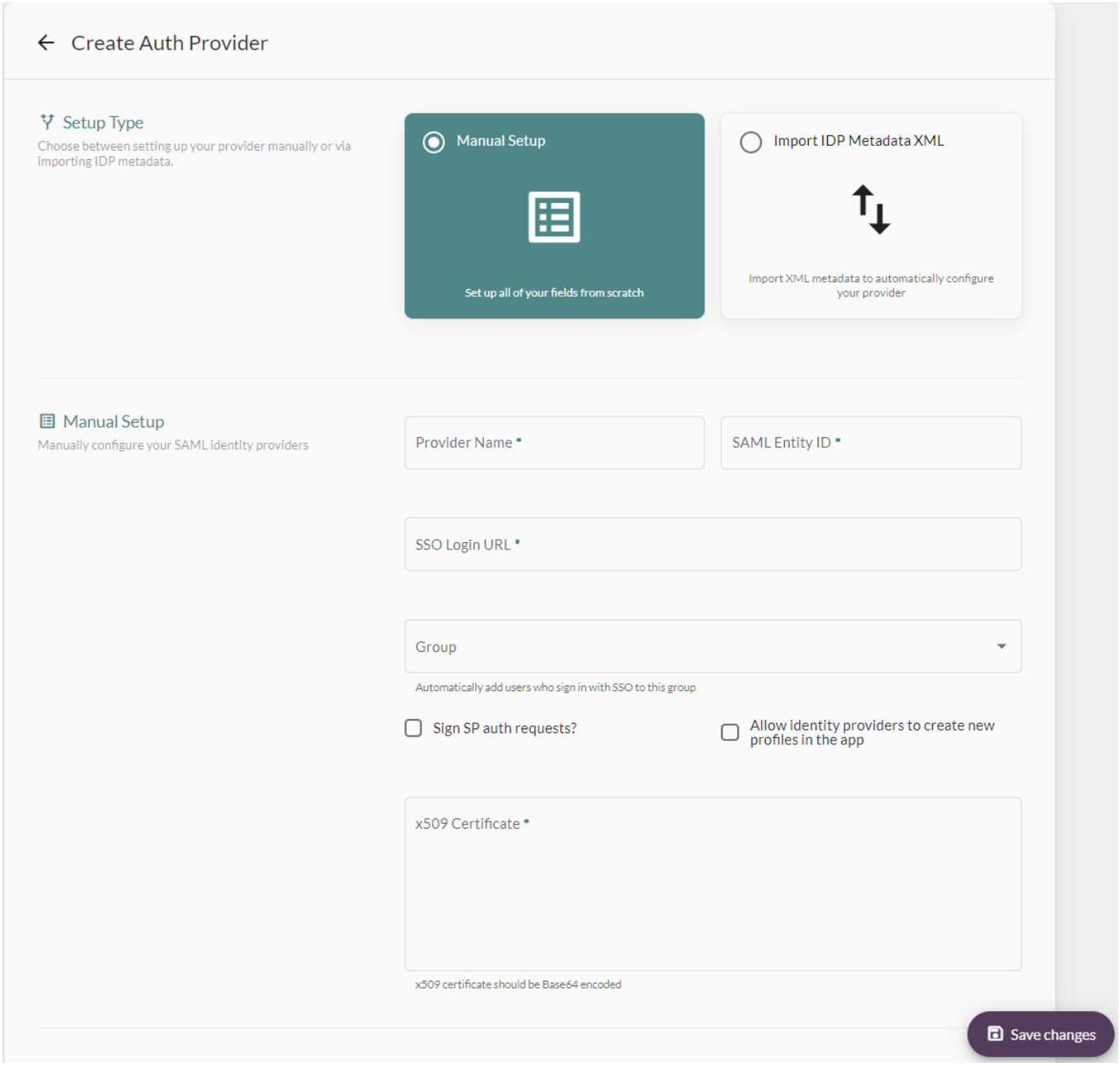
SAML2

How **does SSO work**? **SSO works** based upon a trust relationship set up between an application, known as the service provider, and an identity provider, like OneLogin. ... In **SSO**, this identity data takes the form of tokens that contain identifying bits of information about the user like a user's email address or a username.

