

TECHNIQUE

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

2.2025 – Version 2.3

1.	But du document.....	2
2.	Prérequis.....	2
3.	Création des attributs Edulog.....	3
3.1	Création de l'application d'attributs d'extension.....	3
3.2	Script pour l'ajout d'attributs.....	5
3.3	Création d'un utilisateur test.....	5
4.	Création et configuration de l'application Edulog.....	6
4.1	Création d'une application <i>Enterprise</i>	6
4.2	Métadonnées SAML de l'application.....	7
4.3	Configuration de l'authentification unique.....	8
5.	Configuration du déploiement automatique des utilisatrices et utilisateurs (avec SCIM).....	12
5.1	Obtention d'un jeton SCIM.....	12
5.2	Configuration dans <i>Entra ID</i>	13
5.2.1	Connexion.....	13
5.2.2	Mappages.....	13
5.2.3	Test.....	16

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 <i>userPrincipalName</i>
givenName	Prénom	
sn	Nom	
mail	Adresse courriel	
EdulogPersonBirthDate	Date de naissance au format AAAAMMMJJ	
preferredLanguage	Langue préférée, parmi les valeurs suivantes: <i>de-CH, fr-CH, it-CH, rm-CH, en</i>	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: <i>pupil, teacher, administration, principal, legal_guardian, technician, other</i>	
EdulogPersonLevel	Degré(s) d'enseignement parmi les valeurs suivantes: <i>primary, secondary1, secondary2, tertiary</i>	
EdulogPersonCycle	Cycle(s) parmi les valeurs suivantes: <i>0, 1, 2, 3</i>	
EdulogPersonCanton	Code à deux lettres du canton (par ex. <i>VD, BE, GE, ZH</i>)	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](#).

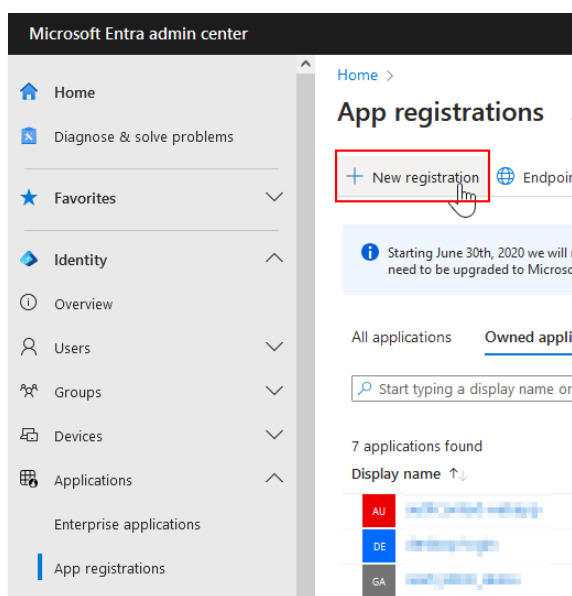
Si certains des attributs attendus par Edulog ne sont pas déjà présents dans votre *Entra tenant* en tant qu'attributs utilisateur, vous pouvez les créer en tant qu'attributs supplémentaires ou «attributs d'extension». Les paragraphes 3.1 à 3.3 décrivent la création des attributs suivants:

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*).



Home > App registrations >

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Edulog Extended Attributes

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (MSFT only - Single tenant)
☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (Xbox)
☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional, but a value is required for most authentication scenarios.

Select a platform:

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding them to the app catalog.

By proceeding, you agree to the [Microsoft Platform Policies](#)

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.

Microsoft Entra admin center

Home >

App registrations

+ New registration | Endpoints | Troubleshoot

Starting June 30th, 2020 we will no longer accept applications that need to be upgraded to Microsoft Authentication Library (MSAL).

