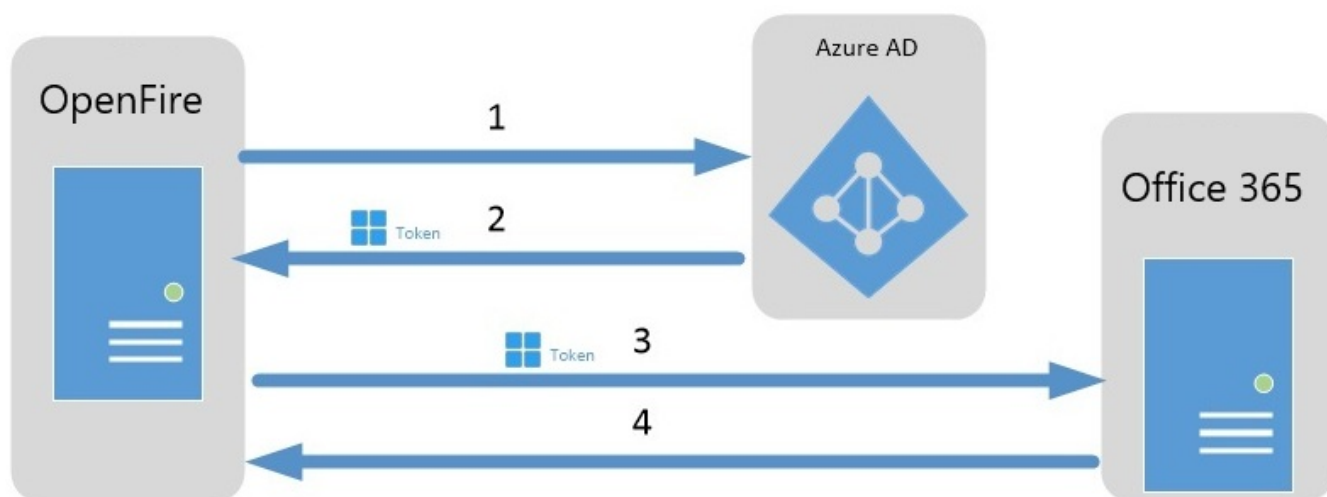


## Authentification Azure pour Office 365

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](mailto:support@openfire.fr) ou par téléphone au [02.30.96.02.65](tel: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\\*](#)


portal.azure.com/#home

Microsoft Azure


Rechercher dans les ressources, services et documents (G+)

### 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 Microsoft Entra ID**  
Azure Active Directory devient Microsoft Entra ID. Accès sécurisé pour tout le monde.  
[Vue](#) [En savoir plus](#)



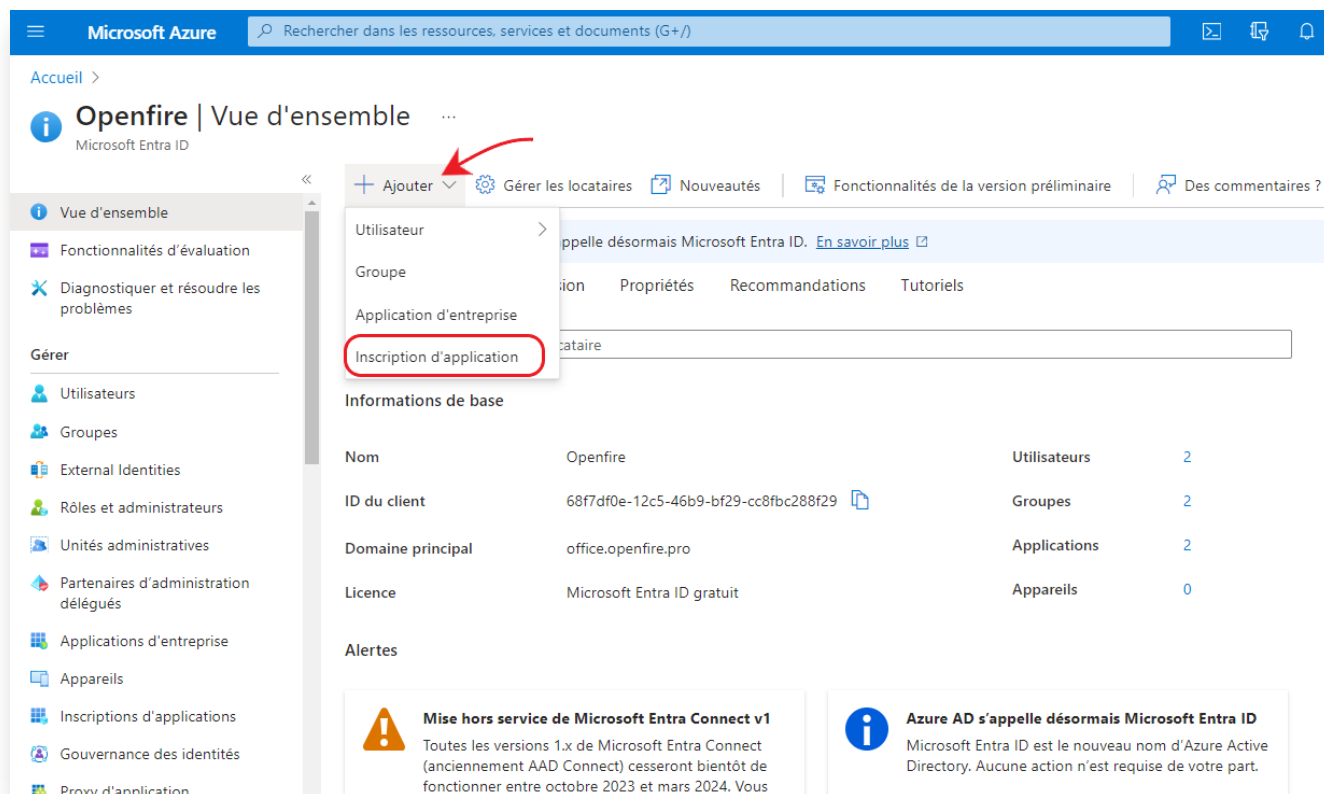
**Accéder aux avantages des étudiants**  
Bénéficiez de logiciels gratuits, de crédit Azure ou d'un accès à Azure Dev Tools for Teaching après avoir vérifié votre statut scolaire.  
[Explorer](#) [En savoir plus](#)

### Services Azure

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

\* Si cette icone n'apparait pas, cliquez alors sur [Autres Services](#) puis recherchez [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](https://mabase.openfire.fr/microsoft_outlook/confirm) (en remplaçant la valeur en bleue par l'url de votre baseOpenFire).

Microsoft Azure Rechercher dans les ressources, services et docu

Accueil > Openfire | Vue d'ensemble >

## Inscrire une application

**\* Nom**

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

**Types de comptes pris en charge**

Qui peut utiliser cette application ou accéder à cette API ?

