



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=pdpsshare>
- 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 où 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.



Autorisations demandées

Microsoft Graph Command Line Tools

Microsoft Corporation

Cette application souhaite :

- ✓ Read and write all applications
- ✓ Manage app permission grants and app role assignments
- ✓ Lire les données de l'annuaire
- ✓ Afficher le profil de base des utilisateurs
- ✓ Conserver l'accès aux données auxquelles vous lui avez donné accès
- Consentement pour le compte de votre organisation

Si vous acceptez, cette application aura accès aux ressources spécifiées pour tous les utilisateurs de votre organisation. Personne d'autre ne sera invité à passer en revue ces autorisations.

Accepter ces autorisations signifie que vous autorisez cette application à utiliser vos données comme indiqué dans les [conditions d'utilisation du service](#) et la [déclaration de confidentialité](#). Vous pouvez modifier ces autorisations à l'adresse <https://myapps.microsoft.com>. [Afficher les détails](#)

Cette application semble-t-elle suspecte ? [Signaler ici](#)

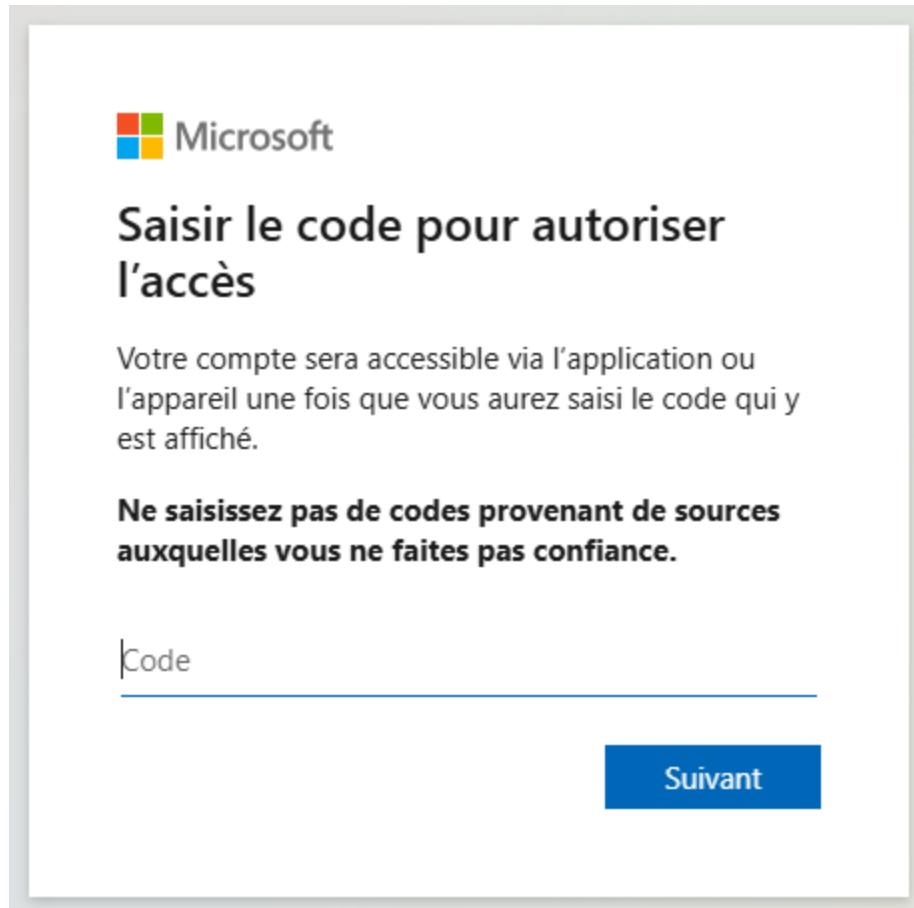
Annuler

Accepter

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)

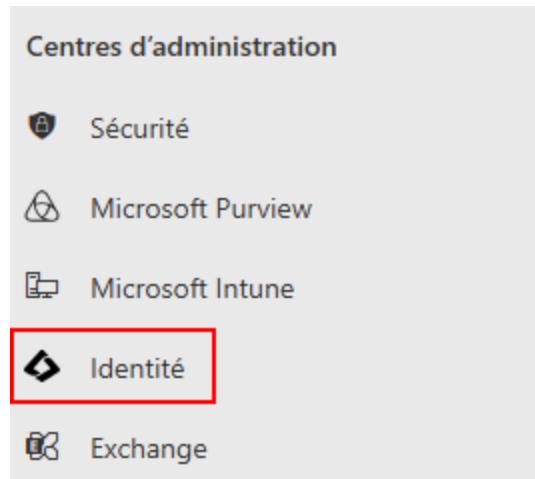
```
=====  
CONFIGURATION DU CONNECTEUR MICROSOFT 365 TERMINÉE  
=====  
  
Informations de configuration:  
-----  
Directory (tenant) ID: [REDACTED]  
Application (client) ID: [REDACTED]  
Client Secret Value: [REDACTED]
```

