

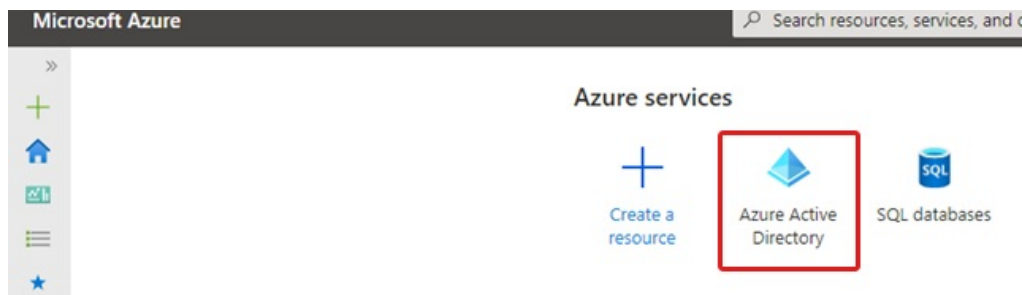
Setting up Single Sign-On (SSO) for users with Azure Active Directory

Last Modified on 04/29/2024 5:29 am EDT

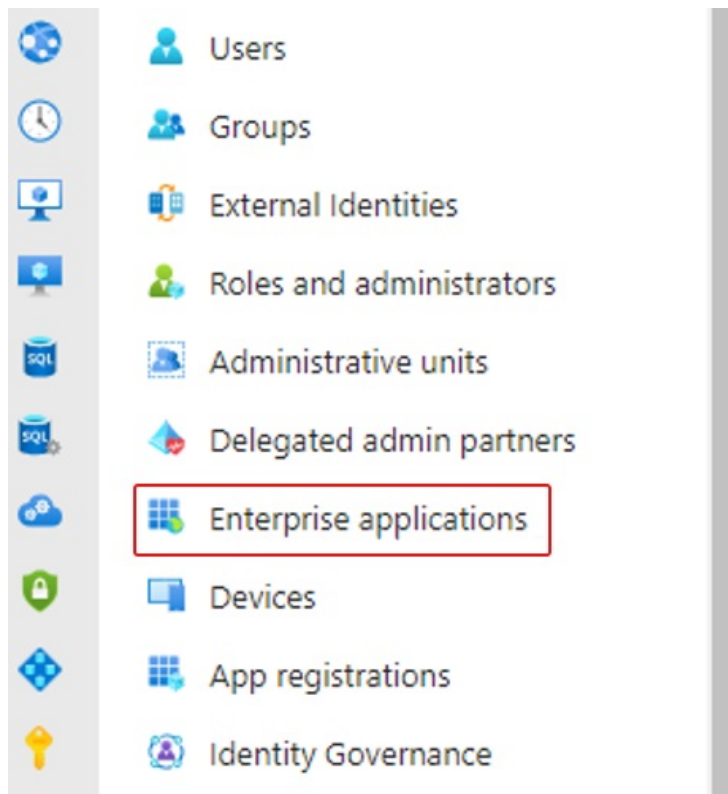
This article tells you to set up Single Sign-On integration with a Microsoft Azure (Active Directory) AD account, for your EventsAir users (people who work in your team).

Create a new Enterprise Application in Azure

1. Log into your Microsoft Azure
2. Under Azure services, find Azure AD in the portal



3. You should be able to see Enterprise Application as an option on the left.




After selecting this option, click on the + icon at the top to add a new Enterprise Application. This will be the basis for your AD set up.

4. Click on **+Create your own application** and enter a unique name, such as **alias-sso** [where **alias** is your EventsAir unique alias].

Leave the bottom radio button [Non-gallery option] selected and click "Create". This may take a couple of minutes.

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)

5. Assign users/groups to the Enterprise App. (You'll need to have at least one user in your Azure AD)

6. Click on the second link under Overview, "2. Set up single sign on", Get Started.

7. Select SAML, and you should now see the below:

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating alias-ssso.

