Authentification avec Azure AD

Juin 2023

Résumé du document
Résumé

Version du 5 juin 2023

Berger Levrault

CONTACTS

coba.activites@berger-levrault.com
coba.collegial@berger-levrault.com
coba.finance@berger-levrault.com
coba.pedago@berger-levrault.com
coba.rhpaie@berger-levrault.com

Berger-Levrault Canada
2130, boulevard Dagenais Ouest, bureau 200
Laval (Québec) H7L 5X9

514 251-2622 | 1 844 228-2622
ventes.canada@berger-levrault.com

AVERTISSEMENT ET NOTES

Dans le présent document, le genre masculin est utilisé au sens neutre et désigne les femmes autant que les hommes.

berger-levrault.com

Table des matières

Introduction

À l'ère de la transformation numérique, des mécanismes d'authentification sécurisés et fiables sont essentiels pour protéger les données sensibles et garantir que seuls les utilisateurs autorisés ont accès aux ressources.

Dans l'optique de permettre aux collèges d'utiliser un fournisseur d'authentification pour remplacer l'authentification propriétaire de COBA, nous avons intégré le fournisseur d'authentification Azure AD (Azure Active Directory) à nos portails, à nos applications mobiles et à nos applications administratives V6.

L'utilisation d'un fournisseur d'authentification est et restera une option facultative pour les institutions qui utilisent actuellement nos produits.

Vous trouverez dans ce guide, l'ensemble des étapes pour paramétrer votre fournisseur d'authentification Azure AD et vos applications COBA dans le but de les intégrer avec une authentification avec Azure AD.

PRÉREQUIS

L'authentification avec un fournisseur d'authentification tel qu'Azure AD nécessite l'option **Authentification Azure AD** à la licence d'utilisation du logiciel.

Définition un fournisseur d'authentification

Azure AD

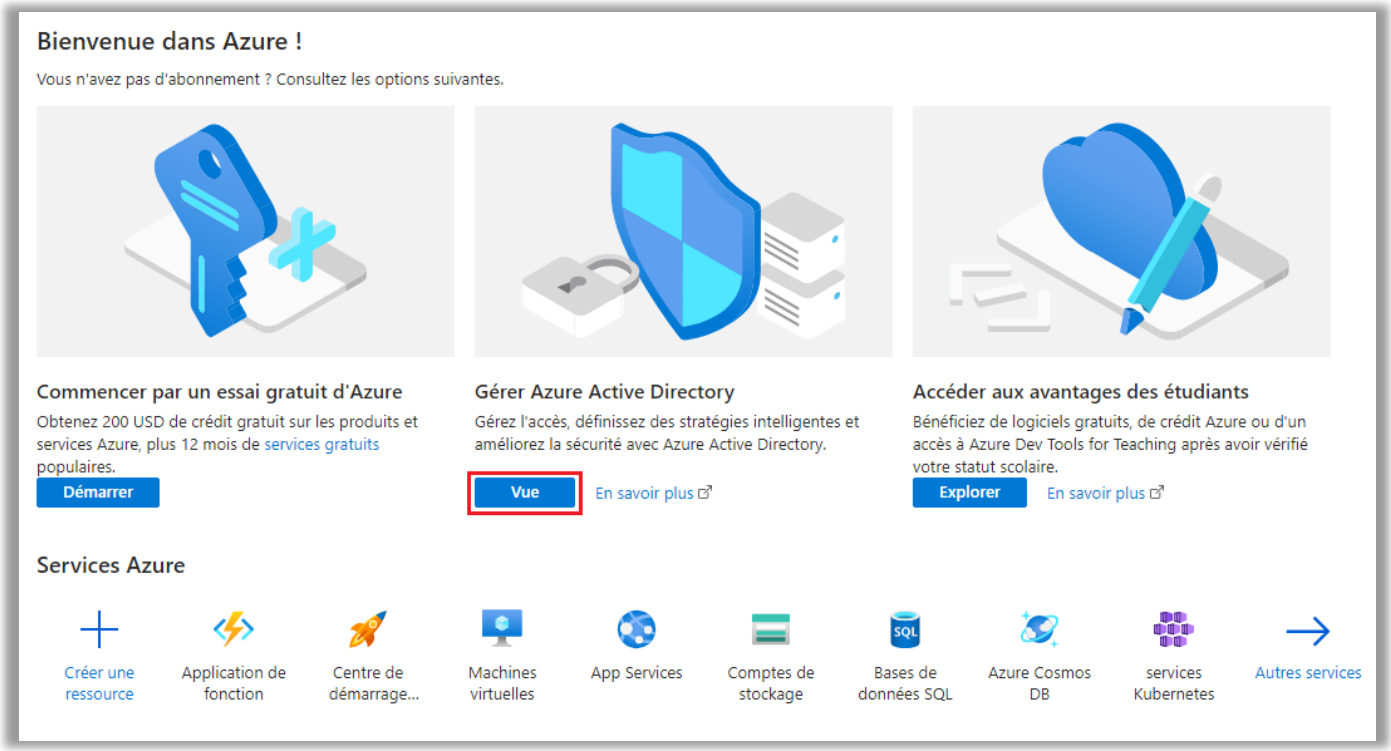
Pour permettre à des applications d'utiliser Azure AD comme fournisseur d'authentification, vous devez au préalable vous connecter dans le portail Azure afin d'y définir des applications. Les paramètres de ces applications seront utilisés afin de configurer les fournisseurs d'authentification pour les applications, les portails et les applications mobiles de la gamme COBA.

Étape 1 – Accéder au portail Azure

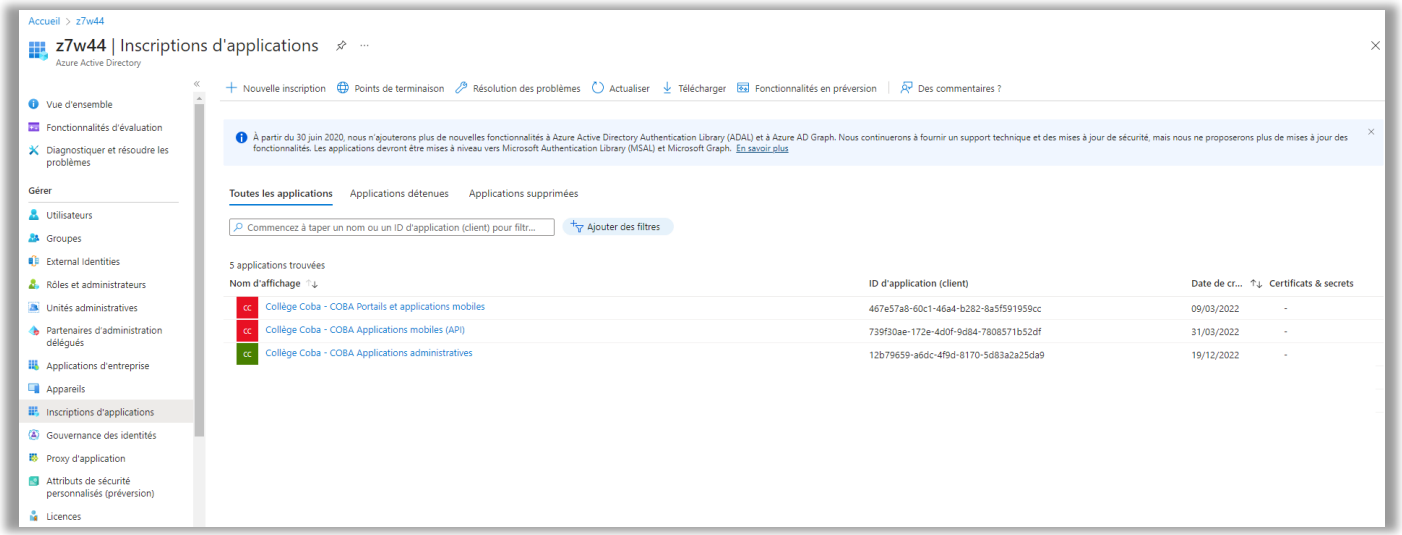
Connectez-vous au portail Azure (https://portal.azure.com/) avec vos informations comme administrateur du portail.

Étape 2 – Accéder aux inscriptions d'applications

Cliquer sur le bouton **Vue** de la section Gérer **Azure Active Directory**.



Sélectionner l'item **Inscriptions d'applications** dans le menu de gauche et l'onglet **Toutes les applications**.

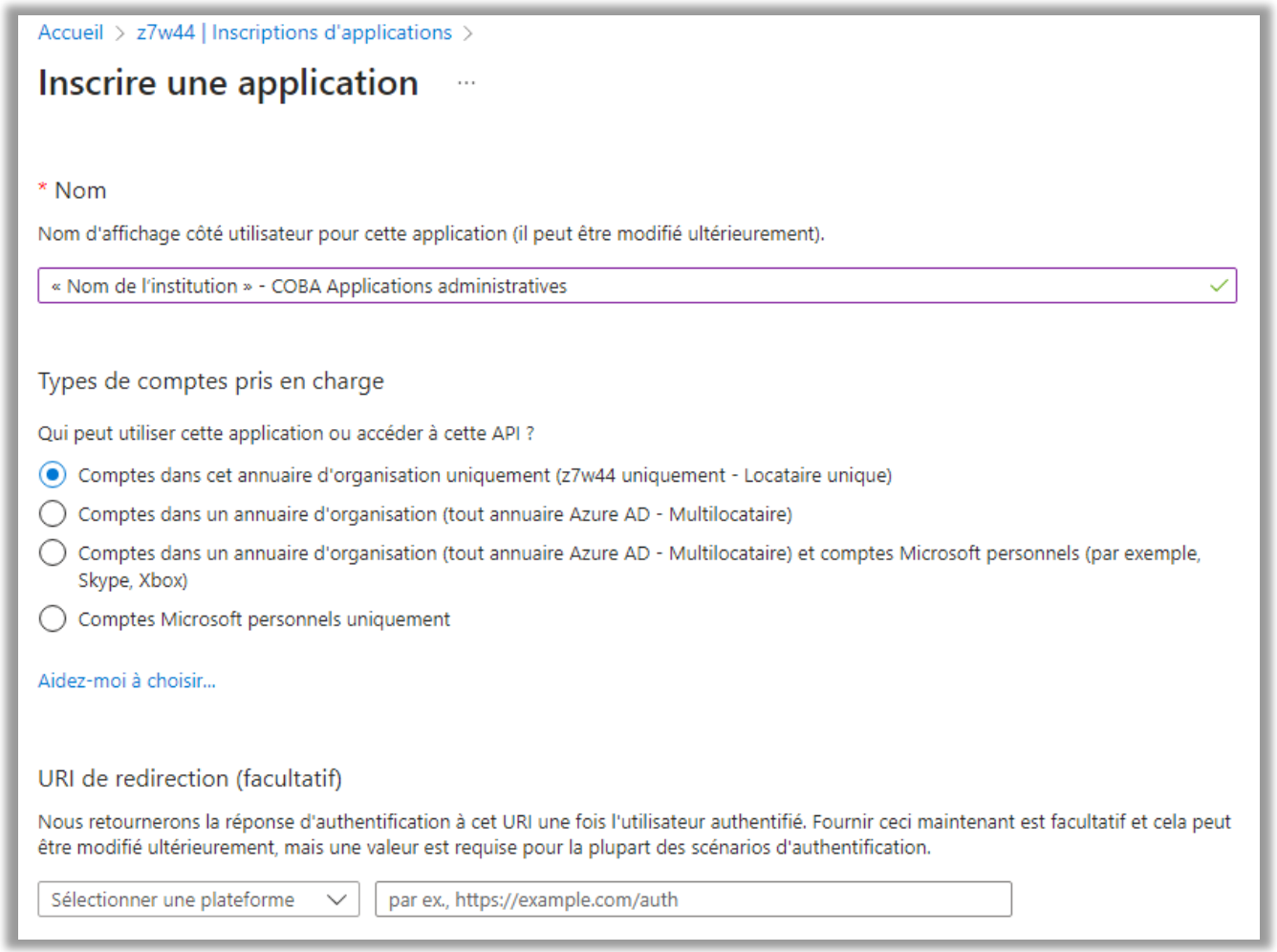


Note :

Selon le type d'implantation que votre institution veut réaliser et les produits de la gamme COBA que votre institution possède, vous aurez à créer d'une à trois inscriptions dans Azure.

Étape 3 – Créer une nouvelle inscription pour le logiciel administratif V6

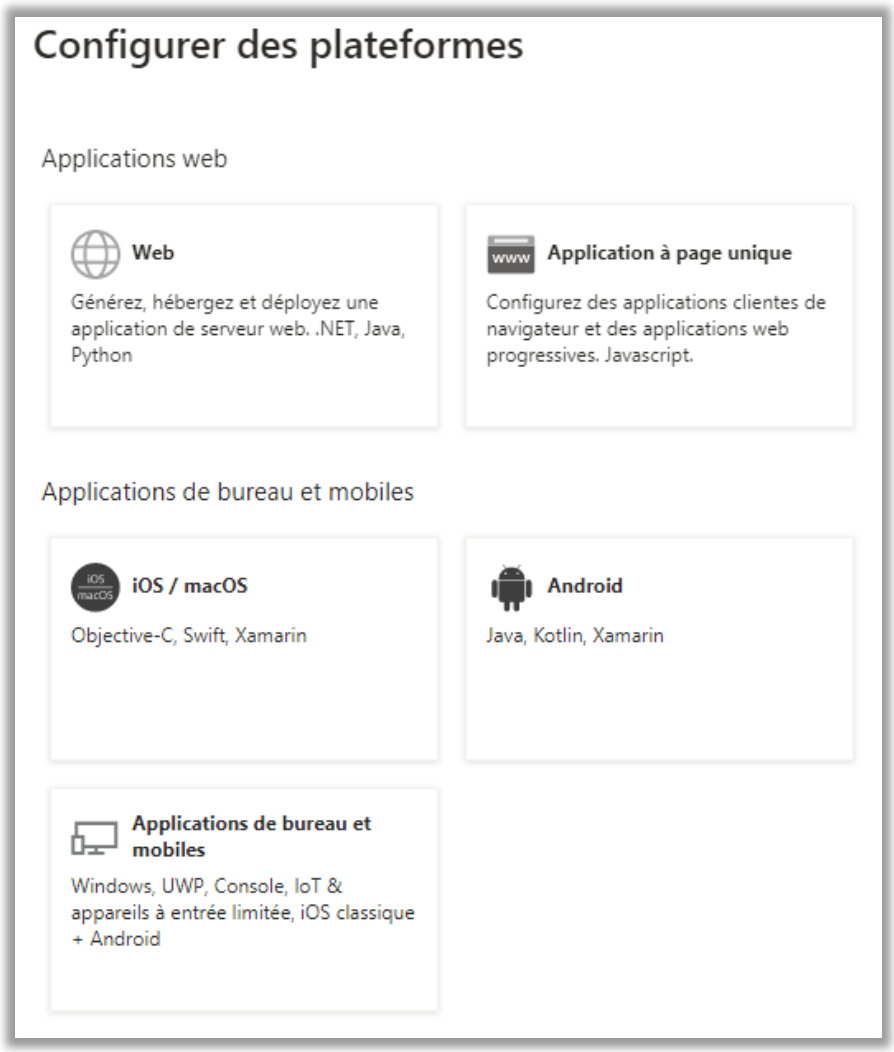
Étape 3.1 - Cliquer sur le bouton **+ Nouvelle inscription** pour créer une nouvelle inscription.



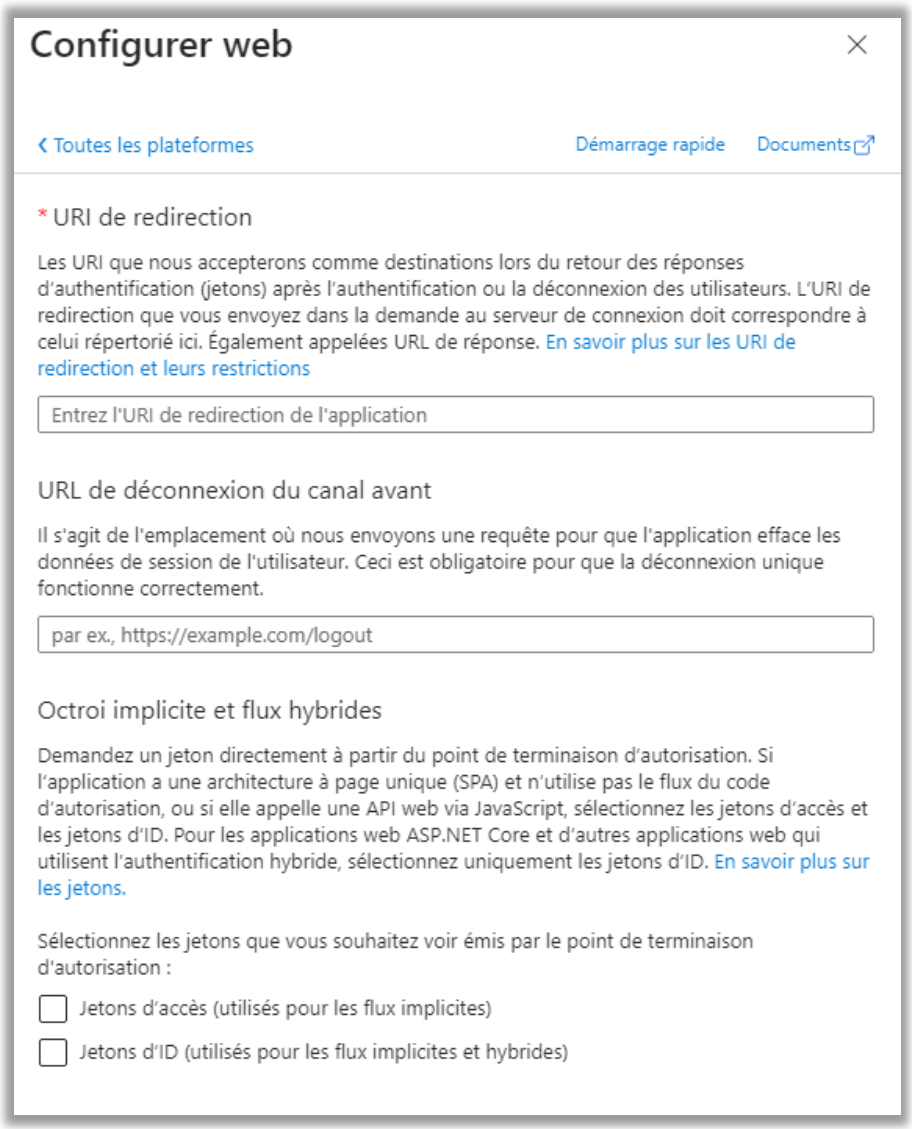
- **Nom**
  - Saisir « Nom de l'institution » - COBA Applications administratives
- **Types de comptes pris en charge**
  - Sélectionner Compte dans cet annuaire d'organisation uniquement
- **Sélectionner l'URI de redirection**
  - Ne pas compléter cette section

Étape 3.2 - Accéder à l'option **Authentification** du menu de gauche et cliquer sur le lien **+ Ajouter une plateforme**.

