Geschäftsstelle Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNISCHES

Erstellen einer Hybrid-Infrastruktur (lokales *AD* und *Azure AD*) für einen IdP

22.3.2021 – Version 1.0

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

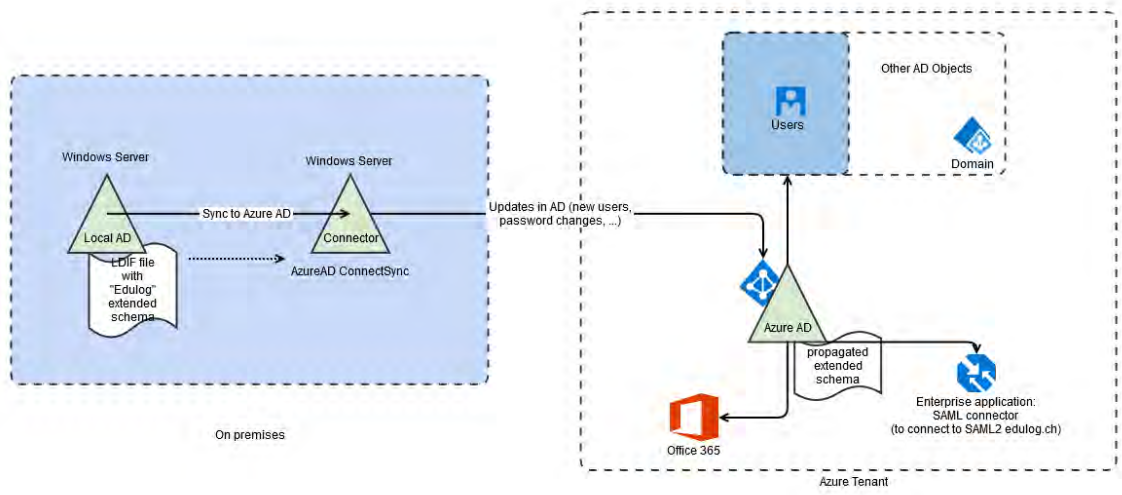
1. Ziel des Dokuments

Dieses Dokument erklärt Identitätsanbietern (IdP), wie sie eine hybride Infrastruktur (lokales AD und Azure AD) vorbereiten können.

Um Edulog beizutreten, müssen IdP:

- Überprüfen, ob ihre Identitäten eine bestimmte Anzahl von Attributen[1] haben. Einige dieser Attribute sind weder im ursprünglichen AD-Schema noch im Azure AD-Schema vorhanden. *Der erste Teil dieses Dokuments erklärt, wie Sie die AD-Schema-Erweiterung installieren, die Attribute propagieren und deren Verfügbarkeit verifizieren.*
- Im Besitz einer Infrastruktur mit einer SAML-Schnittstelle sein. *Der zweite Teil dieses Dokuments erklärt, wie Sie eine Enterprise Application in Azure einrichten, um diese Schnittstellenfunktion zu übernehmen.*

Dieses Dokument ist an IdP gerichtet, die ein lokales AD haben und Azure AD als SAML-Schnittstelle verwenden, um Verbindungen mit Edulog herzustellen.



[1] Diese Attribute sind im «Leitfaden Attribute – Identitätsanbieter» aufgeführt, verfügbar unter https://edulog.ch/de/beitritt/dokumentation

2. Vorbedingungen

Der vorliegende Leitfaden kann nur zur Anwendung kommen, wenn die folgenden technischen Voraussetzungen gegeben sind:

- Der IdP verwendet in seiner eigenen Infrastruktur ein AD (im folgenden Local AD genannt).
- Der IdP verwendet einen Server mit *Azure AD ConnectSync*, um die Attribute (zumindest die von Edulog verwendeten), mit seinem *Azure AD*-Konto zu synchronisieren.
- Der IdP hat einen *Azure-Tenant* mit *Azure AD*. Er verwendet *Azure AD* als SAML-Schnittstelle mit Edulog

3. Vollständiger Ablauf

Wir weisen an dieser Stelle auf die technischen Schritte[2] hin, die für einen IdP (mit der genannten Infrastruktur) notwendig sind, um die erforderliche Konfiguration für das Onboarding mit Edulog zu erreichen:

Nr.	Durchzuführende Massnahmen	Zeitpunkt
1	Installieren der AD-Schema-Erweiterung für Edulog.	Kapitel 4
2	Propagieren der Attribute mit *Azure AD ConnectSync* im *Azure-Tenant* und überprüfen, ob die neuen Attribute verfügbar sind.	Kapitel 4
3	Eine *Enterprise Application* (EA) erstellen.	Kapitel 5
4	Die EA konfigurieren: autorisierte Benutzer, SSO mit den notwendigen SAML-Parametern. Generieren einer metadata.xml-Datei.	Kapitel 6
5	Mit ELCA Kontakt aufnehmen, ihnen die Datei metadata.xml schicken.	Kapitel 6
6	Von ELCA bereitgestellte Daten beziehen und den SSO-Teil in der Azure-Holding mit den erforderlichen Daten ändern.	Kapitel 6
7	Verbindungstests mit ELCA durchführen.	Im Anschluss
8	Föderation der Identitäten mit ELCA durchführen	Im Anschluss

Dieses Dokument behandelt nur die Punkte 1 bis 6.

[2] Weitere nicht-technische Schritte (Verträge etc.) sind für ein Onboarding notwendig. Sie werden in diesem Dokument nicht behandelt.

4. Installieren der *AD*-Schema-Erweiterung für Edulog

Das Erweitern des AD-Schemas kann problematisch sein. Wird ein neues Attribut erstellt, gibt es keine Möglichkeit, es wieder aus dem Schema zu entfernen, falls man einen Fehler gemacht hat. Es ist daher vorzuziehen, dafür eine Datei zu verwenden, die die Attribute und ihre Eigenschaften enthält. Dazu kann eine LDIF-Datei verwendet werden.

Wichtig: Testen Sie immer, bevor Sie Änderungen am AD-Schema vornehmen!

Gesamter Prozess

1. Laden der neuen Attribute in das lokale AD-Schema:
   a. dem AD erlauben, das Schema zu ändern;
   b. die Visualisierung des Schemas ermöglichen;
   c. eine LDIF-Datei mit den neuen Attributen laden[3].
2. Verwenden Sie Azure AD ConnectSync, um die neuen Attribute von Azure AD zu propagieren.
3. Überprüfen Sie die Erstellung der neuen Attribute im Azure AD-Schema (und einige Testwerte).

LDIF Datei: Die aktuelle Version der LDIF Datei die in diesem Dokument verwendet wird können Sie von der Geschäftsstelle Edulog via info@edulog.ch anfragen.

4.1 Anlegen der neuen Attribute im lokalen AD-Schema

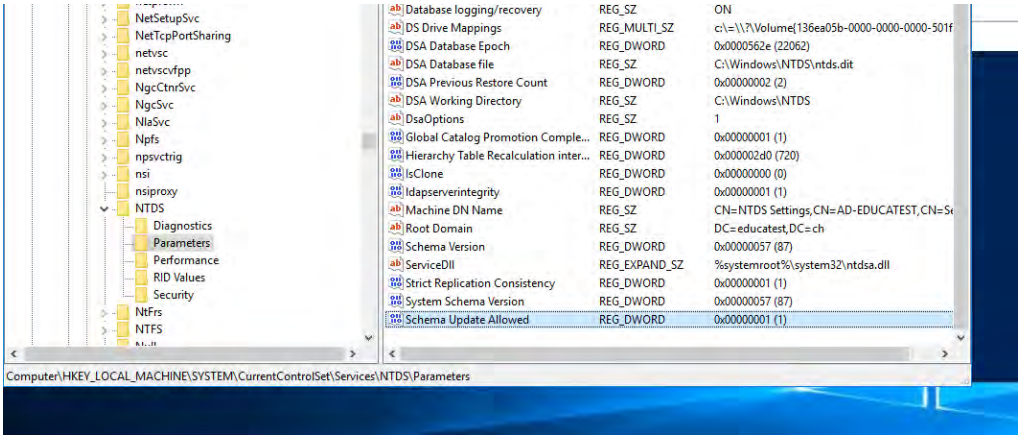
Bevor diese neuen Attribute erstellt werden können, müssen bestimmte Operationen an der AD durchgeführt werden. Der Zugriff muss mit «Schema Admin»-Rechten erfolgen (ein Domänenadministrator-Konto sollte in der Regel ausreichen). Wenn Ihre Infrastruktur mehr als einen «Domain Controller»-Server umfasst, muss der Zugriff auf demjenigen erfolgen, der die Rolle des «Schema Master» hat.

4.1.2 Erlauben einer Änderung des *AD*-Schemas

Es muss ein Registrierungsschlüssel hinzugefügt werden unter HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters.

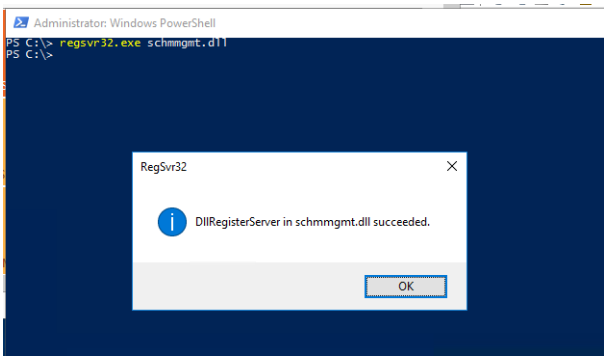
Der Name des neuen Schlüssels muss «Schema Update Allowed» mit dem Wert 1 und dem Format REG_DWORD sein.

