

TECHNISCHES

Vorbereitung eines *Azure AD Tenant* als IdP für Edulog

7.1.2022 – Version 1.2

1.	Ziel des Dokuments	2
2.	Voraussetzung	2
2.1	Allgemeine Vorgehensweise.....	2
2.2	Bemerkungen.....	2
2.3	Erforderliche Elemente.....	3
3.	Erstellen einer <i>Application</i>	4
3.1	Über das <i>Azure</i> -Portal	4
4.	Edulog-Attribute erstellen	5
5.	Anlegen eines Testbenutzers	7
6.	Erstellen einer <i>Enterprise Application</i>	8
7.	Erstellen einer <i>claim mapping policy</i>	11
8.	IdP und Testbenutzer föderieren.....	13
9.	Interne Verbindungstests.....	14
10.	Tests mit Edulog.....	14
11.	Anhang: Nützliche Powershell-Befehle.....	14

1. Ziel des Dokuments

Dieses Dokument beschreibt die notwendigen Schritte, wie ein IdP *Azure AD* als SAML-Endpoint konfigurieren kann, um sich bei Edulog zu integrieren.

Es zeigt nicht, wie das *Onboarding* der Identitäten erfolgen soll. Dieser Schritt wird erst nach der Integration vorgenommen.

2. Voraussetzung

Sie haben

- ein Konto bei *Azure*. Erstellen Sie einen *Azure AD Tenant* aus einem «global Administrator»-Konto.
- eine Maschine mit Windows 10 und einem Benutzer mit Administratorenrechten.
- das *AzureADPreview*-Moduls für *Powershell* installiert.
- bereits einen Vertrag mit Edulog unterzeichnet.

2.1 Allgemeine Vorgehensweise

Nr.	Aktionen	Ziel/Kommentar
1	<i>Application</i> erstellen	Diese Anwendung ist notwendig, um die spezifischen Attribute für Edulog zu integrieren
2	Edulog-Attribute erstellen	Kann nicht über das <i>Azure</i> -Portal erstellt werden.
3	Testbenutzer anlegen	Die im vorherigen Punkt erstellten Attribute sind nur sichtbar, wenn ihr Wert ungleich Null ist. Dieser Punkt wird für die Validierung verwendet.
4	<i>Enterprise Application</i> erstellen	Diese Anwendung wird als <i>SAML-Endpoint</i> dienen.
5	<i>claim mapping policy</i> erstellen	Dies ist die Definition der Attribute, die vom <i>Azure AD</i> gesendet werden.
6	<i>Föderieren Sie den erstellten IdP und einige Testbenutzer</i>	Testen der Föderation mit Edulog.
7	Interne Verbindungstests	Wird verwendet, um das Senden der neuen Attribute in der <i>SAML2</i> -Anfrage zu überprüfen.

Alle Aktionen können über *Powershell* in der Befehlszeile ausgeführt werden. In diesem Bericht wird jedoch aus Gründen der Übersichtlichkeit die *Azure*-Benutzeroberfläche für die Punkte 1, 4, 5 verwendet.

