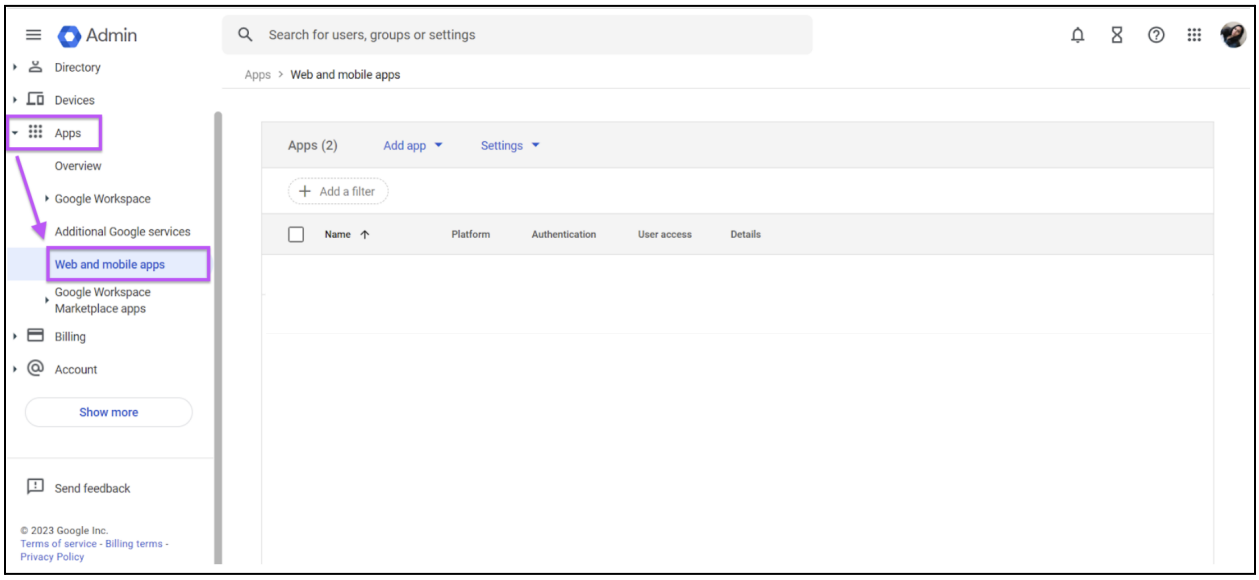
SAML based SSO - Login with Google Workspace

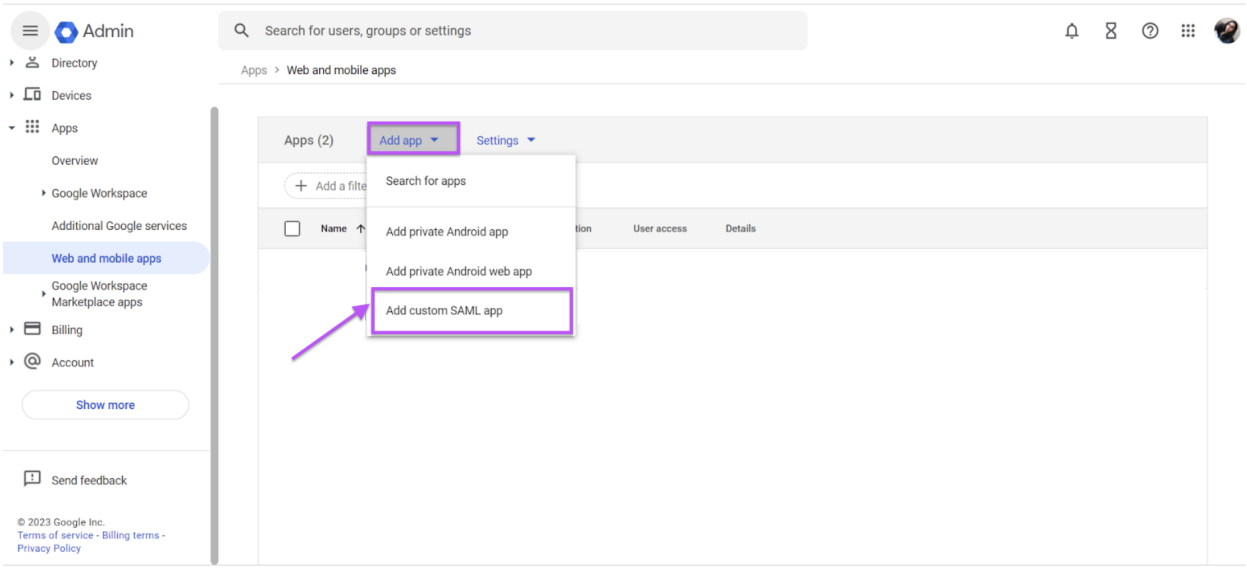
Organimi has implemented SAML based SSO for Premium account holders … this document will walk you through the steps to set up the integration with Google Workspace

Step 1

Go to your Google Workspace admin console and click “Web and mobile apps” from the Apps tab.

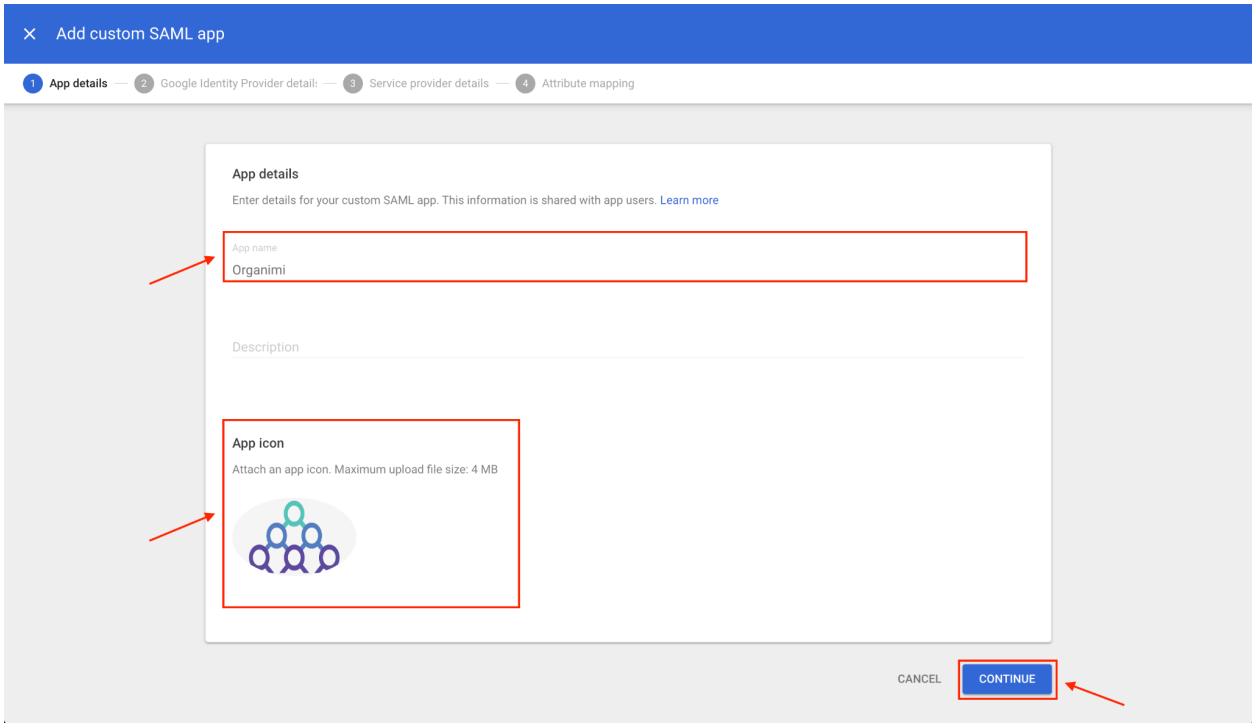


Click on Add app and then “Add custom SAML app”.



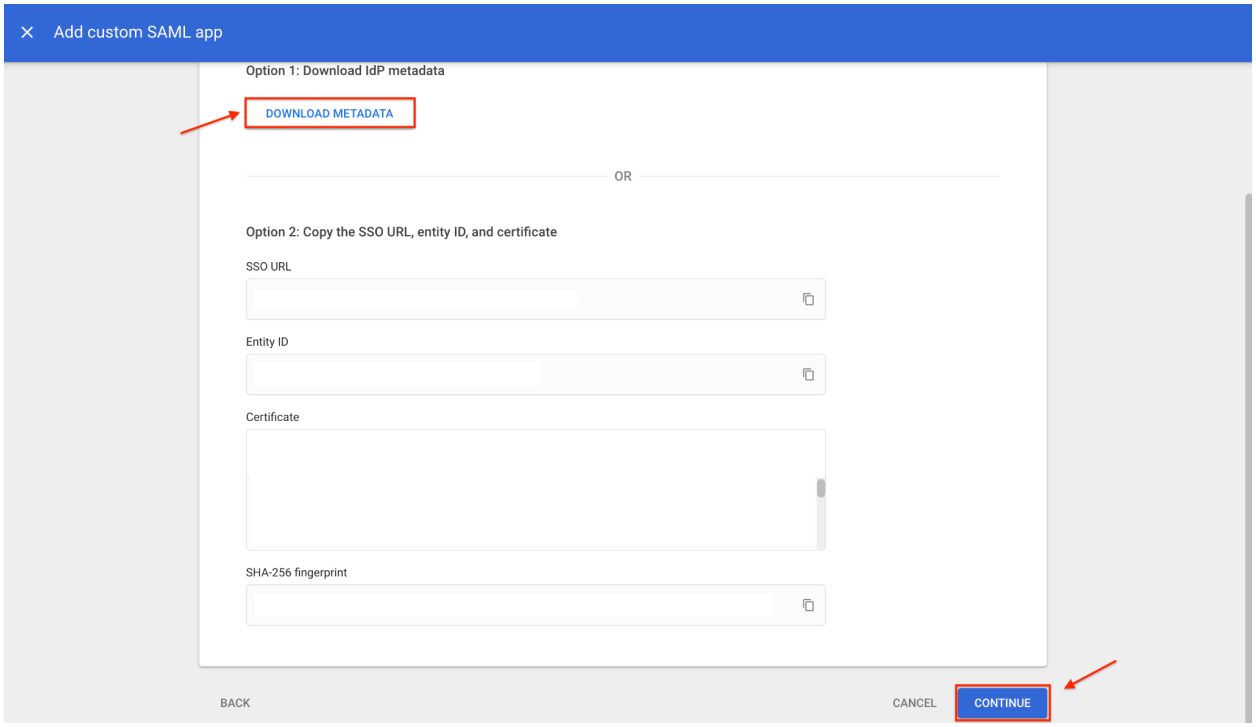
Step 2

Under App details, enter App name as “Organimi”, upload Organimi’s logo and click continue (you can download the Organimi logo at: Organimi_LogoOnly.png)



Step 3

Click on “Download Metadata” and then click continue. You will be using the downloaded file in the following steps.

