## FileSender - AzureAD as IdP - setup guide (External)

#### Description

- Configuration example: Microsoft Azure AD as IDP, FileSender (simpleSAMLphp) as SP
  - PrerequisitesStep 1: Create an Enterprise application in Azure AD
  - Step 1: Create an Enterprise application in Azure At
    Step 2: Configure the Token encryption
  - Step 2: Configure the Token energy
     Step 3: Manage Users and groups
  - Step 3: Manage Osers 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	Browse Azure AD Gallery			
E All services				☆ Got feedback?
	+ Create your own application 🕅 🕅 Got feedbac	k?		If you are developing your own application, using Application Proxy, or want to integrate an
Azure Active Directory	The Azure AD App Gallery is a catalog of thousands of a apps. Browse or create your own application here. If you	pps that make it easy to deploy and configure single sign-on (SS are wanting to publish an application you have developed into	50) and automated user provisioning. When deploying an app from the the Azure AD Gallery for other organizations to discover and use, you (	application that is not in the gallery, you can create your own application here.
Enterprise applications				What's the name of your app?
Enterprise appreciations	Jo Search application	Single Sign-on : All User Account Management : All	Categories : All	Input name
	Cloud platforms			What are you looking to do with your application?
	Amazon Web Services (AWS)	Google Cloud Platform	Oracle	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)
	aws	Google Cloud	6	
• Enter Fi	leSender as your AppName ir	the field, then click Add		
Wait white	ile Azure AD is adding the app	lication		
	<ul> <li>Adding application</li> </ul>		Running	×
Ad	lding application FileSe	nder.		
			a few seconds ag	0

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



Adding application

Application FileSender added successfully

a few seconds ago

 $\times$ 

## Step 2: Configure the Token encryption

• Retrieve/Donwload now the Belnet Filsender certificate used for metadatas:

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

All services > Enterprise application	ns   All applications FileSen	der				
FileSender   Toke	en encryption					×
<ul> <li>Coverview</li> <li>Deployment Plan</li> <li>Diagnose and solve problems</li> <li>Maage</li> <li>Properties</li> <li>Roles and administrators</li> <li>Users and groups</li> <li>Single sign-on</li> <li>Provisioning</li> <li>Application proxy</li> <li>Sett-service</li> <li>Custom security attributes (prevey)</li> <li>Security</li> <li>Conditional Access</li> <li>Permissions</li> <li>Token encryption</li> <li>Activity</li> <li>Sin-in hops</li> </ul>	Control Certificate Upload a certificate Upload a certificate Can Status	R       Got feedback?         e	Start Date	Expiration Date	Inumpprint	
	All services > Enterprise applicatio FileSender   Toke Enterprise Applicatio FileSender   Toke Enterprise Applicatio Logicoverview Deployment Plan Control Properties Owners Single sign-on Provisioning Single sign-on Provisioning Single sign-on Provisioning Control Security Conditional Access Conditional Access Conditional Access Conditional Access Conditional Access Termissions Termissions Termissions Termissions Sign-in logs Sign-in logs	<ul> <li>All services &gt; Enterprise applications (All applications)</li> <li>FileSender   Token encryption</li> <li>Enterprise Application</li> <li>Deployment Plan</li> <li>Dagnose and solve problems</li> <li>Manage</li> <li>Properties</li> <li>Solvenses</li> <li>Solvenses</li> <li>Solvenses and administrators</li> <li>Users and groups</li> <li>Single sign-on</li> <li>Provisioning</li> <li>Application proxy</li> <li>Set-service</li> <li>Conditional Access</li> <li>Permissions</li> <li>Tempsion</li> <li>Activity</li> <li>Single ingn</li> </ul>	<ul> <li>All services &gt; Enterprise applications   All applications : FuldSender</li> <li>FileSender   Token encryption</li> <li>FileSender   Token encryption</li> <li>FileSender   Token encryption</li> <li>Porevise</li> <li>Deployment Plan</li> <li>Desland administrators</li> <li>Users and groups</li> <li>Single sign-on</li> <li>Provisioning</li> <li>Application proxy</li> <li>Set-service</li> <li>Conditional Access</li> <li>Permissions</li> <li>Termissions</li> <li>Activity</li> <li>Sign-in logs</li> </ul>	<ul> <li>All services &gt; Enterprise applications   All applications ? EleiSender</li> <li>FileSender_Token encryption</li> <li>Enterprise Application</li> <li>Deployment Plan</li> <li>Dopose and solve problems</li> <li>Manage</li> <li>Manage</li> <li>Properties</li> <li>Owners</li> <li>Add</li> <li>Cancel</li> <li>Samuel Status</li> <li>Key tor</li> <li>Start Uate</li> </ul>	All services > Enterprise applications   All applications ? FeldSender	All services > Enterprise applications   All applications : Enterprise Applications : Enterprise Application : Enterpr

