Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNIQUE

# Préparation d'un *Azure AD Tenant* en tant qu'IdP pour Edulog

7.1.2022 – Version 1.2



Föderation der Identitätsdienste im Bildungsraum Schweiz
Fédération des services d'identité de l'espace suisse de formation
Federazione dei servizi di identità nello spazio formativo svizzero
Federaziun dals servetschs d'identitad en il spazi da furmaziun svizzer

# 1. But du Document

Ce document décrit les étapes nécessaires pour qu'un IdP puisse configurer *Azure AD* comme *SAML-endpoint*, à intégrer avec Edulog.

Il ne montre pas comment l'*onboarding* des identités doit se faire. Cette étape sera réalisée après l'intégration.

# 2. Prérequis

Vous avez :

- un compte sur *Azure*. Créer un *Azure AD Tenant* à partir d'un compte « global administrator ».
- une machine Windows 10 avec un utilisateur administrateur.
- installé le module *AzureADPreview* pour *Powershell*.
- déjà signé un contrat avec la fédération Edulog.

## 2.1 Procédure globale

| N° | Actions | But/Commentaire |
|---|---|---|
| 1 | Création d'une *Application* | Cette application est nécessaire pour y intégrer les attributs spécifiques pour Edulog. |
| 2 | Création des attributs Edulog | Ne peuvent être créés sur le portail *Azure*. |
| 3 | Création d'un utilisateur de test | Les attributs créés au point précédent ne sont visibles que si leur valeur est non-nulle. Ce point servira pour la validation. |
| 4 | Création d'une *Enterprise Application* | Cette application va servir de *SAML-endpoint*. |
| 5 | Création d'une *claim mapping policy* | C'est la définition des attributs qui sont envoyés depuis l'*Azure AD*. |
| 6 | Fédérer l'IdP créé et quelques utilisateurs de test | Pour pouvoir tester la fédération avec Edulog. |
| 7 | Tests internes de connexion | Servira à vérifier l'envoi des nouveaux attributs dans la requête SAML2. |

Toutes les actions peuvent se faire depuis *Powershell* en ligne de commande. Toutefois, dans ce rapport pour des raisons de visibilité, l'interface du portail *Azure* sera utilisée pour les points 1, 4, 5.

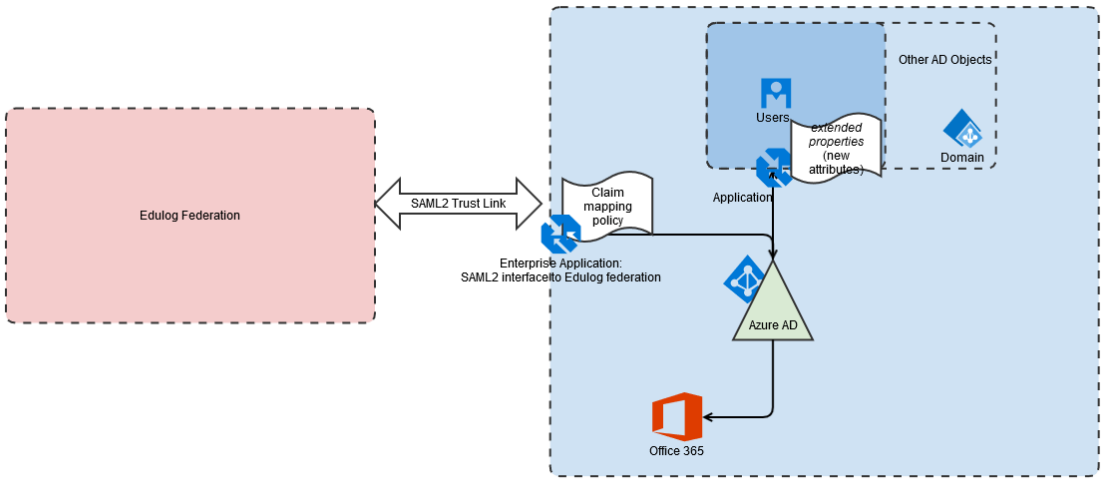
## 2.2 Remarques

*Azure AD* ne contient qu'un sous-groupe des attributs présents dans le schéma d'un *AD* local. Afin d'augmenter les attributs, il est possible d'utiliser Microsoft Graph ou Powershell.

Contrairement à *AD*, où les nouveaux attributs créés à partir d'une extension du schéma de l'*AD* sont visibles dans *Azure* (interface web), ici il faut utiliser les deux outils précédents pour les voir.

### 2.3 Eléments requis

Le schéma ci-dessous représente les éléments requis pour créer un IdP complet *Azure* pouvant se connecter à Edulog.