- Comptes dans cet annuaire d'organisation uniquement (Openfire uniquement - Locataire unique)
- Comptes dans un annuaire d'organisation (tout locataire Microsoft Entra ID – Multilocataire)
- Comptes dans un annuaire d'organisation (tout locataire Microsoft Entra ID – 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.

Inscrivez ici une application sur laquelle vous travaillez. Intégrez des applications de la galerie et d'autres applications externes à votre organisation

En continuant, vous acceptez les stratégies de la plateforme Microsoft

[S'inscrire](#)

Cliquez sur [S'inscrire](#).

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

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and navigation options. The main content area displays the configuration details for an application named 'OpenFire'. The configuration includes fields for 'Nom d'affichage', 'ID d'application (client)', 'ID de l'objet', 'ID de l'annuaire (locataire)', and 'Types de comptes pris en compte'. There are also links for 'Ajouter un certificat ou un secret', 'Ajouter un URI de redirection', 'Ajouter un URI d'application', and 'Ajouter un URI de redirection'. Below the configuration details, there are several informational messages and a warning about the deprecation of ADAL and Graph. At the bottom, there is a section titled 'Générez votre application avec la plateforme d'identités Microsoft' with a sub-section 'Démarrer' and 'Documentation'.

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Accueil > OpenFire | Vue d'ensemble >

OpenFire

Rechercher

Supprimer Points de terminaison Fonctionnalités en préversion

Vous avez une seconde ? Nous aimerions obtenir vos commentaires sur Microsoft Identity Platform (précédemment appelée Azure AD pour les développeurs). →

Bases

Nom d'affichage : [OpenFire](#) Informations d'identificat... : [Ajouter un certificat ou un secret](#)

ID d'application (client) : e869e4fe-d10d-4597-a619-23d57ebc02e5 URI de redirection : [1\\_web\\_0\\_spa\\_0\\_client\\_public](#)

ID de l'objet : af5e2600-2e5d-4e1b-ad54-0fa47a7cf719 URI ID d'application : [Ajouter un URI d'application](#)

ID de l'annuaire (locataire) : 68f7df0e-12c5-46b9-bf29-cc8fbc288f29 Application gérée da... : [OpenFire](#)

Types de comptes pris e... : [Plusieurs organisations](#)

Bienvenue dans les nouvelles Inscriptions d'applications améliorées. Vous cherchez à connaître les changements depuis Inscriptions d'applications (héritées) ? [En savoir plus](#)

Depuis le 30 juin 2020, nous n'ajoutons plus de nouvelles fonctionnalités à Azure Active Directory Authentication Library (ADAL) ni à Azure Active Directory Graph. Nous continuerons à fournir un support technique et mises à jour des fonctionnalités. Les applications devront être mises à niveau vers Microsoft Authentication Library (MSAL) et Microsoft Graph. [En savoir plus](#)

À partir du 9 novembre 2020, les utilisateurs finaux ne pourront plus accorder de consentement aux applications multilocataire nouvellement inscrites sans éditeurs validés. [Ajouter l'ID.MPN pour vérifier l'éditeur](#)

Démarrer Documentation

## Générez votre application avec la plateforme d'identités Microsoft

La plateforme d'identités Microsoft inclut un service d'authentification, des bibliothèques open source et des outils de gestion des applications. Vous pouvez créer des solutions d'authentification modernes, basées sur des normes, accéder à des API et les protéger, et ajouter une connexion pour vos utilisateurs et vos clients. [En savoir plus](#)

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

Accueil > Openfire | Vue d'ensemble > OpenFire

## OpenFire | API autorisées

Rechercher

Actualiser | Des commentaires ?

Vue d'ensemble  
Démarrage rapide  
Assistant Intégration

Gérer

- Personnalisation et propriétés
- Authentification
- Certificats & secrets
- Configuration du jeton
- API autorisées**
- Exposer une API
- Rôles d'application
- Propriétaires
- Rôles et administrateurs

La colonne « Consentement de l'administrateur requis » indique la valeur par défaut pour une organisation où cette application sera utilisée. [En savoir plus](#)

### Autorisations configurées

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part de l'utilisateur. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin.

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

API / noms des autorisations	Type	Description
Microsoft Graph (1)		
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur

Pour afficher et gérer les autorisations accordées pour des applications individuelles, ainsi que les paramètres d'entreprise.

\* 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 :

The screenshot shows the 'API autorisées' (API Authorized) page in the OpenFire administration interface. The page title is 'OpenFire | API autorisées'. On the left, there is a navigation menu with categories like 'Gérer', 'Support + dépannage', and 'Nouvelle demande de support'. The main content area has a search bar and buttons for 'Actualiser' and 'Des commentaires?'. There are two warning messages at the top: one about user consent and another about the November 9, 2020 deadline for multi-tenant applications. Below these, an information message explains the 'Consentement de l'administrateur requis' column. The main section is titled 'Autorisations configurées' and contains a table of permissions. The table has columns for 'API / noms des autorisations', 'Type', 'Description', 'Consentement de l'a...', and 'Statut'. There are 9 permissions listed under the 'Microsoft Graph' group. The last permission, 'User.Read.All', has a status of 'Pas accordé pour Openfire'.

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
▼ Microsoft Graph (9)				
IMAP.AccessAsUser.All	Déléguée	Read and write access to mailboxes via IMAP.	Non	...
Mail.ReadWrite	Déléguée	Accéder en lecture et en écriture aux e-mails utilisateur	Non	...
Mail.Send	Déléguée	Envoyer un e-mail en tant qu'utilisateur	Non	...
Mail.Send.Shared	Déléguée	Envoyer un e-mail au nom d'autres utilisateurs	Non	...
offline_access	Déléguée	Conservé l'accès aux données auxquelles vous lui avez do...	Non	...
POP.AccessAsUser.All	Déléguée	Read and write access to mailboxes via POP.	Non	...
SMTP.Send	Déléguée	Send emails from mailboxes using SMTP AUTH.	Non	...
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur	Non	...
User.Read.All	Déléguée	Lire les profils complets de tous les utilisateurs	Oui	⚠ Pas accordé pour Openfire... ..

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](#)



Accueil > Openfire | Vue d'ensemble > OpenFire

OpenFire | API autorisées

Rechercher

Actualiser | Des commentaires ?

Vous êtes en train de modifier une ou plusieurs autorisations pour votre application, les utilisateurs doivent donner leur consentement.

À partir du 9 novembre 2020, les utilisateurs finaux ne pourront plus accorder de consentement aux applications muen...

La colonne « Consentement de l'administrateur requis » indique la valeur par défaut pour une organisation. Toutefois, les organisations où cette application sera utilisée. [En savoir plus](#)

**Autorisations configurées**

Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs munis d'un consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application a besoin.

