

TECHNISCHES

Synchronisierung von Identitäten mit SCIM auf Edulog

21.12.2021 – Version 1.0

1.	Ziel des Dokuments.....	2
2.	Voraussetzung	2
2.1	Allgemeine Vorgehensweise	2
2.2	Elemente der Infrastruktur.....	3
3.	Einrichten der SCIM-Funktionalität	4
3.1	Erzeugen eines Tokens mit langer Laufzeit.....	4
3.2	SCIM-Verbindung einrichten.....	4
4.	Aktivierung des Provisioning	11
4.1	Starten des Provisioning	11
4.2	Provisioning-Logs	11

1. Ziel des Dokuments

Dieses Dokument beschreibt, wie ein Identitätsanbieter (IdP) die Provisionierungsfunktion SCIM von Azure nutzen kann, um Identitäten mit Edulog zu föderieren.

2. Voraussetzung

Sie haben:

- einen Vertrag mit Edulog unterzeichnet;
- ein Konto auf Azure;
- alle Identitäten Ihres IdP in Ihrem Azure-Tenant;
- eine Enterprise Application von Azure erstellt, die als SAML-Endpunkt dient;
- mit ELCA die korrekte Föderation Ihres IdP überprüft.

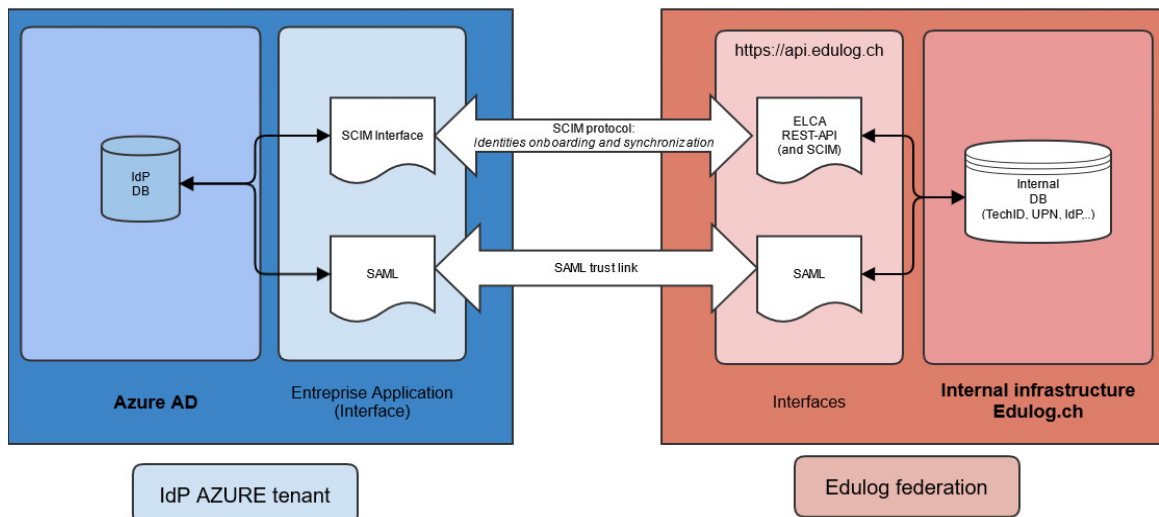
2.1 Allgemeine Vorgehensweise

Nr	Aktionen	Ziel/Kommentar
1	Erstellen eines Langzeit-Tokens	Dies ist notwendig, um die Synchronisation zwischen den Identitäten Ihres Tenants und Edulog durchführen zu können.
2	Einrichten der SCIM-Funktionalität	Um Identitäten in Edulog zu föderieren.
3	Synchronisationstests	Werden benötigt, um zu überprüfen, ob neue Attribute über das SCIM-Protokoll gesendet wurden.

Punkt 1 muss mittels Kommandozeile (unter Windows oder Linux) ausgeführt werden, die restlichen Aktionen können über die Schnittstelle des Azure-Portals erfolgen.

2.2 Elemente der Infrastruktur

Das folgende Schema stellt die verschiedenen Elemente der SCIM-Synchronisation dar.



Es wird unterschieden zwischen:

- Einem IdP, dessen Identitäten sich in einem *Azure AD Tenant* befinden.
- Einer *Enterprise Application* als SAML-Endpoint und als SCIM-Schnittstelle im Azure-Tenant.
- Der Edulog-Infrastruktur mit der REST-API und dem SAML-Endpoint.

