Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNISCHES

Vorbereitung einer lokalen Infrastruktur (lokales *AD* und *AD* FS) als IdP

22.02.2022 – Version 1.0

1. Ziel des Dokuments 2
2. Vorbedingungen 3
3. Vollständiger Ablauf 3
4. Installieren der *AD*-Schema-Erweiterung für Edulog 4
4.1 Anlegen der neuen Attribute in das lokale *AD*-Schema: 4
4.2 Merkmale der neuen Attribute im *AD* 6
5. Installation eines Servers mit der Funktion *AD FS* 6
6. Konfiguration des *AD FS*-Servers 7
6.2 Einrichten eines *Relying Party Trust* für Edulog 7
6.3 Anlegen einer *Claim Issuance Policy* 9

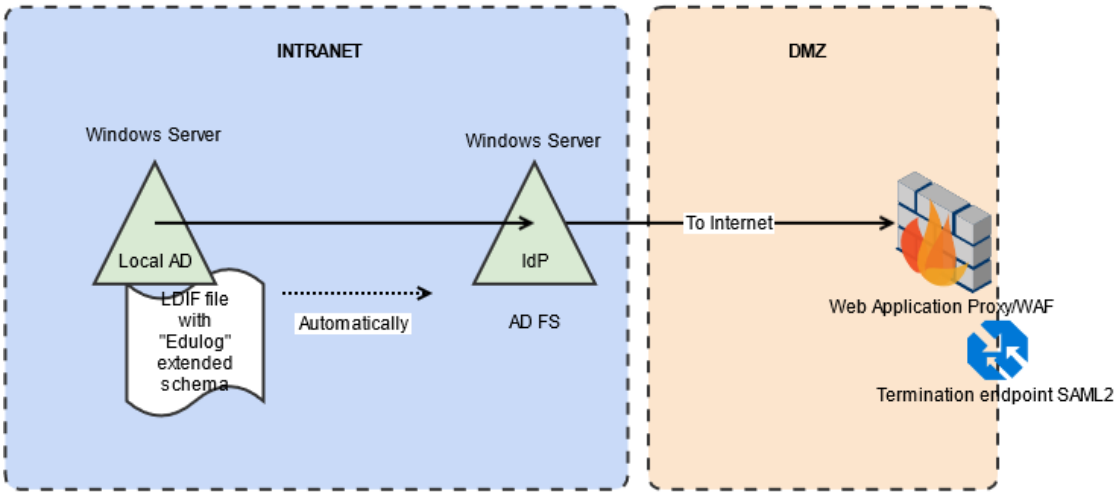
1. Ziel des Dokuments

Dieses Dokument zeigt auf, wie ein Identitätsanbieter (IdP) eine lokale Infrastruktur (lokales *AD* und FS *AD*) vorbereiten können.

Um Edulog beizutreten, muss ein IdP:

- **Überprüfen, ob seine Identitäten über eine bestimmte Anzahl von Attributen verfügen[1].** Einige dieser Attribute existieren jedoch ursprünglich nicht im Schema eines *AD*. Im ersten Teil dieses Dokuments wird erläutert, wie Sie die Erweiterung des *AD*-Schemas installieren, die at-Tribute übermitteln und überprüfen, ob sie zugänglich sind.
- **Über eine Infrastruktur mit einer SAML-Schnittstelle verfügen.** Der zweite Teil dieses Dokuments beschreibt, wie Sie ein *AD* FS so konfigurieren, dass es als Schnittstelle genutzt werden kann.

Dieses Dokument richtet sich an IdP, die ein lokales *AD* haben und *AD* FS als SAML-Schnittstelle verwenden, um Verbindungen mit Edulog herzustellen.



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

2. Vorbedingungen

Dieser Leitfaden kann nur verwendet werden, wenn die folgenden technischen Anforderungen erfüllt sind:

- Der IdP verwendet - in seiner eigenen Infrastruktur - ein *AD* (im Folgenden als *Local AD* bezeichnet).
- Der IdP verwendet einen Server mit der Funktion *Active Directory Federation Services* (*AD FS*), um sich mit Edulog unter Verwendung des *SAML2*-Protokolls zu verbinden.