Azure AD Tenant as an IdP

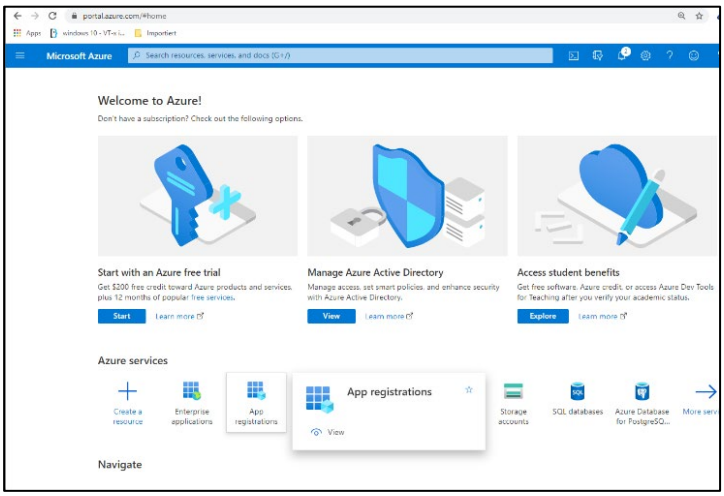
- Un *Azure AD Tenant*
- Une *application*
- Une *Enterprise application*
- Une *claim mapping policy*
- Les nouveaux attributs (*extended properties*) associés à l'application registration.

# 3. Création de l'*Application*

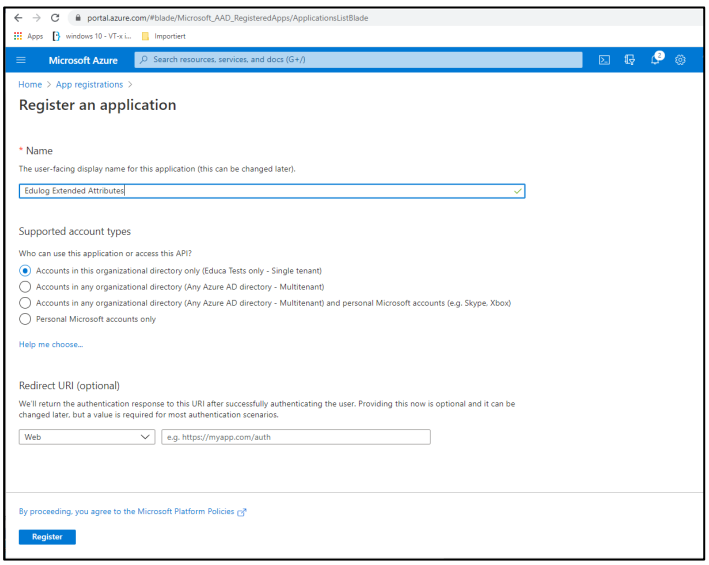
## 3.1 A travers le portail *Azure*

Se connecter à votre compte. Sélectionner le bon directory si nécessaire.

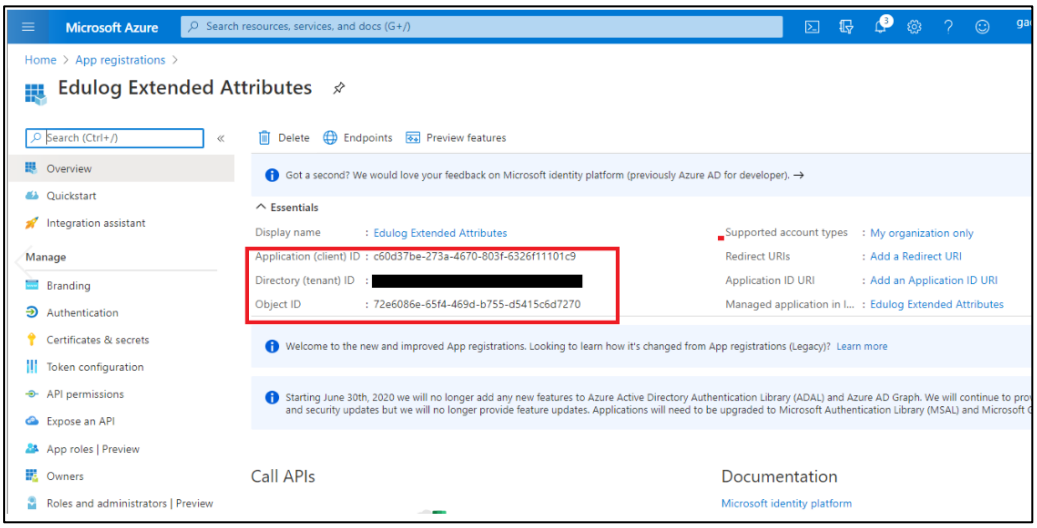
a. Aller à « Application registrations »




b. Nommer l'application (ici : « Edulog Extended Attributes »)



c. Noter l'« Object ID » de l'application




## 4. Création des attributs Edulog

Un script *Powershell* est utilisé. Il permet de :

