

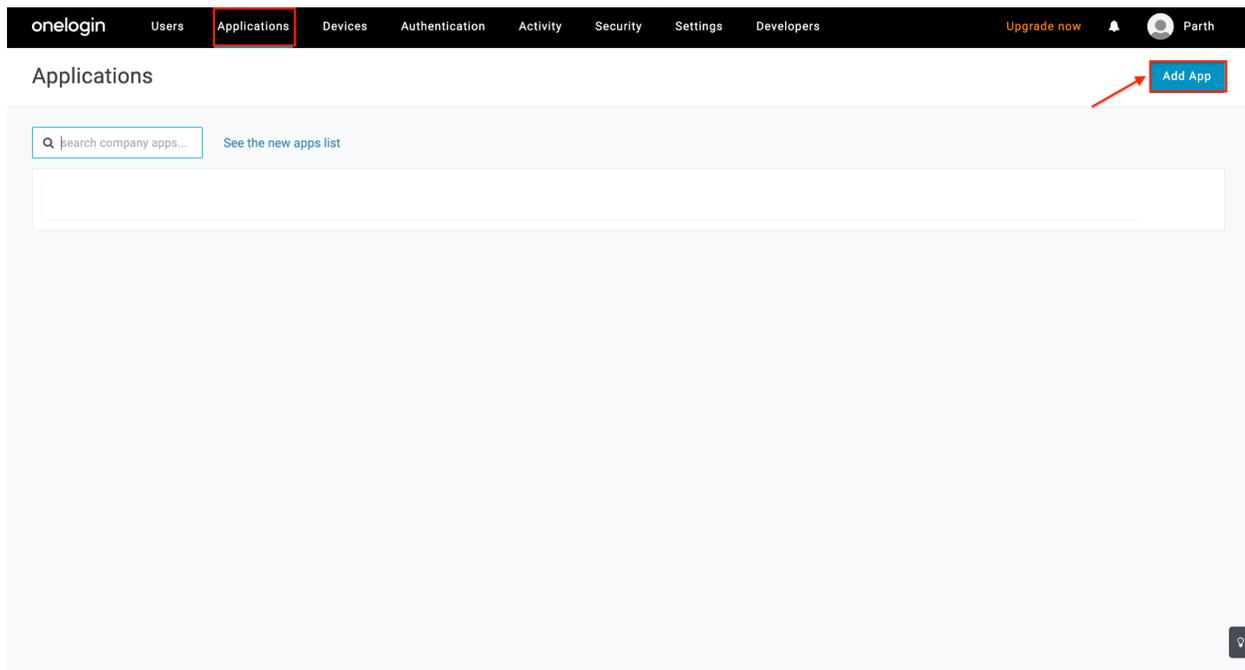


SAML based SSO - Login with OneLogin

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)"

onelogin Users Applications Devices Authentication Activity Security Settings Developers Upgrade now Parth

Find Applications

Search for "saml custom connector"

Select the highlighted app

1	SAML Custom Connector (Advanced) OneLogin, Inc.	SAML2.0
1	SAML Custom Connector (SP Shibboleth) OneLogin, Inc.	SAML2.0
	SAML Custom Connector (SP Shibboleth + Sign SLO) OneLogin, Inc.	SAML2.0

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](#))

onelogin Users Applications Devices Authentication Activity Security Settings Developers Upgrade now Parth

App Listing / Add SAML Custom Connector (Advanced) Cancel Save

Configuration

Portal

Display Name
Organimi

Visible in portal

Rectangular icon

Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Square icon

Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

Description
200 characters

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)

The screenshot shows the OneLogin configuration interface for a SAML Custom Connector. The 'Configuration' tab is active. The following fields are highlighted with red boxes and arrows:

- RelayState:** {"company":"your-company-name"}
- Audience (EntityID):** https://app.organimi.com
- ACS (Consumer) URL Validator*:** https://app.organimi.com/api/v7/auth/login/saml/callback
- ACS (Consumer) URL*:** https://app.organimi.com/api/v7/auth/login/saml/callback

Other fields visible include Recipient, Single Logout URL, and a 'Save' button.

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 Initiator.

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

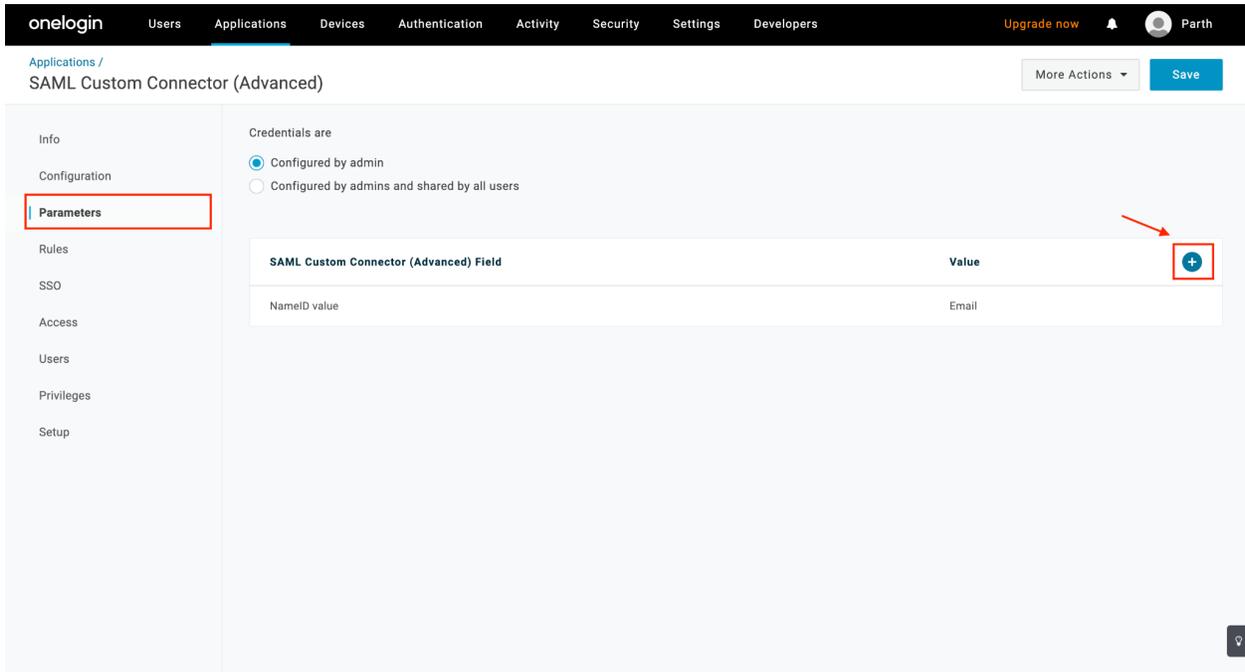
Specifies the time period, in minutes, the session is valid for. Default is 1440 minutes (24 Hours).

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.