- 1** Basic SAML Configuration Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- 2** Attributes & Claims
⚠ Fill out required fields in Step 1

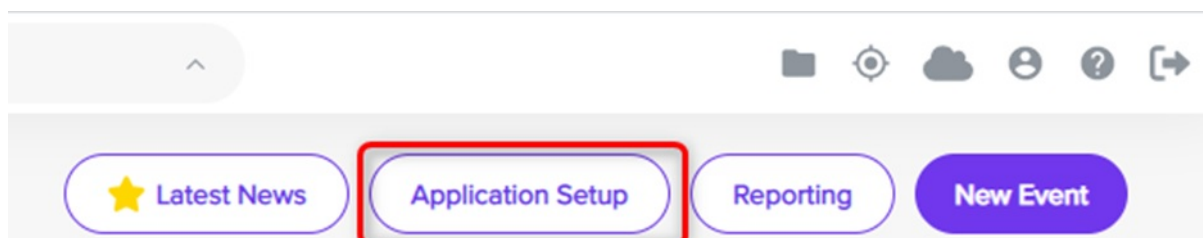
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- 3** SAML Certificates Edit

Token signing certificate	
Status	Active
Thumbprint	F8A23-...
Expiration	10/3/2027, 4:06:49 AM
Notification Email	k.petrat@eventsair.com
App Federation Metadata Url	https://login.microsoftonline.com/6bd11972-...
Certificate (Base64)	Download

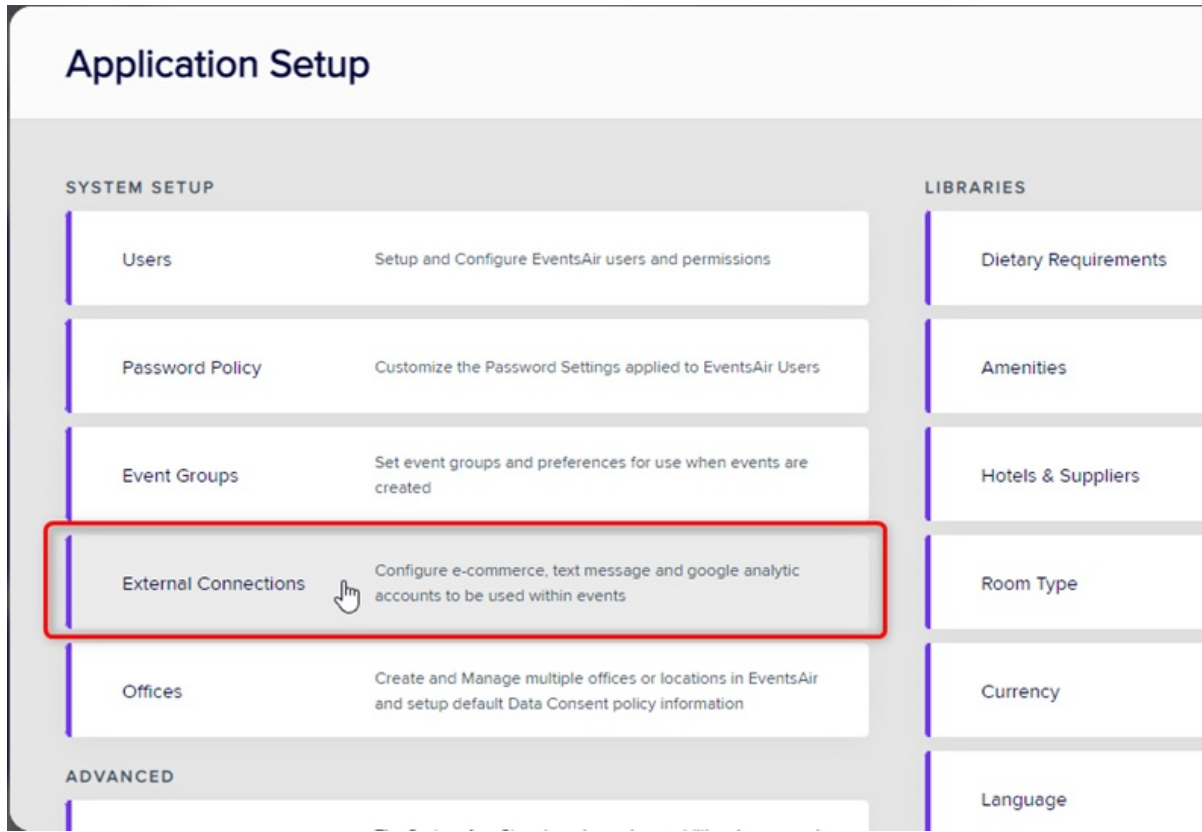
Set up the link between EventsAir and your Azure AD