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

API / noms des autorisations	Type	Description
Microsoft Graph (9)		
IMAP.AccessAsUser.All	Déléguée	Read and write access to mailboxes via IMAP.
Mail.ReadWrite	Déléguée	Accéder en lecture et en écriture aux e-mails utilisateur
Mail.Send	Déléguée	Envoyer un e-mail en tant qu'utilisateur
Mail.Send.Shared	Déléguée	Envoyer un e-mail au nom d'autres utilisateurs
offline_access	Déléguée	Conserver l'accès aux données auxquelles vous lui avez do...
POP.AccessAsUser.All	Déléguée	Read and write access to mailboxes via POP.
SMTP.Send	Déléguée	Send emails from mailboxes using SMTP AUTH.

**Demander des autorisations d'API**

Sélectionner une API

API Microsoft Graph **API utilisées par mon organisation** Mes API

Les applications dans votre annuaire qui exposent les API sont indiquées ci-dessous

office 365 exchange online

Nom

Office 365 Exchange Online

Cliquez sur [Office 365 Exchange Online > Autorisations d'applications](#)

## Demander des autorisations d'API

[Toutes les API](#)

Office 365 Exchange Online  
<https://outlook.office.com>

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.

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.

Vous êtes en train de modifier une ou plusieurs autorisations pour votre application, les utilisateurs doivent donner leur consentement, 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 Openfire

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
Microsoft Graph (9)				
IMAP.AccessAsUser.All	Déléguée	Read and write access to mailboxes via IMAP.	Non	⚠ Pas accordé pour Openf...
Mail.ReadWrite	Déléguée	Accéder en lecture et en écriture aux e-mails utilisateur	Non	⚠ Pas accordé pour Openf...
Mail.Send	Déléguée	Envoyer un e-mail en tant qu'utilisateur	Non	⚠ Pas accordé pour Openf...
Mail.Send.Shared	Déléguée	Envoyer un e-mail au nom d'autres utilisateurs	Non	⚠ Pas accordé pour Openf...
offline_access	Déléguée	Conserver l'accès aux données auxquelles vous lui avez do...	Non	⚠ Pas accordé pour Openf...
POP.AccessAsUser.All	Déléguée	Read and write access to mailboxes via POP.	Non	⚠ Pas accordé pour Openf...
SMTP.Send	Déléguée	Send emails from mailboxes using SMTP AUTH.	Non	⚠ Pas accordé pour Openf...
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur	Non	⚠ Pas accordé pour Openf...
User.Read.All	Déléguée	Lire les profils complets de tous les utilisateurs	Oui	⚠ Pas accordé pour Openf...
Office 365 Exchange Online (3)				
IMAP.AccessAsApp	Application	IMAP.AccessAsApp	Oui	⚠ Pas accordé pour Openf...
POP.AccessAsApp	Application	POP.AccessAsApp	Oui	⚠ Pas accordé pour Openf...
SMTP.SendAsApp	Application	Application access for sending emails via SMTP AUTH	Oui	⚠ Pas accordé pour Openf...

Consentement administrateur donné pour les autorisations demandées.

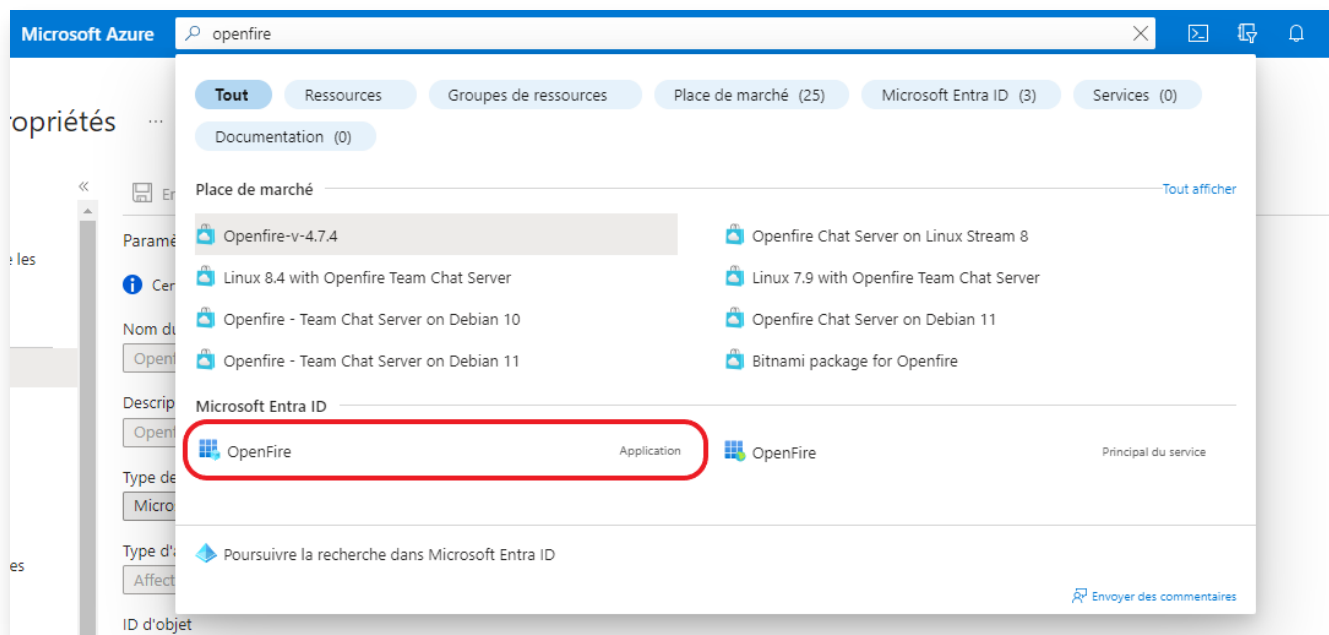
**Autorisations configurées**  
Les applications sont autorisées à appeler des API quand elles reçoivent des autorisations de la part des utilisateurs/administrateurs dans le cadre du processus de consentement. La liste des autorisations configurées doit comprendre toutes les autorisations dont l'application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

+ Ajouter une autorisation  Accorder un consentement d'administrateur pour Openfire