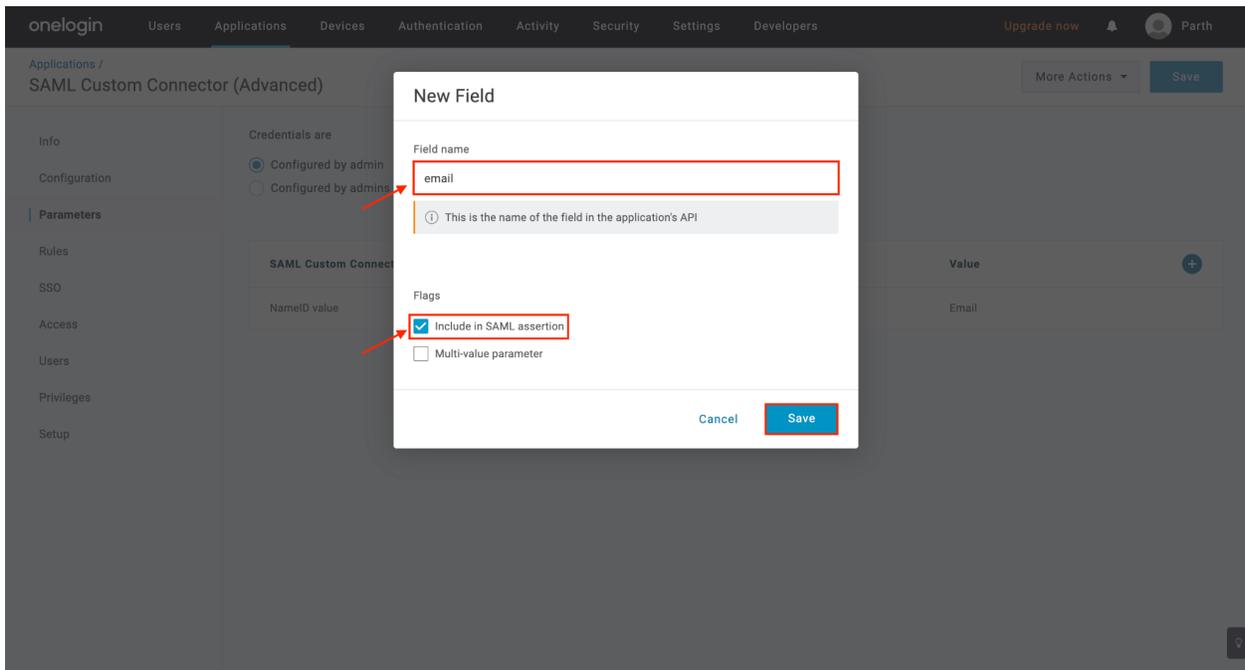
1. email
2. firstname
3. lastname



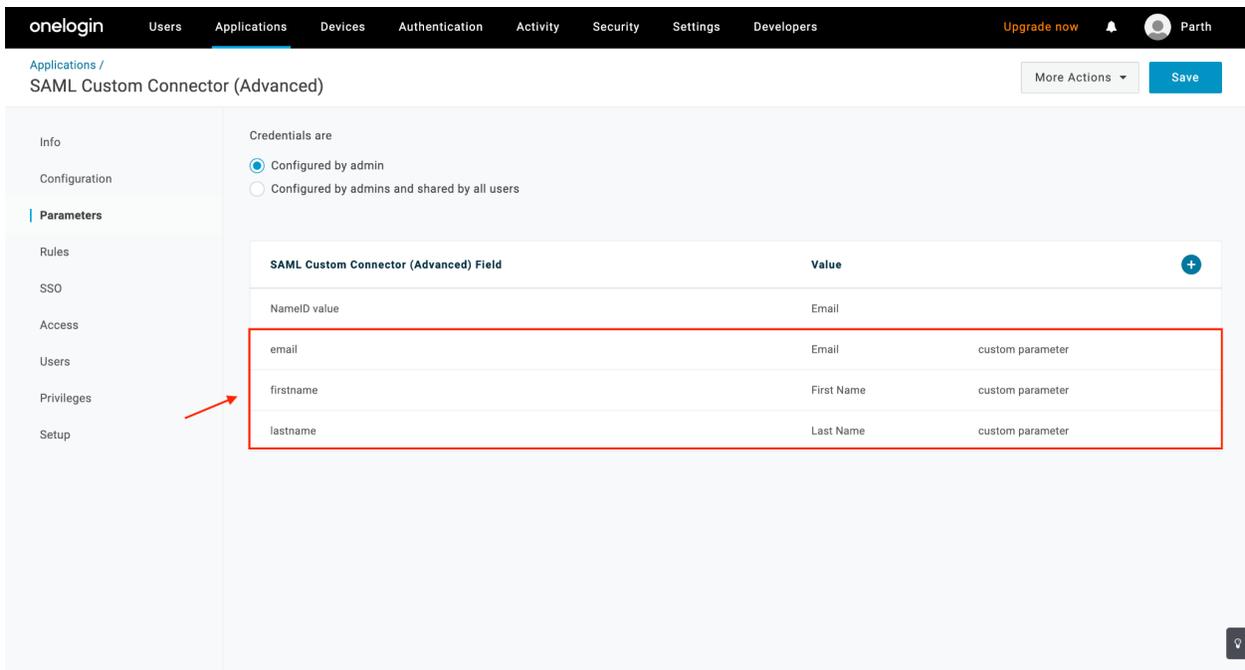
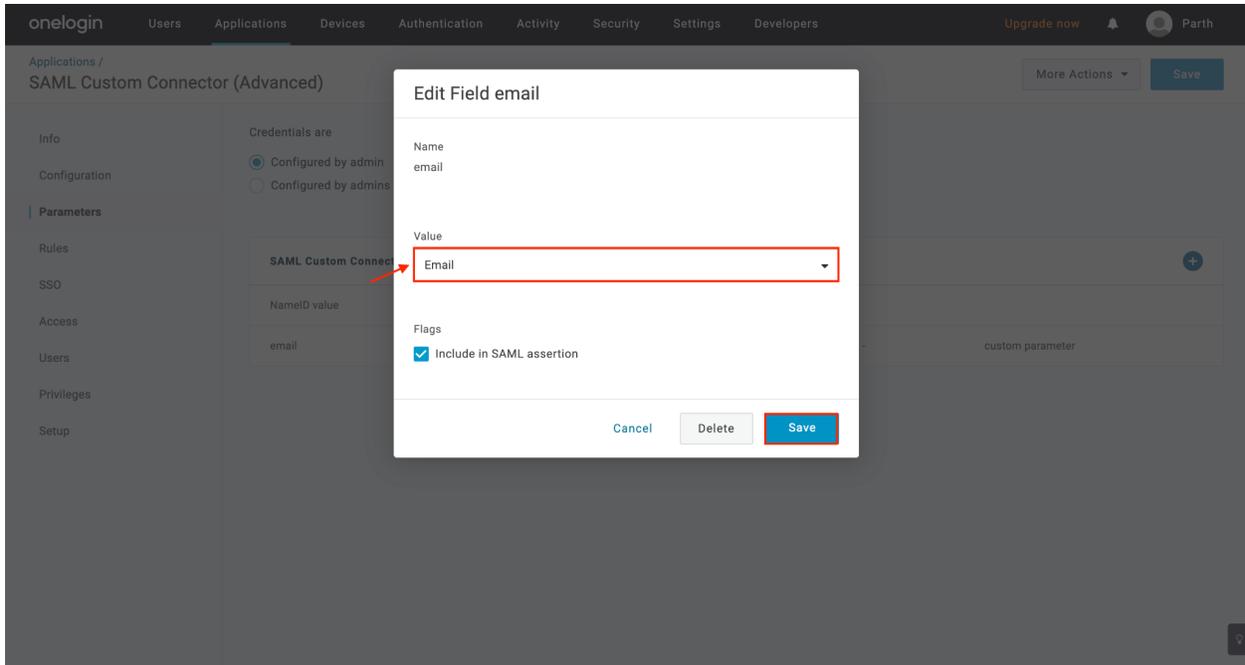
The screenshot shows the OneLogin interface for configuring a SAML Custom Connector. The left sidebar lists various configuration options, with "Parameters" highlighted. The main content area shows the "SAML Custom Connector (Advanced)" configuration. Under "Credentials are", the "Configured by admin" option is selected. A table lists the configured fields:

SAML Custom Connector (Advanced) Field	Value
NameID value	Email

A red box highlights a plus sign (+) in the top right corner of the table, indicating where to click to add a new field.



