Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNISCHES

Konfiguration eines *Microsoft Entra ID tenant* als 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. Ziel des Dokuments

Dieses Dokument beschreibt die notwendigen Schritte zur Konfiguration eines *Entra ID tenant* als Identitätsanbieter (IdP) für Edulog mithilfe einer SAML-Trust-Konfiguration.

Es enthält alle Schritte zur Konfiguration der SAML-Verbindung (§3-4) und der SCIM-Bereitstellung (§5). Diese Schritte müssen zuerst für die Integrationsumgebung von Edulog (INT) und dann für die Produktionsumgebung (PROD) durchgeführt werden.

2. Vorbedingungen

Sie benötigen ein Administratorkonto in Ihrem *Microsoft Entra admin center*.

Die folgenden Attribute werden von Edulog benötigt:

Edulog-Attributname	Beschreibung	Kommentar
uid	Benutzerkennung: dies ist der Wert, den Benutzende zum Anmelden verwenden	In Entra ist dies in der Regel der *userPrincipalName*
givenName	Vorname	
sn	Name	
mail	E-Mail-Adresse	
EdulogPersonBirthDate	Geburtsdatum im Format JJJJMMTT	
preferredLanguage	Bevorzugte Sprache, unter den folgenden Werten: *de-CH, fr-CH, it-CH, rm-CH, en*	Je nach IdP-Kontext kann dieser Wert für alle Benutzende identisch sein.
title	Funktion, nicht zutreffend für Schülerinnen/Schüler	
EdulogPersonRole	Hauptrolle(n) unter den folgenden Werten: *pupil, teacher, administration, principal, legal_guardian, technician, other*	
EdulogPersonLevel	Bildungsstufe(n) unter den folgenden Werten: *primary, secondary1, secondary2, tertiary*	
EdulogPersonCycle	Bildungszyklus(en) unter den folgenden Werten: *0, 1, 2, 3*	
EdulogPersonCanton	Zwei-Buchstaben-Code des Kantons (z.B. *VD, BE, GE, ZH*)	Dieser Wert ist wahrscheinlich für alle Benutzenden eines IDP gleich.
o	Organisation oder Institution	

Weitere Details zu den einzelnen Attributen finden Sie in der Edulog-Dokumentation, im «Leitfaden Attribute – Identitätsanbieter».

3. Erstellung der Edulog-Attribute

Hinweis: Diese Konfiguration erfolgt im *Microsoft Entra admin center*.

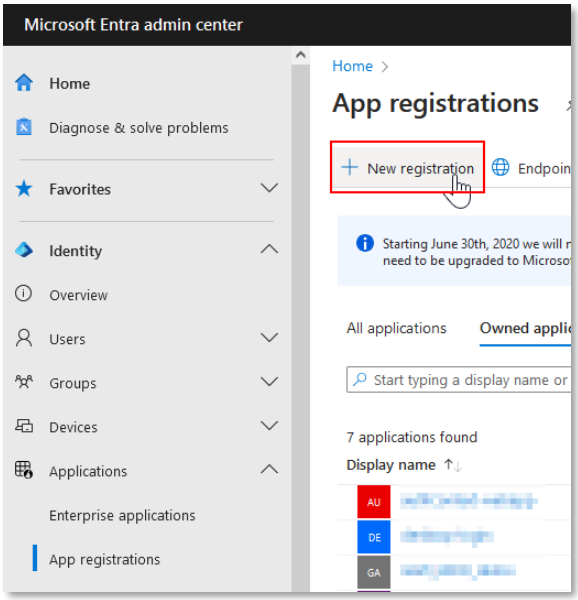
Wenn einige der von Edulog erwarteten Attribute nicht bereits als Benutzerattribute in Ihrem *Entra tenant* vorhanden sind, können Sie sie als zusätzliche Attribute oder «erweiterte Attribute» erstellen. In den Absätzen 3.1 bis 3.3 wird die Erstellung folgender Attribute beschrieben:

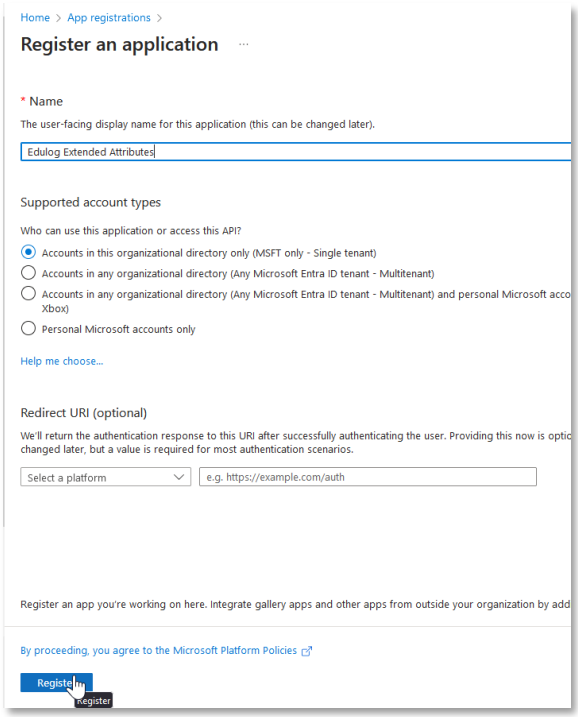
1. *EdulogPersonBirthDate*
2. *EdulogPersonRole*
3. *EdulogPersonLevel*
4. *EdulogPersonCycle*
5. *EdulogPersonCanton*
6. o
7. *title*

Wenn einige dieser Attribute bereits in Ihrem *tenant* vorhanden sind (unter einem anderen Namen), können Sie die entsprechenden Zeilen aus den Skripten entfernen.

