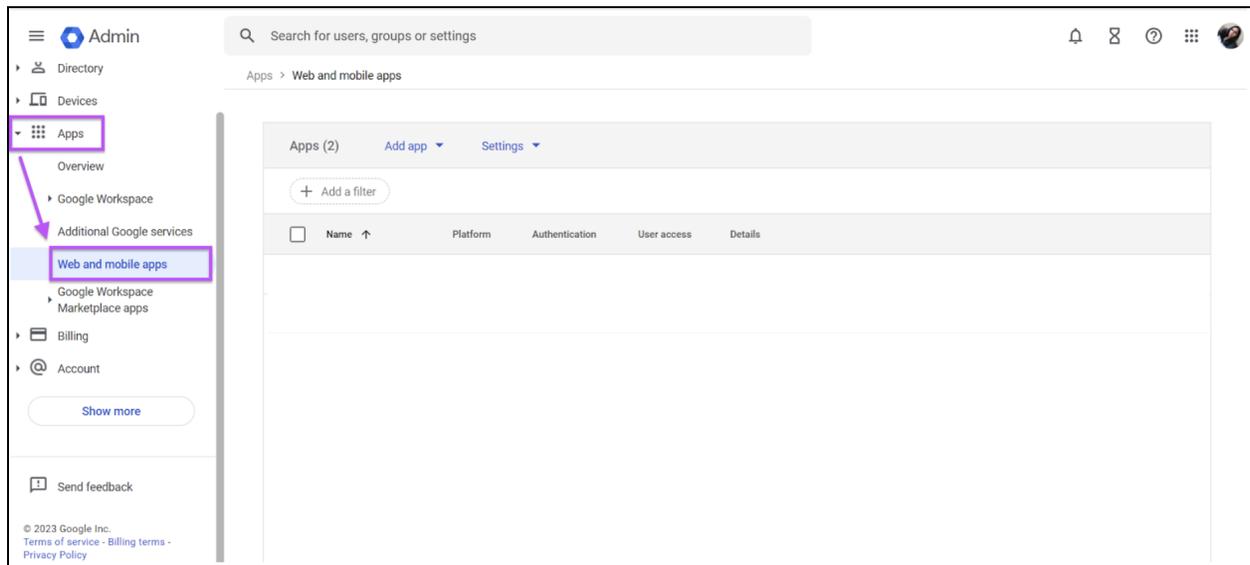


## SAML based SSO - Login with Google Workspace

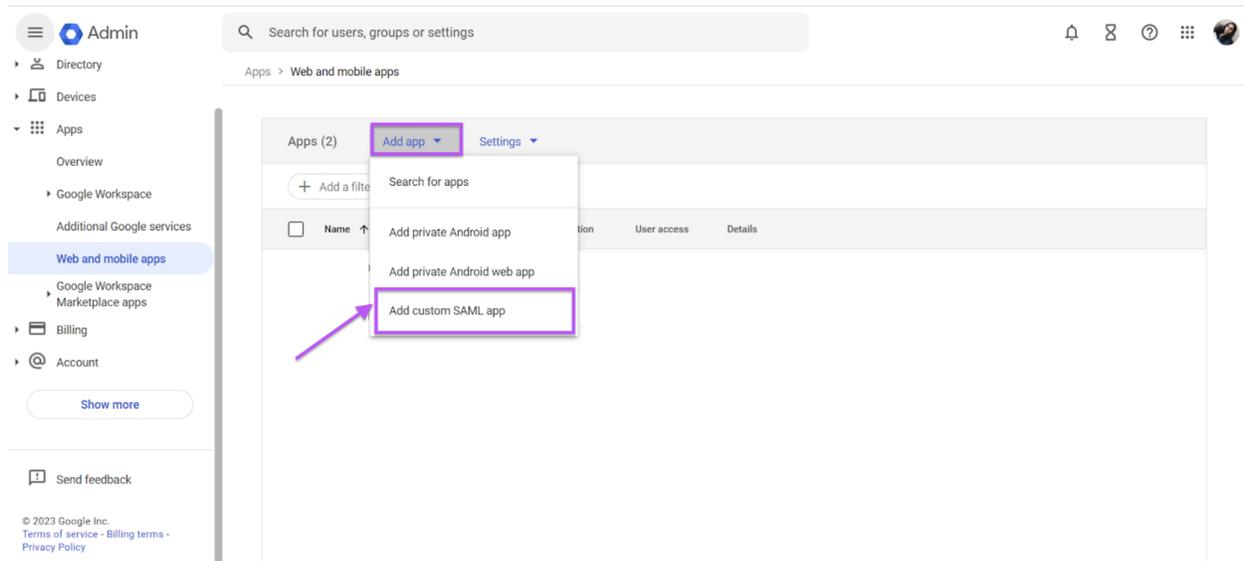
Organimi has implemented SAML based SSO for Premium account holders ... this document will walk you through the steps to set up the integration with Google Workspace