[3] Für diese Teilaufgaben kann das folgende Dokument von Microsoft verwendet werden: https://social.technet.microsoft.com/wiki/contents/articles/51121.active-directory-how-to-add-custom-attribute-to-schema.aspx

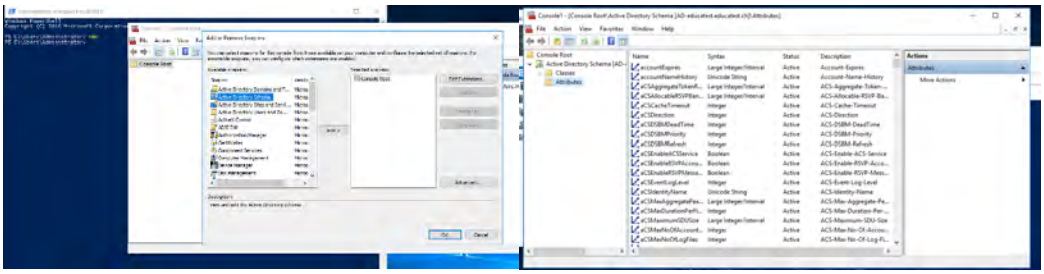


4.1.3 Schema-Visualisierung ermöglichen

Um das «Schema Management» in der MMC visualisieren zu können, müssen Sie zunächst auch die entsprechende DLL registrieren, indem Sie den Befehl *regsvr32.dll schmmgmt.dll* eingeben.



Sie können dann das Tool «Active Directory Schema» von MMC importieren und schließlich die Attribute des Schemas sehen:



4.1.4 Importieren der LDIF-Datei in *AD*

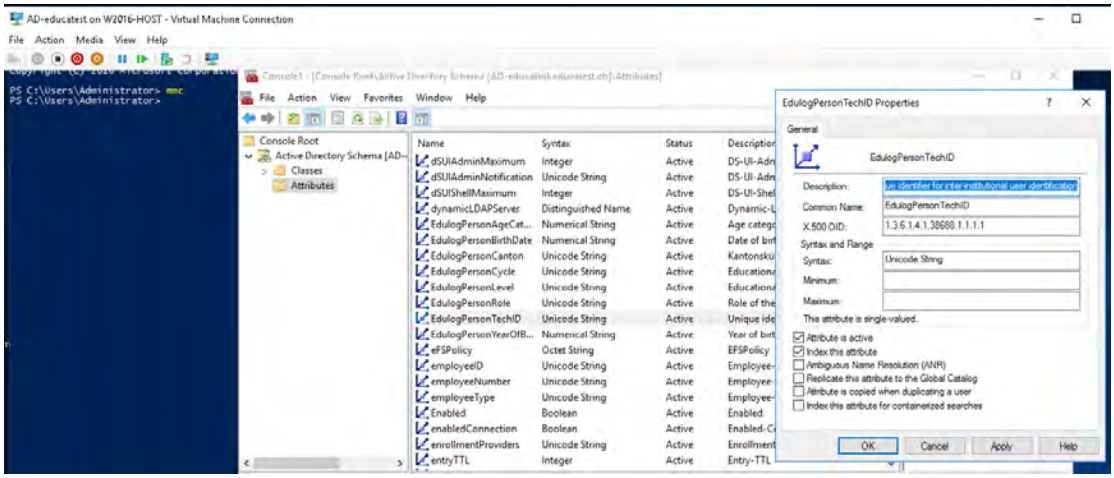
Um die LDIF-Datei mit den neuen Attributen in das AD-Schema zu importieren, müssen Sie (als Administrator des Schemas/der Domäne) den folgenden Befehl verwenden:

```
ldifde -i -f .\ldif_name_des_Datei.ldif -v -j .
```

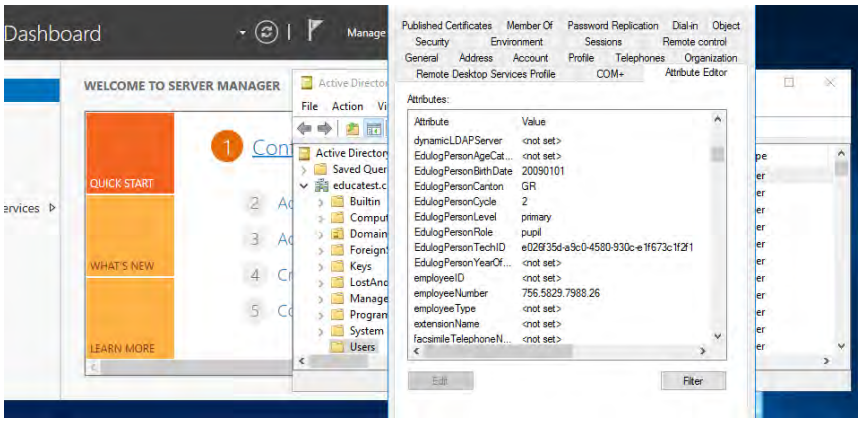
Wichtig: Die LDIF-Datei muss angepasst werden, um den Namen der Domäne zu berücksichtigen, in der sie verwendet wird (z. B.: DC=educatest,DC=ch, wenn die Domäne educatest.ch ist).

4.2 Merkmale der neuen Attribute im *AD*

Wenn der Import abgeschlossen ist, überprüfen Sie im Index des globalen Katalogs, ob die Attribute nun vorhanden sind.



Mit dem Verwaltungstool «Active Directory Users and Computers» ist es möglich, einige der neuen Attribute mit dem Attribut-Editor zu bearbeiten. Sobald die Synchronisierungsvorgänge abgeschlossen sind, können Sie auf diese Weise überprüfen, ob die Attribute in *Azure* vorhanden sind.

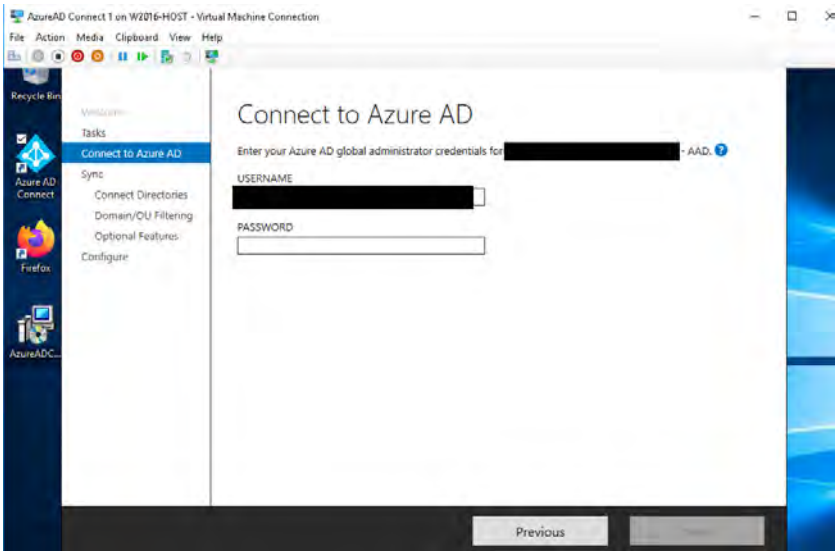


4.3 Konfigurieren des *Azure AD ConnectSync*-Dienstes

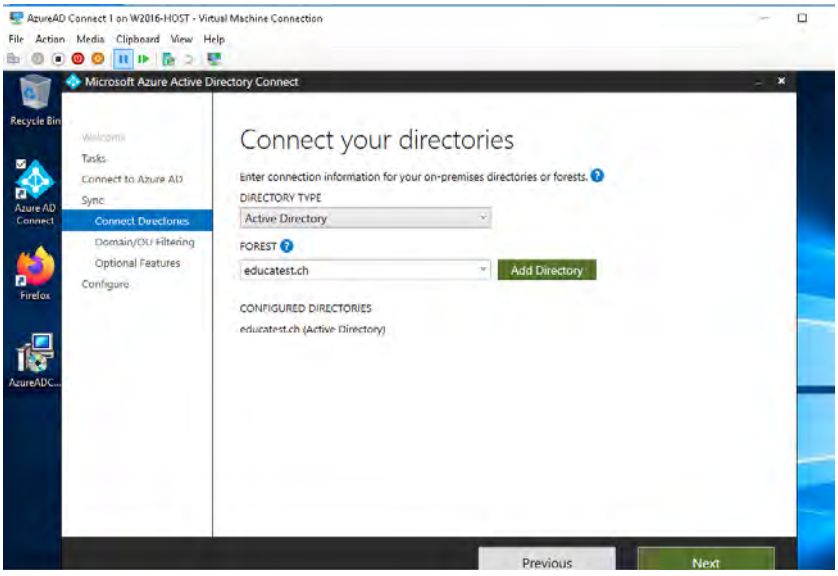
Um die neuen Attribute aus dem Schema in *Azure AD* zu exportieren, müssen Sie *AAD ConnectSync* verwenden. Dazu müssen Sie einen eigenen Server für dieses Tool haben.

