

TECHNISCHES

Konfiguration eines *Microsoft Entra ID tenant* als IdP – SAML

12.2025 – Version 2.4

1.	Ziel des Dokuments	2
2.	Vorbedingungen	2
3.	Erstellung der Edulog-Attribute	3
3.1	Erstellung der erweiterten Attribute-Anwendung	3
3.2	Skript zum Hinzufügen der Attribute.....	5
3.3	Erstellung eines Testbenutzers.....	6
4.	Erstellung und Konfiguration der Edulog-Anwendung	6
4.1	Erstellung einer Enterprise-Anwendung.....	6
4.2	SAML-Metadaten der Anwendung.....	7
4.3	Single Sign-on-Konfiguration.....	8
5.	Konfiguration der automatischen Benutzerbereitstellung (mit SCIM)	12
5.1	Erhalt eines SCIM-Tokens	12
5.2	Konfiguration in Entra ID	13
5.2.1	Verbindung	13
5.2.2	Mappings	13
5.2.3	Test.....	16

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 <i>userPrincipalName</i>
givenName	Vorname	
sn	Name	
mail	E-Mail-Adresse	
EdulogPersonBirthDate	Geburtsdatum im Format JJJJMMTT	
preferredLanguage	Bevorzugte Sprache, unter den folgenden Werten: <i>de-CH, fr-CH, it-CH, rm-CH, en</i>	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: <i>pupil, teacher, administration, principal, legal_guardian, technician, other</i>	
EdulogPersonLevel	Bildungsstufe(n) unter den folgenden Werten: <i>primary, secondary1, secondary2, tertiary</i>	
EdulogPersonCycle	Bildungszyklus(en) unter den folgenden Werten: <i>0, 1, 2, 3</i>	
EdulogPersonCanton	Zwei-Buchstaben-Code des Kantons (z.B. <i>VD, BE, GE, ZH</i>)	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.

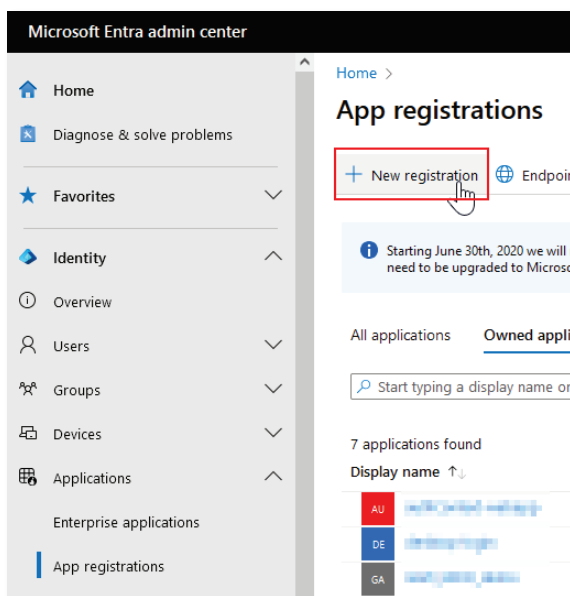
Wenn einige der von Edulog erwarteten Attribute nicht bereits als Benutzerattribute in Ihrem *Entra tenant* vorhanden sind, können Sie sie als zusätzliche Attribute oder «erweiterte Attribute» erstellen. In den Absätzen 3.1 bis 3.3 wird die Erstellung folgender Attribute beschrieben:

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*).



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: [v] e.g. https://example.com/auth

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

By proceeding, you agree to the Microsoft Platform Policies

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.

Microsoft Entra admin center

Home >

App registrations

+ New registration | Endpoints | Tr...