- se connecter à notre *Azure AD Tenant* (et au directory utilisé, s'il y en a plusieurs)
- récupérer l'« Object ID » de l'application créée au point précédent (« Edulog Extended Attributes »)
- créer les attributs en utilisant la fonction **New-AzureADApplicationExtensionProperty**
- vérifier que les attributs sont correctement créés avec la fonction **Get-AzureADApplicationExtensionProperty**

```
# tenant-Anmeldung - wird Sie nach Benutzer und Passwort fragen
Connect-AzureAD -TenantId "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXX"

# Abrufen von Daten aus der Anwendung
$appregObjId=(Get-AzureADApplication -Filter "DisplayName eq 'Edulog Extended Attributes'").ObjectId

# Erstellen der neuen Edulog-Attribute
New-AzureADApplicationExtensionProperty -ObjectID $appregObjId -DataType "string" -Name "EdulogPersonBirthDate" -TargetObjects
@("User")
New-AzureADApplicationExtensionProperty -ObjectID $appregObjId -DataType "string" -Name "EdulogPersonRole" -TargetObjects @("User")
New-AzureADApplicationExtensionProperty -ObjectID $appregObjId -DataType "string" -Name "EdulogPersonLevel" -TargetObjects
@("User");
New-AzureADApplicationExtensionProperty -ObjectID $appregObjId -DataType "string" -Name "EdulogPersonCycle" -TargetObjects
@("User");
New-AzureADApplicationExtensionProperty -ObjectID $appregObjId -DataType "string" -Name "EdulogPersonCanton" -TargetObjects
@("User");
New-AzureADApplicationExtensionProperty -ObjectID $appregObjId -DataType "string" -Name "EdulogPersonTechID" -TargetObjects
@("User");

New-AzureADApplicationExtensionProperty -ObjectID $appregObjId -DataType "string" -Name "o" -TargetObjects @("User");
New-AzureADApplicationExtensionProperty -ObjectID $appregObjId -DataType "string" -Name "title" -TargetObjects @("User");

# Verifizierung von objectsId
Get-AzureADApplicationExtensionProperty -ObjectId $appregObjId

ObjectId                             Name                                                                    TargetObjects
--------                             ----                                                                    -------------
4721fc2d-f16a-40b9-80fe-HHHHHHHHHHHH extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_title                {User}
88648513-5a68-4542-8281-HHHHHHHHHHHH extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_o                    {User}
5c13622c-67cc-4b8f-9a0e-HHHHHHHHHHHH extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonTechID    {User}
3ee8a766-6c4a-47c2-aff0-HHHHHHHHHHHH extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonCanton    {User}
691e71d7-8c9e-4b49-b5c5-HHHHHHHHHHHH extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonCycle     {User}
e110281f-e087-4862-99c4-HHHHHHHHHHHH extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonLevel     {User}
bc7c04a4-52e7-402e-8274-HHHHHHHHHHHH extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonRole      {User}
0897a8ef-8b99-4dba-9a62-HHHHHHHHHHHH extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonBirthDate {User}
```

**La dernière commande *Get-AzureADApplicationExtensionProperty* montre les attributs « extended property ». Le nom de ceux-ci correspond au format suivant :**

extension_numero de l'ObjetId de l'application « Edulog Extended Attributes »_nom de l'attribut
Par exemple : *extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonTechID*
A noter que le format de l'« Object ID » ne contient pas le symbole « - »

## 5. Création d'un utilisateur de test

a. Créer un utilisateur de test (à travers l'interface *Azure* ou avec *Powershell*).
b. Ajouter des valeurs aux nouveaux attributs (uniquement avec *Powershell* ou *Microsoft Graph*), selon la syntaxe définie dans le document « Guide des attributs – fournisseur d'identité »[1]

