Azure Entra ID (Azure AD) – SAML SSO Configuration Guide

Step 1: Create an Enterprise Application

1. Go to https://entra.microsoft.com
2. In the left menu, click **"Applications"** → **"Enterprise applications"**
3. Click **"+ New application"**
4. Select **"Create your own application"**
5. Enter a name (e.g. `Sadevio Visitor SSO`)
6. Choose **"Integrate any other application you don't find in the gallery"**
7. Click **Create**

Step 2: Add entra information to sadevio

https://help.sadevio.com/books/entra-ad-sso-saml/page/sadevio-configuration

Step 3: Configure SAML-based Sign-On

1. In the new app, go to **"Single sign-on"**
2. Select **SAML** as the sign-on method
3. Fill out the **Basic SAML Configuration** with the following values:

Field	Value
Identifier (Entity ID)	`https://cloud.sadevio.com/sadevio_module/api/localhost/saml/{tenant_id}`
Reply URL (ACS URL)	`https://cloud.sadevio.com/sadevio_module/api/localhost/saml/callback?tenant=` `{tenant_id}`
Sign on URL	`https://cloud.sadevio.com`
Relay State (Optional)	*(Leave empty)*

Field	Value
Logout URL (Optional)	`https://cloud.sadevio.com/adevio_module/api/localhost/saml/logout?tenant=` `{tenant_id}`

You can copy and paste these values from the configuration form inside the Sadevio admin panel

Step 4: Configure User Attributes & Claims

1. Click **Edit** under **Attributes & Claims**
2. Ensure the following claims are included (default setup should already have them):
   - `email` → user's email address
   - `givenname` → user's first name
   - `surname` → user's last name
   - `name` or `userprincipalname` → unique identifier (used as NameID)

i The `NameID` claim should ideally be set to the user's **email** address (you can adjust this in "Unique User Identifier").

Verification certificates.

On the sadevio platform, you can download the certificate to sign the authentication request. Download the certificate and upload it to entra.microsoft.com

Select "Require verification certificats" and upload the sadevio certificate

Step 5: Download Certificate and SSO URL

1. Under **SAML Signing Certificate**, download the following:
   - **Certificate (Base64)** – This is the **X.509 Certificate**
2. Also copy the **Login URL** – This is the **Azure SSO URL**
3. (Optional) Copy the **App Federation Metadata URL** – used if you want dynamic configuration

Step 6: Download Certificate and SSO URL

1. Under **SAML Signing Certificate**, download the following:
   - **Certificate (Base64)** – This is the **X.509 Certificate**

2. Also copy the **Login URL** – This is the **Azure SSO URL**
3. (Optional) Copy the **App Federation Metadata URL** – used if you want dynamic configuration

Step 7: Assign Users

1. In Azure, go to the **Users and groups** section of the Enterprise App
2. Click **+ Add user/group**
3. Select the users or groups who should be able to sign in using SSO
4. Click **Assign**

Revision #4
Created 31 May 2025 06:04:00 by Admin
Updated 2 February 2026 21:48:10 by Admin