How to set up saml2-compatible identity providers

Manual Set Up

- Log into CMS
- Select App
- Click on "Settings"
- Click on "Authentication" and then "Single Sign On"
- Click on "Add Provider"
- Check the "Manual Set Up" option
- Fill in; "Provider Name"
- Copy the "Issuer URL" into the "SAML Entity I.D" in CMS
- Copy the "SAML2 Endpoint" into the "SSO Login URL" field in CMS
- Copy the "Certificate" into the required field in CMS
- Fill in the "Unique ID" field in CMS under field mapping
- Click "Save changes" in CMS



Import IDP Metadata XML

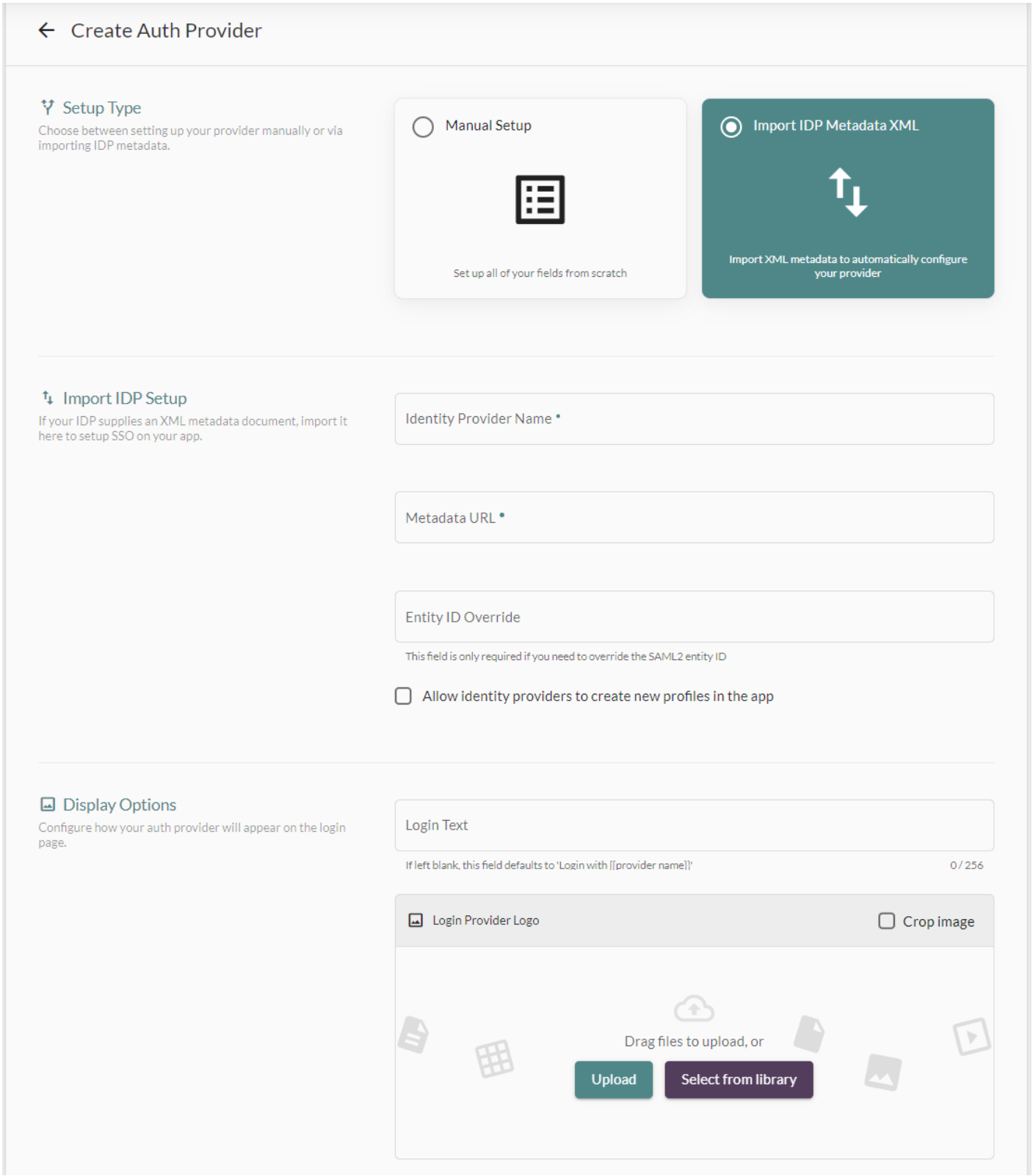
Required details:

- Entity ID: https://saml.crowdcomms.com
- Reply URL: https://api.crowdcomms.com/complete/saml/ Note: this needs to be summit-api for apps using the Summit enviroment, and dlt-api for apps using the Deloitte environment. Deloitte apps using the main environment should still use just api.