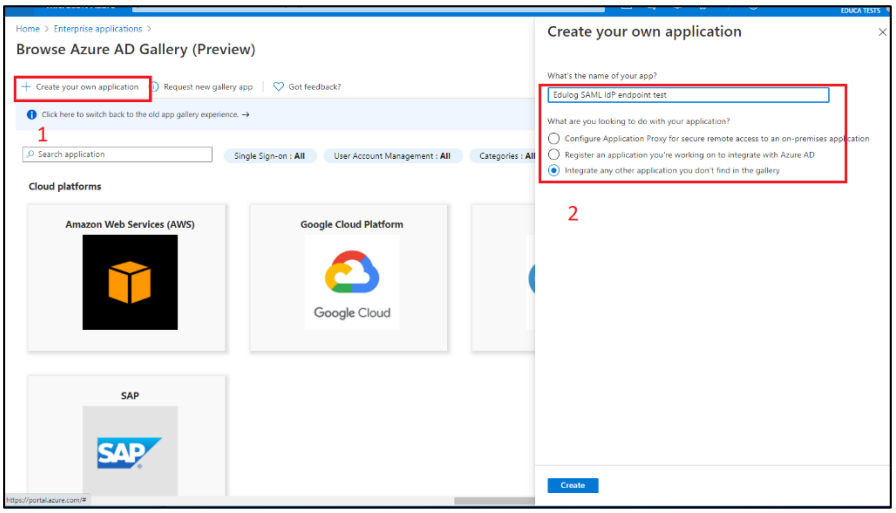
```
# Creation d'un utilisateur

$PasswordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile

$PasswordProfile.Password = "Ceciestunmotdep4sse"

New-AzureADUser -DisplayName "Isabelle Rochat" -PasswordProfile $PasswordProfile
-UserPrincipalName "Isabelle.Rochat@educatests.ch" -AccountEnabled $true -Givenname
"Isabelle" -Surname "Rochat" -PreferredLanguage "fr-CH"  -MailNickName "Newuser"

# Ajouter des valeurs des extended attributes à l'utilisateur

Set-AzureADUserExtension -ObjectId Isabelle.Rochat@educatests.ch -ExtensionName
"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonBirthDate" -ExtensionValue
"19700101"

Set-AzureADUserExtension -ObjectId Isabelle.Rochat@educatests.ch -ExtensionName
"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonRole" -ExtensionValue
"teacher##principal##technician"

Set-AzureADUserExtension -ObjectId Isabelle.Rochat@educatests.ch -ExtensionName
"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonLevel" -ExtensionValue
"primary##secondary1##secondary2"

Set-AzureADUserExtension -ObjectId Isabelle.Rochat@educatests.ch -ExtensionName
"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonCycle" -ExtensionValue
"1##2##3"

Set-AzureADUserExtension -ObjectId Isabelle.Rochat@educatests.ch -ExtensionName
"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonCanton" -ExtensionValue "VD"

Set-AzureADUserExtension -ObjectId Isabelle.Rochat@educatests.ch -ExtensionName
"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonTechID" -ExtensionValue
"110e8400-e29b-11d4-a716-446655440007"

Set-AzureADUserExtension -ObjectId Isabelle.Rochat@educatests.ch -ExtensionName
"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_o" -ExtensionValue "Gymnase de Beaulieu"

Set-AzureADUserExtension -ObjectId Isabelle.Rochat@educatests.ch -ExtensionName
"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_title" -ExtensionValue "Enseignant
maths"
```

[1]Disponible sous : https://edulog.ch/fr/adhesion/documentation

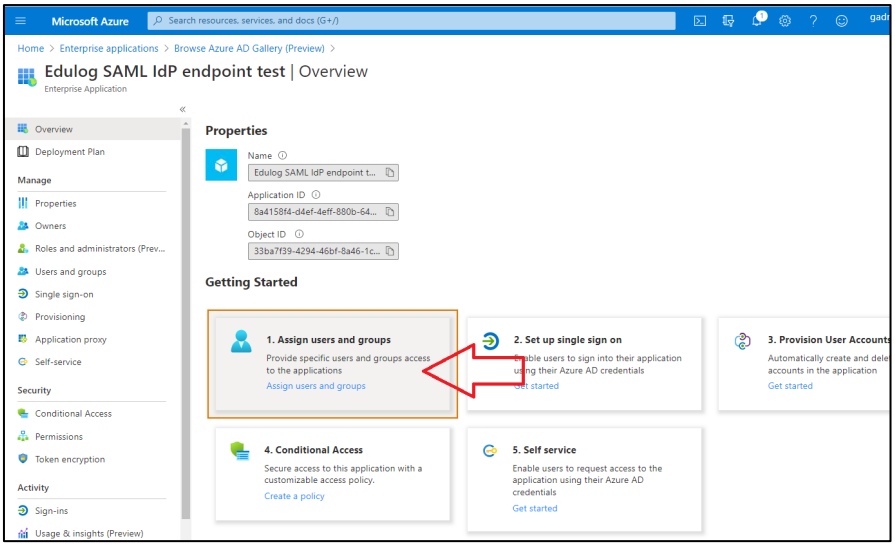
## 6. Création d'une *Enterprise Application*

Azure distingue les *Applications* des *Enterprise Applications*. L'*Application* peut recevoir les nouveaux attributs, alors que l'*Enterprise Application* permet de mettre en place la connexion SAML de la façon recherchée par Edulog.

