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

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 manaegement 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"):

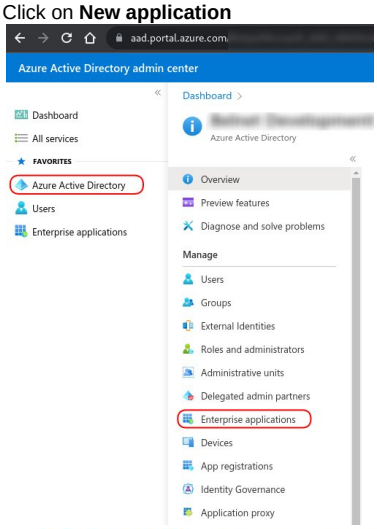
```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -sha256 -days 3650 -nodes -subj "
/C=XX/ST=StateName/L=CityName/O=CompanyName/OU=CompanySectionName/CN=CommonNameOrHostname"

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

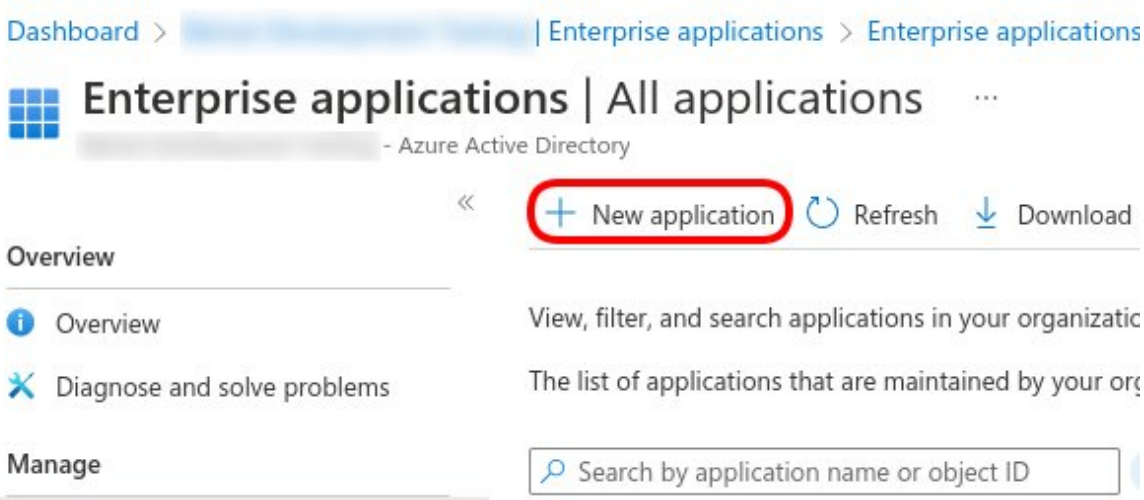
Note that you MUST use a passphrase for your .pfx file; an empty passphrase won't be accepted by Entra ID later.

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.

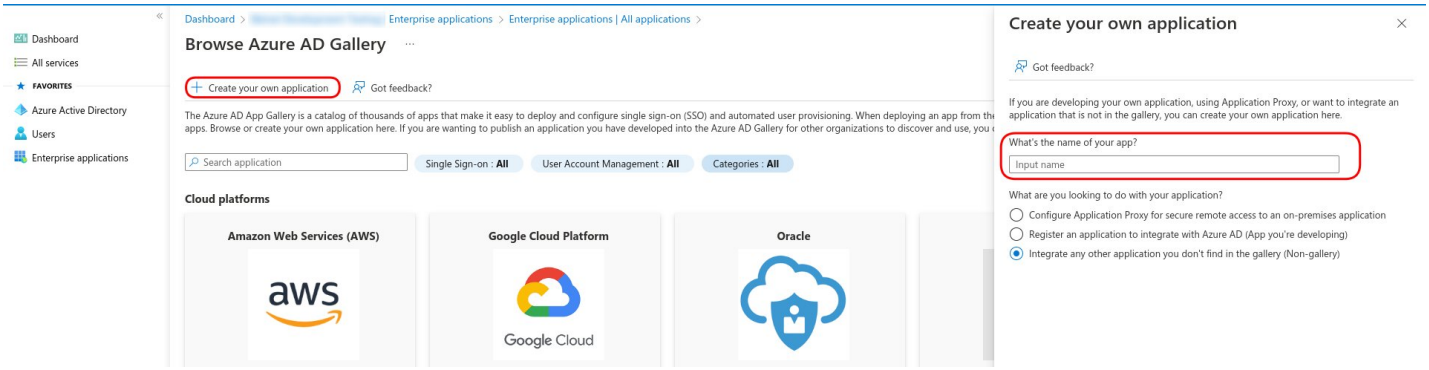
Step 1: Create an Enterprise application in Entra ID

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

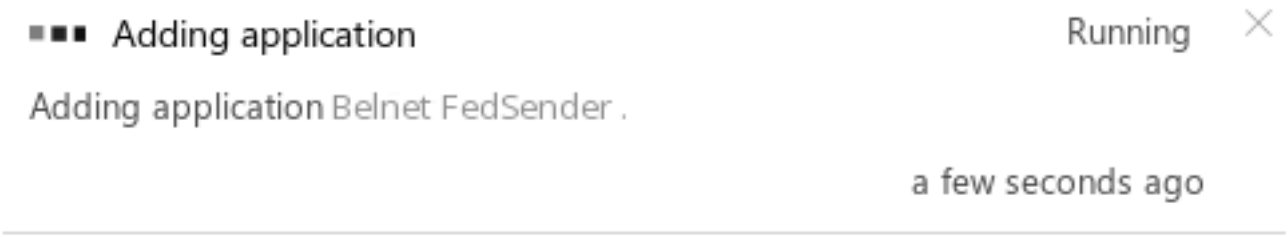




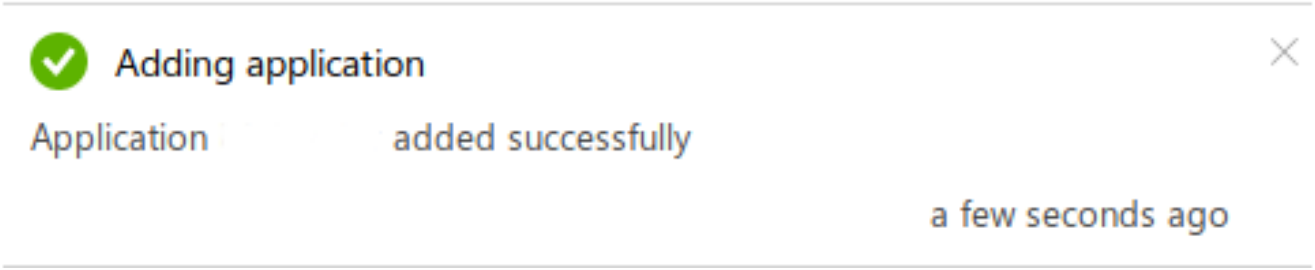