All applications | Owned applications

Edulog

1 applications found

Display name ↑↓

EE Edulog Extended Attributes

Delete | Endpoints | Preview features

Essentials

Display name : [Edulog Extended Attributes](#)

Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : [My organization only](#)

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_<applID>_<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 "extension_<appID>_EdulogPersonBirthDate" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "extension_<appID>_EdulogPersonRole" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "extension_<appID>_EdulogPersonLevel" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "extension_<appID>_EdulogPersonCycle" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "extension_<appID>_EdulogPersonCanton" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "extension_<appID>_o" -ExtensionValue <value>
Set-AzureADUserExtension -ObjectId <user principal name> -ExtensionName "extension_<appID>_title" -ExtensionValue <value>
```

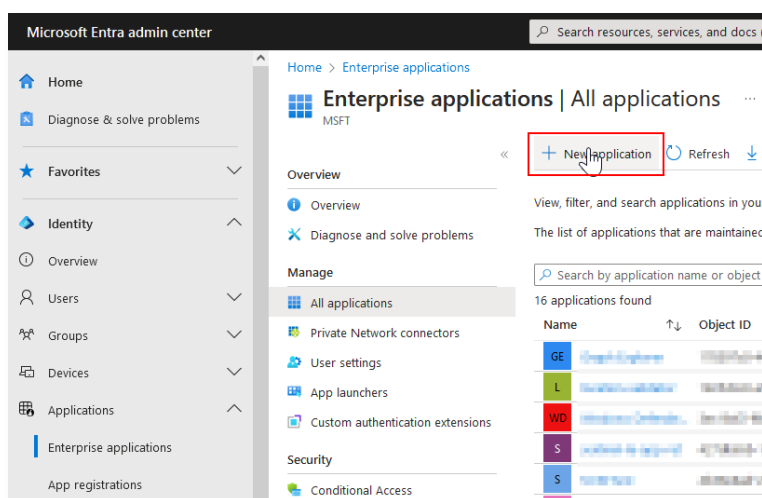
Exemples d'attributs:

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

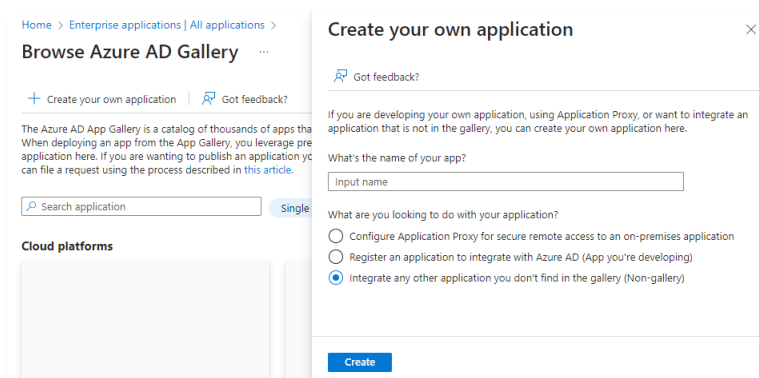
4. Création et configuration de l'application Edulog

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)*.



Home > Enterprise applications | All applications >

Browse Azure AD Gallery

+ Create your own application | Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps that you can use to integrate with your organization. When deploying an app from the App Gallery, you leverage pre-validated configurations. If you are wanting to publish an application you can file a request using the process described in [this article](#).

Search application Single

Cloud platforms

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

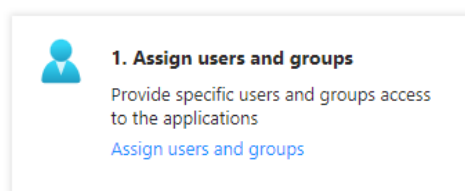
Input name

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises application
☐ Register an application to integrate with Azure AD (App you're developing)
☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

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



1. Assign users and groups

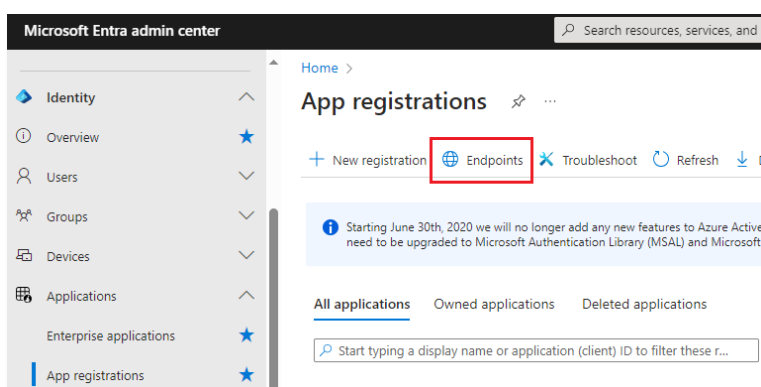
Provide specific users and groups access to the applications

[Assign users and groups](#)

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*.



Microsoft Entra admin center

Search resources, services, and...

Home >

App registrations

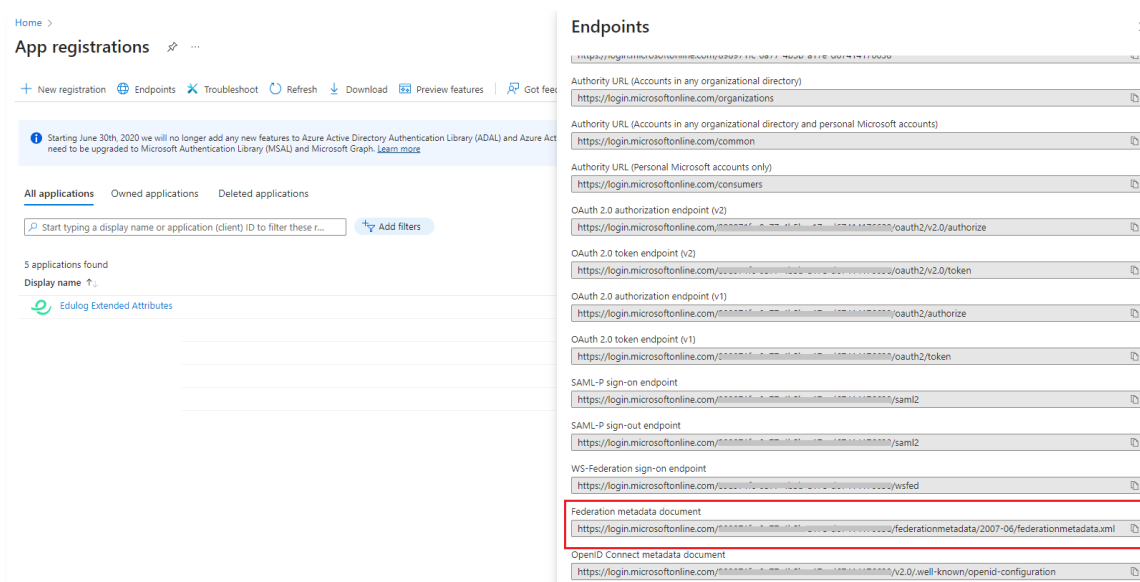
+ New registration **Endpoints** Troubleshoot Refresh

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory. You need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft

All applications Owned applications Deleted applications

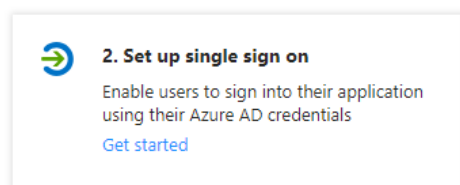
Start typing a display name or application (client) ID to filter these r...

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.

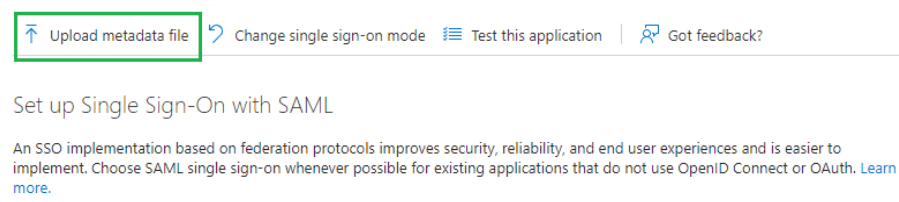


4.3 Configuration de l'authentification unique

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



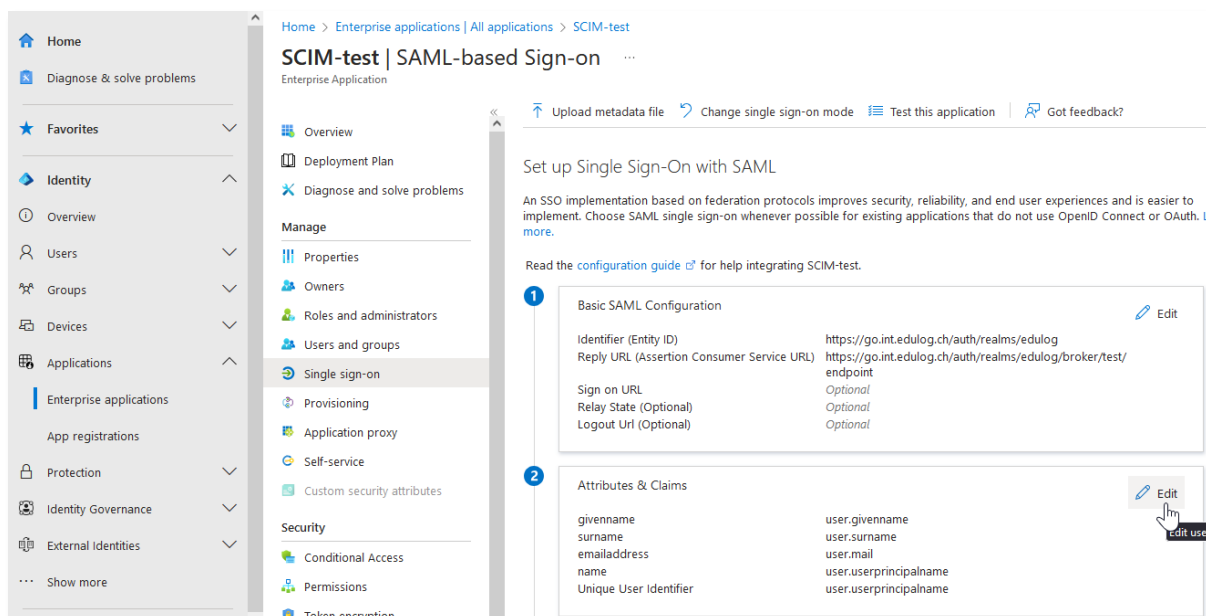
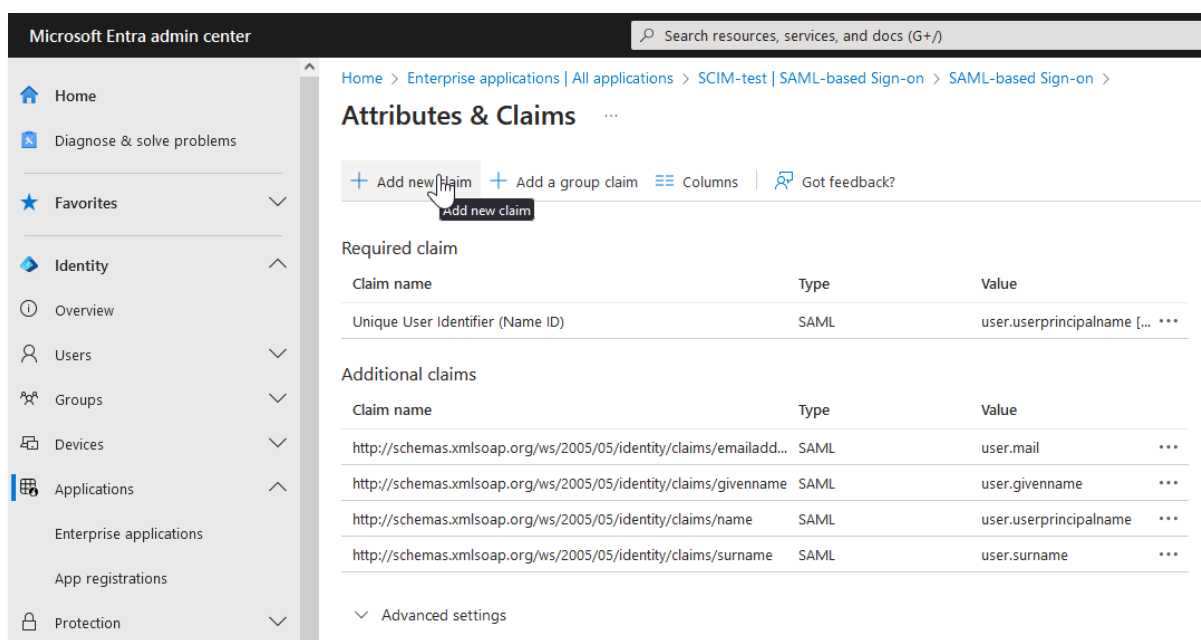
Sélectionnez «SAML», puis téléversez le fichier de métadonnées validé par l'équipe d'onboarding d'Edulog.



Cela remplit les URL pour la configuration SAML de base:

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

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ...

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

- Attributs qui existaient déjà dans votre *tenant* (en général: *uid*, *givenName*, *sn*, *title*)
- Attributs ajoutés en tant qu'attributs d'extension au §3 (en général: *EduLogPerson-BirthDate*, *EduLogPersonRole*, *EduLogPersonLevel*, *EduLogPersonCycle*)
- Attributs identiques pour chaque utilisatrice et utilisateur (en général: *preferredLanguage*, *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).

Manage claim ...

Save
 Discard changes
 Got feedback?

Name *

Namespace

Choose name format

Source * ☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute *

Claim conditions