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
Microsoft Graph (9)				
IMAP.AccessAsUser.All	Déléguée	Read and write access to mailboxes via IMAP.	Non	✅ Accordé pour Openfire
Mail.ReadWrite	Déléguée	Accéder en lecture et en écriture aux e-mails utilisateur	Non	✅ Accordé pour Openfire
Mail.Send	Déléguée	Envoyer un e-mail en tant qu'utilisateur	Non	✅ Accordé pour Openfire
Mail.Send.Shared	Déléguée	Envoyer un e-mail au nom d'autres utilisateurs	Non	✅ Accordé pour Openfire
offline_access	Déléguée	Conserver l'accès aux données auxquelles vous lui avez do...	Non	✅ Accordé pour Openfire
POP.AccessAsUser.All	Déléguée	Read and write access to mailboxes via POP.	Non	✅ Accordé pour Openfire
SMTP.Send	Déléguée	Send emails from mailboxes using SMTP AUTH.	Non	✅ Accordé pour Openfire
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur	Non	✅ Accordé pour Openfire
User.Read.All	Déléguée	Lire les profils complets de tous les utilisateurs	Oui	✅ Accordé pour Openfire
Office 365 Exchange Online (3)				
IMAP.AccessAsApp	Application	IMAP.AccessAsApp	Oui	✅ Accordé pour Openfire
POP.AccessAsApp	Application	POP.AccessAsApp	Oui	✅ Accordé pour Openfire
SMTP.SendAsApp	Application	Application access for sending emails via SMTP AUTH	Oui	✅ Accordé pour Openfire

## 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.

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar with the text "Rechercher dans les ressources, services et documents (G+)". Below this, the page title "OpenFire" is displayed. A navigation menu on the left includes options like "Vue d'ensemble", "Démarrage rapide", "Assistant Intégration", and "Gérer". The main content area shows the application's configuration details under the heading "Bases".

Nom d'affichage	: <a href="#">OpenFire</a>
ID d'application (client)	: <u>e869e4fe-d10d-4597-a619-23d57ebc02e5</u> <span>Copier dans le Presse-papiers</span>
ID de l'objet	: af5e2600-2e5d-4e1b-ad54-0fa47a7cf719
ID de l'annuaire (locataire)	: 68f7df0e-12c5-46b9-bf29-cc8fbc288f29
Types de comptes pris en...	: <a href="#">Plusieurs organisations</a>

Below the configuration details, there are two informational messages:

- Info:** Depuis le 30 juin 2020, nous n'ajoutons plus de nouvelles fonctionnalités à Azure Active Directory Authentication Extensions mises à jour de sécurité, mais nous ne proposerons plus de mises à jour des fonctionnalités. Les applications existantes continueront de fonctionner.
- Warning:** À partir du 9 novembre 2020, les utilisateurs finaux ne pourront plus accorder de consentement aux applications.

At the bottom of the configuration page, there are links for "Démarrer" and "Documentation".

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](#) :

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and navigation options. The main content area is titled 'OpenFire' and shows various management options. The 'Certificats & secrets' section is highlighted with a red box. Below this, there are details for the application, including its name, application ID, object ID, and tenant ID. A warning message is displayed, stating that new features will not be added to Azure Active Directory authentication after June 30, 2020, and that users will no longer be able to grant consent to applications starting from November 9, 2020.

Puis cliquez sur [Nouveau secret client](#) et sélectionnez la durée de votre choix :

The screenshot shows the 'Ajouter un secret client' dialog box in the Microsoft Azure portal. The dialog box is open, and the 'Date d'expiration' dropdown menu is expanded, showing several options: 'Recommandé : 180 jours (6 mois)', '90 jours (3 mois)', '365 jours (12 mois)', '545 jours (18 mois)', '730 jours (24 mois)', and 'Personnalisé'. The 'Recommandé : 180 jours (6 mois)' option is selected. The dialog box also shows the description of the secret client, which is 'OpenFire Mail'.

**⚠ Attention** la clé sera à recréer 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) :

### Ajouter un secret client

Description

Date d'expiration

- Recommandé : 180 jours (6 mois)
- 90 jours (3 mois)
- 365 jours (12 mois)
- 545 jours (18 mois)
- 730 jours (24 mois)
- Personnalisé

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

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Accueil > Openfire | Vue d'ensemble > OpenFire

## OpenFire | Certificats & secrets

Rechercher

Des commentaires ?

Vous avez une seconde pour nous faire part de vos commentaires ? →

Les informations d'identification permettent aux applications confidentielles de s'identifier auprès du service d'authentification lors de la réception de jetons à un emplacement adressable 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.

Les certificats d'inscription d'application, les secrets et les informations d'identification fédérées se trouvent dans les onglets ci-dessous.

Certificats (0) **Secrets client (1)** Informations d'identification fédérées (0)

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
OpenFire Mail	27/05/2024	_-38Q~zPAH5XwvSWoa82mT1bBEuFuDv... 2cd23c06-7b... 8-4f86-81a6-321e8d84bf83

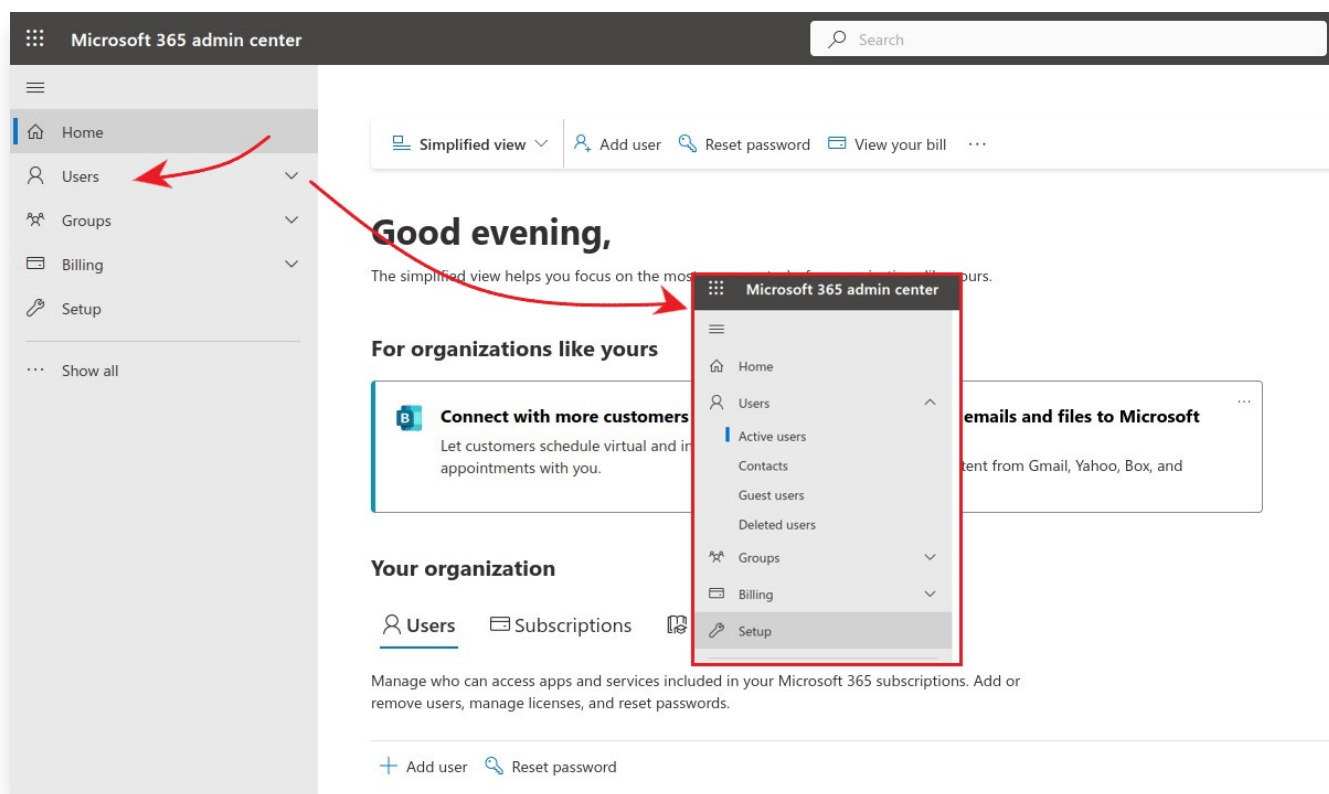
**⚠ Attention :** la clé ne sera plus affichée après fermeture de la fenêtre Microsoft Azure. En effet, la valeur de la clé secrète client n'est visible qu'immédiatement après la création. Veillez donc à bien enregistrer la clé avant de quitter la page.