• Wait for the successful import of the certificate

Token Encryption (Preview)

Successful import of your token encryption certificate

×

• Click on the 3 dots button and click on Activate token encryption

fL token encryption enat ccepted, and personal or tatus nactive	les the use of encrypted SAML assertion corporate data compromised. Learn mot	with an application that supports it. Encrypting the SA e. Start Date 6/29/2022, 3:04:18 PM	ML assertions between Azure AD and the applic Expiration Date 6/28/2032, 3:04:18 PM	ation provides additional assurance that the content of the toke Thumbprint
itatus nactive	Key Id	Start Date 6/29/2022, 3:04:18 PM	Expiration Date 6/28/2032, 3:04:18 PM	Thumbprint
nactive		6/29/2022, 3:04:18 PM	6/28/2032, 3:04:18 PM	The sector is a first sector of
ick on <b>Yes</b>				Activate token en certificate Delete token en certificate Delete token en certificate Delete token en certificate
You are about	to activate token encryptic	n for your application. Please ensure	that your certificate has been s	uccessfully onboarded on your application
rify the succes	sful activation of the tok	en encryption certificate		
Succes	oken Encryption (F	' <b>review)</b> ur token encryption certif	icate	×
	,	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	a few seconds ag	go
↑ Import Certificate	R Got feedback?			
	enabled			
O Token encryption is				
Token encryption is AL token encryption enab rcepted, and personal or	es the use of encrypted SAML assertions corporate data compromised. Learn more	with an application that supports it. Encrypting the SAN	IL assertions between Azure AD and the applicat	tion provides additional assurance that the content of the token

## 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 FileSend
er Under Manage (Left Pane) Users and groups, click on Add user

MICrosoft Azure		> Search resources, services, and docs (G+7)		STANDA
«	Home > Standaardmap > Enterprise ap	oplications - All applications > FileSender - Users and groups		
+ Create a resource	FileSender - Users and g	jroups		
🛧 Home	«	+ Add user		
💻 Dashboard	📕 Overview			
∃ All services	🥳 Getting started	Ine application will appear on the Access Panel for assigned users. Set Visible to users? to no in properties to pre- ter application will appear on the Access Panel for assigned users. Set Visible to users?	event this. 🤿	
<b>†</b> FAVORITES	Deployment Plan	First 100 shown, to search all users & groups, enter a display name.		
All resources	✗ Diagnose and solve problems	DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
📦 Resource groups	Manage	No application assignments found		
🔇 App Services	Properties			
🗟 SQL databases	🗳 Owners			
💓 Azure Cosmos DB	x <sup>A</sup> Users and groups			
Virtual machines	Single sign-on			
💠 Load balancers	Provisioning			
Storage accounts	Application proxy			
Virtual networks	<ul> <li>Self-service</li> </ul>			
Azure Active Directory	Security			
Monitor	Conditional Access			
🗣 Advisor	2 Dermissions			
Security Center	Tolog acception (Descious)			
Ost Management + Billing	<ul> <li>Token encrypaon (Preview)</li> </ul>			
Page Help + support	Activity			

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

Users and groups None Selected	>
Select Role	

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 X

Search by no	ame or email address	~
BE	beta	
	filesender	

Selected	members:	
FI	filesender	Remove

#### Click on Assign

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

 Add Assignment

Users and groups 1 group selected.	>
Select Role	>

	DISPLAY NAMÉ	OBJECT TYPE	ROLE ASSIGNED
First 100 shown, to search all users & groups, enter a display nam	1e.		
The application will appear on the Access Panel for assigned	users. Set 'visible to users?' to no in properties to	prevent this. 🔿	
- Add user 💉 Edit   Remove 🔎 Update Crede	ntials Columns		
		a few seconds ago	
0 users & 1 group have beer	assigned access		
• · · · •			
Application assignmen	t succeeded	×	
ip filesender has been assigned acco	ess (as <b>user</b> ) to the <b>FileSend</b>	ler 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 S
 AML