Étape 3.3 – Sélectionner la plateforme **Web**.



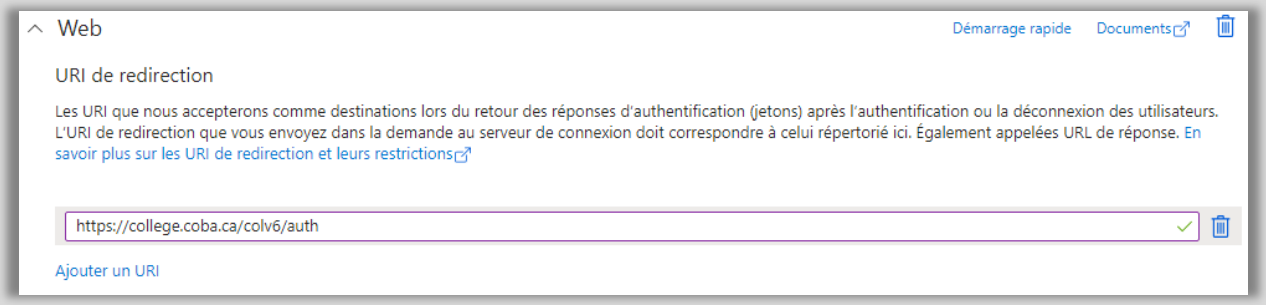
Étape 3.4 – Compléter les champs ci-dessous et cliquer sur le bouton **Configurer**.



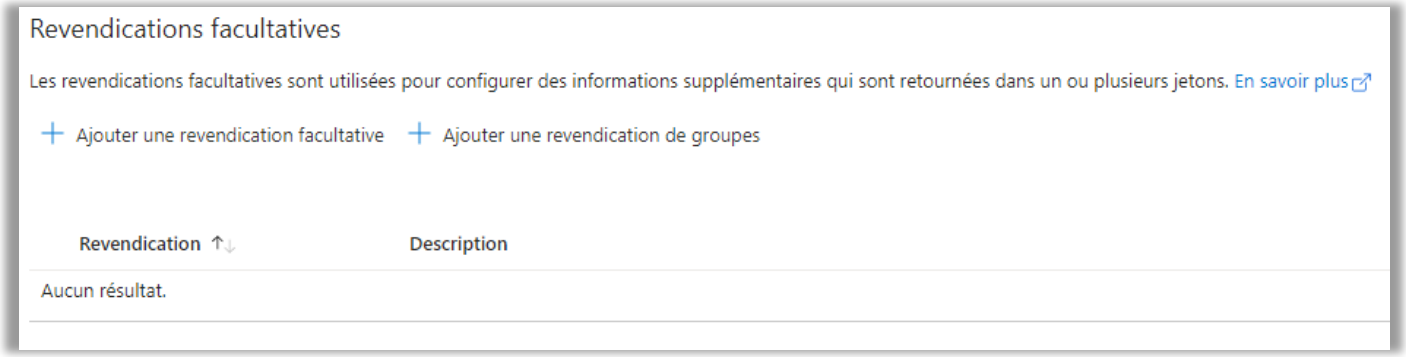
- **URI de redirection**
  - Saisir l'URI de l'application V6 **en minuscule** suivi de /auth (ex. https://college.coba.ca/colv6/auth)
- Décocher **Jeton d'accès**
- Cocher **Jeton d'ID**

Note :

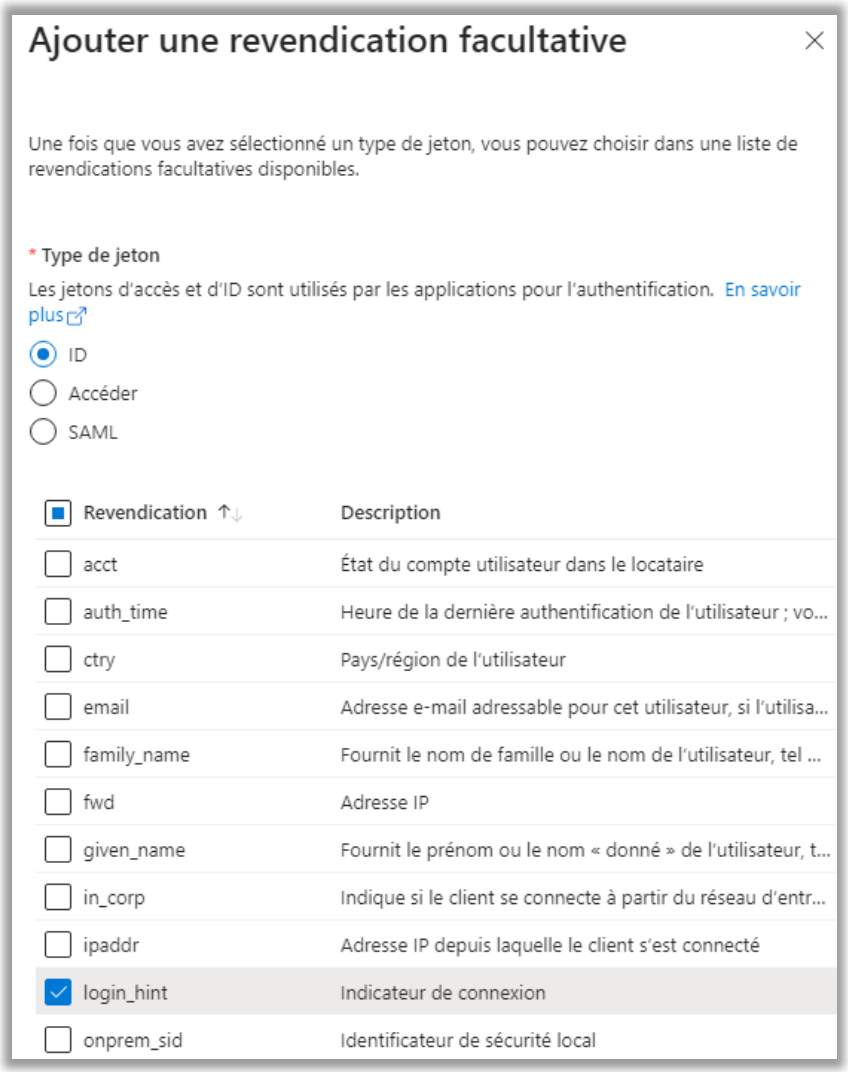
Si votre institution utilise d'autres applications administratives V6 de COBA pour lesquels vous voulez activer l'authentification avec Azure AD, vous devez accéder à l'option **Authentification** du menu de gauche, cliquer sur le lien **+ Ajouter une URI** et saisir l'URI de l'application **en minuscule** suivi de /auth.



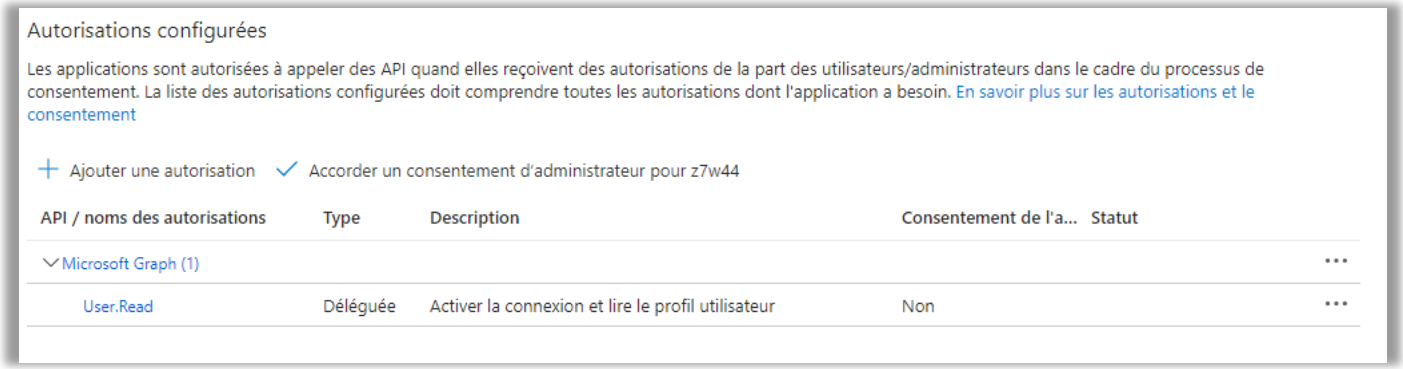
Étape 3.5 - Accéder à l'option **Configuration du jeton** du menu de gauche et cliquer sur le lien **+ Ajouter une revendication facultative**.



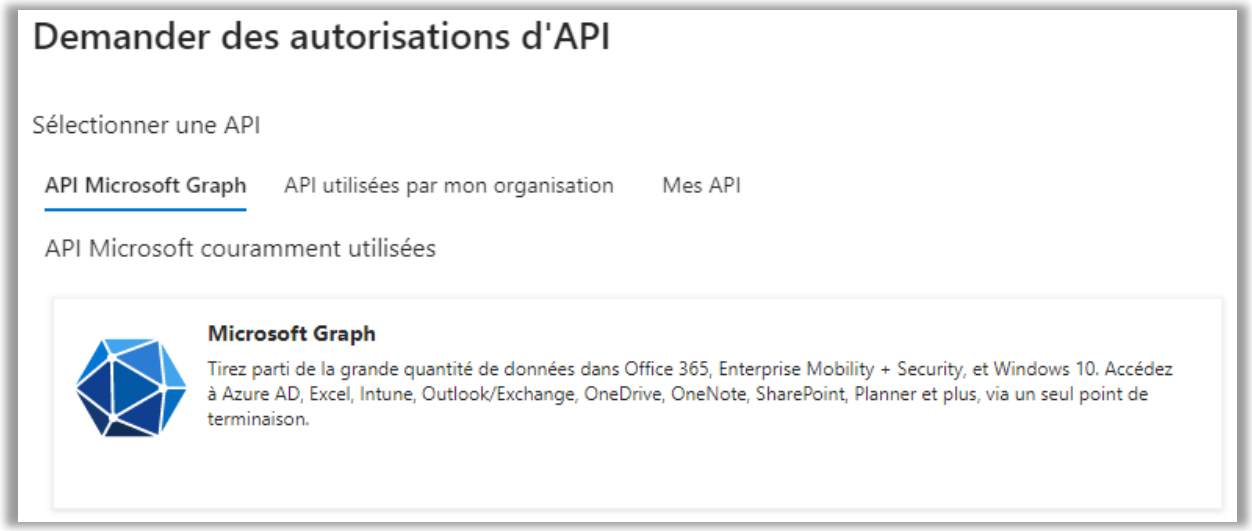
Étape 3.6 – Cocher le **Type de jeton** ID, cocher la **Revendication** login_hint et cliquer sur le bouton **Ajouter**.

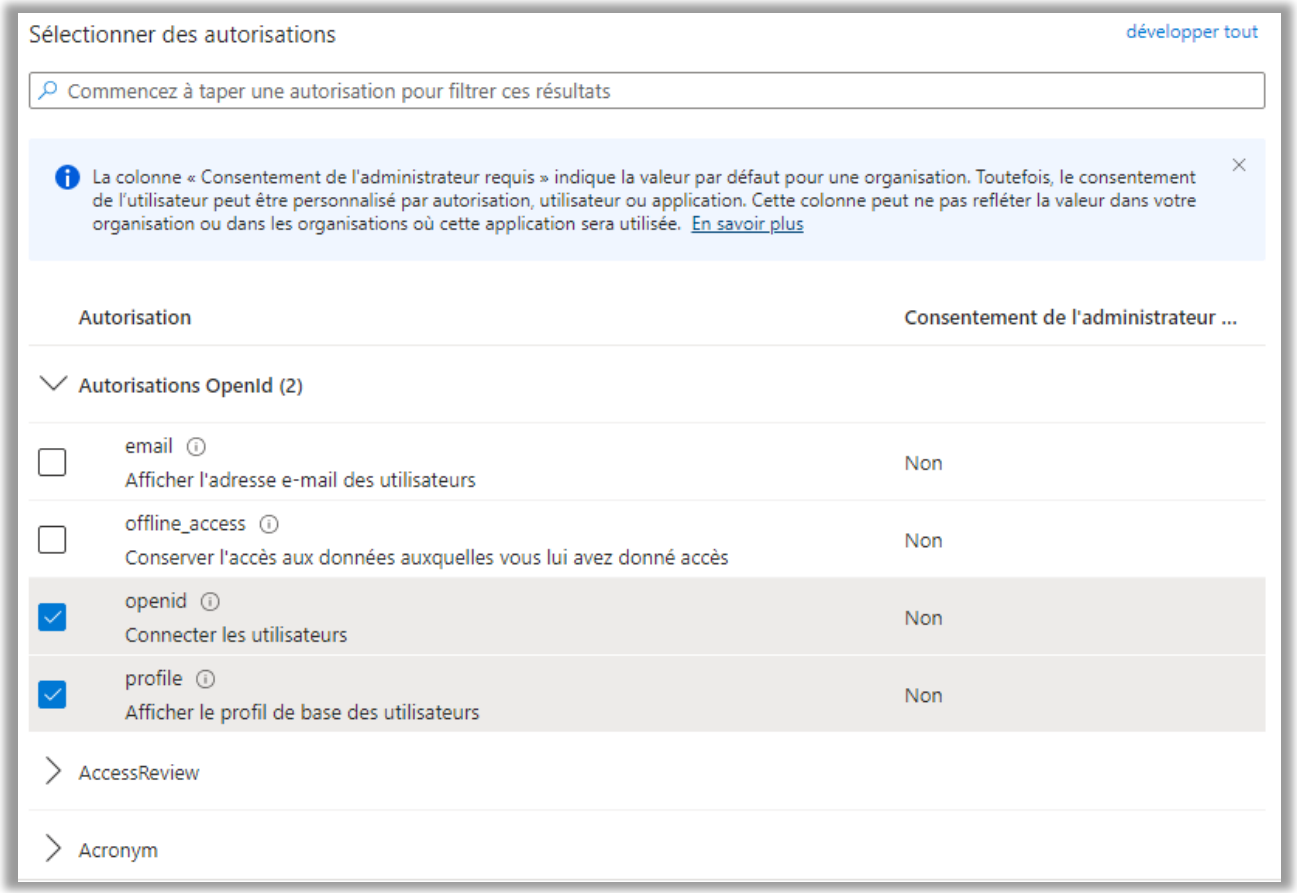


Étape 3.7 - Accéder à l'option **API autorisée** du menu de gauche et cliquer sur le lien **+ Ajouter une autorisation**.



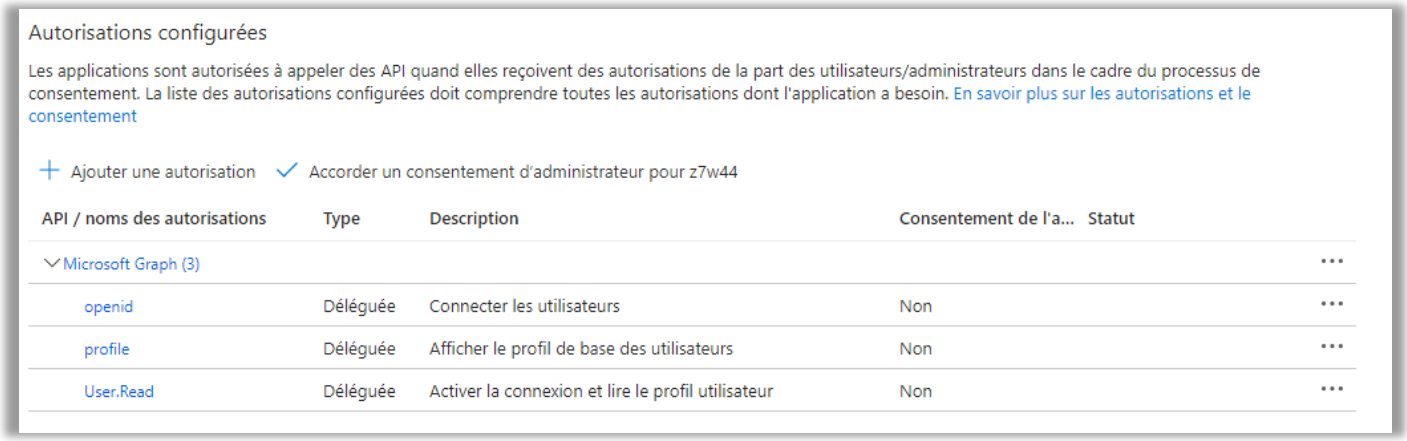
Étape 3.8 – Sélectionner **Microsoft Graph**, sélectionner **Autorisations déléguées**, cocher les autorisation **openid** et **profile** et cliquer sur le bouton **Ajouter des autorisations**.