Nachfolgend finden Sie chronologisch aufgelistet die verschiedenen Schritte der Konfiguration des Dienstes zur Synchronisation einer Domain/eines Forests (hier: educatest.ch).

4.3.1 Verbindung mit dem Administrationskonto des *Azure Tenant*

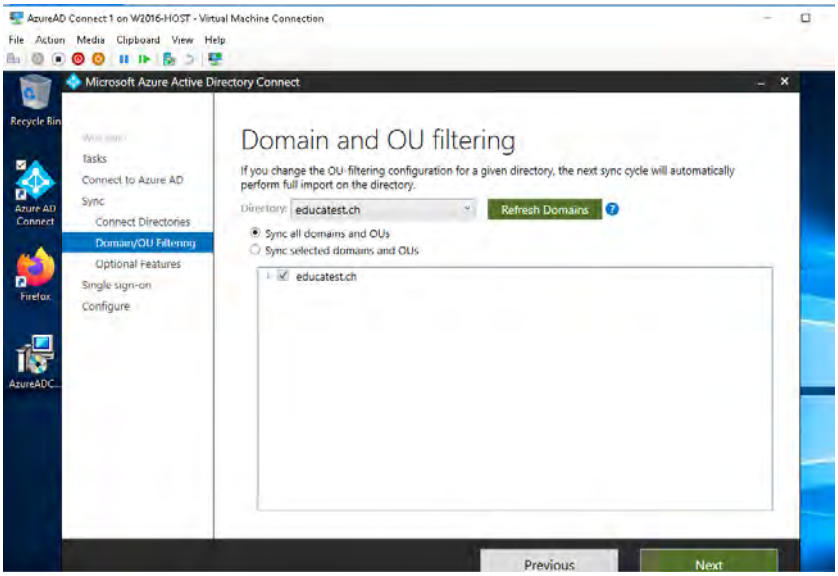


4.3.2 Typ und *forest* des *AD* auswählen

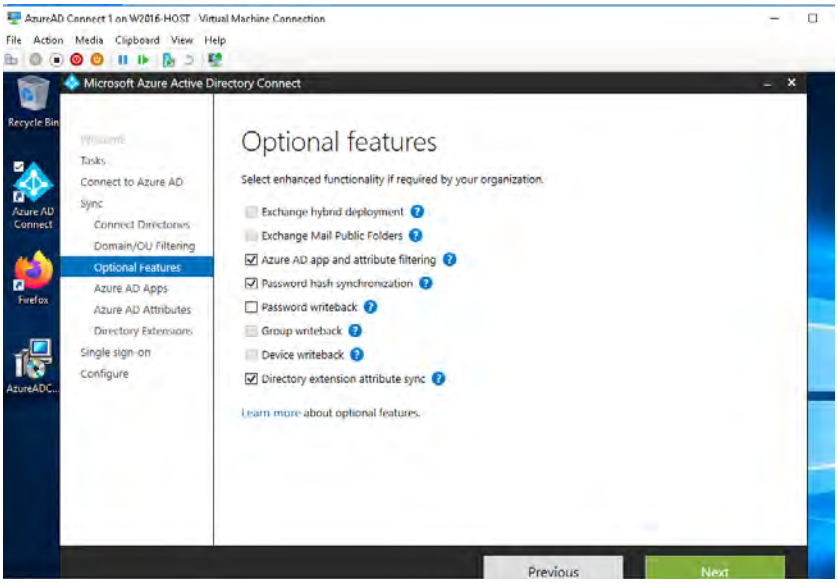


4.3.3 Organisatorische Bereiche und Abteilungen (OU) auswählen

Im Beispiel synchronisieren wir alle Domänen und OU des *AD*.



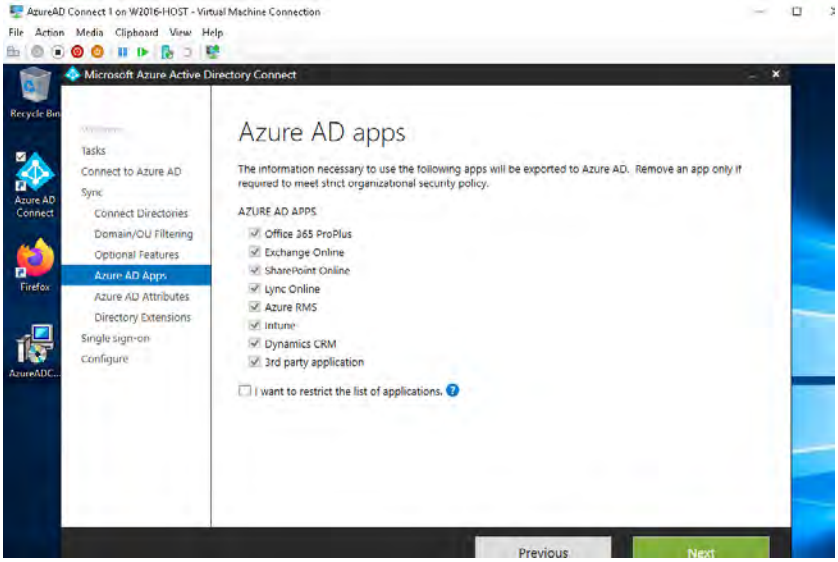
4.3.4 Konfigurieren der Synchronisations-Optionen



Passen Sie die Synchronisations-Optionen an ihre Infrastruktur an.

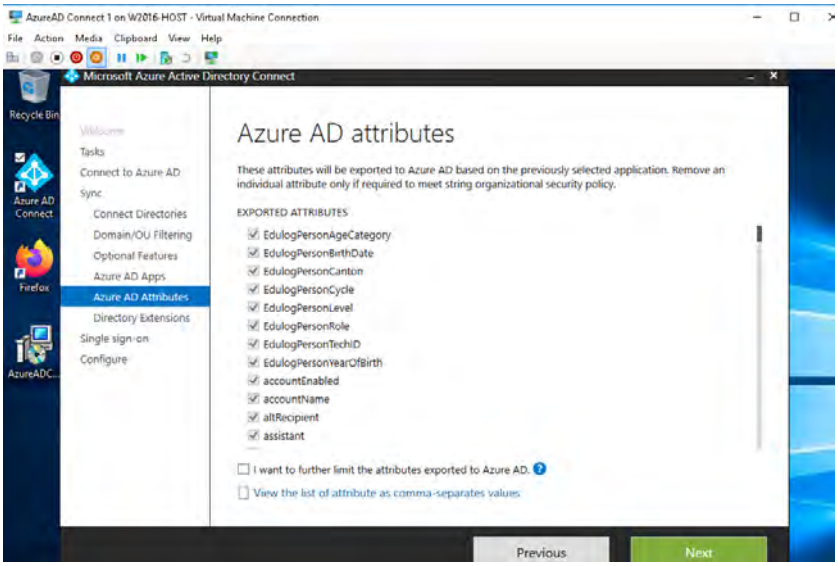
4.3.5 Auswählen von externen Anwendungen

Im folgenden Schritt können Sie die externen Anwendungen auswählen, mit denen Informationen aus dem AD geteilt werden sollen.



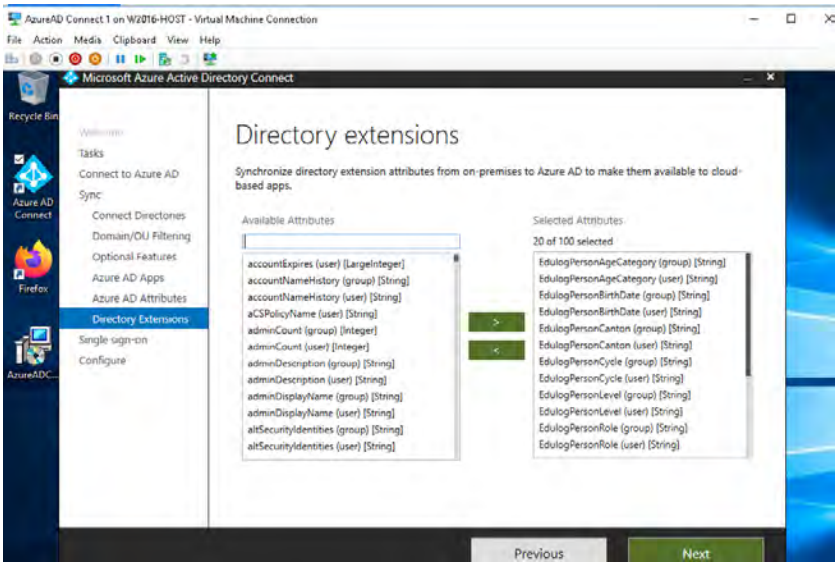
4.3.6 Zu exportierende Attribute auswählen

Wählen Sie die Attribute aus, die Sie auf *Azure* exportieren möchten. Vergessen Sie nicht die Edulog-Attribute!