Advanced SAML claims options

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.

Home > Enterprise applications | All applications > | SAML-based Sign-on > SAML-based

Manage claim ...

Save
 Discard changes
 Got feedback?

Name *

Namespace

Choose name format

Source * ☐ Attribute ☐ Transformation ☒ Directory schema extension (Preview)

Schema extension attribute (Preview) Undefined

Claim conditions

Advanced SAML claims options

Add Extension Attributes

Extension attributes from 'Edulog Extended Attributes' application.

Select Application

The list of available extension attributes configured against the application: 'Edulog Extended Attributes'.

Name	Data Type	Synced From ...
user.title	String	false
user.o	String	false
user.EdulogPersonTechID	String	false
user.EdulogPersonCanton	String	false
user.EdulogPersonCycle	String	false
user.EdulogPersonLevel	String	false
user.EdulogPersonRole	String	false
user.EdulogPersonBirthDate	String	false

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.

Manage claim

Save
 Discard changes
 Got feedback?

Name *

Namespace

Choose name format

Source *

☒ Attribute
 ☐ Transformation
 ☐ Directory schema extension

Source attribute *

Claim conditions

Advanced SAML claims options

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.

Attributes & Claims

Add new claim
 Add a group claim
 Columns
 Got feedback?

Required claim		
Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...] ***

Additional claims		
Claim name	Type	Value
EdulogPersonBirthDate	SAML	user.edulogpersonbirthd... ***
EdulogPersonCanton	SAML	"VD" ***
EdulogPersonCycle	SAML	user.edulogpersoncycle (...) ***
EdulogPersonLevel	SAML	user.edulogpersonlevel (...) ***
EdulogPersonRole	SAML	user.edulogpersonrole (e... ***
givenName	SAML	user.givenname ***
mail	SAML	user.mail ***
o	SAML	"School A" ***
preferredLanguage	SAML	"fr-CH" ***
sn	SAML	user.surname ***
title	SAML	user.jobtitle ***
uid	SAML	user.userprincipalname ***

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
```

