Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNIQUE

Configuration d'un *tenant Microsoft Entra ID* en tant qu'IdP – SAML

2.2025 – Version 2.3

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 configurer un *tenant Entra ID* en tant que fournisseur d'identité (IdP) pour Edulog à l'aide d'une configuration *SAML Trust*.

Il contient toutes les étapes de configuration de la connexion SAML (§3-4) et du déploiement SCIM (§5). Ces étapes doivent être effectuées d'abord pour l'environnement d'intégration d'Edulog (INT) et ensuite pour l'environnement de production (PROD).

2. Prérequis

Vous devez disposer d'un compte administrateur dans votre *Microsoft Entra admin center*.

Les attributs suivants sont requis par Edulog:

Nom de l'attribut Edulog	Description	Commentaire
uid	Identification de l'utilisateur: il s'agit de la valeur utilisée par les utilisatrices et utilisateurs pour se connecter.	Dans Entra, il s'agit généralement du *userPrincipalName*
givenName	Prénom	
sn	Nom	
mail	Adresse courriel	
EdulogPersonBirthDate	Date de naissance au format AAAAMMJJ	
preferredLanguage	Langue préférée, parmi les valeurs suivantes: *de-CH, fr-CH, it-CH, rm-CH, en*	Selon le contexte de l'IdP, cette valeur peut être identique pour toutes les utilisatrices et tous les utilisateurs.
title	Fonction, non applicable aux élèves	
EdulogPersonRole	Rôle(s) principal(aux) parmi les valeurs suivantes: *pupil, teacher, administration, principal, legal_guardian, technician, other*	
EdulogPersonLevel	Degré(s) d'enseignement parmi les valeurs suivantes: *primary, secondary1, secondary2, tertiary*	
EdulogPersonCycle	Cycle(s) parmi les valeurs suivantes: *0, 1, 2, 3*	
EdulogPersonCanton	Code à deux lettres du canton (par ex. *VD, BE, GE, ZH*)	Cette valeur est probablement la même pour toutes les utilisatrices et tous les utilisateurs d'un IDP.
o	Organisation ou institution	

Pour plus de détails sur chaque attribut, consultez le «Guide des attributs - fournisseur d'identité» dans la documentation Edulog.

3. Création des attributs Edulog

Remarque: cette configuration s'effectue dans le *Microsoft Entra admin center*.

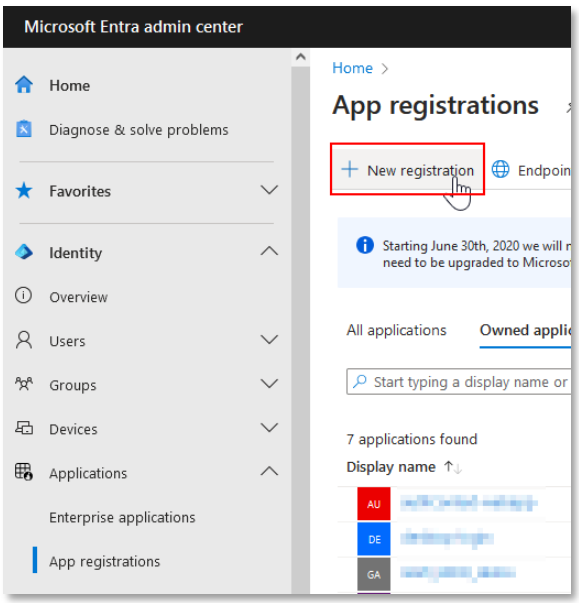
Si certains des attributs attendus par Edulog ne sont pas déjà présents dans votre *Entra tenant* en tant qu'attributs utilisateur, vous pouvez les créer en tant qu'attributs supplémentaires ou «attributs d'extension». Les paragraphes 3.1 à 3.3 décrivent la création des attributs suivants:

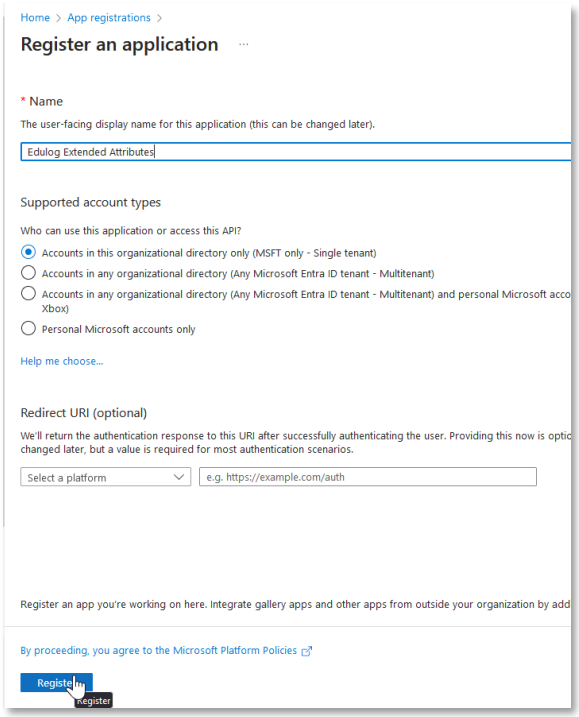
1. *EdulogPersonBirthDate*
2. *EdulogPersonRole*
3. *EdulogPersonLevel*
4. *EdulogPersonCycle*
5. *EdulogPersonCanton*
6. o
7. *title*

Si certains de ces attributs sont déjà présents dans votre *tenant* (sous un autre nom), vous pouvez supprimer les lignes correspondantes des scripts.