3. Vollständiger Ablauf

Nachfolgend eine Übersicht über die **technischen**[2] Schritte, die ein IdP (mit der zuvor erwähnten Infrastruktur) durchführen muss, um die für das Onboarding mit Edulog erforderliche Konfiguration vorzunehmen:

N°	Actions à réaliser	Moment
1	Installieren der *AD*-Schema-Erweiterung für Edulog	Kapitel 4
2	Installation eines *AD* FS-Servers	Kapitel 5
3	Konfiguration eines *AD* FS-Servers mit Edulog	Kapitel 6
4	Verbindungstests mit ELCA durchführen	Im Anschluss
5	Föderierung der Identitäten mit ELCA durchführen	Im Anschluss

Dieses Dokument behandelt die Punkte 1 und 3.

[2] Für die Integration in die Föderation sind weitere nicht-technische Schritte erforderlich. Sie werden in diesem Dokument nicht behandelt. Eine Übersicht über den gesamten Prozess finden Sie unter https://edulog.ch/de/beitritt

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. Anlegen 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. Die neuen Attribute sind automatisch für alle Server verfügbar, die zum selben Forest gehören.

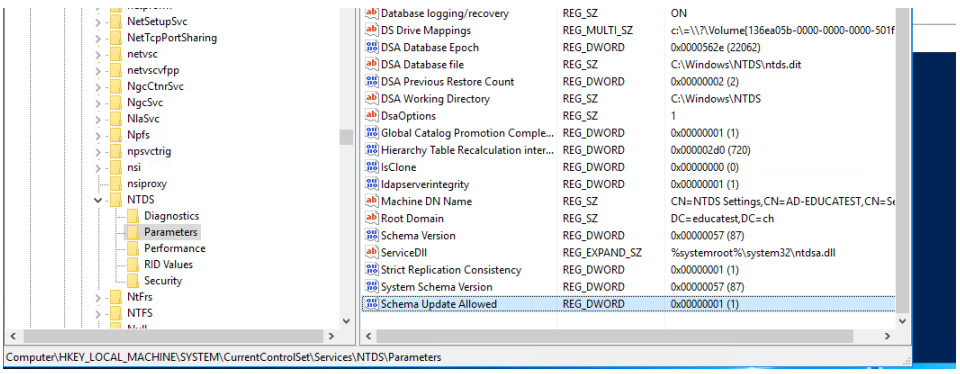
LDIF Datei: Die aktuelle Version der LDIF Datei die in diesem Dokument verwendet wird können Sie von der Geschäftsstelle Edulog via info@edulog.ch anfragen.

4.1 Anlegen der neuen Attribute in das lokale *AD*-Schema:

Bevor diese neuen Attribute erstellt werden können, müssen bestimmte Operationen am *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.

4.1.1 Dem *AD* erlauben, das Schema zu ändern

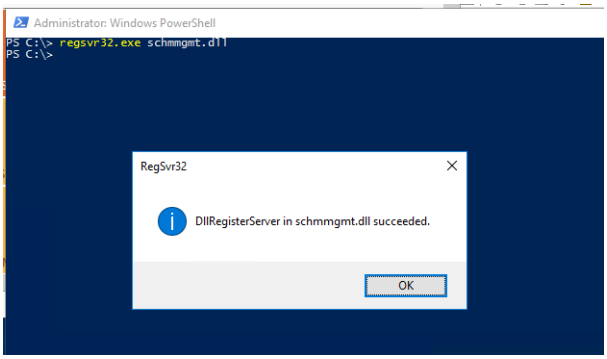
Es muss ein Registrierungsschlüssel hinzugefügt werden unter HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters. Der Name des neuen Schlüssels muss «Schema Update Allowed» mit dem Wert 1 und dem Format REG_DWORD sein.



