

# Setting up Delegated Authentication with SAML on Microsoft Azure

Before setting up the installer, you have to configure Microsoft Entra ID.

## Set up Microsoft Entra ID

With an account with enough rights, go to : Enterprise Applications

- Click on New Application
- Click on Create your own application on the top left corner
- Choose a name for it, and select Integrate any other application you don't find in the gallery
- Click on "Create"
- Select Set up single sign on
- Select SAML
- Edit on Basic SAML Configuration
- In Identifier , add the following URL : `https://<synapse fqdn>/_synapse/client/saml2/metadata.xml`
- Remove the default URL
- In Reply URL , add the following URL : `https://<synapse fqdn>/_synapse/client/saml2/authn_response`
- Click on Save

Home > Enterprise applications | All applications > ESS

ESS | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

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 ESS.

1 Basic SAML Configuration

Identifier (Entity ID) `https://matrix.example.com/_synapse/client/saml2/metadata.xml`

Reply URL (Assertion Consumer Service URL) `https://matrix.example.com/_synapse/client/saml2/authn_response`

Sign on URL `Optional`

Relay State (Optional) `Optional`

Logout URL (Optional) `Optional`

2 Attributes & Claims

uid `ExtractMailPrefix (user.userprincipalname)`

email `user.mail`

displayName `user.displayName`

Unique User Identifier `user.userprincipalname`

3 SAML Certificates

Token signing certificate `Active`

Status `Active`

Basic SAML Configuration

Save Got feedback?

Identifier (Entity ID) \*

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

`https://matrix.example.com/_synapse/client/saml2/metadata.xml`

Add identifier

Reply URL (Assertion Consumer Service URL) \*

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

`https://matrix.example.com/_synapse/client/saml2/authn_response`

Add reply URL

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

- Make a note of the App Federation Metadata Url under SAML Certificates as this will be required in a later step.
- Edit on Attributes & Claims
- Remove all defaults for additional claims
- Click on Add new claim to add the following (suggested) claims (the UID will be used as the MXID):
  - Name: uid , Transformation : ExtractMailPrefix , Parameter 1 : user.userprincipalname
  - Name: email , Source attribute : user.mail
  - Name: displayName , Source attribute : user.displayName
- Click on Save

## Attributes & Claims ...

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

### Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

### Additional claims

Claim name	Type	Value
displayName	SAML	user.displayname
email	SAML	user.mail
uid	SAML	ExtractMailPrefix (user.us...

▼ Advanced settings

- In the application overview screen select `Users` and `Groups` and add groups and users which may have access to element

## Configure the installer

Add a SAML provider in the 'Synapse' configuration after enabling `Delegated Auth` and set the following (suggested) fields in the installer:

- `Allow Unknown Attributes`
- Under `Attribute Map`, select the `Identifier` - `URN: Oasis: Names: TC: SAML: 2. 0: Attrname`  
`Format: Basic`

# User Mapping Provider

## Mapping between SAML attributes and MXIDs

MXID Mapping

Dotreplace

Two modes of mapping - hexencode maps unpermitted characters to '=xx'  
dotreplace replaces unpermitted characters with '.'

MXID Source Attribute \*

uid

The SAML Source attribute used to generate MXIDs

- Under Mapping add the following (suggested) mappings:
  - From: Primary Email To: email
  - From: First Name To: firstname
  - From: Last Name To: lastname

# Attribute Map

Map from SAML Name-format attribute to attributes

Identifier 

URN:Oasis:Names:TC:SAML:2.0:Attrname Format:Basic

The identifier is the name-format you expect to support

## Mapping

=

From \*

Primary Email

The SAML name-format to read

To \*

email

The attribute to convert the saml name-format to

=

From \*

First Name

The SAML name-format to read

To \*

firstname

The attribute to convert the saml name-format to

=

- Under `Entity`, enter a `description`, the `Entity ID` (from Azure) and a `name`.

## Entity

### How Synapse will expose itself as a SAML Entity

Description \*

Element Server

Edited

Your synapse deployment description

Entity ID \*

https://<matrix fqdn>/\_synapse/client/saml2/metadata.xml

Edited

Your Synapse entity ID

Name \*

ElementChat

Your synapse deployment name

- Under `User Mapping Provider` select the following:
  - `MXID Mapping`: `Dotreplace`
  - `MXID Source Attribute`: `uid`
- Under `Metadata URL`, add the `App Federation Metadata URL` from Azure.

When clients connect, along with any existing authentication methods still enabled, they should now also have an option to `Continue with SAML`:



# Sign in

Homeserver



Edit

Sign in with

Username



Username

Password

[Forgot password?](#)

**Sign in**

**Continue with SAML**

English



[New here? Create an account](#)



# Welcome back!

Where your conversations live

[Redacted]  
[Redacted]

Edit

Username / Email / Phone

Password

[Forgot password](#)

Next

or

Continue with SAML

Revision #30

Created 1 February 2023 10:37:05 by Simon Addis

Updated 8 May 2024 16:30:28 by Kieran Mitchell Lane