Log into EventsAir, and keep the two screens (EventsAir and Azure AD) open side-by-side so you can copy information across.

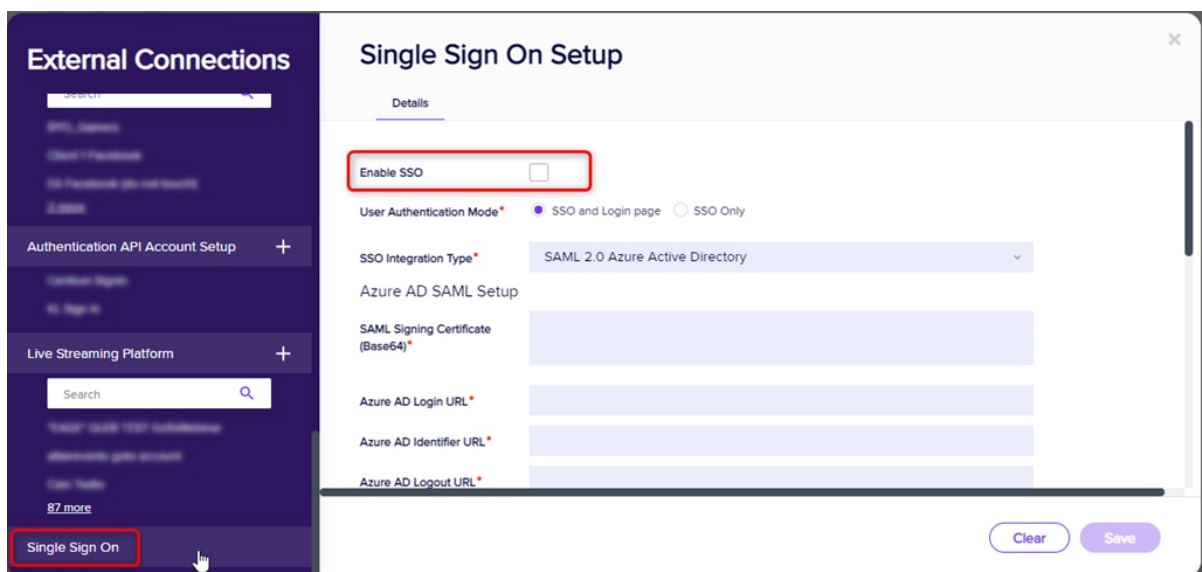
8. In EventsAir, go to Application Setup



9. Select External Connections



10. Select Single Sign-On from the left-hand menu and tick the checkbox for Enable SSO.



Leave the User Authentication mode as **SSO and Login page**. This allows EventsAir technical support and your Success Specialist to sign in and help as required within your environment as needed. When you create an

EventsAir from your own organization, you can set this to login via SSO only.

11. Return to the Azure AD SAML set-up to fill in more details:

Go to **Box1** and select **Edit**

Add your unique identifier (the one you entered earlier, e.g. **alias-sso**)

From the EventsAir SSO set-up, scroll down to **Reply URL** and copy the URL

Back in Azure AD SAML Box 1, paste the URL into the "**Add reply URL**" field

Click Save in Azure AD.

12. Still in Azure AD, jump to **box 3** and select **Edit**.

13. Click **+New Certificate**, then **Save** and close the window. This will generate a new certificate for you to download.

