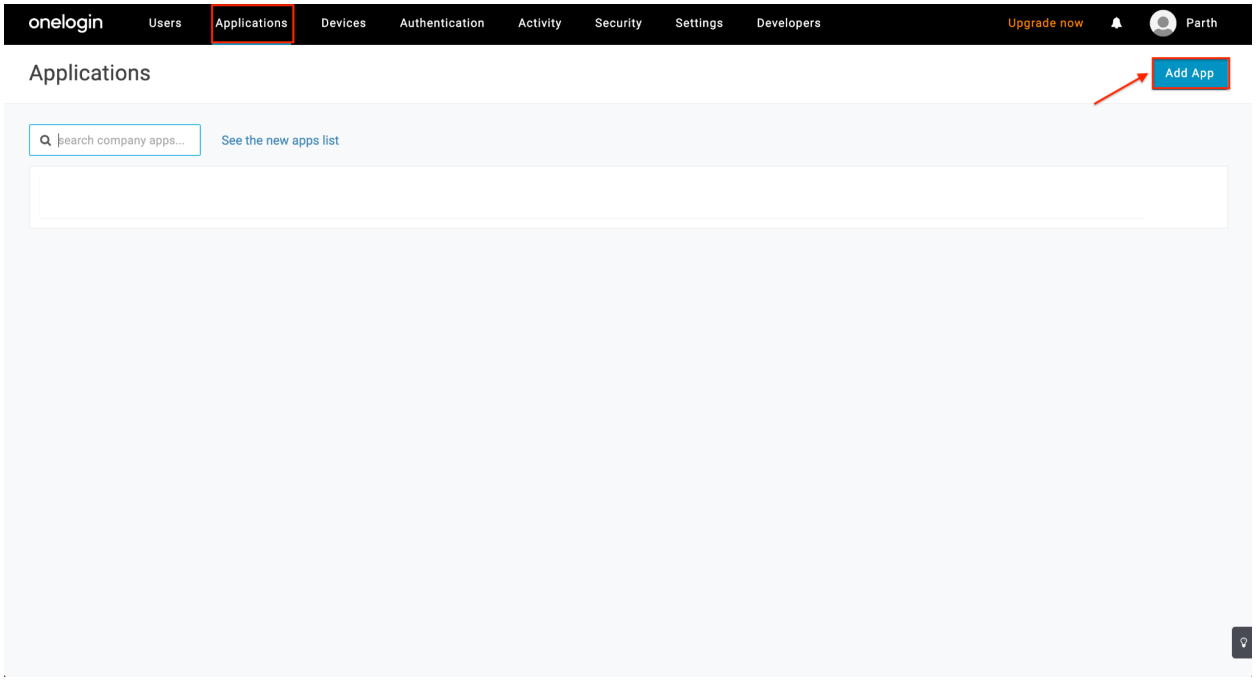
SAML based SSO - Login with OneLogin

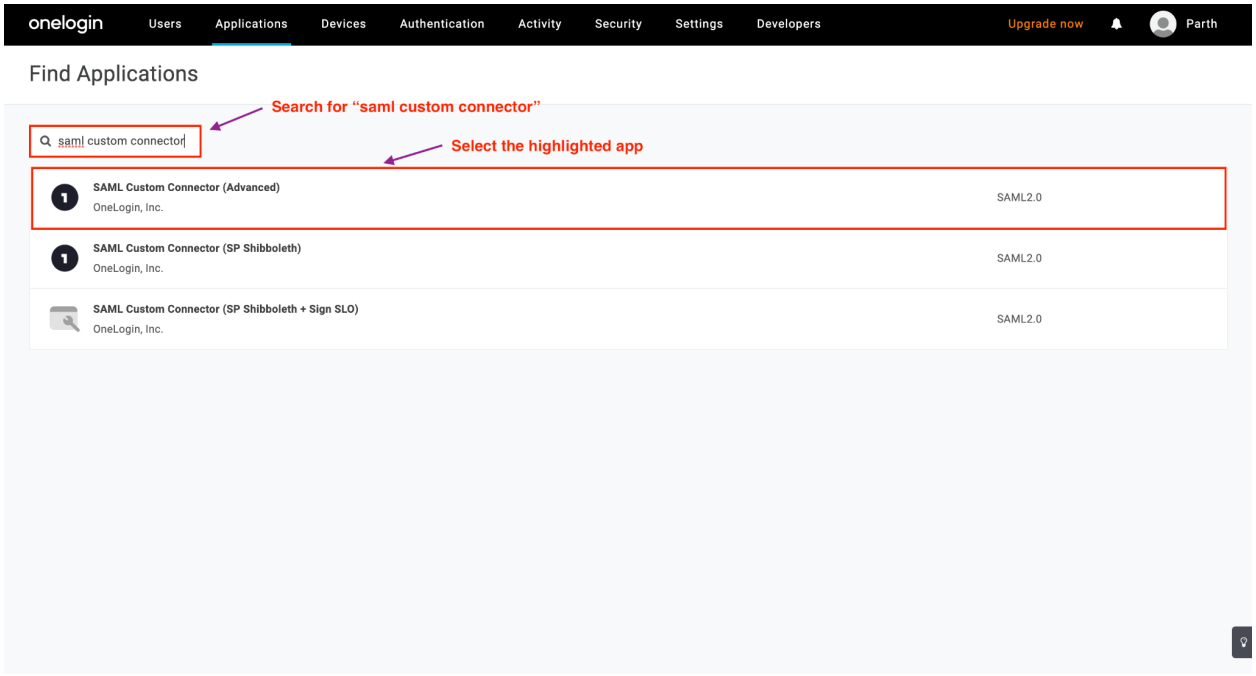
Organimi has implemented SAML based SSO for Premium account holders … this document will walk you through the steps to set up Organimi with OneLogin

Step 1

Go to your OneLogin dashboard and click “Add App” from the Applications tab

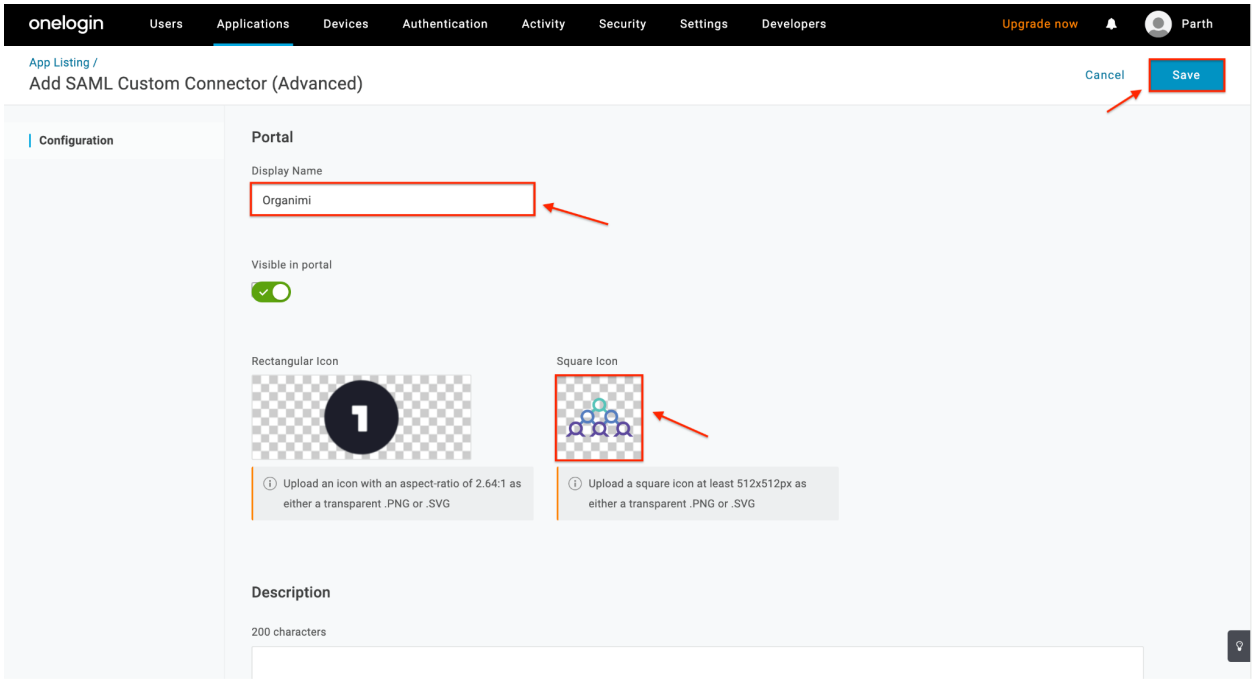


Search for “saml custom connector” and click on the highlighted application in the below screenshot … “SAML Custom Connector (Advanced)”



Step 2

Under Configuration, enter Display Name as “Organimi”, upload Organimi’s logo and click Save (you can download the Organimi logo at: Organimi_LogoOnly.png)