Zu beachten:

- **SAML trustlink:** dient der sicheren Kommunikation der Attribute von Edulog-Benutzern, wenn diese sich mit einem Dienstanbieter (Service Provider) verbinden. Er ist ständig in Betrieb.
- **SCIM-Schnittstelle:** dient der Synchronisation von Änderungen in den Identitäten, die Edulog betreffen (Föderierung / Deföderierung neuer Benutzer, Änderung der UID, ...).

3. Einrichten der SCIM-Funktionalität

Um die Föderierung / Deföderierung von Benutzern aus Azure AD in Edulog zu erleichtern, steht eine SCIM-Schnittstelle zur Verfügung. Dieser Abschnitt beschreibt detailliert die Konfiguration von Azure AD, um diese standardisierte Schnittstelle zu nutzen.

3.1 Erzeugen eines Tokens mit langer Laufzeit

Edulog stellt den IdP eine REST-API für bestimmte Funktionen zur Verfügung, die automatisiert werden können. Jeder IdP, der dies wünscht, kann einen technischen Benutzer mit zugehörigem Authentifikator erhalten. Eine dieser Funktionen ermöglicht die Generierung eines langfristigen Tokens, der in der SCIM-Konfiguration zur Authentifizierung des IdP verwendet wird.

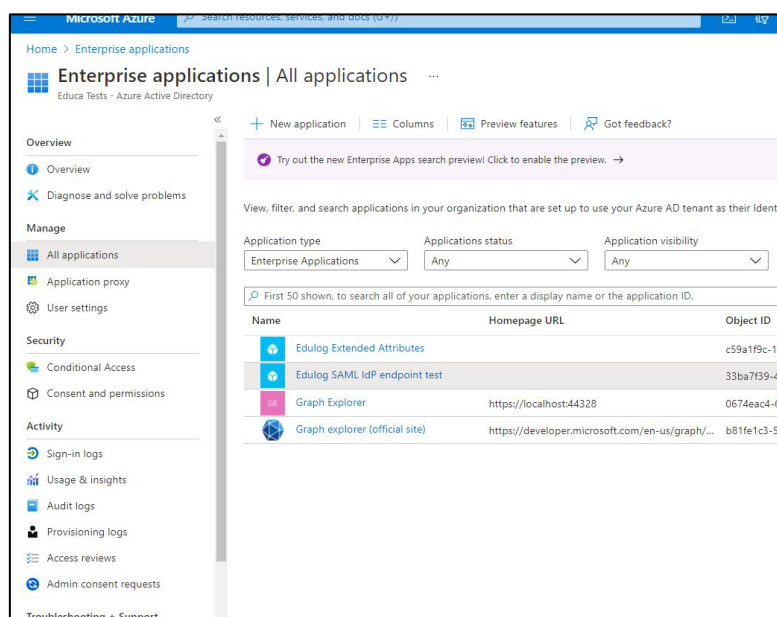
Die Generierung dieses Token kann von der Kommandozeile aus erfolgen, beispielsweise mit Hilfe des Programms `curl`.

Die gesamte Funktionalität sowie die Details des oben angegebenen Befehls sind im Dokument « **Edulog API reference** » (nicht öffentlich) verfügbar.

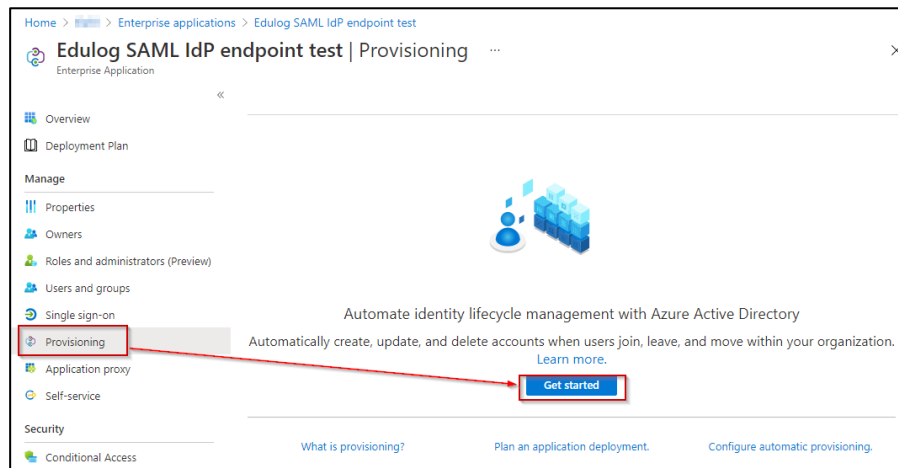
3.2 SCIM-Verbindung einrichten

Wählen Sie zunächst im Azure-Tenant die Enterprise-Application aus, die zuvor in der Föderationsphase erstellt wurde. Sie wird nun verwendet, um das Onboarding der Identitäten auszuführen.