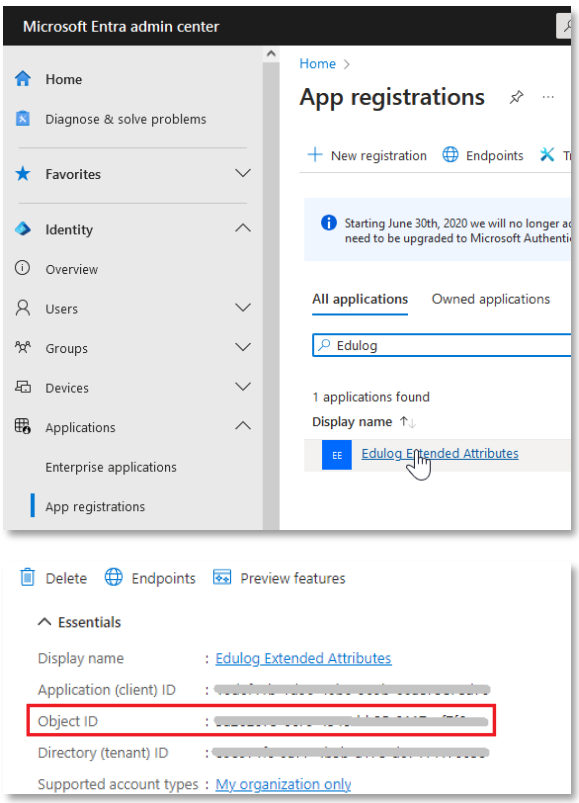
3.1 Création de l'application d'attributs d'extension

Dans le *Microsoft Entra admin center* allez sur *Identity* > *Applications* > *App registrations*. Enregistrez une nouvelle application (*New registration* > *Name «Edulog Extended Attributes»* > *Register*).





Après avoir cliqué sur «Register», vous serez redirigé vers la liste des applications. Notez l'ID de l'objet, vous en aurez besoin au paragraphe 3.2.



Pour trouver les applications enregistrées, recherchez «Edulog Extended Attributes» sous *Identity* > *Applications* > *App registrations* > *All applications*.

3.2 Script pour l'ajout d'attributs

Dans Powershell, vérifiez d'abord si le module AzureAD est disponible et importé, et installez-le si nécessaire.

```
# Check if Module is available and imported
Get-Module -Name AzureAD


# if no output is shown install and import the module AzureAD
Install-Module AzureAD -Scope CurrentUser
Import-Module AzureAD
```

Exécutez le script Powershell comme suit:

```
# tenant login - will ask for username and password
Connect-AzureAD -TenantId "<Tenant ID>"

# Retrieving data from the application
$appregObjId=(Get-AzureADApplication -Filter "DisplayName eq 'Edulog Extended
Attributes'").ObjectId

# Creating the new Edulog attributes
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 "o" -TargetObjects @("User");
New-AzureADApplicationExtensionProperty -ObjectID $appregObjId -DataType
"string" -Name "title" -TargetObjects @("User");

# Verification of objectsId
Get-AzureADApplicationExtensionProperty -ObjectId $appregObjId
```

La commande `Get-AzureADApplicationExtensionProperty` affiche les nouvelles propriétés de l'extension au format *extension_<appID>_<attribute name>*.

3.3 Création d'un utilisateur test

Vous pouvez utiliser le script Powershell suivant pour créer un utilisateur test, en suivant les informations du «Guide des attributs - fournisseurs d'identité» pour le format de chaque valeur.

```
# Add values to the user extended attributes
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "ex-
tension_<appID>_EdulogPersonBirthDate" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "ex-
tension_<appID>_EdulogPersonRole" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "ex-
tension_<appID>_EdulogPersonLevel" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "ex-
tension_<appID>_EdulogPersonCycle" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "ex-
tension_<appID>_EdulogPersonCanton" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "ex-
tension_<appID>_o" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "ex-
tension_<appID>_title" -ExtensionValue <value>
```

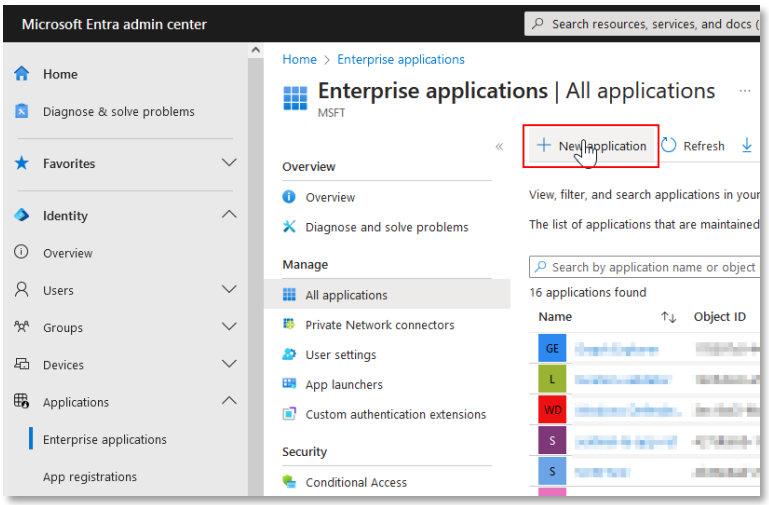
Exemples d'attributs:

EdulogPersonBirthDate	20120119
EdulogPersonRole	pupil
EdulogPersonLevel	primary
EdulogPersonCycle	1
EdulogPersonCanton	VD
o	Ecole primaire de la Vallée##Institut Brenet
title	étudiante

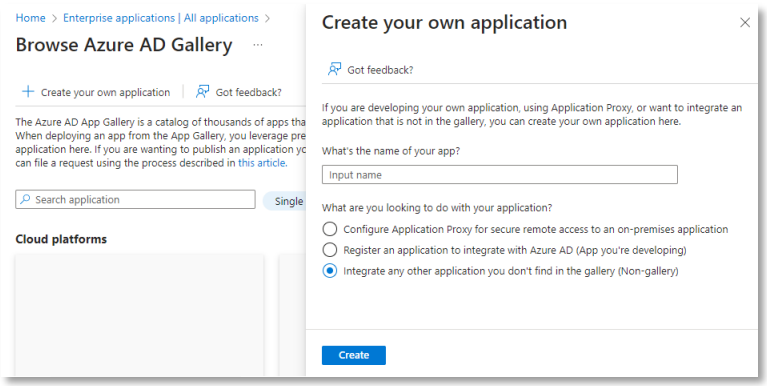
4. Création et configuration de l'application Edulog

4.1 Création d'une application *Enterprise*

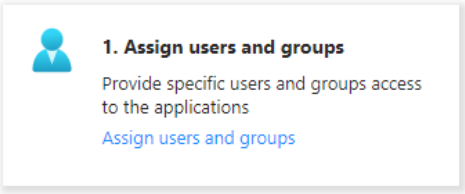
1. Allez sur *Identity > Applications > Enterprise applications*.