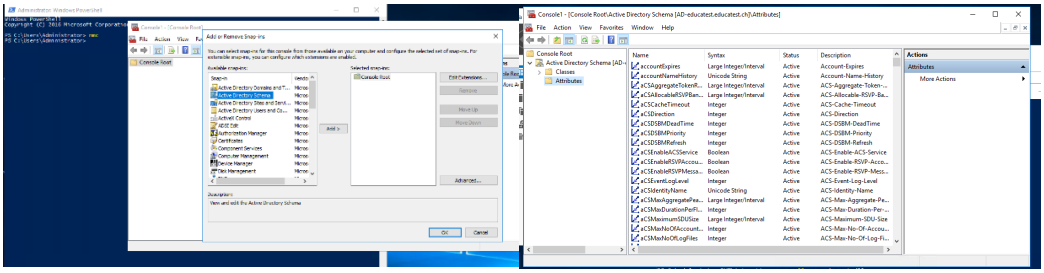
[3] Für diese Teilaufgaben kann das folgende Dokument von Microsoft verwendet werden: https://social.technet.microsoft.com/wiki/contents/articles/51121.active-directory-how-to-add-custom-attribute-to-schema.aspx

4.1.2 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:



4.1.3 Importieren der LDIF-Datei ins *AD*

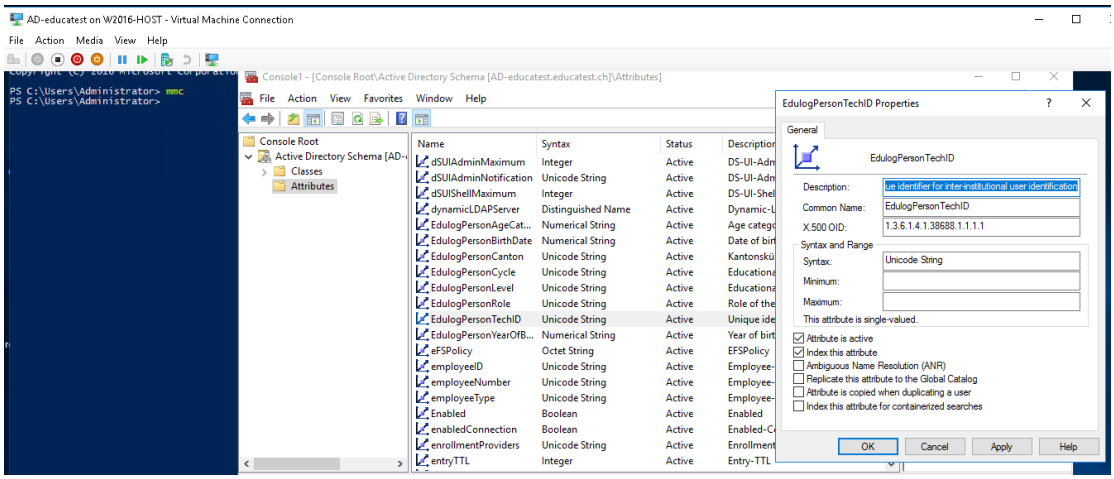
Um die LDIF-Datei mit den neuen Attributen in das *AD*-Schema zu importieren, müssen Sie (als Administrator des Schemas/der Domäne) den folgenden Befehl verwenden:

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

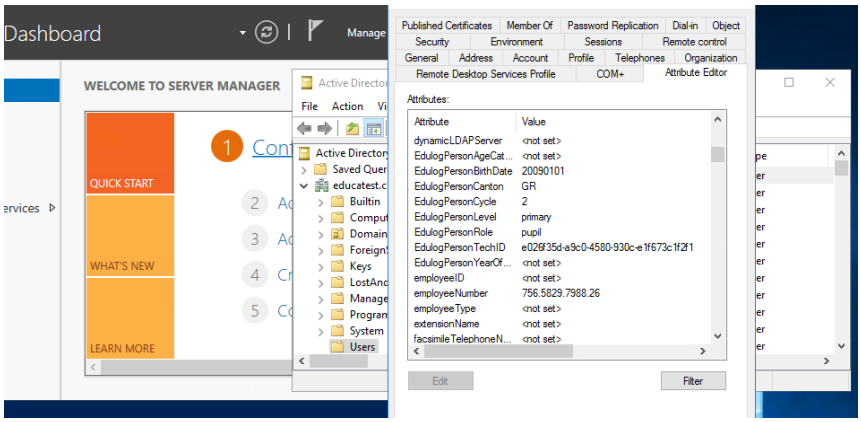
Wichtig: Die LDIF-Datei muss angepasst werden, um den Namen der Domäne zu berücksichtigen, in der sie verwendet wird (z. B.: DC=educatest,DC=ch, wenn die Domäne educatest.ch ist).

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 innerhalb der Domain vorhanden sind.