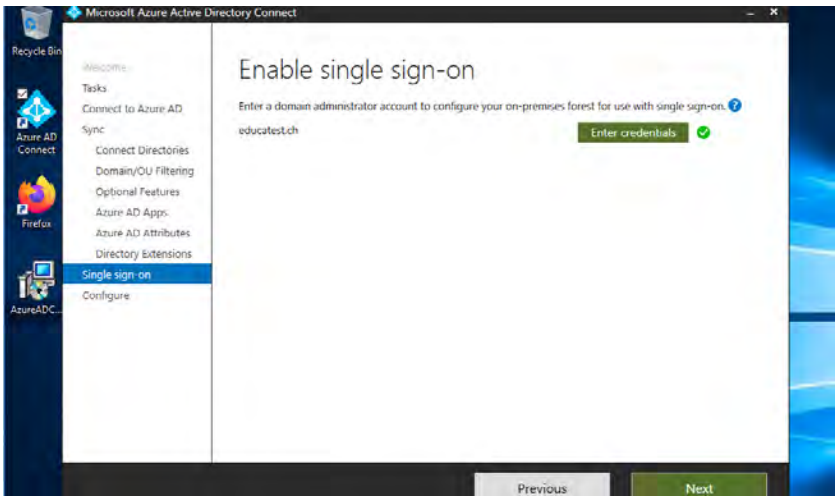
4.3.7 Directory extensions

Auswahl weiterer Attribute (falls erfoderlich)



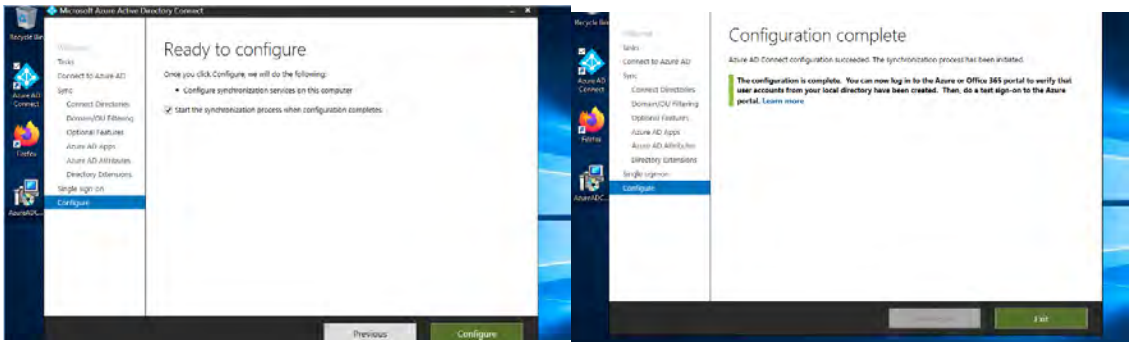
4.3.8 SSO konfigurieren

Um SSO einrichten zu können, müssen Sie sich mit einem Domänenadministrator-Konto anmelden.



4.3.9 Konfiguration validieren

Nachdem Sie die Optionen ausgewählt haben, drücken Sie die Taste «Configure». Es wird eine Reihe von Operationen durchgeführt. Eine Meldung, die anzeigt, dass die Konfiguration abgeschlossen ist, erscheint dann auf dem Bildschirm.



4.3.10 Hinweis

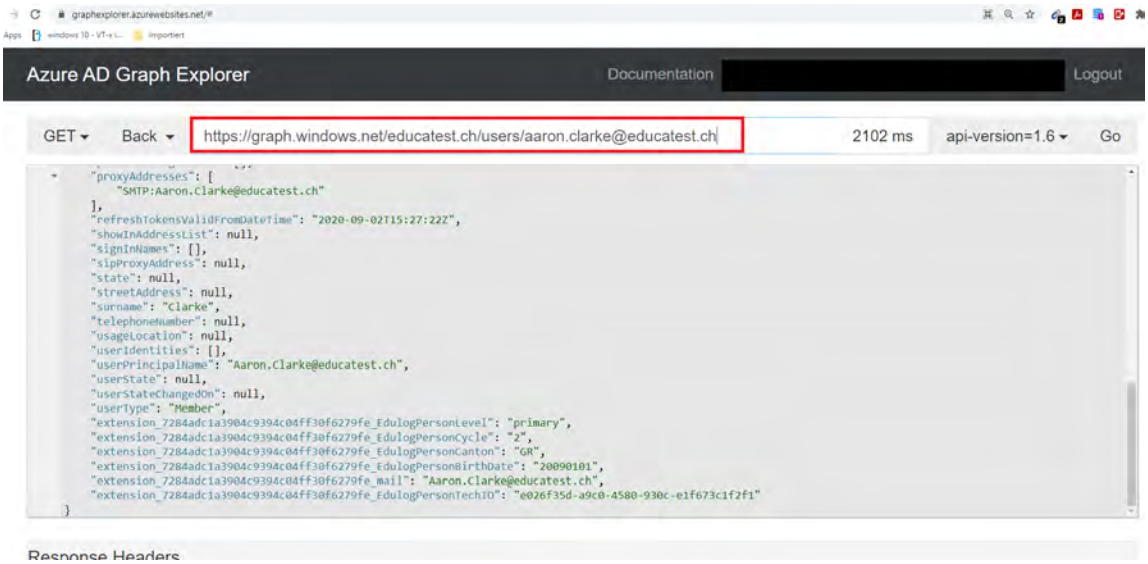
Die Benutzerattribute Ihres *AD* werden periodisch aktualisiert. Wenn Sie die Synchronisierung mit Ihrem *Azure*-Inhaber erzwingen möchten, verwenden Sie in Powershell (als Administrator, auf dem *Azure AD ConnectSync*-Server) den Befehl:

```
> Start-ADSyncSyncCycle
```

4.4 Überprüfen ob die Attribute im *Azure AD* vorhanden sind

Nach dem Abwarten der notwendigen Zeit für die Propagierung der Schemaänderungen - oder nach dem Erzwingen der Synchronisation - sind die neuen Attribute und ihre Werte unter *Azure* mit dem Tool https://graphexplorer.azurewebsites.net, mit dem notwendigen Bezug zum Benutzer und der betrachteten AD-Domäne sichtbar (siehe Bild).

Sie müssen mit dem *Tenant* verbunden sein, um darauf zugreifen zu können.



Sie können anschliessend überprüfen, ob die Edulog-Attribute des AD-Schemas in *Azure* vorhanden sind (sie sind aber nicht über portal.azure.com sichtbar!). Beachten Sie, dass das Format der Edulog-Attributnamen wie folgt ist:

extension_Nummer der eindeutigen ID Ihrer Anwendung_Name des Edulog-Attributs

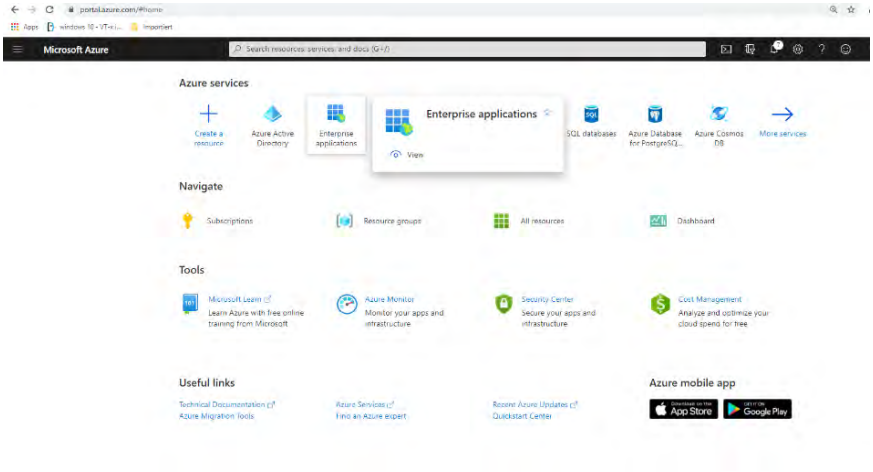
Beispiel: **extension_111222233344556667788889999eeffff_EdulogPersonCanton**

5. Erstellen einer *Enterprise Application*

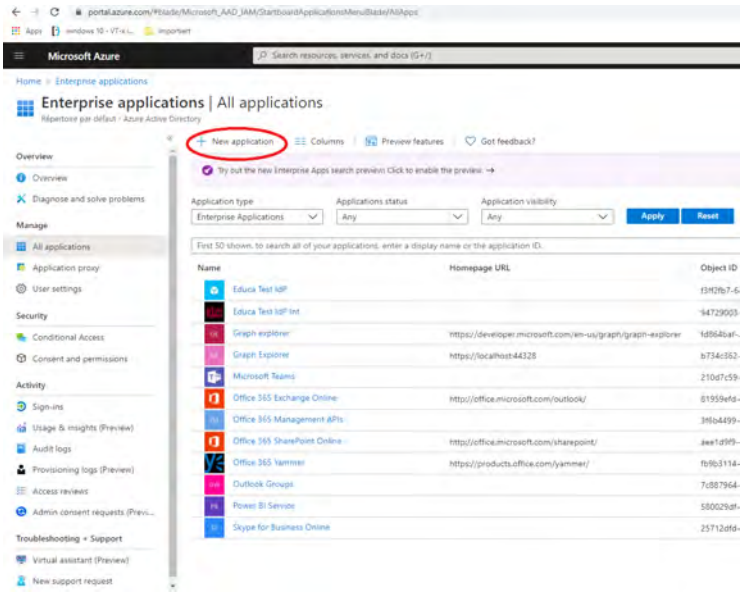
5.1 Auswahl der *Enterprise Application*

Die *Azure Enterprise Applications* ermöglichen nicht nur den Zugriff auf bestimmte Anwendungen, sondern auch die Definition von Ad-hoc-Anwendungen, die die Verwendung von vordefinierten Schnittstellen für den Zugriff auf unsere in *Azure AD* enthaltenen Identitäten ermöglichen.

