DOCUMENTATION / SUPPORT DE FORMATION

Table des matières

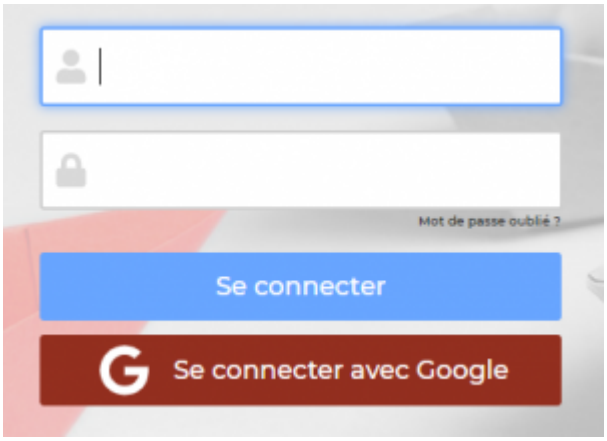
Authentifications externes

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.

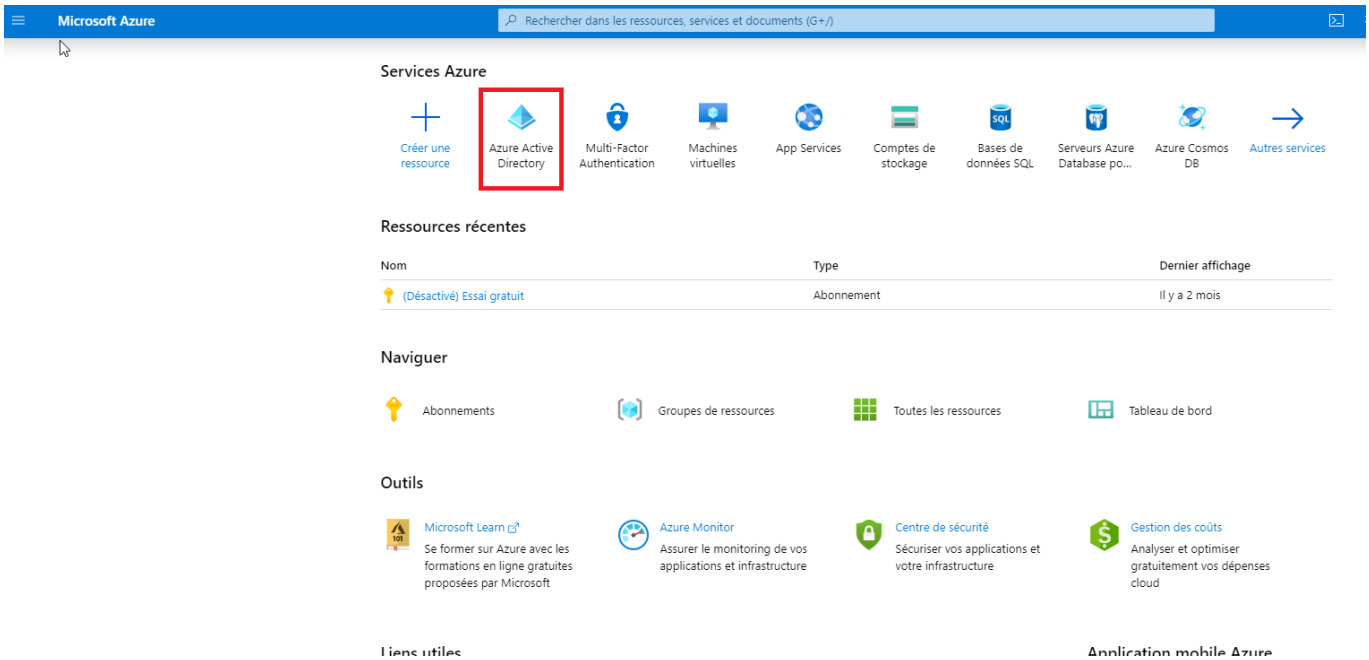
Cette méthode permet à vos utilisateurs de ne pas avoir à mémoriser ou gérer un autre identifiant et mot de passe pour l'accès à l'application.

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.

