Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNIQUE

Synchronisation d'identités avec SCIM sur Edulog

21.12.2021 – 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. But du document

Ce document décrit comment un fournisseur d'identité (IdP) peut utiliser la fonction de provisioning SCIM d'Azure pour fédérer les identités avec Edulog.

2. Prérequis

Vous avez déjà :

- signé un contrat avec Edulog ;
- un compte sur *Azure* ;
- toutes les identités de votre IdP présentes dans votre tenant Azure ;
- créé une Entreprise Application d'Azure pour servir comme SAML endpoint ;
- vérifié avec ELCA la fédération correcte de votre IdP.

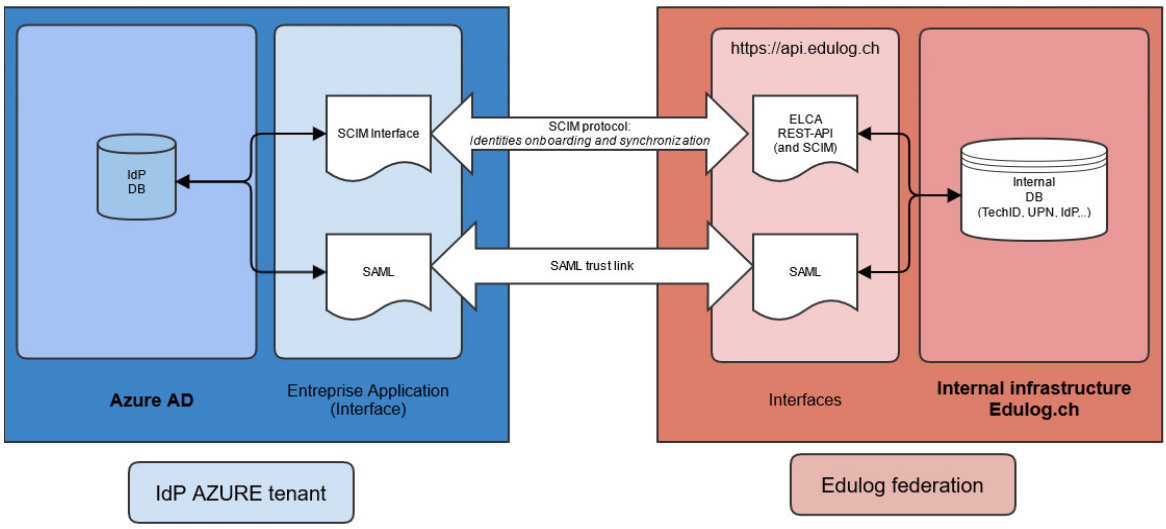
2.1 Procédure globale

N°	Actions	But/Commentaire
1	Création d'un *token* longue durée	Ceci est nécessaire pour pouvoir effectuer les synchronisations entre les identités de votre tenant et Edulog.
2	Configuration de la fonctionnalité SCIM	Pour fédérer les identités dans Edulog.
3	Tests de synchronisation	Serviront à vérifier l'envoi des nouveaux attributs à travers le protocole SCIM.

Le point 1 doit être réalisé en ligne de commande (sous Windows ou Linux), le reste des actions peuvent se faire depuis l'interface du portail *Azure*.

2.2 Eléments de l'infrastructure

Le schéma ci-dessous représente les différents éléments de la synchronisation SCIM.



On peut distinguer :

- Un IdP dont les identités sont dans un Azure AD Tenant.
- Une Enterprise application comme SAML endpoint et comme interface SCIM dans le tenant Azure.
- L'infrastructure d'Edulog avec le REST-API et le SAML endpoint.

A noter :

- SAML trustlink : sert à communiquer de façon sûre les attributs des utilisateurs d'Edulog, lorsque ceux-ci se connectent à un fournisseur de services (Service Provider). Il est continuellement en fonctionnement.
- Interface SCIM : sert à synchroniser les changements dans les identités qui affectent Edulog (fédération / défédération de nouveaux utilisateurs, changement d'UID...).

3. Configuration de la fonctionnalité SCIM

Afin de faciliter la fédération / défédération des utilisateurs depuis Azure AD dans Edulog, une interface SCIM est disponible. Cette section détaille la configuration d'Azure AD pour tirer parti de cette interface standardisée.