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

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 Entra-Modul verfügbar und importiert ist, und installieren Sie es gegebenenfalls.

```
# Check if module is available
Get-Module -Name Microsoft.Entra -ListAvailable

# If no output is shown, install the module
Install-Module -Name Microsoft.Entra -Repository PSGallery -Scope CurrentUser -Force -AllowClobber
```

Führen Sie das Powershell-Skript wie folgt aus:

```
# Entra ID tenant login - will ask for username and password
Connect-Entra -TenantId <Tenant ID> -Scopes "Application.ReadWrite.All","User.ReadWrite.All"

# Retrieving the application
$application = Get-EntraApplication -Filter "DisplayName eq 'Edulog Extended Attributes'"

# Creating the new Edulog attributes
New-EntraApplicationExtensionProperty -ApplicationId $application.Id -
  DataType "string" -Name "EdulogPersonBirthDate" -TargetObjects @("User")

New-EntraApplicationExtensionProperty -ApplicationId $application.Id -
  DataType "string" -Name "EdulogPersonRole" -TargetObjects @("User")

New-EntraApplicationExtensionProperty -ApplicationId $application.Id -
  DataType "string" -Name "EdulogPersonLevel" -TargetObjects @("User")

New-EntraApplicationExtensionProperty -ApplicationId $application.Id -
  DataType "string" -Name "EdulogPersonCycle" -TargetObjects @("User")

New-EntraApplicationExtensionProperty -ApplicationId $application.Id -
  DataType "string" -Name "EdulogPersonCanton" -TargetObjects @("User")

New-EntraApplicationExtensionProperty -ApplicationId $application.Id -
  DataType "string" -Name "o" -TargetObjects @("User")

New-EntraApplicationExtensionProperty -ApplicationId $application.Id -
  DataType "string" -Name "title" -TargetObjects @("User")

# Display the new attributes
(Get-EntraApplicationExtensionProperty -ApplicationId $application.Id).Name
```

Der letzte Befehl `Get-EntraApplicationExtensionProperty` 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
$additionalProperties = @{
    extension_<appID>_EduLogPersonBirthDate = "<value>";
    extension_<appID>_EduLogPersonRole = "<value>";
    extension_<appID>_EduLogPersonLevel = "<value>";
    extension_<appID>_EduLogPersonCycle = "<value>";
    extension_<appID>_EduLogPersonCanton = "<value>";
    extension_<appID>_o = "<value>";
    extension_<appID>_title = "<value>"
}

