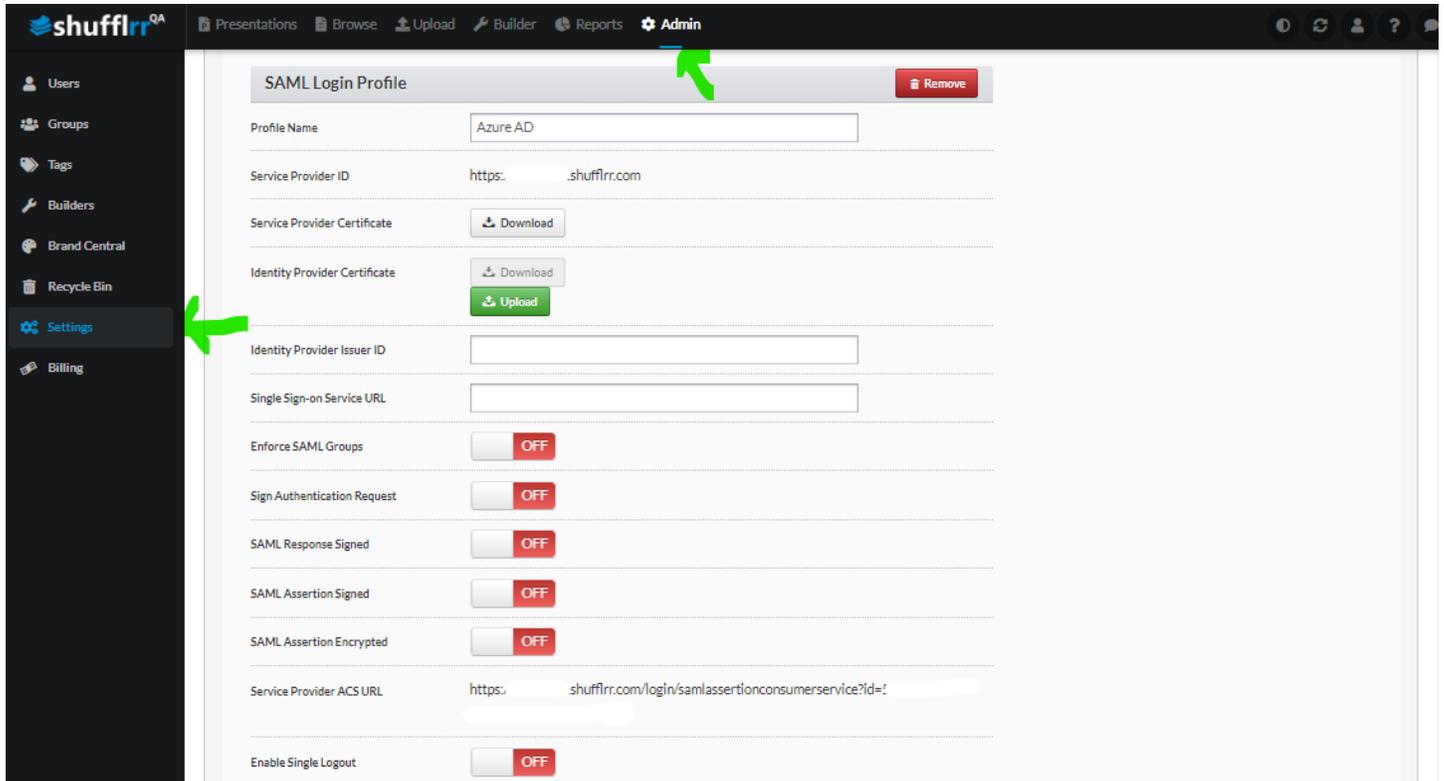


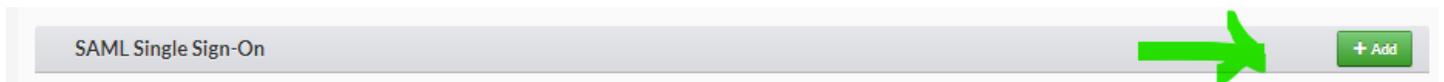
Setting up SSO for Shufflrr using Azure

On Shufflrr, go to your Admin > Settings and scroll down to Authentication, under SAML Sing Sign-On, click on + Add



The screenshot shows the Shufflrr Admin interface. The 'Settings' menu item is highlighted with a green arrow. The 'Admin' menu item is also highlighted with a green arrow. The SAML Login Profile form includes the following fields and options:

- Profile Name: Azure AD
- Service Provider ID: https://...shufflrr.com
- Service Provider Certificate: Download
- Identity Provider Certificate: Download, Upload
- Identity Provider Issuer ID: [Empty field]
- Single Sign-on Service URL: [Empty field]
- Enforce SAML Groups: OFF
- Sign Authentication Request: OFF
- SAML Response Signed: OFF
- SAML Assertion Signed: OFF
- SAML Assertion Encrypted: OFF
- Service Provider ACS URL: https://...shufflrr.com/login/samlassertionconsumerservice?id=!
- Enable Single Logout: OFF



The screenshot shows the SAML Single Sign-On configuration page. The '+ Add' button is highlighted with a green arrow.

