

Authentification avec Azure AD

Juin 2023

Résumé du document

Résumé

Version du 5 juin 2023

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.

Ce document est confidentiel. Il ne peut être copié ou distribué sans l'autorisation de Berger-Levrault Canada Itée

berger-levrault.com

Table des matières

Introduction.....	1
Définition un fournisseur d'authentification	2
Azure AD	2
Étape 1 – Accéder au portail Azure	2
Étape 2 – Accéder aux inscriptions d'applications	2
Étape 3 – Créer une nouvelle inscription pour le logiciel administratif V6.....	4
Étape 4 – Créer une nouvelle inscription pour l'API de l'application mobile	12
Étape 5 – Créer une nouvelle inscription pour portail et application mobile.....	15
Configuration des logiciels de la gamme COBA	30
Authentification dans les applications administratives v6	30
Configuration du fournisseur d'authentification	30
Configuration des utilisateurs administratifs	33
Authentification sur les portails et les applications mobiles	34
Configuration du fournisseur d'authentification	34
Configuration des utilisateurs du portail.....	38
Règles de validation	39
Résolution de problèmes.....	40
Pares-feux.....	40
Exemple d'utilisation de l'authentification	41
Portails	41
Applications mobiles.....	43
Applications administratives V6	47

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 collègues 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**.

Bienvenue dans Azure !

Vous n'avez pas d'abonnement ? Consultez les options suivantes.



Commencer par un essai gratuit d'Azure
Obtenez 200 USD de crédit gratuit sur les produits et services Azure, plus 12 mois de [services gratuits](#) populaires.
[Démarrer](#)



Gérer Azure Active Directory
Gérez l'accès, définissez des stratégies intelligentes et améliorez la sécurité avec Azure Active Directory.
[Vue](#) [En savoir plus](#)

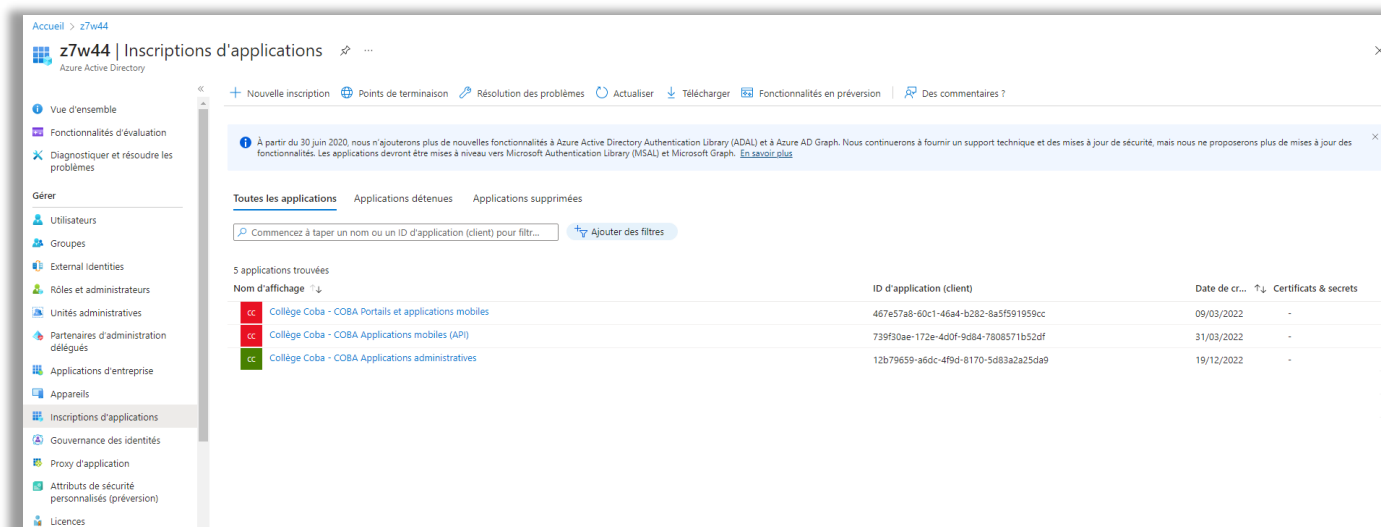


Accéder aux avantages des étudiants
Bénéficiez de logiciels gratuits, de crédit Azure ou d'un accès à Azure Dev Tools for Teaching après avoir vérifié votre statut scolaire.
[Explorer](#) [En savoir plus](#)

Services Azure

[Créer une ressource](#)
[Application de fonction](#)
[Centre de démarrage...](#)
[Machines virtuelles](#)
[App Services](#)
[Comptes de stockage](#)
[Bases de données SQL](#)
[Azure Cosmos DB](#)
[services Kubernetes](#)
[Autres services](#)

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



Accueil > z7w44

z7w44 | Inscriptions d'applications

+ Nouvelle inscription | Points de terminaison | Résolution des problèmes | Actualiser | Télécharger | Fonctionnalités en préversion | Des commentaires ?

À partir du 30 juin 2020, nous n'ajouterons plus de nouvelles fonctionnalités à Azure Active Directory Authentication Library (ADAL) et à Azure AD Graph. Nous continuerons à fournir un support technique et des mises à jour de sécurité, mais nous ne proposerons plus de mises à jour des fonctionnalités. Les applications devront être mises à niveau vers Microsoft Authentication Library (MSAL) et Microsoft Graph. [En savoir plus](#)

Toutes les applications | Applications détenues | Applications supprimées

Commencez à taper un nom ou un ID d'application (client) pour filtrer... | Ajouter des filtres

5 applications trouvées

Nom d'affichage	ID d'application (client)	Date de cr...	Certificats & secrets
Collège Cobra - COBA Portails et applications mobiles	467e57a8-60c1-46a4-b282-8a5f591959cc	09/03/2022	-
Collège Cobra - COBA Applications mobiles (API)	739f30ae-172e-4d0f-9d84-7808571b52df	31/03/2022	-
Collège Cobra - COBA Applications administratives	12b79659-a6dc-4f9d-8170-5d83a2a25da9	19/12/2022	-

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.

Accueil > z7w44 | Inscriptions d'applications >

Inscrire une application ...

*** Nom**

Nom d'affichage côté utilisateur pour cette application (il peut être modifié ultérieurement).

« Nom de l'institution » - COBA Applications administratives ✓

Types de comptes pris en charge

Qui peut utiliser cette application ou accéder à cette API ?

☒ Comptes dans cet annuaire d'organisation uniquement (z7w44 uniquement - Locataire unique)

☐ Comptes dans un annuaire d'organisation (tout annuaire Azure AD - Multilocataire)

☐ Comptes dans un annuaire d'organisation (tout annuaire Azure AD - Multilocataire) et comptes Microsoft personnels (par exemple, Skype, Xbox)

☐ Comptes Microsoft personnels uniquement

[Aidez-moi à choisir...](#)

URI de redirection (facultatif)

Nous retournerons la réponse d'authentification à cet URI une fois l'utilisateur authentifié. Fournir ceci maintenant est facultatif et cela peut être modifié ultérieurement, mais une valeur est requise pour la plupart des scénarios d'authentification.

Sélectionner une plateforme ▼ par ex., https://example.com/auth

- **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**.

Configurations de plateforme

Selon la plateforme ou l'appareil ciblé(e) par cette application, une configuration supplémentaire peut être nécessaire, par exemple, les paramètres d'authentification spécifiques, les URI de redirection ou les champs spécifiques à la plateforme.

[+ Ajouter une plateforme](#)

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

Configurer des plateformes

Applications web



Web

Générez, hébergez et déployez une application de serveur web. .NET, Java, Python



Application à page unique

Configurez des applications clientes de navigateur et des applications web progressives. Javascript.

Applications de bureau et mobiles



iOS / macOS

Objective-C, Swift, Xamarin



Android

Java, Kotlin, Xamarin



Applications de bureau et mobiles

Windows, UWP, Console, IoT & appareils à entrée limitée, iOS classique + Android

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

Configurer web

[← Toutes les plateformes](#)
[Démarrage rapide](#)
[Documents](#)

*** URI de redirection**

Les URI que nous accepterons comme destinations lors du retour des réponses d'authentification (jetons) après l'authentification ou la déconnexion des utilisateurs. L'URI de redirection que vous envoyez dans la demande au serveur de connexion doit correspondre à celui répertorié ici. Également appelées URL de réponse. [En savoir plus sur les URI de redirection et leurs restrictions](#)

URL de déconnexion du canal avant

Il s'agit de l'emplacement où nous envoyons une requête pour que l'application efface les données de session de l'utilisateur. Ceci est obligatoire pour que la déconnexion unique fonctionne correctement.

Octroi implicite et flux hybrides

Demandez un jeton directement à partir du point de terminaison d'autorisation. Si l'application a une architecture à page unique (SPA) et n'utilise pas le flux du code d'autorisation, ou si elle appelle une API web via JavaScript, sélectionnez les jetons d'accès et les jetons d'ID. Pour les applications web ASP.NET Core et d'autres applications web qui utilisent l'authentification hybride, sélectionnez uniquement les jetons d'ID. [En savoir plus sur les jetons.](#)

Sélectionnez les jetons que vous souhaitez voir émis par le point de terminaison d'autorisation :

☐ Jetons d'accès (utilisés pour les flux implicites)
 ☐ Jetons d'ID (utilisés pour les flux implicites et hybrides)

- **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.

