

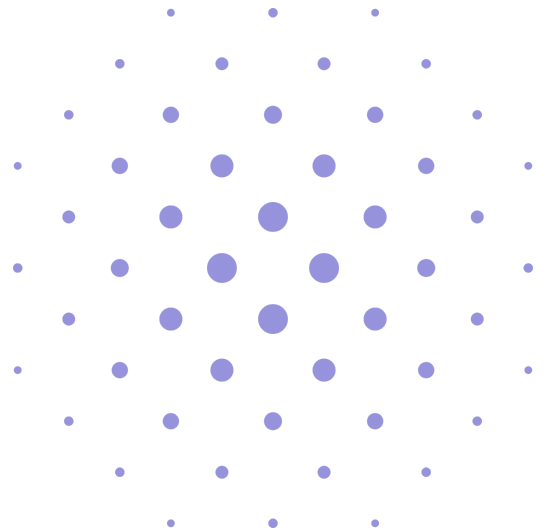


Lizzy SSO Instructions

Single Sign-On (SSO)

ISSUED BY

LizzyAI



Step 1

Open <https://abc.app.lizzyai.com/Saml2> website.
A file named "LizzyWeb.xml" will be downloaded.

Step 2

Open "Azure AZ Enterprise applications. Click New Application"



Home > Enterprise applications



Enterprise applications | All applications ...

Lizzy AI



+ New application



Refresh



Download (Export)

Step 3

Click "Create your application".

Home > Enterprise applications | All applications >

Browse Microsoft Entra Gallery ...



Create your own application



Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use.

Step 4

Type App Name: "LizzyWeb" and click the "Create" button.

 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?

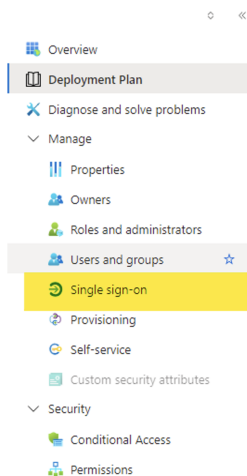
LizzyWeb ✓

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)

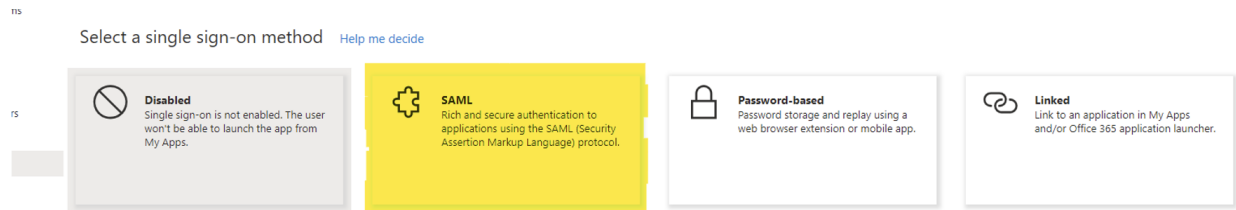
Step 5

On the left side menu click "Single sign-on".



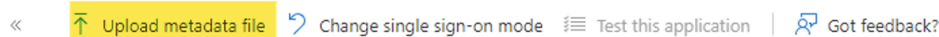
Step 6

Select "SAML".



Step 7

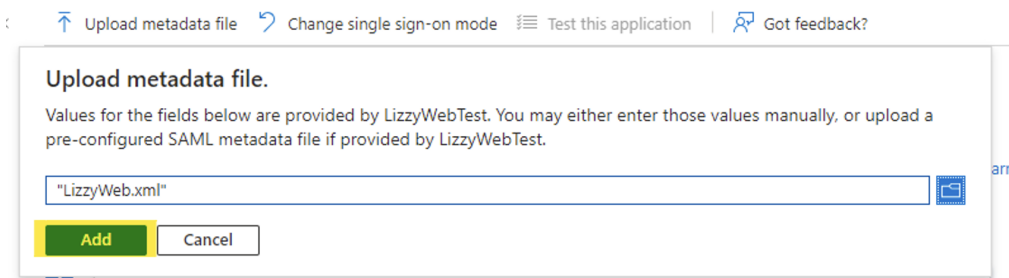
Click "Upload metadata file" and select the "LizzyWeb.xml" file from Step 1.