## Étape 3 : Ajout des Permissions Utilisateurs

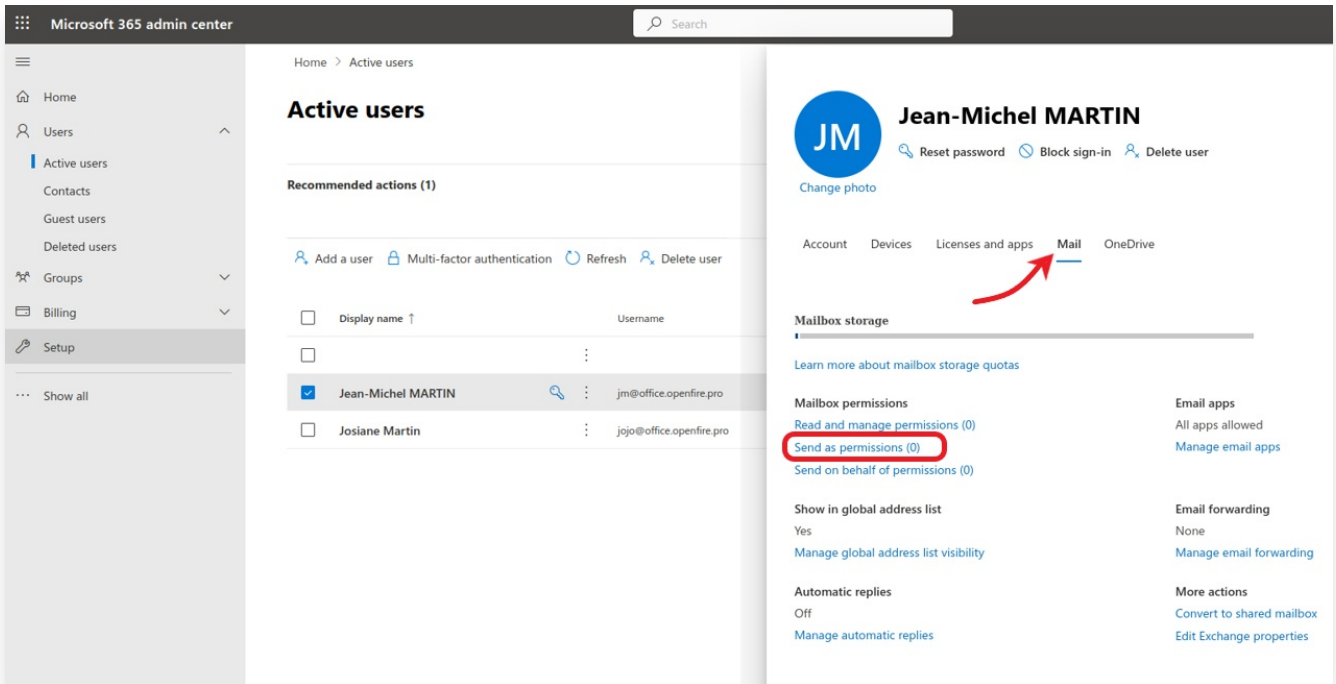
Cette étape va vous permettre d'autoriser les autres utilisateurs de votre espace Office 365 à envoyer des mails depuis OpenFire sans avoir à générer une application et une clé secrète pour chacun d'eux.

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>

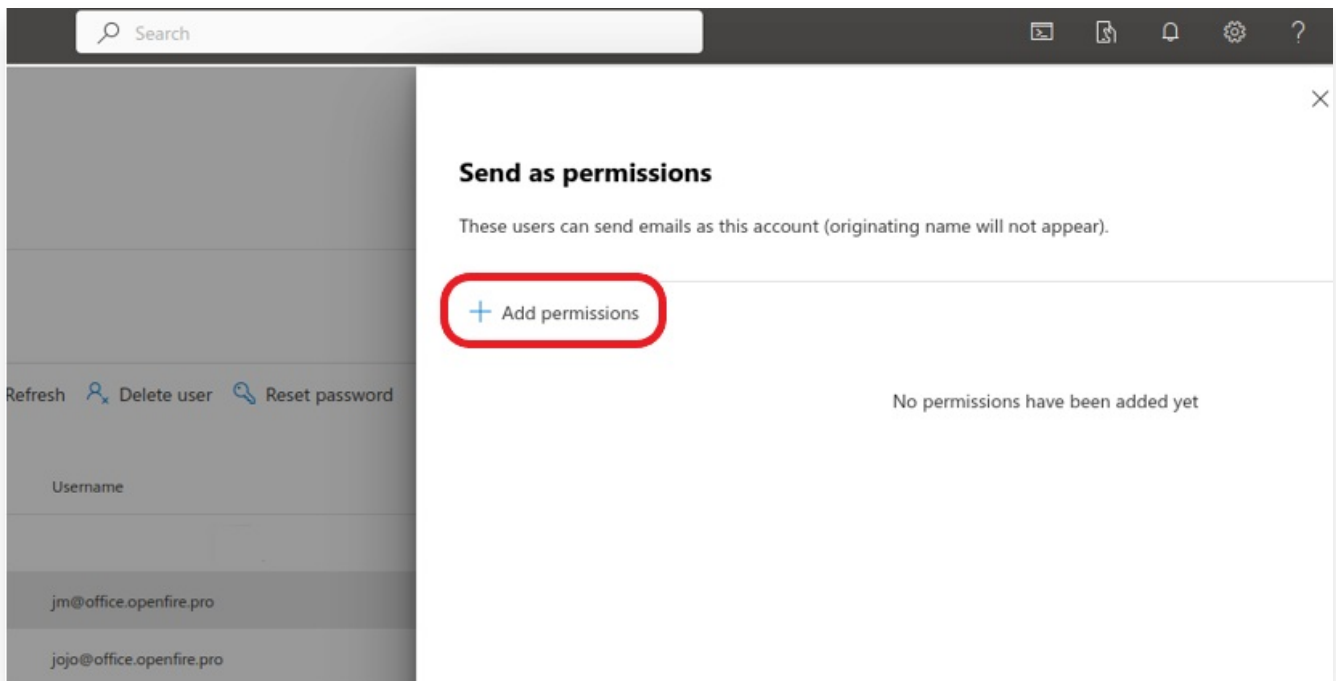
Cliquez sur [Users](#) puis sur [Active Users](#).