The screenshot shows the "New Field" dialog box in the OneLogin interface. The "Field name" is set to "email". Below the field name, there is a note: "This is the name of the field in the application's API". Under the "Flags" section, the "Include in SAML assertion" checkbox is checked, and the "Multi-value parameter" checkbox is unchecked. The "Save" button is highlighted in blue.



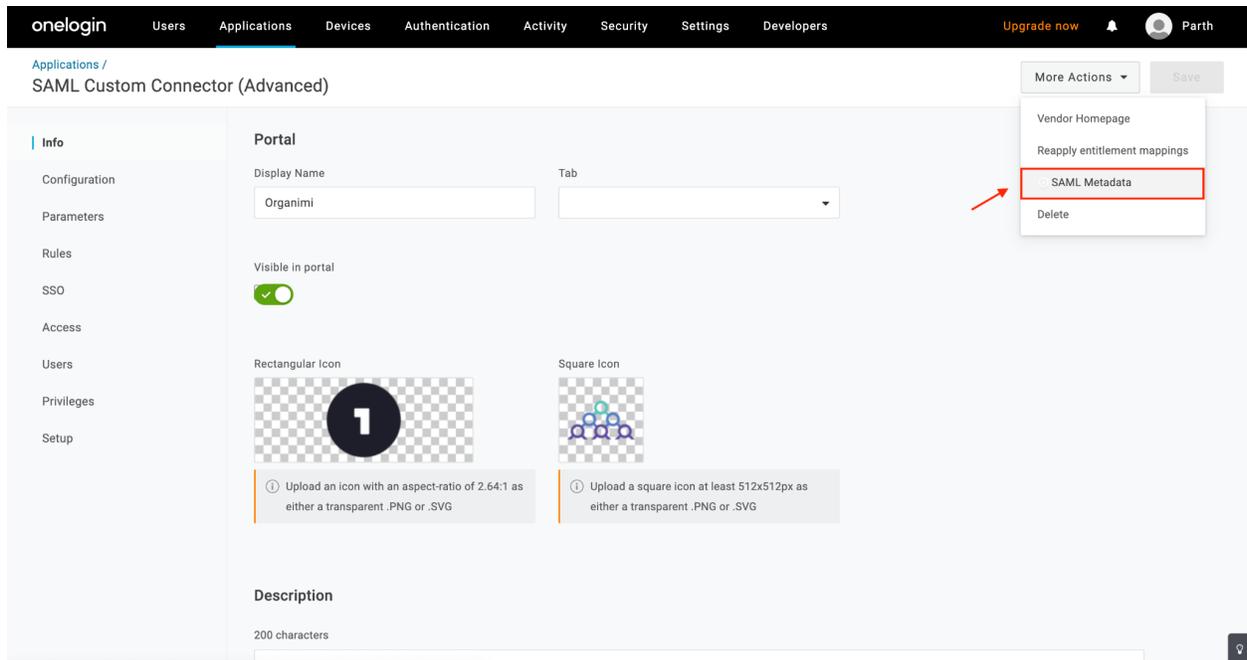
The screenshot displays the OneLogin interface for configuring a SAML Custom Connector. The top navigation bar includes 'onelogin' and various menu items: Users, Applications, Devices, Authentication, Activity, Security, Settings, and Developers. The user 'Parth' is logged in, with an 'Upgrade now' notification. The main content area is titled 'Applications / SAML Custom Connector (Advanced)' and features a 'More Actions' dropdown and a 'Save' button. On the left, a sidebar lists configuration options: Info, Configuration, Parameters, Rules, SSO, Access, Users (highlighted with a red box), Privileges, and Setup. The main area contains a search bar (also highlighted with a red box), filters for 'All roles' and 'All groups', and a table with one user. The table header is 'User' and the content area shows 'Showing 1-1 of 1 users'. A small help icon is visible in the bottom right corner.

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.

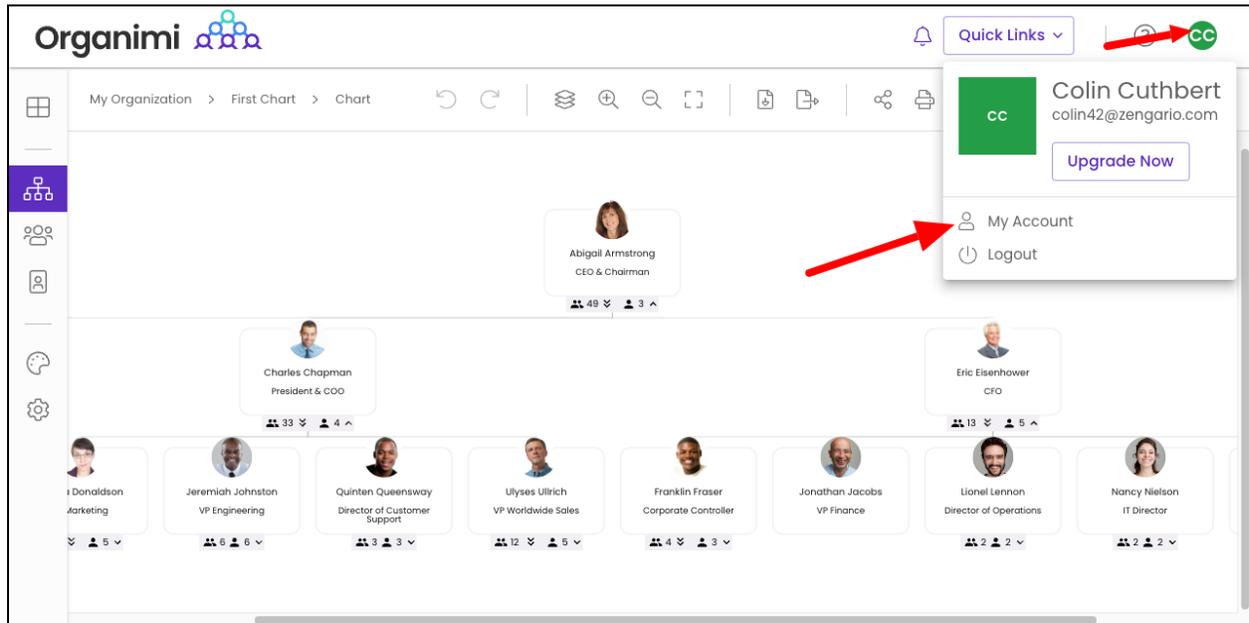
Click on “More Actions” for the Organimi app in OneLogin and select “SAML Metadata” and save the downloaded file to a place you can find it easily ... you will be using the downloaded file in step 6 on the Organimi app setup.