Using the above you should be able to import your metadata with the following steps:

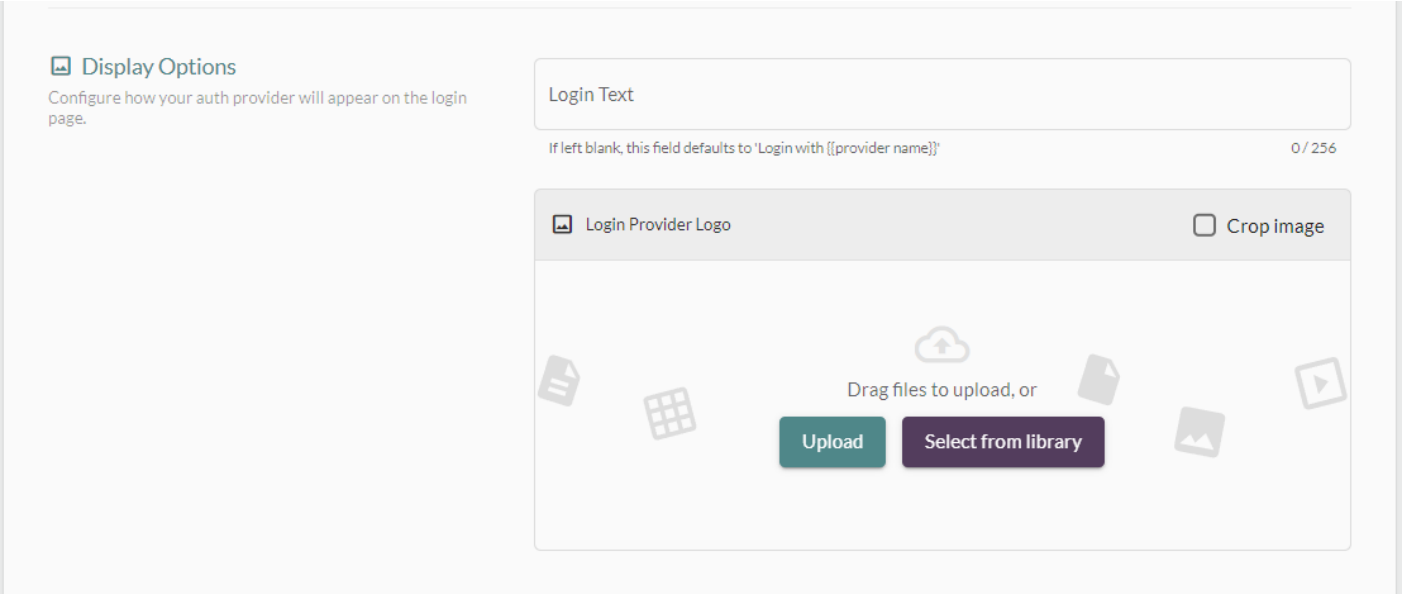
- Fill in; "Provider Name"
- Return to IDP and copy the Metadata URL

- Copy the link into the CMS field "Metadata URL"
- Insert a name into the "Unique User I.D" field (for example; NameId) - this is based on the field mapping the client sets up. They will map their Active Directory fields to potentially something shorter, eg their ID field could be mapped to 'uniqueid', and so instead of filling in NameId here, you'd fill in uniqueid
- Click Save in CMS
- Copy the "Relay State URL" into the Configuration TAB
- Copy the "Audience" into the Configuration TAB
- Copy the "Recipient" into the Configuration TAB