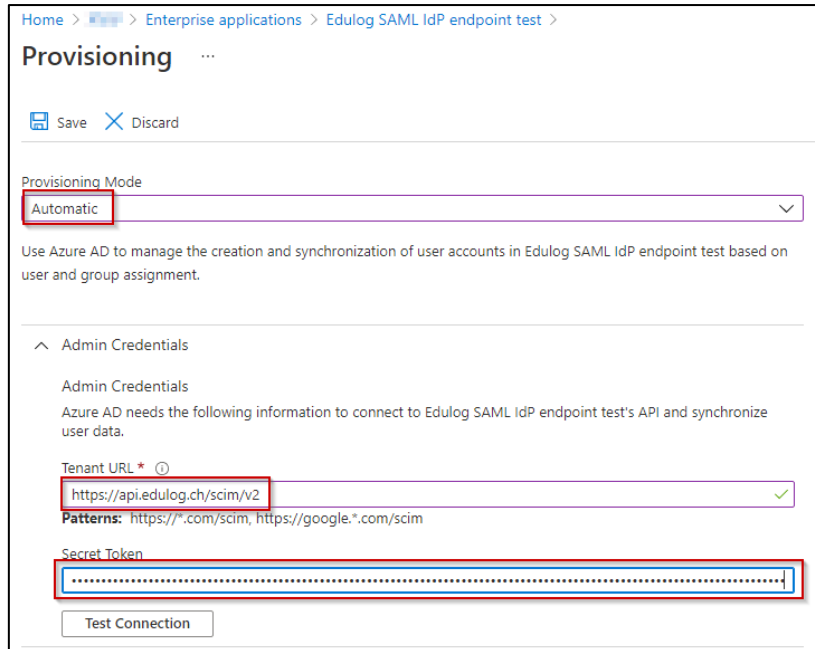
- Auswahl des Enterprise application (hier im Bild heißt sie: «Edulog SAML IdP endpoint test»):



- b. Wählen Sie « Provisioning » aus, und anschliessend « Get started » :



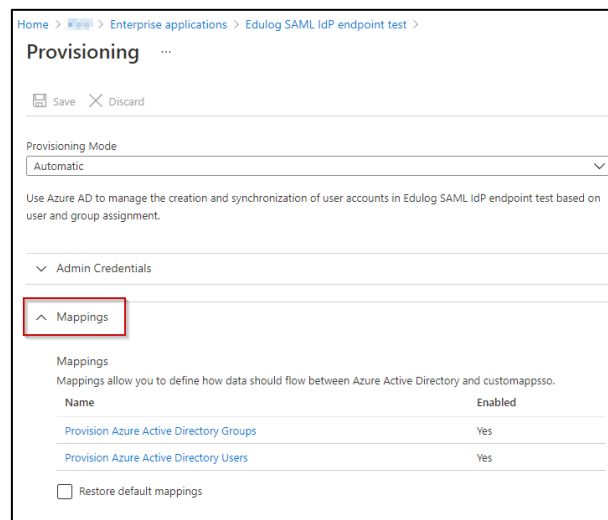
- c. Wählen Sie « Automatic » als « Provisioning Mode ».



- Fügen Sie im Feld « Tenant URL » die SCIM URL Edulog ein (z.B. <https://api.edulog.ch/scim/v2/realms/edulog/>).
- Im Feld « Secret Token » den Token kopieren, der zuvor in Punkt 3.1 mithilfe der Edulog API generiert wurde.

Klicken Sie abschließend auf «Test Connection», um sicherzustellen, dass alle Einstellungen korrekt sind, und speichern Sie die Konfiguration.

Sobald die Konfiguration korrekt gespeichert wurde, erscheint der Abschnitt «Mappings»:



Home > Enterprise applications > Edulog SAML IdP endpoint test > Provisioning

Save Discard

Provisioning Mode
Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Edulog SAML IdP endpoint test based on user and group assignment.

