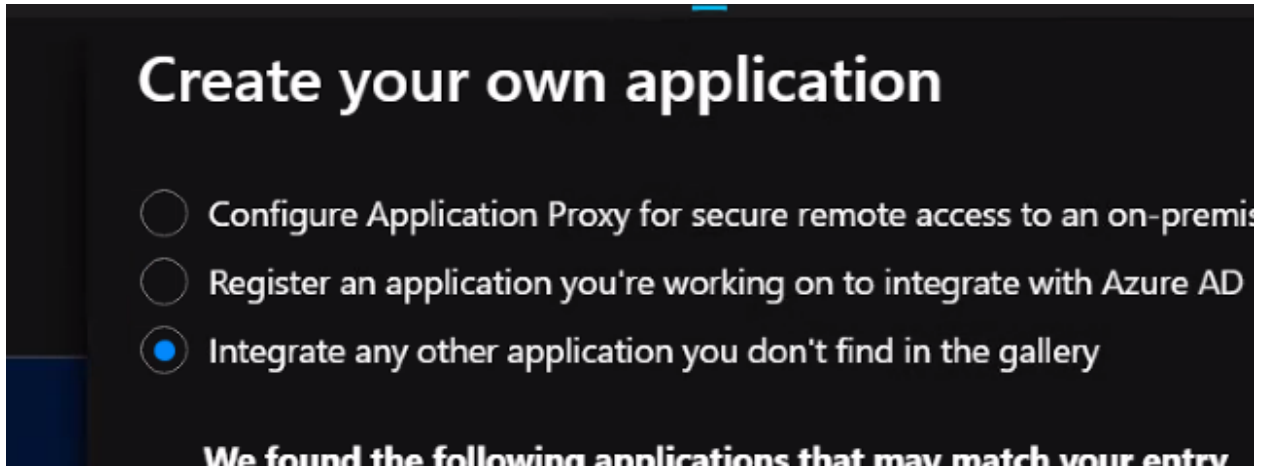


## Azure AD Steps

1. Add a new Application (name it Axomo)  
Non Gallery App



[Azure AD Connect Download Link](#)

[Azure AD Connect Setup Link](#)

Microsoft Azure

Search resources, services, and docs (G+)

Home > [redacted] > Enterprise applications | All applications > Axomo | Overview

### Axomo | Overview

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

#### Manage

- Properties
- Owners
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

#### Security

- Conditional Access
- Permissions
- Token encryption

#### Activity

- Sign-ins
- Usage & insights (Preview)
- Audit logs

### Properties

Name ⓘ  
Axomo

Application ID ⓘ  
09e0cca3-b9d0-42e0-a658-...

Object ID ⓘ  
f35f3c45-0bba-4239-a2e2-9...

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

2. Set up single sign-on with SAML
  - a. Identifier: Axomo
  - b. Reply URL: [https://api.axomo.com/v3/\[STORE\]/SAML2/](https://api.axomo.com/v3/[STORE]/SAML2/)

Microsoft Azure

Home > [redacted] > Enterprise applications | All applications > Axomo | Single sign-on > SAML-based Sign-on

### Axomo | SAML-based Sign-on

Enterprise Application

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

#### Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating Axomo.

- ##### Basic SAML Configuration

Identifier (Entity ID)	Axomo
Reply URL (Assertion Consumer Service URL)	<a href="https://api.axomo.com/v3/[redacted]/SAML2/">https://api.axomo.com/v3/[redacted]/SAML2/</a>
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

Microsoft Azure

Home > [redacted] > Enterprise applications | All applications > Axomo | Single sign-on > SAML-based Sign-on

### Axomo | SAML-based Sign-on

Enterprise Application

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

- ##### User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- ##### SAML Signing Certificate

Status	Active
Thumbprint	6C5196899F4997E249C858FE7695C79E1AA3FA0C
Expiration	5/13/2023, 4:13:53 PM
Notification Email	[redacted]
App Federation Metadata Url	<a href="https://login.microsoftonline.com/0722e05a-6a...">https://login.microsoftonline.com/0722e05a-6a...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>
- ##### Set up Axomo

You'll need to configure the application to link with Azure AD.

Login URL	<a href="https://login.microsoftonline.com/0722e05a-6a...">https://login.microsoftonline.com/0722e05a-6a...</a>
Azure AD Identifier	<a href="https://sts.windows.net/0722e05a-6a46-4f3e-9...">https://sts.windows.net/0722e05a-6a46-4f3e-9...</a>
Logout URL	<a href="https://login.microsoftonline.com/common/wsf...">https://login.microsoftonline.com/common/wsf...</a>

[View step-by-step instructions](#)
- ##### Test single sign-on with Axomo

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

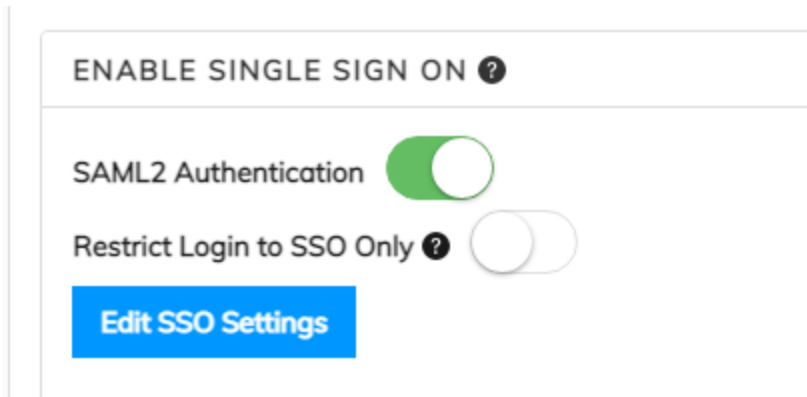
[Test](#)