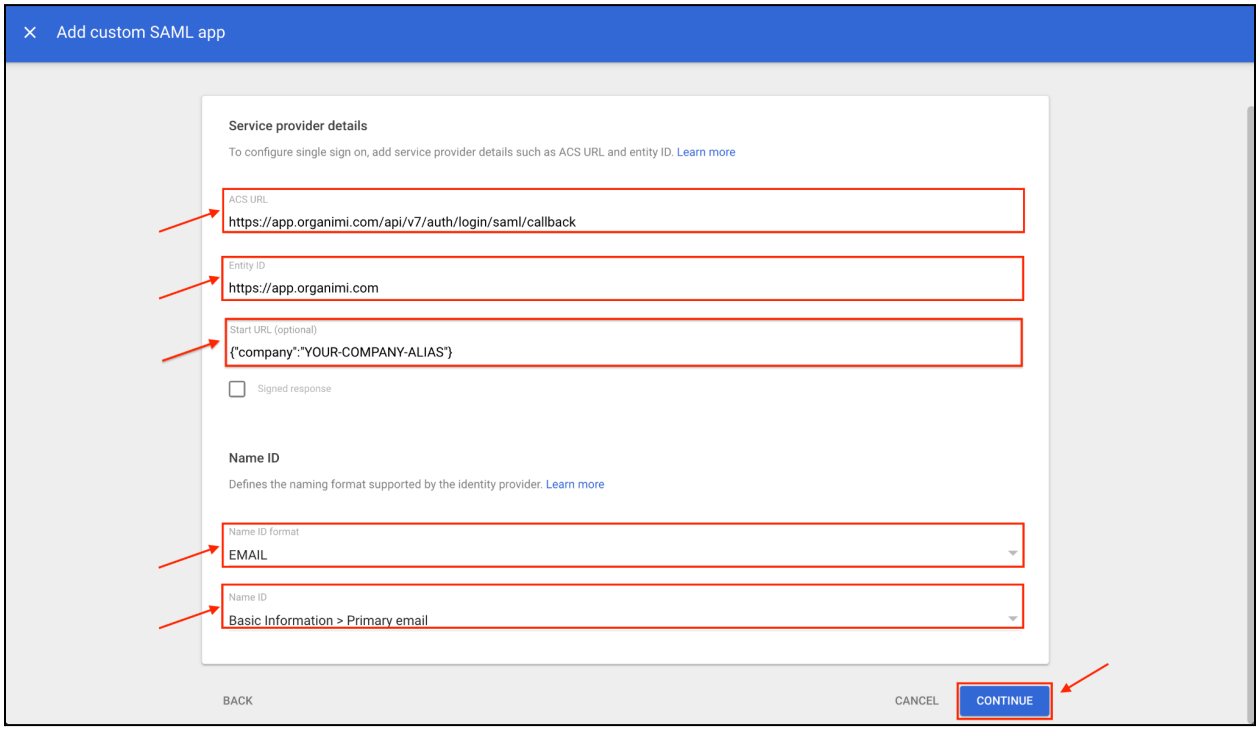


Step 4

Under Service provider details, enter the following information

1. Entity ID: https://app.organimi.com
    a. Only for EU customers - https://eu.app.organimi.com
    b. Only for AU customers - https://au.app.organimi.com
2. ACS URL: https://app.organimi.com/api/v7/auth/login/saml/callback
    a. Only for EU customers - https://eu.organimi.com/api/v7/auth/login/saml/callback
    b. Only for AU customers - https://au.organimi.com/api/v7/auth/login/saml/callback
3. Start URL: {"company":"YOUR-COMPANY-ALIAS"}
    a. ***Start URL should contain the above json object.***
    b. ***Note: Replace the placeholder with your company name. This name will also be required later. And anyone who wishes to login using this IDP, will be asked to enter this name when signing in.***
4. Name ID format: EMAIL

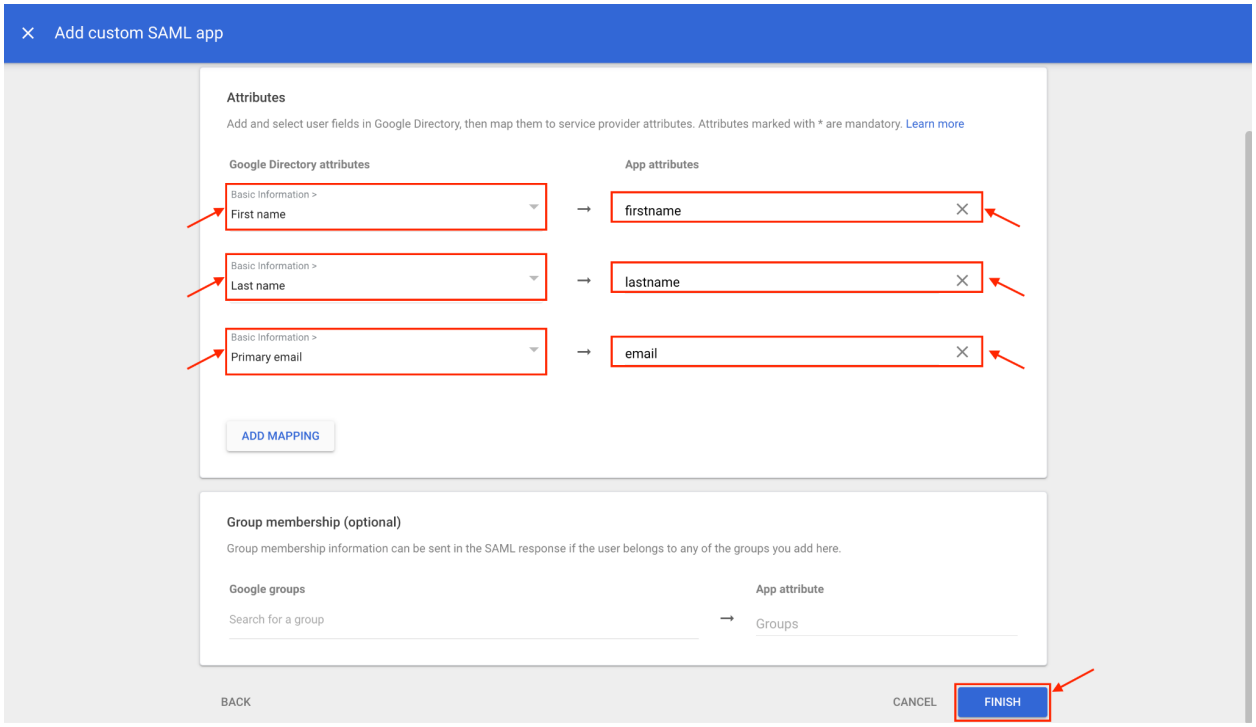
(Note: Please ensure all the values are mapped correctly as per the screenshots)



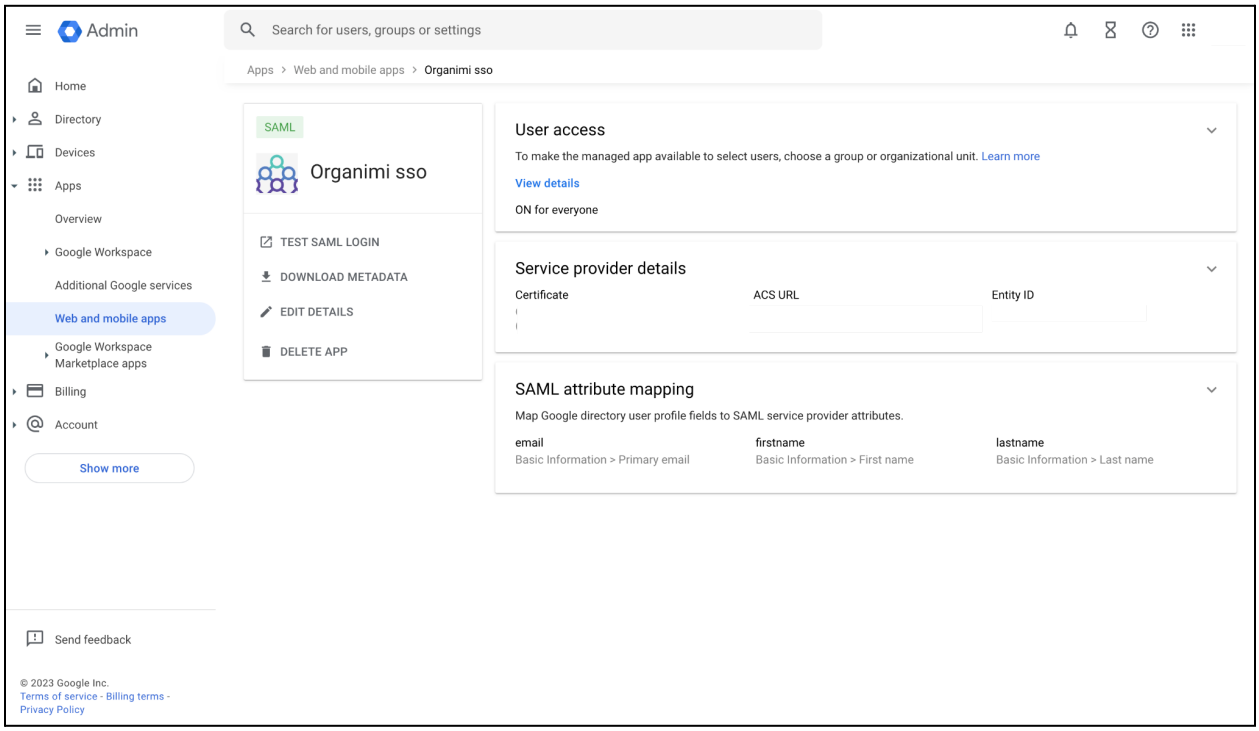
In order for a user to log into Organimi, we require the following three attributes of the user from Google Workspace. Configure them under “Attribute Mapping”. The name should be all lowercase, and the value should be matched accordingly.

1. email
2. firstname
3. lastname

Once all configured, click finish at the bottom.

