

FedSender - setup guide for Entra ID application as IdP (External)

- [Description](#)
- [Contact Belnet Administrative support](#)
- [Microsoft Entra ID as Identity Provider \(IdP\) & Belnet FedSender as Service Provider \(SP\).](#)
 - [Prerequisites](#)
 - [Step 1: Create an Enterprise application in Entra ID](#)
 - [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: SAML Signing Certificate \(Optional - only if you created a dedicated certificate for all your Entra ID Enterprise applications\)](#)
 - [Step 7: Send/Provide your App Federation Metadata URL to Belnet](#)
 - [Step 8: Test Single sign-on with Belnet FedSender](#)

Description

In this document, we will give an example of how to configure a Microsoft Entra ID application as IdP (Identity Provider) for Single Sign On management on Belnet Fedsender (acting as Service Provider).

This documentation is published on the Belnet website, section Fedsender FAQ, to help Belnet customers configure/set up their Identity Provider using Microsoft Entra ID infrastructure.

Contact Belnet Administrative support

Belnet FedSender is a paid service.

Please contact Belnet [administrative support](#) before continuing with this documentation in order to subscribe to this service.

Microsoft Entra ID as Identity Provider (IdP) & Belnet FedSender as Service Provider (SP).

Prerequisites

- Microsoft Entra ID (AD) must be created with at least one (non-admin) user.
- You must be able to configure your Microsoft Entra ID tenant to add new Enterprise Applications.
- [Your Microsoft Entra ID must have access to **Token encryption** and **Single sign-on** functionalities which are part of Entra ID \(premium\) P1 or P2 subscription.](#)
- Your Entra ID IdP application, Belnet's FedSender Service Provider (simpleSAMLPhP) and the FedSender webserver must have their respective domain and **SSL certificate generated** and correct.
- Both servers/service must be **reachable** from each other.

 For the time being, the Belnet Fedsender service is not linked to a Belnet Federation.

However, we were investigating the feasibility and necessity of integrating this service into a new Federation for our Public Organizations customers (Federal, Regional, Municipals).

Please take note of the important note below for your IdP setup using Microsoft Entra ID:

Note about Entra ID Enterprise Application(s) certificates

A note about Entra ID Application's certificates.

By default, Microsoft Entra ID creates a new certificate per application. This is not a good idea, as you must have the same certificate for all applications in the same federation.

So, unless you know for sure that you will never use several applications of the Belnet federation, we strongly advice you to not use the default certificate created by Entra ID but rather create a dedicated certificate for all the Entra ID Enterprise Applications that you'll create.

Such a certificate, with a validity of 10 years, can easily be created using openssl with the following commands (please update the "-subj" field to whatever best suit you eg: "/C=BE/ST=BRUSSEL/L=BRUSSEL/O=ACME/OU=ICT/CN=ENTRA_ID"):

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -sha256 -days 3650 -nodes -subj "/C=XX/ST=StateName/L=CityName/O=CompanyName/OU=CompanySectionName/CN=CommonNameOrHostname"
```

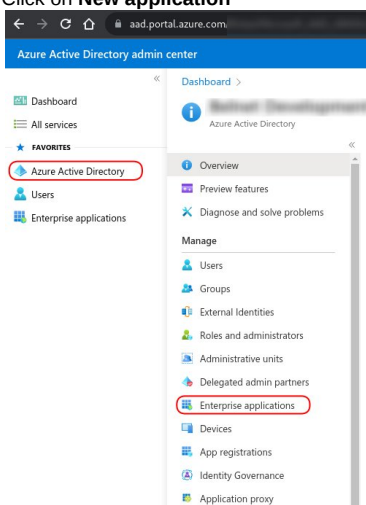
```
openssl pkcs12 -inkey key.pem -in cert.pem -export -out certificate.pfx
```

Note that you **MUST** use a passphrase for your .pfx file; an empty passphrase won't be accepted by Entra ID later.

Failure to do so means you'll have to modify your first application's certificate if ever you want to use a second service from the Belnet federation.

Step 1: Create an Enterprise application in Entra ID

- On Microsoft [Entra ID admin center](#) **Entra ID --> Enterprise apps**
- 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

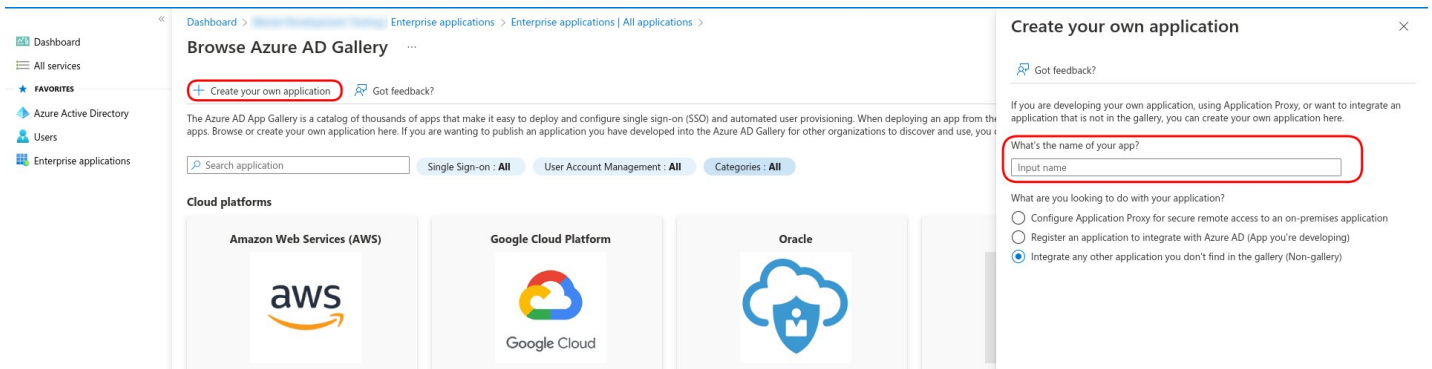
The list of applications that are maintained by your organization

Manage

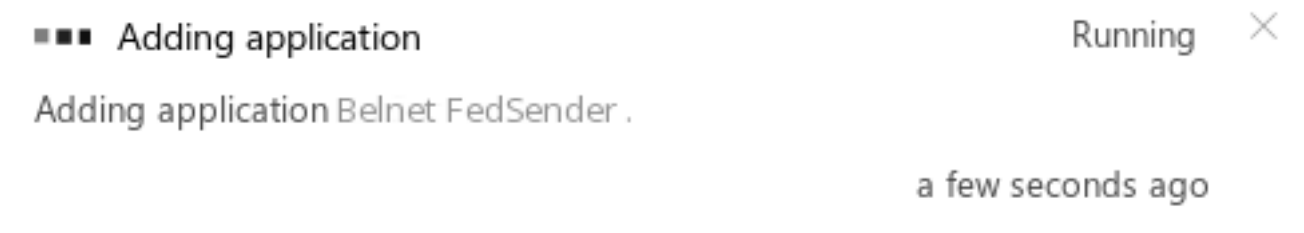


Search by application name or object ID

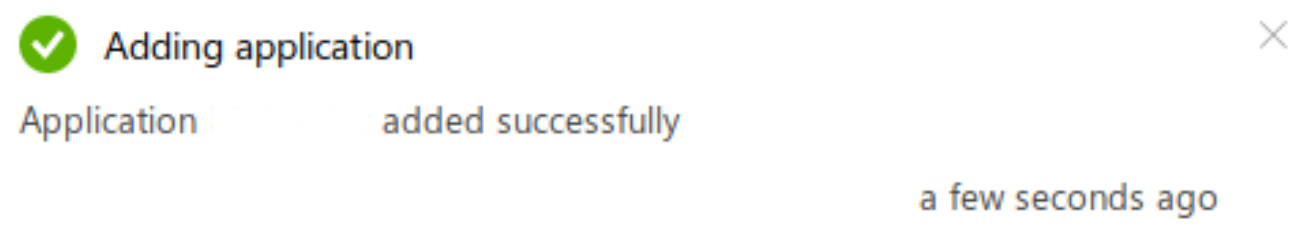
- Click on  **Create your own application**, enter **Belnet FedSender** in the **Name** field and click **Create**



- Enter **Belnet FedSender** as your AppName in the field, then click **Add**
- Wait while Entra ID is adding the application



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



Step 2: Configure the Token encryption

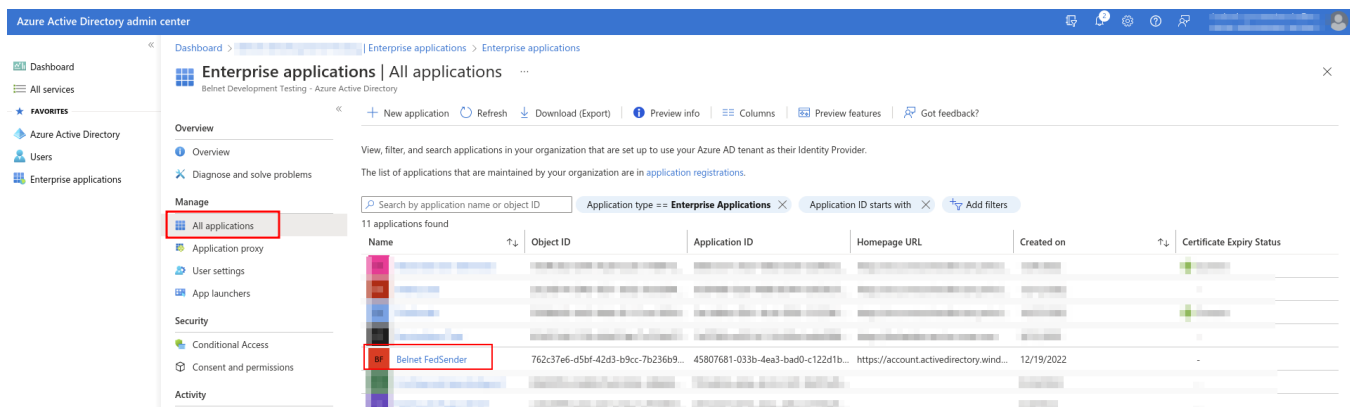
- Retrieve/Download now the Belnet Fedsender certificate used for metadatas:

This can be done in two different ways:

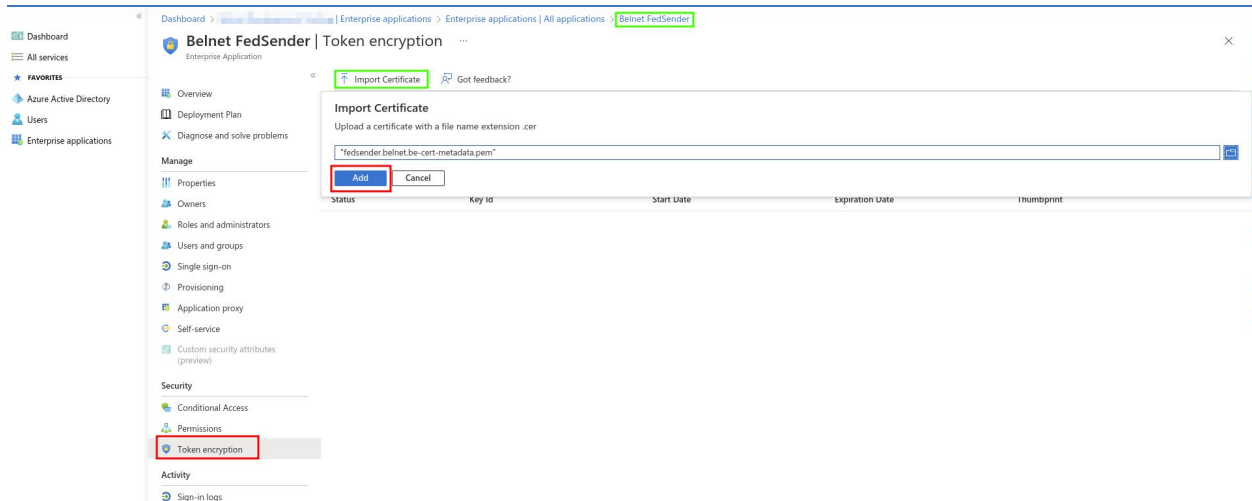
- by downloading the certificate itself on: <https://fedsender.belnet.be/fedsender.belnet.be-metadatas-ss.crt>
- or by consulting SAML Metadata on the Service Provider itself (FedSender SP) at url: <https://fedsender.belnet.be/simplesaml/module.php/saml/sp/metadata.php/belnet-gcloud-idp>

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

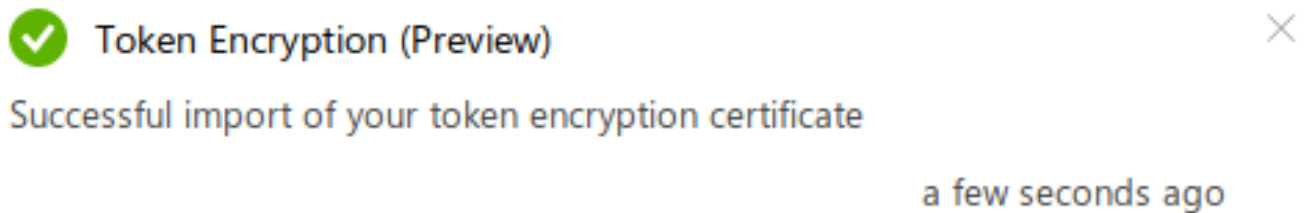
- On Microsoft [Entra ID admin center](#) **Entra ID --> Enterprise apps All Applications**
- **Select** your newly created application named **Belnet FedSender**



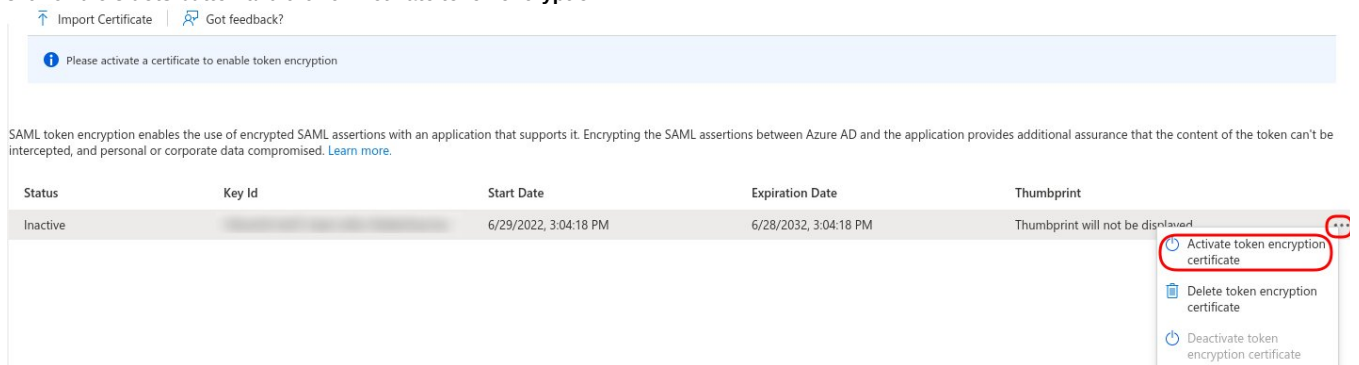
- Click on **Token encryption**, then click on **Import Certificate**
- Select the **certificate** fetched previously and click on **Add**



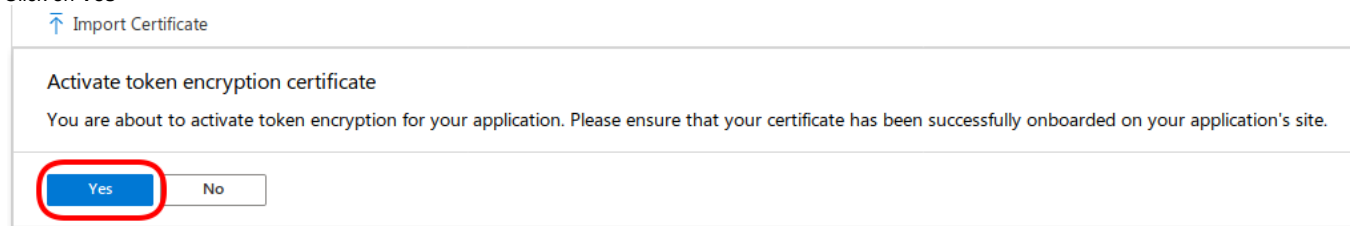
- Wait for the **successful** import of the certificate



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



- Click on **Yes**



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

Token Encryption (Preview)

Successful activation of your token encryption certificate

a few seconds ago

Import Certificate

Got feedback?

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

Monitor on your Tenant the expiration of the certificate!

To prevent or minimize outage due to a certificate expiring, use roles and email distribution lists to ensure that certificate-related change notifications are closely monitored.

Step 3: Manage Users and groups

- On Microsoft Entra ID admin center, go to **Entra ID Enterprise apps All applications Belnet FedSender** Under **Manage** (Left Pane) **Users and groups**, click on **Add user**

Dashboard

All services

Azure Active Directory

Users

Enterprise applications

FAVORITES

Azure Active Directory

Users

Enterprise applications

Belnet FedSender | Users and groups

+ Add user/group

Edit assignment

Remove

Update credentials

Columns

Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

First 200 shown, to search all users & gro...

Display Name	Object Type	Role assigned
No application assignments found		

- Click on **User and groups**

Home

Standardmap

Enterprise applications

All applications

FleSender

Users and groups

Add Assignment

Add Assignment

Dashboard

Users and groups

None Selected

Users

Assign

- For this example, we will select the group **fedsender** 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

beta

fedsender

Selected members:

fedsender

Remove

- Click on **Assign**

Home > Enterprise applications > All applications > fedsender > Users and groups > Add Assignment

Add Assignment

Users and groups

1 group selected

Users

User

- Group **fedsender** has been assigned access (as **user**) to the **Belnet FedSender** application

✓

Application assignment succeeded

0 users & 1 group have been assigned access

a few seconds ago

+ 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
fedsender	Group	User

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

- On Microsoft Entra ID admin center, go to **Entra ID Enterprise apps All applications Belnet FedSender Manage Single sign-on**, click on **SAML**

Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more](#).

Manage

- Overview
- Deployment Plan
- Diagnose and solve problems
- Single sign-on**
- Provisioning
- Application proxy
- Self-service
- Custom security attributes (preview)

Security

- Conditional Access
- Permissions
- Token encryption

Select a single sign-on method [Help me decide](#)

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
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.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

- Download the Belnet FedSender metadatas from <https://fedsender.belnet.be/simplesaml/module.php/saml/sp/metadata.php/belnet-gcloud-idp> as an **xml** file

- Click on **Upload metadata file**, select the **Belnet FedSender metadata xml file** and click on **Add**

Upload metadata file.

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

- 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

[Got feedback?](#)

Identifier (Entity ID) * ⓘ

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

[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://fedsender.belnet.be/simplesaml/module.php/saml/sp/saml2-accs.php/belnet...	☒ ⓘ Add

[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.

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.

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

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

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://fedsender.belnet.be>
Reply URL (Assertion Consumer Service URL): <https://fedsender.belnet.be/simplesaml/module.php/saml/sp/saml2-acss.php/belnet-gcloud-idp>
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

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?

Yes

No, I'll test later

Step 5: Configure User Attributes & Claims

- Click on the **edit button** of **User Attributes & Claims**
Belnet FedSender | 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 (preview)

Security

Conditional Access

Permissions

Token encryption

«

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

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 Belnet FedSender.

1

Basic SAML Configuration

Identifier (Entity ID)	https://fedsender.belnet.be
Reply URL (Assertion Consumer Service URL)	https://fedsender.belnet.be/simplesaml/module.php/saml/sp/saml2-acss.php/belnet-gcloud-idp
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	https://fedsender.belnet.be/simplesaml/module.php/saml/sp/saml2-logout.php/belnet-gcloud-idp

Edit

2

Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

Edit

- 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

Required claim	
CLAIM NAME	VALUE
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress] ...

Additional claims	
CLAIM NAME	VALUE
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

Required claim	
CLAIM NAME	VALUE
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress] ...

Additional claims	
CLAIM NAME	VALUE
cn	user.displayname ...
eduPersonPrincipalName	user.userprincipalname ...
mail	user.userprincipalname ...

- Please ensure that you used the **lower-case** spelling on claim names

Result:

2

Attributes & Claims

cn	user.displayname
eduPersonPrincipalName	user.userprincipalname
mail	user.userprincipalname
Unique User Identifier	user.userprincipalname

Step 6: SAML Signing Certificate (Optional - only if you created a dedicated certificate for all your Entra ID Enterprise applications)

You may decided to created a dedicated certificate for all your Entra ID Enterprise Applications. See the introduction note in the Prerequisites.

In this case, you now have to import it in your application.

 **You can skip this step if you didn't create a dedicated certificate for all your Entra ID Enterprise Apps** and this is the first Entra ID application you create, but you'll break things later when you create your second application (because you cannot skip this step for your second application).

- Click on "Edit" on the "SAML Certificates" tile of your application:

name

Unique User Identifier

user.userprincipalname

3

SAML Certificates

Token signing certificate

Status

Active

Thumbprint

F469A7C853E485CDE13AE476DA6BD2BE09CBA3B6

Expiration

8/28/2028, 10:02:40 PM

Notification Email

admin@test-belnet.be

App Federation Metadata Url

<https://login.microsoftonline.com/44b8a7f1-9432-...>

Certificate (Base64)

Download

Certificate (Raw)

Download

Federation Metadata XML

Download

Verification certificates (optional)

Required

No

Active

0

Expired

0

- In the "SAML Signing Certificate" pane on the right, click "Import Certificate":

PrincipalType/Application/fromNav/

admin@test-belnet.be

BELNET SERVICES TEST (OFFICE3...

SAML Signing Certificate

Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

Save

+ New Certificate

Import Certificate

Got feedback?

Status	Expiration Date	Thumbprint
Active	8/28/2028, 10:02:40 PM	F469A7C853E485CDE13AE476DA6BD2BE09CBA3B6

Signing Option

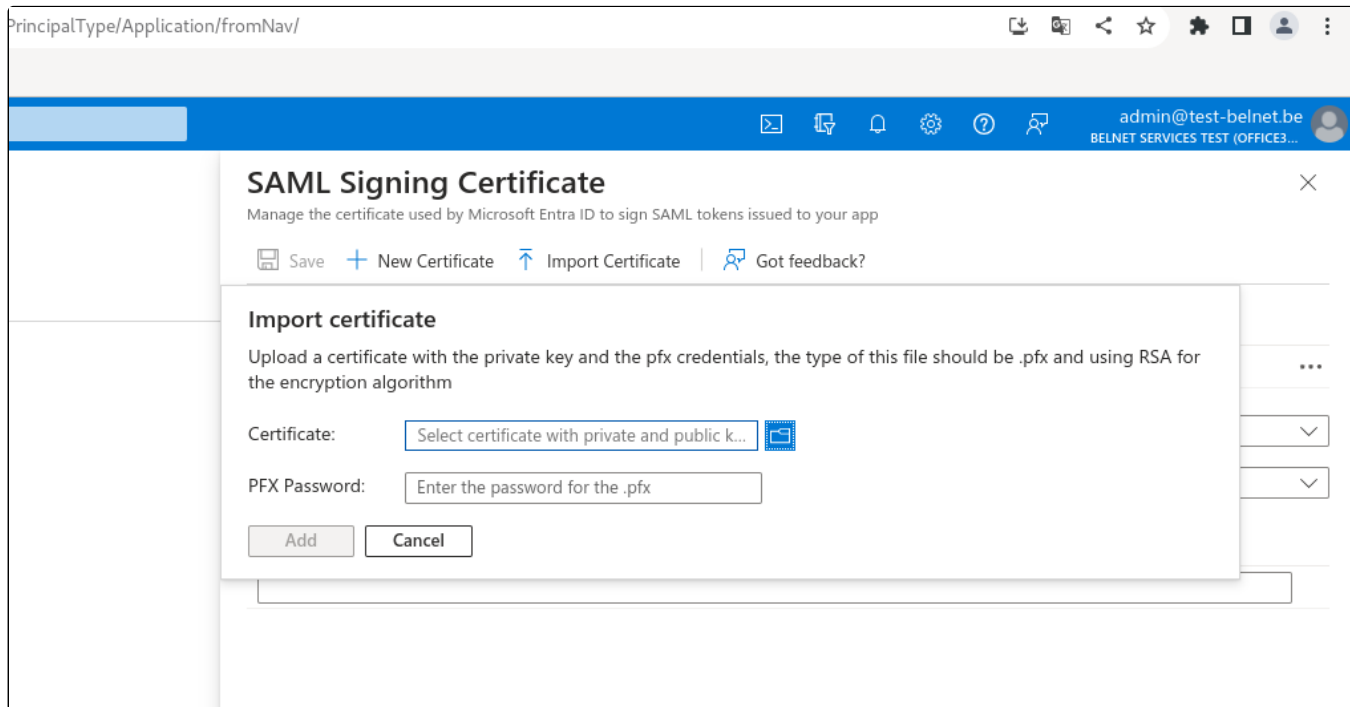
Sign SAML assertion

Signing Algorithm

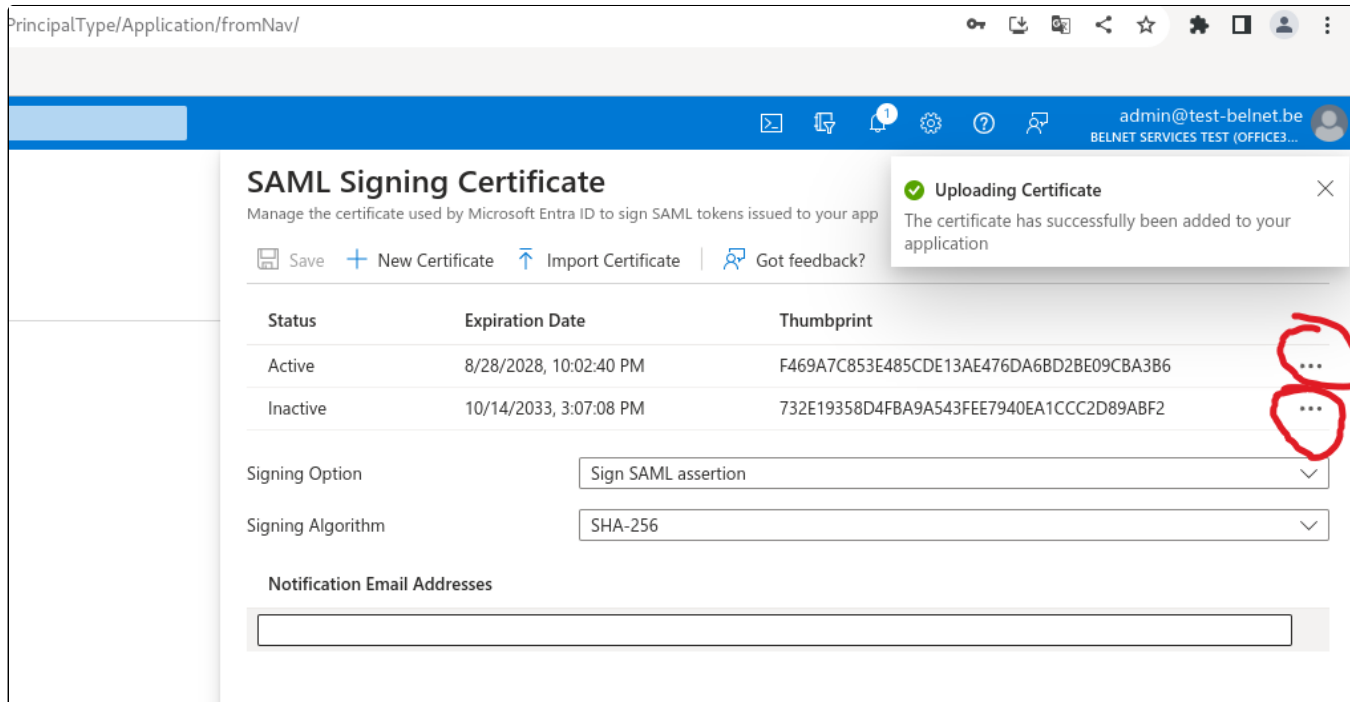
SHA-256

Notification Email Addresses

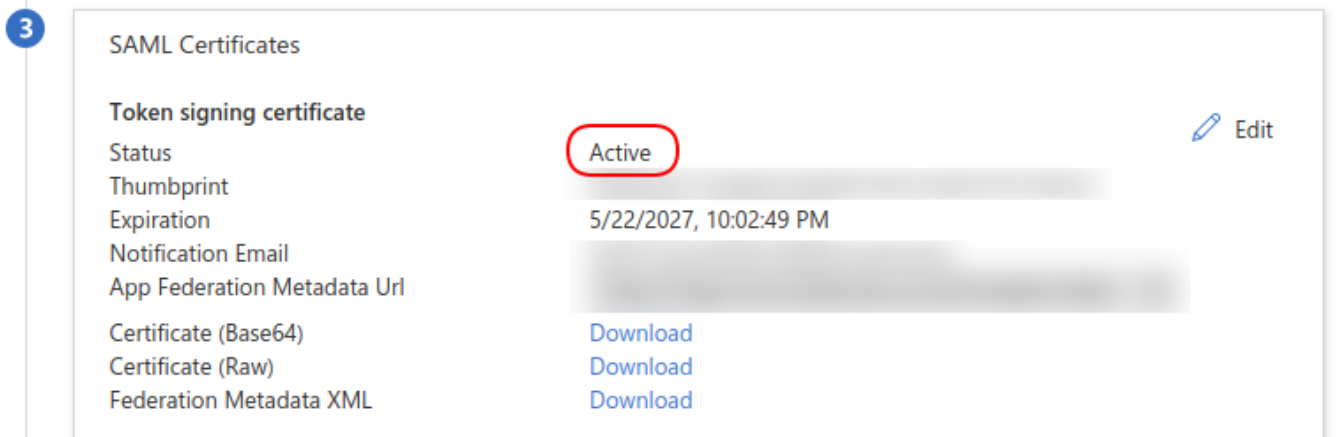
- Select the .pfx file you have created earlier, type its passphrase, and click on "Add":



- Your certificate is now uploaded. Now, activate it and deactivate the autogenerated one by using their 3-dots menu:



- Verify that the SAML Signing Certificate is Active



Step 7: Send/Provide your App Federation Metadata URL to Belnet

3

SAML Certificates

Token signing certificate

StatusActive

Thumbprint

Expiration10/2/2027, 8:06:49 PM

Notification Email

App Federation Metadata Urlhttps://login.microsoftonline.com/...

Certificate (Base64)Download

Certificate (Raw)Download

Federation Metadata XMLDownload

Edit

- Open a ticket by sending an email to [Belnet Administrative Support](#) providing these details:
 - Subject: **FedSender: Add Entra ID Enterprise Apps IdP for <your Organisation name>**
 - In the message body, mention:
 - Onboarding request to Belnet FedSender**
 - Technical Contact responsible for the IdP setup: **First name, Last name & email address**
 - Business service: **FED_APPS_87: FedSender**
 - Assignment group: **Order Delivery**
 - Paste your **App Federation Metadata Url** (see above capture, 3rd window in SAML config for your app).
- Wait for confirmation from your Account Manager and/or Belnet's technical team.

Step 8: Test Single sign-on with Belnet FedSender

Once Belnet has added your IdP to the Service Provider (FedSender) configuration files, your IdP will be listed when you connect to Belnet FedSender.

Your organisation's employees will have to choose your organisation's name in the IdP list on fedsender.belnet.be in order to be able to authenticate via your IdP.

Example of the Idp selection menu during the login phase:

Belnet

dedicated connectivity

g-cloud

English

If you were using FedSender before and your Organisation is not listed below, choose G-Cloud as authentication method.

You have previously chosen to authenticate at G-Cloud (All other users)

Login at G-Cloud (All other users)

IdP used during the previous login.

Miscellaneous

List of IdPs proposed for authentication

Incremental search...

Belnet Staff IdP with MFA

G-Cloud (All other users)



The choice of IdP in the discovery service is cached by the user's web browser.

If one of your user has selected the wrong IdP, clear the browser cache on the user's computer.

