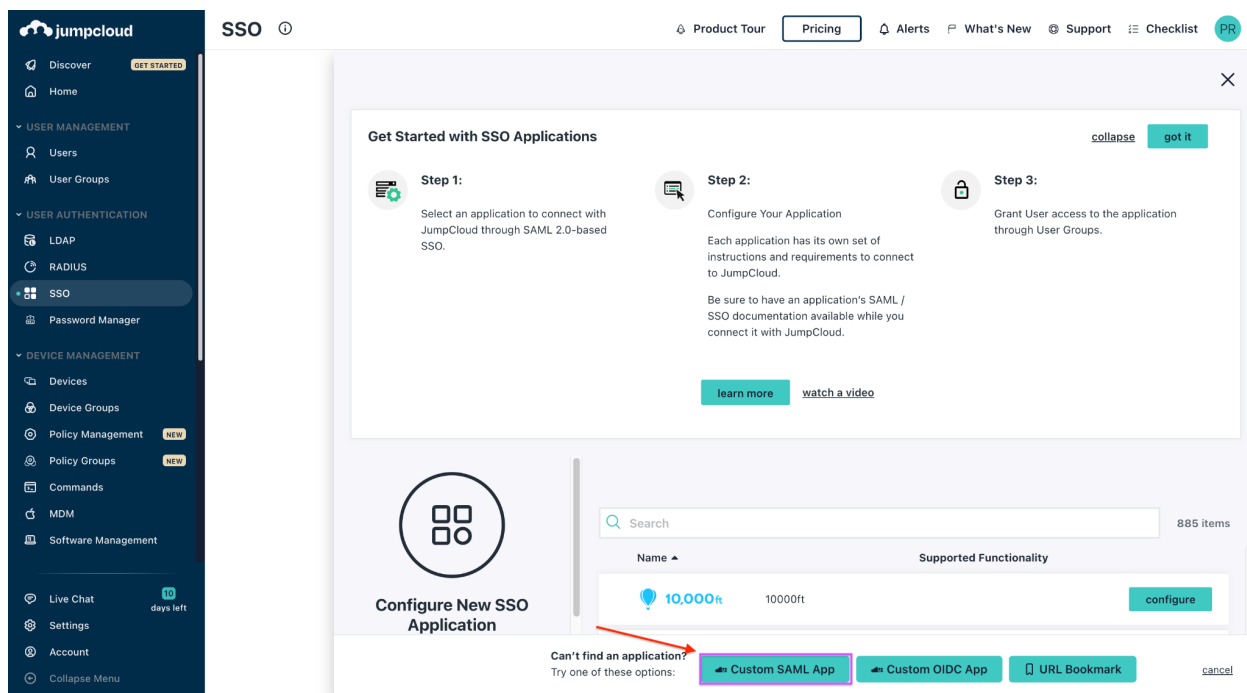


## SAML based SSO - Login with Jumpcloud

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

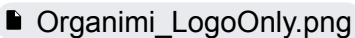
### Step 1

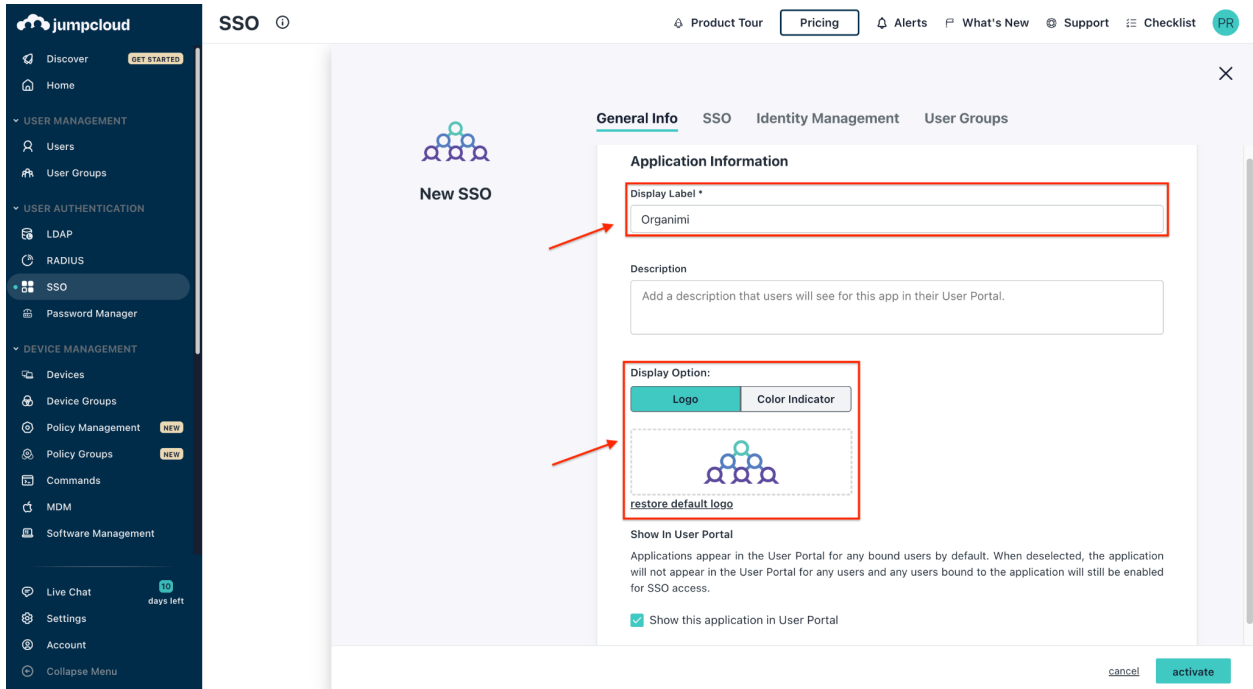
Go to your Jumpcloud dashboard and click “Custom SAML App” from the SSO tab



The screenshot shows the Jumpcloud SSO dashboard. On the left is a dark blue sidebar with navigation options: Discover (GET STARTED), Home, USER MANAGEMENT (Users, User Groups), USER AUTHENTICATION (LDAP, RADIUS, SSO, Password Manager), DEVICE MANAGEMENT (Devices, Device Groups, Policy Management, Policy Groups, Commands, MDM, Software Management), Live Chat (10 days left), Settings, Account, and Collapse Menu. The main content area is titled 'SSO' and contains a 'Get Started with SSO Applications' section with three steps: Step 1 (Select an application to connect with JumpCloud through SAML 2.0-based SSO), Step 2 (Configure Your Application), and Step 3 (Grant User access to the application through User Groups). Below this is a 'Configure New SSO Application' section with a search bar and a list of applications. A red arrow points to the 'Custom SAML App' button in the 'Can't find an application?' section.

### Step 2

Under General Info, enter Display Label as “Organimi”, upload Organimi’s logo and click next (you can download the Organimi logo at: )



### Step 3

Click on SSO and enter the following information

1. IdP Entity ID: YOUR-COMPANY-ALIAS
2. Audience URI (SP 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>
3. Single sign-on URL: <https://app.organimi.com/api/v7/auth/login/saml/callback>
4. Default Relay State: {"company": "YOUR-COMPANY-ALIAS"}
  - a. **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.**
5. Name ID format: EmailAddress

**(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 Jumpcloud. Configure them under "Attribute Statements (optional)". The name should be all lowercase, and the value should be matched accordingly.