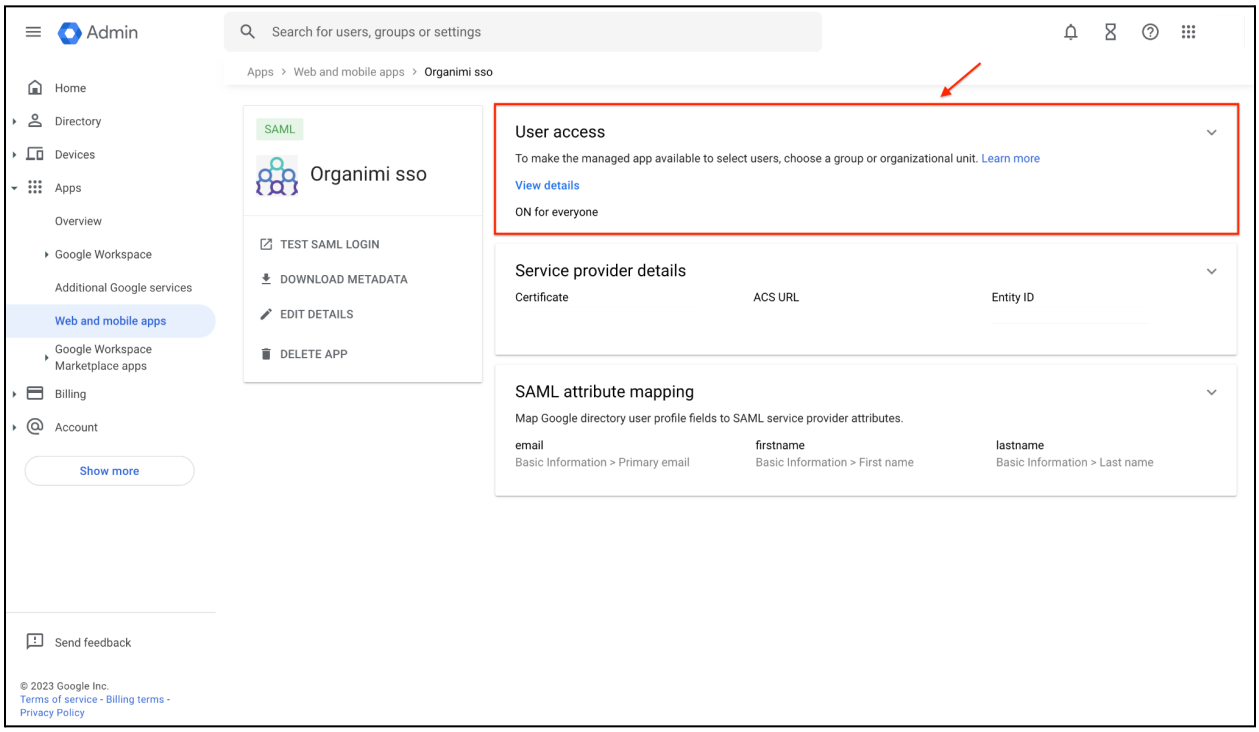


The overview screen should look something like this after the initial configuration.

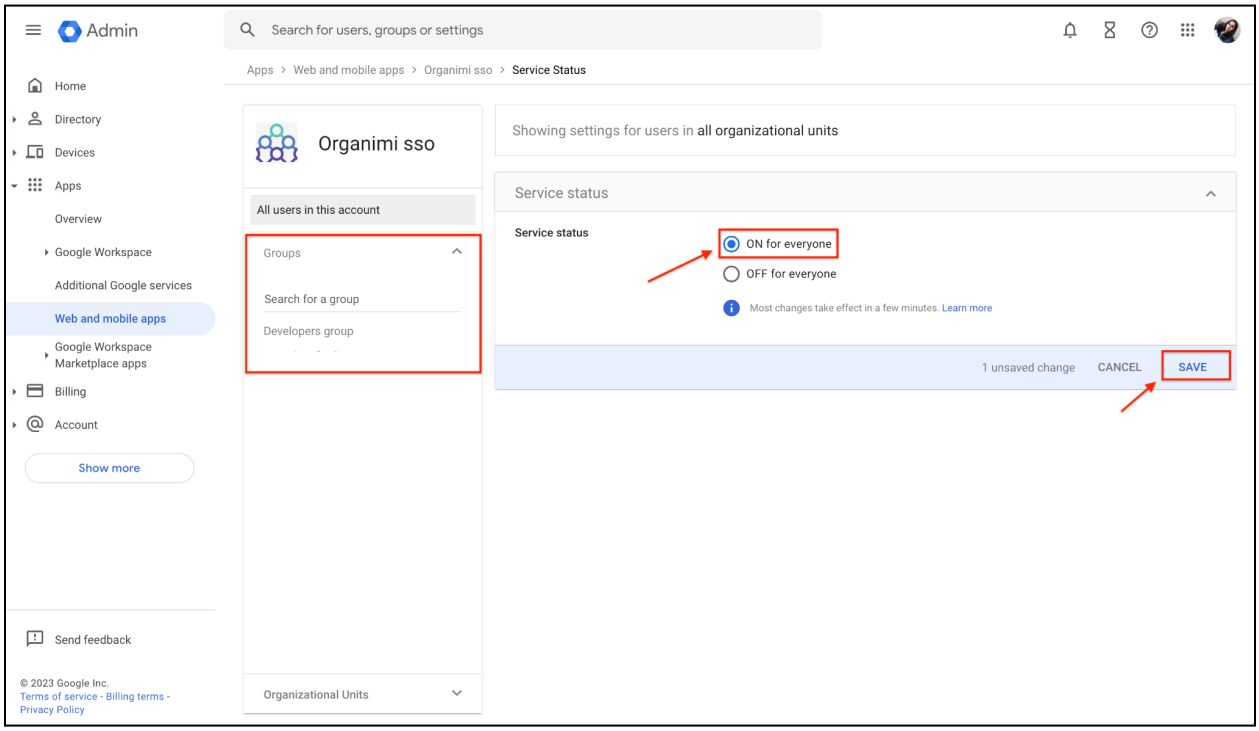


Step 5

In order to grant access to a group, click on “User Access”.

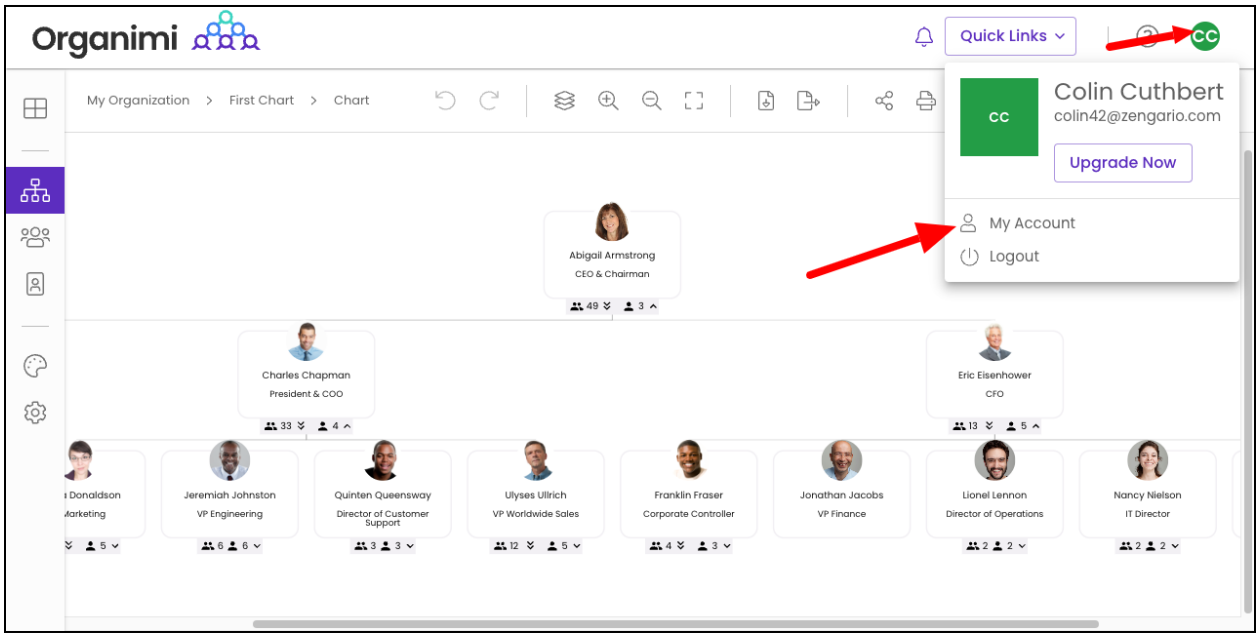


Click on “ON for everyone” for Service status or select groups that need to be granted access, and then click on “SAVE”.

