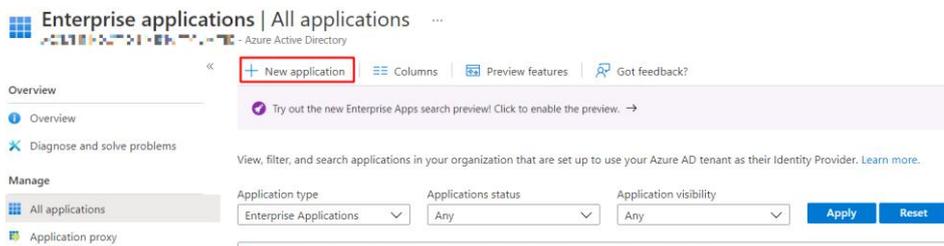


Setting up Azure SSO with EEG Cloud

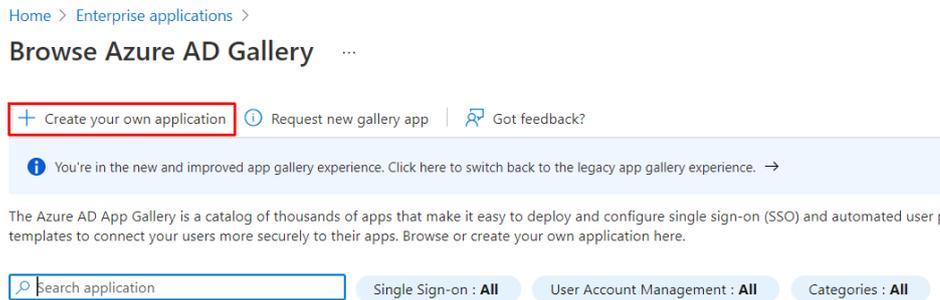
This guide provides instructions on setting up SSO logins into EEGCloud with Microsoft’s Azure system as your SAML Identity Provider.

Create a New Application

1. Navigate to Enterprise Application on your Azure Portal or by clicking on the link: https://portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/AllApps/menuId/
2. Click on the “New Application”



3. Select “Create your own Application”



4. Enter “EEG Cloud” for your application name and select the same option as screen shot below and select 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?

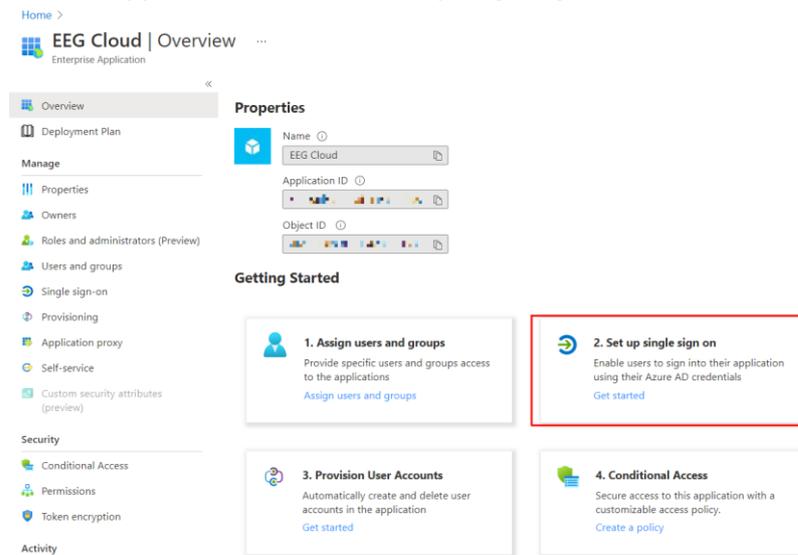
What are you looking to do with your application?

