

DOCUMENTATION / SUPPORT DE FORMATION



Table des matières

Authentifications externes	3
<i>Authentification Google Apps</i>	3
<i>Authentification Azure Active Directory (Office 365 enterprise)</i>	4
Authentification via le portail Web	4

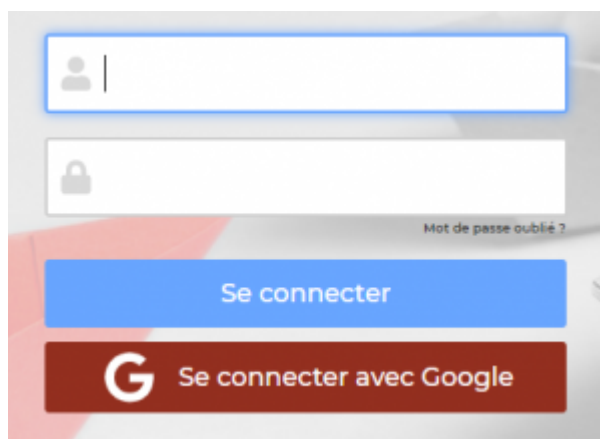
Authentifications externes

L'application vous permet d'utiliser un système externe pour l'authentification de vos utilisateurs.

Plusieurs modes d'authentification sont disponibles

- Authentification Google Apps
- Authentification Office 365 directe
- Authentification Azure Active Directory (fonctionne avec Office 365 enterprise)

Authentification Google Apps



L'application vous permet d'utiliser Google Apps pour authentifier les utilisateurs. Cette méthode est possible uniquement si vous disposez d'un domain Google Apps pour gérer vos email d'entreprise.

Cette méthode permet à vos utilisateur de ne pas avoir à mémoriser ou gérer un autre identifiant et mot de passe pour l'accès à l'application.

L'authentification est intégralement gérée par Google via le protocole oauth 2.0.

Pour activer l'authentification Google Apps

1. Contacter le support Veryswing directement depuis l'application en demandant l'activation de ce mode d'authentification dans votre environnement.
2. Nous faisons ensuite l'activation pour vous et nous faisons le nécessaire auprès de Google
3. Une fois ce mode d'authentification activée, une image rouge "Se connecter avec Google" apparait sur l'écran de connexion
4. Il est nécessaire de changer le mode d'authentification de vos utilisateurs depuis l'écran Administration > Utilisateur

Dans le formulaire, vous devez choisir explicitement le mode d'authentification Google dans le formulaire de gestion de l'utilisateur. Il existe également une action de masse pour le faire sur plusieurs utilisateurs en même temps.

Une fois l'authentification Google activée sur un utilisateur, il doit obligatoire cliquer sur le bouton "Se

connecter avec Google” pour accéder à l'application. Il sera alors redirigé vers le site Google qui gère l'authentification puis redirigé vers l'application.

Authentification Azure Active Directory (Office 365 enterprise)

Si vous disposez d'un abonnement Azure avec Active Directory ou Office 365 enterprise, vous pouvez disposer d'une authentification sécurisée via Azure Active Directory.