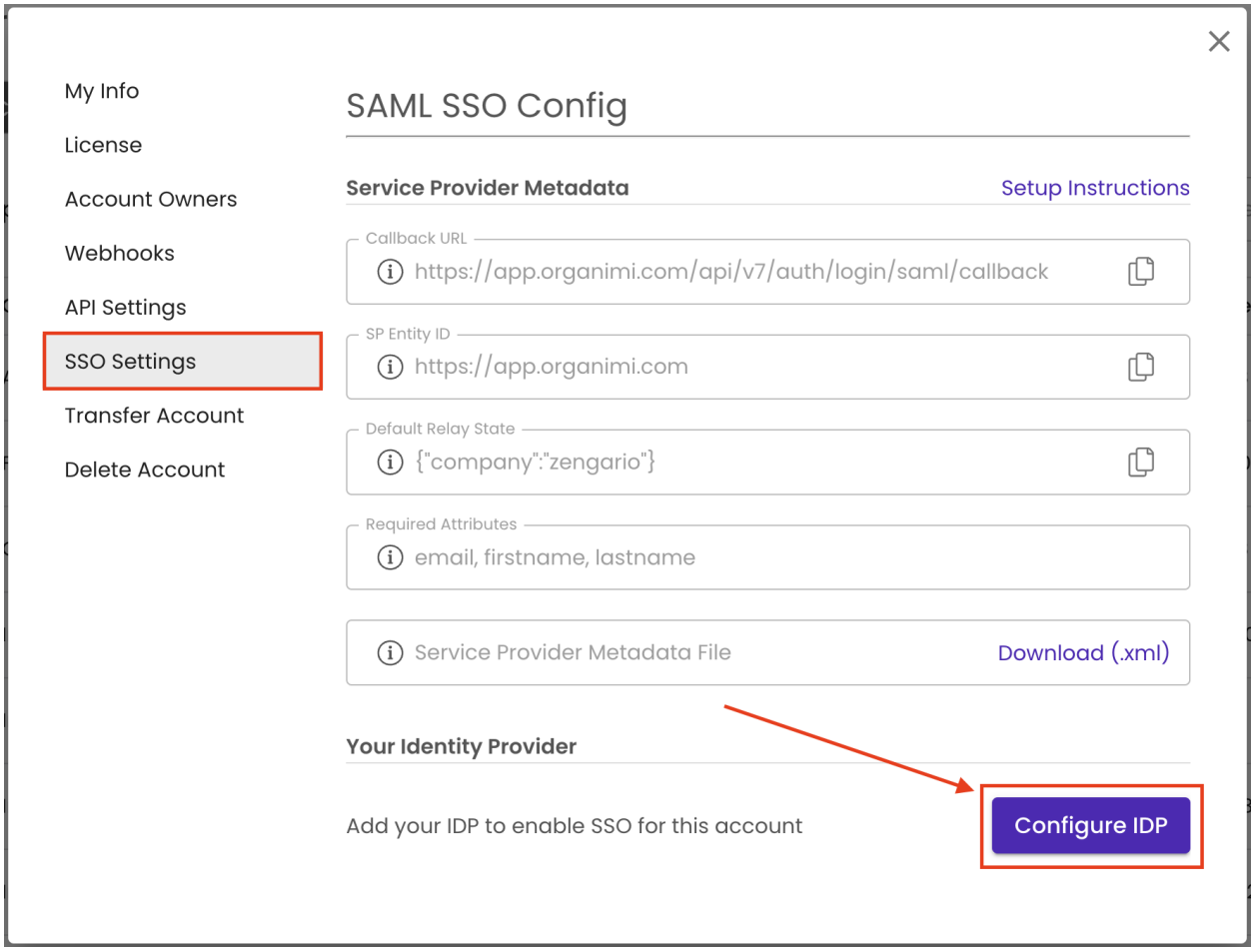


Step 6

Visit https://app.organimi.com (for EU customers - https://eu.app.organimi.com and for AU customers - https://au.app.organimi.com), login to your account using any social login, or username/password. Click “My Account” and select the “SSO Settings” tab.



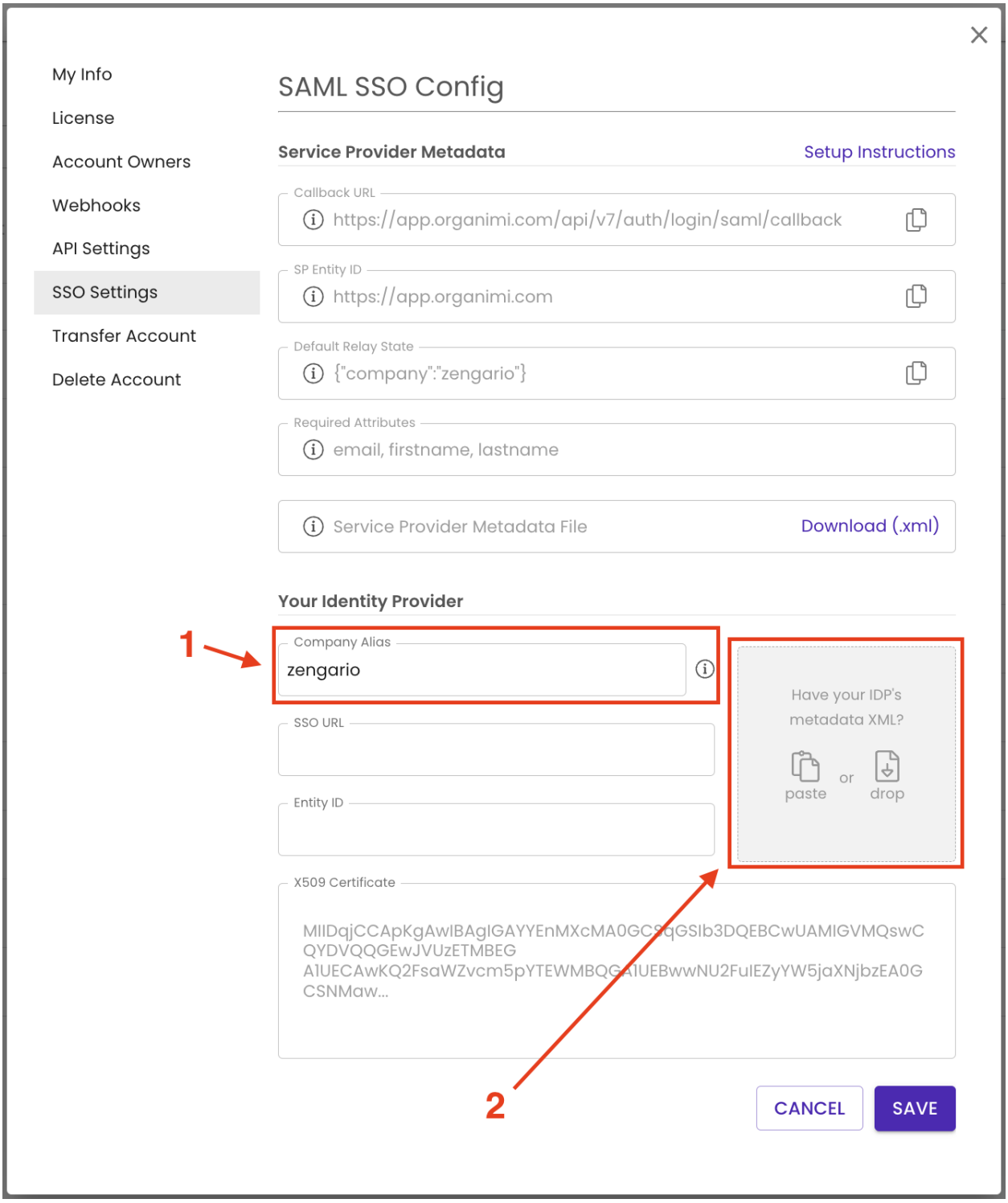
Note: if you don’t see the “SSO Settings” tab? Contact Organimi to have SSO enabled for your account (Premium account required)


My Info
License
Account Owners
Webhooks
API Settings
SSO Settings
Transfer Account
Delete Account
SAML SSO Config
Service Provider Metadata
Setup Instructions
Callback URL
https://app.organimi.com/api/v7/auth/login/saml/callback
SP Entity ID
https://app.organimi.com
Default Relay State
{"company":"zengario"}
Required Attributes
email, firstname, lastname
Service Provider Metadata File
Download (.xml)
Your Identity Provider
Add your IDP to enable SSO for this account
Configure IDP

Step 7

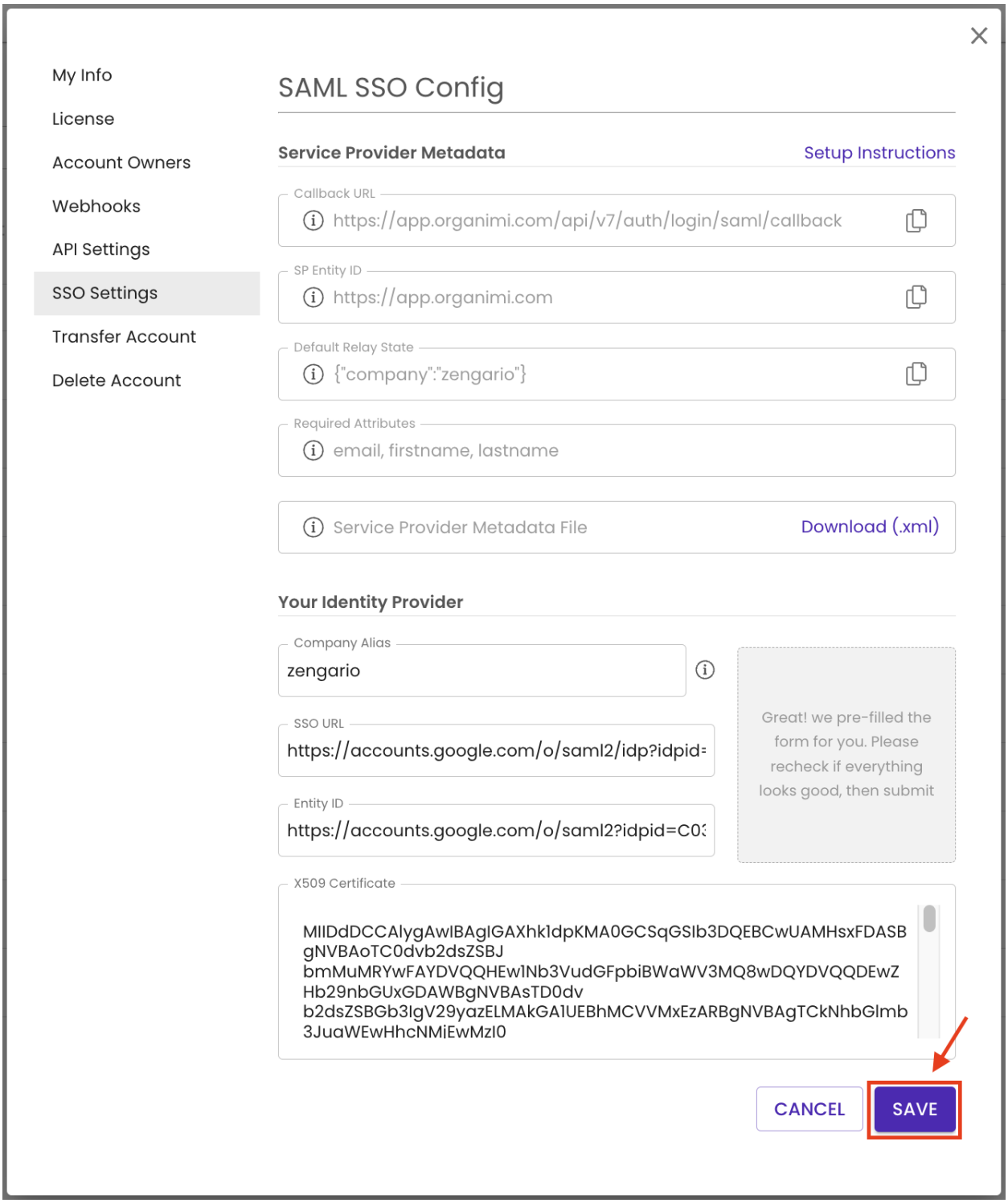
Click on the “Configure IDP” button and enter:

1. **Company Alias: Enter your company name. It should match exactly with the name entered for step 4.3**
2. IDP Metadata: Drag and Drop the XML Metadata file that you downloaded in step 3 into the “drop area” as highlighted below.