Cochez le compte administrateur, puis cliquez sur [Mail](#), puis sur [Send As Permissions](#)

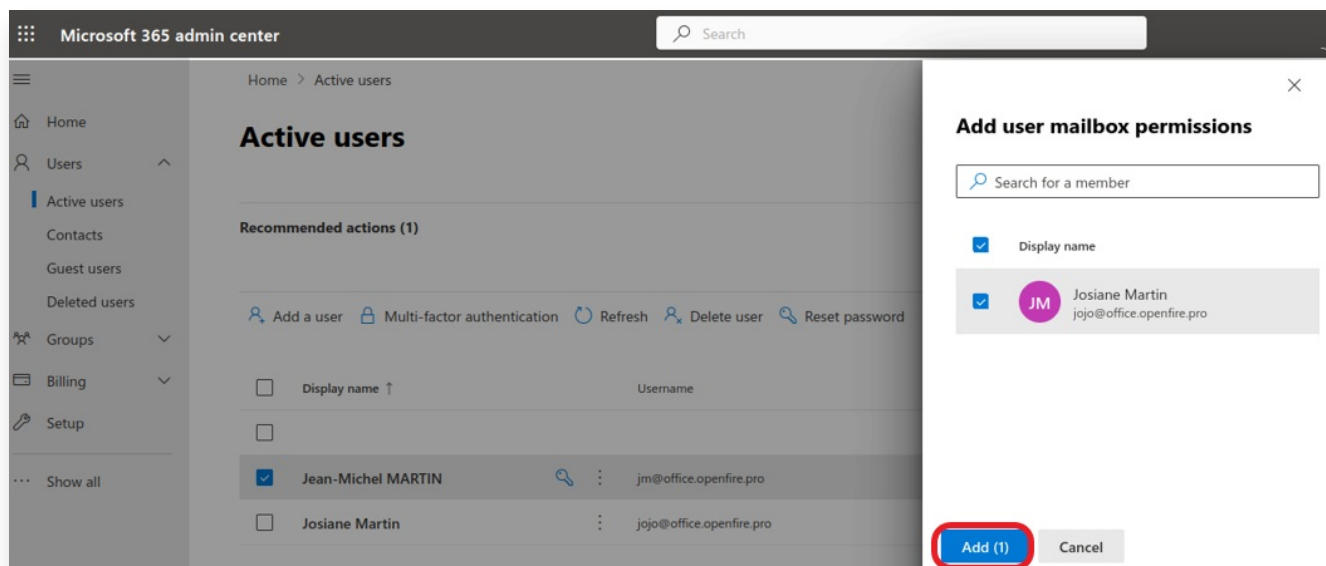


Cliquez ensuite sur [Add Permissions](#)



Puis cochez les utilisateurs qui auront à envoyer des mails depuis OpenFire et cliquez sur [Add](#) :





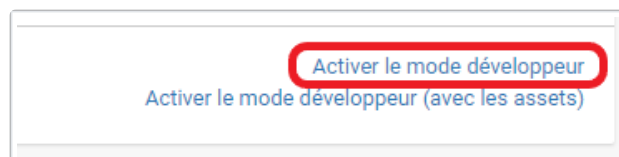
**⚠ Attention :** cette manipulation sera a faire à chaque nouvel employé devant envoyer des mails sur OpenFire:

- 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

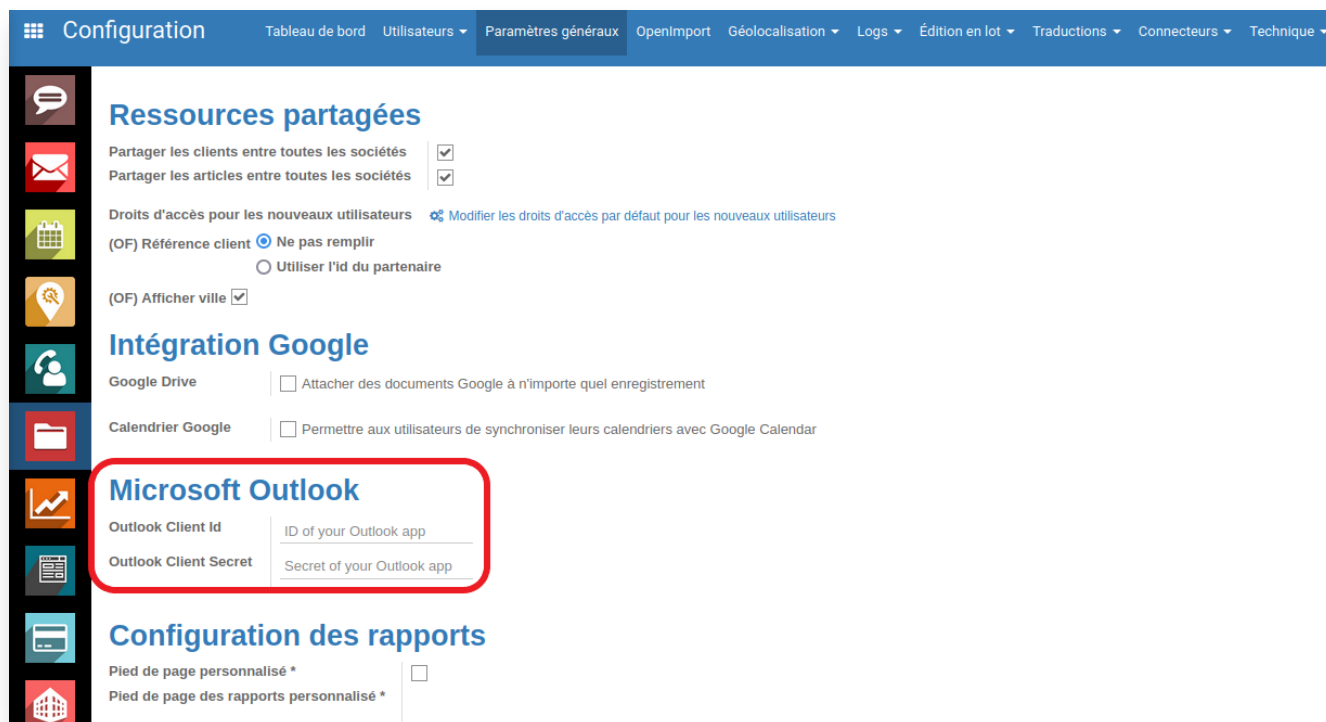
La configuration des envois d'emails se fait depuis le menu Configuration et nécessite l'activation du mode développeur.

