

Microsoft Entra Tutorial: Setting Up Enterprise Applications for SAML SSO Access

Introduction

This tutorial will guide you through the process of using Microsoft Entra (formerly Azure Active Directory) to set up an enterprise application for SAML Single Sign-On (SSO) access to Wazzl.

Prerequisites

- An active Microsoft Entra admin account.

IMPORTANT NOTE: When SSO is enabled for existing users in the system, upon first login with SSO the users will not be able to login again with their old username and password anymore! they should from now on only login with SSO.

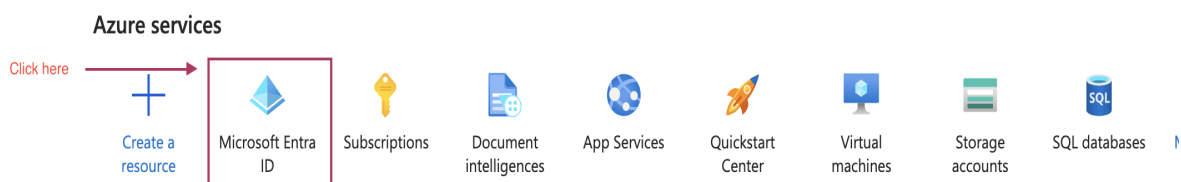
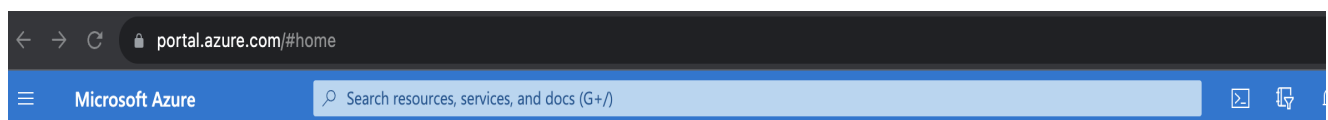
IMPORTANT NOTE: For none yet existing users in the system, they need to contact their realm manager to activate their accounts before being able to login with SSO.

IMPORTANT NOTE: The SSO configuration is only available for **Realm Managers**.

Step-by-Step Guide

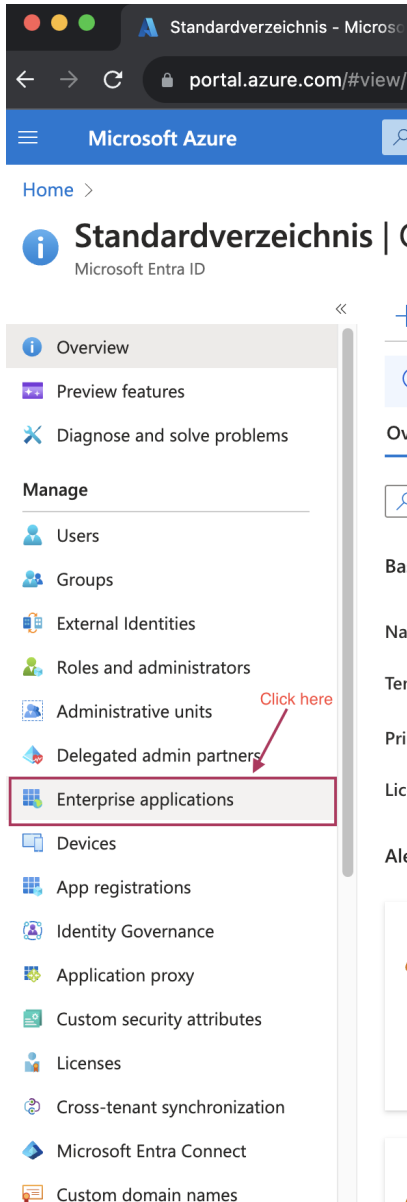
Step 1: Accessing Microsoft Entra

1. Open your web browser and navigate to the [Microsoft Entra admin portal](#).
2. Sign in with your administrator credentials.
3. Select or Search for the Microsoft Entra ID service

