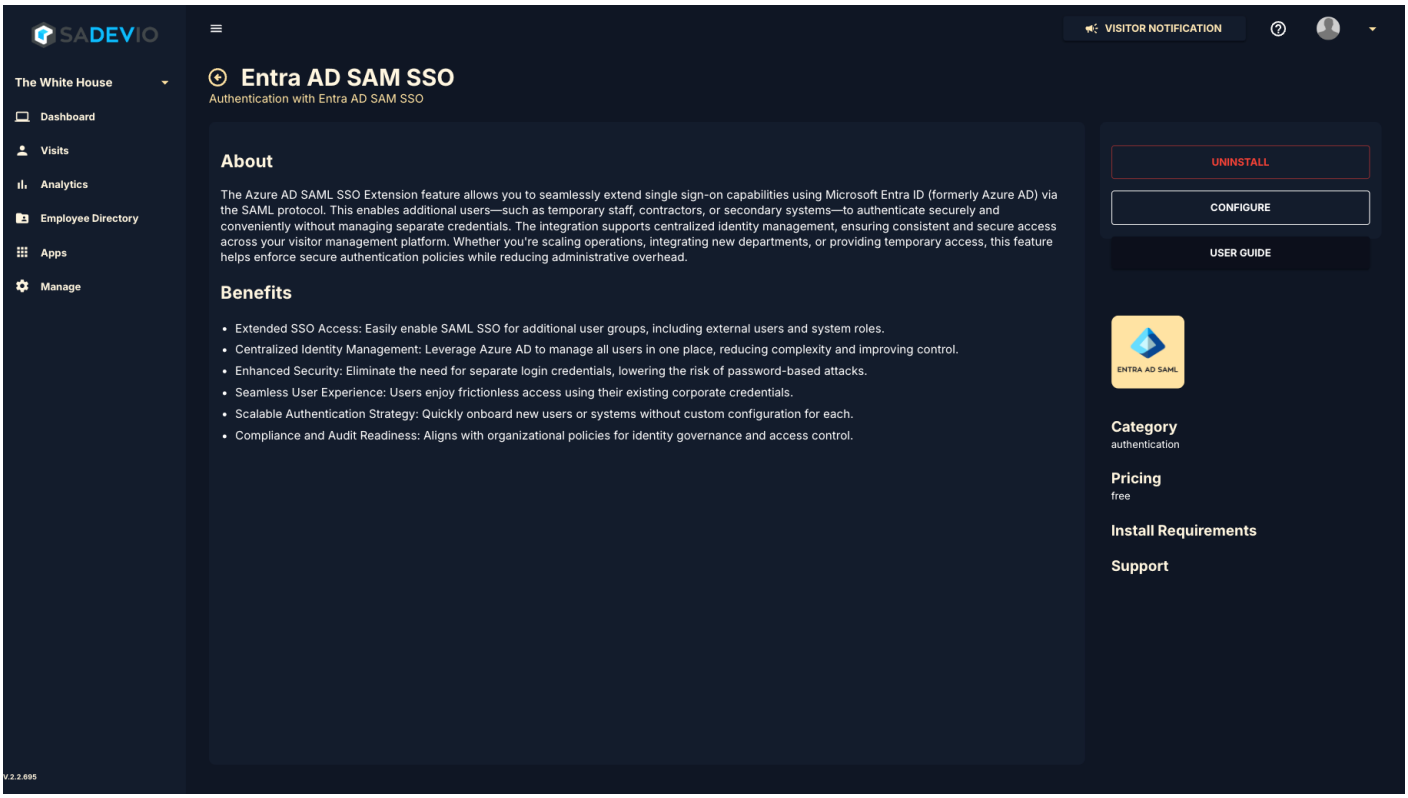
Entra AD SSO SAML

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

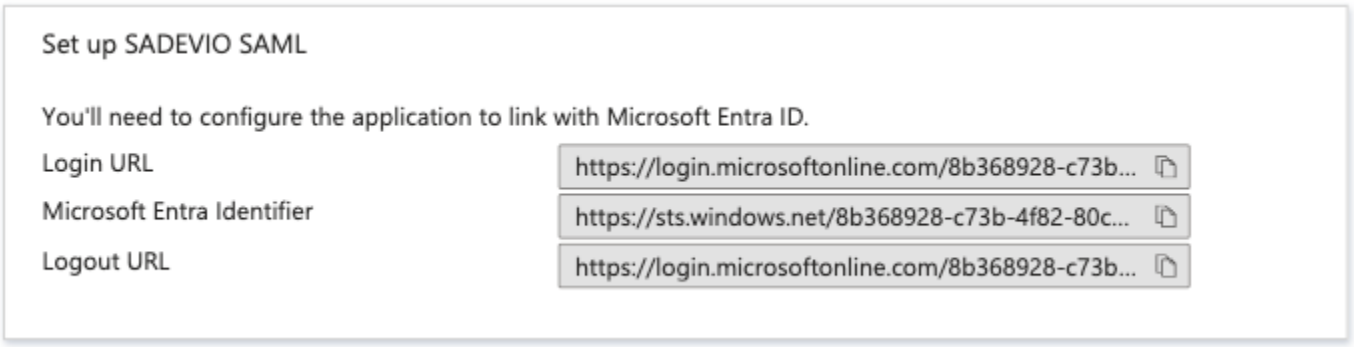
Sadevio Configuration

To activate the sadevio Entra AD sso saml login to your application and go to Apps and select Entra AD SSO SAML

Install the application.



Under step 4 you can find the needed urls on the azure portal.



Azure Entity ID (entra_entity_id)

Copy the "microsoft Entra identifier" e.g. https://sts.windows.net/8b368928-c73b-4f82-80c3-5718b55b7351/

Azure SSO URL

Copy the "Login URL" e.g.

https://login.microsoftonline.com/8b368928-c73b-4f82-80c3-5718b55b7351/saml2

X.509 Certificate

Download the Certificate (Base64) and paste the content

e.g. -----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQL44GWK+1j5pEf9lbkJiRfTANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD
EylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yNTA1MzAyMzE2
NThaFw0yODA1MzAyMzE2NThaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQg
U1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqAS1wuq1oXaO
sdcuFZj/HCMKs2wdsfx0V0Jw+UOxaE0YuWycze70F2v4MvOOk/KwOOz8czCTvn43VVQlrUTX2ylv