3.1 Génération d'un *token* de longue durée

Edulog met à disposition des IdP une REST-API pour certaines fonctions qui peuvent être automatisées. Chaque IdP qui le souhaite peut recevoir un utilisateur technique et son authentifiant. Une de ces fonctions permet la génération d'un *token* de longue durée, qui va être utilisé dans la configuration de SCIM pour authentifier l'IdP.

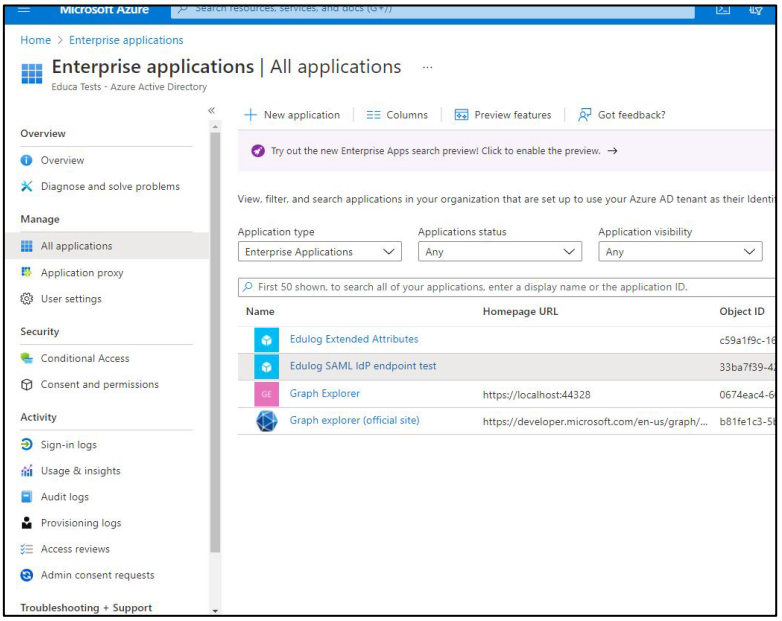
La génération de celui-ci peut être faite depuis la ligne de commande en utilisant, par exemple, le programme *curl*.

L'ensemble des fonctionnalités, ainsi que le détail de la commande ci-dessus indiquée, sont disponibles dans le document **« Edulog API reference »** (qui n'est pas public).

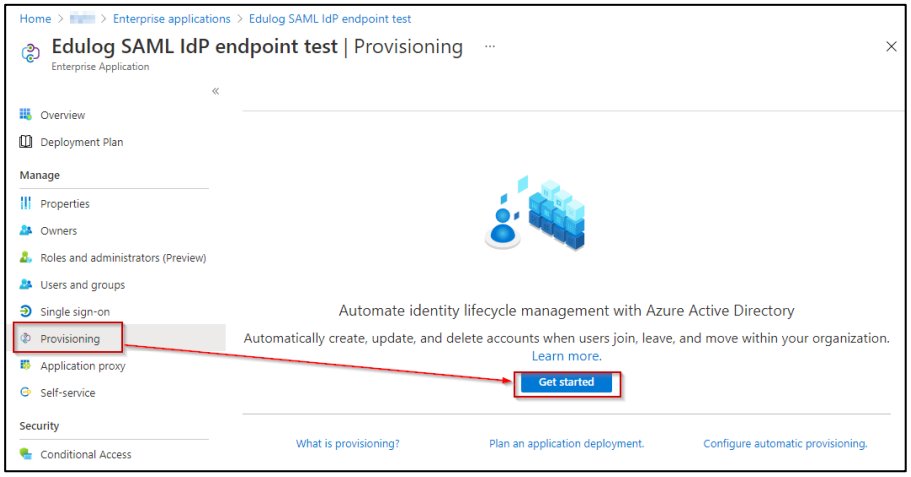
3.2 Configurer la connexion SCIM

Commencer par sélectionner, dans le tenant Azure, l'Enterprise application qui a dû être antérieurement créée lors de la phase de fédération. Elle va maintenant être utilisée pour effectuer l'*onboarding* des identités.