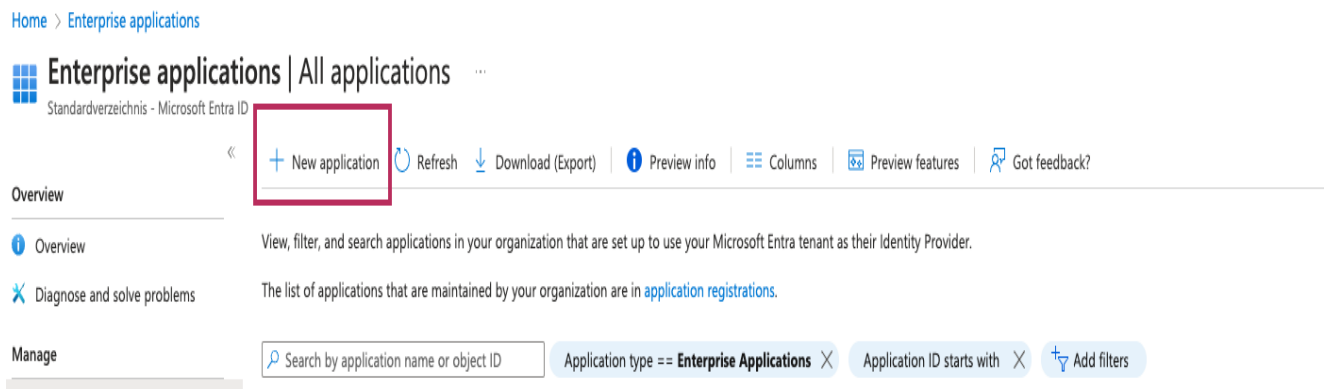


Step 2: Creating a New Enterprise Application

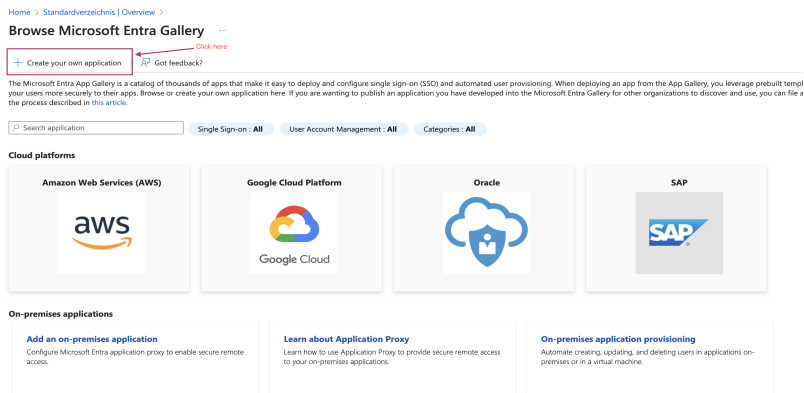
1. In the left-hand navigation pane, click on "Enterprise applications".



2. Click on "New application" at the top of the screen.



3. Click on "Create your own application" at the top of the screen.



4. Enter a name for your application like "wazzl" and select the option "integrate any other application you don't find in the gallery (Non-gallery)" then click "Create".

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Microsoft Entra ID (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

Create

Step 3: Configuring SAML SSO

1. Once the application is created, navigate to the "Single sign-on" section from the application's left-hand navigation menu.

Properties

Name

Application ID

Object ID

Getting Started

- 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 Microsoft Entra credentials
[Get started](#)
- 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](#)
- 5. Self service**
Enable users to request access to the application using their Microsoft Entra credentials
[Get started](#)

What's New

2. Select "SAML" as the single sign-on method.

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID 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.](#)

Select a single sign-on method [Help me decide](#)

- 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.
- 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.

3. Fill in the SAML configuration details:

- o Edit the **Basic SAML Configuration**:

wazzl | 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
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity

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

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 wazzl.

- 1 **Basic SAML Configuration** Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- 2 **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
- 3 **SAML Certificates**

Token signing certificate	Active	Edit
Status		

- o the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** should be provided.