- Click on **Create your own application,** enter **Belnet FedSender** in the **Name** field and click **Create**



- Enter **Belnet FedSender** 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

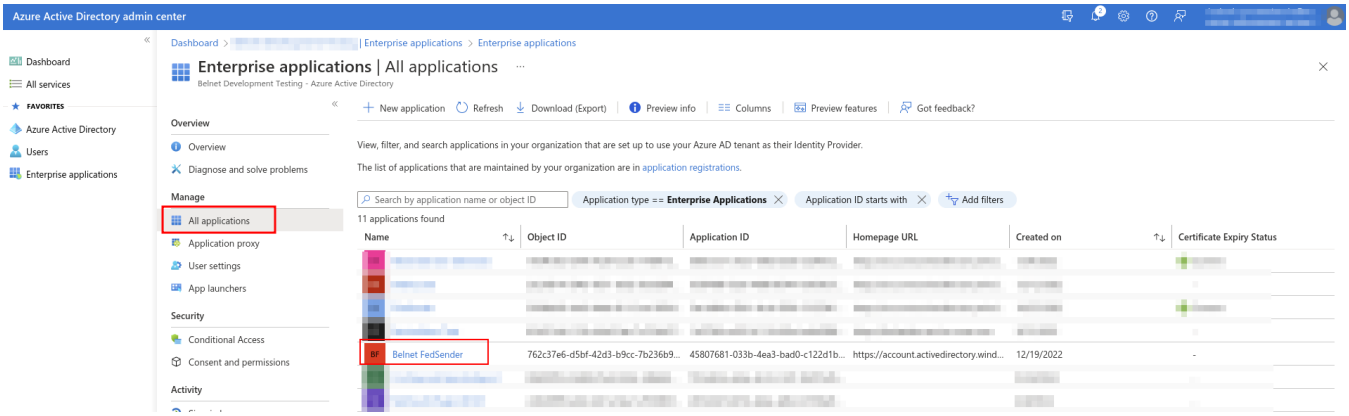
- Retrieve/Donwload now the Belnet Fedsender certificate used for metadatas:

  This can be done in two different ways:

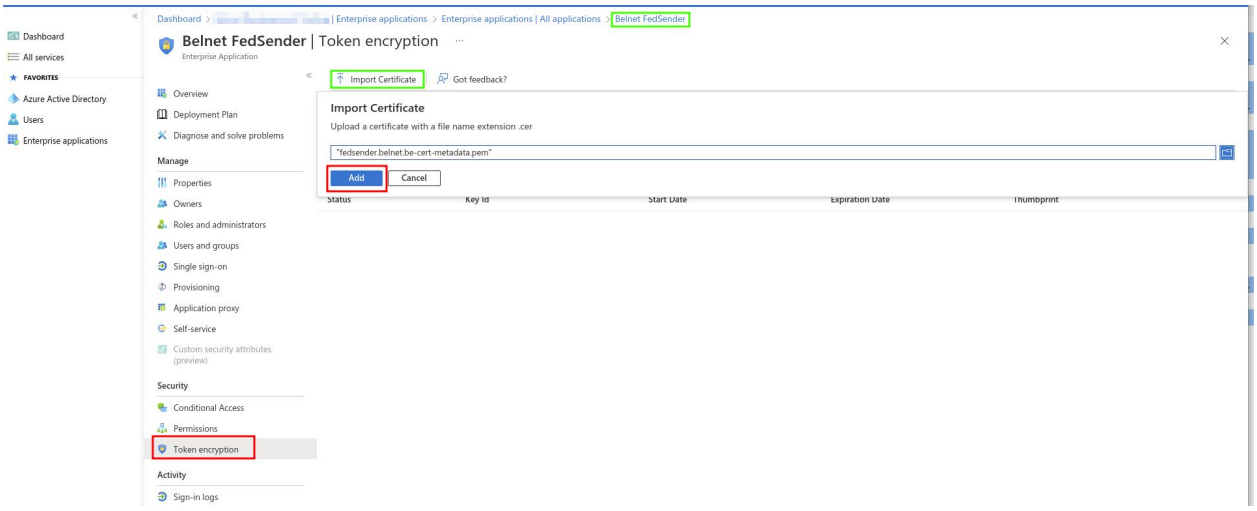
  - by downloading the certificate itself on: https://fedsender.belnet.be/fedsender.belnet.be-metadata-ss.crt
    or
  - by consulting SAML Metadata on the Service Provider itself (FedSender SP) at url: https://fedsender.belnet.be/simplesaml/module.php/saml/sp/metadata.php/belnet-gcloud-idp

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

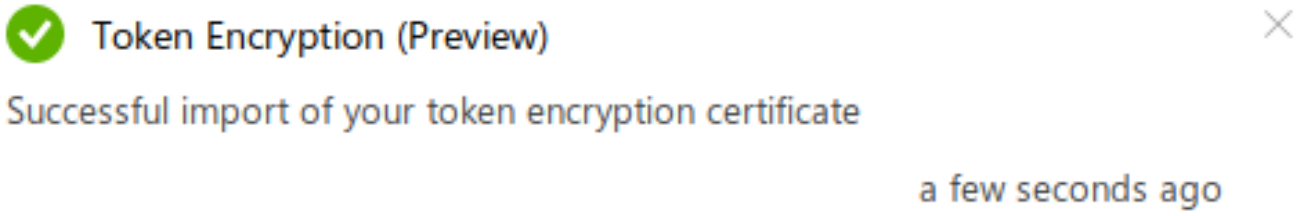
- On Microsoft Entra ID admin center **Entra ID** --> **Enterprise apps** **All Applications**
