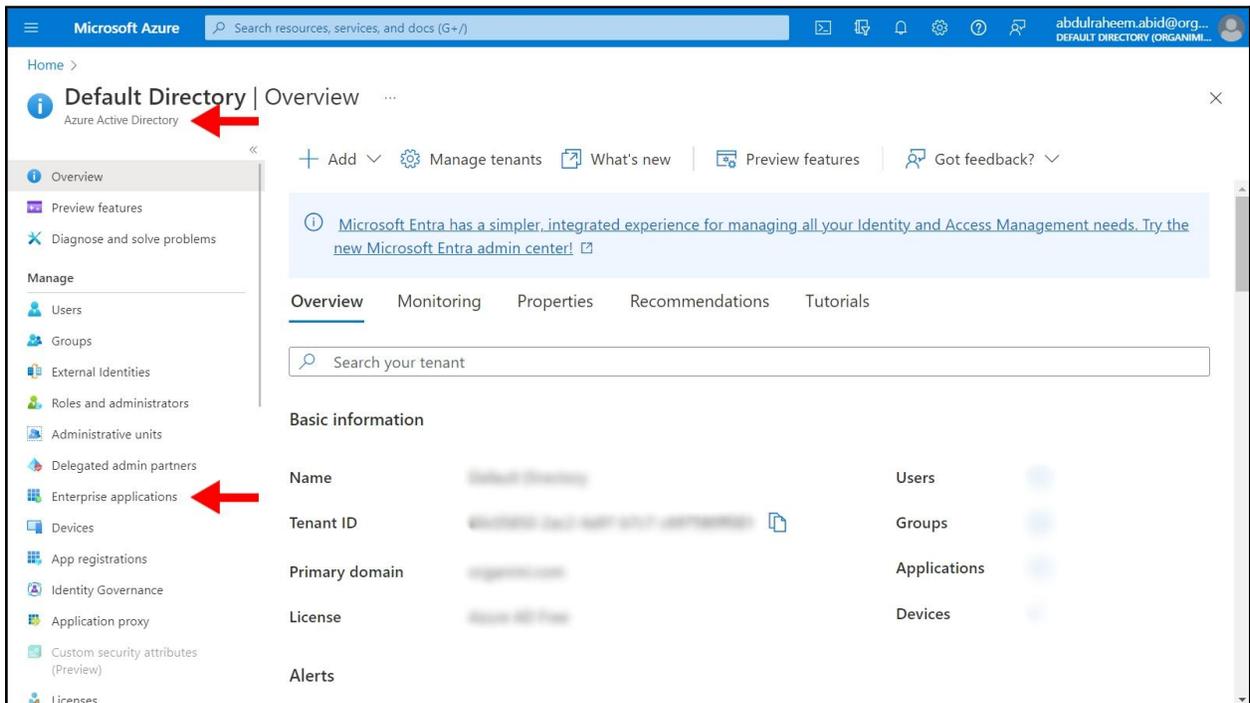


## SAML based SSO - Login with MS Azure AD

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

### Step 1

Go to your Azure AD default directory and click “Enterprise Applications”



The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation at the top reads "Home > Default Directory | Overview". A red arrow points to "Default Directory". The left-hand navigation pane is expanded, and a red arrow points to "Enterprise applications". The main content area displays the "Basic information" section for the "Default Directory".

Basic information	
Name	Default Directory
Tenant ID	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
Primary domain	organimi.com
License	Basic AD Plan

On the right side of the "Basic information" section, there are four links: "Users", "Groups", "Applications", and "Devices".

Then click on “Create New Application”

The screenshot shows the Microsoft Azure portal interface for managing Enterprise applications. The page title is "Enterprise applications | All applications". A red arrow points to the "New application" button in the top navigation bar. The page includes a search bar, a filter for "Application type = Enterprise Applications", and a table listing 19 applications. The table columns are Name, Object ID, Application ID, Homepage URL, Created on, and Certificate Expiry St... The table contains several rows of application data, each with a small icon and a link to the application details.

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry St...
Application 1	...	...	...	...	...
Application 2	...	...	...	...	...
Application 3	...	...	...	...	...
Application 4	...	...	...	...	...
Application 5	...	...	...	...	...
Application 6	...	...	...	...	...
Application 7	...	...	...	...	...
Application 8	...	...	...	...	...
Application 9	...	...	...	...	...
Application 10	...	...	...	...	...
Application 11	...	...	...	...	...
Application 12	...	...	...	...	...
Application 13	...	...	...	...	...
Application 14	...	...	...	...	...
Application 15	...	...	...	...	...
Application 16	...	...	...	...	...
Application 17	...	...	...	...	...
Application 18	...	...	...	...	...
Application 19	...	...	...	...	...

## Step 2

Then click on “Create your own application” and enter “Organimi” as the name of the APP

Select the radio button that says “Integration any other application you don’t find in the gallery (Non-gallery)”

Click the “Create” button

The screenshot displays the Microsoft Azure portal interface for creating a new application. The main navigation bar at the top shows the user is logged in as 'abdulraheem.abid@org...' under the 'DEFAULT DIRECTORY (ORGANIMI...)'. The breadcrumb trail indicates the user is in 'Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Browse Azure AD Gallery'. The 'Browse Azure AD Gallery' section on the left includes a search bar and a '+ Create your own application' link, which is highlighted with a red arrow. Below this, there are cards for 'Cloud platforms' including 'Amazon Web Services (AWS)', 'Google Cloud Platform', and 'SAP'. The 'Google Cloud Platform' card is also highlighted with a red arrow. On the right, the 'Create your own application' wizard is open. It features a 'Got feedback?' link and a description of the process. The 'What's the name of your app?' field contains 'Organimi'. Under 'What are you looking to do with your application?', the radio button for 'Integrate any other application you don't find in the gallery (Non-gallery)' is selected. Below this, there is a section 'We found the following applications that may match your entry' with suggestions for 'Origami' and 'Rimo'. At the bottom right of the wizard, the 'Create' button is highlighted with a red arrow.

Now select “Single sign-on” and click on the big button area for item “2. Set up single sign on”

The screenshot displays the Microsoft Azure portal interface for an enterprise application named "organimi-setup-instructions". The top navigation bar includes the Microsoft Azure logo, a search bar, and the user's profile information (abdulraheem.abid@org...). The breadcrumb trail indicates the path: Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Browse Azure AD Gallery > organimi-setup-instructions | Overview.

The left-hand navigation pane is categorized into "Manage" and "Security". Under "Manage", the "Single sign-on" option is highlighted with a red arrow. Other options in this category include Overview, Deployment Plan, Diagnose and solve problems, Properties, Owners, Roles and administrators, Users and groups, Provisioning, Application proxy, and Self-service. Under "Security", options include Conditional Access, Permissions, and Telepresence.

The main content area is divided into "Properties" and "Getting Started" sections. The "Getting Started" section contains four numbered cards:

- 1. Assign users and groups**: Provide specific users and groups access to the applications. [Assign users and groups](#)
- 2. Set up single sign on**: Enable users to sign into their application using their Azure AD credentials. [Get started](#) (highlighted with a red arrow)
- 3. Provision User Accounts**: Automatically create and delete user accounts in the application. [Get started](#)
- 4. Conditional Access**: Secure access to this application with a customizable access policy. [Create a policy](#)

On the Single sign-on page chose the big button for SAML

The screenshot shows the Microsoft Azure portal interface. At the top, the header includes the Microsoft Azure logo, a search bar, and the user's profile information (abdulraheem.abid@org...). The breadcrumb trail indicates the current location: Home > Default Directory | Enterprise applications > Enterprise applications | All applications > organimi-setup-instructions.

The main content area is titled "organimi-setup-instructions | Single sign-on". Below the title, there is a brief explanation of Single sign-on (SSO): "Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more."