2. Cliquez sur *New Application* > *Create your own application* > *Integrate any other application you don't find in the gallery (Non-gallery).*



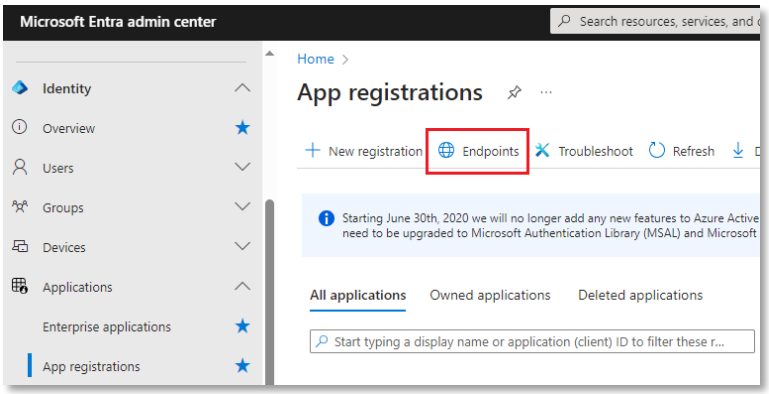
3. Saisissez un nom et cliquez sur «Create».



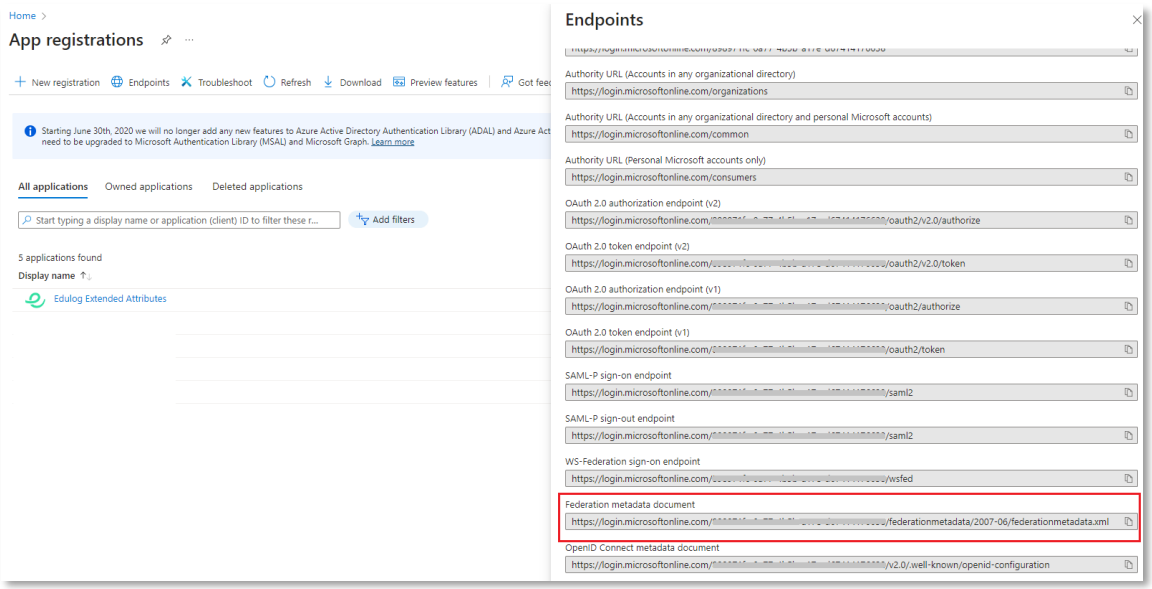
4. Attribuez les utilisateurs test à l'application créée.

4.2 Métadonnées SAML de l'application

Les métadonnées SAML de l'application sont disponibles dans *Identity* > *Applications* > *App registrations* > *Endpoints* > *Federation metadata document*.

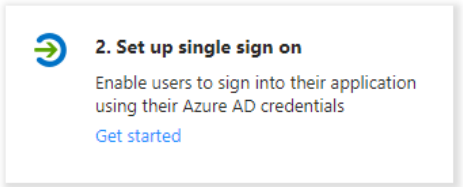


Envoyez le lien vers ce document XML (voir illustration ci-dessous) à ELCA, responsable de l'exploitation technique et de l'onboarding: onboarding_edulog@elca.ch.

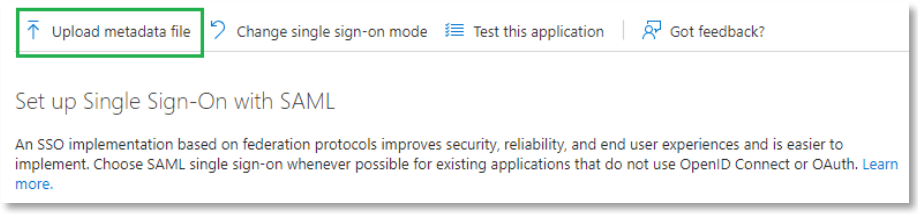


4.3 Configuration de l'authentification unique

Retournez à l'application dans *Identity > Applications > Enterprise applications* et sélectionnez «Set up single sign on» dans l'onglet «Overview» de l'application.