### Step 1

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

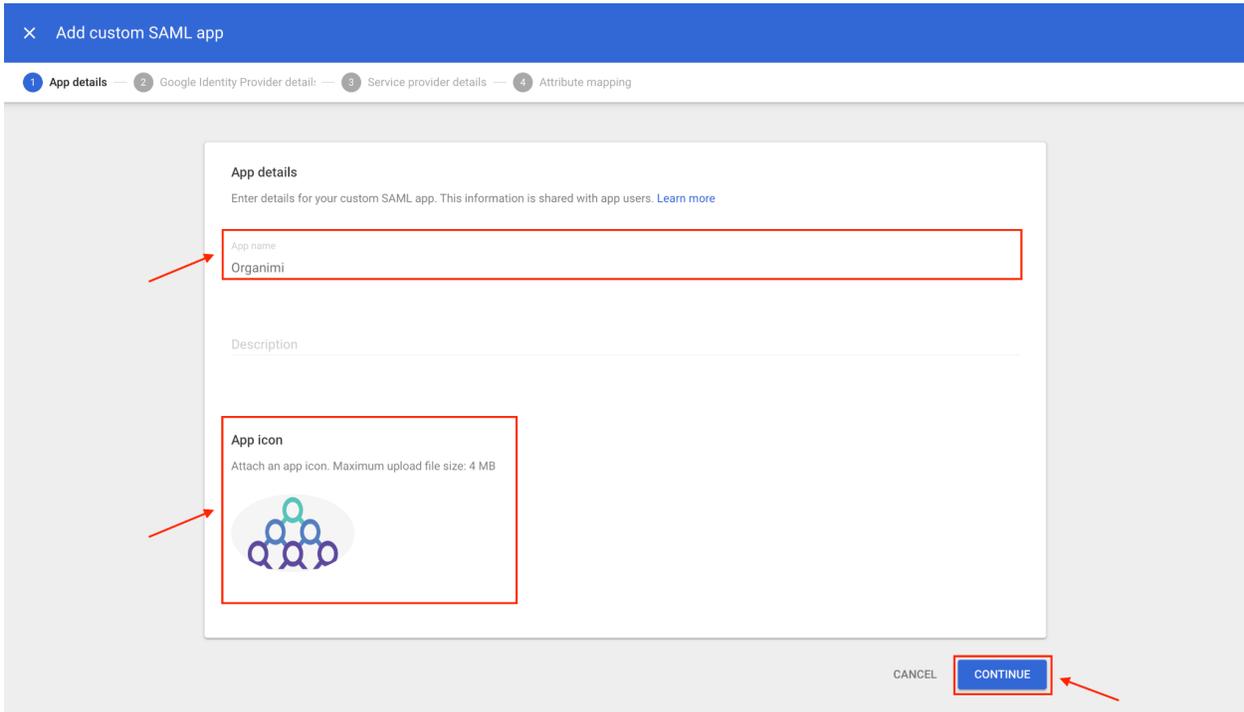


Click on Add app and then “Add custom SAML app”.



## 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.

× Add custom SAML app

Option 1: Download IdP metadata

**DOWNLOAD METADATA**

OR

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL

Entity ID

Certificate

SHA-256 fingerprint

BACK CANCEL **CONTINUE**

## 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.app.organimi.com/api/v7/auth/login/saml/callback>
  - b. Only for AU customers - <https://au.app.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)

The screenshot shows a web interface for configuring a custom SAML application. The page title is 'Add custom SAML app'. The main section is 'Service provider details', which includes a sub-section for 'Name ID'. The 'Service provider details' section contains the following fields and options:

- ACS URL: <https://app.organimi.com/api/v7/auth/login/saml/callback>
- Entity ID: <https://app.organimi.com>
- Start URL (optional): {"company":"YOUR-COMPANY-ALIAS"}
- Signed response

The 'Name ID' section contains the following fields and options:

- Name ID format: EMAIL
- Name ID: Basic Information > Primary email

At the bottom of the form, there are three buttons: 'BACK', 'CANCEL', and 'CONTINUE'. Red arrows in the original image point to the ACS URL, Entity ID, Start URL, Name ID format, Name ID, and the CONTINUE button.

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 screenshot shows the 'Add custom SAML app' configuration page. The main section is titled 'Attributes' and contains a table for mapping Google Directory attributes to App attributes. Three mappings are shown: 'First name' to 'firstname', 'Last name' to 'lastname', and 'Primary email' to 'email'. Each mapping is highlighted with a red box and a red arrow. Below the mappings is an 'ADD MAPPING' button. The bottom section is titled 'Group membership (optional)' and contains a search for groups and an 'App attribute' field. At the bottom of the page, there are 'BACK', 'CANCEL', and 'FINISH' buttons. The 'FINISH' button is highlighted with a red box and a red arrow.