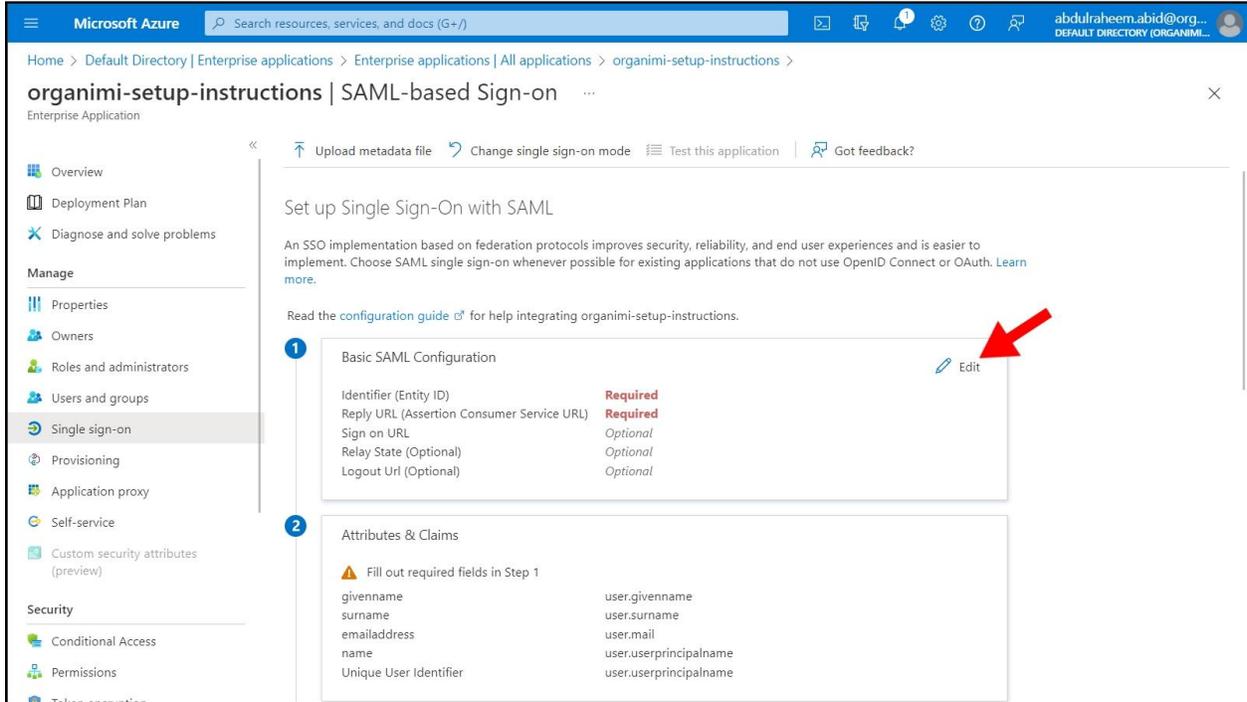
The "Select a single sign-on method" section offers four options:

- Disabled**: Single sign-on is not enabled. The user won't be able to launch the app from My Apps.
- SAML**: Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol. A red arrow points to this option.
- Password-based**: Password storage and replay using a web browser extension or mobile app.
- Linked**: Link to an application in My Apps and/or Office 365 application launcher.

A left-hand navigation pane lists various management tasks such as Overview, Deployment Plan, Properties, Owners, Roles and administrators, Users and groups, Single sign-on (highlighted), Provisioning, Application proxy, Self-service, Custom security attributes, Conditional Access, and Permissions.

### Step 3

On the SAML-based Sign-on page click on the “Edit” button for item 1 the Basic SAML Configuration.



Microsoft Azure | Search resources, services, and docs (G+)

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > organimi-setup-instructions >

## organimi-setup-instructions | SAML-based Sign-on

Enterprise Application

Overview  
Deployment Plan  
Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes (preview)

Security

- Conditional Access
- Permissions

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

### Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating organimi-setup-instructions.

- Basic SAML Configuration** Edit

Identifier (Entity ID)	<b>Required</b>
Reply URL (Assertion Consumer Service URL)	<b>Required</b>
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

- Attributes & Claims**

⚠ Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

In the Basic SAML Configuration popup set the value for the “Identifier (Entity ID)” to be “https://app.organimi.com”

And set the value for the “Reply URL (Assertion Consumer Service URL)” to be “https://app.organimi.com/api/v7/auth/login/saml/callback”

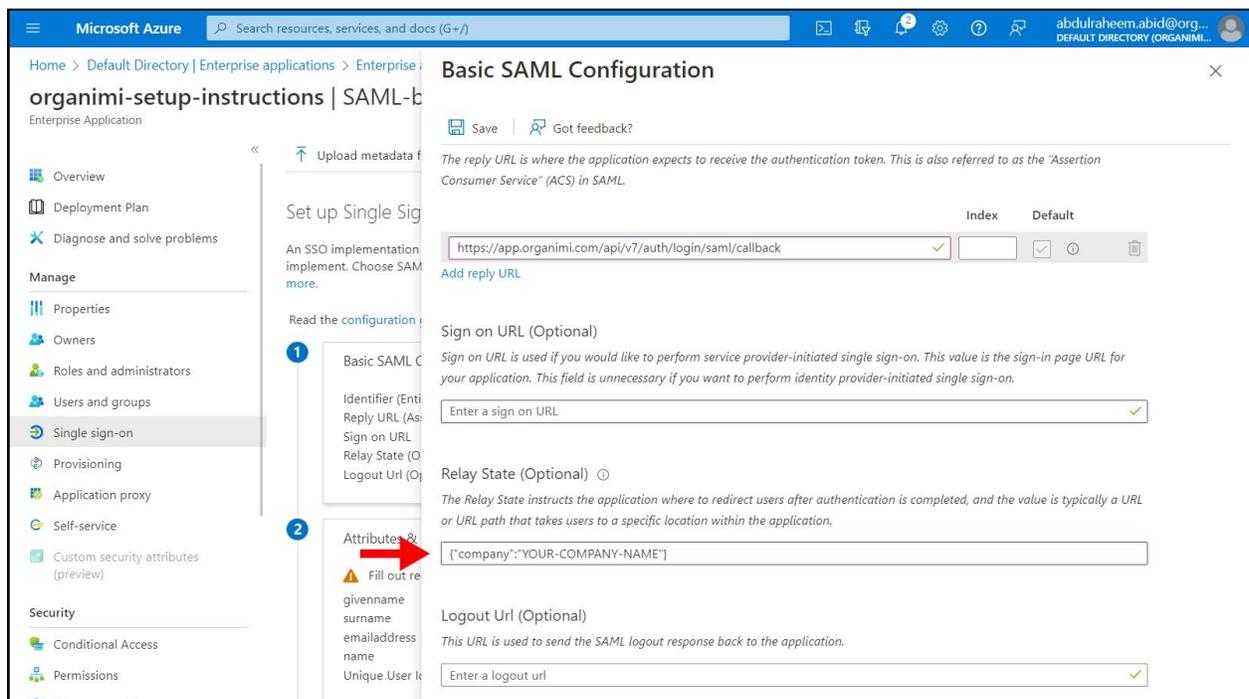
The screenshot displays the 'Basic SAML Configuration' interface in the Microsoft Azure portal. The page is titled 'Basic SAML Configuration' and includes a 'Save' button and a 'Got feedback?' link. The main content area is divided into three sections:

- Set up Single Sign-on:** This section provides instructions on how to set up single sign-on for the application. It includes a red arrow pointing to the 'Identifier (Entity ID)' field.
- Basic SAML Configuration:** This section contains the primary configuration fields:
  - Identifier (Entity ID):** A required field (marked with an asterisk) that identifies the application to Azure Active Directory. The value is set to 'https://app.organimi.com'. It is marked as the 'Default'.
  - Reply URL (Assertion Consumer Service URL):** A required field (marked with an asterisk) where the application expects to receive the authentication token. The value is set to 'https://app.organimi.com/api/v7/auth/login/saml/callback'. It is also marked as the 'Default'.
  - Sign on URL (Optional):** A field for service provider-initiated single sign-on, currently empty.
- Attributes & Claims:** This section is partially visible and includes a warning icon and a list of attributes to be passed to the application, such as 'givenname', 'surname', 'emailaddress', 'name', and 'Unique User ID'.

Scroll down the pop-up window and set the “Relay State” value to be a small JSON object that is in the format of:

```
{"company" : "YOUR-COMPANY-ALIAS"}
```

Where you replace the placeholder with your company name. This name will also be required later when setting up on the Organimi side and asked for the company-alias. And anyone who wishes to login using this IDP, will be asked to enter this name when signing in from the Organimi login page.