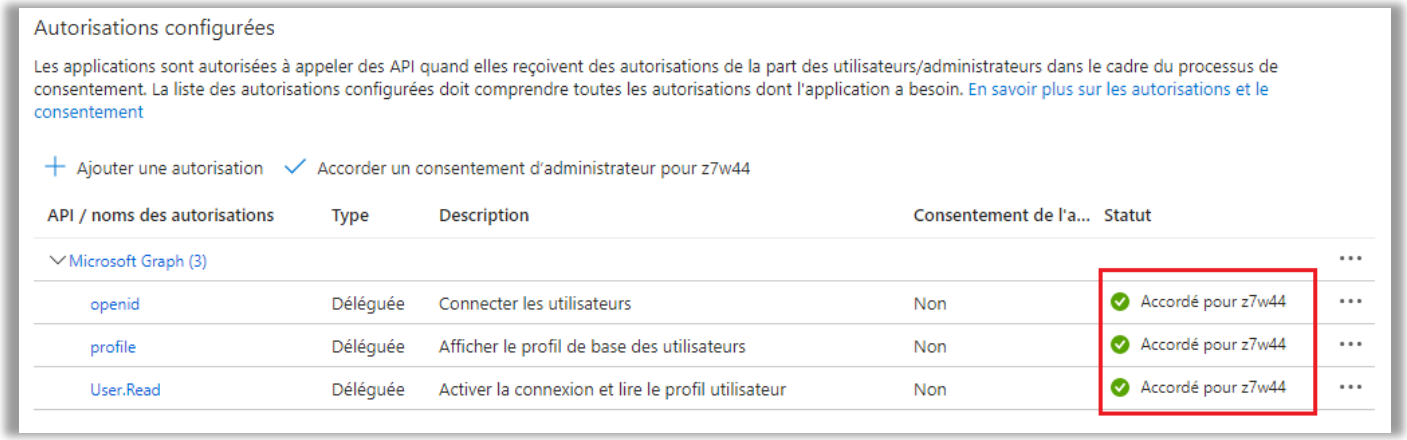


Étape 3.9 – Cliquer sur le lien **Accorder un consentement d'administrateur pour « votre domaine »** et confirmer.

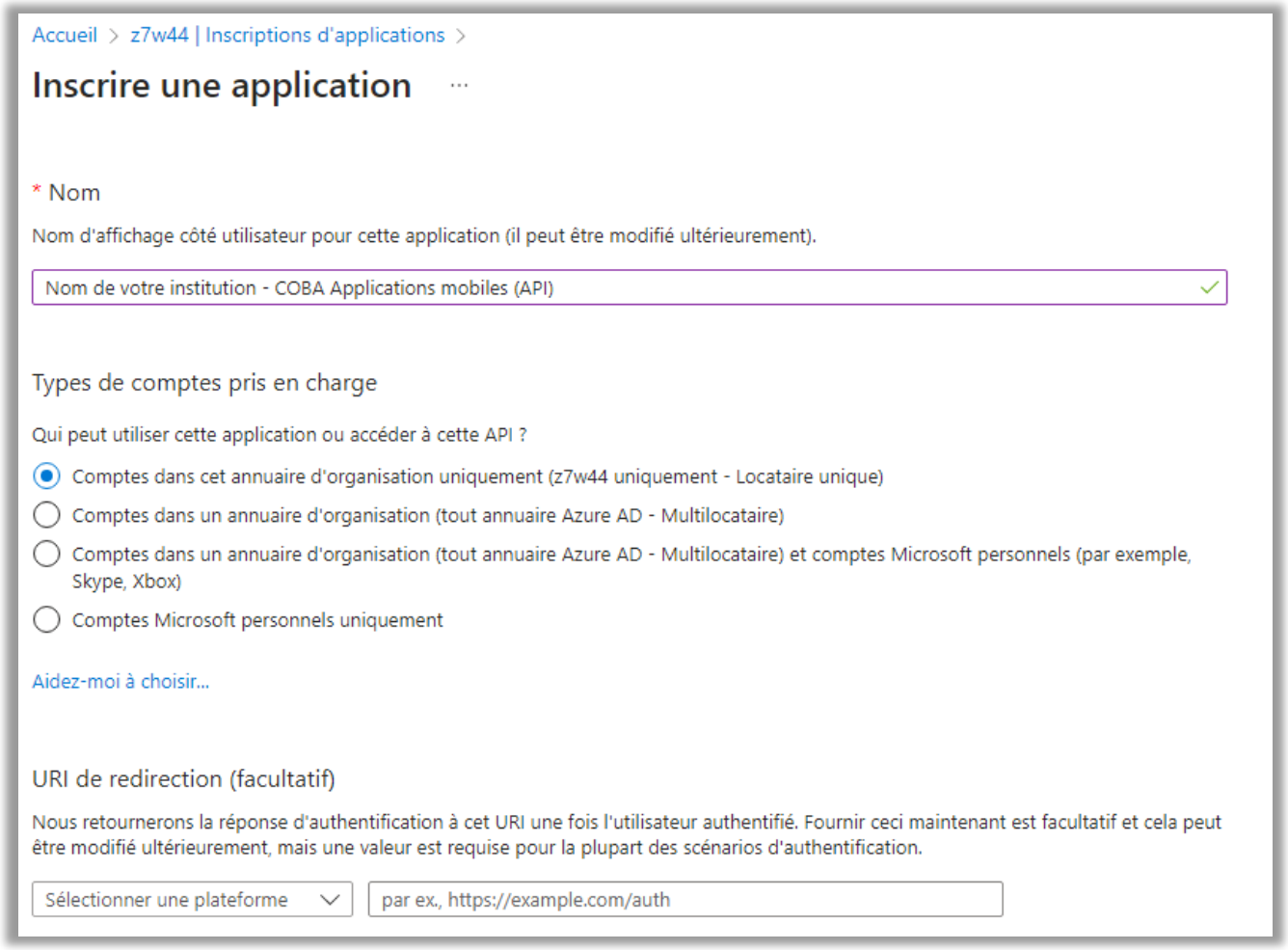
Avant



Après

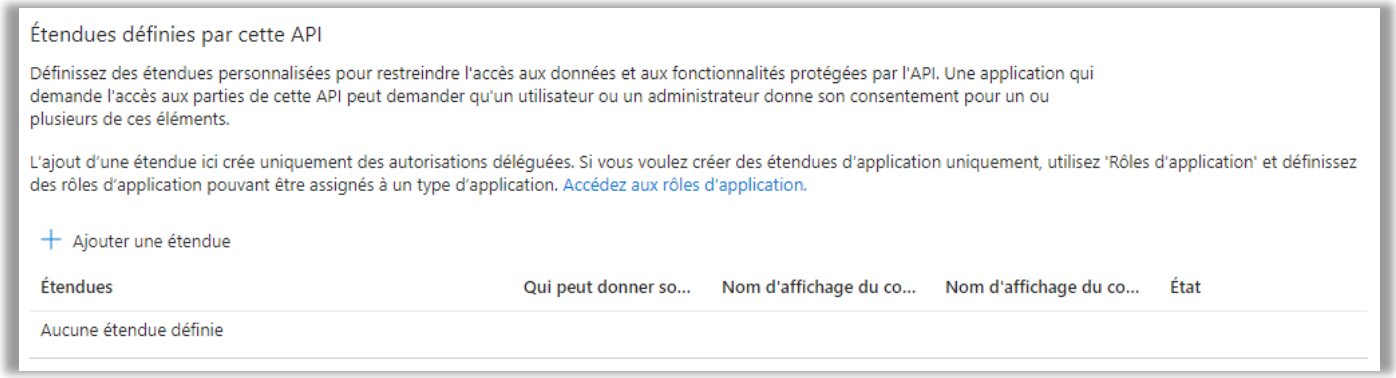


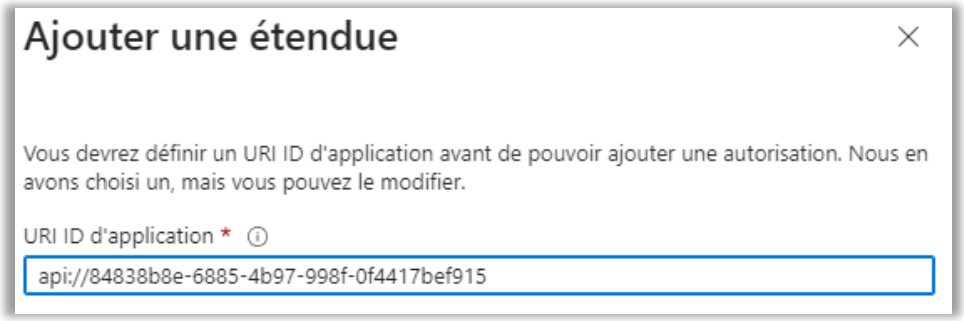
Étape 4.1 - Cliquer sur le bouton **+ Nouvelle inscription** pour créer une nouvelle inscription.



- **Nom**
  - Saisir « Nom de votre institution » - COBA Applications mobiles (API)
- **Types de comptes pris en charge**
  - Sélectionner Compte dans cet annuaire d'organisation uniquement
- **Sélectionner l'URI de redirection**
  - Ne pas compléter cette section

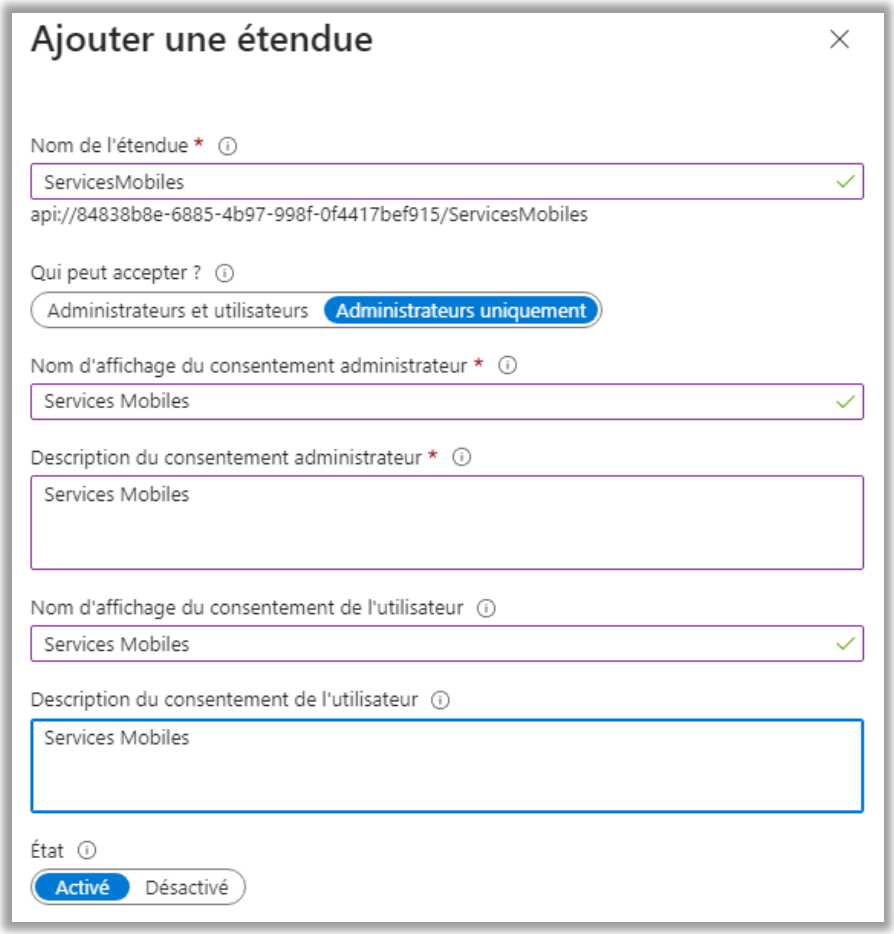
Étape 4.2 - Accéder à l'option **Exposer un API** du menu de gauche et cliquer sur le lien **+ Ajouter une étendue**.





Étape 4.3 – Cliquer sur le bouton **Enregistrer et continuer**

Étape 4.4 – Compléter les champs ci-dessous et cliquer sur le bouton **Ajouter une étendue**.



Administrateur et utilisateurs + Refaire l'image

Nom de l'étendue

- Saisir ServicesMobile

Nom d'affichage du consentement administrateur

- Saisir Services Mobiles

Description du consentement administrateur

- Saisir Services Mobiles

Nom d'affichage du consentement de l'utilisateur

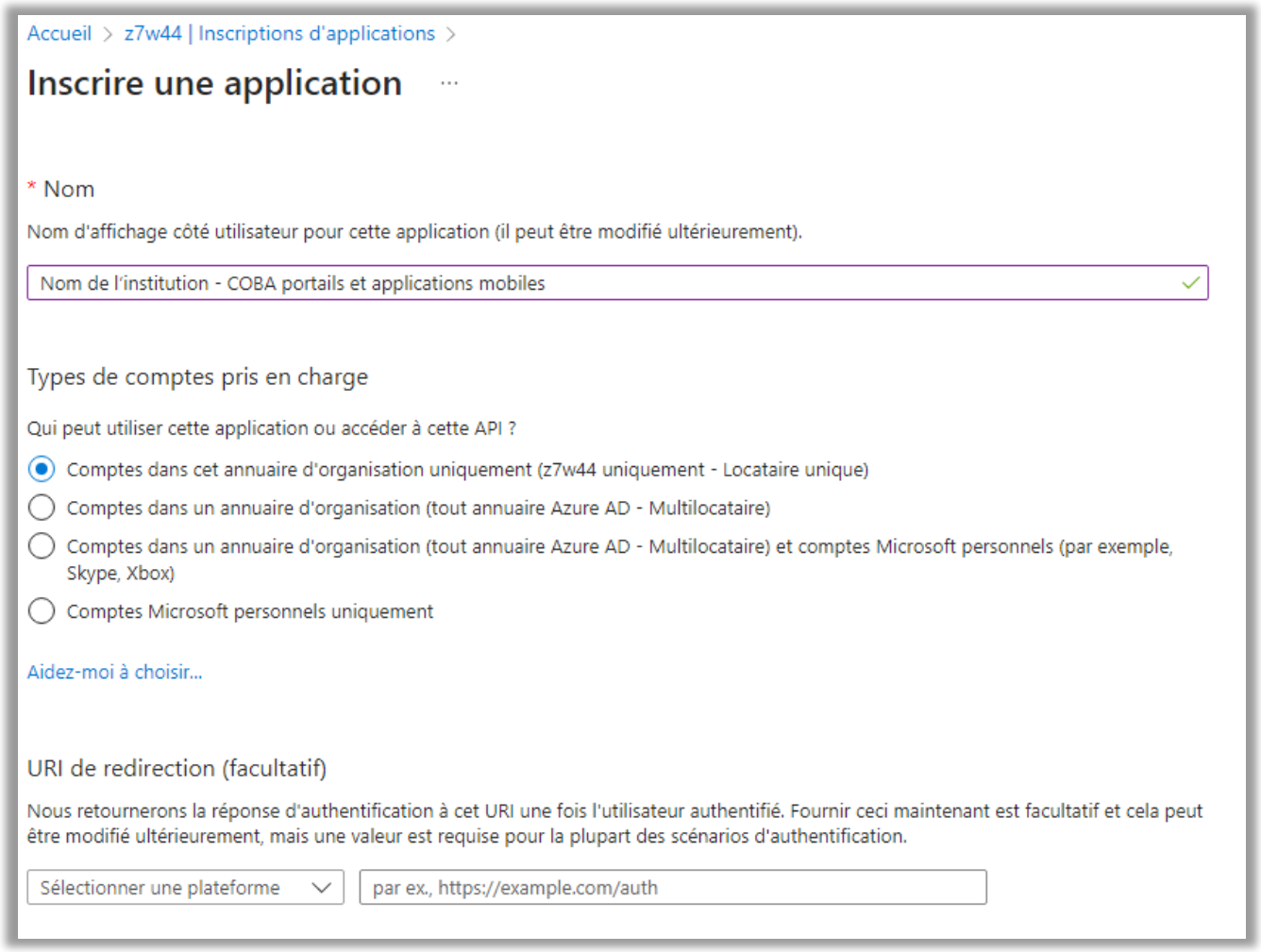
- Saisir Services Mobiles

Description du consentement de l'utilisateur

- Saisir Services Mobiles

Étape 5 – Créer une nouvelle inscription pour portail et application mobile

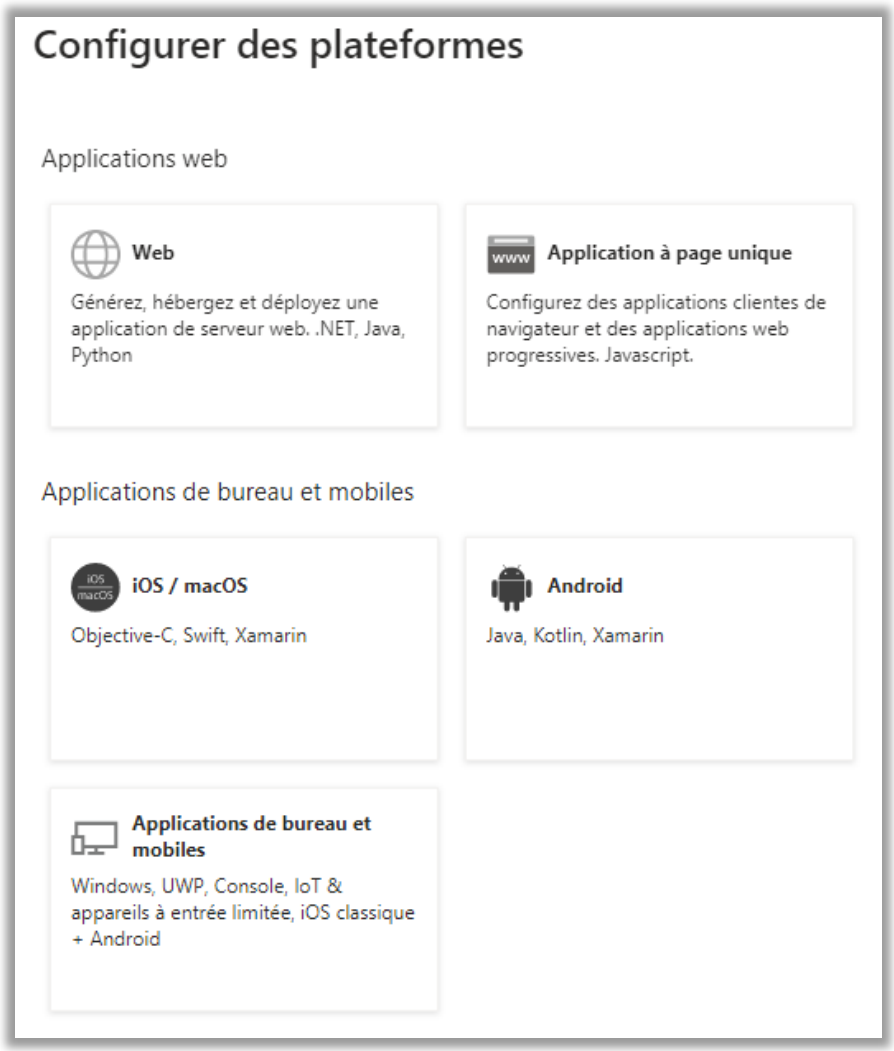
Étape 5.1 - Cliquer sur le bouton **+ Nouvelle inscription** pour créer une nouvelle inscription.