^ Web
Démarrage rapide
Documents

URI de redirection

Les URI que nous accepterons comme destinations lors du retour des réponses d'authentification (jetons) après l'authentification ou la déconnexion des utilisateurs. L'URI de redirection que vous envoyez dans la demande au serveur de connexion doit correspondre à celui répertorié ici. Également appelées URL de réponse. [En savoir plus sur les URI de redirection et leurs restrictions](#)

Ajouter un URI

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

Revendications facultatives

Les revendications facultatives sont utilisées pour configurer des informations supplémentaires qui sont retournées dans un ou plusieurs jetons. [En savoir plus](#)

[+ Ajouter une revendication facultative](#)
[+ Ajouter une revendication de groupes](#)

Revendication ↑↓	Description
Aucun résultat.	

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

Ajouter une revendication facultative

Une fois que vous avez sélectionné un type de jeton, vous pouvez choisir dans une liste de revendications facultatives disponibles.

*** Type de jeton**
 Les jetons d'accès et d'ID sont utilisés par les applications pour l'authentification. [En savoir plus](#)

☒ ID
☐ Accéder
☐ SAML

☒ Revendication ↑↓	Description
☐ acct	État du compte utilisateur dans le locataire
☐ auth_time	Heure de la dernière authentification de l'utilisateur ; vo...
☐ cty	Pays/région de l'utilisateur
☐ email	Adresse e-mail adressable pour cet utilisateur, si l'utilisa...
☐ family_name	Fournit le nom de famille ou le nom de l'utilisateur, tel ...
☐ fwd	Adresse IP
☐ given_name	Fournit le prénom ou le nom « donné » de l'utilisateur, t...
☐ in_corp	Indique si le client se connecte à partir du réseau d'entr...
☐ ipaddr	Adresse IP depuis laquelle le client s'est connecté
☒ login_hint	Indicateur de connexion
☐ onprem_sid	Identificateur de sécurité local

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

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

[+ Ajouter une autorisation](#) [✓ Accorder un consentement d'administrateur pour z7w44](#)

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
▼ Microsoft Graph (1) ...				
User.Read	Délégée	Activer la connexion et lire le profil utilisateur	Non	...

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

Demander des autorisations d'API

Sélectionner une API

API Microsoft Graph API utilisées par mon organisation Mes API

API Microsoft couramment utilisées



Microsoft Graph

Tirez parti de la grande quantité de données dans Office 365, Enterprise Mobility + Security, et Windows 10. Accédez à Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner et plus, via un seul point de terminaison.

Sélectionner des autorisations

développer tout

Commencez à taper une autorisation pour filtrer ces résultats

i La colonne « Consentement de l'administrateur requis » indique la valeur par défaut pour une organisation. Toutefois, le consentement de l'utilisateur peut être personnalisé par autorisation, utilisateur ou application. Cette colonne peut ne pas refléter la valeur dans votre organisation ou dans les organisations où cette application sera utilisée. [En savoir plus](#)

Autorisation	Consentement de l'administrateur requis
✓ Autorisations OpenId (2)	
☐ email ⓘ Afficher l'adresse e-mail des utilisateurs	Non
☐ offline_access ⓘ Conserver l'accès aux données auxquelles vous lui avez donné accès	Non
☒ openid ⓘ Connecter les utilisateurs	Non
☒ profile ⓘ Afficher le profil de base des utilisateurs	Non
> AccessReview	
> Acronym	

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

Avant

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

+ Ajouter une autorisation ✓ Accorder un consentement d'administrateur pour z7w44

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
▼ Microsoft Graph (3)				...
openid	Délégée	Connecter les utilisateurs	Non	...
profile	Délégée	Afficher le profil de base des utilisateurs	Non	...
User.Read	Délégée	Activer la connexion et lire le profil utilisateur	Non	...

Après

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

+ Ajouter une autorisation ✓ Accorder un consentement d'administrateur pour z7w44

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
▼ Microsoft Graph (3)				...
openid	Délégée	Connecter les utilisateurs	Non	✓ Accordé pour z7w44 ...
profile	Délégée	Afficher le profil de base des utilisateurs	Non	✓ Accordé pour z7w44 ...
User.Read	Délégée	Activer la connexion et lire le profil utilisateur	Non	✓ Accordé pour z7w44 ...

Étape 4 – Créer une nouvelle inscription pour l'API de l'application mobile

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

Accueil > z7w44 | Inscriptions d'applications >

Inscrire une application ...

*** Nom**

Nom d'affichage côté utilisateur pour cette application (il peut être modifié ultérieurement).

Nom de votre institution - COBA Applications mobiles (API) ✓

Types de comptes pris en charge

Qui peut utiliser cette application ou accéder à cette API ?

☒ Comptes dans cet annuaire d'organisation uniquement (z7w44 uniquement - Locataire unique)

☐ Comptes dans un annuaire d'organisation (tout annuaire Azure AD - Multilocataire)

☐ Comptes dans un annuaire d'organisation (tout annuaire Azure AD - Multilocataire) et comptes Microsoft personnels (par exemple, Skype, Xbox)

☐ Comptes Microsoft personnels uniquement

[Aidez-moi à choisir...](#)

URI de redirection (facultatif)

Nous retournerons la réponse d'authentification à cet URI une fois l'utilisateur authentifié. Fournir ceci maintenant est facultatif et cela peut être modifié ultérieurement, mais une valeur est requise pour la plupart des scénarios d'authentification.

Sélectionner une plateforme ▼ par ex., https://example.com/auth

- **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**.

Étendues définies par cette API

Définissez des étendues personnalisées pour restreindre l'accès aux données et aux fonctionnalités protégées par l'API. Une application qui demande l'accès aux parties de cette API peut demander qu'un utilisateur ou un administrateur donne son consentement pour un ou plusieurs de ces éléments.

L'ajout d'une étendue ici crée uniquement des autorisations déléguées. Si vous voulez créer des étendues d'application uniquement, utilisez 'Rôles d'application' et définissez des rôles d'application pouvant être assignés à un type d'application. [Accédez aux rôles d'application.](#)

[+](#) Ajouter une étendue

Étendues	Qui peut donner so...	Nom d'affichage du co...	Nom d'affichage du co...	État
Aucune étendue définie				

Ajouter une étendue



Vous devrez définir un URI ID d'application avant de pouvoir ajouter une autorisation. Nous en avons choisi un, mais vous pouvez le modifier.

URI ID d'application * ⓘ

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**.

Ajouter une étendue

Nom de l'étendue *

ServicesMobiles

api://84838b8e-6885-4b97-998f-0f4417bef915/ServicesMobiles

Qui peut accepter ?

Administrateurs et utilisateurs

Administrateurs uniquement

Nom d'affichage du consentement administrateur *

Services Mobiles

Description du consentement administrateur *

Services Mobiles

Nom d'affichage du consentement de l'utilisateur

Services Mobiles

Description du consentement de l'utilisateur

Services Mobiles

État

Activé

Désactivé

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.

Accueil > z7w44 | Inscriptions d'applications >

Inscrire une application ...

* Nom

Nom d'affichage côté utilisateur pour cette application (il peut être modifié ultérieurement).

Nom de l'institution - COBA portails et applications mobiles ✓

Types de comptes pris en charge

Qui peut utiliser cette application ou accéder à cette API ?

☒ Comptes dans cet annuaire d'organisation uniquement (z7w44 uniquement - Locataire unique)

☐ Comptes dans un annuaire d'organisation (tout annuaire Azure AD - Multilocataire)

☐ Comptes dans un annuaire d'organisation (tout annuaire Azure AD - Multilocataire) et comptes Microsoft personnels (par exemple, Skype, Xbox)

☐ Comptes Microsoft personnels uniquement

[Aidez-moi à choisir...](#)

URI de redirection (facultatif)

Nous retournerons la réponse d'authentification à cet URI une fois l'utilisateur authentifié. Fournir ceci maintenant est facultatif et cela peut être modifié ultérieurement, mais une valeur est requise pour la plupart des scénarios d'authentification.

Sélectionner une plateforme ▼ par ex., https://example.com/auth

- **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**.

Configurations de plateforme

Selon la plateforme ou l'appareil ciblé(e) par cette application, une configuration supplémentaire peut être nécessaire, par exemple, les paramètres d'authentification spécifiques, les URI de redirection ou les champs spécifiques à la plateforme.

[+ Ajouter une plateforme](#)

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

Configurer des plateformes

Applications web



Web

Générez, hébergez et déployez une application de serveur web. .NET, Java, Python



Application à page unique

Configurez des applications clientes de navigateur et des applications web progressives. Javascript.

Applications de bureau et mobiles



iOS / macOS

Objective-C, Swift, Xamarin



Android

Java, Kotlin, Xamarin



Applications de bureau et mobiles

Windows, UWP, Console, IoT & appareils à entrée limitée, iOS classique + Android

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

Configurer web

[← Toutes les plateformes](#)
[Démarrage rapide](#)
[Documents](#)

*** URI de redirection**

Les URI que nous accepterons comme destinations lors du retour des réponses d'authentification (jetons) après l'authentification ou la déconnexion des utilisateurs. L'URI de redirection que vous envoyez dans la demande au serveur de connexion doit correspondre à celui répertorié ici. Également appelées URL de réponse. [En savoir plus sur les URI de redirection et leurs restrictions](#)

URL de déconnexion du canal avant

Il s'agit de l'emplacement où nous envoyons une requête pour que l'application efface les données de session de l'utilisateur. Ceci est obligatoire pour que la déconnexion unique fonctionne correctement.