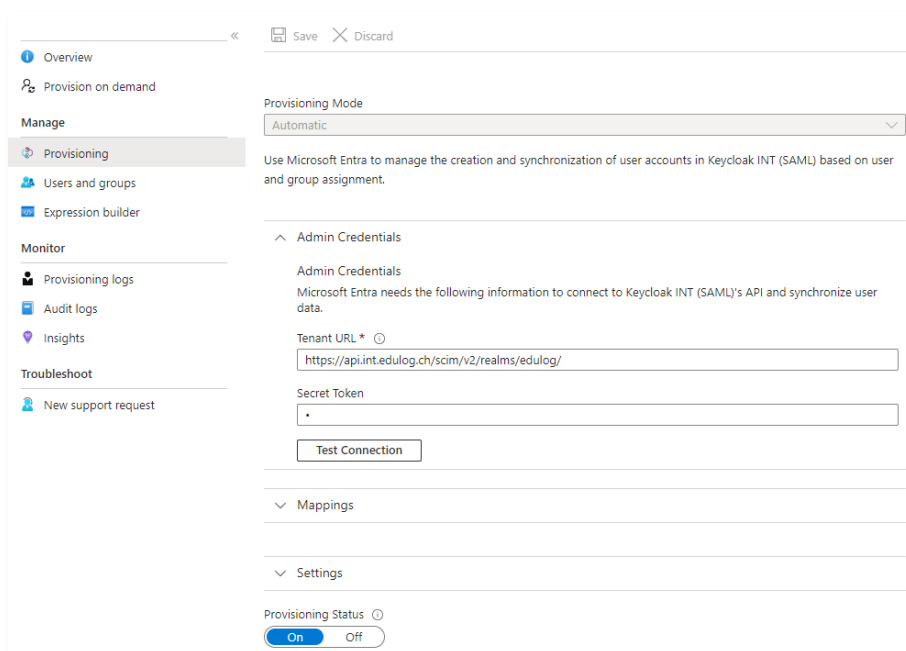
Copiez le <refresh token>, en veillant à supprimer les espaces.