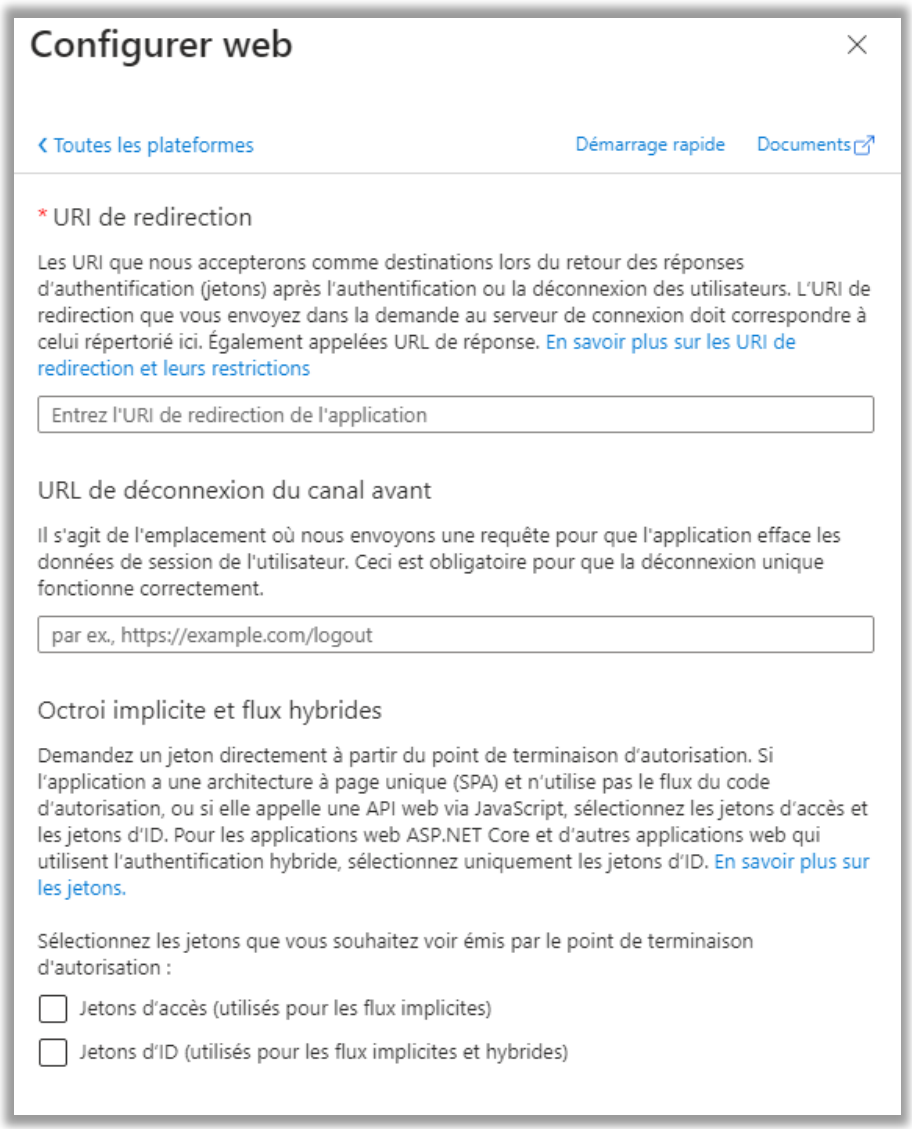
- **Nom**
  - Saisir « Nom de l'institution » - COBA portails et applications mobiles
- **Types de comptes pris en charge**
  - Sélectionner Compte dans cet annuaire d'organisation uniquement
- **Sélectionner l'URI de redirection**
  - Ne pas compléter cette section

Étape 5.2 - Accéder à l'option **Authentification** du menu de gauche et cliquer sur le lien **+ Ajouter une plateforme**.

Étape 5.3 – Sélectionner la plateforme **Web**.



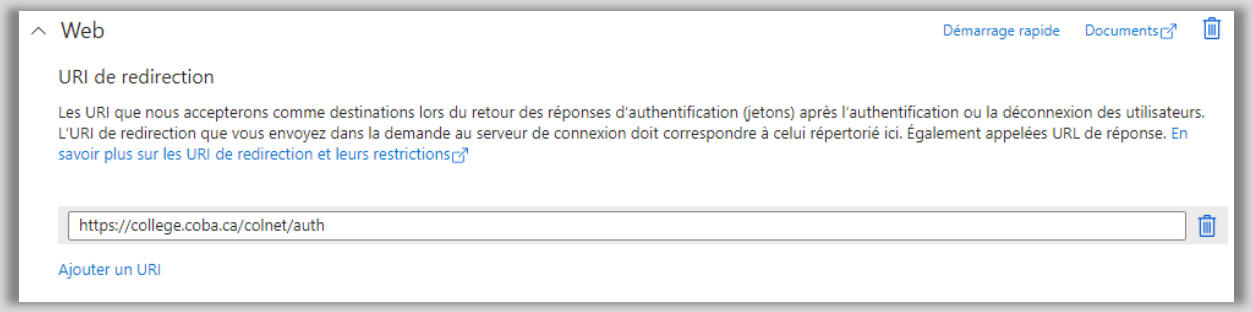
Étape 5.4 – Compléter les champs ci-dessous et cliquer sur le bouton **Configurer**.



- **URI de redirection**
  - Saisir l'URI du portail **en minuscule** suivi de /auth (ex. https://college.coba.ca/colnet/auth)
- Cocher **Jeton d'accès**
- Cocher **Jeton d'ID**

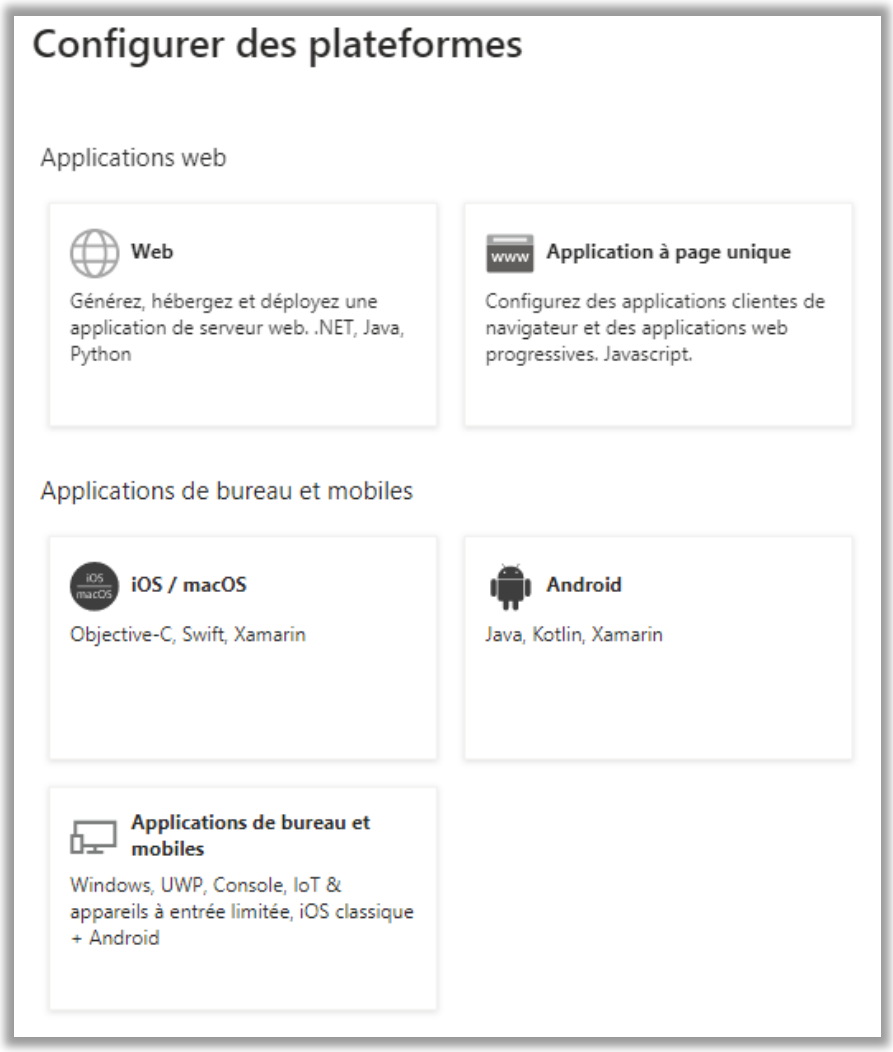
Note :

Si votre institution utilise d'autres portails de COBA pour lesquels vous voulez activer l'authentification avec Azure AD, vous devez accéder à l'option **Authentification** du menu de gauche, cliquer sur le lien **+ Ajouter une URI** et saisir l'URI du portail **en minuscule** suivi de /auth.



Étape 5.5 - Accéder à l'option **Authentification** du menu de gauche et cliquer sur le lien **+ Ajouter une plateforme**.

Étape 5.6 – Sélectionner la plateforme **iOS / macOS**.



Étape 5.7 – Compléter les champs ci-dessous, cliquer sur le bouton **Configurer** et cliquer sur le bouton **Terminé.**

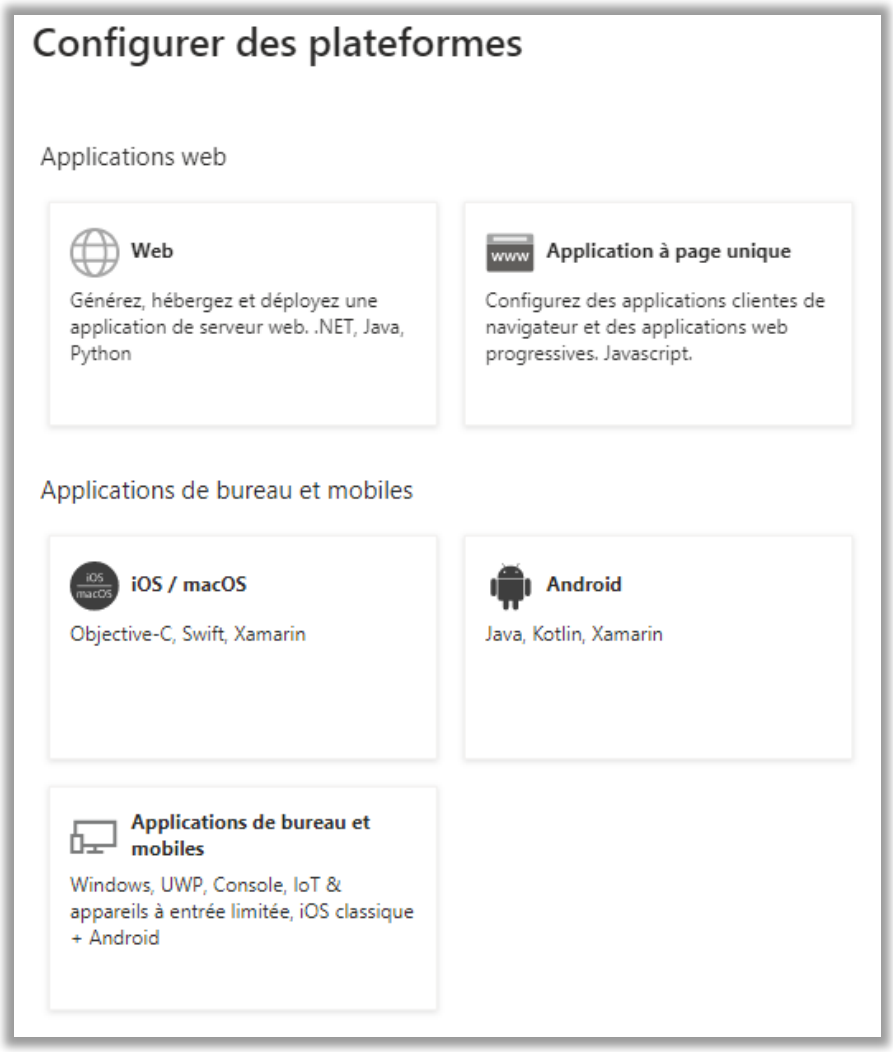
- **ID d'offre groupée**
  - Saisir ca.coba.scolarit
- **URI de redirection**
  - msauth.ca.coba.scolarit://auth

Note :

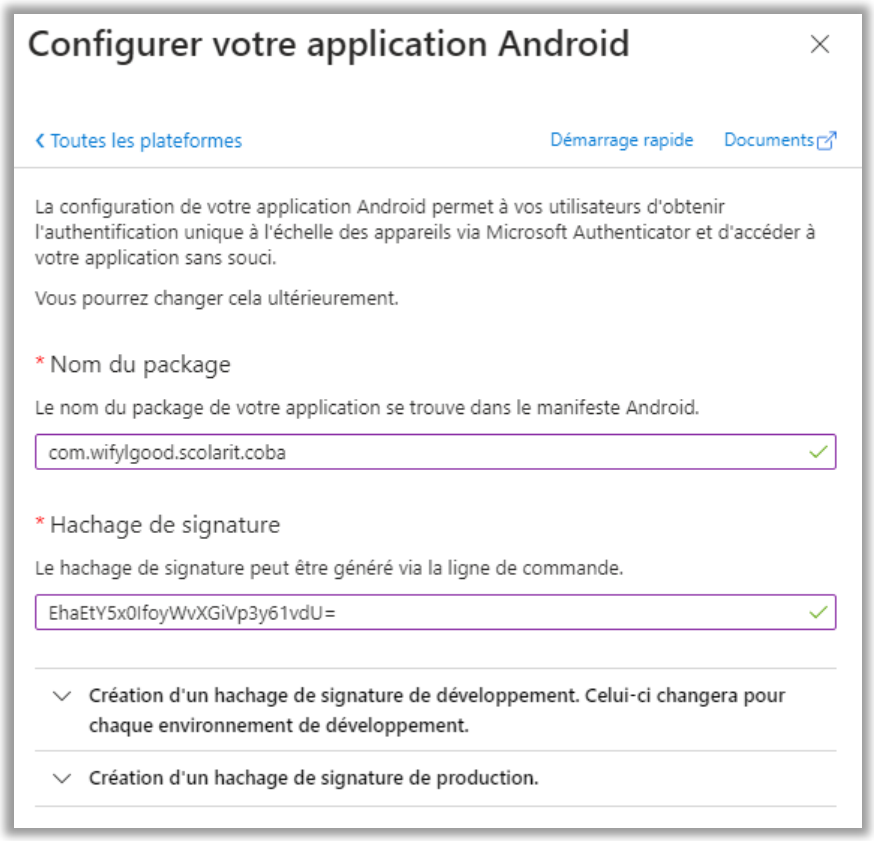
Si votre institution possède une version personnalisée de l'application COBA Campus sur les magasins Android et iOS, vous devez communiquer avec notre service à la clientèle, car les informations à saisir seront liées à votre application personnalisée.

Étape 5.8 - Accéder à l'option **Authentification** du menu de gauche et cliquer sur le lien **+ Ajouter une plateforme**.

Étape 5.9 – Sélectionner la plateforme **Android**.