Set-EntraUser -UserId "<user principal name>" -AdditionalProperties $additionalProperties
```

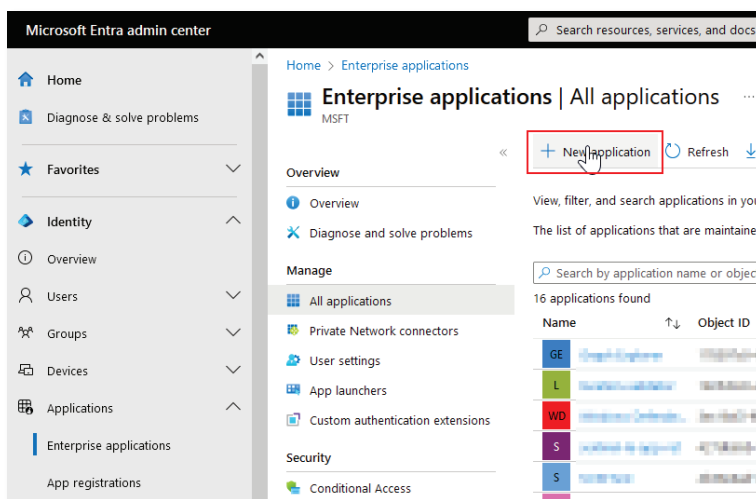
Beispiele von Attributen:

EduLogPersonBirthDate	20120119
EduLogPersonRole	pupil
EduLogPersonLevel	primary
EduLogPersonCycle	1
EduLogPersonCanton	VD
o	Ecole primaire de la Vallée##Institut Brenet
title	étudiante

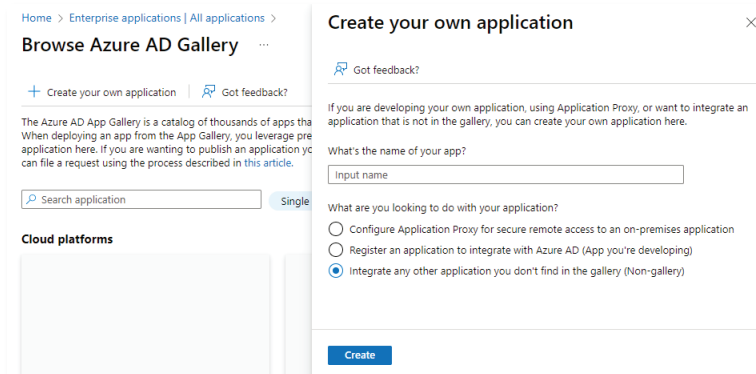
4. Erstellung und Konfiguration der Edulog-Anwendung

4.1 Erstellung einer Enterprise-Anwendung

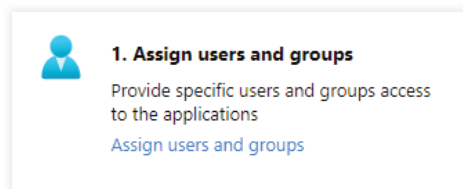
1. Navigieren Sie zu *Identity > Applications > Enterprise applications*.



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



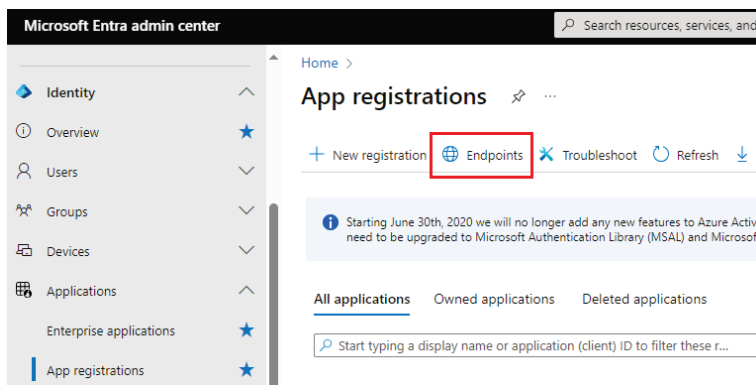
3. Geben Sie einen Namen ein und klicken sie auf «Create».



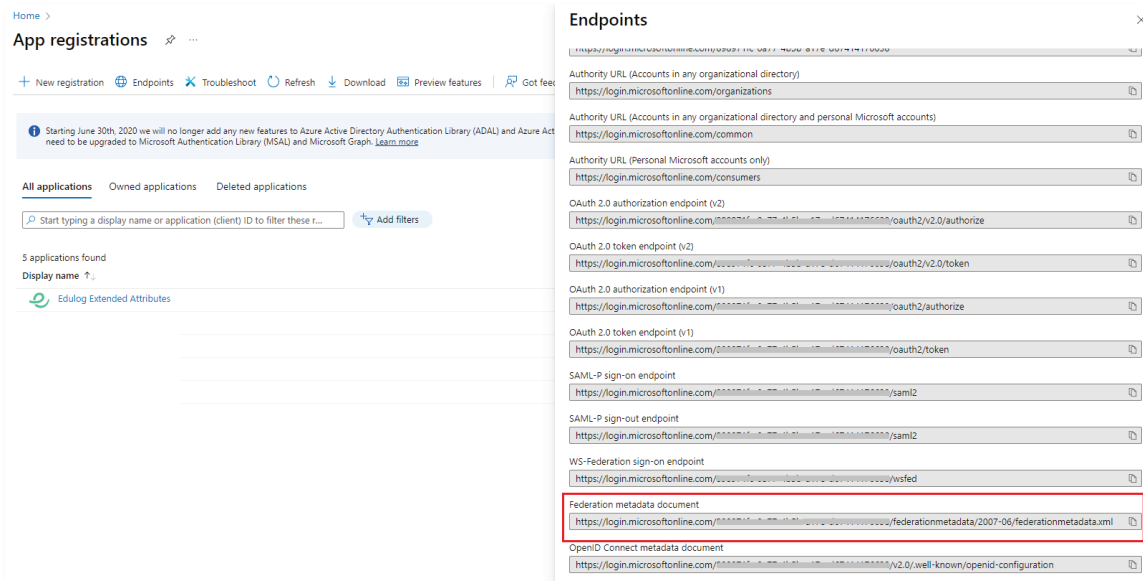
4. Weisen Sie die Testbenutzenden der erstellten Anwendung zu.

4.2 SAML-Metadaten der Anwendung

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

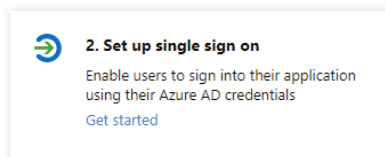


