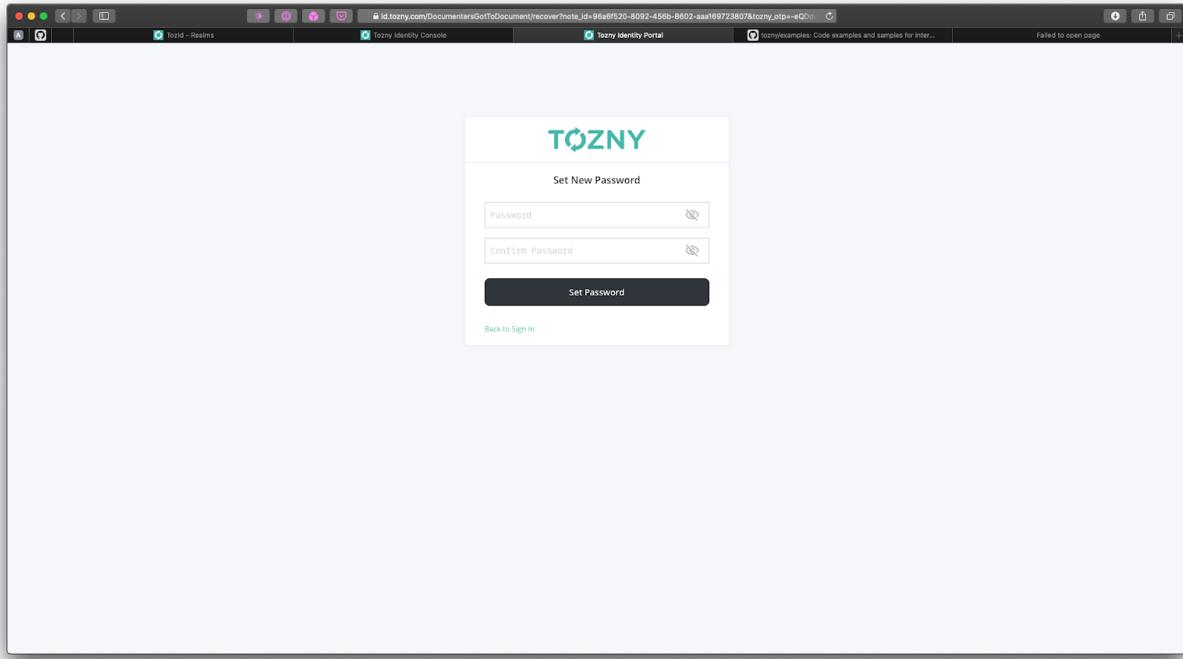
Click create, and after a few seconds the new identity will be created.



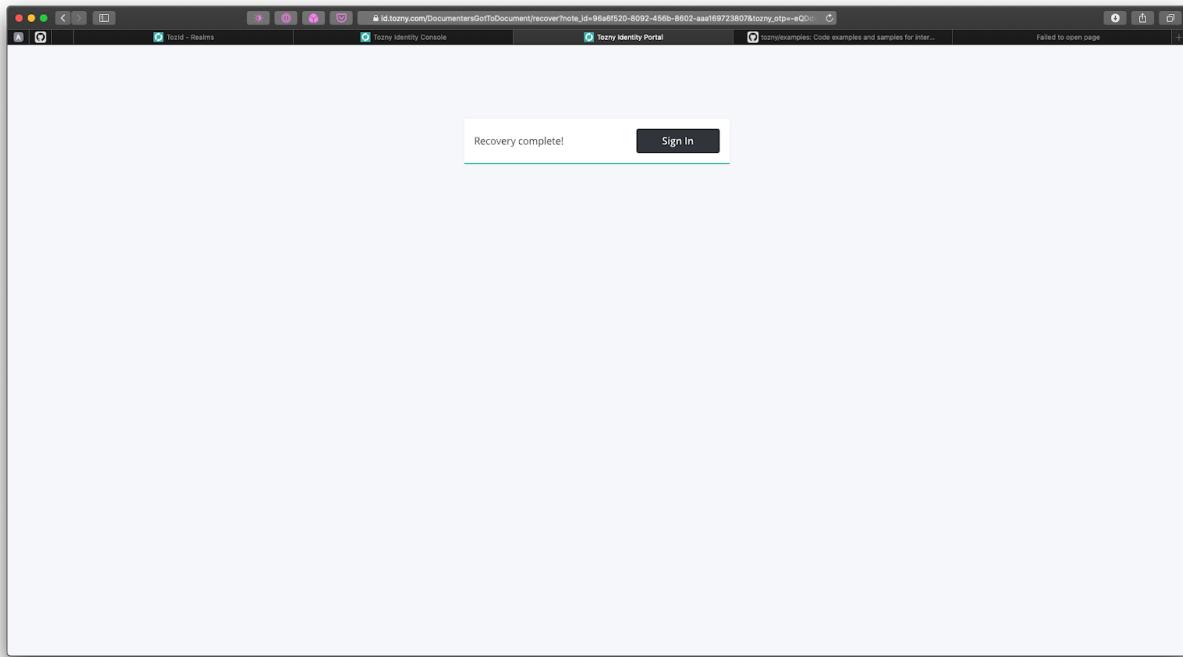
An email will be sent to the specified email address containing a link for the new identity to set their password, or you can also use the 'Password Reset Link' value (which will only be shown on initial identity creation, but a password reset can be triggered at a later time as well) to give to the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