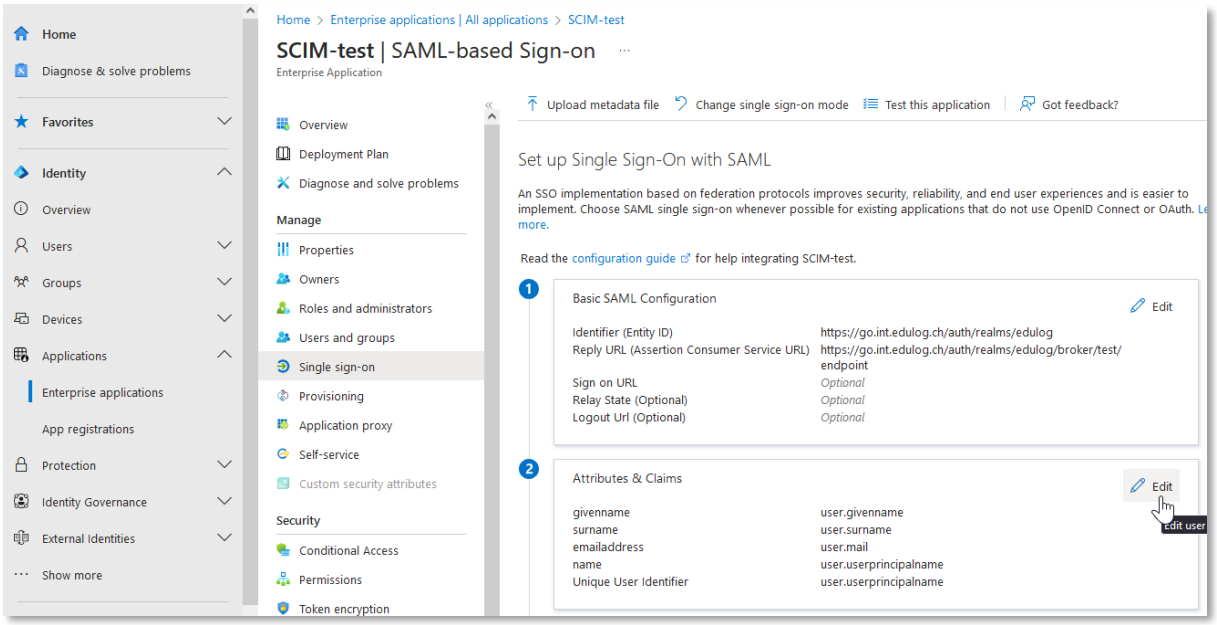
Sélectionnez «SAML», puis téléversez le fichier de métadonnées validé par l'équipe d'onboarding d'Edulog.

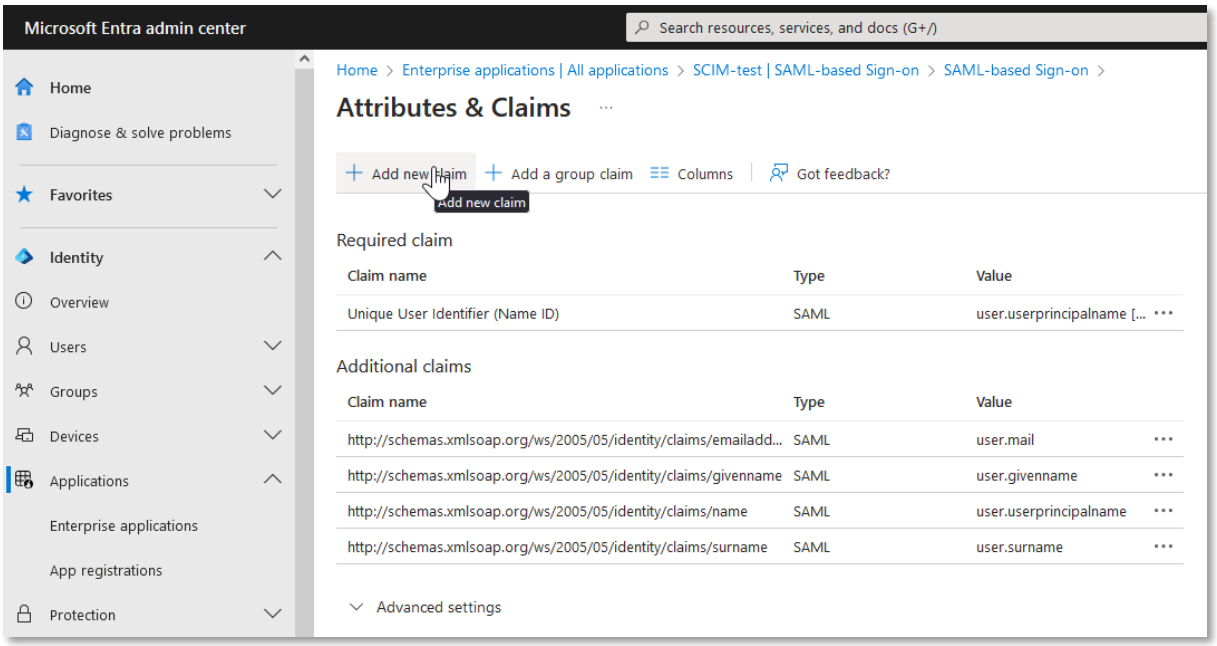


Cela remplit les URL pour la configuration SAML de base:

	Exemple INT	Exemple PROD
Identifier (Entity ID)	https://go.int.edulog.ch/auth/realms/edulog	https://go.edulog.ch/auth/realms/edulog
Reply URL (Assertion Consumer Service URL)	https://go.int.edulog.ch/auth/realms/edulog/broker/<idp name>/endpoint	https://go.edulog.ch/auth/realms/edulog/broker/<idp name>/endpoint
Logout URL (optionnel)	https://go.int.edulog.ch/auth/realms/edulog/broker/<idp name>/endpoint	https://go.edulog.ch/auth/realms/edulog/broker/<idp name>/endpoint

Pour la configuration de «Attributes & Claims», ajoutez les attributs qui seront envoyés à Edulog.