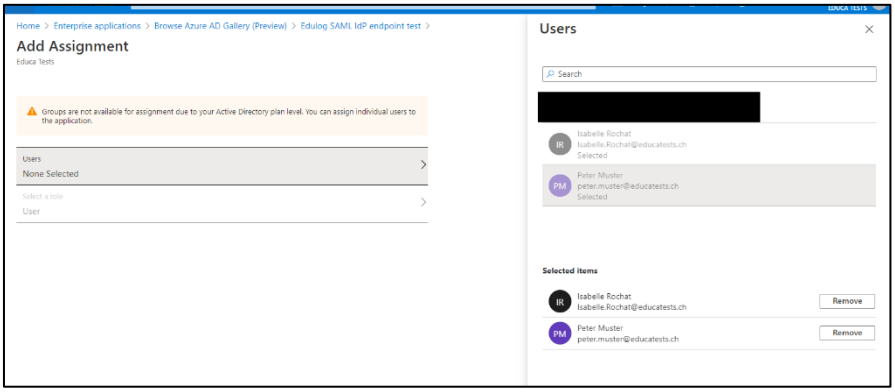
a. Aller dans *Enterprise Application* et sélectionner « Create your own application »
b. Nommer l'application. Ici « Edulog SAML IdP endpoint test »



