Enregistrement de l’application “Microsoft ODSP Connector GLIMPS”

Contexte

Ce guide explique comment configurer le connecteur GLIMPS pour Microsoft 365 dans Azure afin de permettre l’accès aux données de messagerie via l’API Microsoft Graph.
Cette configuration est nécessaire pour que votre application puisse lire, écrire et envoyer des e-mails au nom des utilisateurs de votre organisation.

Vous pouvez choisir entre :

- une **procédure automatique** (via un script PowerShell),
- ou une **procédure manuelle** (via le portail Microsoft 365).

Prérequis

- PowerShell Core 7.0+ (**Ne fonctionnera pas en version 5**) https://apps.microsoft.com/detail/9MZ1SNWT0N5D?hl=neutral&gl=FR&ocid=pdpshare
- Un compte Microsoft 365 disposant d’un des rôles suivants :
  - `Application Developer`
  - `Application Administrator`
  - `Global Administrator`

Création de l’application - méthode automatique

Exécutez simplement le script PowerShell fourni pour automatiser la création de l’application :

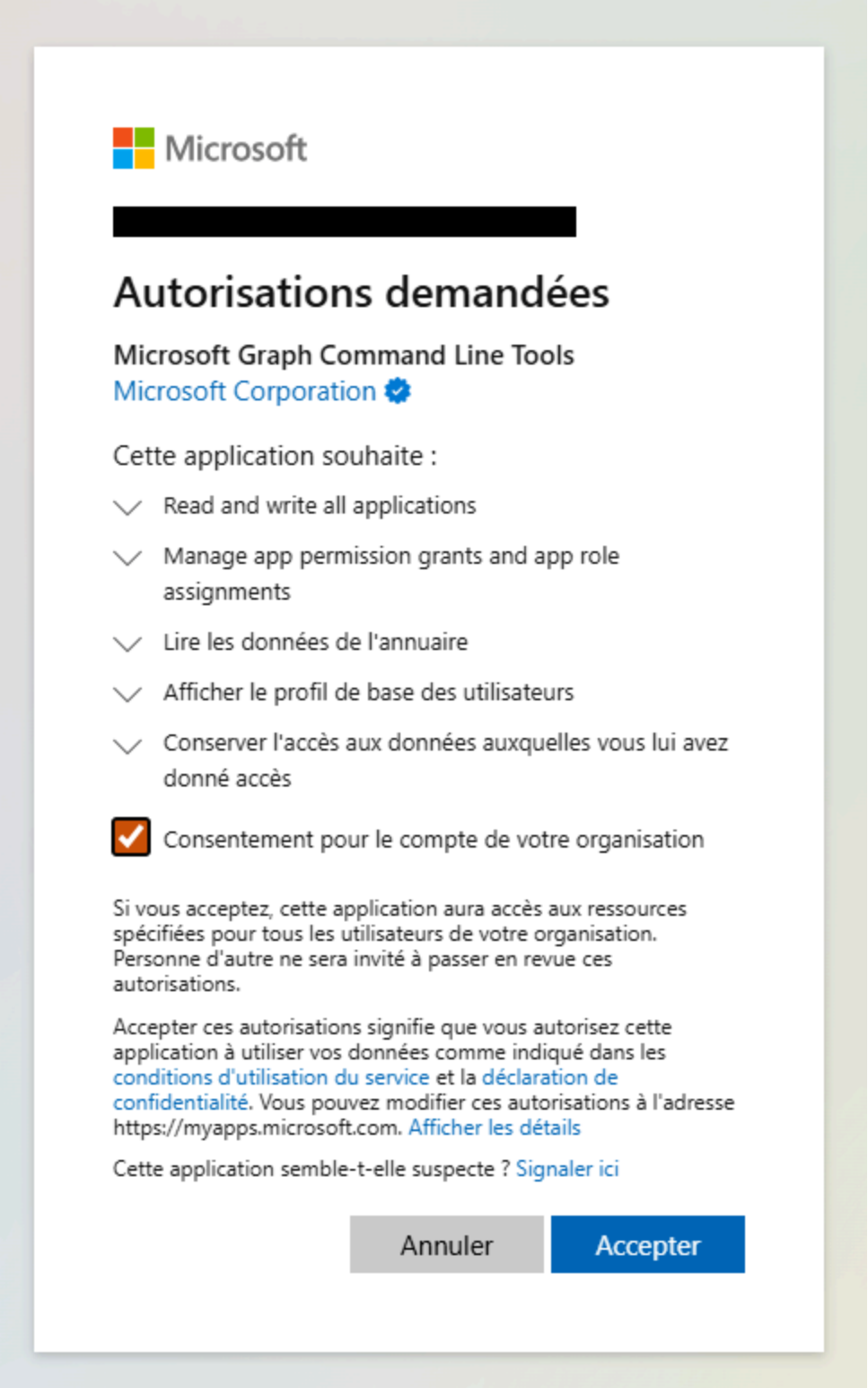
```
./GLIMPS-ODSP-AppRegistration.ps1
```

Exécution dans un environnement sans interface graphique

Dans le cas ou le script est exécuté dans un environnement sans interface graphique (serveur, SSH, ...), il vous sera demandé de vous authentifier sur l’url https://microsoft.com/devicelogin avec le code fournis par le script.

```
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code XXXXXXXXX to authenticate.
```