Basic SAML Configuration

✕

Save | Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Add identifier

← Click here

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

[Add reply URL](#)

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

✓

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

✓


- o Set the **Identifier (Entity ID)** to **"wazzl-azure"** and the **Reply URL (Assertion Consumer Service URL)** to **"https://card.wazzl.me/account/saml2/authenticate/acs/"** and click save and close the dialog.

Basic SAML Configuration

 Save |  Got feedback?

Identifier (Entity ID) *



The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
<input type="text" value="wazzl-azure"/>	<input checked="" type="checkbox"/>  

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
<input type="text" value="https://card.wazzl.me/account/saml2/authenticate/acs/"/>	<input type="text"/>	<input checked="" type="checkbox"/>  

[Add reply URL](#)

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

4. Edit the **Attributes & Claims** section. In this section, you can add additional attributes and claims to the SAML assertion. The following attributes are required for the SAML SSO integration to work:

- **email:** user.mail
- **firstName:** user.givenname
- **lastName:** user.surname

2

Attributes & Claims

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

 Edit

- The claims should be modified, to do so click for example on the mail

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

- and change the Name to "email" and remove the Namespace.

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

Source attribute * user.mail

Claim conditions

Advanced SAML claims options

change this to email

remove Namespace

- Click save and close the dialog.

Manage claim

Save Discard changes | Got feedback?

Name * email

Namespace Enter a namespace URI

Choose name format

Source * Attribute Transformation Directory schema extension

Source attribute * user.mail

Claim conditions

Advanced SAML claims options

- delete the claim "name".

+ 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
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

- repeat the same steps for the firstName and lastName attributes.

- The **firstName** attribute should be set from **givenname** to **"firstName"**
- The **lastName** attribute should be set from **surname** to **"lastName"**.
- The **Namespace** should be removed for both attributes.
- Click save and close the dialog.

[Home](#) > [Enterprise applications | All applications](#) > [wazzl | 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

[v](#) Advanced settings

4. Download the configuration.

from the **"SAML Certificate"** section, click on **"Federation Metadata XML"** to download the xml file.

[Home](#) > [Enterprise applications | All applications](#) > [wazzl](#) >

wazzl | 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](#)

Security

[Conditional Access](#)
[Permissions](#)
[Token encryption](#)

Activity

[Sign-in logs](#)
[Usage & insights](#)

[↑](#) Upload metadata file [↔](#) Change single sign-on mode [🧪](#) Test this application [🔔](#) Got feedback?

[Sign on URL](#)
[Relay State \(Optional\)](#)
[Logout Uri \(Optional\)](#)

Optional
Optional
Optional

2

Attributes & Claims

email user.mail [Edit](#)
 firstName user.givenname
 lastName user.surname
 Unique User Identifier user.userprincipalname

3

SAML Certificates

Token signing certificate [Edit](#)
 Status Active
 Thumbprint F8C9E25790307ED526C0BA0D7AAB215F6947195C
 Expiration 12/6/2026, 6:53:32 PM
 Notification Email dev@wazzl.de
 App Federation Metadata Uri <https://login.microsoftonline.com/e01049e2-a730...>
 Certificate (Base64) [Download](#)
 Certificate (Raw) [Download](#)
 Federation Metadata XML [Download](#)

Verification certificates (optional)