- **Select** your newly created application named Belnet **FedSender**



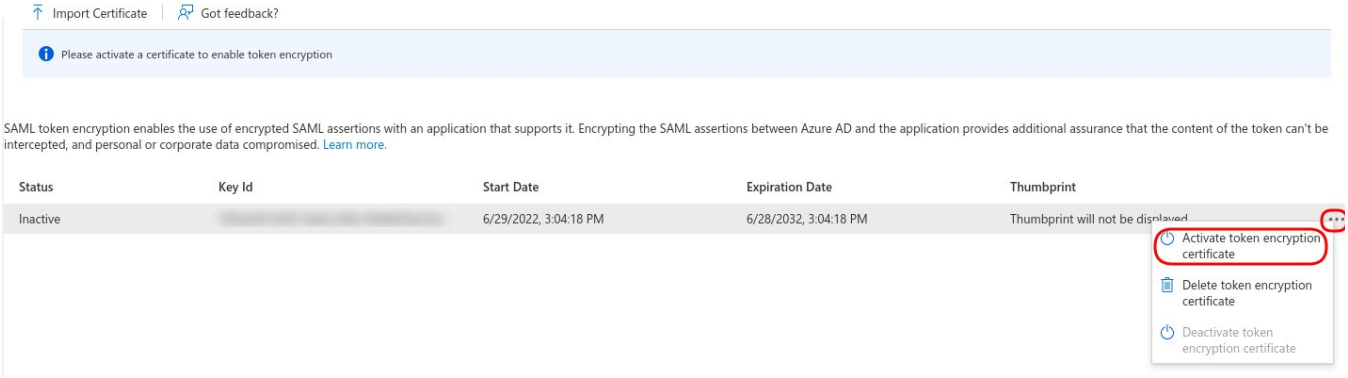
- Click on **Token encryption**, then click on **Import Certificate**
- Select the **certificate** fetched previously and click on **Add**



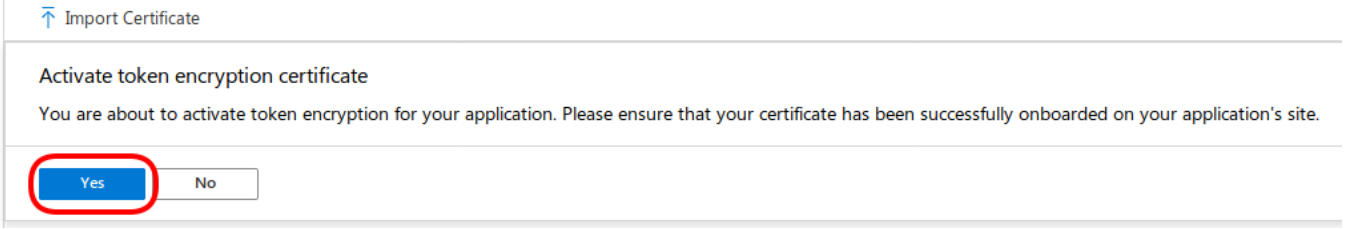
- Wait for the **successful** import of the certificate



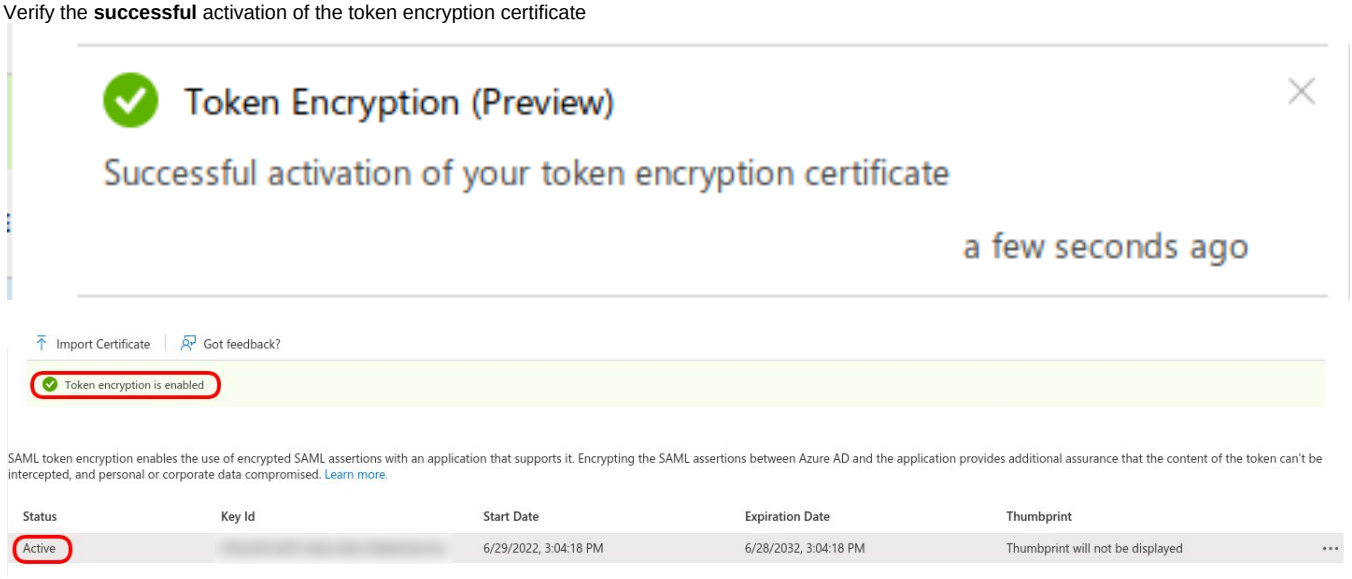
- Click on the **3 dots button** and click on **Activate token encryption**



- Click on **Yes**



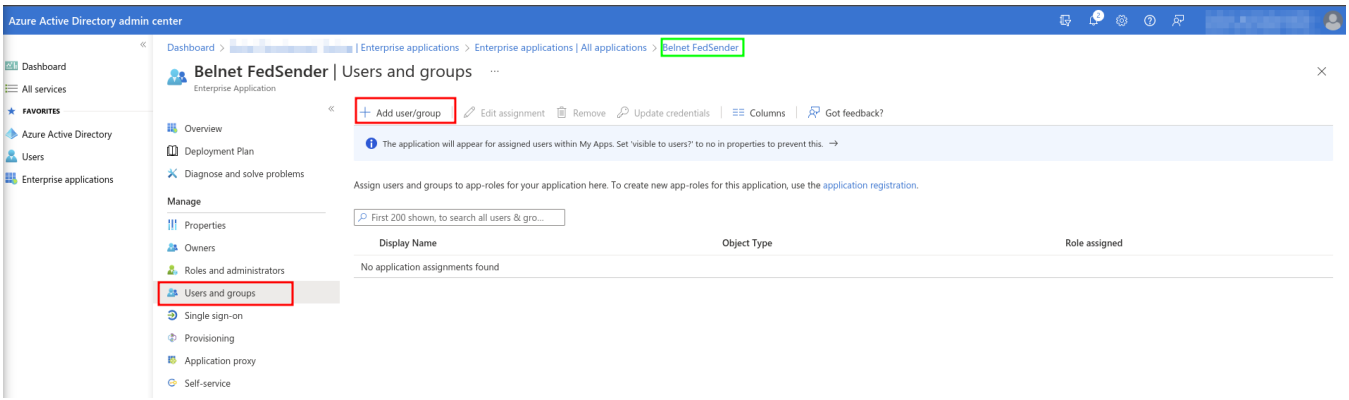
- Verify the **successful** activation of the token encryption certificate



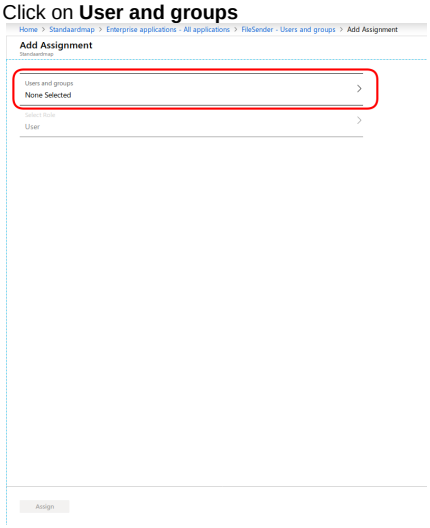
> **Monitor on your Tenant the expiration of the certificate!**
>
> To prevent or minimize outage due to a certificate expiring, use roles and email distribution lists to ensure that certificate-related change notifications are closely monitored.

