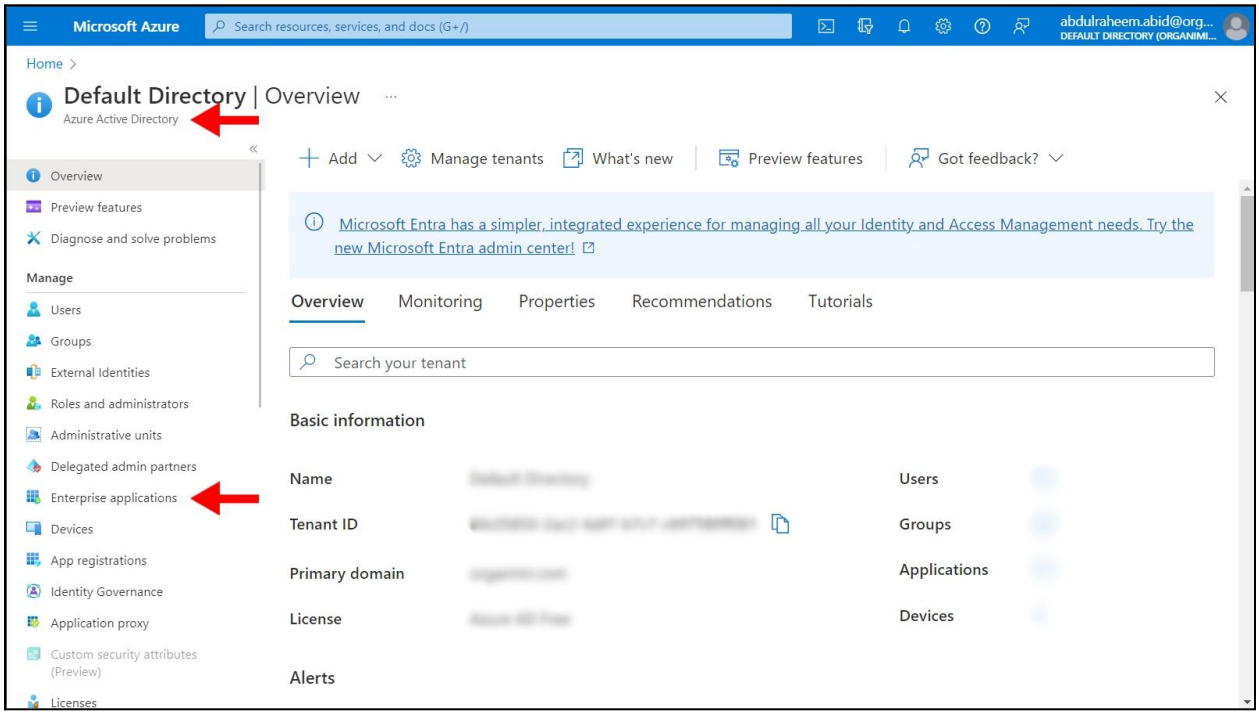
SAML based SSO - Login with MS Azure AD

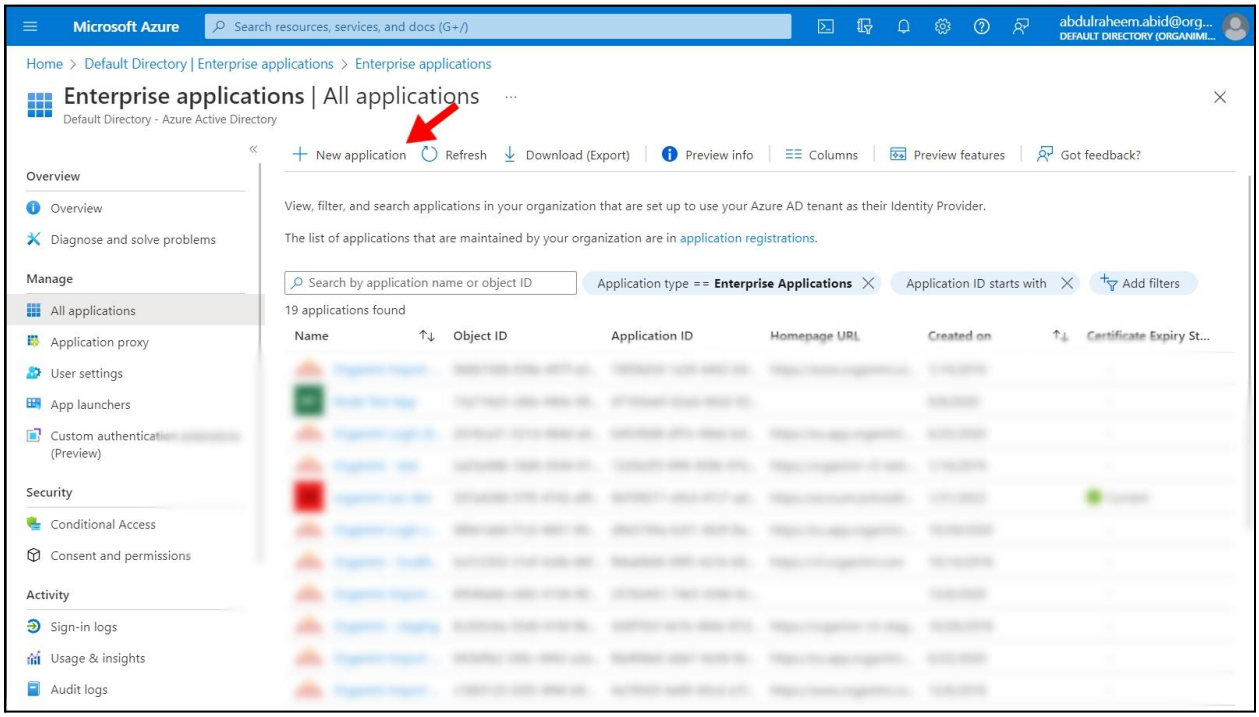
Organimi has implemented SAML based SSO for Premium account holders … this document will walk you through the steps to set up the integration with Microsoft Azure Active Directory

Step 1

Go to your Azure AD default directory and click “Enterprise Applications”



Then click on “Create New Application”

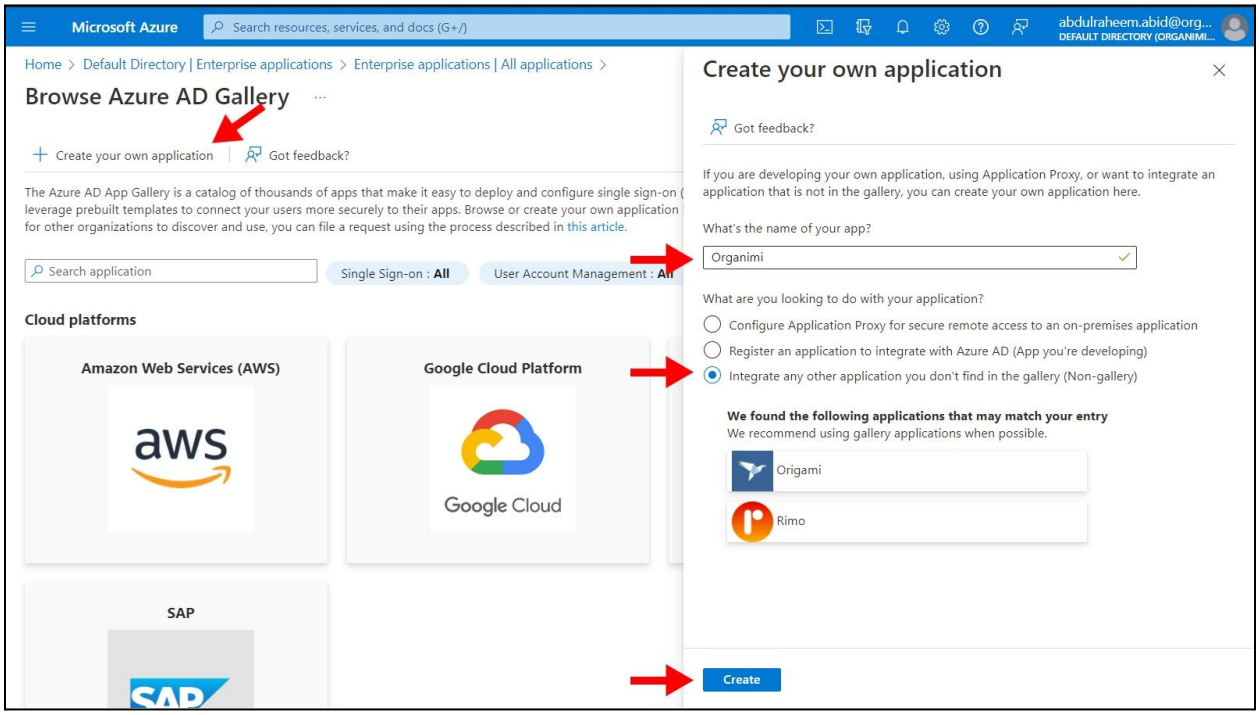


Step 2

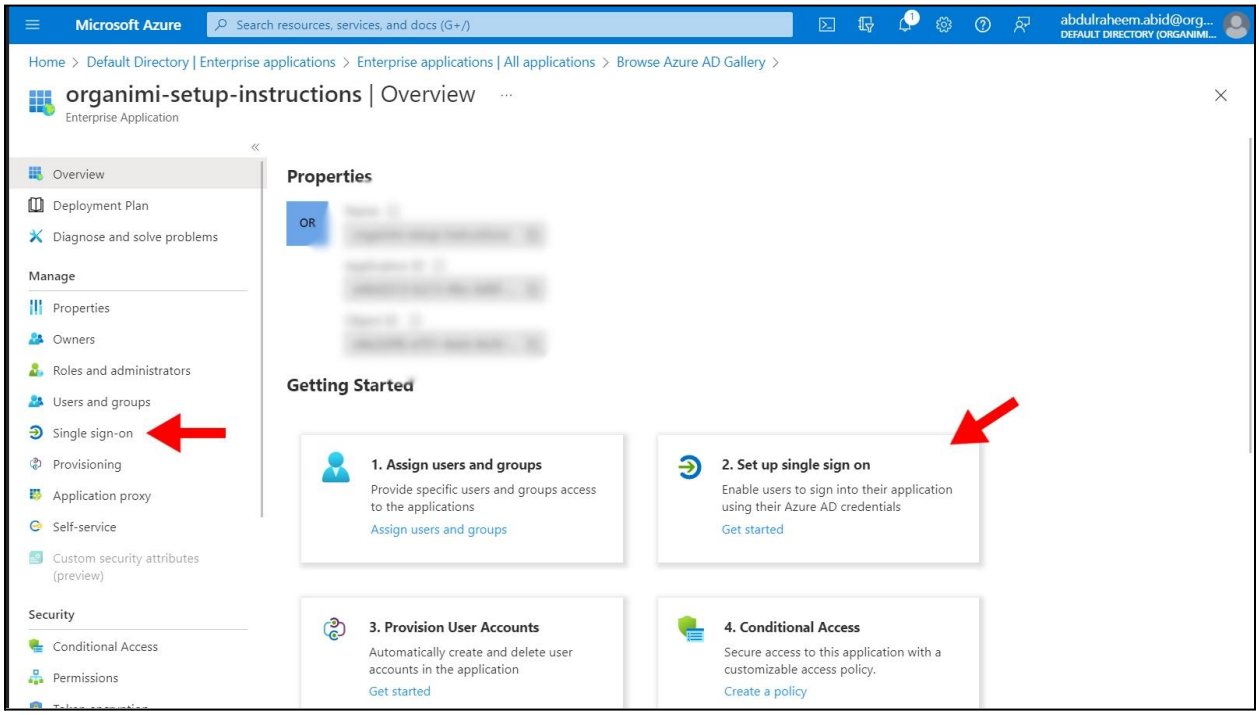
Then click on “Create your own application” and enter “Organimi” as the name of the APP

Select the radio button that says “Integration any other application you don’t find in the gallery (Non-gallery)”

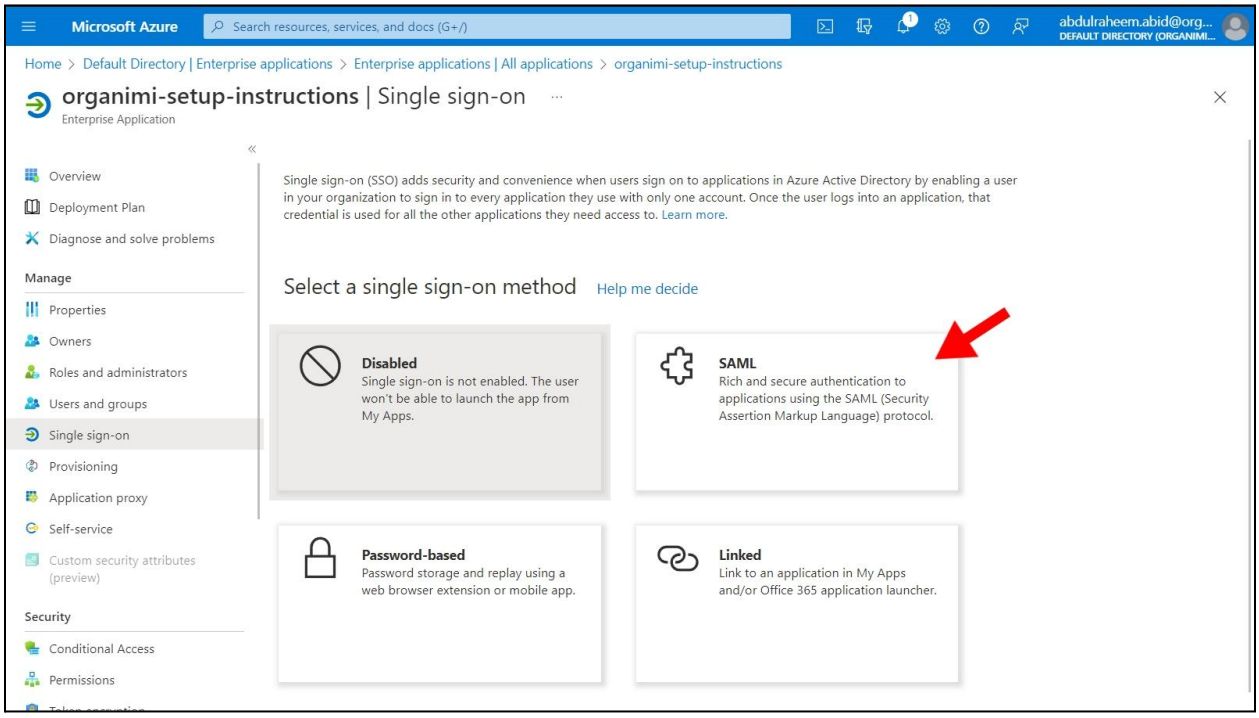
Click the “Create” button



Now select “Single sign-on” and click on the big button area for item “2. Set up single sign on”