The screenshot shows the OneLogin interface for configuring a SAML Custom Connector. The top navigation bar includes 'onelogin', 'Users', 'Applications', 'Devices', 'Authentication', 'Activity', 'Security', 'Settings', and 'Developers'. The user 'Parth' is logged in. The main content area is titled 'SAML Custom Connector (Advanced)'. On the left, a sidebar menu lists 'Info', 'Configuration', 'Parameters', 'Rules', 'SSO', 'Access', 'Users', 'Privileges', and 'Setup'. The 'Portal' section is active, showing 'Display Name' as 'Organimi' and a 'Tab' dropdown. The 'Visible in portal' toggle is turned on. There are two icon upload sections: 'Rectangular Icon' (with a 2:1 aspect ratio icon) and 'Square Icon' (with a 1:1 aspect ratio icon). A 'More Actions' dropdown menu is open, with 'SAML Metadata' highlighted by a red box and a red arrow pointing to it. Other options in the menu are 'Vendor Homepage', 'Reapply entitlement mappings', and 'Delete'. A 'Save' button is visible in the top right corner of the configuration area.

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.



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". A red arrow points to the "My Account" option in the dropdown menu. The main content area shows a hierarchical organizational chart with several levels of employees, including Abigail Armstrong (CEO & Chairman), Charles Chapman (President & COO), and Eric Eisenhower (CFO). Other employees listed include I Donaldson (Marketing), Jeremiah Johnston (VP Engineering), Quinten Queensway (Director of Customer Support), Ulyses Ullrich (VP Worldwide Sales), Franklin Fraser (Corporate Controller), Jonathan Jacobs (VP Finance), Lionel Lennan (Director of Operations), and Nancy Nielson (IT Director).

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)

SAML SSO CONFIG

License

Account Owners

Webhooks

API Settings

SSO Settings

Transfer Account

Delete Account

Service Provider Metadata [Setup Instructions](#)

Callback URL

SP Entity ID

Default Relay State

Required Attributes

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

Your Identity Provider

1 **Company Alias**

SSO URL

Entity ID

2 **Have your IDP's metadata XML?**

paste or drop

X509 Certificate

MIIDqjCCApKgAwIBAgIGAYYEnMXcMA0GCSqGSIb3DQEBCwUAMIGVMQswC
QYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcms5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzEA0G
CSNMaw...

[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

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

The screenshot shows a web interface for SAML SSO configuration. On the left is a sidebar 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 contains a toggle for 'Force SAML SSO Login' which is currently off. Below this is a section titled 'Your Identity Provider' which lists the following details: Alias: zengario-test-nine and Entity ID: http://www.okta.com/exk8p15q6mCk3OgDA5d7. A red hand-drawn circle highlights the alias and entity ID text, along with edit and delete icons to their right.