On Azure, go to your Azure Active Directory Admin Center.

1. In the left menu, select **Enterprise applications**.
2. Click on the + sign to create New application, Select Azure AD SAML Toolkit
3. Name the application Shufflrr SSO (or something appropriate) and click Create
4. In the **Manage** section of the left menu, select **Single sign-on** to open the Single sign-on pane for editing.
5. Select SAML to open the SSO configuration page.
6. On the **Basic Simple Configuration** settings, click **Edit** and add values from Shufflrr based off the newly created SAML Profile above, accordingly.
 - a. Identifier (Entity DI) – <https://YOURSITE.shufflrr.com>
 - b. Sign on URL – <https://YOURSITE.shufflrr.com/login/samlassertionconsumerservice?id=xxxxxxxxxxxxxxxxxxx>
 - c. Sign on URL - <https://YOURSITE.shufflrr.com>
 - d. Relay State - Optional
 - e. Logout URL - Optional
7. On the **Attributes & Claims** settings, click **Edit**, click on **Add a new claim** and set values below, accordingly.

- Claim name & Namespace (email), Source attribute Value(user.mail)
- Claim name & Namespace (givenname), Source attribute Value(user.givenname)
- Claim name & Namespace(surname), Source attribute Value(user.surname)
- Claim name & Namespace (group), Source attribute Value(user.group)

Note that the email attribute is the unique identifier for each user. Also, the group attribute is Optional and only needed if you want to use the Enforce SAML feature of Shufflrr

Azure Active Directory admin center

Dashboard > Enterprise applications > Shufflrr >

Shufflrr | SAML-based Sign-on

Enterprise Application

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

Read the configuration guide for help integrating Shufflrr.

- #### Basic SAML Configuration

Identifier (Entity ID)	https://shufflrr.com	Edit
Reply URL (Assertion Consumer Service URL)	https://shufflrr.com/login/samlassertionconsumerservice?id=	
Sign on URL	https://shufflrr.com	
Relay State (Optional)	Optional	
Logout Url (Optional)	Optional	
- #### Attributes & Claims

user.mail/email	user.mail	Edit
user.givenname/givenname	user.givenname	
user.surname/surname	user.surname	
Unique User Identifier	user.userprincipalname	
- #### SAML Signing Certificate

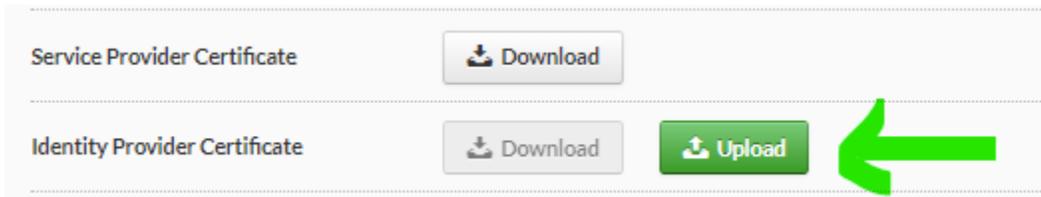
Status	Active	Edit
Thumbprint		
Expiration	7/6/2025, 4:12:31 PM	
Notification Email		
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com"/>	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Set up Shufflrr