Admin Credentials

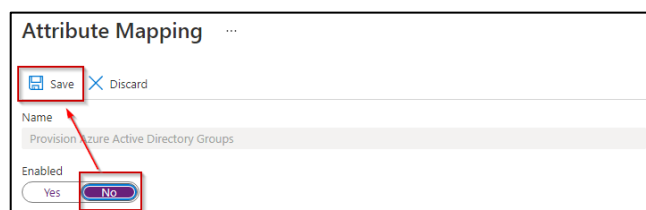
Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

☐ Restore default mappings

- d. Klicken Sie auf « Provision Azure Active Directory Groups » um sie zu deaktivieren und speichern Sie die Konfiguration



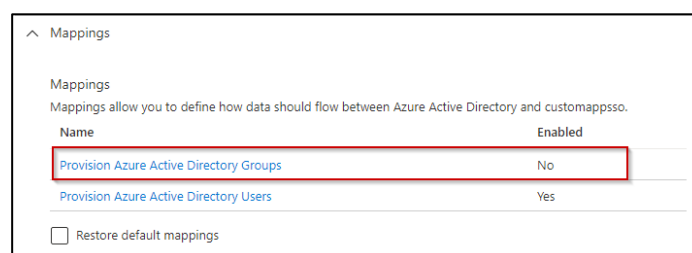
Attribute Mapping

Save Discard

Name
Provision Azure Active Directory Groups

Enabled
Yes No

- e. Gehen Sie zurück auf die Provisioning-Konfiguration. Stellen Sie sicher, dass das Provisioning von Gruppen deaktiviert ist:



^ Mappings

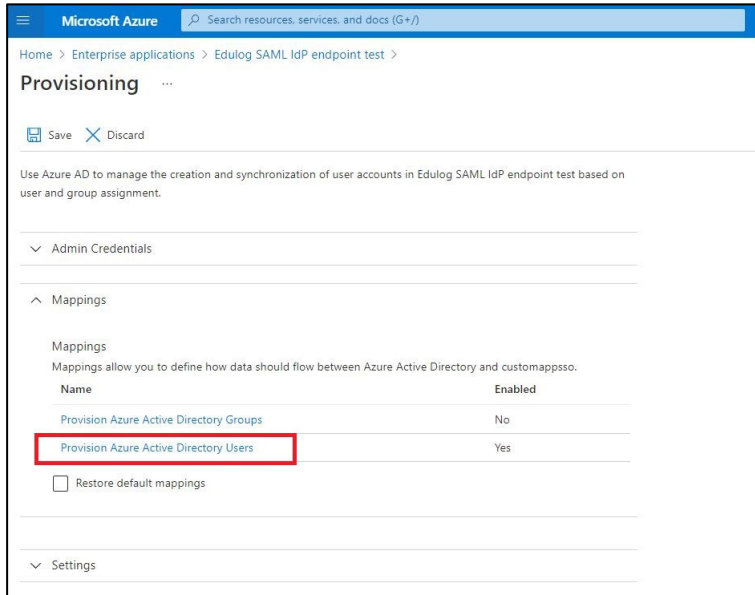
Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

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

☐ Restore default mappings

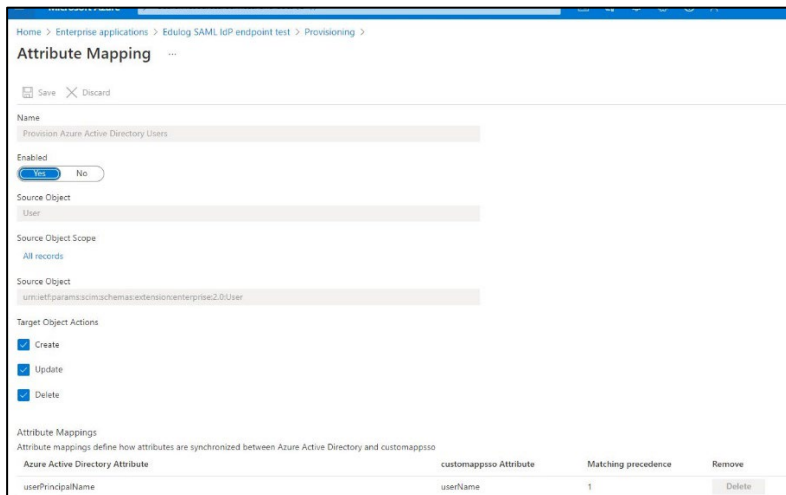
f. Klicken Sie auf «Provision Azure Active Directory Users»



The screenshot shows the 'Provisioning' page in the Microsoft Azure portal. The breadcrumb trail is 'Home > Enterprise applications > Edulog SAML IdP endpoint test > Provisioning'. Below the title, there are 'Save' and 'Discard' buttons. A description states: 'Use Azure AD to manage the creation and synchronization of user accounts in Edulog SAML IdP endpoint test based on user and group assignment.' There are expandable sections for 'Admin Credentials', 'Mappings', and 'Settings'. The 'Mappings' section is expanded, showing a table of mappings. The table has two columns: 'Name' and 'Enabled'. One mapping is highlighted with a red box: 'Provision Azure Active Directory Users' with the 'Enabled' status set to 'Yes'.