Click Save on the Pop-up and then “No I’ll test later” when prompted

## Step 4

In part 2 of the setup “Attributes & Claims”, click on the edit button.

The screenshot shows the Microsoft Azure portal interface for configuring an enterprise application named "organimi-setup-instructions". The left-hand navigation pane includes sections for Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service), and Security (Custom security attributes, Conditional Access, Permissions). The main content area is titled "organimi-setup-instructions | SAML-based Sign-on" and contains a "Test single sign-on with organimi-setup-instructions" dialog box. This dialog box asks, "To ensure that single sign-on works for your application, we recommend using the testing capability (in the last step) to test the changes you recently made. Would you like to test now?" and provides two buttons: "Yes" and "No, I'll test later". A red arrow points to the "No, I'll test later" button. Below the dialog box, there are two configuration sections: "1 Basic SAML Configuration" and "2 Attributes & Claims". The "Attributes & Claims" section is currently selected and shows a table of attributes and their corresponding values. A red arrow points to the "Edit" button in the top right corner of this section.

Attribute	Value
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

In the “Attributes & Claims” window we will set up 4 claims, one Required claim for the Unique Identifier and 3 Additional claims for the attributes used to match over to the Organimi system for the User’s details.

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > organimi-setup-instructions | SAML-based Sign-on > SAML-based Sign-on >

## Attributes & Claims

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...] ***

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ***

Advanced settings

For the Unique User Identifier Required Claim (the first one), we need to make sure it's set to Email Address. This is typically the "user.userprincipalname" in Azure AD but may be different depending on how your Azure AD is set up.

The screenshot shows the 'Manage claim' interface in the Microsoft Azure portal. The breadcrumb navigation at the top indicates the path: Enterprise applications > All applications > organimi-setup-instructions | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims > Manage claim. The page includes a header with the Microsoft Azure logo, a search bar, and the user's profile information (abdulraheem.abid@org...).

The main content area is titled 'Manage claim' and contains the following configuration fields:

- Name:** nameidentifier
- Namespace:** http://schemas.xmlsoap.org/ws/2005/05/identity/claims
- Choose name identifier format:** A dropdown menu with 'Email address' selected. A red arrow points to this selection.
- Source:** Radio buttons for 'Attribute' (selected), 'Transformation', and 'Directory schema extension (Preview)'. The 'Attribute' option is selected.
- Source attribute:** A dropdown menu with 'user.userprincipalname' selected. A red arrow points to this selection.
- Claim conditions:** A section with a downward arrow, currently collapsed.
- Advanced SAML claims options:** A section with a downward arrow, currently collapsed.

For the 3 Additional claims we will set up with email, firstname & lastname.

For the first one change the name from “emailaddress” to be just “email” all lower case and should map to the Source attribute of *user.email*. Make sure to delete the Namespace default value as the Namespace should be empty.

Microsoft Azure | Search resources, services, and docs (G+)

abdulraheem.abid@org...  
DEFAULT DIRECTORY (ORGANIMI...)

Enterprise applications | All applications > organimi-setup-instructions | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

### Manage claim

Save | Discard changes | Got feedback?

Name \* **emailaddress**

Namespace **http://schemas.xmlsoap.org/ws/2005/05/identity/claims**

Choose name format

Source \*  Attribute  Transformation  Directory schema extension (Preview)

Source attribute \* **user.mail**

Claim conditions

Advanced SAML claims options

Microsoft Azure | Search resources, services, and docs (G+)

abdulraheem.abid@org...  
DEFAULT DIRECTORY (ORGANIMI...)

Enterprise applications | All applications > organimi-setup-instructions | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

### Manage claim

Save | Discard changes | Got feedback?

Name \* **email**

Namespace **Enter a namespace URI**

Choose name format

Source \*  Attribute  Transformation  Directory schema extension (Preview)

Source attribute \* **user.mail**

Claim conditions

Advanced SAML claims options

For the second Additional Claim set the Name to be “firstname” all lower case, remove the Namespace value so that is empty and then set the source attribute to be “user.givenname”

The screenshot shows the 'Manage claim' interface in the Microsoft Azure portal. The breadcrumb navigation indicates the path: Enterprise applications | All applications > organimi-setup-instructions | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims > Manage claim. The page includes a header with 'Microsoft Azure', a search bar, and user information for 'abdulraheem.abid@org...'. Below the title, there are action buttons: 'Save', 'Discard changes', and 'Got feedback?'. The main configuration area contains the following fields:

- Name \***: A text input field containing 'firstname'. A red arrow points to this field.
- Namespace**: A text input field that is empty. A red arrow points to this field.
- Choose name format**: A section with three radio button options: 'Attribute' (selected), 'Transformation', and 'Directory schema extension (Preview)'.
- Source \***: A dropdown menu with 'user.givenname' selected. A red arrow points to this dropdown.
- Source attribute \***: A text input field containing 'user.givenname'. A red arrow points to this field.
- Claim conditions**: A section with a collapsed arrow.
- Advanced SAML claims options**: A section with a collapsed arrow.

There is a default Additional claim usually for “*user.userprincipalname*” but we can delete this one as it is not used.

The screenshot shows the Microsoft Azure portal interface for configuring SAML-based sign-on. The page title is "Attributes & Claims". It features a navigation breadcrumb: Home > Default Directory | Enterprise applications > Enterprise applications | All applications > organimi-setup-instructions | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims. The page includes a search bar and a user profile in the top right corner. Below the navigation, there are options to "Add new claim", "Add a group claim", "Columns", and "Got feedback?". The main content is divided into two sections: "Required claim" and "Additional claims".

**Required claim**

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

**Additional claims**

Claim name	Type	Value	
email	SAML	user.mail	...
firstname	SAML	user.givenname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname	Delete
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname	...

At the bottom of the page, there is a "Advanced settings" section with a dropdown arrow.

The final Additional claim is of the last name ... set the Name to be "lastname" all lower case, remove the Namespace value so that is empty and then set the source attribute to be "user.surname"

The screenshot shows the 'Manage claim' configuration page in the Microsoft Azure portal. The breadcrumb navigation is: Enterprise applications | All applications > organimi-setup-instructions | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >. The page title is 'Manage claim'. At the top, there are buttons for 'Save', 'Discard changes', and 'Got feedback?'. The configuration fields are as follows:

- Name \***: lastname (indicated by a red arrow)
- Namespace**: Enter a namespace URI (indicated by a red arrow)
- Choose name format**: (Expanded section)
- Source \***: Attribute (selected with a radio button, indicated by a red arrow)
- Source attribute \***: user.surname (indicated by a red arrow)
- Claim conditions**: (Collapsed section)
- Advanced SAML claims options**: (Collapsed section)

It should look like this once all claims are mapped.

Microsoft Azure Search resources, services, and docs (G+)

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > organimi-setup-instructions | SAML-based Sign-on > SAML-based Sign-on >

## Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
email	SAML	user.mail
firstname	SAML	user.givenname
lastname	SAML	user.surname

Advanced settings

With these sections completed it should look something like this.

The screenshot displays the Microsoft Azure portal interface for configuring SAML-based Sign-on for an application named 'organimi-setup-instructions'. The left-hand navigation pane includes sections for Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, Custom security attributes), and Security (Conditional Access, Permissions). The main content area is titled 'Set up Single Sign-On with SAML' and includes a brief introduction and a link to the configuration guide. Two configuration sections are highlighted with a red border and numbered 1 and 2:

- 1 Basic SAML Configuration** (with an Edit icon):
  - Identifier (Entity ID): `https://app.organimi.com`
  - Reply URL (Assertion Consumer Service URL): `https://app.organimi.com/api/v7/auth/login/saml/callback`
  - Sign on URL: *Optional*
  - Relay State (Optional): `{"company":"YOUR-COMPANY-NAME"}`
  - Logout Url (Optional): *Optional*
- 2 Attributes & Claims** (with an Edit icon):
  - email: `user.mail`
  - firstname: `user.givenname`
  - lastname: `user.surname`
  - Unique User Identifier: `user.userprincipalname`

## Step 5

With the configuration completed you will want to download and save the “Federation Metadata XML”. This is an XML file and will be needed to configure the setup on the Organimi side.