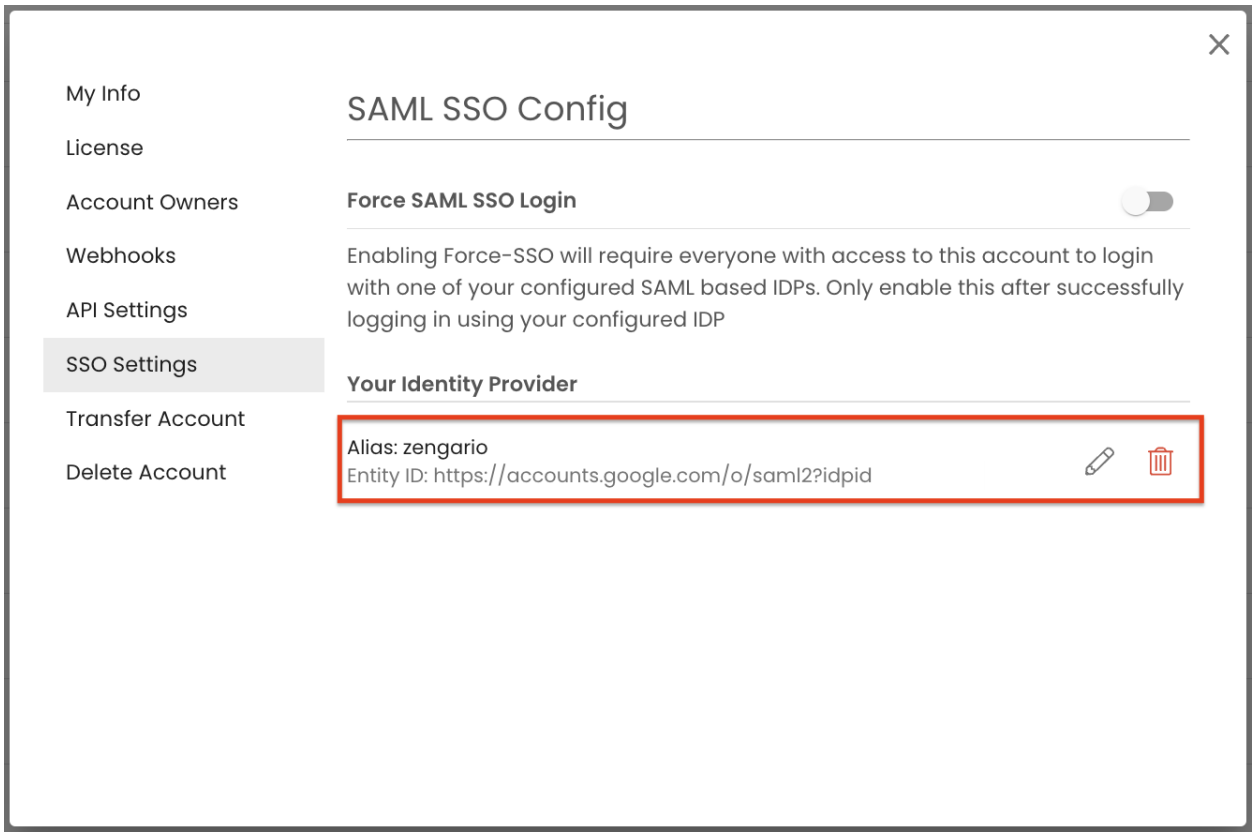


3. The remaining fields for the “SSO URL”, “Entity ID”, and “x509 Certificate” should be automatically filled out from the contents of the XML file.

4. Click the SAVE button



Google Workspace is now set up as the Identity Provider

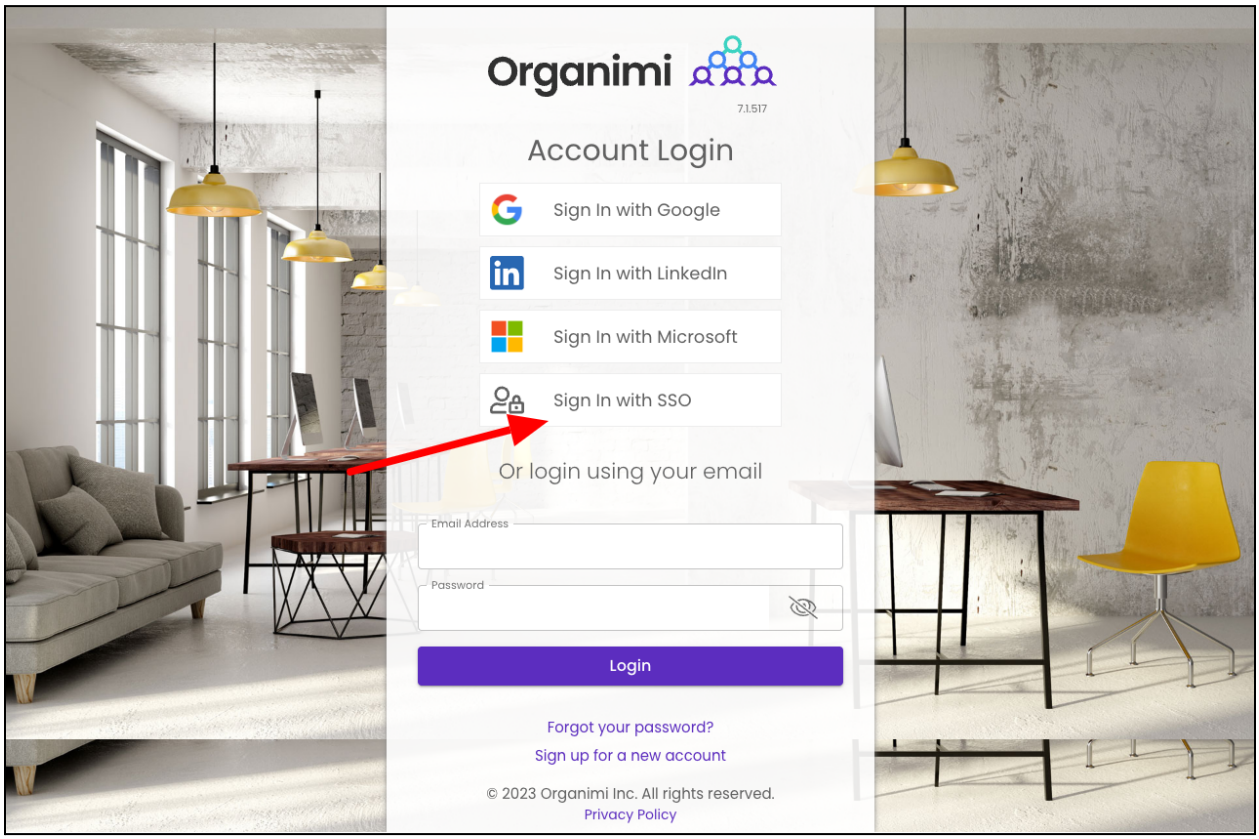


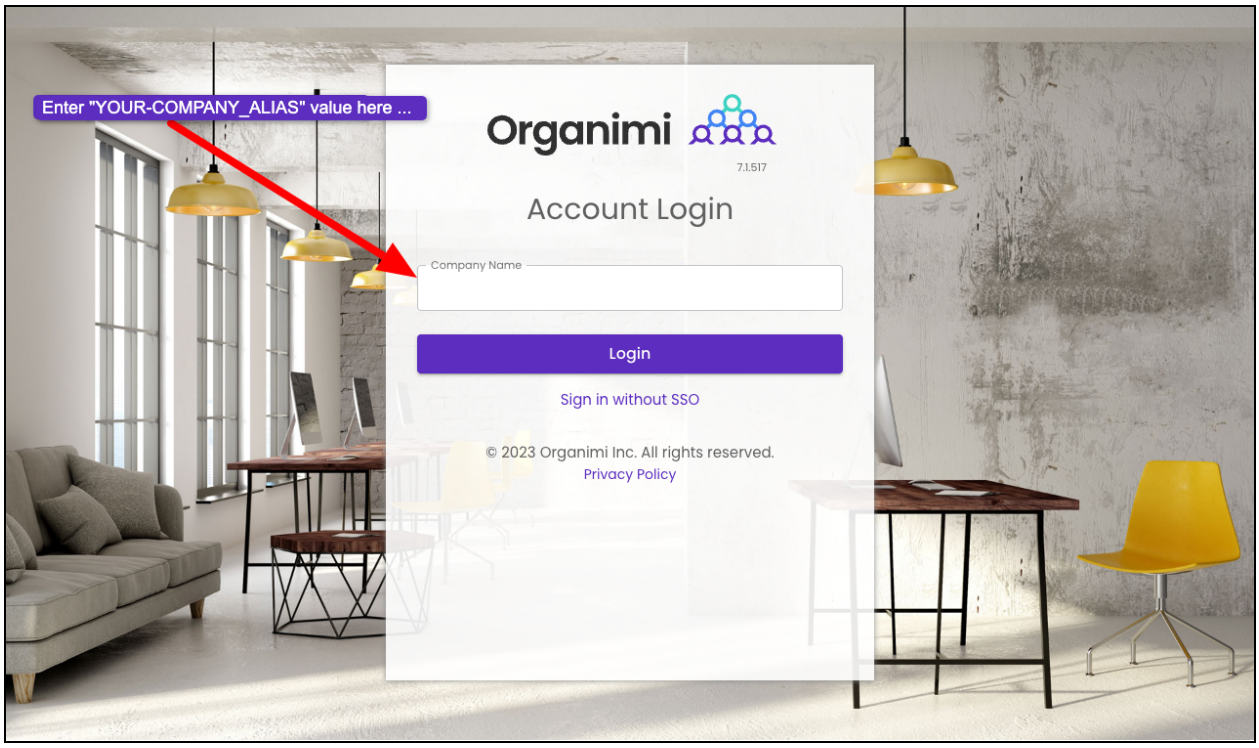
Note: If you do not reach to this point and see an error message on clicking the "SAVE" button, Contact Organimi support @ support@organimi.com