**Attributes**  
Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with \* are mandatory. [Learn more](#)

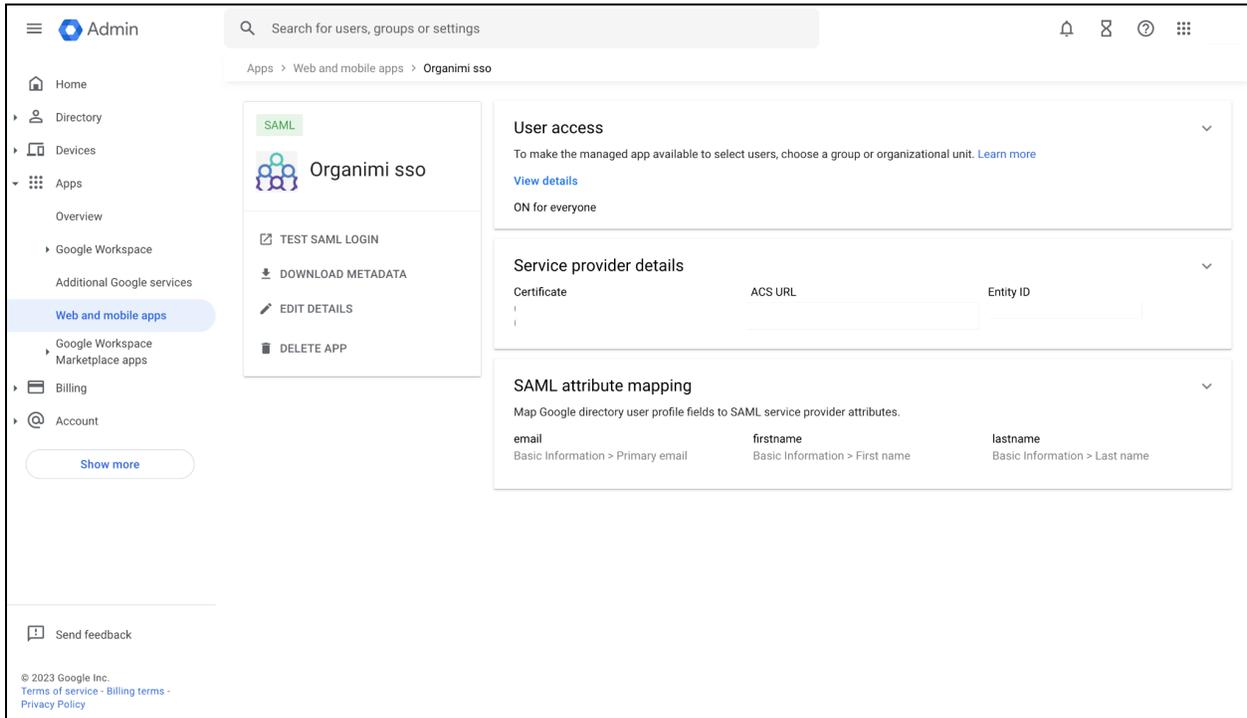
| Google Directory attributes          | App attributes |
|--------------------------------------|----------------|
| Basic Information ><br>First name    | firstname      |
| Basic Information ><br>Last name     | lastname       |
| Basic Information ><br>Primary email | email          |

**Group membership (optional)**  
Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.

| Google groups      | App attribute |
|--------------------|---------------|
| Search for a group | Groups        |

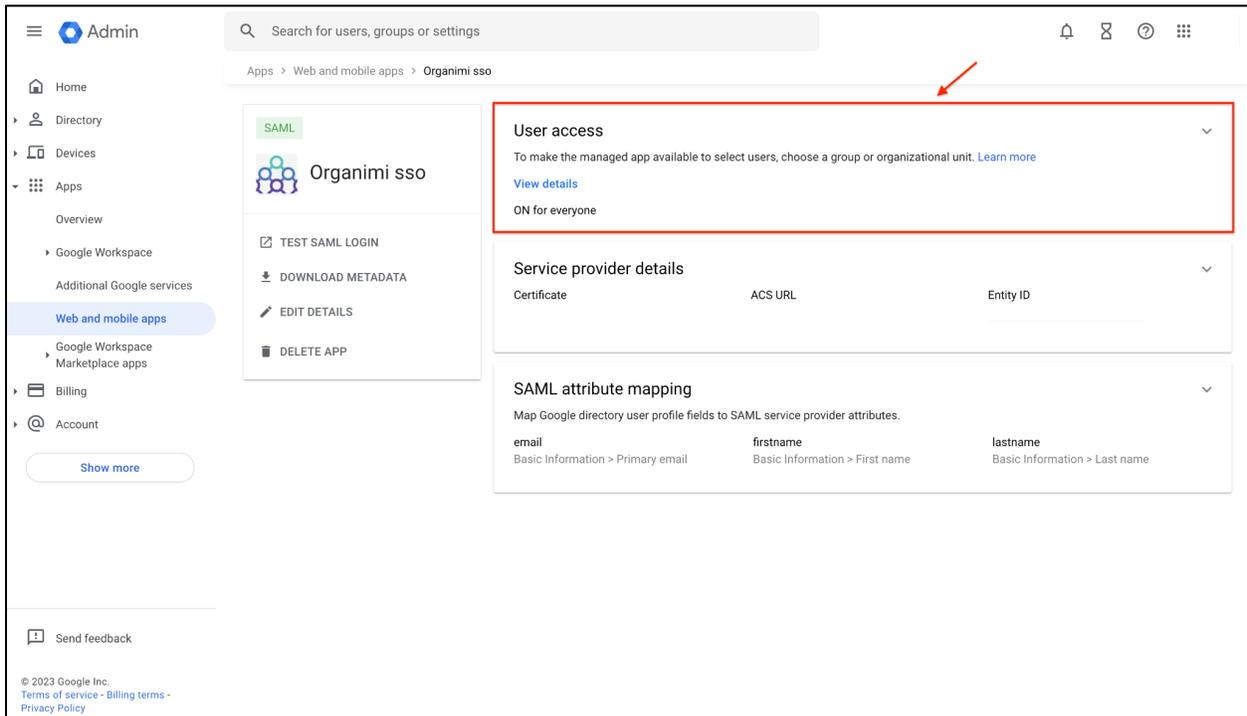
BACK CANCEL **FINISH**

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”.