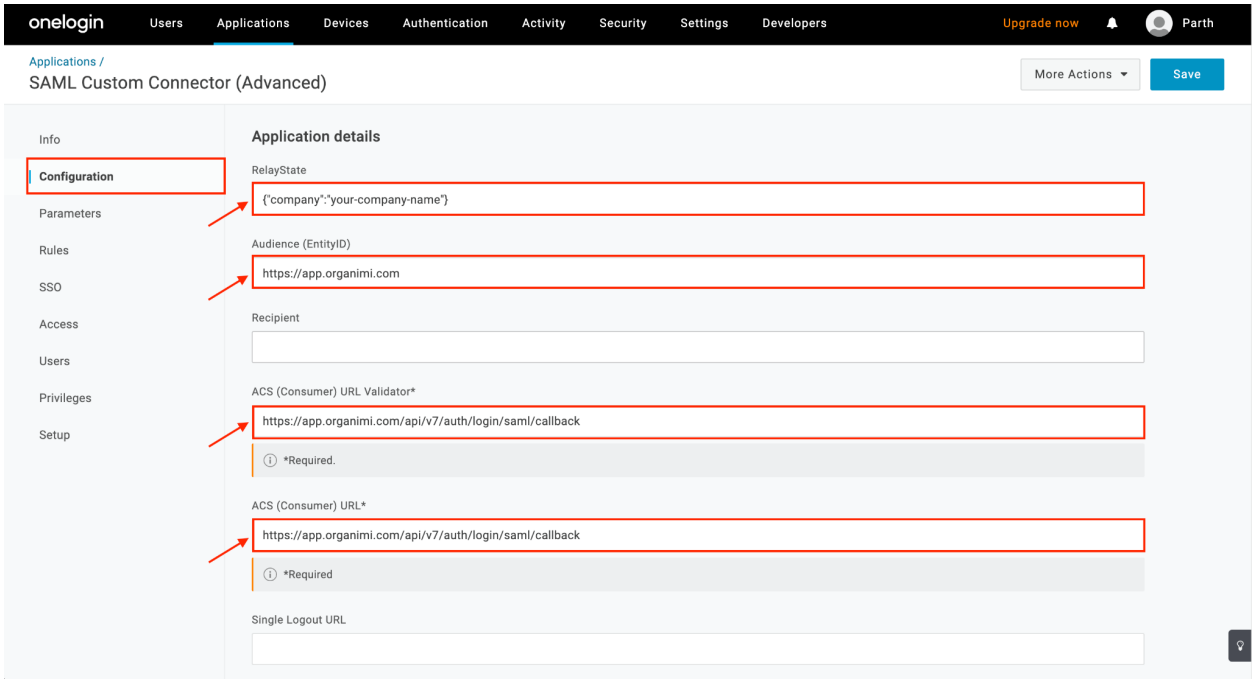


Step 3

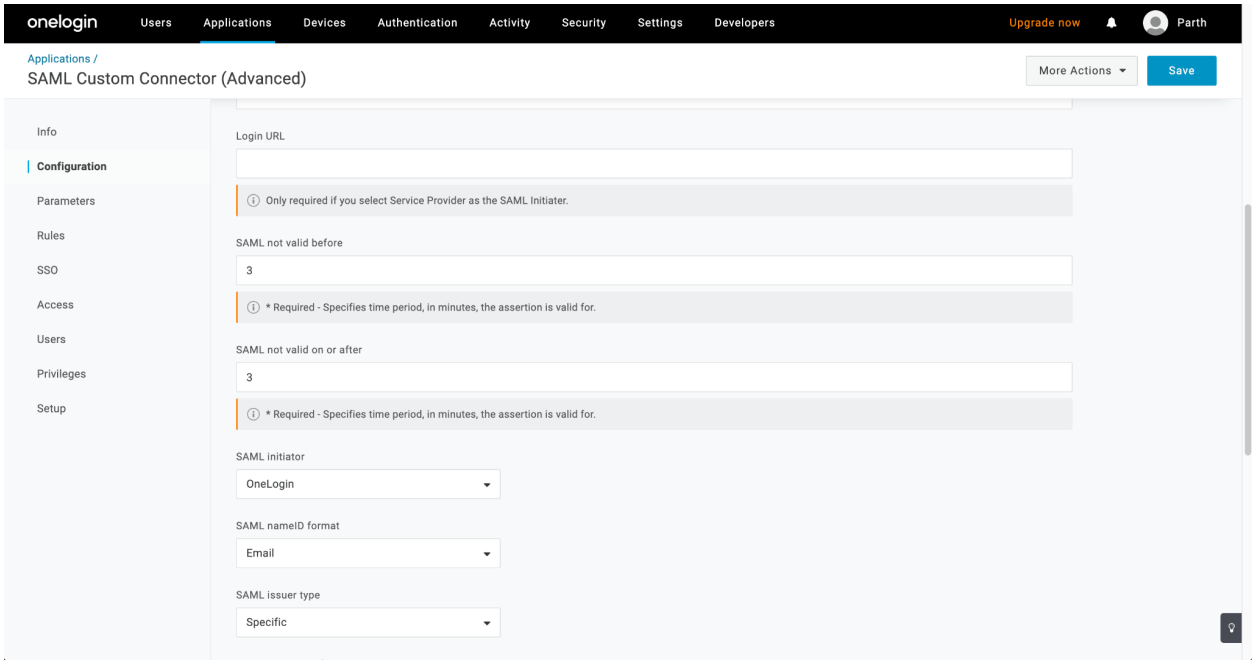
Click on SSO and enter the following information

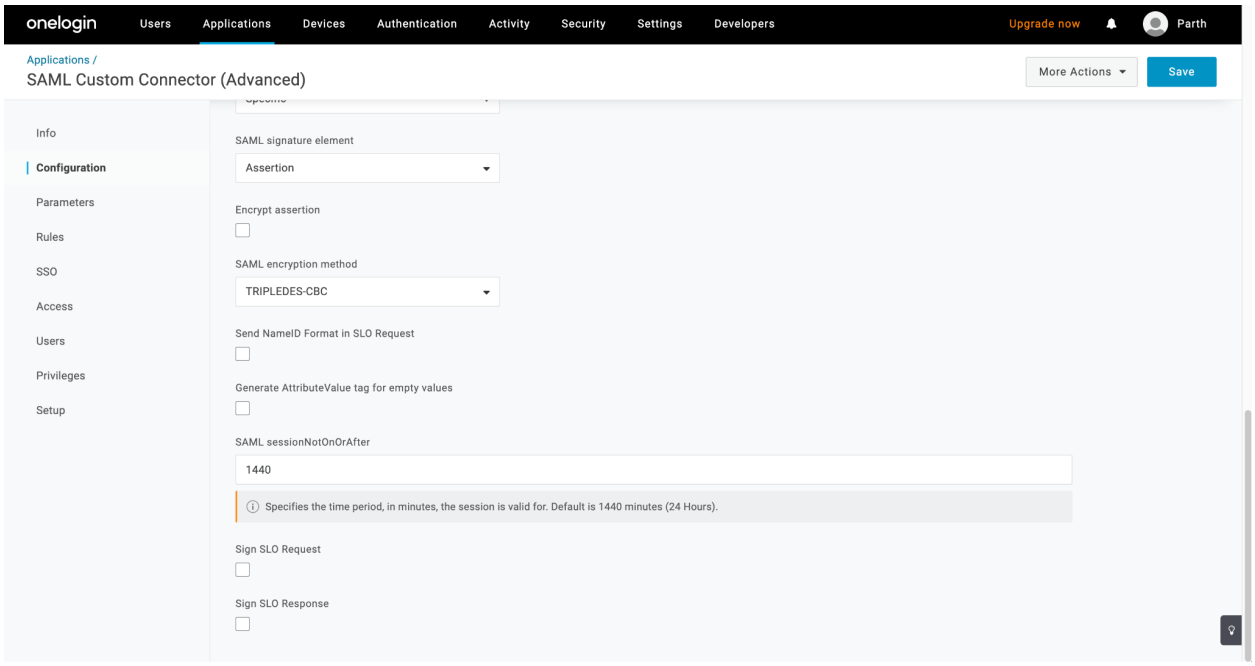
1. RelayState: {"company":"YOUR-COMPANY-ALIAS"}
    a. ***Note: Replace the placeholder with your company name. This name will also be required later on the Organimi side of the setup. And anyone who wishes to login using this IDP, will be asked to enter this name when signing in from the Organimi Login Page.***
2. Audience (EntityID): https://app.organimi.com
    a. Only for EU customers specifically set up on the EU server - https://eu.app.organimi.com
    b. Only for AU customers specifically set up on the AU server - https://au.app.organimi.com
3. ACS (Consumer) URL Validator: 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
4. ACS (Consumer) 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

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



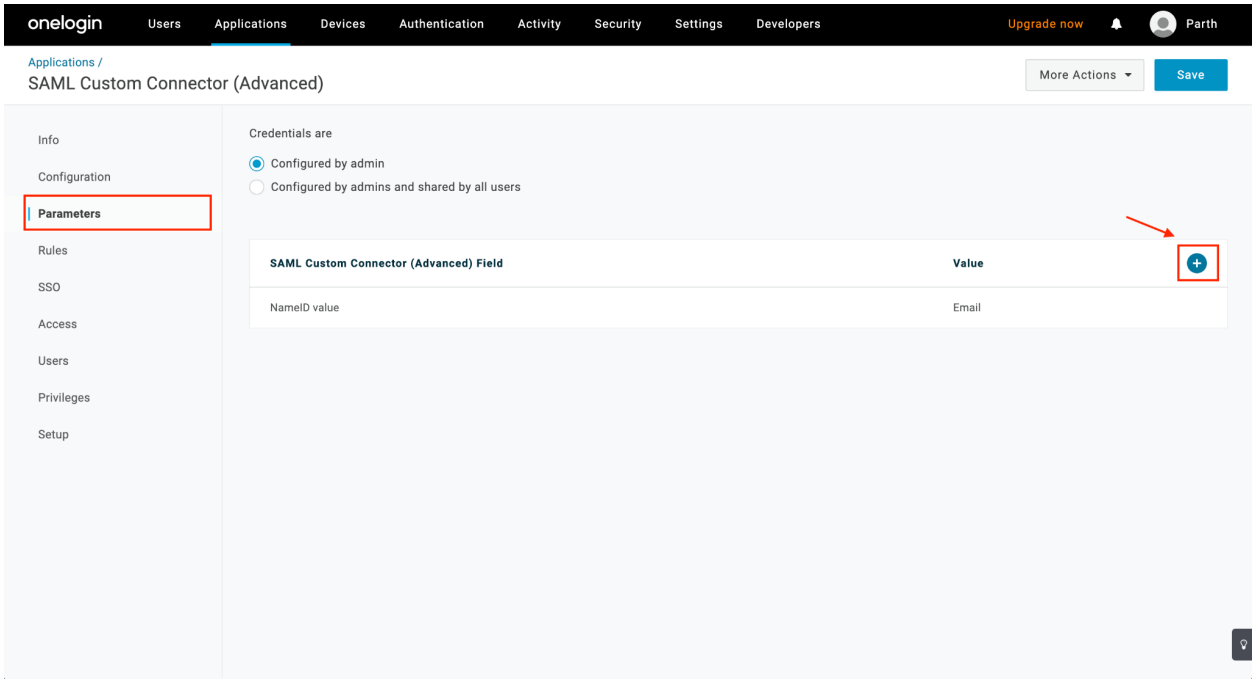
Leave all other configuration settings as it is, to the default value (screenshots attached below for reference).