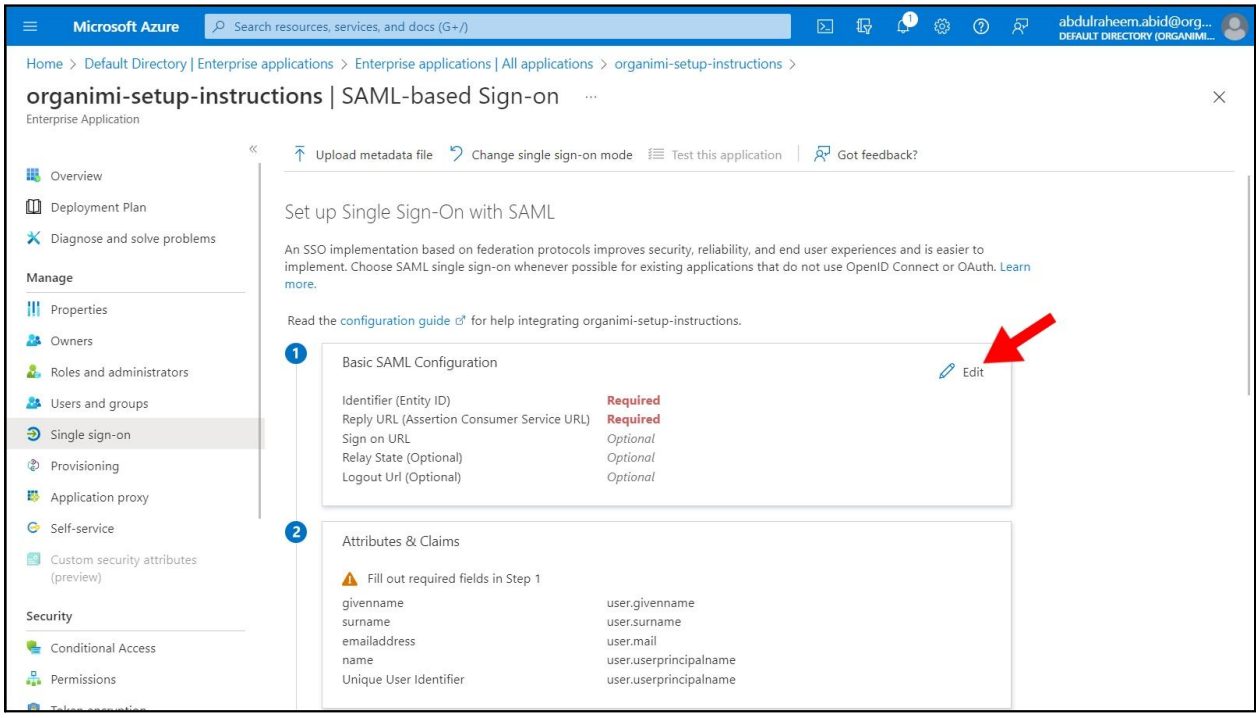


On the Single sign-on page chose the big button for SAML



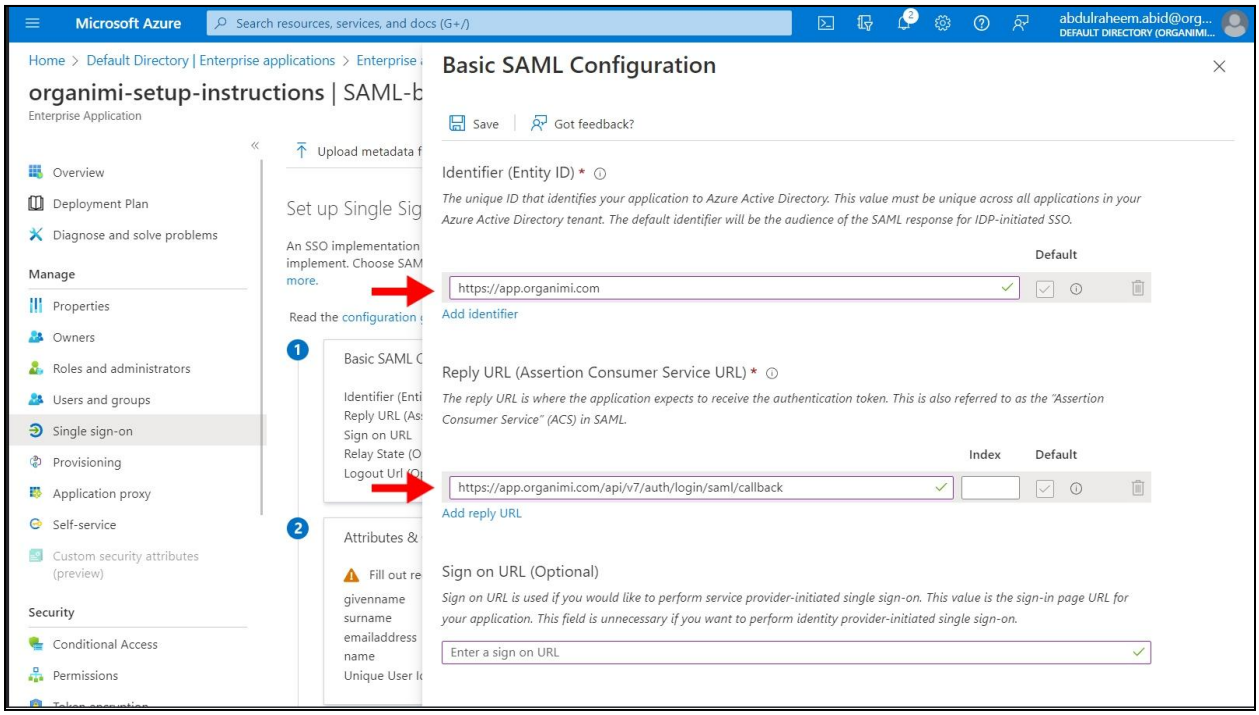
Step 3

On the SAML-based Sign-on page click on the “Edit” button for item 1 the Basic SAML Configuration.



In the Basic SAML Configuration popup set the value for the “Identifier (Entity ID) to be “*https://app.organimi.com*”

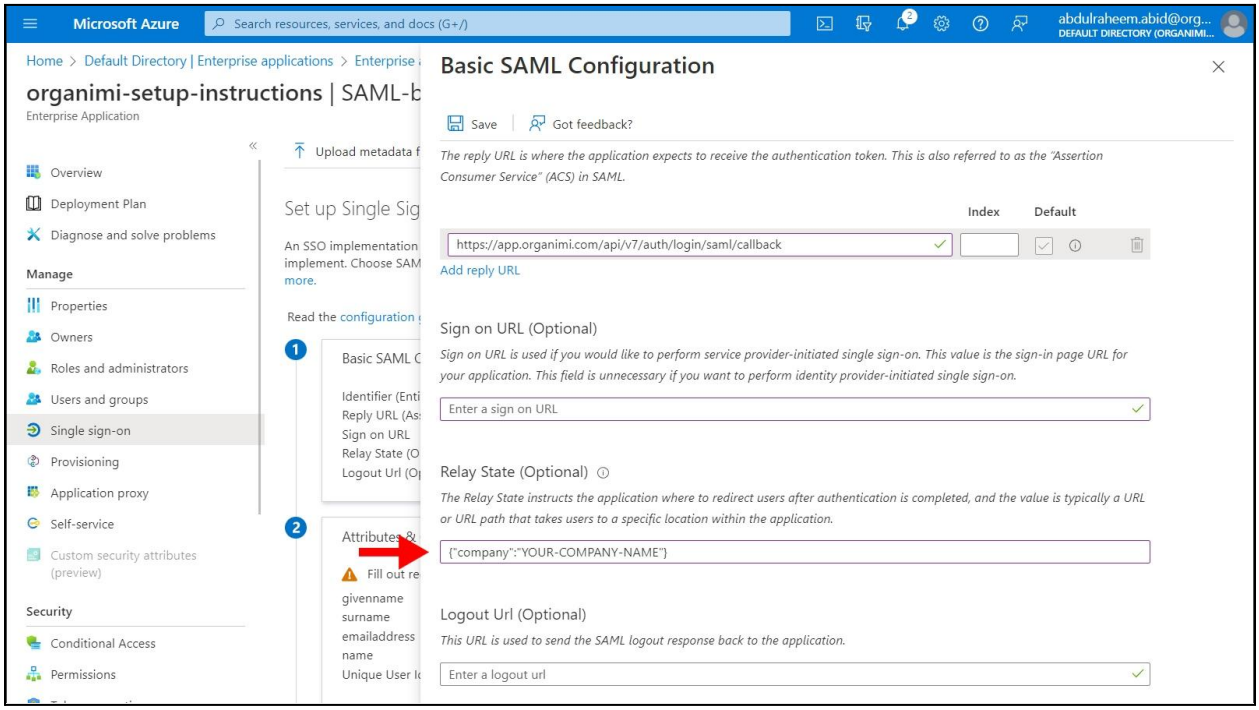
And set the value for the “Reply URL (Assertion Consumer Service URL)” to be “*https://app.organimi.com/api/v7/auth/login/saml/callback*”



Scroll down the pop-up window and set the “Relay State” value to be a small JSON object that is in the format of:

```
{"company":"YOUR-COMPANY-ALIAS"}
```

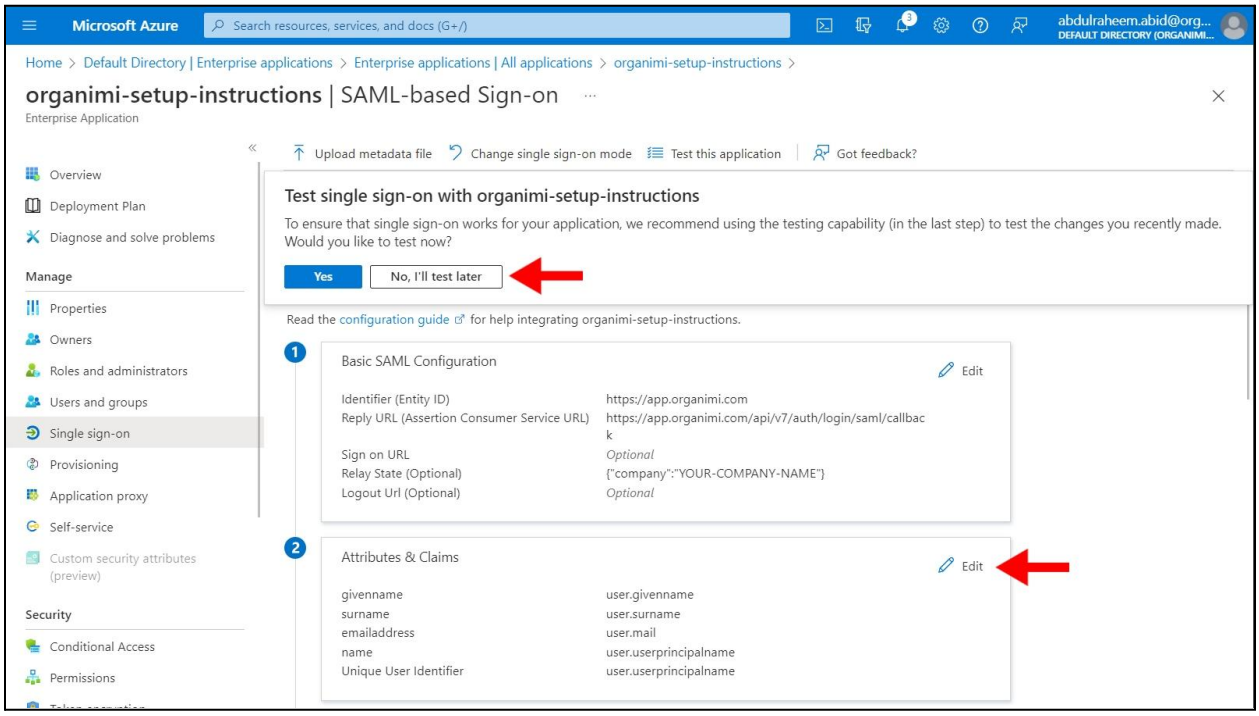
Where you replace the placeholder with your company name. This name will also be required later when setting up on the Organimi side and asked for the company-alias. And anyone who wishes to login using this IDP, will be asked to enter this name when signing in from the Organimi login page.



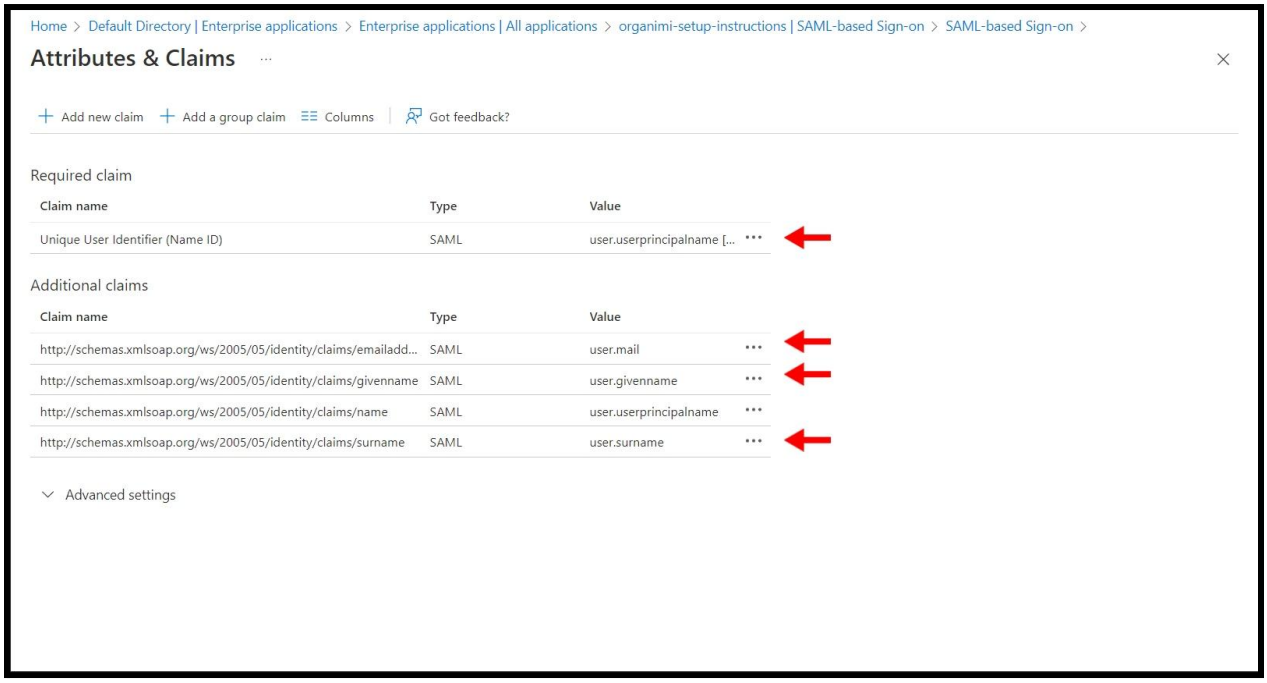
Click Save on the Pop-up and then “No I’ll test later” when prompted

Step 4

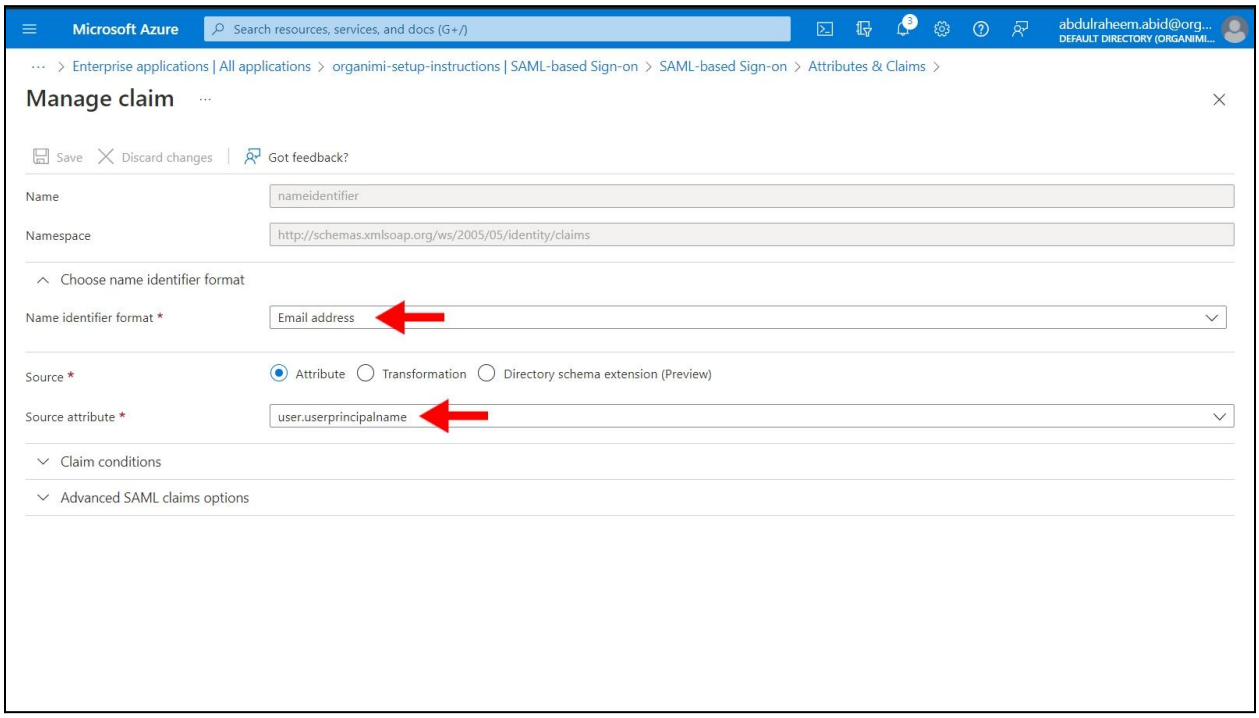
In part 2 of the setup “Attributes & Claims”, click on the edit button.