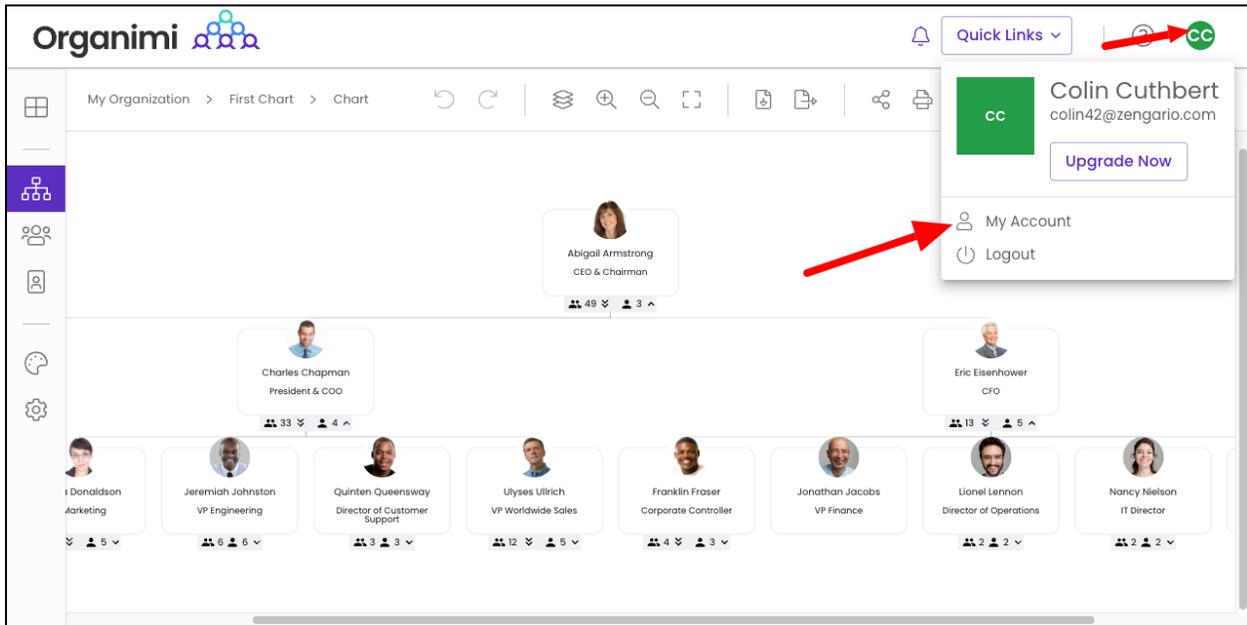


Click on “ON for everyone” for Service status or select groups that need to be granted access, and then click on “SAVE”.

The screenshot displays the Google Admin console interface for the 'Organimi sso' application. The left sidebar shows navigation options like Home, Directory, Devices, Apps, and Billing. The main content area is titled 'Organimi sso' and shows settings for 'All users in this account'. The 'Service status' section has two radio buttons: 'ON for everyone' (selected) and 'OFF for everyone'. A red box highlights the 'ON for everyone' option, with a red arrow pointing to it. Below the radio buttons, there is a message: 'Most changes take effect in a few minutes. [Learn more](#)'. At the bottom right, there is a '1 unsaved change' indicator, a 'CANCEL' button, and a 'SAVE' button. The 'SAVE' button is highlighted with a red box, and a red arrow points to it. The 'Groups' dropdown menu is open, showing 'All users in this account' and 'Organizational Units'.

## 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.



The screenshot displays the Organimi application interface. At the top left is the Organimi logo. The main header shows the navigation path: "My Organization > First Chart > Chart". A user profile dropdown menu is open in the top right corner, showing the user's name "Colin Cuthbert" and email "colin42@zengario.com". The dropdown menu includes an "Upgrade Now" button and two options: "My Account" and "Logout". A red arrow points to the "My Account" option. Another red arrow points to a green circular profile icon in the top right corner of the application. The main content area shows a hierarchical organizational chart with several employee cards, each displaying a name, title, and a small group icon.

*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.

The screenshot shows the 'SAML SSO Config' interface. On the left is a navigation menu with 'SSO Settings' selected. The main area is divided into two sections: 'Service Provider Metadata' and 'Your Identity Provider'. The 'Service Provider Metadata' section contains fields for Callback URL, SP Entity ID, Default Relay State, and Required Attributes, each with an information icon and a copy icon. A 'Download (.xml)' button is also present. The 'Your Identity Provider' section contains fields for Company Alias, SSO URL, Entity ID, and X509 Certificate. The 'Company Alias' field is highlighted with a red box and a red arrow labeled '1'. To the right of this field is a 'drop area' highlighted with a red box, containing the text 'Have your IDP's metadata XML?' and icons for 'paste' and 'drop'. A red arrow labeled '2' points from the X509 Certificate field to the drop area. At the bottom right are 'CANCEL' and 'SAVE' buttons.