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

Create

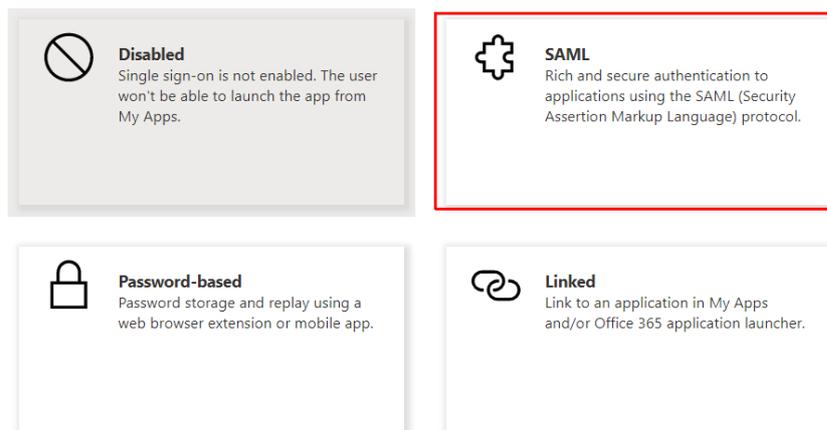
Set up Single Sign On

1. In the newly created application, select “2. Set up single sign on”



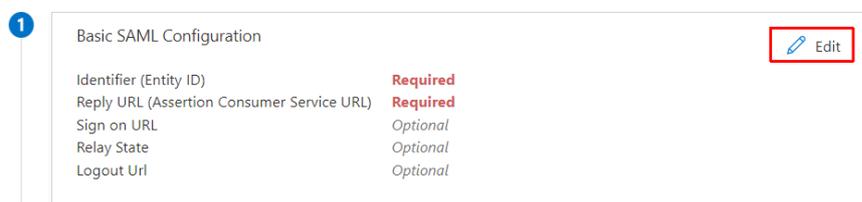
2. Select “SAML”

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



1. Basic SAML Configuration

1. Select “Edit” in the Basic SAML Configuration



2. Fill in the Identifier (Entity ID) and Reply URL (Assertion Consumer Service URL) as provided by your EEG support contact. Typically, this will look like:

Entity ID: *https://eegcloud.tv/saml/metadata/*

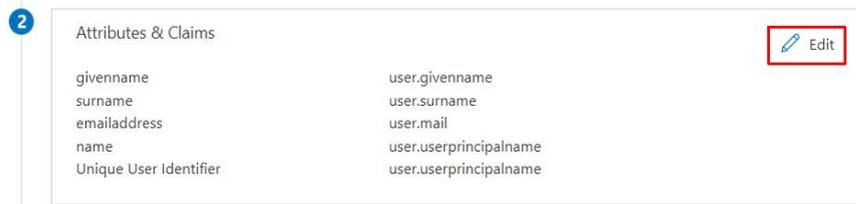
Sign on URL: *https://eegcloud.tv/saml?acs*

3. Save

2. Attributes & Claims

If your company does not have multiple Billing Groups with EEG Cloud, you can leave this as default and continue to the step 3. If you have multiple Billing Groups, continue with this step.

1. Select “Edit” under “Attributes & Claims”



2. Select “Add a group claim”

[Home](#) > [EEG Cloud](#) > [SAML-based Sign-on](#) >

Attributes & Claims

[+ Add new claim](#) [+ Add a group claim](#) [Columns](#) | [Got feedback?](#)

3. Select the following options as the screenshot below and “save”

Group Claims ×

Manage the group claims used by Azure AD 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

Advanced options

Customize the name of the group claim

Name (required)

Namespace (optional)

Emit groups as role claims ⓘ

4. For each group you add to the Application under Users and Groups. You will need to provide the Object ID of the group to the matching Billing ID.
5. You can find the Groups Object ID in the groups settings View in Azure AD

Delete | Got feedback?

EE

EEGCloud

Membership type	Assigned
Source	Windows Server AD
Type	Security
Object id	[Object ID]
Creation date	06/09/2021, 10:25:42 am

3. SAML Signing Certificate

1. After configuring Step 1. Step 3 in the SAML Signing Certificate will have automatically generated your certificate.
2. Please download all 3 of the options and send to your EEG support contact, or the general helpdesk at support@eegent.com

SAML Signing Certificate

Edit

Status	Active
Thumbprint	[Thumbprint]
Expiration	18/11/2024, 7:48:10 pm
Notification Email	[Email]
App Federation Metadata Url	https://login.microsoftonline.com/
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4. Set up EEG Cloud

1. To finalise your configuration. Please provide the follow data to the EEG support contact:

4

Set up EEG Cloud

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

Login URL	https://login.microsoftonline.com/
Azure AD Identifier	https://sts.windows.net/
Logout URL	https://login.microsoftonline.com/

[View step-by-step instructions](#)

Final Testing

Once you have provided the details to EEG, we will configure the entries on our end. Once the link is established, we can start testing the SSO configuration.