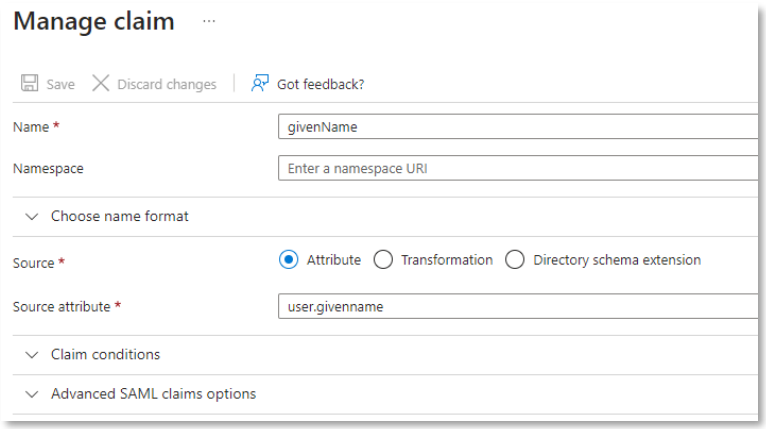


Tous les attributs mentionnés au §2 Prérequis doivent être configurés. On distingue les trois cas suivants:

a. Attributs qui existaient déjà dans votre *tenant* (en général: *uid*, *givenName*, *sn*, *title*)
b. Attributs ajoutés en tant qu'attributs d'extension au §3 (en général: *EdulogPerson-BirthDate*, *EdulogPersonRole*, *EdulogPersonLevel*, *EdulogPersonCycle*)
c. Attributs identiques pour chaque utilisatrice et utilisateur (en général: *preferredLan-guage*, *o*, *EdulogPersonCanton*)

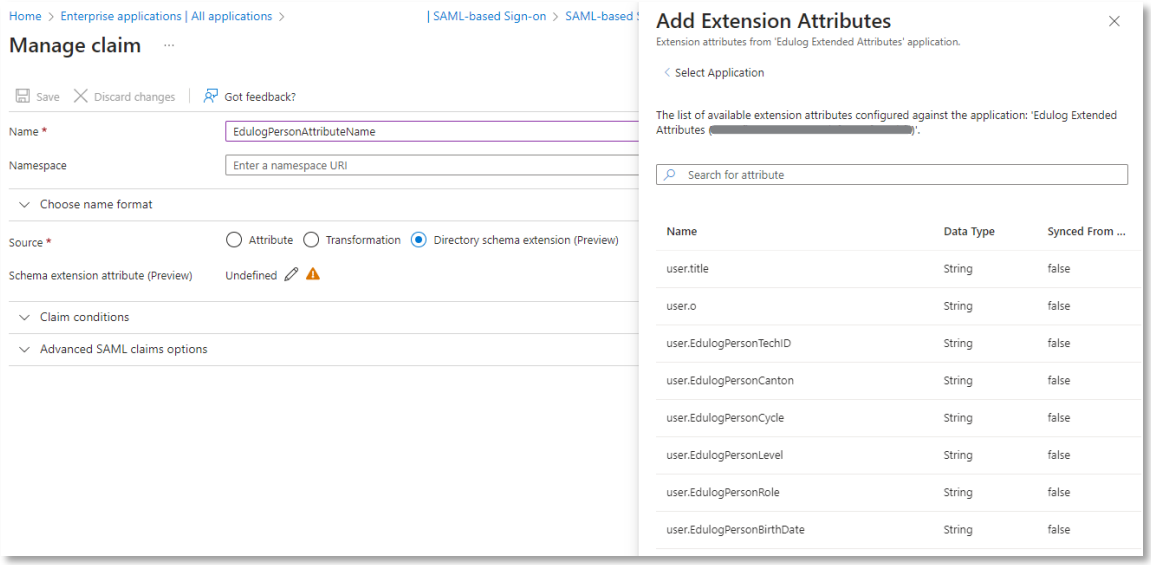
a. Attributs déjà existants

Vous pouvez configurer les attributs déjà existants comme décrit ci-dessous, en associant le nom de l'attribut Edulog (dans le champ «Name») au «Source attribute» correspondant (laissez le «Namespace» vide).



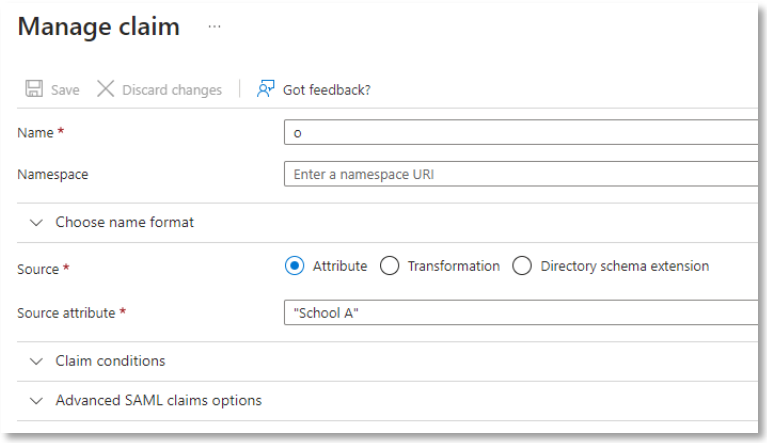
b. Attributs d'extension

Pour chaque attribut d'extension, sélectionnez la «Directory schema extension» correspondante de l'application d'attributs d'extension que vous avez créée à l'étape précédente, comme indiqué ci-dessous.