My Info

License

Account Owners

Webhooks

API Settings

**SSO Settings**

Transfer Account

Delete Account

### SAML SSO Config

**Service Provider Metadata** [Setup Instructions](#)

Callback URL

SP Entity ID

Default Relay State

Required Attributes

[Download \(.xml\)](#)

**Your Identity Provider**

Company Alias

SSO URL

Entity ID

X509 Certificate

Have your IDP's metadata XML?

or

**1** →

**2** →

[CANCEL](#) [SAVE](#)

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

My Info

License

Account Owners

Webhooks

API Settings

**SSO Settings**

Transfer Account

Delete Account

## SAML SSO Config

**Service Provider Metadata** [Setup Instructions](#)

Callback URL

SP Entity ID

Default Relay State

Required Attributes

[Download \(.xml\)](#)

**Your Identity Provider**

Company Alias

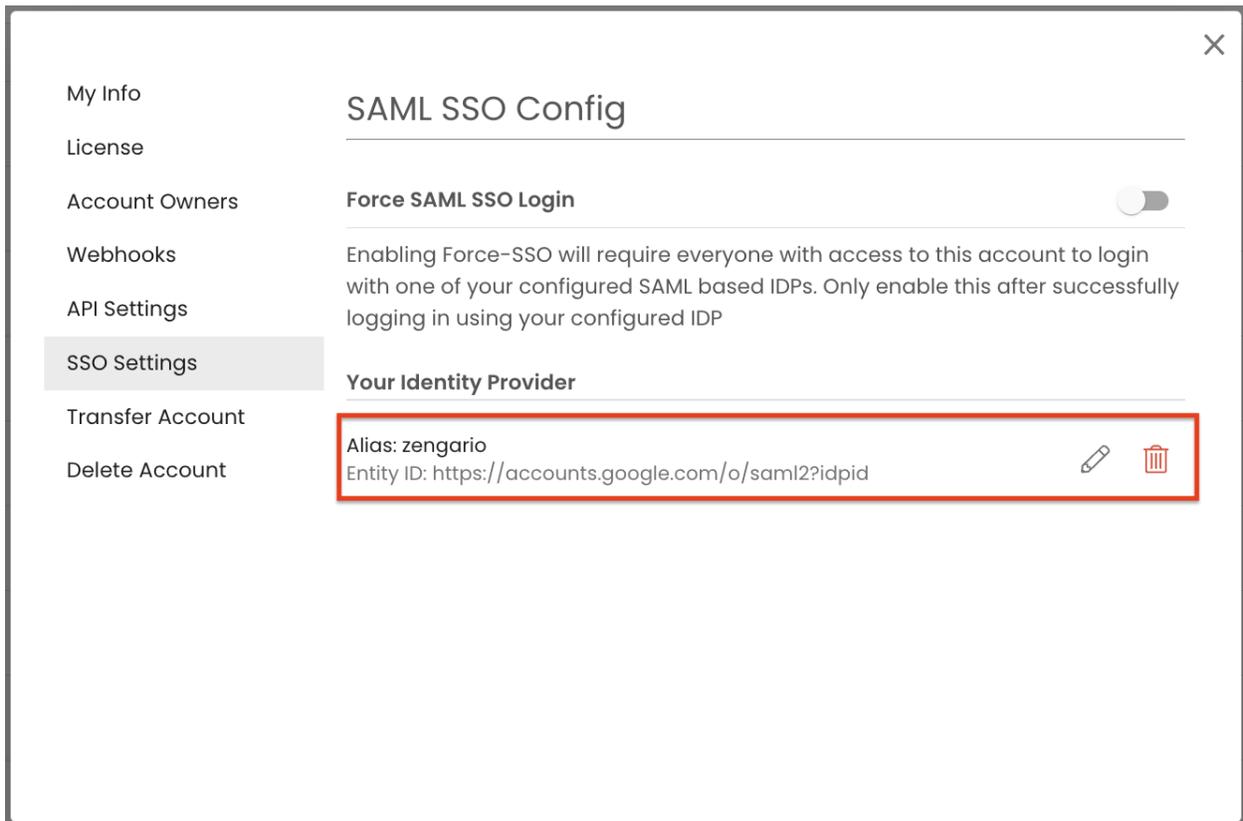
SSO URL

Entity ID

X509 Certificate

Great! we pre-filled the form for you. Please recheck if everything looks good, then submit