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](#).

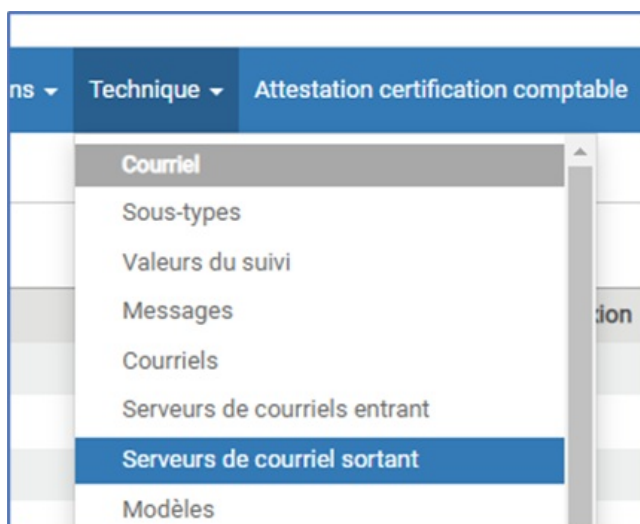
Rendez-vous dans le menu [Paramètres Généraux](#) puis dans la Partie Microsoft Outlook.



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 :

The screenshot shows the 'Configuration' page in OpenFire, specifically the 'Serveurs de courriel sortant' section for '(TEST MICROSOFT OUTLOOK)'. The interface includes a navigation menu on the left with icons for various settings. The main content area is divided into sections: 'Informations sur la connexion' and 'Sécurité et Authentification'. In the 'Informations sur la connexion' section, the 'Serveur SMTP' is set to 'smtp.office365.com', the 'Port SMTP' is '587', and the 'Authentification OAuth Outlook' option is checked. A blue arrow icon is visible below the 'Authentification OAuth Outlook' label. In the 'Sécurité et Authentification' section, the 'Sécurité de la connexion' is set to 'TLS (STARTTLS)' and the 'Nom d'utilisateur' is 'jm@office.openfire.pro'. There is also a 'Mot de passe' field which is currently empty, and a 'Test de connexion' button below it.

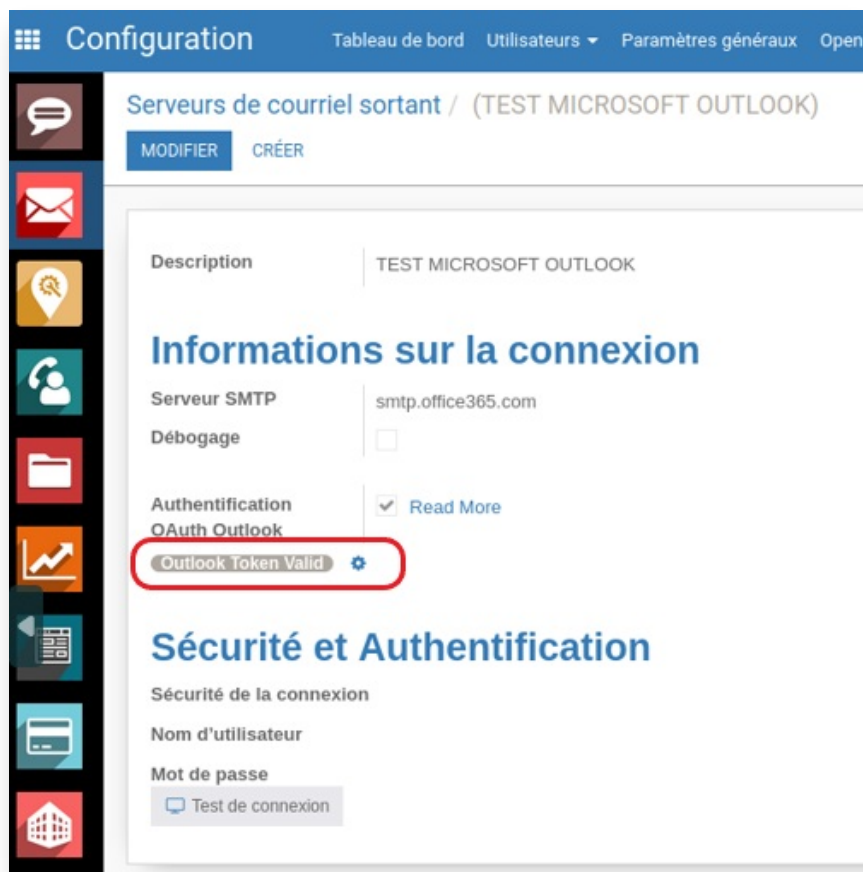
**⚠ Attention :** Laissez le champ **Mot de passe** vide car celui-ci n'est pas utilisé pour l'authentification.

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

This is a close-up view of the 'Informations sur la connexion' section. It shows the 'Serveur SMTP' field with the value 'smtp.office365.com', the 'Débogage' checkbox which is unchecked, and the 'Authentification OAuth Outlook' section. In this section, the 'Authentification OAuth Outlook' checkbox is checked, and a blue arrow icon is visible below the label. A red circle is drawn around the 'Authentification OAuth Outlook' label and the arrow icon to highlight them.