1. email
2. firstname
3. lastname

**jumpcloud**

- Discover **GET STARTED**
- Home
- USER MANAGEMENT
  - Users
  - User Groups
- USER AUTHENTICATION
  - LDAP
  - RADIUS
  - SSO**
  - Password Manager
- DEVICE MANAGEMENT
  - Devices
  - Device Groups
  - Policy Management **NEW**
  - Policy Groups **NEW**
  - Commands
  - MDM
  - Software Management
- Live Chat **1** days left
- Settings
- Account

**SSO** ⓘ

Product Tour Pricing Alerts What's New Support Checklist **PR**

Configured App **SAML 2.0**

+ Add New Application

General Info **SSO** Identity Management User Groups

JumpCloud Metadata:
 

- Export Metadata ↓
- Copy Metadata URL ↗

Service Provider Metadata:
 

- Upload Metadata

IdP Entity ID: ⓘ  
YOUR-COMPANY-NAME

IdP Private Key:  
Replace IdP Private Key

IdP Certificate:  
Replace IdP Certificate

SP Entity ID: ⓘ  
https://app.organimi.com

ACS URLs ⓘ  
Enter at least one ACS URL. IdP initiated logins will use the first, or lowest index, ACS URL listed. The ACS URL used for SP initiated logins will depend on the authentication request received.

**Single sign-on**

- Integration Status
- IdP Certificate Valid expires 04-27-2028
- IdP Private Key Valid

**Identity Management**

- Integration Status

**User Portal Visibility**

- Visible in user portal

**jumpcloud**

- Discover **GET STARTED**
- Home
- USER MANAGEMENT
  - Users
  - User Groups
- USER AUTHENTICATION
  - LDAP
  - RADIUS
  - SSO**
  - Password Manager
- DEVICE MANAGEMENT
  - Devices
  - Device Groups
  - Policy Management **NEW**
  - Policy Groups **NEW**
  - Commands
  - MDM
  - Software Management
- Live Chat **1** days left
- Settings
- Account

**SSO** ⓘ

Product Tour Pricing Alerts What's New Support Checklist **PR**

Configured App **SAML 2.0**

+ Add New Application

General Info **SSO** Identity Management User Groups

ACS URLs ⓘ  
Enter at least one ACS URL. IdP initiated logins will use the first, or lowest index, ACS URL listed. The ACS URL used for SP initiated logins will depend on the authentication request received.

Index: 0  
Default URL \*  
https://app.organimi.com/api/v7/auth/login/saml/callback

+ Add URL

SP Certificate:  
Replace SP Certificate

SAMLSubject NameID: ⓘ  
email

SAMLSubject NameID Format: ⓘ  
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Signature Algorithm: ⓘ  
RSA-SHA1

Sign Assertion

**Single sign-on**

- Integration Status
- IdP Certificate Valid expires 04-27-2028
- IdP Private Key Valid

**Identity Management**

- Integration Status

**User Portal Visibility**

- Visible in user portal

The screenshot shows the 'Configured App' window for a SAML 2.0 application. The 'SSO' tab is selected, displaying the following configuration details:

- Default RelayState:** `{"company": "YOUR-COMPANY-ALIAS"}`
- IDP URL:** `https://sso.jumpcloud.com/saml2/saml2`
- User Attributes:** A table mapping Service Provider Attribute Names to JumpCloud Attribute Names:

Service Provider Attribute Name	JumpCloud Attribute Name
email	email
firstname	firstname
lastname	lastname

Red arrows indicate the configuration fields for Default RelayState, IDP URL, and the User Attributes table.

Once all configured, click activate at the bottom.

The screenshot shows the 'Configured App' window for a Custom SAML App. The 'SSO' tab is selected, displaying the following configuration details:

- IDP URL:** `https://sso.jumpcloud.com/saml2/saml2`
- User Attribute Mapping:** A table mapping Service Provider Attribute Names to JumpCloud Attribute Names:

Service Provider Attribute Name	JumpCloud Attribute Name
email	email
firstname	firstname
lastname	lastname

At the bottom right, the 'activate' button is highlighted with a red box and arrow.

On the "Confirmation" dialog, you can simply click "Continue".

## Please confirm your new SSO connector instance



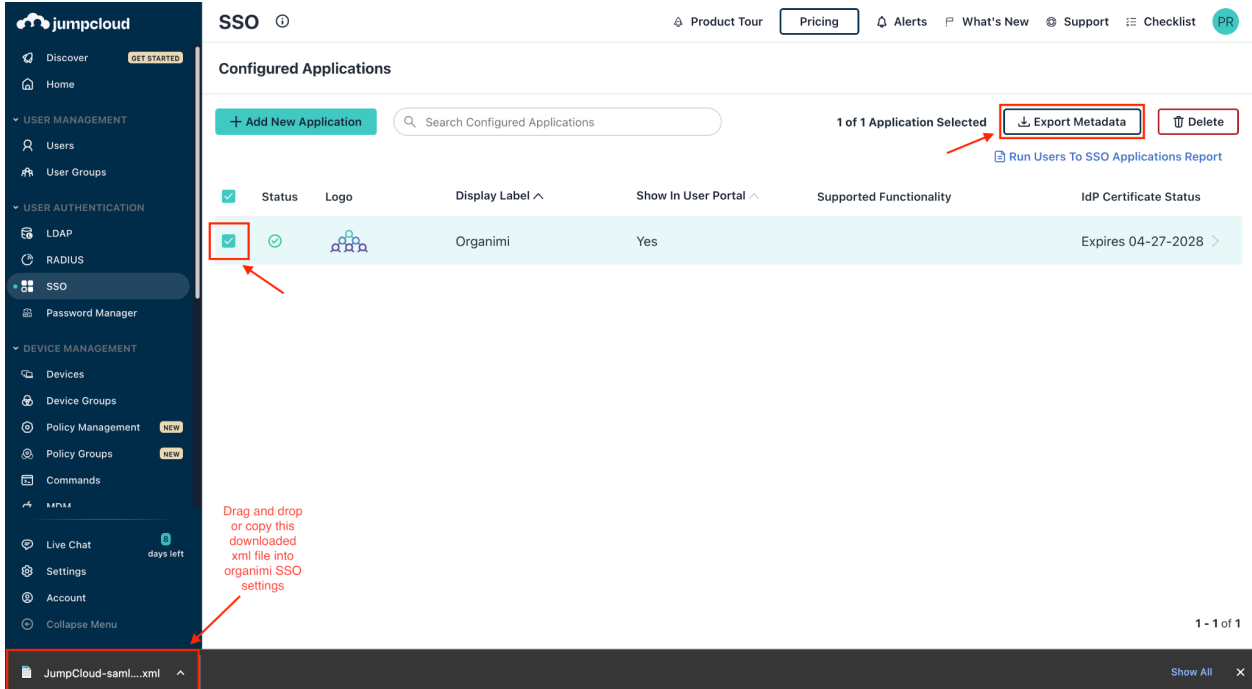
Note that the IdP URL cannot be shared across applications and this URL is not editable after creation.