Google Workspace is now set up as the Identity Provider



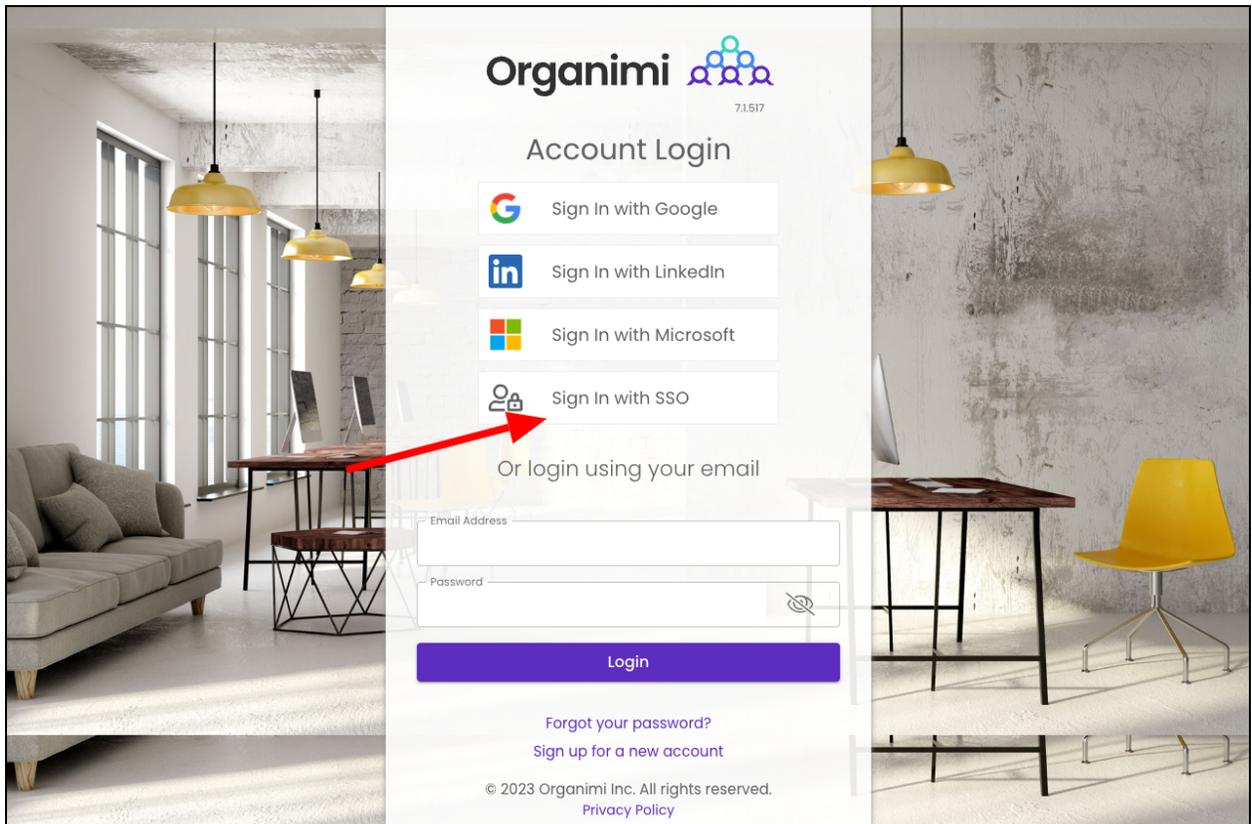
The screenshot displays the 'SAML SSO Config' page in the Google Workspace Admin console. On the left is a navigation menu with options: My Info, License, Account Owners, Webhooks, API Settings, SSO Settings (highlighted), Transfer Account, and Delete Account. The main content area is titled 'SAML SSO Config' and includes a toggle for 'Force SAML SSO Login' which is currently turned on. Below this is a descriptive text: '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'. The 'Your Identity Provider' section contains two fields: 'Alias: zengario' and 'Entity ID: https://accounts.google.com/o/saml2?idpid'. A red rectangular box highlights these two fields, and to their right are icons for editing (pencil) and deleting (trash).

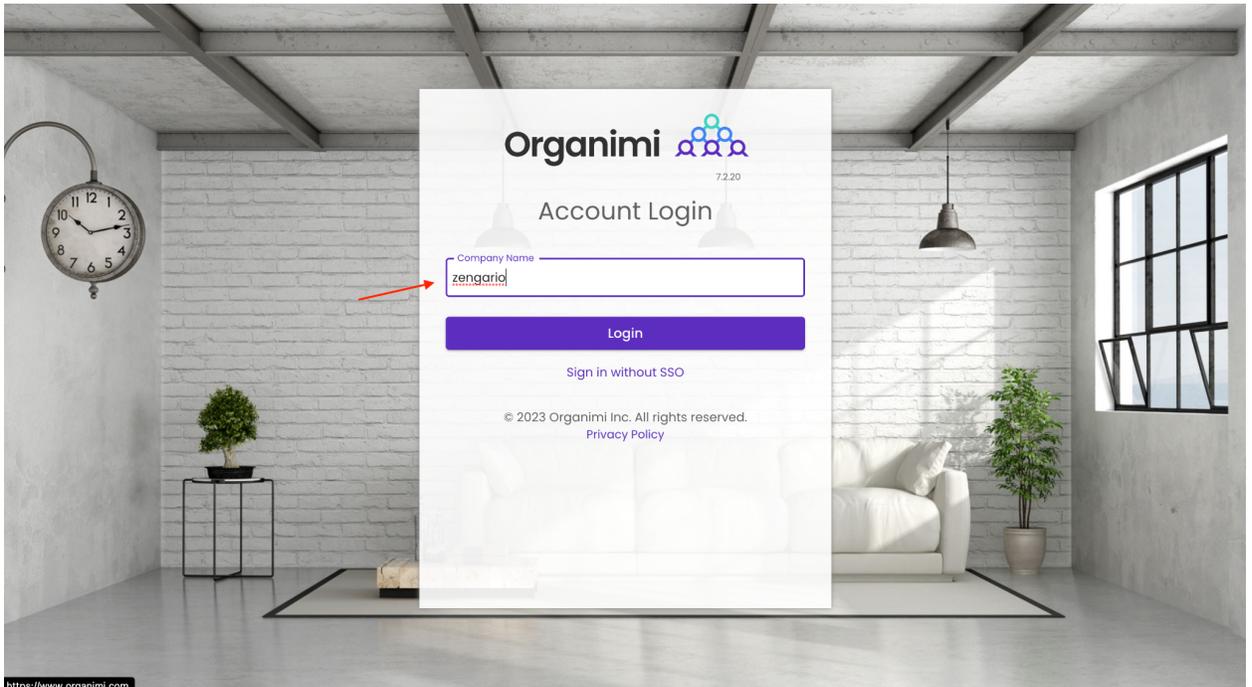
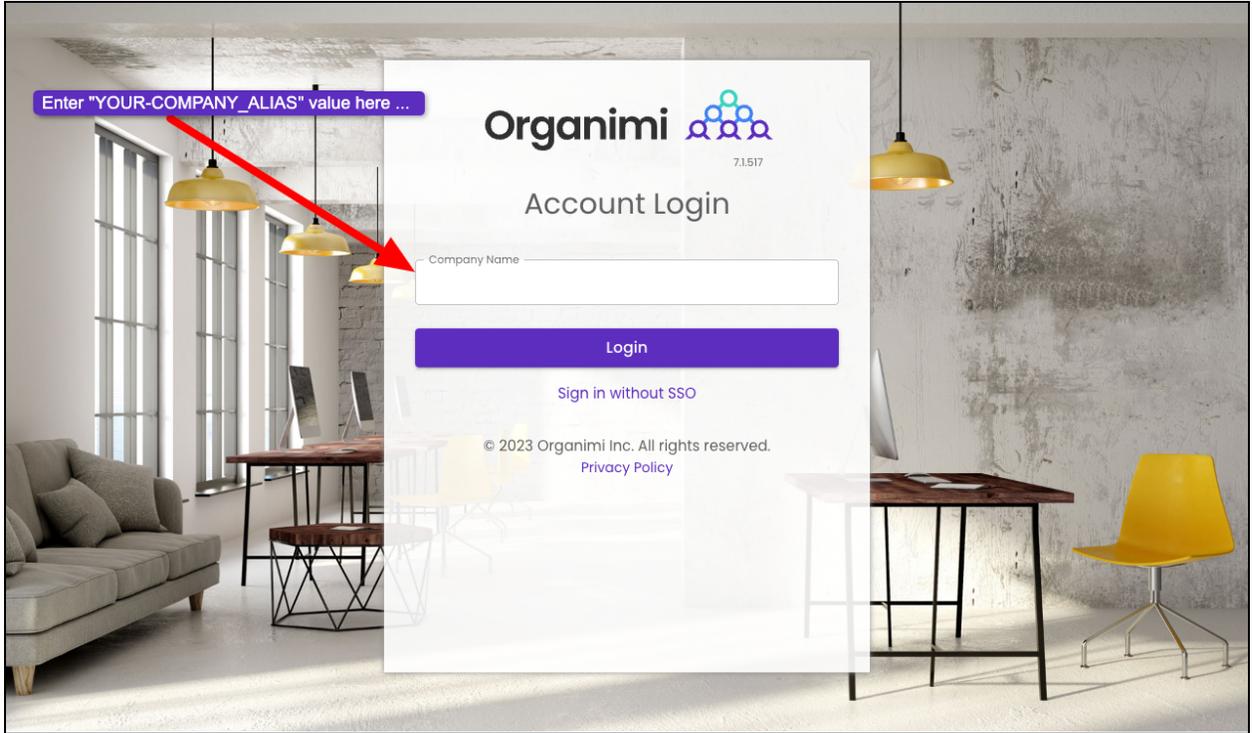
*Note: If you do not reach to this point and see an error message on clicking the "SAVE" button, Contact Organimi support @ [support@organimi.com](mailto:support@organimi.com)*