A screenshot of an email inbox. The subject line is "A Password Reset H...". The recipient is "To: levi+demo@tozny.com". The email body contains a message from Tozny: "Hello User! A password reset request has occurred for Tozny Identity, please click the button below to reset your password." Below this is a blue "Reset Password" button. Further down, it says "If you did not request password assistance, please disregard this email." and "This is an automated email. Please do not reply to this message." At the bottom right of the email body, it says "Identity Powered by Tozny". The top right corner of the email shows the time "2:12 PM" and a "Details" link.

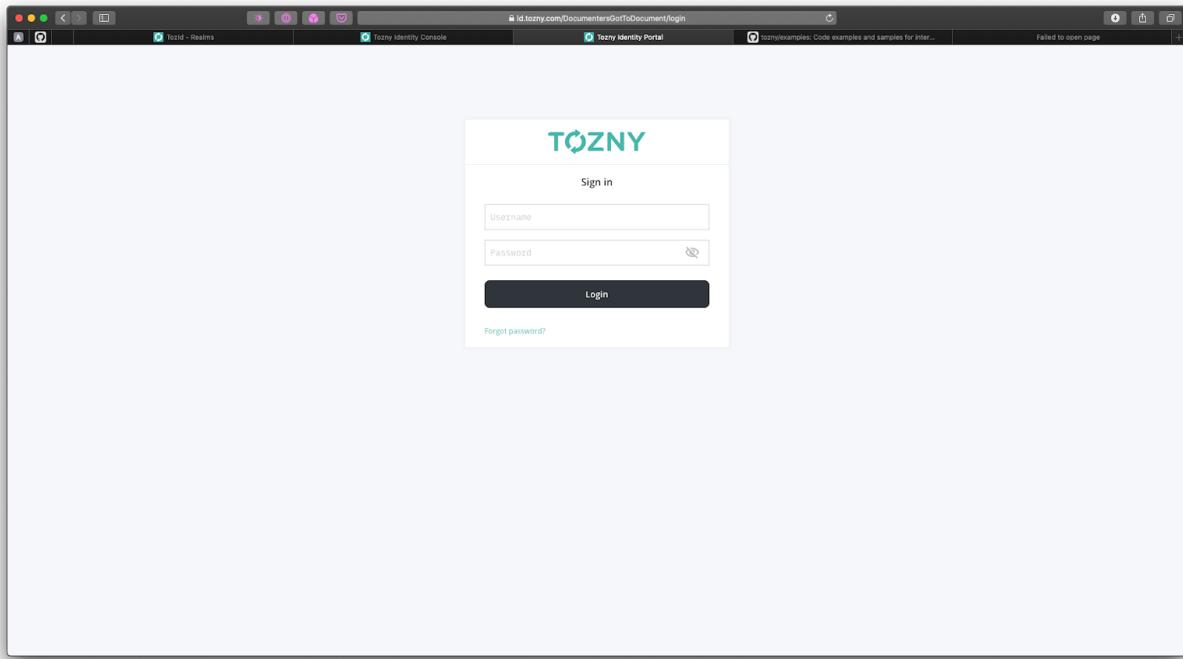
To finish setting up the identity, either click the 'Reset Password' button in the email or navigate to the url specified by the 'Password Reset Link' .