Octroi implicite et flux hybrides

Demandez un jeton directement à partir du point de terminaison d'autorisation. Si l'application a une architecture à page unique (SPA) et n'utilise pas le flux du code d'autorisation, ou si elle appelle une API web via JavaScript, sélectionnez les jetons d'accès et les jetons d'ID. Pour les applications web ASP.NET Core et d'autres applications web qui utilisent l'authentification hybride, sélectionnez uniquement les jetons d'ID. [En savoir plus sur les jetons.](#)

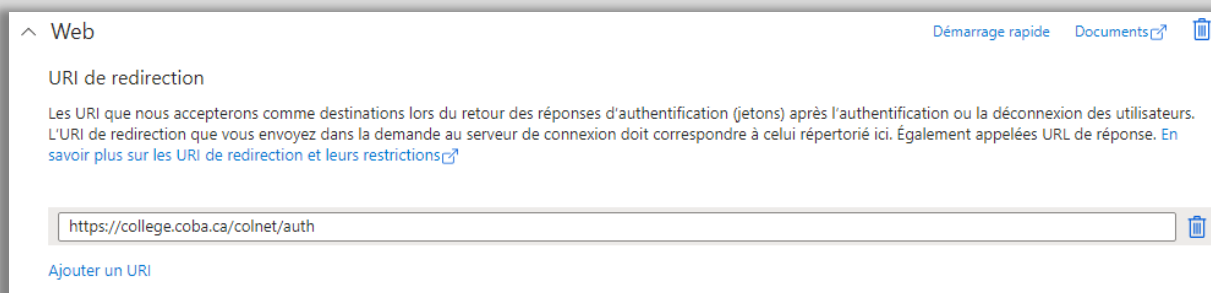
Sélectionnez les jetons que vous souhaitez voir émis par le point de terminaison d'autorisation :

☐ Jetons d'accès (utilisés pour les flux implicites)
 ☐ Jetons d'ID (utilisés pour les flux implicites et hybrides)

- **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.



Web

Démarrage rapide Documents

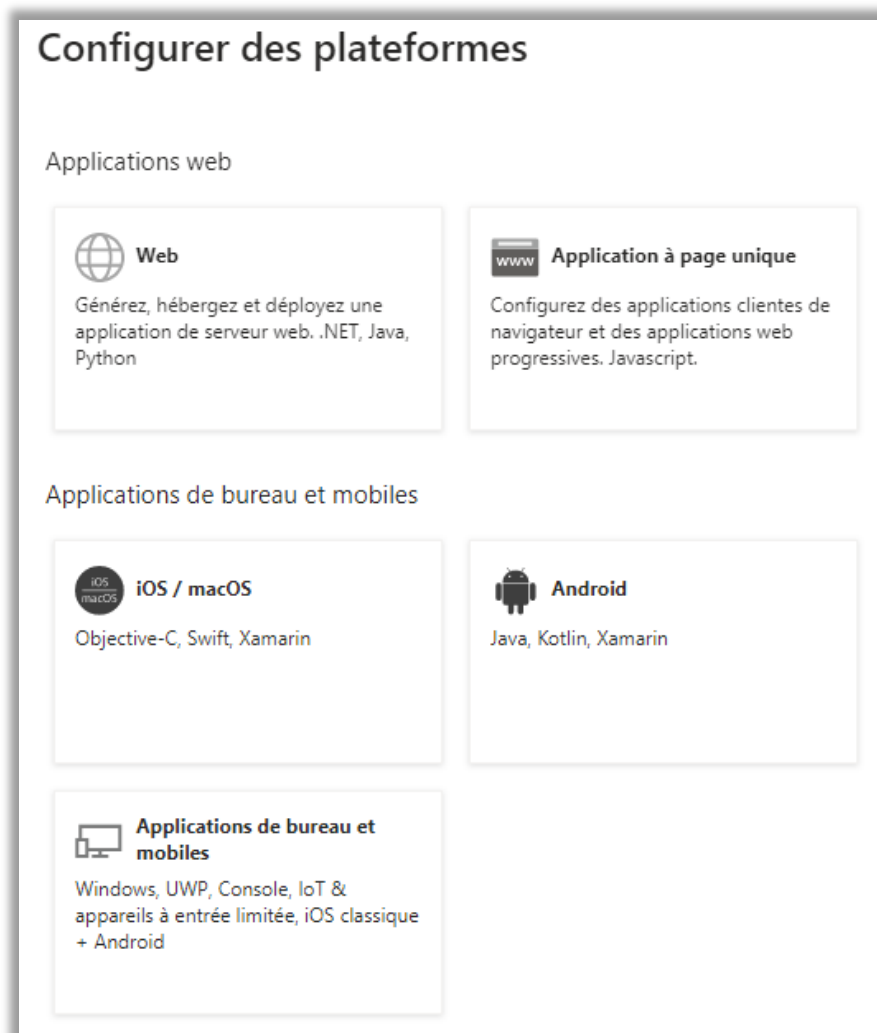
URI de redirection

Les URI que nous accepterons comme destinations lors du retour des réponses d'authentification (jetons) après l'authentification ou la déconnexion des utilisateurs. L'URI de redirection que vous envoyez dans la demande au serveur de connexion doit correspondre à celui répertorié ici. Également appelées URL de réponse. [En savoir plus sur les URI de redirection et leurs restrictions](#)

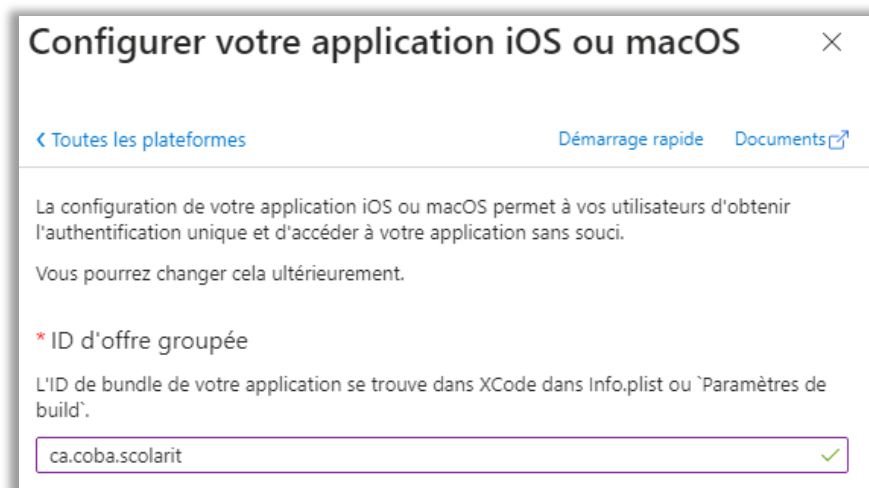
[Ajouter un URI](#)

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**.



Configurer votre application iOS ou macOS

[Toutes les plateformes](#) [Démarrage rapide](#) [Documents](#)

La configuration de votre application iOS ou macOS permet à vos utilisateurs d'obtenir l'authentification unique et d'accéder à votre application sans souci.

Vous pourrez changer cela ultérieurement.

*** ID d'offre groupée**

L'ID de bundle de votre application se trouve dans XCode dans Info.plist ou `Paramètres de build`.

ca.coba.scolarit

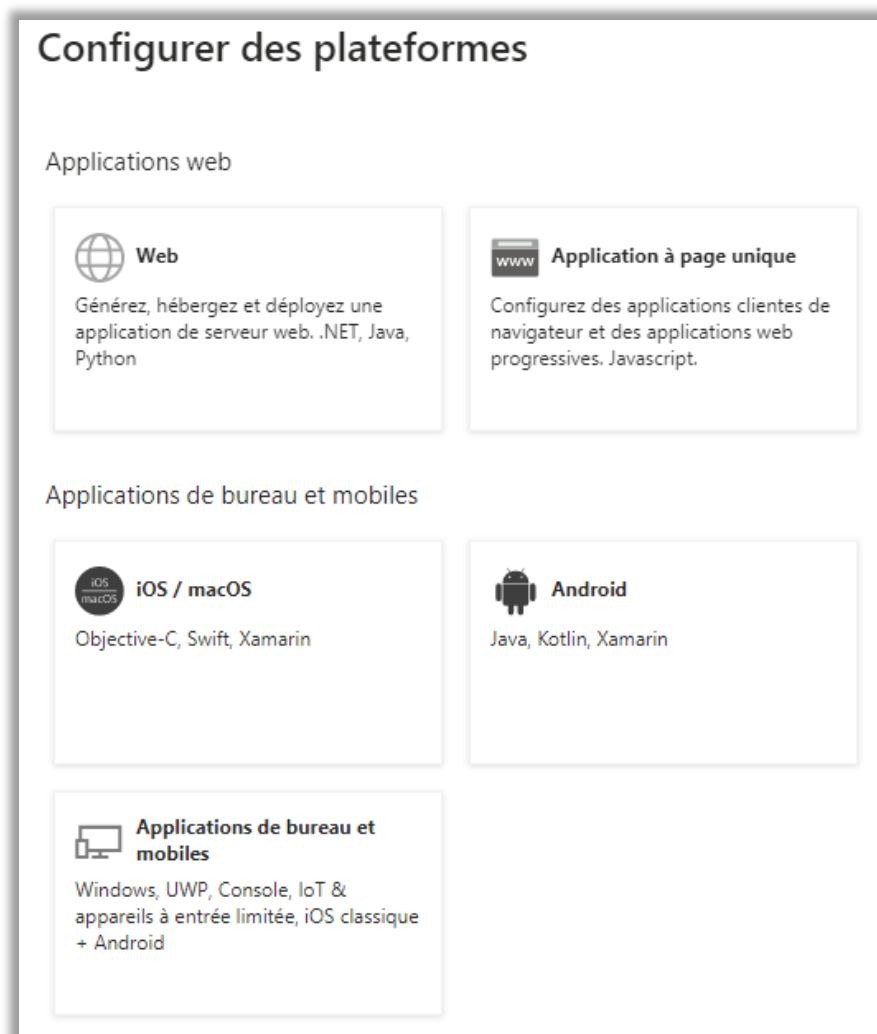
- **ID d'offre groupée**
 - Saisir ca.coba.scolarit
- **URI de redirection**
 - msauth.ca.coba.scolarit://auth

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**.