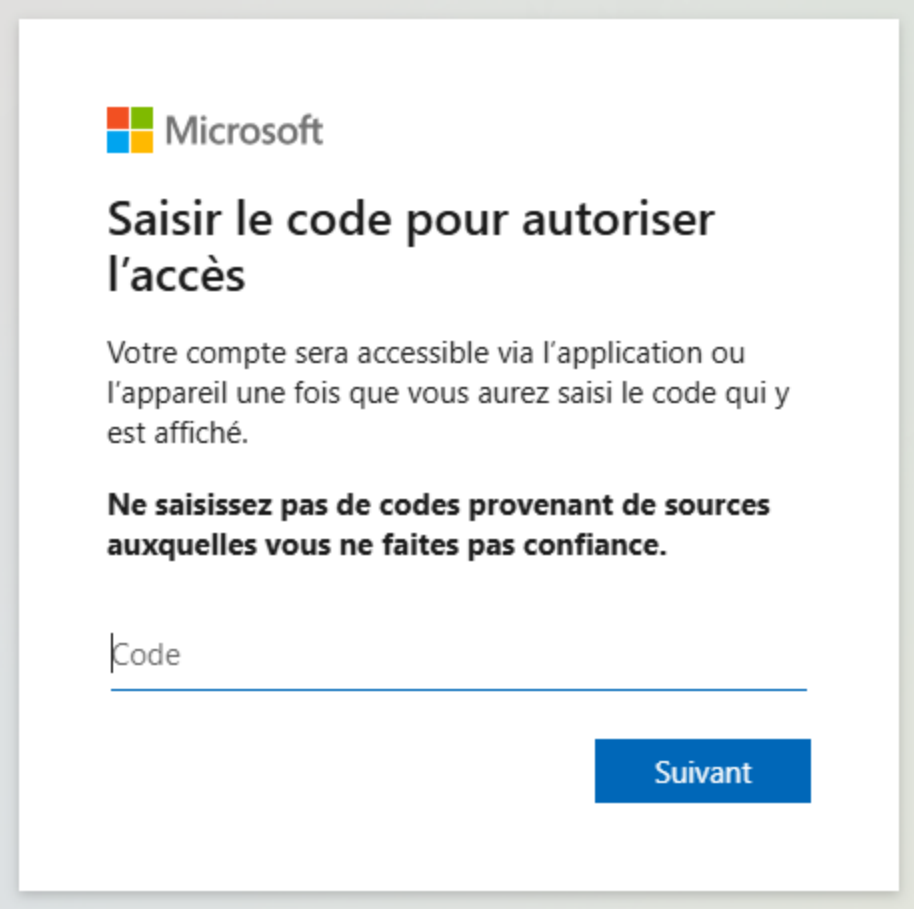
Il faut alors ouvrir un navigateur, accéder à l’url et renseigner le code.



Prompt authentification avec code M365

Exécution dans un environnement avec interface graphique

Lors de l'exécution du script, une fenêtre de navigateur s'ouvrira pour vous inviter à vous connecter avec votre compte Azure disposant des droits nécessaires. (cf. Prérequis)



Prompt authentification M365 avec code

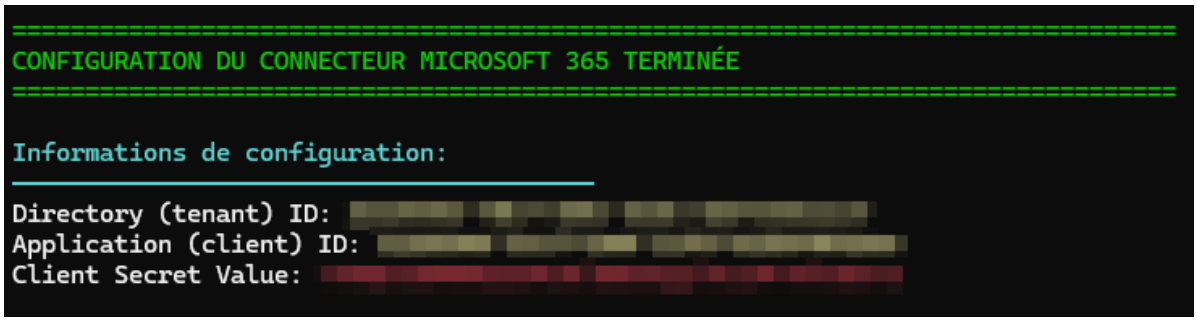
Une fois l'authentification terminée et les autorisations acceptées, la page du navigateur peut être fermée, le script poursuivra son exécution.

Récupération des informations

Après exécution, conservez précieusement les informations suivantes, affichées dans le terminal, nécessaires pour configurer votre connecteur :

- **ID de répertoire (tenant)** : Directory (tenant) ID

- **ID d’application (client)** : Application (client) ID
- **Secret client** : Valeur récupérée lors de la création du secret (à sauvegarder immédiatement, elle ne sera affichée qu’une fois)