In the “Attributes & Claims” window we will set up 4 claims, one Required claim for the Unique Identifier and 3 Additional claims for the attributes used to match over to the Organimi system for the User’s details.

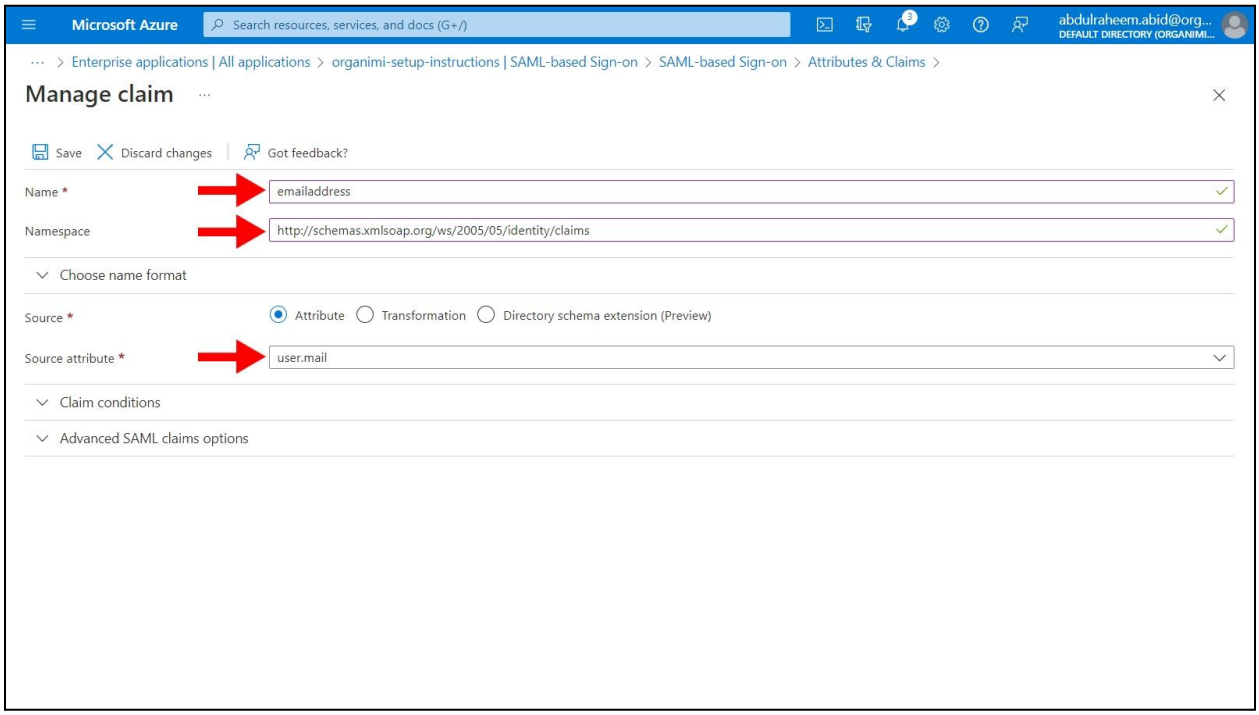


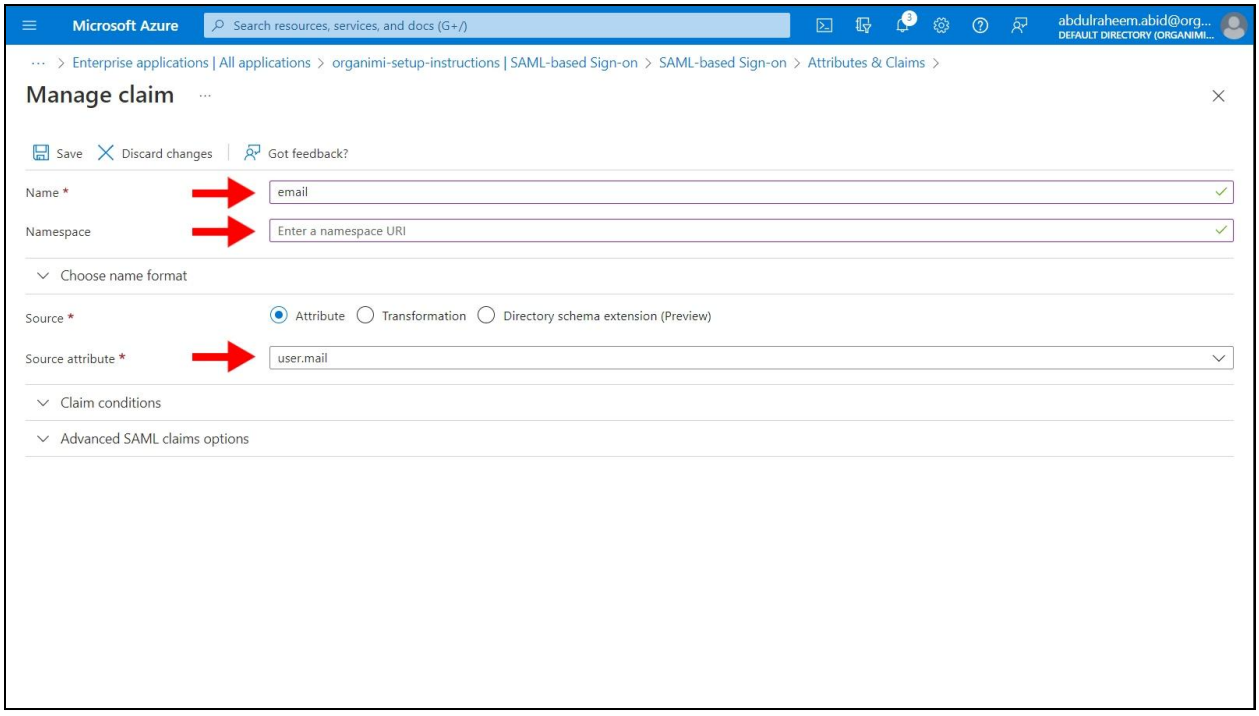
For the Unique User Identifier Required Claim (the first one), we need to make sure it's set to Email Address. This is typically the "*user.userpricipalname*" in Azure AD but may be different depending on how your Azure AD is set up.



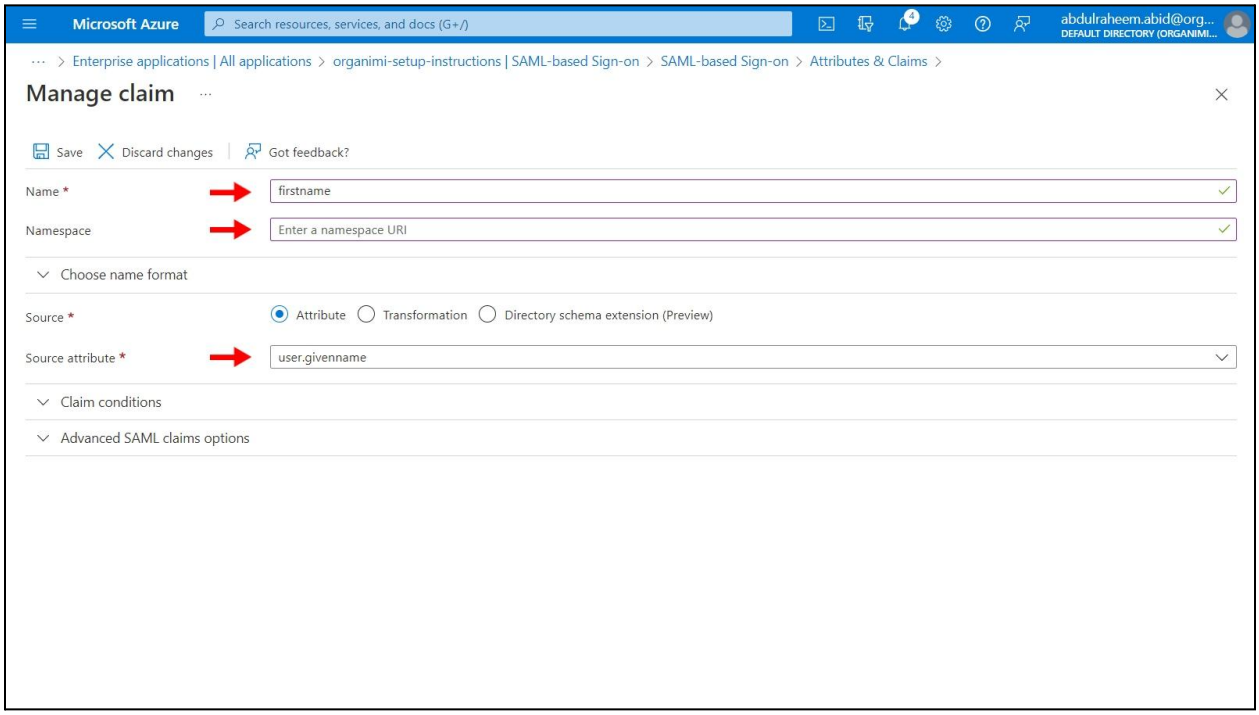
For the 3 Additional claims we will set up with email, firstname & lastname.

For the first one change the name from “emailaddress” to be just “email” all lower case and should map to the Source attribute of *user.email*. Make sure to delete the Namespace default value as the Namespace should be empty.

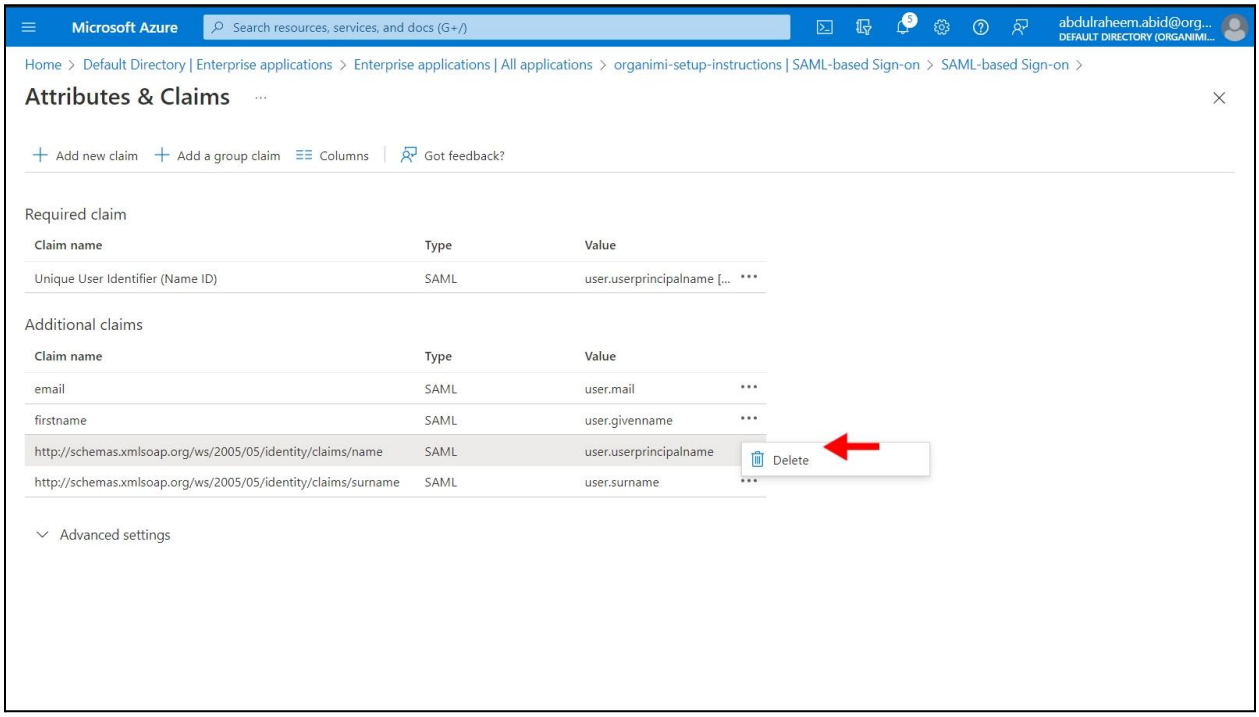




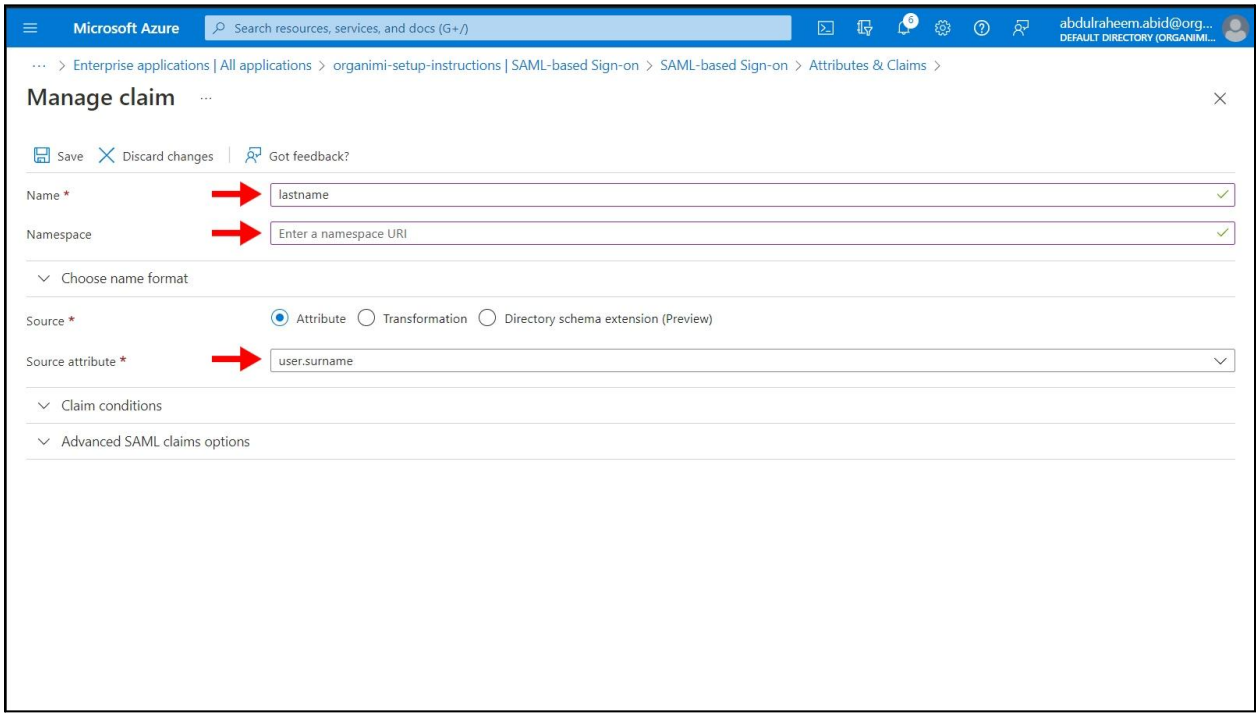
For the second Additional Claim set the Name to be “firstname” all lower case, remove the Namespace value so that is empty and then set the source attribute to be “*user.givenname*”