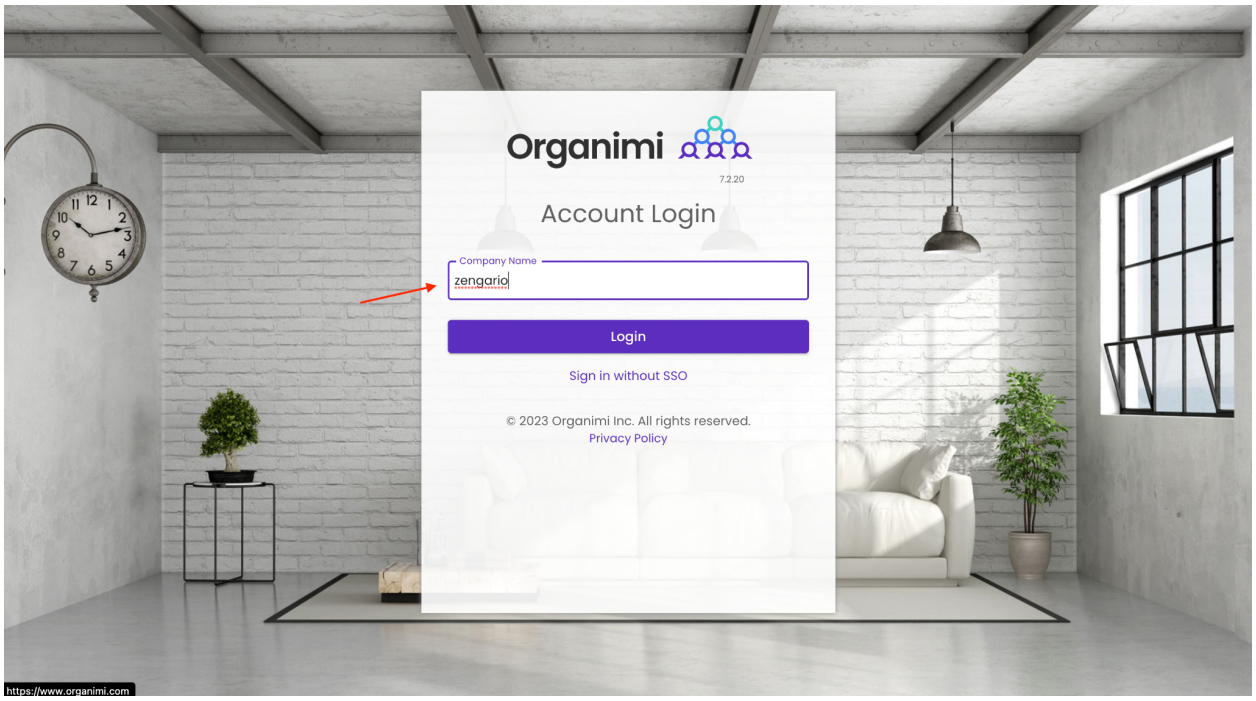
Step 8

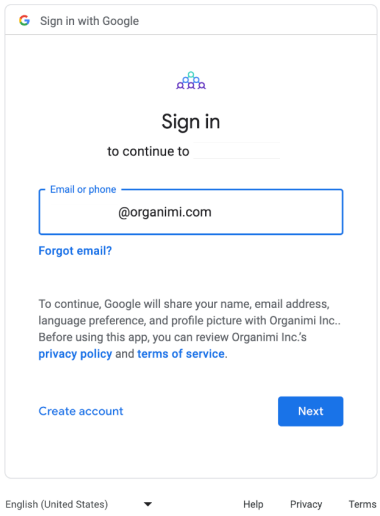
Now it's time to test logging in with your configured IDP. First logout from your account. Then login by clicking “Sign in with SSO”. In the next screen, type in the company name matching from the earlier steps for “`YOUR_COMPANY_ALIAS`” then click login.

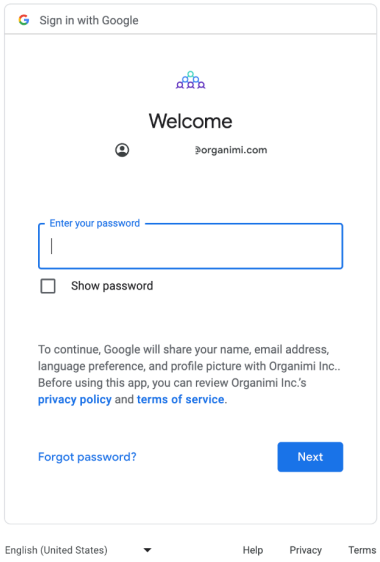
You should be redirected to your Google workspace IDP where you can be authenticated. Once successful, you will be redirected back to Organimi and will be logged in.



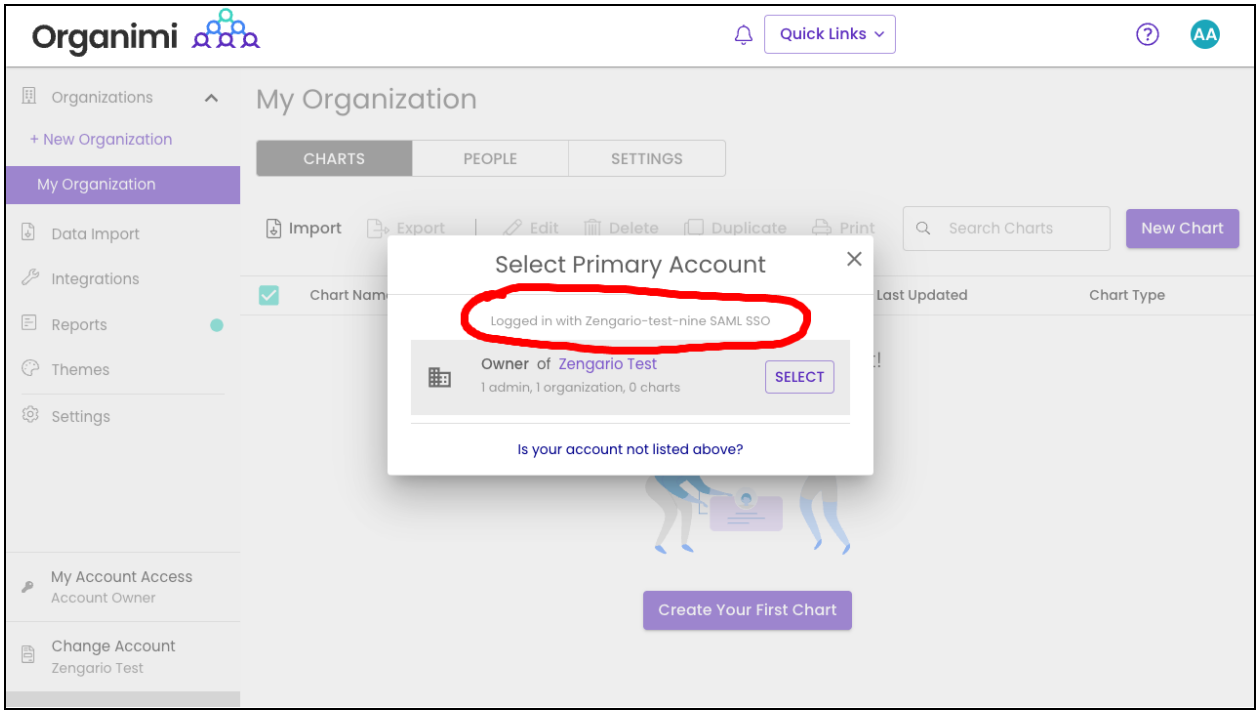

Enter "YOUR-COMPANY_ALIAS" value here ...
Organimi
7.1.517
Account Login
Company Name
Login
Sign in without SSO
© 2023 Organimi Inc. All rights reserved.
Privacy Policy


Organimi
7.2.20
Account Login
Company Name
zengario
Login
Sign in without SSO
© 2023 Organimi Inc. All rights reserved.
Privacy Policy
https://www.organimi.com





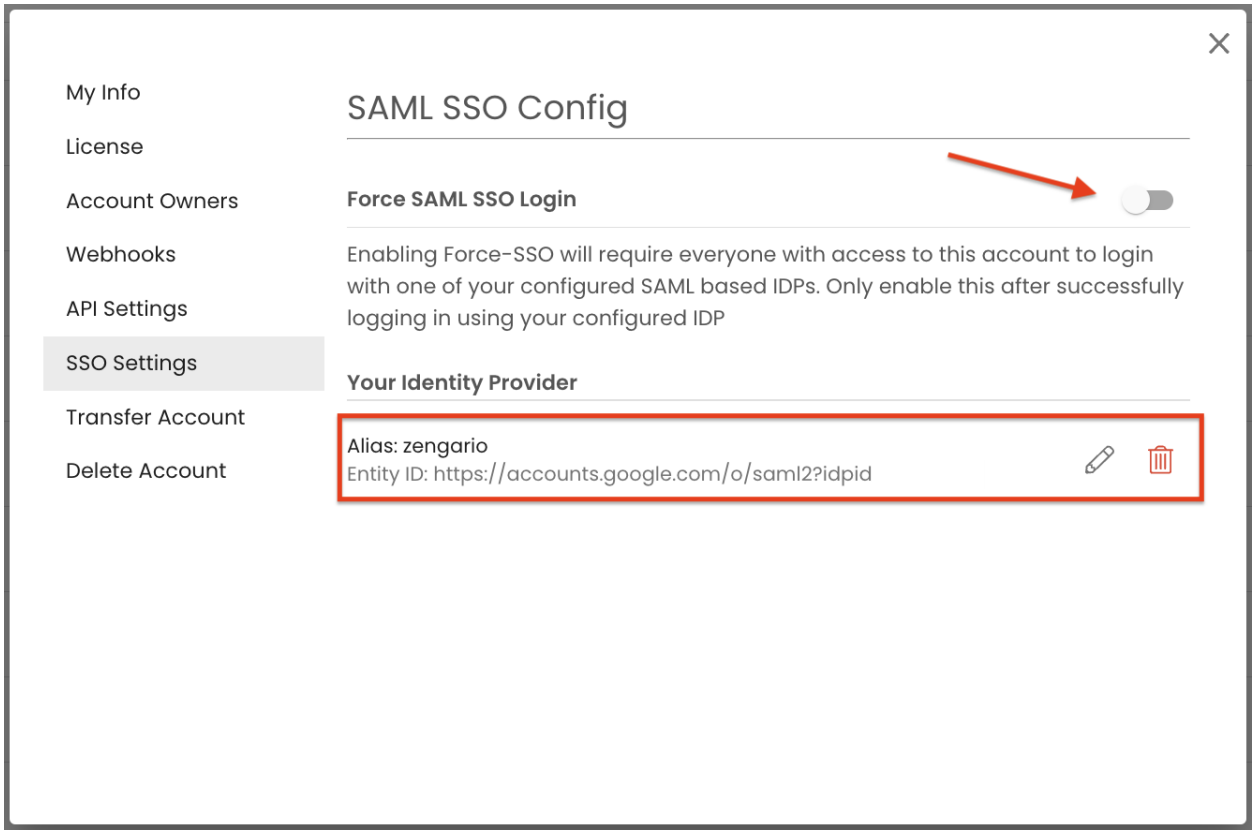
And you are in. If you click the Change Account link on the Organimi screen you will see that you are logged in with SAML SSO