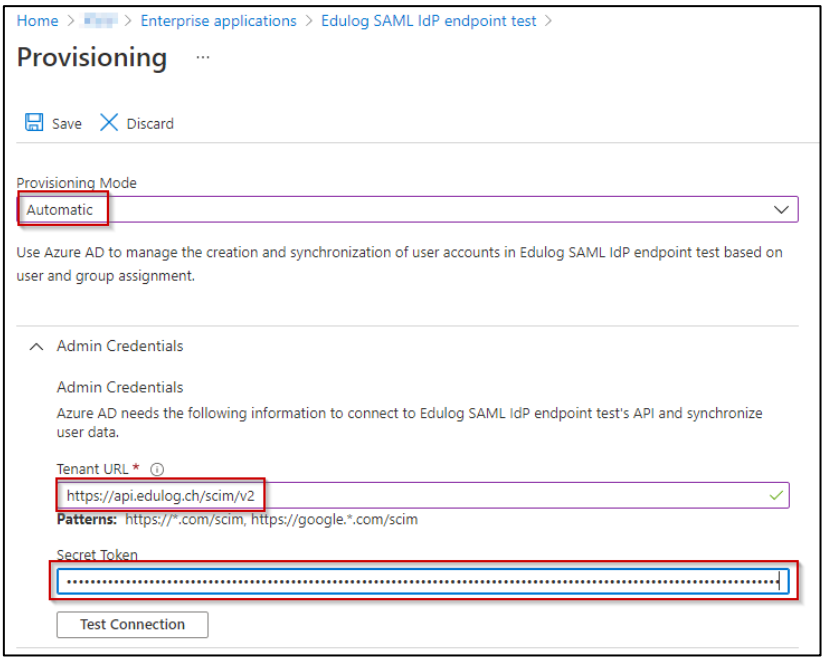
a. Sélection de l'Enterprise application (sur l'image: « Edulog SAML IdP endpoint test ») :



b. Sélectionner « Provisioning», et enfin « Get started » :



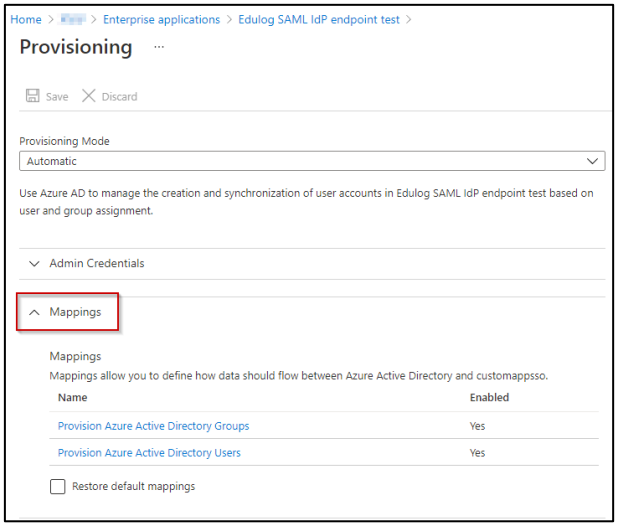
c. Sélectionner « Automatic » en tant que « Provisioning Mode ».



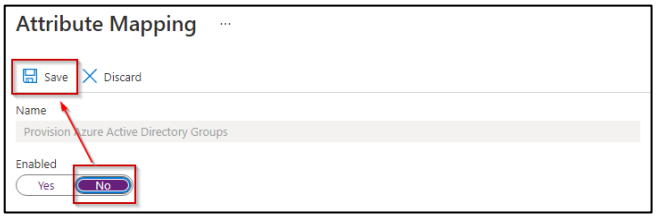
- Dans le champ « Tenant URL », inscrire l'URL SCIM Edulog (p.ex. https://api.edulog.ch/scim/v2/realms/edulog/).
- Dans le champ « Secret Token », copier le token généré antérieurement au point 3.1 grâce à l'API d'Edulog.

Finalement, appuyer sur « Test Connection » pour s'assurer que tous les paramètres sont corrects, puis sauvegarder la configuration.