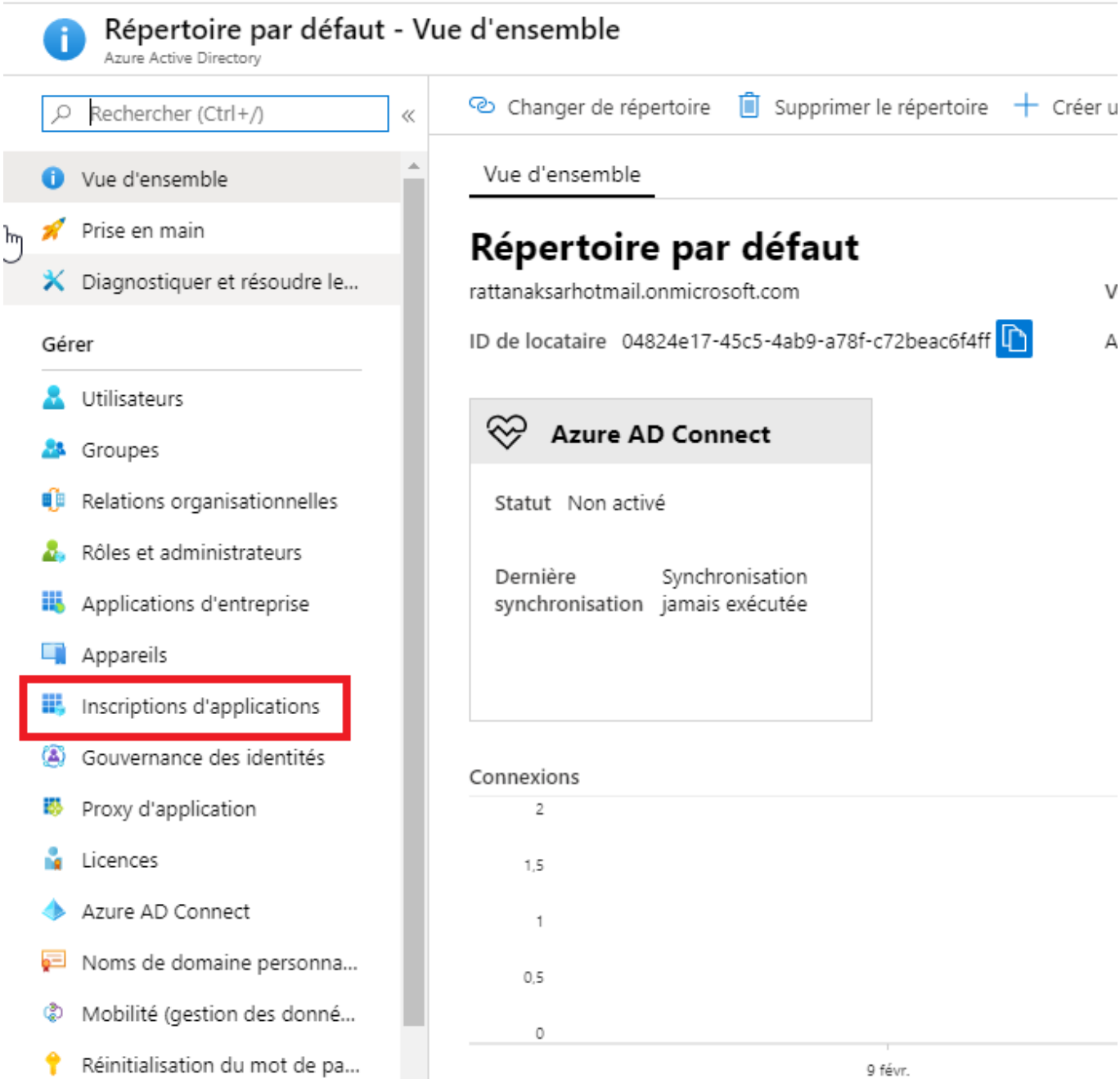
Authentification via le portail Web

Depuis la console Microsoft Azure

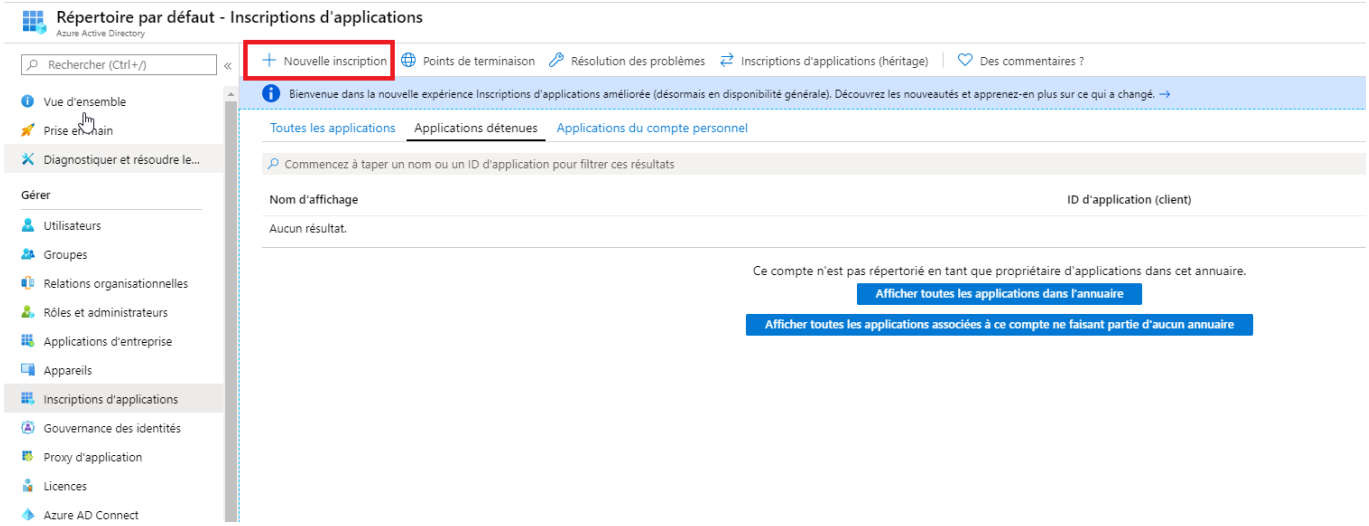


Depuis votre console Azure, cliquez sur Azure Active Directory dans les items à gauche.

Cliquez ensuite sur l'onglet Inscriptions des applications.

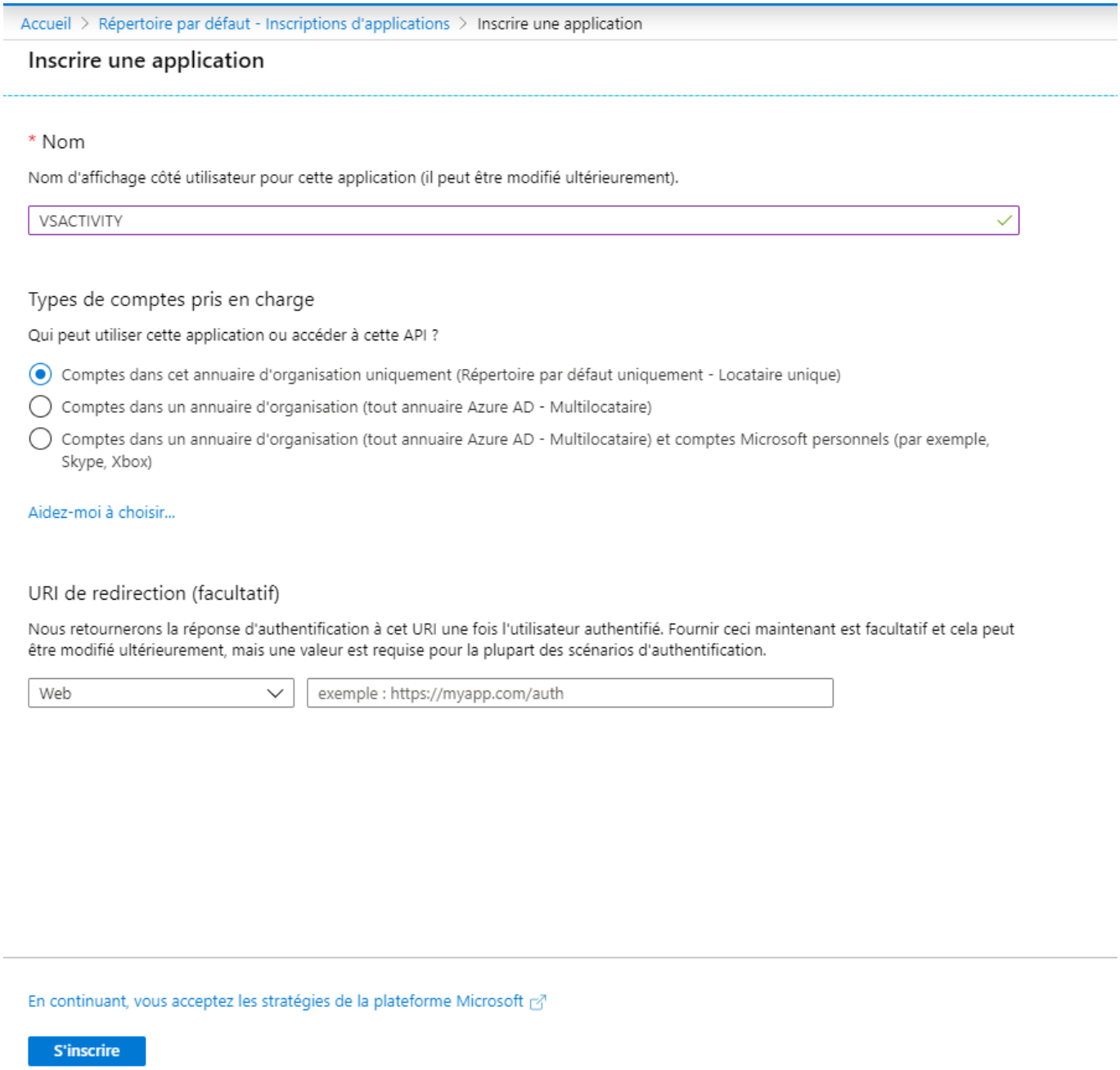


Cliquez sur + Nouvelle Inscription d'application en haut de l'interface pour ajouter une application à votre tenant Azure AD.