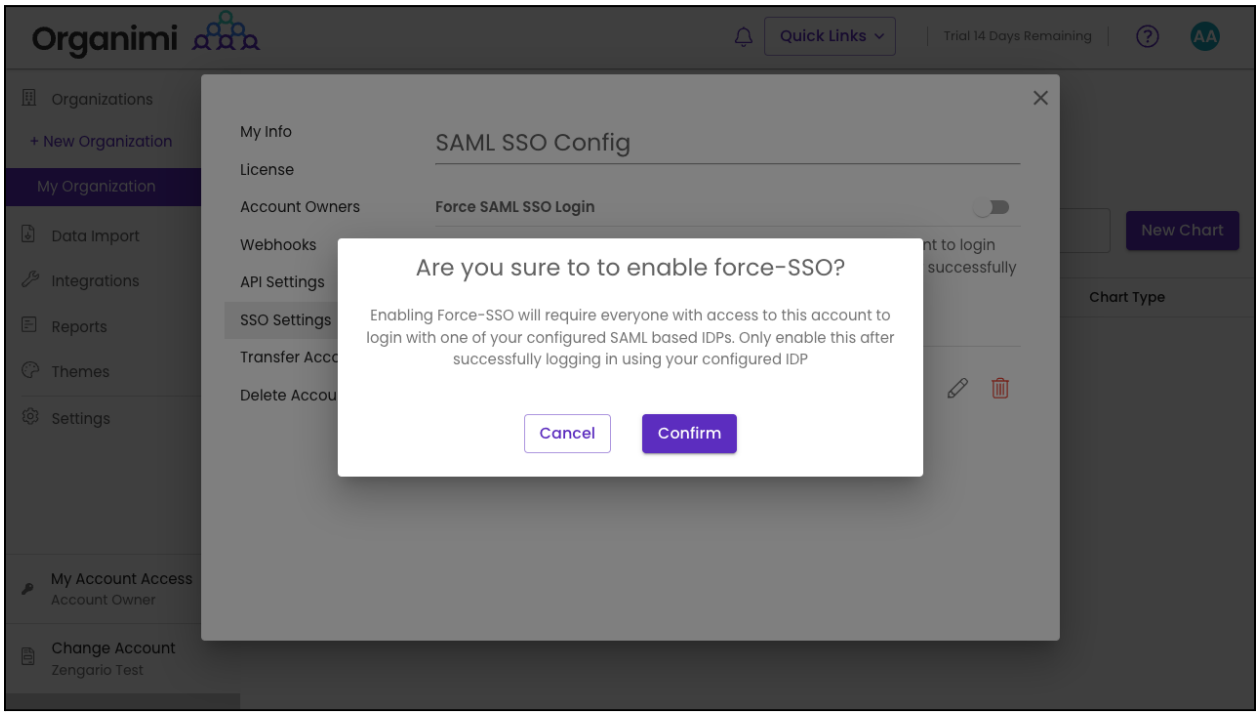


Step 9

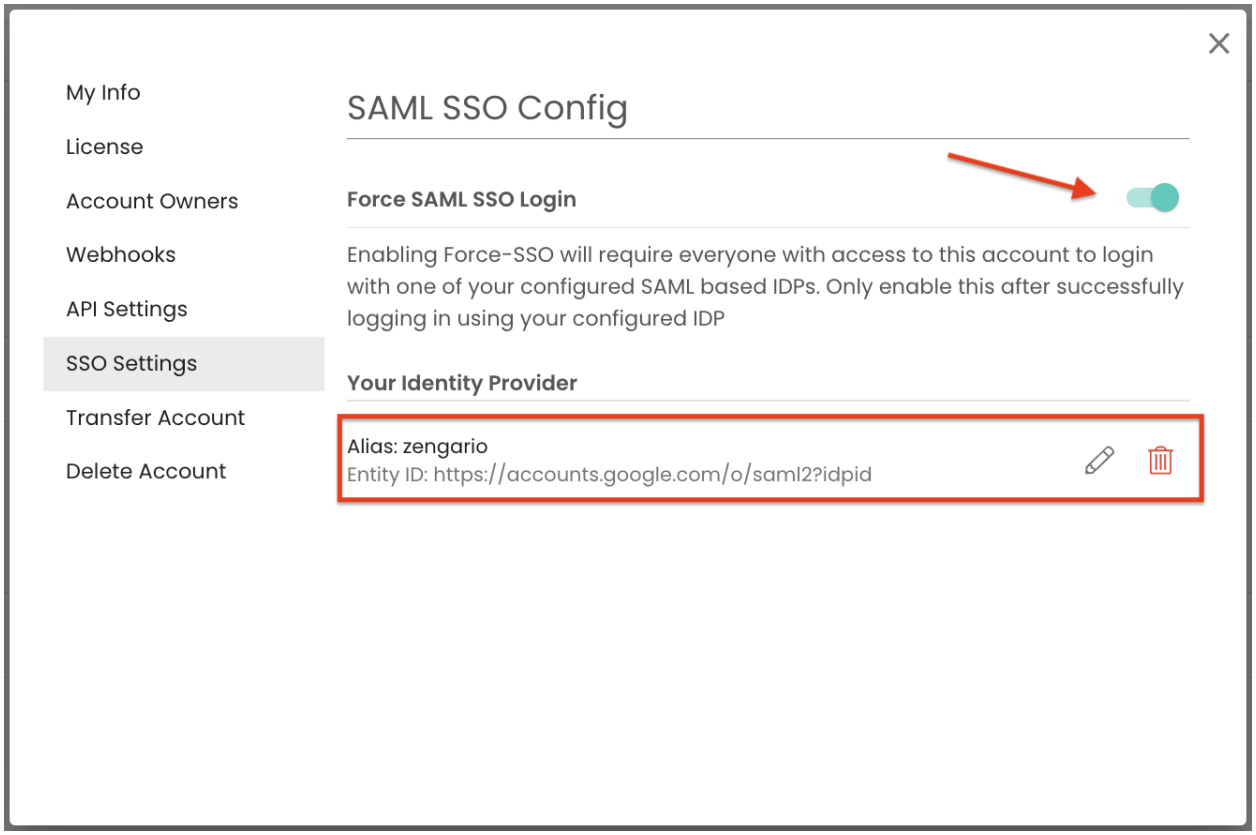
You can also enable “Force-SSO” from the configuration tab. Which will require everyone using this account (including you), to login using your configured IDP only, in order to access resources under this account. Other login methods (social & username/password) will not be allowed access to the account.

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.

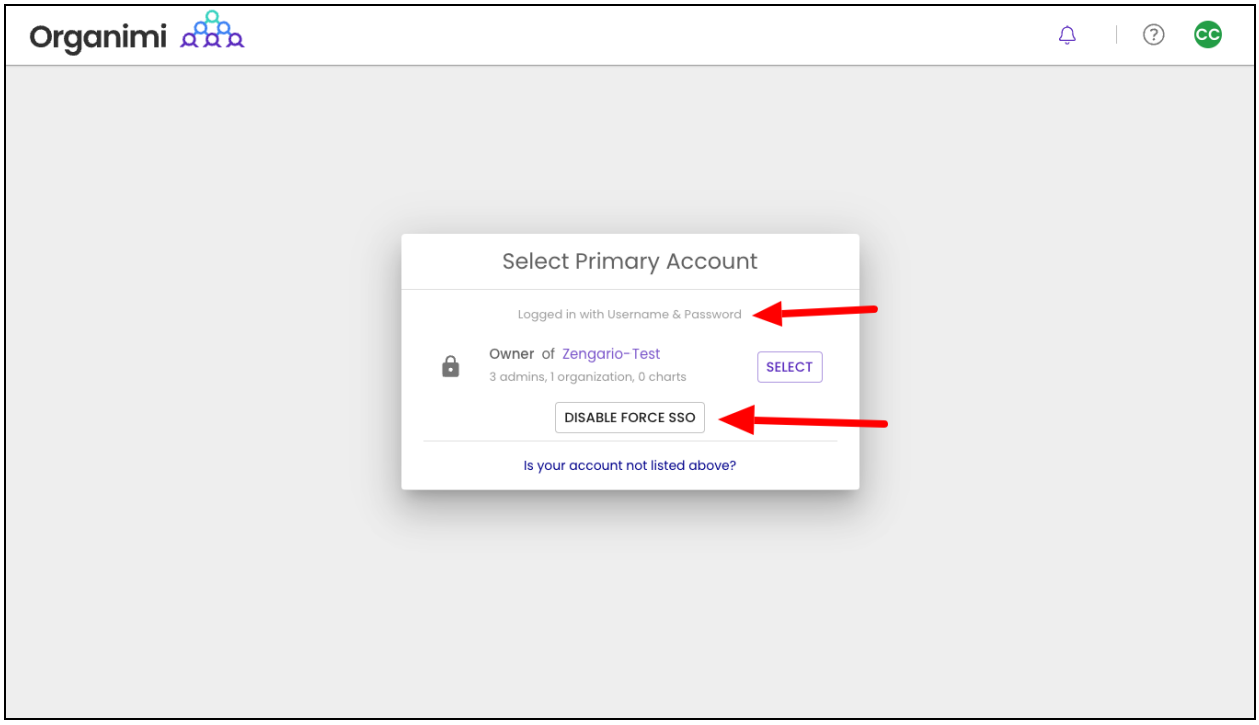

My Info
License
Account Owners
Webhooks
API Settings
SSO Settings
Transfer Account
Delete Account
SAML SSO Config
Force SAML SSO Login
Enabling Force-SSO will require everyone with access to this account to login with one of your configured SAML based IDPs. Only enable this after successfully logging in using your configured IDP
Your Identity Provider
Alias: zengario
Entity ID: https://accounts.google.com/o/saml2?idpid