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





Sign in with Google



### Sign in

to continue to \_\_\_\_\_

Email or phone

[Forgot email?](#)

To continue, Google will share your name, email address, language preference, and profile picture with Organimi Inc.. Before using this app, you can review Organimi Inc.'s [privacy policy](#) and [terms of service](#).

[Create account](#) [Next](#)

English (United States) Help Privacy Terms

Sign in with Google



### Welcome

 @organimi.com

Enter your password

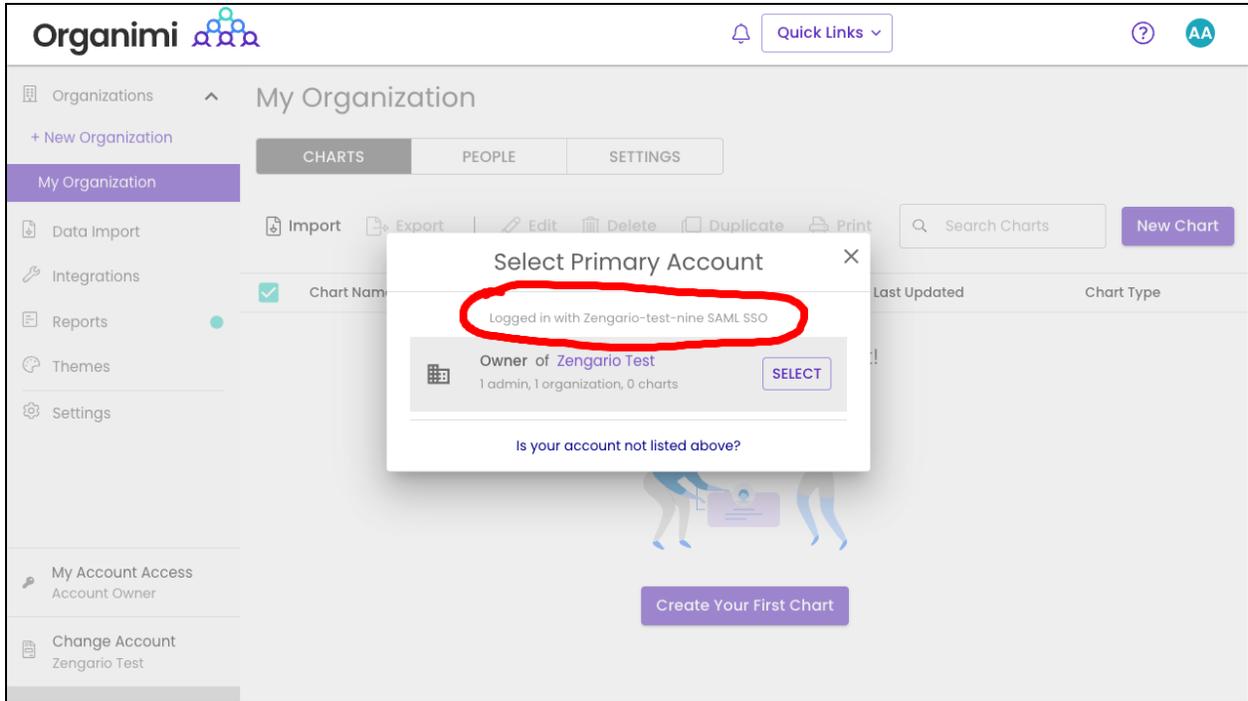
Show password

To continue, Google will share your name, email address, language preference, and profile picture with Organimi Inc.. Before using this app, you can review Organimi Inc.'s [privacy policy](#) and [terms of service](#).

[Forgot password?](#) [Next](#)

English (United States) Help Privacy Terms

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

## 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

Alias: zengario  
Entity ID: <https://accounts.google.com/o/saml2?idpid>  

**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

New Chart

Chart Type

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”

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>

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.

### Select Primary Account

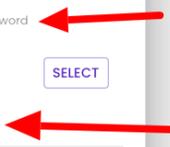
Logged in with Username & Password

 Owner of **Zengario-Test**  
3 admins, 1 organization, 0 charts

[SELECT](#)

[DISABLE FORCE SSO](#)

[Is your account not listed above?](#)



### 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?](#)

 **Colin Cuthbert**  
colin42@zengario.com

 Logout





## 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

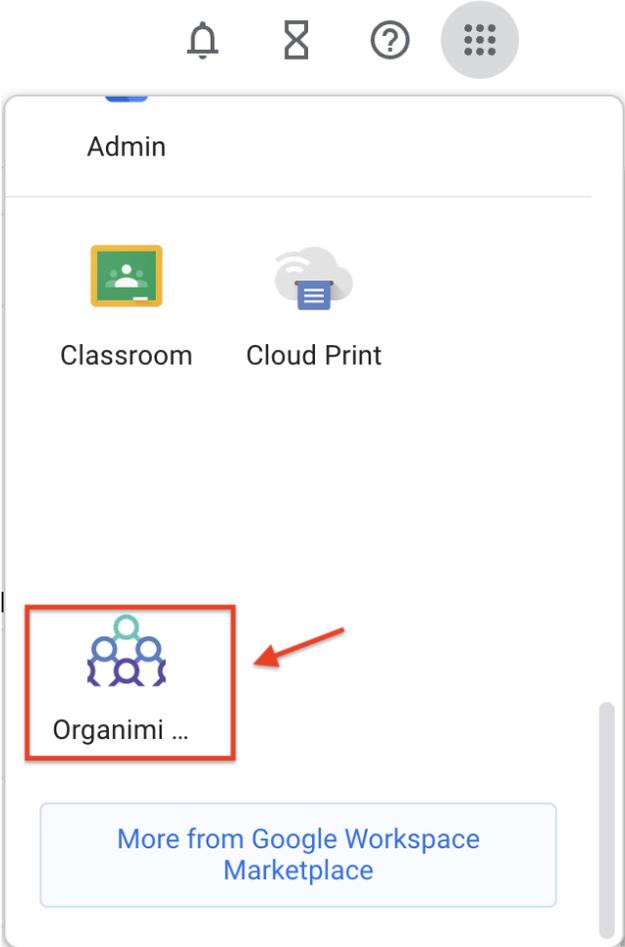
Password  

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.

**Chart Sharing Options**

**General Sharing**

- SSO IDP
- Coming Soon

**Private Sharing**

- Bulk Invites
- Private Access

**Link Sharing**

- Public Link
- Password Protected Link

**Website Embed**

- Iframe Code
- Whitelisted Domains

**SSO IDP**

Restrict SSO users to have default access to this chart. Viewer and Editor access supported; when SSO enabled.

**SSO Logged In User Access**

- SSO login does NOT imply chart access
- SSO login can VIEW this chart by default
- SSO login can EDIT roles in this chart by default

**COMING SOON**

New Generic options allowing people in your charts to be given access to the chart without having to manage their access individually.

Contact [support@organimi.com](mailto:support@organimi.com) for more details

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.

The screenshot shows the Organimi web application interface. At the top left is the Organimi logo. At the top right, there are navigation icons for notifications, help, and a user profile dropdown. The user profile dropdown is open, showing the name 'Danica Donaldson', email 'ddl01@zengario.com', and a 'Logout' button. In the center, a 'Select Primary Account' dialog box is displayed. It shows the user is logged in with 'Zengario-test-nine SAML SSO'. Below this, the text 'No Accounts Found' is circled in red, followed by the question 'Were you invited to Organimi under another email?'. Below this is a link that says 'Is your account not listed above?'. Further down, there is explanatory text: 'You may have been invited under a different email. If you know the account owner's contact, enter their email below and we can inform them you would like account access.' At the bottom of the dialog, there is an input field labeled 'Owner Email' with the placeholder text 'Account Owner Email' and a green 'REQUEST ACCESS' button.