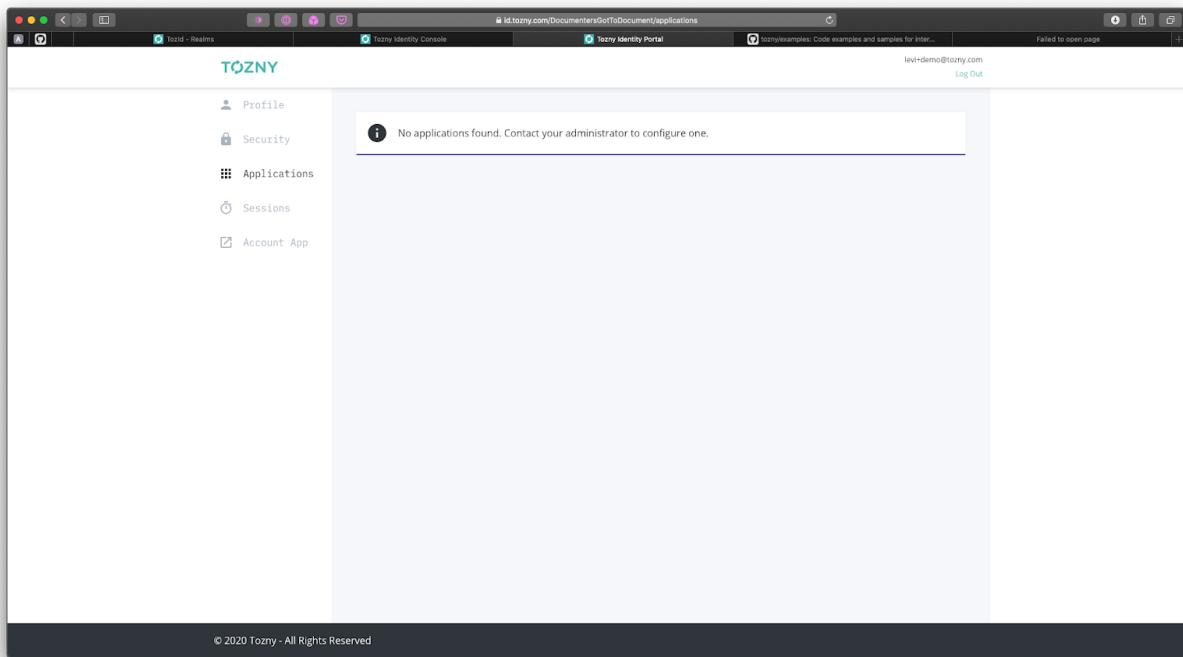
Enter a strong password and click 'Set Password'. Upon success the following screen will be shown:



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

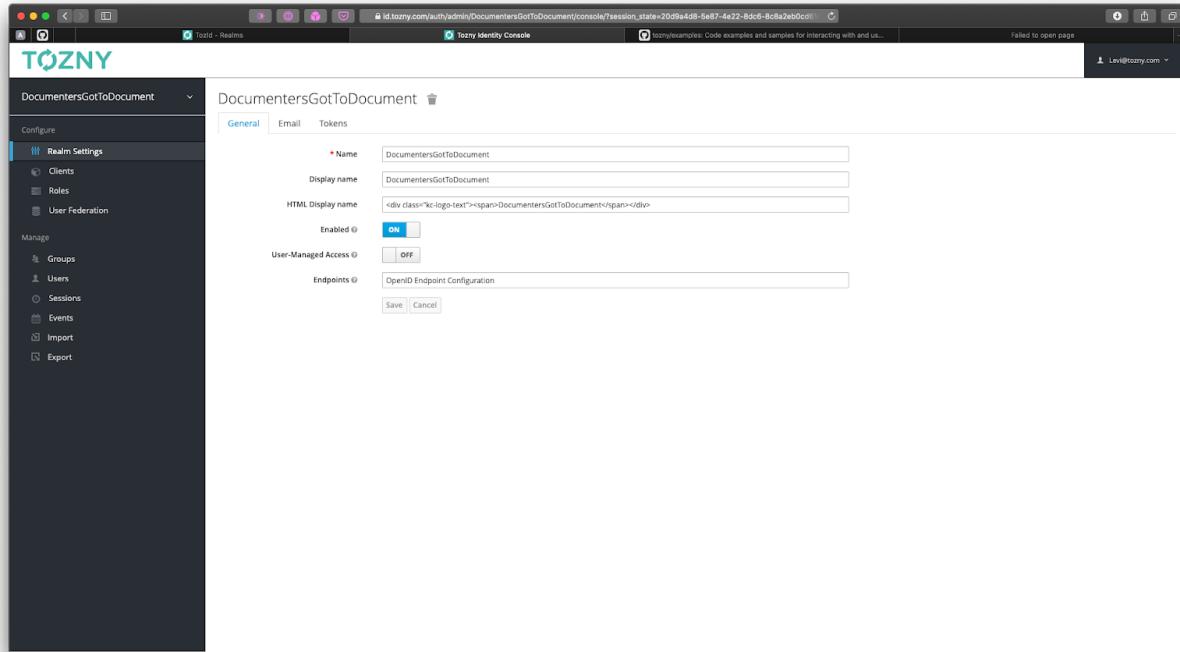


Click 'Login' and you will be taken to the Identity Portal page, at this time the identity will have no applications associated with them.