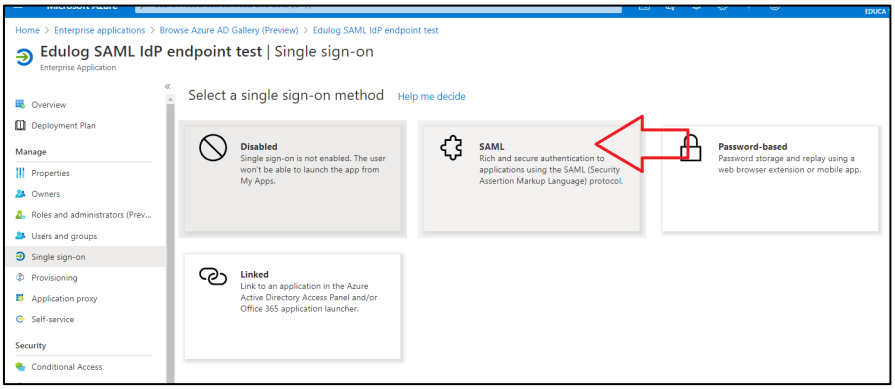

c. Configurer l'*Enterprise Application*



2. Sélectionner les utilisateurs ou les groupes qui vont pouvoir utiliser l'interface SAML que l'on crée.[2]

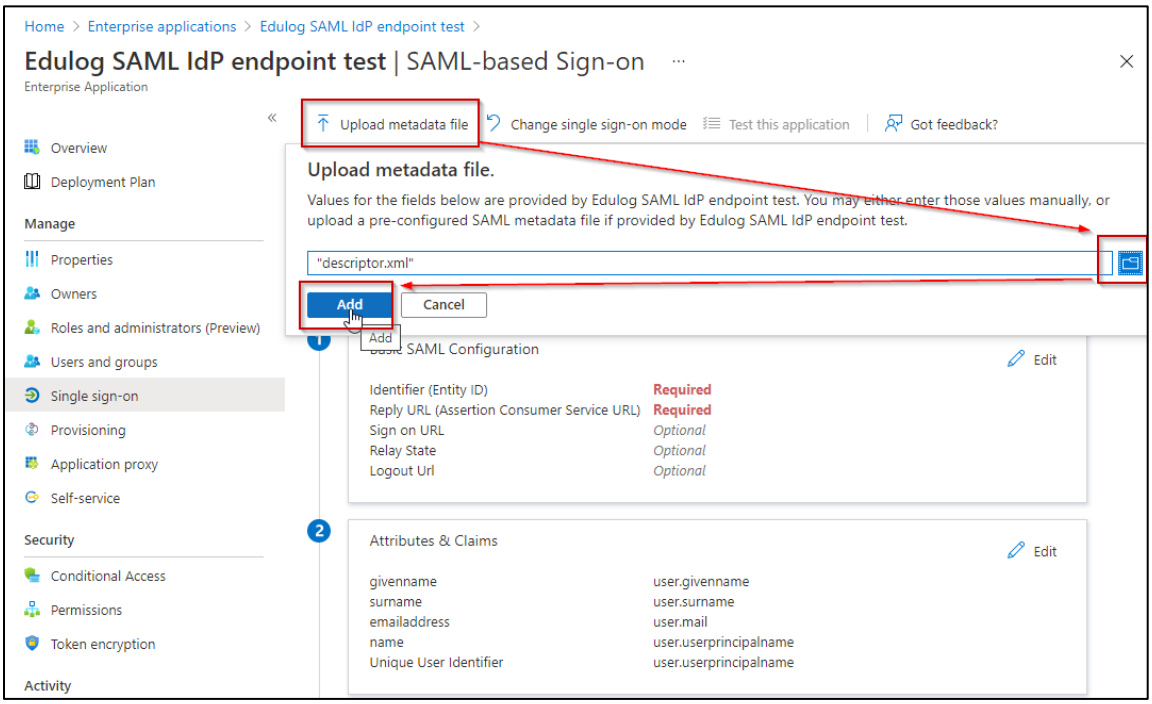



3. Valider la sélection sur le bouton « Assign » en bas à gauche.




[2] Des opérations sur des groupes ou des ensembles d'utilisateurs peuvent être menées.

5. Importer les métadonnées transmises par ELCA AG




- « Identifier (Entity ID) »
  - (p.ex. https://go.edulog.ch/auth/realms/edulog)
- « Reply URL (Assertion Consumer Service URL) »
  - (p.ex. https://go.edulog.ch/auth/realms/edulog/broker/school-idp/endpoint)
- « Logout Url »
  - (p.ex. https://go.edulog.ch/auth/realms/edulog/edulog-api/logout)

Finalement, sauvegarder la configuration : Save

## 7. Création d'une *claim mapping policy*

Il n'est pas possible de sélectionner les nouveaux attributs pour Edulog afin de configurer la partie « User Attributes & Claims » dans la configuration « SAML-based sign-on » de l'*Enterprise Application* nouvellement créée.[3]

A cet effet, il faut créer une *claim mapping policy* sous *Powershell* (ou *Microsoft Graph*) qui permettra de définir les attributs envoyés dans la *SAML-response* de l'IdP qui a été défini. Il est ensuite possible de sélectionner les attributs (« extended ») pour Edulog et leur faire correspondre le nom souhaité de façon à être identifié par Edulog.

Voici comment créer une telle *policy* que l'on appellera : ClaimsEdulog.

Il faut utiliser la commande **New-AzureADPolicy**.

```
New-AzureADPolicy -Definition
@('{"ClaimsMappingPolicy":{"Version":1,"IncludeBasicClaimSet":"false","ClaimsSchema
": [

{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPe
rsonBirthDate","SamlClaimType": "EdulogPersonBirthDate"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPe
rsonRole","SamlClaimType": "EdulogPersonRole"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPe
rsonLevel","SamlClaimType": "EdulogPersonLevel"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPe
rsonCycle","SamlClaimType": "EdulogPersonCycle"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPe
rsonCanton","SamlClaimType": "EdulogPersonCanton"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPe
rsonTechID","SamlClaimType": "EdulogPersonTechID"},

{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_o","Saml
ClaimType": "o"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_title","
SamlClaimType": "title"},
{"Source":"user","ID":"UserPrincipalName","SamlClaimType": "mail"},
{"Source":"user","ID":"UserPrincipalName","SamlClaimType": "uid"},
{"Source":"user","ID":"PreferredLanguage","SamlClaimType": "preferredLanguage"},
{"Source":"user","ID":"Surname","SamlClaimType": "sn"},
{"Source":"user","ID":"Givenname","SamlClaimType": "givenName"}]}}') -DisplayName
"ClaimsEdulog" -Type "ClaimsMappingPolicy"
```

Selon Azure, le mot-clé *ExtensionID* est utilisé pour identifier les *extended attributes*. Dans le cas des attributs qui existent dans *Azure AD*, sélectionnez le mot-clé *ID*.

Le premier nom correspond au nom de l'attribut dans *Azure AD* (par ex. : extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_title). Le second, situé après *SamlClaimType*, correspond au nom de l'attribut dans la *SAML-response* d'*Azure* à Edulog.

Pour vérifier la création de la *policy*, utiliser la commande : **Get-AzureADPolicy.**

L'identifiant unique de la *policy* sera de la forme : ZZZZZZZZ-ZZZZ-ZZZZ-ZZZZ-ZZZZZZZZZZZZ