The screenshot shows the Microsoft Azure portal interface for configuring an enterprise application named "organimi-setup-instructions". The page is titled "organimi-setup-instructions | SAML-based Sign-on". The left sidebar contains navigation options such as Overview, Deployment Plan, Diagnose and solve problems, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, Custom security attributes (preview), Security, Conditional Access, Permissions, and Token assignment. The main content area is divided into two sections. The first section, "SAML Certificates", is marked with a blue circle "3" and contains a table for the "Token signing certificate". The table lists the following details: Status (Active), Thumbprint (E0D838EEE42DEC9F642C1CFB685CA880B67D85FF), Expiration (3/9/2026, 1:36:57 PM), Notification Email (abdulraheem.abid@organimi.com), App Federation Metadata Url (https://login.microsoftonline.com/60c05850-2ac2-...), Certificate (Base64) (Download), Certificate (Raw) (Download), and Federation Metadata XML (Download). A red arrow points to the "Download" link for the Federation Metadata XML. Below this is a section for "Verification certificates (optional) (Preview)" with an "Edit" link. The second section, "Set up organimi-setup-instructions", is marked with a blue circle "4" and contains instructions for linking the application with Azure AD. It lists the Login URL (https://login.microsoftonline.com/60c05850-2ac2-...) and the Azure AD Identifier (https://sts.windows.net/60c05850-2ac2-4a97-b7c-...).

Token signing certificate		Edit
Status	Active	
Thumbprint	E0D838EEE42DEC9F642C1CFB685CA880B67D85FF	
Expiration	3/9/2026, 1:36:57 PM	
Notification Email	abdulraheem.abid@organimi.com	
App Federation Metadata Url	https://login.microsoftonline.com/60c05850-2ac2-...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Verification certificates (optional) (Preview)		Edit
Required	No	
Active	0	
Expired	0	

Set up organimi-setup-instructions	
You'll need to configure the application to link with Azure AD.	
Login URL	https://login.microsoftonline.com/60c05850-2ac2-...
Azure AD Identifier	https://sts.windows.net/60c05850-2ac2-4a97-b7c-...

## Step 6

You can set up the Organimi logo on the “Properties” page. A suitably sized Organimi logo is available for easy download at:

<https://drive.google.com/file/d/1IW90r60-mUPM-MRt6qDySBJs774knBaE/view>

The screenshot displays the Microsoft Azure portal interface for managing an enterprise application. The breadcrumb trail indicates the path: Home > Default Directory | Enterprise applications > Enterprise applications | All applications > organimi-setup-instructions. The main heading is "organimi-setup-instructions | Properties".

The left-hand navigation pane is categorized into "Manage" and "Security". Under "Manage", the "Properties" option is highlighted with a red arrow. Other options include Overview, Deployment Plan, Diagnose and solve problems, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, and Custom security attributes (preview). Under "Security", there are options for Conditional Access, Permissions, and Terms of service.

The main content area contains the following settings:

- Enabled for users to sign-in?: Yes (selected) / No
- Name: organimi-setup-instructions
- Homepage URL: https://account.activedirectory.windowsazure.com:444/applications/de...
- Logo: A section with a blue "OR" button and a "Select a file" input field. A red arrow points to the "Select a file" button.
- User access URL: https://myapps.microsoft.com/signin/e06d3212-b213-4fec-8d8f-8e62...
- Application ID: e06d3212-b213-4fec-8d8f-8e623a4a5e13
- Object ID: e9e2d3fb-a701-4eeb-8e26-a47e308c8ed2
- Terms of Service Url: Publisher did not provide this information
- Privacy Statement Url: Publisher did not provide this information

## Step 7

Now over to the Organimi side of the set up ... visit <https://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 top right corner features a notification bell, a 'Quick Links' dropdown, and a user profile icon with the initials 'CC'. A red arrow points to this icon. Below the navigation bar, the breadcrumb path reads 'My Organization > First Chart > Chart'. A central card displays the profile of Abigail Armstrong, CEO & Chairman, with 49 followers and 3 connections. Below this is an organization chart with several levels of employees. A dropdown menu is open over the user profile icon, showing the user's name 'Colin Cuthbert', email 'colin42@zengario.com', and an 'Upgrade Now' button. A red arrow points to the 'My Account' option in the dropdown menu, which also includes a 'Logout' option.

Name	Role	Followers	Connections
Abigail Armstrong	CEO & Chairman	49	3
Charles Chapman	President & COO	33	4
Eric Eisenhower	CFO	13	5
Donaldson	Marketing	5	
Jeremiah Johnston	VP Engineering	6	6
Quinten Queensway	Director of Customer Support	3	3
Ulyses Ullrich	VP Worldwide Sales	12	5
Franklin Fraser	Corporate Controller	4	3
Jonathan Jacobs	VP Finance		
Lionel Lennon	Director of Operations	2	2
Nancy Nielson	IT Director	2	2

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

Click on the "Configure IDP" button

The screenshot shows the 'SAML SSO Config' page. On the left sidebar, 'SSO Settings' 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 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'. At the bottom, there is a 'Your Identity Provider' section with 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.

For the remainder of this set up example the value that we will use for the "YOUR-COMPANY-ALIAS" will be "zengario-test-nine" so you would replace the small JSON object from above that was ...

```
{"company": "YOUR-COMPANY-ALIAS"}
```

... with the small JSON object that is ...

```
{"company": "zengario-test-nine"}
```

On the “SAML SSO Config” screen enter:

1. **Company Alias:** Enter your company alias. It should match exactly with the name entered in Azure AD for the “YOUR\_COMPANY\_ALIAS” value.
2. **IDP Metadata:** Drag and drop the XML file that was downloaded from the “Federation Metadata XML” step on the Azure AD side into the “drop area” as highlighted below.

The screenshot shows the 'SAML SSO CONFIG' interface. On the left is a navigation menu with options: License, Account Owners, Webhooks, API Settings, SSO Settings (highlighted), Transfer Account, and Delete Account. The main content area is titled 'Service Provider Metadata' and includes fields for Callback URL, SP Entity ID, Default Relay State, and Required Attributes. Below this is a 'Download (.xml)' button. The 'Your Identity Provider' section contains a 'Company Alias' field with the value 'zengario', an 'SSO URL' field, an 'Entity ID' field, and an 'X509 Certificate' field containing a long alphanumeric string. A red circle labeled '1' highlights the 'Company Alias' field. To the right of the 'Your Identity Provider' section is a dashed box labeled 'Have your IDP's metadata XML?' with 'paste' and 'drop' options. A red circle labeled '2' highlights this area, and a red arrow points from the 'drop' option to the 'X509 Certificate' field. At the bottom right are 'CANCEL' and 'SAVE' buttons.

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

3. Click the SAVE button

The screenshot displays the 'SAML SSO Config' page. 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 'Service Provider Metadata' section with a 'Setup Instructions' link. This section contains several input fields: '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"}), and 'Required Attributes' (email, firstname, lastname). Below these is a 'Service Provider Metadata File' section with a 'Download (.xml)' link. The 'Your Identity Provider' section includes 'Company Alias' (zengario-test-nine), 'SSO URL' (https://dev-55539452.okta.com/app/dev-55539), 'Entity ID' (http://www.okta.com/exk8p15q6mCk3OgDA5d7), and 'X509 Certificate' (MIIDqDCCApCgAwIBAgIGAYbcTh0zMA0GCSqGSib3DQEBCwUAMIGUMQs wCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcmlkZm9udGVzYXV0eWVwYXNjaXNjbzEN MAsGATUECgwET2t0YTEU MBIGATUECwwLUINPUHJvdmlkZXIxFtATBgNVBAMMDGRldi01NTUzOTQ1MjEj MB0GCSaGSib3DOEJ). A red arrow points to the 'SAVE' button at the bottom right.

The screenshot shows a settings page titled "SAML SSO Config". On the left is a navigation menu with items: My Info, License, Account Owners, Webhooks, API Settings, SSO Settings (highlighted), Transfer Account, and Delete Account. The main content area has a sub-header "SAML SSO Config" and a toggle for "Force SAML SSO Login" which is currently off. Below this is a descriptive paragraph: "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 is circled in red and contains the following information: "Alias: zengario-test-nine" and "Entity ID: https://sts.windows.net/60c05850-2ac2-4a97-b7c7-c697580ff0..." with a pencil icon for editing and a trash icon for deletion.