### Step 4

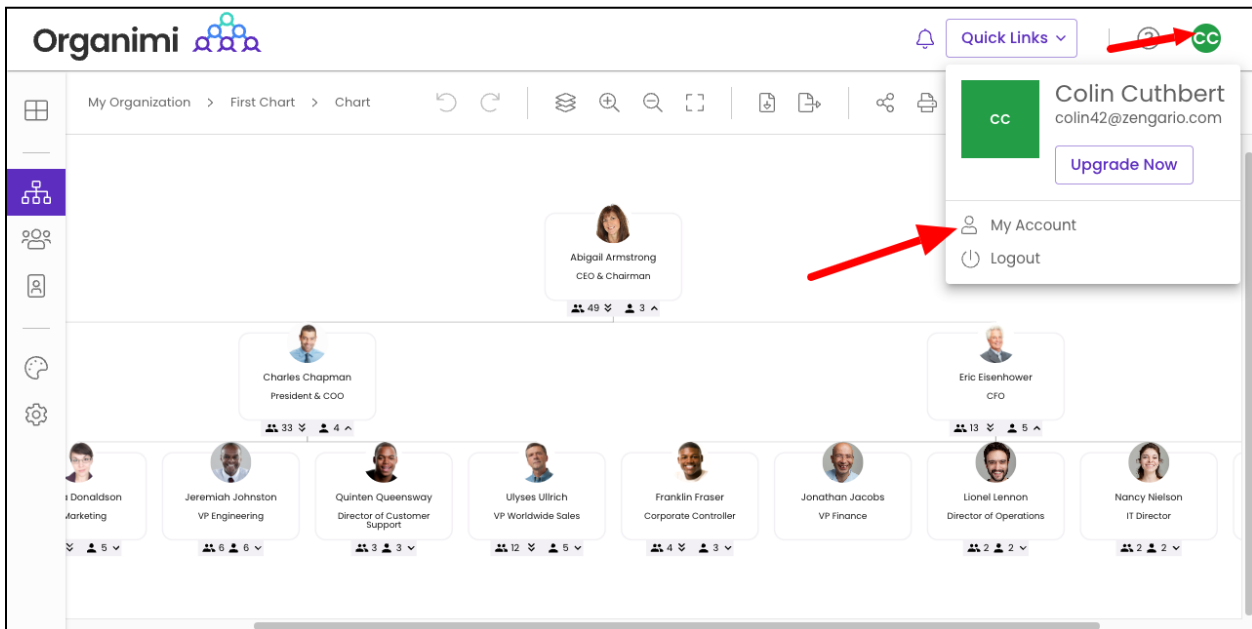
Now that the Organimi App is set up at the Jumpcloud side, we now have to configure this IDP in Organimi.

Select the checkbox for the Organimi app in Jumpcloud and click on “Export Metadata”. You will be using the downloaded file in the following steps.



## Step 5

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)

The screenshot displays the 'SAML SSO Config' interface. On the left sidebar, the 'SSO Settings' tab is highlighted with a red circle. The main content area is titled 'SAML SSO Config' and includes a 'Service Provider Metadata' section with a 'Setup Instructions' link. Below this, there are four input fields: 'Callback URL' with the value 'https://app.organimi.com/api/v7/auth/login/saml/callback', 'SP Entity ID' with 'https://app.organimi.com', 'Default Relay State' with '{\"company\":\"zengario-test-nine\"}', and 'Required Attributes' with 'email, firstname, lastname'. A 'Service Provider Metadata File' section contains a 'Download (.xml)' link. The 'Your Identity Provider' section at the bottom features the text 'Add your IDP to enable SSO for this account' and a purple 'Configure IDP' button, which is pointed to by a red arrow.

## Step 6

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 3.4**
2. IDP Metadata: Copy and paste the XML downloaded in step 4 in to the “drop area” as highlighted below (click in the gray box and then paste)



## SAML SSO CONFIG

License

Account Owners

Webhooks

API Settings

SSO Settings

Transfer Account

Delete Account

### 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

1

Company Alias

zengario



SSO URL

Entity ID

X509 Certificate

```
MIIDqjCCApKgAwIBAgIeGAYYEnMXcMA0GCSqGSIb3DQEBCwUAMIGVMQswC
QYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMFEuGAIUEBwwNU2FuIEZyYW55aXNjbzEA0G
CSNMaw...
```

Have your IDP's metadata XML?

or

2

CANCEL

SAVE

3. Click the SAVE button

My Info

License

Account Owners

Webhooks

API Settings

**SSO Settings**

Transfer Account

Delete Account

## SAML SSO Config

[Setup Instructions](#)

### Service Provider Metadata

Callback URL  
https://app.organimi.com/api/v7/auth/login/saml/callback

SP Entity ID  
https://app.organimi.com

Default Relay State  
{"company":"zengario-test-nine"}

Required Attributes  
email, firstname, lastname

Service Provider Metadata File [Download \(.xml\)](#)

### Your Identity Provider

Company Alias  
zengario-test-nine

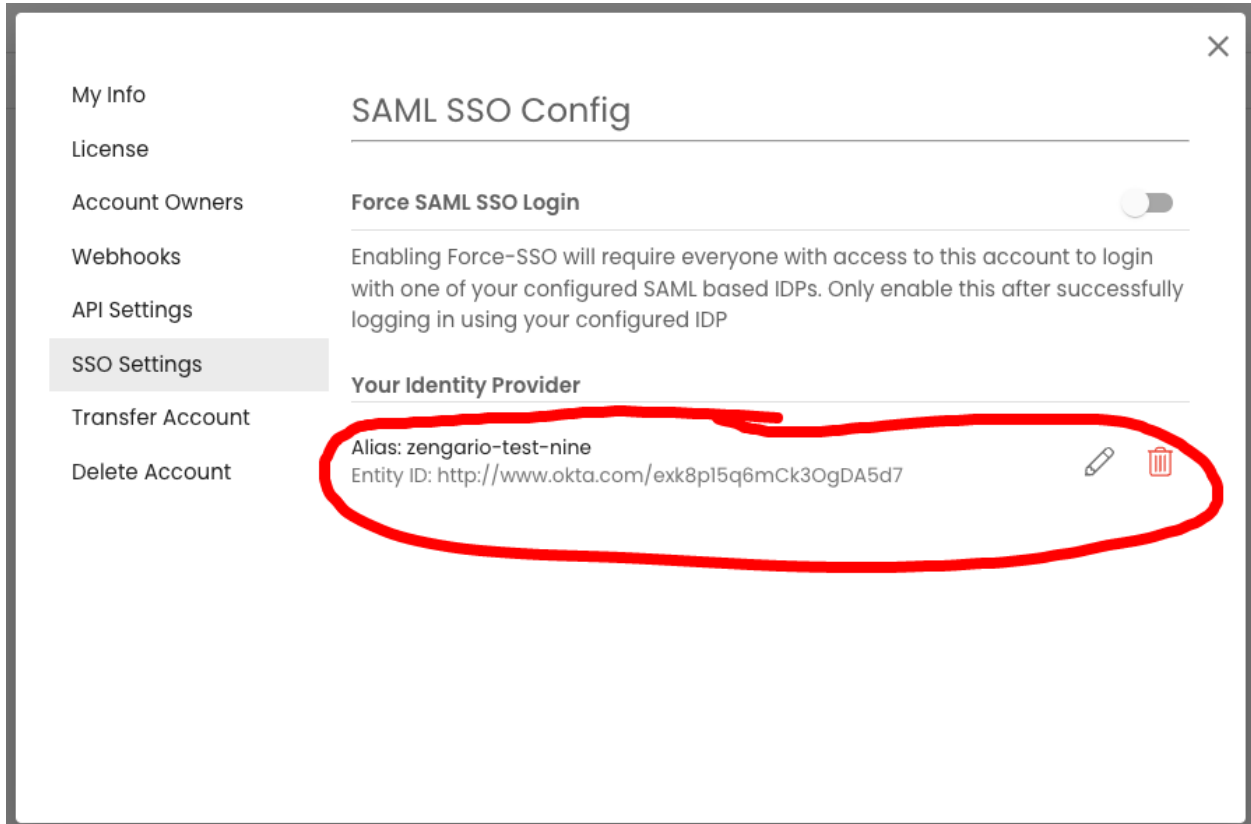
SSO URL  
https://dev-55539452.okta.com/app/dev-55539