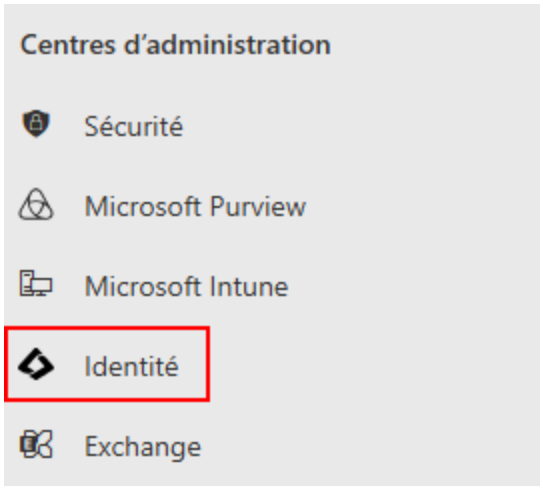


Aperçu des informations affichées dans le terminal, à conserver précieusement

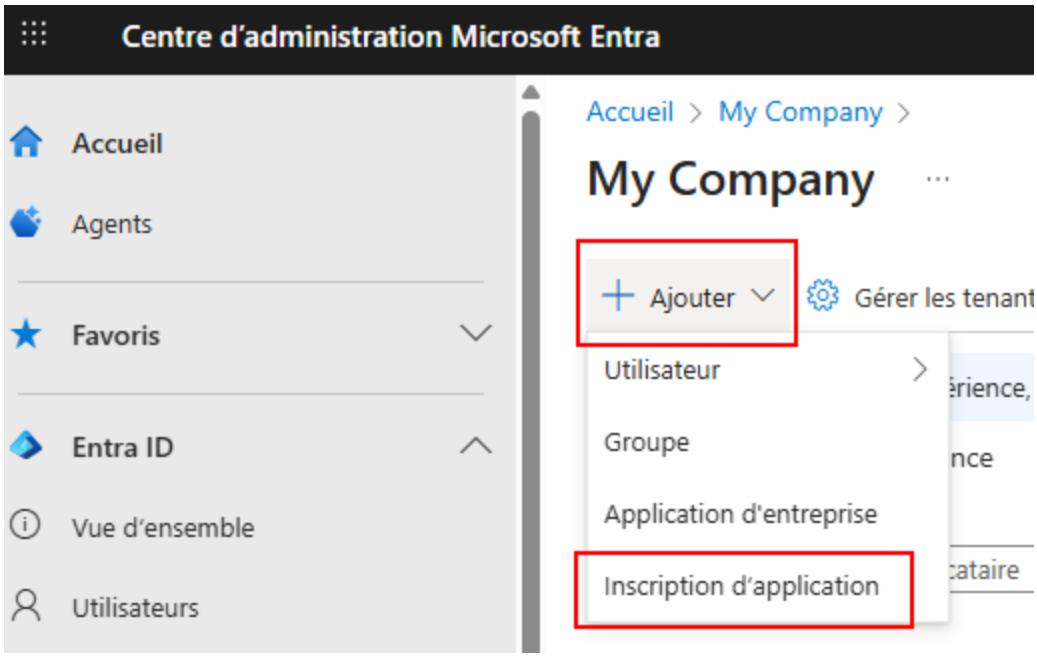
Création d’une application - méthode manuelle

Création de l’application

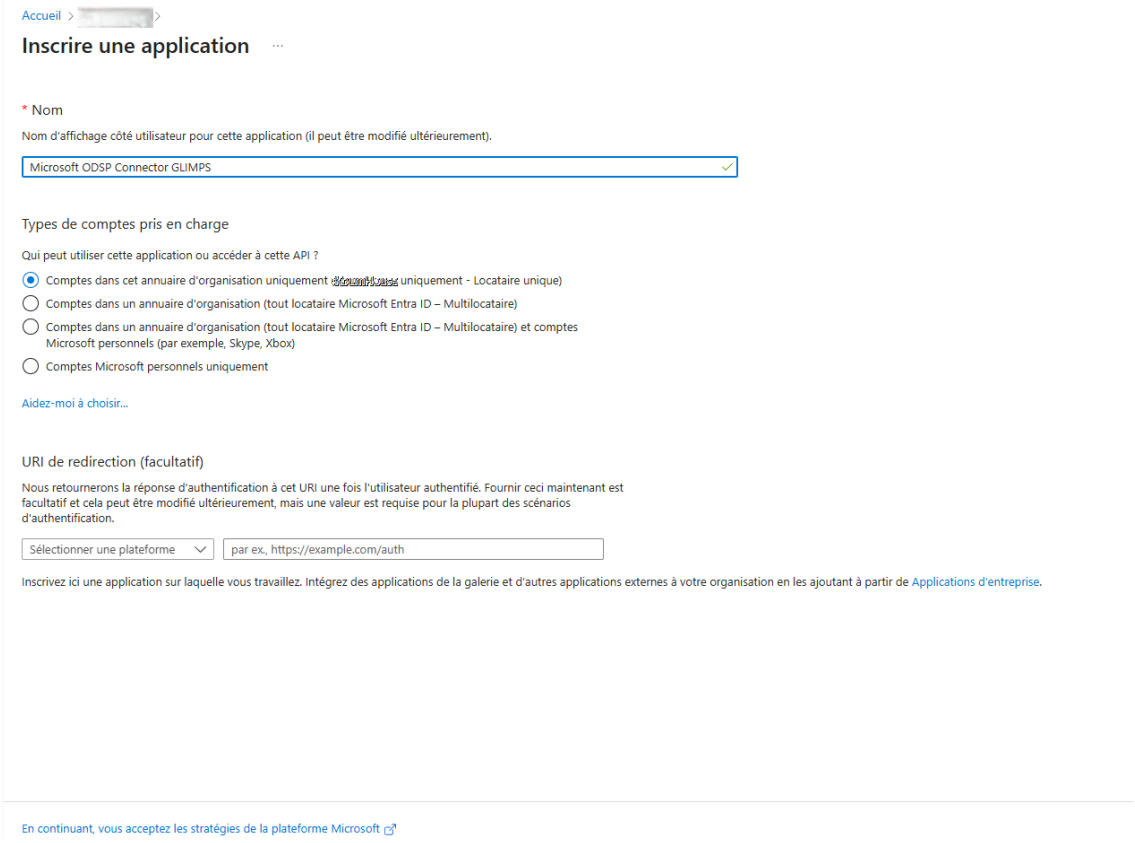
1. Connectez vous au centre d’administration Microsoft 365 (https://admin.microsoft.com/)
2. Accédez à au centre d’administration “Identité” (ou “Entra ID”) (https://entra.microsoft.com/)