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

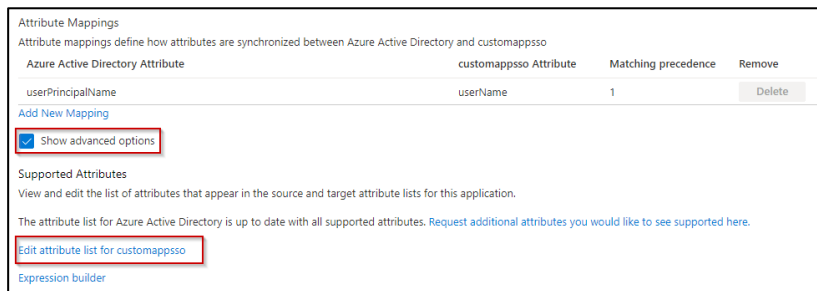
Löschen Sie im Abschnitt «Attribute Mappings» alle vorhandenen Mappings, außer «userPrincipalName».



The screenshot shows the 'Attribute Mapping' page for the 'Provision Azure Active Directory Users' mapping. The breadcrumb trail is 'Home > Enterprise applications > Edulog SAML IdP endpoint test > Provisioning > Attribute Mapping'. There are 'Save' and 'Discard' buttons. The 'Name' field is 'Provision Azure Active Directory Users'. The 'Enabled' toggle is set to 'Yes'. The 'Source Object' is 'User'. The 'Source Object Scope' is 'All records'. The 'Source Object' field contains the URI 'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User'. Under 'Target Object Actions', the 'Create', 'Update', and 'Delete' checkboxes are all checked. At the bottom, there is an 'Attribute Mappings' section with a table showing the mapping between 'Azure Active Directory Attribute' and 'customappsso Attribute'. The mapping for 'userPrincipalName' is shown with a matching precedence of 1 and a 'Delete' button.

Azure Active Directory Attribute	customappsso Attribute	Matching precedence	Remove
userPrincipalName	userName	1	Delete

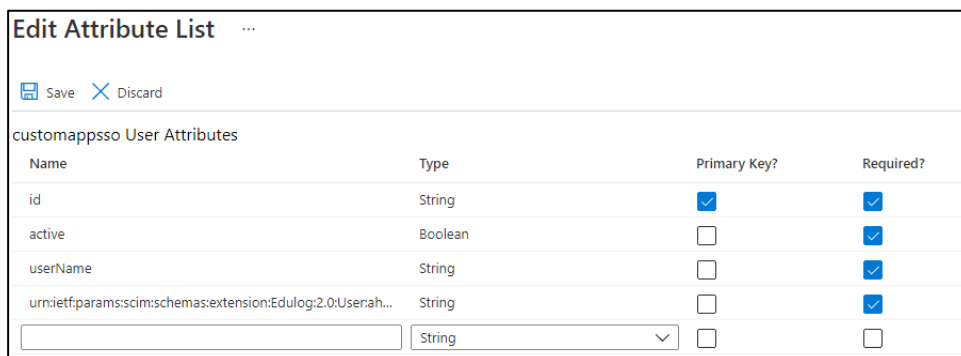
- g. Klicken Sie auf «Show advanced options» und dann auf «Edit attribute list for customappsso», um die von Edulog unterstützten Attribute zu deklarieren:



- h. Bearbeiten Sie die Attributliste. In der Attributliste:

- Fügen Sie das Flag "Required" für das Attribut «active» hinzu
- Fügen Sie das folgende neue Attribut hinzu:
Name : urn:ietf:params:scim:schemas:extension:Edulog:2.0:User:ahvn13
Type : String
Required : true

Speichern Sie die Änderungen.

