

FileSender - AzureAD as IdP - setup guide (External)

- [Description](#)
- [Configuration example: Microsoft Azure AD as IDP, FileSender \(simpleSAMLphp\) as SP](#)
 - [Prerequisites](#)
 - [Step 1: Create an Enterprise application in Azure AD](#)
 - [Step 2: Configure the Token encryption](#)
 - [Step 3: Manage Users and groups](#)
 - [Step 4: Configure the Single sign-on \(SAML\)](#)
 - [Step 5: Configure User Attributes & Claims](#)
 - [Step 6: Verify SAML Signing Certificate](#)
 - [Step 7: Ensure that your metadata is up-to-date and correct in the Belnet Federation](#)
 - [Step 8: Test Single sign-on with FileSender](#)

Description

In this document, we will give an example of how to configure an Azure AD as IdP (Identity Provider) for Single Sign On management on the Belnet Filesender (acting as Service Provider).

This documentation is published on the [Filesender FAQ on the Belnet website](#) to help Belnet customers configure/set up their Azure AD Identity Provider

Configuration example: Microsoft Azure AD as IDP, FileSender (simpleSAMLphp) as SP

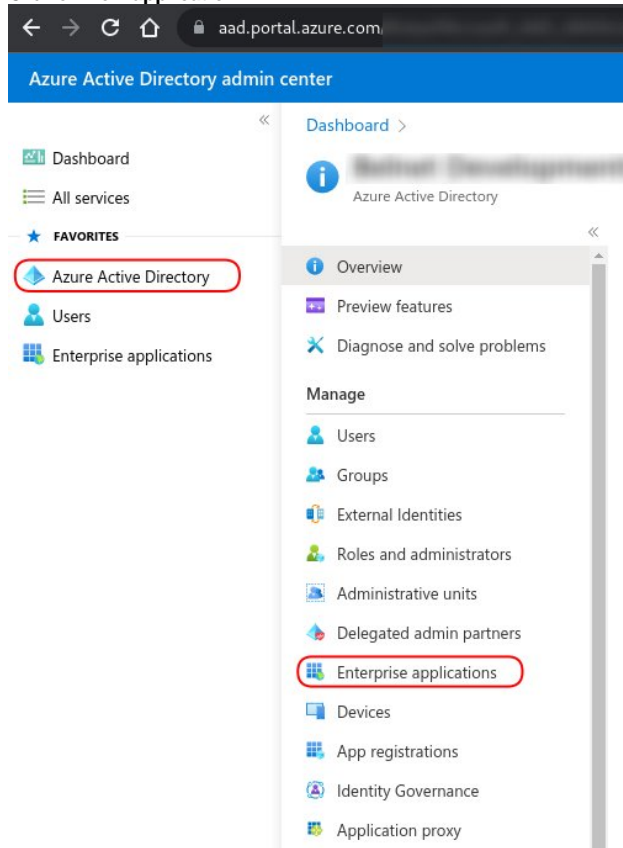
Prerequisites

- The Azure AD must be created with at least one (non-admin) user.
- [The Azure AD must have access to Token encryption and Single sign-on functionalities which are part of Azure AD Premium P1 or P2 subscription.](#)
- The Azure AD, the simpleSAMLphp and the FileSender server must have their respective domain and **SSL certificate generated** and correct.
- Both servers/service must be **reachable** from each other and from you (Azure AD via Azure portal and FileSender server via SSH).