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"

The screenshot shows the Microsoft Entra Admin Center interface. On the left, there's a navigation sidebar with links like Accueil, Agents, Favoris, Entra ID, Vue d'ensemble, and Utilisateurs. The main area is titled 'My Company' and shows a breadcrumb path: Accueil > My Company > My Company. Below the title, there are four main options: 'Ajouter' (with a plus sign icon), 'Gérer les tenant' (with a gear icon), 'Utilisateur', and 'Groupe'. A red box highlights the 'Ajouter' button. To its right, there are three more options: 'Application d'entreprise', 'Inscription d'application', and 'Locataire'. Another red box highlights the 'Inscription d'application' button.

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)

Accueil >  >

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 ([Mon organisation](#) 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'authe... 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'authe...

Inscrivez ici une application sur laquelle vous travaillez. Intégrez des applications de la galerie et d'autres applications externes à votre organisation en les ajoutant à partir de [Applications d'entreprise](#).

[En continuant, vous acceptez les stratégies de la plateforme Microsoft](#) 

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

Accueil >  >

Microsoft ODSP Connector GLIMPS

 Rechercher  Supprimer Points de terminaison Fonctionnalités en préversion

 Vous avez une seconde ? Nous aimerais obtenir vos commentaires sur Microsoft Identity

 **Bases**

Nom d'affichage	: Microsoft ODSP Connector GLIMPS
ID d'application (client)	: 1052313-3114-4e39-9457-3430111
ID de l'objet	: 29fe997a-a546-41d6-8a52-3ac11aeb8a30
ID de l'annuaire (locataire)	: 1052313-3114-4e39-9457-3430111
Types de comptes pris en...	: Mon organisation uniquement

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**

The screenshot shows the Microsoft ODSP Connector GLIMPS application settings page. On the left, there is a sidebar with various options like Vue d'ensemble, Démarrage rapide, Assistant Intégration, Diagnostiquer et résoudre les problèmes, Gérer, Personnalisation et propriétés, Authentication (Preview), Certificats & secrets, Configuration du jeton, API autorisées (which is highlighted with a red box), Exposer une API, Rôles d'application, Propriétaires, Rôles et administrateurs, Manifeste, Support + dépannage, and Nouvelle demande de support.

The main content area is titled "Microsoft ODSP Connector GLIMPS | API autorisées". It has a search bar, refresh button, and a "Des commentaires ?" link. A warning message states: "L'octroi d'un consentement au niveau du locataire peut révoquer les autorisations qui ont déjà été accordées sur le locataire pour cette application. Les autorisations que les utilisateurs ont affectées." Below it, a note says: "La colonne « Consentement de l'administrateur requis » indique la valeur par défaut pour une organisation. Toutefois, le consentement de l'utilisateur peut être personnalisé par autorisation et refléter la valeur dans votre organisation ou dans les organisations où cette application sera utilisée." A "Ajouter une autorisation" button is visible. The "Autorisations configurées" section lists "Microsoft Graph (1)" with a "User.Read" permission entry. The table columns are API / noms des autorisations, Type, Description, Consentement de l'a..., and Statut. The "User.Read" entry shows Type: Déléguée, Description: Activer la connexion et lire le profil utilisateur, Consentement de l'a...: Non, and Statut: ... (with a three-dot ellipsis).

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.

▼ Files (1)

<input checked="" type="checkbox"/>	Files.Read.All ⓘ Read files in all site collections	Oui
<input type="checkbox"/>	Files.ReadWrite.All ⓘ Read and write files in all site collections	Oui
<input type="checkbox"/>	Files.ReadWrite.AppFolder ⓘ Have full access to the application's folder without a signed in user.	Oui
<input type="checkbox"/>	Files.SelectedOperations.Selected ⓘ Access selected Files without a signed in user.	Oui

- **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

▼ Group (1)

<input type="checkbox"/>	Group.Create ⓘ Create groups	Oui
<input checked="" type="checkbox"/>	Group.Read.All ⓘ Read all groups	Oui
<input type="checkbox"/>	Group.ReadWrite.All ⓘ Read and write all groups	Oui

- **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.

Sites (1)		
<input type="checkbox"/>	SitesArchive.All ⓘ Archive/reactivate Site Collections without a signed in user.	Oui
<input type="checkbox"/>	SitesFullControl.All ⓘ Have full control of all site collections	Oui
<input type="checkbox"/>	SitesManage.All ⓘ Create, edit, and delete items and lists in all site collections	Oui
<input checked="" type="checkbox"/>	SitesRead.All ⓘ Read items in all site collections	Oui
<input type="checkbox"/>	SitesReadWrite.All ⓘ Read and write items in all site collections	Oui
<input type="checkbox"/>	SitesSelected ⓘ Access selected site collections	Oui

- **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.