Configurer votre application Android

[< Toutes les plateformes](#)
[Démarrage rapide](#)
[Documents](#)

La configuration de votre application Android permet à vos utilisateurs d'obtenir l'authentification unique à l'échelle des appareils via Microsoft Authenticator et d'accéder à votre application sans souci.

Vous pourrez changer cela ultérieurement.

*** Nom du package**

Le nom du package de votre application se trouve dans le manifeste Android.

*** Hachage de signature**

Le hachage de signature peut être généré via la ligne de commande.

✓

Création d'un hachage de signature de développement. Celui-ci changera pour chaque environnement de développement.

✓

Création d'un hachage de signature de production.

- **Nom du package**
 - com.wifylgood.scolarit.coba
- **Hachage de signature**
 - EhaEtY5x0lfoyWvXGiVp3y61vdU=
- **URI de redirection**
 - msauth://com.wifylgood.scolarit.coba/EhaEtY5x0lfoyWvXGiVp3y61vdU%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**.

Revendications facultatives

Les revendications facultatives sont utilisées pour configurer des informations supplémentaires qui sont retournées dans un ou plusieurs jetons.

[+ Ajouter une revendication facultative](#) [+ Ajouter une revendication de groupes](#)

Revendication ↑↓

Description

Aucun résultat.

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

Ajouter une revendication facultative

Une fois que vous avez sélectionné un type de jeton, vous pouvez choisir dans une liste de revendications facultatives disponibles.

*** Type de jeton**
 Les jetons d'accès et d'ID sont utilisés par les applications pour l'authentification. [En savoir plus](#)

☒ ID
☐ Accéder
☐ SAML

☒ Revendication ↑↓	Description
☐ acct	État du compte utilisateur dans le locataire
☐ auth_time	Heure de la dernière authentification de l'utilisateur ; vo...
☐ ctry	Pays/région de l'utilisateur
☐ email	Adresse e-mail adressable pour cet utilisateur, si l'utilisa...
☐ family_name	Fournit le nom de famille ou le nom de l'utilisateur, tel ...
☐ fwd	Adresse IP
☐ given_name	Fournit le prénom ou le nom « donné » de l'utilisateur, t...
☐ in_corp	Indique si le client se connecte à partir du réseau d'entr...
☐ ipaddr	Adresse IP depuis laquelle le client s'est connecté
☒ login_hint	Indicateur de connexion
☐ onprem_sid	Identificateur de sécurité local

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

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

[+ Ajouter une autorisation](#) [✓ Accorder un consentement d'administrateur pour z7w44](#)

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
▼ Microsoft Graph (1)				
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur	Non	...

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**.

Demander des autorisations d'API

Sélectionner une API

API Microsoft Graph

API utilisées par mon organisation

Mes API

API Microsoft couramment utilisées



Microsoft Graph

Tirez parti de la grande quantité de données dans Office 365, Enterprise Mobility + Security, et Windows 10. Accédez à Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner et plus, via un seul point de terminaison.

Sélectionner des autorisations

développer tout

Commencez à taper une autorisation pour filtrer ces résultats

i La colonne « Consentement de l'administrateur requis » indique la valeur par défaut pour une organisation. Toutefois, le consentement de l'utilisateur peut être personnalisé par autorisation, utilisateur ou application. Cette colonne peut ne pas refléter la valeur dans votre organisation ou dans les organisations où cette application sera utilisée. [En savoir plus](#)

Autorisation

Consentement de l'administrateur ...

✓ Autorisations OpenId (3)

☐	email ⓘ Afficher l'adresse e-mail des utilisateurs	Non
☒	offline_access ⓘ Conserver l'accès aux données auxquelles vous lui avez donné accès	Non
☒	openid ⓘ Connecter les utilisateurs	Non
☒	profile ⓘ Afficher le profil de base des utilisateurs	Non

> AccessReview

> Acronym

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

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

[+ Ajouter une autorisation](#) ☒ Accorder un consentement d'administrateur pour z7w44

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
▼ Microsoft Graph (4) ...				
offline_access	Délégée	Conserver l'accès aux données auxquelles vous lui avez do...	Non	...
openid	Délégée	Connecter les utilisateurs	Non	...
profile	Délégée	Afficher le profil de base des utilisateurs	Non	...
User.Read	Délégée	Activer la connexion et lire le profil utilisateur	Non	...

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

Demander des autorisations d'API

Sélectionner une API

API Microsoft Graph API utilisées par mon organisation Mes API

Les applications qui exposent les autorisations sont indiquées ci-dessous

Nom	ID d'application (client)
Nom de votre institution - COBA Applications mobiles (API)	84838b8e-6885-4b97-998f-0f4417bef915

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

Demander des autorisations d'API

[← Toutes les API](#)

Nom de votre institution - COBA Applications mobiles (API)
api://84838b8e-6885-4b97-998f-0f4417bef915

Quel type d'autorisation votre application nécessite-t-elle ?

Autorisations déléguées

Votre application doit accéder à l'API en tant qu'utilisateur connecté.

Autorisations d'application

Votre application s'exécute en tant que service en arrière-plan ou démon sans utilisateur connecté.

Sélectionner des autorisations [développer tout](#)

i La colonne « Consentement de l'administrateur requis » indique la valeur par défaut pour une organisation. Toutefois, le consentement de l'utilisateur peut être personnalisé par autorisation, utilisateur ou application. Cette colonne peut ne pas refléter la valeur dans votre organisation ou dans les organisations où cette application sera utilisée. [En savoir plus](#)

Autorisation	Consentement de l'administrateur r...
✓ Autorisations (1) ☒ ServicesMobiles ⓘ Services Mobiles	Oui

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

Avant

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

+ Ajouter une autorisation ✓ Accorder un consentement d'administrateur pour z7w44

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
Microsoft Graph (4)				...
offline_access	Délégée	Conserver l'accès aux données auxquelles vous lui avez do...	Non	...
openid	Délégée	Connecter les utilisateurs	Non	...
profile	Délégée	Afficher le profil de base des utilisateurs	Non	...
User.Read	Délégée	Activer la connexion et lire le profil utilisateur	Non	...

Après

Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin. [En savoir plus sur les autorisations et le consentement](#)

+ Ajouter une autorisation ✓ Accorder un consentement d'administrateur pour z7w44

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
Microsoft Graph (4)				...
offline_access	Délégée	Conserver l'accès aux données auxquelles vous lui avez do...	Non	✓ Accordé pour z7w44 ...
openid	Délégée	Connecter les utilisateurs	Non	✓ Accordé pour z7w44 ...
profile	Délégée	Afficher le profil de base des utilisateurs	Non	✓ Accordé pour z7w44 ...
User.Read	Délégée	Activer la connexion et lire le profil utilisateur	Non	✓ Accordé pour z7w44 ...
Nom de votre institution - COBA A _i				...
ServicesMobiles	Délégée	Services Mobiles	Oui	✓ Accordé pour z7w44 ...

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**.

Configuration

Gestionnaire de base de données: Microsoft SQL Server 2019 version 15.00.2101
 Client du GBD: msoledbsql.dll 18.3.0000.0, OledB 02.80, Session 125, Exe 10388 (TCP)
 Nom de la base de données: COBA_00046_001_CEGEP_MONTMORENCY_CARL_ANONYME_COL
 Nom du serveur: cobra-sql2019-02
 Chemin des fichiers supplémentaires: \\cobra-partage-01\Produits\Col\ColWin50.016\Donnees\

Info. générale | Paramètres de communication | Logiciels externes | **Sécurité des comptes** | Individus à notifier | Politiques MFA

Règles de validation des mots de passe

Longueur minimale: 5
 Longueur maximale: 30

Caractères obligatoires:

- Au moins une lettre minuscule: ☐
- Au moins une lettre majuscule: ☐
- Au moins un chiffre: ☐
- Au moins un caractère spécial: ☐

Liste des caractères spéciaux:

Bloquer la réutilisation des derniers mots de passe: ☐
 Nombre de derniers mots de passe à bloquer: 5

Tester un mot de passe:

MFA COBA

Code de politique V5: ...
 Code de politique V6: ...

Accès au compte

Verrouiller le compte après plusieurs tentatives échouées: ☒
 Nbre de tentatives permises: 5
 Durée du verrouillage (heures): 1

Activer le renouvellement de mot de passe: ☒
 Nbre de jours avant le renouvellement: 90

Fournisseur d'authentification

Fournisseur OIIC:
 Identification:
 Tenant:
 Domaine:
 Mode d'authentification:

Licence d'utilisation | Base de données | **OK** | Annuler

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.

^ Bases	
Nom d'affichage	: Collège Cobra - COBA Applications administratives
ID d'application (client)	: 12b79659-a6dc-4f9d-8170-5d83a2a25da9
ID de l'objet	: b0266975-0ddf-45c7-bb15-c0aeb82cc85d
ID de l'annuaire (locataire)	: 1830c498-b4ce-4ab4-9b12-be22bf04a02a
Types de comptes pris en...	: Mon organisation uniquement

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.