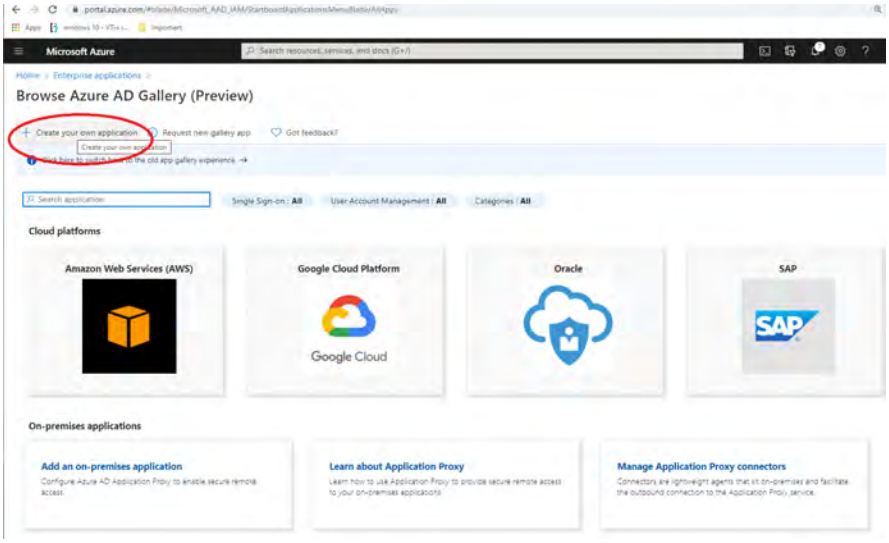
5.1.1 Klicken Sie auf «Enterprise applications»



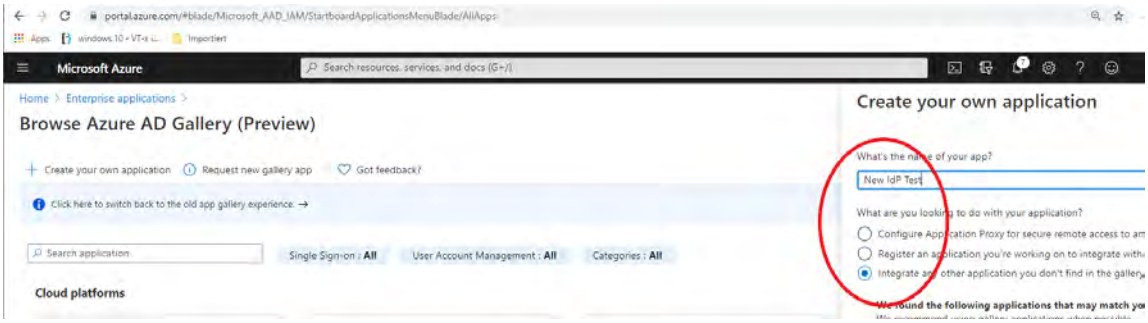
5.1.2 Klicken Sie auf «New application»



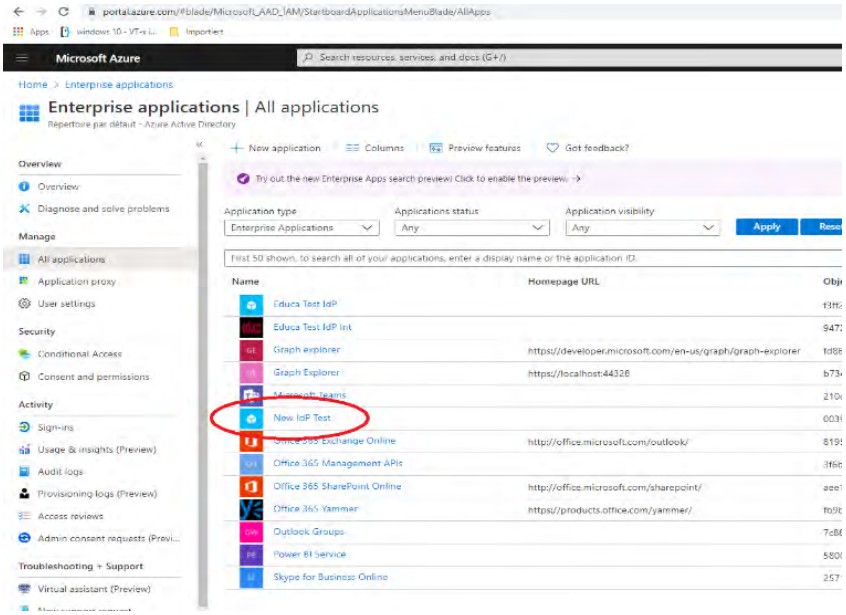
5.1.3 Wählen Sie «Create your own application» aus



5.1.4 Geben Sie Ihrer neuen Applikation einen Namen (hier: «New IdP Test») und wählen Sie «Integrate any other application...» aus



5.1.5 Stellen Sie sicher, dass die neue Applikation erstellt worden ist



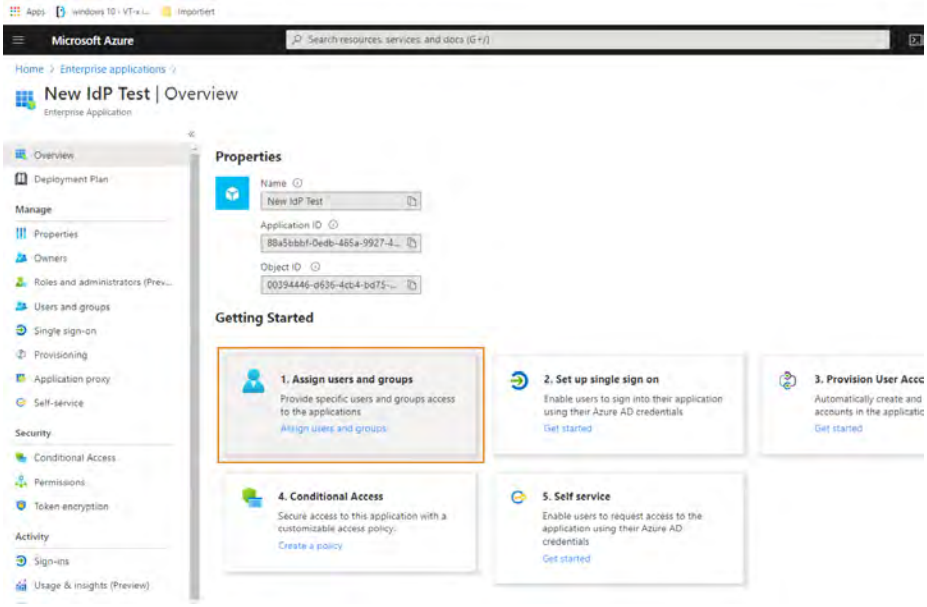
6. Konfiguration der *Enterprise Application*

Ist die Applikation erstellt, müssen Sie noch folgende Schritte vornehmen:

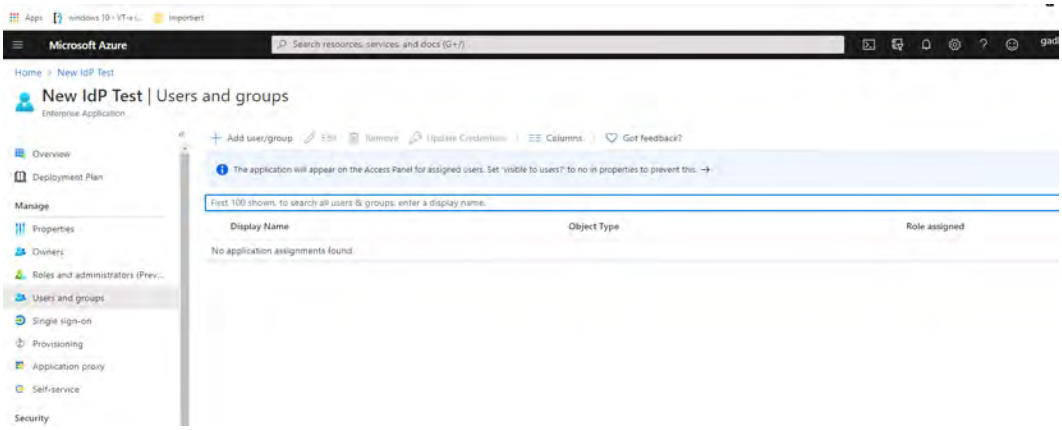
- Benutzende autorisieren, die Applikation zu nutzen
- SSO (und das SAML-Interface) konfigurieren
- Einen Verbindungstest durchführen (intern – nicht mit Edulog)