NqQCWMmEwShrQ1CHRoh5T3R4wXn1aC5XRJFnPepBartmUTAwoyCriTOrhFW4xU8jmQT1i3EP5tkq
FOmZ97hOOgSD+G4lQUkR+b1gAnN/1HBx9r5q9+R2tZB2+t+i3EI3JVXF6XmcYVPnJR/M2wEPqlil
FiY/nOxjnnQ4nFF5VzzWGjD1vfSuOXswxqZRLoE+wTK2LqhKfF7xUx9UFdfCQMV0rahE5ZR8lLTf
6h0q356goOyE6pT1ymwLSfZ17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBygoMNWNjmUlCa/U/6
U1l2uZb9IHwudCEIDOc0iXSCQxwlIob9S5R7mIFNx847xQTNWterrwEsddSxwznzeR4lRZpNQHzI
nReymGubELCHhW6AqMjyQzEr2wst41qPufecfa9n/dPUFSBDbeuqHBhAj0hb3jF5m4g4Ewry9ewz
pcqO0wQNnN2Wd9pQuSekw2CZH76IWBD1Y/Sdi4Knm/zMpzPosUidKcs3glLSrEOT/sow+EMoz1k1
7T41JBDCSHd0Q2bNW5zSGv8o6p7rWSQQ32YPY3VajmPdBsp/6vjQWDNpvoCJ1GjeQaUA0Ohitw5D
4RzXYDT93h1EmzyylAJa
-----END CERTIFICATE-----

Azure Metadata URL

Copy the App Federation Metadata Url in section 3e.g. https://login.microsoftonline.com/8b368928-c73b-4f82-80c3-5718b55b7351/federationmetadata/2007-06/federationmetadata.xml?appid=bfb35151-15fd-4e1d-a357-6cb695f2c282

Example Configuration



User authentication activation

To activate the authentication type Entra SAML SSO, you need to configure the user to the entra saml soo authentication type under Employees.

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**