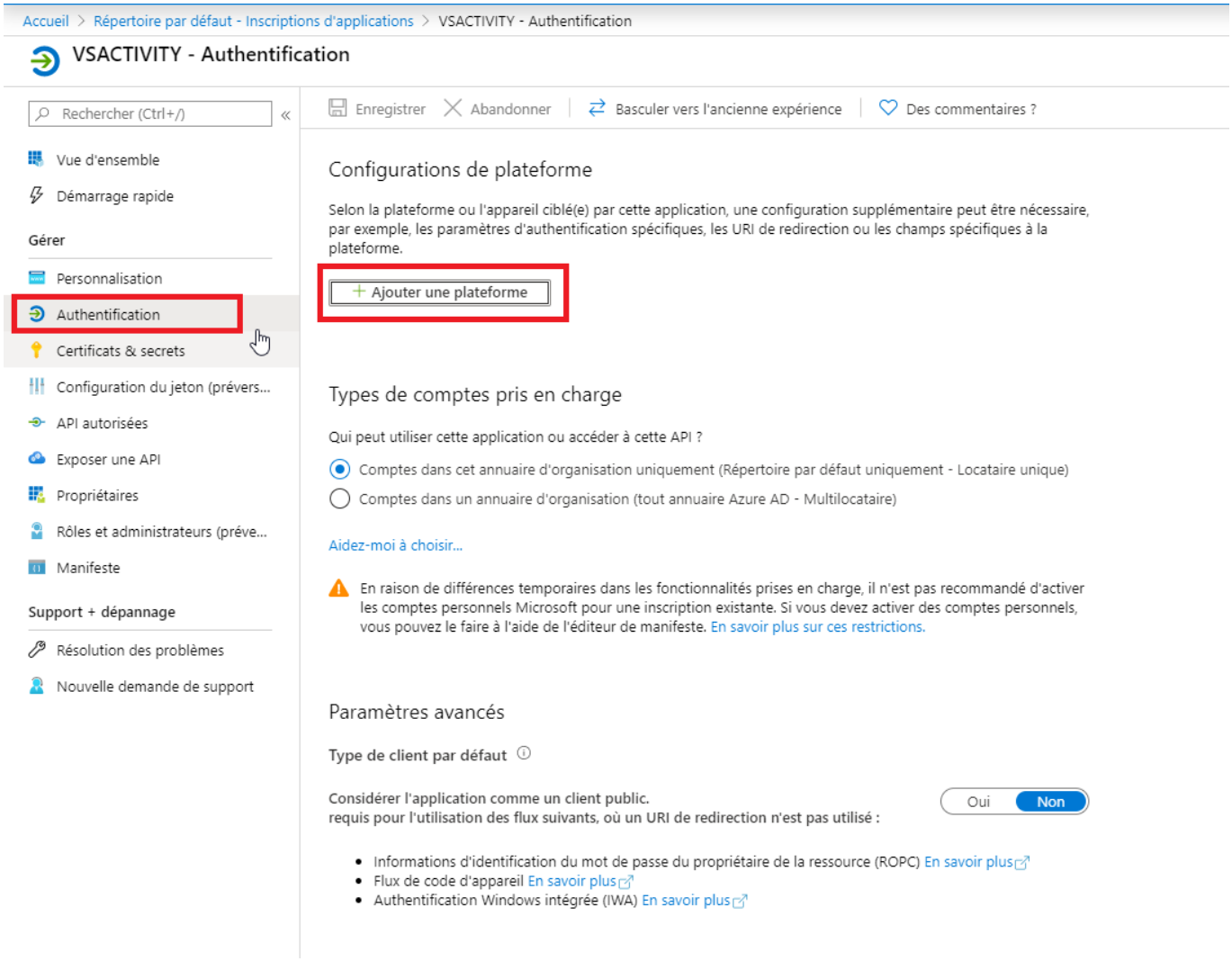


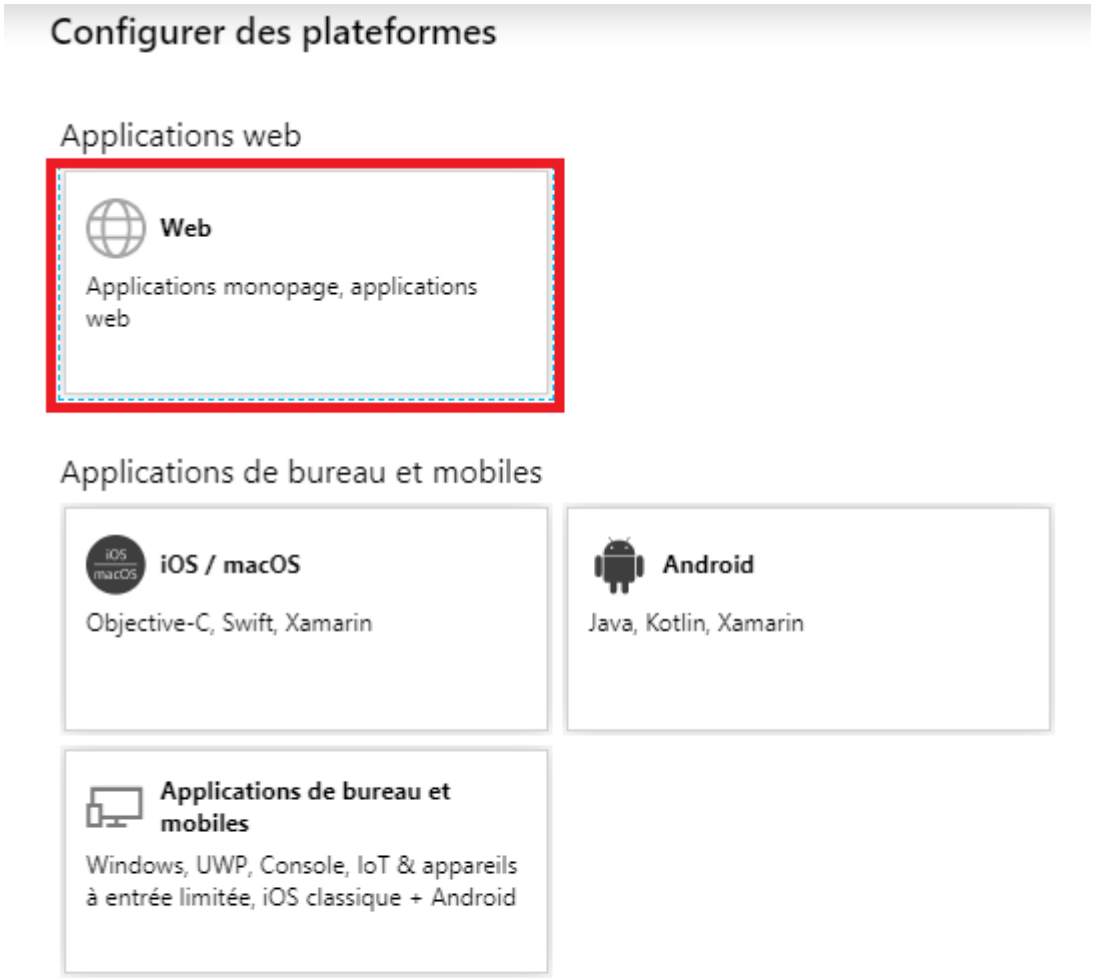
Remplissez les informations demandées :