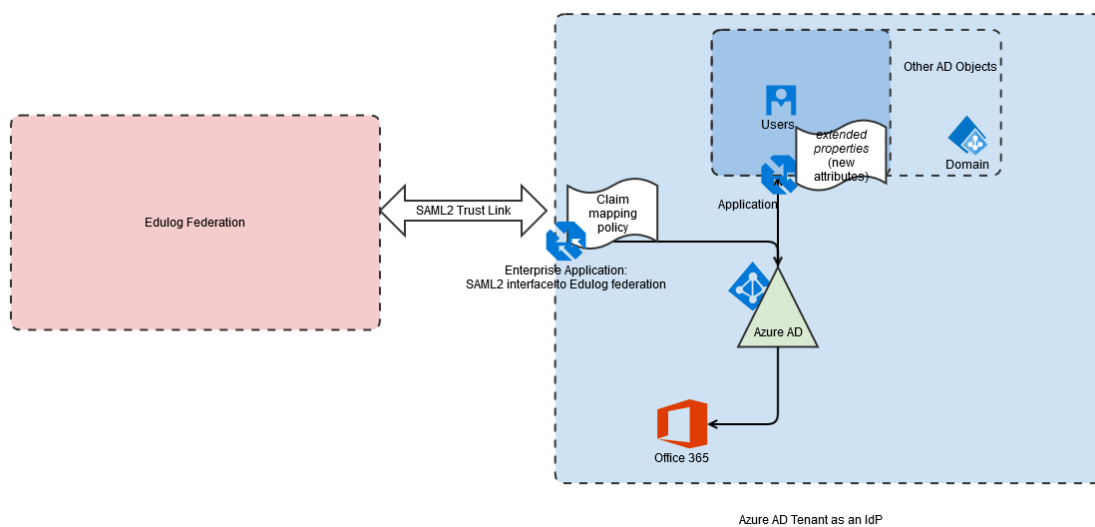
2.2 Bemerkungen

Azure AD enthält nur eine Teilmenge der Attribute, die im Schema eines lokalen *AD* vorhanden sind. Um die Attribute zu erweitern, können Sie *Microsoft Graph* oder *Powershell* verwenden.

Im Gegensatz zu AD, wo neue Attribute, die durch eine Erweiterung des AD-Schemas erstellt wurden, in Azure (Webinterface) sichtbar sind, müssen Sie hier die beiden vorgenannten Tools verwenden, um sie zu sehen.

2.3 Erforderliche Elemente

Das folgende Diagramm zeigt die Elemente, die benötigt werden, um einen vollständigen Azure-IdP zu erstellen, der sich mit Edulog verbinden kann.



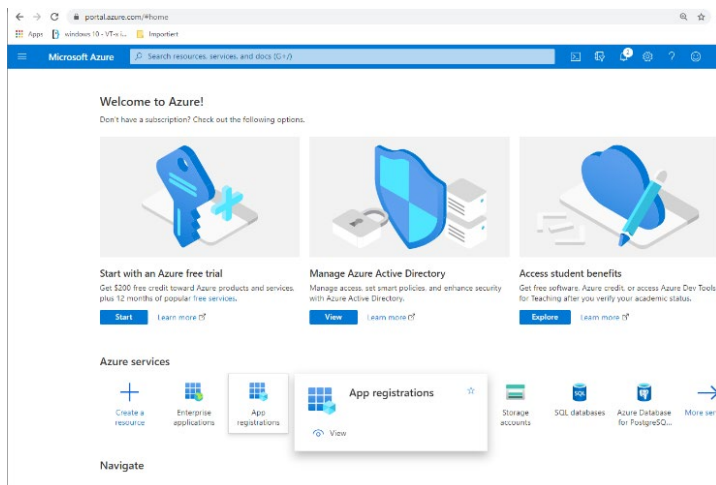
- Ein *Azure AD Tenant*
- Eine *application*
- Eine *Enterprise application*
- Eine *claim mapping policy*
- Die neuen Attribute (*extended properties*), die mit der *application registration* verbunden sind.

3. Erstellen einer *Application*

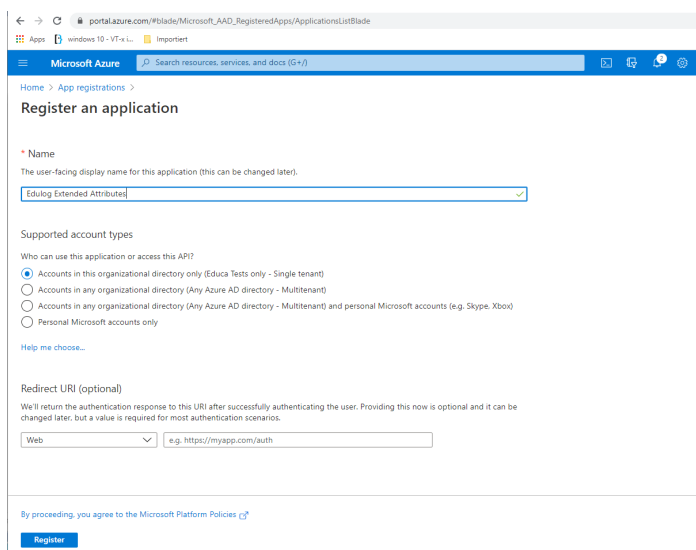
3.1 Über das *Azure*-Portal

Melden Sie sich bei Ihrem Konto an. Wählen Sie ggf. das richtige directory.