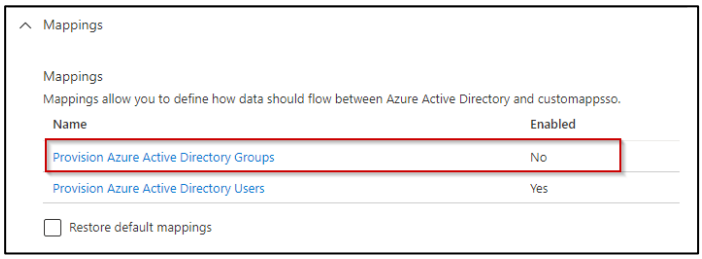
Une fois que la configuration est correctement sauvegardée, la section « Mappings » apparaît :



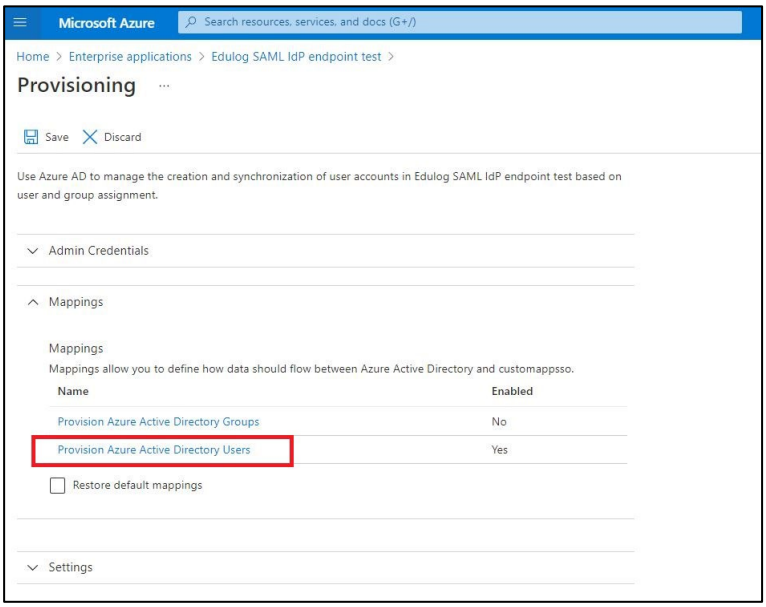
d. Cliquer sur « Provision Azure Active Directory Groups » pour la désactiver. Sauvegarder la configuration:



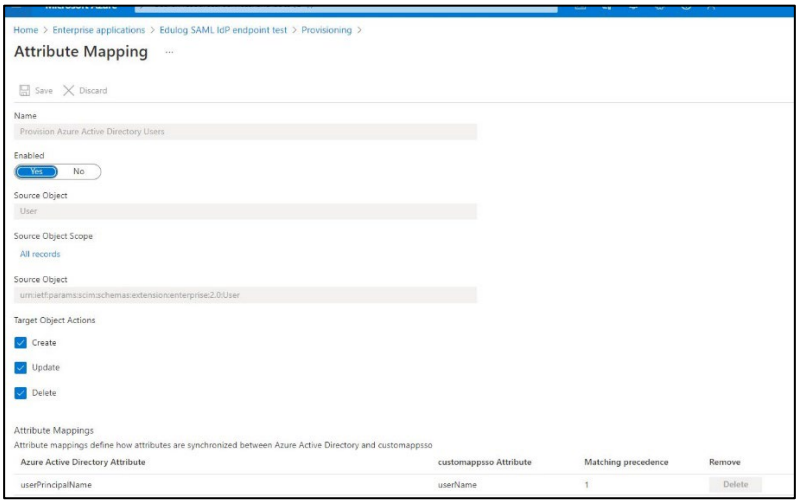
e. Revenir sur la configuration du provisioning. S'assurer que le provisioning des groupes est bien désactivé :



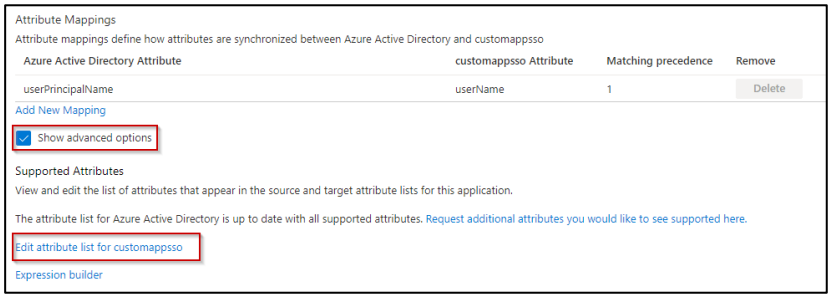
f. Cliquer sur « Provision Azure Active Directory Users »