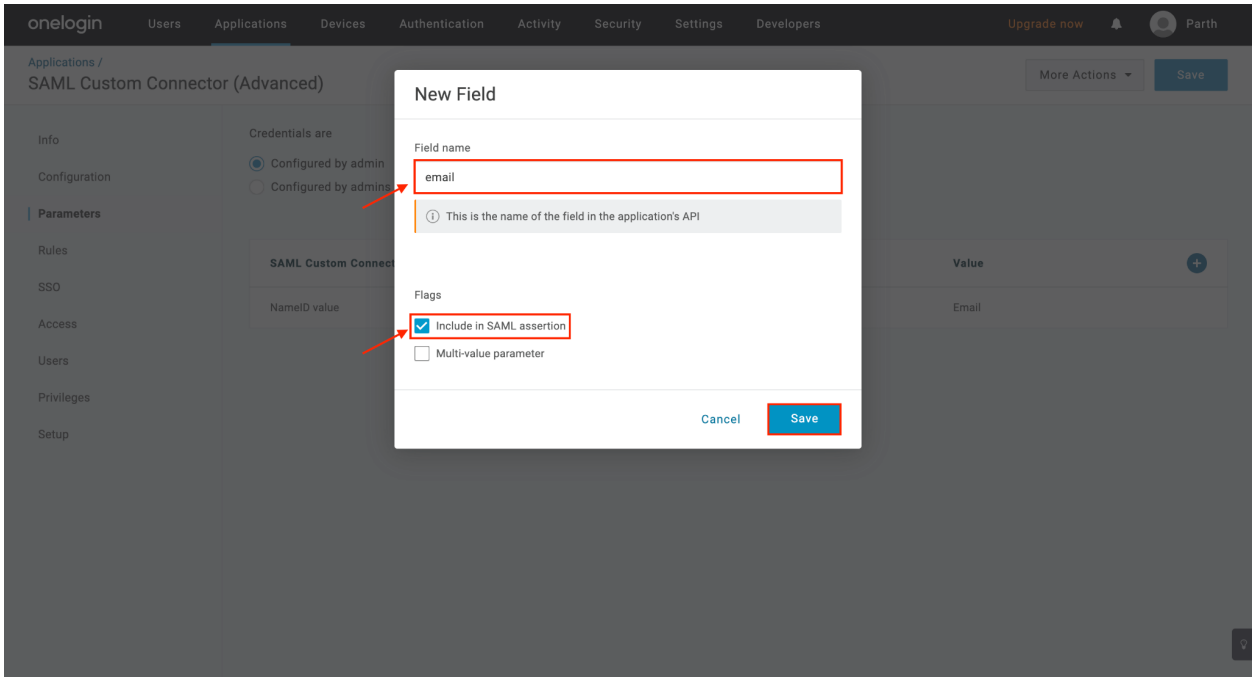

onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers
Upgrade now
Parth
Applications /
SAML Custom Connector (Advanced)
More Actions
Save
Info
Configuration
Parameters
Rules
SSO
Access
Users
Privileges
Setup
Login URL
Only required if you select Service Provider as the SAML Initiater.
SAML not valid before
3
* Required - Specifies time period, in minutes, the assertion is valid for.
SAML not valid on or after
3
* Required - Specifies time period, in minutes, the assertion is valid for.
SAML initiator
OneLogin
SAML nameID format
Email
SAML issuer type
Specific

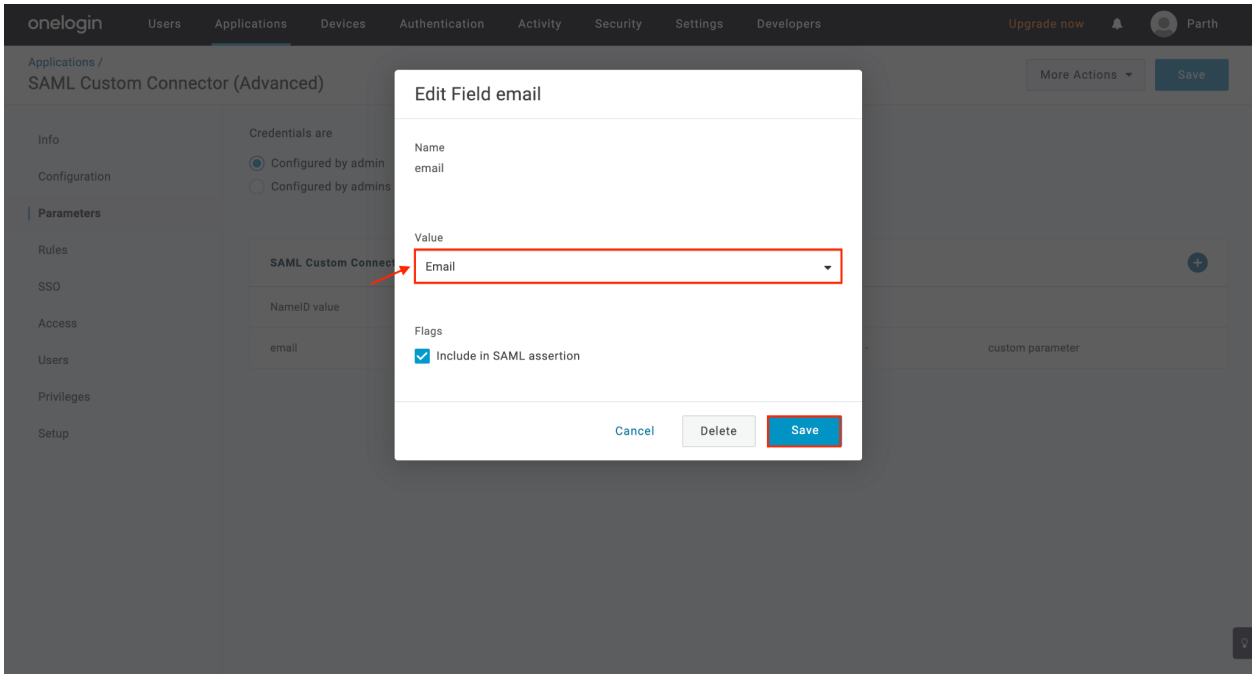

onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers
Upgrade now
Parth
Applications /
SAML Custom Connector (Advanced)
More Actions
Save
Info
Configuration
Parameters
Rules
SSO
Access
Users
Privileges
Setup
SAML signature element
Assertion
Encrypt assertion
SAML encryption method
TRIPLEDES-CBC
Send NameID Format in SLO Request
Generate AttributeValue tag for empty values
SAML sessionNotOnOrAfter
1440
Specifies the time period, in minutes, the session is valid for. Default is 1440 minutes (24 Hours).
Sign SLO Request
Sign SLO Response

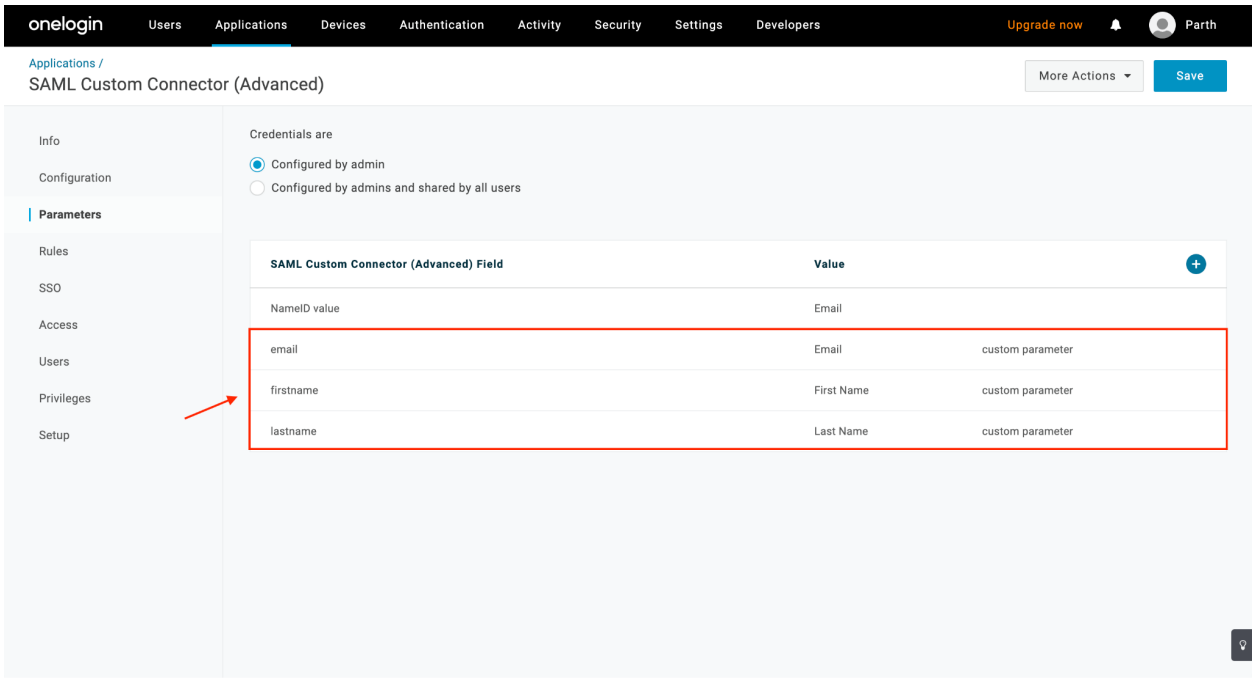
In order for a user to log into Organimi, we require the following three attributes of the user from OneLogin. Configure them under “Attribute Statements (optional)”. The names should be all lowercase, and the value should be matched accordingly.

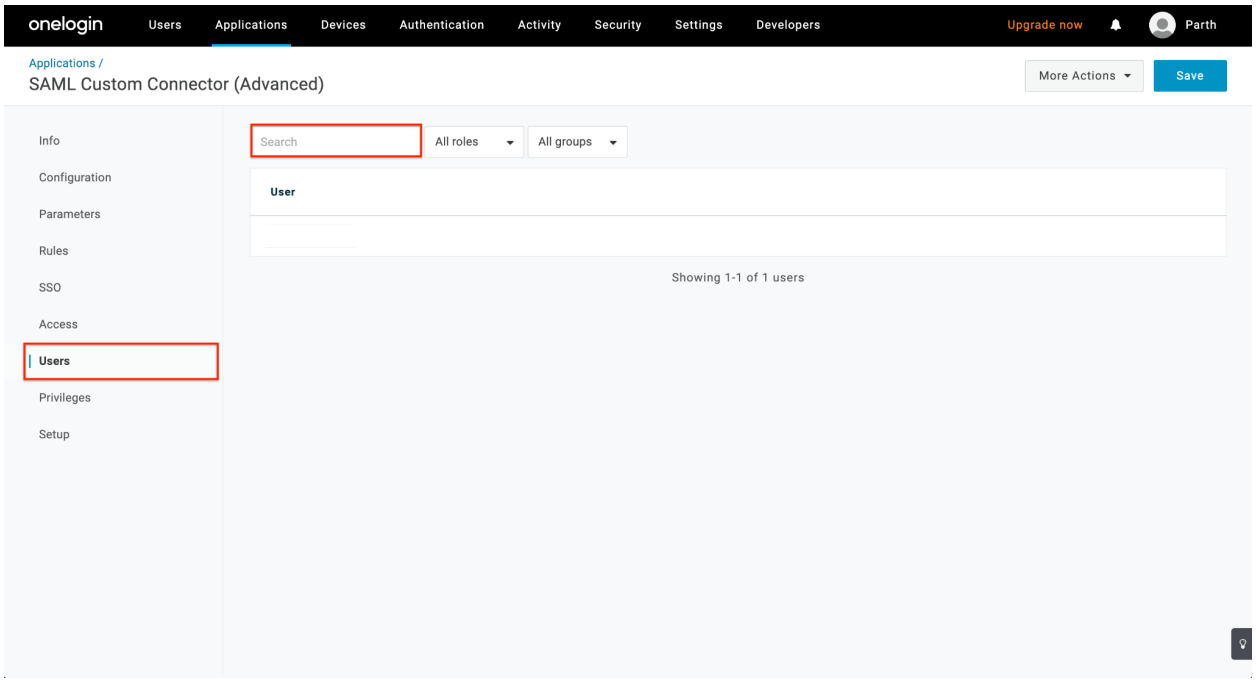
1. email
2. firstname
3. lastname






onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers
Upgrade now
Parth
Applications /
SAML Custom Connector (Advanced)
More Actions
Save
Info
Configuration
Parameters
Rules
SSO
Access
Users
Privileges
Setup
Credentials are
Configured by admin
Configured by admins
SAML Custom Connect
NameID value
email
custom parameter
Edit Field email
Name
email
Value
Email
Flags
Include in SAML assertion
Cancel
Delete
Save


onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers
Upgrade now
Parth
Applications /
SAML Custom Connector (Advanced)
More Actions
Save
Info
Configuration
Parameters
Rules
SSO
Access
Users
Privileges
Setup
Credentials are
Configured by admin
Configured by admins and shared by all users
SAML Custom Connector (Advanced) Field
Value
NameID value
Email
email
Email
custom parameter
firstname
First Name
custom parameter
lastname
Last Name
custom parameter