6.1 Autorisierung der Benutzenden

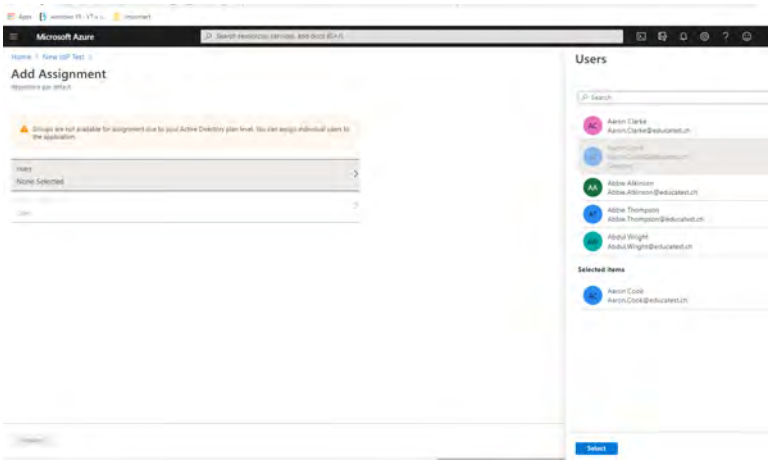
6.1.1 Öffnen Sie die erstellte Applikation



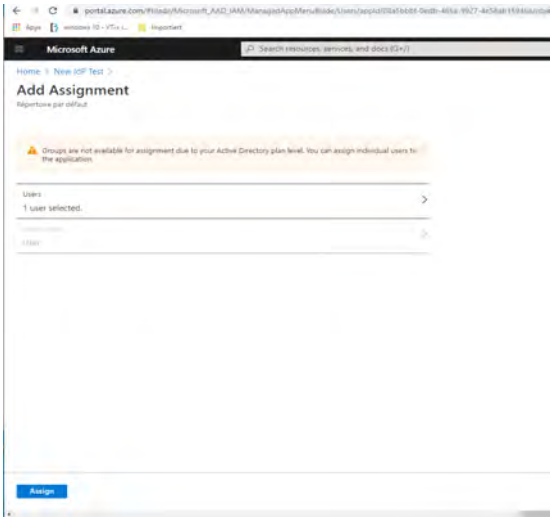
6.1.2 Klicken Sie auf «Users and Groups»



6.1.3 Wählen Sie einen Benutzer Ihres *Azure AD* aus (klicken Sie dazu auf «Select»)

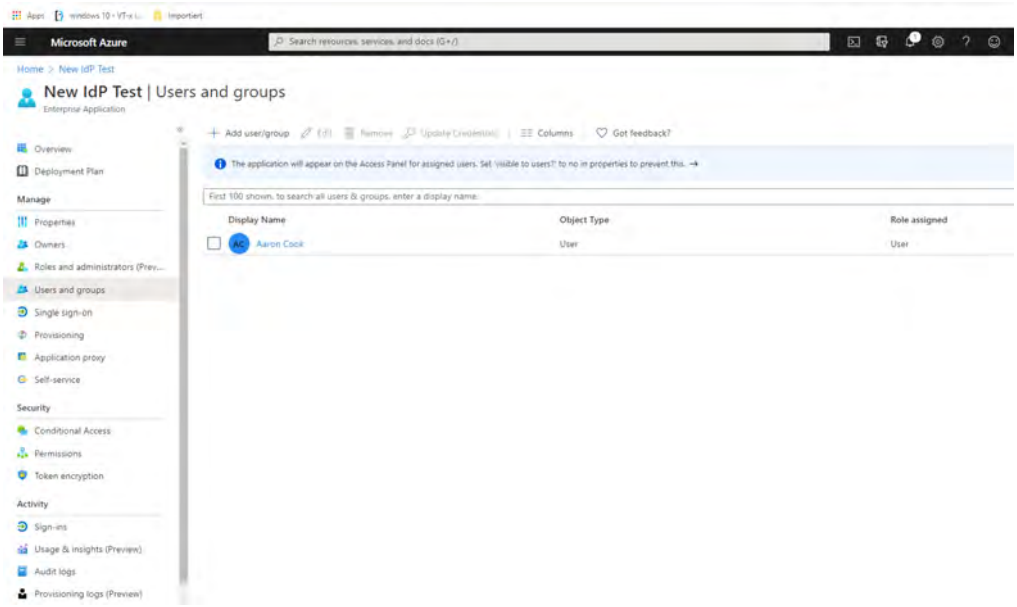


6.1.4 Klicken Sie auf «Assign » (per default ist die Rolle «user» zugewiesen)



In unserem Beispiel ist der ausgewählte Benutzer der einzige, der sich über SAML2 in der Anwendung authentifizieren kann. Es ist möglich, Berechtigungen auf Gruppenbasis zu erteilen oder *bulk operations* durchzuführen, um zu vermeiden, dass Sie dies einzeln pro Benutzer tun müssen.

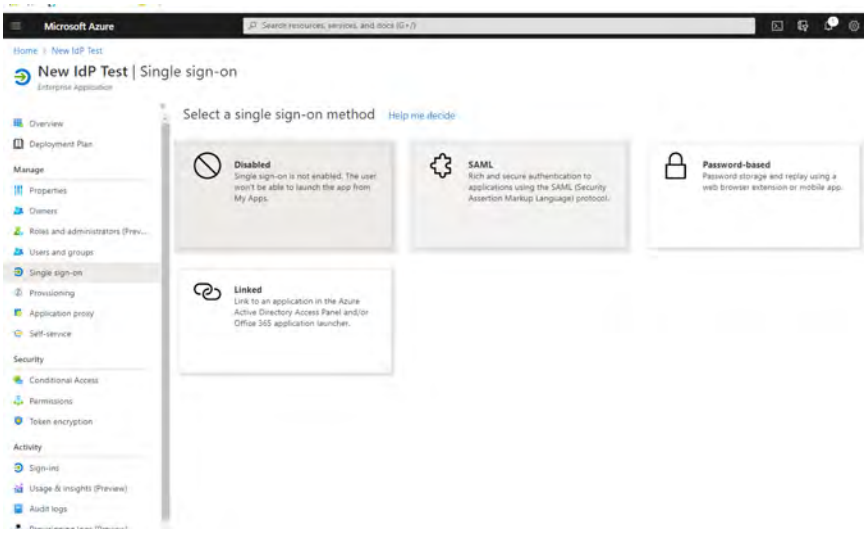
6.1.5 Benutzerauswahl abgeschlossen



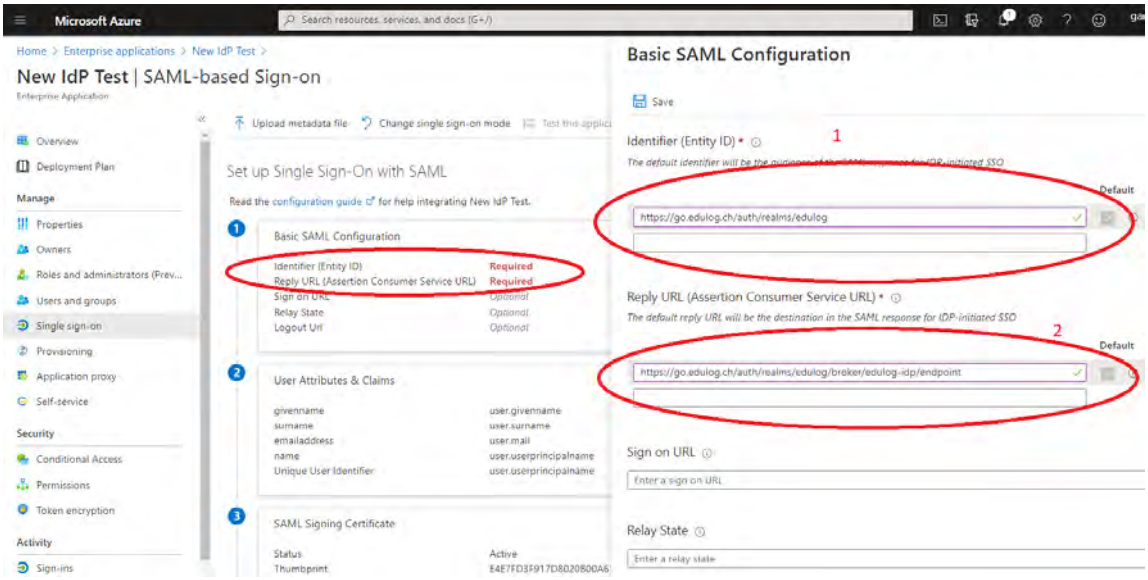
6.2 Konfiguration des SSO mit SAML

Die *Enterprise Applications* von *Azure* können *Single Sign On* (SSO) zur Authentifizierung verwenden. Es werden verschiedene Methoden vorgeschlagen, aber Edulog unterstützt nur SAML2. Wir werden nun die zuvor erstellte Anwendung für diesen Zweck konfigurieren.

6.2.1 Klicken Sie auf «Single Sign On» und dann auf «SAML»



6.2.2 Passen Sie die Parameter im Abschnitt «Basic SAML configuration» an



Zwei Werte sind erforderlich:

- «Identifier (Entity ID)»: auf https://go.edulog.ch/auth/realms/edulog setzen.
- «Reply URL (Assertion Consumer Service URL)»
  - Achtung! Den endgültigen Wert erhalten Sie während des Onboardings von ELCA. Sie müssen ihn zu diesem Zeitpunkt anpassen.
  - Sie müssen diesen Wert jedoch ausfüllen, um die Konfiguration abzuschließen. Als Beispiel können Sie hier https://go.edulog.ch/auth/realms/edulog/broker/edulog-idp/endpoint eingeben.