Étape 5.10 – Compléter les champs ci-dessous, cliquer sur le bouton **Configurer** et cliquer sur le bouton **Terminé.**

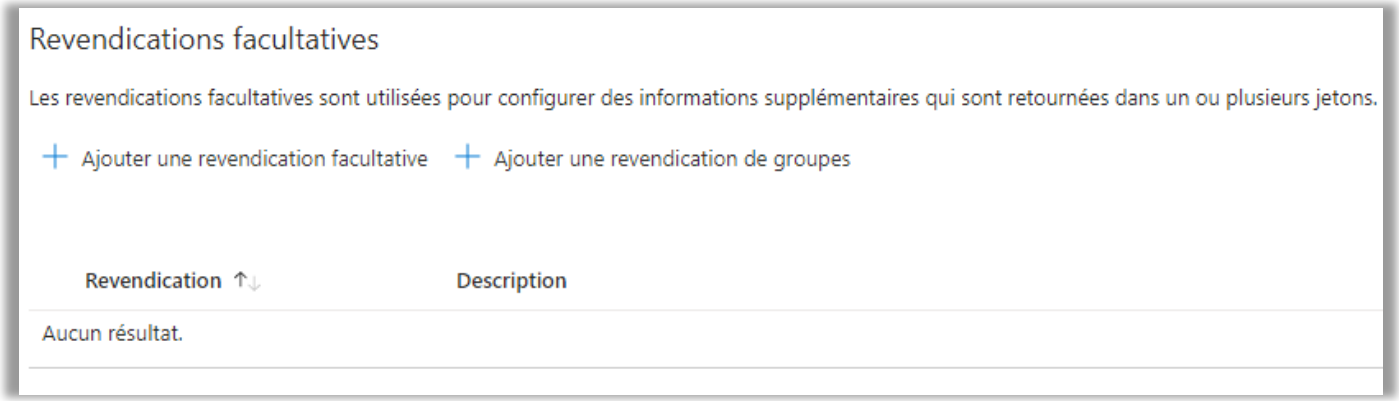


- **Nom du package**
  - com.wifylgood.scolarit.coba
- **Hachage de signature**
  - EhaEtY5x0IfoyWvXGiVp3y61vdU=
- **URI de redirection**
  - msauth://com.wifylgood.scolarit.coba/EhaEtY5x0IfoyWvXGiVp3y61vdU%3D

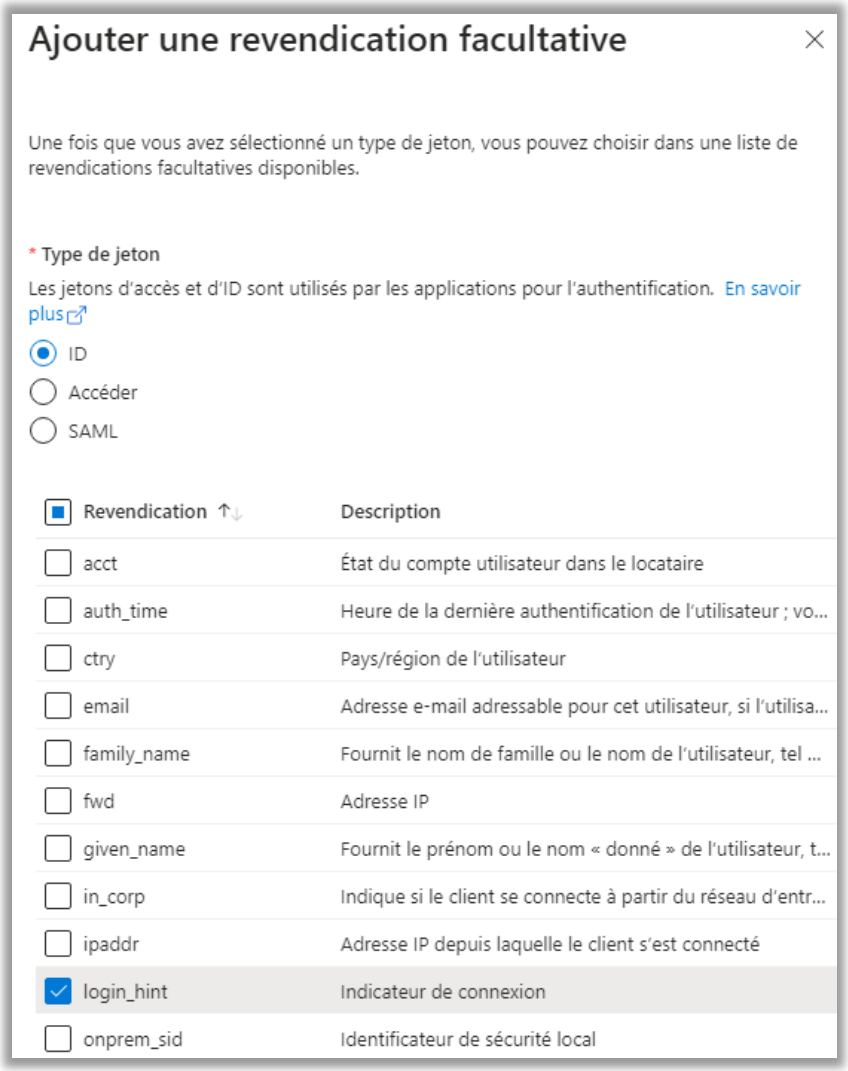
Note :

Si votre institution possède une version personnalisée de l'application COBA Campus sur les magasins Android et iOS, vous devez communiquer avec notre service à la clientèle, car les informations à saisir seront liées à votre application personnalisée.

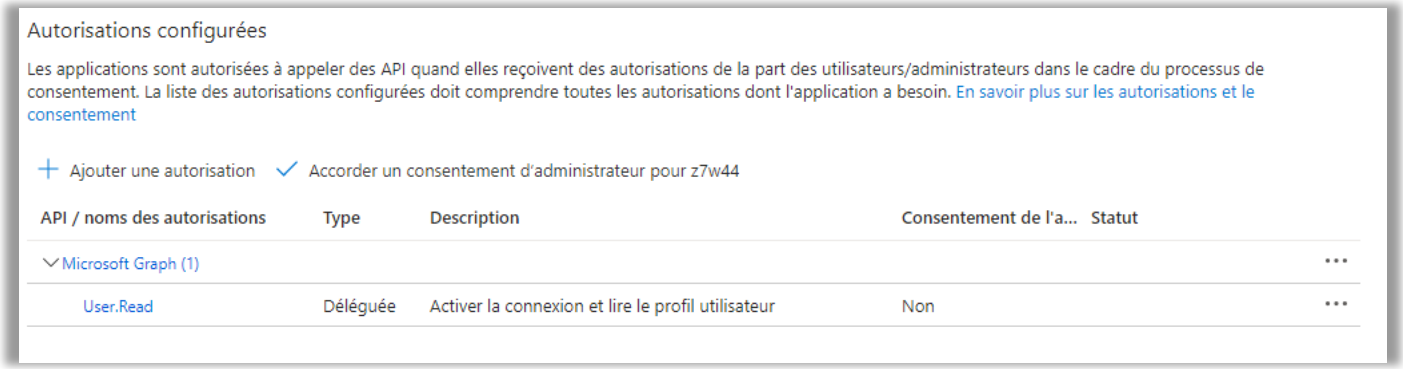
Étape 5.11 - Accéder à l'option **Configuration du jeton** du menu de gauche et cliquer sur le lien **+ Ajouter une revendications facultatives**.



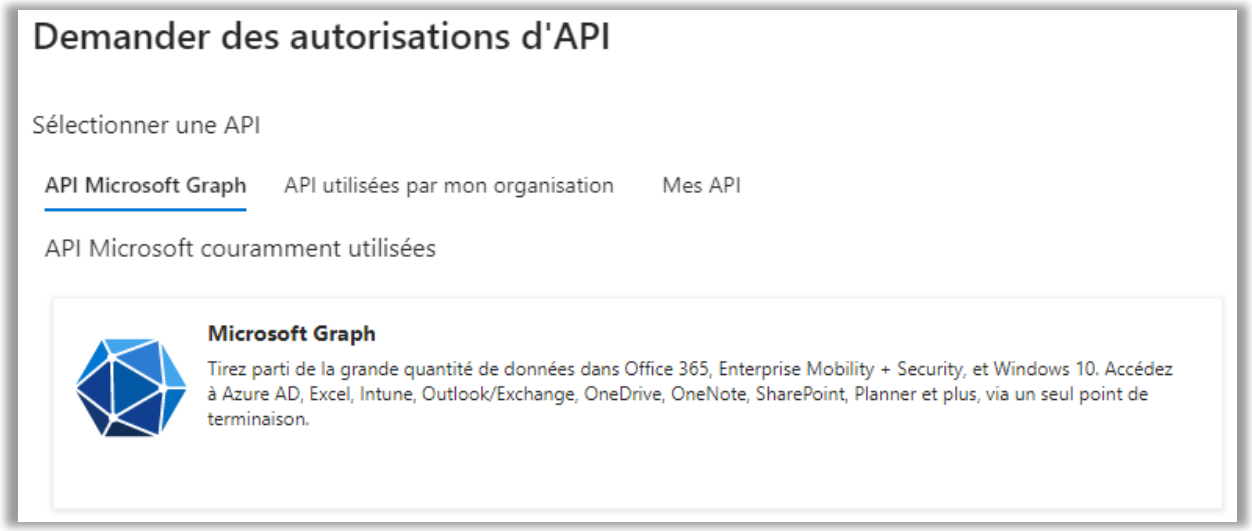
Étape 5.12 – Cocher le **Type de jeton** ID, cocher la **Revendication** login_hint et cliquer sur le bouton **Ajouter**.

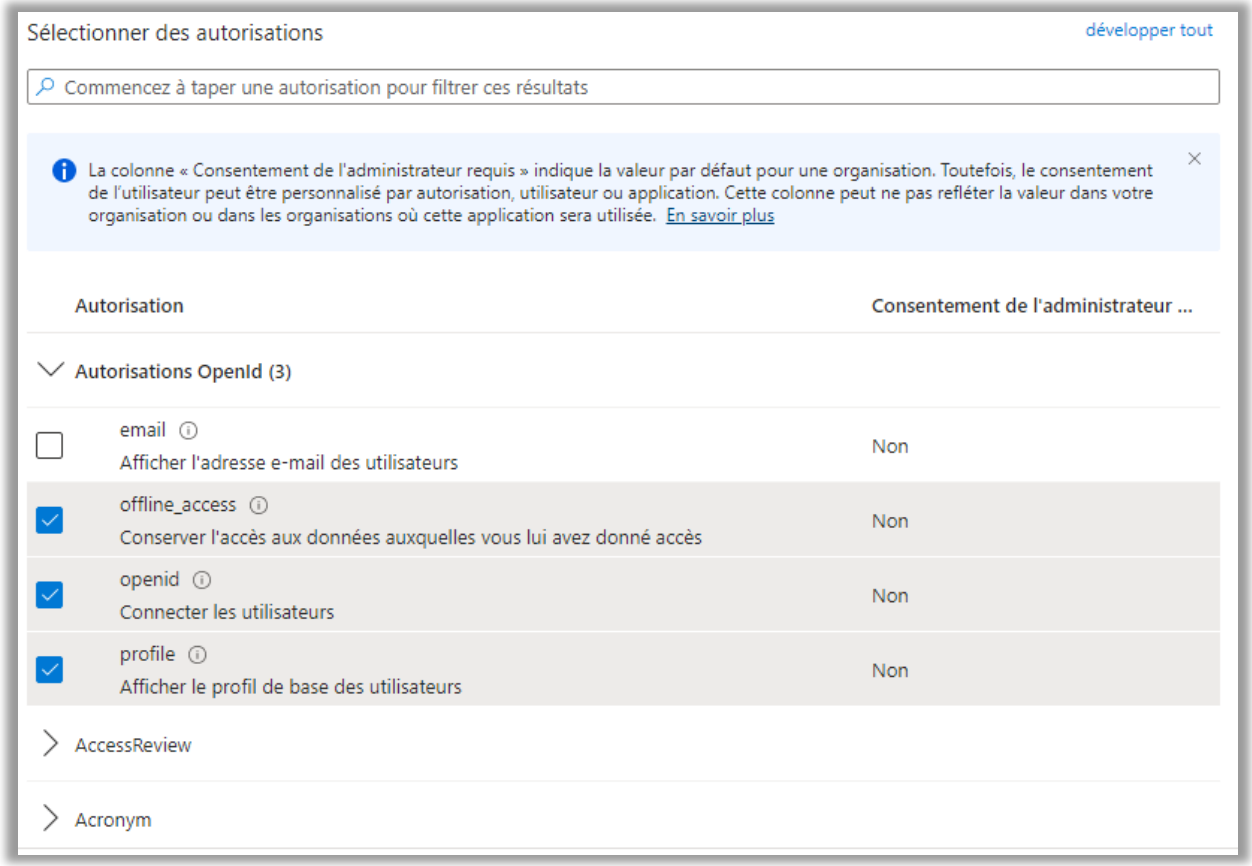


Étape 5.13 - Accéder à l'option **API autorisée** du menu de gauche et cliquer sur le lien **+ Ajouter une autorisation**.

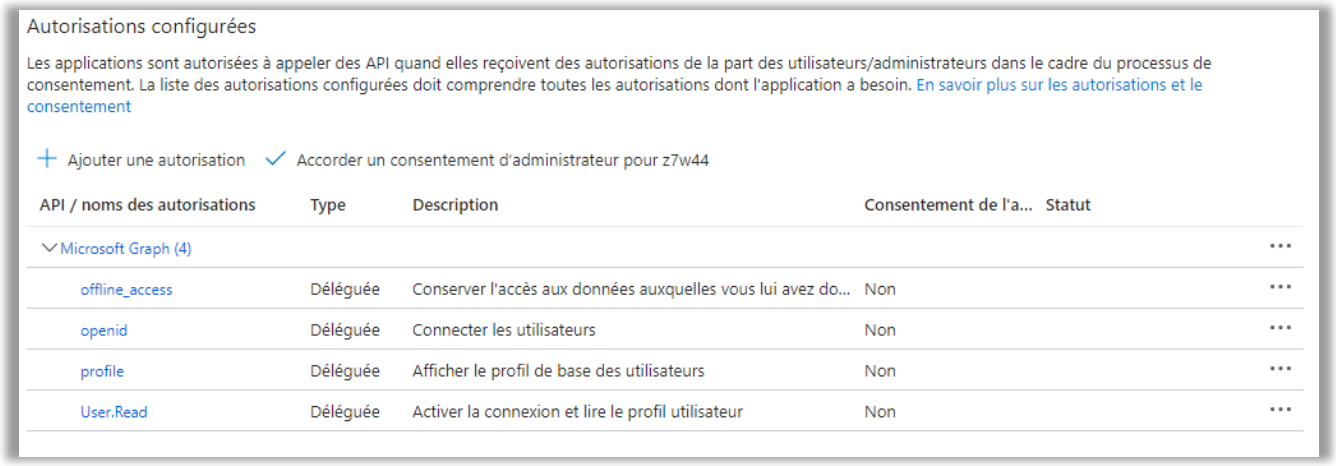


Étape 5.14 – Sélectionner **Microsoft Graph**, sélectionner **Autorisations déléguées**, cocher les autorisations **offline_access**, **openid** et **profile** et cliquer sur le bouton **Ajouter des autorisations**.

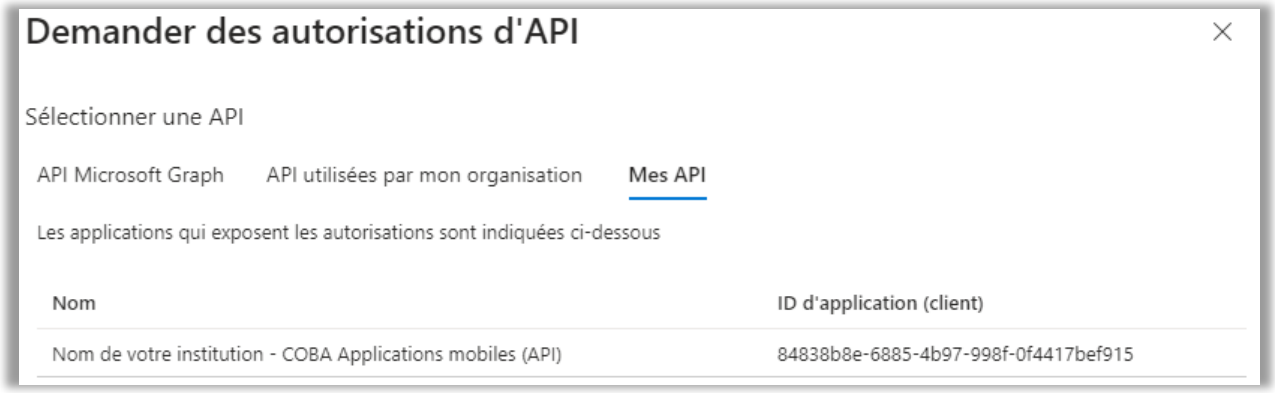




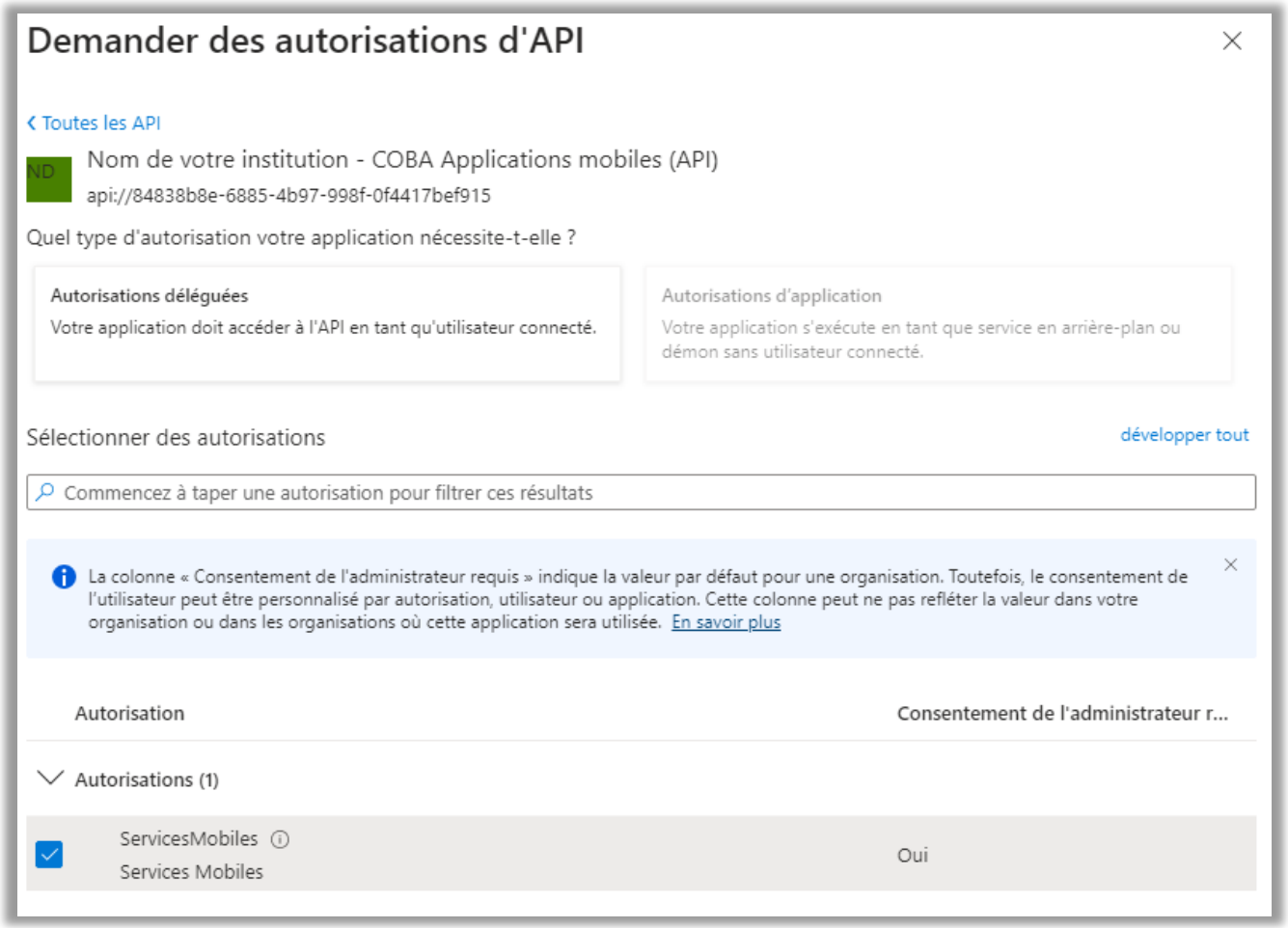
Étape 5.15 – Cliquer sur le lien **+ Ajouter une autorisation**.