Entity ID  
http://www.okta.com/exk8p15q6mCk3OgDA5d7

X509 Certificate  
MIIDqDCCApCgAwIBAgIGAYbcTh0zMA0GCSqGSib3DQEBCwUAMIGUMQs  
wCQYDVQQGEwJVUzETMBEG  
A1UECAwKQ2FsaWZvcmlkZXIwYXNjaXNjbzEN  
MAsGAIUECgwET2t0YTEU  
MBIGAIUECwwLU1NPUHJvdmlkZXIwYXNjaXNjbzEN  
MBoGCSaGSib3DOEJ

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

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



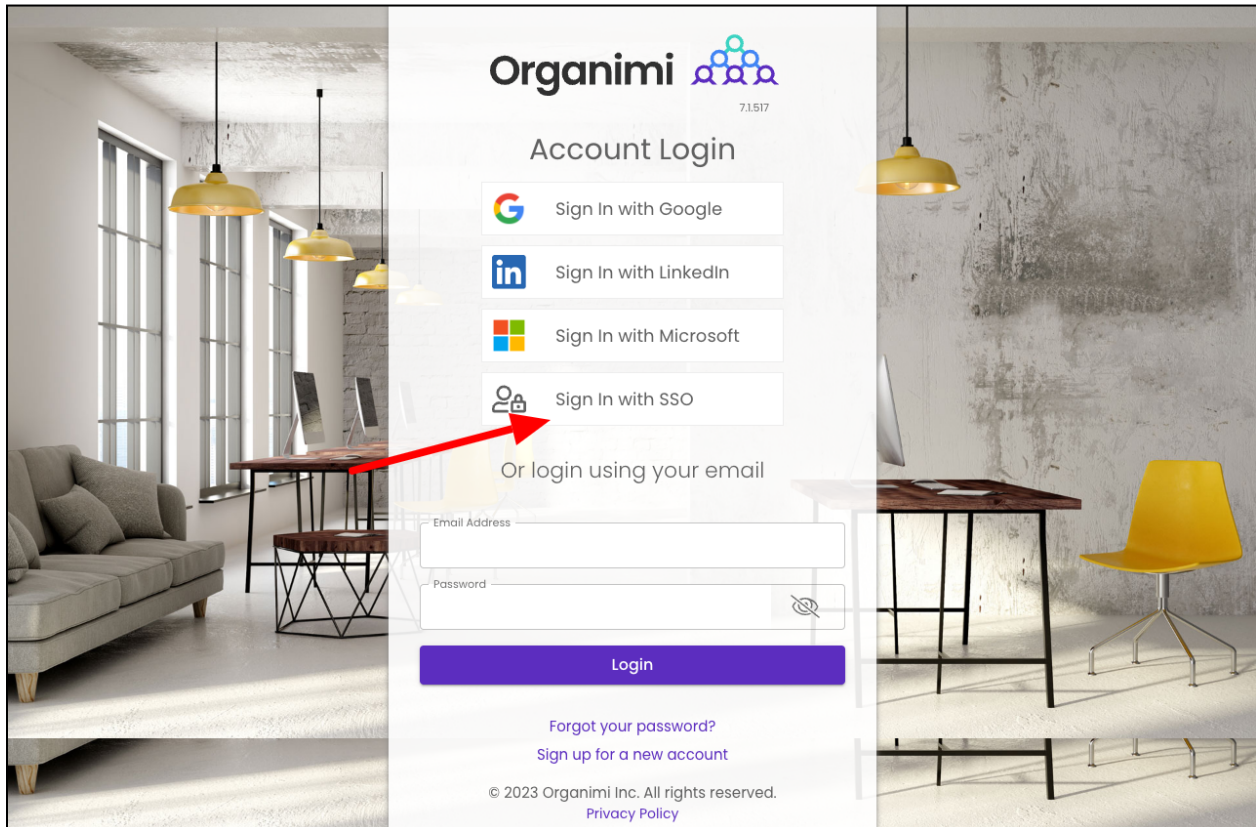
## Step 7

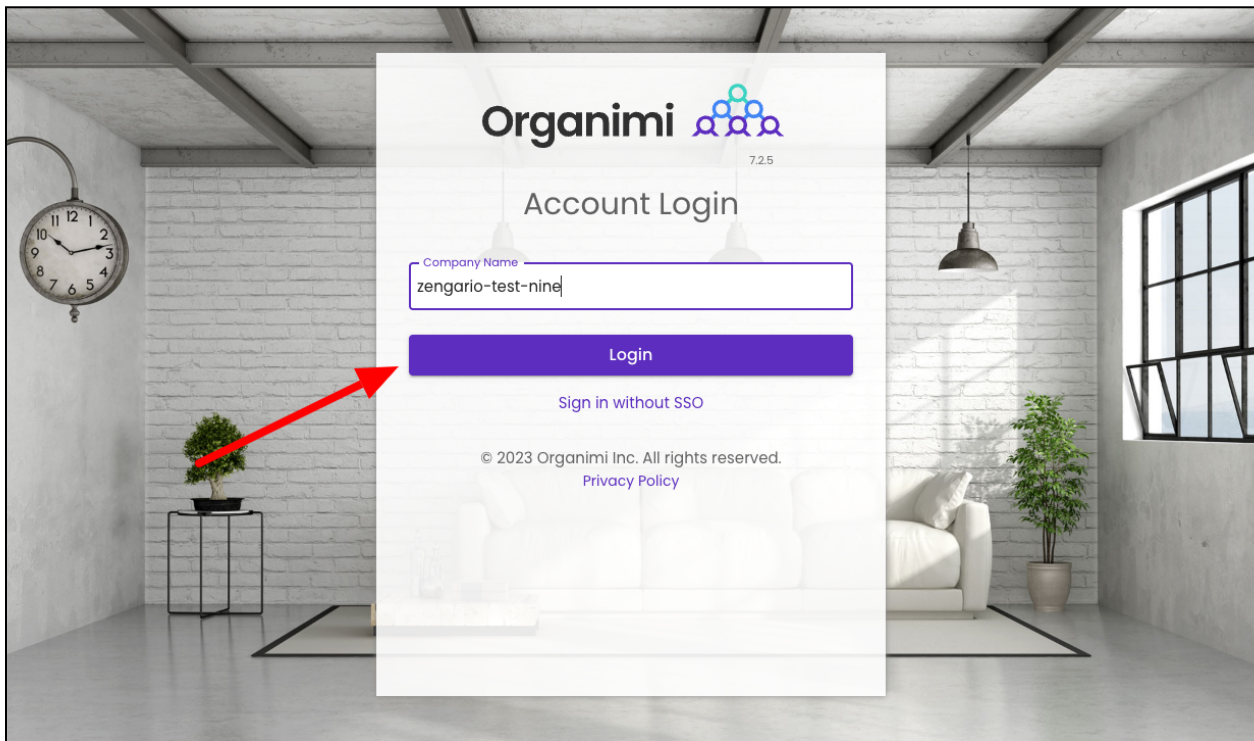