Required No [Edit](#)
 Active 0
 Expired 0

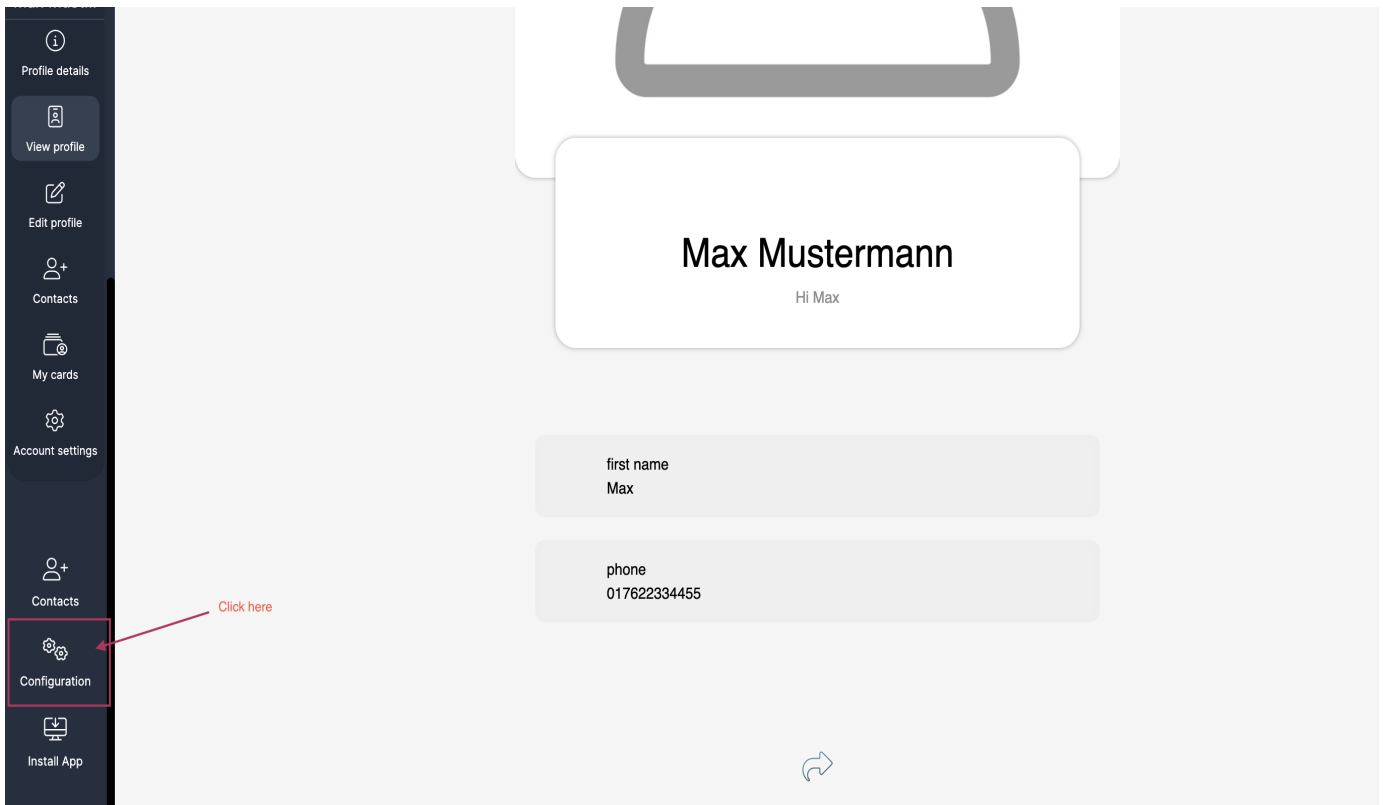
Step 4: Assigning Users/Groups

1. Go to the **"Users and groups"** section in the application's navigation menu.
2. Click on **"Add user/group"**.
3. Select the user or group you want to give access to and click **"Assign"**.

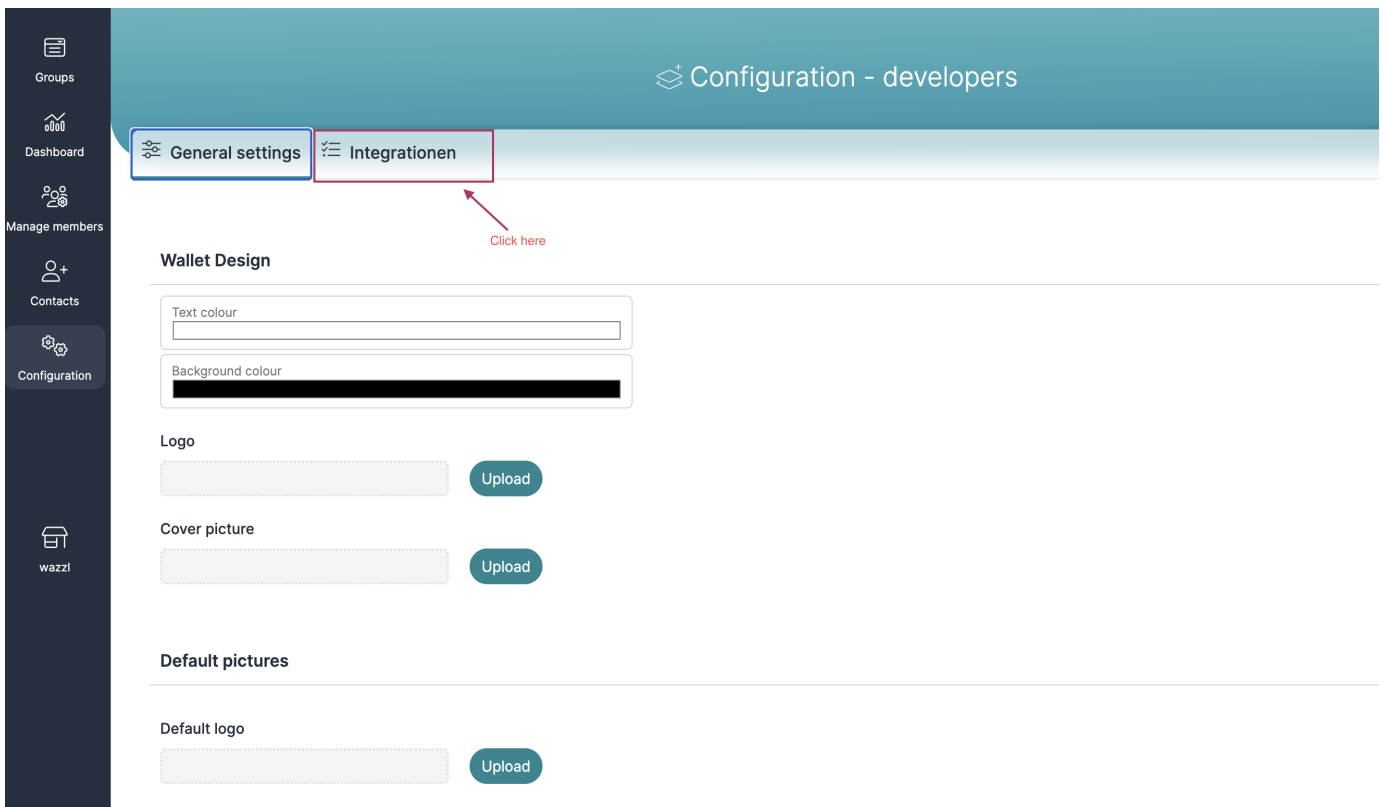
Attention: make sure that the users have the attributes **"mail"**, **"givenname"** and **"surname"** set in Microsoft Entra.

Step 5: Testing the SSO Configuration

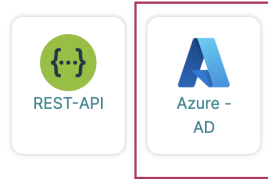
1. Navigate back to the **"Wazzl Application"** login as a **Realm Manager** and click on the **Configuration** section.



2. Click on the "Integration" tab



3. Click on the "Azure AD" button



wazzl

EN ▾

[Imprint](#) [Privacy Policy](#)

4. activate the "SSO Enabled" and upload the configuration file downloaded in step 4.

The screenshot shows a configuration window titled 'Azure - AD' with a close button (X) in the top right. It features a toggle switch for 'SSO enabled' which is currently turned off. Below this is a file selection area with a 'Choose file' button and the text 'No file chosen'. Underneath is a section for 'XML data' with a label 'XML Data' and a large empty text area. At the bottom center is a 'Save' button.

5. Click on the "Save" button.

SSO enabled



Choose file wazzl.xml

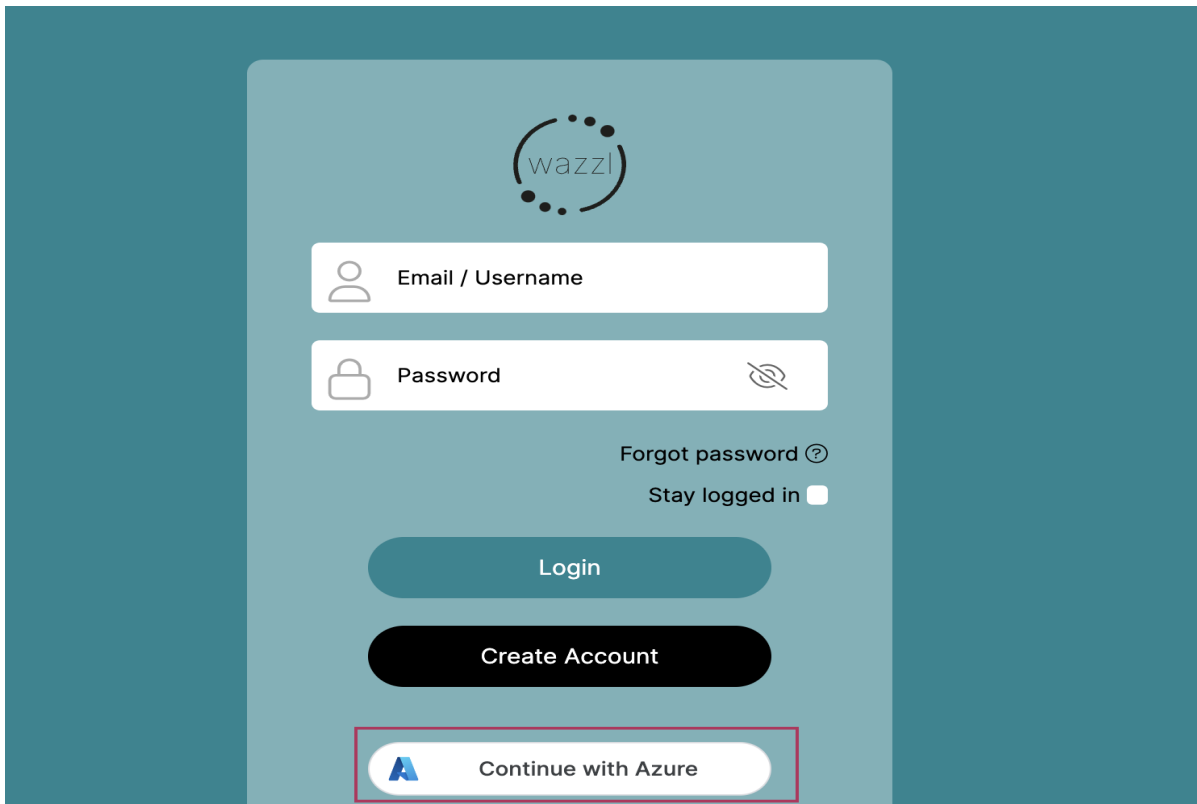
XML data

XML Data

```
<?xml version="1.0" encoding="utf-8"?><EntityDescriptor ID=".B9b5b172-8004-4f06-a90c-f33f8b657dce" entityID="https://sts.windows.net/e01049e2-a730-4353-8d0b-ff1647eaf436/" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><Reference URI="#.B9b5b172-8004-4f06-a90c-f33f8b657dce"><Transforms>< TransformAlgorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />< TransformAlgorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
```

Save

6. Now you can test the SSO configuration by going to your Realm URL and try to login with Azure.



Conclusion

Congratulations! You have successfully set up an enterprise application in Microsoft Entra for SAML SSO access. For more detailed information or support, visit the [Microsoft Entra documentation](#).

Additional Resources

- [Microsoft Entra Documentation](#)
- [Understanding SAML-based SSO](#)