Senden Sie den Link zu diesem XML-Dokument (siehe Abbildung unten) an ELCA, verantwortlich für den technischen Betrieb und das Onboarding: onboarding_edulog@elca.ch.

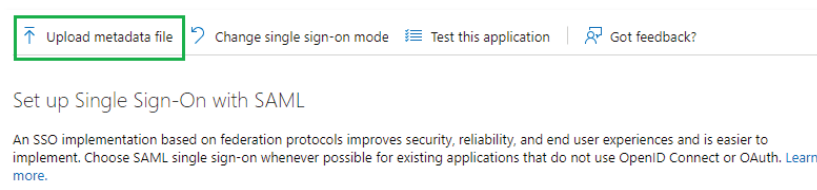


4.3 Single Sign-on-Konfiguration

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.



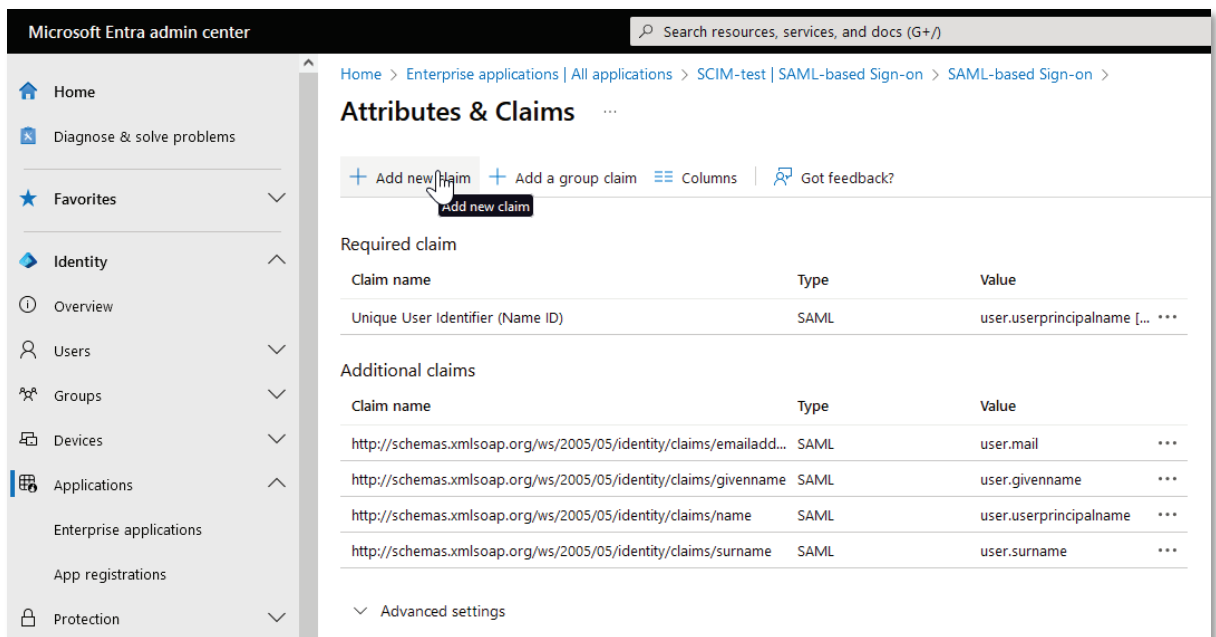
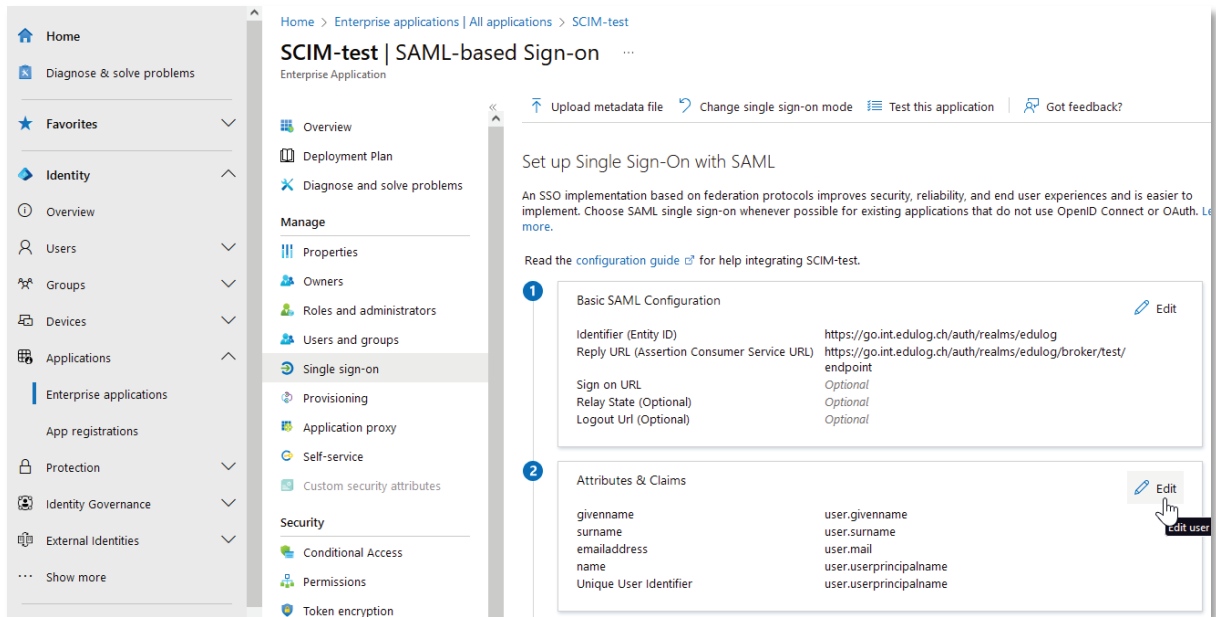
Wählen Sie «SAML» aus und laden Sie dann die vom Edulog-Onboarding-Team freigegebene Metadaten-datei hoch.



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

	Beispiel INT	Beispiel PROD
Identifizier (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.

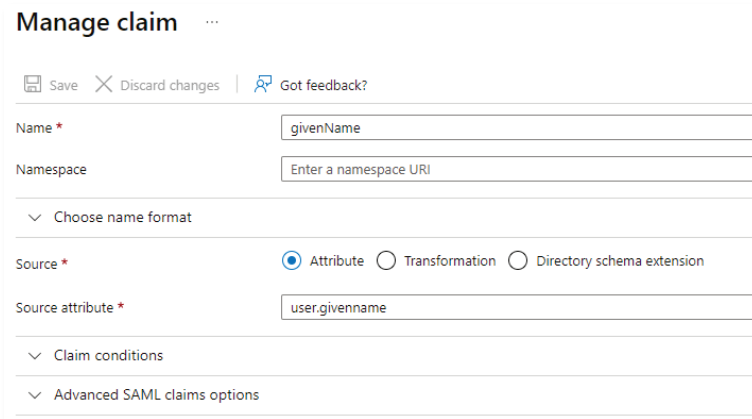


Alle Attribute, die unter §2 Voraussetzungen aufgeführt sind, müssen konfiguriert werden. Folgende drei Fälle werden unterschieden:

- Attribute, die bereits in Ihrem *tenant* vorhanden waren (in der Regel: *uid*, *givenName*, *sn*, *title*)
- Attribute, die als Erweiterungsattribute in §3 hinzugefügt wurden (in der Regel: *Edu-
logPersonBirthDate*, *Edu-
logPersonRole*, *Edu-
logPersonLevel*, *Edu-
