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

Description

In this document, we give an example of how to configure a Microsoft Entra ID Enterprise Applications as IdP (Identity Provider) for Single Sign On management on the Belnet Filesender (acting as Service Provider).
Microsoft officially rebranded Azure Active Directory (Azure AD) to Microsoft Entra ID in late 2023.

It is published on the Filesender FAQ on the Belnet website to help Belnet customers configure/set up their heir Identity Provider using Microsoft Entra ID infrastructure.

Microsoft Entra ID as Identity Provider (IdP) & Belnet FileSender 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 Filesender Service Provider (simpleSAMLPhP) and the FileSender webserver must have their respective domain and **SSL certificate.**
- Both servers/service must be **reachable** from each other.

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"):

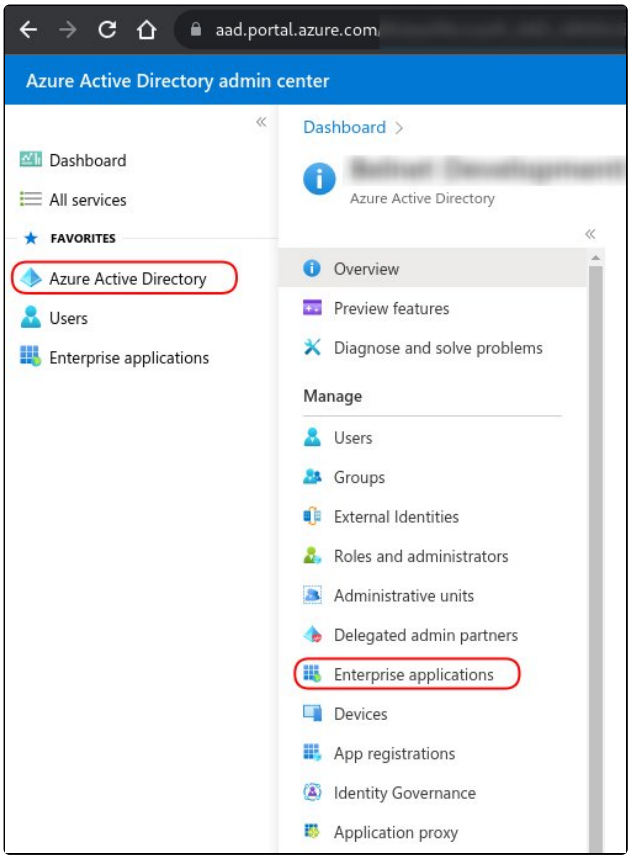
```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -sha256 -days 3650 -nodes -subj "/C=XX
/ST=StateName/L=CityName/O=CompanyName/OU=CompanySectionName/CN=CommonNameOrHostname"

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

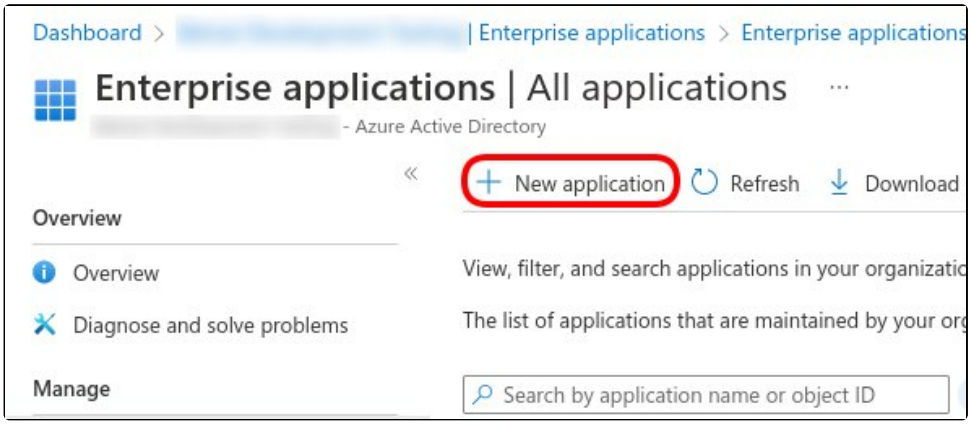
Note that you MUST use a passphrase for your .pfx file; an empty passphrase won't be accepted by Entra ID later.

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.

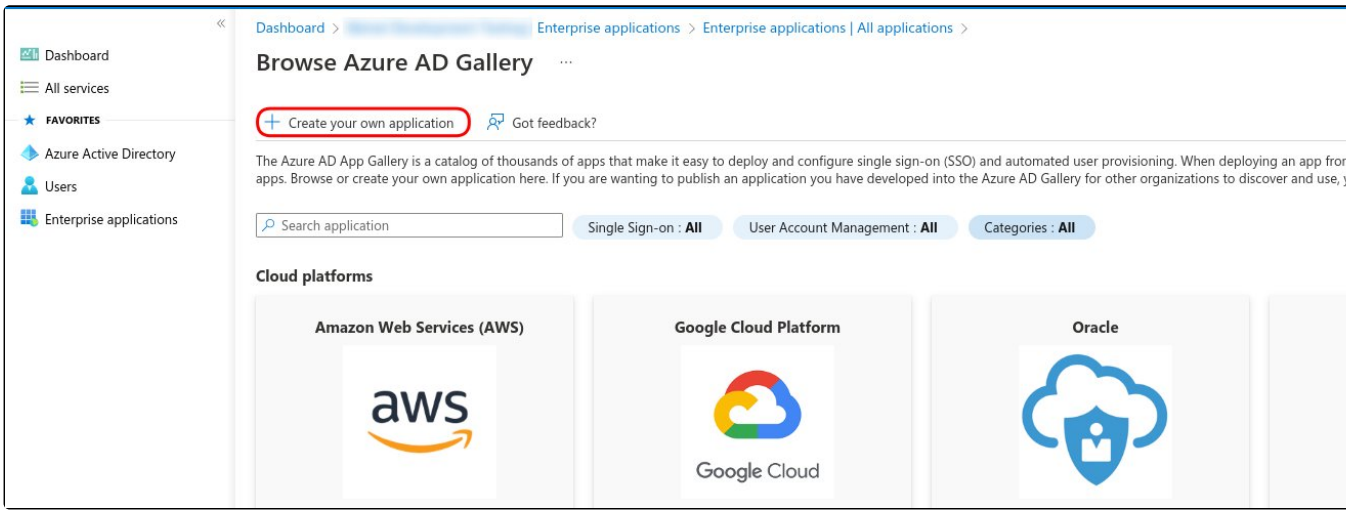
Step 1: Create an Enterprise application in Entra ID

- On Microsoft Entra ID admin center **Entra ID** --> **Enterprise apps**
- Click on **New application:**

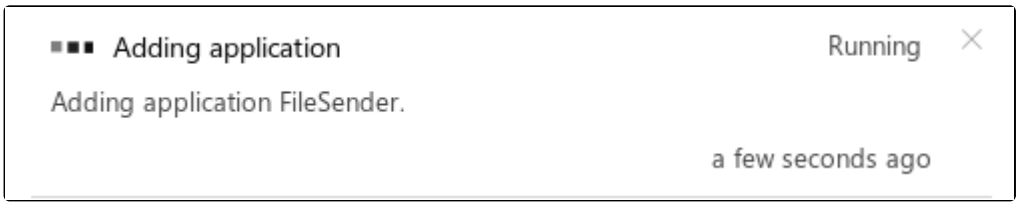




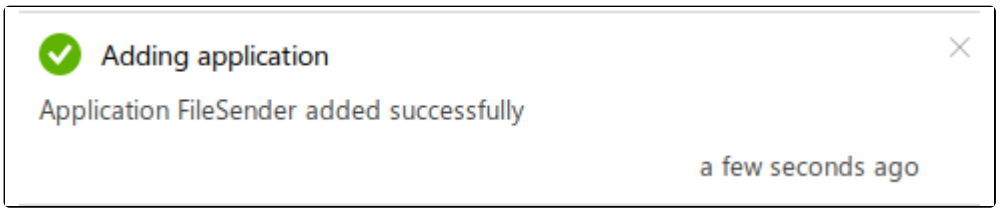
- Click on **Create your own application,** enter **FileSender** in the **Name** field and click **Create**



- Enter **FileSender** as your App**Name** 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

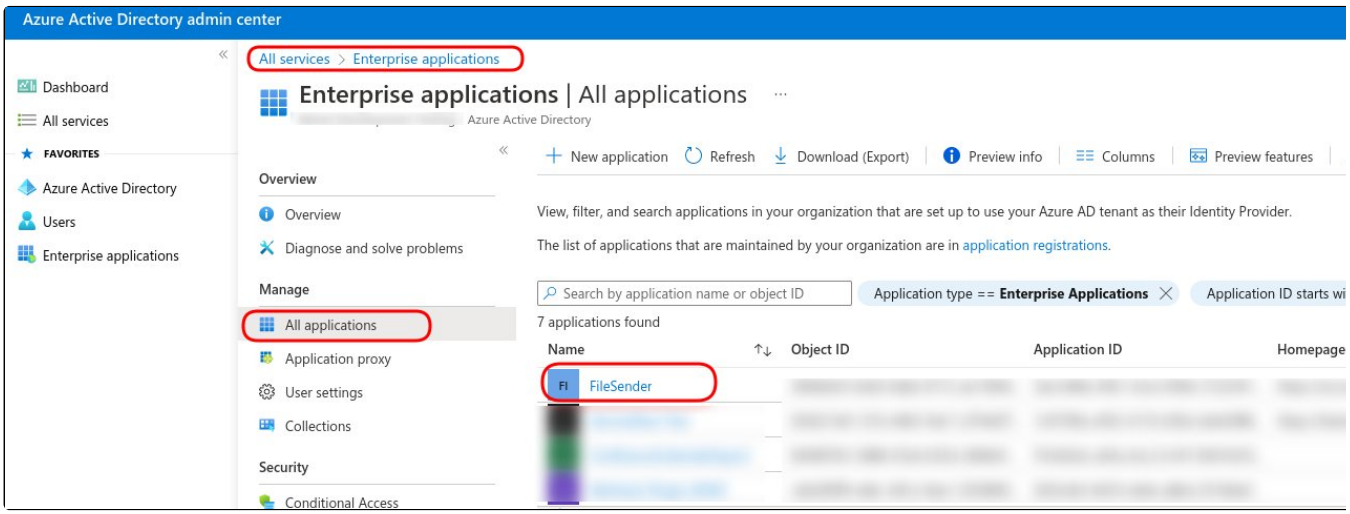
- Retrieve/Download the Belnet Filsender certificate used for metadatas:

  This can be done in two different ways:

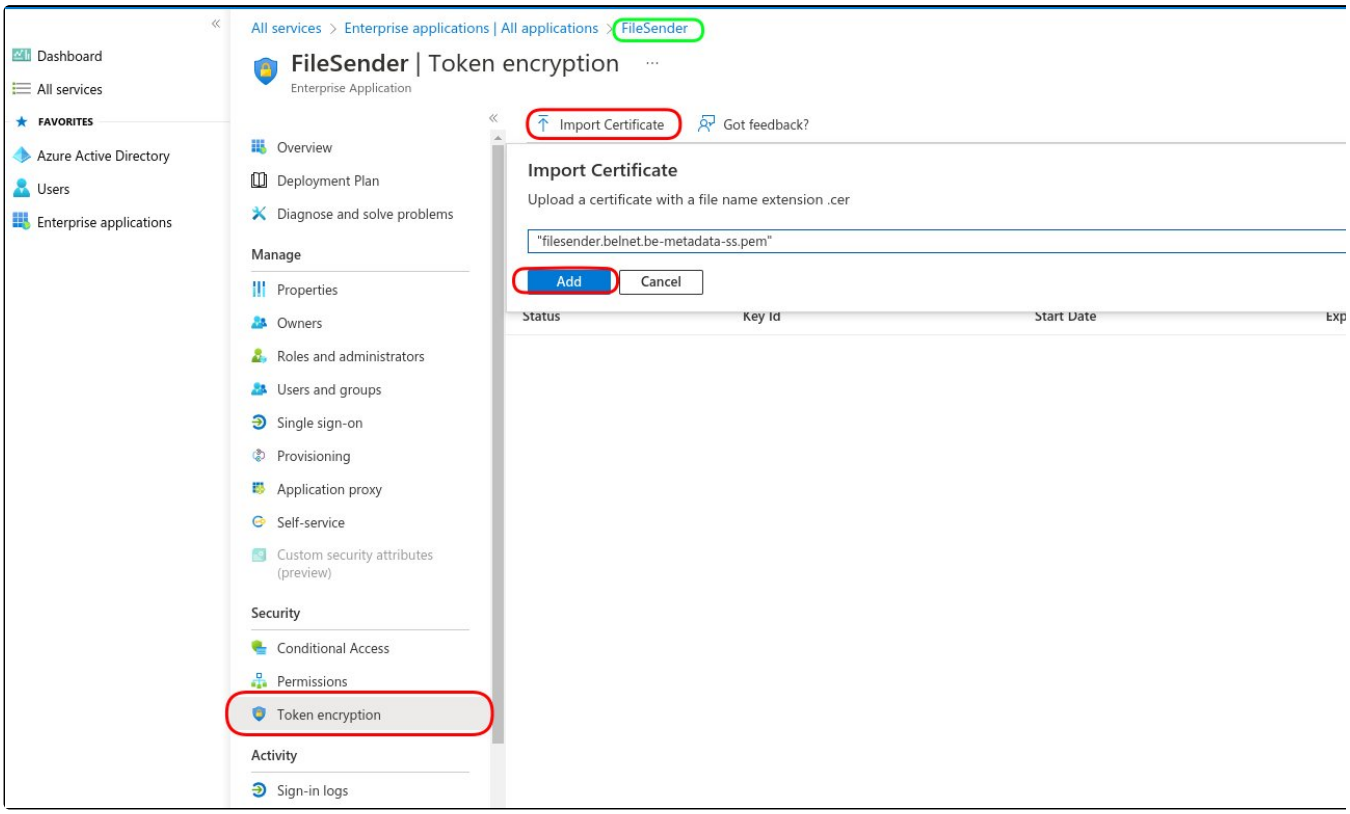
  - by downloading the certificate itself on: https://filesender.belnet.be/filesender.belnet.be-metadata-ss.pem
    or
  - by consulting SAML Metadata on the Service Provider itself (FileSender SP) at url: https://filesender.belnet.be/simplesaml/module.php/saml/sp/metadata.php/belnet-filesender-sp?output=xhtml&language=en

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

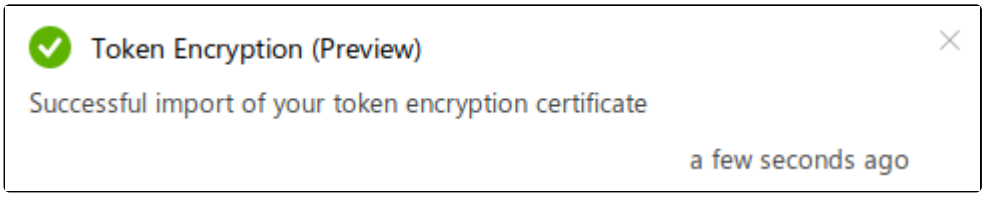
- On Microsoft Entra ID admin center **Entra ID** --> **Enterprise apps** **All Applications**
- **Select** your newly created application named **FileSender**