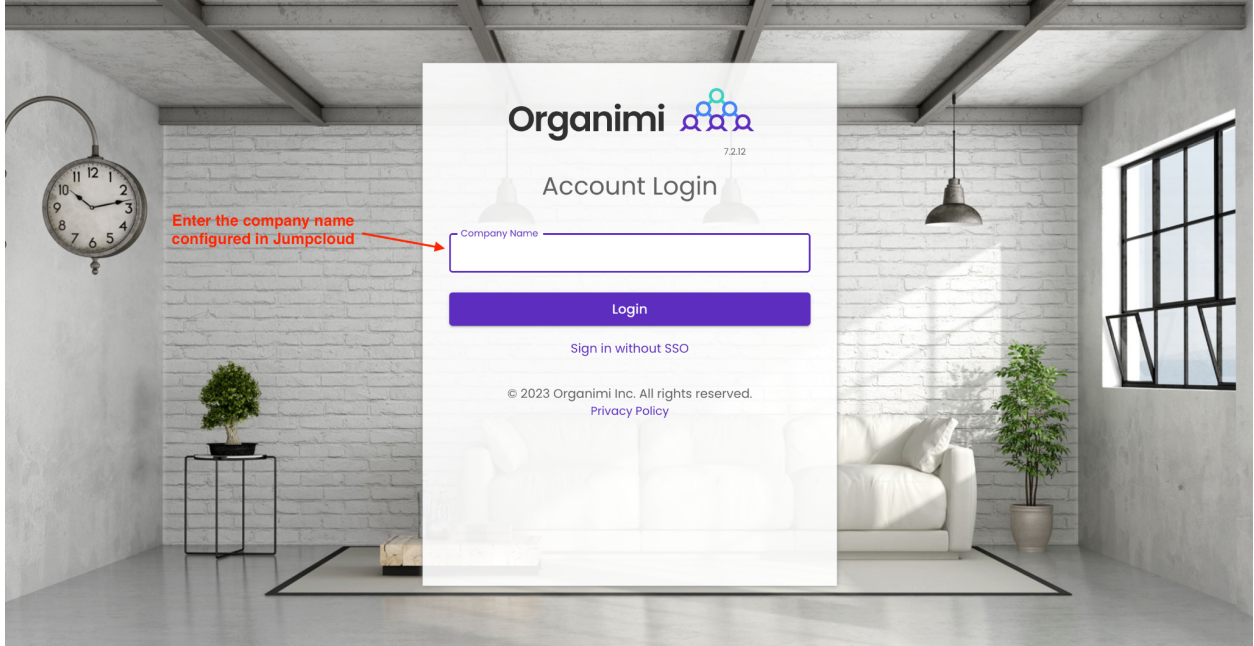
Your Identity Provider should show the Jumpcloud Entity ID that you just set up, which means IDP configuration is accepted.

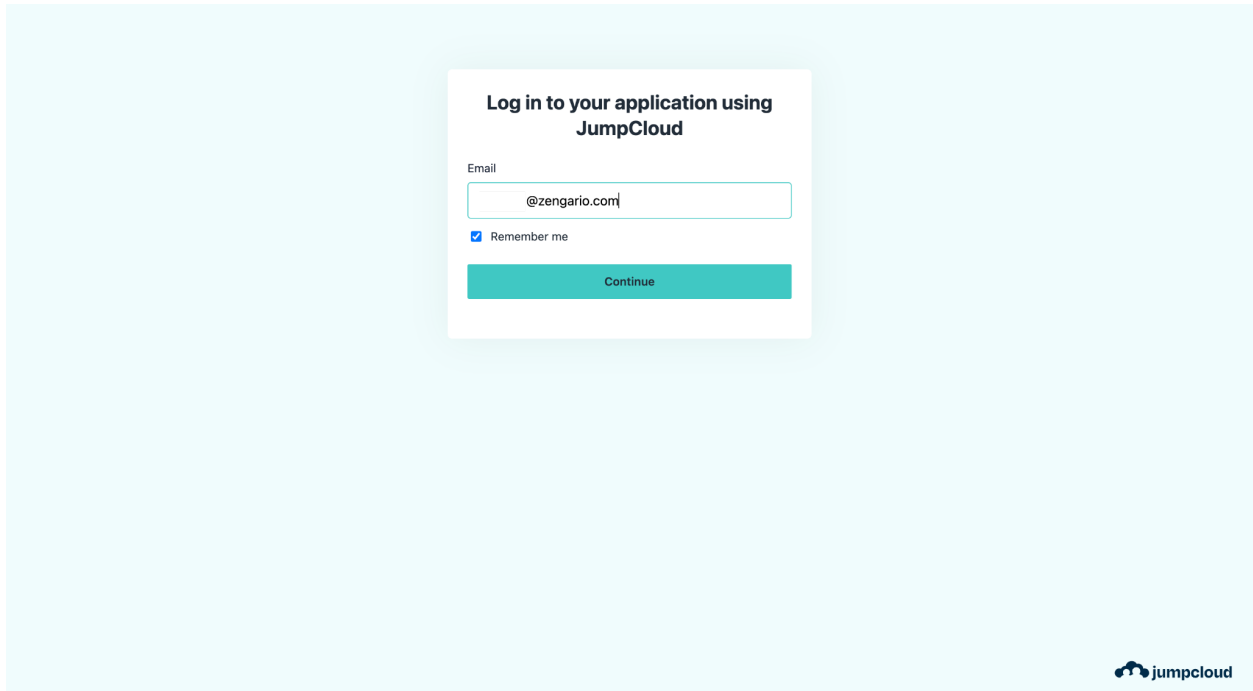
*Note: If you do not reach to this point and see an error message on clicking the "SAVE" button, Contact Organimi support @ [support@organimi.com](mailto:support@organimi.com)*

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 step 3.4 & 6.1 and then click login.