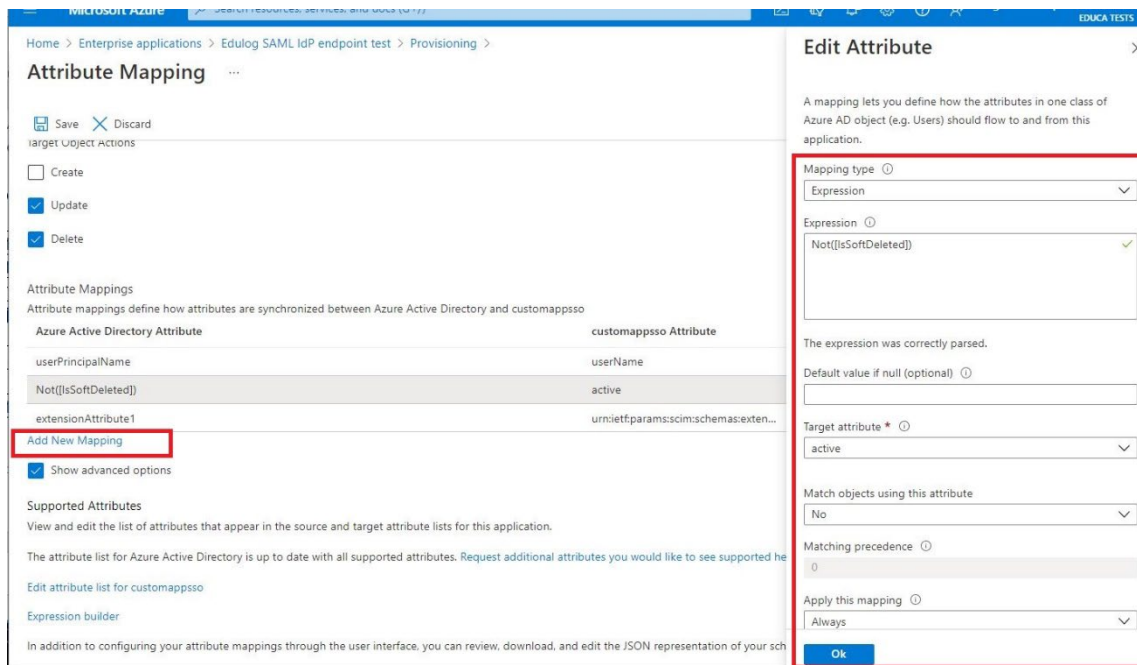


An dieser Stelle ist es wahrscheinlich notwendig, eine Aktualisierung der grafischen Benutzeroberfläche von Azure durchzuführen (drücken Sie F5), um sicherzustellen, dass die neuen Attribute berücksichtigt werden und im nächsten Schritt verfügbar sind.

- i. Zwei neue Mappings hinzufügen:

- `Not([IsSoftDeleted])`

Mapping type	Expression
Source attribute	<code>Not([IsSoftDeleted])</code>
Target attribute	active
Match object using this attribute	No
Apply this mapping	Always



Home > Enterprise applications > Edulog SAML IdP endpoint test > Provisioning >

Attribute Mapping

Save Discard

target Object Actions

- ☐ Create
- ☒ Update
- ☒ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

Azure Active Directory Attribute	customappsso Attribute
userPrincipalName	userName
Not([IsSoftDeleted])	active
extensionAttribute1	urn:ietf:params:scim:schemas:extension:...

Add New Mapping

☒ 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 Azure Active Directory is up to date with all supported attributes. Request additional attributes you would like to see supported here.

Edit attribute list for customappsso

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.

Edit Attribute

A mapping lets you define how the attributes in one class of Azure AD object (e.g. Users) should flow to and from this application.

Mapping type

Expression

The expression was correctly parsed.

Default value if null (optional)