^ Bases	
Nom d'affichage	: Collège Cobra - COBA Applications administratives
ID d'application (client)	: 12b79659-a6dc-4f9d-8170-5d83a2a25da9
ID de l'objet	: b0266975-0ddf-45c7-bb15-c0aeb82cc85d
ID de l'annuaire (locataire)	: 1830c498-b4ce-4ab4-9b12-be22bf04a02a
Types de comptes pris en...	: Mon organisation uniquement

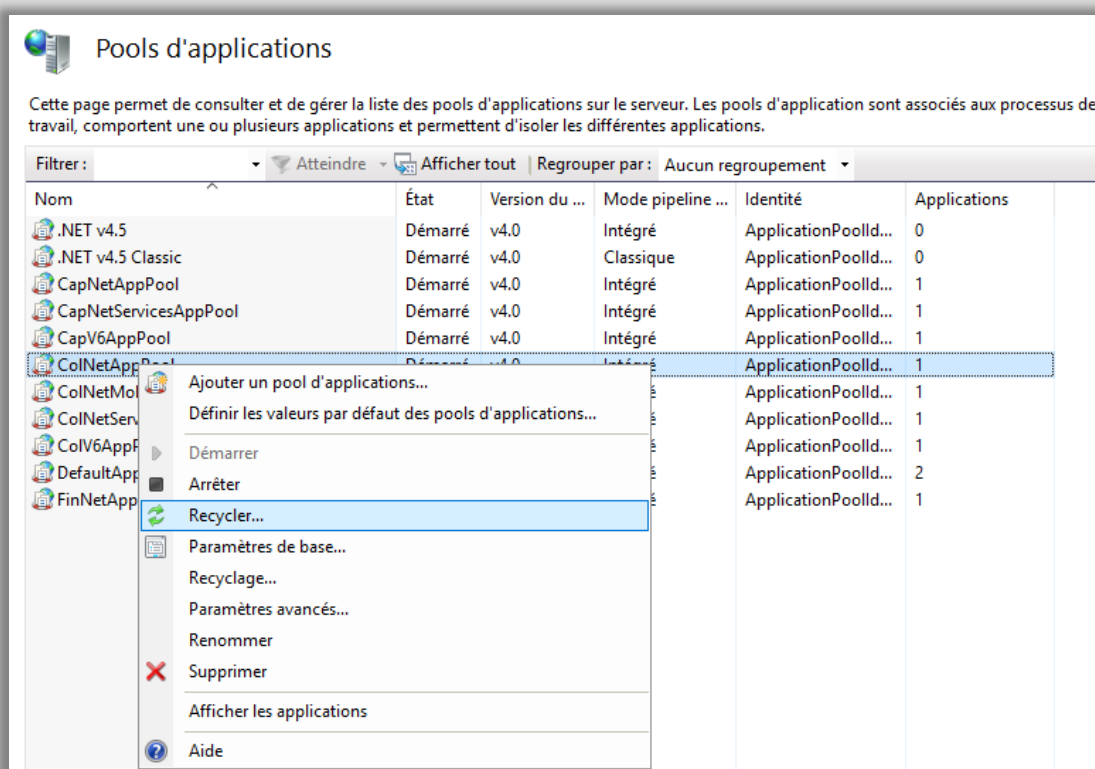
Domaine

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 :

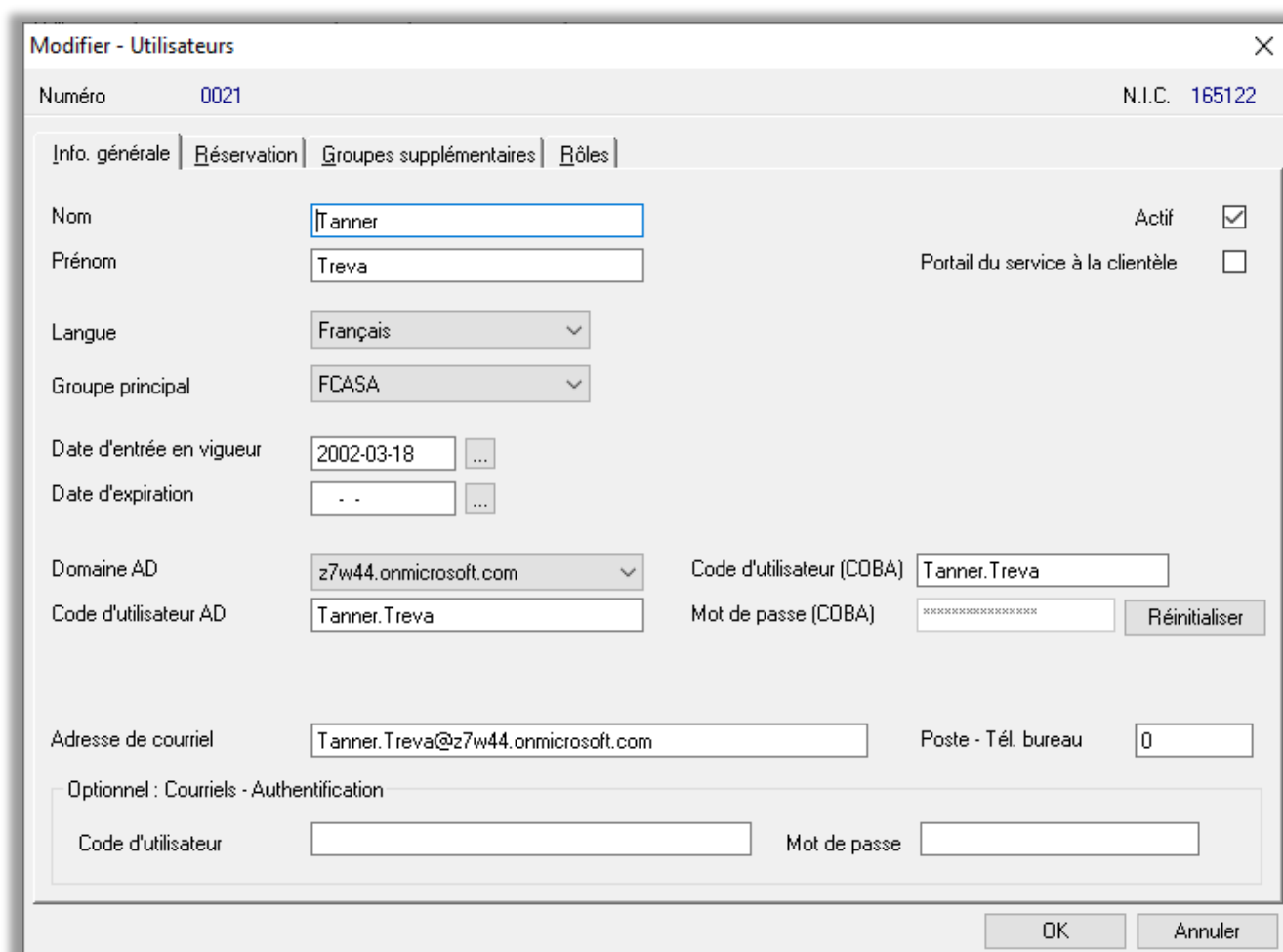
Pour activer le bouton d'authentification Azure AD sur la l'application V6, vous devez ajouter la ligne suivante dans le fichier **ColV6\Config\Config.txt** sur le serveur où l'application V6 est installée.

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.



The screenshot shows a window titled "Modifier - Utilisateurs" with a close button (X) in the top right corner. The window displays the configuration for a user with "Numéro 0021" and "N.I.C. 165122". The "Info. générale" tab is selected, showing fields for "Nom" (Tanner), "Prénom" (Treva), "Langue" (Français), "Groupe principal" (FCASA), "Date d'entrée en vigueur" (2002-03-18), "Date d'expiration" (- -), "Domaine AD" (z7w44.onmicrosoft.com), "Code d'utilisateur AD" (Tanner.Treva), "Code d'utilisateur (COBA)" (Tanner.Treva), "Mot de passe (COBA)" (masked), "Adresse de courriel" (Tanner.Treva@z7w44.onmicrosoft.com), and "Poste - Tél. bureau" (0). There are checkboxes for "Actif" (checked) and "Portail du service à la clientèle" (unchecked). A "Réinitialiser" button is next to the password field. An "Optionnel : Courriels - Authentification" section contains fields for "Code d'utilisateur" and "Mot de passe". "OK" and "Annuler" buttons are at the bottom right.

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.

Authentification sur les portails et les applications mobiles

Configuration du fournisseur d'authentification

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.

^ Bases	
Nom d'affichage	: Collège Cobra - COBA Portails et applications mobiles
ID d'application (client)	: 467e57a8-60c1-46a4-b282-8a5f591959cc
ID de l'objet	: f758a49d-91e9-4d6f-bbf0-c57488be3702
ID de l'annuaire (locataire)	: 1830c498-b4ce-4ab4-9b12-be22bf04a02a
Types de comptes pris en...	: Mon organisation uniquement

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.