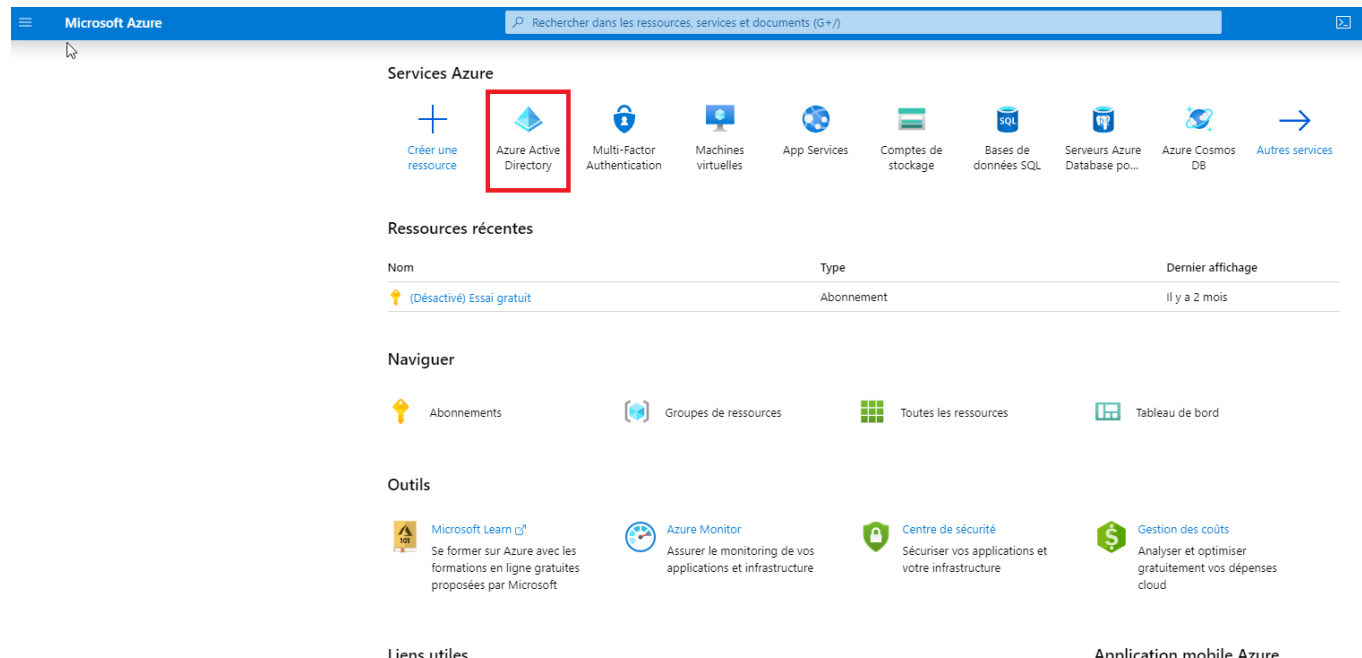
Cette méthode permet à vos utilisateurs de ne pas avoir à mémoriser ou gérer un autre identifiant et mot de passe pour l'accès à l'application.

L'authentification est intégralement gérée par Microsoft via le protocole oauth 2.0 sur la plateforme Azure.

Vous trouverez ci-dessous les différentes étapes pour activer ce mode d'authentification pour le portail Web et ensuite pour les applications mobiles.

Authentification via le portail Web

Depuis la console Microsoft Azure



Depuis votre console Azure, cliquez sur Azure Active Directory dans les items à gauche.

Cliquez ensuite sur l'onglet Inscriptions des applications.

Copyright © Veryswing SAS, Tous droits réservés.

Répertoire par défaut - Inscriptions d'applications

Rechercher (Ctrl+/) << **+ Nouvelle inscription** Points de terminaison Résolution des problèmes Inscriptions d'applications (héritage) Des commentaires ?

Bienvenue dans la nouvelle expérience Inscriptions d'applications améliorée (désormais en disponibilité générale). Découvrez les nouveautés et apprenez-en plus sur ce qui a changé. →

Toutes les applications Applications détenues Applications du compte personnel

Commencez à taper un nom ou un ID d'application pour filtrer ces résultats

Nom d'affichage	ID d'application (client)
Aucun résultat.	

Ce compte n'est pas répertorié en tant que propriétaire d'applications dans cet annuaire.

[Afficher toutes les applications dans l'annuaire](#)

[Afficher toutes les applications associées à ce compte ne faisant partie d'aucun annuaire](#)

Remplissez les informations demandées :

- Nom : VSActivity ou VSPortage
- Type de comptes pris en charge : Comptes dans cet annuaire d'organisation uniquement (Répertoire par défaut uniquement - Locataire unique)

Inscrire une application

* Nom

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

VSACTIVITY 

Types de comptes pris en charge

Qui peut utiliser cette application ou accéder à cette API ?