logPersonCycle*)
- Attribute, die für jede Benutzerin, jeden Benutzer gleich sind (in der Regel: *preferredLanguage*, *o*, *Edu-
logPersonCanton*)

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).



Manage claim ...

Save | Discard changes | Got feedback?

Name *

Namespace

Choose name format

Source * Attribute Transformation Directory schema extension

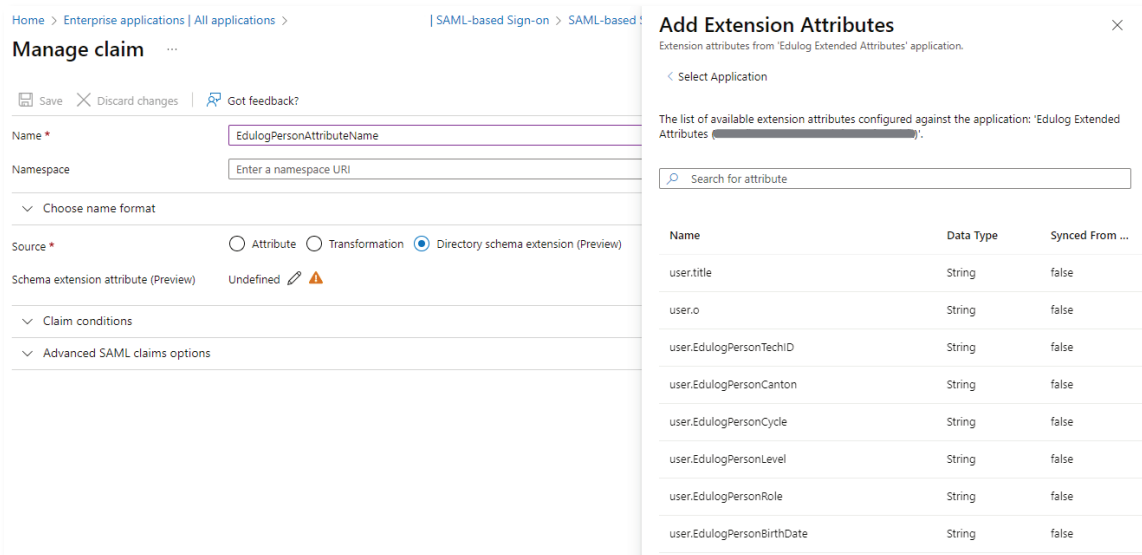
Source attribute *

Claim conditions

Advanced SAML claims options

b. 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.



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)  

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. Konstante Attribute

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

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. Eindeutige Benutzererkennung (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.

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. 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/edulog/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
```