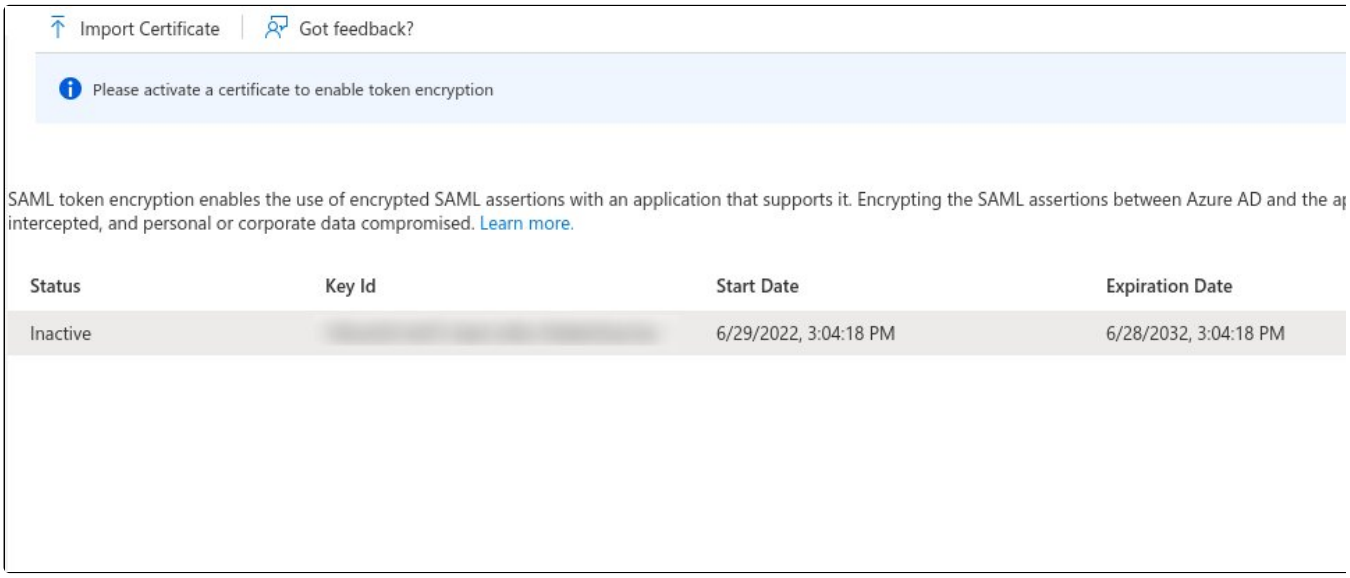
- Click on **Token encryption**, then click on **Import Certificate**
- Select the **certificate** fetched previously and click on **Add**



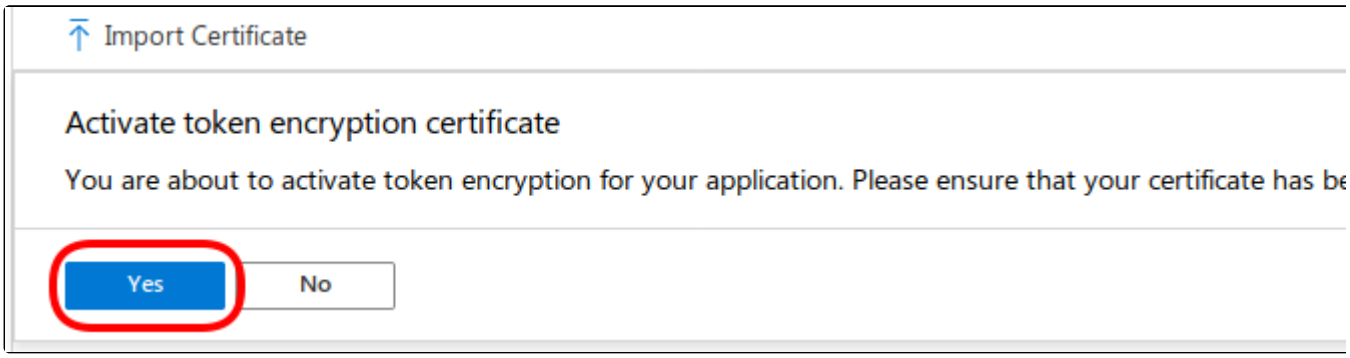
- Wait for the **successful** import of the certificate:



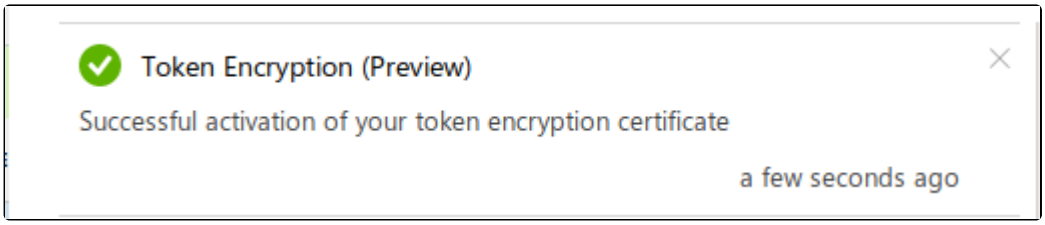
- Click on the **3 dots button** and click on **Activate token encryption:**

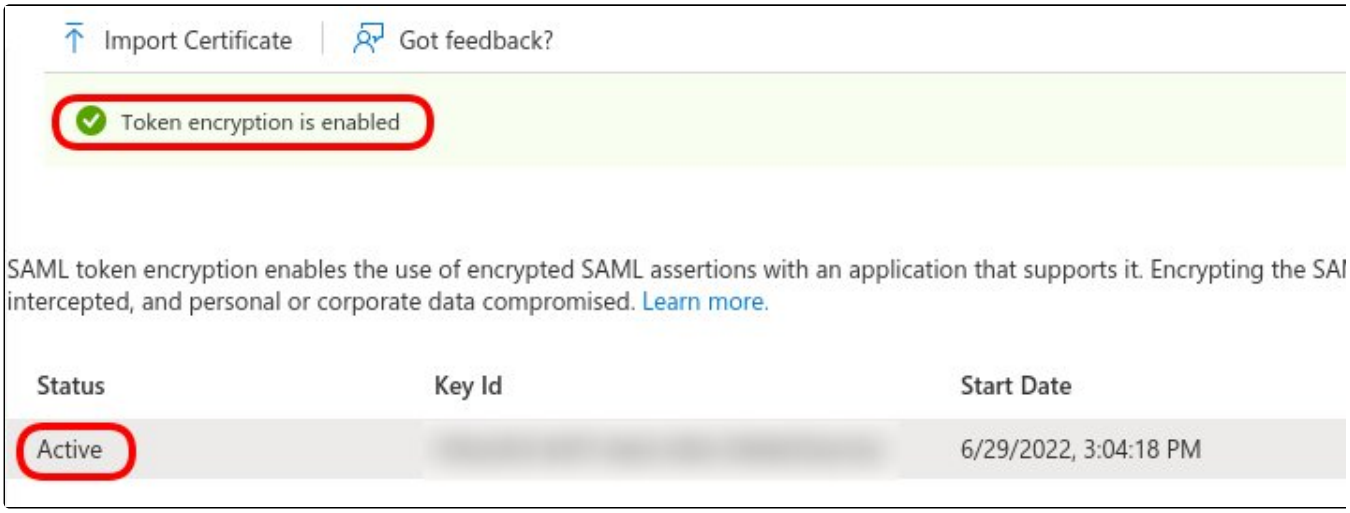


- Click on **Yes:**



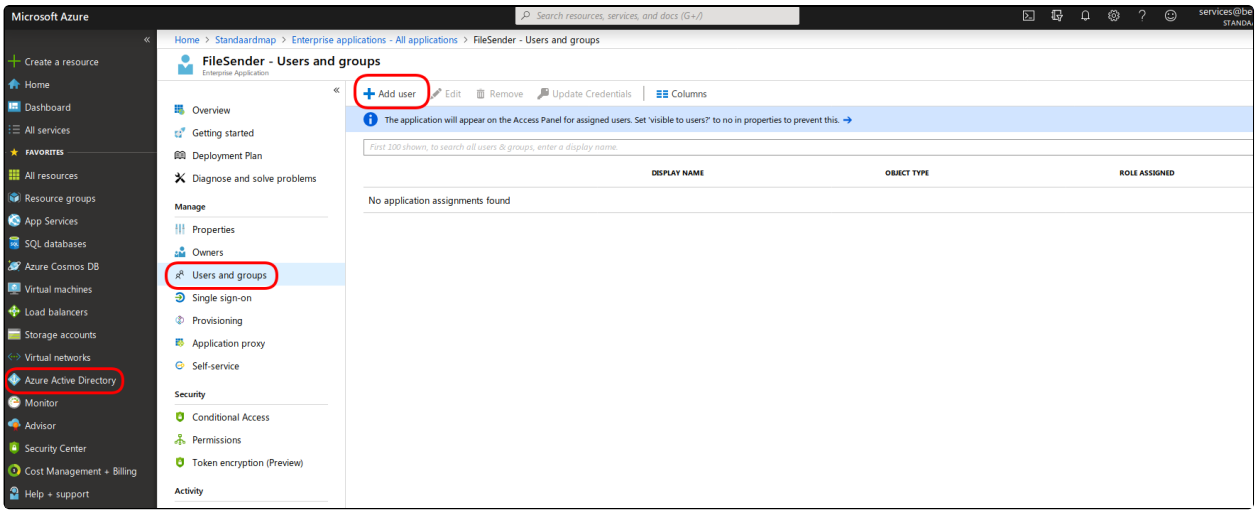
- Verify the **successful** activation of the token encryption certificate:



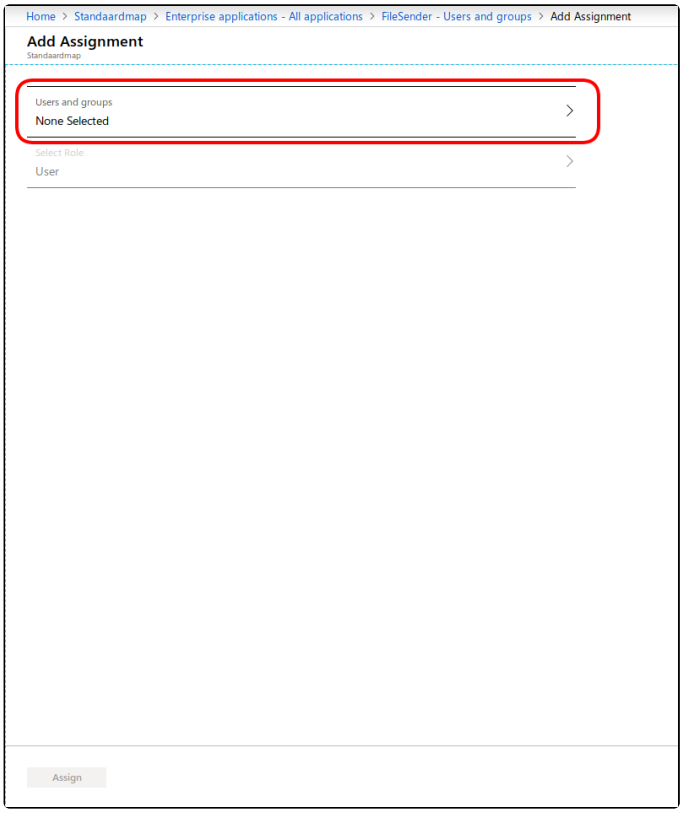


Step 3: Manage Users and groups

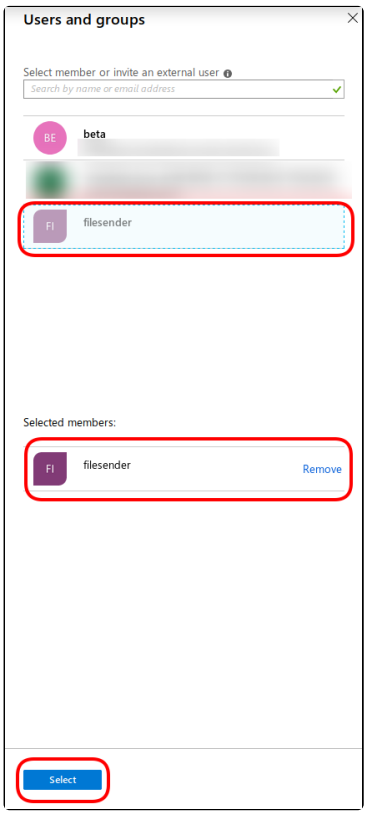
- On Microsoft Entra ID admin center, go to **Entra ID** **Enterprise apps** **All applications** **FileSender** Under **Manage** (Left Pane) **Users and groups**, click on **Add user:**



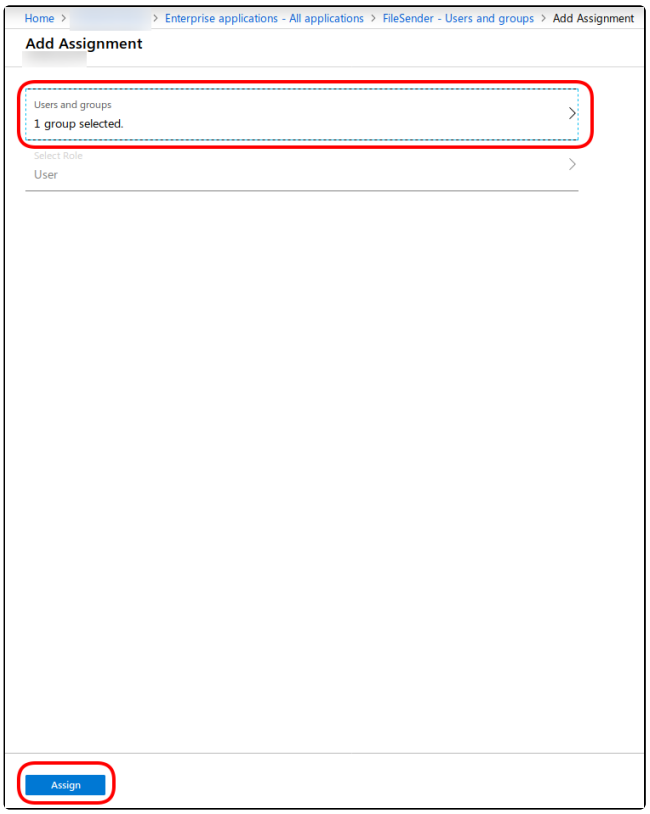
- Click on **User and groups:**



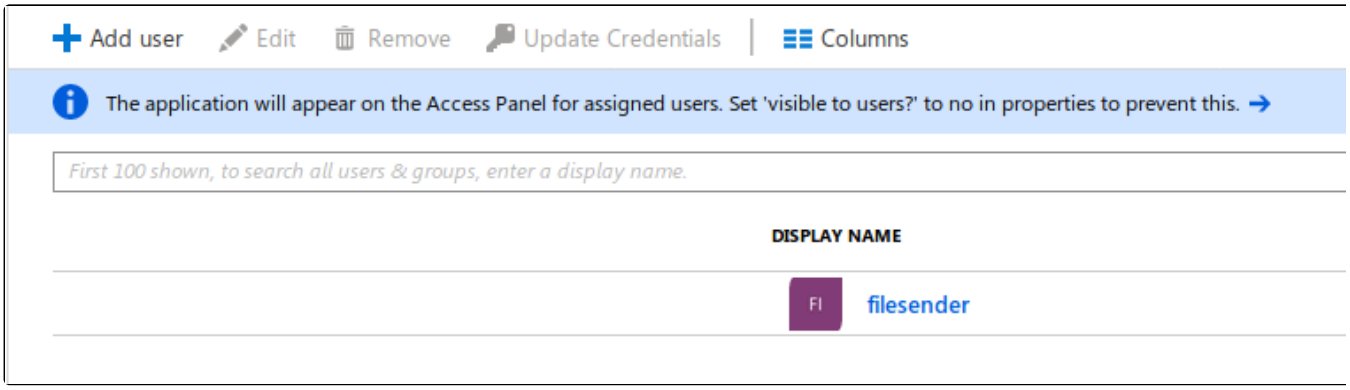
- For this example, we will select the group **filesender** with user **beta** as member of. **Please adapt as it fits to your organisation.** Click on **Select:**



- Click on Assign:

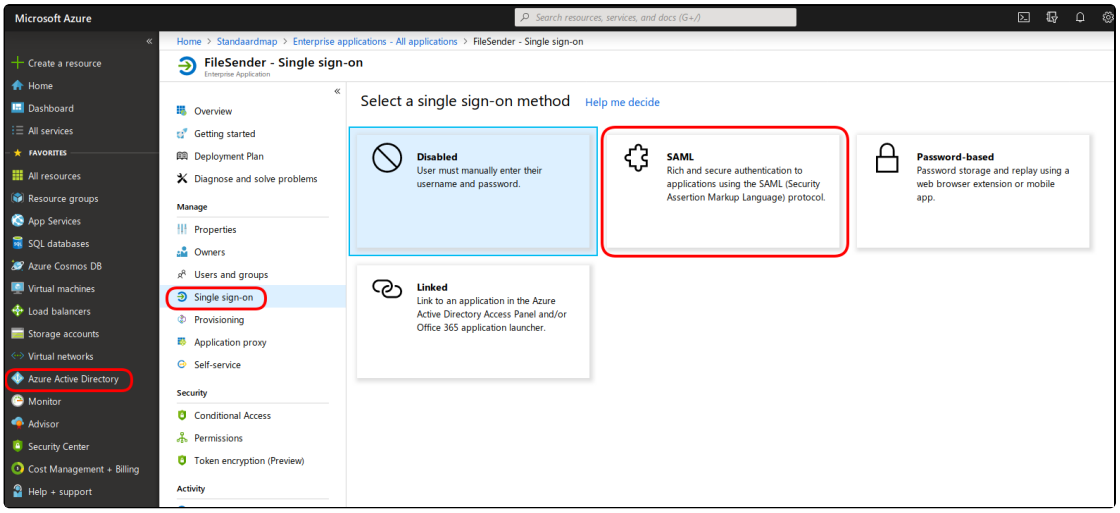


- Group **filesender** has been assigned access (as **user**) to the **FileSender** application:



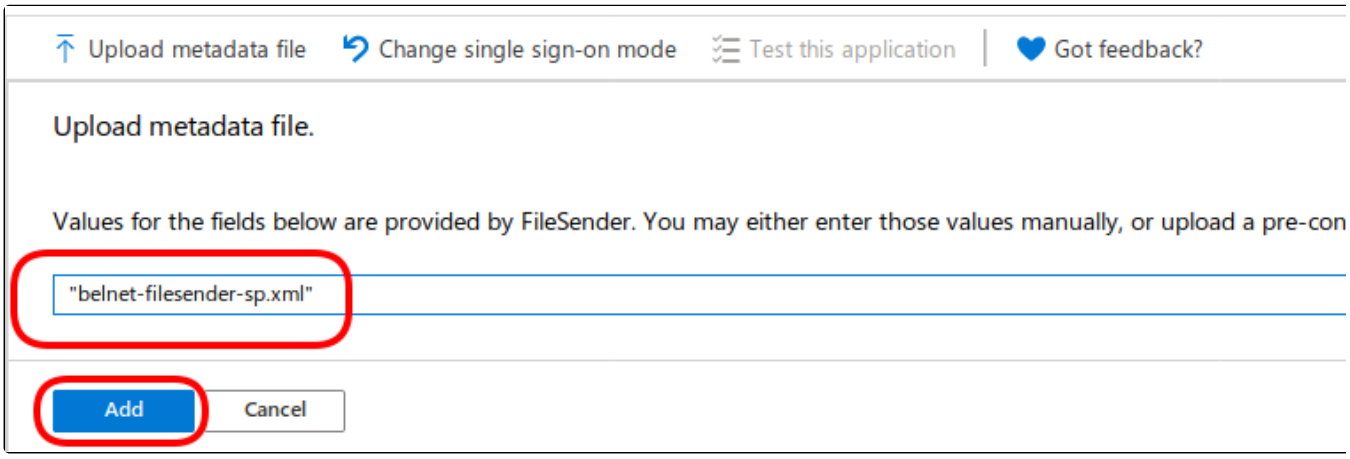
Step 4: Configure the Single sign-on (SAML)

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



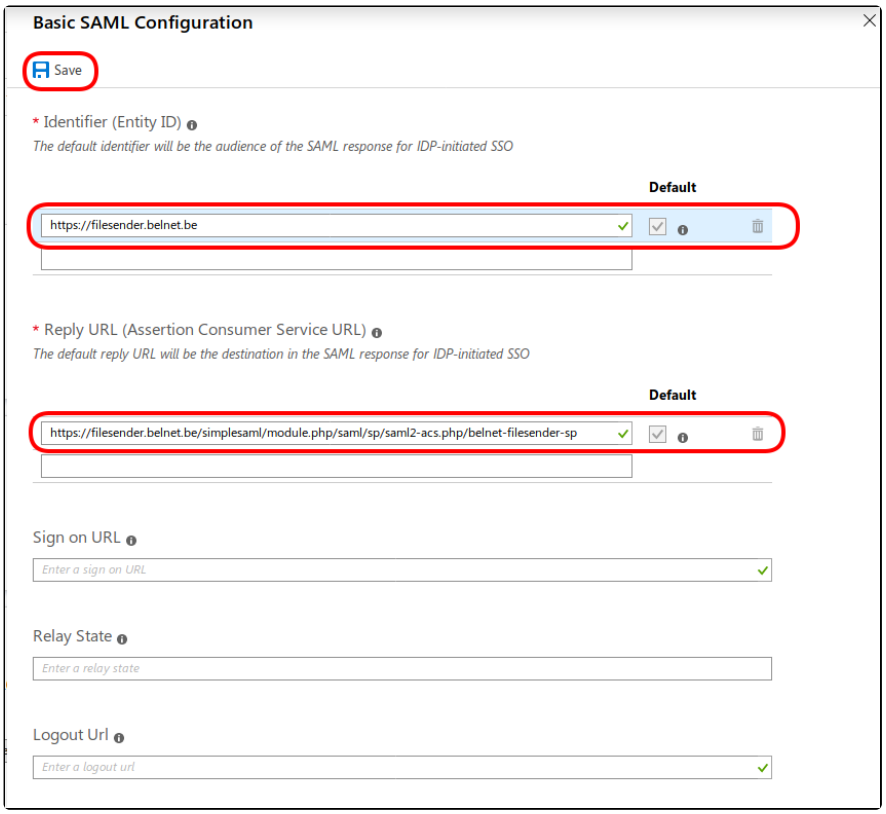
- Download the Belnet FileSender SP metadata from https://filesender.belnet.be/simplesaml/module.php/saml/sp/metadata.php/belnet-filesender-sp as an **.xml** file:

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

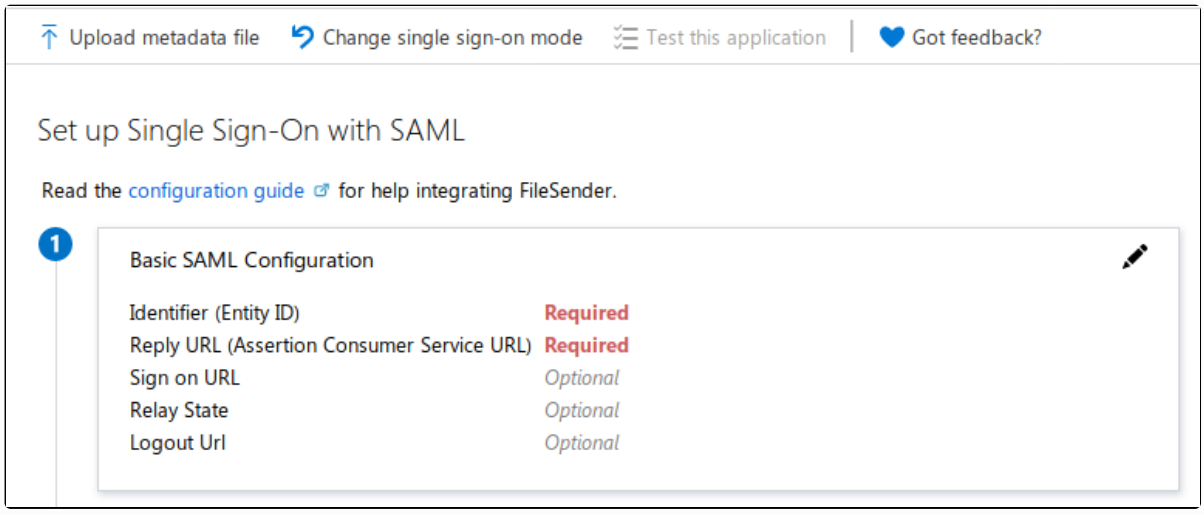


- If the metadata file upload is **successful**, you will get the **Basic SAML Configuration** with the fields **Identifier (Entity ID)**, **Reply URL (Assertion Consumer Service URL)** & **Logout Url** already filled in.

- Click on **Save:**



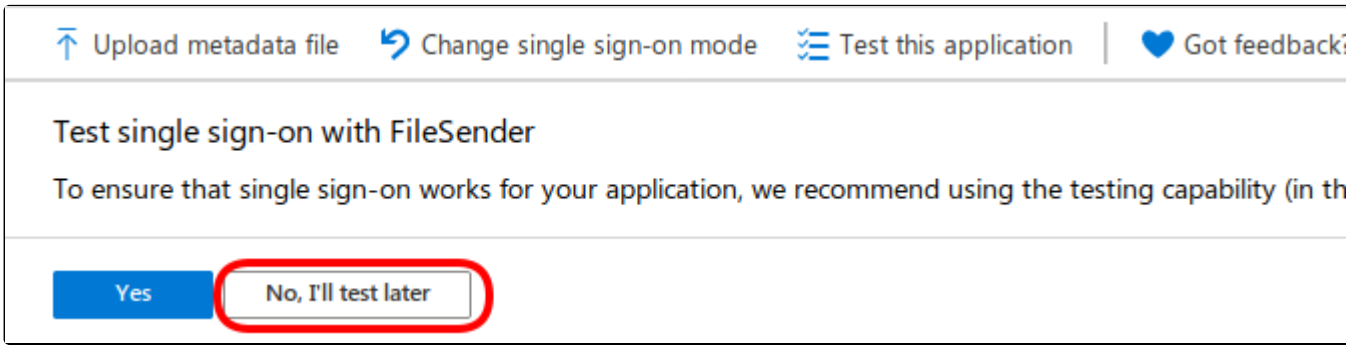
If your attemps to upload (above steps) your metadatas is **unsuccessful**, click on the **edit button** of **Basic SAML Configuration:**



- 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

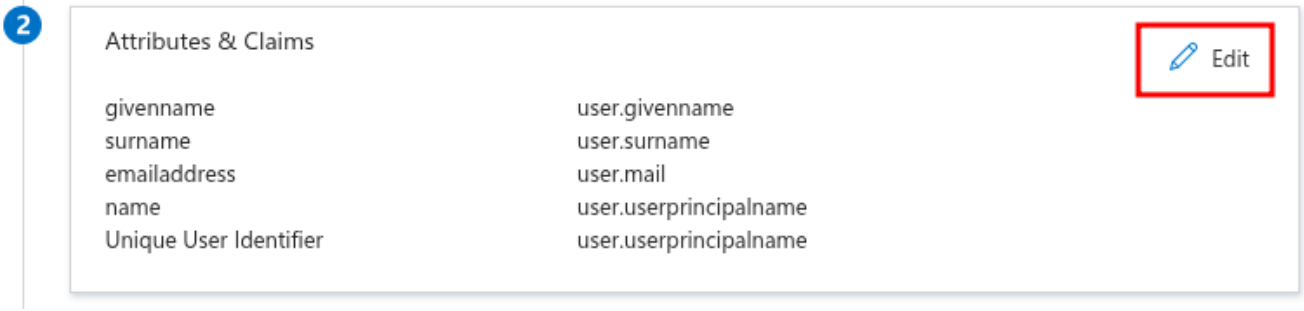
  Logout Url (Optionnal) https://filesender.belnet.be/simplesaml/module.php/saml/sp/saml2-logout.php/belnet-filesender-sp
- Click on **Save**

- The system will ask you if you want to test Single sign-on with FileSender, click on **No, I'll test later** for now:

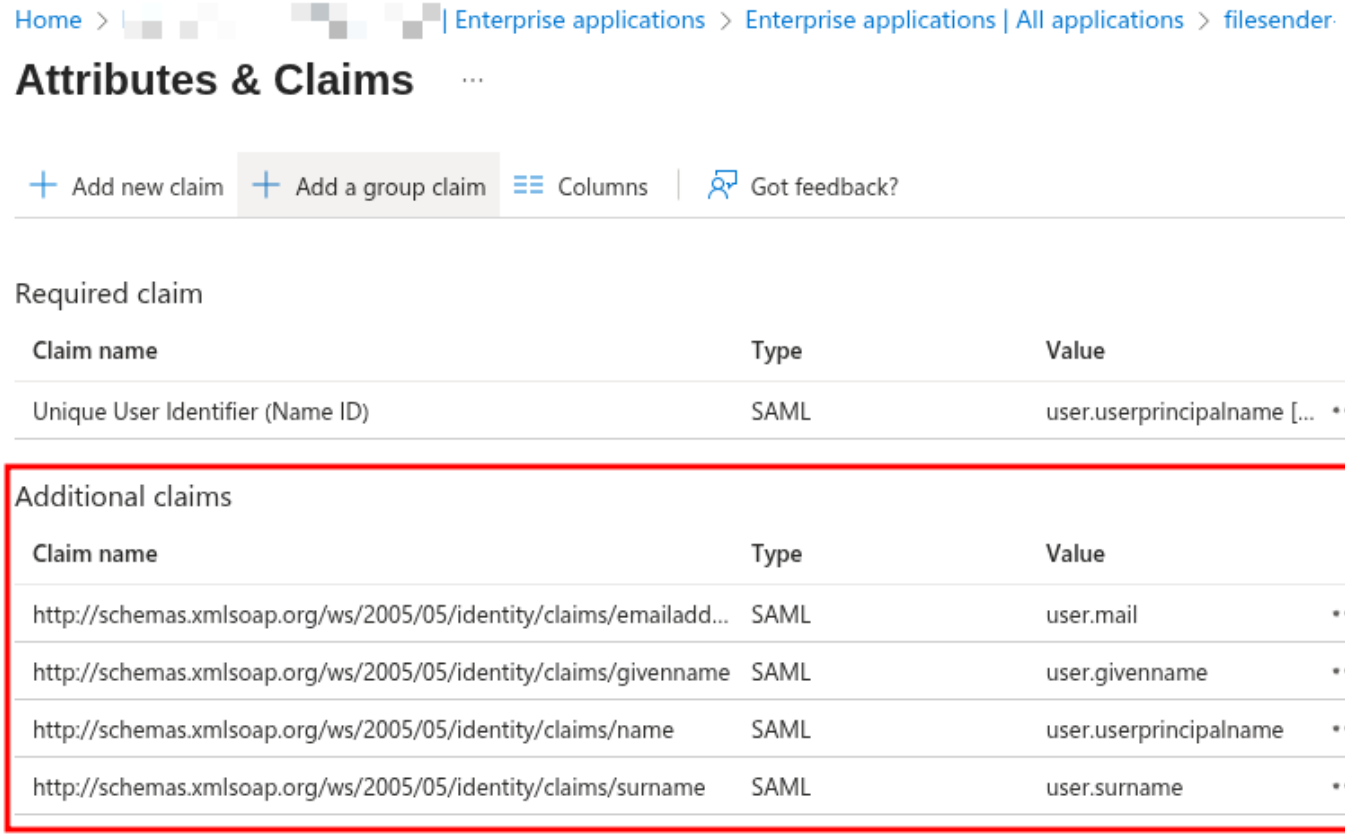


Step 5: Configure Attributes & Claims

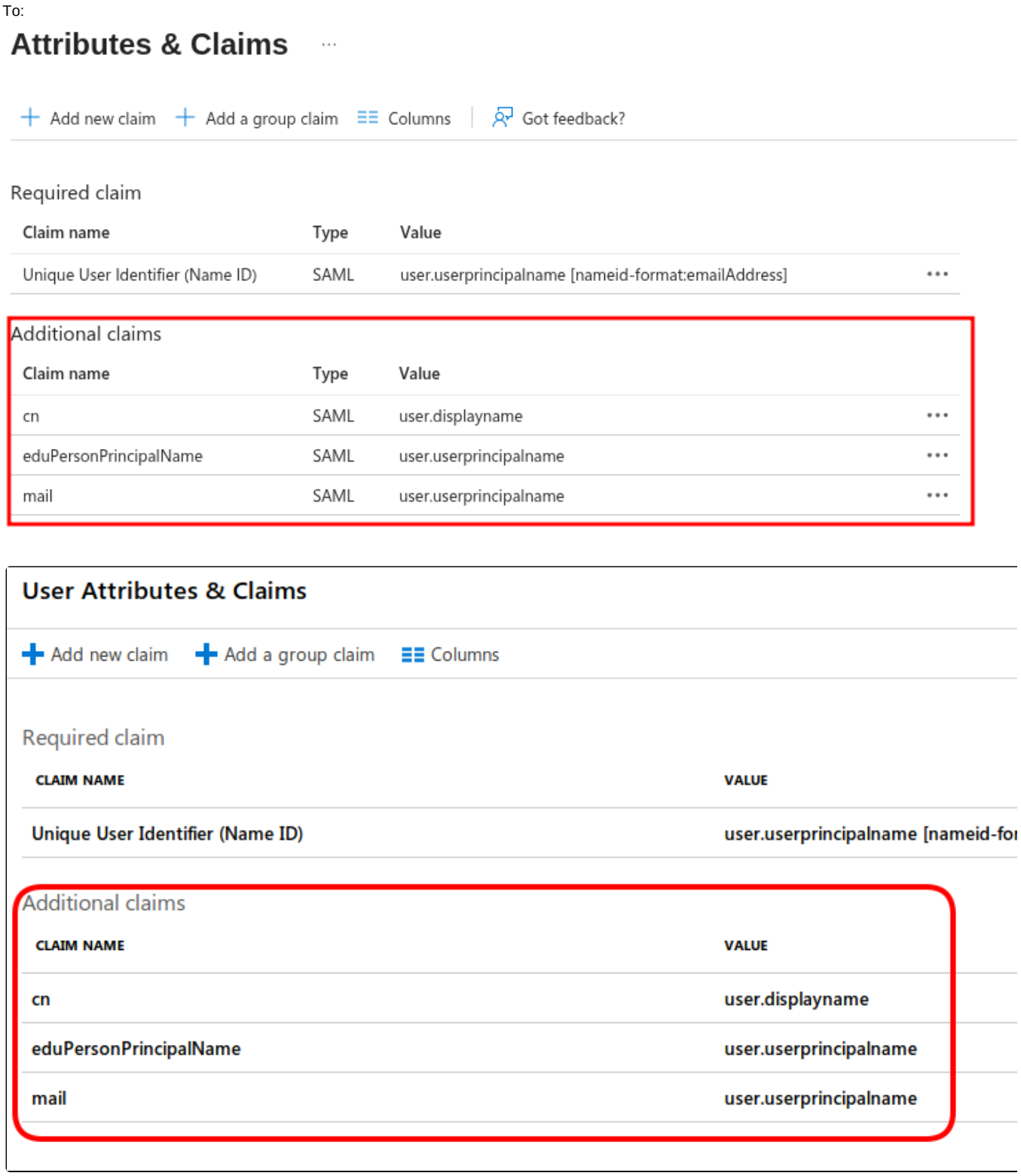
- Click on the edit button for **Attributes & Claims**:



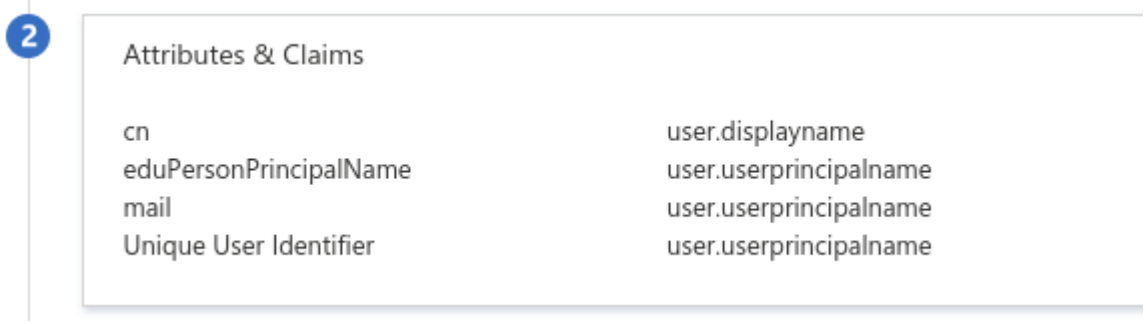
- Modify the Additional claims from:



- To:



- Result:



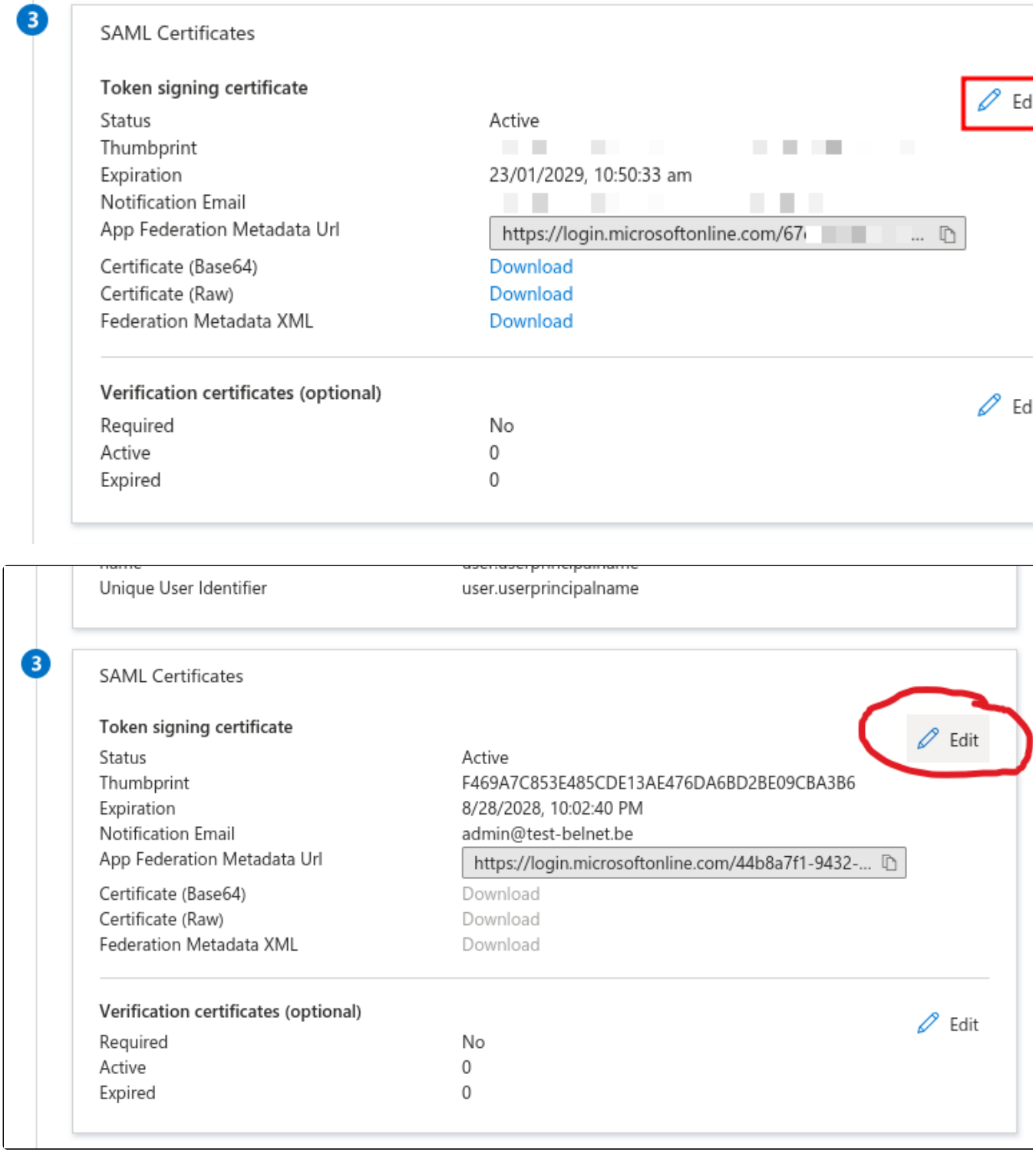
Step 6: Import SAML signing certificate

If you did things right, you've created a dedicated certificate for all your Entra ID Enterprise Applications See the introduction note in the Prerequisites.

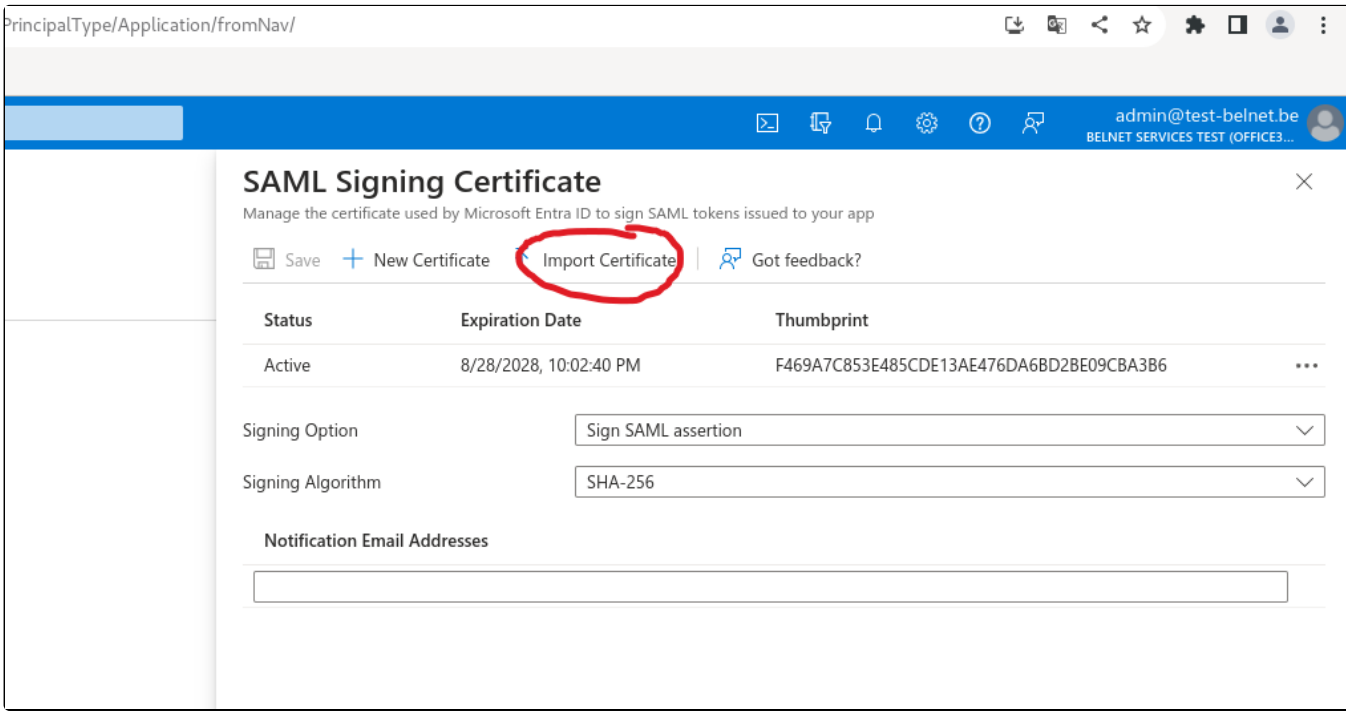
In this case, you now have to import it in your application.

> ⚠ **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).

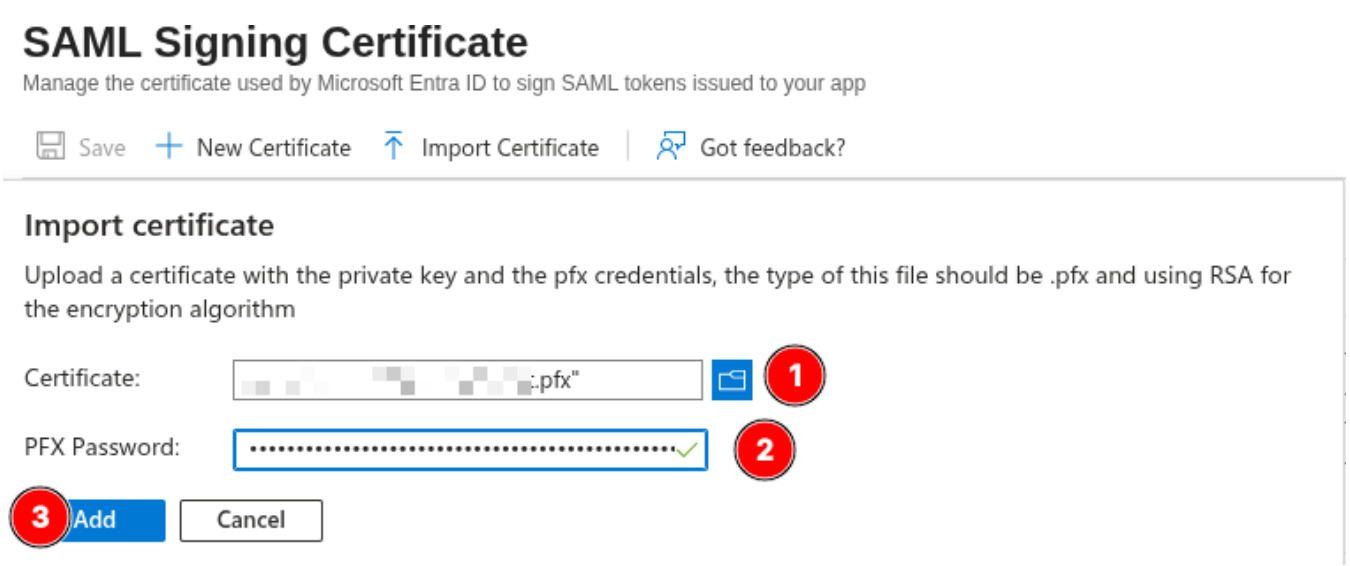
- Click on "Edit" on the "SAML Certificates" tile of your application:



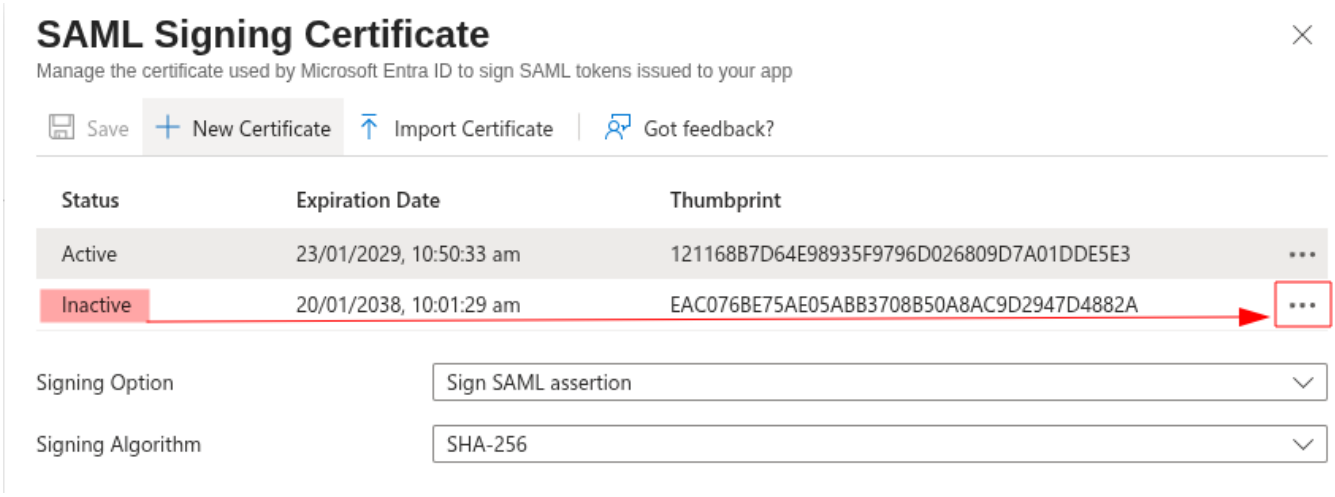
- In the "SAML Signing Certificate" pane on the right, click "**Import Certificate**":

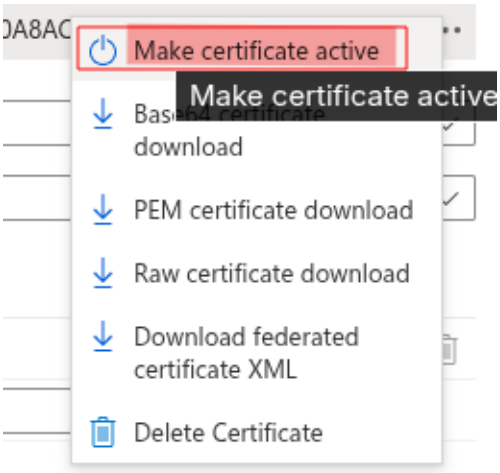


- Select the .pfx file you have created earlier, type its passphrase, and click on "Add":



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

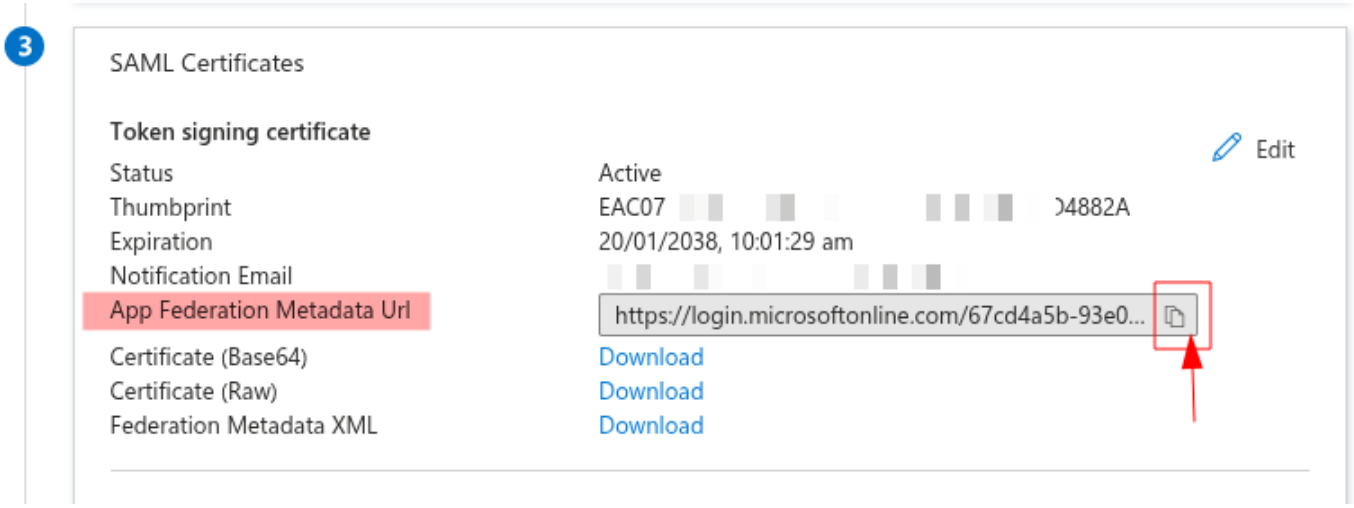




Step 7: Modify manually your Entra ID App Metadatas

Get your App Federation Metedatas and save/store them.

- Copy to your clipboard your **App Federation Metedata Url:**



- Download your IdP App Metadatas using the tool/command of your choice (powershell; wget, curl) and save the output to a **.xml** file

```
Invoke-WebRequest -Uri "https://login.microsoftonline.com/<teannt_entity_id>/federationmetadata/2007-06
/federationmetadata.xml?appid=<your_idp_app_id>" -OutFile "idpapp.xml"
```

Enrich your IdP App Metadatas with additional tags required by the Belnet R&E Federation

You'll now have to **manipulate your metadatas to add some tags that are required by the Belnet R&E Federation**.
Without adding these additionals tags, your IdP app metadatas will be refused later on when you'll upload them on the Belnet Federation portal .

Add additionals tags

- Open your downloaded metadata file
- Add these hereunder additionals tags :

You **MUST** add these additionals tags at the end of your metadata between::

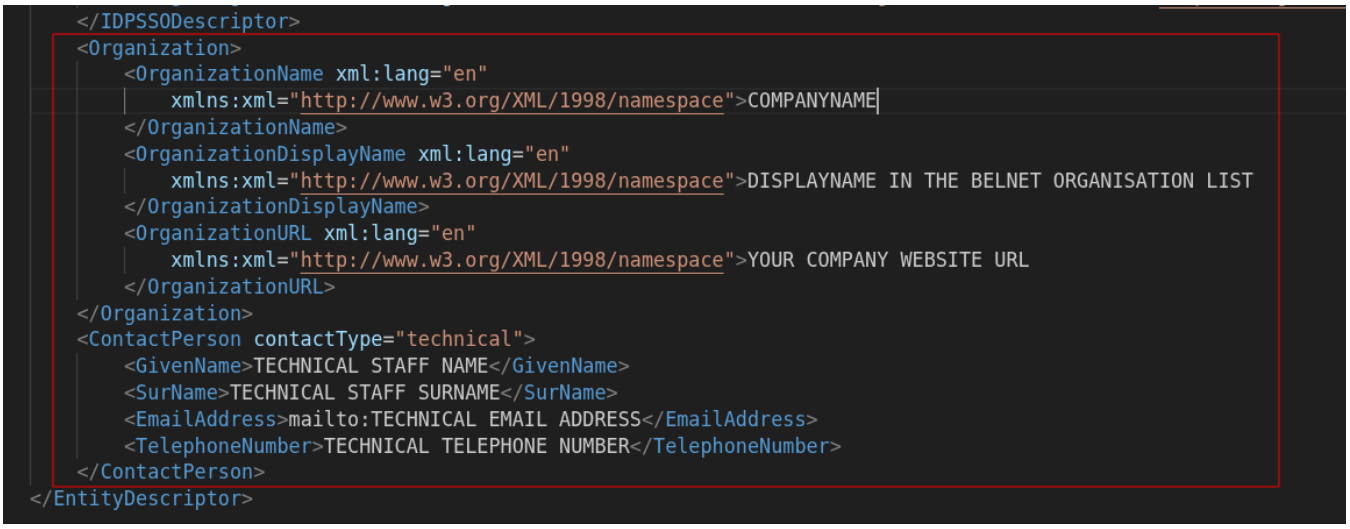
- the closing tag: </IDPSSODescriptor>

  ...

- the closing tag: </EntityDescriptor>

```
<Organization>
<OrganizationName xml:lang="en"
xmlns:xml="http://www.w3.org/XML/1998/namespace">COMPANYNAME
</OrganizationName>
<OrganizationDisplayName xml:lang="en"
xmlns:xml="http://www.w3.org/XML/1998/namespace">DISPLAYNAME IN THE BELNET ORGANISATION LIST
</OrganizationDisplayName>
<OrganizationURL xml:lang="en"
xmlns:xml="http://www.w3.org/XML/1998/namespace">COMPANY WEBSITE URL
</OrganizationURL>
</Organization>
<ContactPerson contactType="technical">
<GivenName>TECHNICAL STAFF NAME</GivenName>
<SurName>TECHNICAL STAFF SURNAME</SurName>
<EmailAddress>mailto:TECHNICAL EMAIL ADDRESS</EmailAddress>
<TelephoneNumber>TECHNICAL TELEPHONE NUMBER</TelephoneNumber>
</ContactPerson>
```

- **OrganizationName**: Please replace COMPANYNAME by your company's name
- **OrganizationDisplayName**: Please replace "DISPLAYNAME IN THE BELNET ORGANISATION LIST" by the name you want to be shown in the list of IDP when logging in on the Belnet federation services
- **OrganizationURL**: Please replace "COMPANY WEBSITE URL"
- **<GivenName>**: Please replace "TECHNICAL STAFF NAME"
- **<Surname>**: Please replace "TECHNICAL STAFF SURNAME"
- **<EmailAddress>**: Please replace "TECHNICAL EMAIL ADDRESS"
- **<TelephoneNumber>**: Please replace "TECHNICAL TELEPHONE NUMBER"



- Save your enriched metadata file.

Metadata template

At this stage, the new content of your metadata file should contain all the tags from the template shown below.

idpmetadata.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="Your Entra Tenant Identifier">
<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>CERTIFICATE</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<KeyDescriptor use="encryption">
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>CERTIFICATE</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</NameIDFormat>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="LOGIN URL" />
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="LOGIN URL" />
</IDPSSODescriptor>
<Organization>
<OrganizationName xml:lang="en"
xmlns:xml="http://www.w3.org/XML/1998/namespace">COMPANYNAME
</OrganizationName>
<OrganizationDisplayName xml:lang="en"
xmlns:xml="http://www.w3.org/XML/1998/namespace">DISPLAYNAME IN
THE BELNET ORGANISATION LIST
</OrganizationDisplayName>
<OrganizationURL xml:lang="en"
xmlns:xml="http://www.w3.org/XML/1998/namespace">COMPANY
WEBSITE URL
</OrganizationURL>
</Organization>
<ContactPerson contactType="technical">
<GivenName>TECHNICAL STAFF NAME</GivenName>
<SurName>TECHNICAL STAFF SURNAME</SurName>
<EmailAddress>mailto:TECHNICAL EMAIL ADDRESS</EmailAddress>
<TelephoneNumber>TECHNICAL TELEPHONE NUMBER</TelephoneNumber>
</ContactPerson>
</EntityDescriptor>
```

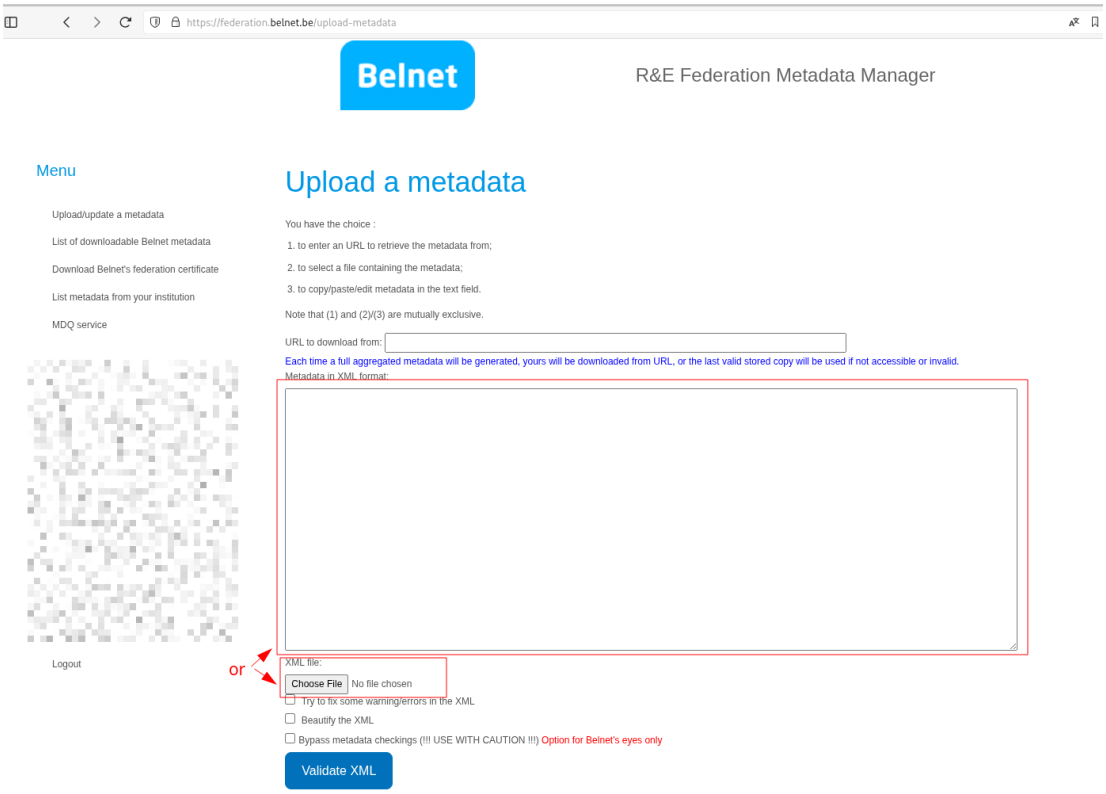
Step 8: Publish your metadata in the Belnet Federation

If this the first Entra Enterprise Application you create (or if you had modified your metadatas already published in the Belnet R&E Federation), **you now have to publish your metadata in the Belnet R&E Federation**:

- Log on to Belnet Federation Metadata Manager website (https://federation.belnet.be).
- Upload the metadatas of your Entra IdP:
  - copy /paste all the content of your enriched .xml file in the in the box provided for metadata

    OR

  - Click the button to choose your metadatas file.



- Click on: Validate XML
- Please now wait that Belnet enginners, in charge of the Federation, verify/approve your metadatas and place them in the dedicated Federation.

> 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).
>
> New metadatas are generally validated by Belnet **once or twice a day**.

Step 9: Test Single sign-on with FileSender (24h later)

We recommend that you wait 24 hours between sending your metadata to Belnet's R&E Federation and testing SSO authentication on Belnet Filesender.