Step 1: Create an Enterprise application in Azure AD

- On Microsoft Azure Portal or [Azure Active Directory admin center](#) **Azure Active Directory --> Enterprise applications**

- Click on **New application**



Dashboard > Enterprise applications > Enterprise applications

Enterprise applications | All applications

- Azure Active Directory

+ New application Refresh Download

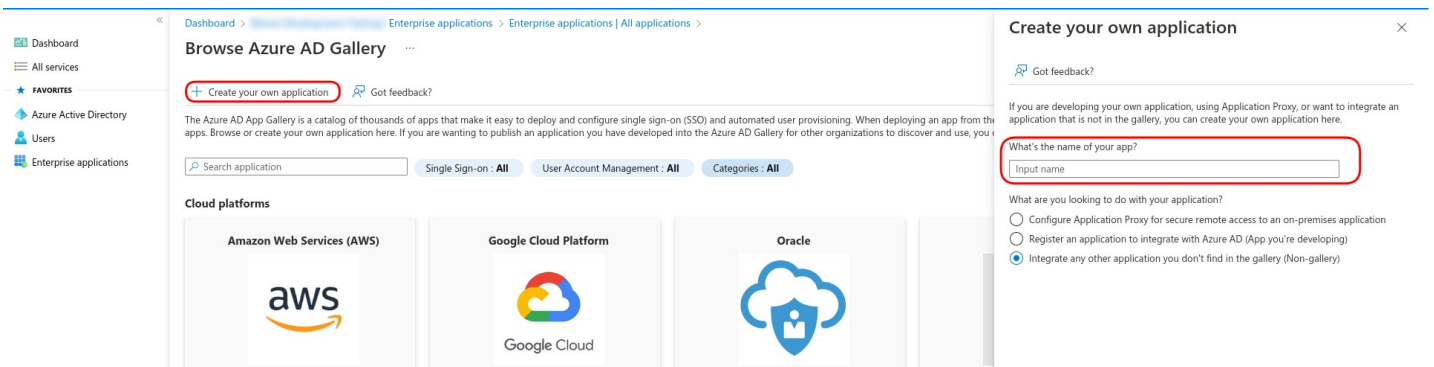
Overview

- Overview View, filter, and search applications in your organization
- Diagnose and solve problems The list of applications that are maintained by your organization

Manage

Search by application name or object ID

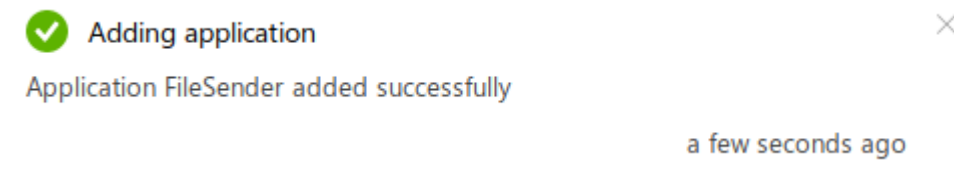
- Click on **+ Create your own application**, enter **FileSender** in the **Name** field and click **Create**



- Enter **FileSender** as your AppName in the field, then click **Add**
- Wait while Azure AD is adding the application



- After the application is added successfully, proceed to next step



Step 2: Configure the Token encryption

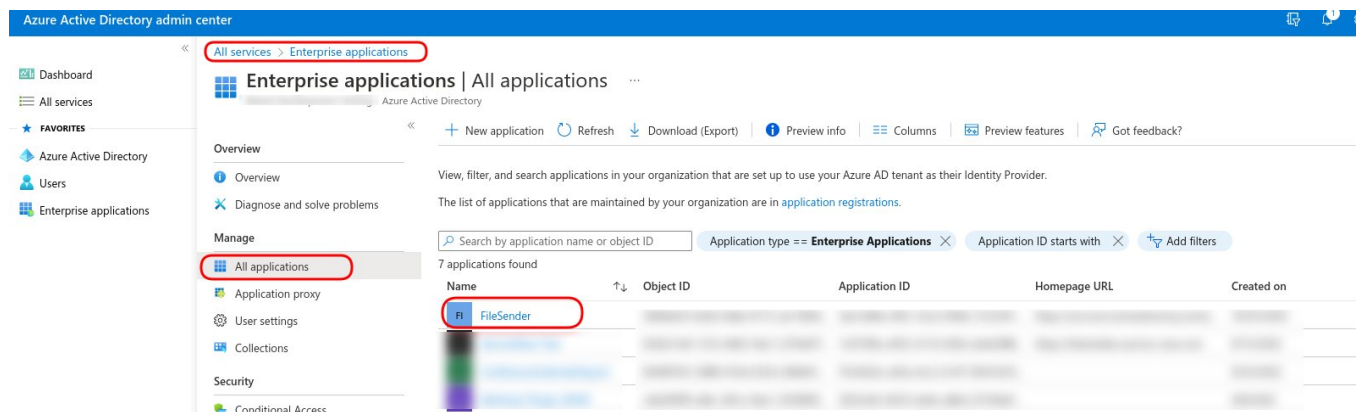
- Retrieve/Download now the Belnet Filsender certificate used for metadata:

This can be done in two different ways:

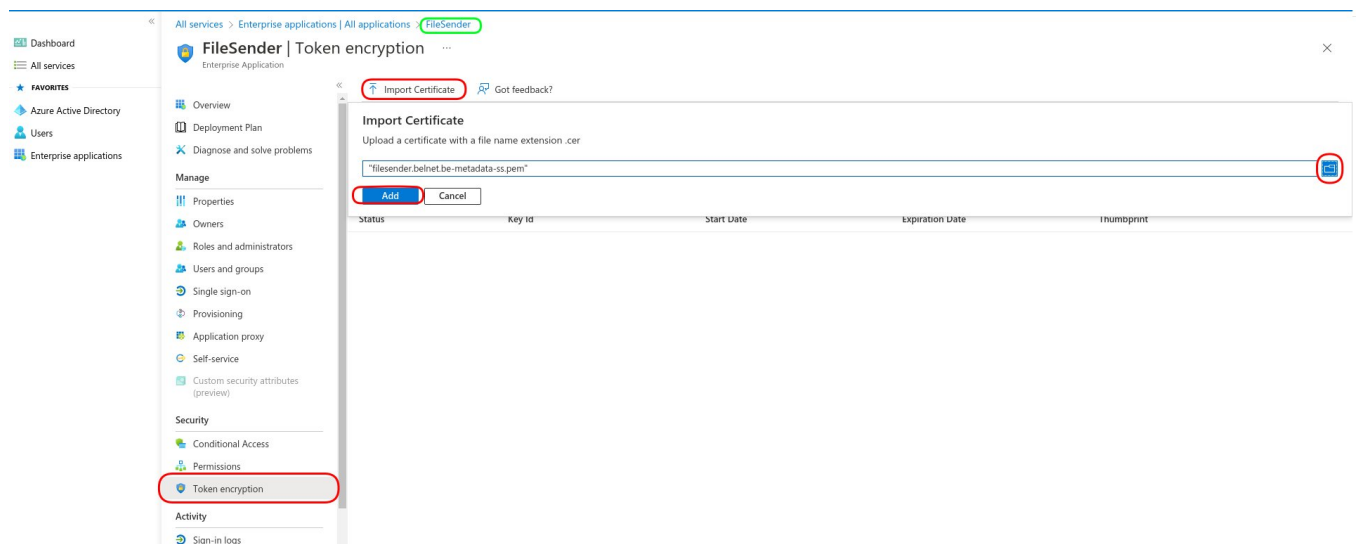
- by downloading the certificate itself on: <https://filesender.belnet.be/filesender.belnet.be-metadata-ss.pem>
or
- by consulting SAML Metadata on the Service Provider itself (FileSender SP) at url: <https://filesender.belnet.be/simplesaml/module.php/saml/sp/metadata.php/belnet-filesender-sp?output=xhtml&language=en>

certificate content is available within attributes `<ds:X509Certificate></ds:X509Certificate>`