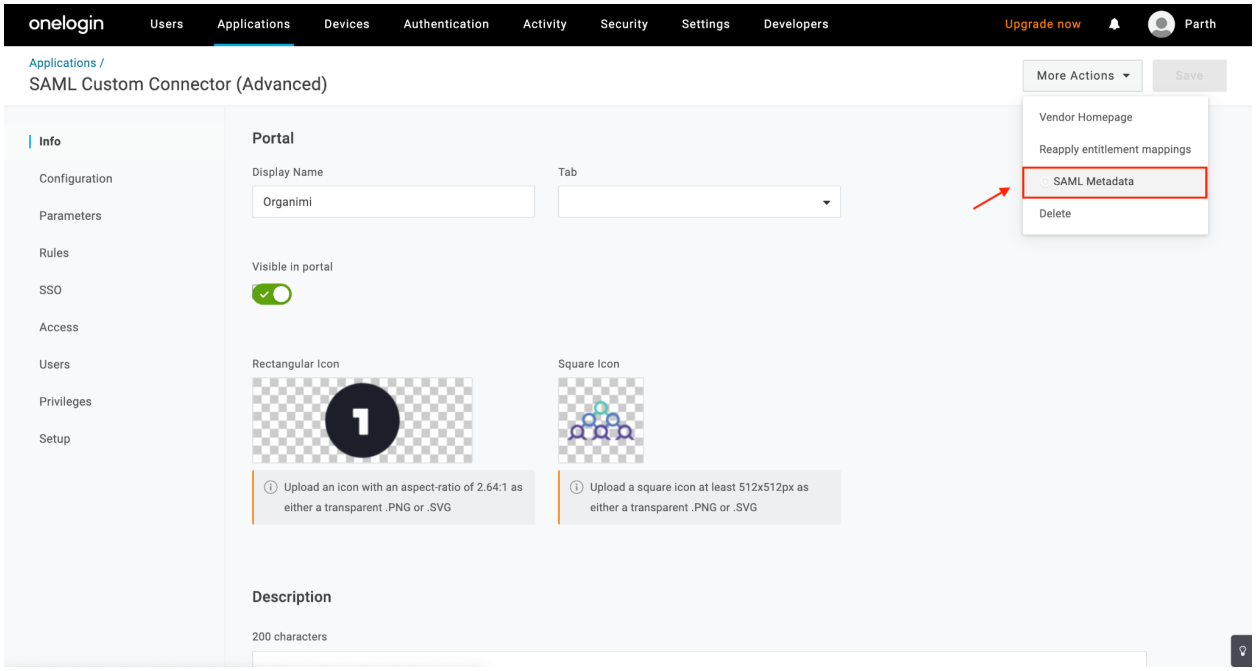


Once all the users are assigned and configured, click Save at the top-right.

Step 4

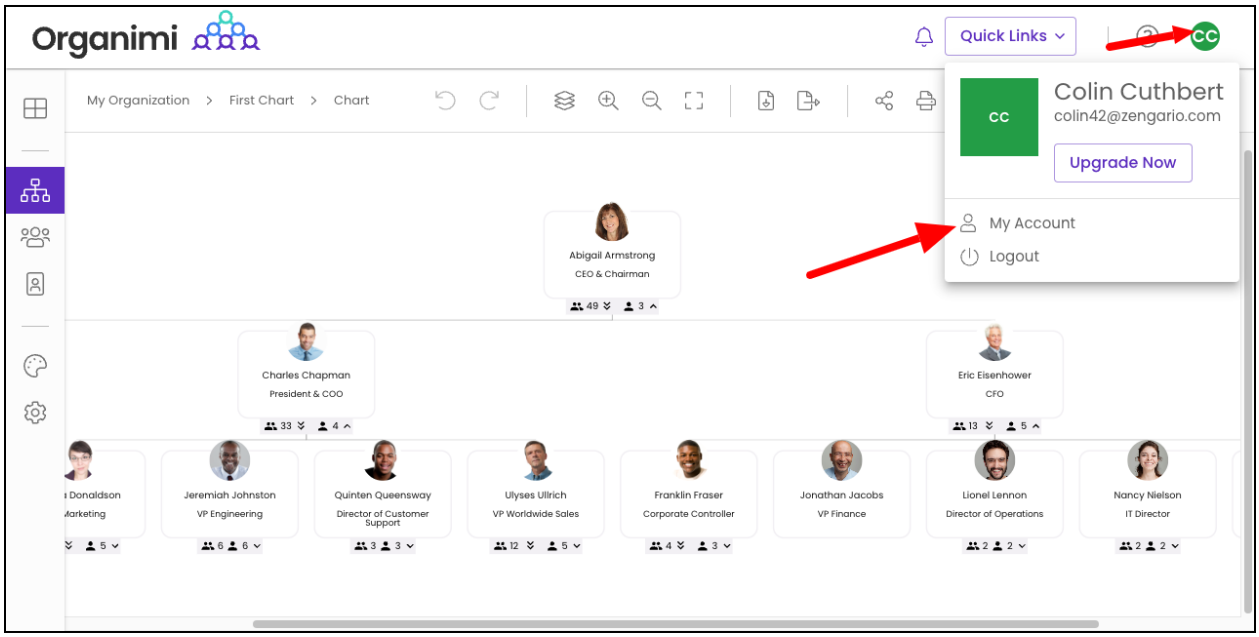
Now that the Organimi App is set up at the OneLogin side, we now have to configure this IDP in Organimi.

Click on “More Actions” for the Organimi app in OneLogin and select “SAML Metadata” and save the downloaded file to a place you can find it easily … you will be using the downloaded file in step 6 on the Organimi app setup.



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.

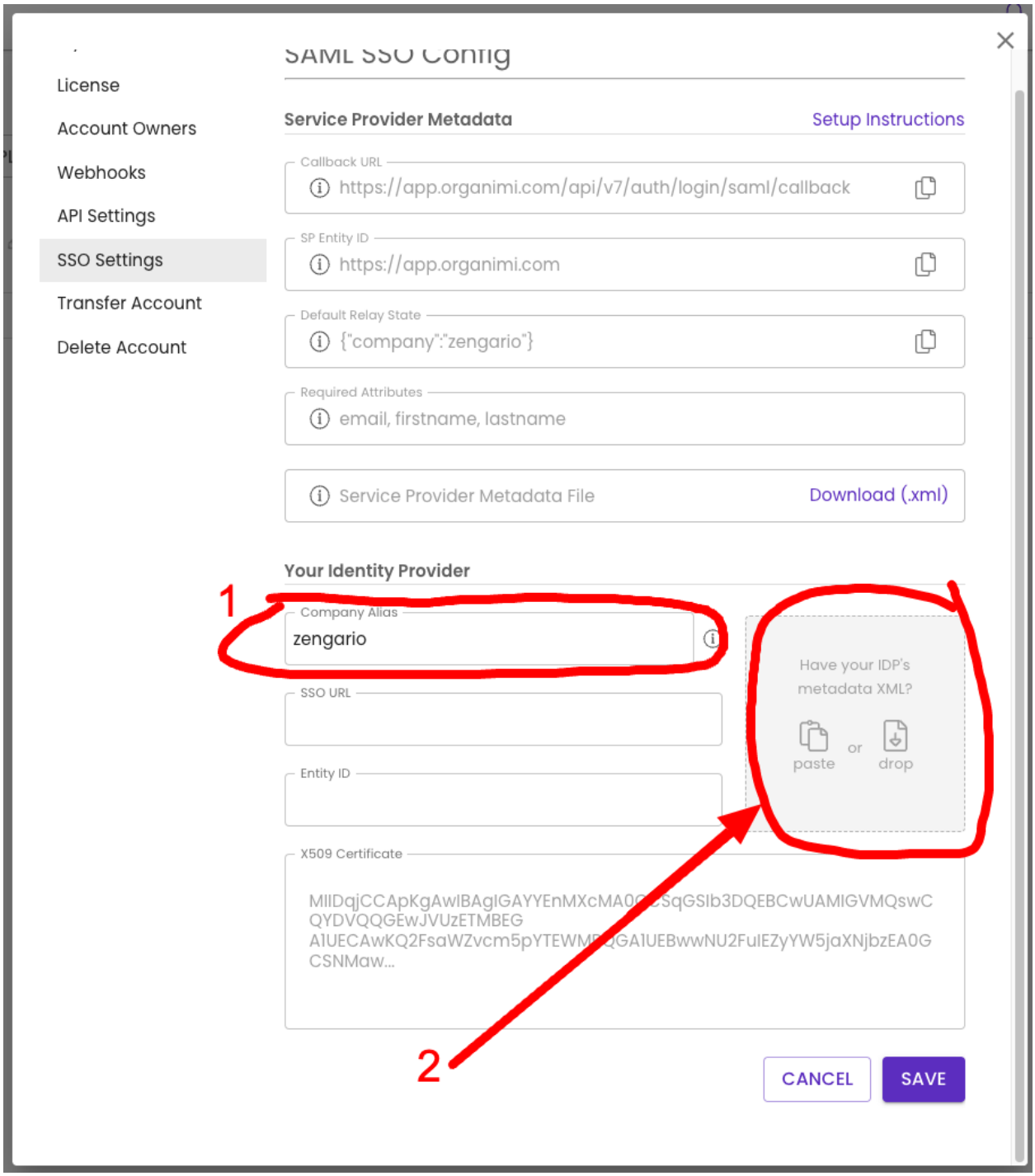


Note: if you don’t see the “SSO Settings” tab or it shows that SSO is not enabled for your account ? Please contact Organimi at support@organimi.com to have SSO enabled for your account. A premium account is required to enable SSO

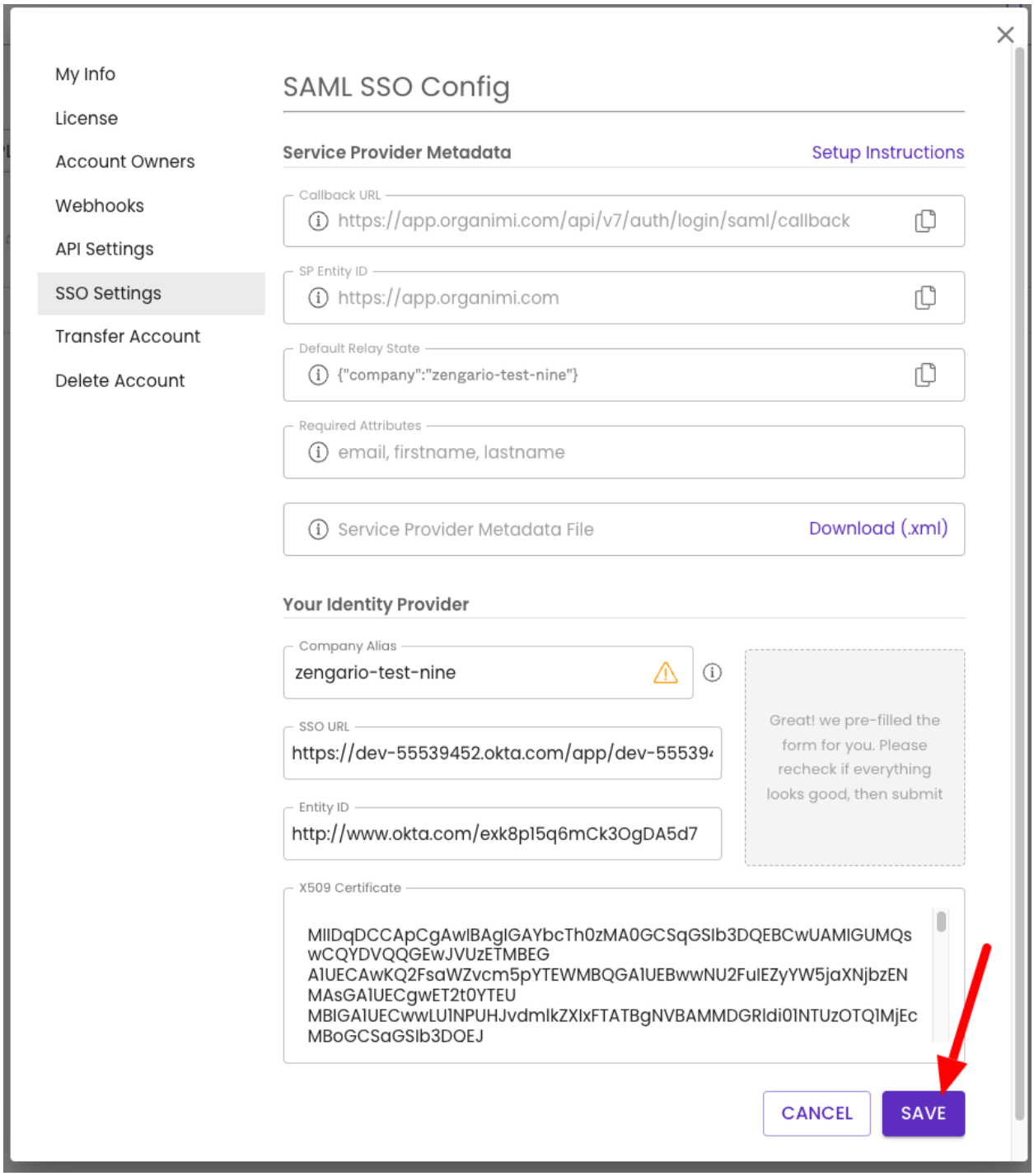
Step 6

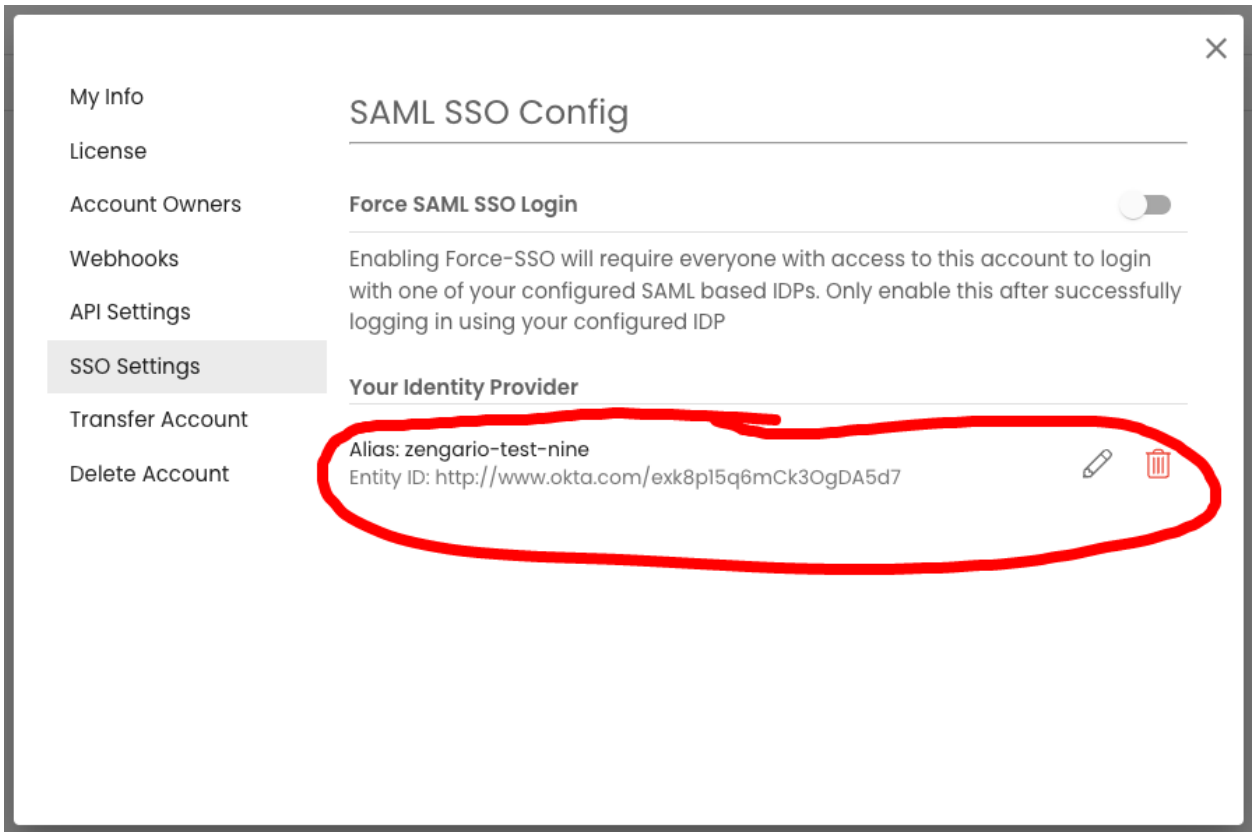
Click on the “Configure IDP” button and enter:

1. **Company Alias: Enter your company name. It should match exactly with the name entered for step 3.1 in place of the** “YOUR-COMPANY-ALIAS” **placeholder.**
2. IDP Metadata: Drag and drop the file that was downloaded in step 4 in to the “drop area” as highlighted below (click in the gray box and then paste)



3. Click the SAVE button





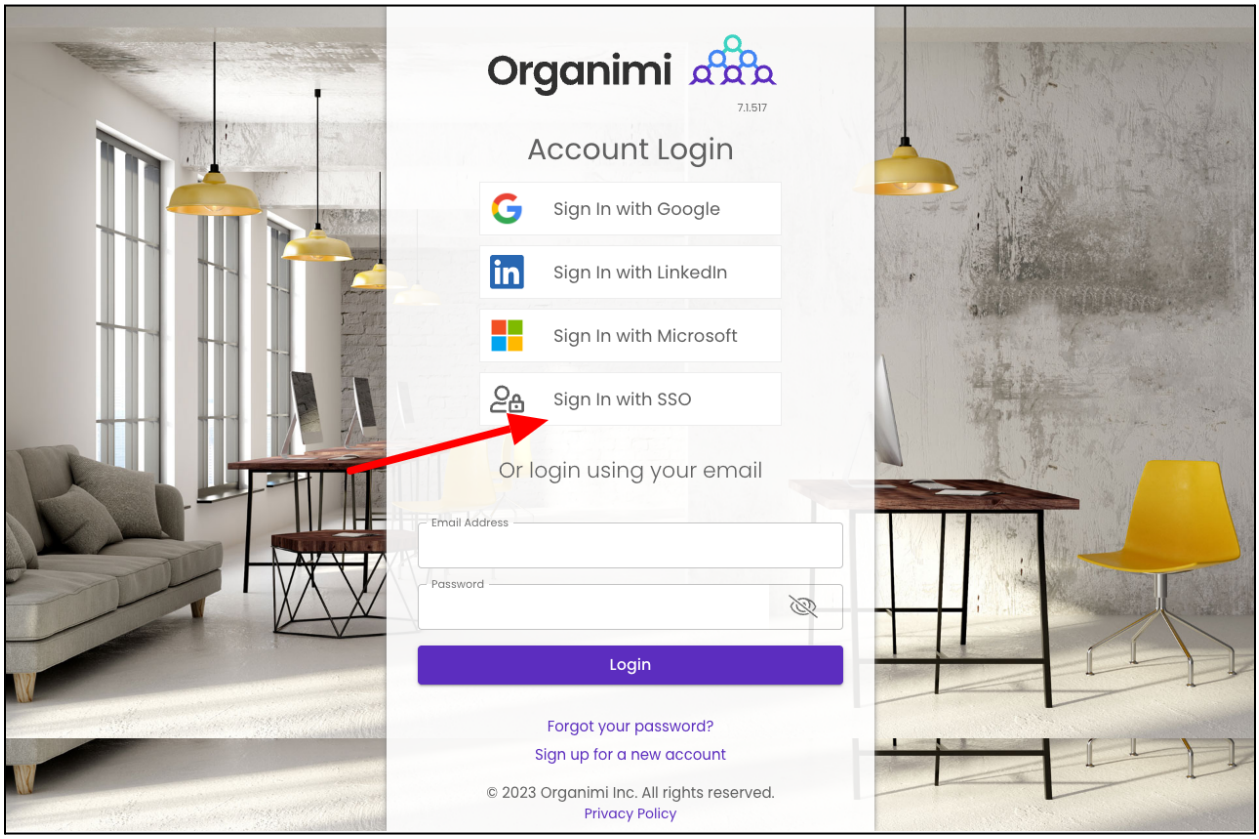
Step 7

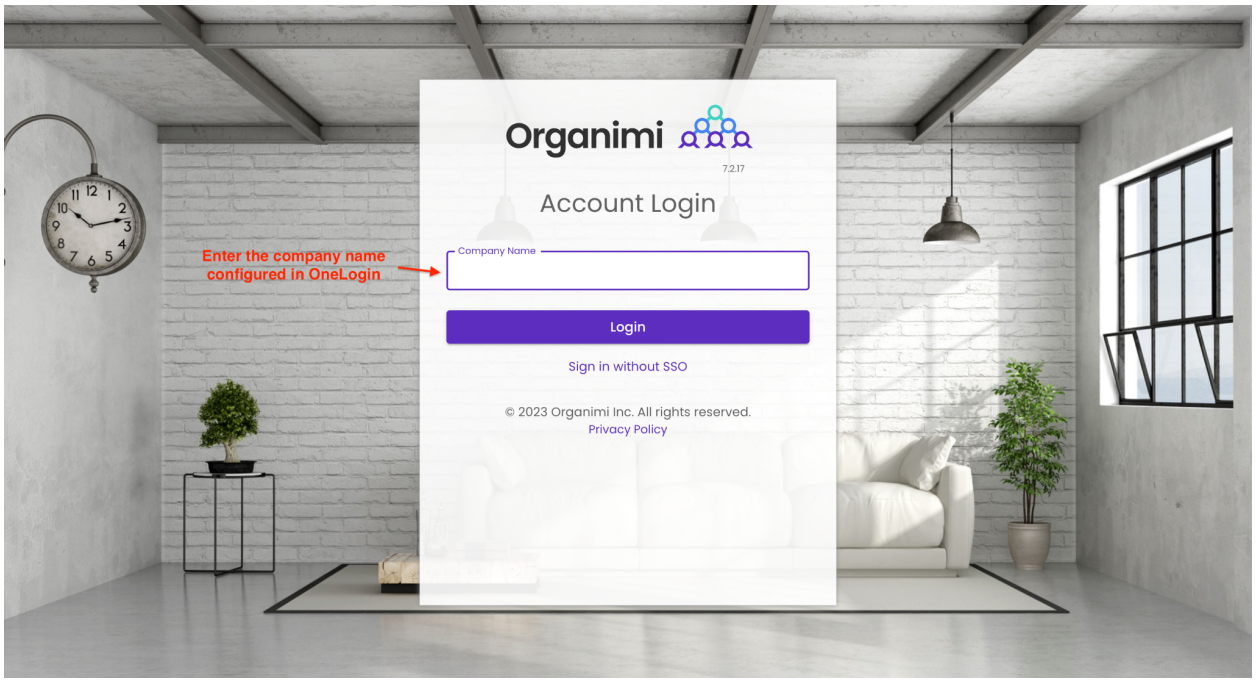
Your Identity Provider should show the OneLogin Entity ID that you just set up, which means IDP configuration is accepted.

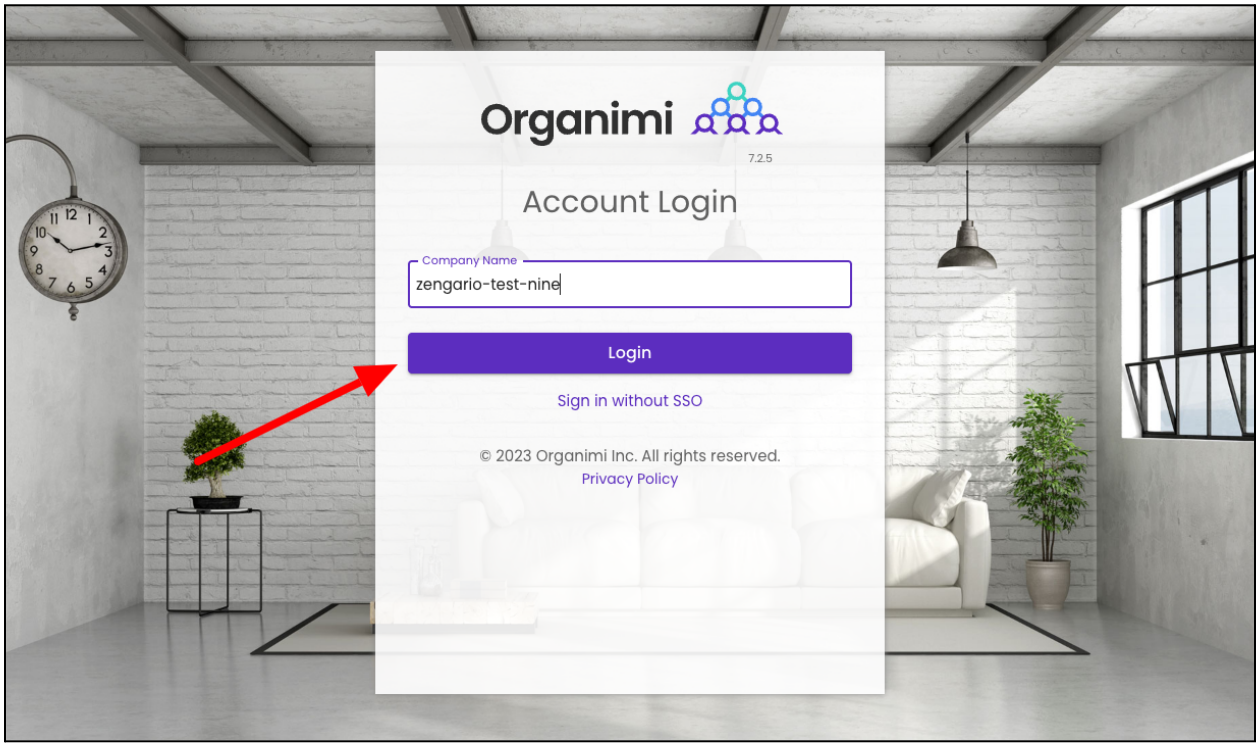
Note: If you do not reach to this point and see an error message on clicking the "SAVE" button, Contact Organimi support @ support@organimi.com

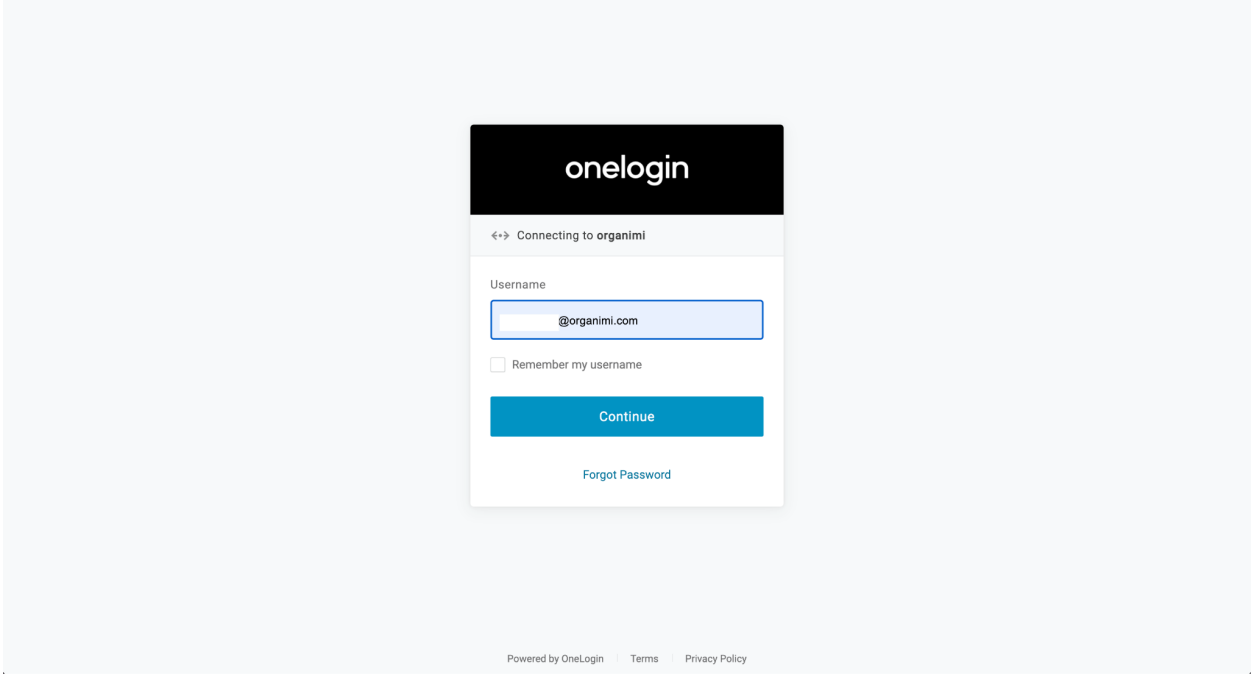
Now it's time to test logging in with your configured IDP. First logout from your account. Then login by clicking “Sign in with SSO”. In the next screen, type in the company name matching from step 3.4 & 6.1 and then click login.

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

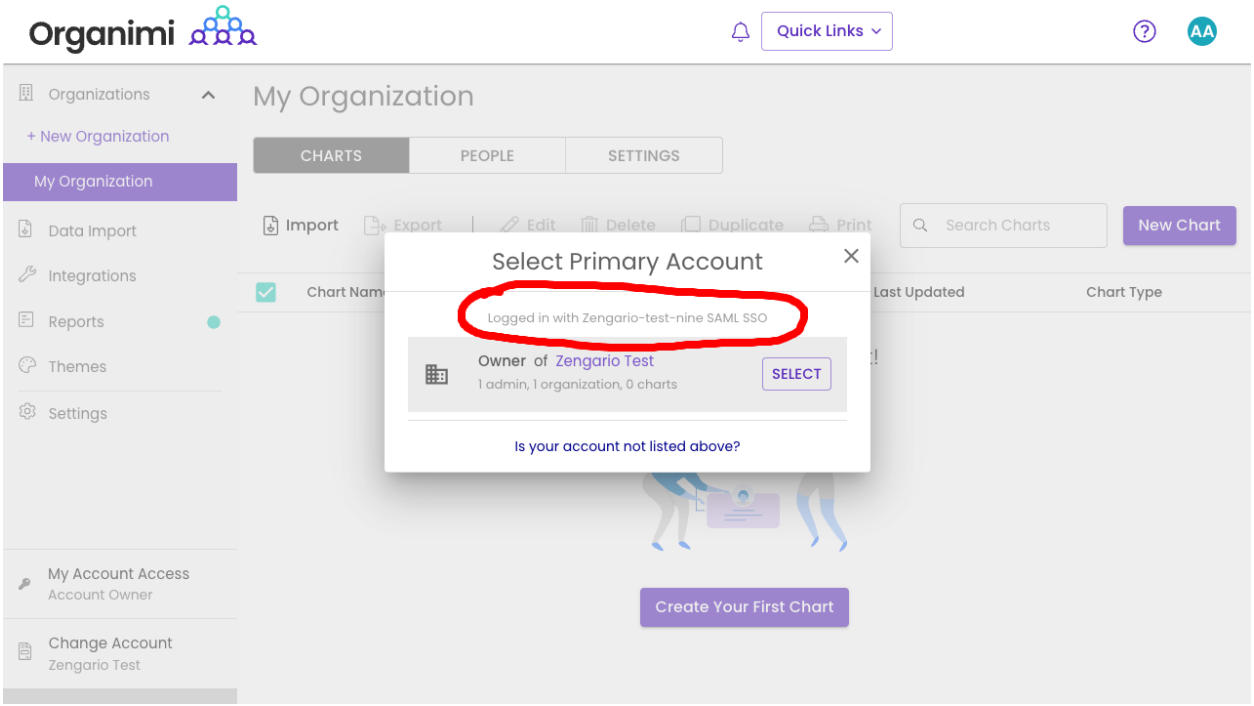



Organimi
7.2.17
Account Login
Enter the company name configured in OneLogin
Company Name
Login
Sign in without SSO
© 2023 Organimi Inc. All rights reserved.
Privacy Policy


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



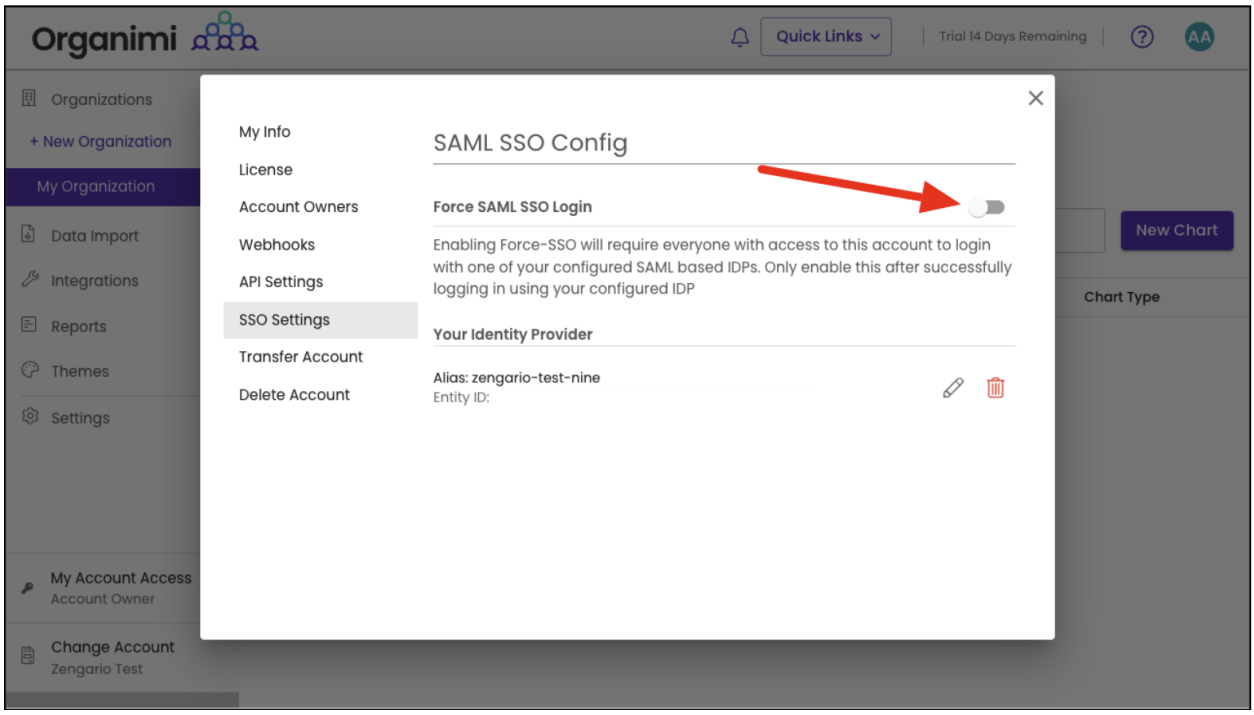
And you are in. If you click the Change Account link on the Organimi screen you will see that you are logged in with SAML SSO

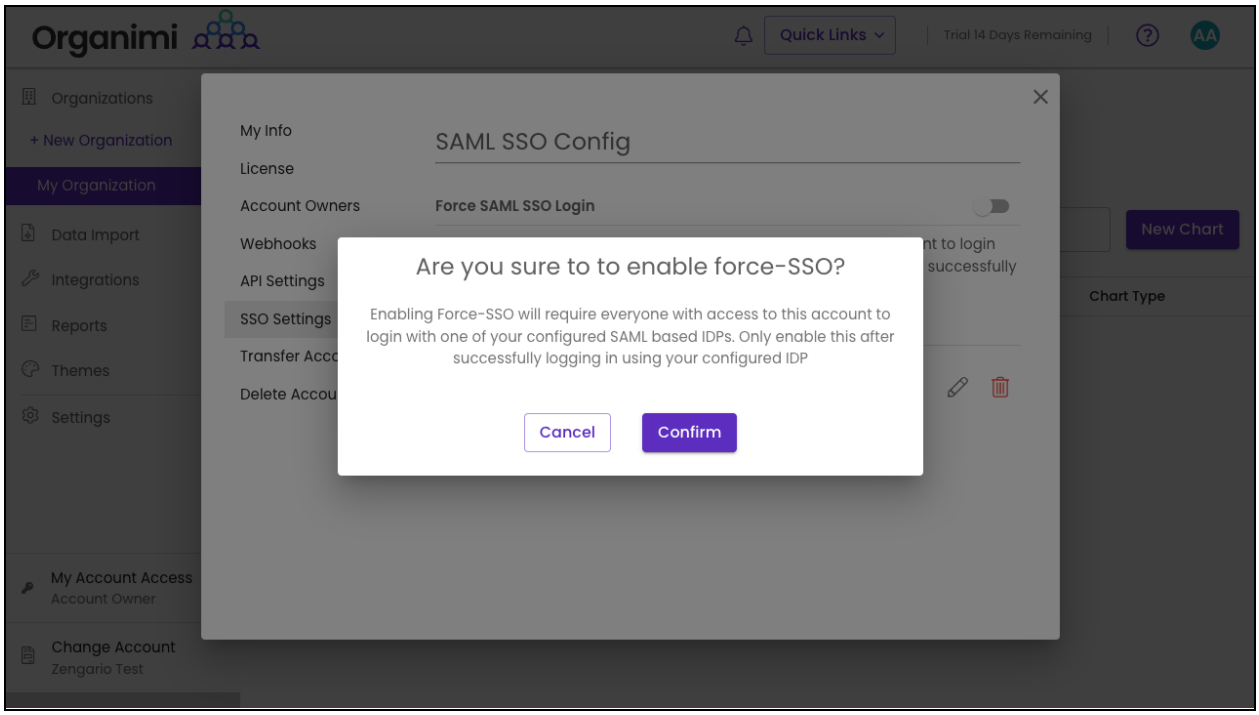


Step 8

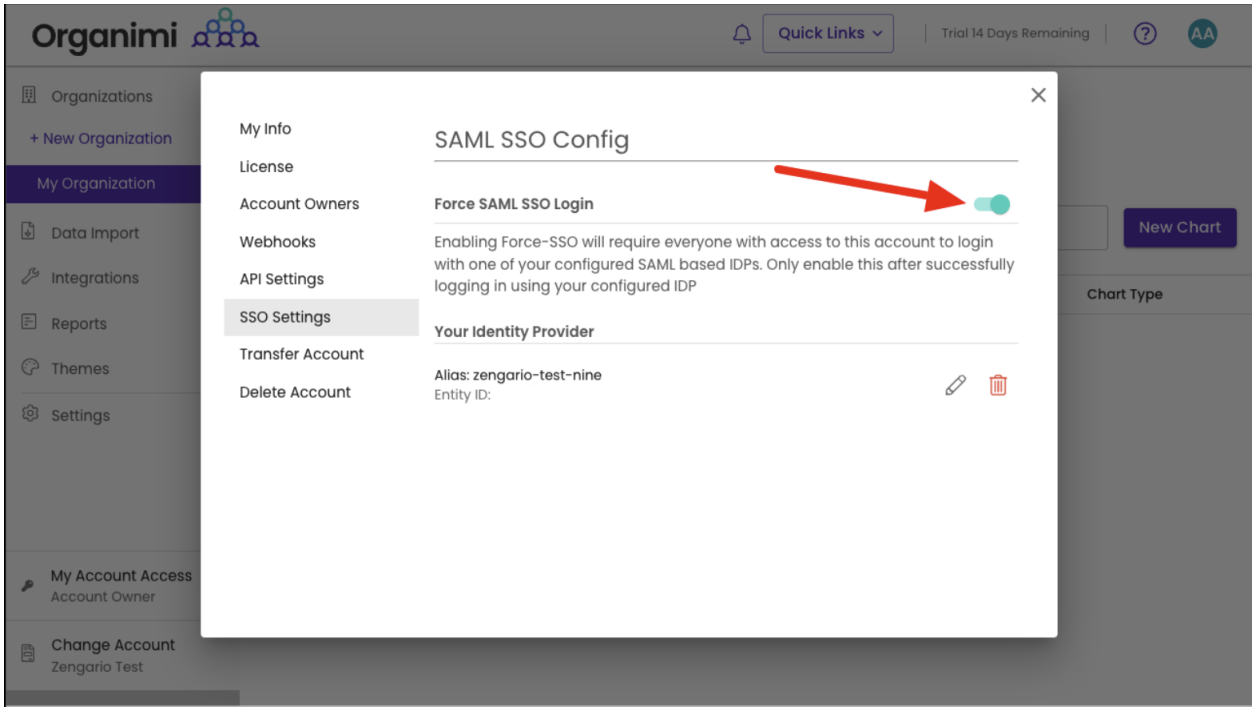
You can also enable “Force-SSO” from the configuration tab. Which will require everyone using this account (including you), to login using your configured IDP only, in order to access resources under this account. Other login methods (social & username/password) will not be allowed access to the account.

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.