^ Bases	
Nom d'affichage	: Collège Cobra - COBA Portails et applications mobiles
ID d'application (client)	: 467e57a8-60c1-46a4-b282-8a5f591959cc
ID de l'objet	: f758a49d-91e9-4d6f-bbf0-c57488be3702
ID de l'annuaire (locataire)	: 1830c498-b4ce-4ab4-9b12-be22bf04a02a
Types de comptes pris en...	: Mon organisation uniquement

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/EhaEtY5x0lfoyWvXGiVp3y61vdU%3D

Titre français

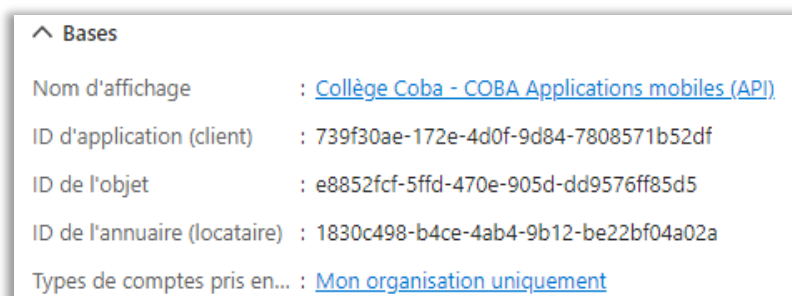
Saisir le titre du bouton à afficher pour la connexion en français avec le fournisseur d'authentification sur le portail et sur l'application mobile.

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.



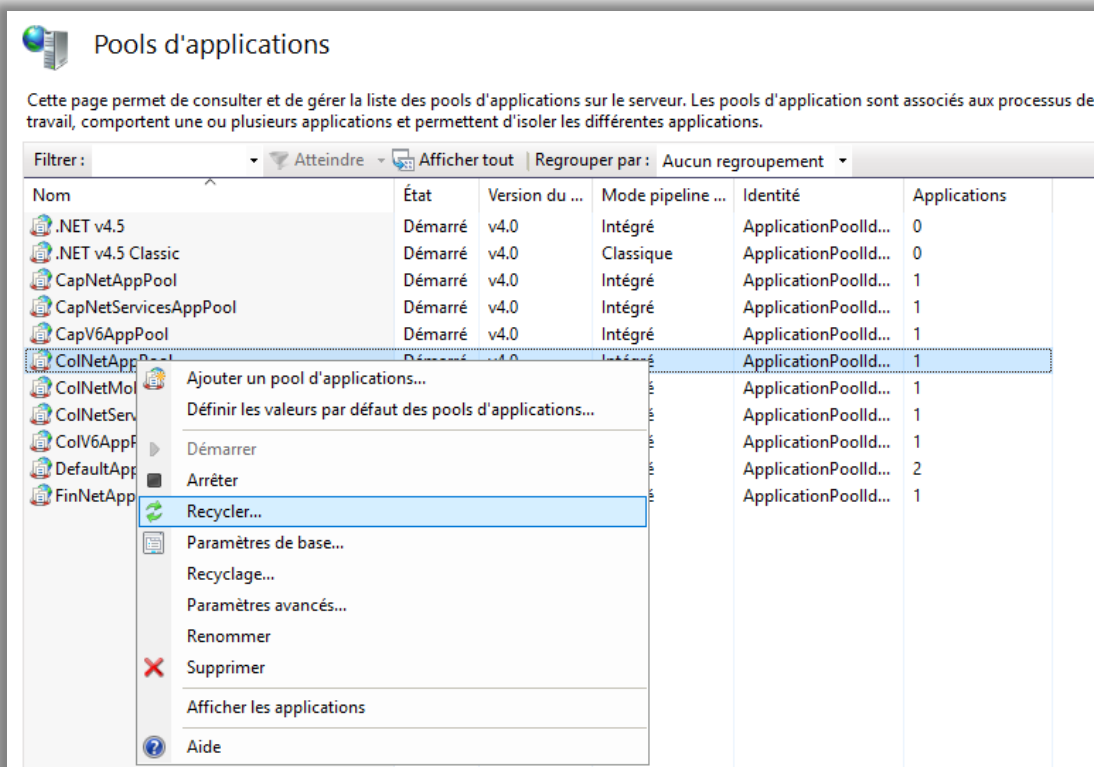
Domaine

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.

Résolution de problèmes

Pares-feux

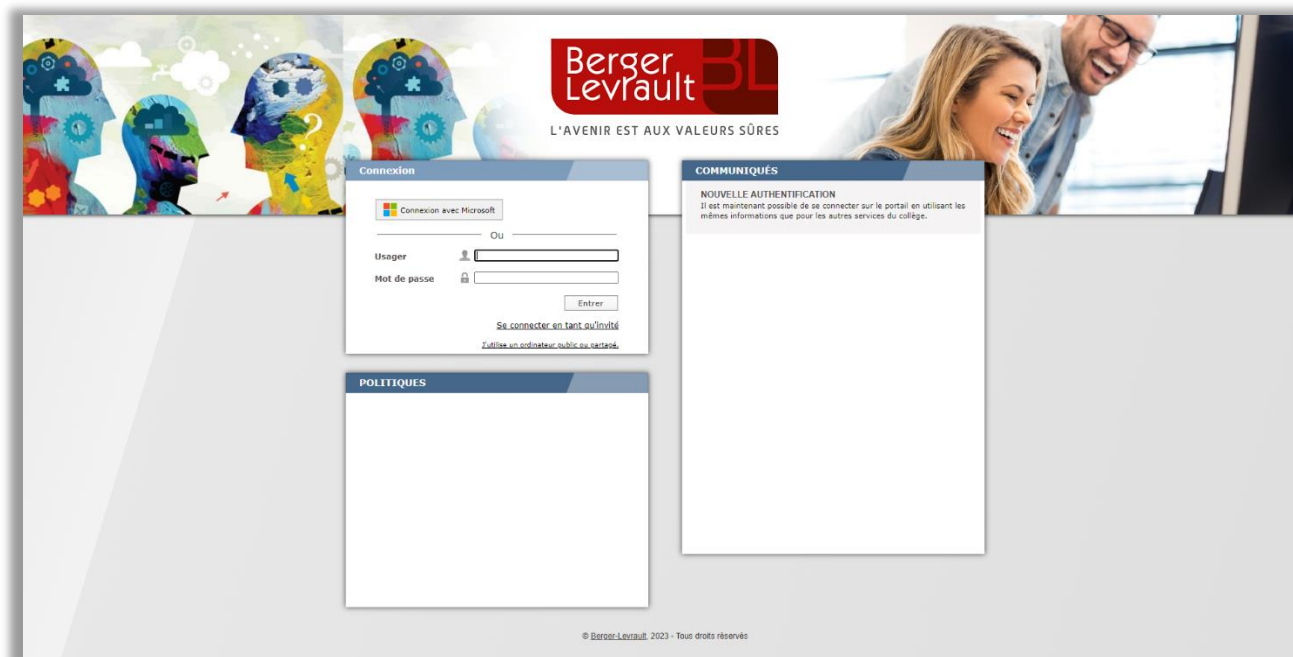
Les URI suivants doivent être accessible à partir du serveur des portails et des applications administratives V6 :

- <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.

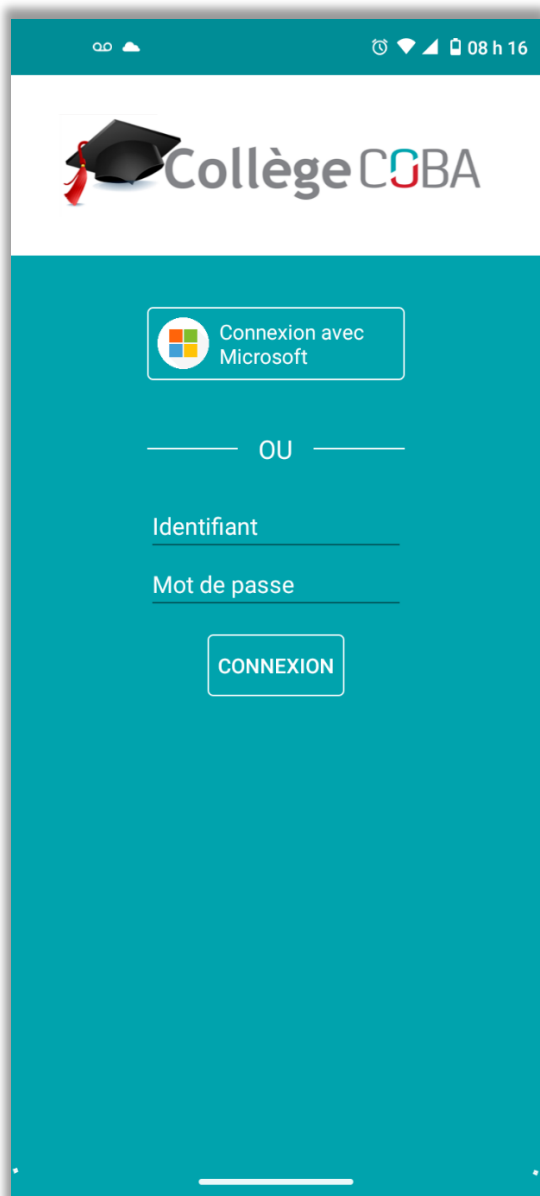
Voici un exemple de la séquence des opérations pour un utilisateur de l'application mobile qui s'authentifie avec le fournisseur d'authentification Azure AD.

The image shows two sequential screenshots of a mobile application's authentication interface. The first screenshot is the 'Sign in' screen, featuring the Microsoft logo, the title 'Sign in', a text input field for 'Email, phone, or Skype', a link for 'Can't access your account?', and a blue 'Next' button. Below this is a section for 'Sign-in options' with a key icon. The second screenshot is the 'Enter password' screen, showing the Microsoft logo, a back arrow, the email address 'lana.gravel@z7w44.onmicrosoft.com', the title 'Enter password', a text input field for 'Password', a link for 'Forgot my password', and a blue 'Sign in' button.

Lien ColNET => PaieNET ???