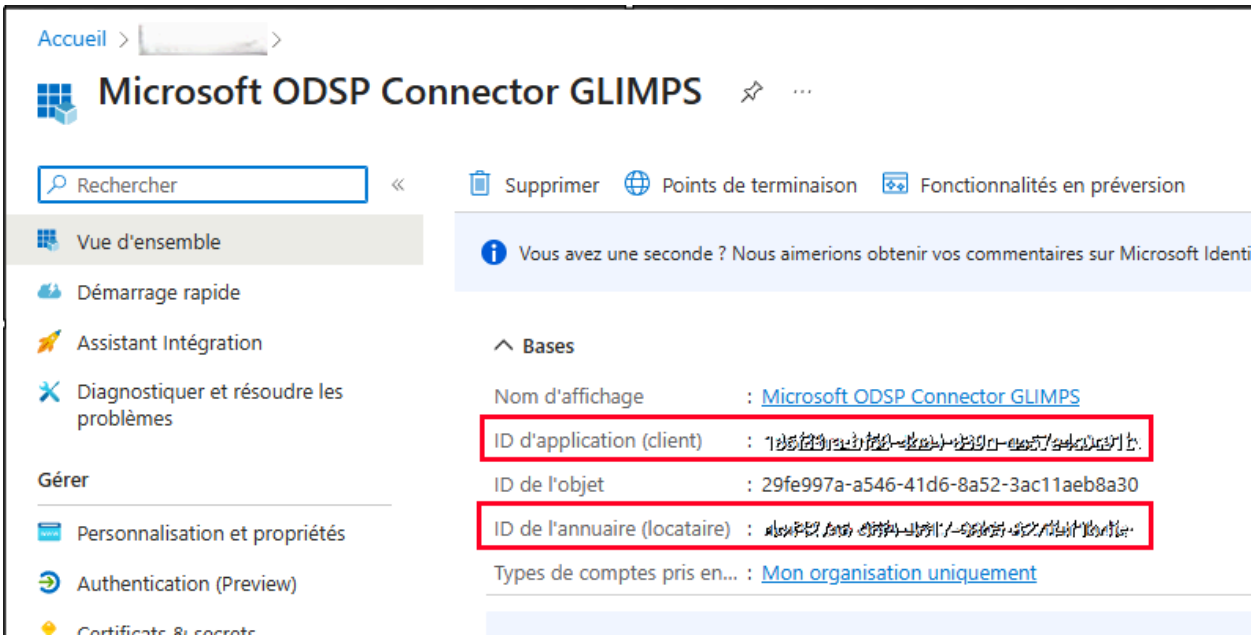
3. Cliquez sur “Vue d’ensemble”, “Ajouter” puis “Inscription d’application”



4. Renseignez les champs suivants puis valider avec le bouton “S’inscrire” :
   - **Nom** : `Microsoft ODSP Connector GLIMPS`
     - **Types de comptes pris en charge** : `Comptes dans ce répertoire organisationnel uniquement` Comptes dans cet annuaire d'organisation uniquement (My Company uniquement - Locataire unique)



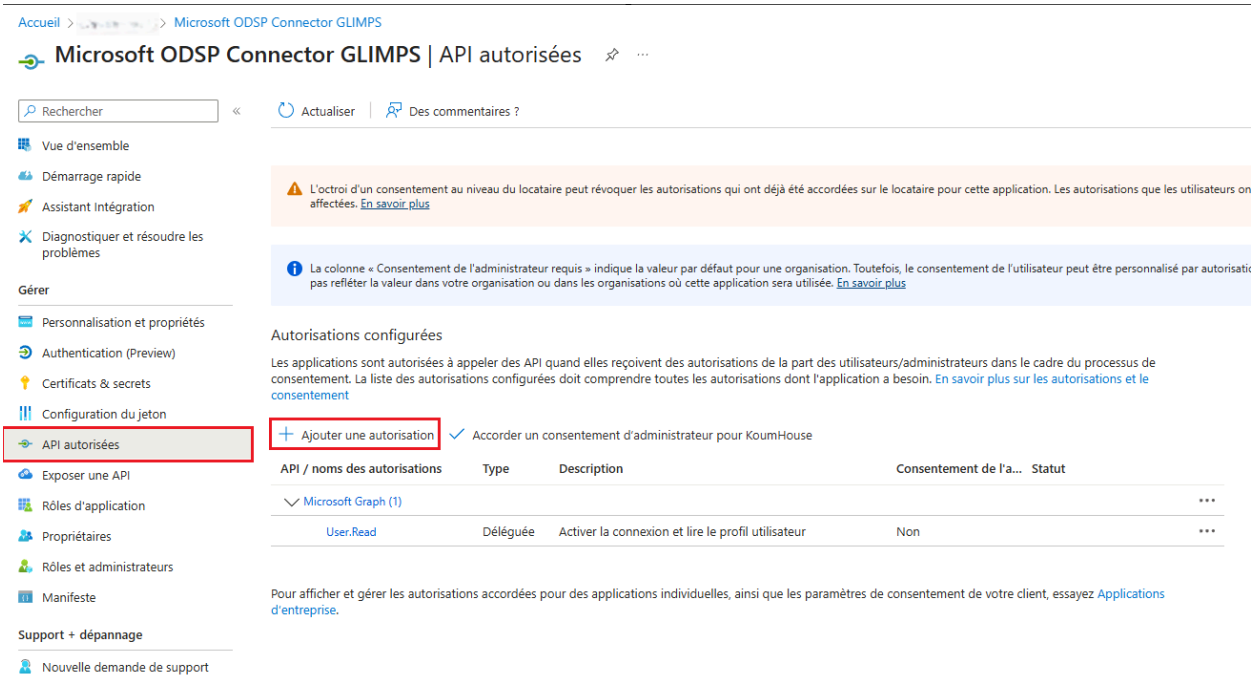
5. L'application d'entreprise est désormais inscrite, récupérez et conserver l'**ID d'application (client)** ainsi que l'**ID de l'annuaire (locataire)** depuis le menu **Vue d'ensemble,** ils seront nécessaire pour la suite de la configuration