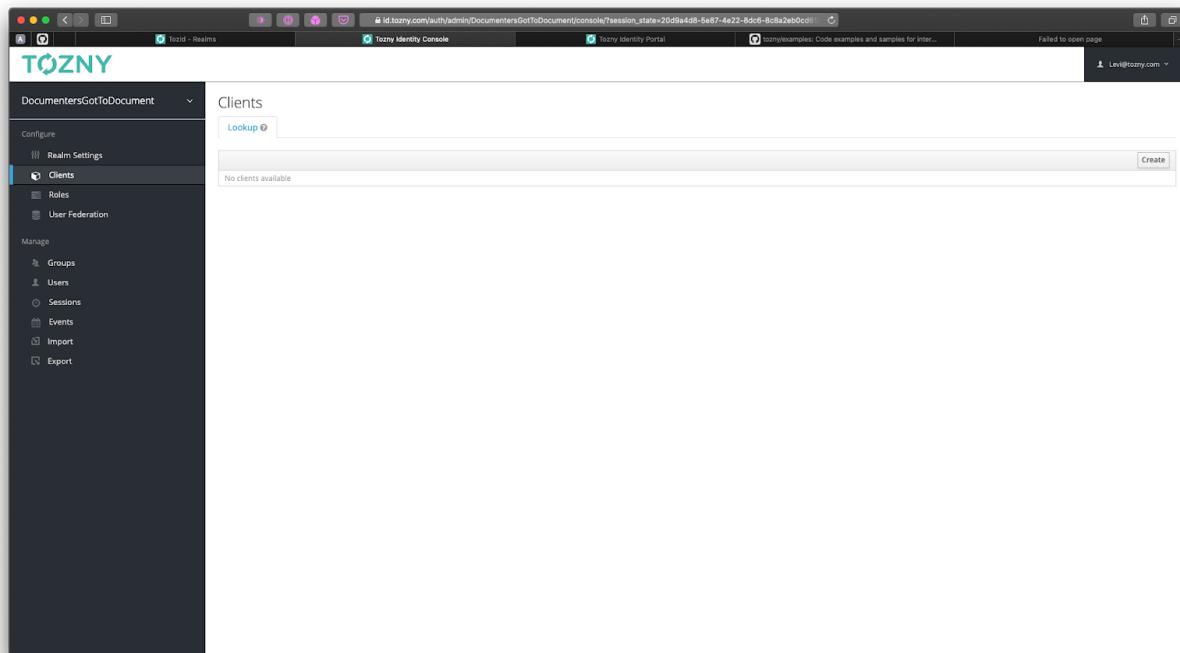


## Create Realm Client Application

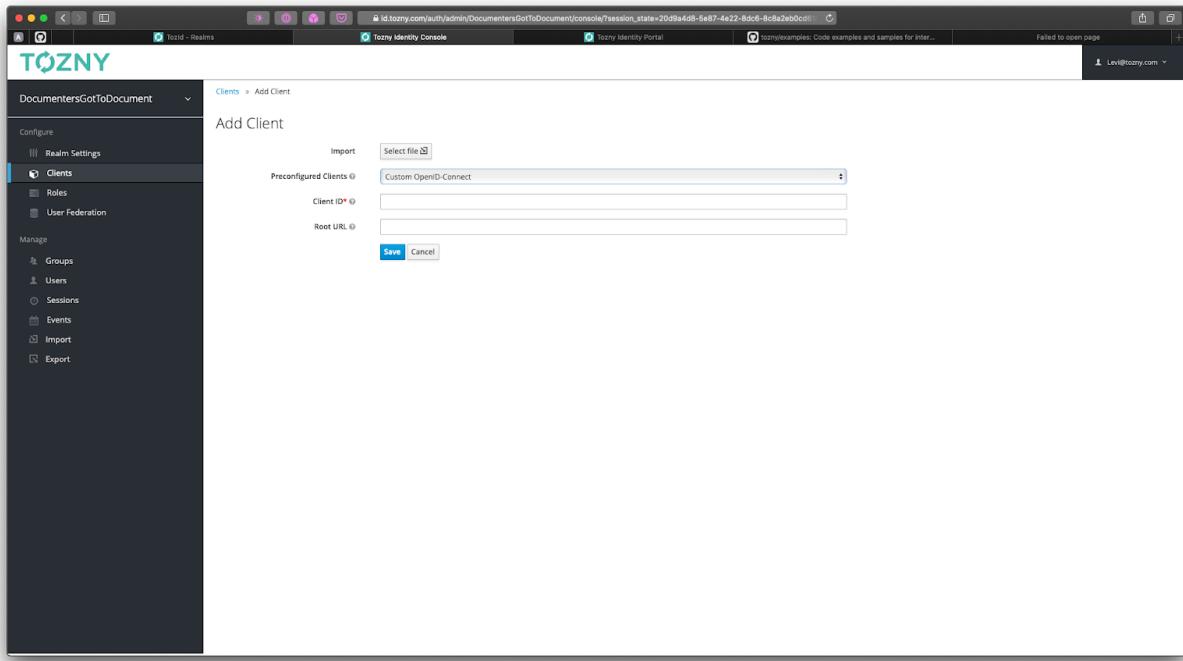
Next you will create an application for the identity to be able to log in to. Navigate back to the Realm Admin Portal for the previously created realm.



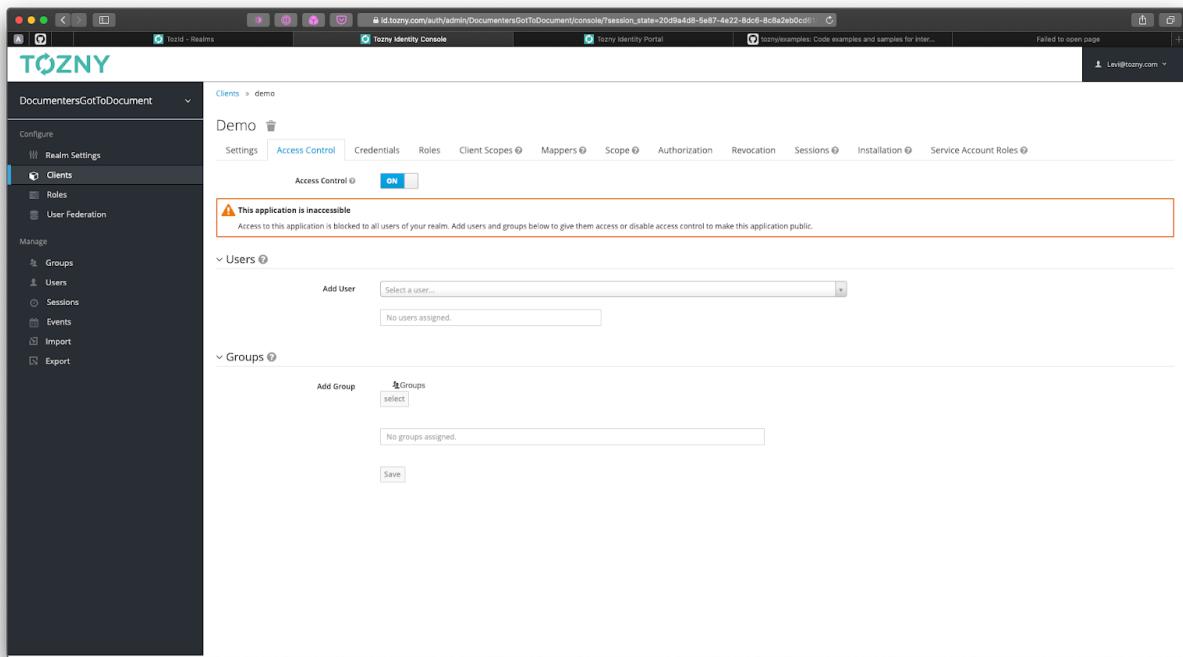
On the upper left menu, click on 'Clients'



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.