Applications mobiles

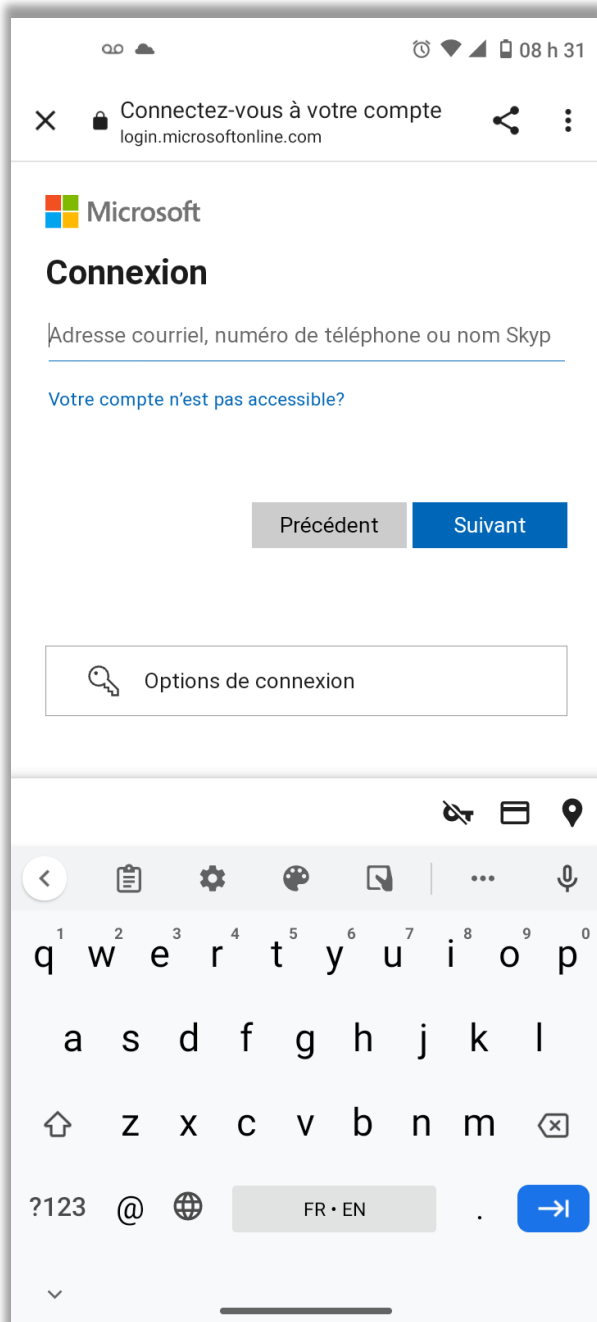
À la suite de la configuration d'un fournisseur d'authentification pour le portail, les utilisateurs seront invités à se connecter dans l'application mobile avec l'aide de l'authentification avec le fournisseur d'authentification Azure AD ou avec l'aide de l'authentification traditionnelle de COBA.



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.



Connectez-vous à votre compte
login.microsoftonline.com

Microsoft

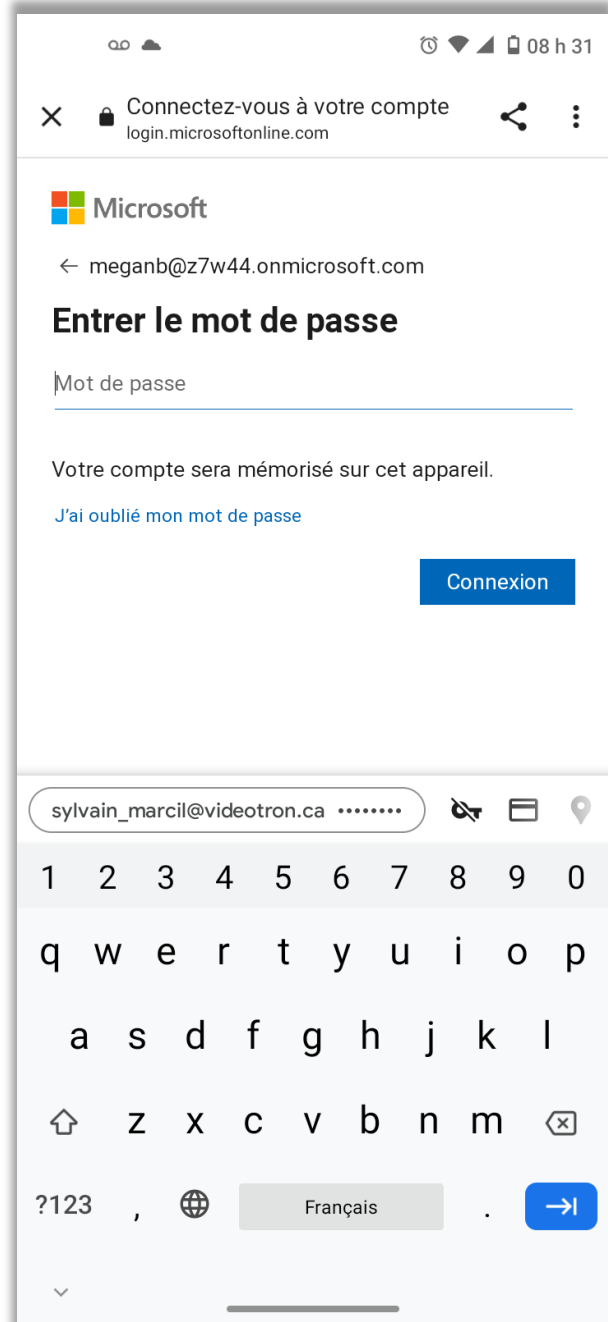
Connexion

Adresse courriel, numéro de téléphone ou nom Skyp

[Votre compte n'est pas accessible?](#)

Précédent Suivant

Options de connexion



Connectez-vous à votre compte
login.microsoftonline.com

Microsoft

← meganb@z7w44.onmicrosoft.com

Entrer le mot de passe

Mot de passe

Votre compte sera mémorisé sur cet appareil.

[J'ai oublié mon mot de passe](#)