- ☒ Comptes dans cet annuaire d'organisation uniquement (Répertoire par défaut 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)

[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.

Web 

exemple : <https://myapp.com/auth>

En continuant, vous acceptez les stratégies de la plateforme Microsoft 

S'inscrire

Une fois l'application créée, cliquez sur Authentification situé dans la partie droite puis sur le bouton Ajouter une plateforme ⇒ Applications Web

VSACTIVITY - Authentification

Rechercher (Ctrl+/) «

Vue d'ensemble

Démarrage rapide

Gérer

Personnalisation

Authentification

Certificats & secrets

Configuration du jeton (prévers...

API autorisées

Exposer une API

Propriétaires

Rôles et administrateurs (préve...

Manifeste

Support + dépannage

Résolution des problèmes

Nouvelle demande de support



Enregistrer



Abandonner



Basculer vers l'ancienne expérience



Des commentaires ?

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

Types de comptes pris en charge

Qui peut utiliser cette application ou accéder à cette API ?

- ☒ Comptes dans cet annuaire d'organisation uniquement (Répertoire par défaut uniquement - Locataire unique)
- ☐ Comptes dans un annuaire d'organisation (tout annuaire Azure AD - Multilocataire)

[Aidez-moi à choisir...](#)

⚠ En raison de différences temporaires dans les fonctionnalités prises en charge, il n'est pas recommandé d'activer les comptes personnels Microsoft pour une inscription existante. Si vous devez activer des comptes personnels, vous pouvez le faire à l'aide de l'éditeur de manifeste. [En savoir plus sur ces restrictions.](#)

Paramètres avancés

Type de client par défaut ⓘ

Considérer l'application comme un client public.
requis pour l'utilisation des flux suivants, où un URI de redirection n'est pas utilisé :

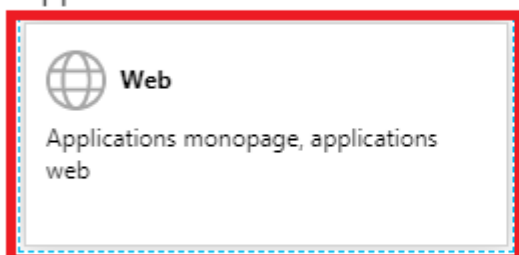
Oui

Non

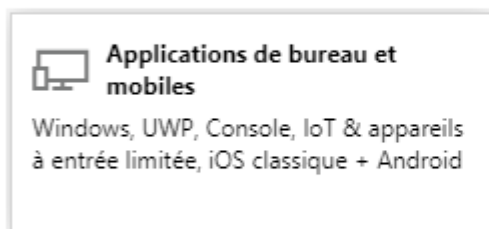
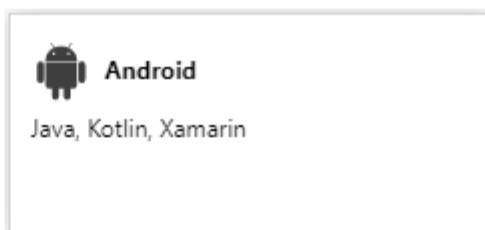
- Informations d'identification du mot de passe du propriétaire de la ressource (ROPC) [En savoir plus](#)
- Flux de code d'appareil [En savoir plus](#)
- Authentification Windows intégrée (IWA) [En savoir plus](#)

Configurer des plateformes

Applications web



Applications de bureau et mobiles



Une fois que vous êtes dans « Configurer WEB » vous devez ajouter dans le champ URI de redirection l'URL suivante : <https://ENTREPRISE.vsactivity.com/common/azuread/callback.php>

URI de redirection

URI que nous accepterons comme destinations lors du renvoi des réponses d'authentification (jetons) après l'authentification des utilisateurs. Ils sont aussi parfois appelés URL de réponse.
[En savoir plus sur les URI de redirection et les restrictions](#)

`https://ENTREPRISE.vsactivity.com/common/azuread/callback.php`



URL de déconnexion

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.