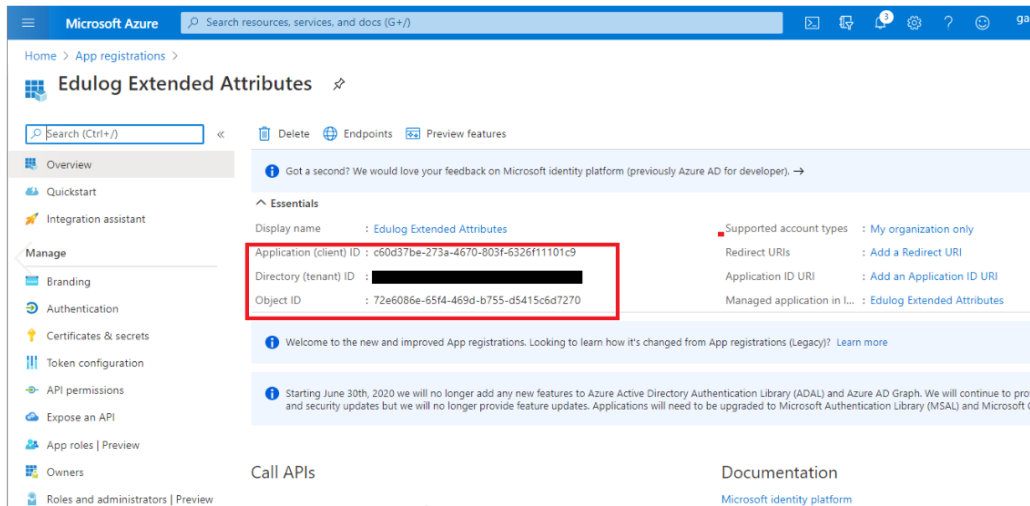
a. Gehen Sie zu «Application registrations»



b. Benennen Sie die Applikation (hier: «Edulog Extended Attributes»)



c. Notieren Sie die «Object ID» der Anwendung



4. Edulog-Attribute erstellen

Es wird ein *Powershell*-Skript verwendet. Es ermöglicht,

- sich mit unserem *Azure AD Tenant* (und mit dem verwendeten *directory*, falls es mehrere gibt) zu verbinden
- die «ObjectID» der im vorherigen Punkt erstellten Anwendung abzurufen («EduLog Extended Attributes»)
- die Attribute mit der Funktion **New-AzureADApplicationExtensionProperty** zu erstellen.
- zu überprüfen, ob die Attribute mit der Funktion **Get-AzureADApplicationExtensionProperty** korrekt erstellt wurden.

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

# 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}

Der letzte Befehl *Get-AzureADApplicationExtensionProperty* zeigt die Attribute der «extended property». Der Name dieser Attribute entspricht dem folgenden Format:

extension_Nummer der ObjectId der Application «Edulog Extended Attributes»_ Name des Attributs

Zum Beispiel: *extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonTechID*

Beachten Sie, dass das Format der «Object ID» das Symbol «-» nicht enthält.