Target attribute *

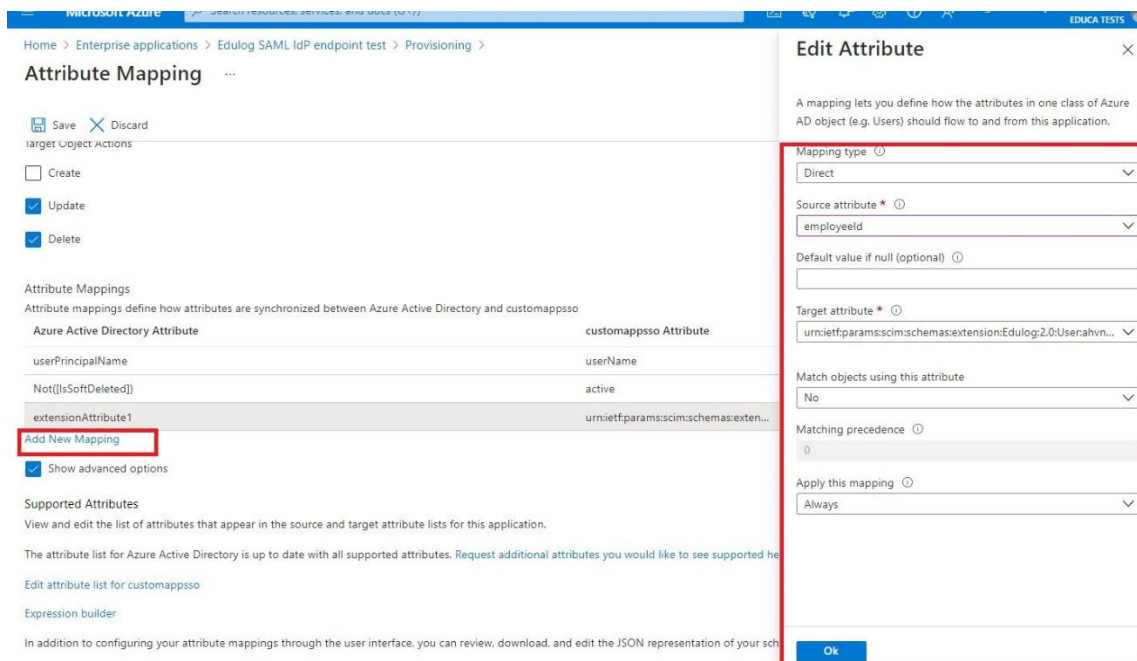
Match objects using this attribute

Matching precedence

Apply this mapping

Ok

- *extensionAttribute1* (oder ein anderes Attribut, das die AHV-Nummer enthält)



Home > Enterprise applications > Edulog SAML IdP endpoint test > Provisioning >

Attribute Mapping

Save Discard

target Object Actions

- ☐ Create
- ☒ Update
- ☒ Delete

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

Azure Active Directory Attribute	customappsso Attribute
userPrincipalName	userName
Not([IsSoftDeleted])	active
extensionAttribute1	urn:ietf:params:scim:schemas:extension:...

Add New Mapping

☒ 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 Azure Active Directory is up to date with all supported attributes. Request additional attributes you would like to see supported here.

Edit attribute list for customappsso

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.

Edit Attribute

A mapping lets you define how the attributes in one class of Azure AD object (e.g. Users) should flow to and from this application.

Mapping type

Source attribute *

Default value if null (optional)

Target attribute *

Match objects using this attribute

Matching precedence

Apply this mapping

Ok

Mapping type	Direct
Source attribute	<i>le nom de l'attribut contenant le numéro AVS</i>
Target attribute	urn:ietf:params:scim:schemas:extension:Edulog:2.0:User:ahvn13
Match object using this attribute	No
Apply this mapping	Only during object creation

j. Überprüfen Sie das Mapping *userName*

Stellen Sie sicher, dass das bereits vorhandene Mapping (*userName*) mit dem Azure AD-Attribut verknüpft ist, das den Identifikator enthält, welchen der Benutzer kennt, um auf sein Konto zuzugreifen (z.B. E-Mail-Adresse).

Hinweis: Der folgende Screenshot zeigt nur ein Beispiel für eine mögliche Konfiguration. Die Attribute in der Spalte "Azure Active Directory Attribute" müssen entsprechend der Konfiguration Ihres Tenant angepasst werden:

Attribute Mappings			
Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso			
Azure Active Directory Attribute	customappsso Attribute	Matching precedence	Remove
userPrincipalName	userName	1	<button>Delete</button>
extensionAttribute1	urn:ietf:params:scim:schema...		<button>Delete</button>
Not([IsSoftDeleted])	active		<button>Delete</button>
Add New Mapping			

Speichern Sie abschließend die Änderungen, indem Sie auf « Save » klicken.