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»:

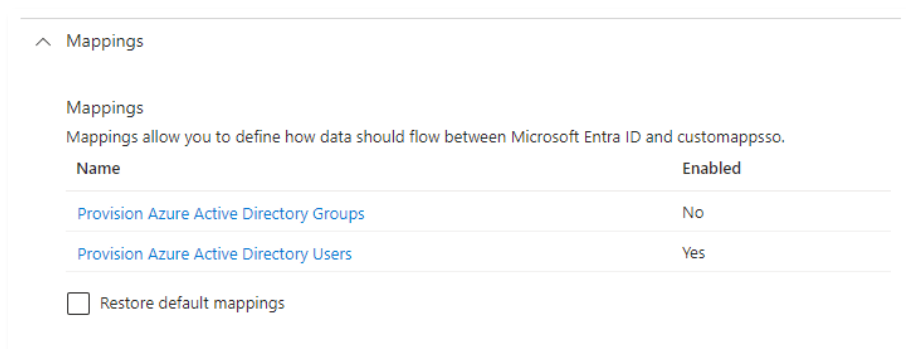
- <https://api.int.edulog.ch/scim/v2/realms/edulog/> (INT)
- <https://api.edulog.ch/scim/v2/realms/edulog/> (PROD)

«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».



Name	Enabled
Provision Azure Active Directory Groups	No
Provision Azure Active Directory Users	Yes

☐ Restore default mappings

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

Attribute Mappings

Attribute mappings define how attributes are synchronized between Microsoft Entra ID and customappsso

customappsso Attribute	Microsoft Entra ID Attribute	Matching precedence	Edit	Remove
userName	userPrincipalName	1	Edit	Delete

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

☒ Show advanced options

Supported Attributes

View and edit the list of attributes that appear in the source and target attribute lists for this application.

The attribute list for Microsoft Entra ID is up to date with all supported attributes. [Request additional attributes you would like to see supported here.](#)

[Edit attribute list for customappsso](#)

[Use the expression builder](#)

In addition to configuring your attribute mappings through the user interface, you can review, download, and edit the JSON representation of your schema. [Review your schema here.](#)

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 ? ».

customappsso User Attributes

Name	Type	Primary Key?	Required?
id	String	☒	☒
active	Boolean	☐	☒
userName	String	☐	☒
urn:ietf:params:scim:schemas:extension:Edulog:2.0:User:ahvn13	String	☐	☒

3. Enregistrez les modifications.

Ajoutez les mappages suivants:

1. Mapping type: Expression

«Expression»: *Not([IsSoftDeleted])*

«Target attribute»: *active*

Edit Attribute

Mapping type

Expression

Enter an expression

Default value if null (optional)

Use the expression builder

Target attribute *

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*

Edit Attribute

A mapping lets you define how the attributes in one class of Microsoft Entra object (e.g. Users) should flow to and from this application.

Mapping type ⓘ
Direct

Source attribute * ⓘ
employeeid

Default value if null (optional) ⓘ

Target attribute * ⓘ
urn:ietf:params:scim:schemas:extension:Edulog:2.0>User:ahvn13

Match objects using this attribute
No

Matching precedence ⓘ

Apply this mapping ⓘ
Always

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).

Edit Attribute

A mapping lets you define how the attributes in one class of Microsoft Entra object (e.g. Users) should flow to and from this application.

Mapping type ⓘ
Direct

Source attribute * ⓘ
userPrincipalName

Default value if null (optional) ⓘ

Target attribute * ⓘ
userName

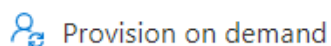
Match objects using this attribute
Yes

Matching precedence * ⓘ
1

Apply this mapping ⓘ
Always

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.