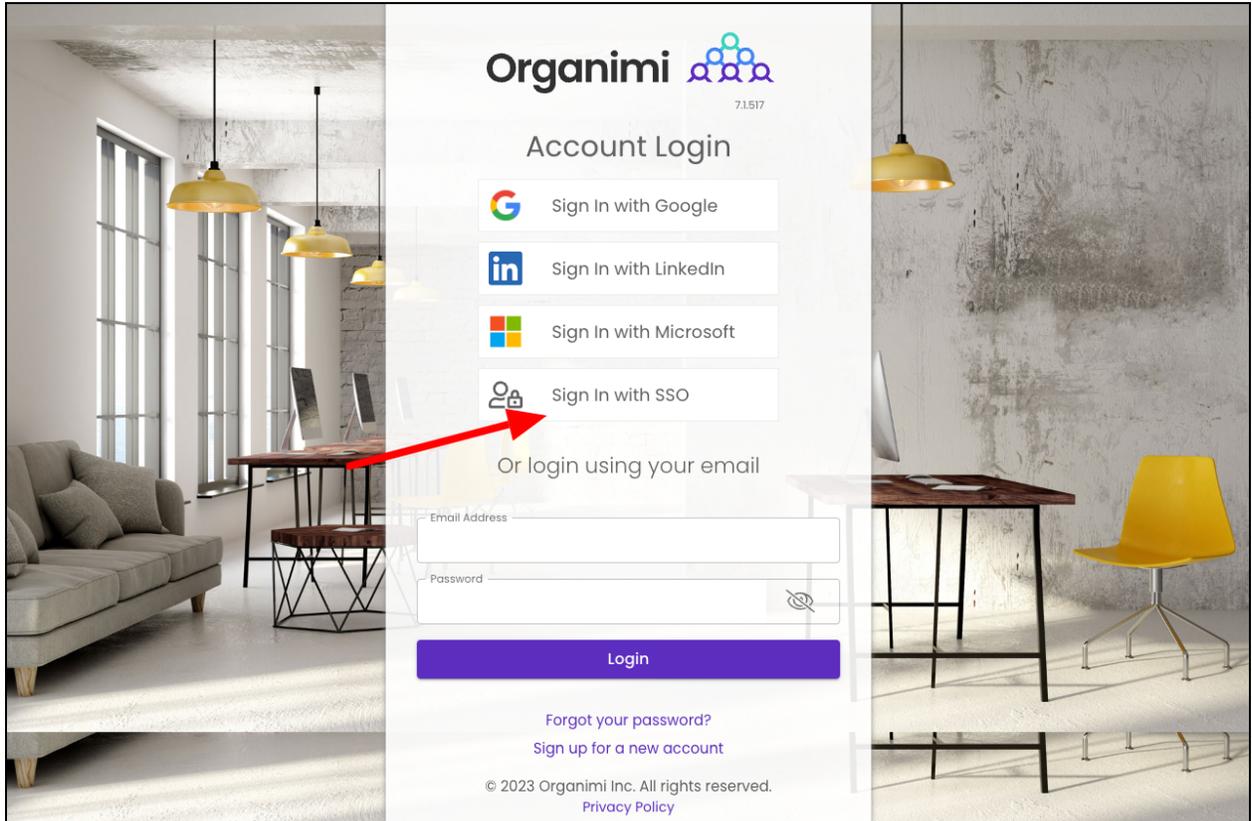
Your Identity Provider should show the Azure AD Entity ID that you just set up, which means IDP configuration is accepted.

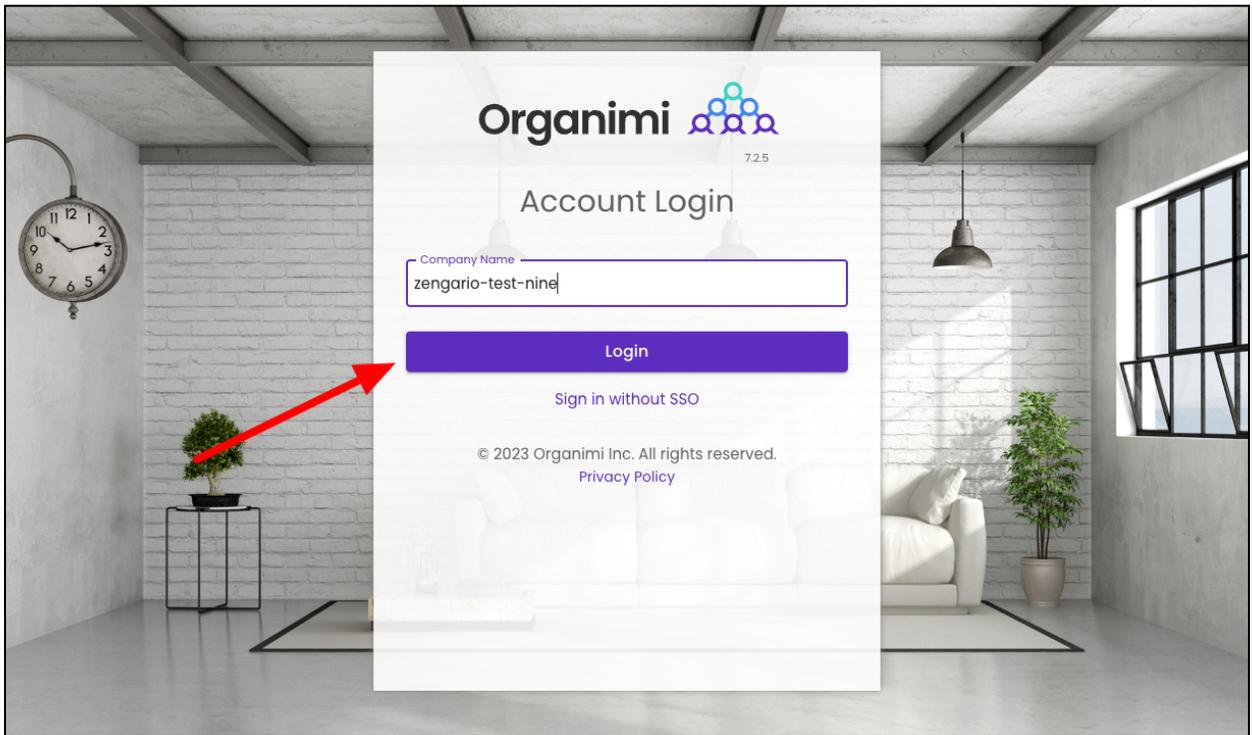
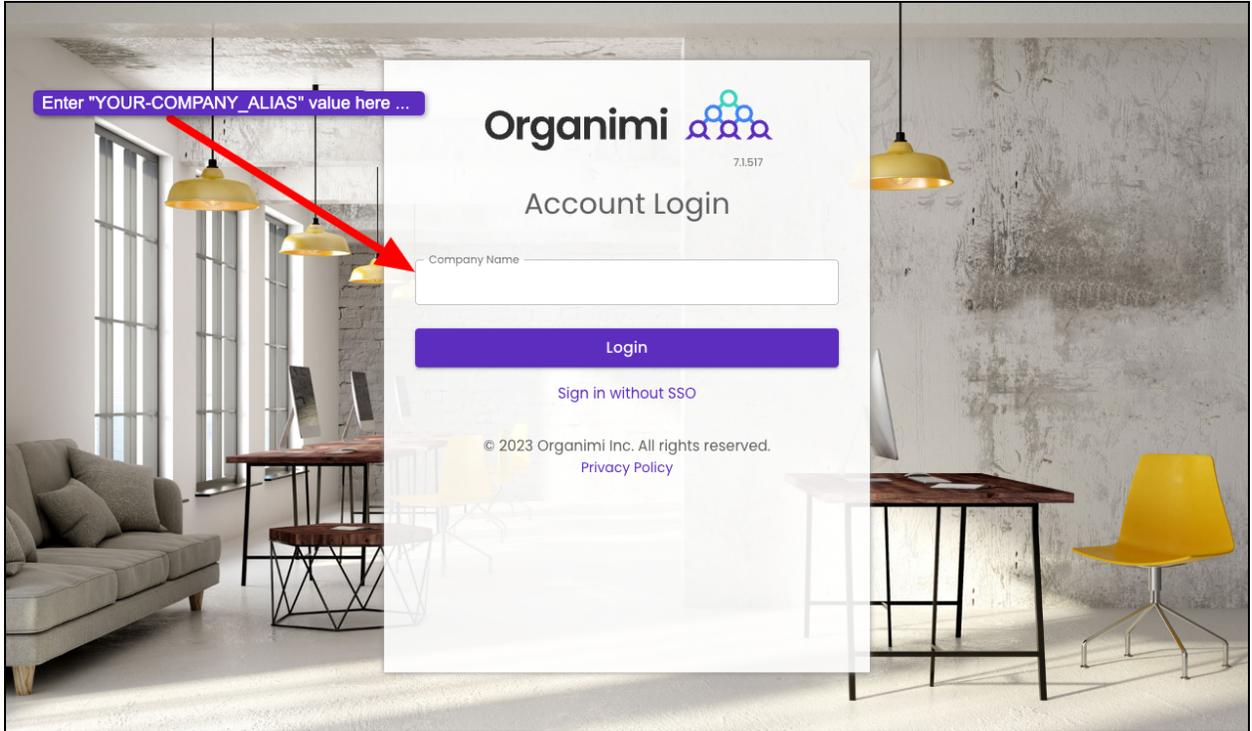
*Note: If you do not reach to this point and see an error message on clicking the "SAVE" button, Contact Organimi support @ [support@organimi.com](mailto:support@organimi.com)*

