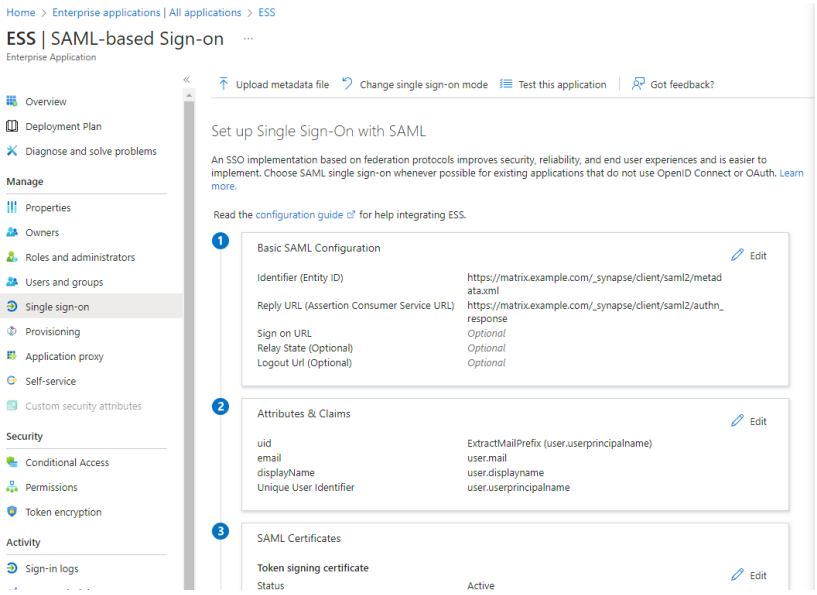
Setting up Delegated Authentication with SAML on Microsoft Azure

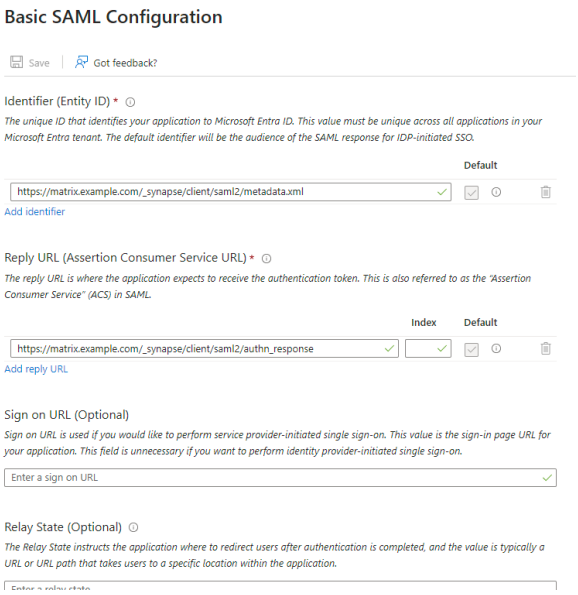
Before setting up the installer, you have to configure Microsoft Entra ID.