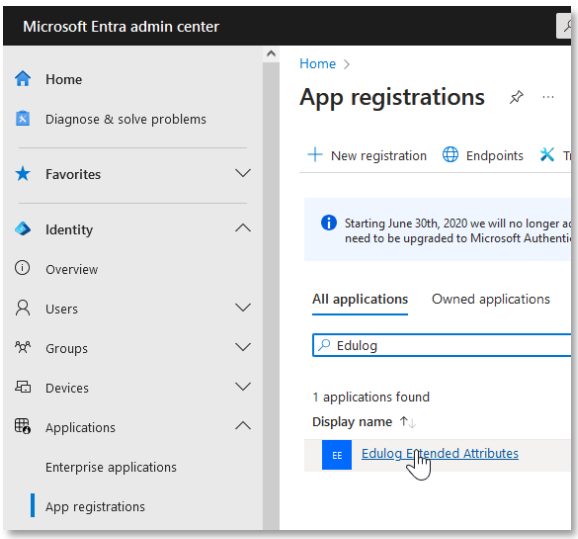
3.1 Erstellung der erweiterten Attribute-Anwendung

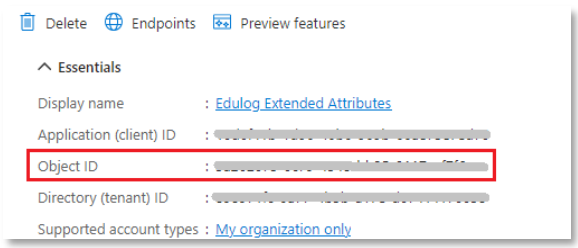
Im *Microsoft Entra admin center* navigieren Sie zu *Identity* > *Applications* > *App registrations*. Registrieren Sie eine neue Anwendung (*New registration* > *Name «Edulog Extended Attributes»* > *Register*).





Nachdem Sie auf «Register» geklickt haben, werden Sie zur Anwendungsübersicht weitergeleitet. Notieren Sie sich die Objekt-ID, diese werden Sie beim Absatz 3.2 benötigen.





Um die registrierten Anwendungen zu finden, suchen Sie unter: *Identity* > *Applications* > *App registrations* > *All applications* nach «Edulog Extended Attributes».

3.2 Skript zum Hinzufügen der Attribute

Überprüfen Sie in Powershell zunächst, ob das AzureAD-Modul verfügbar und importiert ist, und installieren Sie es gegebenenfalls.

```
# 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
```

Führen Sie das Powershell-Skript wie folgt aus:

```
# 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
```

Der Befehl `Get-AzureADApplicationExtensionProperty` zeigt die neuen Erweiterungseigenschaften im Format *extension_<appID>_<attribute name>* an.

3.3 Erstellung eines Testbenutzers

Sie können das folgende Powershell-Skript verwenden, um einen Testbenutzer zu erstellen, wobei Sie die Informationen im «Leitfaden Attribute – Identitätsanbieter» für das Format jedes Werts beachten.

```
# 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>
```

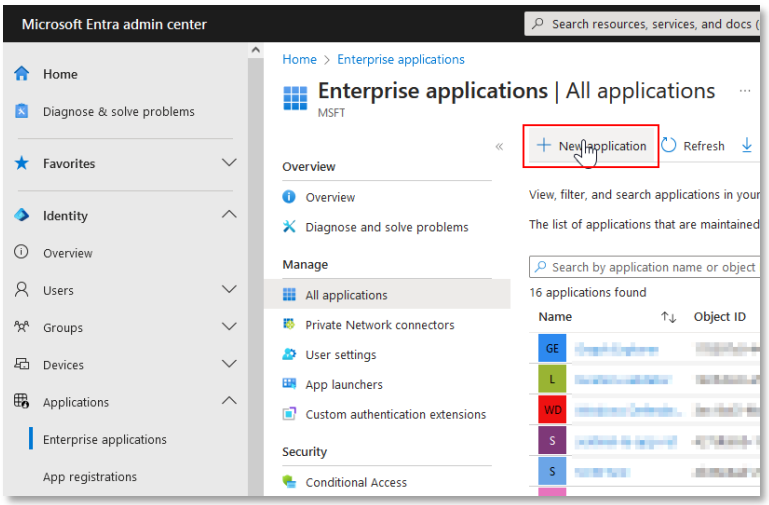
Beispiele von Attributen:

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

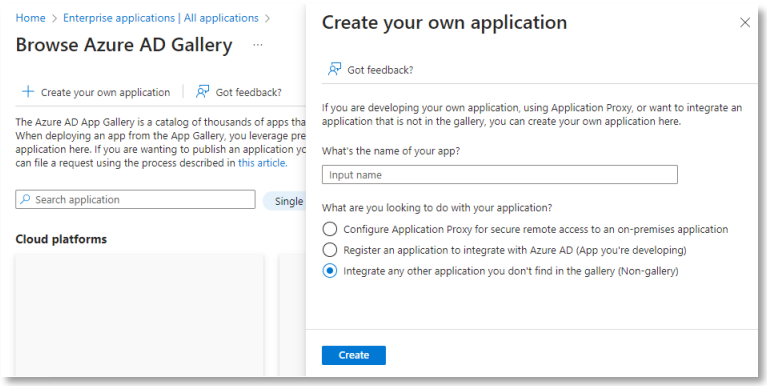
4. Erstellung und Konfiguration der Edulog-Anwendung

4.1 Erstellung einer Enterprise-Anwendung

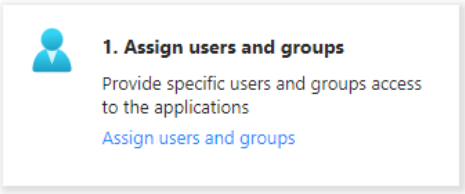
1. Navigieren Sie zu *Identity > Applications > Enterprise applications*.



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



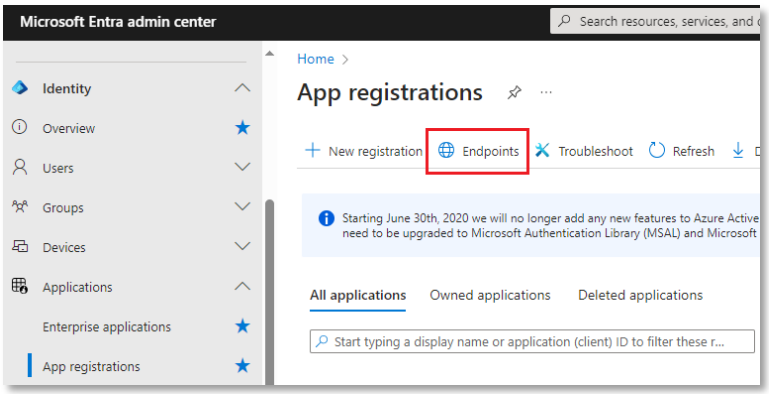
3. Geben Sie einen Namen ein und klicken sie auf «Create».



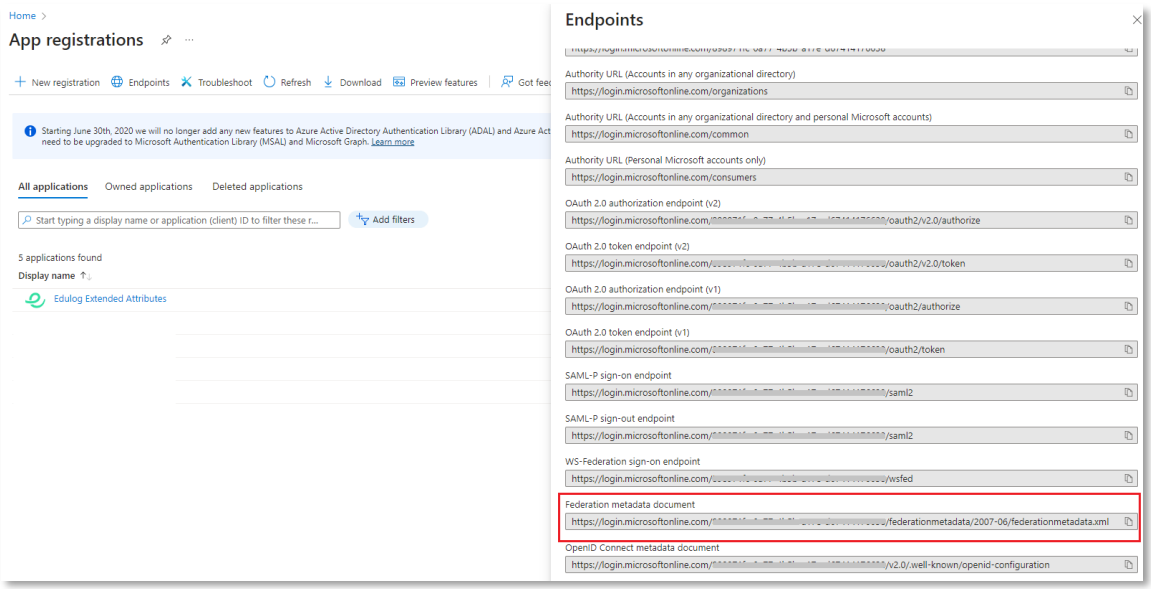
4. Weisen Sie die Testbenutzenden der erstellten Anwendung zu.

4.2 SAML-Metadaten der Anwendung

Die SAML-Metadaten der Anwendung finden Sie unter *Identity > Applications > App registrations > Endpoints > Federation metadata document*.

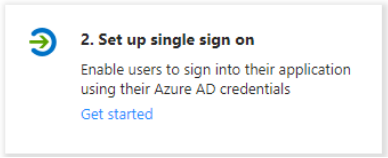


Senden Sie den Link zu diesem XML-Dokument (siehe Abbildung unten) an ELCA, verantwortlich für den technischen Betrieb und das Onboarding: onboarding_edulog@elca.ch.

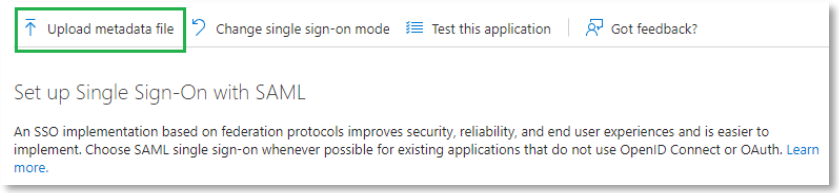


4.3 Single Sign-on-Konfiguration

Gehen Sie zurück zur App in *Identity > Applications > Enterprise applications* und wählen Sie «Set up single sign on» auf der Registerkarte «Overview» der Anwendung aus.



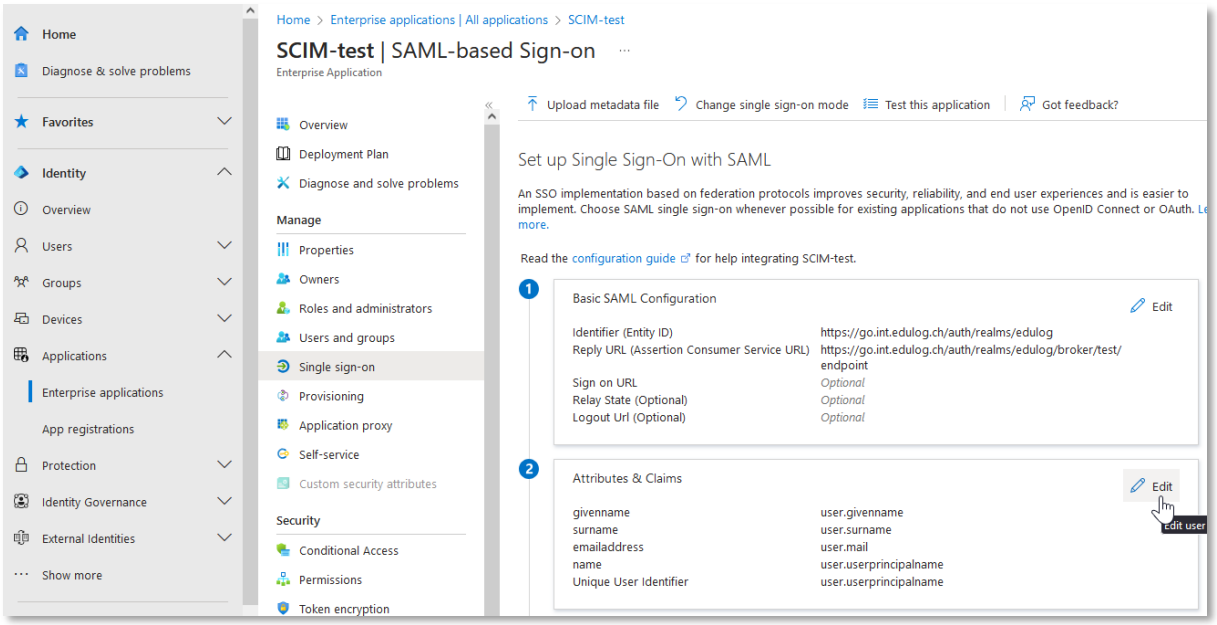
Wählen Sie «SAML» aus und laden Sie dann die vom Edulog-Onboarding-Team freigegebene Metadatendatei hoch.

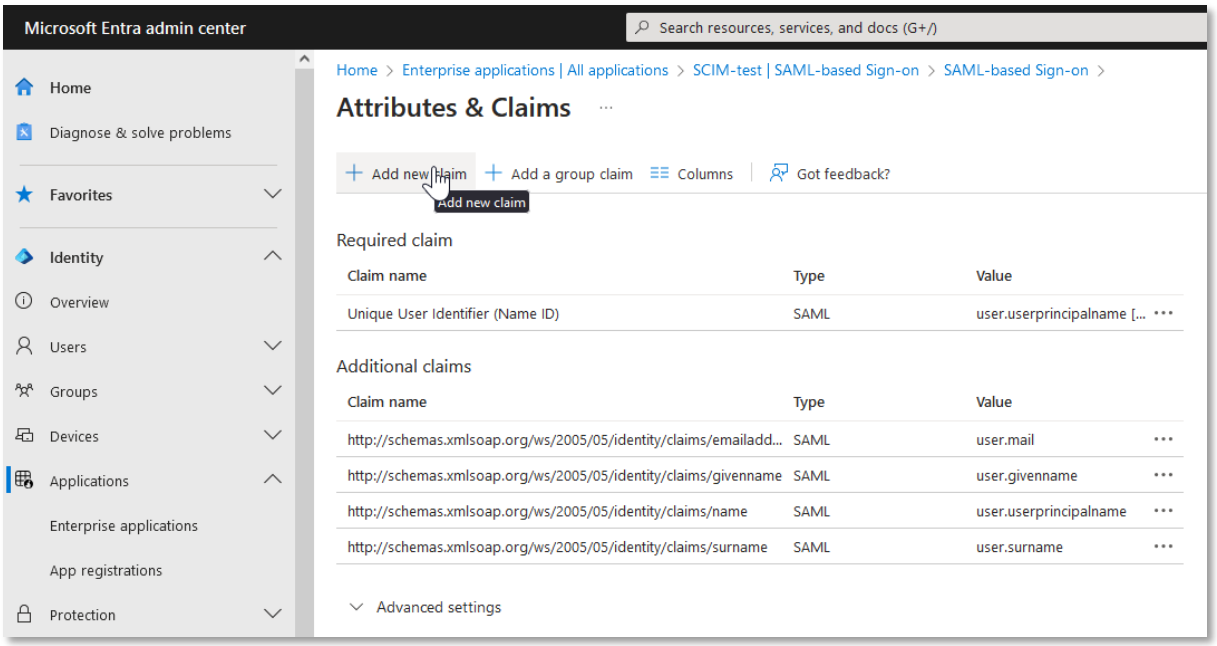


Dies füllt die URLs für die grundlegende SAML-Konfiguration aus:

	Beispiel INT	Beispiel 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 (Optional)	https://go.int.edulog.ch/auth/realms/edulog/broker/<idp name>/endpoint	https://go.edulog.ch/auth/realms/edulog/broker/<idp name>/endpoint

Für die Konfiguration von «Attributes & Claims» fügen Sie die Attribute hinzu, die an Edulog gesendet werden.



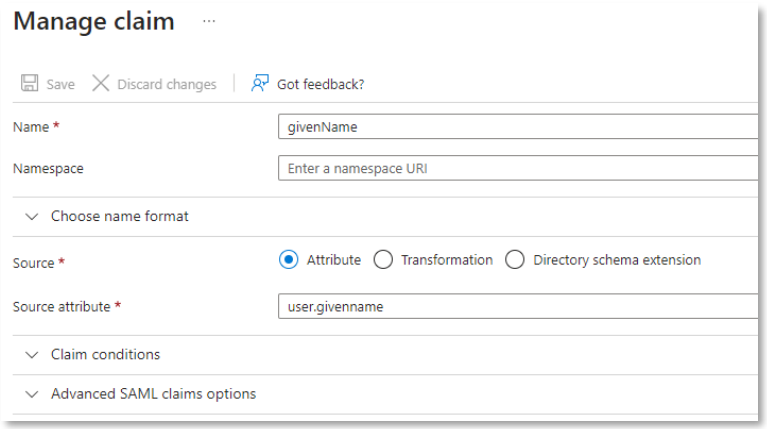


Alle Attribute, die unter §2 Voraussetzungen aufgeführt sind, müssen konfiguriert werden. Folgende drei Fälle werden unterschieden:

a. Attribute, die bereits in Ihrem *tenant* vorhanden waren (in der Regel: *uid*, *givenName*, *sn*, *title*)
b. Attribute, die als Erweiterungsattribute in §3 hinzugefügt wurden (in der Regel: *EdulogPersonBirthDate*, *EdulogPersonRole*, *EdulogPersonLevel*, *EdulogPersonCycle*)
c. Attribute, die für jede Benutzerin, jeden Benutzer gleich sind (in der Regel: *preferredLanguage*, *o*, *EdulogPersonCanton*)

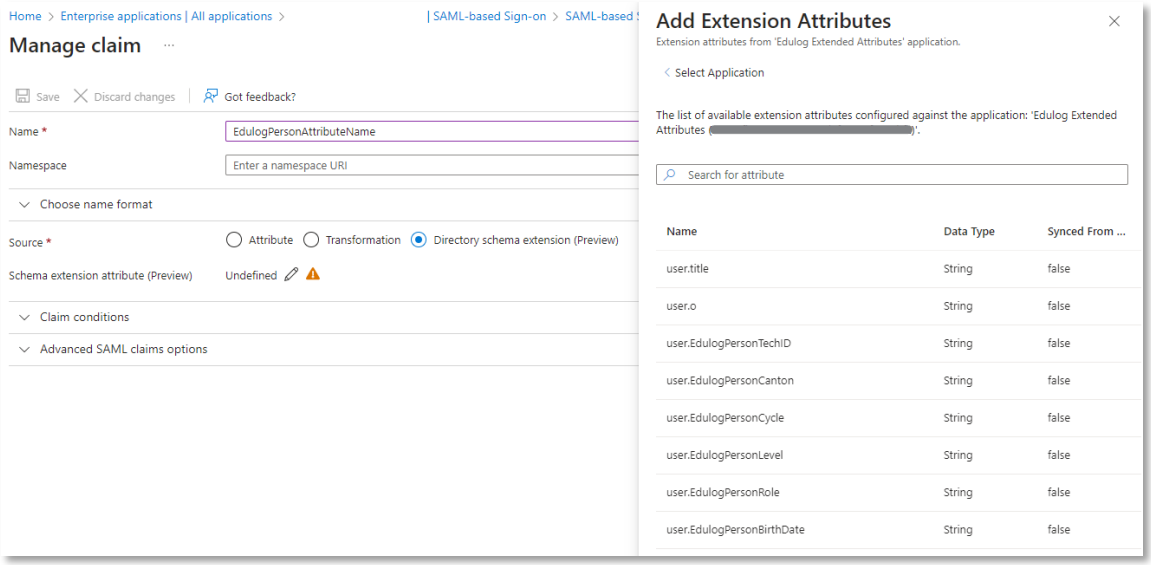
a. Bereits vorhandene Attribute

Sie können die bereits vorhandenen Attribute wie unten beschrieben konfigurieren, indem Sie den Edulog-Attributnamen (im Feld «Name») dem entsprechenden «Source attribute» zuordnen (lassen Sie den «Namespace» leer).



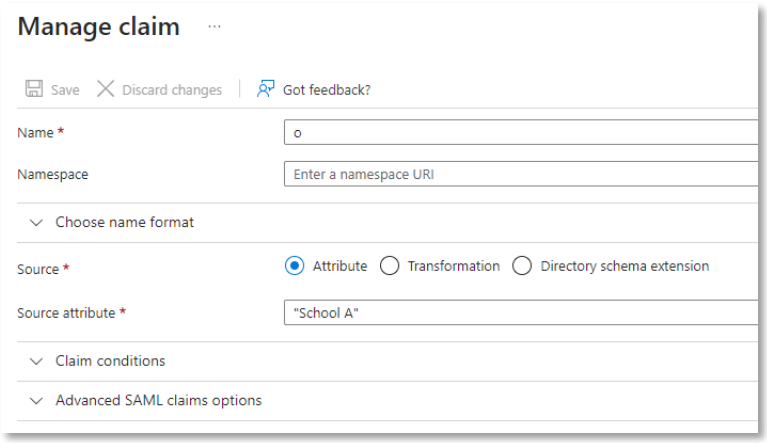
b. Erweiterungsattribute

Wählen Sie für jedes Erweiterungsattribut die entsprechende «Directory schema extension» der erweiterten Attribute-Anwendung aus, die Sie im vorherigen Schritt erstellt haben, wie unten dargestellt.



c. Konstante Attribute

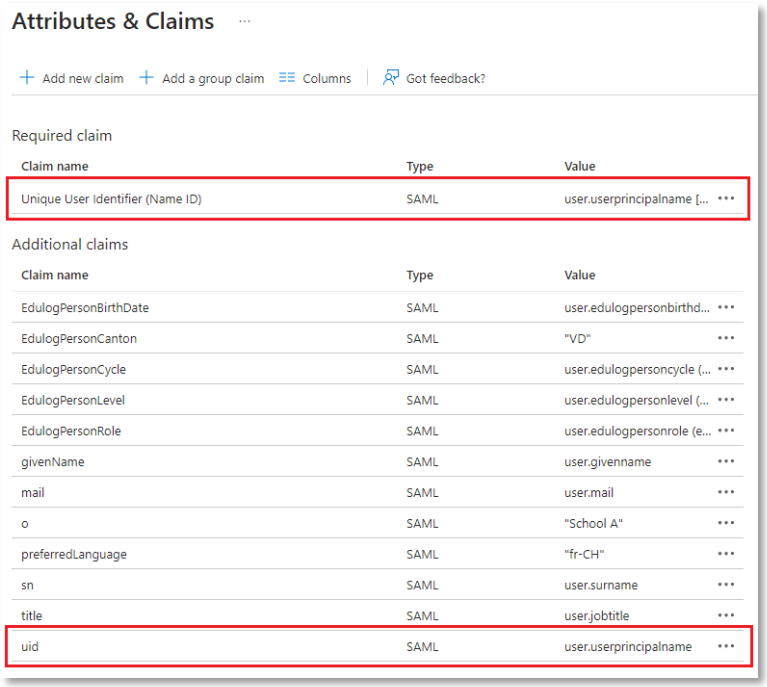
Attribute, die für jede Benutzerin, jeden Benutzer den gleichen Wert haben, können auf einen konstanten Wert gesetzt werden, wie unten dargestellt.



d. Eindeutige Benutzerkennung (SAML nameID)

Das SAML-Protokoll verwendet ein spezielles Attribut namens «nameID», um Benutzende eindeutig zu identifizieren. Sie finden das Attribut in Ihren Attributen unter «Unique User Identifier». Stellen Sie sicher, dass der Wert des Attributs dem «uid»-Attribut entspricht.

Im folgenden Beispiel verwenden wir den «userPrincipalName» als Wert für beide Ansprüche.



5. Konfiguration der automatischen Benutzerbereitstellung (mit SCIM)

Um die automatische Bereitstellung in Entra ID zu konfigurieren, müssen Sie die AHV-Nummer Ihrer Benutzenden in einem der Entra-Attribute speichern. Dies kann entweder in einem Erweiterungsattribut (wie in §3.1) oder in einem anderen nicht verwendeten Attribut (z.B. Mitarbeiter-ID oder Faxnummer, wenn eines dieser Attribute von Ihrer Organisation nicht verwendet wird) erfolgen.

5.1 Erhalt eines SCIM-Tokens

Die vollständige Dokumentation finden Sie im Leitfaden «Edulog API reference». Die relevanten Schritte werden hier detailliert beschrieben.

> **Voraussetzungen**: Benutzername und Passwort des API-Benutzers, die Ihnen vom Edulog-Onboarding-Team mitgeteilt wurden.

Mit Powershell können Sie die Edulog-API mit dem folgenden Befehl nach einem Token abfragen:

```
$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>` sollten durch die Anmeldedaten Ihres API-Benutzers ersetzt werden.
`<authdomain>` sollte ersetzt werden durch:

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

Sie erhalten eine Antwort von Edulog in folgender Form:

```
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
```

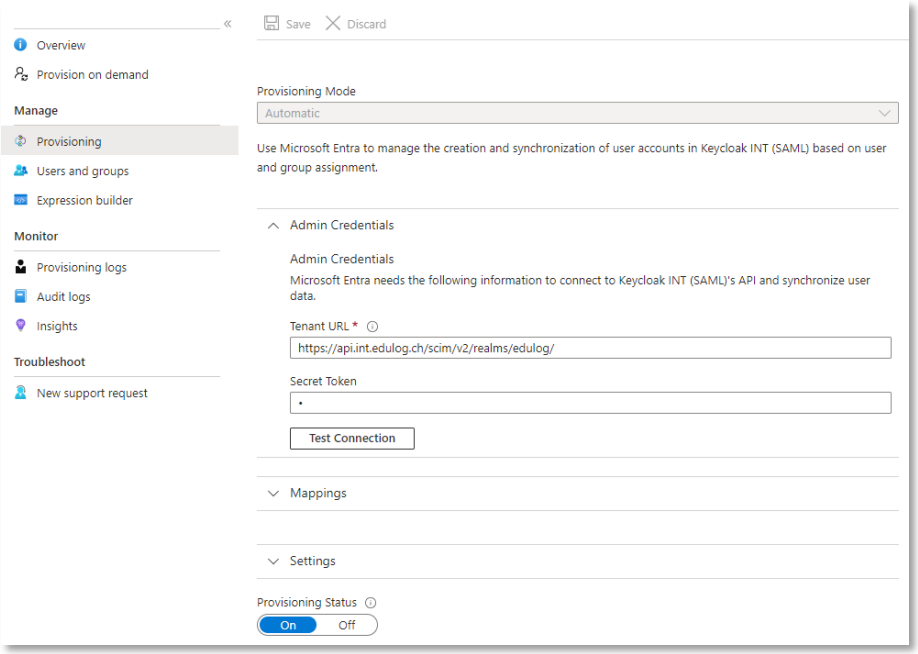
Kopieren Sie das `<refresh token>`, und achten Sie darauf, die Leerzeichen zu entfernen.

> **Warnung**: Der *<refresh_token>* ist ein sensibler Wert (genau wie das API-Passwort), da er seinem Besitzer permanenten Zugriff auf die Edulog SCIM API ermöglicht. Wenn Sie ihn an einen Zwischenort kopieren, bevor Sie ihn in Entra importieren, stellen Sie sicher, dass Sie ihn anschliessend ordnungsgemäss löschen.

5.2 Konfiguration in Entra ID

5.2.1 Verbindung

Konfigurieren Sie unter *Entra ID > Enterprise applications* > *your Edulog application* > *Provisioning* die «Admin Credentials» wie unten dargestellt.



«Tenant URL»:

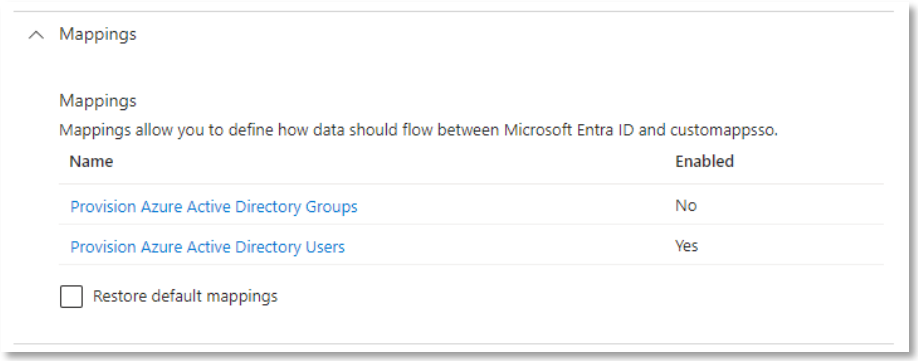
- https://api.int.edulog.ch/scim/v2/realms/edulog/ (INT)
- https://api.edulog.ch/scim/v2/realms/edulog/ (PROD)

«Secret token»: das Refresh-Token, das Sie im vorherigen Schritt kopiert haben (§5.1).

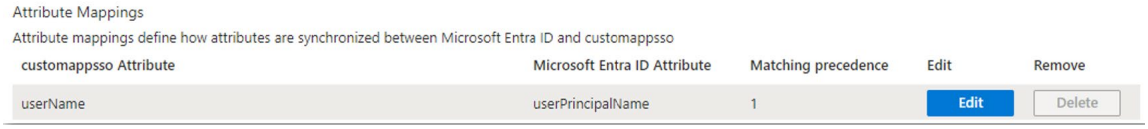
Um die Verbindung zu testen, klicken Sie auf den Button «Test Connection».

5.2.2 Mappings

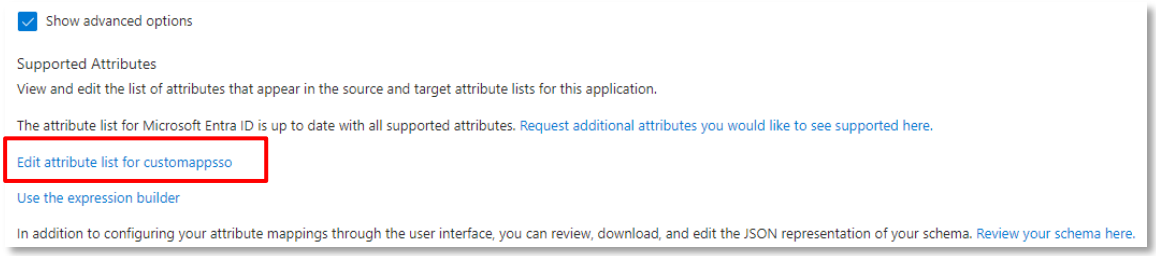
Sie werden Users und nicht Gruppen provisionieren. Deaktivieren Sie darum die «Groups Mappings», indem Sie den Status von «Provision Azure Active Directory Groups» auf «No» setzen.



Klicken Sie auf die «Users Mappings» und löschen Sie alle vorhandenen Mappings ausser «userPrincipalName»:



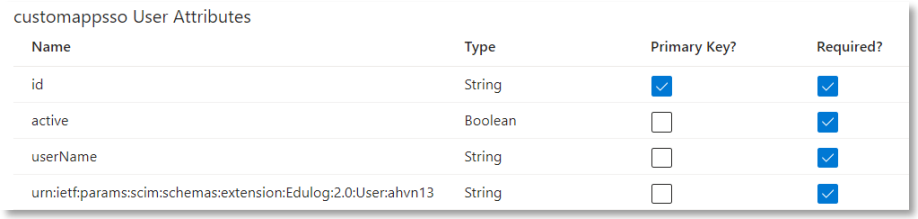
Klicken Sie auf das Kontrollkästchen «Show advanced options» und navigieren Sie zu «Edit attribute list for customappsso».