Dans la section « Attribute Mappings », supprimer tous les mappings existants, sauf « userPrincipalName » :



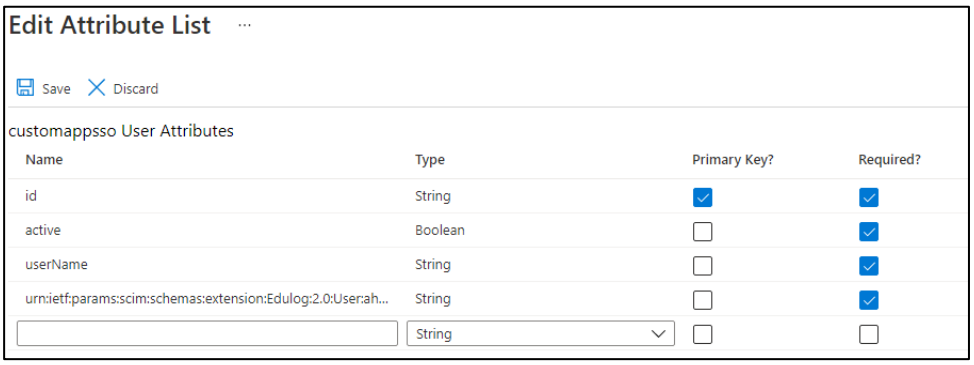
g. Cliquer sur « Show advanced options », puis sur « Edit attribute list for customappsso » pour déclarer les attributs supportés par Edulog :



h. Modifier la liste des attributs. Dans la liste d'attributs :

- Ajouter le flag « Required » pour l'attribut « active »
- Ajouter le nouvel attribut suivant :
  Name : urn:ietf:params:scim:schemas:extension:Edulog:2.0:User:ahvn13
  Type : String
  Required : true

Sauvegarder les changements.

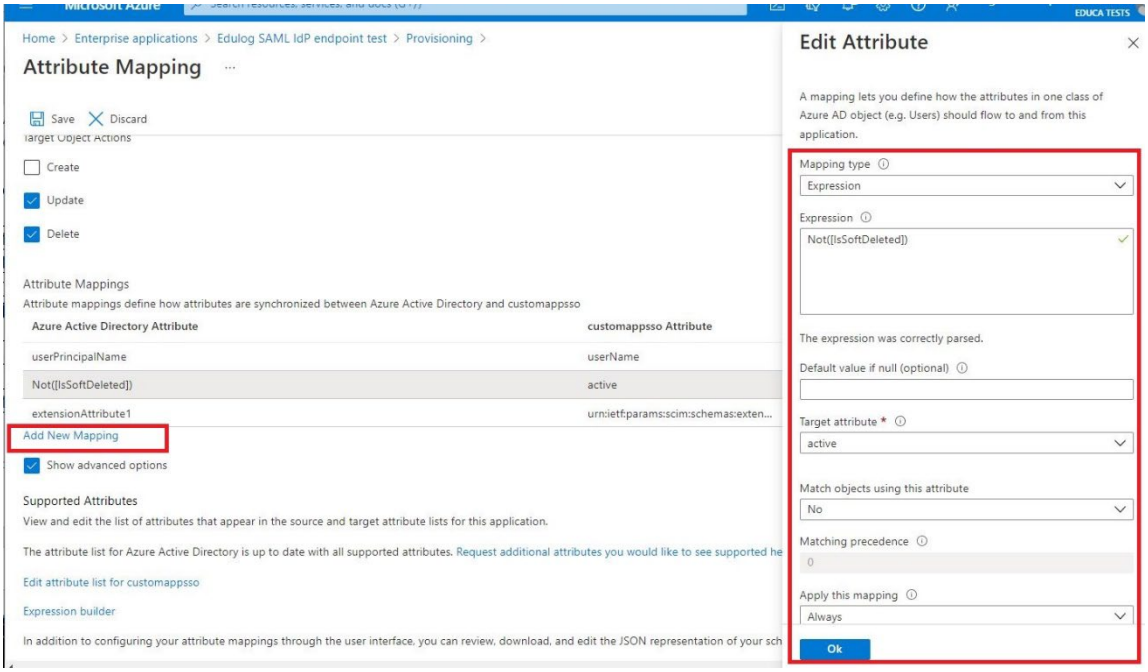


Il est probablement nécessaire à ce stade d'effectuer un rafraîchissement de l'interface graphique Azure (appuyer sur F5) pour être sûr que les nouveaux attributs sont pris en compte et disponibles pour l'étape suivante.