Step 3: Manage Users and groups

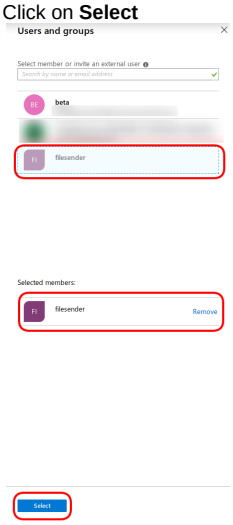
- On Microsoft Entra ID admin center, go to **Entra ID** **Enterprise apps** **All applications** **Belnet FedSender** Under **Manage** (Left Pane) **Users and groups**, click on **Add user**



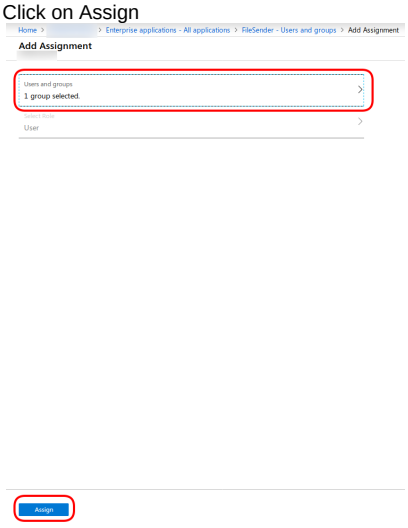
- Click on **User and groups**



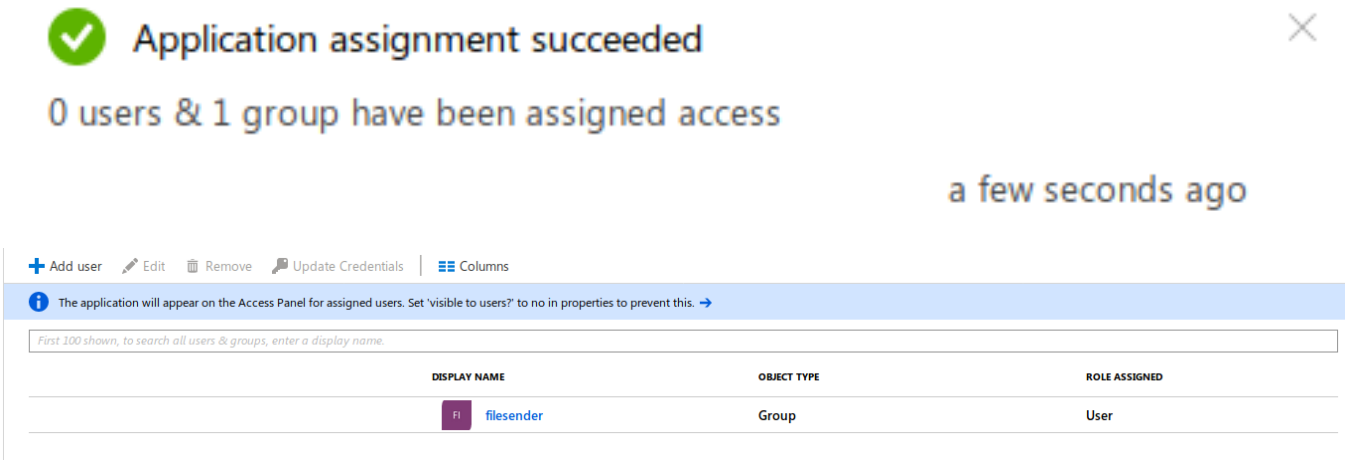
- For this example, we will select the group **fedsender** with user **beta** as member of. **Please adapt as it fits to your organisation.**
  Click on **Select**



- Click on Assign

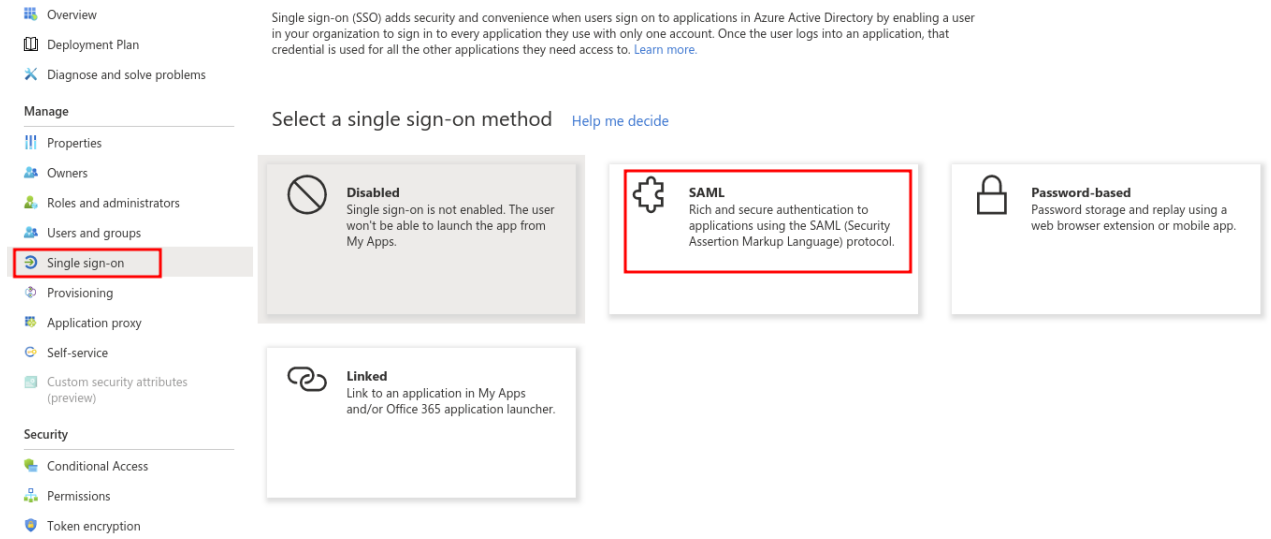


- Group **fedsender** has been assigned access (as **user**) to the **Belnet FedSender** application