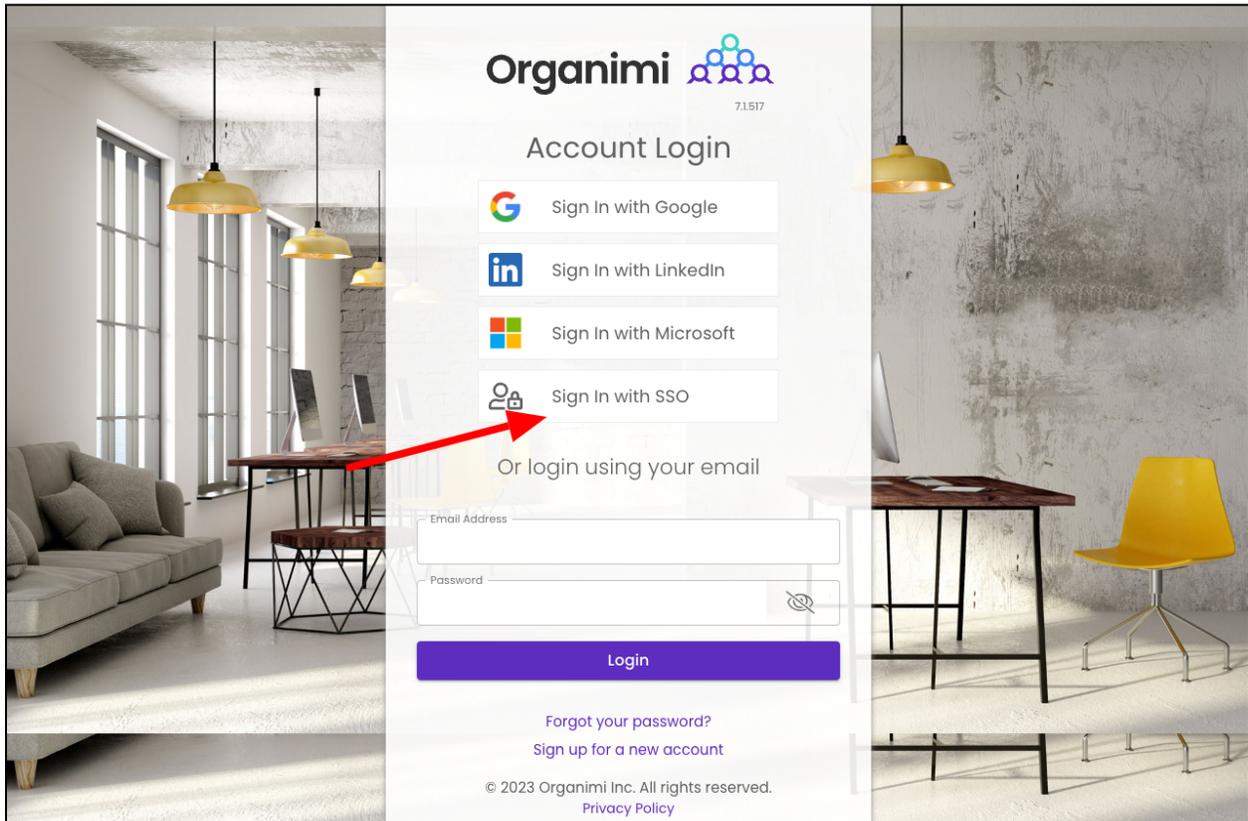
Step 7

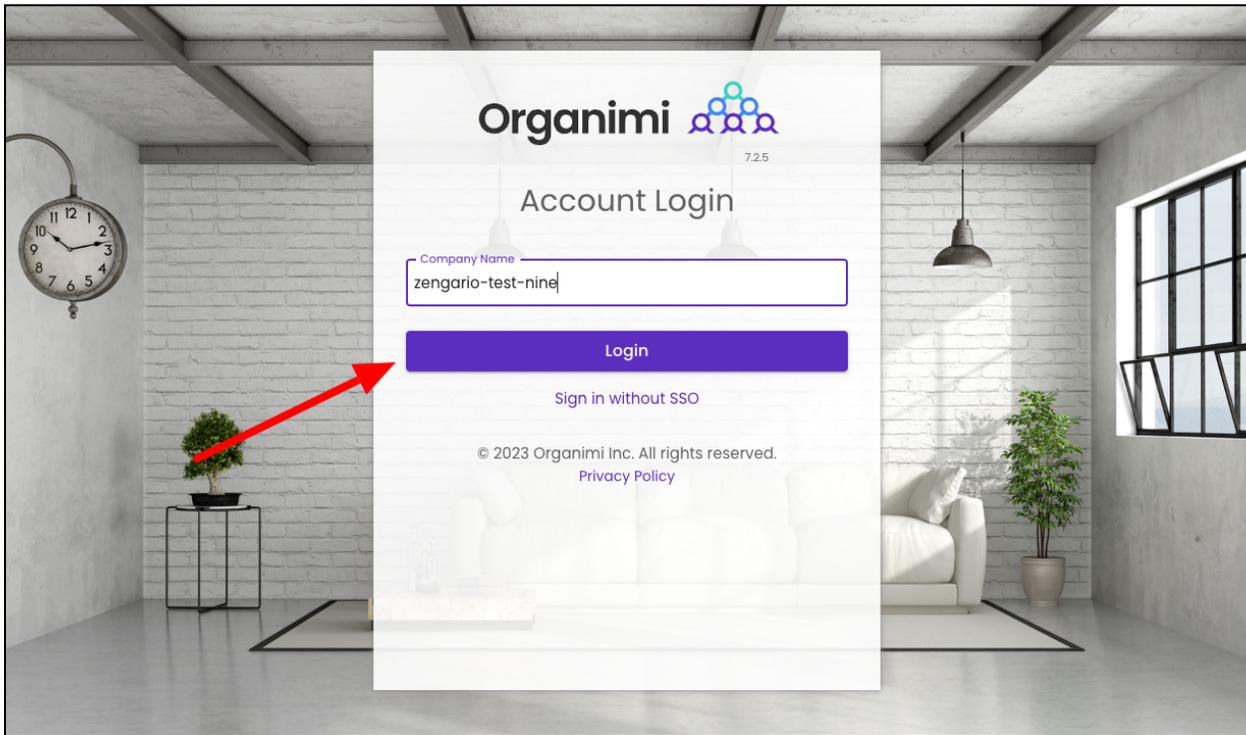
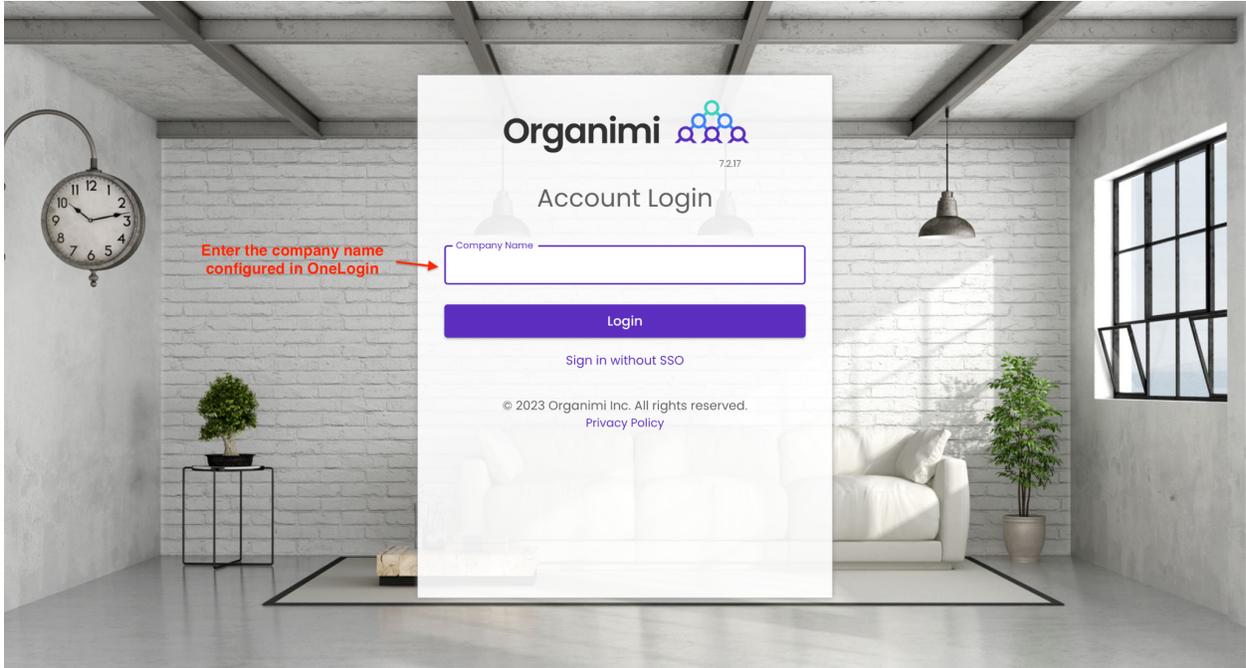
Your Identity Provider should show the OneLogin Entity ID that you just set up, which means IDP configuration is accepted.

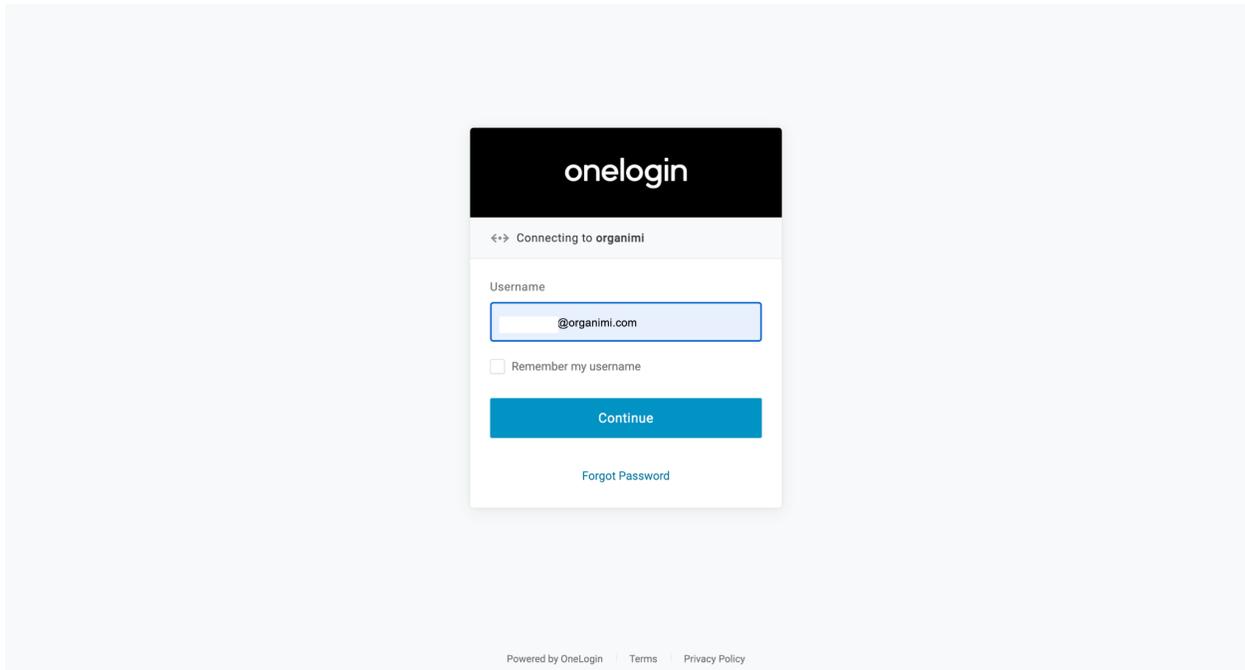
Note: If you do not reach to this point and see an error message on clicking the "SAVE" button, Contact Organimi support @ support@organimi.com

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.