c. Attributs constants

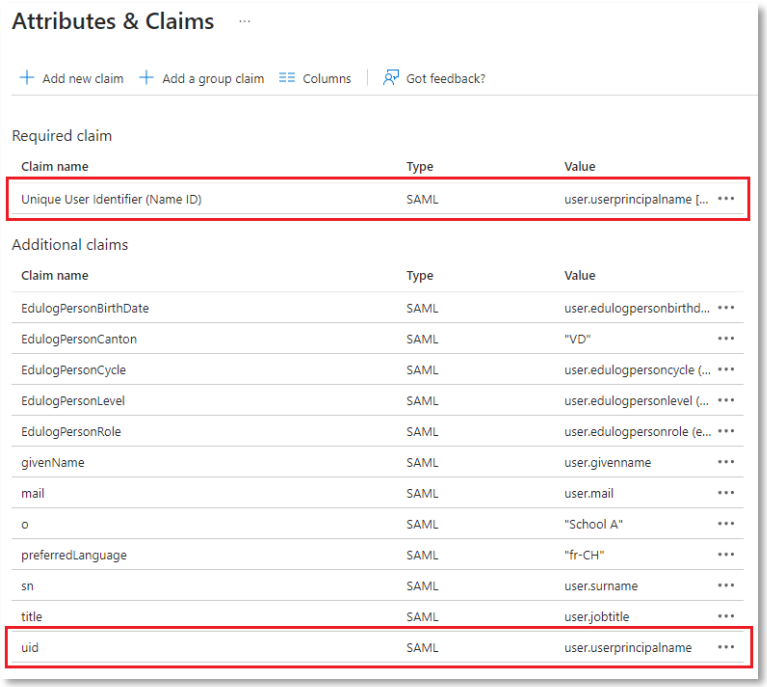
Les attributs qui ont la même valeur pour chaque utilisatrice et utilisateur peuvent être définis sur une valeur constante, comme illustré ci-dessous.



d. Identifiant unique (SAML nameID)

Le protocole SAML utilise un attribut spécial appelé «nameID» pour identifier les utilisatrices et utilisateurs de manière univoque. Vous trouverez cet attribut dans vos attributs sous «Unique User Identifier». Assurez-vous que la valeur de l'attribut correspond à l'attribut «uid».

Dans l'exemple suivant, nous utilisons le «userPrincipalName» comme valeur pour les deux requêtes.



5. Configuration du déploiement automatique des utilisatrices et utilisateurs (avec SCIM)

Pour configurer la mise à disposition automatique dans *Entra ID*, vous devez enregistrer le numéro AVS de vos utilisatrices et utilisateurs dans l'un des attributs d'Entra. Cela peut se faire soit dans un attribut d'extension (comme au §3.1), soit dans un autre attribut non utilisé (par exemple l'identifiant de l'employé ou le numéro de fax si l'un de ces attributs n'est pas utilisé par votre organisation).

5.1 Obtention d'un jeton SCIM

Vous trouverez la documentation complète dans le guide «Edulog API reference». Les étapes pertinentes y sont décrites en détail.

Conditions préalables: nom d'utilisateur et mot de passe de l'utilisateur de l'API, qui vous ont été communiqués par l'équipe d'onboarding d'Edulog.

Avec Powershell, interrogez l'API Edulog pour obtenir un jeton à l'aide de la commande:

```
$body = @{
              grant_type = "password"
              client_id = "federation"
              username = "<username>"
              password = "<password>"
              scope = "offline_access"
       }
Invoke-RestMethod -Method Post -Uri https://<authdomain>/auth/realms/edu-
log/protocol/openid-connect/token -Body $body
```

`<username>` und `<password>` doivent être remplacés par les informations de connexion de votre utilisateur API.
`<authdomain>` doit être remplacé par:

- `go.int.edulog.ch` (INT)
- `go.edulog.ch` (PROD)

Vous recevez une réponse d'Edulog sous la forme suivante:

```
access_token       : <access token>
expires_in         : 60
refresh_expires_in : 34560000
refresh_token      : <refresh token>
token_type         : Bearer
not-before-policy  : 0
session_state      : …
scope              : offline_access
```

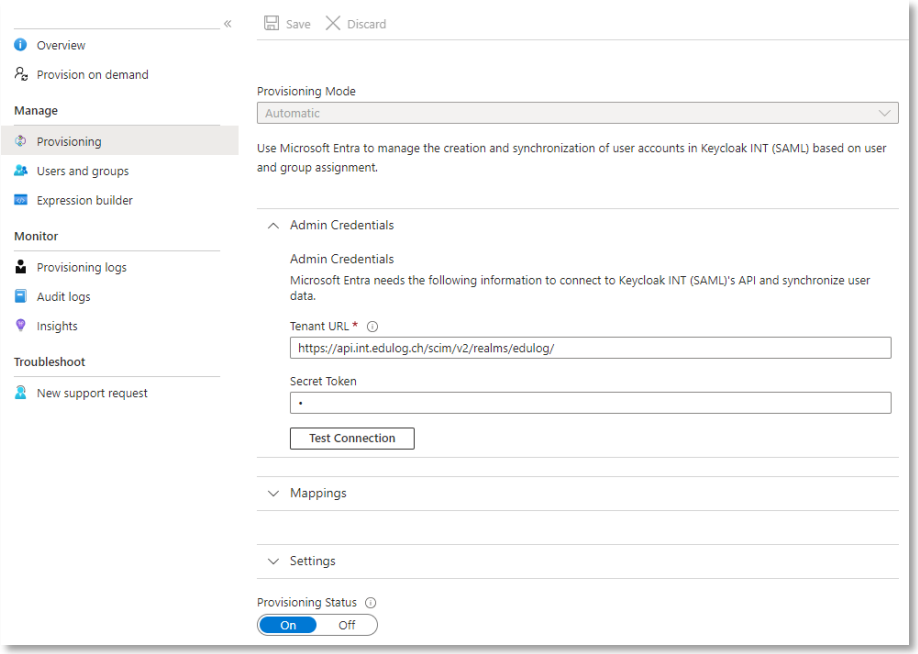
Copiez le `<refresh token>`, en veillant à supprimer les espaces.