5. Anlegen eines Testbenutzers

- Erstellen Sie einen Testbenutzer (entweder über die Azure-Schnittstelle oder mit Powershell).
- Fügen Sie den neuen Attributen Werte hinzu (nur mit *Powershell* oder *Microsoft Graph*), entsprechend der im Dokument «Leitfaden zu den Attributen für Identitätsanbieter» definierten Syntax.¹

```
# Erstellen eines Benutzers

$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"

# Werte der extended attributes zum Benutzer hinzufügen

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

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

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

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

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

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

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

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

¹ Verfügbar unter <https://edulog.ch/de/beitritt/dokumentation>

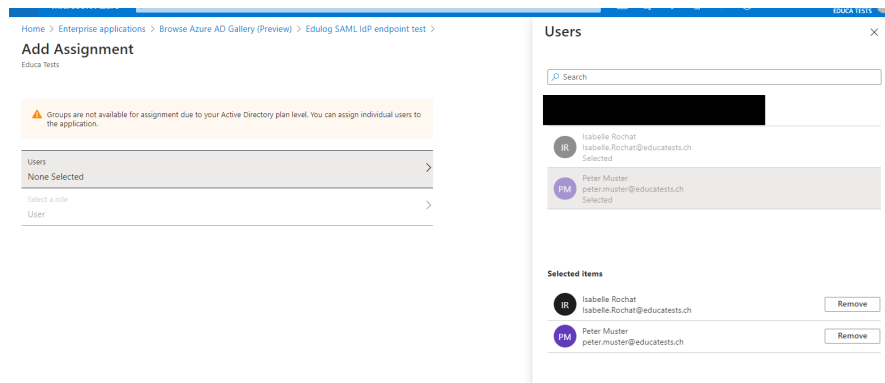
6. Erstellen einer *Enterprise Application*

Azure unterscheidet zwischen *Applications* und *Enterprise Applications*. Die beiden Arten von Funktionen unterscheiden sich in bestimmten Aspekten. Die *Application* kann die neuen Attribute empfangen, während die *Enterprise Application* uns erlaubt, die SAML-Verbindung so einzurichten, wie Edulog es verlangt.

- Gehen Sie zu *Enterprise Application* und wählen Sie «Create your own application».
- Benennen Sie die *Application*. Hier «Edulog SAML IdP endpoint test».

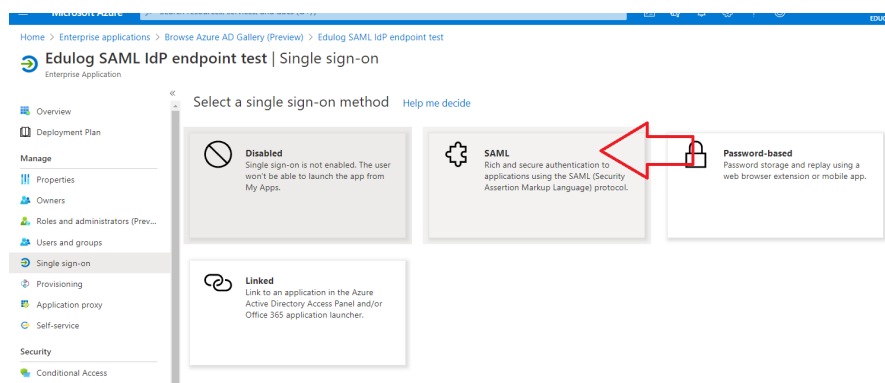
- Wählen Sie die Anwendung aus und gehen Sie zu «Assign users and groups»

- Wählen Sie die Benutzer oder die Gruppen aus, welche die von uns erstellte SAML-Schnittstelle verwenden können.²



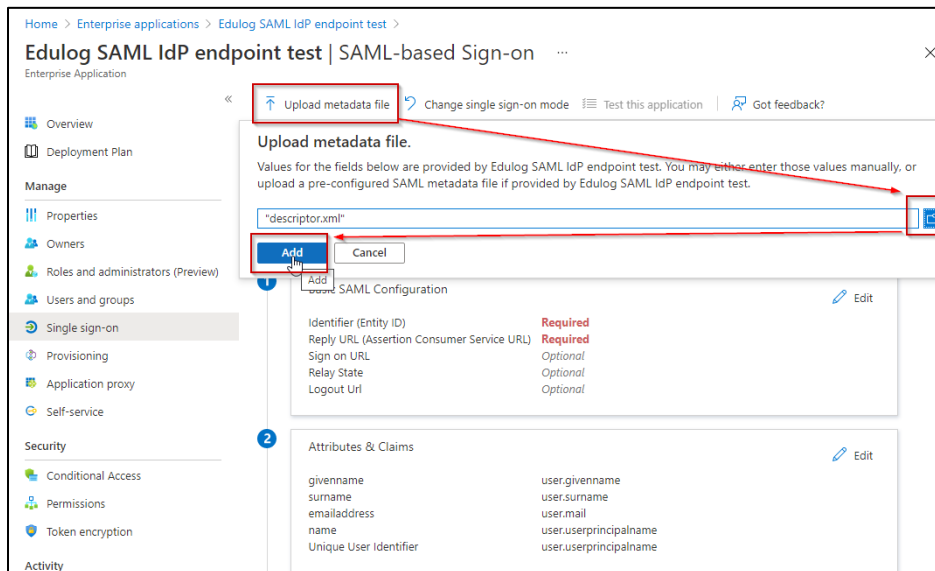
- Bestätigen Sie die Auswahl mit der Taste «Assign» unten links.

- Gehen Sie zu «Single sign-on» und wählen Sie «SAML»



² Aktionen auf Gruppen oder Gruppen von Benutzern können durchgeführt werden.

5. Importieren Sie die Metadaten, die sie von der ELCA AG erhalten haben