Connexion

sylvain_marcil@videotron.ca

1 2 3 4 5 6 7 8 9 0

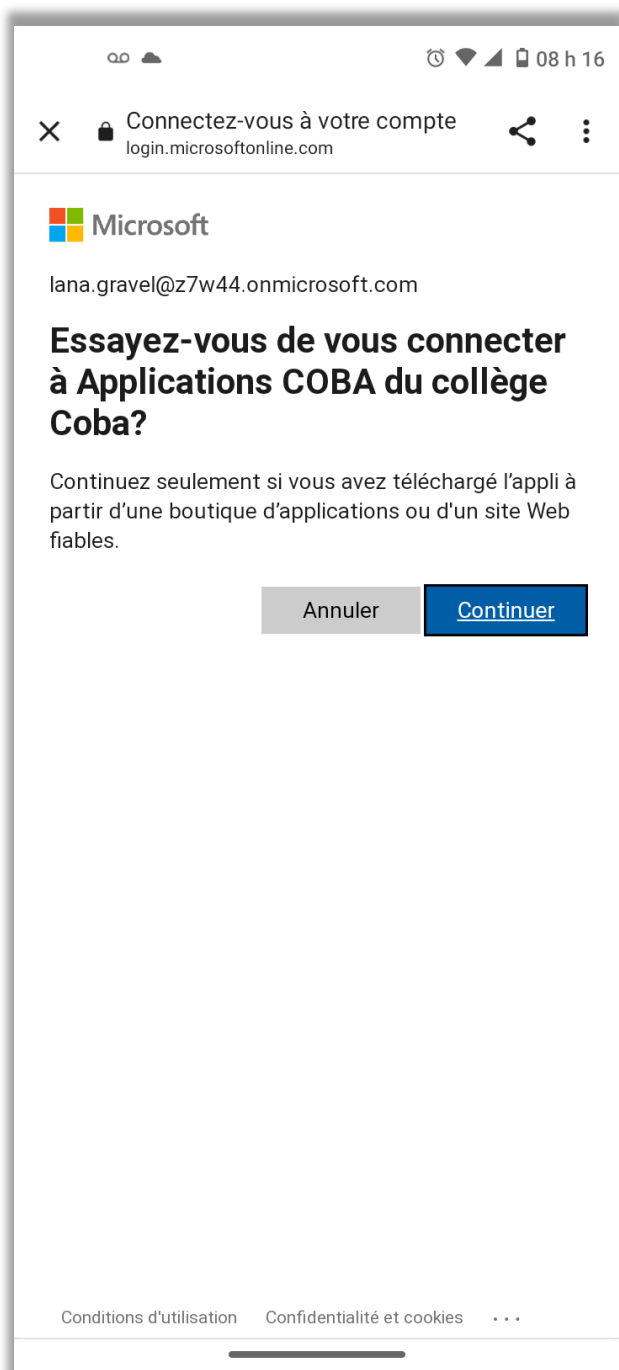
q w e r t y u i o p

a s d f g h j k l

z x c v b n m

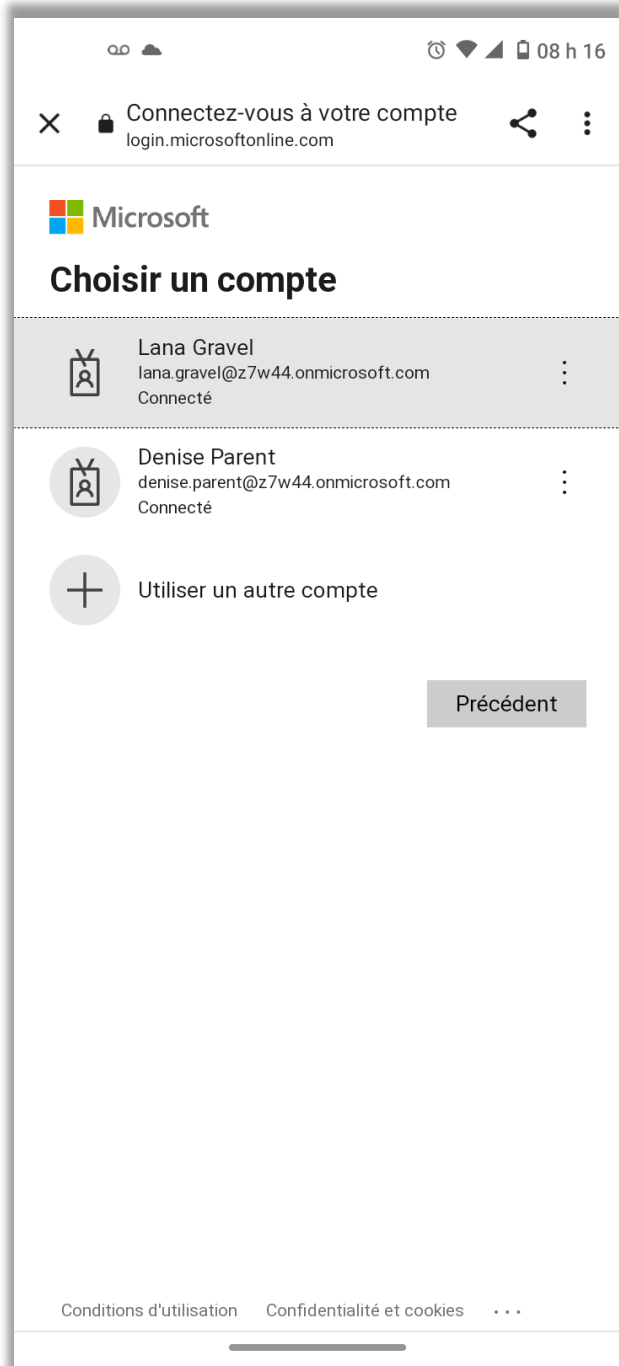
?123 @ . FR • EN →

Français →



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.

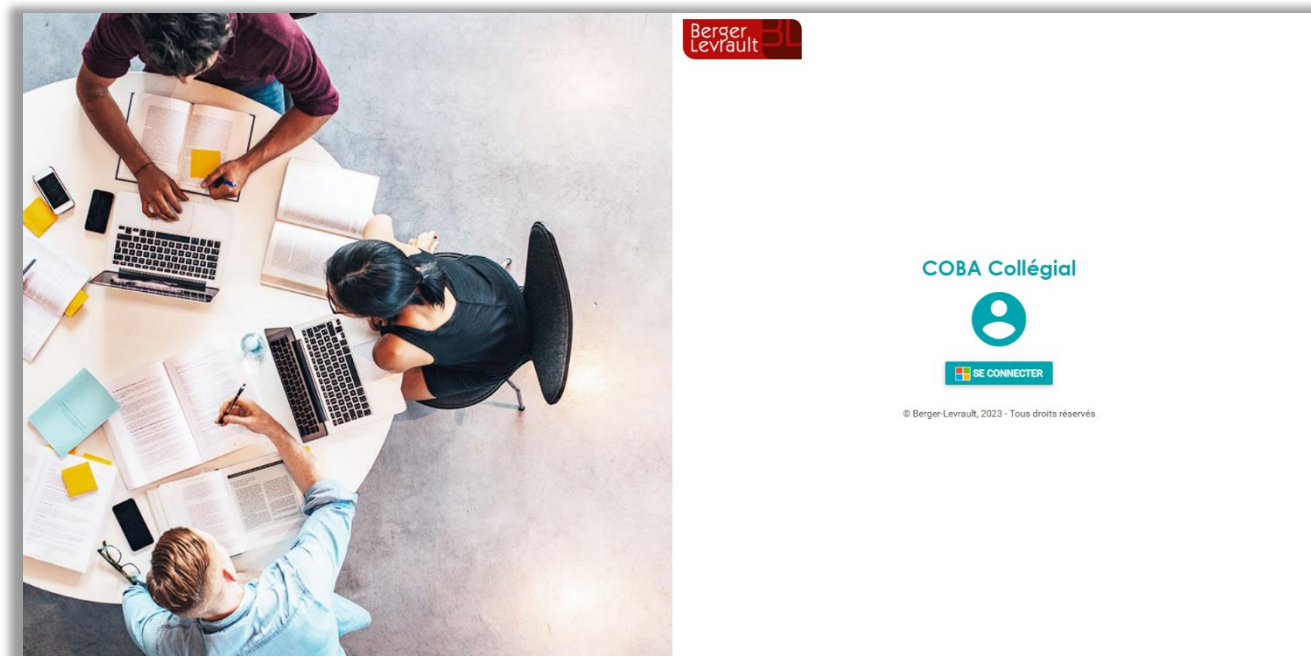
Dans la situation où l'utilisateur utilise déjà plusieurs comptes sur son appareil mobile, celui-ci sera invité à utiliser un compte déjà existant.



Lien Application mobile => PaieNET ???

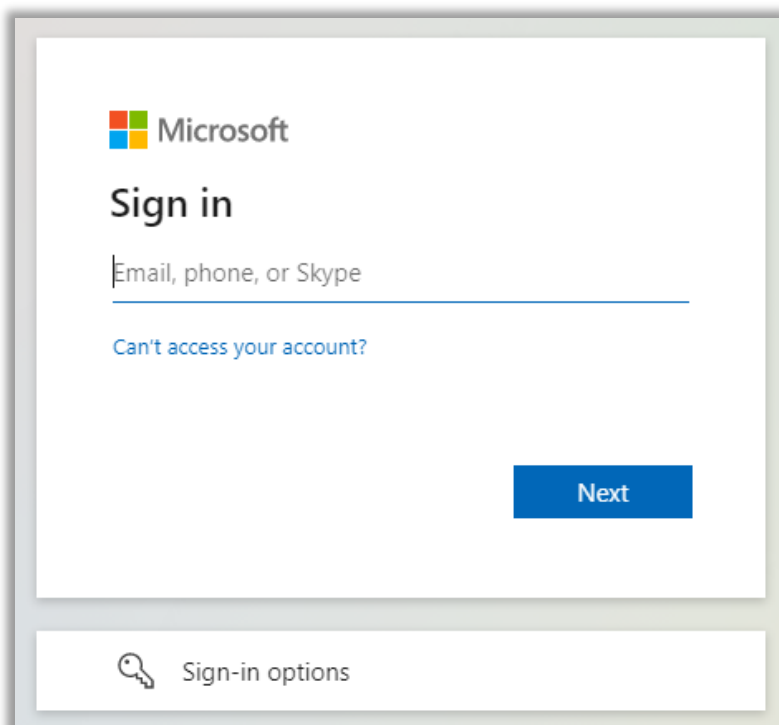
Applications administratives V6

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.

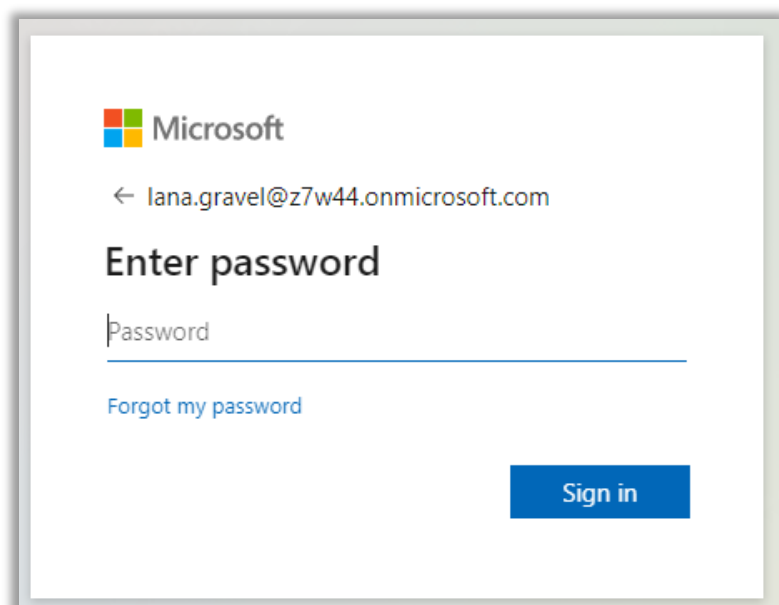


Note : Si la configuration de l'authentification Azure AD de votre institution exige une authentification avec du MFA, celui-ci sera automatiquement intégré dans l'authentification sur nos applications administratives.

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.



The first screenshot shows the Microsoft Sign in page. At the top left is the Microsoft logo. Below it, the text "Sign in" is displayed. Underneath is a text input field with the placeholder text "Email, phone, or Skype". Below the input field is a link that says "Can't access your account?". At the bottom right is a blue button labeled "Next". At the bottom left, there is a key icon and the text "Sign-in options".



The second screenshot shows the Microsoft Enter password page. At the top left is the Microsoft logo. Below it, the text "Enter password" is displayed. Above this text is a back arrow icon and the email address "lana.gravel@z7w44.onmicrosoft.com". Below the text is a text input field with the placeholder text "Password". Below the input field is a link that says "Forgot my password". At the bottom right is a blue button labeled "Sign in".