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

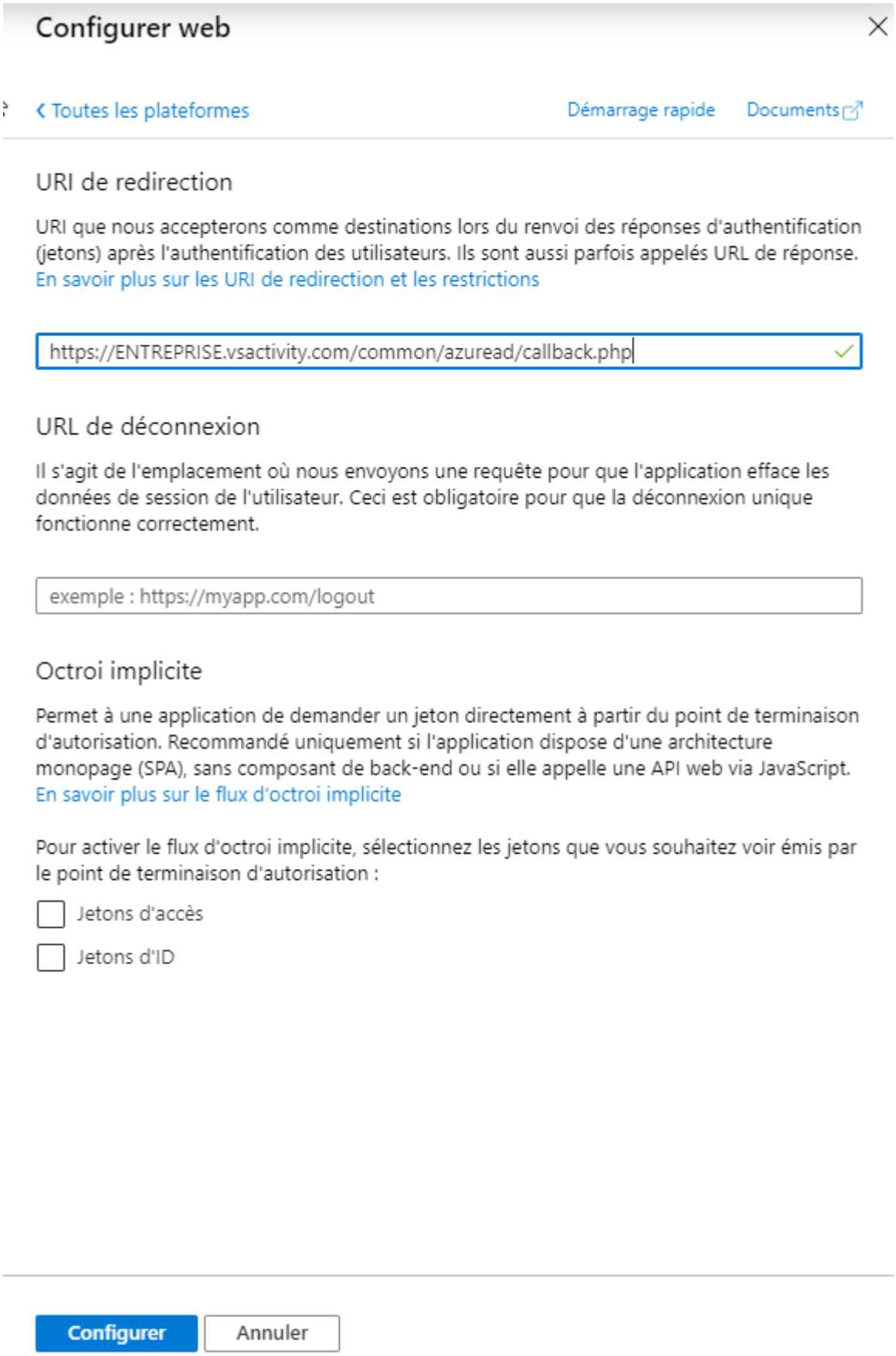


Une fois l'application créée, cliquez sur Authentification situé dans la partie droite puis sur le bouton Ajouter une plateforme ⇒ Applications Web



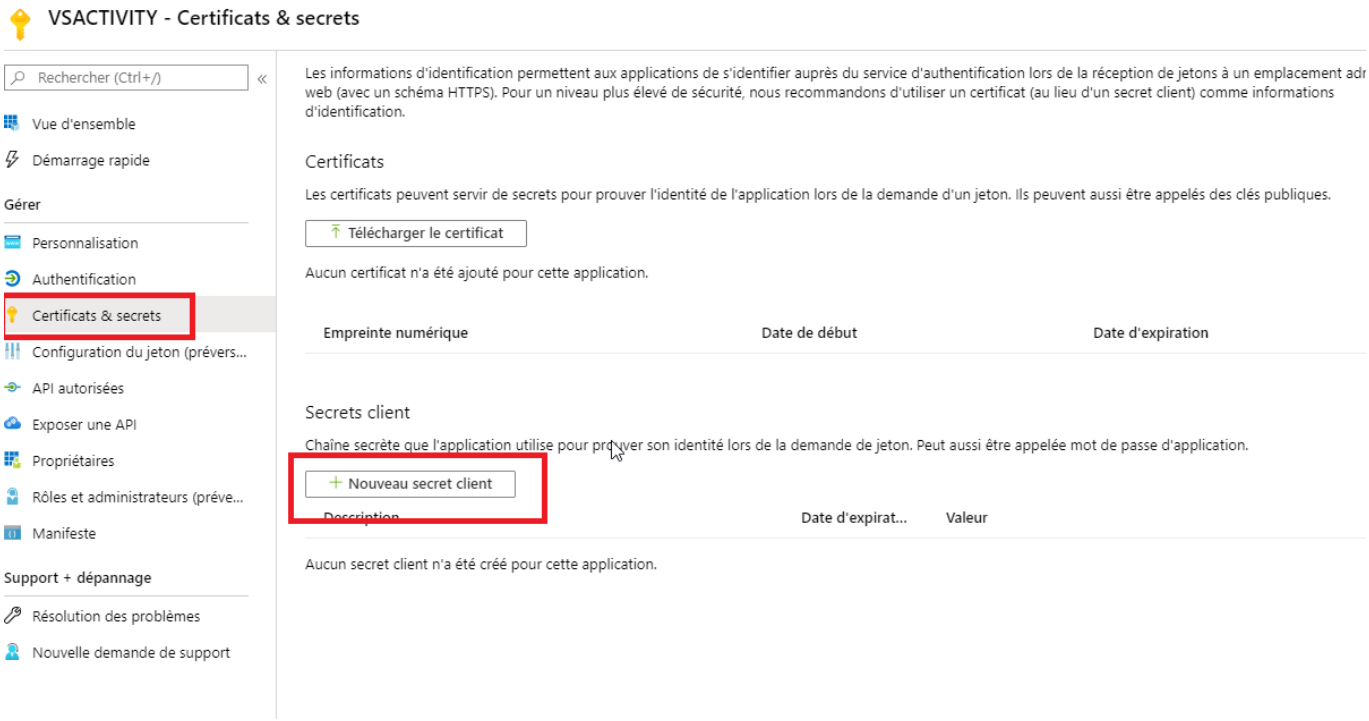


Une fois que vous êtes dans « Configurer WEB » vous devez ajouter dans le champ URI de redirection l'URL suivante : https://ENTREPRISE.vsactivity.com/common/azuread/callback.php

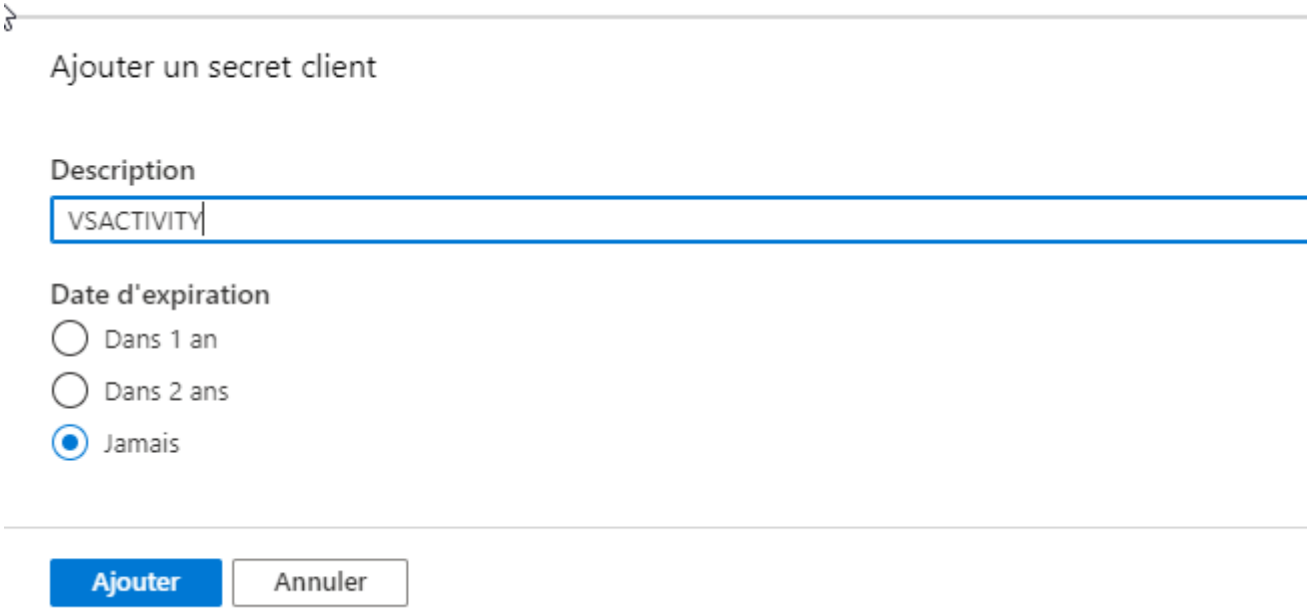


Remplacez ENTREPRISE par le préfixe de l'url d'accès à votre environnement.

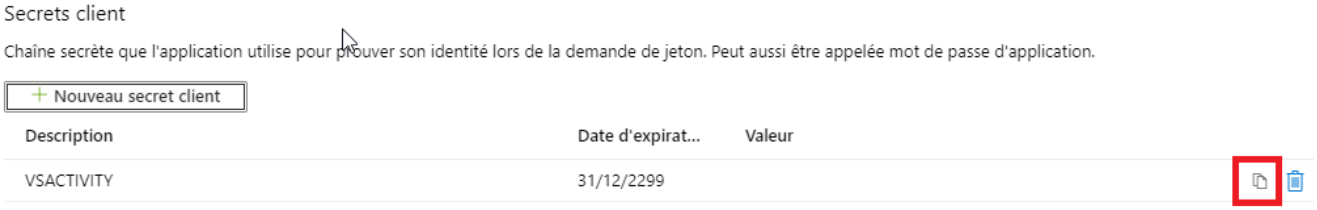
Vous devez ensuite aller sur « Certificats & Secrets » puis cliquer sur « Nouveau secret client“



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



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



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

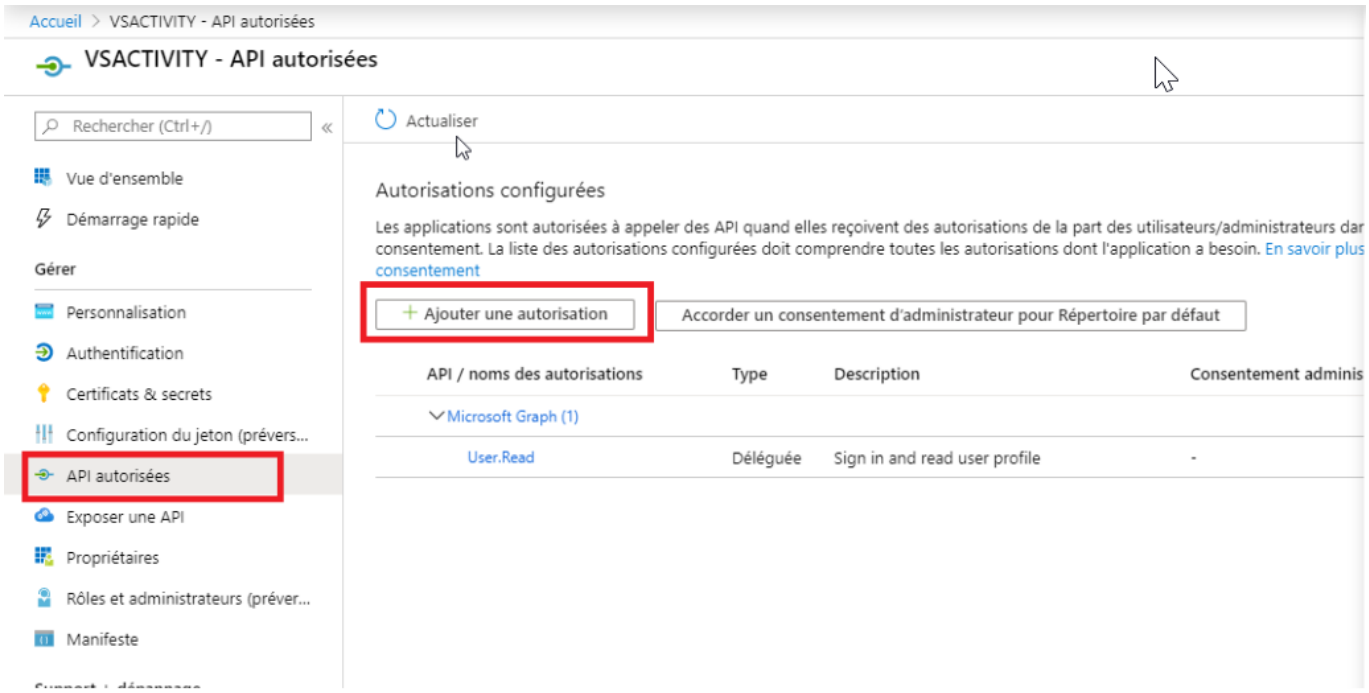
Si vous avez raté la clé, vous pouvez en générer une nouvelle et supprimer l'ancienne.

La sécurité et les autorisations d'accès

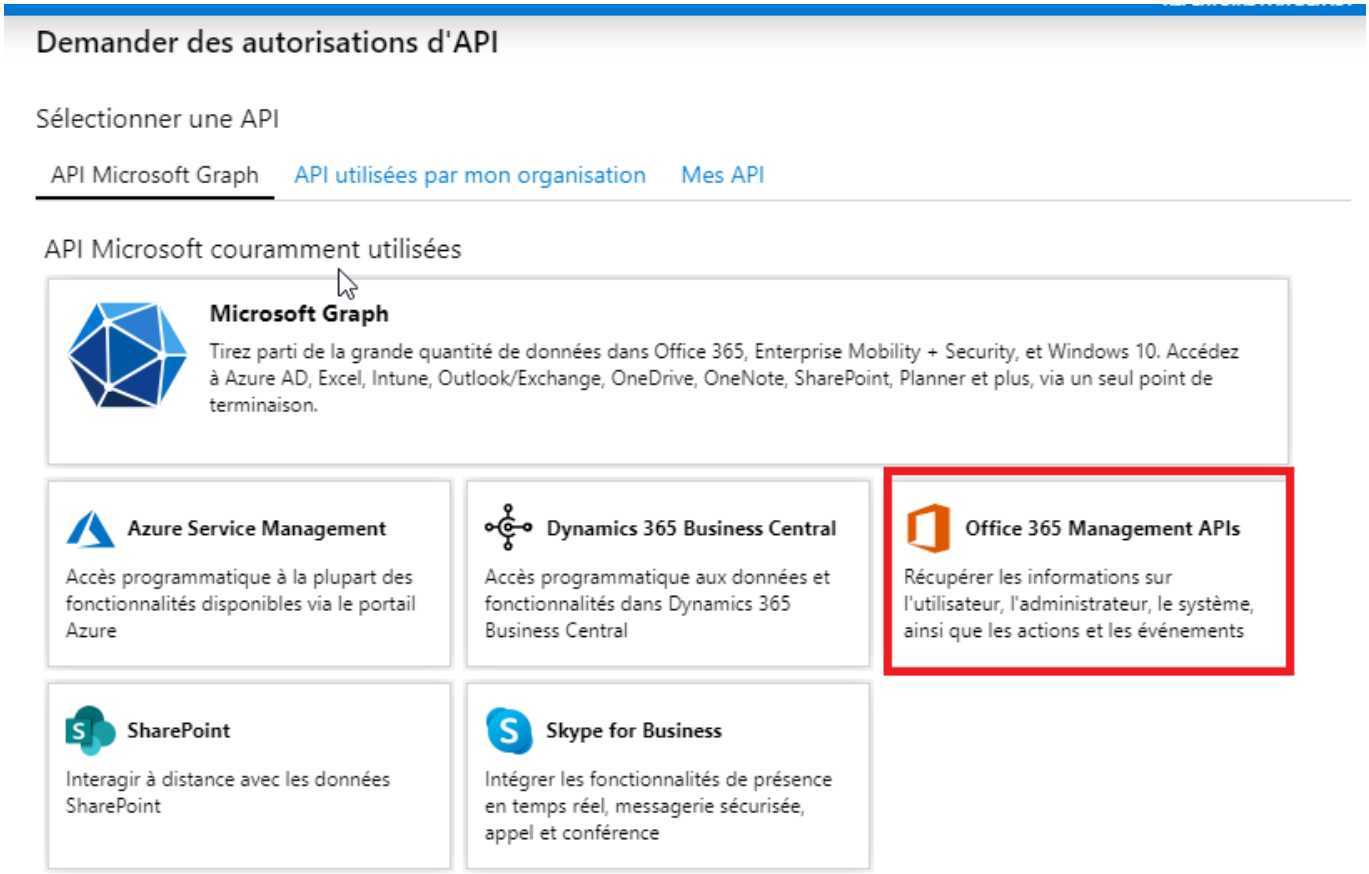
Une fois l'application créée, il est nécessaire d'ajouter des autorisations pour que vos utilisateurs puissent se connecter à l'application depuis votre tenant Azure AD.

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

Cliquez sur « Ajouter une autorisation »

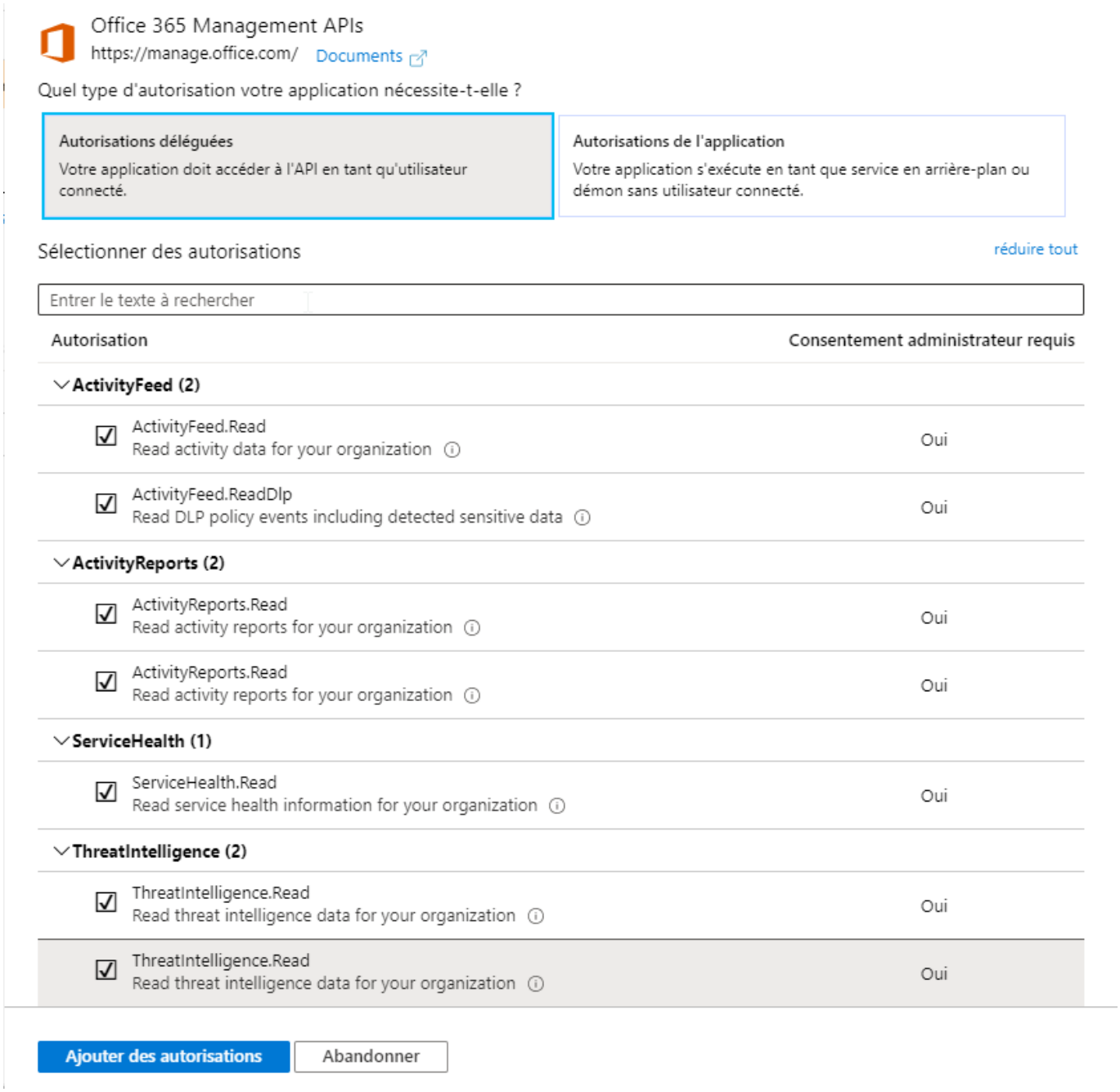


Cliquez sur Office 365 Management Apis.

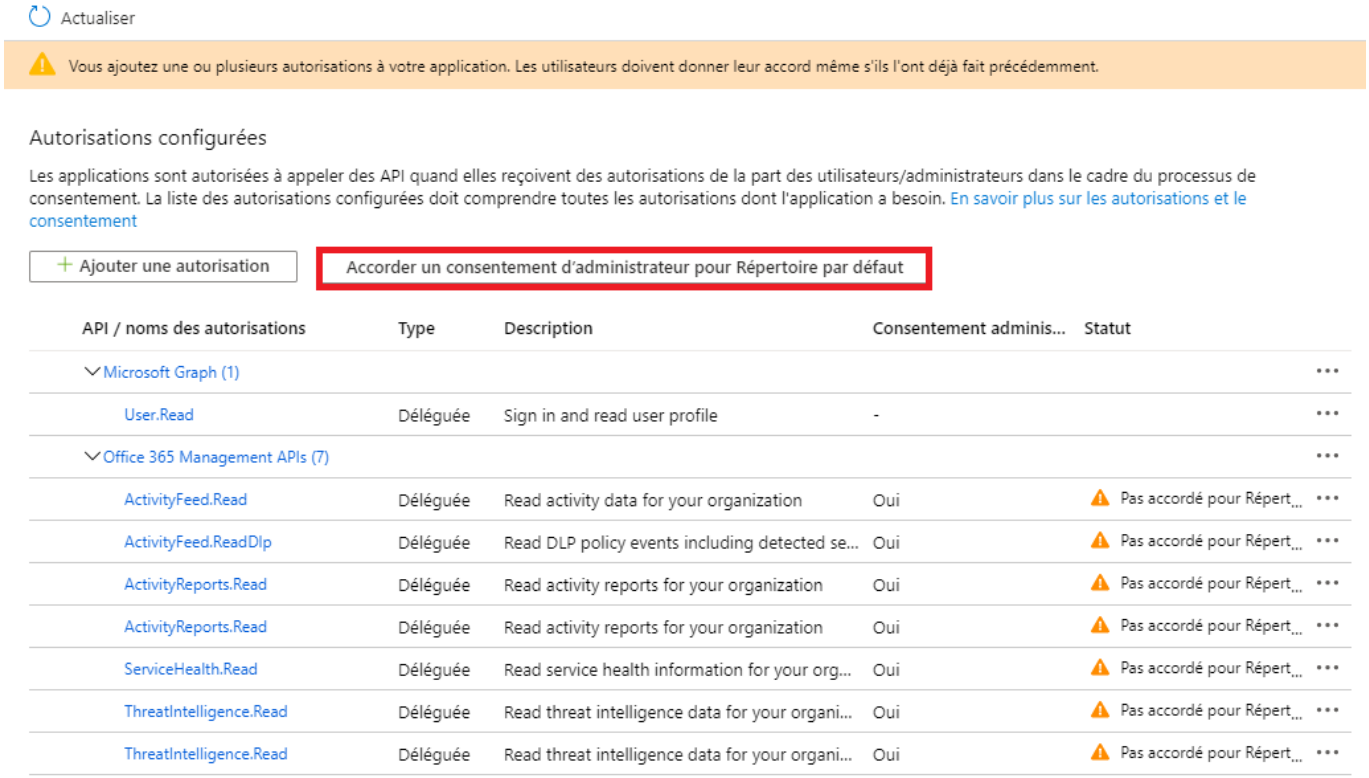


Cliquez sur Autorisations de l'application et Autorisations déléguées pour donner l'accès en lecture.