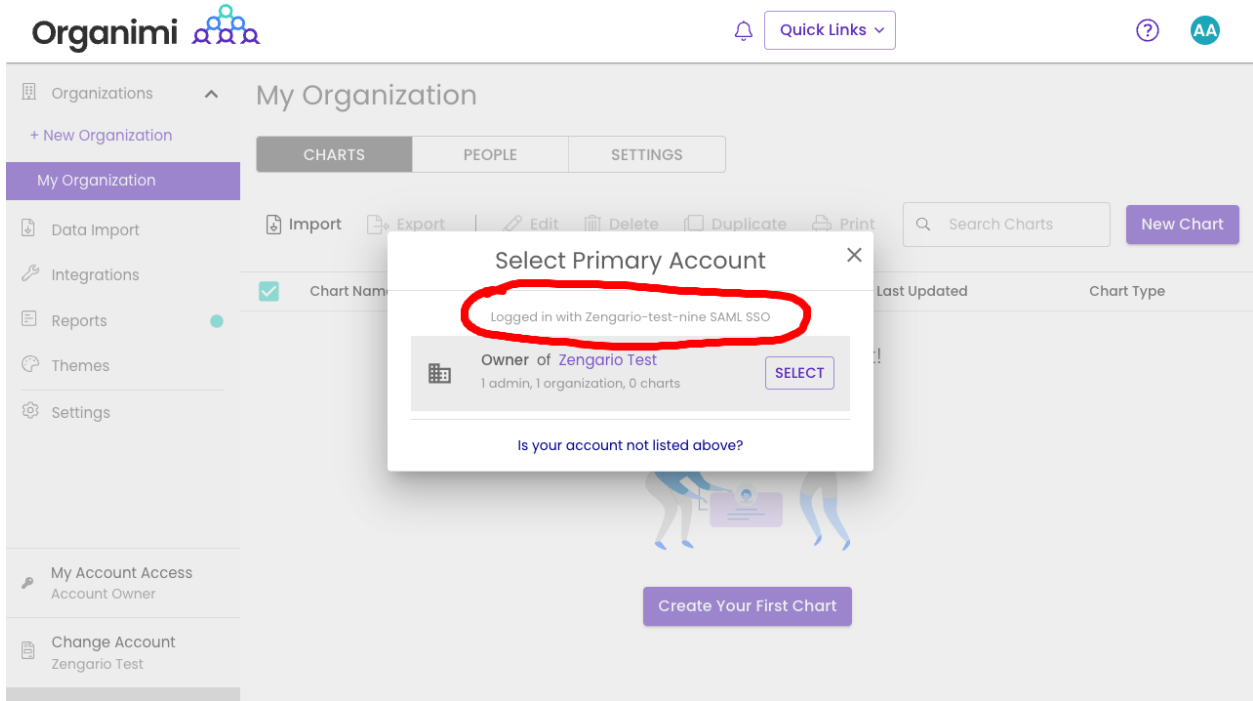
You should be redirected to your Jumpcloud IDP where you can get authenticated. Once successful, you will be redirected back to Organimi and will be logged in.







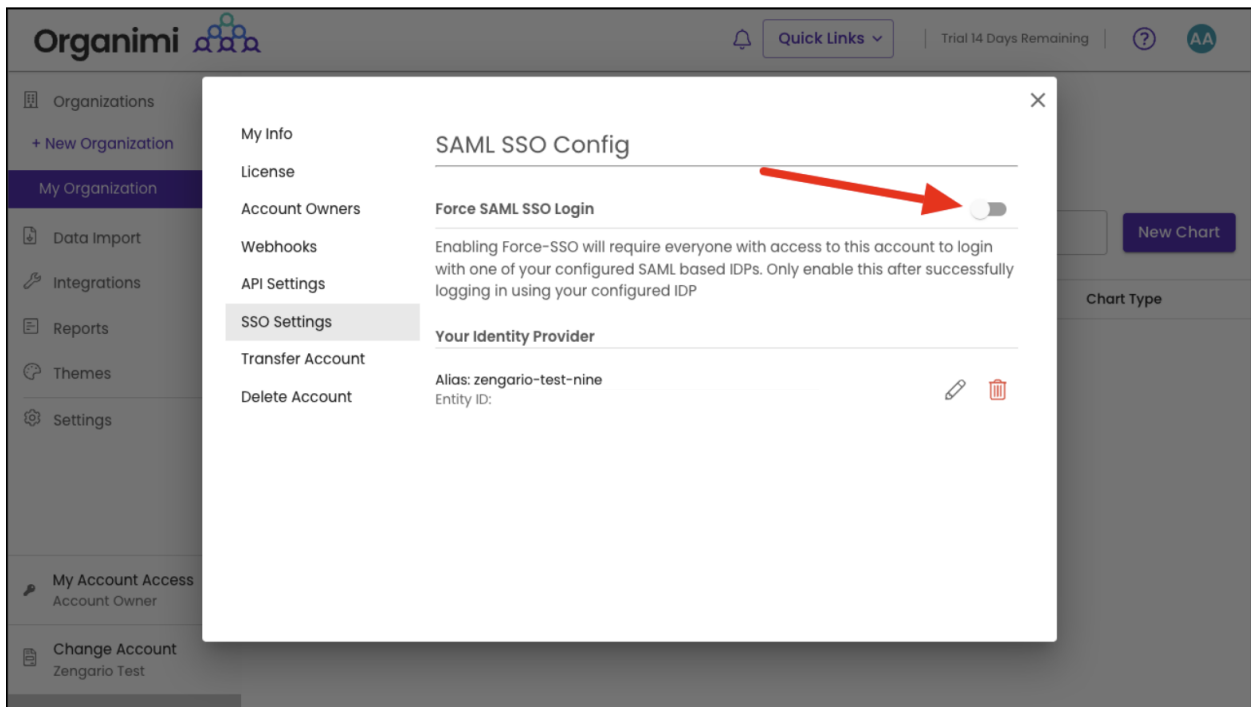
And you are in. If you click the Change Account link on the Organimi screen you will see that you are logged in with SAML SSO