Branding the Login Page with SSO

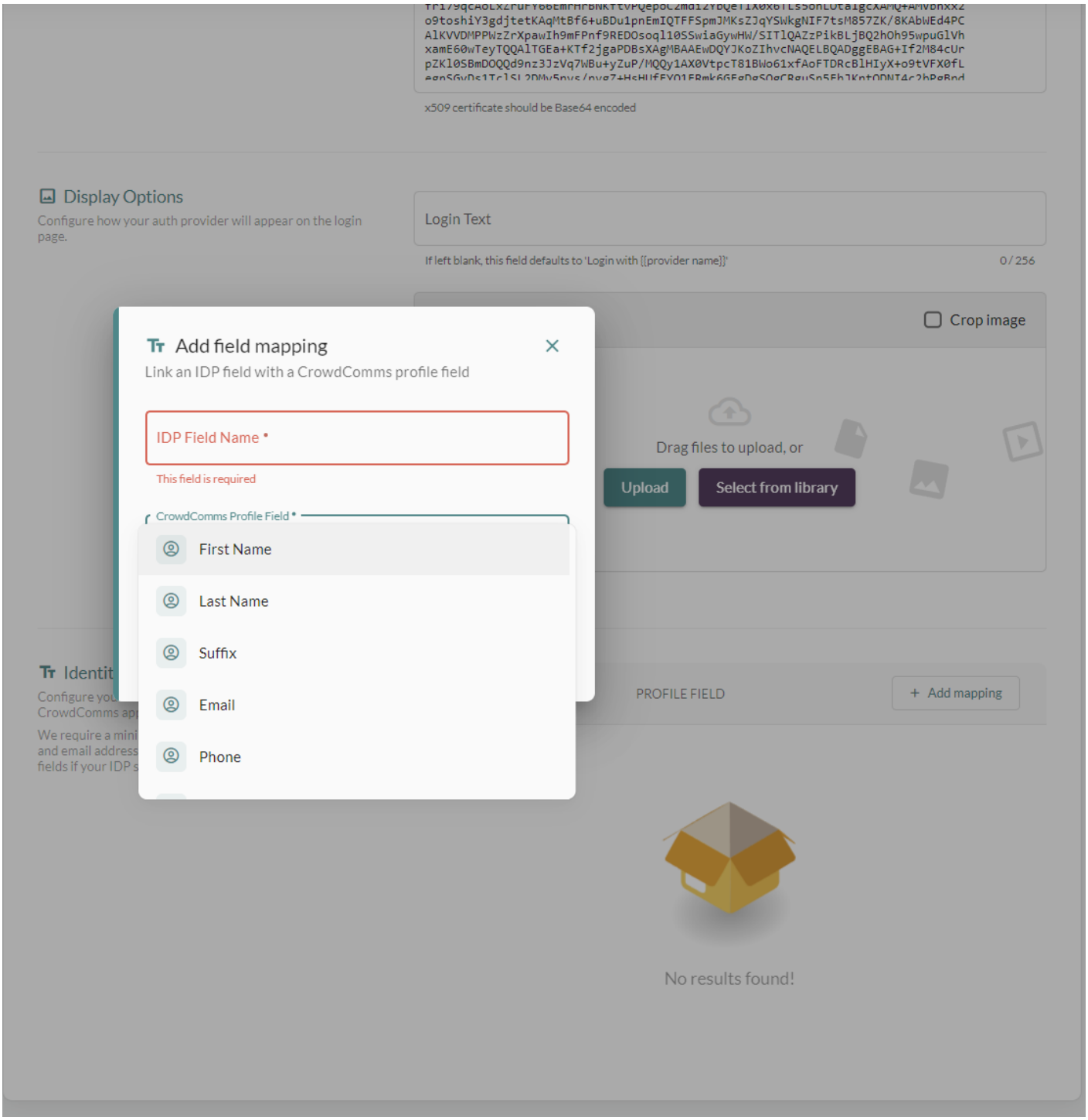
The Front End Login page can be branded with unique text and/or with a logo in the "Display Options" section of the "Edit Auth Provider" page



- Upload the image you wish to add to the login page
- Type the text you would like to appear (For Example... "Please log in")
- Click Save