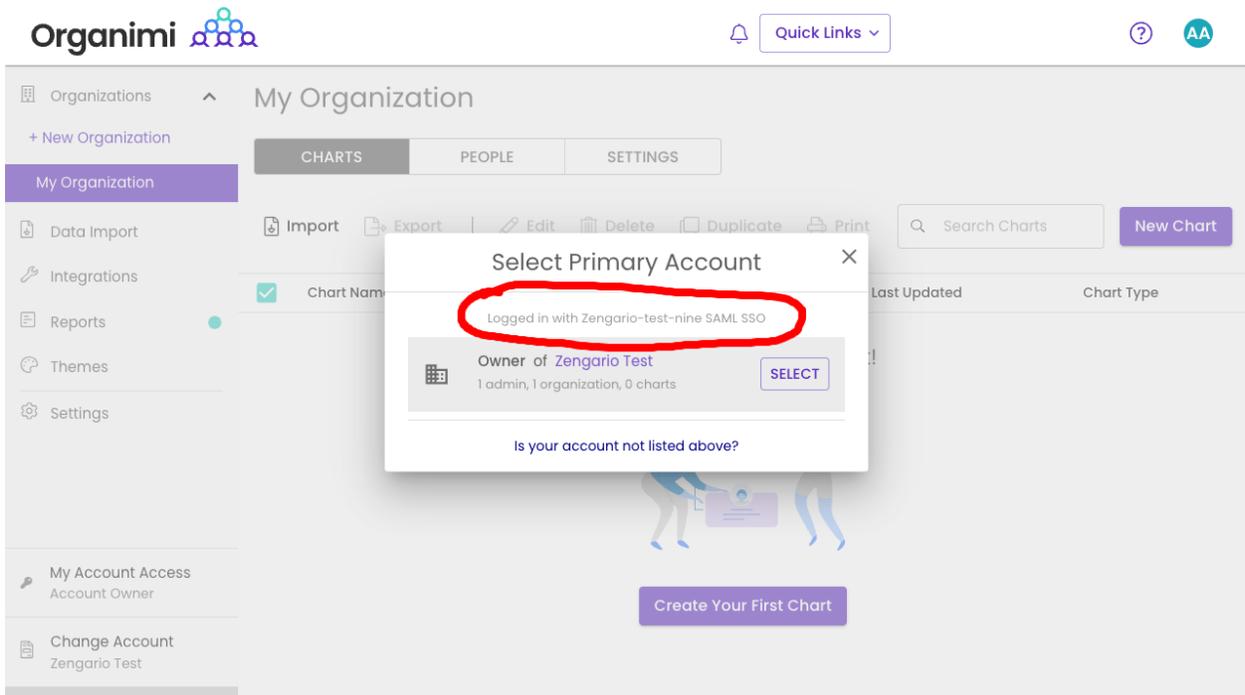
You should be redirected to your OneLogin IDP where you can get authenticated. Once successful, you will be redirected back to Organimi and will be logged in.







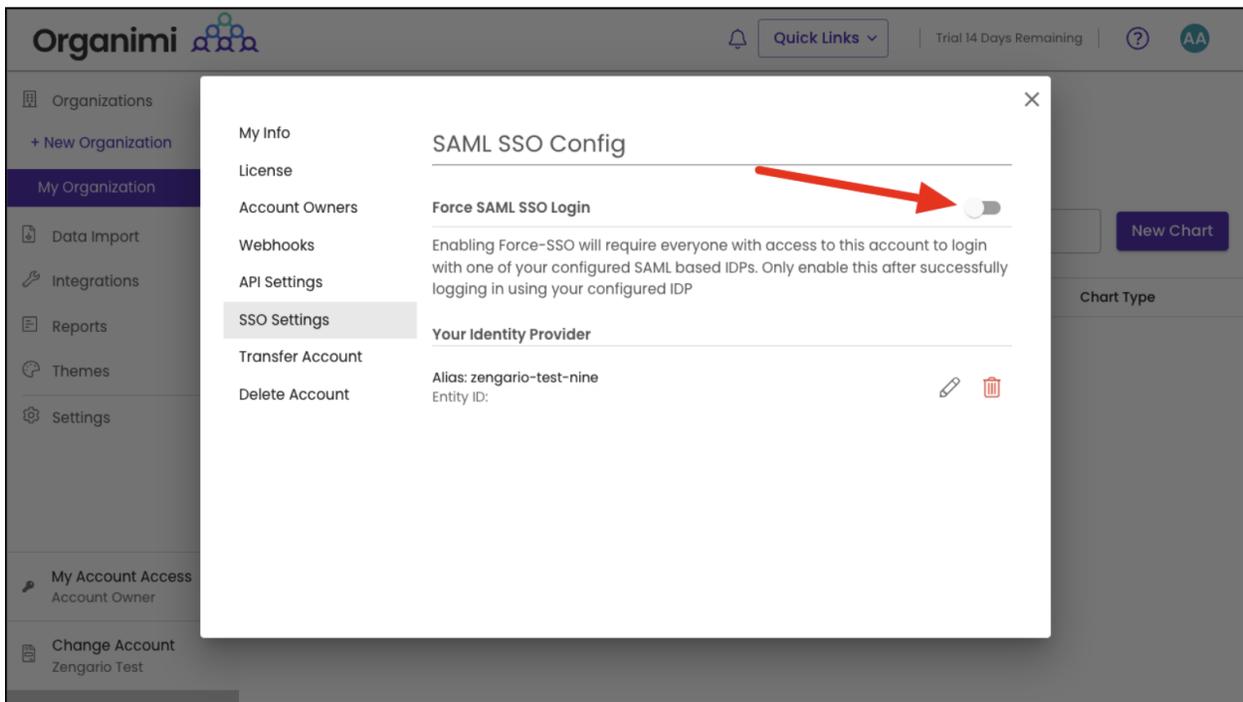
And you are in. If you click the Change Account link on the Organimi screen you will see that you are logged in with SAML SSO