5. Installation eines Servers mit der Funktion *AD FS*

Active Directory - Federation Services (AD FS) ist eine windowsbasierte Implementierung, die Föderationsdienste für eine *AD*-Architektur bereitstellt. Unter anderem ermöglicht sie die Implementierung einer SAML-Schnittstelle.

Dazu müssen Sie einen Windows-Server (vorzugsweise Windows Server 2016 oder höher) vorbereiten und die Funktion *AD FS*[4] installieren.

Ausserdem müssen Sie eine Reihe von «Best Practices» berücksichtigen, die von Microsoft[5] vorgegeben werden. Dazu gehört auch die Installation eines oder mehrerer Web Application Proxy/ies, die zwar nicht zwingend erforderlich ist, aber für einen produktiven Einsatz dringend empfohlen wird.

6. Konfiguration des *AD FS*-Servers

Die Konfiguration des SAML-Links mit Edulog besteht aus drei Teilen:

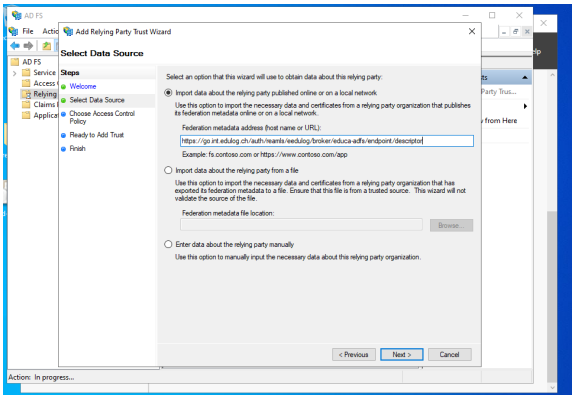
1. Erstellung eines Relying Party Trust.
2. Validierung des Zertifikats von Edulog.
3. Erstellung einer Claim Issuance Policy.

Beachten Sie, dass eine «Relying Party» im SAML Kontext ein *Service Provider* ist (zur Vereinfachung).

6.2 Einrichten eines *Relying Party Trust* für Edulog

Starten Sie im *ADFS*-Server vom «Server Manager» aus die Anwendung *AD* FS (unter der Registerkarte «Tools»). Klicken Sie auf *AD FS* und «Relying Party», wählen Sie «Add Relying Party Trust».

6.2.1 Importieren der Metadaten-Datei von Edulog

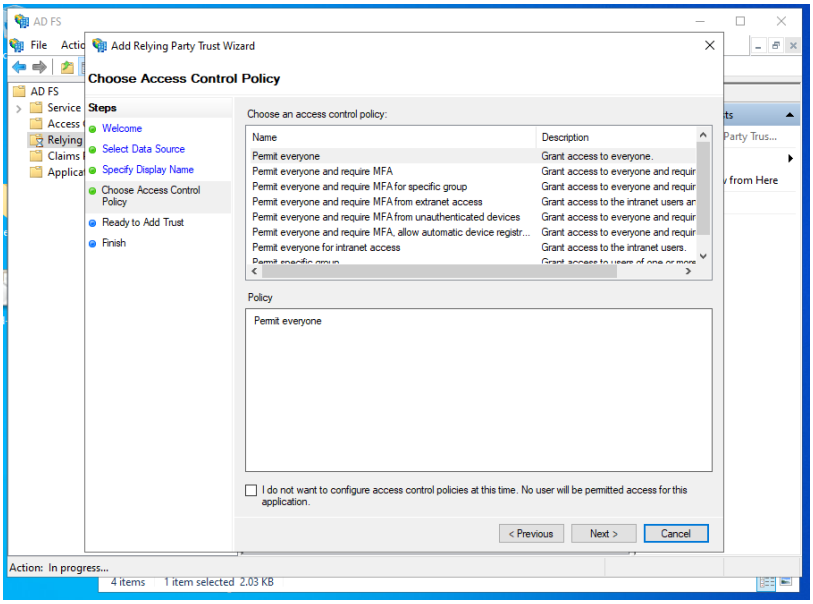


Es bestehen drei Optionen um die Konfiguration umzusetzen.