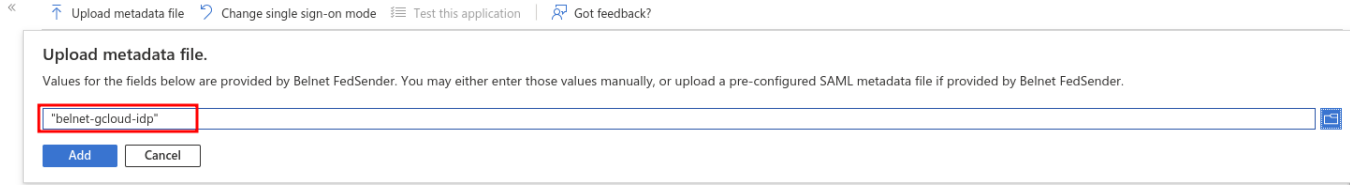
Step 4: Configure the Single sign-on (SAML)

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

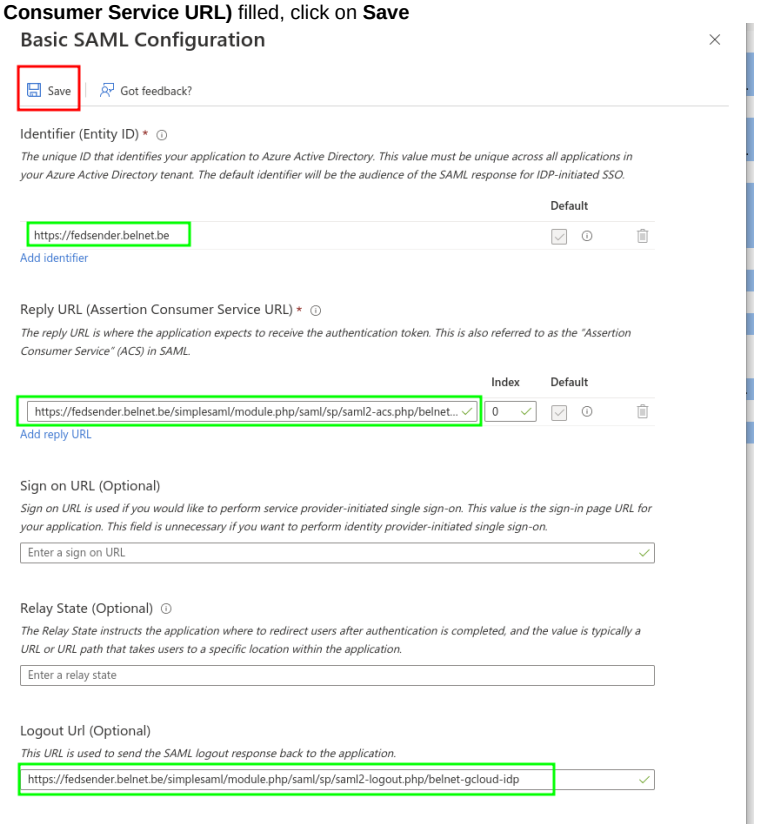


- Download the Belnet FedSender metadatas from https://fedsender.belnet.be/simplesaml/module.php/saml/sp/metadata.php/belnet-gcloud-idp as an **.xml** file

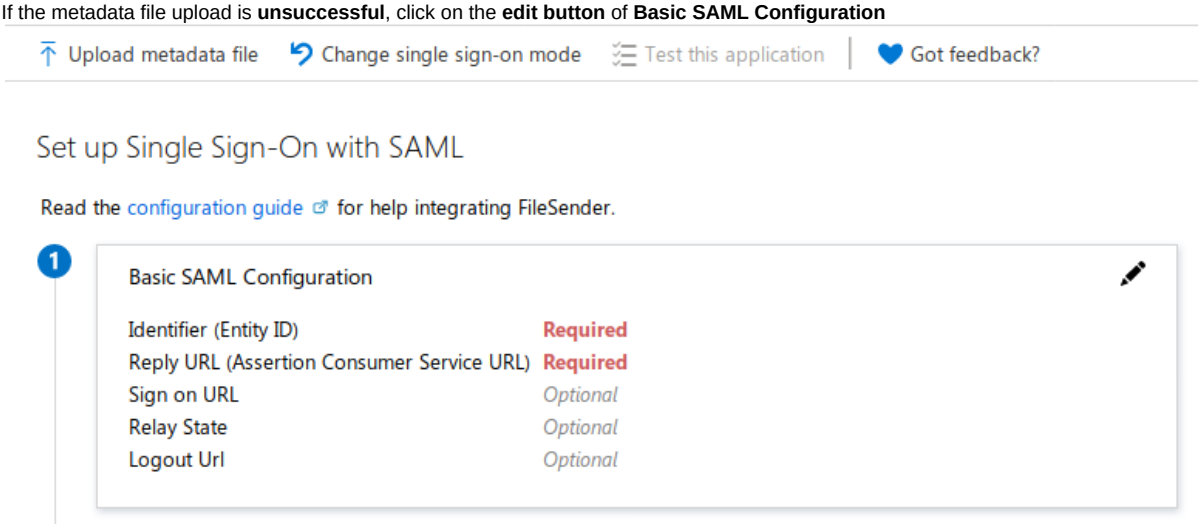
- Click on **Upload metadata file**, select the **Belnet FedSender metadata xml file** and click on **Add**



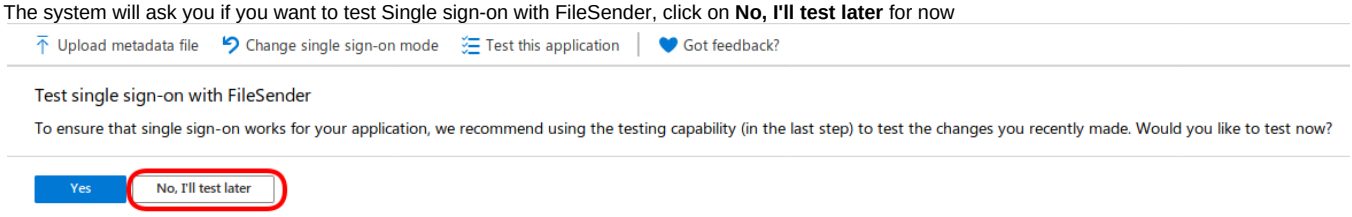
- If the metadata file upload is **successful**, you will get the **Basic SAML Configuration** with the fields **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** filled, click on **Save**