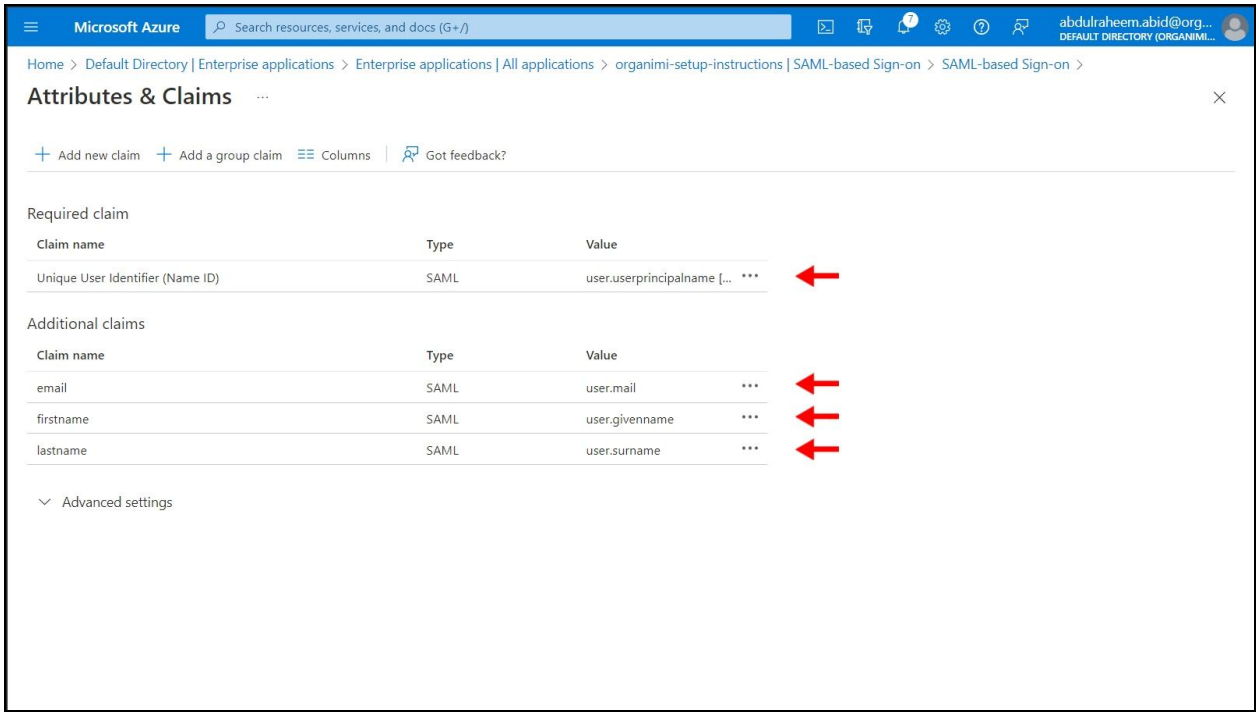
There is a default Additional claim usually for “*user.userpricipalname*” but we can delete this one as it is not used.



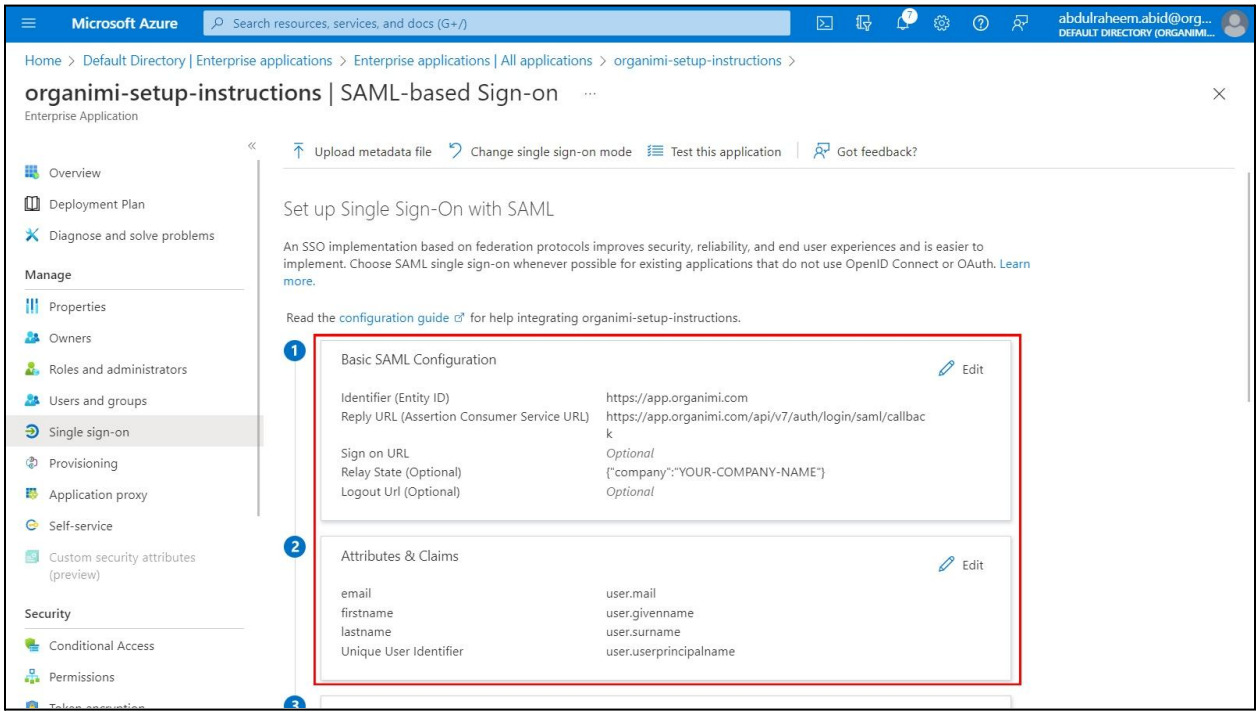
The final Additional claim is of the last name … set the Name to be “lastname” all lower case, remove the Namespace value so that is empty and then set the source attribute to be “*user.surname*”



It should look like this once all claims are mapped.

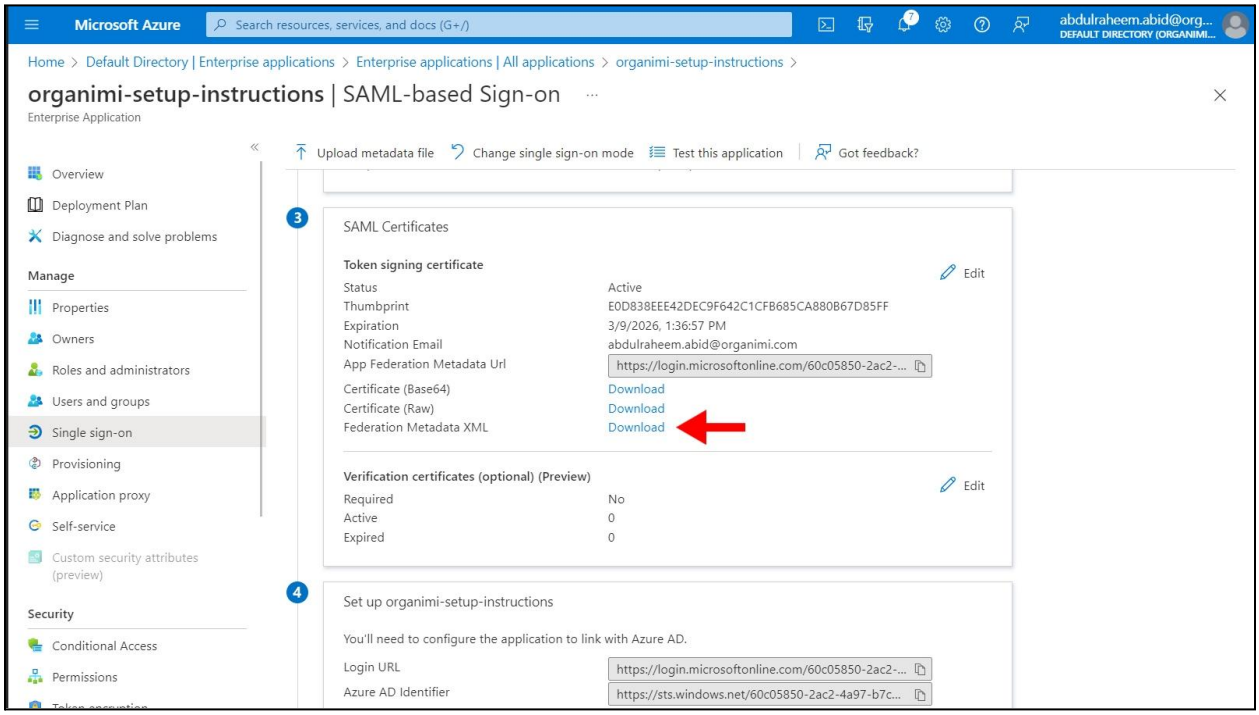

Microsoft Azure
Search resources, services, and docs (G+/)
abdulraheem.abid@org...
DEFAULT DIRECTORY (ORGANIMI...
Home > Default Directory | Enterprise applications > Enterprise applications | All applications > organimi-setup-instructions | SAML-based Sign-on > SAML-based Sign-on >
Attributes & Claims
Add new claim
Add a group claim
Columns
Got feedback?
Required claim
Claim name
Type
Value
Unique User Identifier (Name ID)
SAML
user.userprincipalname [...
Additional claims
Claim name
Type
Value
email
SAML
user.mail
firstname
SAML
user.givenname
lastname
SAML
user.surname
Advanced settings

With these sections completed it should look something like this.



Step 5

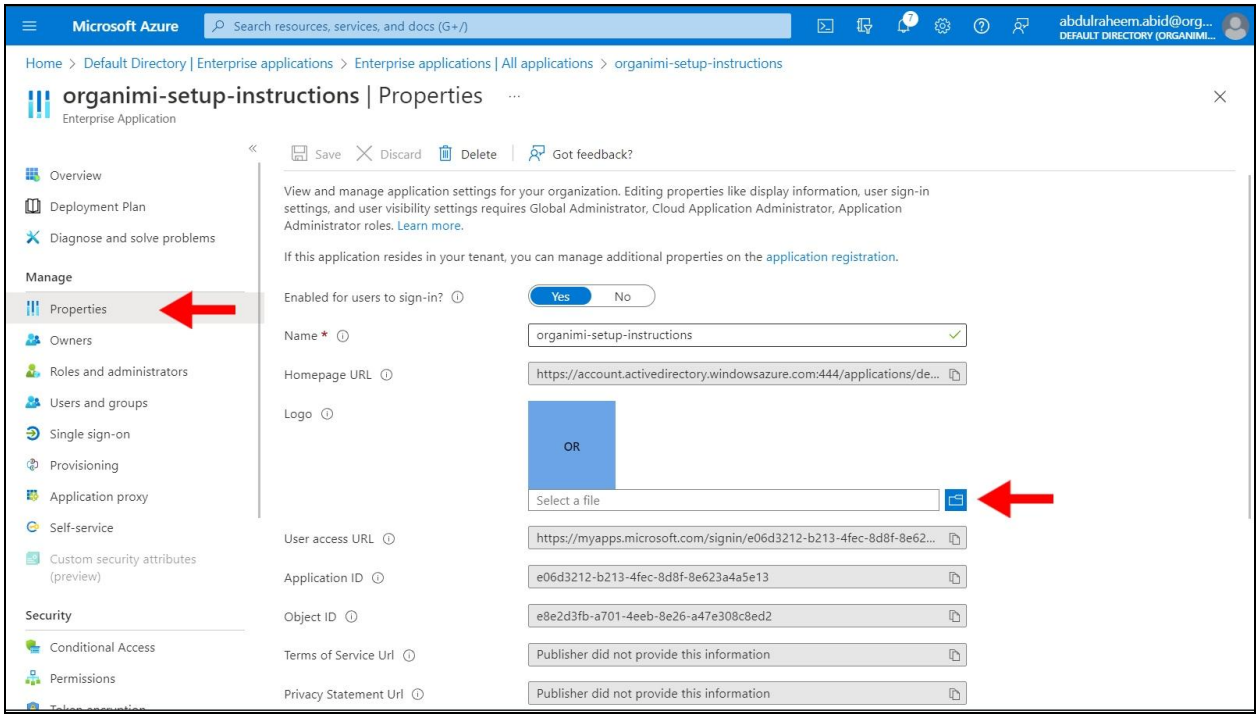
With the configuration completed you will want to download and save the “Federation Metadata XML”. This is an XML file and will be needed to configure the setup on the Organimi side.



Step 6

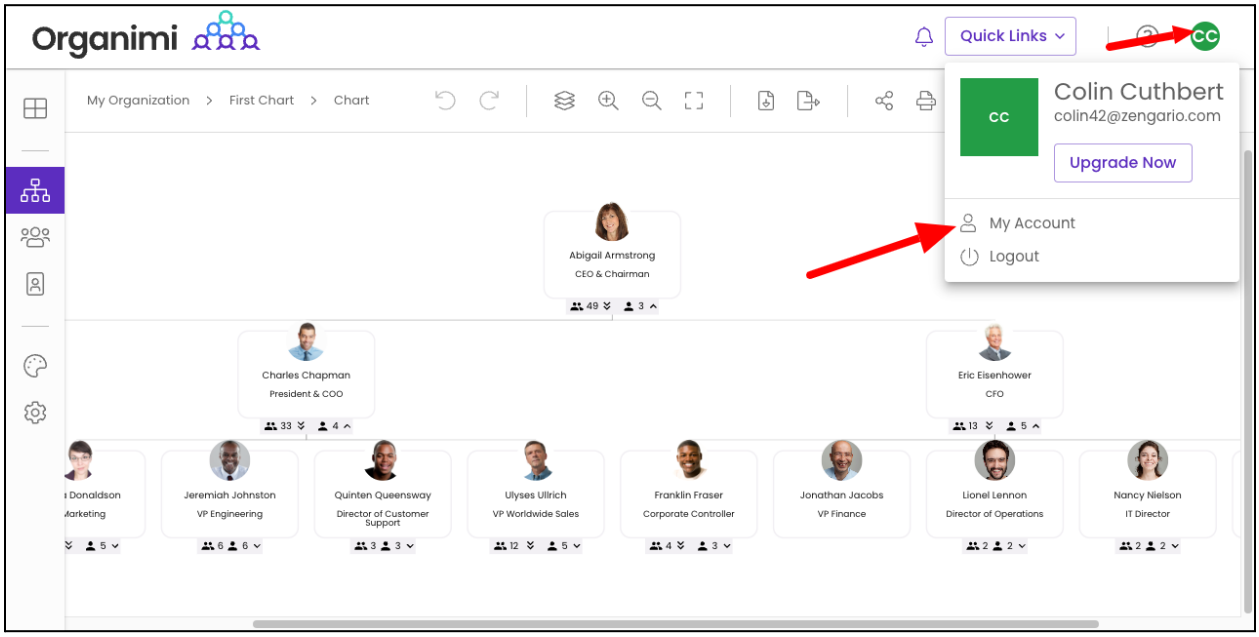
You can set up the Organimi logo on the “Properties” page. A suitably sized Organimi logo is available for easy download at:

https://drive.google.com/file/d/1lW90r60-mUPM-MRt6qDySBJs774knBaE/view



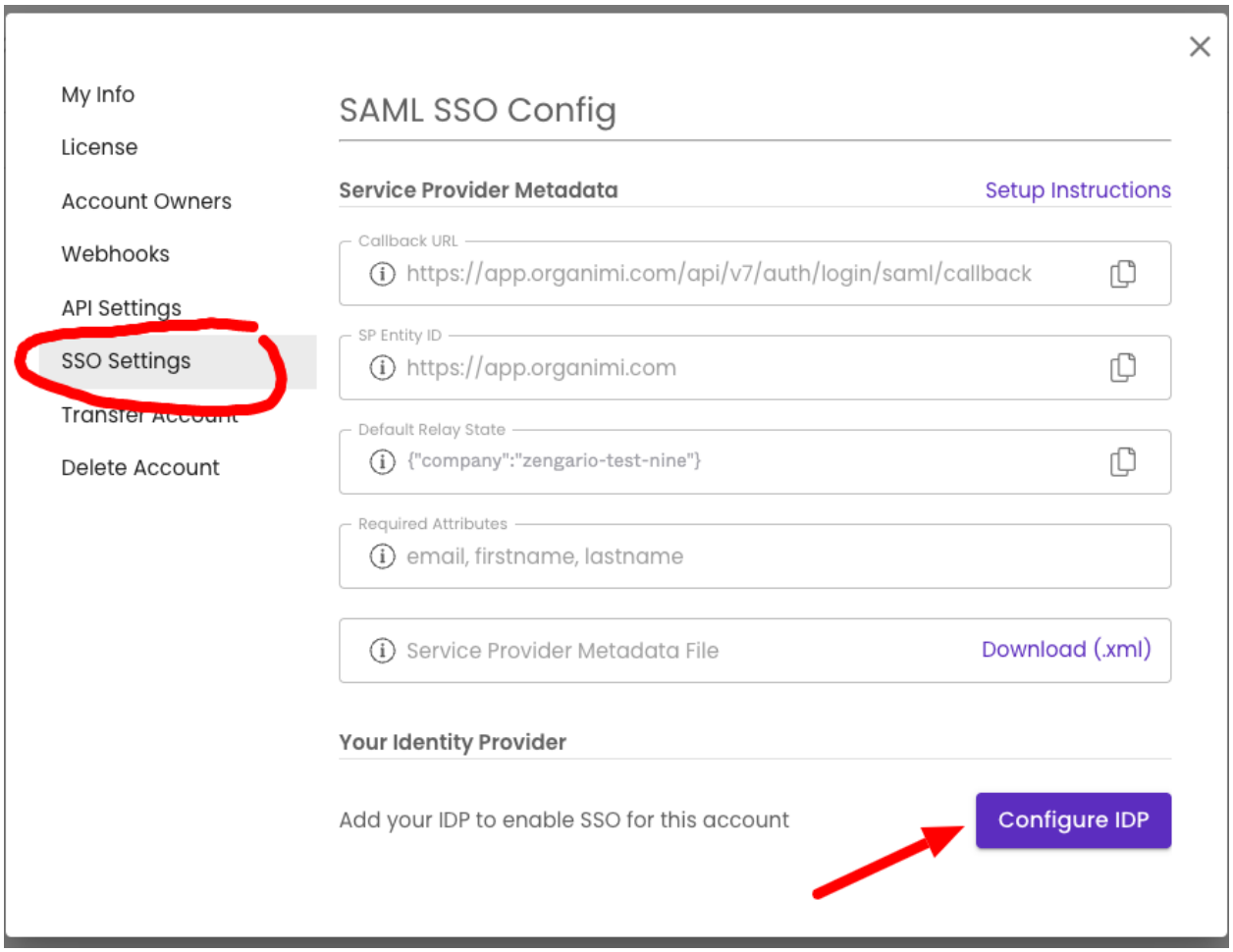
Step 7

Now over to the Organimi side of the set up … visit https://app.organimi.com, login to your account using any social login, or username/password. Click “My Account” and select the “SSO Settings” tab.



Note: if you don't see the "SSO Settings" tab? Contact Organimi to have SSO enabled for your account (Premium account required)

Click on the "Configure IDP" button



For the remainder of this set up example the value that we will use for the "`YOUR-COMPANY-ALIAS`" will be "`zengario-test-nine`" so you would replace the small JSON object from above that was …

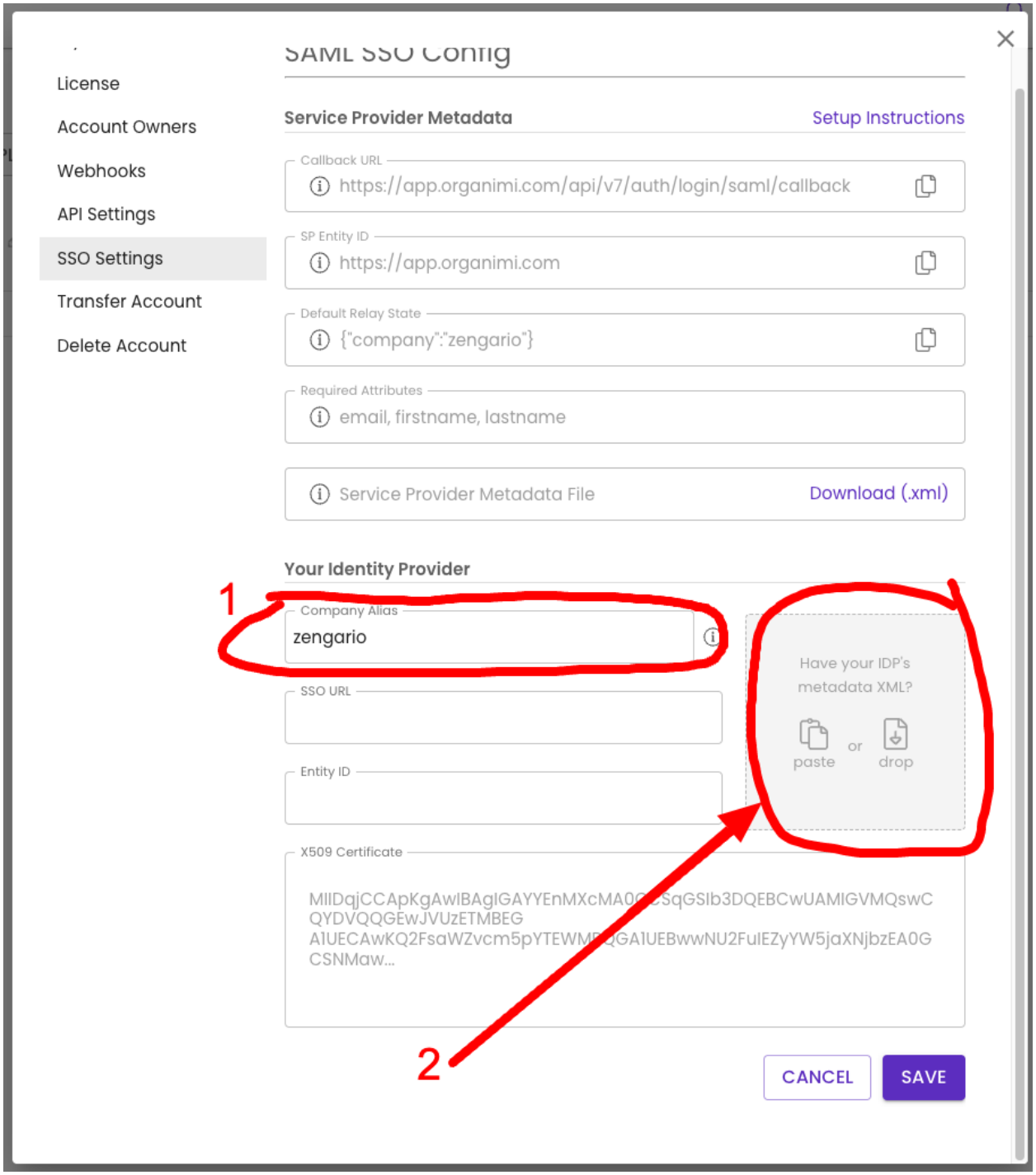
```
{"company":"YOUR-COMPANY-ALIAS"}
```

… with the small JSON object that is …

```
{"company":"zengario-test-nine"}
```

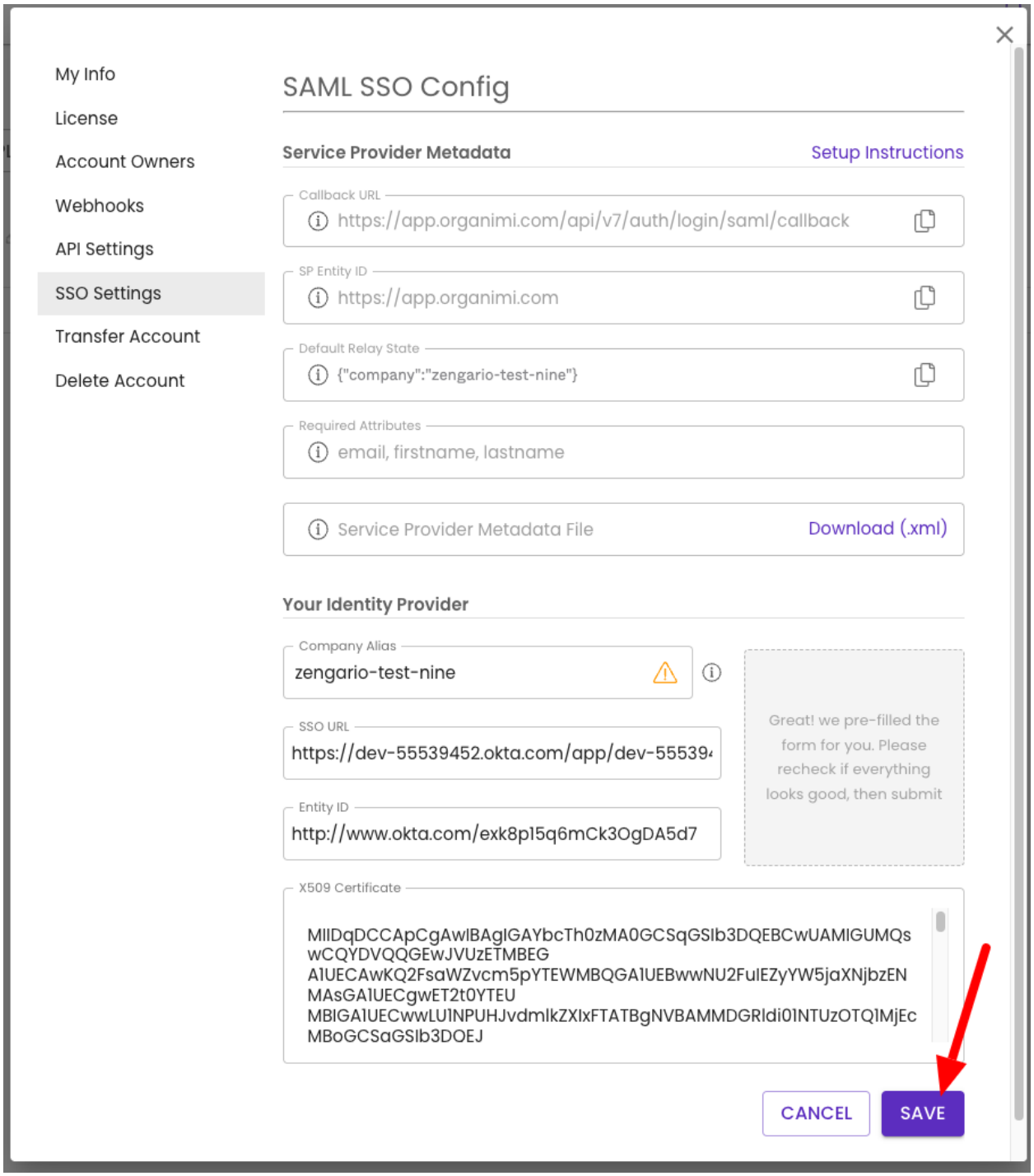
On the “SAML SSO Config” screen enter:

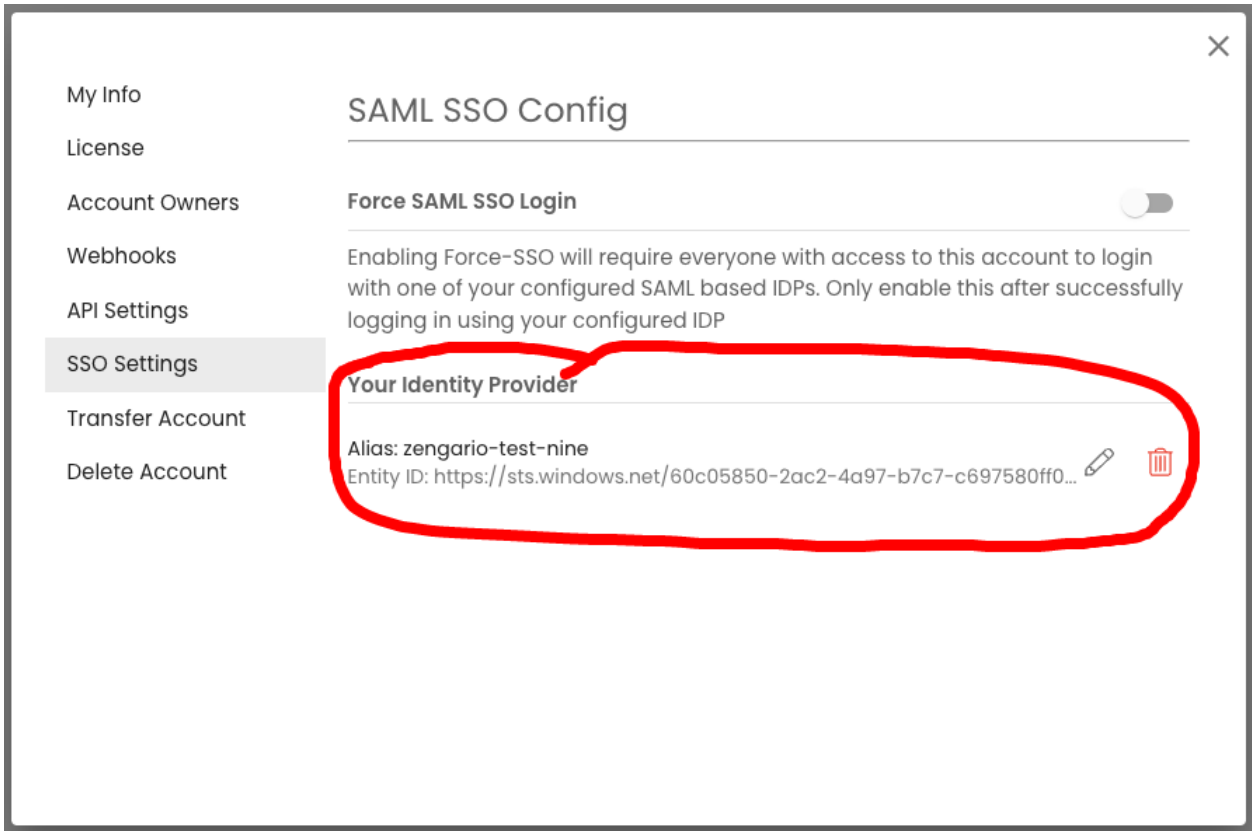
1. **Company Alias: Enter your company alias. It should match exactly with the name entered in Azure AD for the “`YOUR_COMPANY_ALIAS`” value.**
2. IDP Metadata: Drag and drop the XML file that was downloaded from the “Federation Metadata XML” step on the Azure AD side into the “drop area” as highlighted below.



The remaining fields for the “SSO URL”, “Entity ID”, and “x509 Certificate” should be automatically filled out from the contents of the XML file.