6.2.3 Die «User Attributes & Claims» bearbeiten

Standardmässig wählt Azure einige der Attribute Ihrer Benutzer aus, um SAML-Assertions zu erstellen. Diese müssen mit jenen Attributen ausgewechselt werden, die Ihr IdP an die Föderation Edulog senden muss. Hier ist ein Beispiel mit allen im Leitfaden zu den Attributen für Identitätsanbieter (IdP) veröffentlichten Attributen.

Wenn Sie das Schema Ihres *AD* geändert haben, wurden ihm Edulog-spezifische Attribute hinzugefügt. Mit der Synchronisation über *Azure AD ConnectSync* haben Sie diese auf Ihren *Azure-Tenant* übertragen. Sie entsprechen der Form:

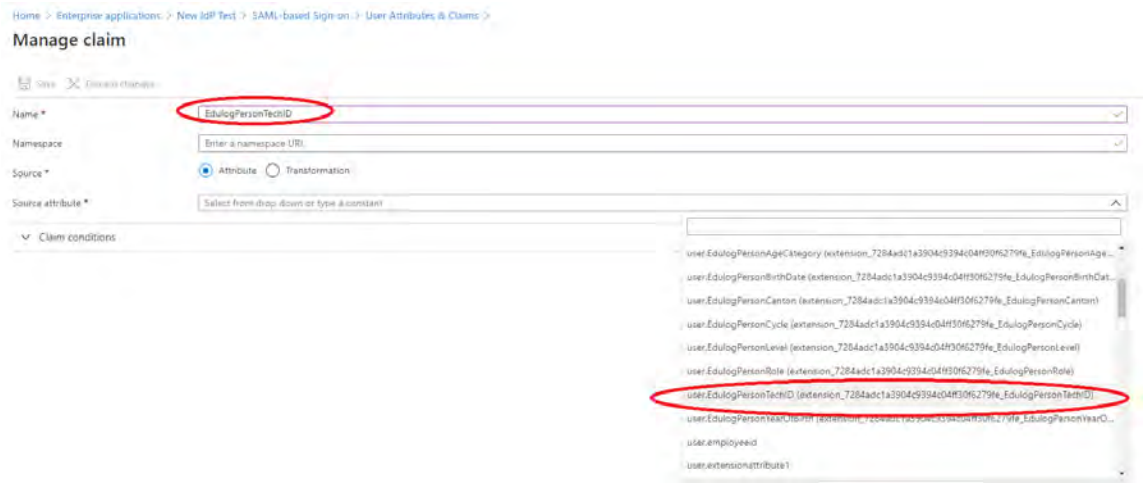
user.*Name des Edulog Attributs (extension_Unique ID ihrer Applikation_Name des Edulog Attributs)*

Beispiel:
user.EdulogPersonCanton (extension_111222233344556667788889999eeffff_EdulogPersonCanton)

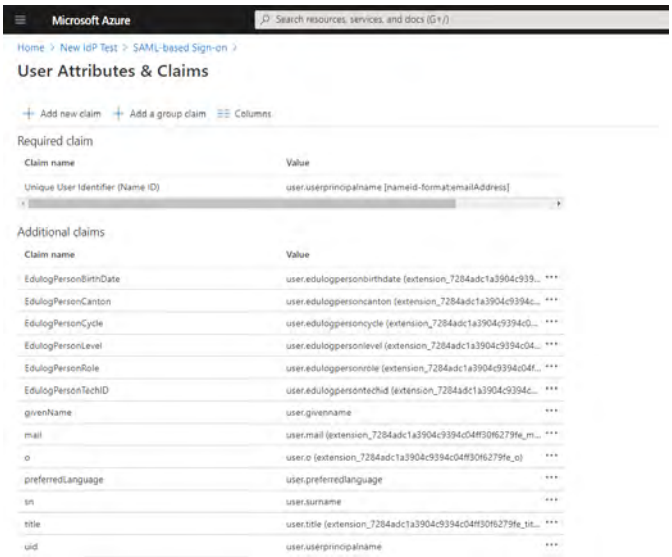
Sie müssen nun «Claims» erstellen, die die Attribute enthalten

- Der «Name» des Claims entspricht dem Namen des Attributs, das an die Föderation weitergegeben wird: Der Name muss mit dem im Leitfaden Attribute übereinstimmen.
- Die «Source» muss auf «Attribute» gesetzt werden.
- Die «Source attribute» muss mit dem ausgewählten Attribut übereinstimmen.

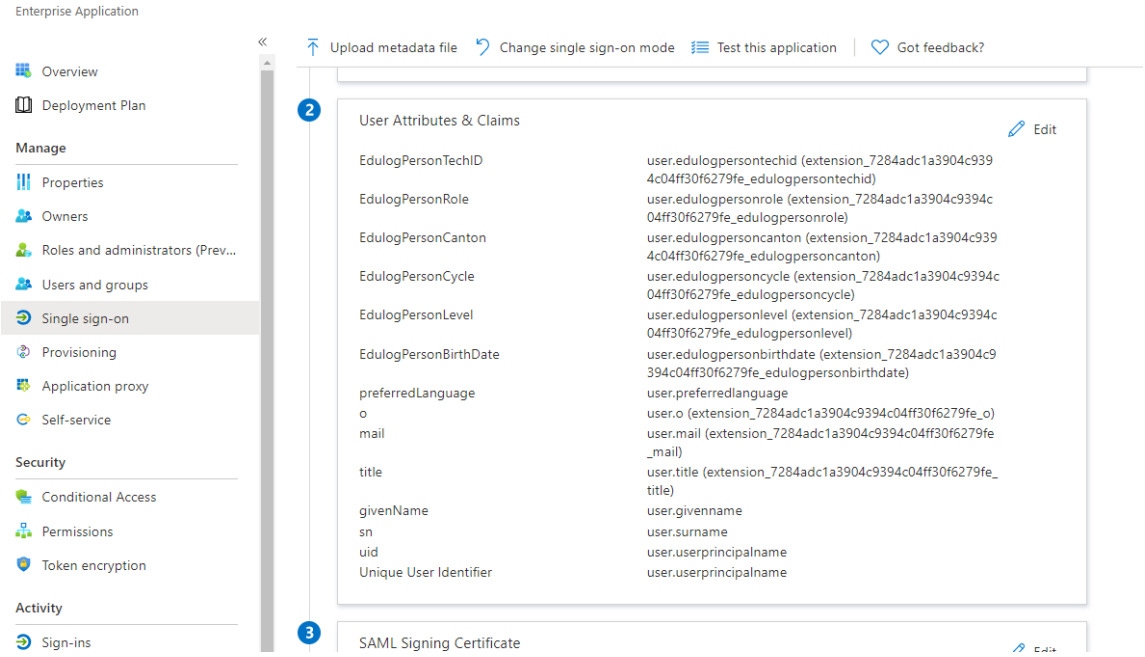
Hier sehen Sie ein Beispiel mit dem Attribut *EdulogPersonTechID*:



Sie müssen diesen Vorgang für jedes der Attribute wiederholen. Die endgültige Liste der Claims sollte wie folgt aussehen:



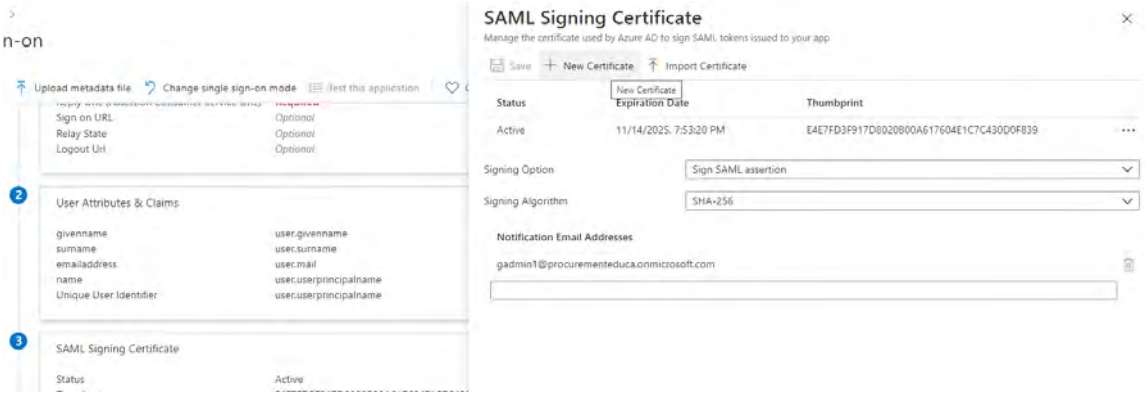
Nachdem die Claims validiert wurden, sieht der Abschnitt «User Attributes & Claims» der SAML-Konfigurationsseite Ihrer Anwendung wie folgt aus:



6.2.4 Erzeugen eines Zertifikats zum Signieren von Assertions

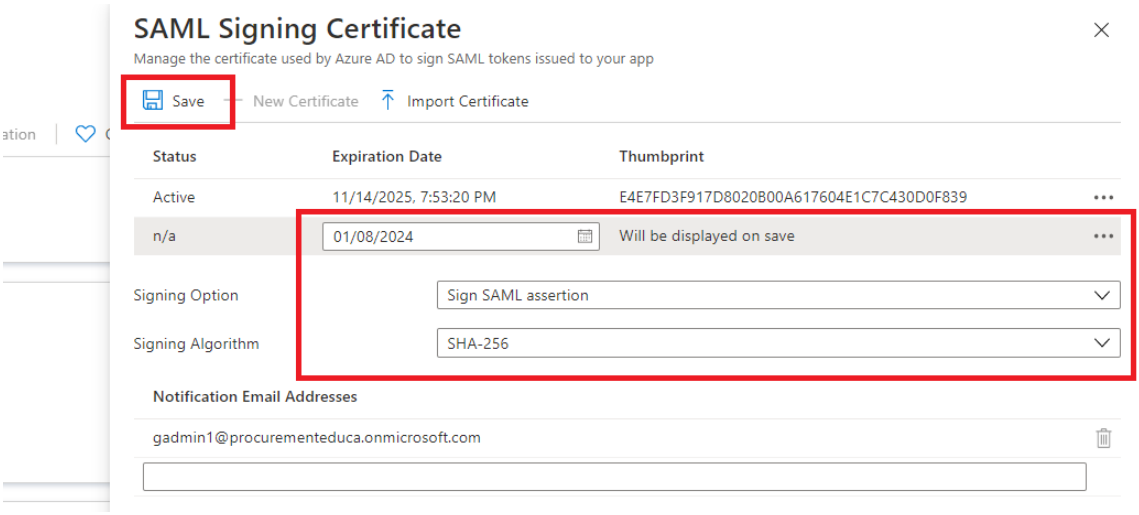
Sie müssen nun überprüfen, ob das Zertifikat die von Edulog geforderten Sicherheitsbedingungen[4] erfüllt. Bei der Erstellung der *Enterprise Application* generiert *Azure* automatisch ein Zertifikat. Dieses Zertifikats entspricht nicht den geforderten Sicherheitsbedingungen. Sie müssen daher ein neues Zertifikat mit den verlangten Sicherheitsbedingungen erstellen (d. h. 3 Jahre Gültigkeit, Verwendung des SHA-256-Verschlusselungsalgorithmus; bitte ändern Sie diese Werte nicht):

a. Um das neue Zertifikat zu erstellen, klicken Sie im Punkt «SAML Signing Certificate» auf «Edit», dann im neuen Fenster auf «New Certificate». Es wird mit einer Gültigkeit von 3 Jahren erzeugt.

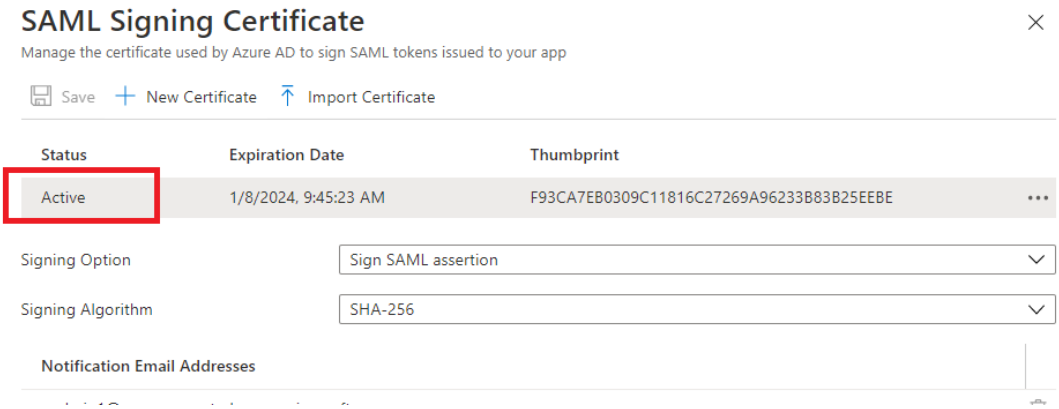


[4] Dokument abrufbar unter https://edulog.ch/de/beitritt/dokumentation, Sicherheitsanforderungen für die Dokumentation

b. Nachdem das Zertifikat erstellt wurde, muss es gespeichert werden, damit es übernommen wird.



c. Abschliessend muss das neue Zertifikat aktiviert werden (Klicken Sie auf die drei Punkte rechts), das alte wird dann gelöscht. Der Status des Zertifikats wird auf «Active» gesetzt.



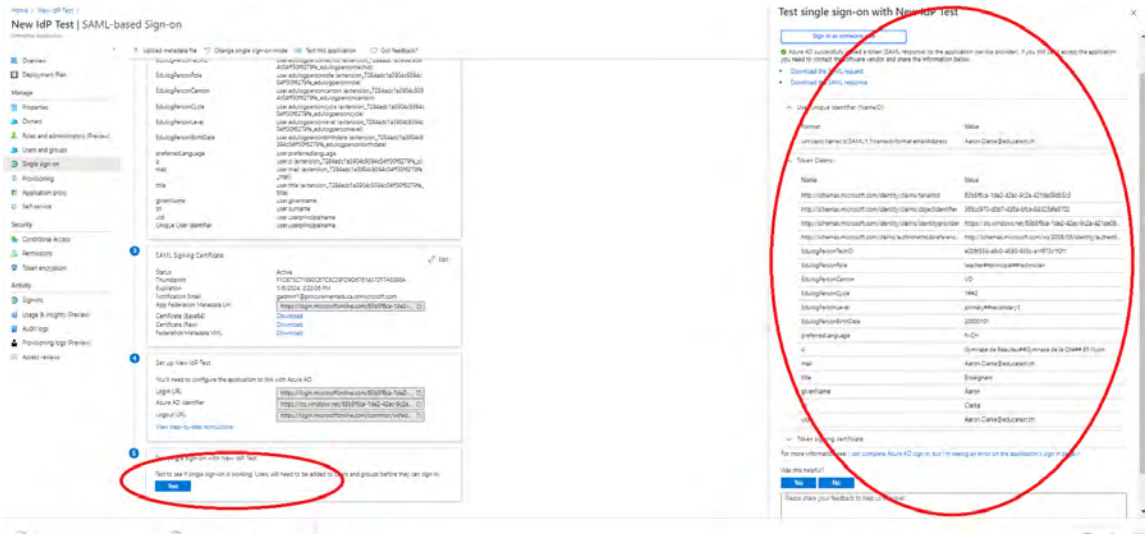
Der Schlüssel muss eine Gültigkeit von 3 Jahren aufweisen. Ein anderer Wert verhindert den Abschluss des Onboardings bei Edulog.

6.2.5 Einen Verbindungstest auf Ihrem SAML-Endpoint durchführen

Mit dem Punkt «Test single sign-on with New IdP Test» in der Konfiguration «SAML-based Sign On» können Sie die von Ihnen erstellte Konfiguration testen. Sie stellt nicht die endgültige Verbindung zu Edulog dar, sondern ermöglicht es Ihnen, die Attribute zu sehen, die in einer SAML-Assertion von Ihrer *Azure*-Applikation gesendet werden.

Der Test muss mit dem in Punkt 6.1 autorisierten Benutzer und dessen Passwort durchgeführt werden. Auf der rechten Seite des Bildschirms sehen Sie im Abschnitt «Token Claims» die übergebenen Werte.

Beispiel:



Wenn der Test gültig ist, werden die Werte zusammen mit der Meldung «Azure AD successfully issued a token (SAML Response)...» angezeigt.

6.2.6 Abrufen des Links und der Datei der Metadaten Ihrer Applikation

- Unter «SAML-Based Sign-on» im Punkt «SAML Signing Certificate» kopieren Sie den Link «App Federation Metadata URL», der wie folgt aussehen sollte: https://login.microsoftonline.com/XXXXXXXX-1de2-42ac-9c2a-421de09d55c3/federationmetadata/2007-06/federationmetadata.xml?appid=XXXXXXX-0edb-465a-9927-XXXXXXXXX
- Immer noch unter dem Punkt «SAML Signing Certificate» klicken Sie auf den Button «Download» neben dem Abschnitt «Federation Metadata XML».

Sie müssen dann diese XML-Metadaten-Datei und den vorherigen Link an ELCA senden, um das *Onboarding* durchzuführen.

6.2.7 Ändern der Reply-URL (Assertion Consumer Service URL)

Sobald ELCA Ihre Konfiguration validiert hat, erhalten Sie die definitive Reply-URL. Diese müssen Sie nun gemäss Punkt 6.2.2 einfügen.

Ihre *Enterprise Application* ist nun für Edulog konfiguriert.

7. Anhang: Mögliche Probleme

Wenn Benutzer angelegt und nicht wie in Punkt 6.1 angegeben autorisiert werden, dann funktioniert der Anmeldetest, der in Punkt 6.2.5 «Einen Verbindungstest auf Ihrem SAML-Endpoint durchführen» gesehen wurde, nicht. Es wird dann eine Meldung «Signing is unsuccessful» wie im folgenden Beispiel angezeigt: