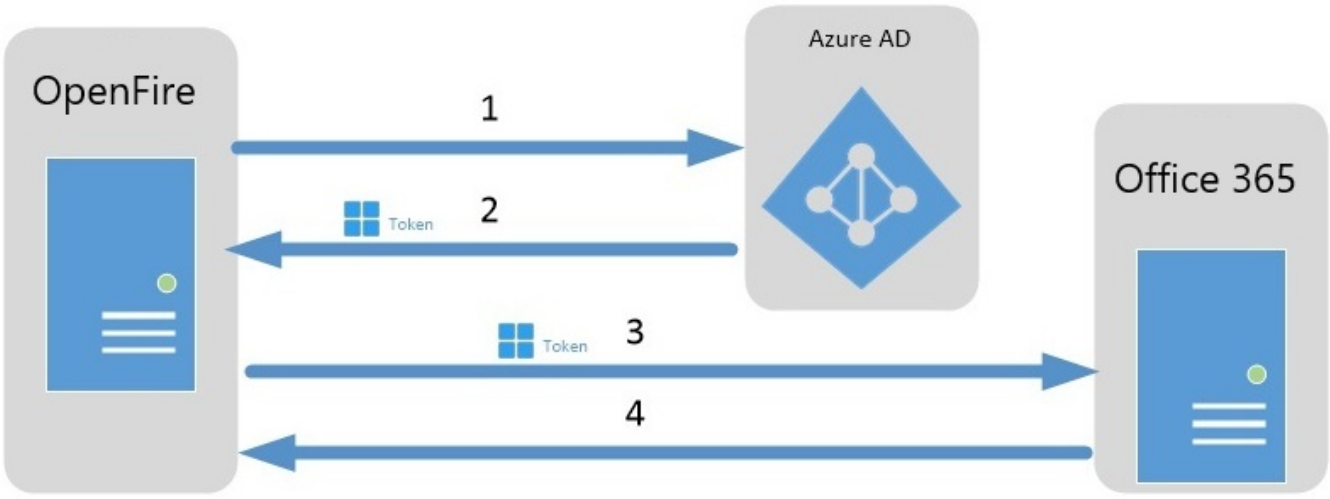
OpenFire
ZA La Brosse – 5 rue de la Garenne
35520 La Chapelle des Fougeretz
France

Authentification Azure pour Office 365

Dans le cadre des nouvelles mesures de sécurité de Microsoft pour les comptes Office 365, l'utilisation d'une authentification forte est désormais obligatoire pour la connexion des serveurs de courrier.

Dans cette optique, OpenFire offre désormais la possibilité d'utiliser la solution Azure OAuth de Microsoft pour authentifier les comptes Office 365.

Ce protocole permet l'utilisation de jeton d'autorisation (Token) pour donner accès à un utilisateur, à la place des informations d'identification habituelle (Identifiant et mot de passe):



Cette configuration passe par la création et la configuration d'une "Application OpenFire" dans l'outil Azure de Microsoft. Vous trouverez ci-dessous l'ensemble des démarches nécessaires à ce fonctionnement.

Prérequis

L'utilisation de l'authentification via Azure nécessite **l'installation d'un module spécifique** sur OpenFire. Ainsi, avant toute configuration, merci de contacter le support OpenFire à l'adresse mail support@openfire.fr ou par téléphone au 02.30.96.02.65 afin de demander l'installation de ce module.

Une fois confirmation que le module est installé, la configuration sera à effectuer sur Office 365.

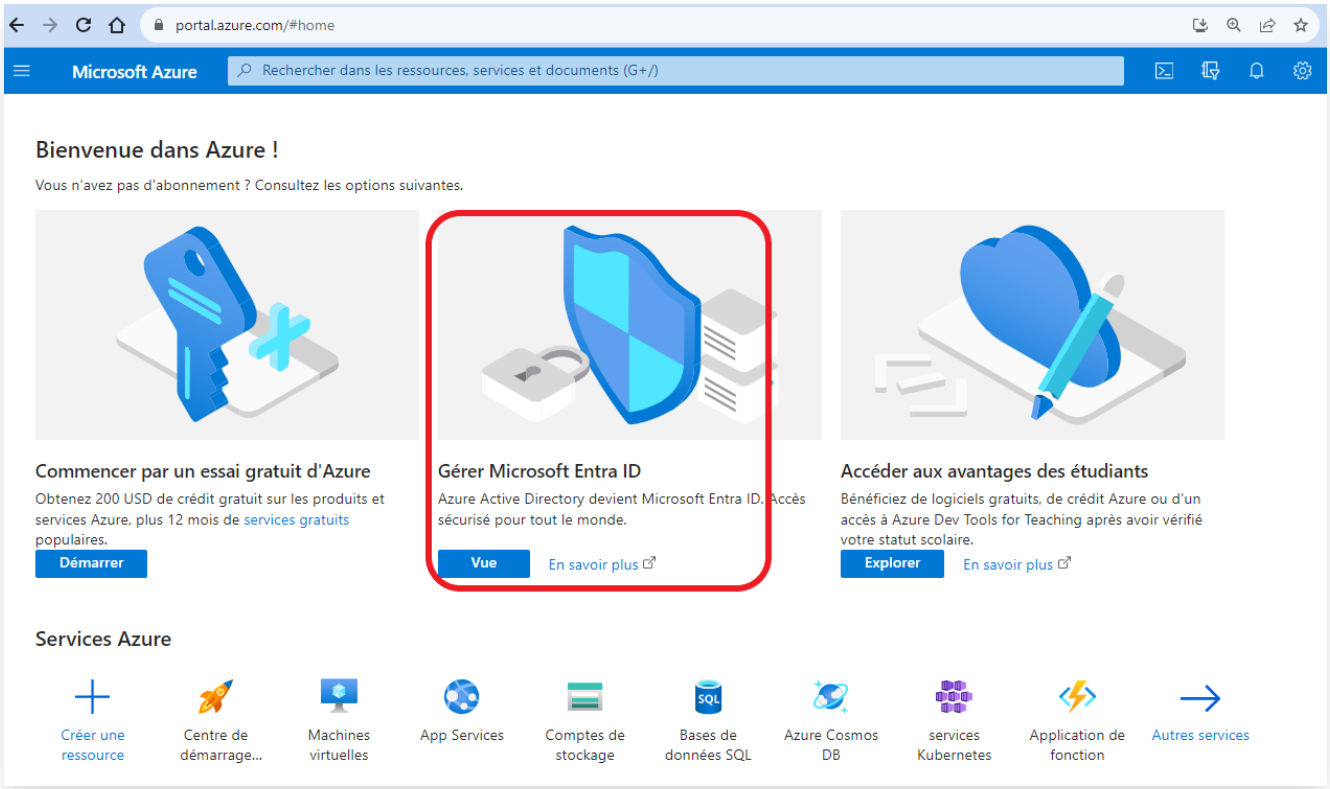
Pour cela, deux portails sont mis à disposition des utilisateurs Office 365.

- Le centre d'administration Microsoft 365 : pour y accéder, rendez-vous sur le site https://admin.microsoft.com/adminportal/home
- Le portail Azure, disponible à l'adresse https://portal.azure.com

La configuration est à effectuer à l'aide d'un compte disposant des droits Administrateur sur Office 365. Dans l'idéal, il faut que ce soit également ce compte qui soit configuré en tant que serveur SMTP sur OpenFire. Si c'est le cas, la dernière étape de cette procédure n'est alors pas nécessaire.

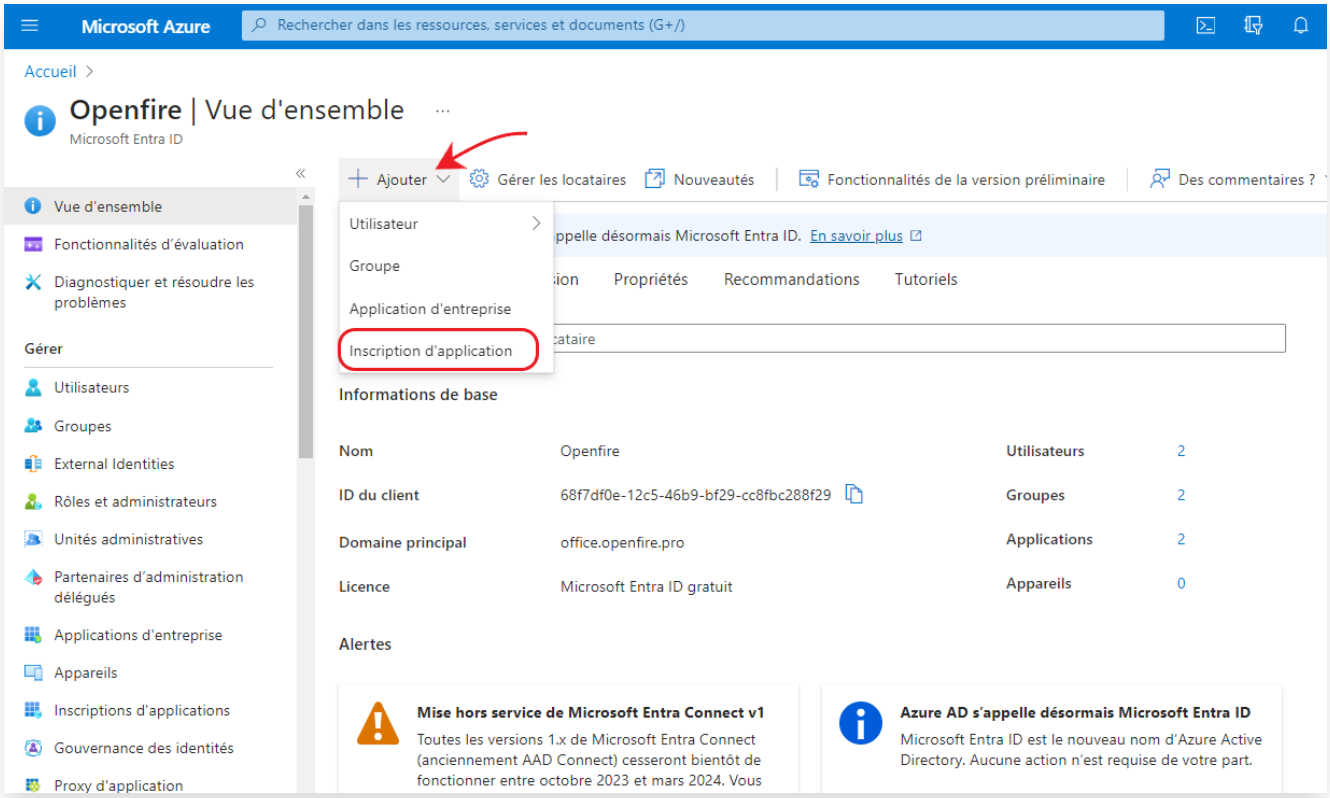
Étape 1 : Création de l'application OpenFire sur Azure

Pour commencer, avec votre compte administrateur, rendez-vous sur le portail Azure et cliquez sur l'icone Microsoft Entra ID*



** Si cette icone n'apparait pas, cliquez alors sur Autres Services puis rechercher Microsoft Entra ID*

Cliquez ensuite sur Ajouter puis sélectionnez l'option Inscription d'application.

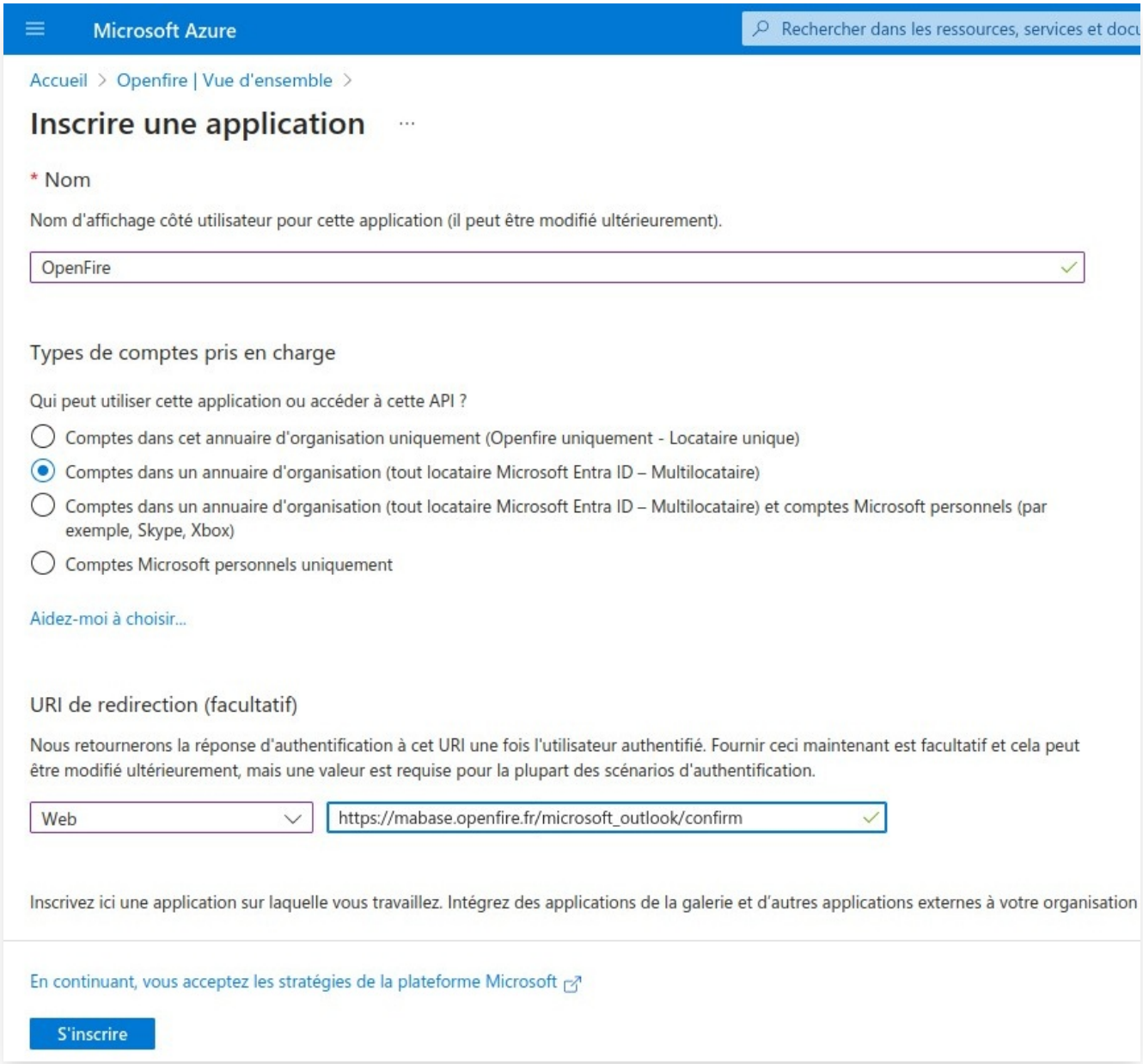


Dans la fenêtre suivante, saisissez les valeurs suivantes :

- Nom : OpenFire
- Cochez le type de compte Comptes dans un annuaire d'organisation (Tout annuaire Microsoft Entra ID - Multilocataire)

URL de redirection : sélectionnez Web puis saisissez l'URL suivante :

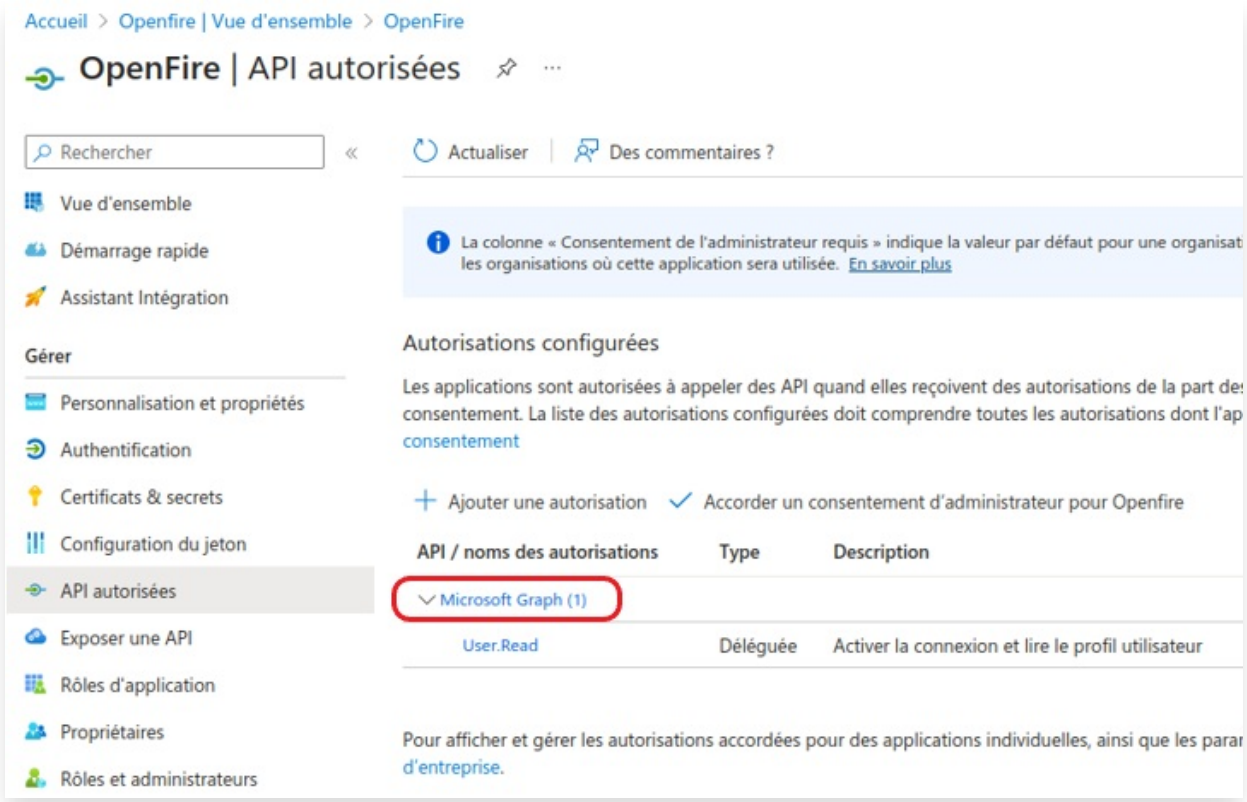
https://**mabase.openfire.fr**/microsoft_outlook/confirm (en remplaçant la valeur en bleue par l'url de votre baseOpenFire).



Cliquez sur S'inscrire.

Vous serez alors redirigé vers la page d'administration de l'application OpenFire que vous venez de créer.

Cliquez ensuite sur API autorisées dans le menu de gauche, puis cliquer sur Microsoft Graph *

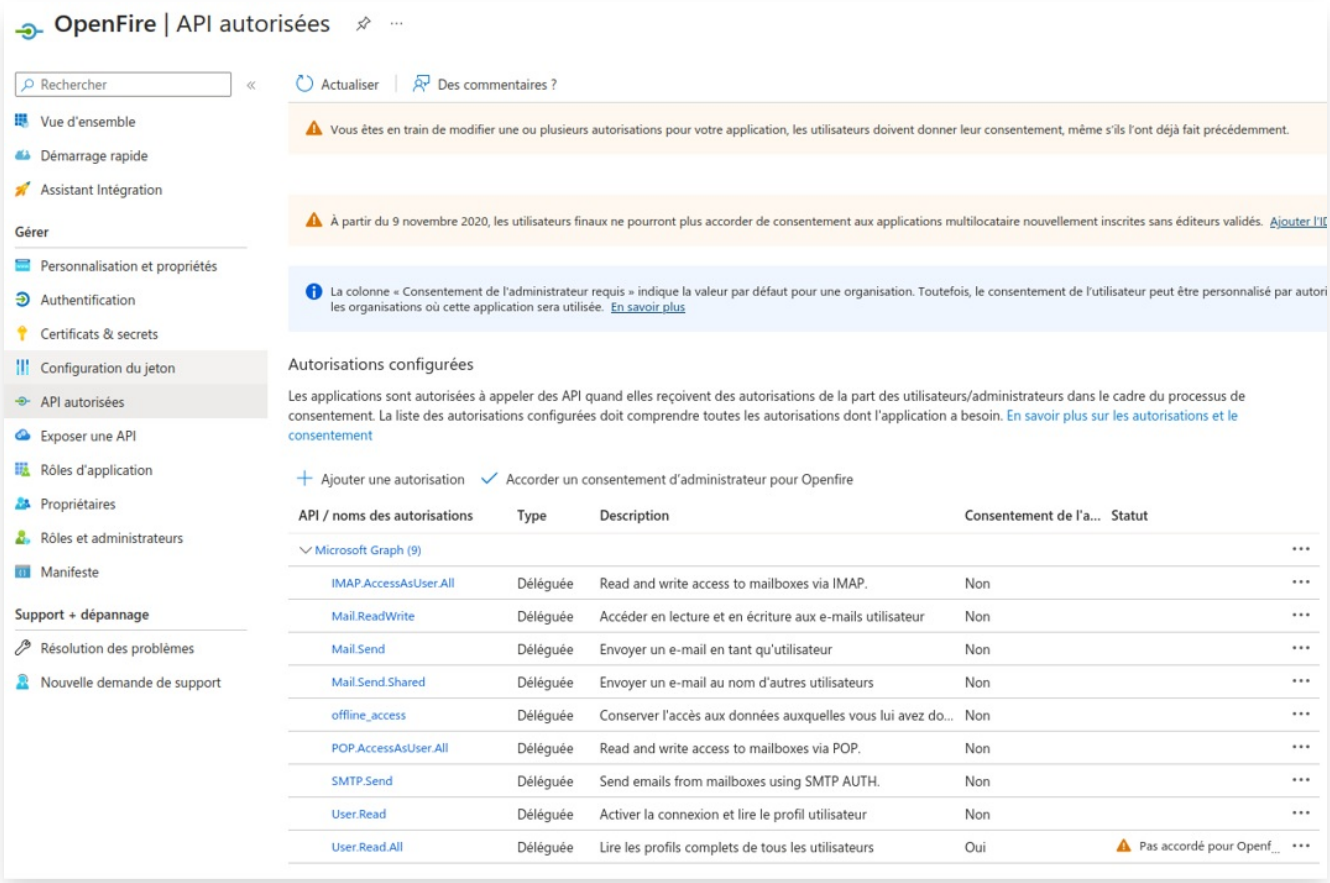


** Si Microsoft Graph n'est pas visible, créez-le en cliquant sur Ajouter une autorisation puis Autorisation déléguées.*

Dans la fenêtre ainsi ouverte, sélectionner les droits suivants:

- User.read (sélectionné par défaut)
- User.Read.All
- Mail.Send
- Mail.Send.Shared
- Mail.ReadWrite
- Offline_access
- SMTP.Send
- Pop.AccessAsUser.all
- Imap.AccessAsUser.all

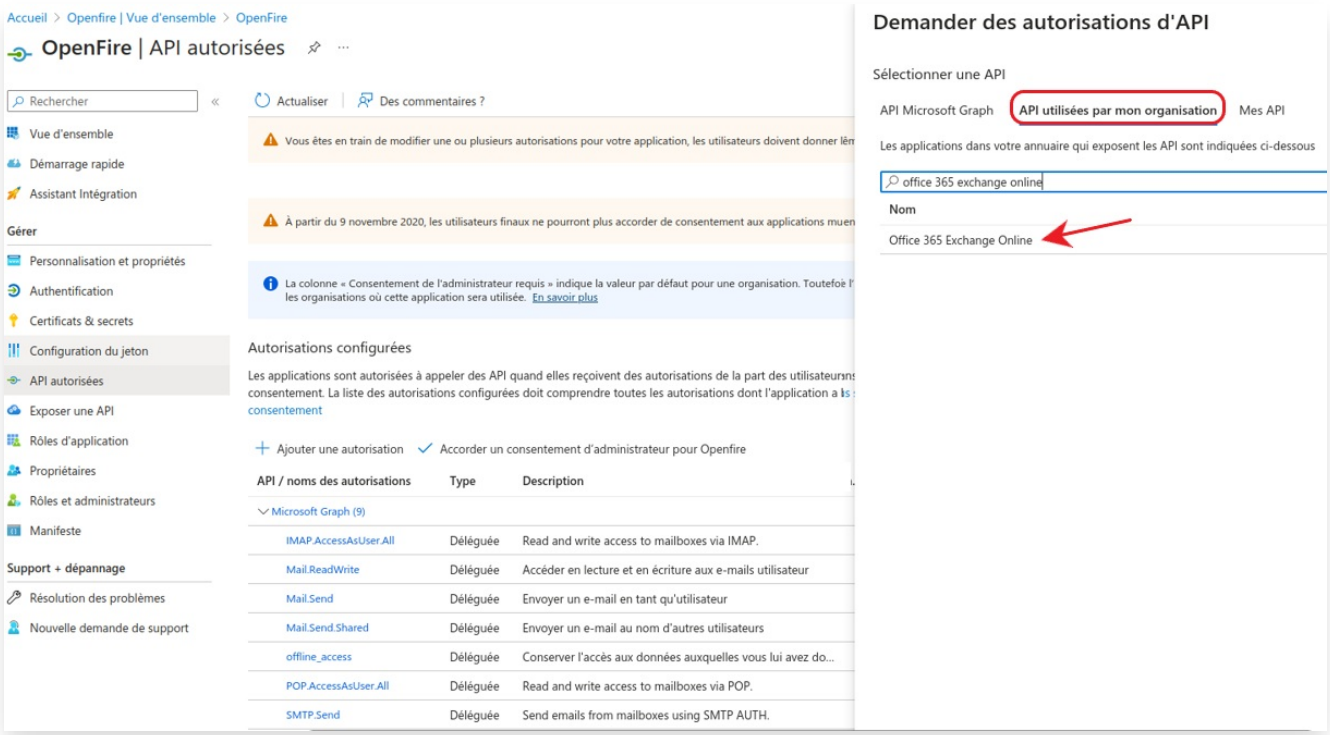
Ce qui devrait donner :



Ensuite, cliquez de nouveau sur Ajouter une Autorisation, puis sur Api utilisées par mon organisation

Cela permettra d'ajouter des droits additionnels.

Tapez: Office 365 Exchange Online



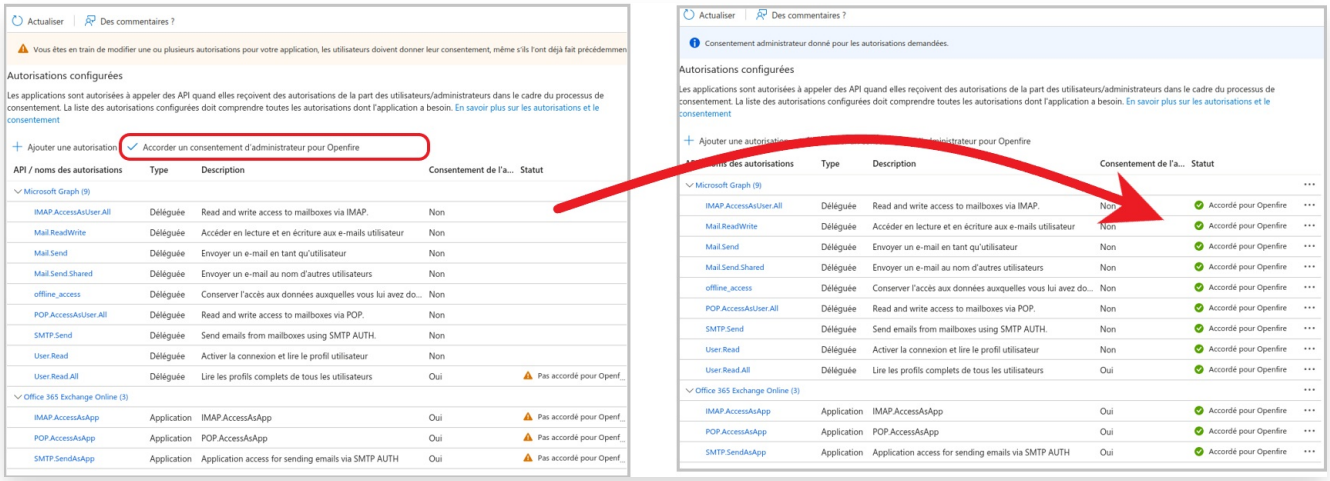
Cliquez sur Office 365 Exchange Online > Autorisations d'applications

Et ajoutez les droits suivants:

- Imap.AccessAsApp
- POP.AccessAsApp
- SMTP.SendAsApp

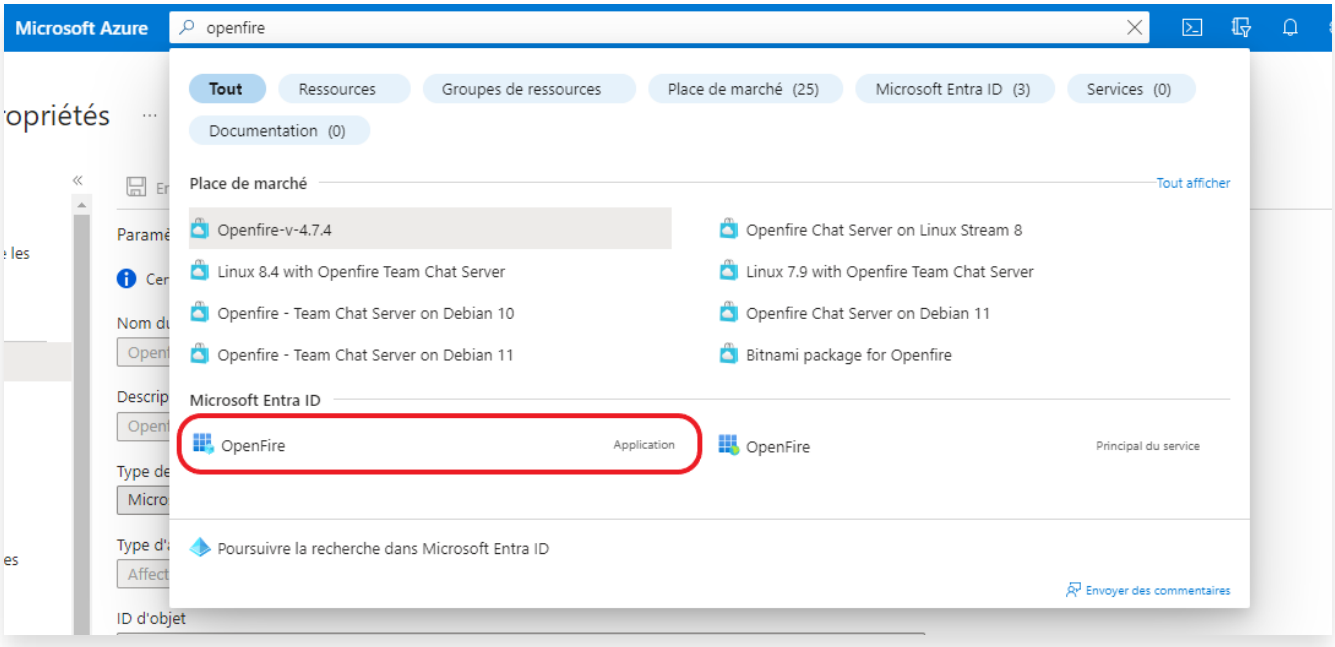
Cliquez ensuite sur Accorder un consentement d'administrateur pour Openfire.

Cette option permet d'ajouter les droits à tous les utilisateurs.



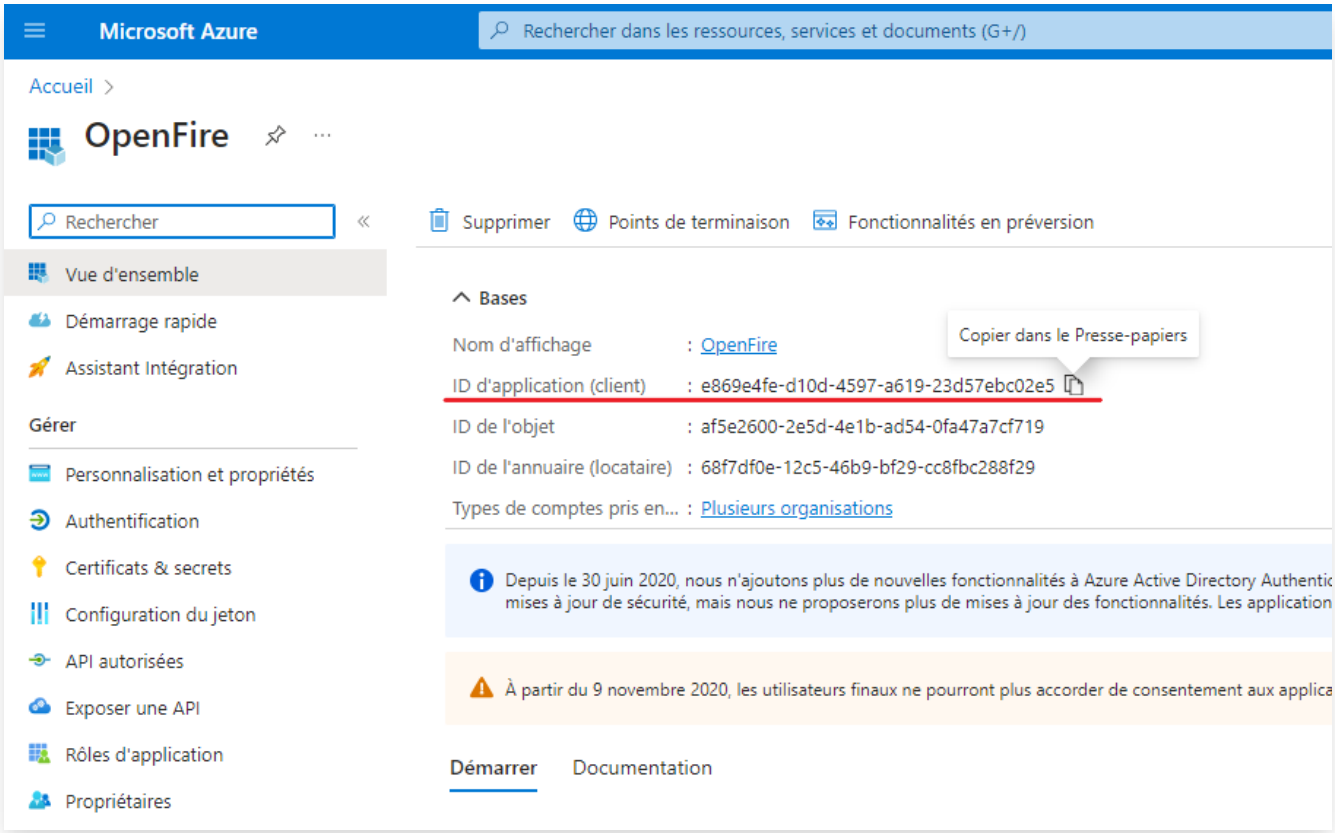
Étape 2 : Création de la clé secrète

Cliquez sur la barre de recherche dans Azure, puis recherchez OpenFire et cliquez sur l'icone d'entreprise.



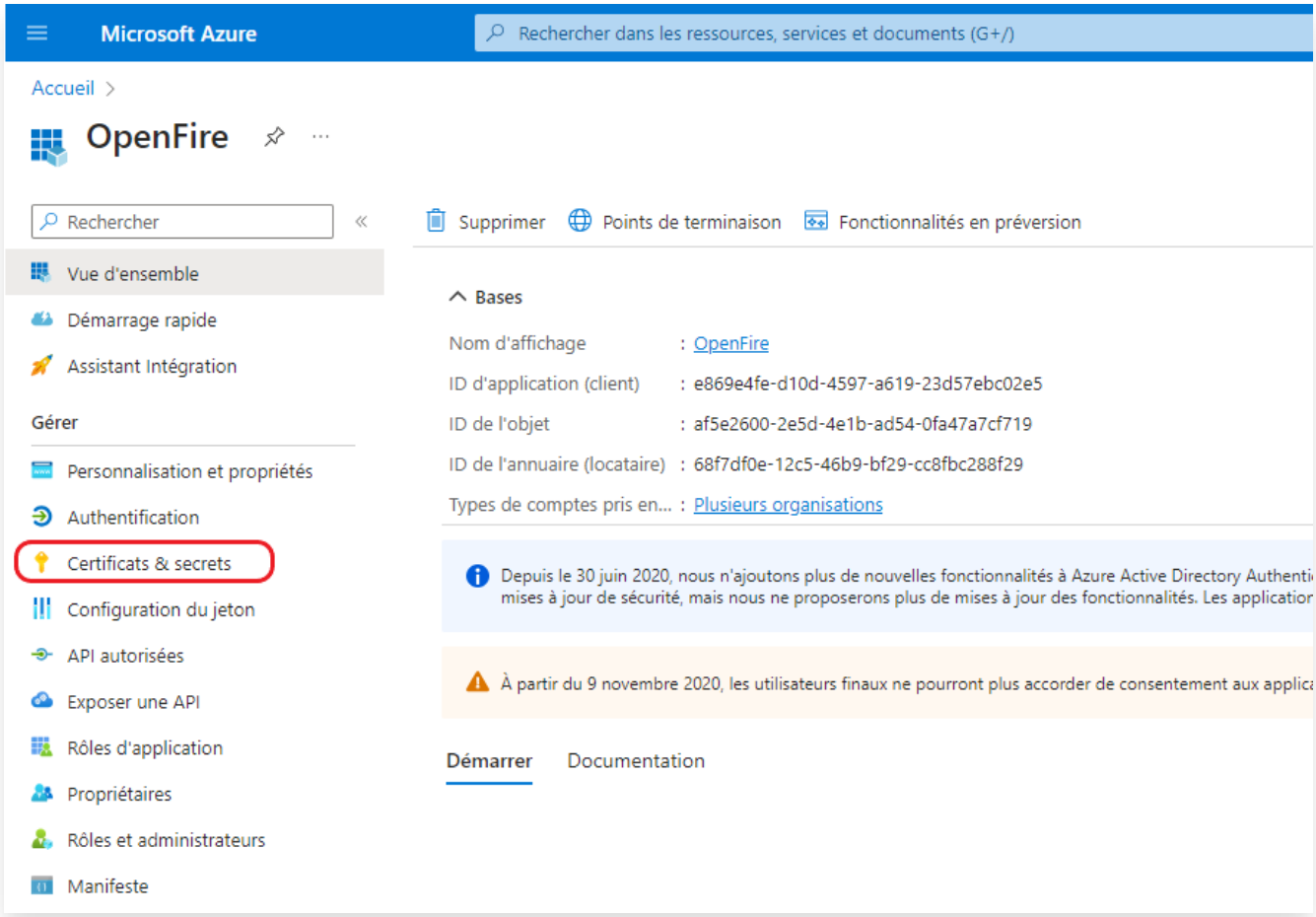
Vous arriverez sur la page d'administration de l'application OpenFire créé dans Azure.

Copiez l'ID de l'application client dans un document texte/bloc-notes afin de le ressaisir ultérieurement dans OpenFire. Cet ID se génère automatiquement à la création de l'application dans Azure.

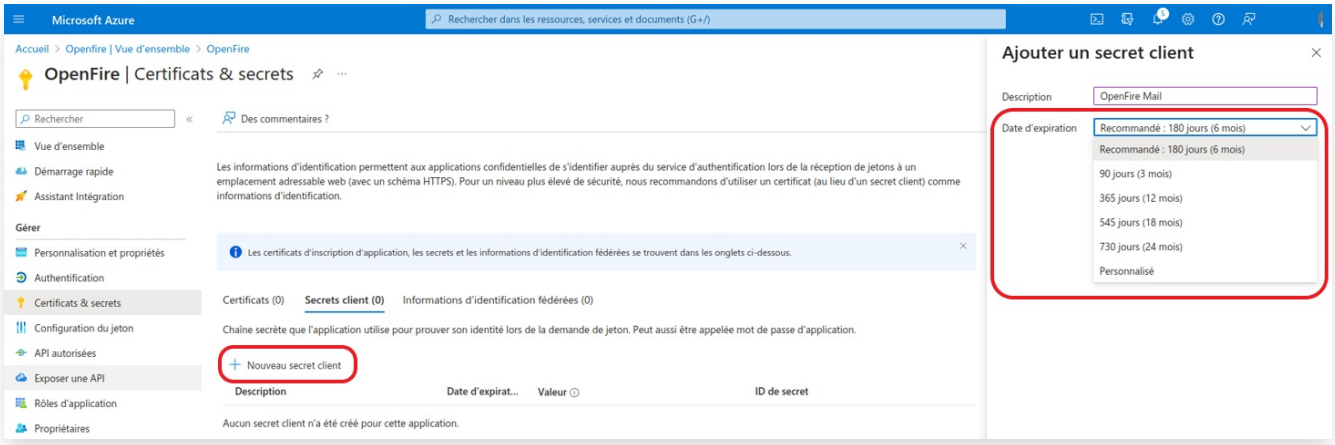


Il faut ensuite générer la clé secrète que l'application va utiliser pour prouver son identité lors de la demande de token.

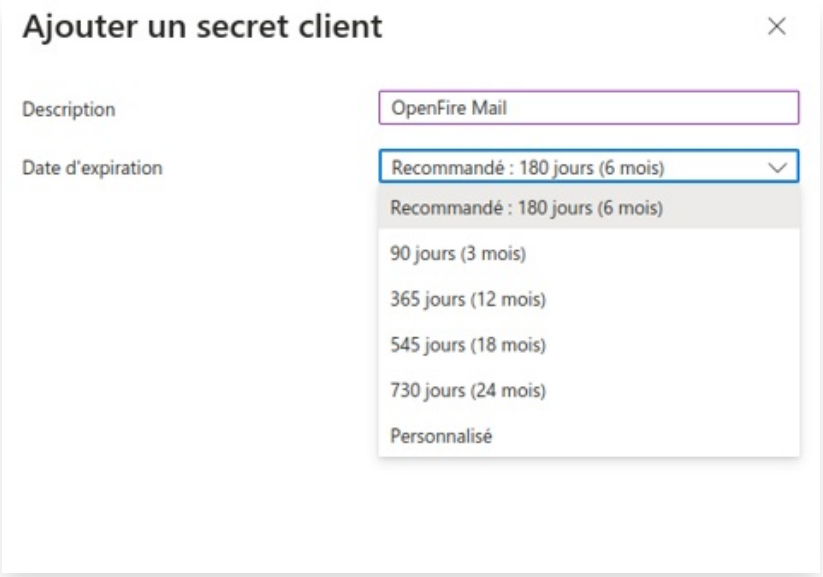
Pour cela, cliquez sur Certificats & Secrets :



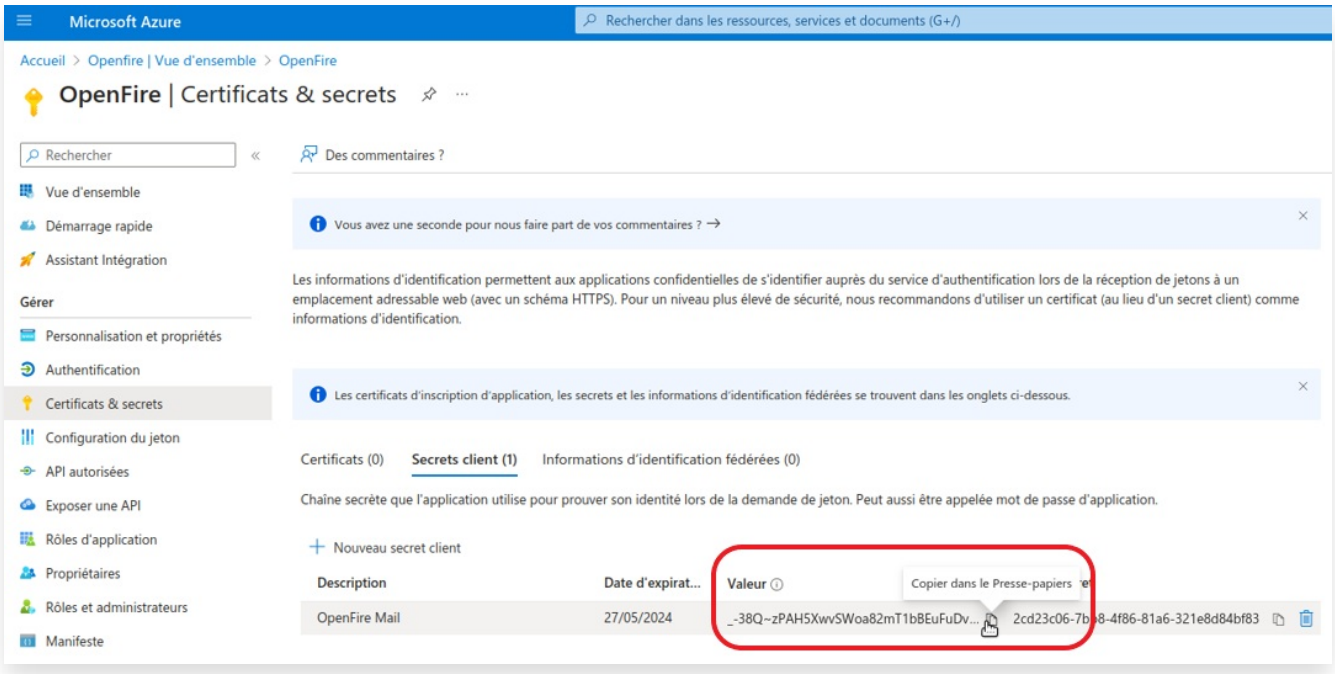
Puis cliquez sur Nouveau secret client et sélectionnez la durée de votre choix :



⚠ Attention la clé sera à récréer au bout de cette durée. Vous pouvez, si vous le souhaitez, sélectionner la durée maximale, 730 jours, afin de ne pas avoir à recréer une clé au bout de 6 mois (valeur par défaut) :



Copiez ensuite la valeur de cette clé secrète dans un document texte/bloc-notes afin de la ressaisir ultérieurement dans OpenFire :



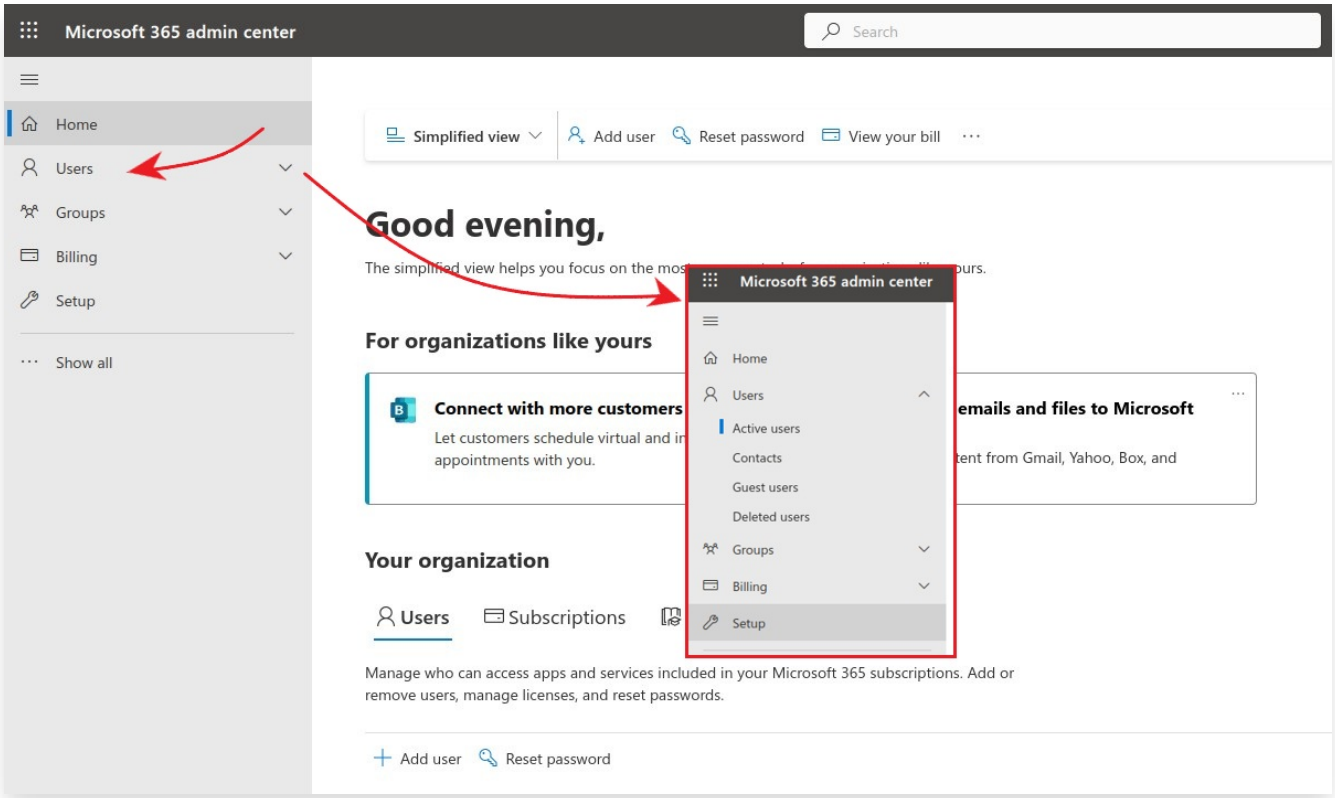
⚠ Attention : la clé ne sera plus affichée après fermeture de la fenêtre Microsoft Azure. En effet, la valeur de la clé secrète client n'est visible qu'immédiatement après la création. Veillez donc à bien enregistrer la clé avant de quitter la page.

Étape 3 : Ajout des Permissions Utilisateurs

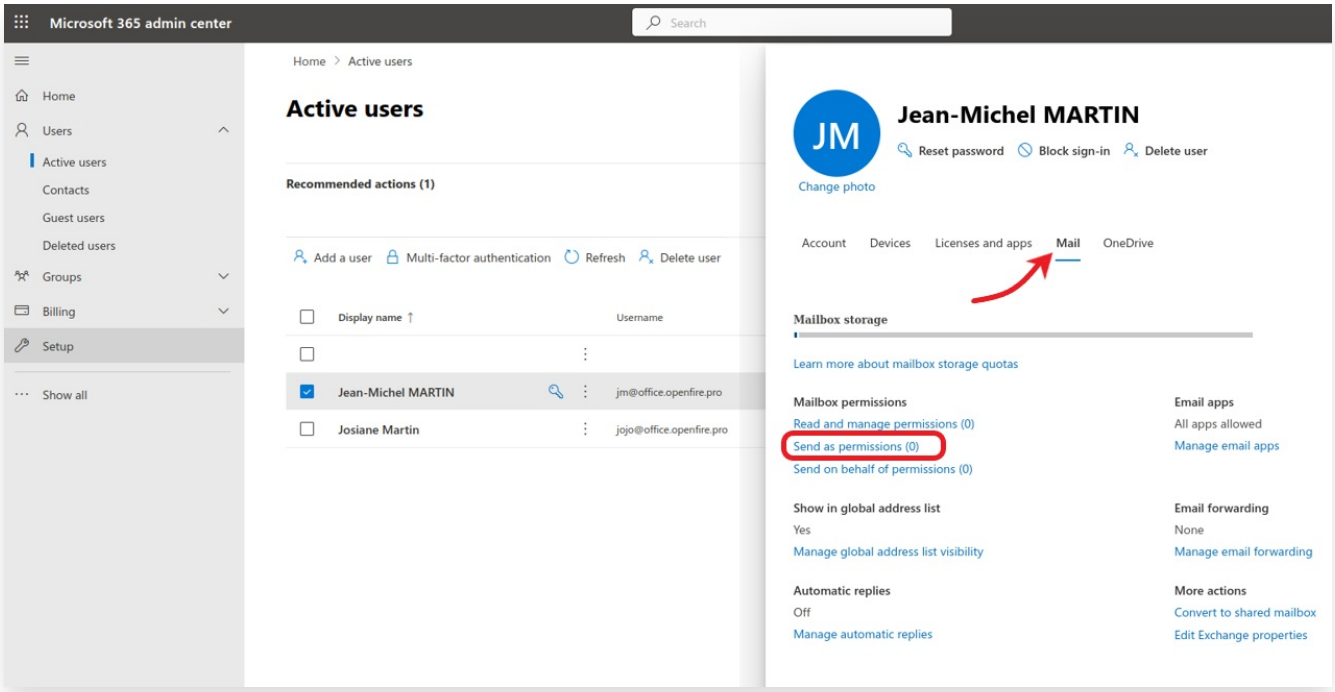
Cette étape va vous permettre d'autoriser les autres utilisateurs de votre espace Office 365 à envoyer des mails depuis OpenFire sans avoir à générer une application et une clé secrète pour chacun d'eux.

Pour cela, rendez-vous sur le centre d'administration Microsoft 365. Pour y accéder, rendez-vous sur le site https://admin.microsoft.com/adminportal/home

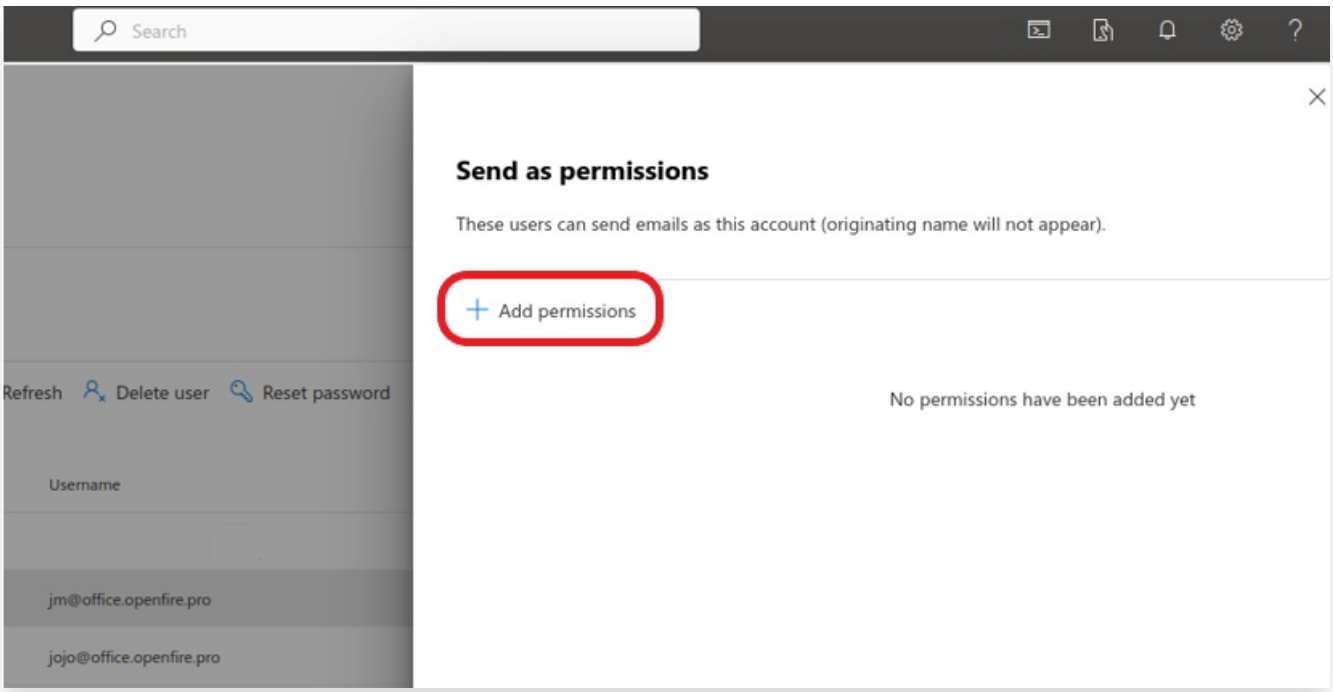
Cliquez sur Users puis sur Active Users.



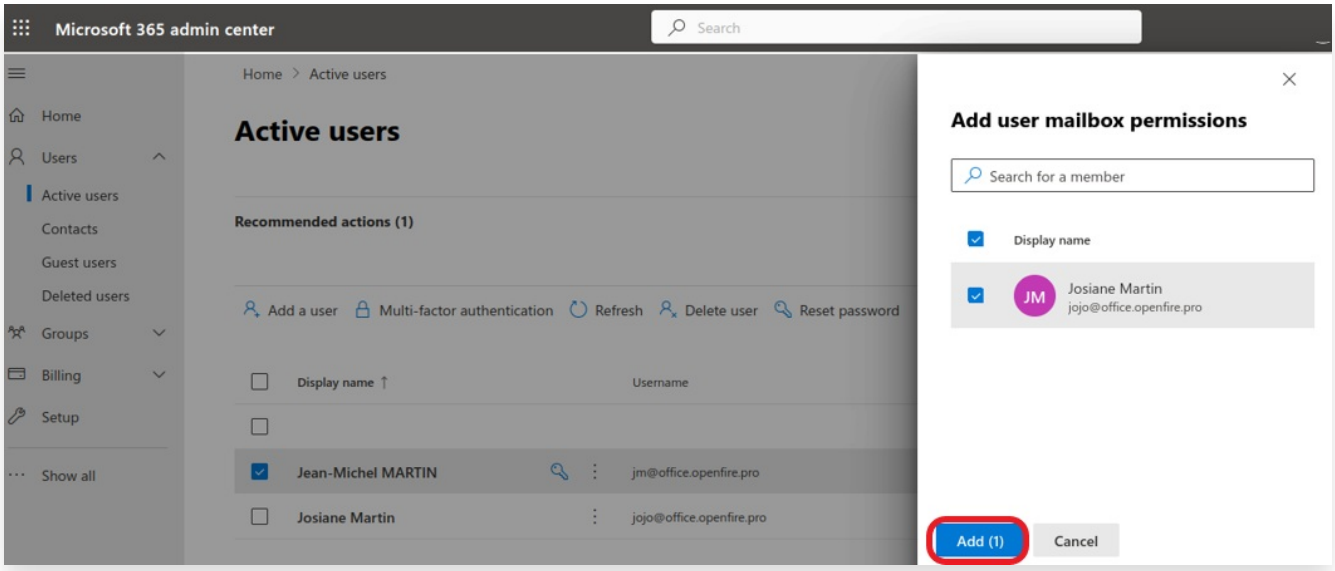
Cochez le compte administrateur, puis cliquez sur Mail, puis sur Send As Permissions



Cliquez ensuite sur Add Permissions



Puis cochez les utilisateurs qui auront à envoyer des mails depuis OpenFire et cliquez sur Add :



⚠ Attention : cette manipulation sera a faire à chaque nouvel employé devant envoyer des mails sur OpenFire:

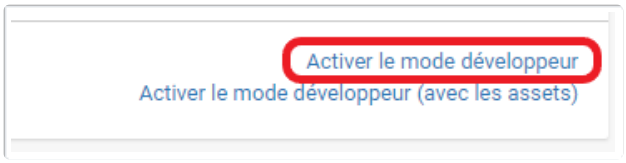
• Allez sur la page d'admin Office 365 pour ajouter les droits ;

• Allez sur Azure et cliquez sur Utilisateurs et Groupe puis Ajouter un utilisateur/Groupe + Aucune sélection, cela ouvre une fenêtre permettant de sélectionner les nouveaux utilisateurs.

Étape 4: Configuration OpenFire

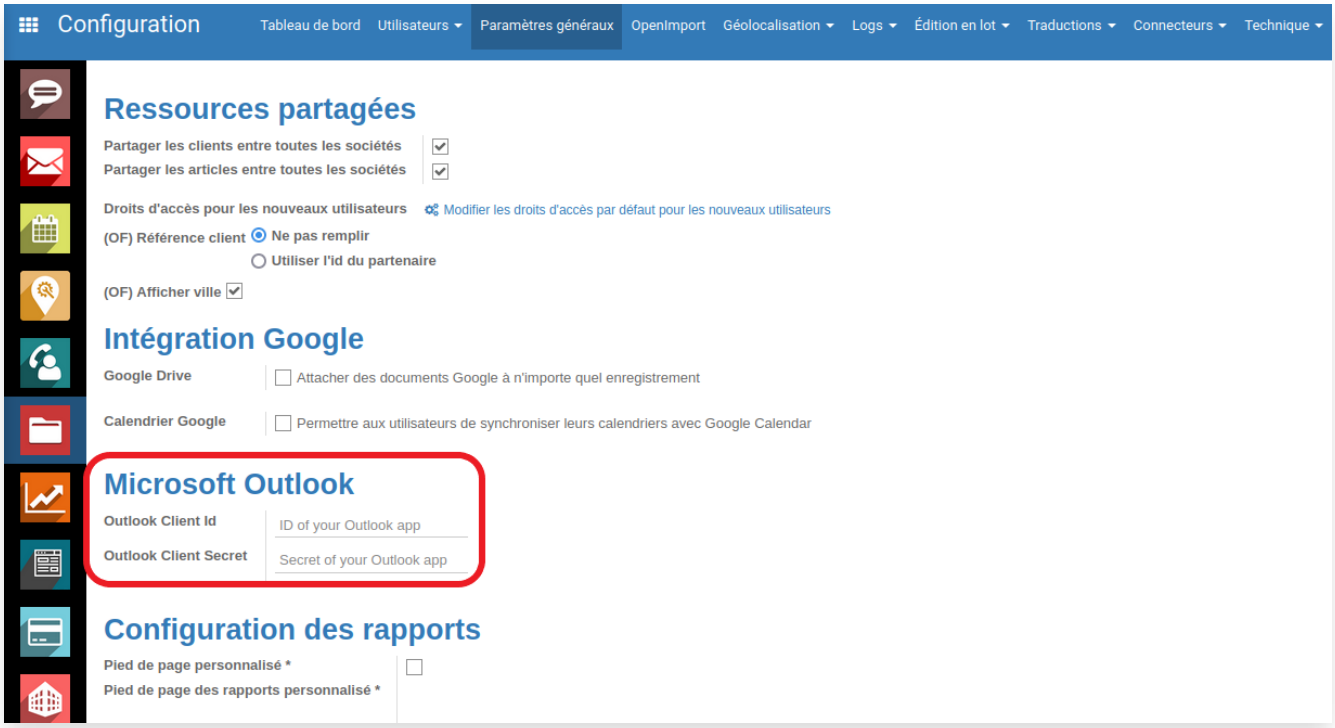
La configuration des envois d'emails se fait depuis le menu Configuration et nécessite l'activation du mode développeur.

Pour cela, sur OpenFire, rendez-vous dans l'onglet **Configuration** puis cliquez sur l'option Activer le mode développeur en bas à droite :



Après le chargement de la page, retournez dans le menu Configuration.

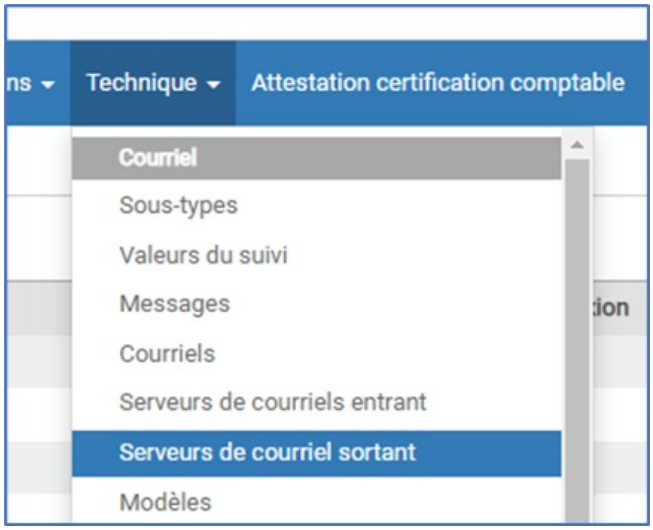
Rendez-vous dans le menu Paramètres Généraux puis dans la Partie Microsoft Outlook.



Dans cette partie, copiez/collez les valeurs de l'ID d'application et de la clé secrète que vous avez du copier précédemment dans un document texte ou un bloc-notes.

Sauvegardez les modifications.

Cliquez ensuite sur **Technique > Serveurs de courriel sortant**

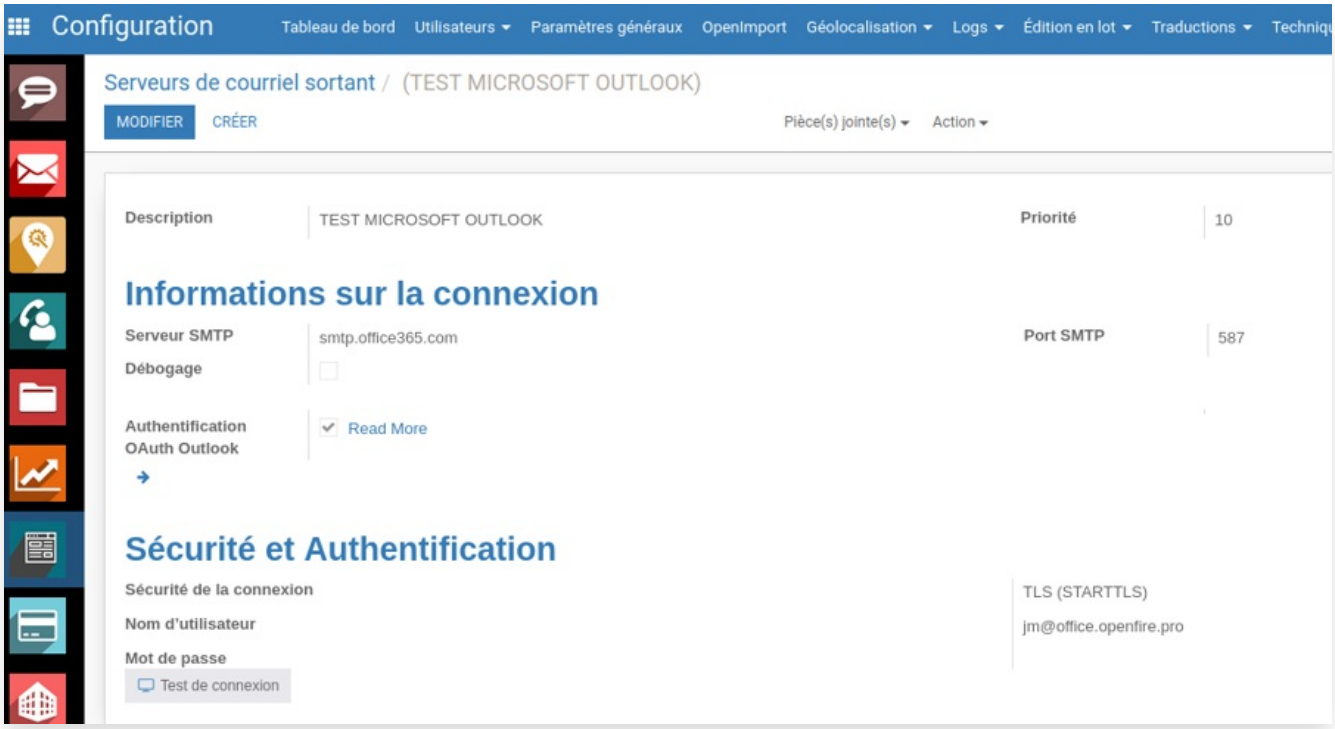


Ces différents menus vous permettent de piloter votre envoi de mails.

Si aucun serveur n'existe, cliquez sur Créer puis renseignez les différents paramètres demandés.

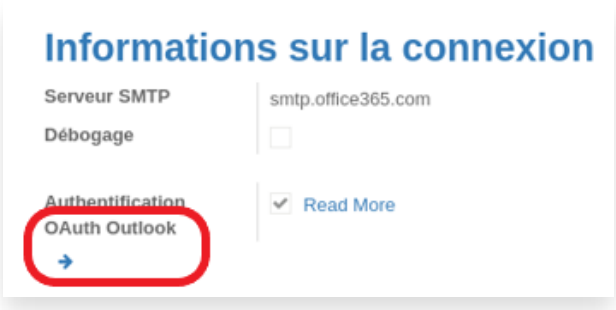
Pour une adresse office 365, renseignez les champs comme suit :

- Serveur SMTP : smtp.office365.com
- Port SMTP : 587
- Sécurité de la connexion : TLS (STARTTLS)
- Puis renseignez l'adresse mail du compte administrateur Office 365 :



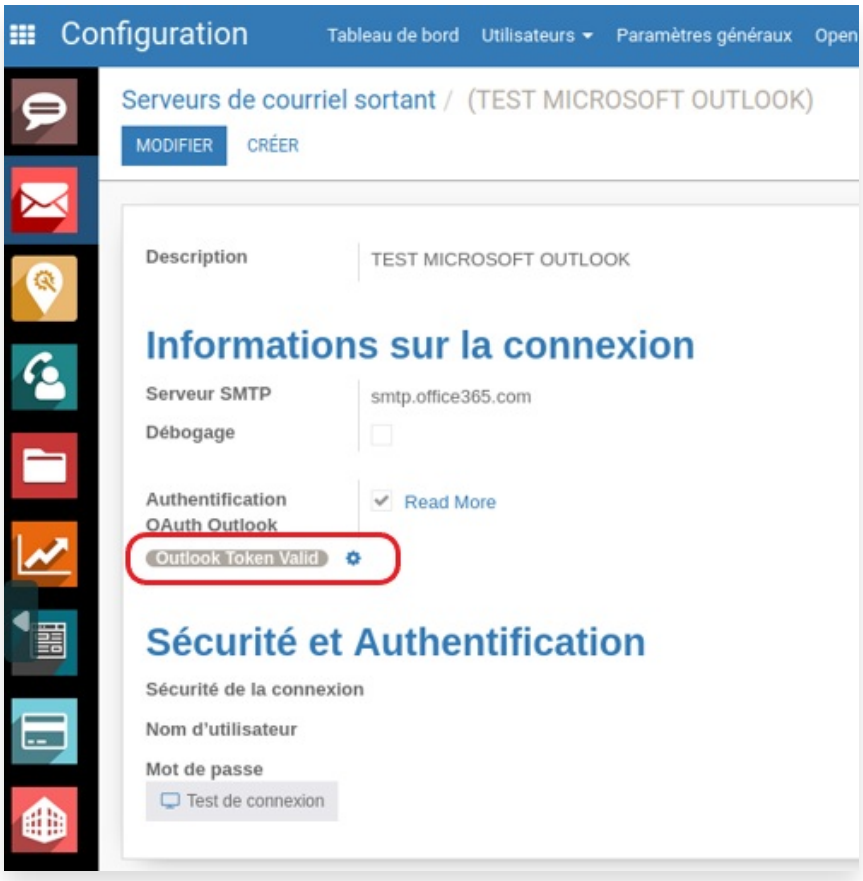
⚠ Attention : Laissez le champ Mot de passe vide car celui-ci n'est pas utilisé pour l'authentification.

Cochez l'option Authentification OAuth Outlook puis sauvegardez puis cliquez sur la flèche disponible dans la partie OAuth Outlook :



Vous serez alors redirigé vers une fenêtre de connexion à votre compte Office 365. Identifiez-vous si besoin. Vous serez ensuite redirigé vers la configuration du serveur SMTP.

Si tout s'est bien déroulé, l'étiquette Outlook Token Validé apparaitra alors :

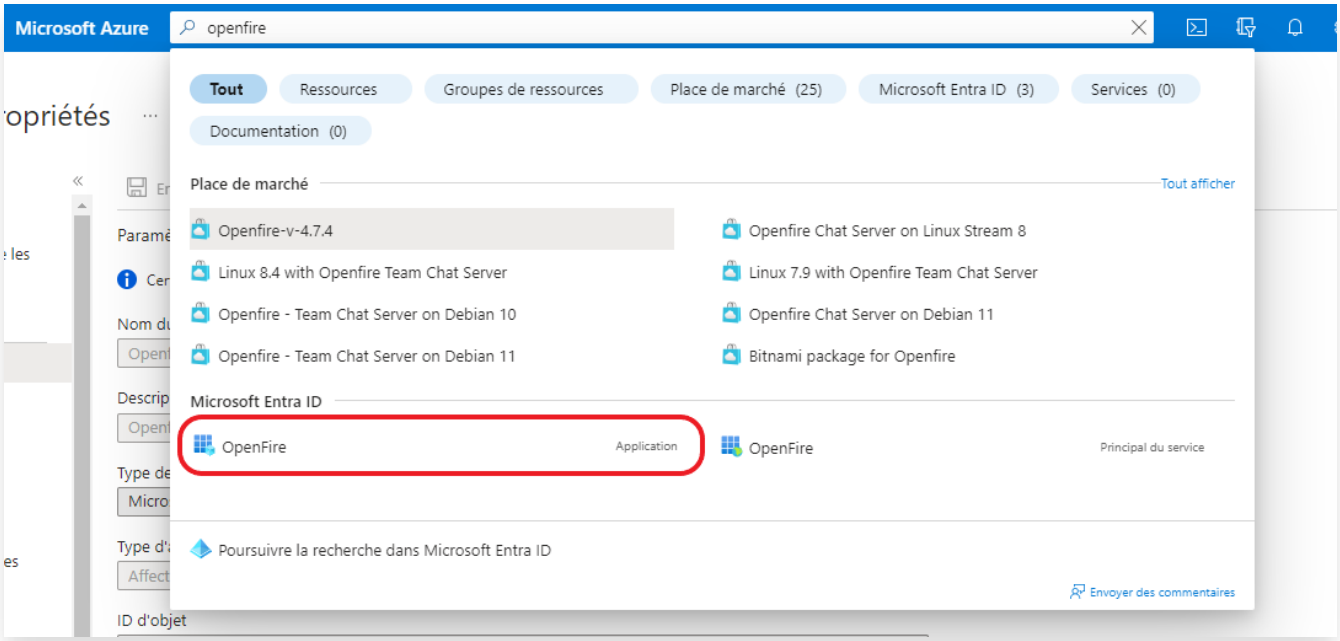


A l'issue de cette étape, l'utilisateur de référence pour lequel le serveur SMTP a été créé, ainsi que les utilisateurs ayant été ajoutés à l'étape 4, pourront envoyer des mails depuis OpenFire.

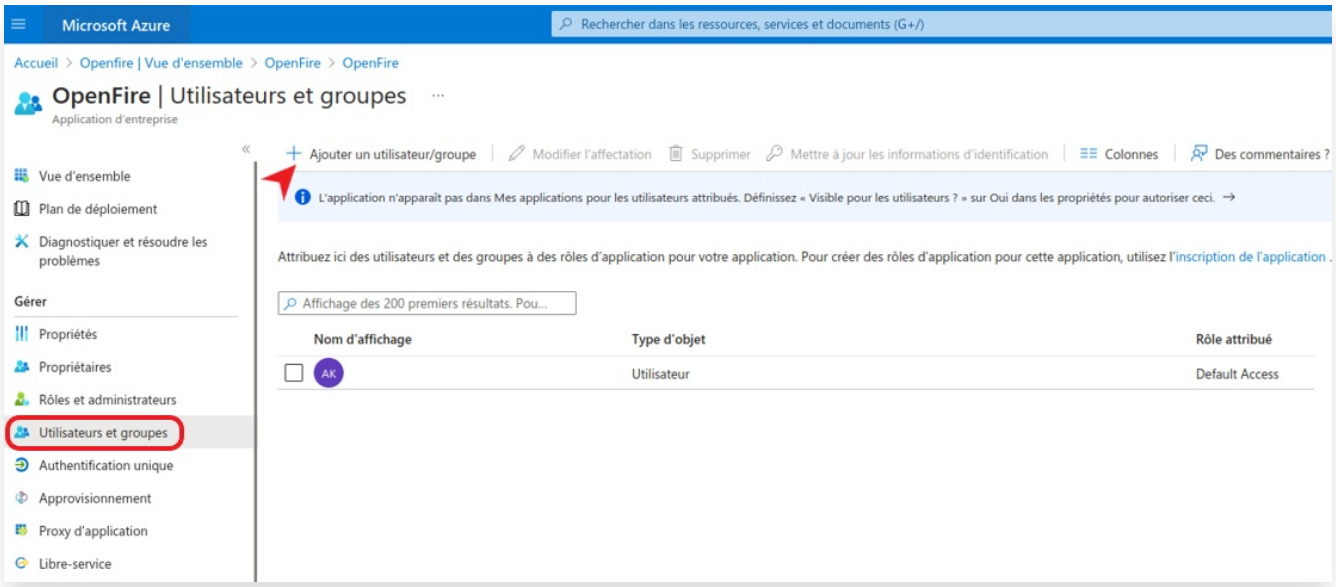
Facultatif : Ajout des groupes Utilisateurs

Cette étape est facultative en fonction du fait que le compte admin et le compte de référence utilisé en tant que serveur SMTP sur OpenFire est le même.

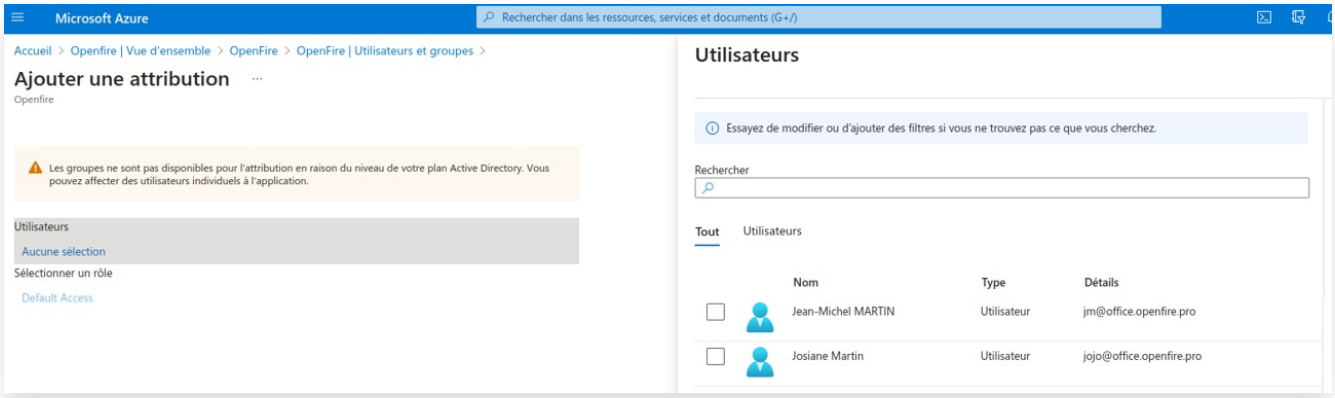
Sur Azure, cliquez sur la barre de recherche, puis recherchez OpenFire et cliquez sur l'icone d'entreprise.



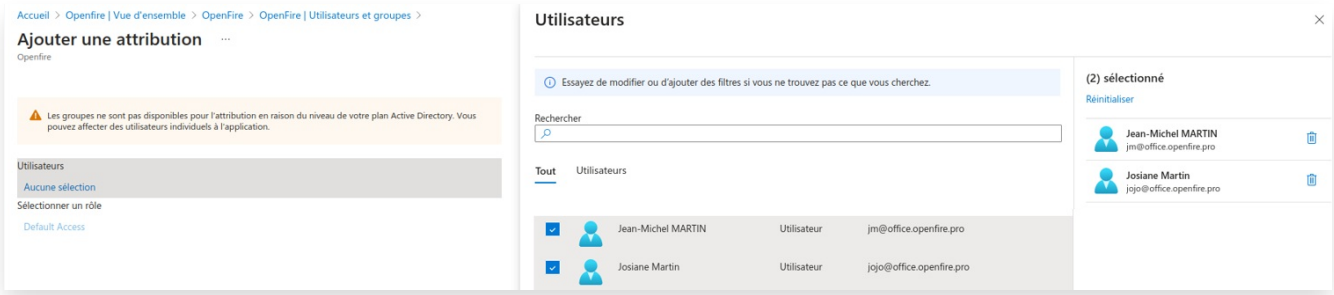
Cliquez ensuite sur Utilisateurs et Groupe puis sur Ajouter un utilisateur/Groupe



Cela ouvre une fenêtre permettant de sélectionner les utilisateurs :



Sélectionnez alors les utilisateurs de votre choix :



Les utilisateurs ont maintenant le droit d'utiliser l'application OpenFire dans Azure.