Étape 5.16 – Sélectionner l'onglet **Mes API** et sélectionner le nom de l'application **COBA Application mobile (API).**

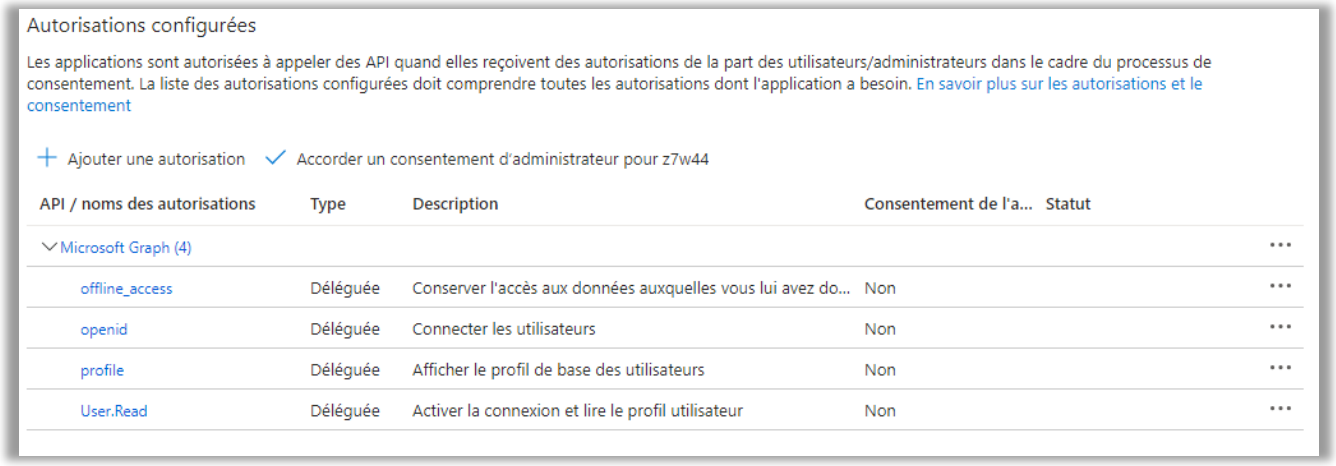


Étape 5.17 – Sélectionner **ServicesMobiles** et cliquer sur le bouton **Ajouter des autorisations**.

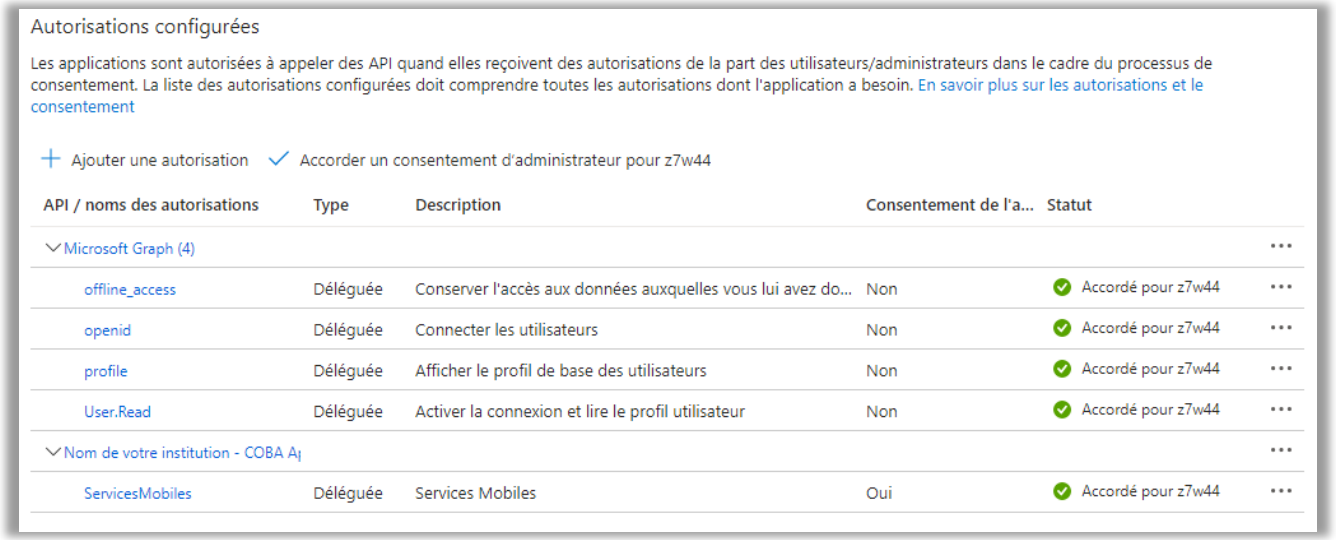


Étape 5.18 – Cliquer sur le lien **Accorder un consentement d'administrateur pour « votre domaine »** et confirmer.

Avant



Après



Configuration des logiciels de la gamme COBA

Authentification dans les applications administratives v6

L'activation de l'authentification avec un fournisseur d'authentification dans nos applications administratives V6 implique que **tous les utilisateurs** devront utiliser le fournisseur d'authentification pour s'authentifier dans le logiciel.

Configuration du fournisseur d'authentification

Accéder à l'onglet **Sécurité des comptes** à l'option **Système > Configuration** pour compléter l'encadré **Fournisseur d'authentification.**

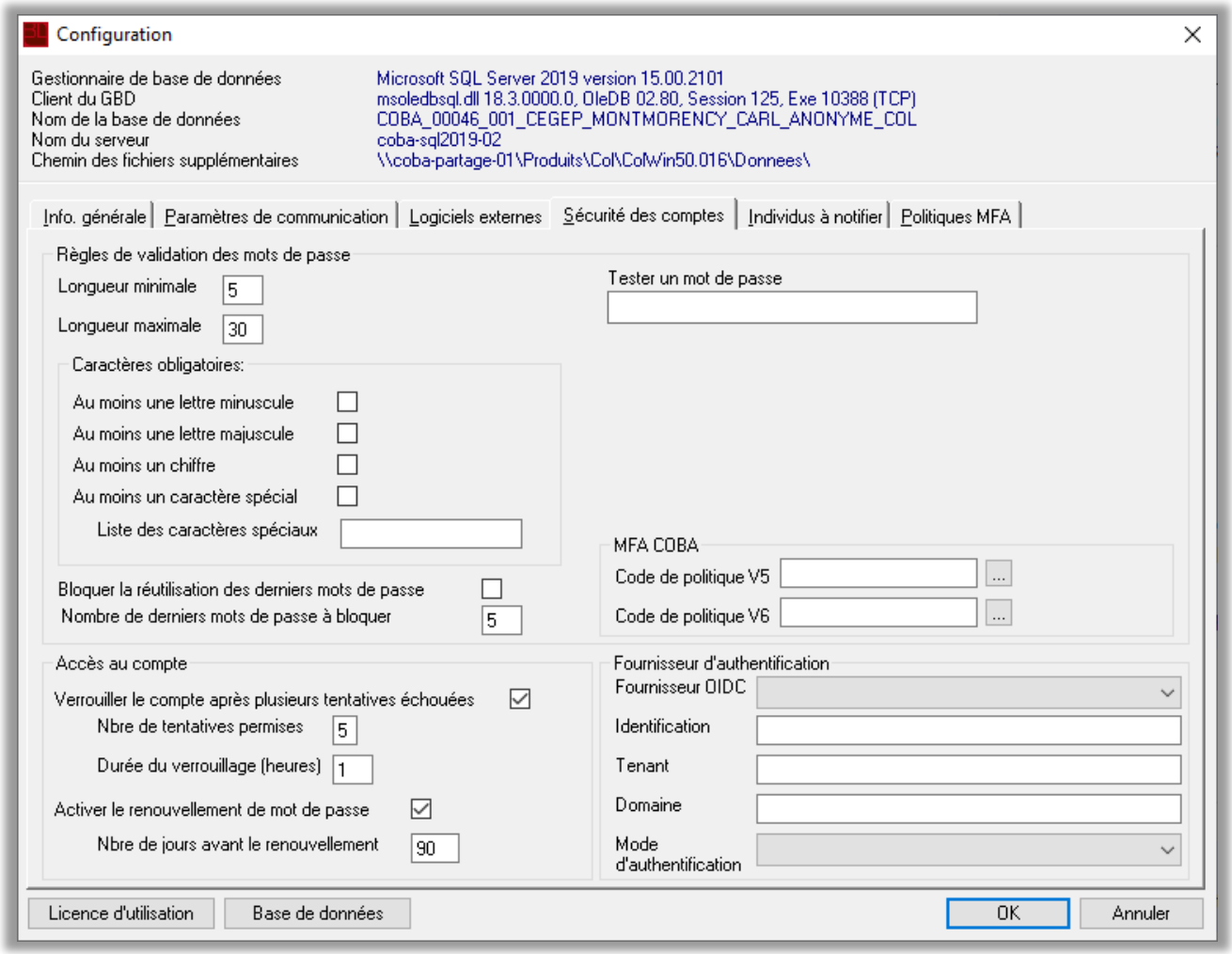


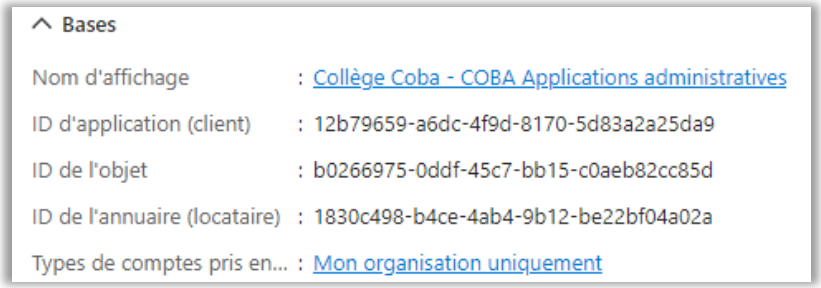
IMAGE À REFAIRE

Fournisseur OIDC

Sélectionnez la valeur **Azure AD.**

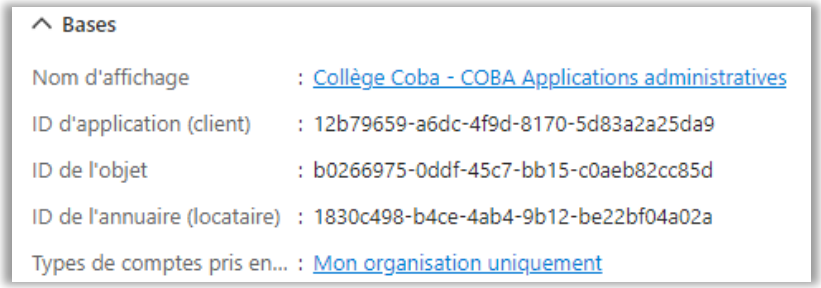
Identification

Copier la valeur du champ **ID d'application (client)** de l'application **« Nom de l'institution » - COBA Applications administratives** de votre portail Azure.



Tenant

Copier la valeur du champ **ID de l'annuaire (locataire)** de l'application **« Nom de l'institution » - COBA Applications administratives** de votre portail Azure.



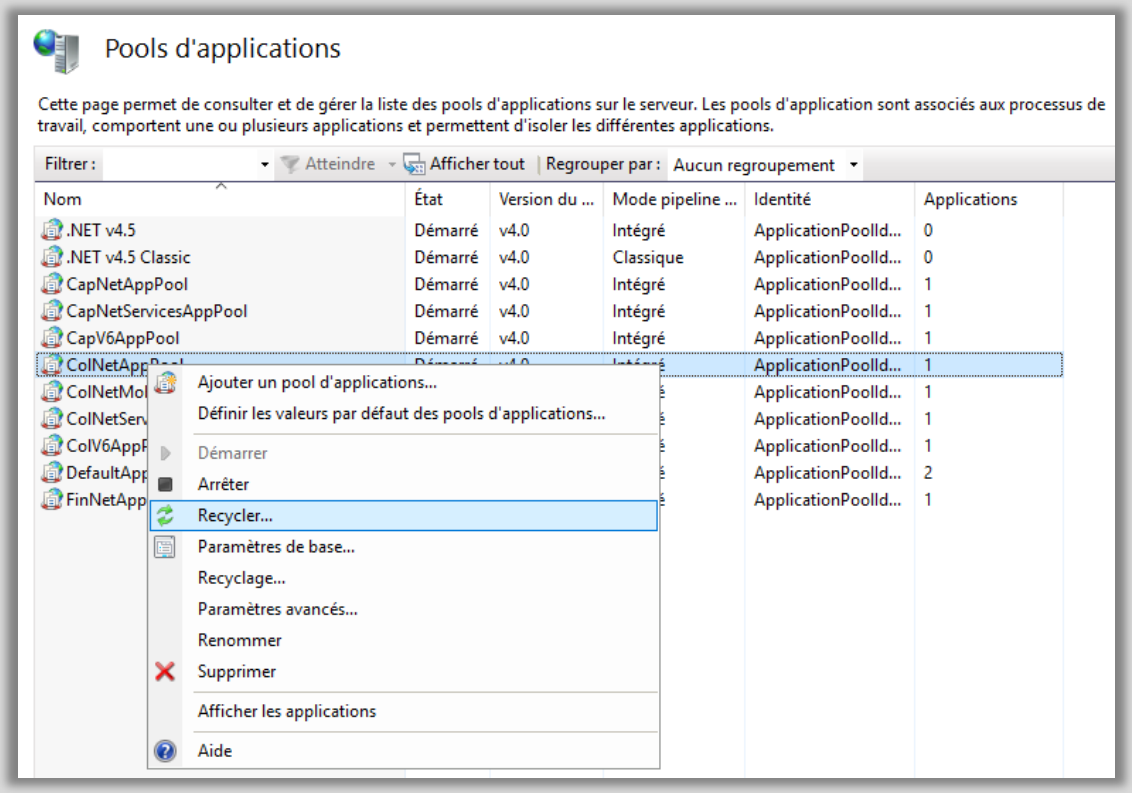
Domaine

Saisir le nom de votre domaine.

Note :

À la suite de la modifications des paramètres pour l'accès aux comptes pour une application administrative, l'application pool lié à l'application administrative doit être recyclé.

1. Se connecter sur le serveur du portail
2. Exécuter le Gestionnaire des services Internet (IIS)
3. Cliquer sur Pool d'applications
4. Cliquer sur le pool de l'application administrative avec le bouton de droit et le recycler.



NOTE :

Pour activer le bouton d'authentification Azure AD sur la l'application V6, vous devez ajouter la ligne suivante dans le fichier **ColV6\Config\Config.txt** sur le serveur où l'application V6 est installée.

ModeAuthentification=3

Après avoir modifié le fichier Config.txt, vous devez recycler le pool de l'application V6 dans IIS.

Configuration des utilisateurs administratifs

Afin qu'un logiciel administratif puisse effectuer l'authentification d'un utilisateur avec un fournisseur d'authentification, les champs Domaine AD et Code d'utilisateur AD doivent être complétés pour tous les utilisateurs actifs du logiciel administratif.