Attention: Le *<refresh_token>* est une valeur sensible (tout comme le mot de passe de l'API) car il donne à son propriétaire un accès permanent à l'API SCIM d'Edulog. Si vous le cochez dans un emplacement intermédiaire avant de l'importer dans Entra, assurez-vous de le supprimer correctement par la suite.

5.2 Configuration dans *Entra ID*

5.2.1 Connexion

Sous *Entra ID > Enterprise applications* > *your Edulog application* > *Provisioning*, configurez les «Admin Credentials» comme indiqué ci-dessous.



«Tenant URL»:

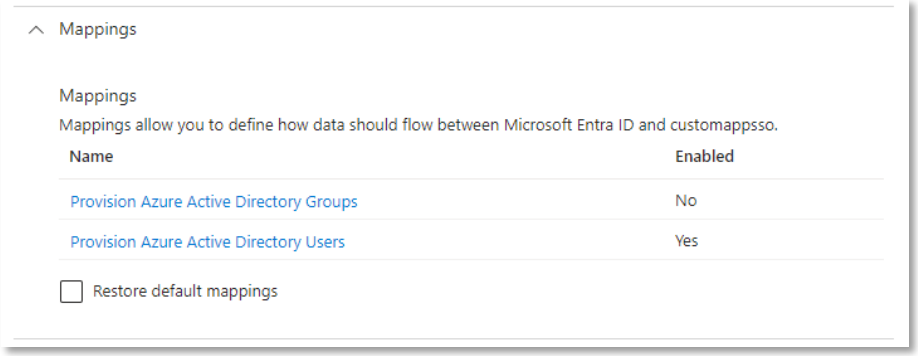
- https://api.int.edulog.ch/scim/v2/realms/edulog/ (INT)
- https://api.edulog.ch/scim/v2/realms/edulog/ (PROD)

«Secret token»: le jeton d'actualisation que vous avez copié à l'étape précédente (§5.1).

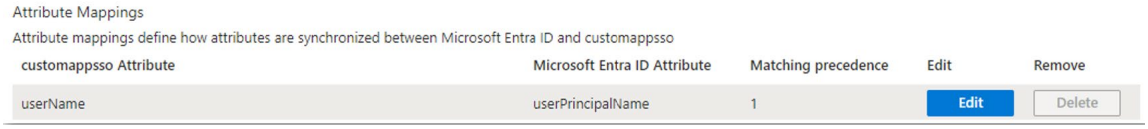
Pour tester la connexion, cliquez sur le bouton «Test Connection».

5.2.2 Mappages

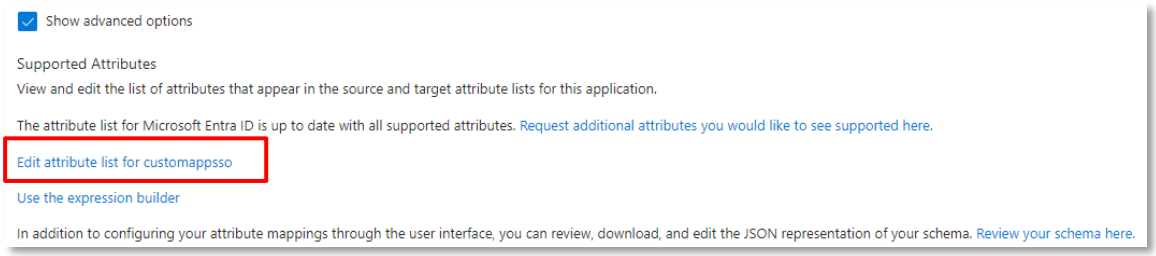
Vous allez provisionner des utilisateurs et non des groupes. Par conséquent, désactivez les «Groups Mappings» en définissant le statut de «Provision Azure Active Directory Groups» sur «No».



Cliquez sur les «Users Mappings» et supprimez tous les mappages existants sauf «userPrincipalName»:



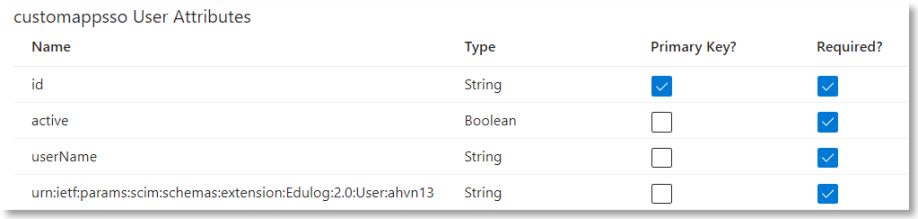
Cliquez sur la case à cocher «Show advanced options» et naviguez vers «Edit attribute list for customappsso».



Dans la liste des attributs:

1. Cochez la case «required» pour l'attribut «active».
2. Ajoutez un nouvel attribut:

   Name: urn:ietf:params:scim:schemas:extension:Edulog:2.0:User:ahvn13
   Type: String
   Cochez la case « Required ? ».