Field Mapping

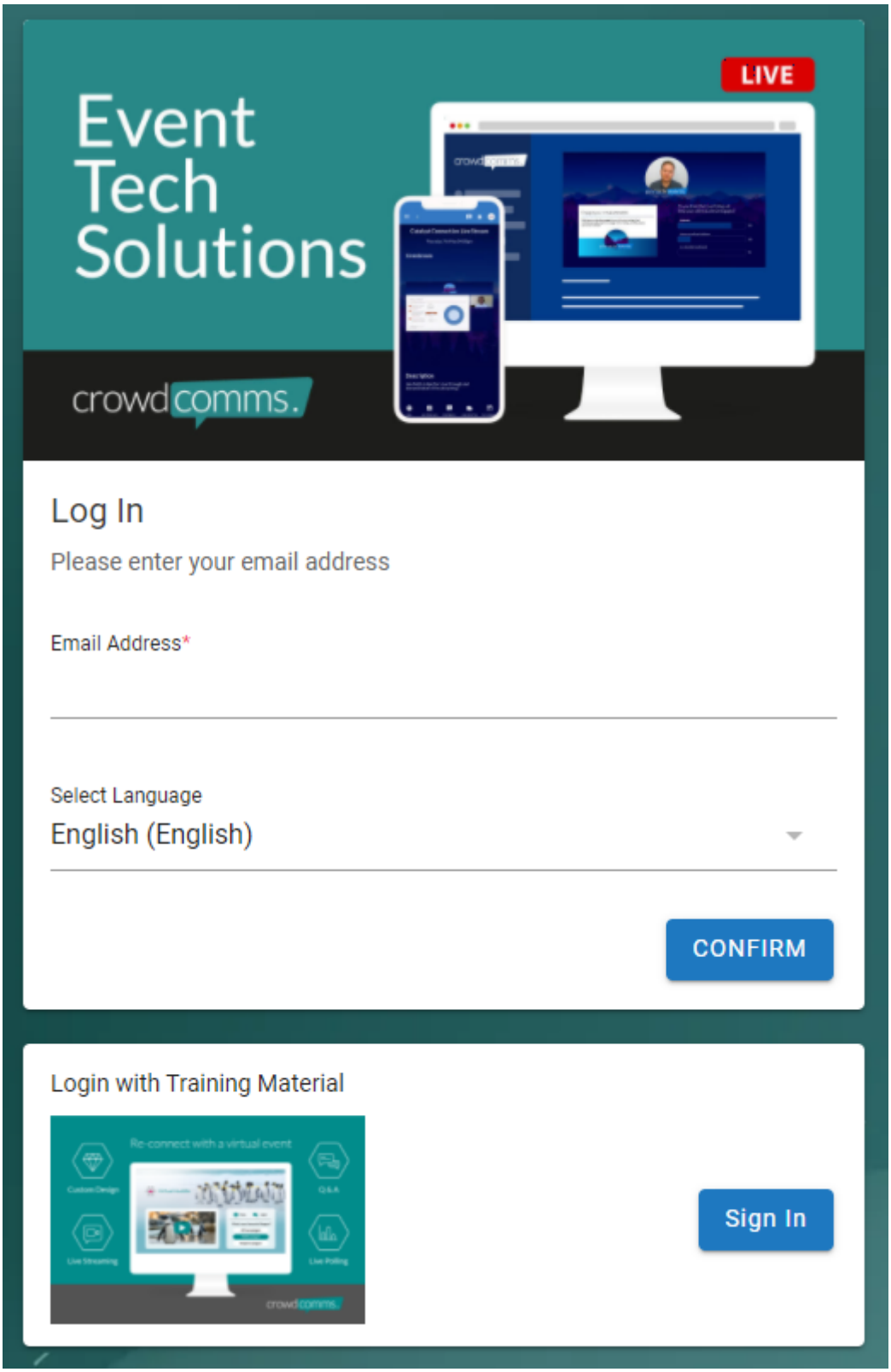
- Click on "Edit Provider" to edit the SSO you set up in the previous step
- Scroll down and click on "Add Mapping"



- Enter each field mapping and click "Save". Again these are based on the field mappings the client sets up. We take the output of their mapping, and map it to a profile field in our own system
- Click Save

Logging into Front End

- Open up Front End of App



- Click on "Sign In"
- Enter your credentials
- At this point, if any more User information is required then a screen will appear for the user to fill them in (for example; first name), otherwise, you will receive a "Success Screen" before FE loads up
- As this is the first time the User will of logged in, they will receive the company privacy message to accept or decline
- The user is now logged into the App

Revision #10
Created 30 April 2021 09:21:38
Updated 20 February 2024 16:20:29 by James