This application is inaccessible  
Access to this application is blocked to all users of your realm. Add users and groups below to give them access or disable access control to make this application public.

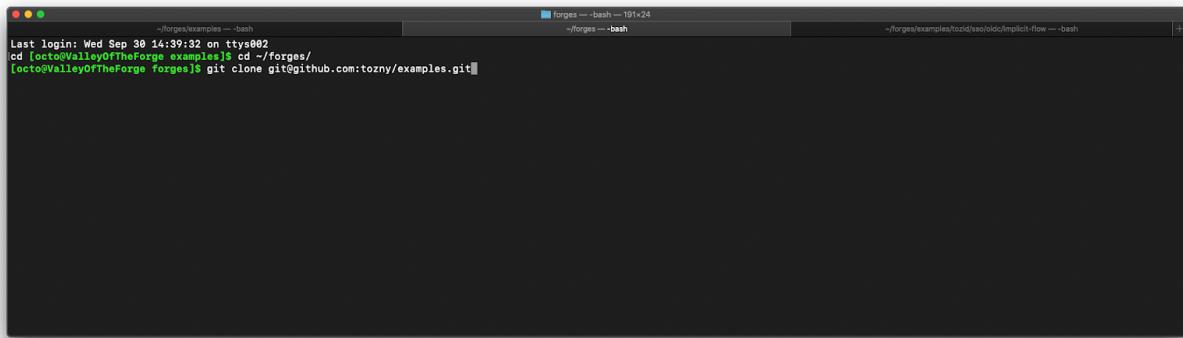
Hit save and now that identity will be authorized to login to this application using TozID.

Success! Access control settings saved.

## 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



A screenshot of a terminal window with three tabs. The first tab shows the command to clone the repository: `Last login: Wed Sep 30 14:39:32 on ttys002  
cd [REDACTED]@[REDACTED]:~/Desktop/forges/  
[REDACTED]@[REDACTED]:~/Desktop/forges> git clone git@github.com:tozny/examples.git`. The second tab shows the command to start the project: `forges -- bash`. The third tab shows the command to run the project: `-/forges/examples/tozid/sso/oidc/implicit-flow -- bash`.

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.

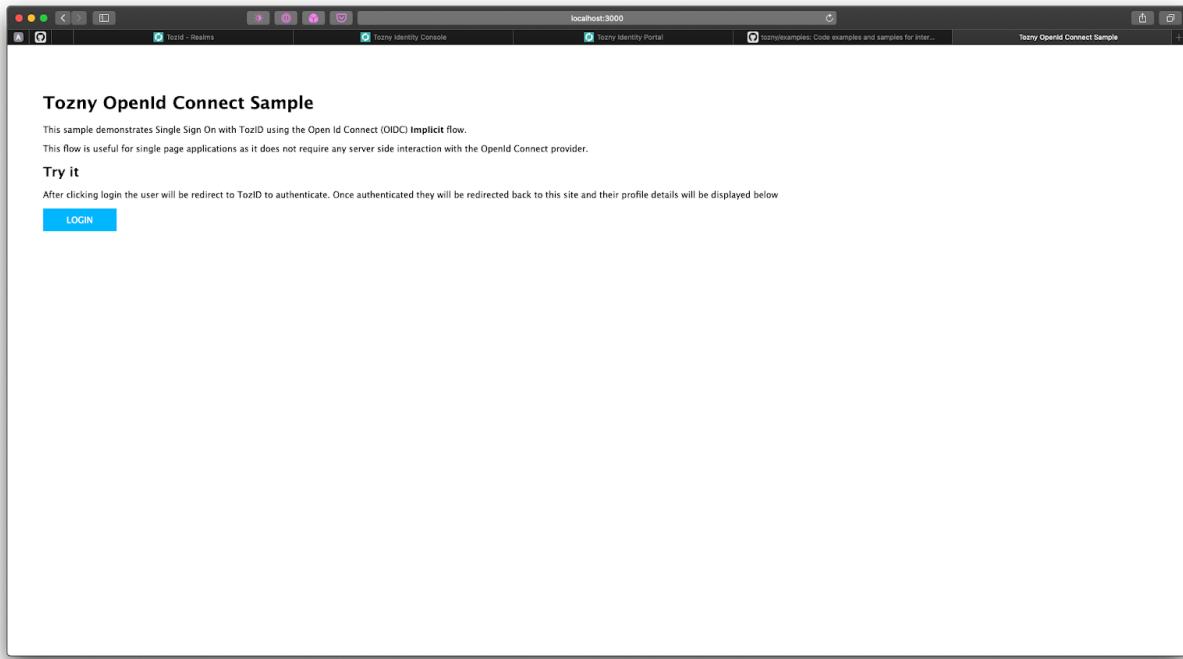
Install all dependencies for the project by running

```
...  
npm install  
...
```