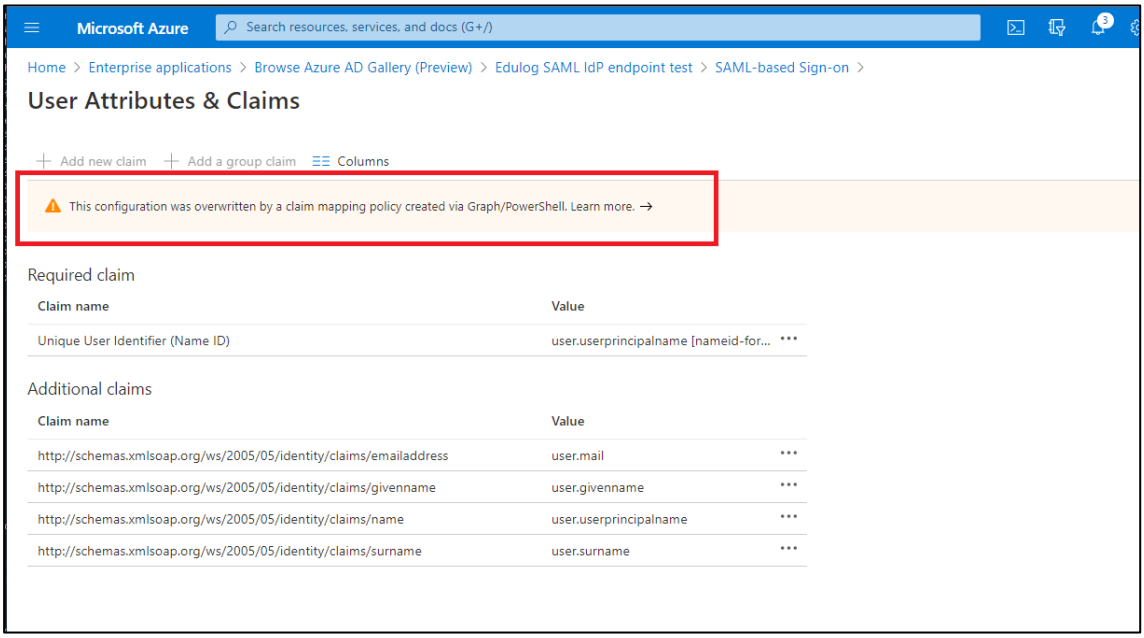
[3] Cela ne fonctionne qu'avec une infrastructure hybride contenant un *AD* local dont le schéma a été changé et propagé dans *Azure* avec *AD Connect Sync*.

Finalement, il faut maintenant associer la *claim mapping policy* à l'*Enterprise Application* créée antérieurement. Pour cela, utiliser la commande : **Add-AzureADServicePrincipalPolicy** :

> *Add-AzureADServicePrincipalPolicy -Id YYYYYYYY-YYYY-YYYY-YYYY-YYYYYYYYYYYY -RefObjectId ZZZZZZZZ-ZZZZ-ZZZZ-ZZZZ-ZZZZZZZZZZZZ*

**RefObjectId** est l'identifiant unique (« ObjectID ») de la *policy* et **Id** est l'identifiant unique de l'*Enterprise Application* créée.[4]

Vérifier la présence de la *claim mapping policy* dans l'*Enterprise Application* en allant sur le point de configuration « User Attributes & Claims ». Un message indique que la configuration a été réalisée par ladite *policy*.



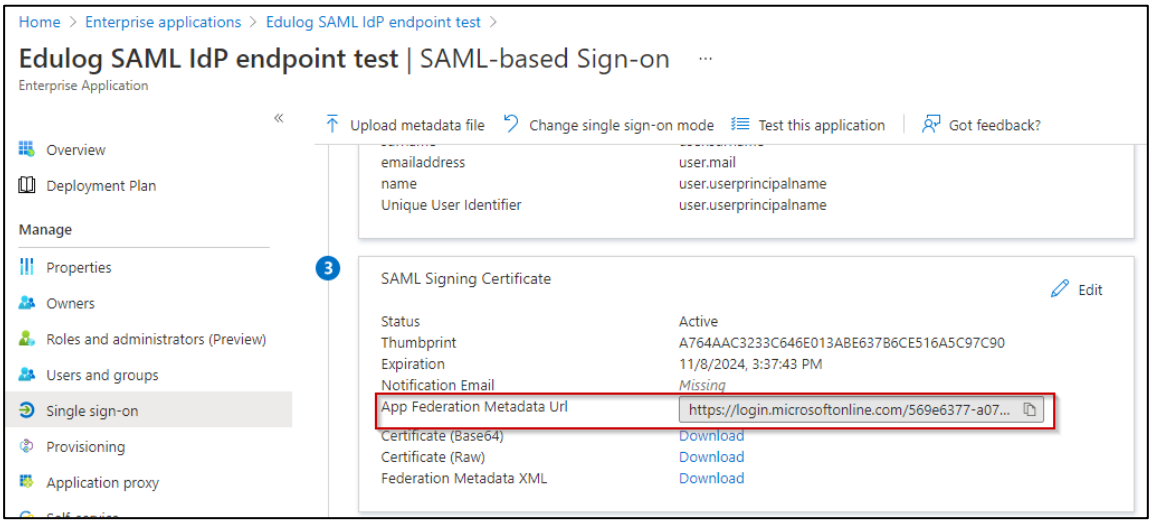

[4] Il ne semble pas possible d'associer une *claim mapping policy* à une *application* simple.