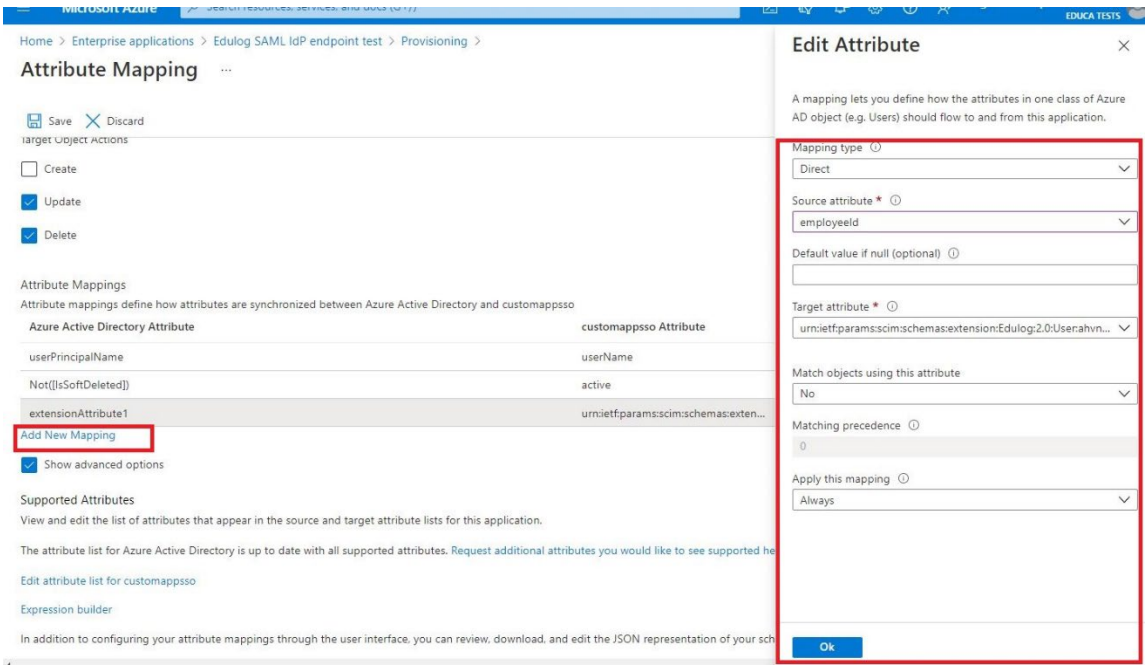
i. Ajouter deux nouveaux mappings :

- *Not([IsSoftDeleted])*

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



- *extensionAttribute1* (ou tout autre attribut contenant le numéro AVS)

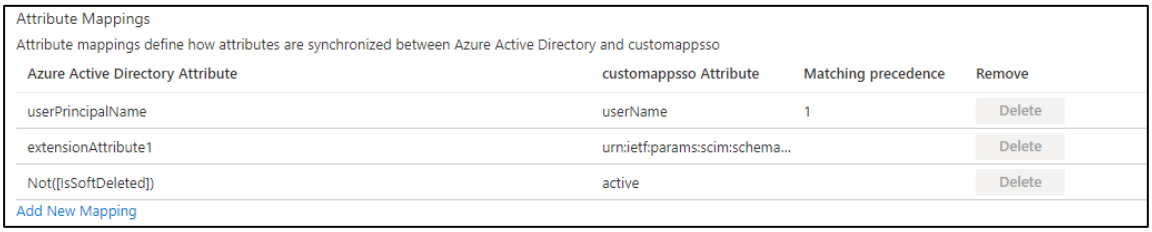


Mapping type	Direct
Source attribute	nom de l'attribut contenant le numéro AVS
Target attribute	urn:ietf:params:scim:schemas:extension:Edulog:2.0:User:ahvn13
Match object using this attribute	No
Apply this mapping	Only during object creation

j. Vérifier le *mapping userName*

S'assurer que le mapping déjà existant (userName) est bien lié à l'attribut Azure AD contenant l'identifiant que l'utilisateur connaît pour accéder à son compte (p.ex. adresse e-mail).