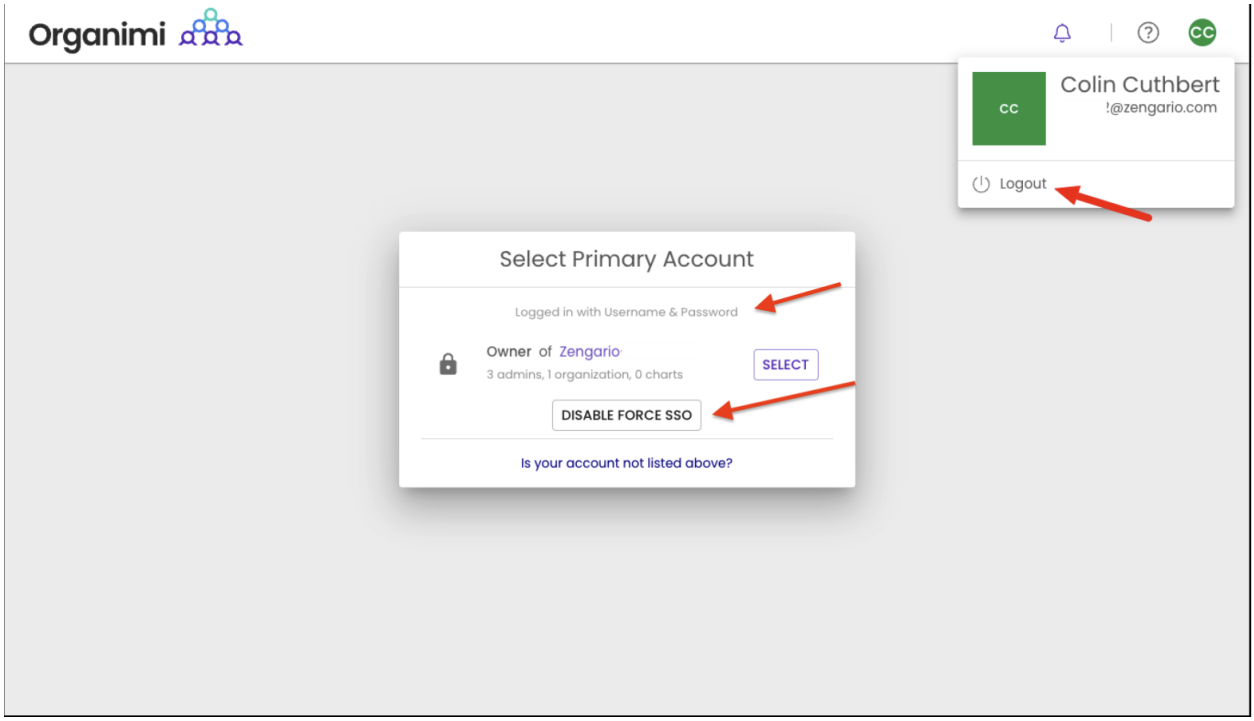


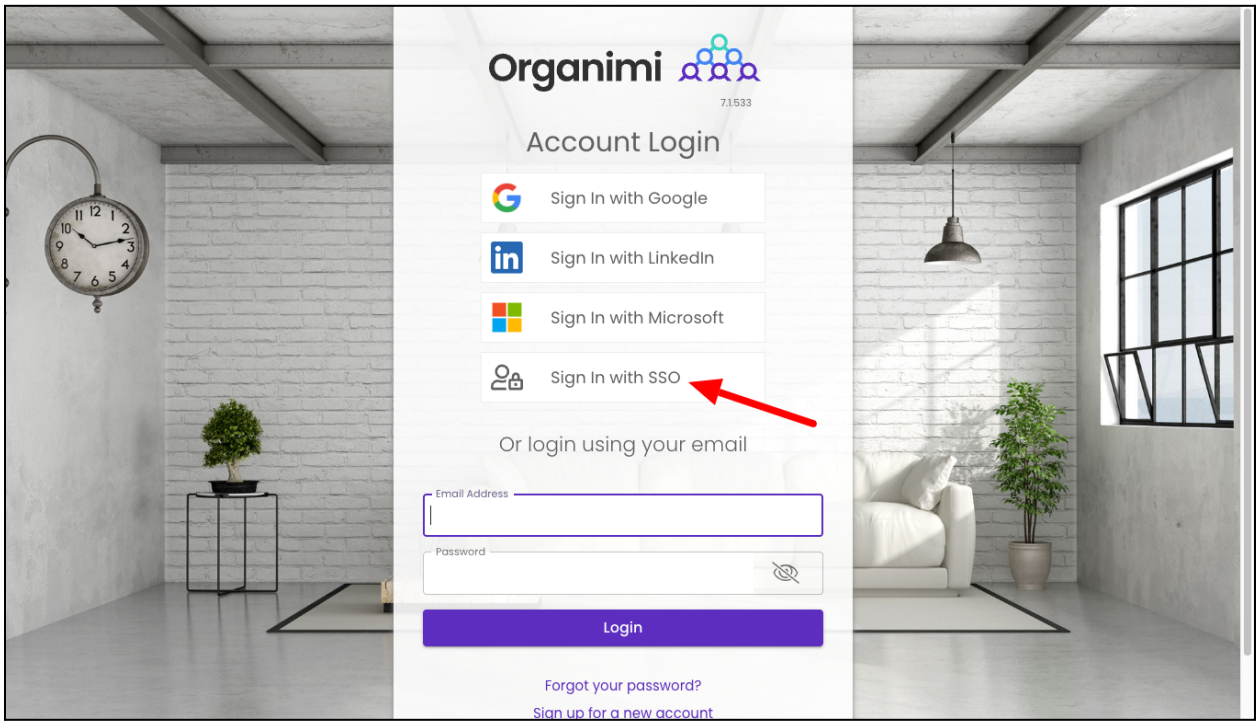
If you were logged into Organimi with you SSO IDP Account then you will just see that the switch is now on for “Force SSO”



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.

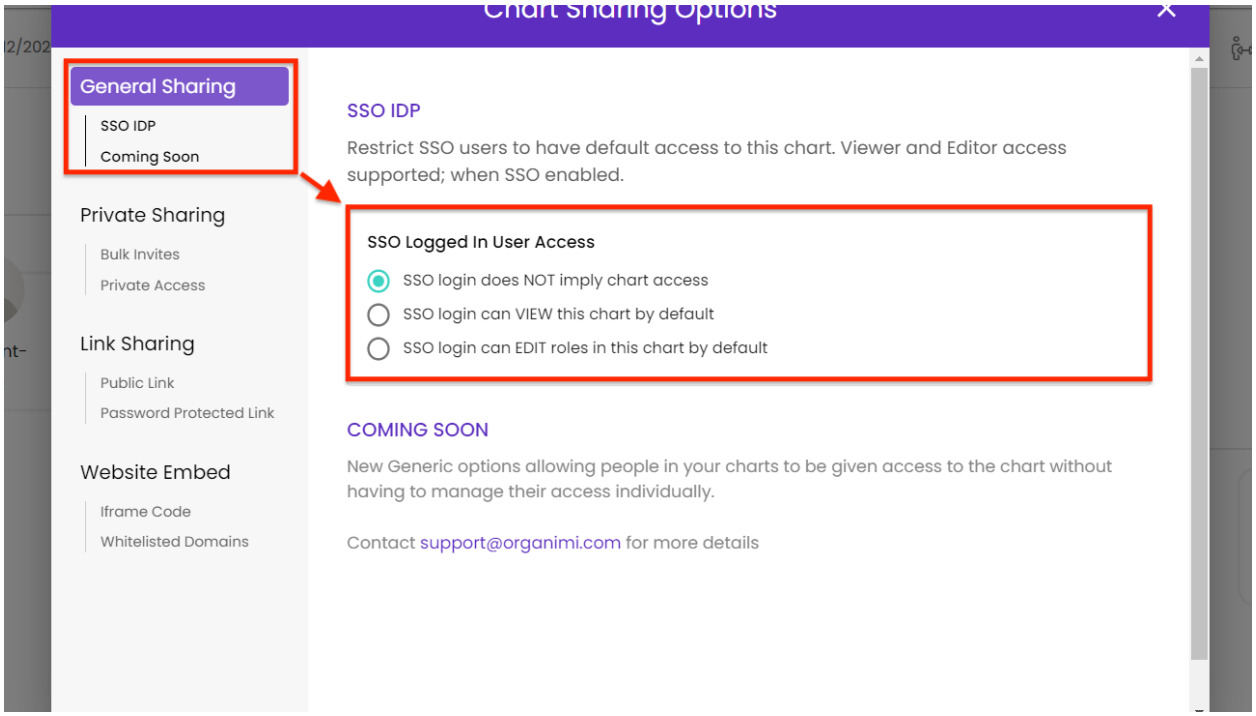




Default share settings for IDPs:

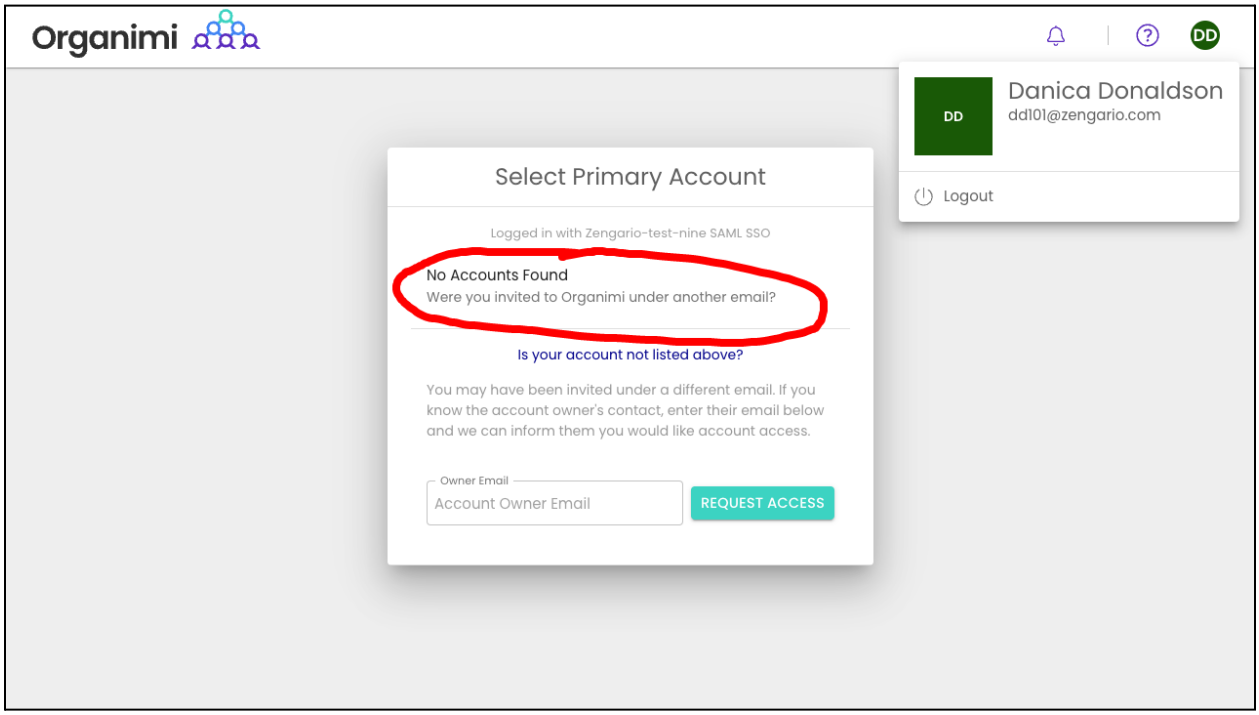
Alternatively users can be invited from the charts as editors or viewers by enabling default sharing settings for SSO IDP. This will not send any email invites to these users. They can login directly using the shared idp. These permissions can be changed, as needed.

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



Please Note …

If default sharing is not enabled as described above … in addition to provisioning the application to users in OneLogin 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 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.