3. Click the SAVE button





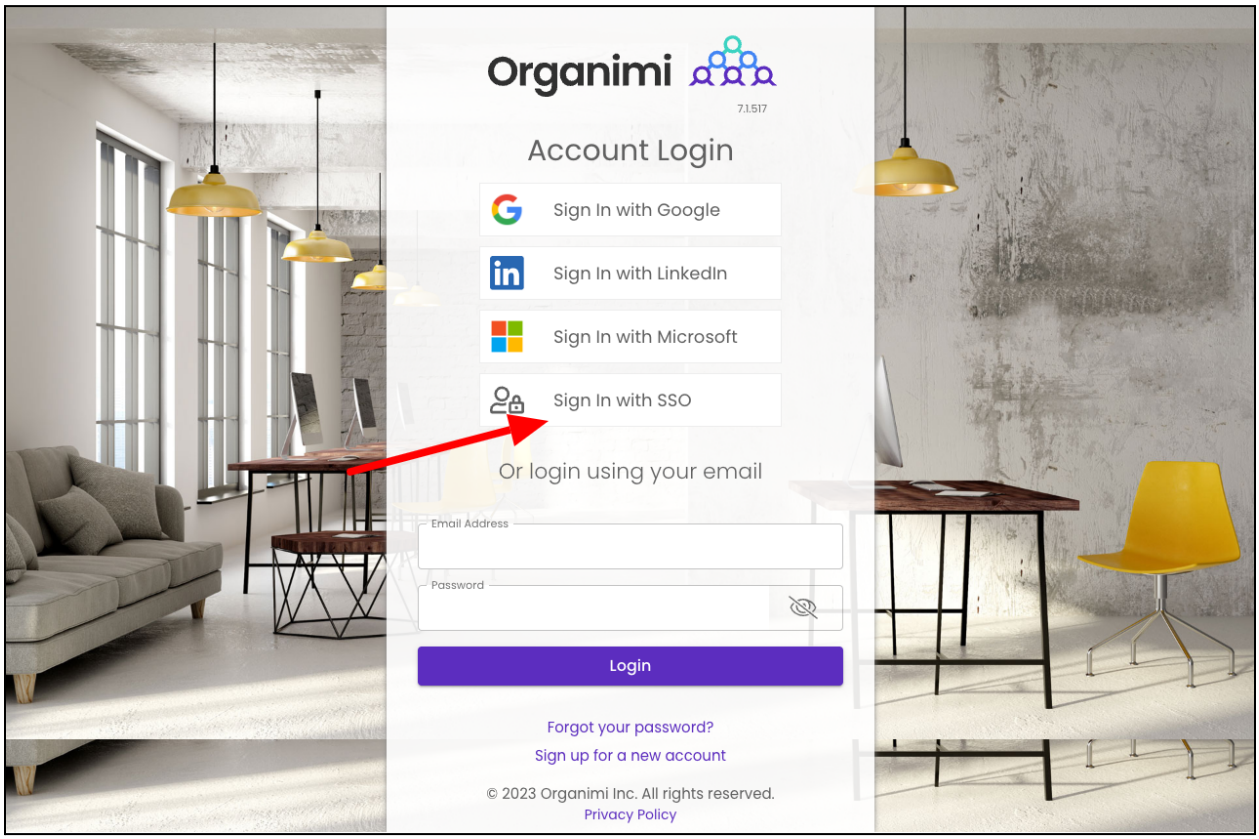
Your Identity Provider should show the Azure AD Entity ID that you just set up, which means IDP configuration is accepted.

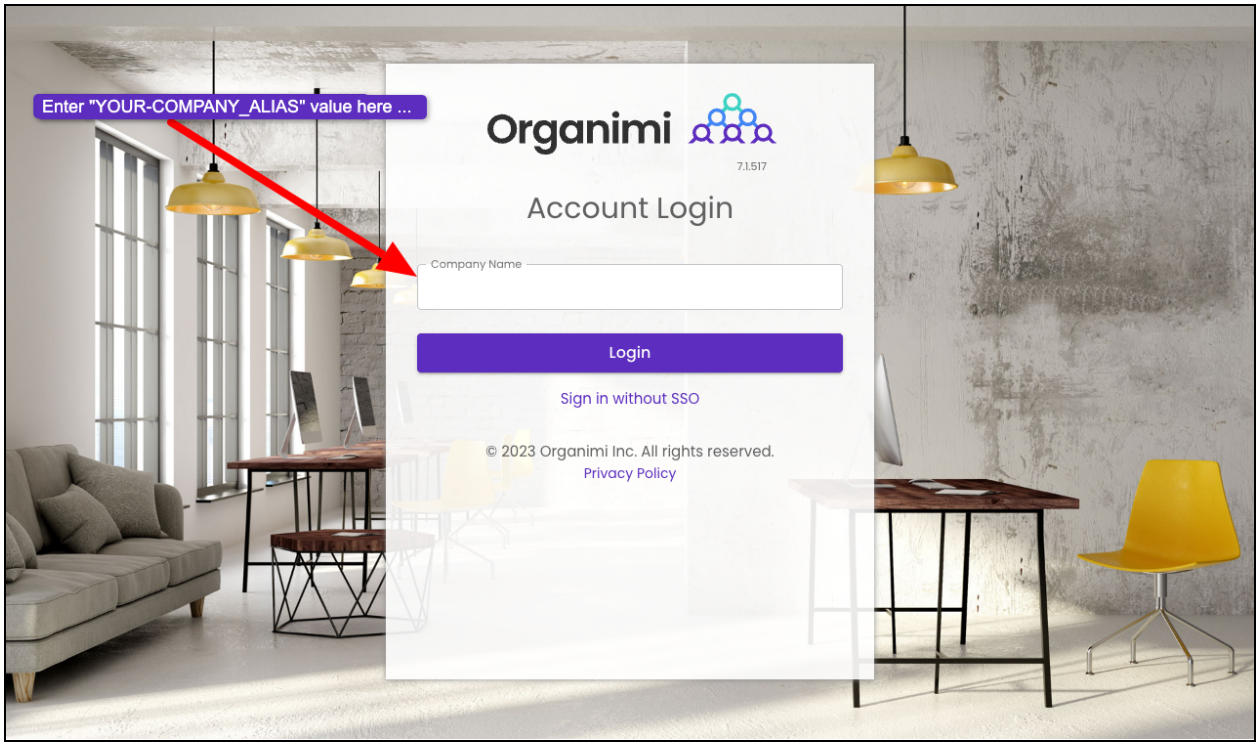
Note: If you do not reach to this point and see an error message on clicking the "SAVE" button, Contact Organimi support @ [*support@organimi.com*](mailto:support@organimi.com)

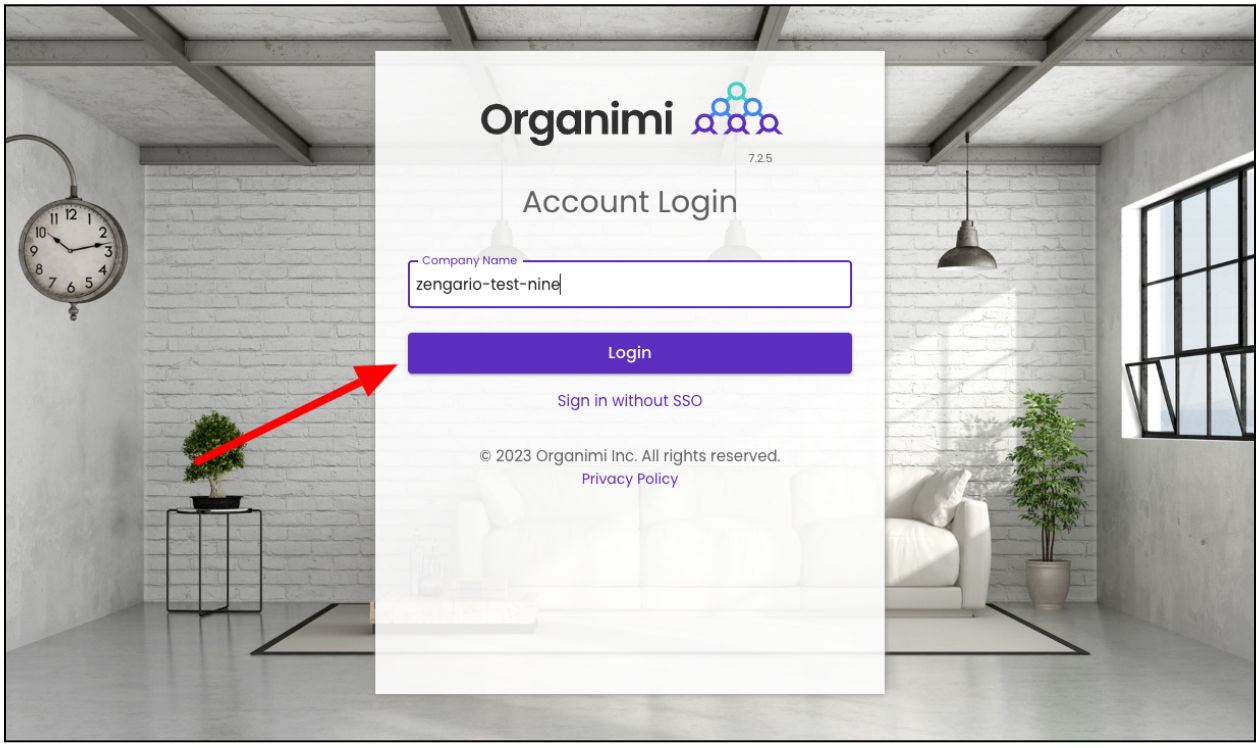
Step 8

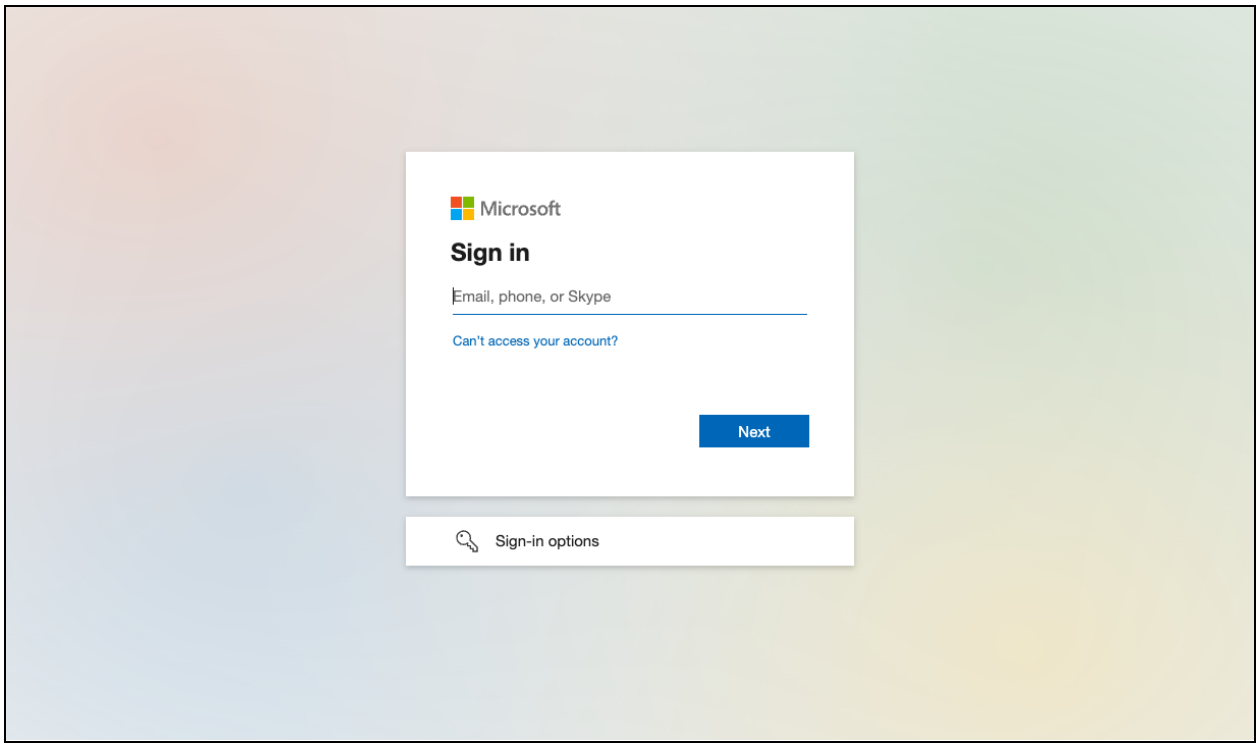
Now it's time to test logging in with your configured IDP. First logout from your account. Then login by clicking “Sign in with SSO”. In the next screen, type in the company name matching from the earlier steps for “`YOUR_COMPANY_ALIAS`” then click login.

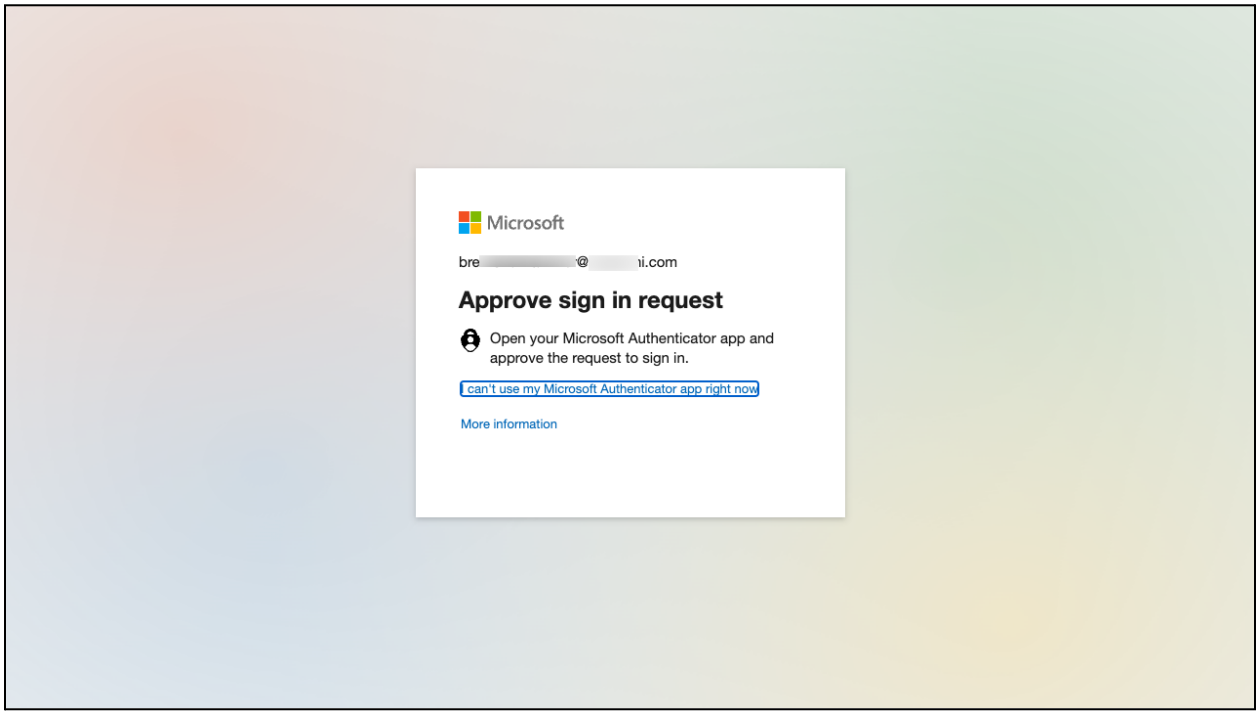
You should be redirected to your Azure AD IDP where you can be authenticated. Once successful, you will be redirected back to Organimi and will be logged in.