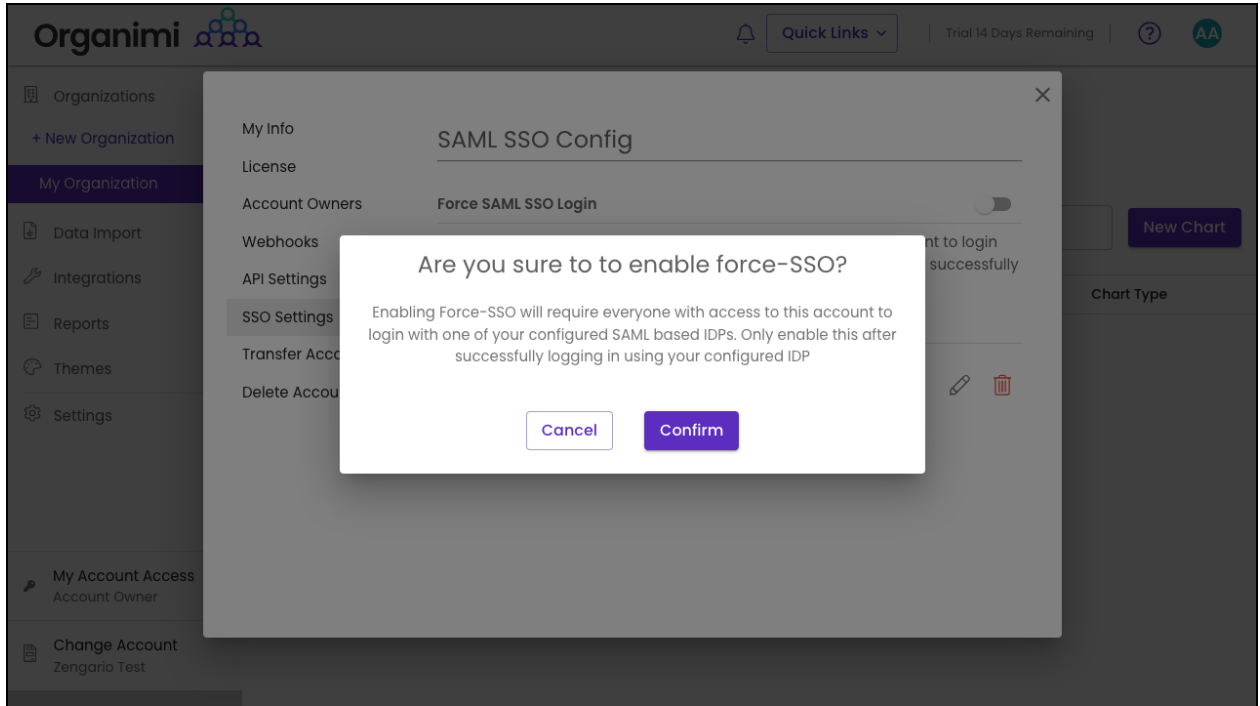
## Step 8

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.

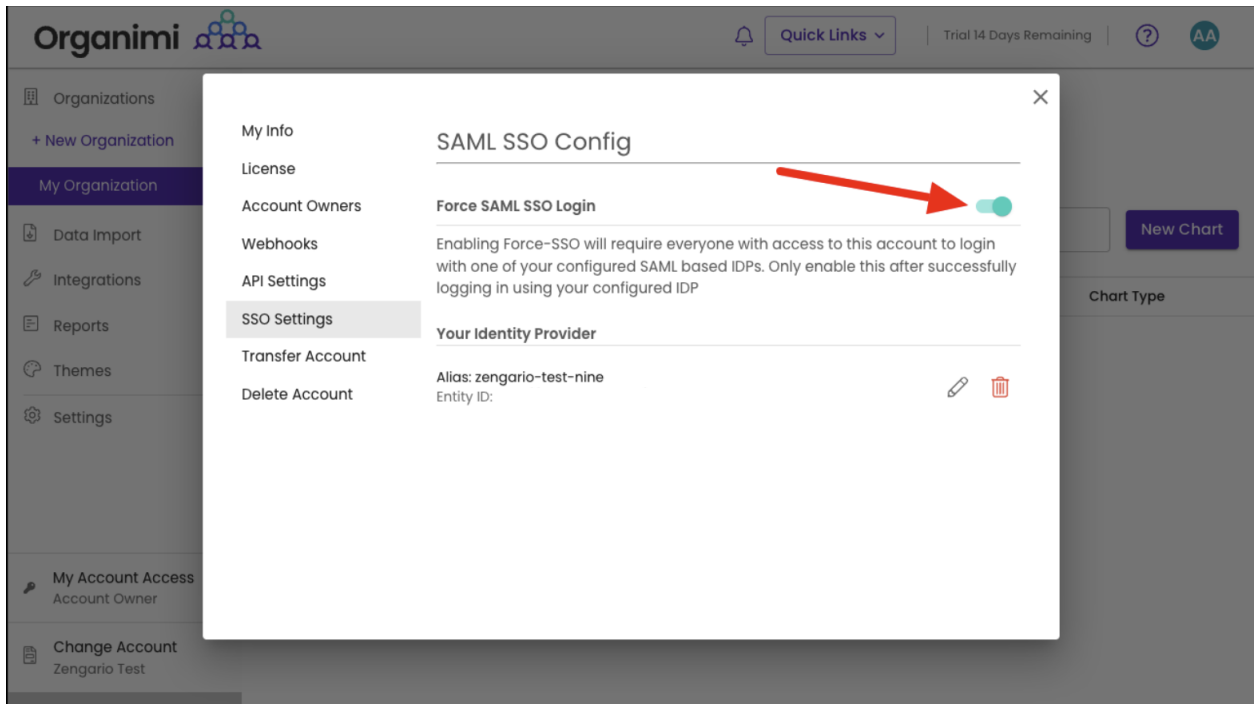
*Note: As the account owner, It's recommended that you test logging in with your IDP first before turning on this setting, as you will not be able to access the account via any other login methods after you enable the “Force-SSO” option.*



The screenshot shows the Organimi user interface. On the left is a navigation sidebar with options like Organizations, My Organization, Data Import, Integrations, Reports, Themes, Settings, My Account Access, and Change Account. The main content area displays the 'SAML SSO Config' settings. A red arrow points to the 'Force SAML SSO Login' toggle switch, which is currently turned off. Below this, there is explanatory 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'. Further down, the 'Your Identity Provider' section shows the alias 'zengario-test-nine' and the entity ID.