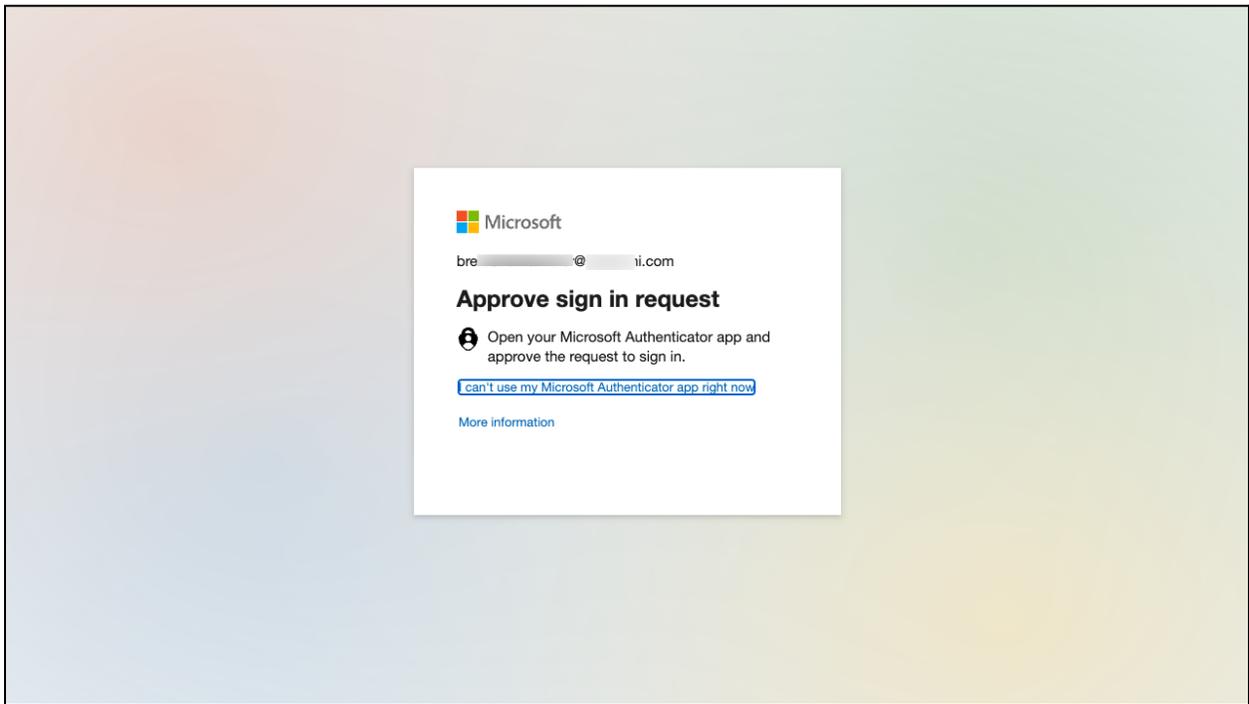
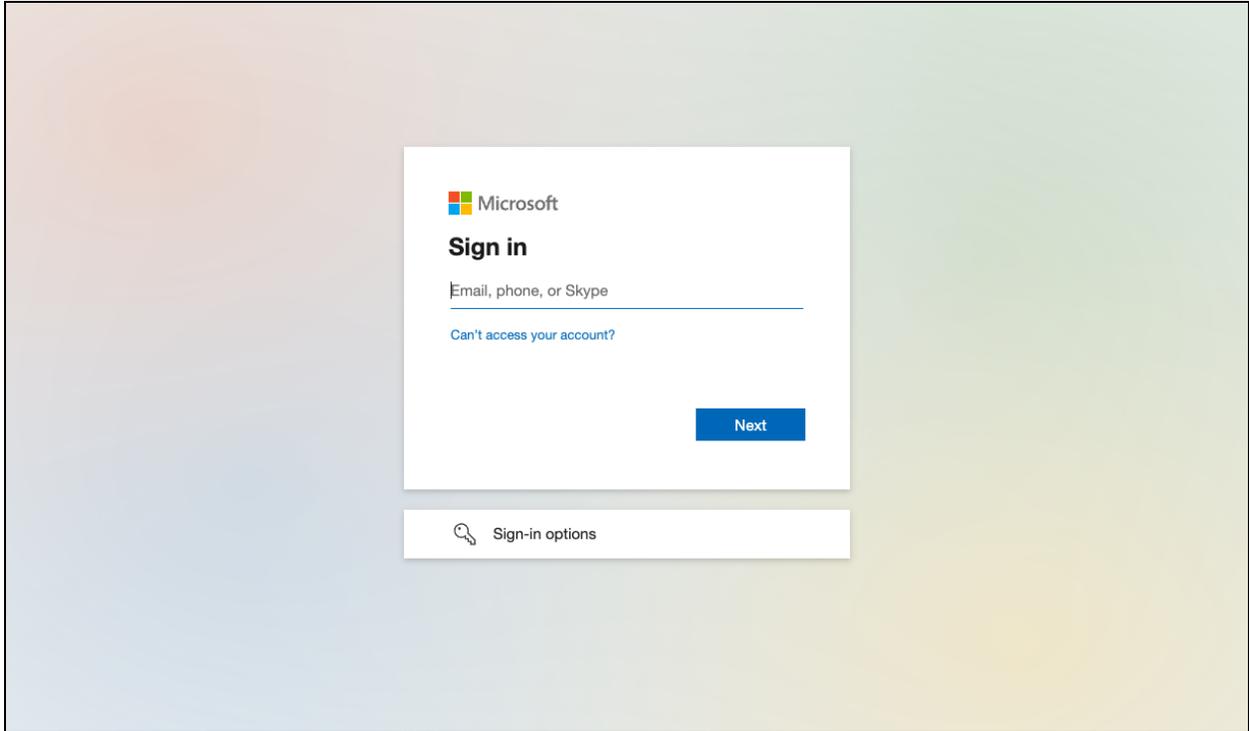
## Step 8

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.