Versichern Sie sich, dass die drei folgenden Werte richtig eingefüllt sind:

- z.B.: <https://go.edulog.ch/auth/realms/edulog> setzen.
- «Reply URL (Assertion Consumer Service URL)»
 - z.B.: <https://go.edulog.ch/auth/realms/edulog/broker/school-idp/endpoint>
- «Logout Url»
 - z.B.: <https://go.edulog.ch/auth/realms/edulog/edulog-api/logout>

Speichern Sie anschliessend die Konfiguration: 

7. Erstellen einer *claim mapping policy*

Es ist nicht möglich, die neuen Attribute für Edulog auszuwählen, um den Teil «User Attributes & Claims» in der «SAML-based sign-on» Konfiguration der neu erstellten *Enterprise Application* zu konfigurieren.³

Dazu muss unter *Powershell* (oder *Microsoft Graph*) eine *claim mapping policy* erstellt werden, die es ermöglicht, die in der SAML-response des definierten IdP gesendeten Attribute zu definieren. Es ist dann möglich, die Attribute («extended») für Edulog auszuwählen und sie mit dem gewünschten Namen zu versehen, damit sie von Edulog identifiziert werden können.

Im Folgenden wird beschrieben, wie Sie eine solche *policy* erstellen, die wir *ClaimsEdulog* nennen.

Sie müssen den Befehl **New-AzureADPolicy** verwenden.

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

{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonBirthDate","SamlClaimType": "EdulogPersonBirthDate"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonRole","SamlClaimType": "EdulogPersonRole"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonLevel","SamlClaimType": "EdulogPersonLevel"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonCycle","SamlClaimType": "EdulogPersonCycle"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonCanton","SamlClaimType": "EdulogPersonCanton"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_EdulogPersonTechID","SamlClaimType": "EdulogPersonTechID"},

{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_o","SamlClaimType": "o"},
{"Source":"user","ExtensionID":"extension_YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY_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"
```

Laut *Azure* wird das Schlüsselwort *ExtensionID* verwendet, um *extended attributes* zu identifizieren. Im Falle von Attributen, die in *Azure AD* vorhanden sind, wählen Sie das Schlüsselwort *ID*.

Der erste Name entspricht dem Attributnamen in *Azure AD* (z. B.: *extension_YYY_title*). Der zweite, nach *SamlClaimType*, ist der Name des Attributs in der *SAML-response* von *Azure* an Edulog.

³ Dies funktioniert nur mit einer hybriden Infrastruktur, die ein lokales AD enthält, dessen Schema geändert und in *Azure* mit *AD Connect Sync* propagiert wurde.

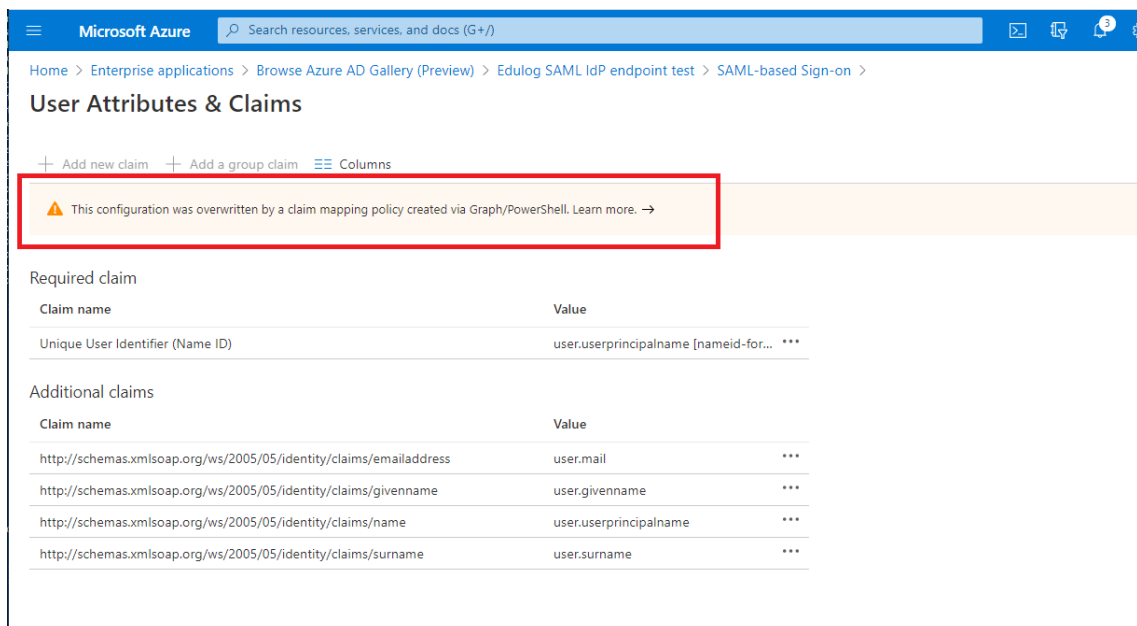
Um die Erstellung der *policy* zu überprüfen, verwenden Sie den Befehl: **Get-AzureADPolicy**.
Der unique identifier der *policy* hat die Form: `ZZZZZZZ-ZZZZ-ZZZZ-ZZZZ-ZZZZZZZZZZZZZZZZZ`

Schliesslich müssen wir nun die erstellte *claim mapping policy* mit der zuvor erstellten *Enterprise Application* verknüpfen. Verwenden Sie dazu den Befehl **Add-AzureADServicePrincipalPolicy**:

```
Add-AzureADServicePrincipalPolicy -Id YYYYYYYYY-YYYY-YYYY-YYYY-YYYYYYYYYYYYYYY
-RefObjectId ZZZZZZZ-ZZZZ-ZZZZ-ZZZZ-ZZZZZZZZZZZZZZZZZ
```

RefObjectId ist die eindeutige Kennung («ObjectID») der *policy* und **Id** ist die eindeutige Kennung der *Enterprise Application*.⁴

Überprüfen Sie die Anwesenheit der *claim mapping policy* in der *Enterprise Application* indem Sie auf den Konfigurationspunkt «User Attributes & Claims» gehen. Eine Meldung zeigt an, dass die Konfiguration von der genannten *policy* durchgeführt wurde.



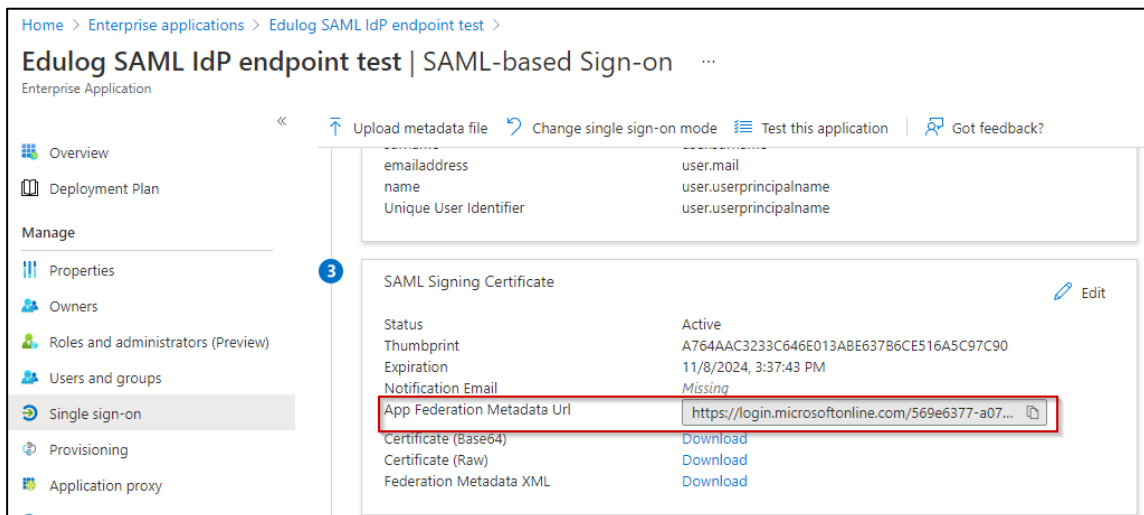
⁴ Es scheint nicht möglich zu sein, eine *claim mapping policy* mit einer einfachen *Application* zu verbinden.

8. IdP und Testbenutzer föderieren

a. Azure IdP föderieren

Dazu müssen Sie die Metadaten-URL der erstellten Enterprise Application abrufen (App Federation Metadata URL).

Senden Sie diese URL an den Technischen Betrieb der Föderation (ELCA AG). ELCA föderiert anschliessend Ihren IdP und stellt Ihnen im Gegenzug die Informationen zur Verfügung, die Sie zur Durchführung des Schrittes von Punkt 6.c.5 dieses Dokuments benötigen.



The screenshot shows the Azure portal interface for an Enterprise Application named 'Edulog SAML IdP endpoint test'. The left sidebar contains navigation options like Overview, Deployment Plan, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, and Application proxy. The main content area displays the application's configuration, including a table for user attributes and a section for the SAML Signing Certificate. The 'App Federation Metadata Url' is highlighted with a red box, showing the value: `https://login.microsoftonline.com/569e6377-a07...`

b. Einen oder mehrere Testbenutzer föderieren

Um die Föderationsvorgänge auszuführen, stehen APIs zur Verfügung. Ihre Funktionsweise wird im Dokument «Edulog API reference» beschrieben, das von der Geschäftsstelle Edulog bereitgestellt wird.

Um das *onboarding* mit den APIs zu automatisieren, gibt es folgende Möglichkeiten:

- SCIM unter Azure verwenden (vgl. «Leitfaden Azure AD SCIM»⁵);
- Ein Produkt vom Typ Postman verwenden;
- Die Benutzer mithilfe der von der Geschäftsstelle Edulog zur Verfügung gestellten PowerShell-Skripte föderieren.

Sobald diese beiden Vorgänge durchgeführt wurden (Föderierung des IdP und mindestens eines Testbenutzers), kann die Verbindung getestet werden.