exemple : `https://myapp.com/logout`

Octroi implicite

Permet à une application de demander un jeton directement à partir du point de terminaison d'autorisation. Recommandé uniquement si l'application dispose d'une architecture monopage (SPA), sans composant de back-end ou si elle appelle une API web via JavaScript.
[En savoir plus sur le flux d'octroi implicite](#)

Pour activer le flux d'octroi implicite, sélectionnez les jetons que vous souhaitez voir émis par le point de terminaison d'autorisation :

☐

Jetons d'accès

☐

Jetons d'ID

Configurer














Annuler

Remplacez ENTREPRISE par le préfixe de l'url d'accès à votre environnement.

Vous devez ensuite aller sur « Certificats & Secrets » puis cliquer sur « Nouveau secret client »

VSACTIVITY - Certificats & secrets

«

-  Vue d'ensemble
-  Démarrage rapide
- Gérer
 -  Personnalisation
 -  Authentification
 -  **Certificats & secrets**
 -  Configuration du jeton (prévers...
 -  API autorisées
 -  Exposer une API
 -  Propriétaires
 -  Rôles et administrateurs (préve...
 -  Manifeste
- Support + dépannage
 -  Résolution des problèmes
 -  Nouvelle demande de support

Les informations d'identification permettent aux applications de s'identifier auprès du service d'authentification lors de la réception de jetons à un emplacement adr web (avec un schéma HTTPS). Pour un niveau plus élevé de sécurité, nous recommandons d'utiliser un certificat (au lieu d'un secret client) comme informations d'identification.

Certificats

Les certificats peuvent servir de secrets pour prouver l'identité de l'application lors de la demande d'un jeton. Ils peuvent aussi être appelés des clés publiques.

[Télécharger le certificat](#)

Aucun certificat n'a été ajouté pour cette application.

Empreinte numérique	Date de début	Date d'expiration
---------------------	---------------	-------------------

Secrets client


Chaîne secrète que l'application utilise pour prouver son identité lors de la demande de jeton. Peut aussi être appelée mot de passe d'application.

[+ Nouveau secret client](#)

Description	Date d'expirat...	Valeur
-------------	-------------------	--------

Aucun secret client n'a été créé pour cette application.

Vous pouvez mettre comme description VSACTIVITY et choisir en date d'expiration « Jamais » Cliquez sur « Ajouter ».

 Ajouter un secret client

Description

Date d'expiration

☐ Dans 1 an

☐ Dans 2 ans

☒ Jamais



Ajouter

Annuler

Attention la clé sera générée à l'enregistrement et n'apparaîtra qu'une seule fois.

Secrets client

Chaîne secrète que l'application utilise pour prouver son identité lors de la demande de jeton. Peut aussi être appelée mot de passe d'application.

+ Nouveau secret client		
Description	Date d'expirat...	Valeur
VSACTIVITY	31/12/2299	 

Il sera nécessaire de la sauvegarder pour nous la communiquer. Il sera ensuite impossible de la voir à nouveau.

Si vous avez raté la clé, vous pouvez en générer une nouvelle et supprimer l'ancienne.

La sécurité et les autorisations d'accès

Une fois l'application créée, il est nécessaire d'ajouter des autorisations pour que vos utilisateurs puissent se connecter à l'application depuis votre tenant Azure AD.

Cliquez sur API autorisées, depuis le panneau de configuration de l'application dans votre console Azure AD.

Cliquez sur « Ajouter une autorisation »

Accueil > VSACTIVITY - API autorisées

VSACTIVITY - API autorisées

Rechercher (Ctrl+/) « Actualiser

Autorisations configurées

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

+ Ajouter une autorisation Accorder un consentement d'administrateur pour Répertoire par défaut

API / noms des autorisations	Type	Description	Consentement adminis
▼ Microsoft Graph (1)			
User.Read	Déléguée	Sign in and read user profile	-







Cliquez sur Office 365 Management Apis.