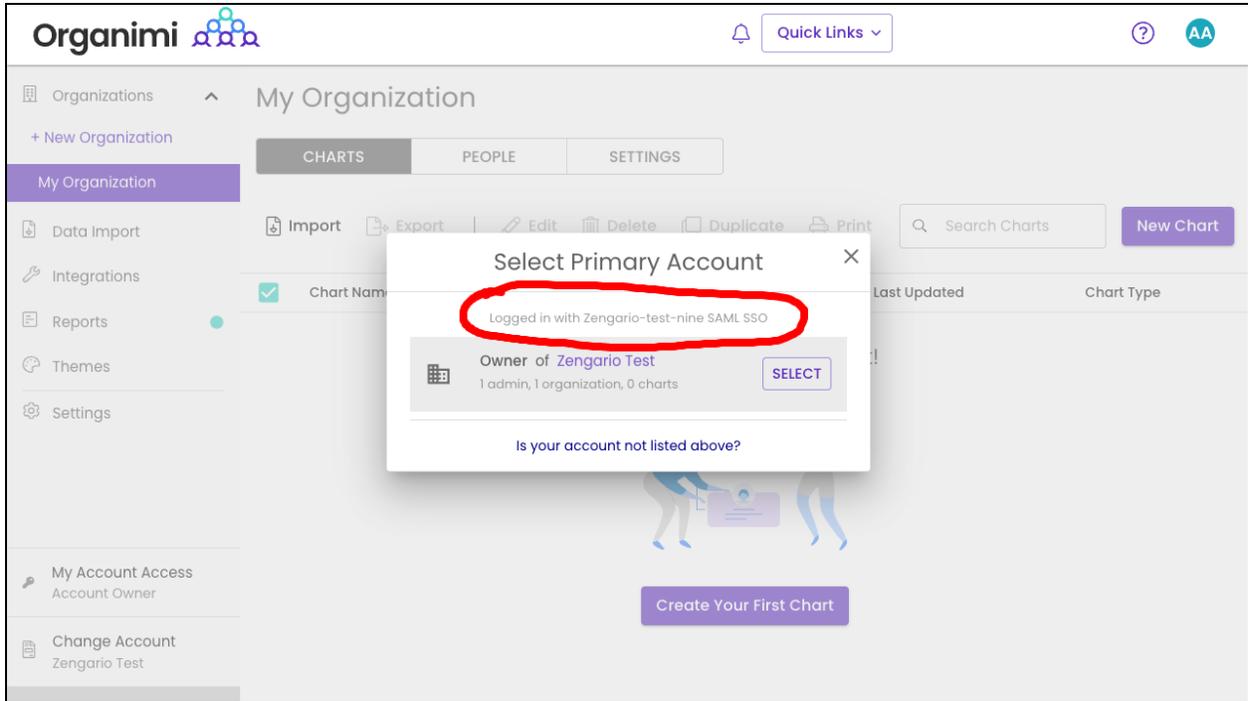
You should be redirected to your Azure AD IDP where you can be authenticated. Once successful, you will be redirected back to Organimi and will be logged in.







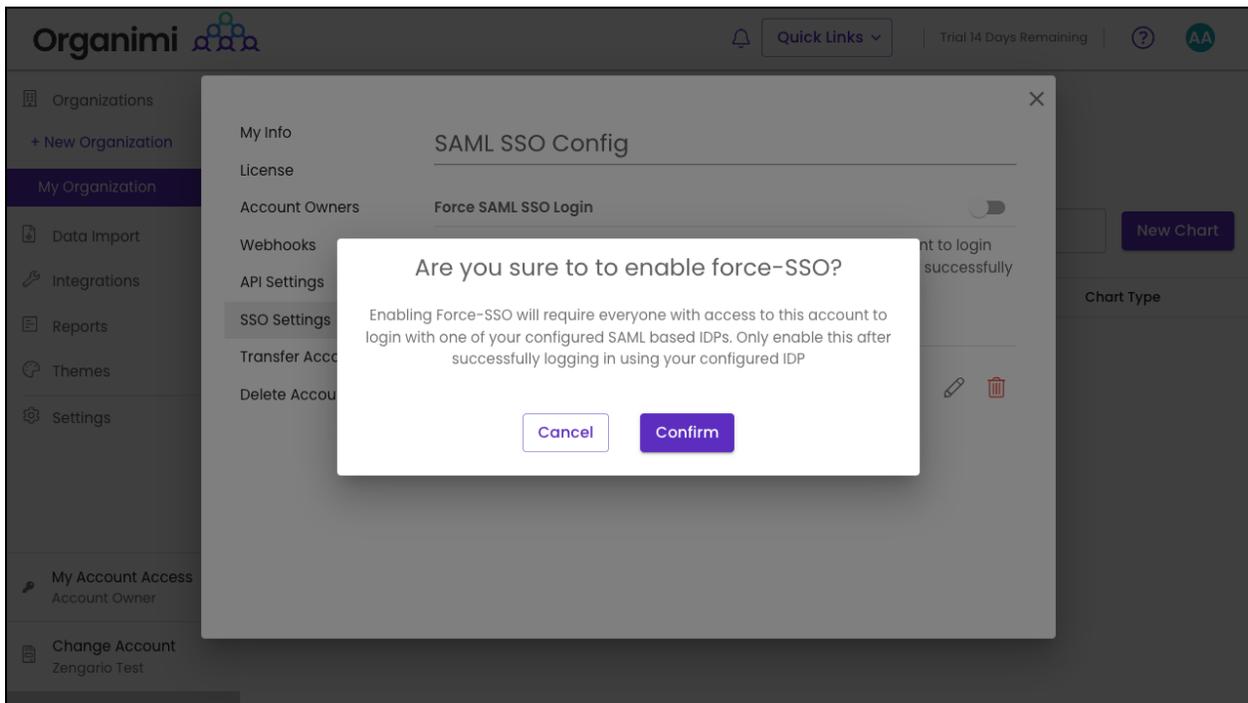
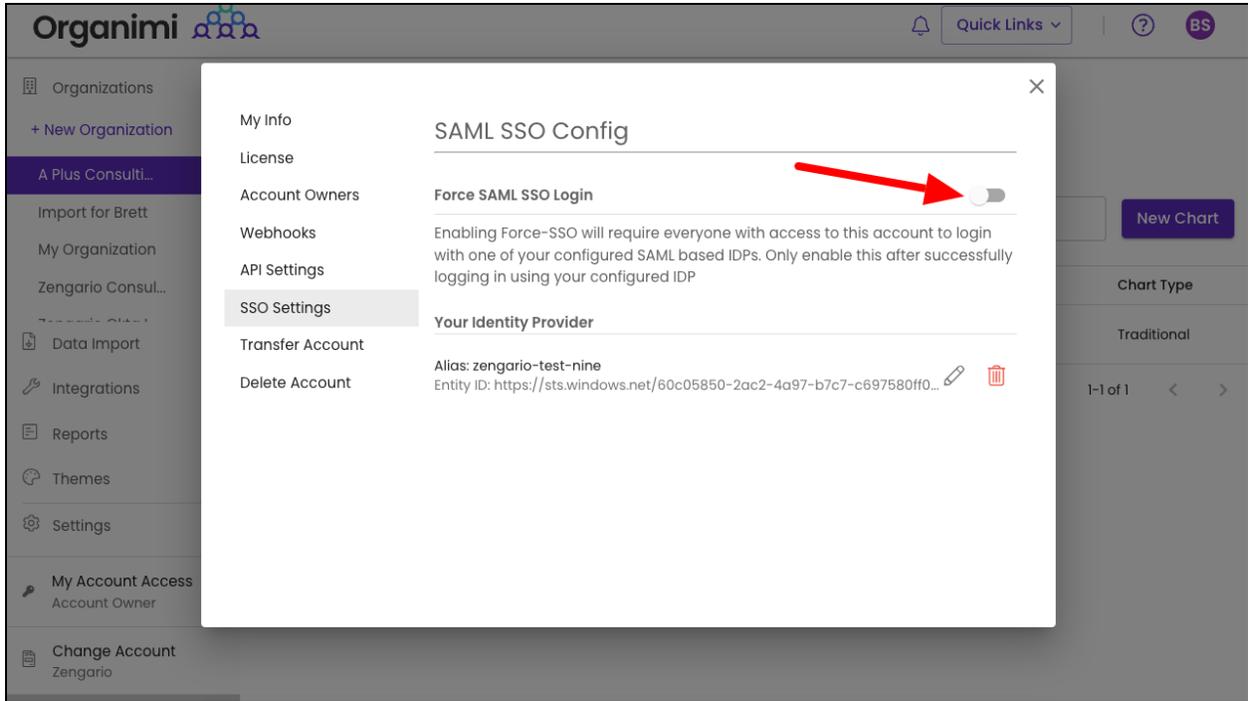
And you are in. If you click the Change Account link on the Organimi screen you will see that you are logged in with SAML SSO