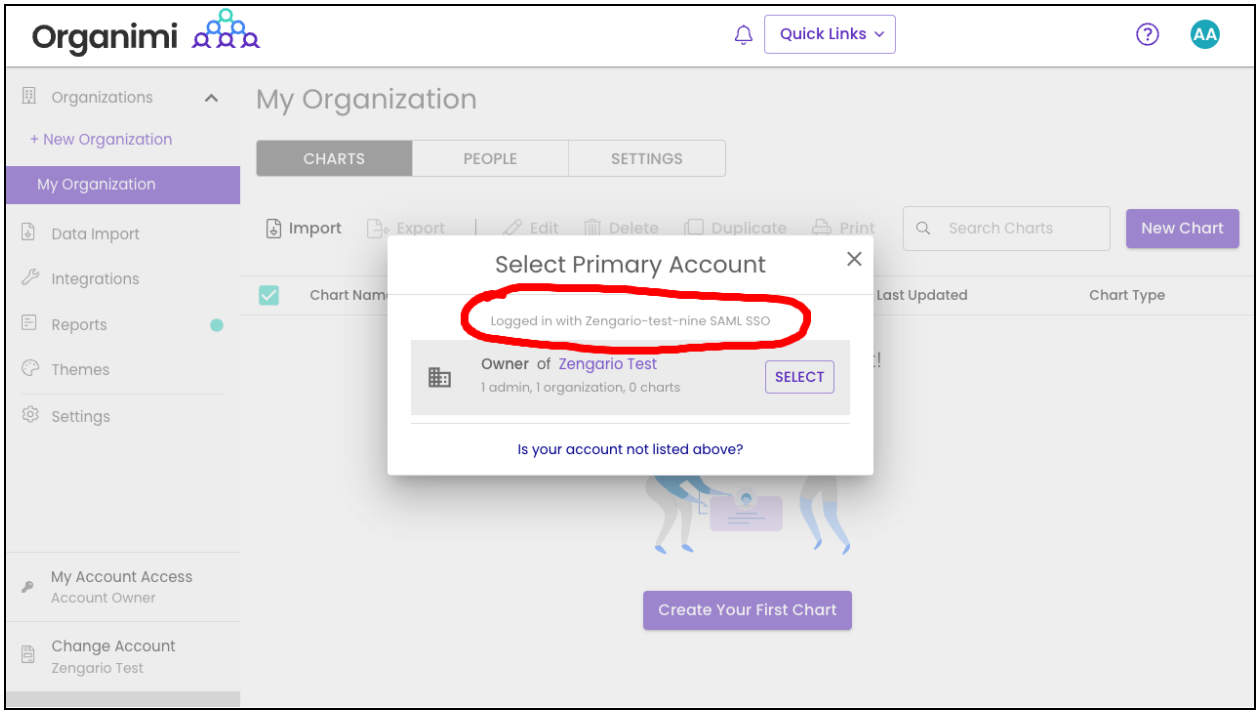

Enter "YOUR-COMPANY_ALIAS" value here ...
Organimi
7.1.517
Account Login
Company Name
Login
Sign in without SSO
© 2023 Organimi Inc. All rights reserved.
Privacy Policy


Organimi
7.2.5
Account Login
Company Name
zengario-test-nine
Login
Sign in without SSO
© 2023 Organimi Inc. All rights reserved.
Privacy Policy





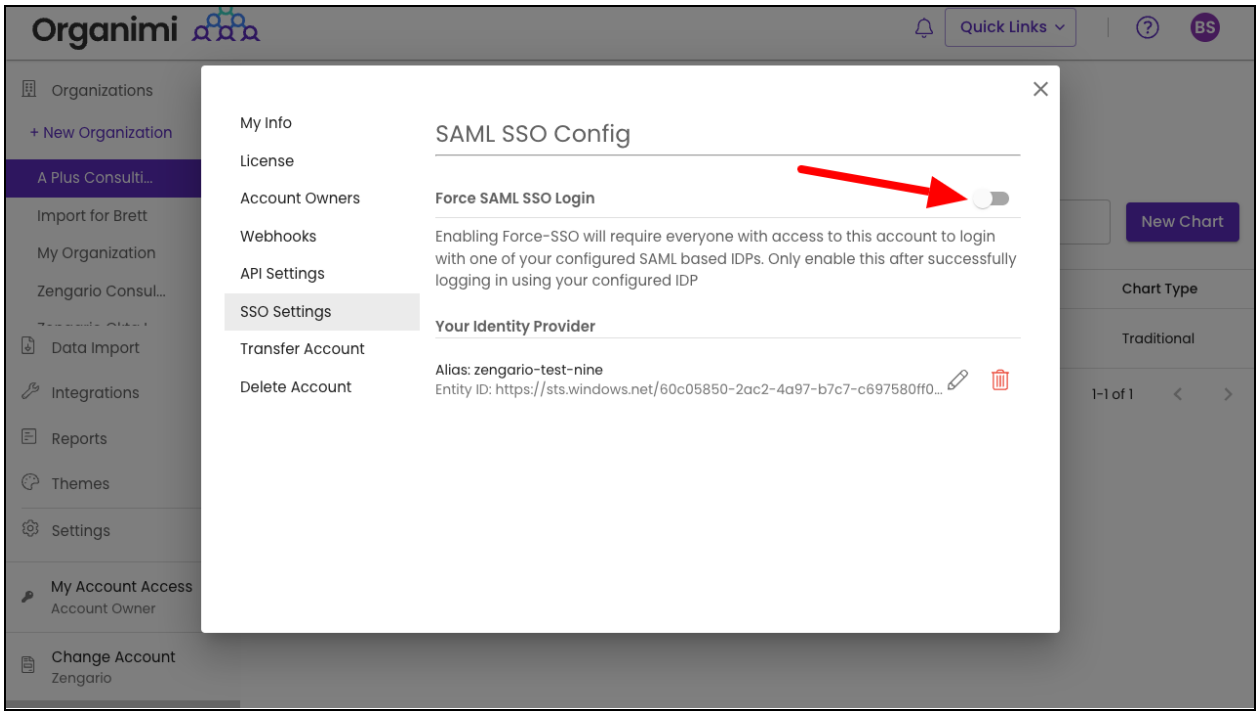
And you are in. If you click the Change Account link on the Organimi screen you will see that you are logged in with SAML SSO

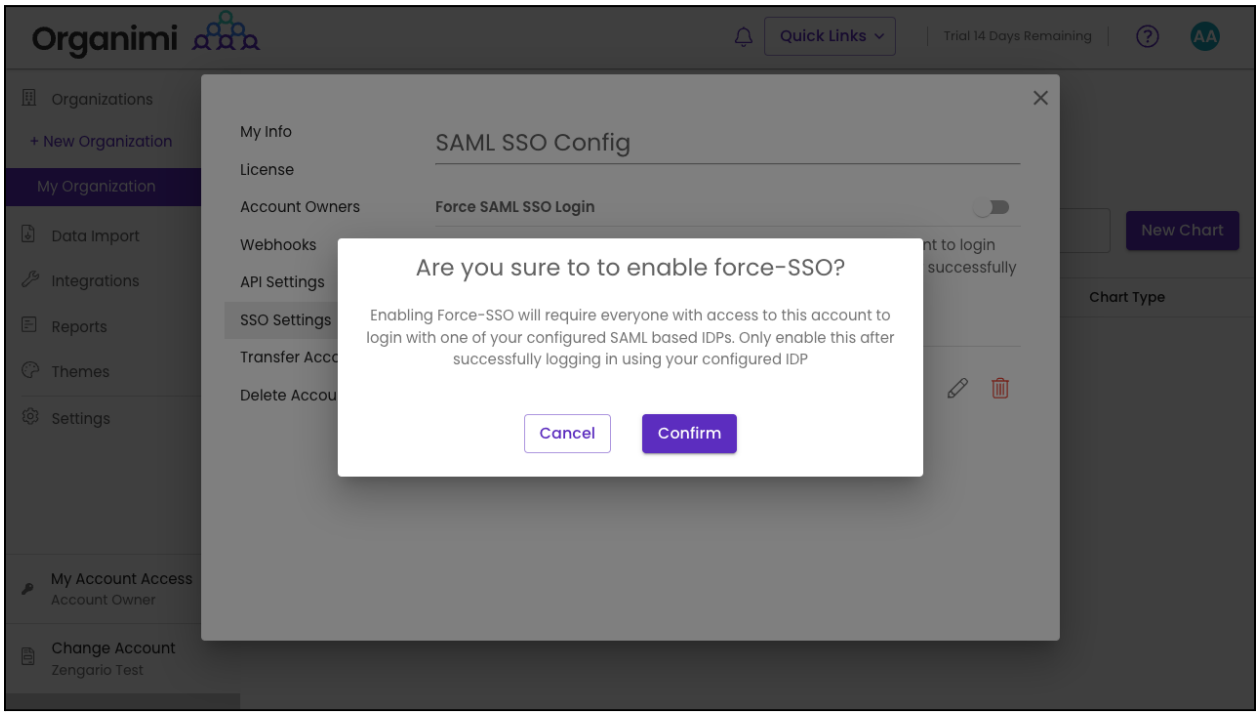


Step 9

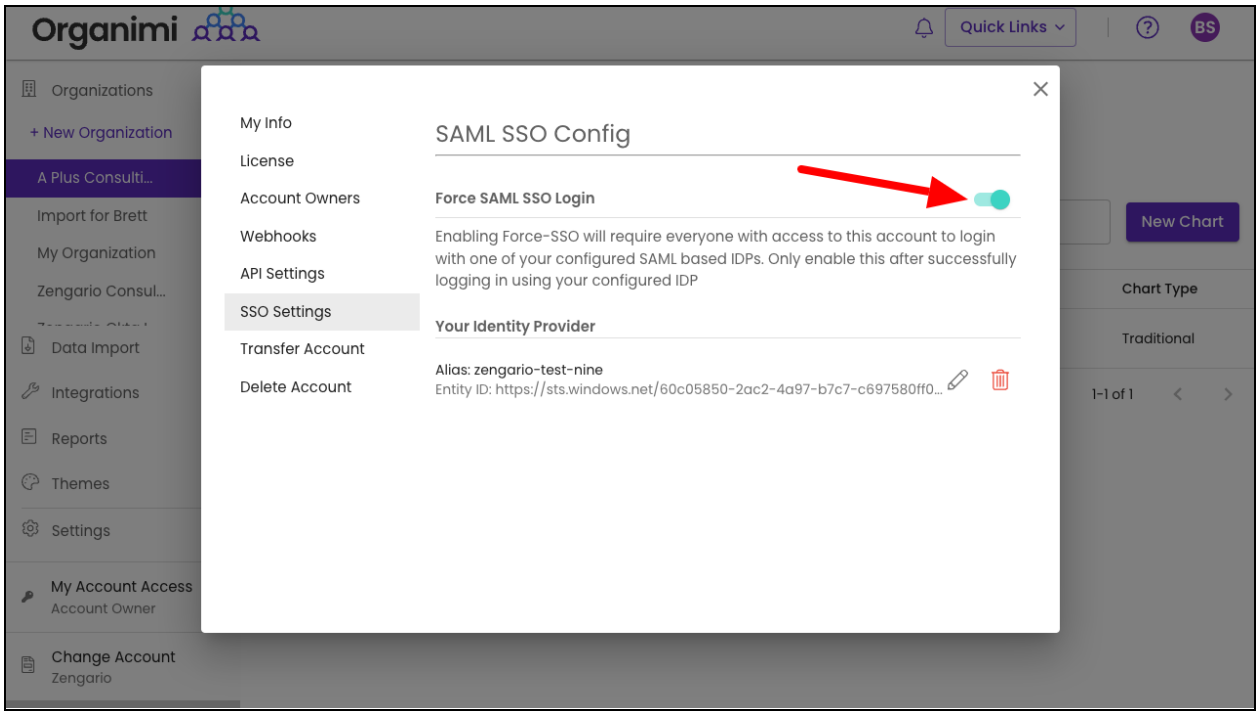
You can also enable “Force-SSO” from the configuration tab. Which will require everyone using this account (including you), to login using your configured IDP only, in order to access resources under this account. Other login methods (social & username/password) will not be allowed access to the account.

Note: As the account owner, It's recommended that you test logging in with your IDP first before turning on this setting, as you will not be able to access the account via any other login methods after you enable the “Force-SSO” option.