Start the web server by running

```
...  
npm run start  
...
```

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



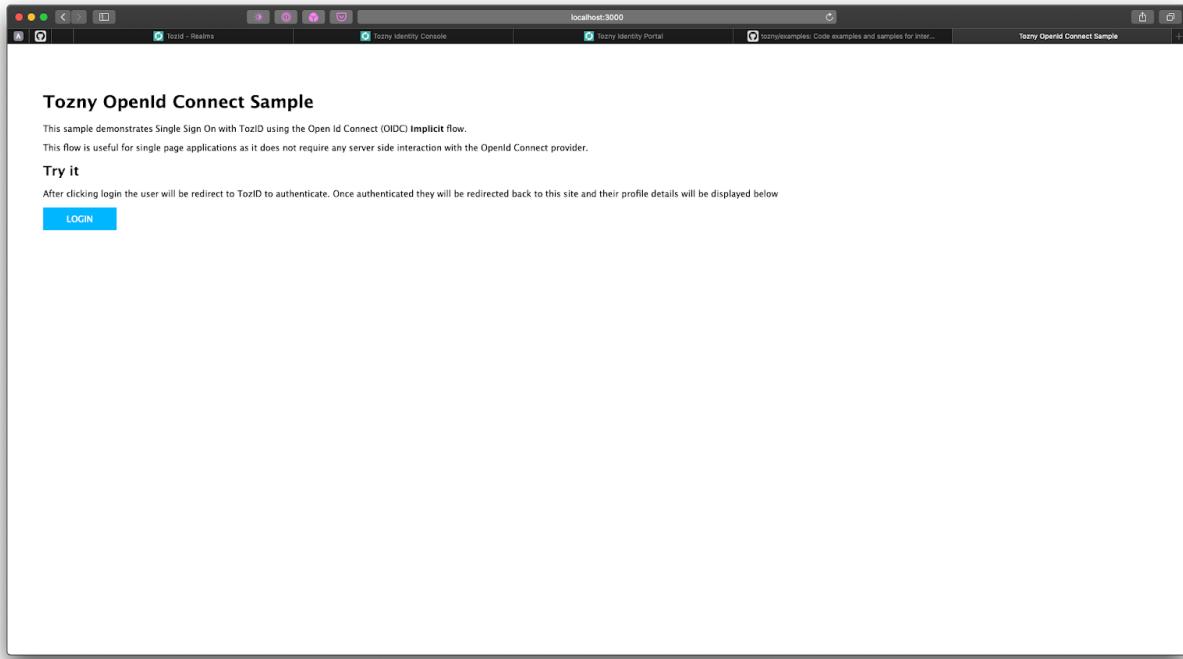
Navigate back to the realm client application, toggle the 'Implicit Flow Enabled' to on and update the redirect URLs to include '<http://localhost:3000>', otherwise the realm will not allow the user to be redirected back to the application once they have signed in or for the application to use the Implicit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

A screenshot of the Tozny Identity Console interface. On the left, a sidebar shows navigation options like "DocumentersGotToDocument", "Configure", "Clients", "Manage", "Groups", "Users", "Sessions", "Events", "Import", and "Export". The main area is titled "Demo" and shows the "Settings" tab for a client named "demo". The configuration includes fields for Client ID (demo), Name, Description, Enabled (ON), Consent Required (OFF), Login Theme, Client Protocol (openid-connect), Access Type (public), Standard Flow Enabled (ON), Implicit Flow Enabled (ON), Direct Access Grants Enabled (ON), Allow API Access (OFF), Root URL, and Valid Redirect URLs (containing "http://localhost:3000"). Other fields shown are Base URL, Admin URL, and Web Origins. At the bottom, there are links for "Fine Grain OpenID Connect Configuration" and "OpenID Connect Compatibility Modes".