14. Return to the same Box 3 and now select the Download link, next to Certificate (Base 64).

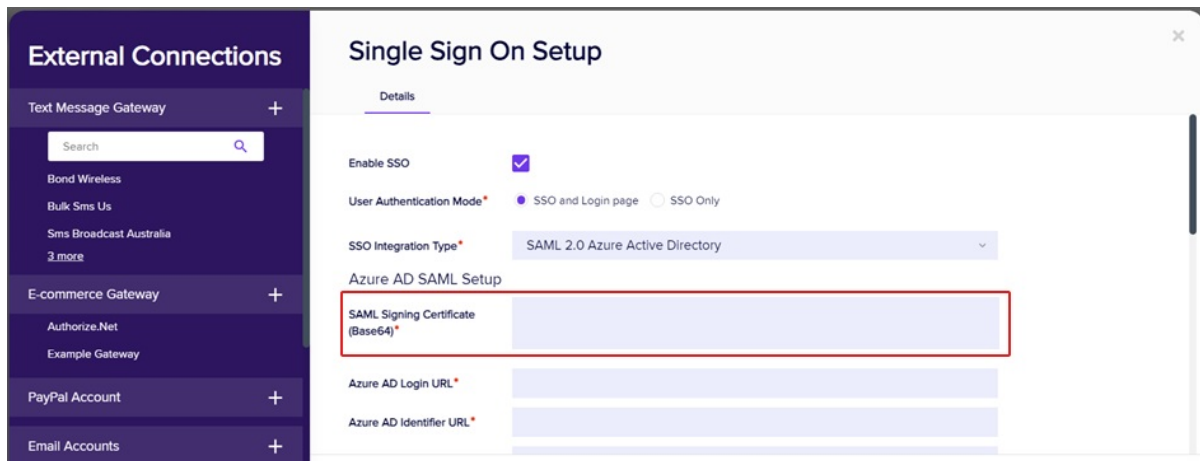
When you open the downloaded Certificate file in Notepad, you should see something like the below. You need to copy ONLY the numbers and letters BETWEEN the "begin certificate" line and the "end certificate" line. [i.e. as shown highlighted in bold here]

----BEGIN CERTIFICATE---

```
T3VyIG1pc3Npb24gaXMgc2ltcGxlOiB0byBoZWxwIGV2ZW50IHBsYW5uZXJzIGRlIGl2ZXIgd
GhllFdpVybBpb0aGVpciBldmVudHMgd2l0aCB3b3JsZCdzIG1vc3QgcG93ZXJmdWwgZXZlbn
QgbWFuYWdlbWVudCBwbGF0Zm9ybS4KClIdlIGRvIHROaXMgYnkkgd29ya2luZyB3aXRoIGFuIG
FtYXppbmcgdGVhbSB0aGF0IHb1c2hlcyB0aGUgbGltXRzIG9mlHdoYXQncyBwb3NzaWJsZS
wgZXZlcnkgZGF5LiBpdXlhc3Rvcnkgc3RhcmlZCBpbAOTkwLCB3aGVuIGV2Z3JvdXAgb2YgZ
XZlbnQgb3JnYW5pemVycyBhbmQgc29mdHdhcmUgZGV2ZWxvcGVycyBzZXQgb3V0IHVudGVud
NoYWxsZW5nZSB0aGUgc3RhdHVzIHVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVud
obm9sb2d5IHVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVud
KU2luY2UgdGh1biwgZGVudmUgZGV2ZWxvcGVkIHVudGVudGVudGVudGVudGVudGVudGVudGVud
3ZhdGlvbnMgaW4gZXZlbnQgbWFuYWdlbWVudCB0aXN0b3J5LgoKQW5kIGFsb25nIHROZS
B3YXksIHdlJ3ZlIHVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVud
0aGUgbGF5Z2VzdCBldmVudHMgaW4gdGhllHdvcmxkLg
```

----END CERTIFICATE----

15. Back in EventsAir, paste this into the box called **SAML Signing Certificate (Base64)**



16. From Azure AD Box 4, copy the Login URL, Azure AD Identifier, and Logout URL. Paste each one into the equivalent field in EventsAir. It will look something like this:

Enable SSO	<input type="checkbox"/>
User Authentication Mode*	<input checked="" type="radio"/> SSO and Login page <input type="radio"/> SSO Only
SSO Integration Type*	SAML 2.0 Azure Active Directory
Azure AD SAML Setup	
SAML Signing Certificate (Base64)*	ZXZlcnkgZGF5LiBpdXlgc3Rvcnkgc3RhcncRIZCBpbAaxOTkwLCB3aGVuIGegZ3JvdXAgb2YgZXZlbnQgb3JnYW5pemVycyBhbmQgc29mdHdhcmUgZGV2ZWxvcGVycyBzZXQgb3V0IHRvIGNoYWxsZW5nZSB0aGUgc3RhdHVzIHFMbyBhbmQgY3JlYXRlIHVuaXF1ZSBldmVudCB0ZWNoYm9sb2d5IHNVbHV0aW9ucyB0aGF0IG1hZGUgdGhllGltcG9zc2libGUgYSByZWZsaXR5LgoKU2luY2UgdGhliwgd2UndmUgZGV2ZWxvcGVkIHNVbWUgb2YgdGhllGpZ2dlc3QgaW5ub3ZhdGlvbnMgaW4gZXZlbnQgbWFuYWdlbWVudCB0aXN0b3J5LgoKQW5klGFsb25nIHRoZSB3YXksIHdlJ3ZlIHByb3VkbHkgc3VvcGxpZWQgb3VyIHRIY2hub2xvZ3kgdG8gc29tZSBvZiB0aGUgbGFyZ2VzdCBldmVudHMgaW4gdGhllHdvcmxkLg
Azure AD Login URL*	https://login.microsoftonline.com/6bd11972-XXXXXXXXXX-XXXXXXXXXX-XXXX
Azure AD Identifier URL*	https://sts.windows.net/6bd11972-XXXXXXXXXX-XXXXXXXXXX-XXXX
Azure AD Logout URL*	https://login.microsoftonline.com/6bd11972-XXXXXXXXXX-XXXXXXXXXX-XXXX
Azure AD SAML User Attributes & Claim Tags	
Unique User ID*	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
First Name*	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Last Name*	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Email*	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

- From Azure AD Box 1, take the unique identifier (Entity ID) that you entered in Step 11, then look in EventsAir for the heading **Azure AD Enterprise Application Information Required**. There is a field called "Identifier" where you should paste the unique identifier/Entity ID.



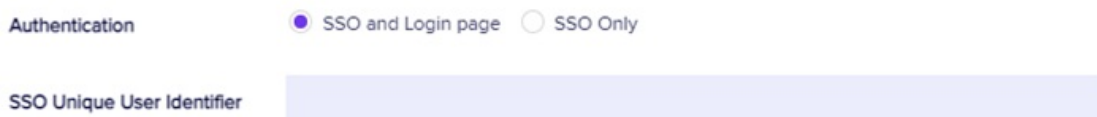
Azure AD Enterprise Application Information Required

Identifier

- In EventsAir, save the SSO set up, and close the External Connections settings panel.

Set up a User with Single Sign-On

- Back in Application Setup, click Users.
- To add a user who is provisioned in your Azure AD account, select whether you want **SSO Only and Login page** (using EventsAir User Name and Password) or **SSO Only**.



Authentication SSO and Login page SSO Only

SSO Unique User Identifier

Ensure the user name as displayed in Azure AD is entered into the SSO Unique User Identifier box.

- Any users who are already provisioned in your Azure AD who also had a user account in EventsAir before you set all this up will need to be updated.

New users who will be accessing EventsAir also need to be added. If not, and they try to access EventsAir via Single Sign-on, they'll get a notification advising them that their account needs to be configured in EventsAir first. (This also triggers an email to your Administrators advising that a new user needs to be provisioned. You can decide who these Administrators should be in your SSO set up, as shown below.)

EventsAir User Provisioning

Send Provisioning Request
Email To

- All EventsAir Administrators
 Specified EventsAir Administrators

Select Users

Once the Administrator creates this user in the EventsAir user list, they should let the user know that SSO login is now available to them.