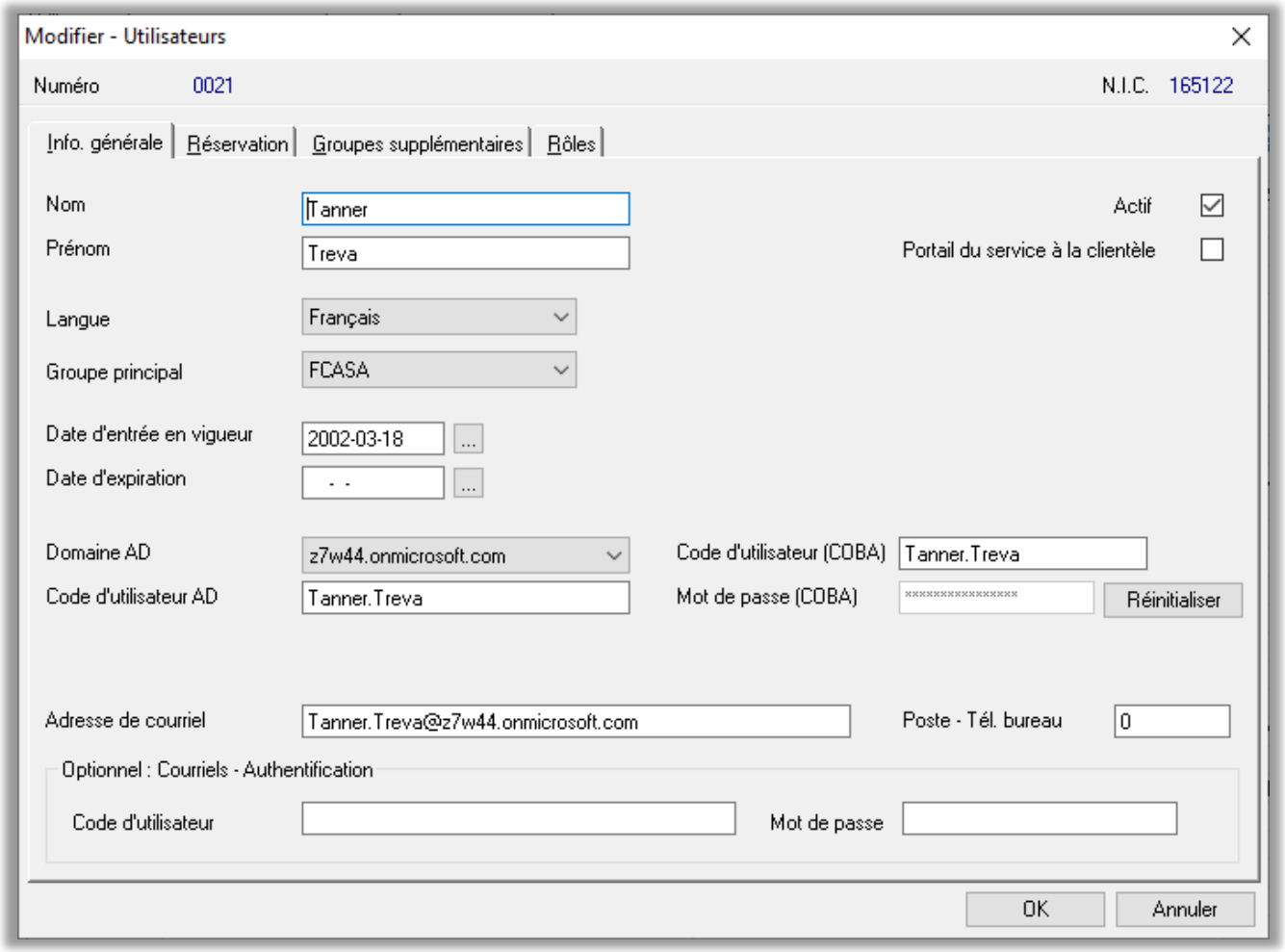


IMAGE À REFAIRE

Note :

Vous pouvez vous référer au guide **Activer le service de domaine Active Directory** pour effectuer cette étape si vous avez des utilisateurs qui ont actuellement plusieurs comptes d'utilisateur.

Accéder au bouton **Accès au compte** de l'option **Collégial > Utilitaires > Campus > Outils > Configuration du portail Internet > Paramètres de bases** pour compléter l'encadré **Fournisseur d'authentification.**

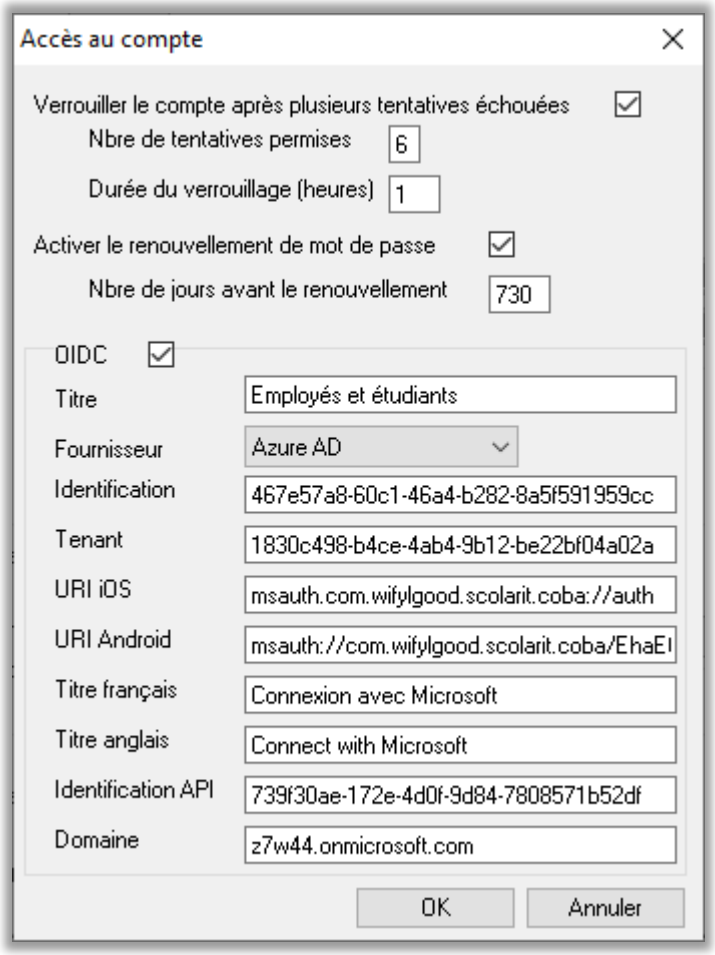


IMAGE À REFAIRE

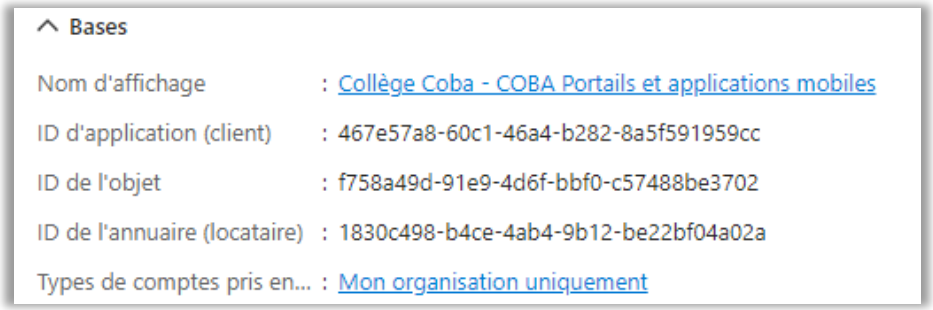
Saisir le titre du bouton à afficher pour la connexion avec Azure AD sur le portail et sur l'application mobile.

Fournisseur OIDC

Sélectionner la valeur **Azure AD.**

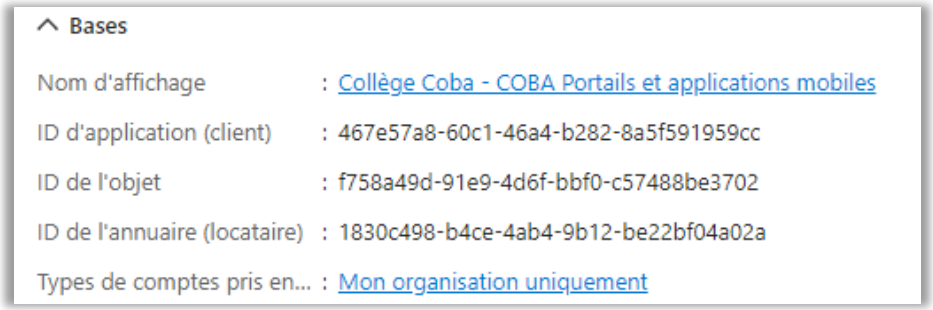
Identification

Copier la valeur du champ **ID d'application (client)** de l'application **« Nom de l'institution » - COBA portails et applications mobiles** de votre portail Azure.



Tenant

Copier la valeur du champ **ID de l'annuaire (locataire)** de l'application **« Nom de l'institution » - COBA portails et applications mobiles** de votre portail Azure.



URI iOS (visible seulement si votre institution a l'application mobile)

Saisir la valeur

msauth.com.wifylgood.scolarit.coba://auth

URI Android (visible seulement si votre institution a l'application mobile)

Saisir la valeur

msauth://com.wifylgood.scolarit.coba/EhaEtY5x0IfoyWvXGiVp3y61vdU%3D

Titre français

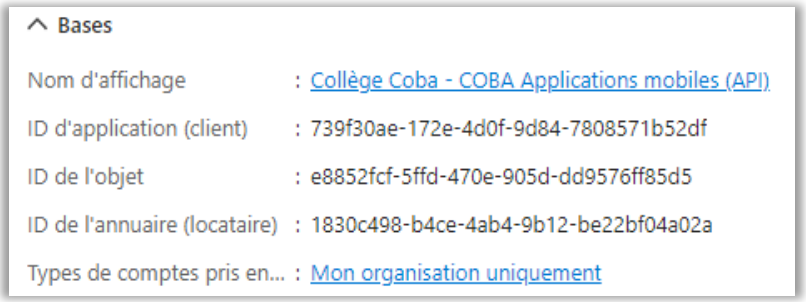
Saisir le titre du bouton à afficher pour la connexion en français avec le fournisseur d'authentification sur le portail et sur l'application mobile.

Titre anglais

Saisir le titre du bouton à afficher pour la connexion en anglais avec le fournisseur d'authentification sur le portail et sur l'application mobile.

Identification API

Copier la valeur du champ **ID d'application (client)** de l'application **« Nom de l'institution » - COBA Applications mobiles (API)** de votre portail Azure.



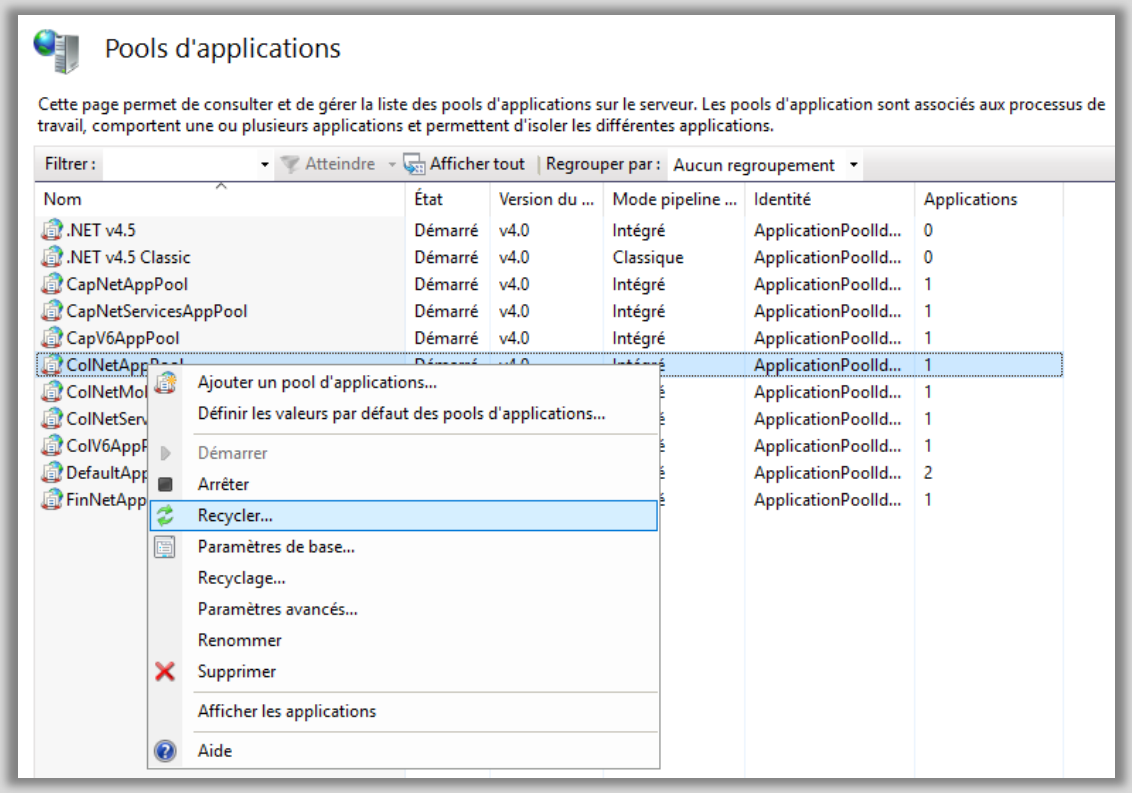
Domaine

Saisir le nom de votre domaine.

Note :

À la suite de la modifications des paramètres pour l'accès aux comptes pour un portail, l'application pool lié au portail doit être recyclé.

5. Se connecter sur le serveur du portail
6. Exécuter le Gestionnaire des services Internet (IIS)
7. Cliquer sur Pool d'applications
8. Cliquer sur le pool du portail avec le bouton de droit et le recycler.



Si une modification touche l'URI pour iOS ou l'URI pour Android, vous devez aussi recycler l'application pool lié à l'application mobile.

Configuration des utilisateurs du portail

Afin qu'un portail puisse effectuer l'authentification d'un utilisateur avec un fournisseur d'authentification, les champs Domaine AD et Code d'utilisateur AD doivent être complétés pour tous les utilisateurs actifs du portail.

Note :

Vous pouvez vous référer au guide **Activer le service de domaine Active Directory** pour effectuer cette étape dans le dossier des utilisateurs des portails.

Règles de validation

Par défaut notre authentification avec Azure AD délègue tout le contrôle des règles de validations à Azure AD selon la configuration de celui-ci.

Pour les institutions désirant appliquer une configuration différente, les logiciels de la gamme COBA permettent d'appliquer des règles, peu importe la configuration du Azure AD.

- Une configuration permet de forcer l'utilisateur à se réauthentifier dans Azure AD à chacune de ses connexions dans nos applications.
    - Lorsque cette configuration est activée, une connexion d'une application COBA déconnecte aussi l'utilisateur de son compte Office 265.

- Une configuration permet d'afficher la liste des utilisateurs AD existants sur le poste de travail à chacune de ses connexions dans nos applications.
    - Cette configuration permet de basculer d'un utilisateur à un autre lorsqu'un poste de travail est utilisé par plusieurs personnes.

Pares-feux

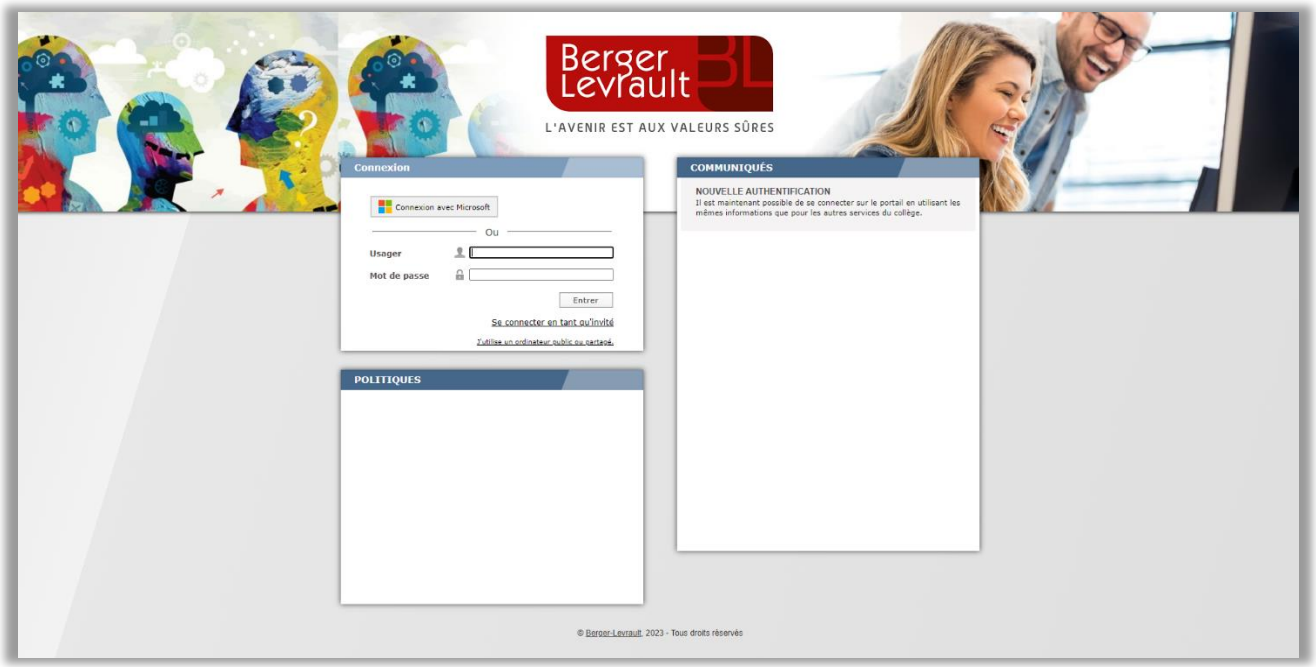
Les URI suivants doivent être accessible à partir du serveur des portails et des applications administratives V6 :

- https://onmicrosoft.com
- https://login.microsoftonline.com/

Exemple d'utilisation de l'authentification

Portails

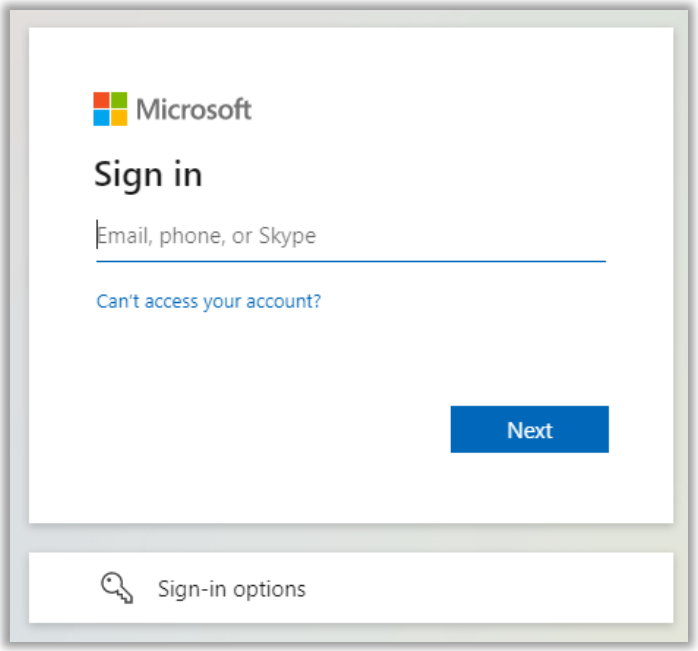
À la suite de la configuration d'un fournisseur d'authentification pour le portail, les utilisateurs seront invités à se connecter dans le portail avec l'aide de l'authentification avec le fournisseur d'authentification Azure AD ou avec l'aide de l'authentification traditionnelle de COBA.

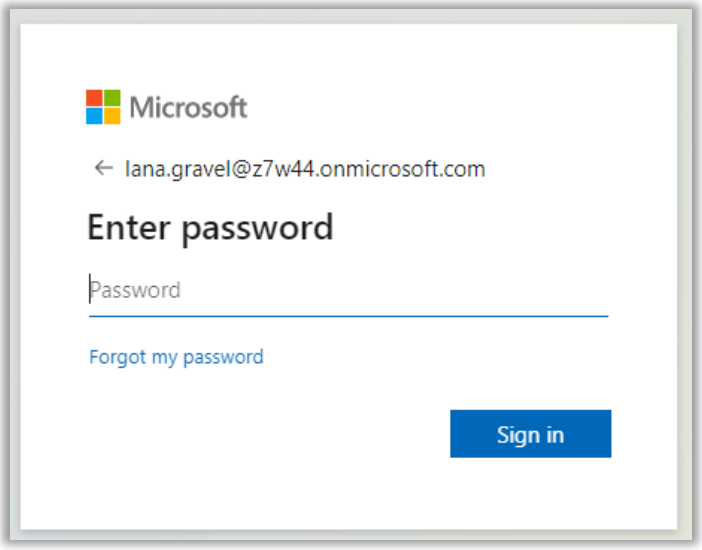


Note : Le libellé sur le bouton de connexion avec le fournisseur d'authentification Azure AD provient de la configuration dans les paramètres du portail.

Si la configuration de l'authentification Azure AD de votre institution exige une authentification avec du MFA, celui-ci sera automatiquement intégré dans l'authentification sur nos portails.

Voici un exemple de la séquence des opérations pour un utilisateur de l'application mobile qui s'authentifie avec le fournisseur d'authentification Azure AD.

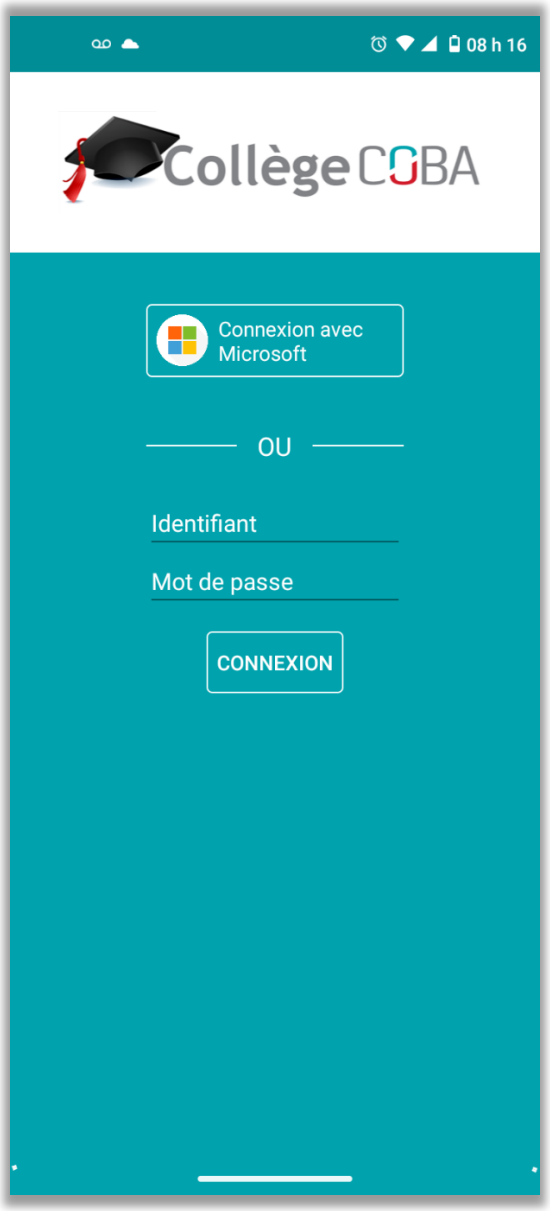




Lien ColNET => PaieNET ???

Applications mobiles

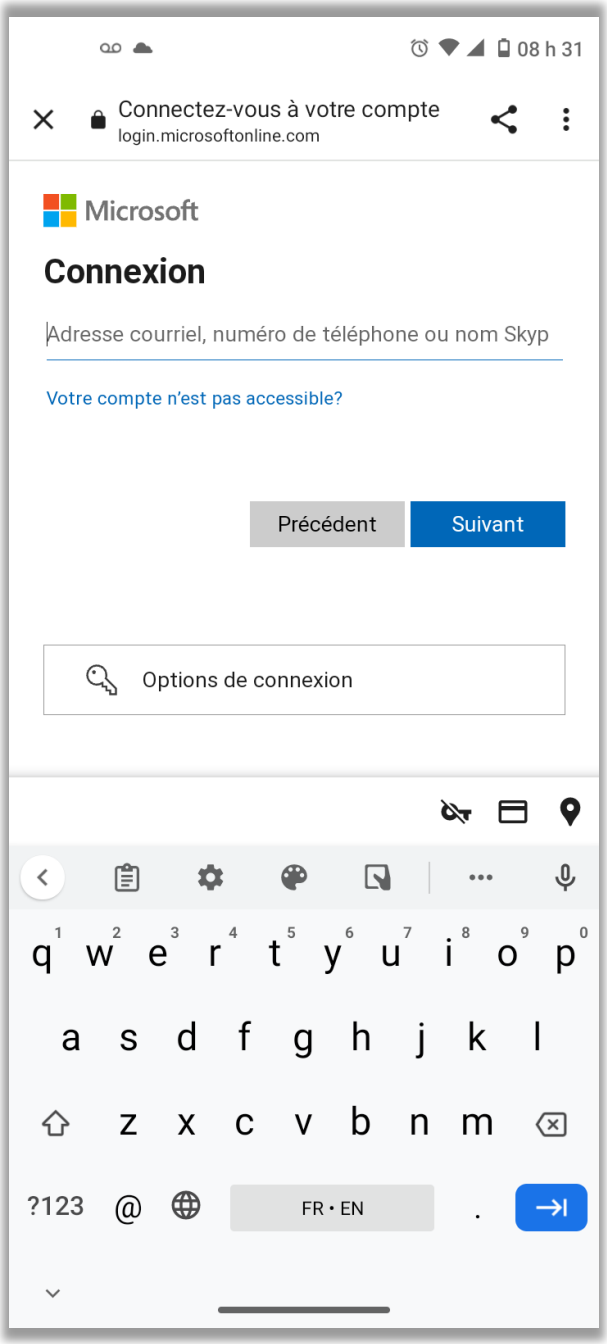
À la suite de la configuration d'un fournisseur d'authentification pour le portail, les utilisateurs seront invités à se connecter dans l'application mobile avec l'aide de l'authentification avec le fournisseur d'authentification Azure AD ou avec l'aide de l'authentification traditionnelle de COBA.

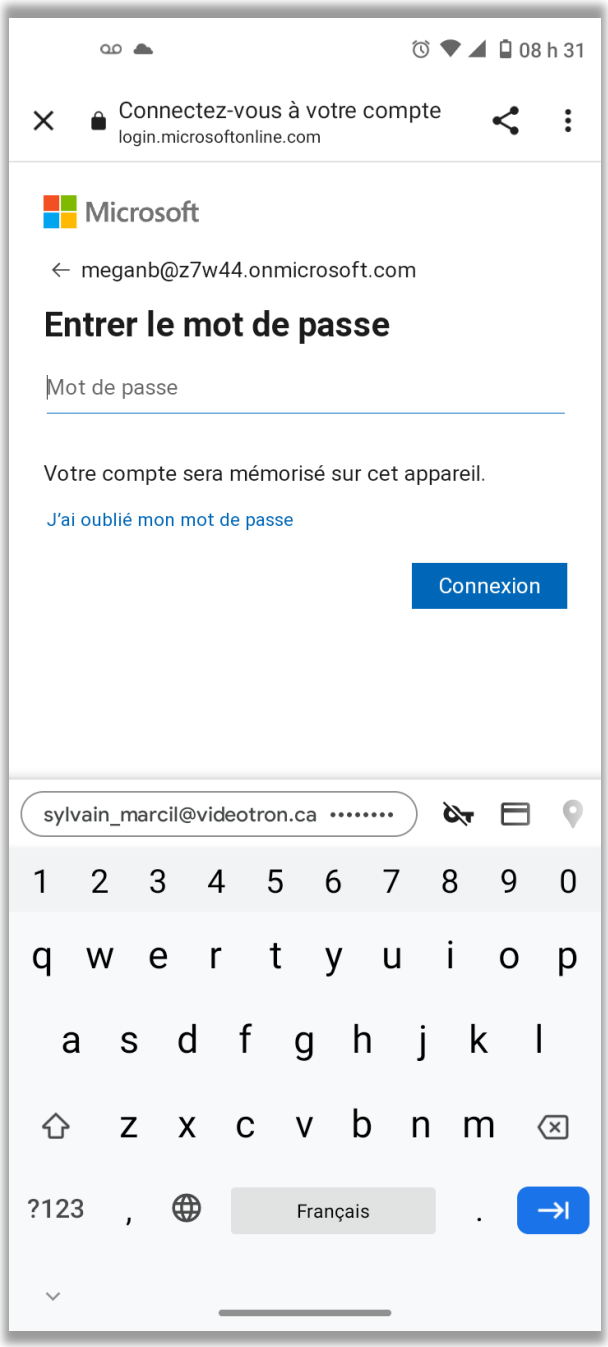


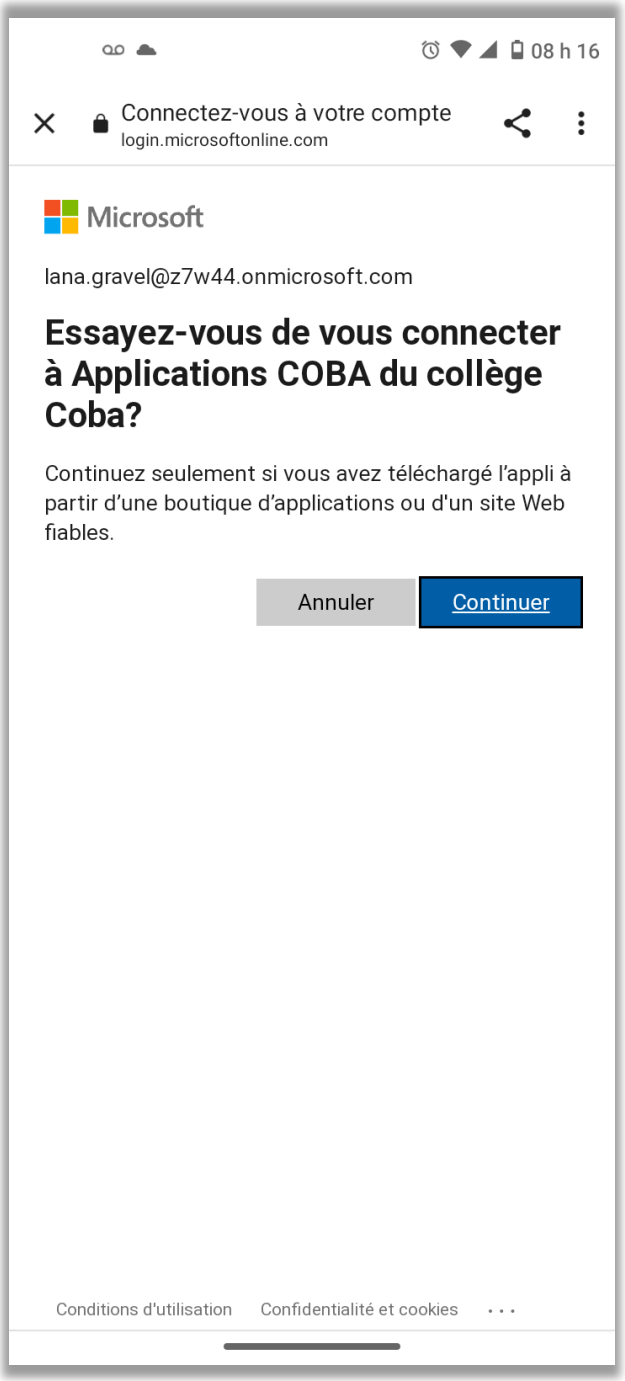
Note : Le libellé sur le bouton de connexion avec le fournisseur d'authentification Azure AD provient de la configuration dans les paramètres du portail.

Si la configuration de l'authentification Azure AD de votre institution exige une authentification avec du MFA, celui-ci sera automatiquement intégré dans l'authentification sur nos applications mobiles.

Voici un exemple de la séquence des opérations pour un utilisateur de l'application mobile qui s'authentifie avec le fournisseur d'authentification Azure AD.

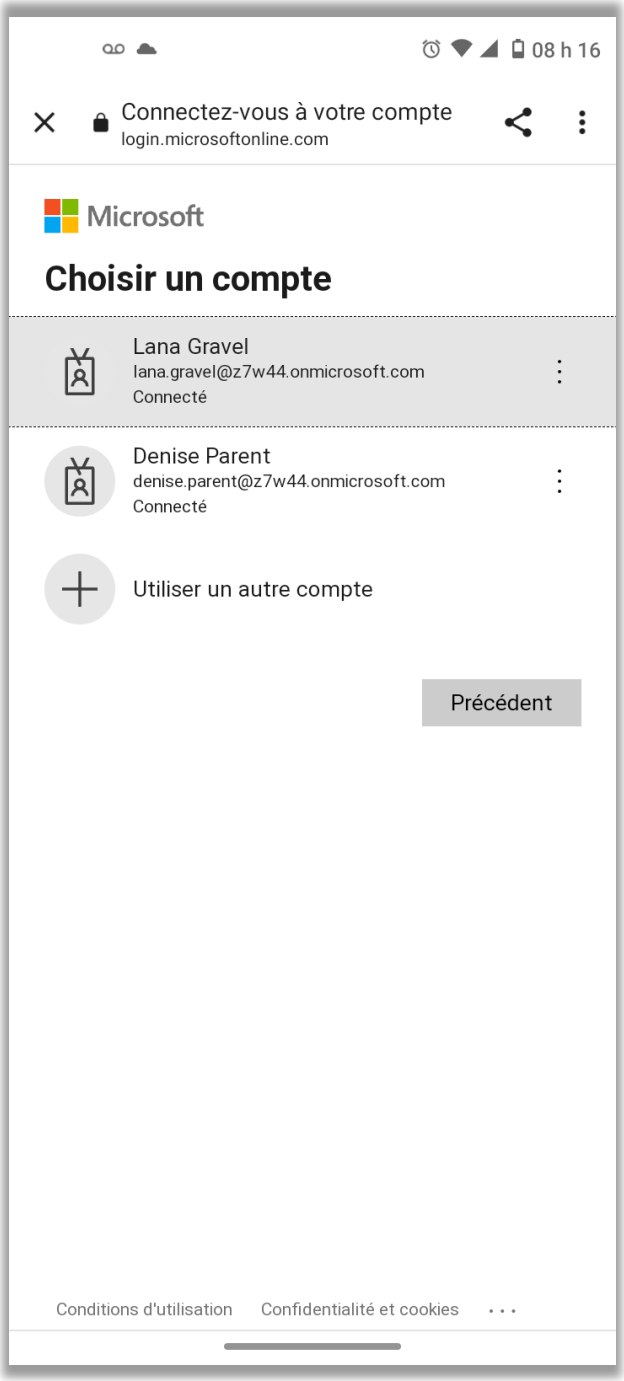






Note : La description de l'application auquel l'utilisateur tente de se connecter provient de la configuration de l'application dans la configuration de Azure AD.

Dans la situation où l'utilisateur utilise déjà plusieurs comptes sur son appareil mobile, celui-ci sera invité à utiliser un compte déjà existant.



Lien Application mobile => PaieNET ???

Applications administratives V6

À la suite de la configuration d'un fournisseur d'authentification pour l'application administrative v6, les utilisateurs seront invités à se connecter dans l'application administrative v6 avec l'aide de l'authentification avec le fournisseur d'authentification Azure AD.

Note : Si la configuration de l'authentification Azure AD de votre institution exige une authentification avec du MFA, celui-ci sera automatiquement intégré dans l'authentification sur nos applications administratives.

Voici un exemple de la séquence des opérations pour un utilisateur de l'application administration V6 qui s'authentifie avec le fournisseur d'authentification Azure AD.