[4] Der vorliegende Leitfaden zeigt nicht, wie man diesen Schritt umsetzt. Ein Beispiel finden Sie unter: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/checklist--setting-up-a-federation-server.
[5] siehe https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

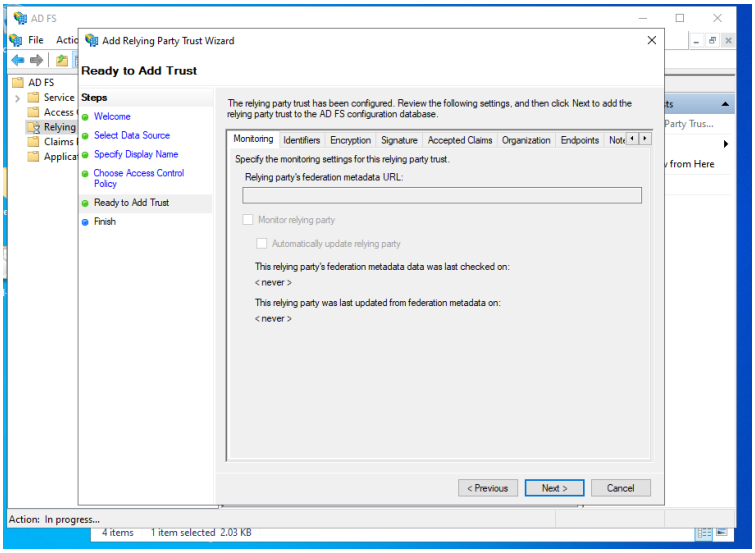
Die ersten beiden sind vorzuziehen: Entweder den http-Link angeben, unter dem die Metadaten-Datei von Edulog zu finden ist, oder die entsprechende Datei importieren. In beiden Fällen ist es notwendig, vorab ELCA zu kontaktieren, die Ihnen die entsprechenden Informationen zur Verfügung stellen wird.

6.2.2 Auswählen der «Access Control Policy»

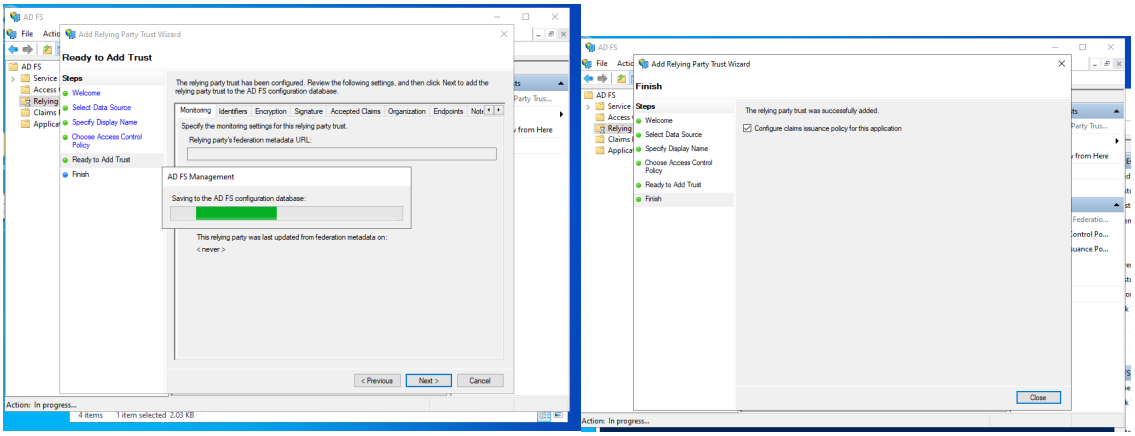


Wählen Sie dazu «Permit everyone».