3. Download the SAML Signing certificate (base64) from Step 3

4. You must manage which users and groups will have access to the Axomo App using AzureAD

## Axomo Steps

1. Navigate to Admin Panel->Users>Users Settings->Enable Single Sign On
2. Turn on Single Sign On



3. Copy over the Axomo Application ID from the App you set up in the first steps
4. SAML Signing Certificate
  - a. Download the SAML Signing certificate (base64) from AD
  - b. Open in it in your favorite text editor
  - c. Copy the Certificate and paste into Axomo
5. Copy the Azure AD Identifier Link into the IDP Issuer field

6. Copy the Login URL Link from Auzre AD to the Login URL on the SAML config

**SAML2 Configuration**

Reply URL: [https://api.axomo.com/v3/\[REDACTED\]/SAML2/](https://api.axomo.com/v3/[REDACTED]/SAML2/)

Application ID [?](#)

'Integration Name (usually axomo)'

SAML Signing Certificate (base64) [?](#)

Download, open in a text editor, and copy the SAML Signing Certificate (base64)

IDP Issuer [?](#)

[https://sts.windows.net/\[TENANTID\]/](https://sts.windows.net/[TENANTID]/)

Login URL [?](#)

[https://login.microsoftonline.com/\[TENANTID\]/saml2](https://login.microsoftonline.com/[TENANTID]/saml2)

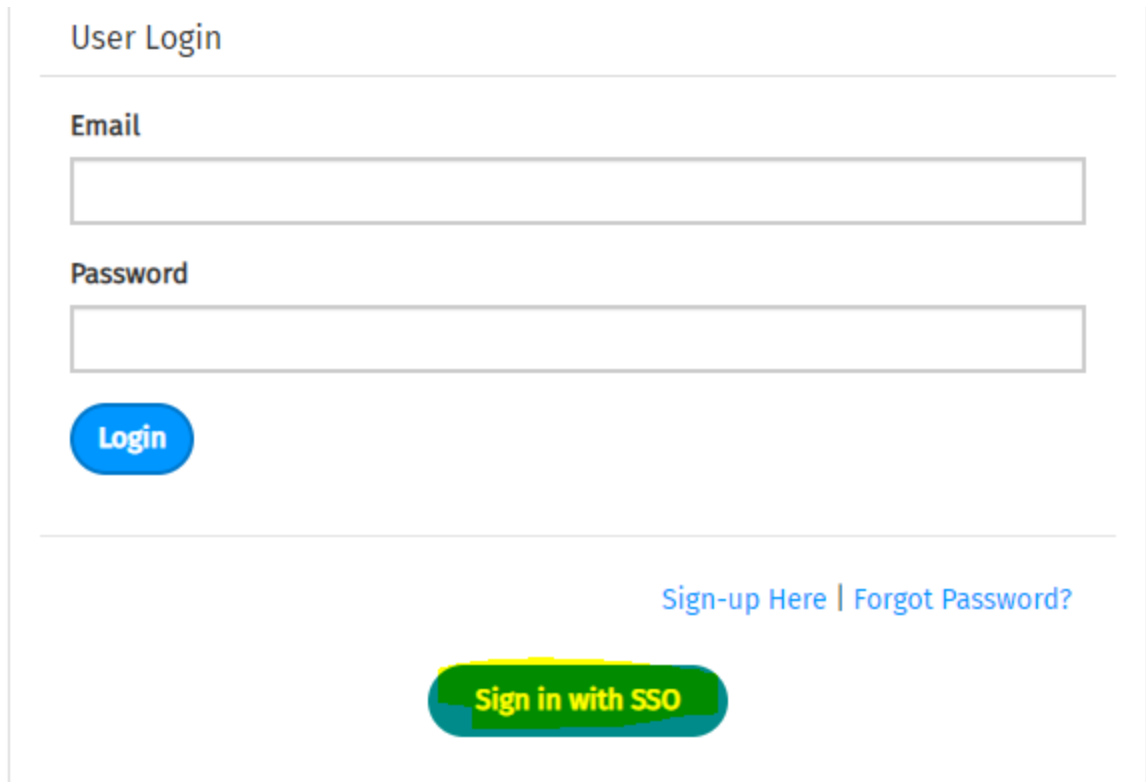
Login ID [?](#)

Email

Cancel OK

7. Click OK
8. Press Save
9. Open an incognito window

10. Verify it works by pressing login and then selecting the SSO button



The image shows a 'User Login' form. At the top, the text 'User Login' is displayed. Below it, there are two input fields: 'Email' and 'Password'. A blue 'Login' button is positioned below the password field. To the right of the login button, there is a link that reads 'Sign-up Here | Forgot Password?'. At the bottom center of the form, there is a prominent green button with a yellow gradient and rounded corners that says 'Sign in with SSO'.

11. Login using your Microsoft credentials

12. You should now successfully be logged into Axomo with your account