Remarque : l'aperçu d'écran ci-dessous n'est qu'un exemple d'une configuration possible. Les attributs de la colonne « Azure Active Directory Attribute » doivent être adaptés en fonction de la configuration de votre tenant :


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	Delete
extensionAttribute1	urn:ietf:params:scim:schema...		Delete
Not([IsSoftDeleted])	active		Delete

Add New Mapping

Finalement, sauvegarder les changements en cliquant sur « Save ».

4. Activation du provisioning

4.1 Lancement du provisioning

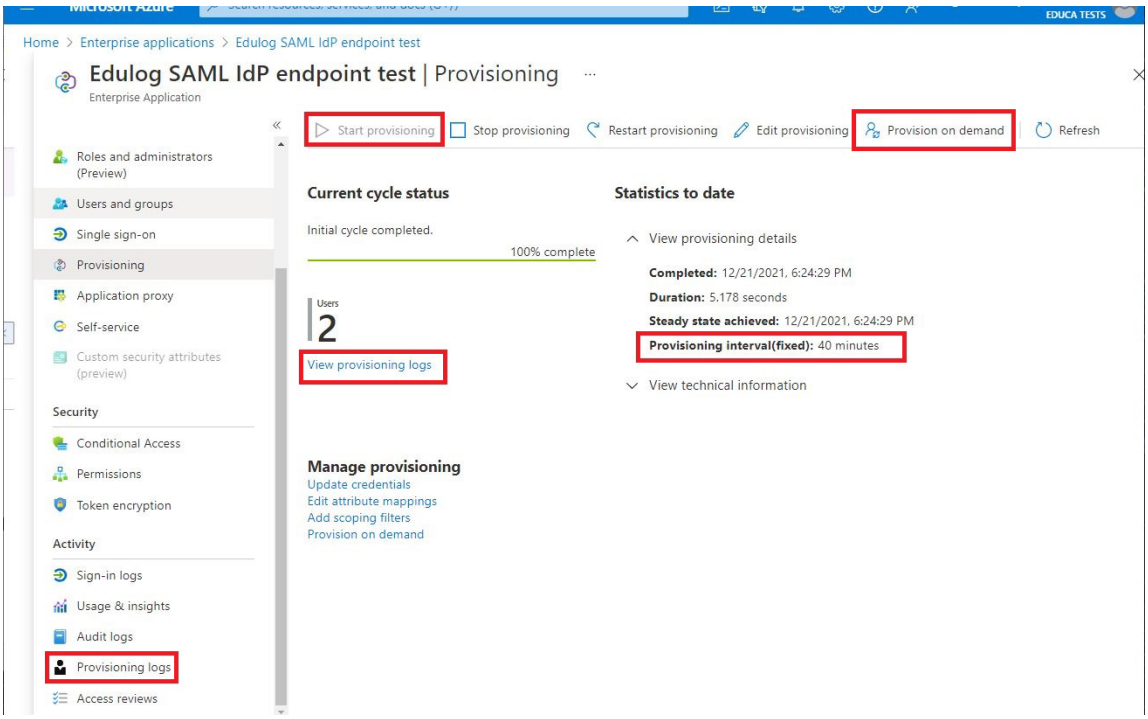
Retourner dans la section « Provisioning » de l'*Enterprise application* et cliquer sur « Start Provisioning » (voir image ci-dessous).

Ceci démarrera le processus de création des utilisateurs de l'*Enterprise application* dans Edulog.

4.2 Logs du provisioning

Le processus de provisioning s'exécute de façon régulière mais est totalement géré par la plateforme Azure (toutes les 40 minutes – voir image ci-dessous). Il n'est pas possible de forcer l'exécution du processus, si ce n'est pour un utilisateur en particulier (*Provisioning on demand*).

Pour obtenir des détails concernant les diverses opérations effectuées par le processus de provisioning, il est possible de consulter les logs de provisioning disponibles dans l'interface Azure (voir image).



En cas de problème, ces logs peuvent être utilisés pour identifier la cause de potentielles erreurs.