6.2.3 Auf «Next» klicken

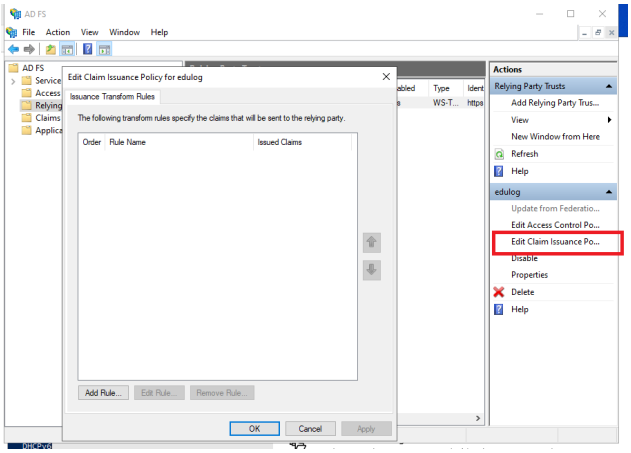


6.2.4 Warten bis der «Trust» erstellt ist und abschliessen.

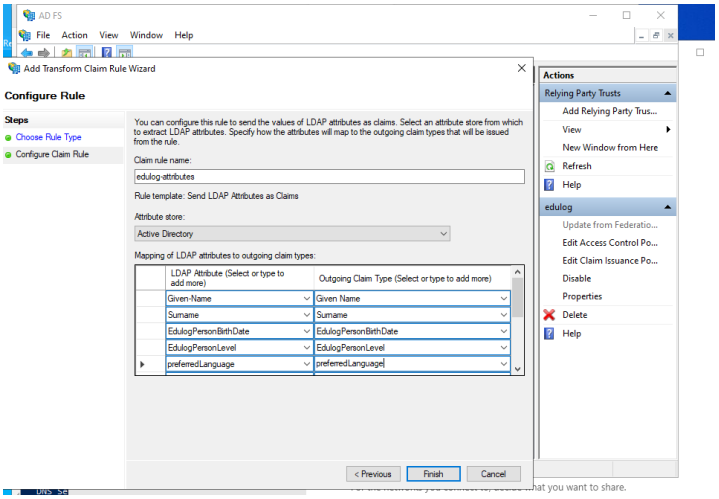


6.3 Anlegen einer *Claim Issuance Policy*

6.3.1 Auf «Edit Claim Issuance Policy» klicken



6.3.2 Eine Regel für die Edulog-Attribute hinzufügen

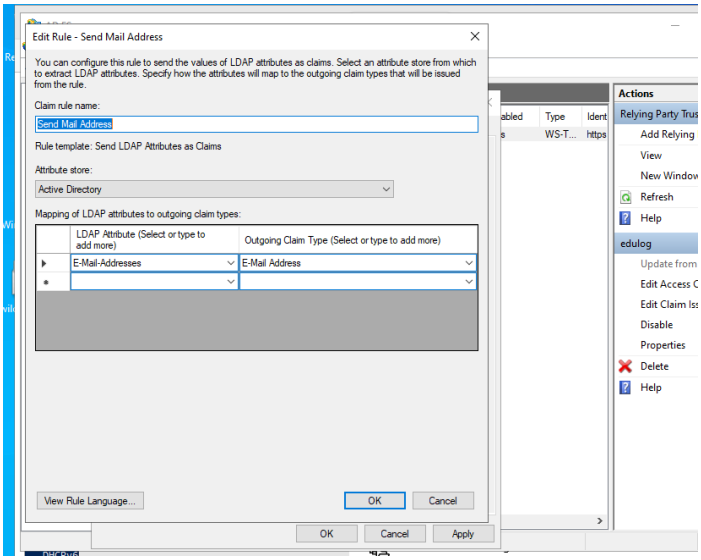


Wählen Sie einen «Attribute store» vom Typ Active Directory. Schreiben Sie dann jedes der Attribute von Edulog in die Spalte «LDAP attribute» (**Die Attribute sind im Drop-down-Menü nicht sichtbar. Sie müssen den genauen Namen des Attributs in jede Zeile schreiben**).

Geben Sie für jedes der Attribute in der Spalte «Outgoing Claim Type» wieder dasselbe Attribut ein (das nun im Dropdown-Menü sichtbar ist).