Set up Microsoft Entra ID

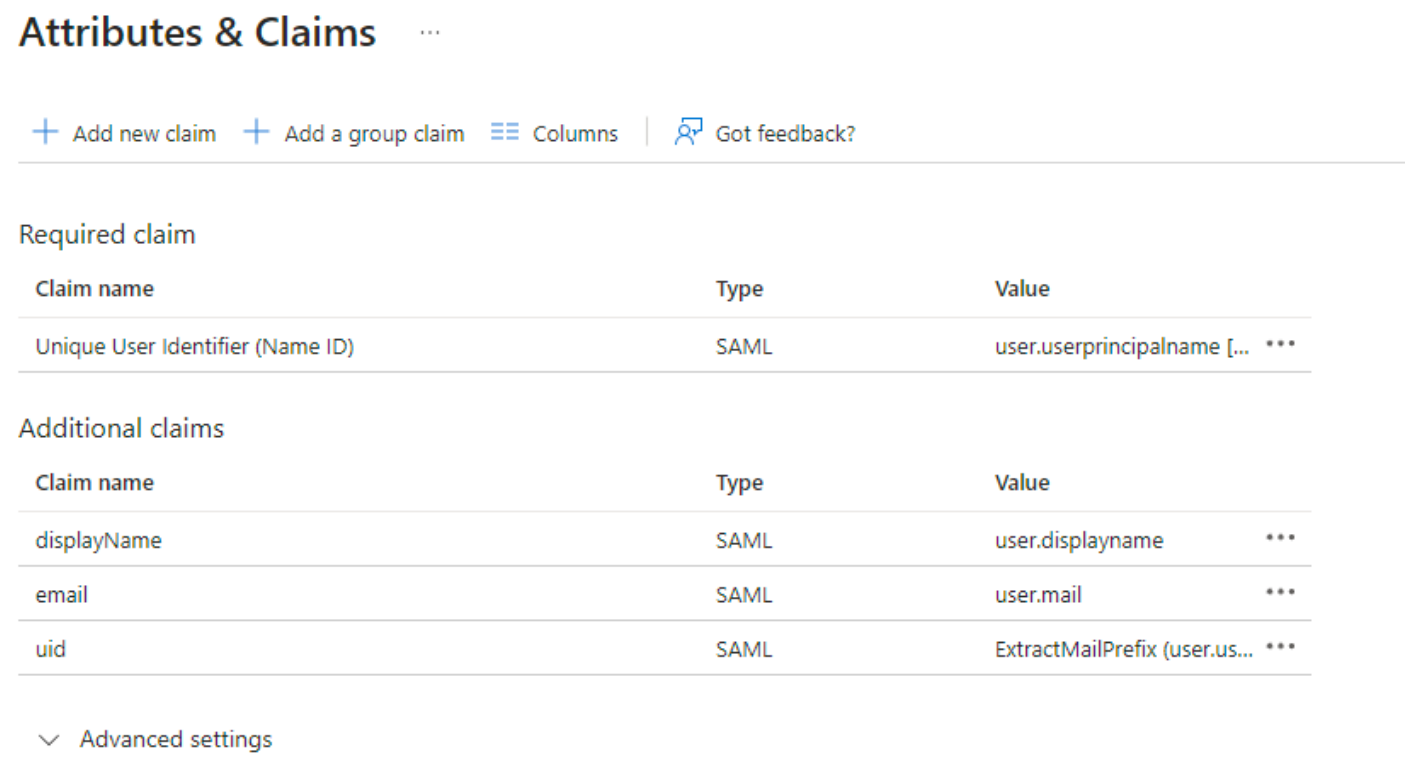
With an account with enough rights, go to : `Enterprise Applications`

- Click on `New Application`
- Click on `Create your own application` on the top left corner
- Choose a name for it, and select `Integrate any other application you don't find in the gallery`
- Click on "Create"
- Select `Set up single sign on`
- Select `SAML`
- `Edit` on `Basic SAML Configuration`
- In `Identifier` , add the following URL : `https://<synapse fqdn>/_synapse/client/saml2/metadata.xml`
- Remove the default URL
- In `Reply URL` , add the following URL : `https://<synapse fqdn>/_synapse/client/saml2/authn_response`
- Click on `Save`





- Make a note of the `App Federation Metadata Url` under `SAML Certificates` as this will be required in a later step.
- `Edit` on `Attributes & Claims`
- Remove all defaults for additional claims
- Click on `Add new claim` to add the following (suggested) claims (the UID will be used as the MXID):
  - Name: `uid` , Transformation : `ExtractMailPrefix` , Parameter 1 : `user.userprincipalname`
  - Name: `email` , Source attribute : `user.mail`
  - Name: `displayName` , Source attribute : `user.displayname`
- Click on `Save`

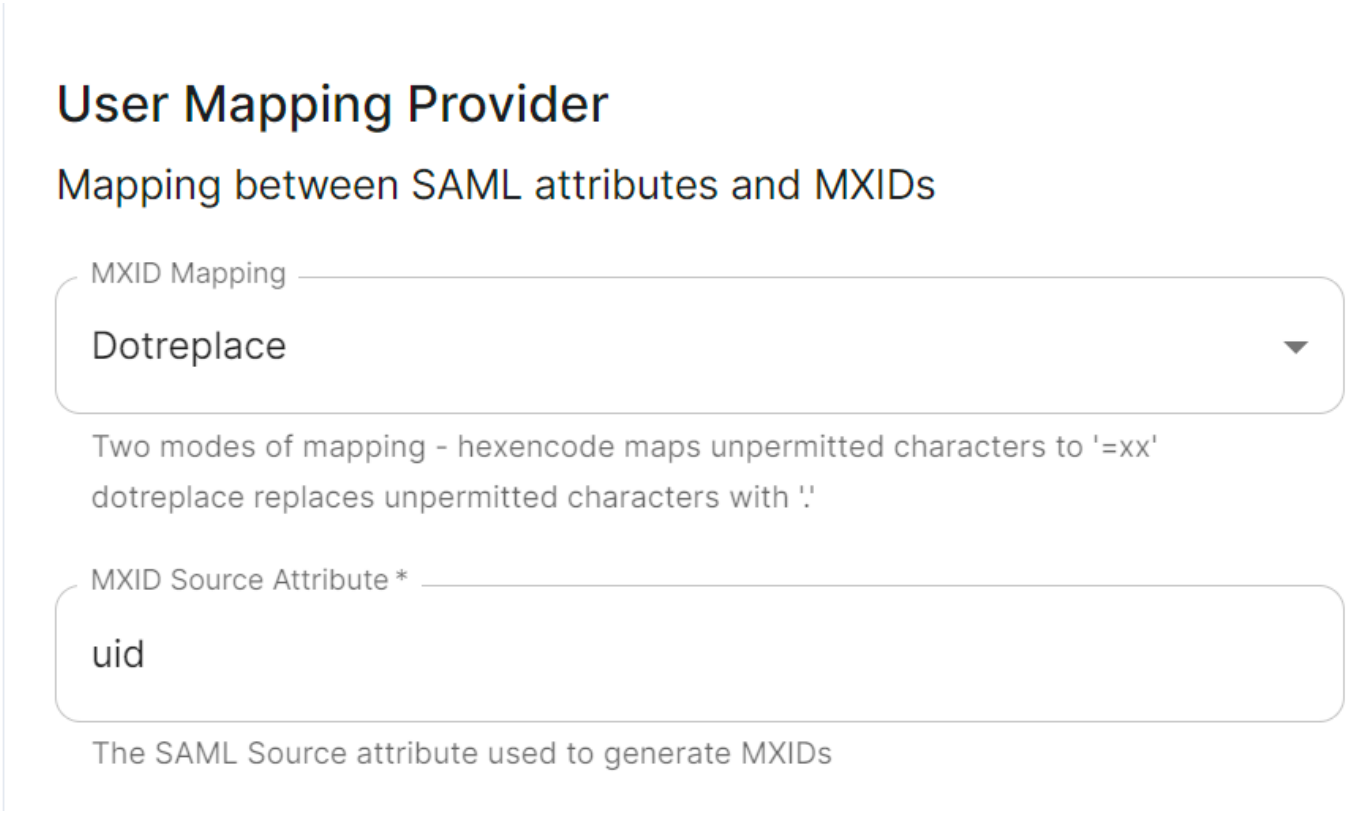


- In the application overview screen select `Users and Groups` and add groups and users which may have access to element

Configure the installer

Add a SAML provider in the 'Synapse' configuration after enabling `Delegated Auth` and set the following (suggested) fields in the installer:

- `Allow Unknown Attributes`
- Under `Attribute Map`, select the `Identifier` - `URN: Oasis: Names: TC: SAML: 2. 0: Attrname Format: Basic`



- Under `Mapping` add the following (suggested) mappings:
  - From: `Primary Email` To: `email`
  - From: `First Name` To: `firstname`
  - From: `Last Name` To: `lastname`

Attribute Map

Map from SAML Name-format attribute to attributes

Identifier

URN:Oasis:Names:TC:SAML:2.0:Attrname Format:Basic

The identifier is the name-format you expect to support

Mapping

From *

Primary Email

The SAML name-format to read

To *

email

The attribute to convert the saml name-format to

From *

First Name

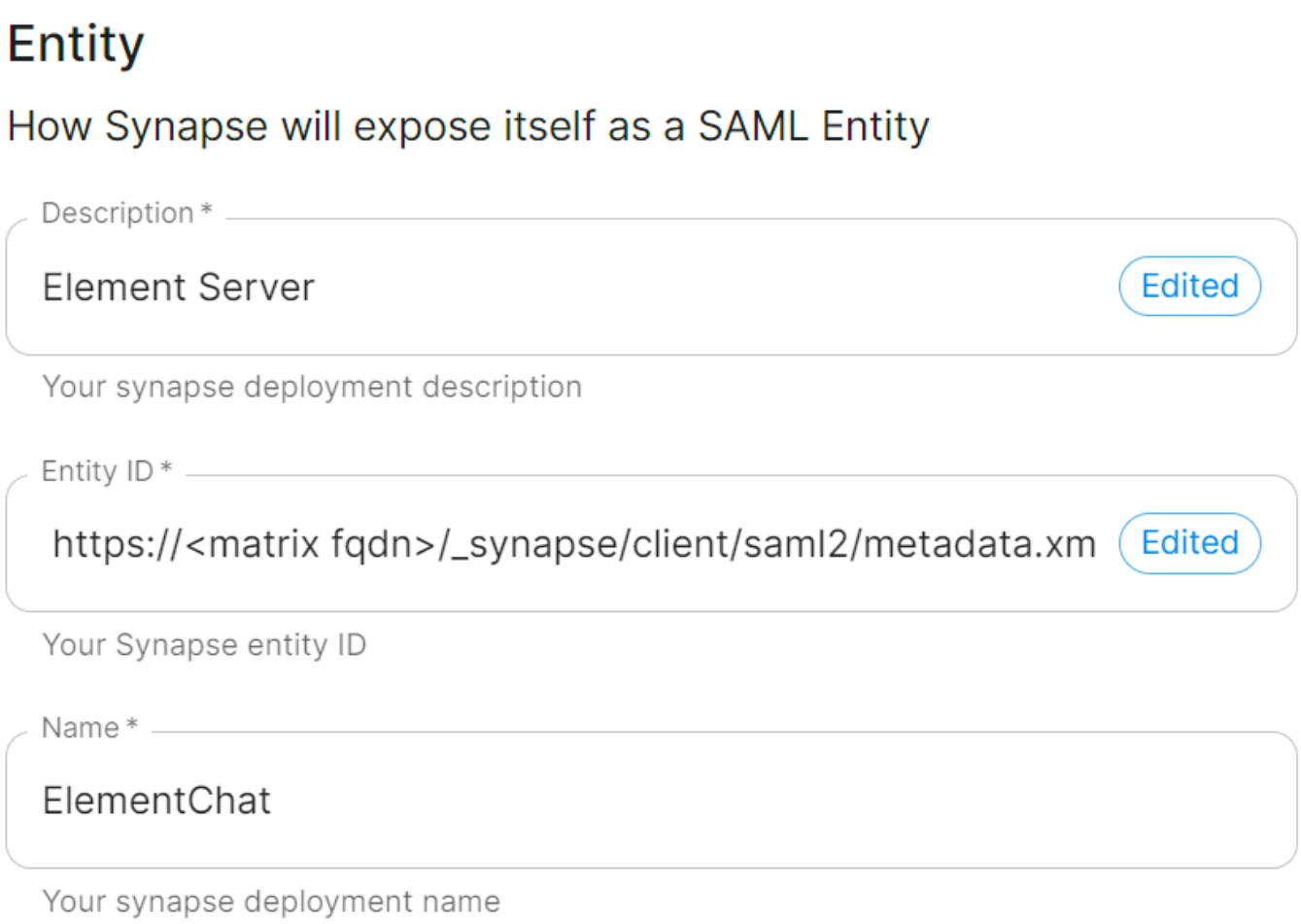
The SAML name-format to read

To *

firstname

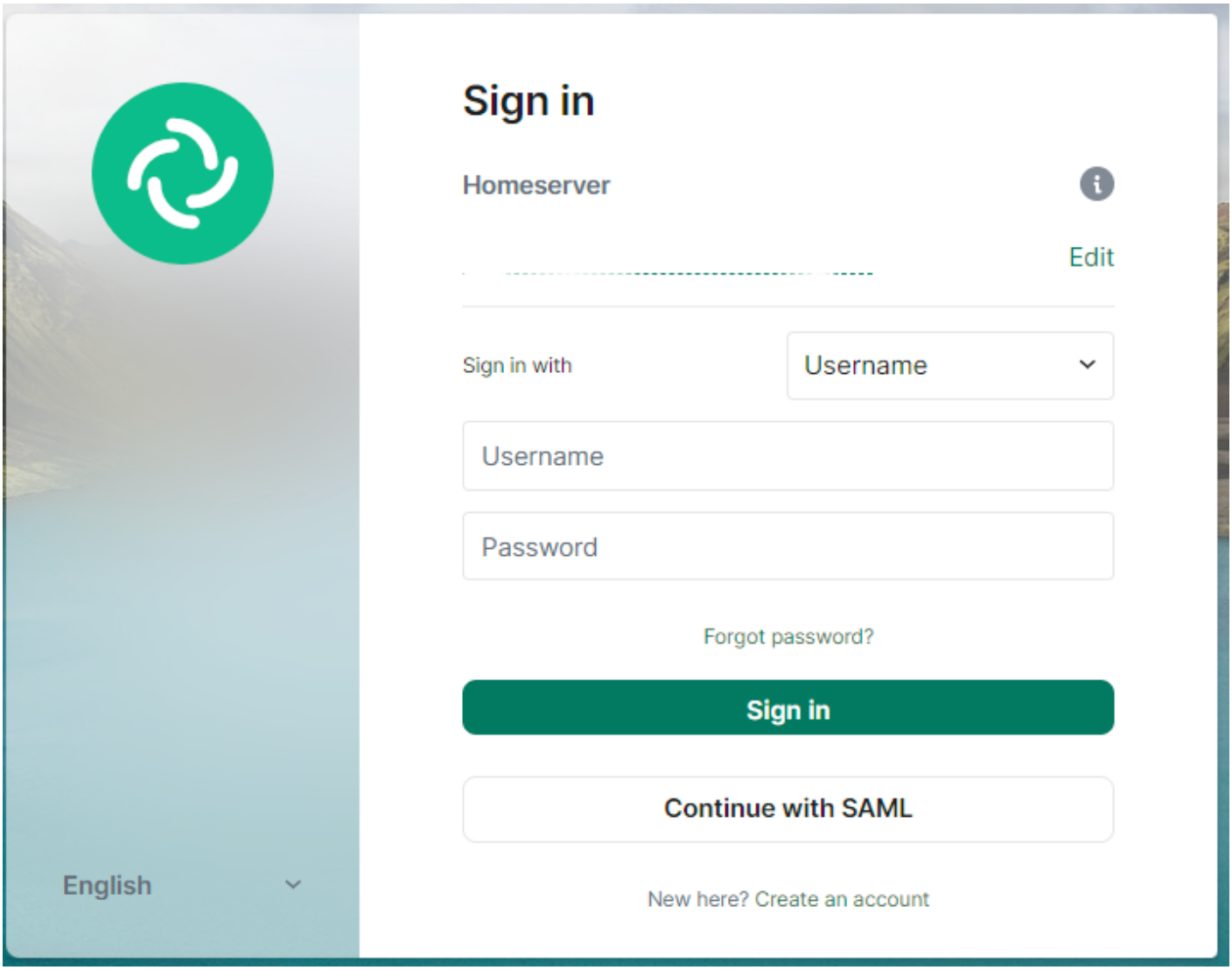
The attribute to convert the saml name-format to

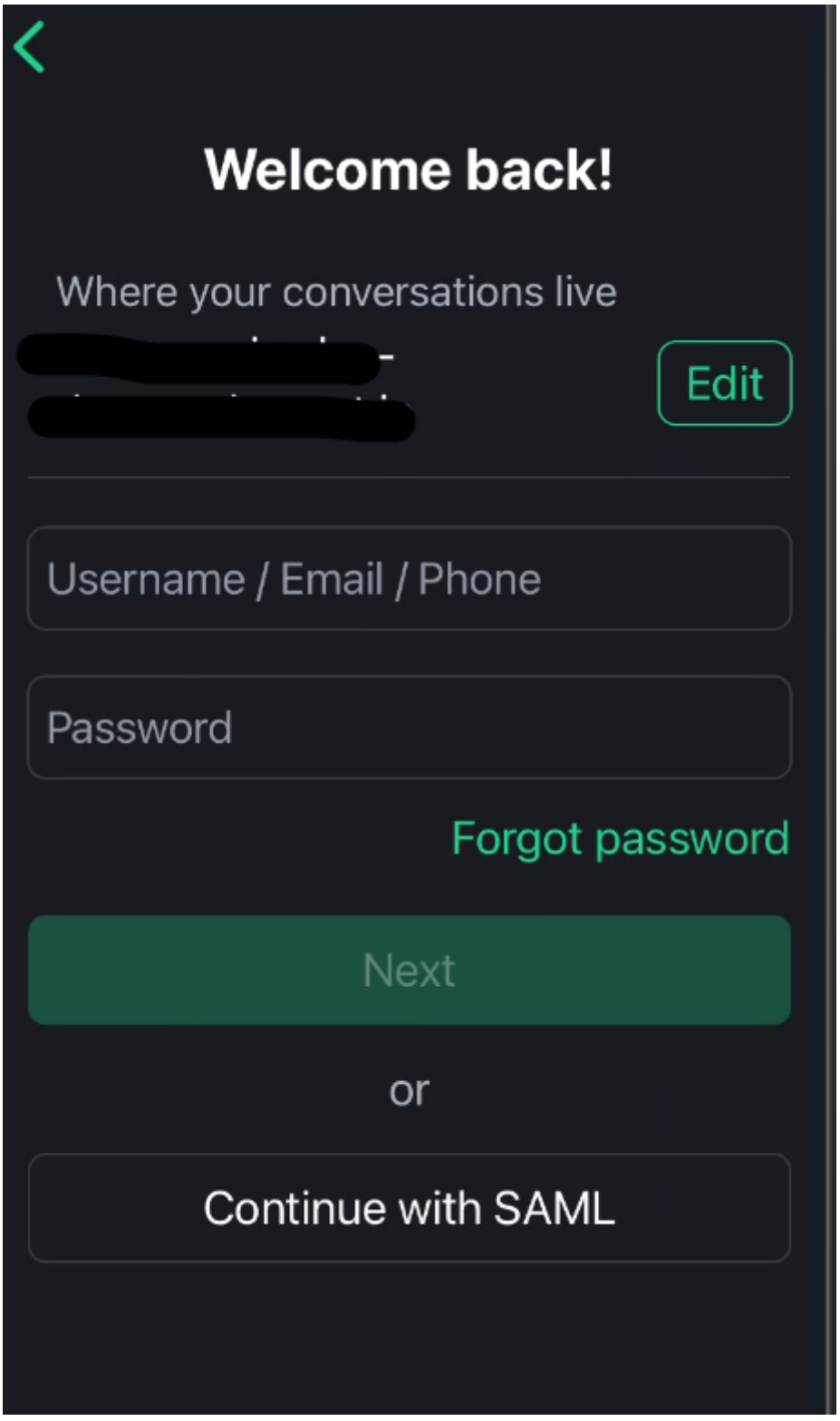
- Under `Entity`, enter a `description`, the `Entity ID` (from Azure) and a `name`.



- Under `User Mapping Provider` select the following:
  - `MXID Mapping`: `Dotreplace`
  - `MXID Source Attribute`: `uid`
- Under `Metadata URL`, add the `App Federation Metadata URL` from Azure.

When clients connect, along with any existing authentication methods still enabled, they should now also have an option to `Continue with SAML`:


Sign in
Homeserver
Edit
Sign in with
Username
Username
Password
Forgot password?
Sign in
Continue with SAML
English
New here? Create an account



Revision #30
Created 1 February 2023 10:37:05 by Simon Addis
Updated 8 May 2024 16:30:28 by Kieran Mitchell Lane