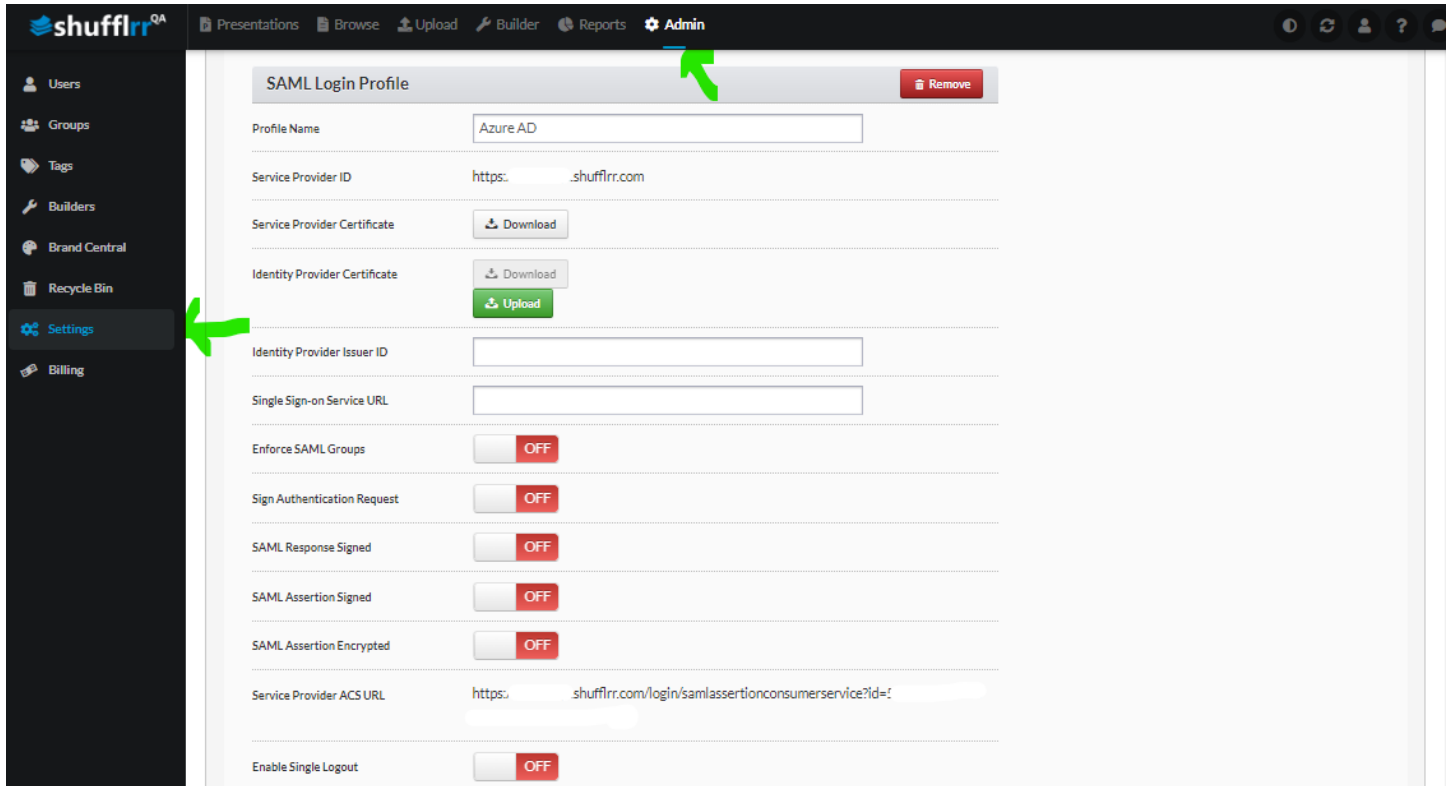


Setting up SSO for Shufflrr using Azure

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



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=xxxxxxxxxxxxxxxxxxxx>
 - 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

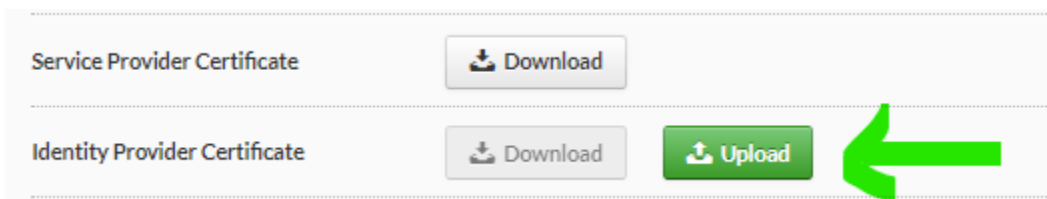
Status	Active	Edit
Thumbprint		
Expiration	7/6/2025, 4:12:31 PM	
Notification Email		
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com"/>	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Set up Shufflrr

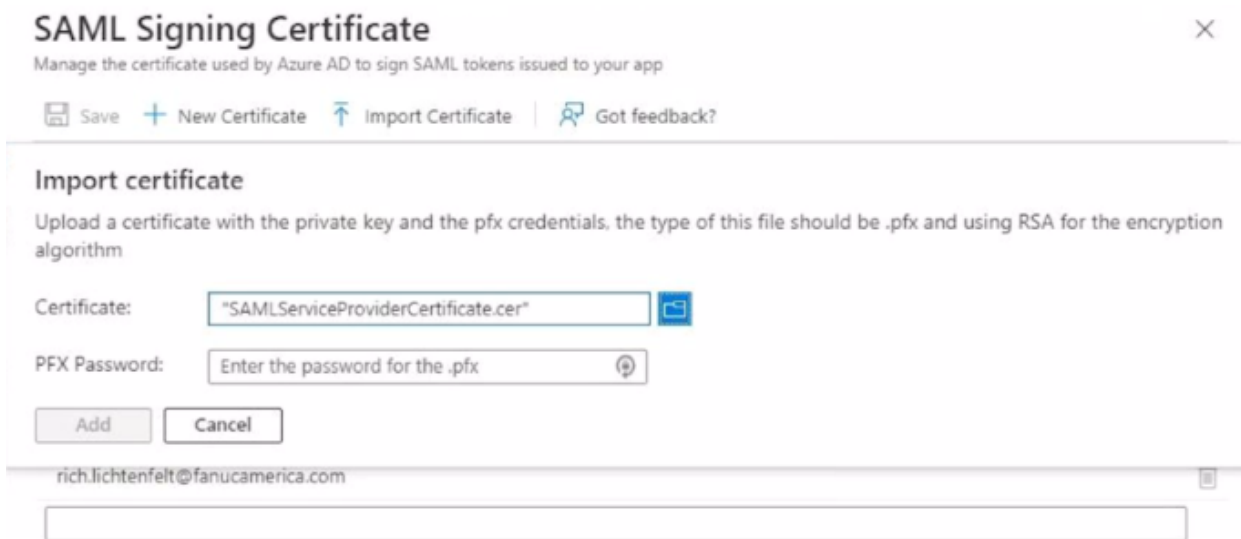
You'll need to configure the application to link with Azure AD.

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. Now, go back to your Shufflrr site and download the **Service Provider Certificate**. Then upload this certificate back to Azure under the SAML Signing Certificate. Scroll down and save these changes



Note that it needs to be a PFX with a password. [Convert cer to pfx.](#)

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

12. After the application is configured, users can sign into it by using their credentials from the Azure AD tenant.
13. 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.
14. When done, go to an incognito browser, visit your site and the login page should look something like below.