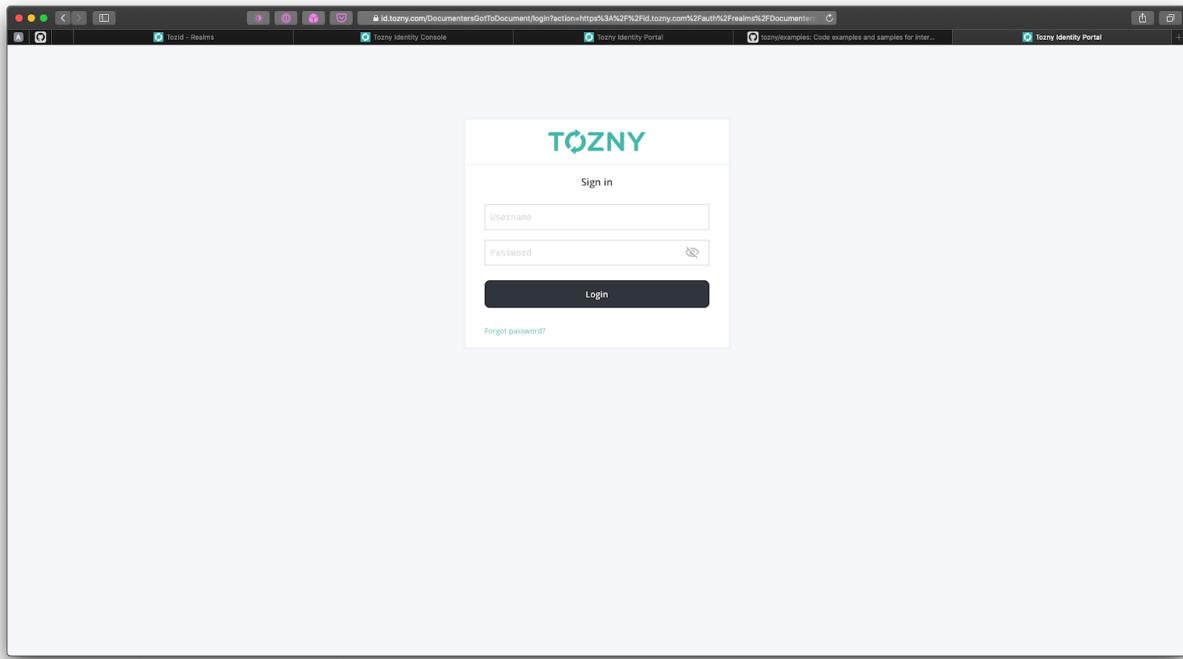
Click 'Save'

# 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.

```
Success

{
  "id_token": "eyJhbGciOiJIUzI1NiJ9.eyJhdWxiaoXlAaS1dHtIwia2kI1IA61CJBZXpMTh3e1U1N2ua3V2OEVhOTREbzMwa2Y3RkhKdFllUmV4cjt4Ng4In0.eyJqdGkiOiIzM0110DbhZC0yNDc4LTmNzTtYjYxMy92MGJkZjdIZWzhMWY1LCJleHAiOjE2MDE1MDcwNTcsIm5iZlEiMCs...",
  "session_state": "cd03f77-187c-468c-8a7a-a1a3352ba554",
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ0b3IwLmNvbmZpZW5kb25lIiwia2lkI1ia61CJBZXpMTh3e1U1N2ua3V2OEVhOTREbzMwa2Y3RkhKdFllUmV4cjt4Ng4In0.eyJqdGkiOiJhNmglMDM3061jN2FiLT01YTktdODk4Ms1mZGY3YWiYjAyNzgiLCJleHAiOjE2MDE1MDcwNTcsIm5iZlEiMCs...",
  "token_type": "bearer",
  "token_expires_in": 3600,
  "profile": {
    "name": "Levi Demo",
    "given_name": "Levi",
    "family_name": "Demo",
    "email": "levi+demo@tozny.com",
    "email_verified": true,
    "preferred_username": "levi+demo@tozny.com",
    "picture": "https://www.gravatar.com/avatar/422b614-4838-441b-b624-2168fdc242ba"
  },
  "state": "some data"
}
```

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