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.		
 Azure Service Management Accès programmatique à la plupart des fonctionnalités disponibles via le portail Azure	 Dynamics 365 Business Central Accès programmatique aux données et fonctionnalités dans Dynamics 365 Business Central	 Office 365 Management APIs Récupérer les informations sur l'utilisateur, l'administrateur, le système, ainsi que les actions et les événements
 SharePoint Interagir à distance avec les données SharePoint	 Skype for Business Intégrer les fonctionnalités de présence en temps réel, messagerie sécurisée, appel et conférence	

Cliquez sur Autorisations de l'application et Autorisations déléguées pour donner l'accès en lecture.

Vous devez cliquer sur les deux boutons « Autorisations déléguées » puis sur le bouton « Ajouter des autorisations »



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

Autorisations déléguées

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

Autorisations de l'application

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

Sélectionner des autorisations

[réduire tout](#)

Autorisation

Consentement administrateur requis

▼ **ActivityFeed (2)**

ActivityFeed.Read

Read activity data for your organization ⓘ

Oui



ActivityFeed.ReadDlp

Read DLP policy events including detected sensitive data ⓘ

Oui

▼ **ActivityReports (2)**

ActivityReports.Read

Read activity reports for your organization ⓘ

Oui



ActivityReports.Read

Read activity reports for your organization ⓘ

Oui

▼ **ServiceHealth (1)**

ServiceHealth.Read

Read service health information for your organization ⓘ

Oui

▼ **ThreatIntelligence (2)**

ThreatIntelligence.Read

Read threat intelligence data for your organization ⓘ

Oui



ThreatIntelligence.Read

Read threat intelligence data for your organization ⓘ

Oui

Ajouter des autorisations

Abandonner

Une fois les autorisations déléguées paramétrées, vous devez cliquer sur le bouton « Accorder un consentement d'administrateur pour « Répertoire par défaut »

⚠ Vous ajoutez une ou plusieurs autorisations à votre application. Les utilisateurs doivent donner leur accord même s'ils l'ont déjà fait précédemment.

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 Répertoire par défaut

API / noms des autorisations	Type	Description	Consentement adminis...	Statut
▼ Microsoft Graph (1) ...				
User.Read	Déléguée	Sign in and read user profile	-	...
▼ Office 365 Management APIs (7) ...				
ActivityFeed.Read	Déléguée	Read activity data for your organization	Oui	⚠ Pas accordé pour Répert... ...
ActivityFeed.ReadDlp	Déléguée	Read DLP policy events including detected se...	Oui	⚠ Pas accordé pour Répert... ...
ActivityReports.Read	Déléguée	Read activity reports for your organization	Oui	⚠ Pas accordé pour Répert... ...
ActivityReports.Read	Déléguée	Read activity reports for your organization	Oui	⚠ Pas accordé pour Répert... ...
ServiceHealth.Read	Déléguée	Read service health information for your org...	Oui	⚠ Pas accordé pour Répert... ...
ThreatIntelligence.Read	Déléguée	Read threat intelligence data for your organi...	Oui	⚠ Pas accordé pour Répert... ...
ThreatIntelligence.Read	Déléguée	Read threat intelligence data for your organi...	Oui	⚠ Pas accordé pour Répert... ...

Répétez l'opération 1 fois pour ajouter l'APIs " **Azure Service Management API**"

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.



Azure Service Management

Accès programmatique à la plupart des fonctionnalités disponibles via le portail Azure



Dynamics 365 Business Central

Accès programmatique aux données et fonctionnalités dans Dynamics 365 Business Central



Office 365 Management APIs

Récupérer les informations sur l'utilisateur, l'administrateur, le système, ainsi que les actions et les événements



SharePoint

Interagir à distance avec les données SharePoint



Skype for Business

Intégrer les fonctionnalités de présence en temps réel, messagerie sécurisée, appel et conférence

Les informations à nous communiquer

Une fois l'application ajoutée dans votre console Azure, il est nécessaire de nous communiquer :

- L'ID de l'application (Authentification Web : Client ID) disponible dans la vue d'ensemble
- La clé secrète (Authentification Web: Client secret) que vous avez générée dans l'écran « Certificats et Secrets »
- L'ID de l'annuaire ⇒ Locataire (Nom du tenant)