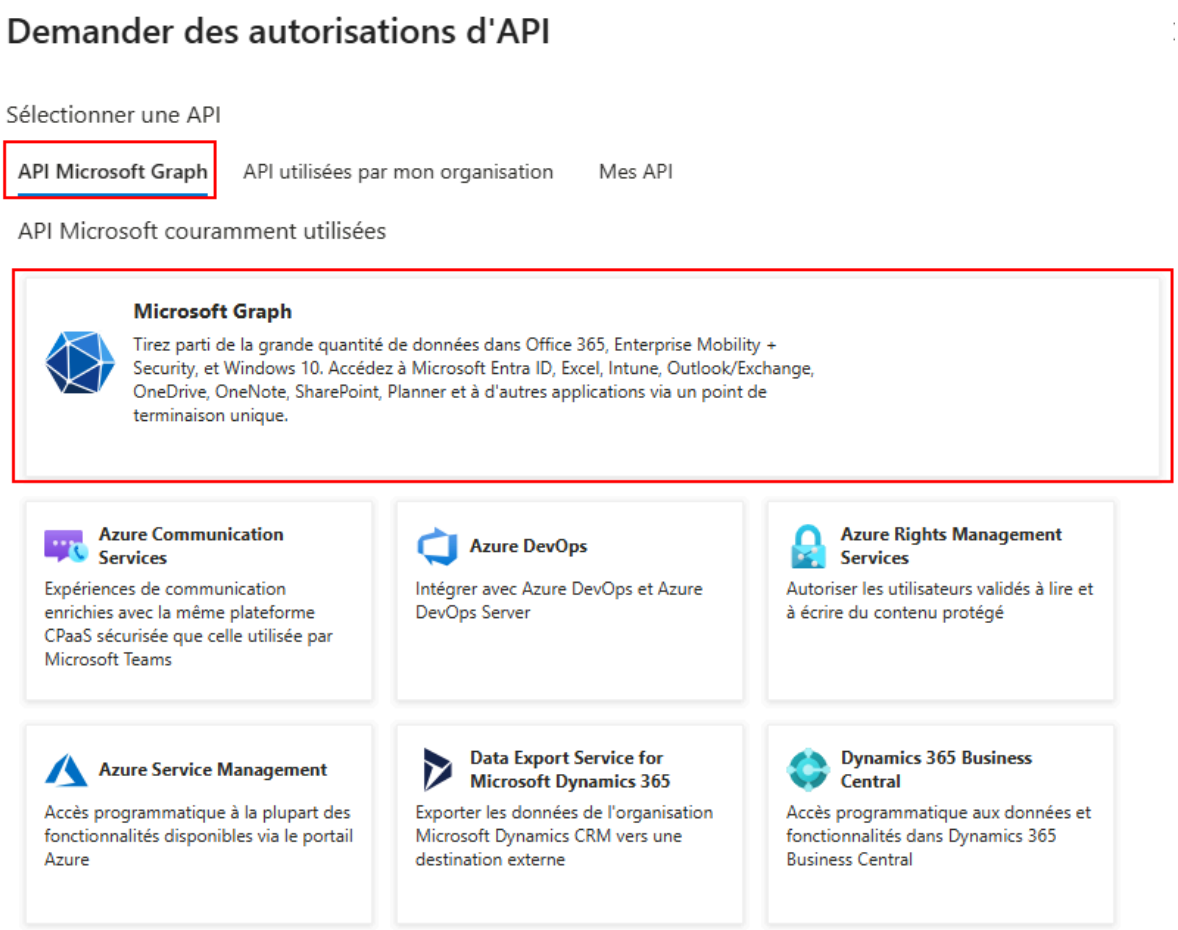
Attribution des permissions API Microsoft Graph à l’application d’entreprise

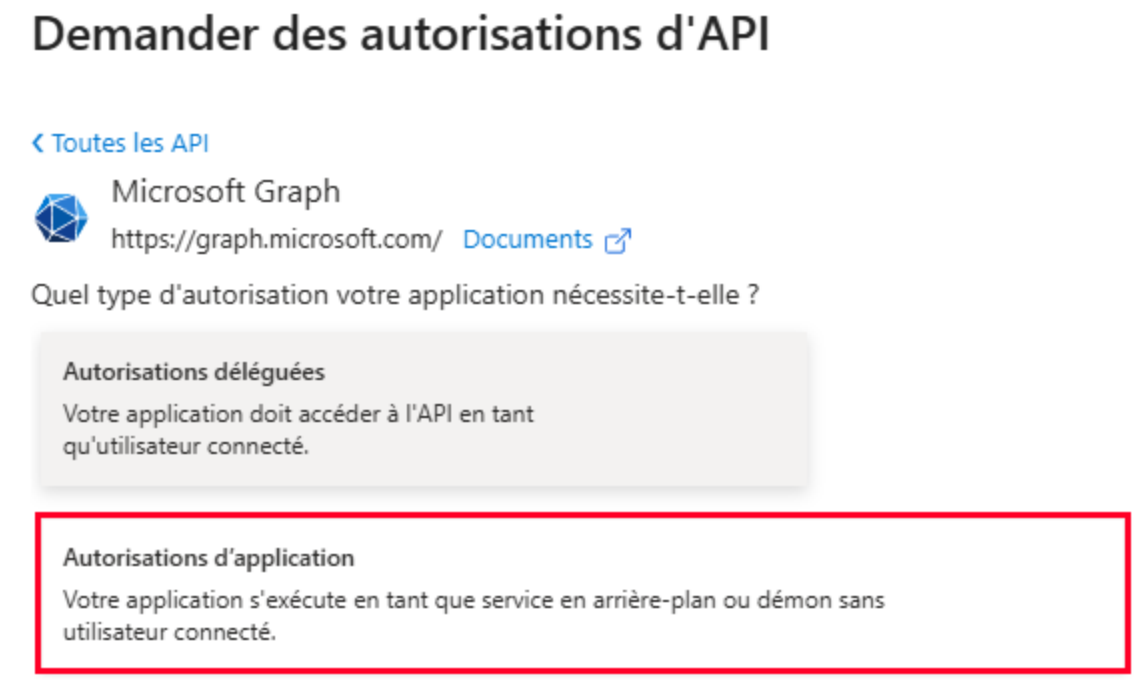
Vous devez ensuite configurer les permissions de l’API Microsoft Graph pour que l’application puisse lire, écrire et envoyer des emails.

1. Dans le menu latéral de l’application, sous la section **Gérer**, accédez à **API Autorisées** puis cliquez sur **Ajouter une autorisation**



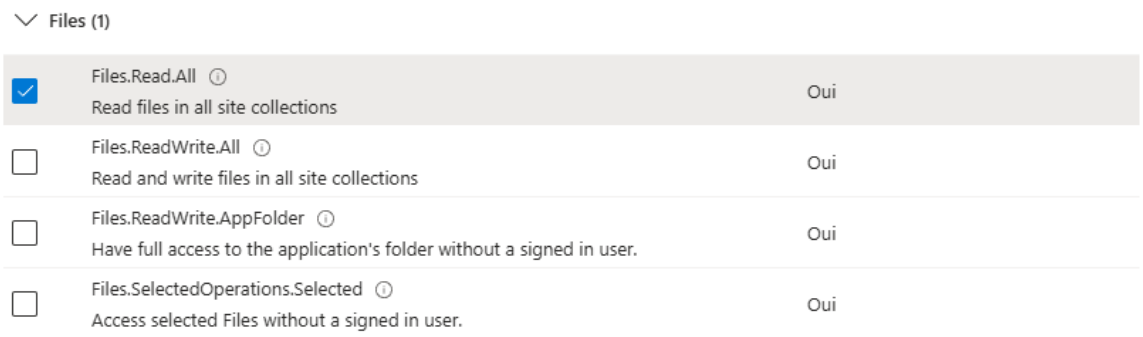
1. Dans la section **API Microsoft Graph**, cliquez sur la tuile **Microsoft Graph**