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** apparaîtra alors :

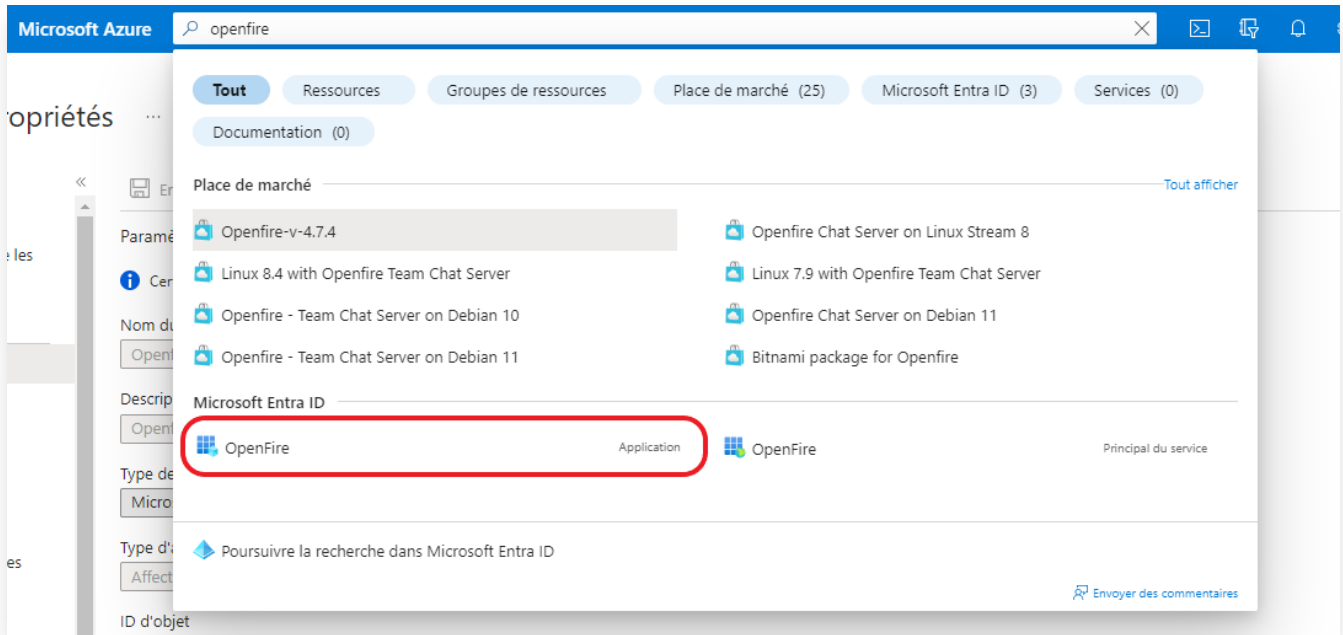


A l'issue de cette étape, l'utilisateur de référence pour lequel le serveur SMTP a été créé, ainsi que les utilisateurs ayant été ajoutés à l'étape 4, pourront envoyer des mails depuis OpenFire.

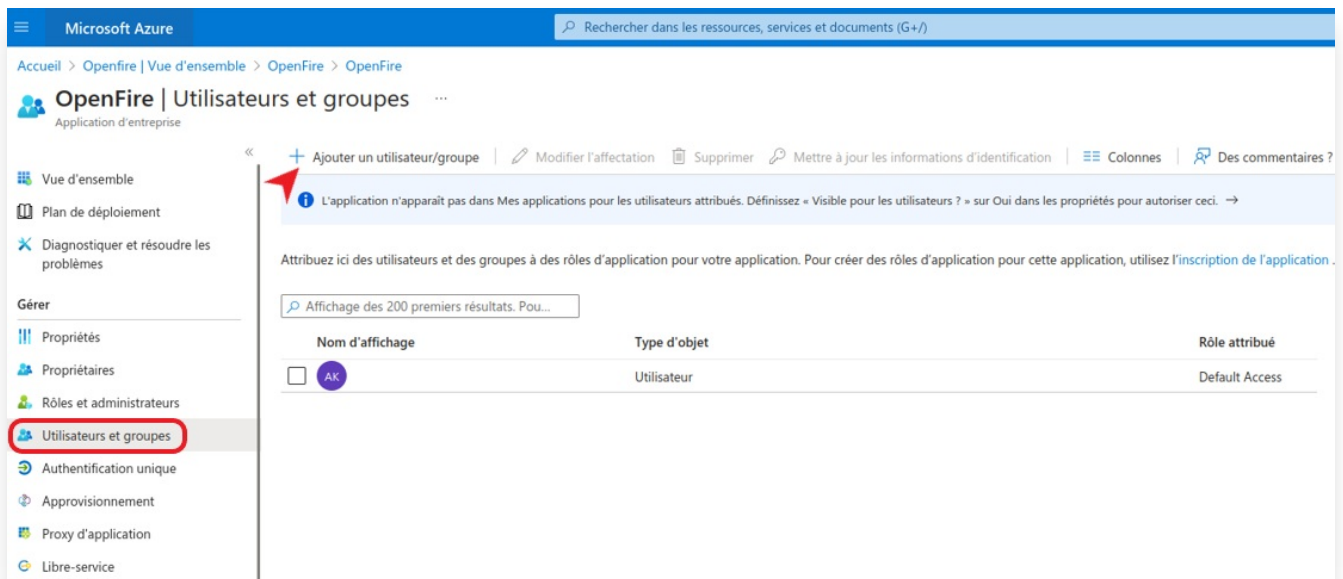
## Facultatif : Ajout des groupes Utilisateurs

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'icône d'entreprise.



Cliquez ensuite sur [Utilisateurs et Groupe](#) puis sur [Ajouter un utilisateur/Groupe](#)



Cela ouvre une fenêtre permettant de sélectionner les utilisateurs :

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Accueil > Openfire | Vue d'ensemble > OpenFire > OpenFire | Utilisateurs et groupes >

### Ajouter une attribution

Openfire

⚠ Les groupes ne sont pas disponibles pour l'attribution en raison du niveau de votre plan Active Directory. Vous pouvez affecter des utilisateurs individuels à l'application.

Utilisateurs

Aucune sélection

Sélectionner un rôle

Default Access

### Utilisateurs

🔍 Essayez de modifier ou d'ajouter des filtres si vous ne trouvez pas ce que vous cherchez.

Rechercher

Tout Utilisateurs

	Nom	Type	Détails
<input type="checkbox"/>	Jean-Michel MARTIN	Utilisateur	jm@office.openfire.pro
<input type="checkbox"/>	Josiane Martin	Utilisateur	jojo@office.openfire.pro

Sélectionnez alors les utilisateurs de votre choix :

Accueil > Openfire | Vue d'ensemble > OpenFire > OpenFire | Utilisateurs et groupes >

### Ajouter une attribution

Openfire

⚠ Les groupes ne sont pas disponibles pour l'attribution en raison du niveau de votre plan Active Directory. Vous pouvez affecter des utilisateurs individuels à l'application.

Utilisateurs

Aucune sélection

Sélectionner un rôle

Default Access

### Utilisateurs

🔍 Essayez de modifier ou d'ajouter des filtres si vous ne trouvez pas ce que vous cherchez.

Rechercher

Tout Utilisateurs

	Nom	Type	Détails
<input checked="" type="checkbox"/>	Jean-Michel MARTIN	Utilisateur	jm@office.openfire.pro
<input checked="" type="checkbox"/>	Josiane Martin	Utilisateur	jojo@office.openfire.pro

(2) sélectionné

Réinitialiser

- Jean-Michel MARTIN  
jm@office.openfire.pro
- Josiane Martin  
jojo@office.openfire.pro

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