Microsoft Azure		₽ Search resource	es, services, and docs (G+/)	図 40 0 0 00
Create a resource	Home > Standaardmap > Enterprise app FileSender - Single sign- Enterprise Application	plications - All applications > FileSender - Single sign-on on		
Home     Dashboard     E All services	« Overview	Select a single sign-on method	elp me decide	
ravontrs     All resources     All resource groups     App Services     Soll databases	Getting started      Deployment Plan      Diagnose and solve problems      Manage      Properties	Disabled User must manually enter their username and password.	Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol	Password-based Password storage and replay using a web browser extension or mobile app.
Ature Cosmos DB  Virtual machines  Load balancers  Storage accounts  Virtual networks	a Owners a Users and groups G Single sign-on Provisioning B Application proxy G Self-service	Linked Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.		
Acure Active Directory  Monitor  Advisor  Security Center  Co Cost Management + Billing Help + support	Security Conditional Access Conditional Access Permissions Coken encryption (Preview) Activity			

• 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

🕐 belnet-filesender-sp.xml

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

, or apread a pre comigure			,	
IL Configuration wi	ith the field	s <b>Identifier (E</b>	Entity ID) and F	Reply URL (Asse
	×			
Default				
✓ <b>⊘</b> a ā				
Default	nfiguratio	1		
Default	nfiguration	♥ Got feedba	ack?	
	AL Configuration w Default	IL Configuration with the field × Default ✓ ✓ ● ■	AL Configuration with the fields Identifier (E	AL Configuration with the fields Identifier (Entity ID) and F

Basic SAML Configuration	
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional
Reply URL (Assertion Consumer Service URL): https://fi Click on Save The system will ask you if you want to test Single sign-on w	lesender.belnet.be/simplesaml/module.php/saml/sp/saml2-acs.php/belnet-filesender-sp vith FileSender, click on <b>No, I'll test later</b> for now
↑ Upload metadata file Change single sign-on mode E Test th	iis application 🛛 🎔 Got feedback?
Test single sign-on with FileSender	
To ensure that single sign-on works for your application, we recommer	nd using the testing capability (in the last step) to test the changes you recently made. Would you like to test now?
Yes No, I'll test later	

Step 5: Configure User Attributes & Claims

•

•

↑ Upload metadata file	Change single sign-on mode	∃ Test this application	💙 Got feedback?
Set up Single Sign-	On with SAML		

Read the configuration guide 𝔄 for help integrating FileSender.

	Basic SAML Configuration	· · · · · · · · · · · · · · · · · · ·	·
		https://filesender.helnet.he	
	Reply URL (Assertion Consumer Service URL)	https://filesender.belnet.be/simplesaml/module.php/sa	
		ml/sp/saml2-acs.php/belnet-filesender-sp	
	Sign on URL	Optional	
	Relay State	Optional	
	Logout Url	Optional	
2	User Attributes & Claims		D
	Givenname	user.givenname	
	Surname	user.surname	
	Emailaddress	user.mail	
	Name	user.userprincipalname	
	Unique User Identifier	user.userprincipalname	
dify the	Additional claims from     Senterprise applications - All applications > FileSe	ender - Single sign-on > SAML-based Sign-on > User Attributes & Claims	
User A	ttributes & Claims	and angle sign on a same based sign on a loss radiotics of claims	
🕂 Add n	ew claim 🕂 Add a group claim 📰 Columns		
Require	d claim		
CLAIM N/	AME	VALUE	
Unique	User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress]	
<b>Unique</b> Addition	User Identifier (Name ID) nal claims	user.userprincipalname [nameid-format:emailAddress]	
Unique Addition	User Identifier (Name ID) nal claims ME	user.userprincipalname [nameid-format:emailAddress]	
Unique Addition claim Na http://sc	User Identifier (Name ID) nal claims MME chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.userprincipalname [nameid-format:emailAddress]	
Unique Additior claim na http://so	User Identifier (Name ID) nal claims ME chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.userprincipalname [nameid-format:emailAddress]	
Unique Additior cLAIM N/ http://sc http://sc	User Identifier (Name ID) nal claims AME chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.userprincipalname [nameid-format:emailAddress]	
Unique Additior cLAIM N/ http://sc http://sc	User Identifier (Name ID) al claims ane chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname [nameid-format:emailAddress]	
Unique Additior cLAIM N/ http://sc http://sc	User Identifier (Name ID) al claims chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/name chemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname [nameid-format:emailAddress]	
Unique Additior cLAIM N/ http://sc http://sc	User Identifier (Name ID) al claims we chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/name chemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.userprincipalname [nameid-format:emailAddress]  vALUE  user.mail  user.givenname  user.surname  user.surname	
Unique Additior cLAIM N/ http://sc http://sc http://sc	User Identifier (Name ID) al claims chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/name chemas.xmlsoap.org/ws/2005/05/identity/claims/surname ributes & Claims	user.userprincipalname [nameid-format:emailAddress]	
Unique Addition cLAIM N/ http://so http://so http://so ser Att	User Identifier (Name ID)  al claims  AME  chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/name chemas.xmlsoap.org/ws/2005/05/identity/claims/name chemas.xmlsoap.org/ws/2005/05/identity/claims/surname  ributes & Claims  v claim + Add a group claim EE Columns	user.userprincipalname [nameid-format:emailAddress]	
Unique Additior cLAIM N/ http://sc http://sc http://sc ser Att	User Identifier (Name ID)  al claims  AME  chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/name chemas.xmlsoap.org/ws/2005/05/identity/claims/surname  ributes & Claims  v claim + Add a group claim == Columns	user.userprincipalname [nameid-format:emailAddress]	
Unique Additior cLAIM N/ http://sc http://sc http://sc ser Att	User Identifier (Name ID)  al claims  MME  chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/surname chemas.xmlsoap.org/ws/2005/05/identity/claims/surna	user.userprincipalname [nameid-format:emailAddress]	
Unique Additior cLAIM N/ http://sc http://sc http://sc ser Att	User Identifier (Name ID)  al claims  AME  chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/name chemas.xmlsoap.org/ws/2005/05/identity/claims/name chemas.xmlsoap.org/ws/2005/05/identity/claims/surname  ributes & Claims  v claim  Add a group claim  Claim	user.userprincipalname [nameid-format:emailAddress]         vALUE         user.mail         user.givenname         user.surname	
Unique Additior cLAIM N/ http://sc http://sc http://sc ser Att Add new equired o cLAIM NAM	User Identifier (Name ID)  All claims  Ame  Chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress  Chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname  Chemas.xmlsoap.org/ws/2005/05/identity/claims/surname  ributes & Claims  v claim  Add a group claim	user.userprincipalname [nameid-format:emailAddress]         vALUE         user.mail         user.givenname         user.surname         value         user.surname         user.userprincipalname         user.surname	
Unique Additior cLAIM N/ http://sc http://sc http://sc http://sc ser Att Add new equired o cLAIM NAM Jnique Us	User Identifier (Name ID)  al claims  AME  chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/surname c	user.userprincipalname [nameid-format:emailAddress]         vALUE         user.givenname         user.userprincipalname         user.surname         vALUE         vALUE	
Unique Additior cLAIM N/ http://sc http://sc http://sc http://sc Seer Att Add new equired of cLAIM NAM	User Identifier (Name ID)  al claims  AME  chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/name chemas.xmlsoap.org/ws/2005/05/identity/claims/name chemas.xmlsoap.org/ws/2005/05/identity/claims/surname chem	user.userprincipalname [nameid-format:emailAddress]         vALUE         user.givenname         user.surname         value         vALUE         vALUE         vALUE         vALUE	
Unique Additior cLAIM NJ http://sc http://sc http://sc http://sc ser Att Add new equired o cLAIM NAM Jnique Us dditional cLAIM NAM	User Identifier (Name ID)  al claims  MME  chemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/surname chemas.xmlsoap.org/ws/2005/05/identity/claims/surna	user.userprincipalname [nameid-format:emailAddress]         vALUE         user.givenname         user.surname         value	
Unique Additior cLAIM NJ http://sc http://sc http://sc http://sc timescale.com/ claim NAM Unique Us dditional cLAIM NAM	User Identifier (Name ID)  al claims  ME  chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/surname c	user.userprincipalname [nameid-format:emailAddress]         vALUE         user.givenname         user.userprincipalname         user.surname         value         value     <	
Unique Additior cLAIM NJ http://sc http://sc http://sc http://sc timescales/sc http://	User Identifier (Name ID)  al claims  AME  chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/givenname chemas.xmlsoap.org/ws/2005/05/identity/claims/surname c	user.userprincipalname [nameid-format:emailAddress]         vALUE         user.givenname         user.userprincipalname         user.surname         value         value         value         value         user.userprincipalname	

## Step 6: Verify SAML Signing Certificate

Verify that the SAML Signing Certificate is Active

SAML Certificates		
Token signing certificate		<i>Л</i> .
Status	Active	6 E
Thumbprint		
Expiration	5/22/2027, 10:02:49 PM	
Notification Email		
App Federation Metadata Url		
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

- ation.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).