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 Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner et à d'autres applications via un point de terminaison unique.
Azure Communication Services
Expériences de communication enrichies avec la même plateforme CPaaS sécurisée que celle utilisée par Microsoft Teams
Azure DevOps
Intégrer avec Azure DevOps et Azure DevOps Server
Azure Rights Management Services
Autoriser les utilisateurs validés à lire et à écrire du contenu protégé
Azure Service Management
Accès programmatique à la plupart des fonctionnalités disponibles via le portail Azure
Data Export Service for Microsoft Dynamics 365
Exporter les données de l'organisation Microsoft Dynamics CRM vers une destination externe
Dynamics 365 Business Central
Accès programmatique aux données et fonctionnalités dans Dynamics 365 Business Central

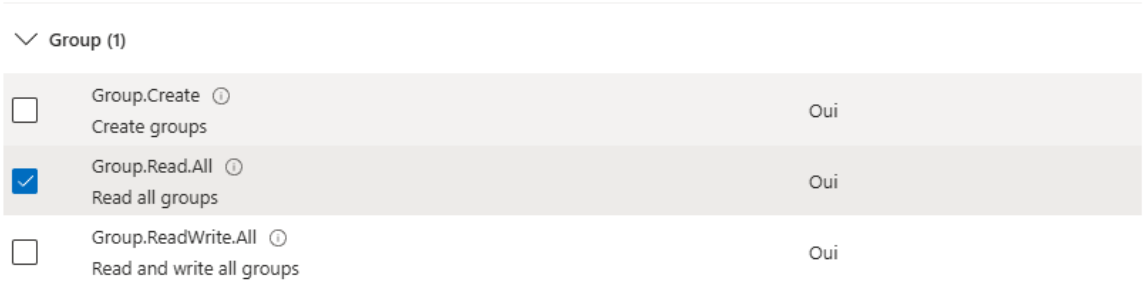

Demander des autorisations d'API
Toutes les API
Microsoft Graph
https://graph.microsoft.com/ Documents
Quel type d'autorisation votre application nécessite-t-elle ?
Autorisations déléguées
Votre application doit accéder à l'API en tant qu'utilisateur connecté.
Autorisations d'application
Votre application s'exécute en tant que service en arrière-plan ou démon sans utilisateur connecté.

2. Sélectionnez le type d'autorisation **Autorisations d'application** puis recherchez et sélectionnez les permissions suivantes :

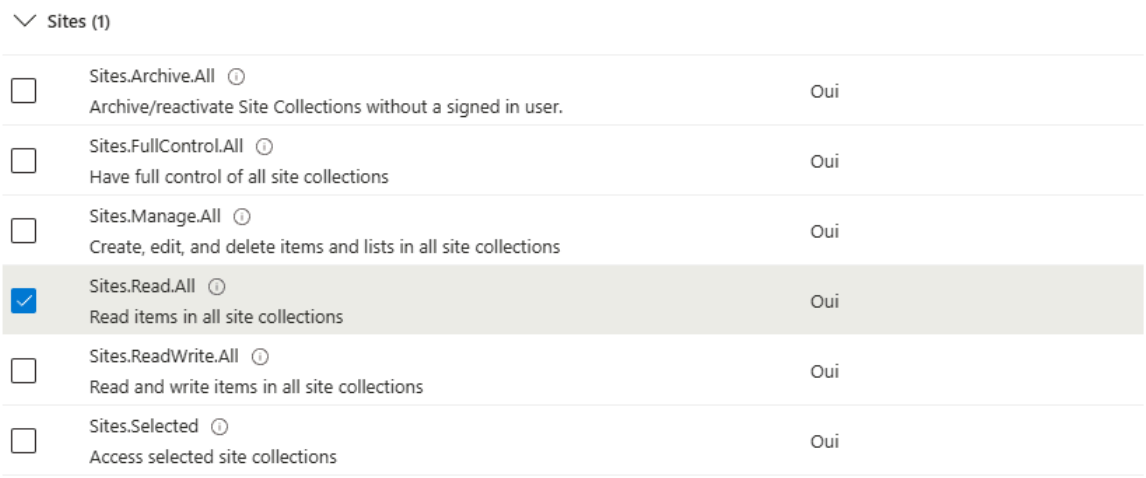
- **File.ReadWrite.All**
  Permet à l'application de lire, créer, mettre à jour et supprimer tous les fichiers dans tous les sites et bibliothèques de documents de l'organisation, y compris les fichiers dans OneDrive et SharePoint. Ce droit donne un accès complet en lecture et écriture à tous les fichiers de l'organisation.