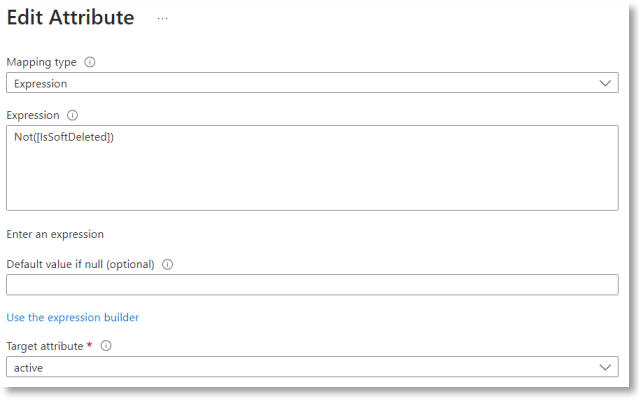


3. Enregistrez les modifications.

Ajoutez les mappages suivants:

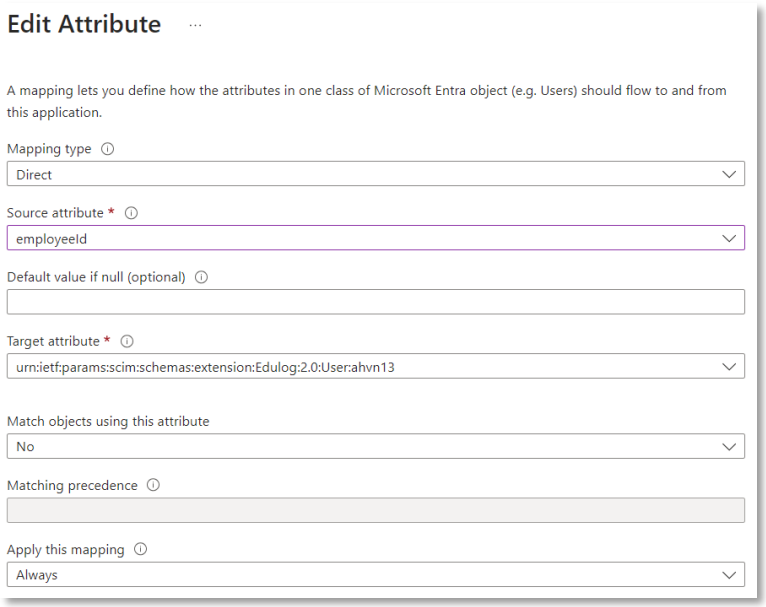
1. Mapping type: Expression

   «Expression»: *Not([IsSoftDeleted])*
   «Target attribute»: *active*

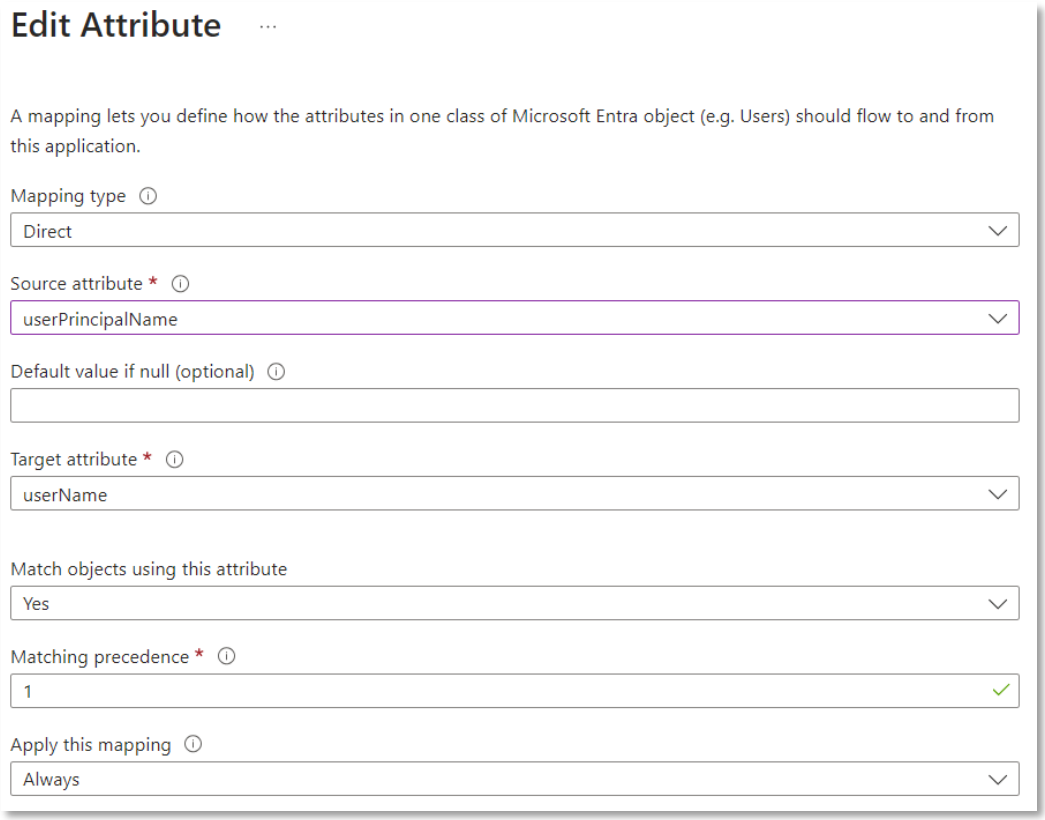


2. Mapping type: Direct

   «Source attribute»: l'attribut que vous utilisez pour enregistrer les numéros AVS
   «Target attribute»: *urn:ietf:params:scim:schemas:extension:Edulog:2.0:User:ahvn13*



Vérifiez le mappage du «userName» pour vous assurer qu'il correspond à l'attribut que vous utilisez comme UID (l'attribut que vos utilisatrices et utilisateurs saisissent lorsqu'ils se connectent).



5.2.3 Test

Vous pouvez utiliser la «Provision on demand» pour fournir un utilisateur test. Le numéro AVS de l'utilisateur test doit être un numéro AVS valide (il doit commencer par 756 et se terminer par une somme de contrôle).

Si le déploiement a réussi, vous pouvez maintenant vous connecter aux applications Edulog avec l'utilisateur test. Vous pouvez tester la connexion sur le portail libre-service d'Edulog:

- https://my.int.edulog.ch/ (INT)
- https://my.edulog.ch/ (PROD)

Remarque: si vous utilisez des mandants Entra différents pour les environnements d'intégration et de production, vérifiez que vous avez configuré l'utilisateur de test pour le bon environnement avant de tester.