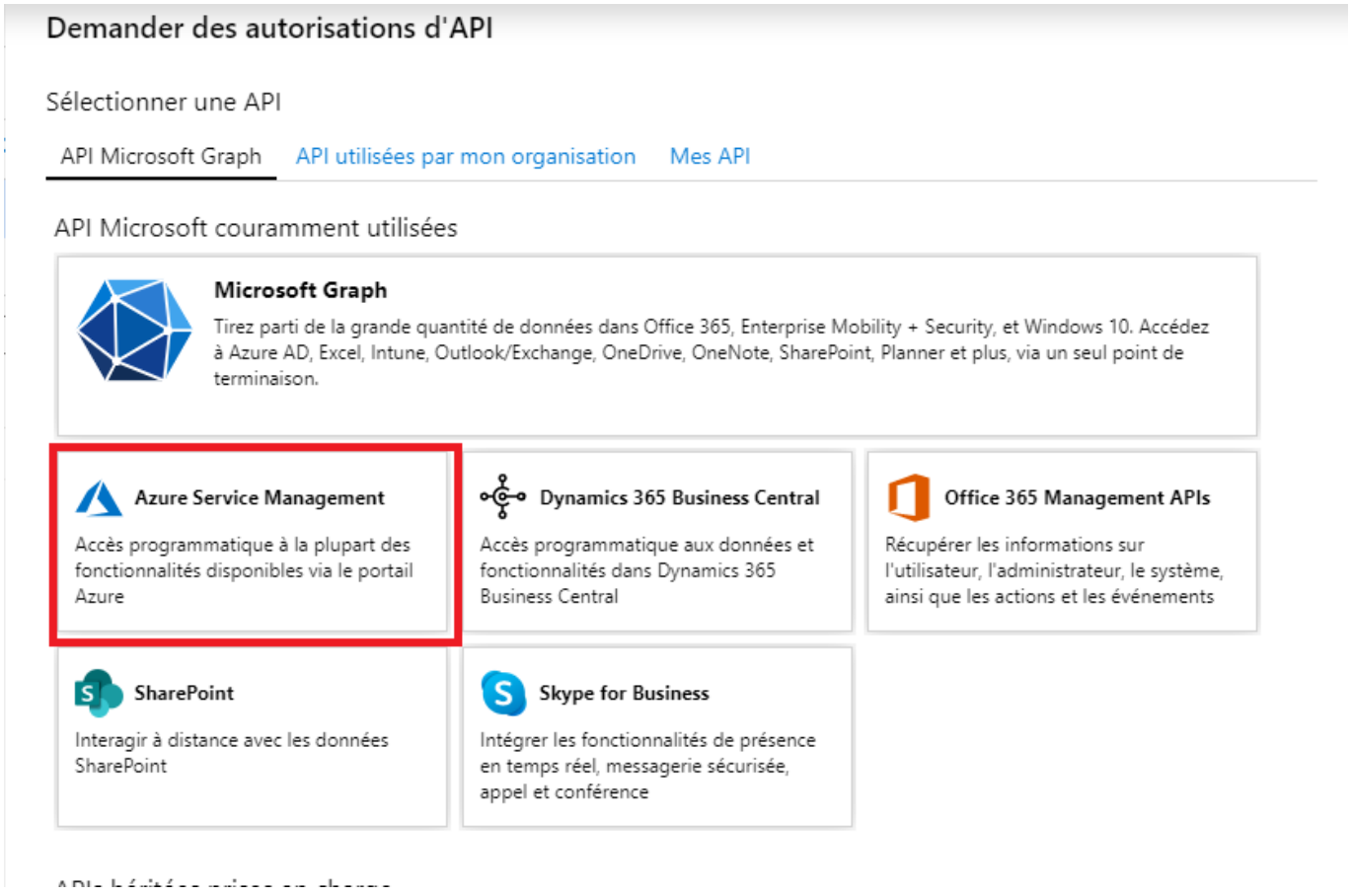
Vous devez cliquer sur les deux boutons « Autorisations déléguées » puis sur le bouton « Ajouter des autorisations »



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



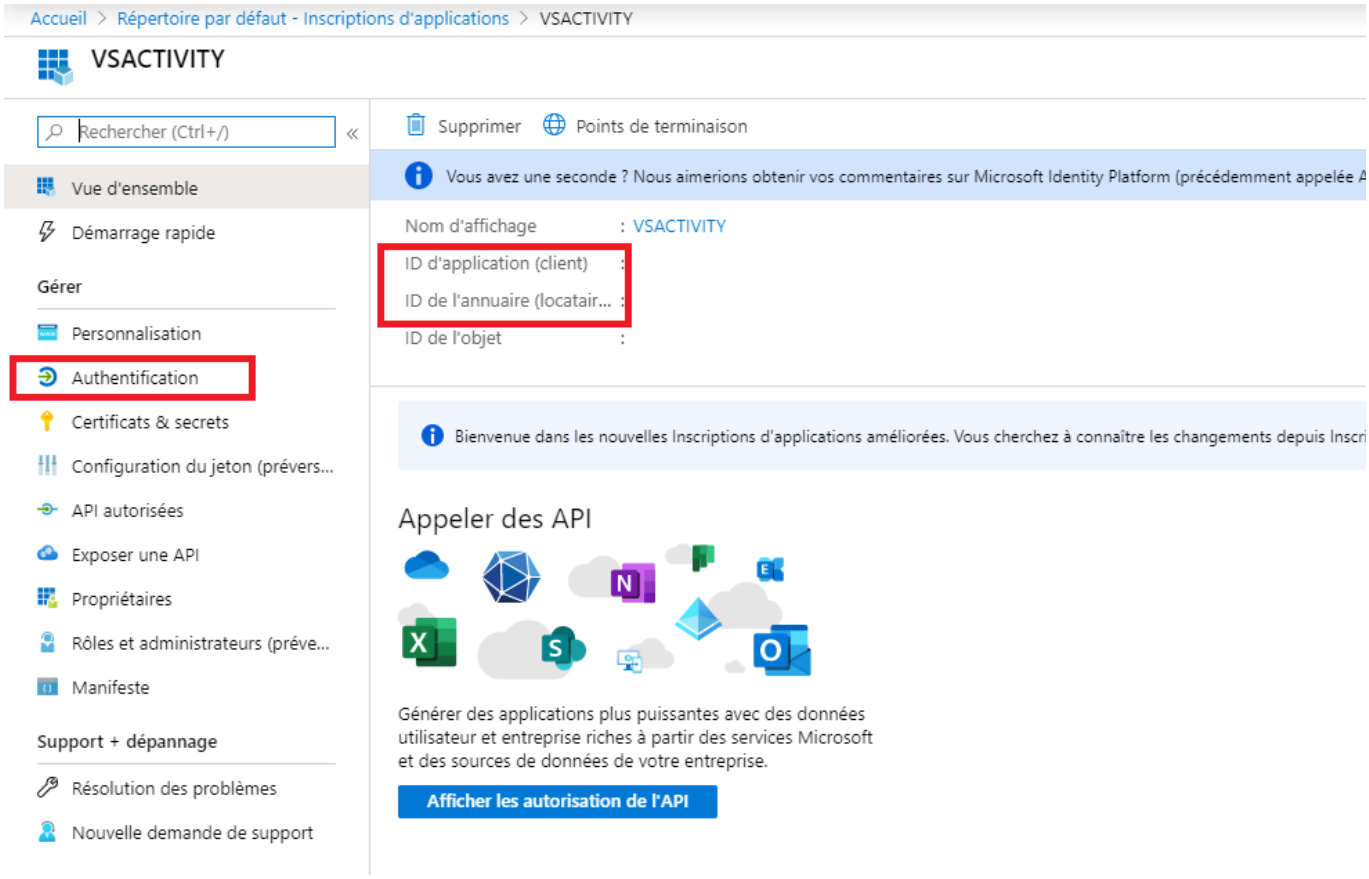
Répétez l'opération 1 fois pour ajouter l'APIs " **Azure Service Management API**"



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)



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 crée 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

Administration > Utilisateur

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.