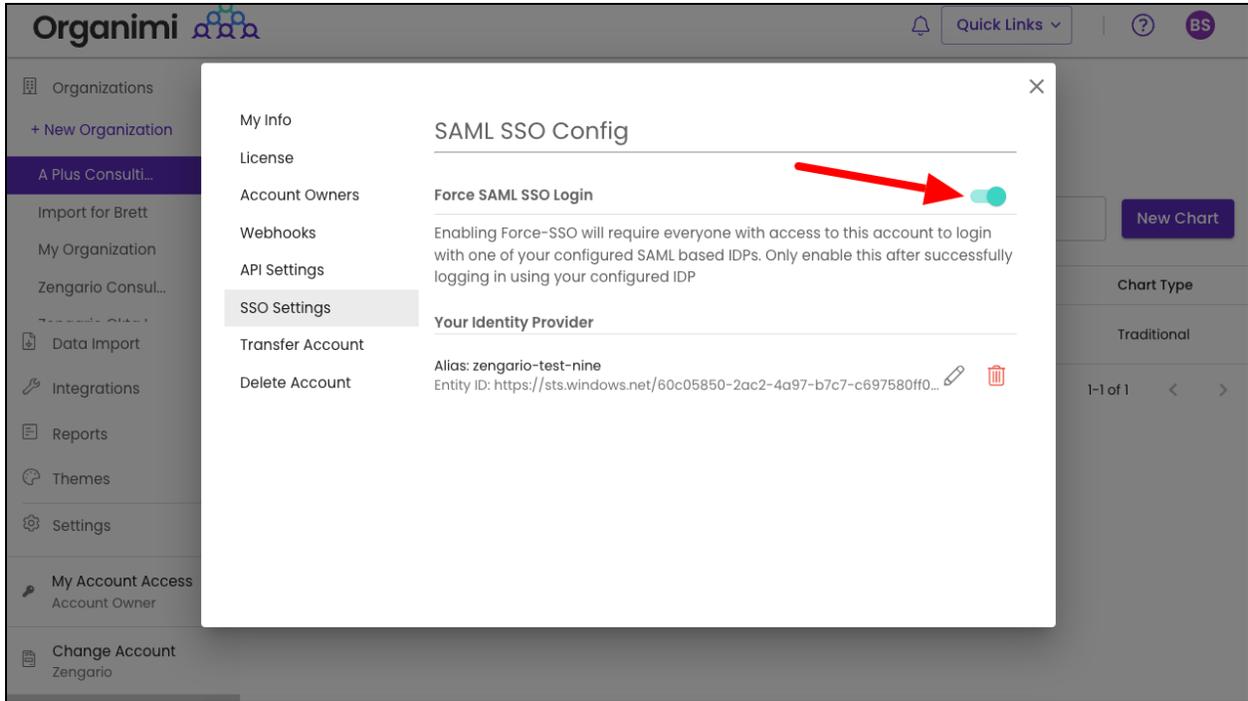
## Step 9

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.

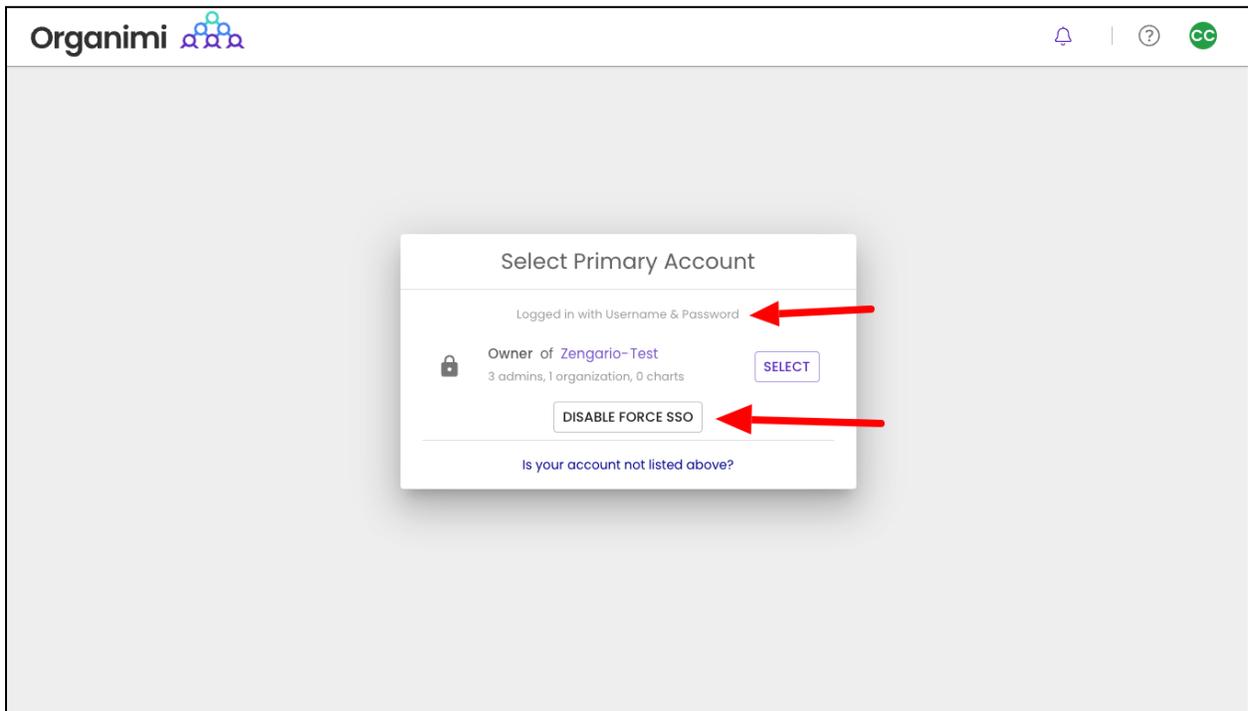
*Note: As the account owner, It's recommended that you test logging in with your IDP first before turning on this setting, as you will not be able to access the account via any other login methods after you enable the “Force-SSO” option.*



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 

7.1533

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

[Forgot your password?](#)  
[Sign up for a new account](#)

Colin Cuthbert  
colin42@zengario.com

Logout

Select Primary Account

Logged in with Username & Password

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

Is your account not listed above?

Organimi 

7.1533

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

[Forgot your password?](#)  
[Sign up for a new account](#)

## 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 is a user profile for Danica Donaldson (ddl01@zengario.com) and a Logout button. In the center, a modal dialog titled "Select Primary Account" is displayed. The dialog indicates the user is logged in with "Zengario-test-nine SAML SSO". A red circle highlights the message "No Accounts Found" and the question "Were you invited to Organimi under another email?". Below this, there is a link "Is your account not listed above?". Further down, there is a text input field labeled "Owner Email" with the placeholder text "Account Owner Email" and a teal "REQUEST ACCESS" button.

## Step 11 - Organimi Direct Access URL

The account owner can send the User access URL from the Azure AD to the group once they have been provisioned access to Organimi ... then users can directly access the Organimi Account from the link with their SSO credentials.

The screenshot shows the Microsoft Azure portal interface for managing an enterprise application. The breadcrumb trail is: Home > Default Directory | Enterprise applications > Enterprise applications | All applications > organimi-setup-instructions. The page title is 'organimi-setup-instructions | Properties'. The left-hand navigation pane includes sections for Overview, Deployment Plan, Diagnose and solve problems, Manage (with 'Properties' highlighted by a red arrow), Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, Custom security attributes (preview), Security, Conditional Access, and Permissions. The main content area shows application settings: 'Enabled for users to sign-in?' is set to 'Yes'; 'Name' is 'organimi-setup-instructions'; 'Homepage URL' is 'https://account.activedirectory.windowsazure.com:444/applications/de...'; 'Logo' is 'OR' with a 'Select a file' button; 'User access URL' is 'https://myapps.microsoft.com/signin/e06d3212-b213-4fec-8d8f-8e62...' (highlighted with a red arrow); 'Application ID' is 'e06d3212-b213-4fec-8d8f-8e623a4a5e13'; 'Object ID' is 'e8e2d3fb-a701-4eeb-8e26-a47e308c8ed2'; 'Terms of Service Url' and 'Privacy Statement Url' are both 'Publisher did not provide this information'.

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.