Set up Single Sign-On with SAML

Step 8

Select the "LizzyWeb.xml" file from Step 1 and Click "Add".



Step 9

Click "Save".

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

LizzyWeb

Add identifier

Step 10

Click "Edit".

Attributes & Claims

Edit

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

Step 11

Click on the first item.

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 [...]

Step 12

Change to "user.objectid" → Click "Save".

Manage claim ...

 Save  Discard changes |  Got feedback?

Name

nameidentifier

Namespace

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

^ Choose name identifier format

Name identifier format *

Email address

Source *

☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute *

user.objectid

∨ Claim conditions

Step 13

Click "Add a group claim".

Attributes & Claims ...

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

Step 14

Fill in the details → Click "Save".

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

☐ None

☐ All groups

☐ Security groups

☐ Directory roles

☒ Groups assigned to the application

Source attribute *

Group ID

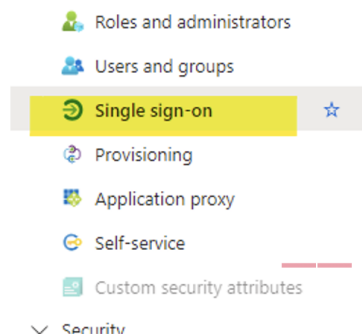
☐ Emit group name for cloud-only groups ⓘ

Advanced options

Save

Step 15

Go back to "Single sign-on" page.



Step 16

Please email us the "App Federation Metadata URL"

3

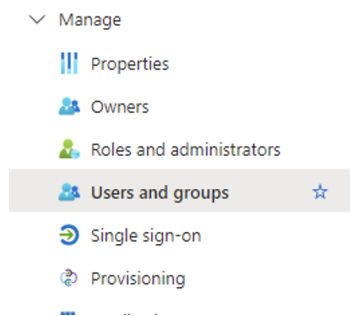
SAML Certificates

Token signing certificate		 Edit
Status	Active	
Thumbprint	B1372056C3917E88AB0E78127E3708683F769167	
Expiration	9/30/2027, 8:52:58 AM	
Notification Email	[REDACTED]	
App Federation Metadata Url	https://login.microsoftonline.com/895a1ba9-8b16-4a1a-b068-246b16400000/tenant/895a1ba9-8b16-4a1a-b068-246b16400000	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Assigning Users & Groups

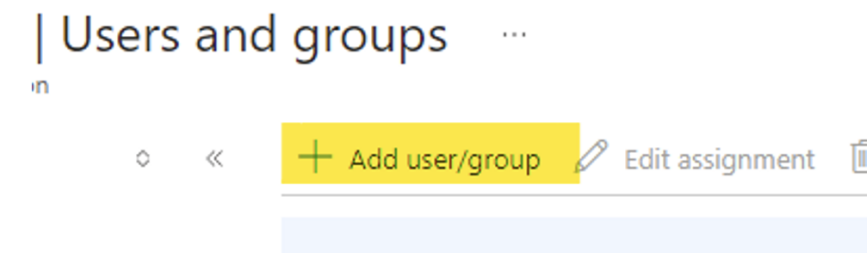
Step 1

On the left side select "Users and groups".



Step 2

Add user/Groups → Assign your users.



Step 3

Please create a User group name "Lizzy administrator", "Lizzy dashboard users" and assign users.

Step 4

Please send us the new group's "Object ID".

Basic information



Lizzy AI 

Lizzy AI

Membership type	Assigned	Total direct members	2
Source	Cloud	User(s)	2
Type	Microsoft 365	Group(s)	0
Object ID	3fbef950-89ff-41ca-b26d-744baa6da4cc 	Device(s)	0
Created on	6/20/2023, 7:23 PM	Other(s)	0

Grant Access and Test



Step 1

Grant Lizzy access to users or groups through Active Directory.



Step 2

Test your organization Lizzy instance by signing in with an email account to which you granted access in the previous step

Go to this link: <https://abc.app.lizyai.com/>



Authorization errors

If you are getting the screen below, it means the relevant user was not properly authorized by you. Ensure you grant access to the relevant user.


LizzyWeb

Sorry, but we're having trouble signing you in.

AADSTS50105: Your administrator has configured the application LizzyWeb () to block users unless they are specifically granted ('assigned') access to the application. The signed in user ' ' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.