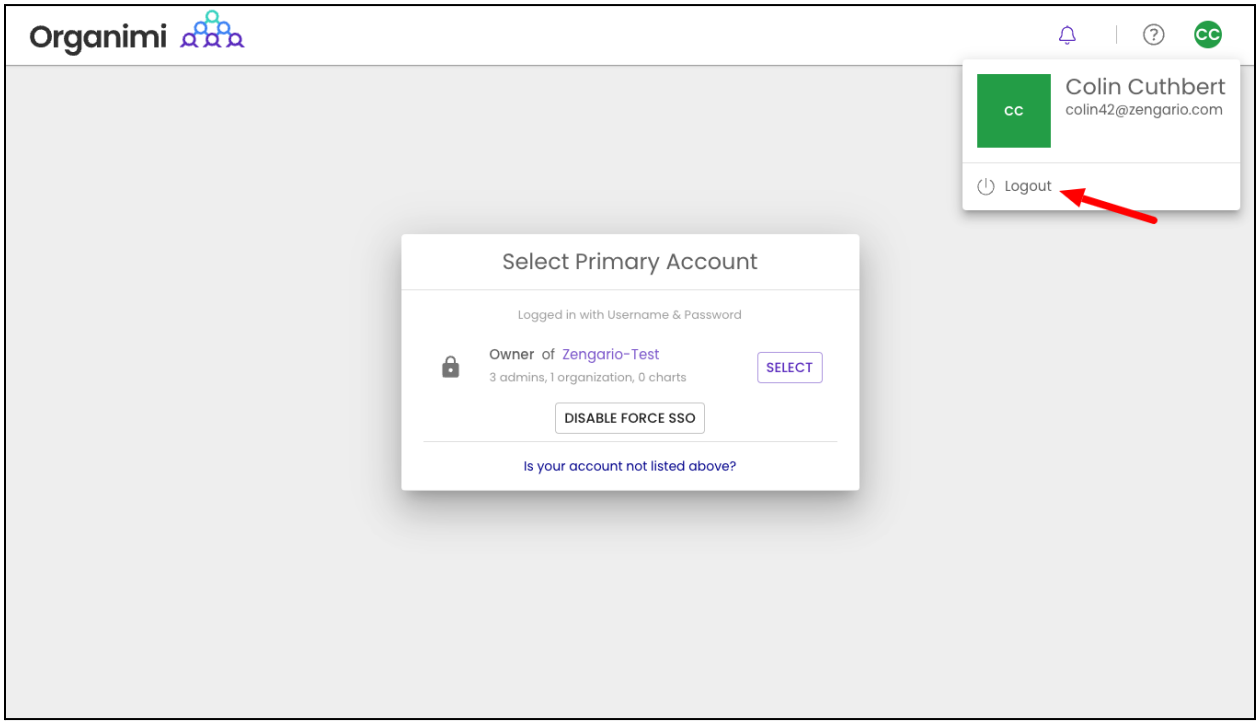

Organimi
Quick Links
Trial 14 Days Remaining
Organizations
+ New Organization
My Organization
Data Import
Integrations
Reports
Themes
Settings
My Account Access
Account Owner
Change Account
Zengario Test
New Chart
Chart Type
My Info
License
Account Owners
Webhooks
API Settings
SSO Settings
Transfer Acco
Delete Accou
SAML SSO Config
Force SAML SSO Login
Are you sure to to enable force-SSO?
Enabling Force-SSO will require everyone with access to this account to login with one of your configured SAML based IDPs. Only enable this after successfully logging in using your configured IDP
Cancel
Confirm

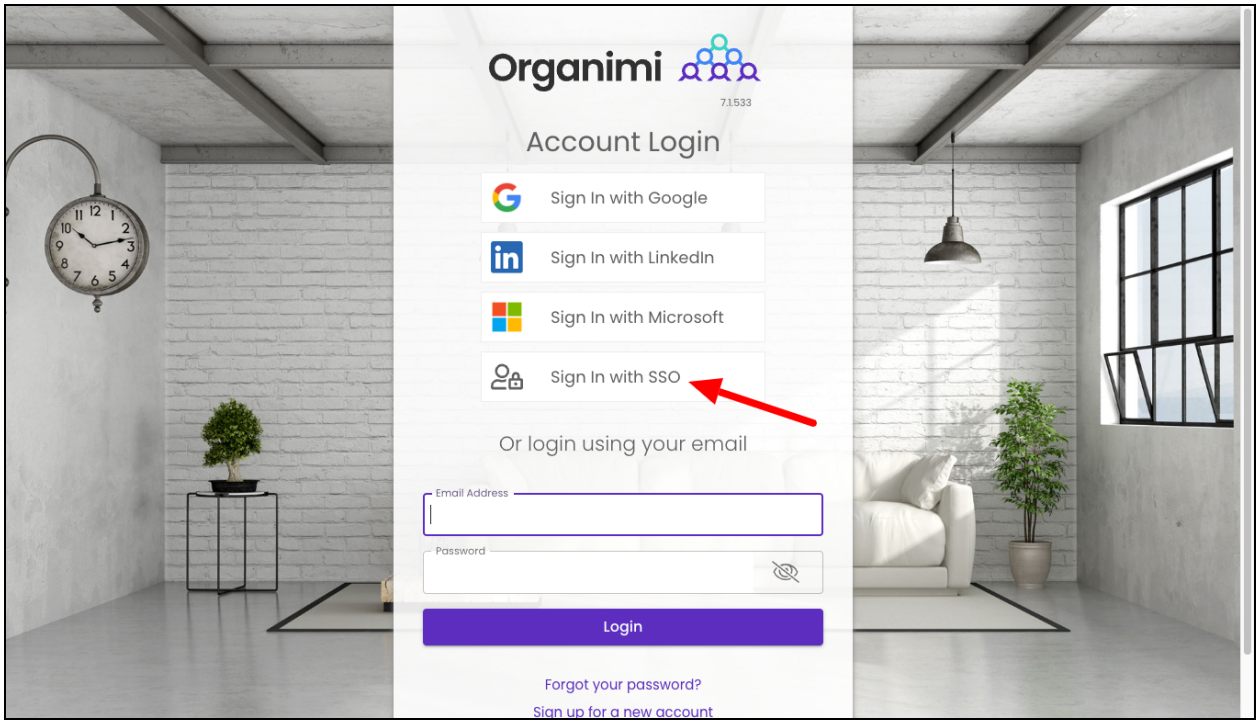
If you were logged into Organimi with you SSO IDP Account then you will just see that the switch is now on for “Force SSO”



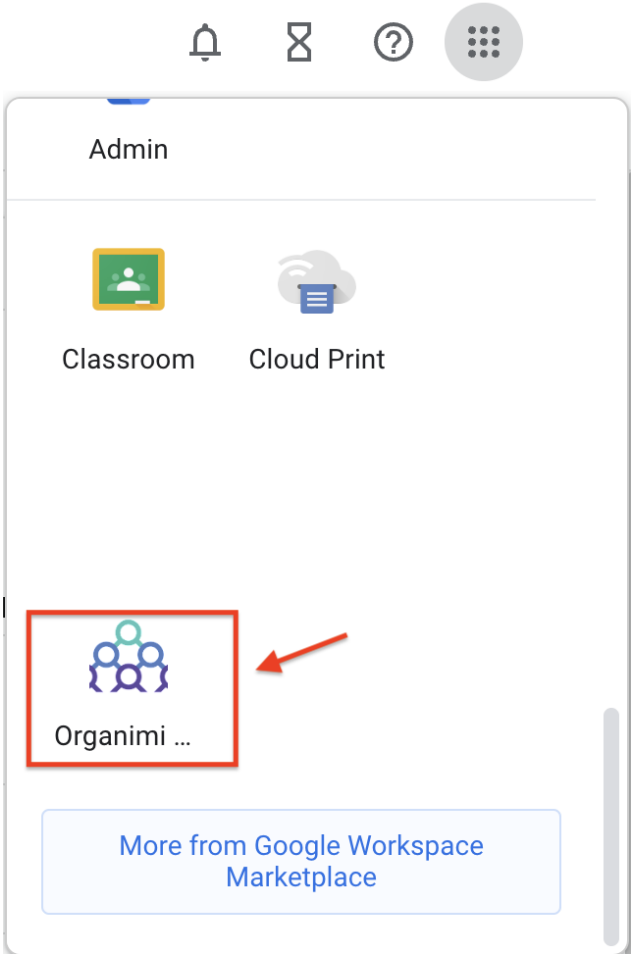
If, however, you were logged in to Organimi with your social login or username/password your access to the account will be immediately disabled and you will be taken to the Account Selection Screen and you will see that your access to the account is locked. You could disable the “Force SSO” (only available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


Organimi
CC
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
CC
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

Note: Now that Organimi access is set up to use SAML based SSO, direct access is available to users from the App Launcher. Users can click on the Organimi icon from the App Launcher icon (9 dots menu) of Google, which will redirect you to the Organimi dashboard.

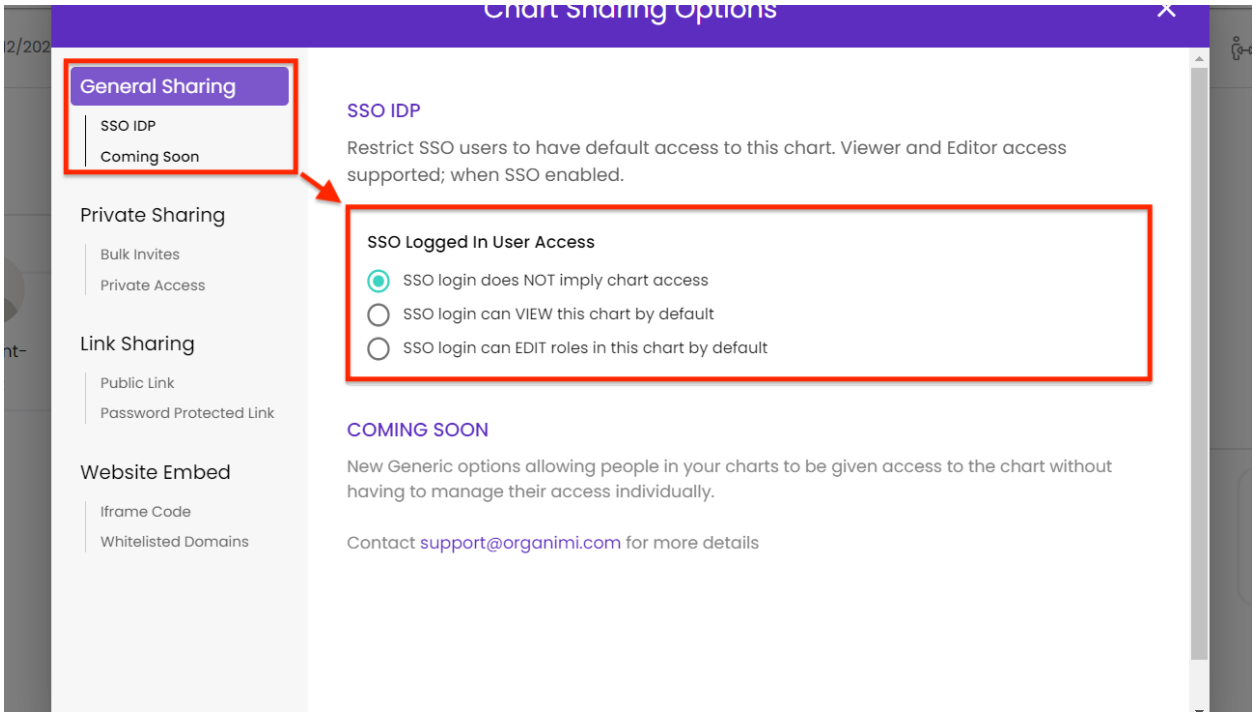


Step 10 - Chart Settings

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.