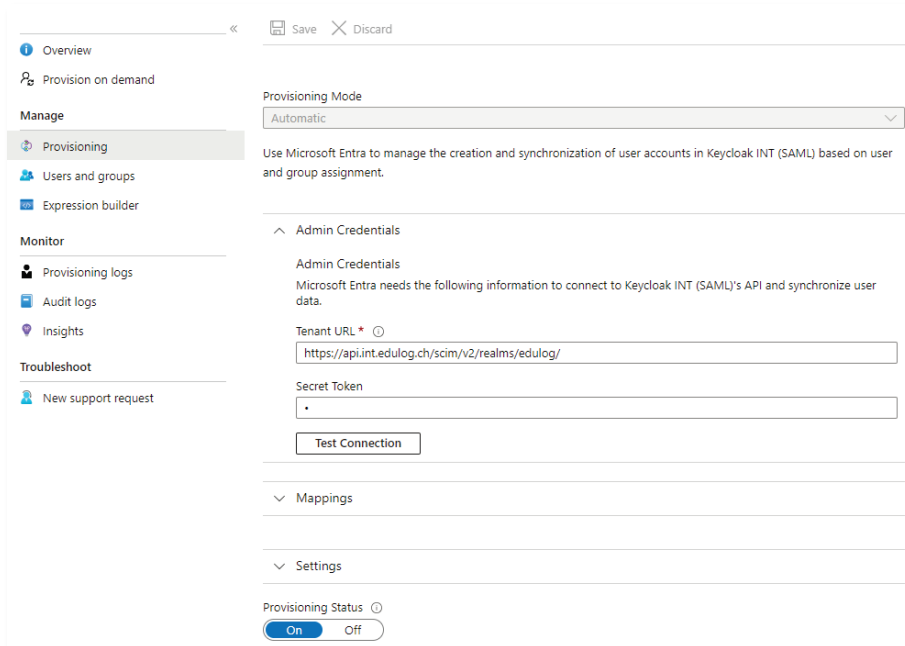
Kopieren Sie das <refresh token>, und achten Sie darauf, die Leerzeichen zu entfernen.