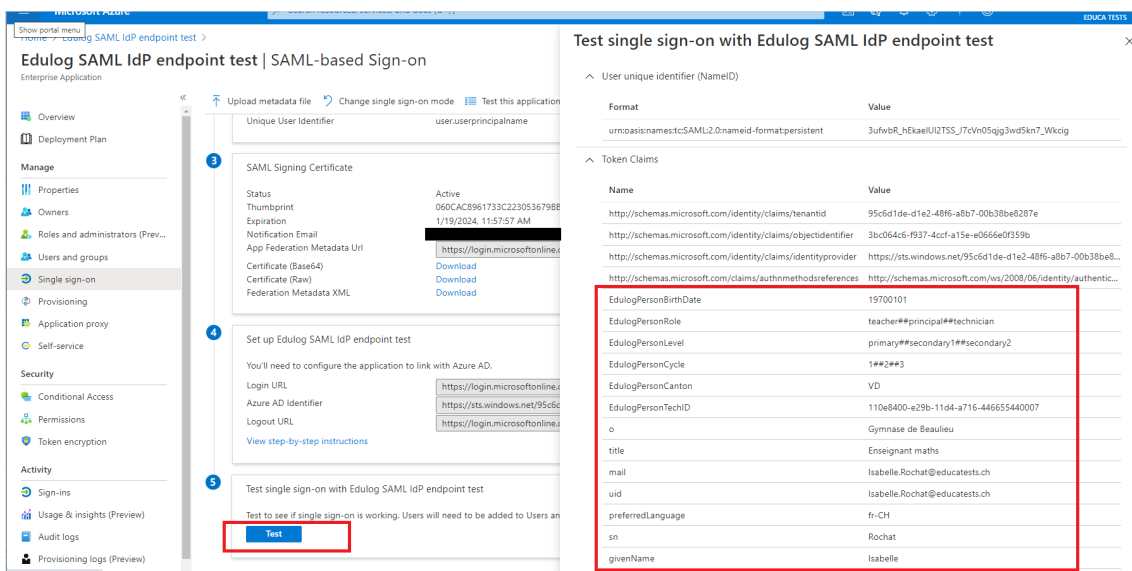
⁵ Verfügbar unter <https://edulog.ch/de/beitritt/dokumentation>

9. Interne Verbindungstests

Es ist möglich, die von der erstellten *Enterprise Application* gesendeten Attribute zu überprüfen, indem eine *Azure-Funktion* verwendet wird, die die Verbindung von einem internen SP simuliert. Diese Funktion finden Sie im Menü der Anwendung:

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

Auf der rechten Seite ermöglicht ein Menü die Verbindung mit dem Testbenutzer (hier: *Isabelle.Rochat@educatests.ch*). Nach der korrekten Authentifizierung sehen wir in der *SAML-response*⁶ eine Liste der gesendeten Attribute. Prüfen Sie, ob die Attribute mit denen übereinstimmen, die diesem Benutzer unter Punkt 5 dieses Dokuments zugewiesen wurden.



The screenshot shows the Azure portal interface for configuring an Enterprise Application. The main area displays the configuration for the 'Edulog SAML IdP endpoint test'. A 'Test single sign-on with Edulog SAML IdP endpoint test' dialog box is open on the right, showing the following token claims:

Name	Value
EdulogPersonBirthDate	19700101
EdulogPersonRole	teacher##principal##technician
EdulogPersonLevel	primary##secondary1##secondary2
EdulogPersonCycle	1##2##3
EdulogPersonCanton	VD
EdulogPersonTechID	110e8400-e29b-11d4-a716-446655440007
o	Gymnase de Beaulieu
title	Enseignant maths
mail	Isabelle.Rochat@educatests.ch
uid	Isabelle.Rochat@educatests.ch
preferredLanguage	fr-CH
sn	Rochat
givenName	Isabelle

10. Tests mit Edulog

Hinweis: Sie müssen zu Punkt 6 zurückgehen, um die «Reply-URL (Assertion Consumer Service URL)» gemäss den Anweisungen der für den technischen Betrieb von ELCA zuständigen Firma zu ändern.

11. Anhang: Nützliche Powershell-Befehle

Es lohnt sich, sich mit einigen Powershell-Befehlen für die policy vertraut zu machen. Insbesondere: *Remove-AzureADPolicy*, *New-AzureADPolicy*, *Get-AzureADPolicy*.

⁶ Sogenannte *Token claims* bei Azure.