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

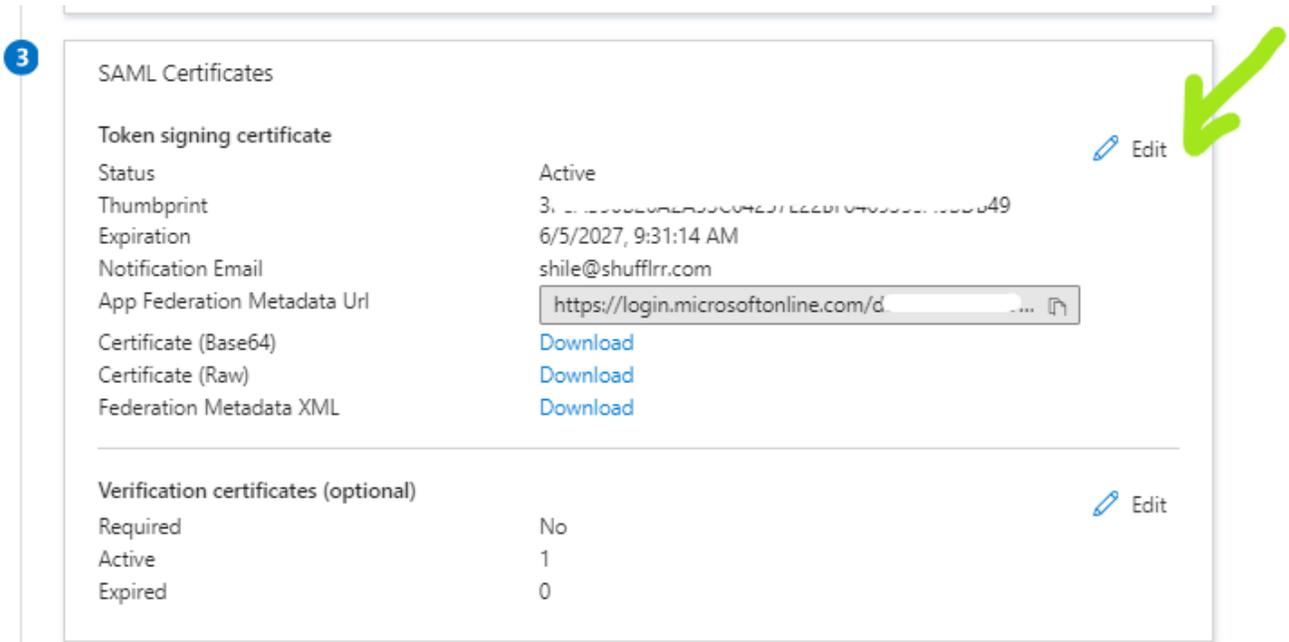
Login URL	<input type="text" value="https://login.microsoftonline.com"/>
Azure AD Identifier	<input type="text" value="https://sts.windows.net"/>
Logout URL	<input type="text" value="https://login.microsoftonline.com"/>

8. On the **SAML Signing Certificate** settings,
 - a. Download the Certificate(Base64)
 - b. Upload it into the Identify Provider Certificate on Shufflrr.



9. On the **Set up Shufflrr(Or your Application Name)** settings, copy the values below and paste into Shufflrr's, accordingly.
 - a. Copy the **Login URL** values and Paste into the **Single Sign-on Service URL** textbox on Shufflrr
 - b. Copy the **Azure AD Identifier** values and Paste into the **Identity Provider Issuer ID** textbox on Shufflrr.
 - c. Scroll down and hit the Blue Save button.

10. Under the **SAML Certificates** section, click on edit and in the new **SAML Signing Certificate** window, click on the signing option dropdown, then select sign SAML response and assertion and then save.



SAML Signing Certificate



Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

Save New Certificate Import Certificate | Got feedback?

Status	Expiration Date	Thumbprint	
Active	6/5/2027, 9:31:14 AM	3F...	...

Signing Option

Signing Algorithm

Notification Email Addresses

shile@shufflrr.com

11. Now on your Shufflrr site, go back to Admin > Settings and then scroll down to your SSO Profile you're working on, then turn on the SAML Response Signed and SAML Assertion Signed options.

Enforce SAML Groups	<input checked="" type="checkbox"/>
Sign Authentication Request	<input checked="" type="checkbox"/>
SAML Response Signed	<input checked="" type="checkbox"/>
SAML Assertion Signed	<input checked="" type="checkbox"/>
SAML Assertion Encrypted	<input type="checkbox"/>

12. If you haven't already done so, assign users to the Shufflrr application by going to User and Groups under the **Manage** section on the left. Search, select and assign users/groups accordingly.

Home > Shufflr. tSAML

Shufflr. Enterprise Application

tSAML | Users and groups

Manage

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

+ Add user/group | Edit assignment | Remove | Update credentials | Columns

i The application will not appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the 'Add app-role' button.

First 200 shown, to search all users & groups...

	Display Name	Object Type
<input type="checkbox"/>		User
<input type="checkbox"/>	 Patrick McKenna	User
<input type="checkbox"/>	 Shile Oguntade	User

13. After the application is configured, users can sign into it by using their credentials from the Azure AD tenant.
14. The process of configuring an application to use Azure AD for SAML-based SSO varies depending on the application. For any of the enterprise applications in the gallery.
15. When done, go to an incognito browser, visit your site and the login page should look something like below.