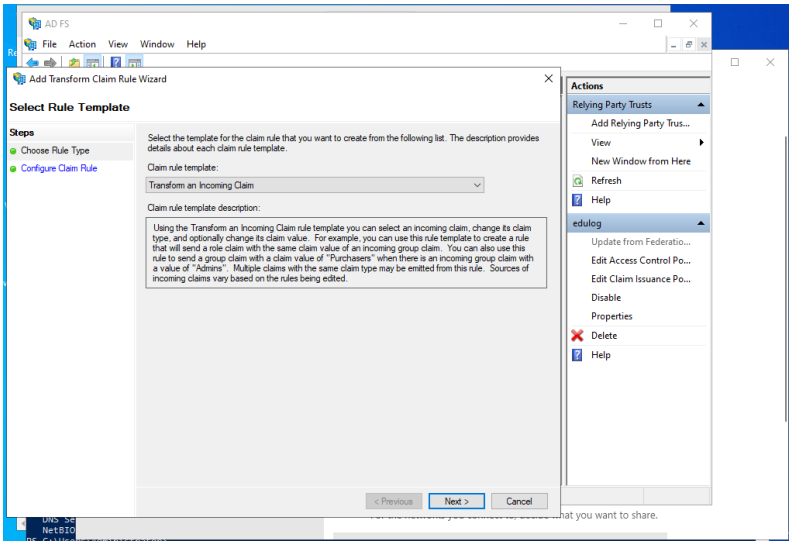
Klicken Sie auf «Finish».

6.3.3 Einrichten einer Regel für das Attribut «E-Mail Address»



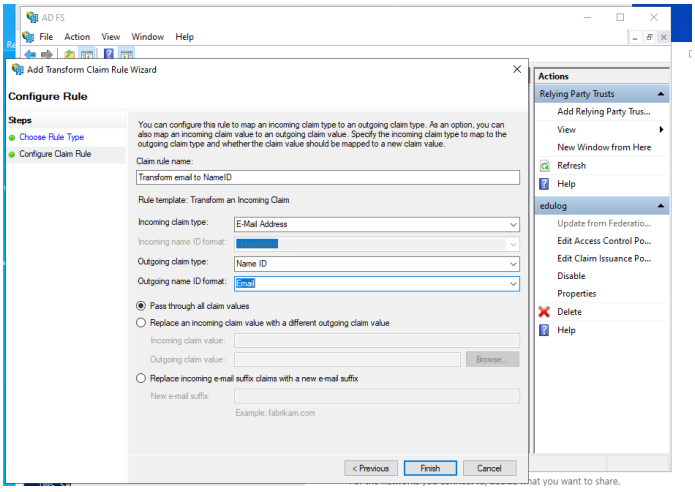
Wiederholen Sie dieselben Schritte (vgl. 6.3.2) für das Attribut «E-Mail-Address» (im Dropdown-Menü sichtbar).

6.3.4 Einrichten einer Regel vom Typ « Transform an Incoming Claim »



Auf «Next» klicken.

6.3.5 Einrichten des Attributs «Name ID»



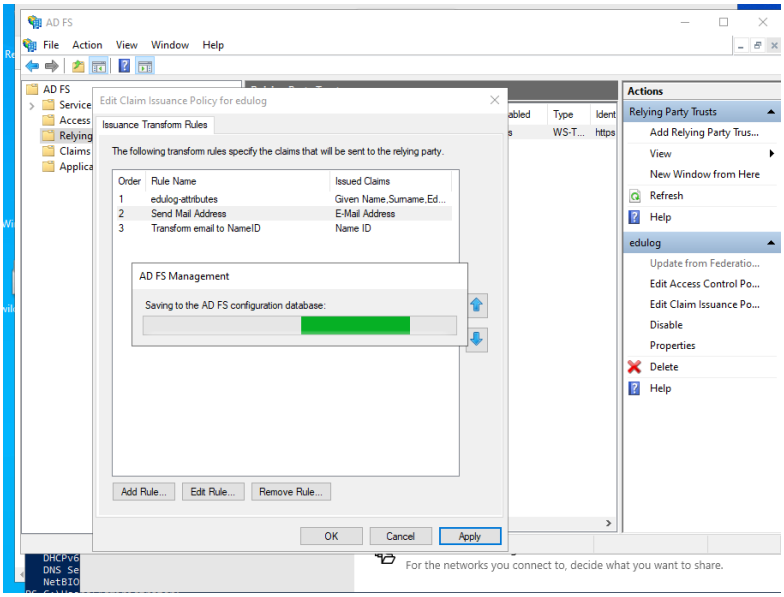
Wählen Sie dazu unter «Incoming claim type» den Typ «E-Mail Address».

Wählen Sie «Email» als Typ für die NameID

Aktivieren Sie die Option «Pass through all claim values».

Klicken Sie auf «Finish».

6.3.6 Konfiguration validieren



Auf «Apply» klicken und das Erstellen des Links abwarten.