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

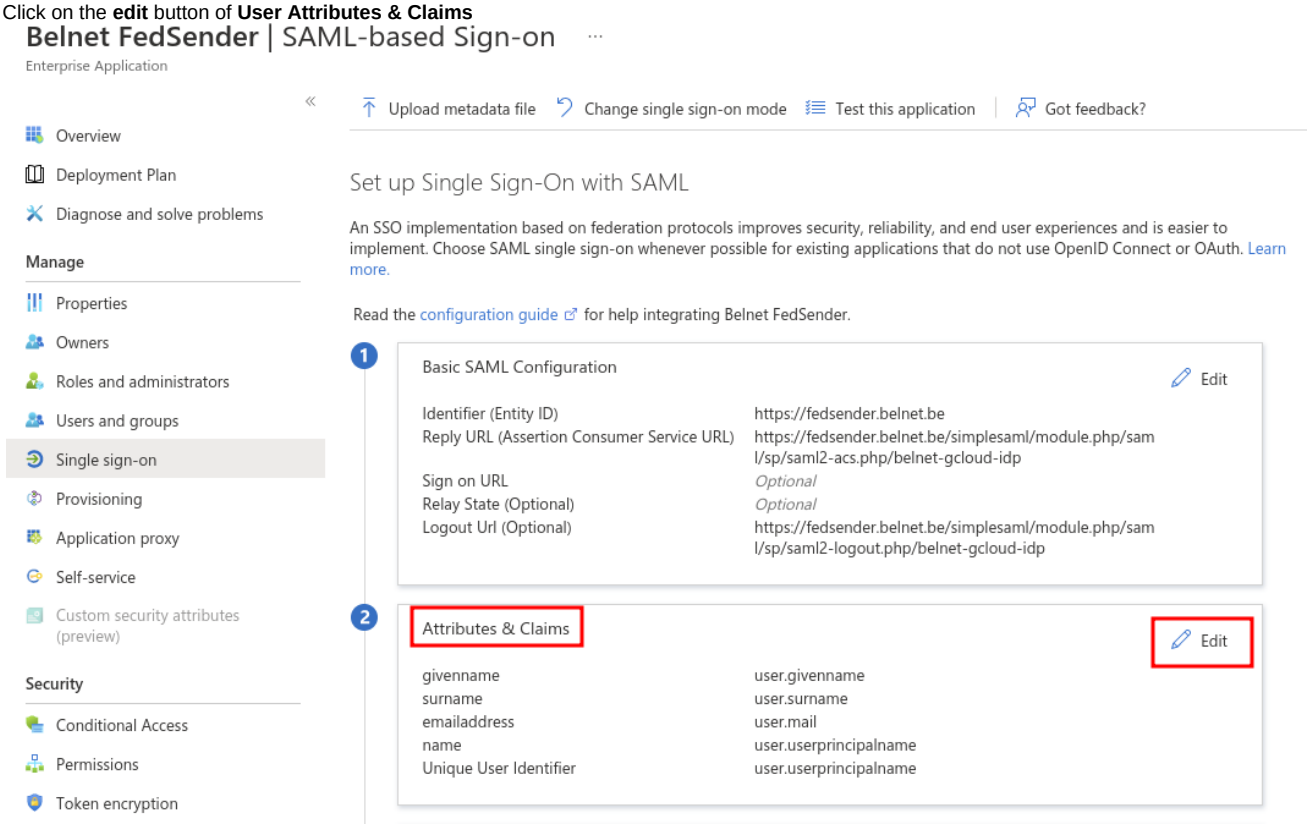


- And fill the following fields:
  Identifier (Entity ID): https://fedsender.belnet.be
  Reply URL (Assertion Consumer Service URL): https://fedsender.belnet.be/simplesaml/module.php/saml/sp/saml2-acs.php/belnet-gcloud-idp
  Click on **Save**
- The system will ask you if you want to test Single sign-on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

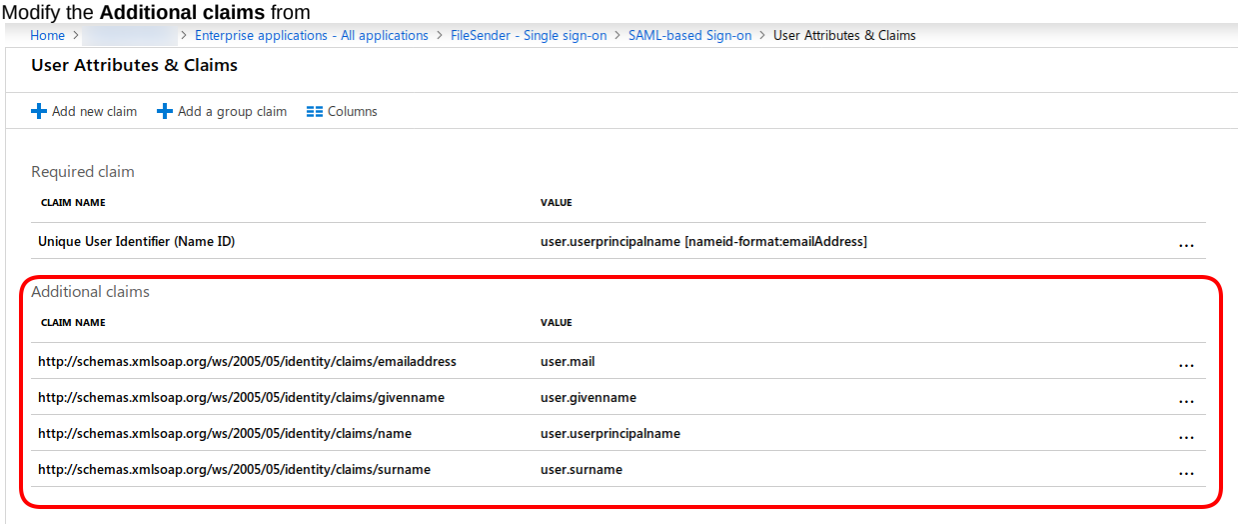


Step 5: Configure User Attributes & Claims

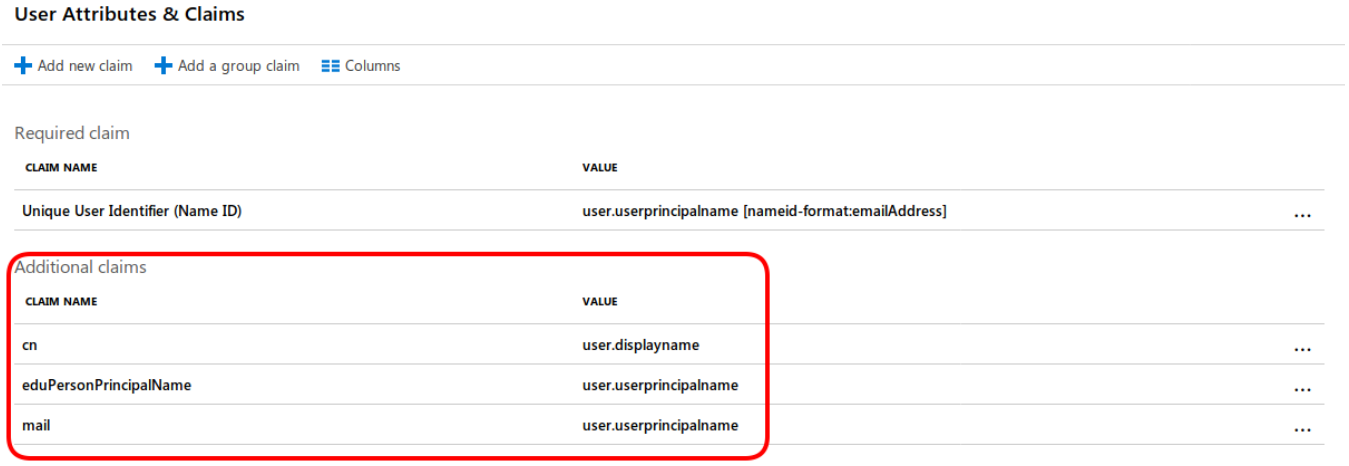