- **Group.Read.All**
  Permet à l'application de lire toutes les propriétés des groupes dans l'organisation, y compris l'appartenance aux groupes, sans utilisateur connecté. Ce droit donne un accès en lecture seule à tous les groupes de l'organisation et leurs métadonnées

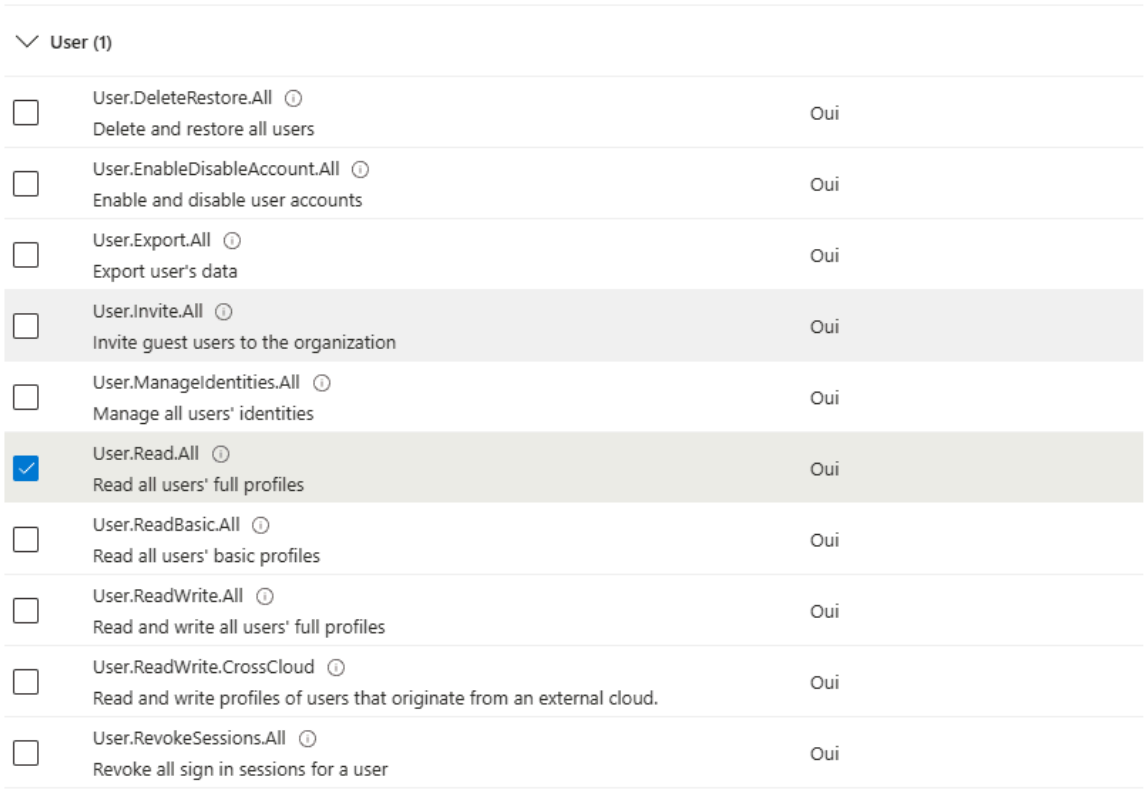


- **Sites.Read.All**
  Permet à l'application de lire les collections de sites, les listes et les éléments dans tous les sites de l'organisation. Ce droit donne un accès en lecture seule à tous les sites SharePoint de l'organisation, y compris leur structure et leur contenu.

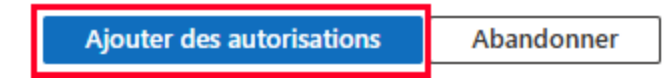


- **User.Read.All**

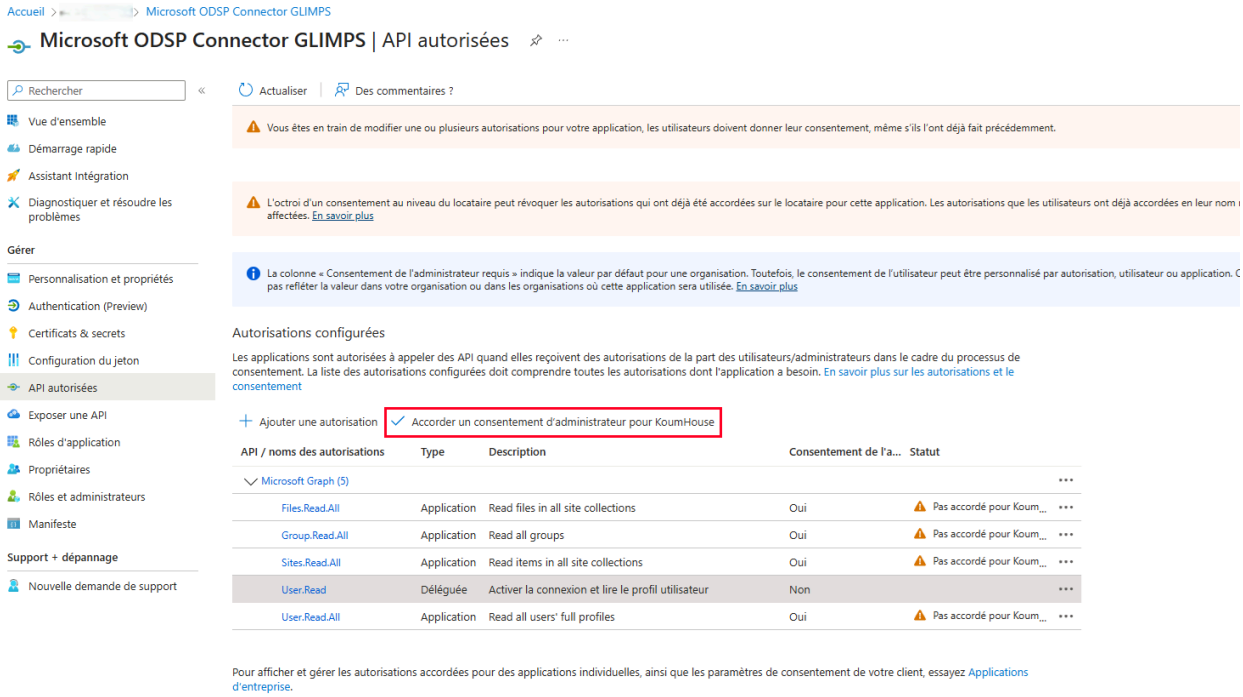
  Permet à l'application de lire le profil de l'utilisateur connecté. Ce droit donne accès aux informations de base du profil utilisateur telles que le nom, l'adresse e-mail, et d'autres propriétés du profil de l'utilisateur actuellement authentifié.