4. Aktivierung des Provisioning

4.1 Starten des Provisioning

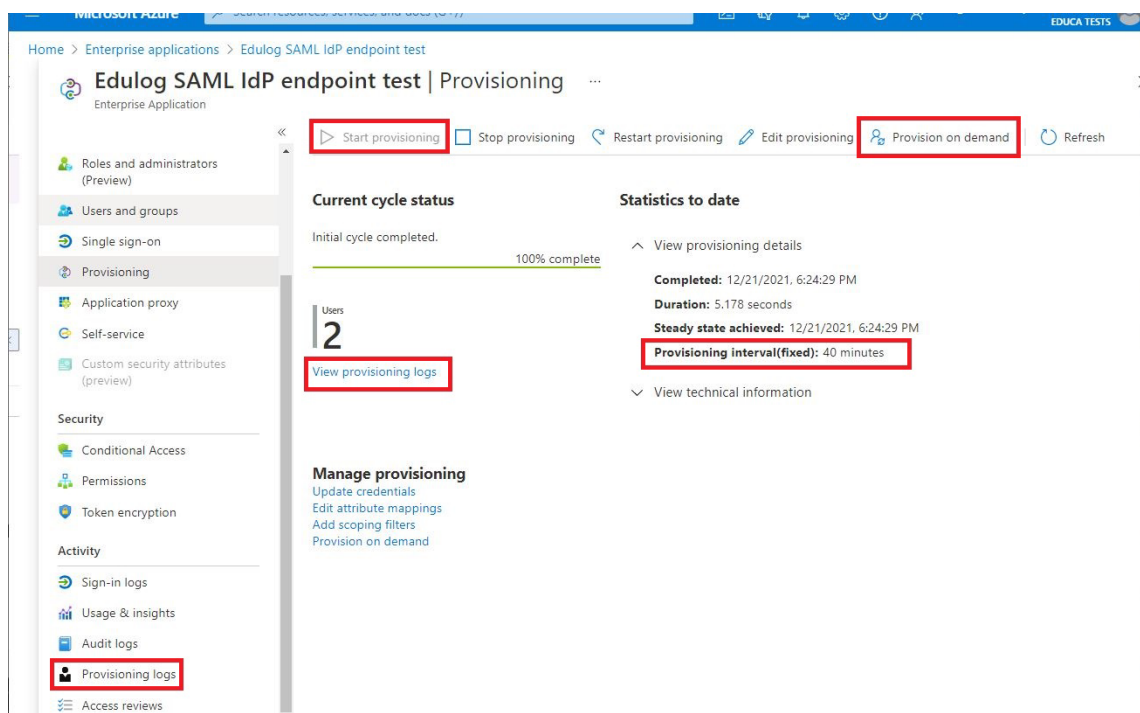
Gehen Sie zurück in den Bereich "Provisioning" der *Enterprise Application* und klicken Sie auf «Start Provisioning» (siehe Bild unten).

Dies wird den Prozess der Erstellung von Benutzern der *Enterprise Application* in Edulog starten.

4.2 Provisioning-Logs

Der Provisioning-Prozess wird regelmäßig ausgeführt, aber vollständig von der Azure-Plattform verwaltet (alle 40 Minuten - siehe Bild unten). Es ist nicht möglich, die Ausführung des Prozesses zu erzwingen, außer für einen bestimmten Benutzer (*Provisioning on demand*).

Um Details über die verschiedenen Operationen zu erhalten, die der Provisioning-Prozess durchführt, können Sie die Provisioning-Logs einsehen, die im Azure-Interface verfügbar sind (siehe Bild).



Im Falle eines Problems können diese Logs verwendet werden, um die Ursache potenzieller Fehler zu identifizieren.

Home > Enterprise applications > Edulog SAML IdP endpoint test >

Provisioning Logs

Download Learn more Refresh Columns Got feedback?

Identity Name or ID Date: Last 24 hours Show dates as: Local Status: All Action: All Application contains 33ba7f39-4294-46bf-8a46-1c718c1ab4e6 Add filters

Date	Identity	Action	Source System	Target System	Status
12/21/2021, 6:24:29 PM	Display Name Scim5 Test Source ID 6fa500fb-bab5-4c6a-ac70-e560f	Create	Azure Active Directory	customappsso	Skipped
12/21/2021, 6:24:29 PM	Display Name Scim4 Test Source ID 7a60c646-6ea4-4e04-b0d7-784f Target ID 403f62e3-b338-4333-97ed-3f92e	Update	Azure Active Directory	customappsso	Success
12/21/2021, 6:24:29 PM	Display Name Scim3 Test Source ID eddcea2d-f767-44f1-bc20-168d Target ID 678806b4-42de-46a9-931d-9073	Update	Azure Active Directory	customappsso	Success
12/21/2021, 6:24:26 PM	Display Name Test2 User Source ID b298ae66-e3a8-4070-a17f-0420 Target ID cff87407-c47b-4ee2-8ab7-1cb3a	Create	Azure Active Directory	customappsso	Skipped