- Click on the **edit** button of **User Attributes & Claims**



- Modify the **Additional claims** from

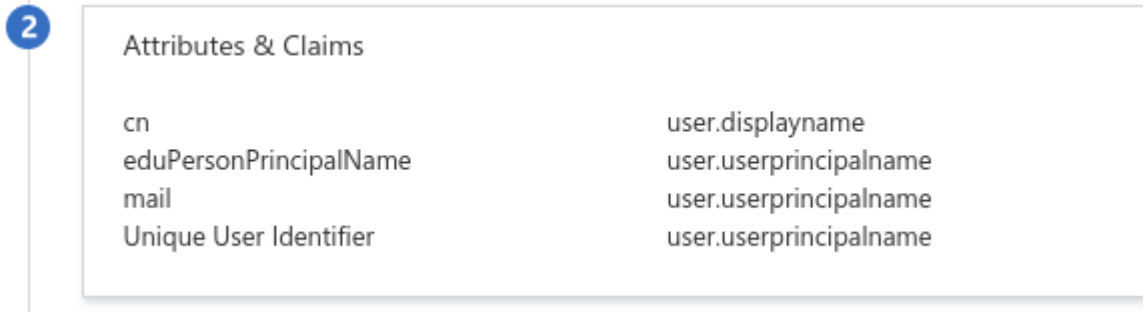


- To:



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

Result:



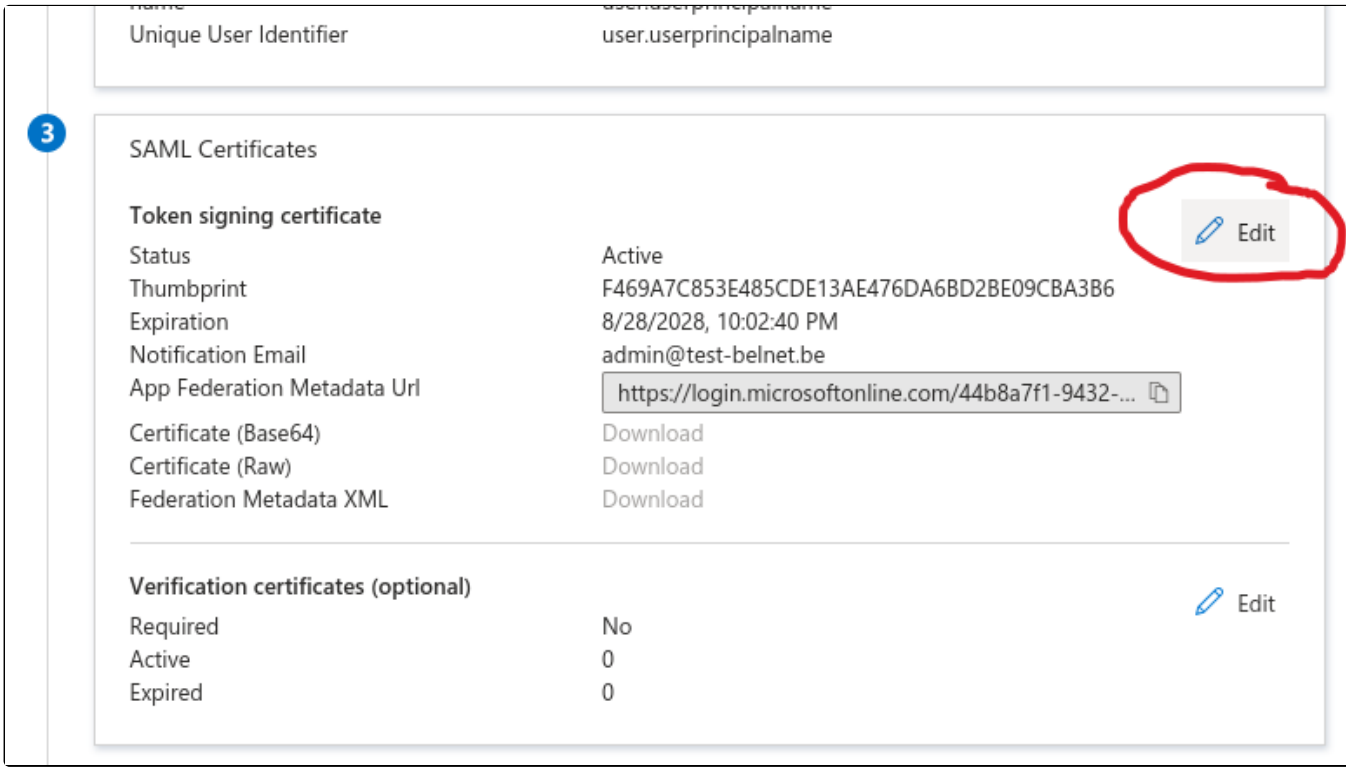
Step 6: SAML Signing Certificate (Optional - only if you created a dedicated certificate for all your Entra ID Enterprise applications)

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

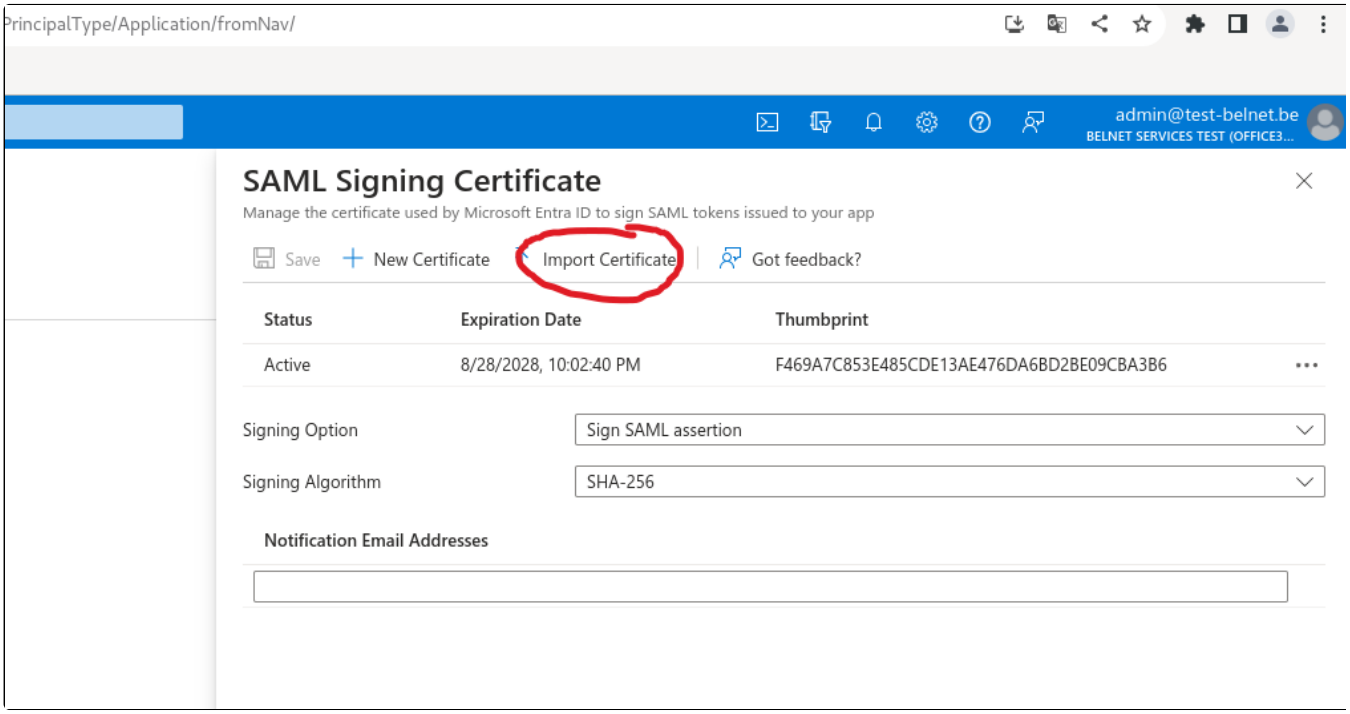
In this case, you now have to import it in your application.

> ⚠ **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).

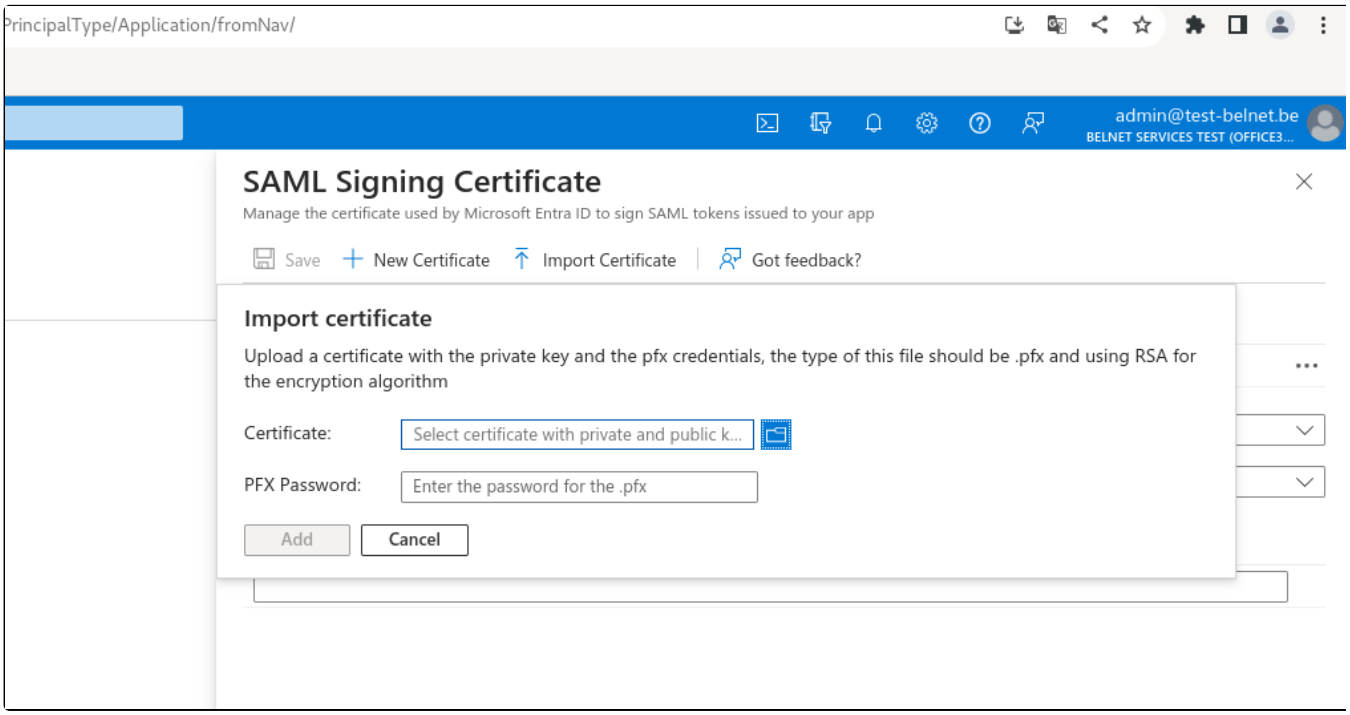
- Click on "Edit" on the "SAML Certificates" tile of your application:



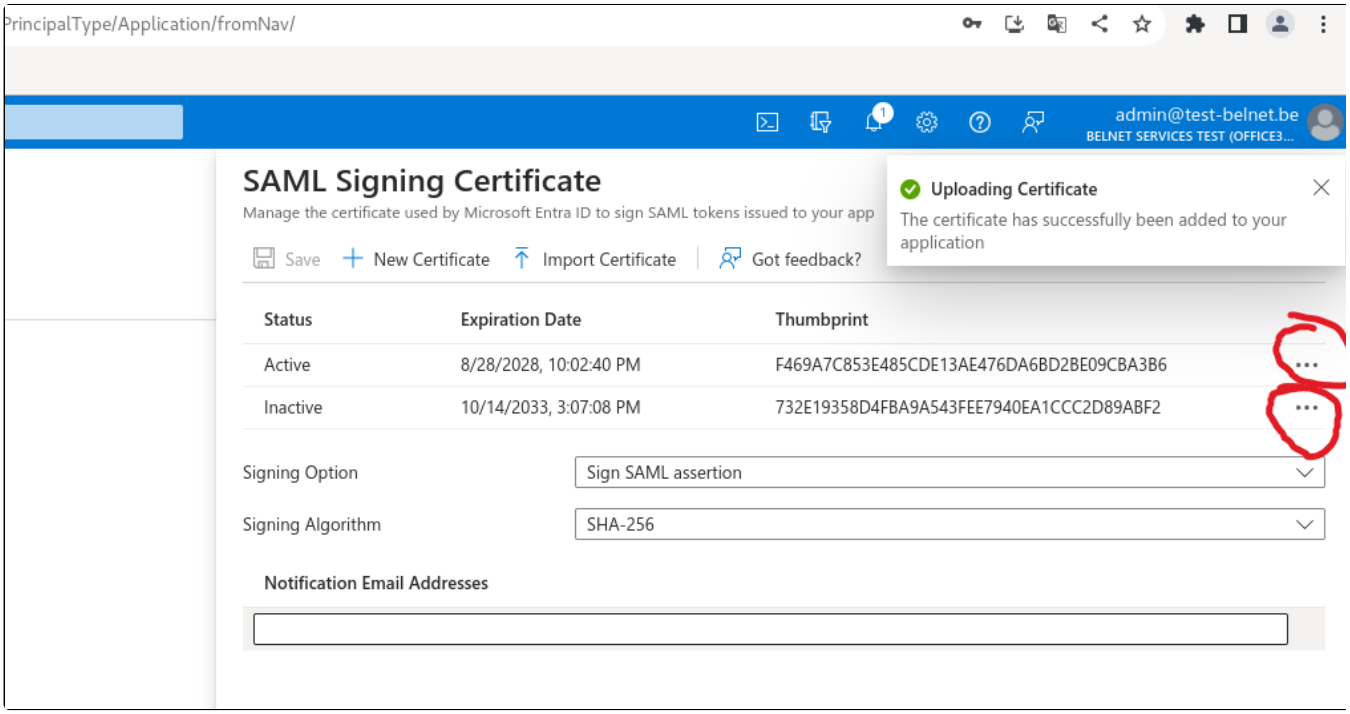
- In the "SAML Signing Certificate" pane on the right, click "Import Certificate":



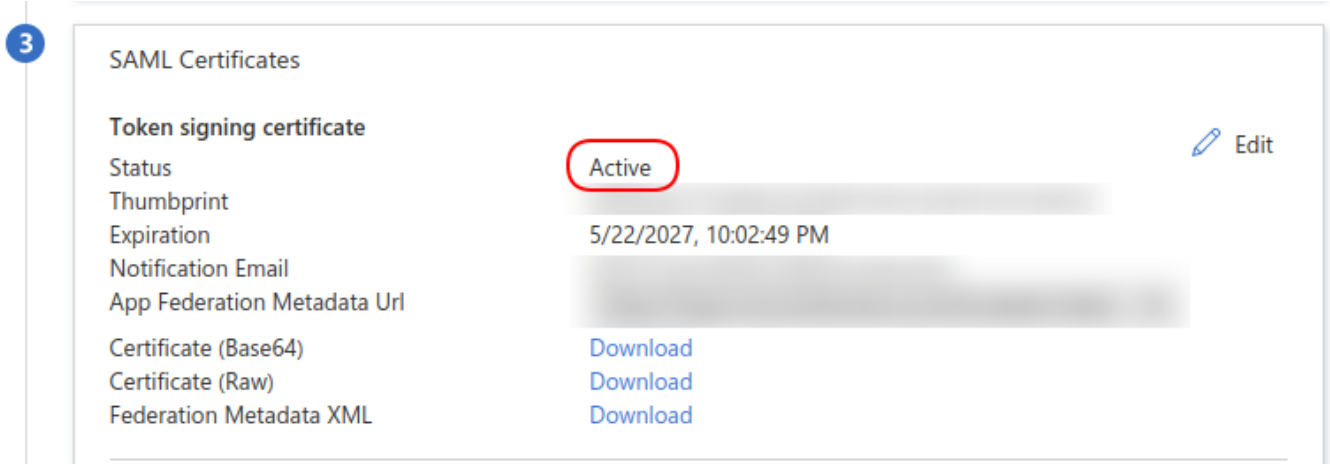
- Select the .pfx file you have created earlier, type its passphrase, and click on "Add":



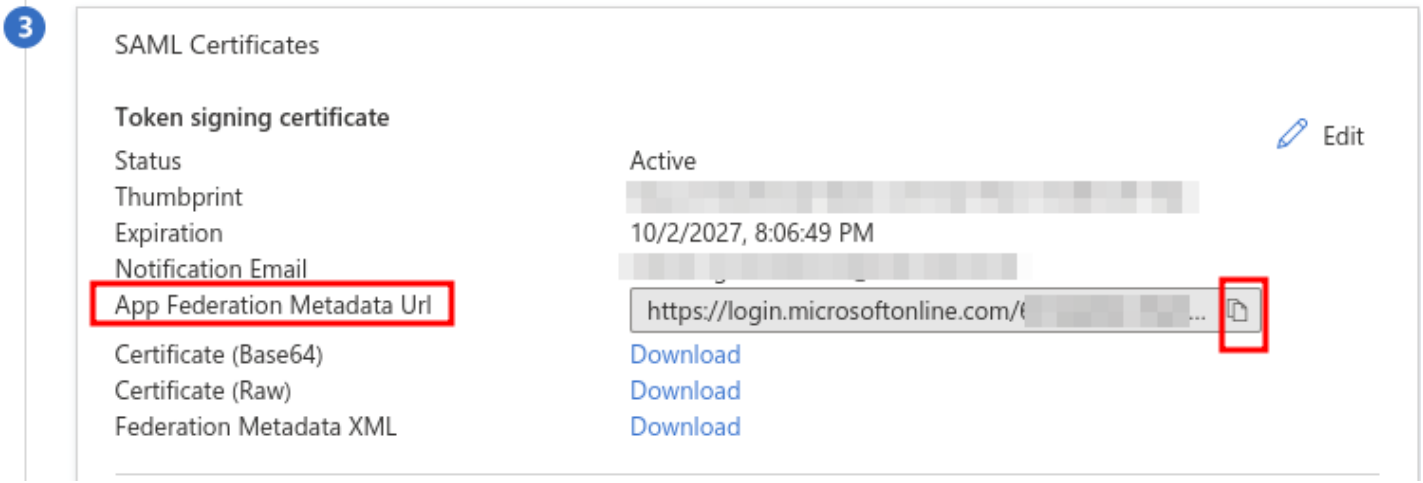
- Your certificate is now uploaded. Now, activate it and deactivate the autogenerated one by using their 3-dots menu:



- Verify that the SAML Signing Certificate is Active



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



- 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:

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.