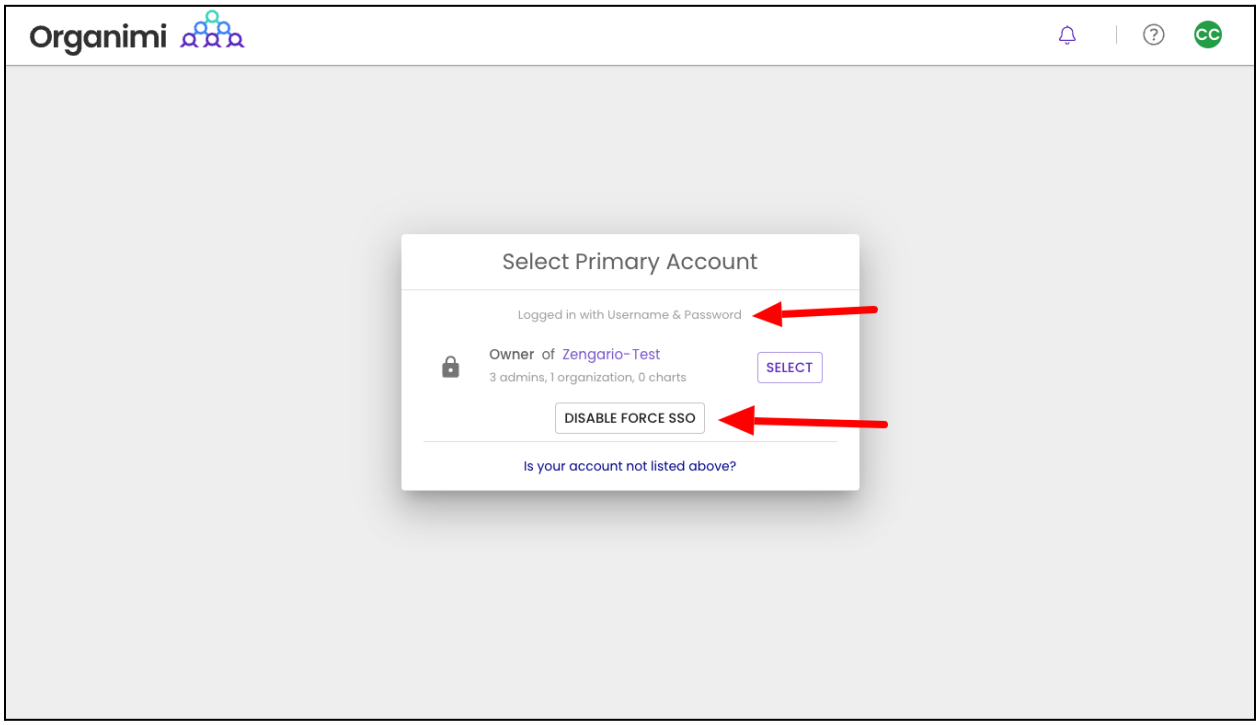


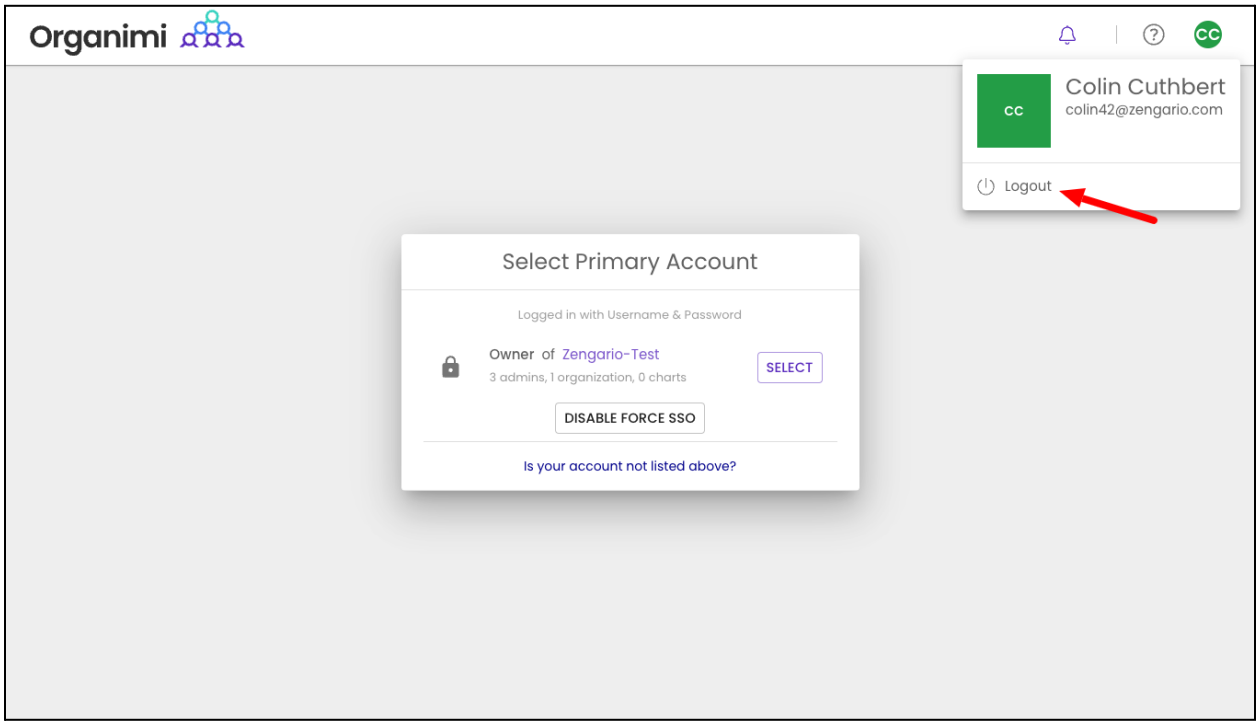


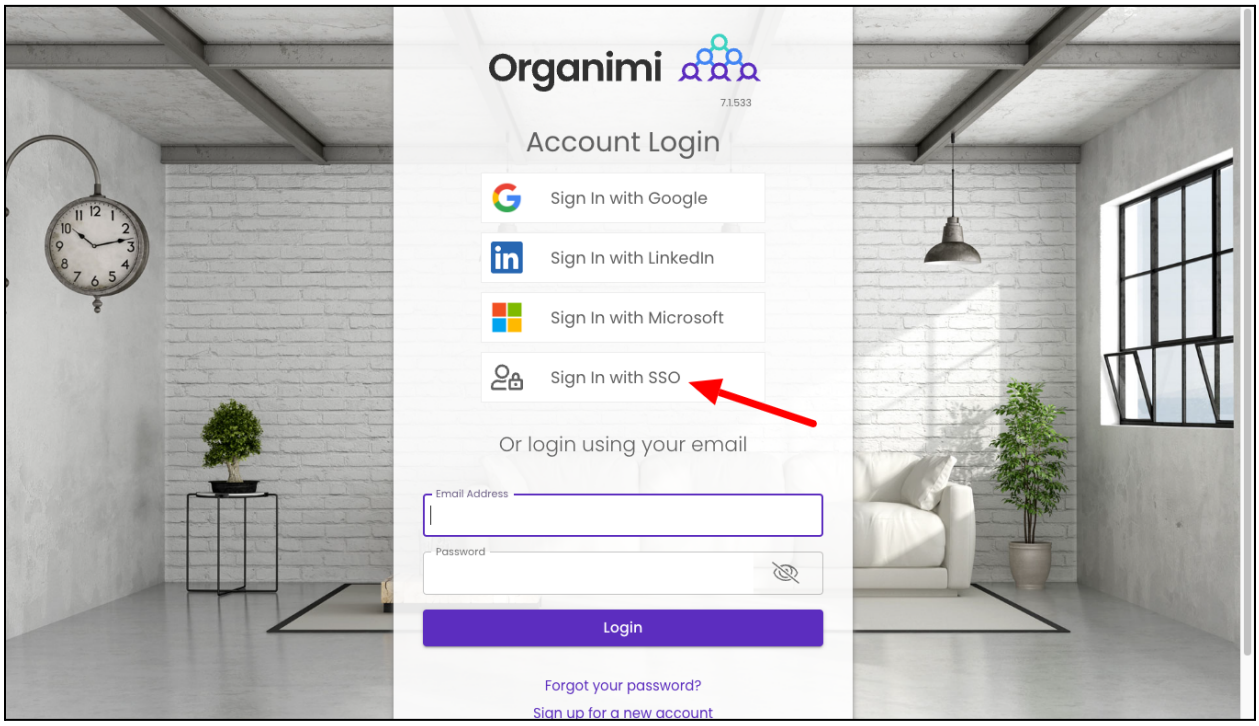
If you were logged into Organimi with you SSO IDP Account then you will just see that the switch is now on for “Force SSO”



If, however, you were logged in to Organimi with your social login or username/password your access to the account will be immediately disabled and you will be taken to the Account Selection Screen and you will see that your access to the account is locked. You could disable the “Force SSO” (only available to account owners) … but normally you would just logout from Organimi and log back in from your SSO IDP Account.




Organimi
CC
Colin Cuthbert
colin42@zengario.com
Logout
Select Primary Account
Logged in with Username & Password
Owner of Zengario-Test
3 admins, 1 organization, 0 charts
SELECT
DISABLE FORCE SSO
Is your account not listed above?

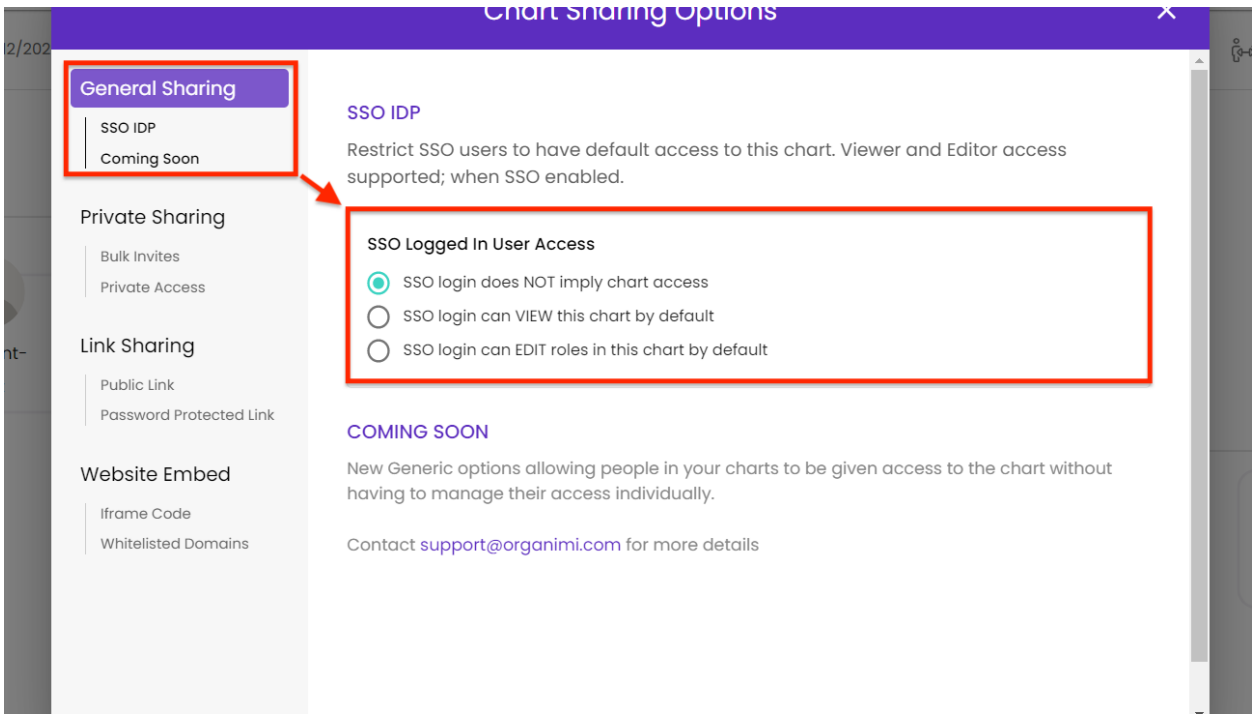

Organimi
7.1.533
Account Login
Sign In with Google
Sign In with LinkedIn
Sign In with Microsoft
Sign In with SSO
Or login using your email
Email Address
Password
Login
Forgot your password?
Sign up for a new account

Step 10 - Chart Settings

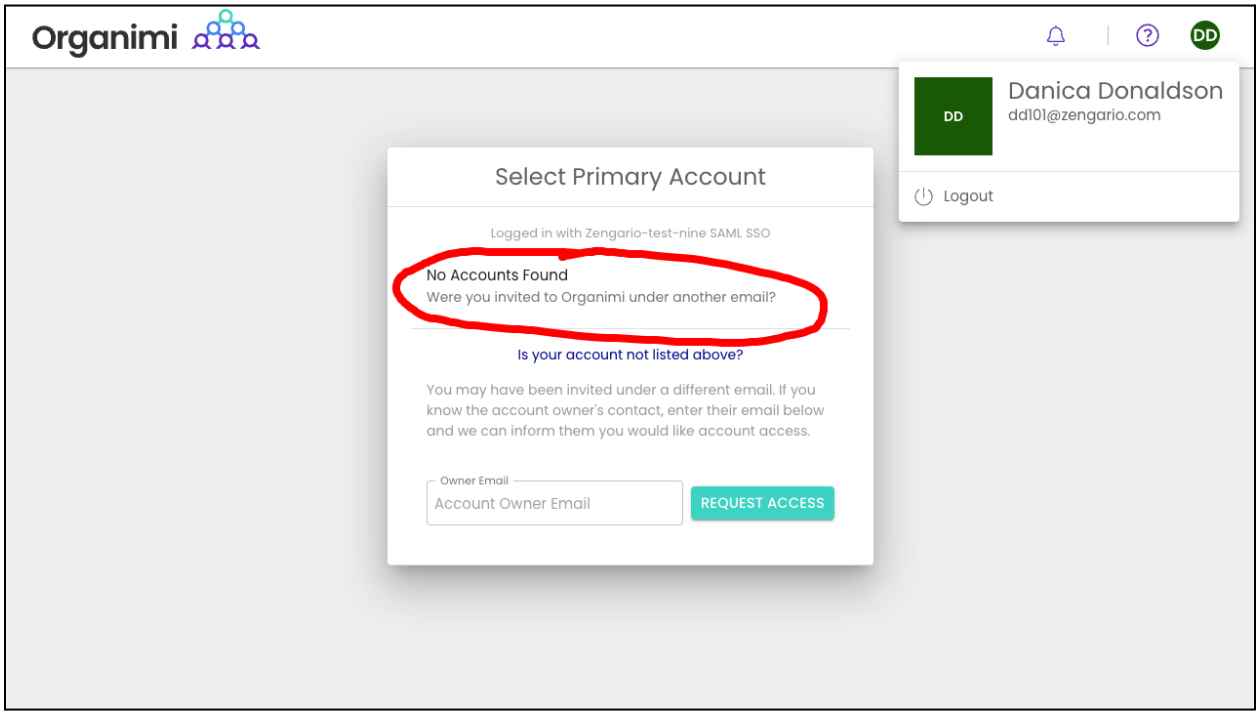
In order for a user to see an Org Chart that has been set up in Organimi … you will have to either invite them specifically to the chart or enable “General Sharing”. We recommend the “General Sharing” set up for SSO users to the primary chart or charts meant to be shared with all SSO users.

Sharing and Invitations are set-up on a per chart basis so for each chart you want to share you would set up General Sharing to one of the three settings shown below in the screen shot.

- *SSO login does NOT imply chart access* - this setting means that just because a user has access to Organimi via SSO they do not automatically have access to this chart. With this setting only users specifically invited to the chart in the Organization settings will be able to access this chart.
- *SSO Login can VIEW this chart by default* - this is the most common setting and will grant anyone who accesses the Organimi account via their SSO login will have Viewer level access to the chart meaning they can see the chart and expand an contract the levels but they cannot make any changes to the role cards, people or the styling.
- *SSO Login can EDIT roles in this chart by default* - this setting will grant anyone who access the Organimi account via their SSO login will have Editor access to the chart and will be able to edit the role carts, people and the chart hierarchy. This setting is usually used when only a few users will be provisioned to access Organimi in SSO.

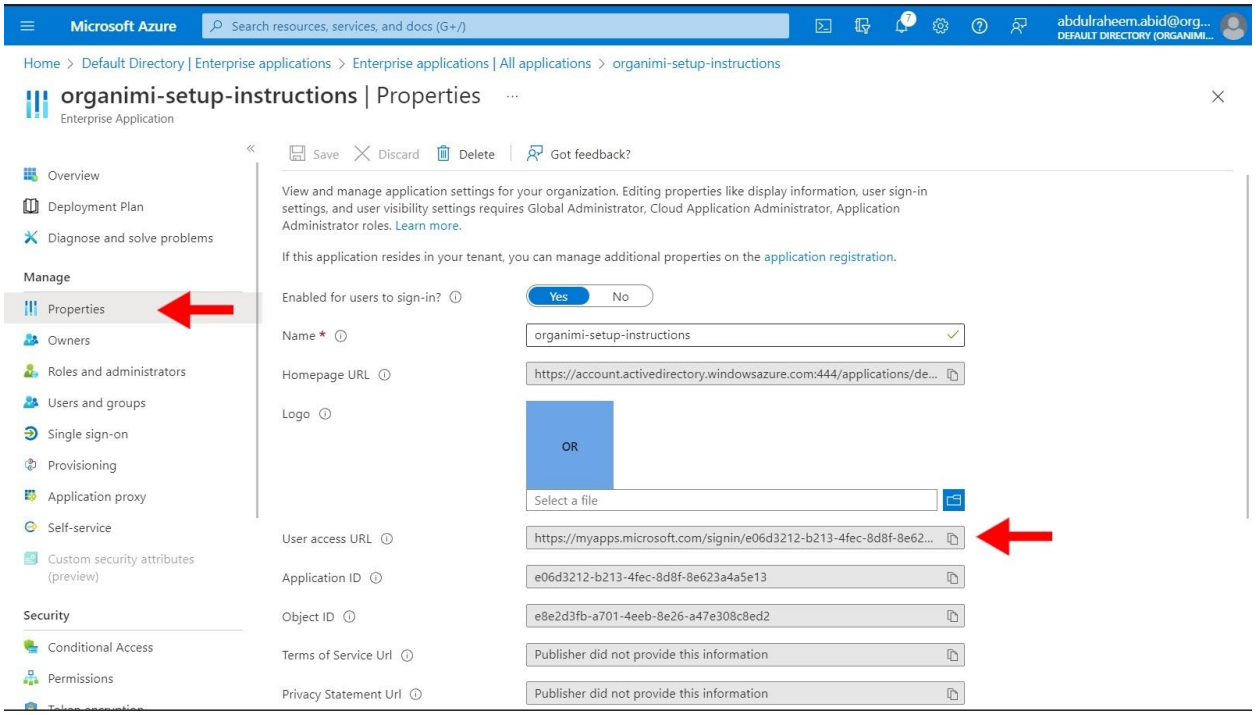


When the General Sharing is set to “NOT imply chart access” (the default) you will need to invite users specifically to your Organizations as Admins or Charts as Editors or Viewers … if the General Sharing is set to “NOT imply chart access” and the user has not been invited and granted access to any Organizations or Charts in Organimi they will be greeted with a message telling them they do not have access to any accounts in Organimi … if this happens then simply invite them to the Organization as an Admin or to one of the Charts as an Editor or Viewer.



Step 11 - Organimi Direct Access URL

The account owner can send the User access URL from the Azure AD to the group once they have been provisioned access to Organimi … then users can directly access the Organimi Account from the link with their SSO credentials.



Thank you for being an Organimi customer and please contact us at support@organimi.com if you run into any issues or have any questions that are not covered in this document or are beyond the scope of this document.