User (1)		
<input type="checkbox"/>	UserDeleteRestore.All ⓘ Delete and restore all users	Oui
<input type="checkbox"/>	UserEnableDisableAccount.All ⓘ Enable and disable user accounts	Oui
<input type="checkbox"/>	UserExport.All ⓘ Export user's data	Oui
<input type="checkbox"/>	UserInvite.All ⓘ Invite guest users to the organization	Oui
<input type="checkbox"/>	UserManageIdentities.All ⓘ Manage all users' identities	Oui
<input checked="" type="checkbox"/>	UserRead.All ⓘ Read all users' full profiles	Oui
<input type="checkbox"/>	UserReadBasic.All ⓘ Read all users' basic profiles	Oui
<input type="checkbox"/>	UserReadWrite.All ⓘ Read and write all users' full profiles	Oui
<input type="checkbox"/>	UserReadWrite.CrossCloud ⓘ Read and write profiles of users that originate from an external cloud.	Oui
<input type="checkbox"/>	UserRevokeSessions.All ⓘ Revoke all sign in sessions for a user	Oui

3. Cliquez sur Ajouter des autorisations



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

Accueil > Microsoft ODSP Connector GLIMPS > Microsoft ODSP Connector GLIMPS | 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, même s'ils l'ont déjà fait précédemment.

L'octroi d'un consentement au niveau du locataire peut révoquer les autorisations qui ont déjà été accordées sur le locataire pour cette application. Les autorisations que les utilisateurs ont déjà accordées en leur nom sont affectées. [En savoir plus](#)

La colonne « Consentement de l'administrateur requis » indique la valeur par défaut pour une organisation. Toutefois, le consentement de l'utilisateur peut être personnalisé par autorisation, utilisateur ou application. Cela reflète la valeur dans votre organisation ou dans les organisations où cette application sera utilisée. [En savoir plus sur les autorisations et le consentement](#)

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 KoumHouse

API / noms des autorisations	Type	Description	Consentement de l'a...	Statut
Microsoft Graph (5)				...
Files.Read.All	Application	Read files in all site collections	Oui	⚠ Pas accordé pour Koum... ...
Group.Read.All	Application	Read all groups	Oui	⚠ Pas accordé pour Koum... ...
Sites.Read.All	Application	Read items in all site collections	Oui	⚠ Pas accordé pour Koum... ...
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur	Non	...
User.Read.All	Application	Read all users' full profiles	Oui	⚠ Pas accordé pour Koum... ...

Pour afficher et gérer les autorisations accordées pour des applications individuelles, ainsi que les paramètres de consentement de votre client, essayez [Applications d'entreprise](#).

Confirmation d'accord de consentement d'administrateur.

Voulez-vous donner le consentement pour les autorisations demandées pour tous les comptes dans [\[nom de votre organisation\]](#) ?
Cette action mettra à jour les consentements administrateur existants de cette application pour qu'ils correspondent à ce qui est indiqué ci-dessous.

Oui

Non

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

Ajouter une autorisation ✓ Accorder un consentement d'administrateur pour					
API / noms des autorisations	Type	Description	Consentement de l'a...	Statut	
▼ Microsoft Graph (5)					
Files.Read.All	Application	Read files in all site collections	Oui	✓ Accordé pour	...
Group.Read.All	Application	Read all groups	Oui	✓ Accordé pour	...
Sites.Read.All	Application	Read items in all site collections	Oui	✓ Accordé pour	...
User.Read	Déléguée	Activer la connexion et lire le profil utilisateur	Non	✓ Accordé pour	...
User.Read.All	Application	Read all users' full profiles	Oui	✓ Accordé pour	...

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**

The screenshot shows the Microsoft ODSP Connector GLIMPS application settings page. The left sidebar has a 'Gérer' section with several options like 'Personnalisation et propriétés', 'Authentication (Preview)', and 'Certificates & secrets' (which is highlighted with a red box). The main area shows a message about using certificates for authentication. Below it, there's a table for managing secrets with columns for 'Description', 'Date d'expiration...', 'Valeur ⓘ', and 'ID de secret'. A note says 'Aucun secret client n'a été créé pour cette application.'

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

X

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.**

Certificats (0)	<u>Secrets client (1)</u>	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 ⓘ
odsp connector glimps	08/08/2026	  
Nom d'affichage ↗	ID d'application (client)	Date de cr... ↗ Certificats & secrets
Microsoft ODSP Connector GLIMPS	166346-0104-0004-0001-000000000000	08/08/2025 Actuel

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.