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.



Provisioning Mode: Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in Keycloak INT (SAML) based on user and group assignment.

Admin Credentials

Admin Credentials
Microsoft Entra needs the following information to connect to Keycloak INT (SAML)'s API and synchronize user data.

Tenant URL *

Secret Token

Mappings

Settings

Provisioning Status On Off

«Tenant URL»:

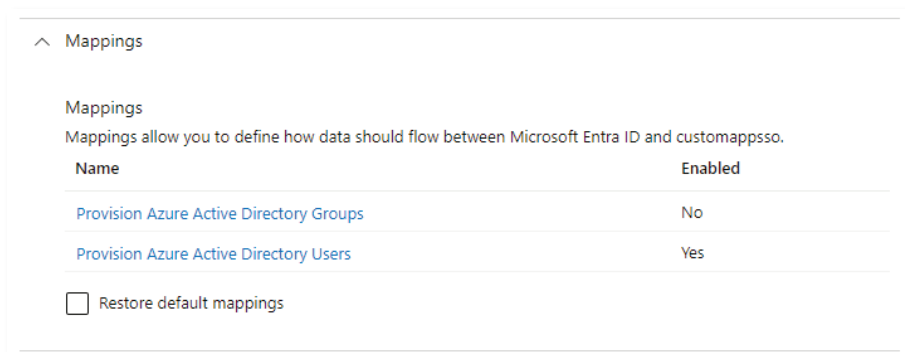
- <https://api.int.edulog.ch/scim/v2/realms/edulog/> (INT)
- <https://api.edulog.ch/scim/v2/realms/edulog/> (PROD)

«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.



Mappings

Mappings allow you to define how data should flow between Microsoft Entra ID and customappsso.

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

Restore default mappings

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

Klicken Sie auf das Kontrollkästchen «Show advanced options» und navigieren Sie zu «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.](#)

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?»

customappsso User Attributes

Name	Type	Primary Key?	Required?
id	String	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
active	Boolean	<input type="checkbox"/>	<input checked="" type="checkbox"/>
userName	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>
urn:ietf:params:scim:schemas:extension:Edulog:2.0:User:ahvn13	String	<input type="checkbox"/>	<input checked="" type="checkbox"/>

3. Speichern Sie die Änderungen.

Fügen Sie die folgenden Mappings hinzu:

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»: das Attribut, das Sie zum Speichern der AHV-Nummern verwenden

«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

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).

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

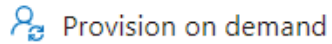
Match objects using this attribute
Yes

Matching precedence * ⓘ
1 ✓

Apply this mapping ⓘ
Always

5.2.3 Test

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.