Accueil > Répertoire par défaut - Inscriptions d'applications > VSACTIVITY

VSACTIVITY

Rechercher (Ctrl+/) <<

Supprimer Points de terminaison

Vous avez une seconde ? Nous aimerions obtenir vos commentaires sur Microsoft Identity Platform (précédemment appelée A

Nom d'affichage : VSACTIVITY

ID d'application (client) :

ID de l'annuaire (locataire... :

ID de l'objet :

Bienvenue dans les nouvelles Inscriptions d'applications améliorées. Vous cherchez à connaître les changements depuis Inscr...

Appeler des API

Générer des applications plus puissantes avec des données utilisateur et entreprise riches à partir des services Microsoft et des sources de données de votre entreprise.

Afficher les autorisation de l'API

En ce qui concerne l'application mobile

Vous devez créer une nouvelle application en l'appelant "VSACTIVITY MOBILE" dans votre console AZURE en suivant les mêmes étapes sauf sur la partie "Authentification" dans lequel vous devez suivre cette procédure ⇒

https://docs.veryswing.com/vsa:myvs_-_procedure_d_autorisation_de_l_application_mobile_dans_la_console_azure

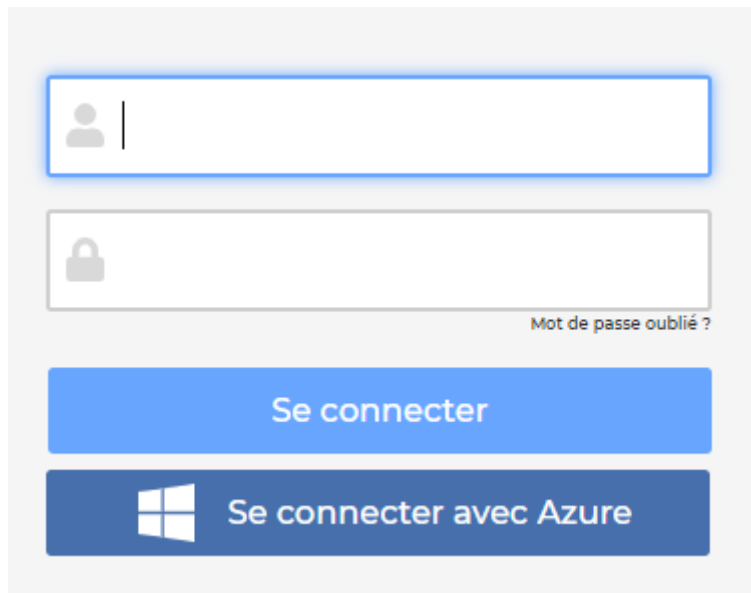
Une fois l'application mobile créée dans votre console AZURE, il faudra nous communiquer l'ID d'application que vous avez dans la partie "Authentification" de votre application VSACTIVITY MOBILE

Une fois que le mode d'authentification Azure AD est activé

Il est nécessaire de changer le mode d'authentification de vos utilisateurs depuis l'écran

Dans le formulaire, vous devez choisir explicitement le mode d'authentification Azure Active Directory dans le formulaire de gestion de l'utilisateur. Il existe également une action de masse pour le faire sur plusieurs utilisateurs en même temps.

Une fois l'authentification Azure Active Directory activée sur un utilisateur, il doit obligatoirement cliquer sur le bouton "Se connecter avec Azure" pour accéder à l'application. Il sera alors redirigé vers le site Microsoft qui gère l'authentification puis redirigé vers l'application.



The image shows a login form with the following elements:

- A text input field for email or username, preceded by a person icon.
- A text input field for password, preceded by a lock icon.
- A link labeled "Mot de passe oublié ?" (Forgot password?) located below the password field.
- A blue button labeled "Se connecter" (Log in).
- A dark blue button labeled "Se connecter avec Azure" (Log in with Azure), which includes the Windows logo icon.