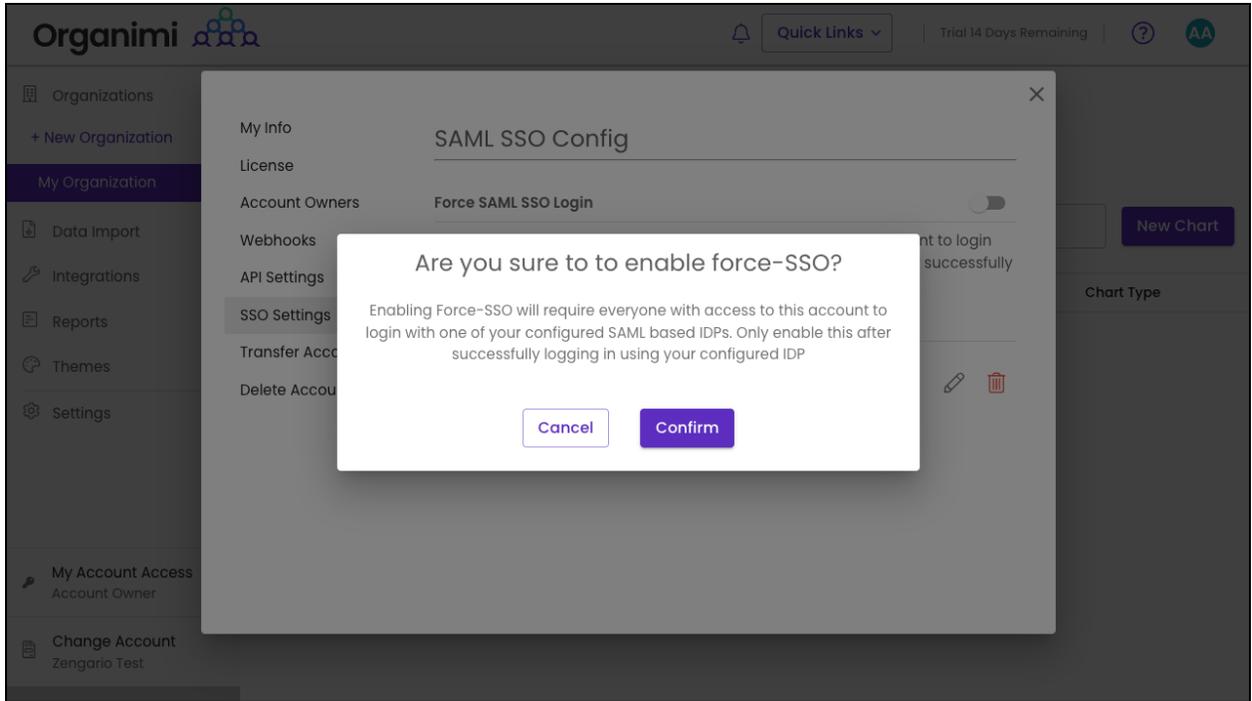
Step 8

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.

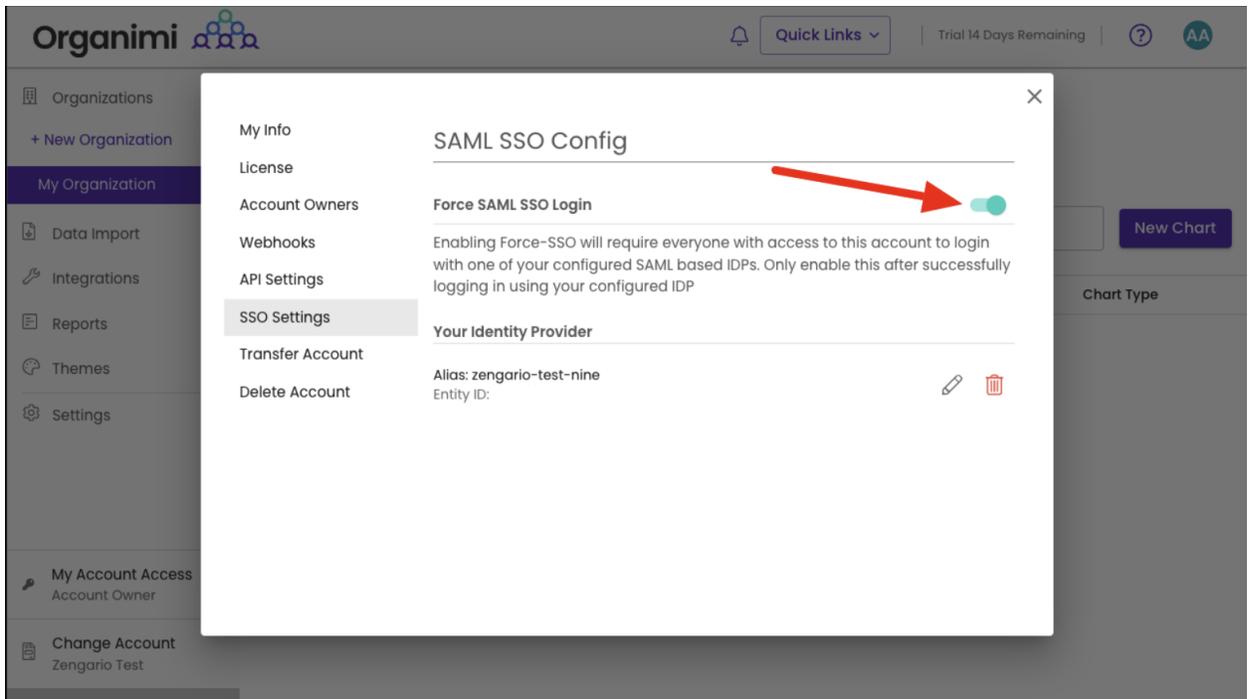
Note: As the account owner, It's recommended that you test logging in with your IDP first before turning on this setting, as you will not be able to access the account via any other login methods after you enable the “Force-SSO” option.



The screenshot shows the Organimi user interface. On the left is a sidebar menu with options: Organizations, + New Organization, My Organization (selected), Data Import, Integrations, Reports, Themes, Settings, My Account Access (Account Owner), and Change Account (Zengario Test). 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'. Under the 'Your Identity Provider' section, the 'Alias' is 'zengario-test-nine' and the 'Entity ID' is visible. There are edit and delete icons next to the Entity ID. The top of the page shows the Organimi logo, a 'Quick Links' dropdown, and a 'Trial 14 Days Remaining' notification. A 'New Chart' button is visible on the right side of the settings panel.