3. Cliquez sur **Ajouter des autorisations**



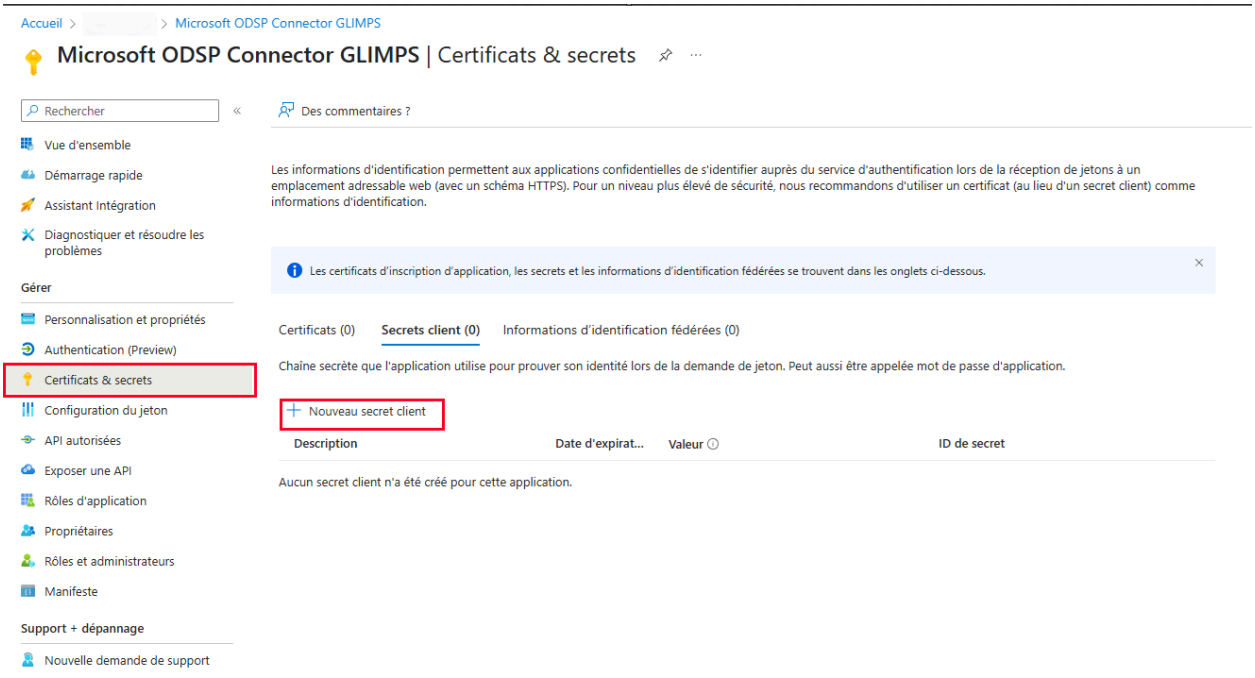
1. Au dessus tu tableau récapitulatif des autorisations, cliquez sur **Accorder le consentement administrateur pour [nom de votre organisation]** puis confirmer le consentement en cliquant sur **Oui**



1. Après quelques secondes, le consentement est validé et le statut des autorisations devient “Accordé pour [nom de votre organisation]”

Création du secret client

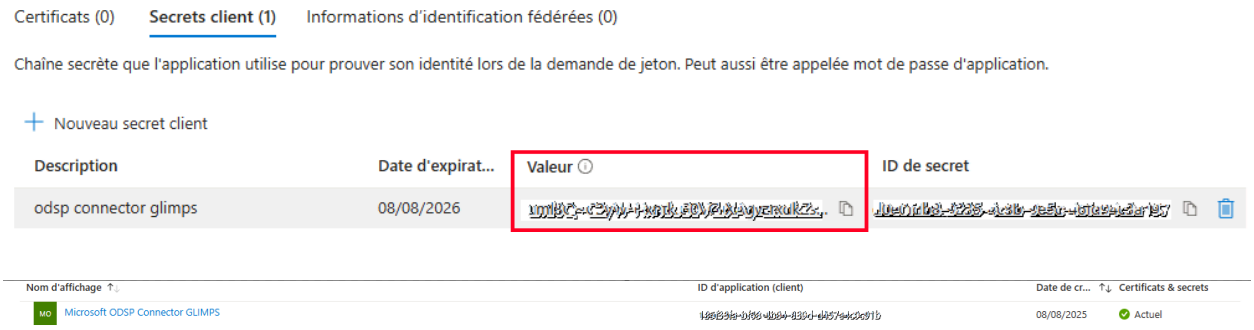
1. Dans le menu latéral de l'application, sous la section **Gérer**, accédez à **Certificats & secrets** puis cliquez sur **Nouveau secret client**



1. Renseignez les champs suivants puis cliquez sur **Ajouter** :
   - **Description** : `odsp connector glimps`
   - **Date d'expiration** : Microsoft recommande 6 mois, mais nous recommandons 12 mois


Ajouter un secret client
Description
odsp connector glimps
Date d'expiration
365 jours (12 mois)
Ajouter
Annuler

2. **Important** : Sauvegardez immédiatement la valeur du champ `Valeur` (par exemple dans un gestionnaire de mots de passe type KeePass, coffre-fort, etc.). **Cette valeur sera nécessaire pour la configuration et ne sera plus accessible par la suite**.



Informations requises pour la suite de la configuration

Pour la suite de la configuration, vous aurez besoin des éléments suivants :

- **ID de répertoire (tenant)** ou **ID de l'annuaire (locataire)** : Valeur récupérée lors de l'étape "Création de l'application"
- **ID d'application (client)** : Valeur récupérée lors de l'étape "Création de l'application"
- **Secret client** : Valeur récupérée lors de l'étape "Création du secret client"

Déploiement du connecteur en SaaS

Dans le cadre d'un déploiement en mode SaaS (hébergé par GLIMPS), veuillez fournir les éléments de configuration et personnalisations éventuelles évoqués ci-dessus à votre contact technique GLIMPS.

Déploiement du connecteur en local

Dans le cadre d'un déploiement en local, veuillez vous référer à la documentation `Documentation_Microsoft ODSP connector_Docker-Compose-GLIMPS-Malware[...].pdf` pour poursuivre la configuration.