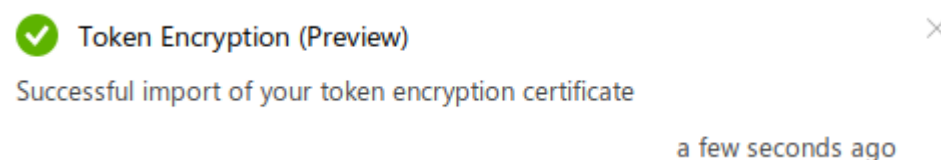
- On Microsoft Azure Portal or [Azure Active Directory admin center](#) **Azure Active Directory --> Enterprise applications All Applications**
- **Select** your newly created application named **FileSender**



- Click on **Token encryption**, then click on **Import Certificate**
- Select the **certificate** fetched previously and click on **Add**



- Wait for the **successful** import of the certificate



- Click on the **3 dots button** and click on **Activate token encryption**

Import Certificate | Got feedback?

Please activate a certificate to enable token encryption

SAML token encryption enables the use of encrypted SAML assertions with an application that supports it. Encrypting the SAML assertions between Azure AD and the application provides additional assurance that the content of the token can't be intercepted, and personal or corporate data compromised. [Learn more.](#)

Status	Key Id	Start Date	Expiration Date	Thumbprint
Inactive		6/29/2022, 3:04:18 PM	6/28/2032, 3:04:18 PM	Thumbprint will not be displayed

- Activate token encryption certificate
- Delete token encryption certificate
- Deactivate token encryption certificate

- Click on **Yes**

Import Certificate

Activate token encryption certificate

You are about to activate token encryption for your application. Please ensure that your certificate has been successfully onboarded on your application's site.

Yes No

- Verify the **successful** activation of the token encryption certificate

Import Certificate | Got feedback?

✔ **Token Encryption (Preview)**

Successful activation of your token encryption certificate

a few seconds ago

Token encryption is enabled

SAML token encryption enables the use of encrypted SAML assertions with an application that supports it. Encrypting the SAML assertions between Azure AD and the application provides additional assurance that the content of the token can't be intercepted, and personal or corporate data compromised. [Learn more.](#)

Status	Key Id	Start Date	Expiration Date	Thumbprint
Active		6/29/2022, 3:04:18 PM	6/28/2032, 3:04:18 PM	Thumbprint will not be displayed

Step 3: Manage Users and groups

- On Microsoft Azure Portal or Azure Active Directory admin center, go to **Azure Active Directory Enterprise applications All applications FileSender** Under **Manage (Left Pane) Users and groups**, click on **Add user**

Microsoft Azure

Home > Standardmap > Enterprise applications - All applications > FileSender - Users and groups

FileSender - Users and groups

+ Add user Edit Remove Update Credentials Columns

The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
No application assignments found		

Manage

- Overview
- Getting started
- Deployment Plan
- Diagnose and solve problems

Users and groups

- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption (Preview)

Activity

- Click on **User and groups**

Home > Standaardmap > Enterprise applications - All applications > FileSender - Users and groups > Add Assignment

Add Assignment

Standardmap

Users and groups
None Selected >

Select name >

User

Assign

- For this example, we will select the group **filesender** with user **beta** as member of. **Please adapt as it fits to your organisation.** Click on **Select**

Users and groups ✕

Select member or invite an external user ⓘ

Search by name or email address ✓

BE beta

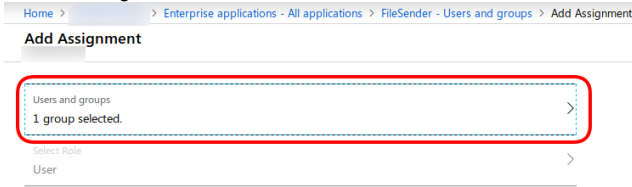
FI filesender

Selected members:

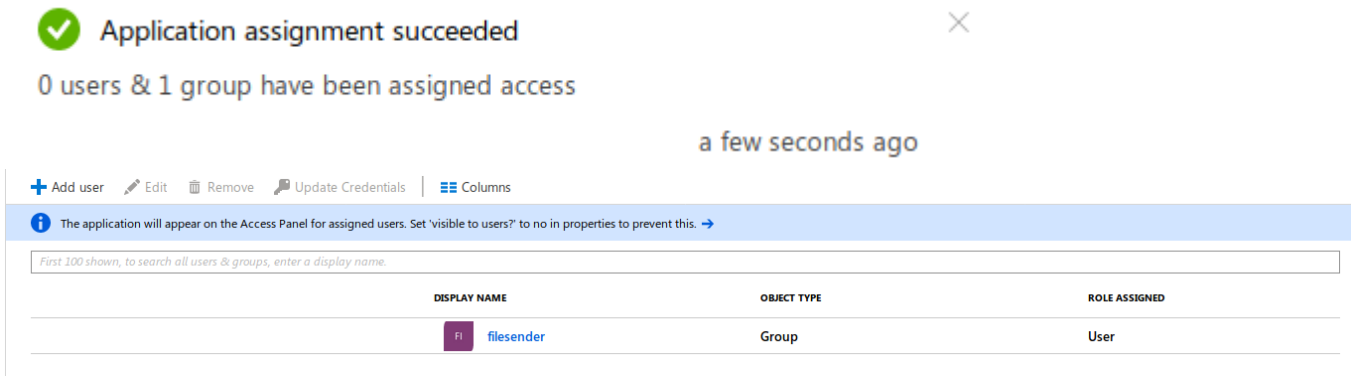
FI filesender Remove

Select

- Click on Assign

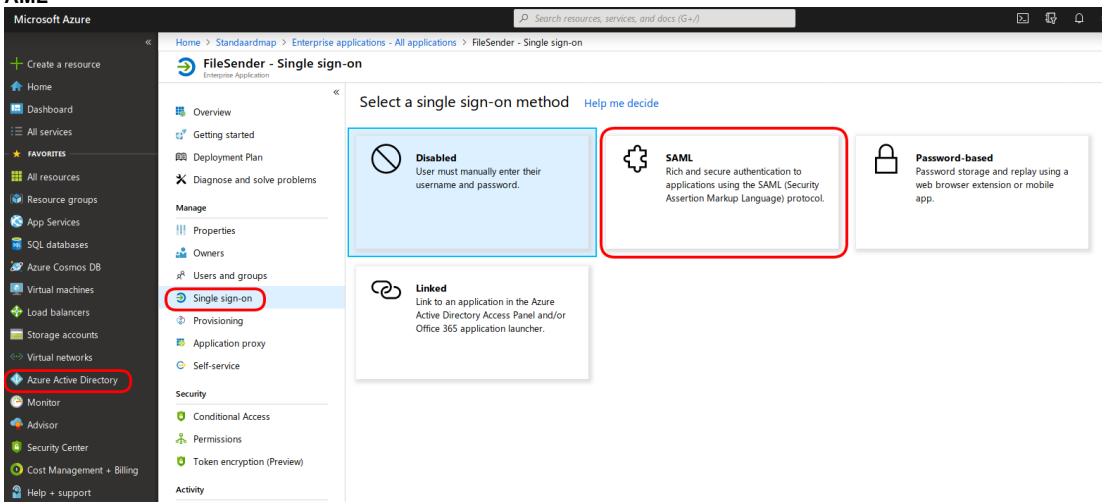


- Group **filesender** has been assigned access (as **user**) to the **FileSender** application

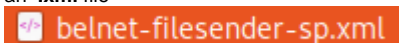


Step 4: Configure the Single sign-on (SAML)

- On Microsoft Azure Portal, go to **Azure Active Directory** **Enterprise applications** **All applications** **FileSender** **Manage** **Single sign-on**, click on **SAML**



- Download the Belnet FileSender SP metadata from <https://filesender.belnet.be/simplesaml/module.php/saml/sp/metadata.php/belnet-filesender-sp> as an **.xml** file



- Click on **Upload metadata file**, select the previously downloaded **Belnet FileSender SP metadata xml file** and click on **Add**

[↑ Upload metadata file](#)
[↺ Change single sign-on mode](#)
[☰ Test this application](#)
[❤️ Got feedback?](#)

Upload metadata file.