## 8. Fédérer l'IdP et des utilisateurs de test

a. Fédérer l'IdP Azure

Pour cela il faut récupérer l'URL des métadonnées de l'Entreprise Application créée (App Federation Metadata URL)

Envoyer cette URL au service technique d'ELCA AG (entreprise responsable de l'exploitation technique de la Fédération). ELCA fédérera alors l'IdP et fournira les informations nécessaires pour effectuer l'étape du point 6. c)5. de ce document.




b. Fédération d'un ou plusieurs utilisateurs de test

Pour effectuer les opérations de fédération, des API sont disponibles. Leur fonctionnement est décrit dans le document « Edulog API reference » fourni par le secrétariat Edulog.

Pour automatiser l'*onboarding* avec les API, les possibilités sont :

- Utiliser SCIM sous Azure (voir le document « Guide Azure AD SCIM »)[5] ;
- Utiliser un produit type Postman ;
- Fédérer les utilisateurs en utilisant les scripts PowerShell mis à disposition par le secrétariat Edulog.

Une fois ces deux opérations réalisées (fédération de l'IdP, et d'au moins un utilisateur de test), il est possible de tester la connexion.

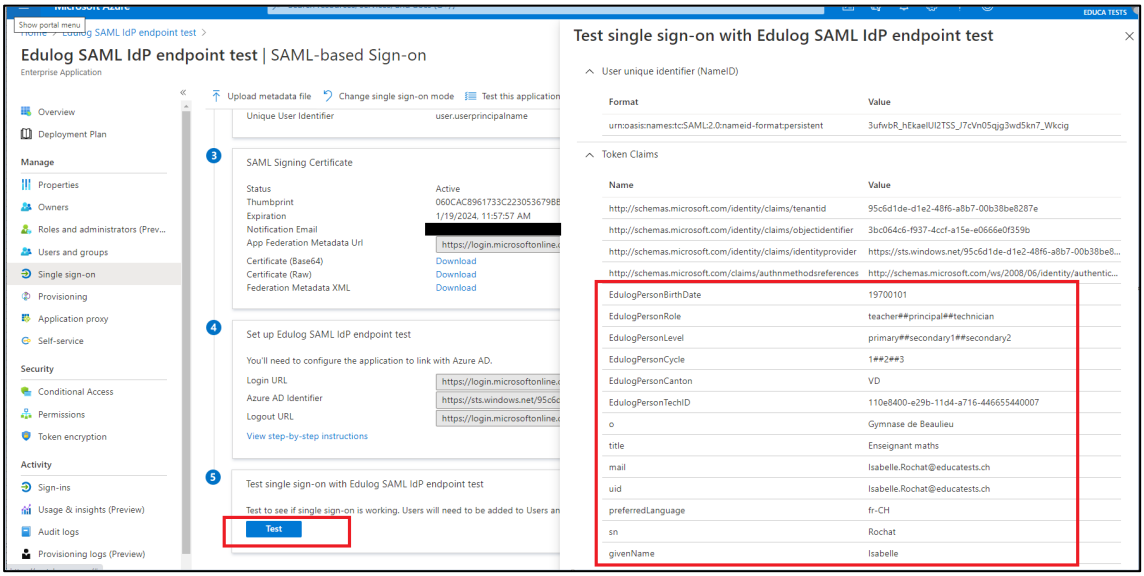
[5] Disponibles sous https://edulog.ch/fr/adhesion/documentation

## 9. Tests internes de connexion

Il est possible de vérifier les attributs envoyés par l'*Enterprise Application* créée, en utilisant une fonction d'*Azure* qui simule la connexion depuis un SP interne. Cette fonction se trouve dans le menu de l'application :

« Single sign-on » → « SAML » → « 5 Test single sign-on with … »

Sur la droite, un menu permet la connexion avec l'utilisateur de test (ici, *Isabelle.Rochat@educatests.ch*). Suite à l'authentification correcte, on verra une liste des attributs envoyés dans la *SAML-response*[6]. Vérifier que les attributs correspondent avec ceux qui ont été assignés à cet utilisatrice au point 5 de ce document.




## 10. Tests avec Edulog

Remarque : si cela n'a pas été fait au point 8, il faudra revenir sur le point 6 pour modifier le « Reply URL (Assertion Consumer Service URL) » selon les instructions de l'entreprise responsable de l'exploitation technique ELCA.

## 11. Annexe : Commandes utiles powershell

Il convient de se familiariser avec quelques commandes powershell pour la gestion des policy. En particulier : Remove-AzureADPolicy, New-AzureADPolicy, Get-AzureADPolicy.

[6] Appelés *Token claims* sous *Azure*.