In der Attributliste:

1. Aktivieren Sie das Kontrollkästchen «required» für das Attribut «active».
2. Fügen Sie ein neues Attribut hinzu:

   Name: urn:ietf:params:scim:schemas:extension:Edulog:2.0:User:ahvn13
   Type: String
   Aktivieren Sie das Kontrollkästchen «Required?»

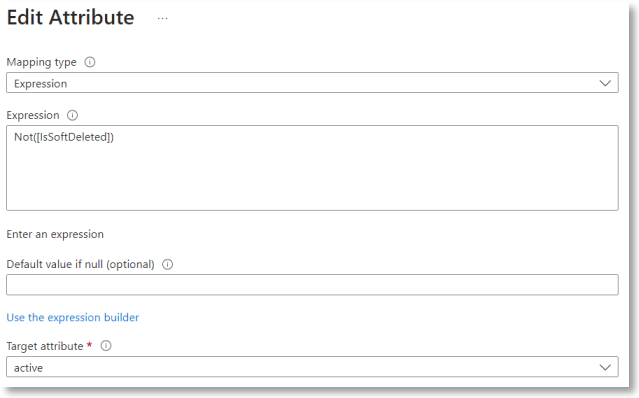


3. Speichern Sie die Änderungen.

Fügen Sie die folgenden Mappings hinzu:

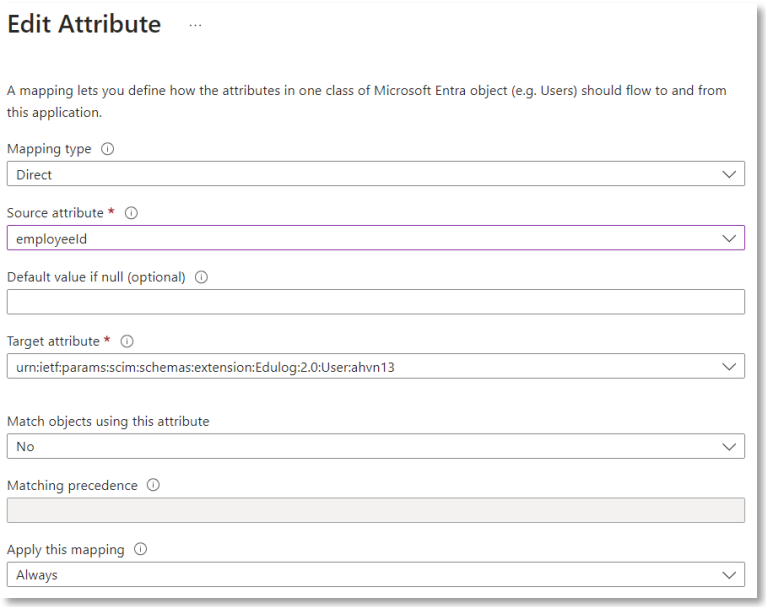
1. Mapping type: Expression

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

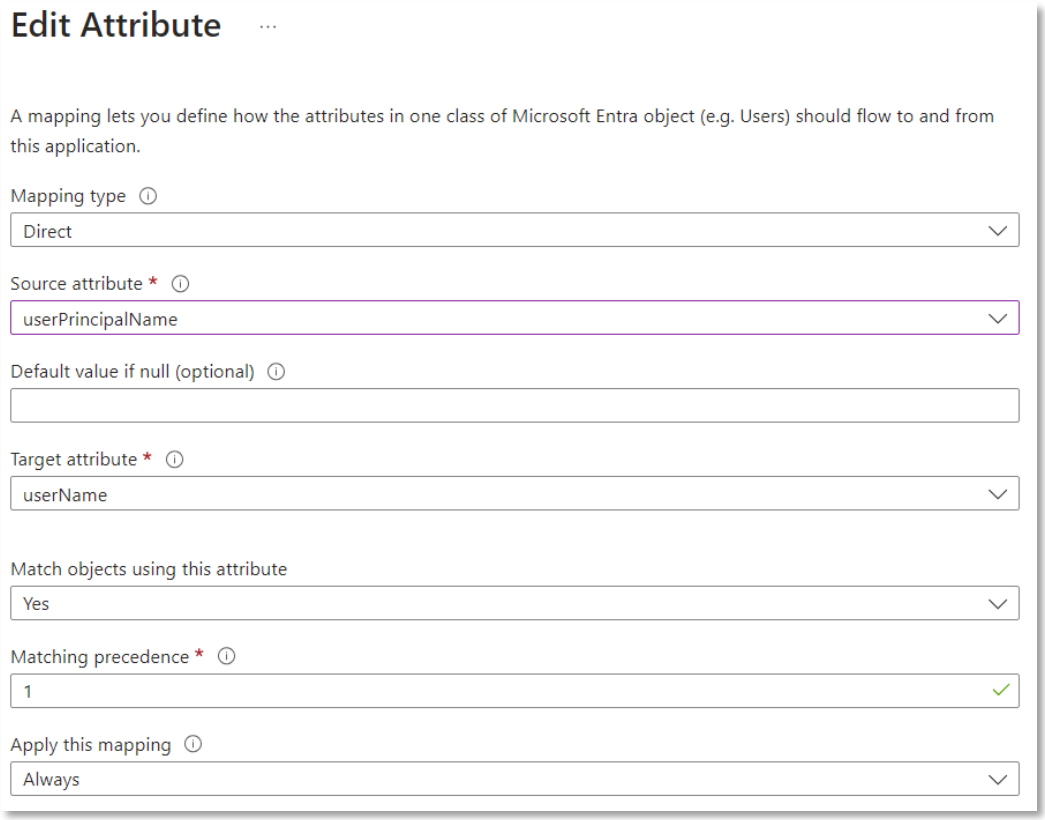


2. Mapping type: Direct

   «Source attribute»: das Attribut, das Sie zum Speichern der AHV-Nummern verwenden
   «Target attribute»: *urn:ietf:params:scim:schemas:extension:Edulog:2.0:User:ahvn13*



Überprüfen Sie das Mapping des «userName», um sicherzustellen, dass es dem Attribut entspricht, das Sie als UID verwenden (das Attribut, das Ihre Benutzenden bei der Anmeldung eingeben).



5.2.3 Test

Sie können die «Provision on demand» verwenden, um einen Testbenutzer bereitzustellen. Die AHV-Nummer des Testbenutzers muss eine gültige AHV-Nummer sein (sie muss mit 756 beginnen und mit einer Prüfsumme enden).

Wenn die Bereitstellung erfolgreich war, können Sie sich jetzt mit dem Testbenutzer bei den Edulog-Anwendungen anmelden. Sie können die Anmeldung auf dem Edulog-Selbstbedienungsportal testen:

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

Hinweis: Wenn Sie für die Integrations- und Produktionsumgebung verschiedene Entra-Mandanten verwenden, überprüfen Sie vor dem Testen, ob Sie den Testbenutzer für die richtige Umgebung konfiguriert haben.