Values for the fields below are provided by FileSender. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by FileSender.

- If the metadata file upload is **successful**, you will get the **Basic SAML Configuration** with the fields **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** filled, click on **Save**

Basic SAML Configuration ✕

* Identifier (Entity ID) ⓘ
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default
 ⓘ

* Reply URL (Assertion Consumer Service URL) ⓘ
The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default
 ⓘ

Sign on URL ⓘ

Relay State ⓘ

Logout Url ⓘ

- If the metadata file upload is **unsuccessful**, click on the **edit button** of **Basic SAML Configuration**

[↑ Upload metadata file](#)
[↺ Change single sign-on mode](#)
[☰ Test this application](#)
[❤️ Got feedback?](#)

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating FileSender.

1 Basic SAML Configuration ✎

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

- And fill the following fields:
Identifier (Entity ID): <https://filesender.belnet.be>
Reply URL (Assertion Consumer Service URL): <https://filesender.belnet.be/simplesaml/module.php/saml/sp/saml2-acs.php/belnet-filesender-sp>
 Click on **Save**
- The system will ask you if you want to test Single sign-on with FileSender, click on **No, I'll test later** for now

[↑ Upload metadata file](#)
[↺ Change single sign-on mode](#)
[☰ Test this application](#)
[❤️ Got feedback?](#)

Test single sign-on with FileSender

To ensure that single sign-on works for your application, we recommend using the testing capability (in the last step) to test the changes you recently made. Would you like to test now?

Step 5: Configure User Attributes & Claims

- Click on the edit button of User Attributes & Claims

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating FileSender.

1

✎

Basic SAML Configuration	
Identifier (Entity ID)	https://filesender.belnet.be
Reply URL (Assertion Consumer Service URL)	https://filesender.belnet.be/simplesaml/module.php/saml/sp/saml2-acs.php/belnet-filesender-sp
Sign on URL	<i>Optional</i>
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>

2

✎

User Attributes & Claims	
Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

- Modify the Additional claims from

[Home](#) > [Enterprise applications - All applications](#) > [FileSender - Single sign-on](#) > [SAML-based Sign-on](#) > [User Attributes & Claims](#)

User Attributes & Claims

[+](#) Add new claim
 [+](#) Add a group claim
 [☰](#) Columns

CLAIM NAME	VALUE	...
Required claim		
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress]	...
Additional claims		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname	...

- To:

User Attributes & Claims

[+](#) Add new claim
 [+](#) Add a group claim
 [☰](#) Columns


CLAIM NAME	VALUE	...
Required claim		
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress]	...
Additional claims		
cn	user.displayname	...
eduPersonPrincipalName	user.userprincipalname	...
mail	user.userprincipalname	...

Step 6: Verify SAML Signing Certificate

- Verify that the SAML Signing Certificate is Active

3

SAML Certificates

Token signing certificate		 Edit
Status	Active	
Thumbprint	[REDACTED]	
Expiration	5/22/2027, 10:02:49 PM	
Notification Email	[REDACTED]	
App Federation Metadata Url	[REDACTED]	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Step 7: Ensure that your metadata is up-to-date and correct in the Belnet Federation

- You must now publish the metadata of your IdP in the official Belnet Federation . Log on to Belnet Federation Metadata Manager website (<https://federation.belnet.be>).
- Add your IdP and upload the metadata of your IdP.

Step 8: Test Single sign-on with FileSender

After your metadata has been verified and approved by Belnet, you can test the SSO with Belnet Filesender (acting as Service Provider) and your Identity Provider (IdP).