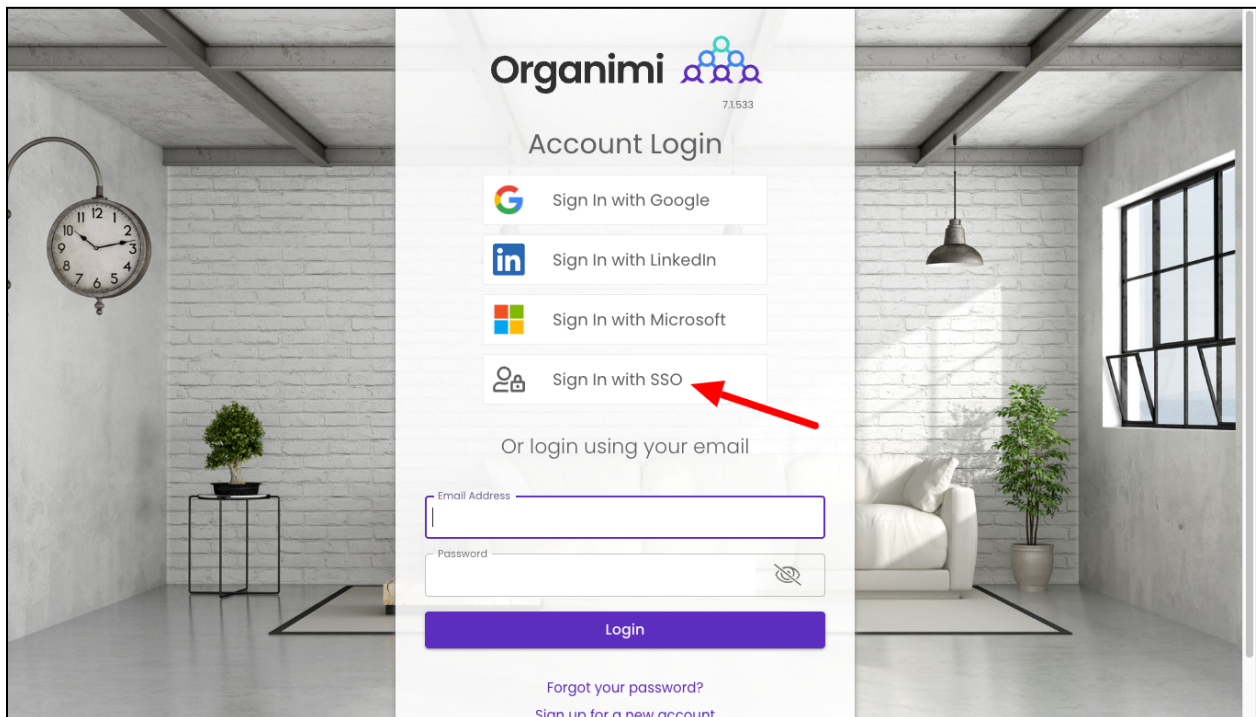
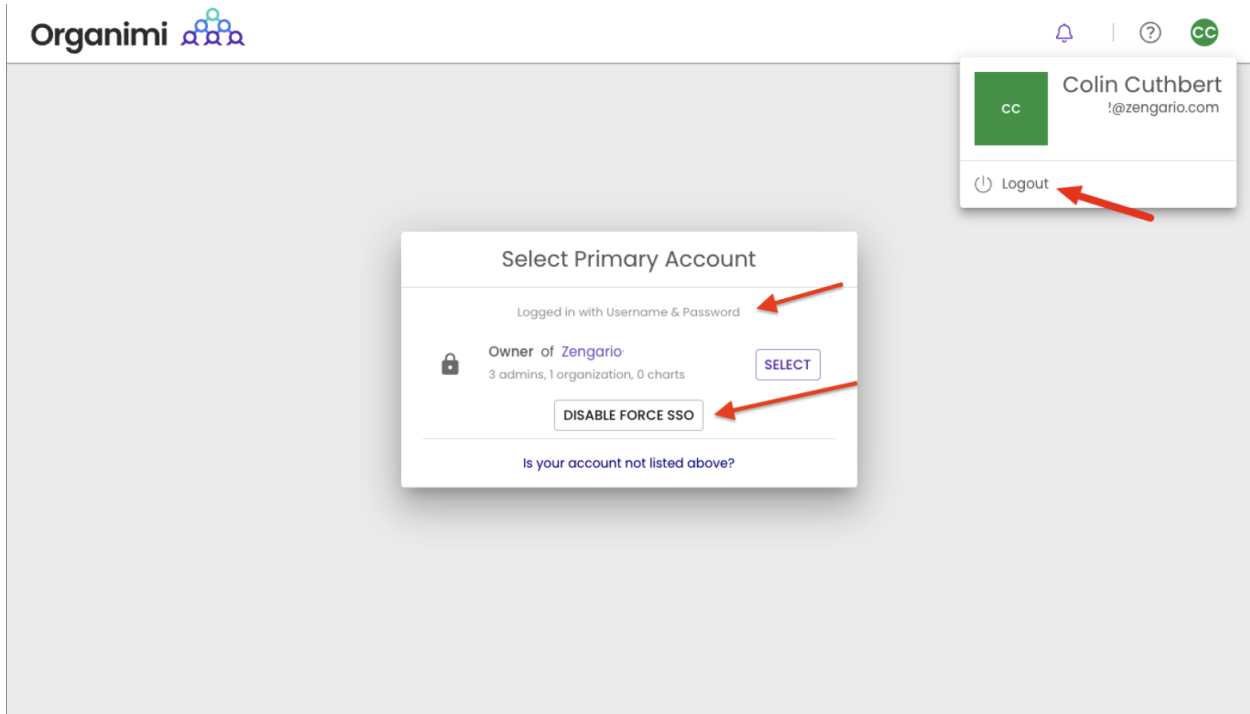
If you were logged into Organimi with you SSO IDP Account then you will just see that the switch is now on for "Force SSO"



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.



## Default share settings for IDP's:

Alternatively users can be invited from the charts as editors or viewers by enabling default sharing settings for SSO IDP. This will not send any email invites to these users. They can login directly using the shared idp. These permissions can be changed, as needed.

SSO Login does not imply chart will remove the access

SSO login can view this chart will assign viewer permissions to the users logging in the SSO IDP

SSO login can edit this chart will enable Editor permissions to the users logging in with the SSO IDP

**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

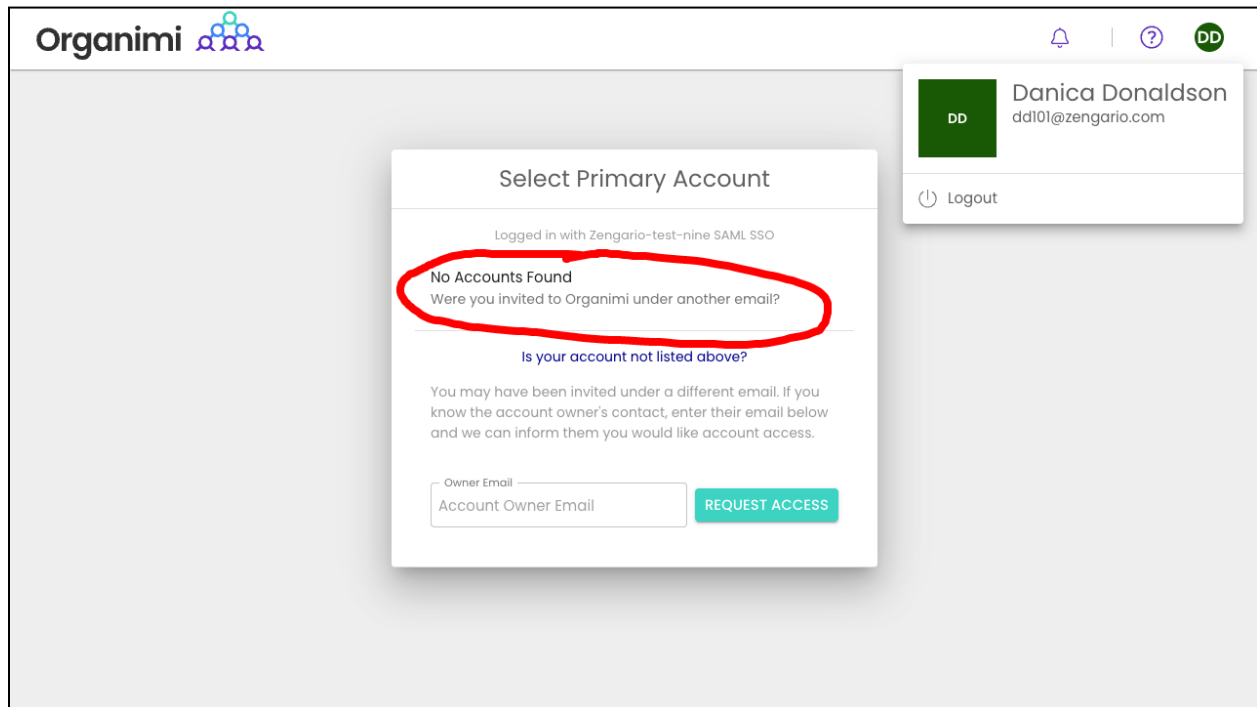
**COMING SOON**

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

## Please Note ...

If default sharing is not enabled as described above ... in addition to provisioning the application to users in Jumpcloud you will also need to invite users to one or your Organizations or Charts or in Organimi ... if 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 or enable default sharing.



Thank you for being an Organimi customer and please contact us at [support@organimi.com](mailto: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.