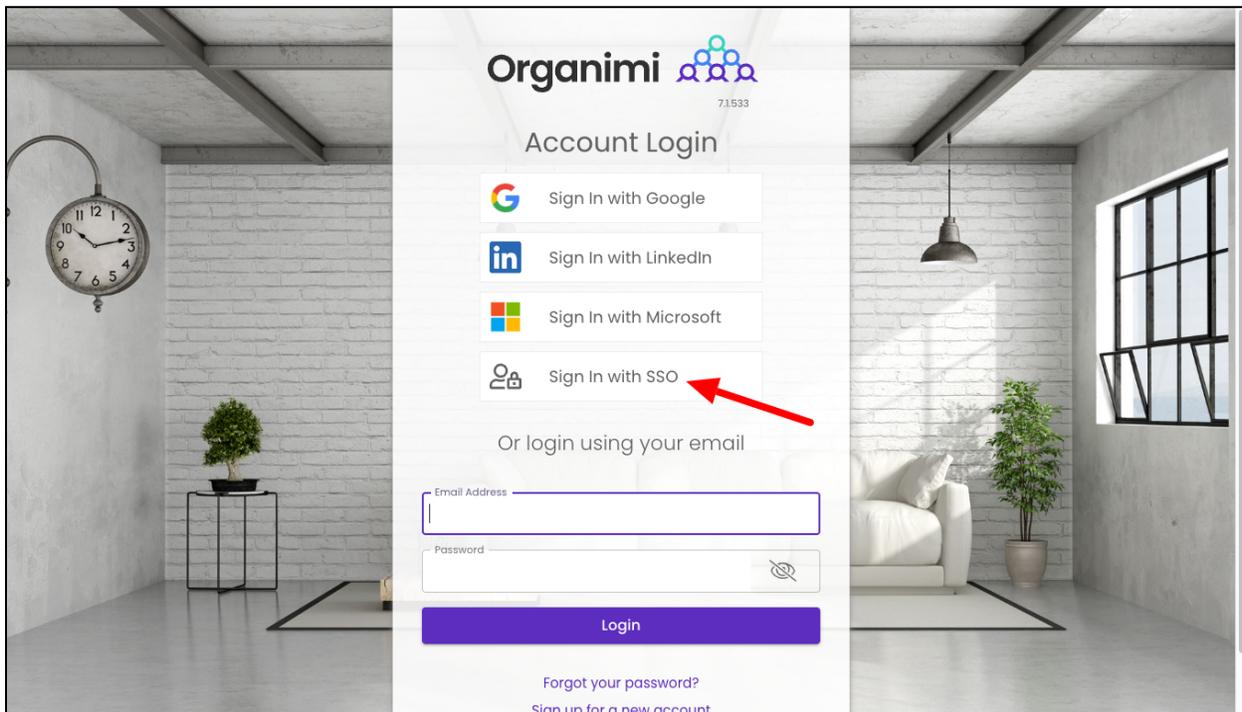
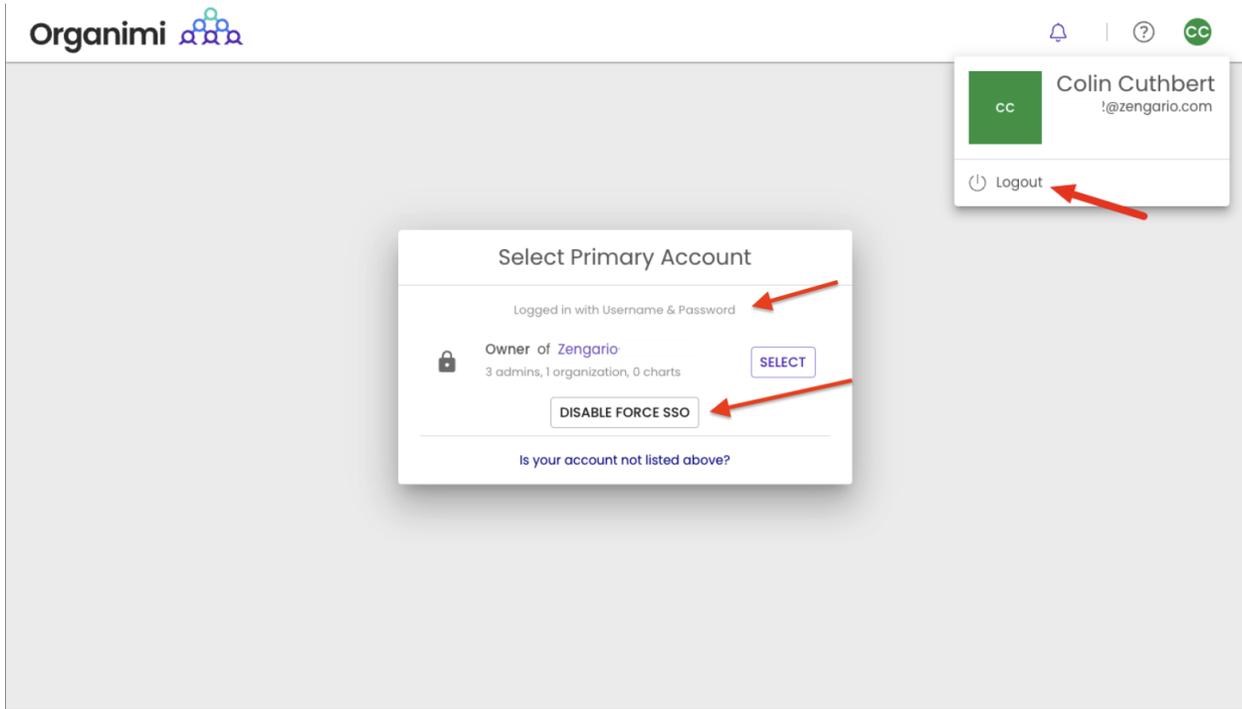


If you were logged into Organimi with you SSO IDP Account then you will just see that the switch is now on for “Force SSO”



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

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

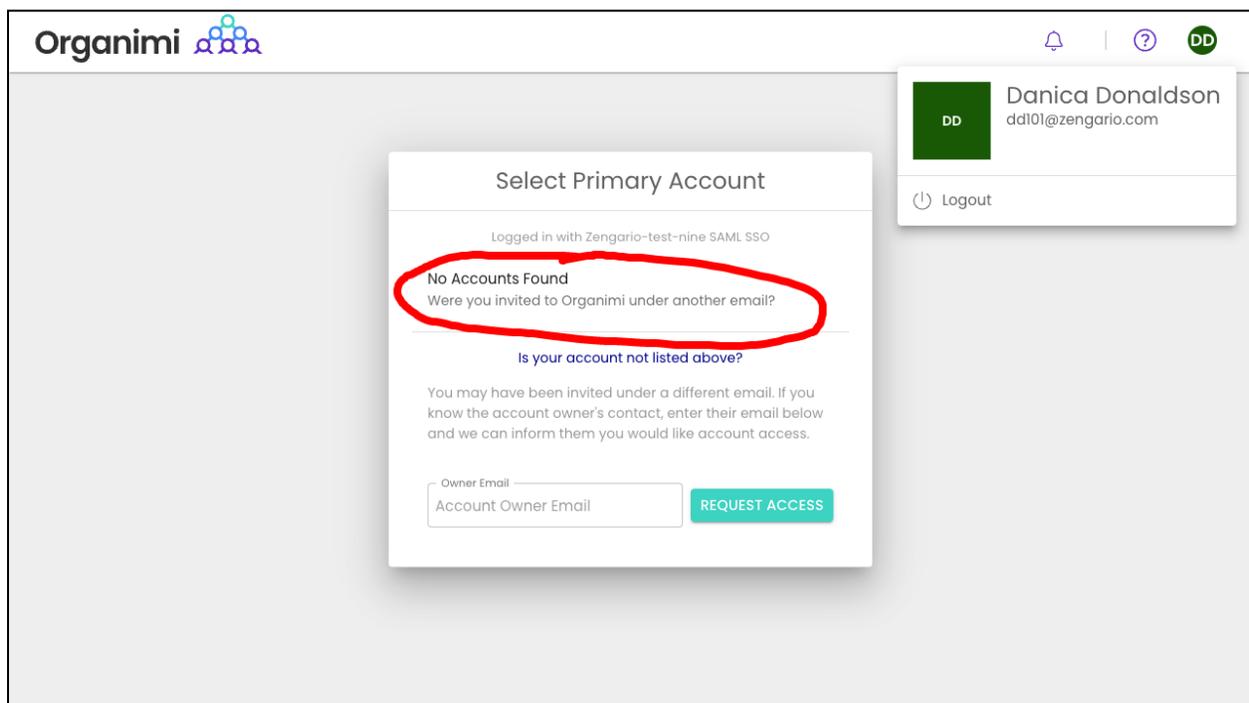
COMING SOON

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 for more details

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.