Configuration d'un accès sécurisé avec Office 365 pour une prévention améliorée des pertes de données

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Configuration sur Azure
- Configuration dans Secure Access

Vérifier

Informations connexes

Introduction

Ce document décrit l'intégration de Data Loss Prevention pour Office 365 avec Secure Access.

Conditions préalables

- **Office 365 E3 Subscription** est présent pour votre service partagé Microsoft
  - L'audit de conformité est configuré comme **ON** dans le portail de conformité avant que vous ne commenciez votre intégration

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé Cisco
- Applications Microsoft Azure Enterprise et inscriptions d'applications

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Accès sécurisé Cisco

- Microsoft Azure
- Portail de conformité Microsoft 365

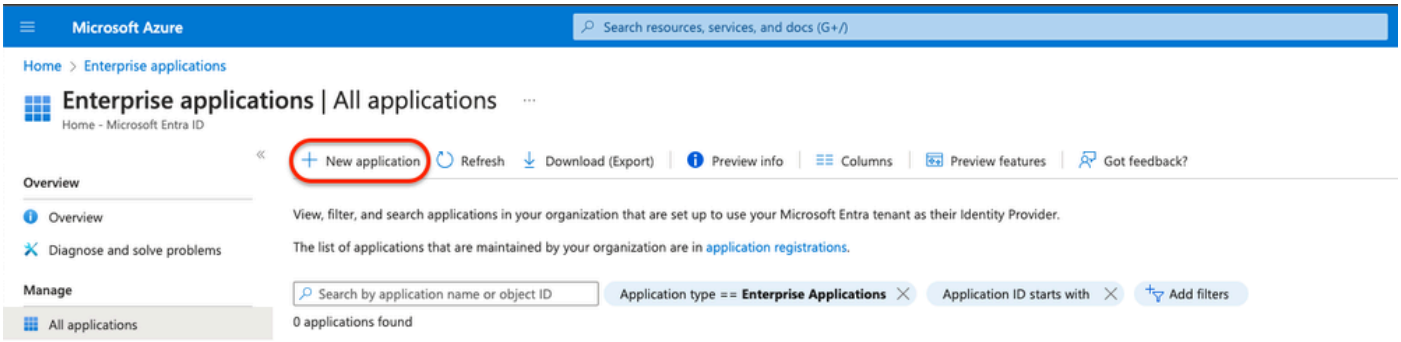
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

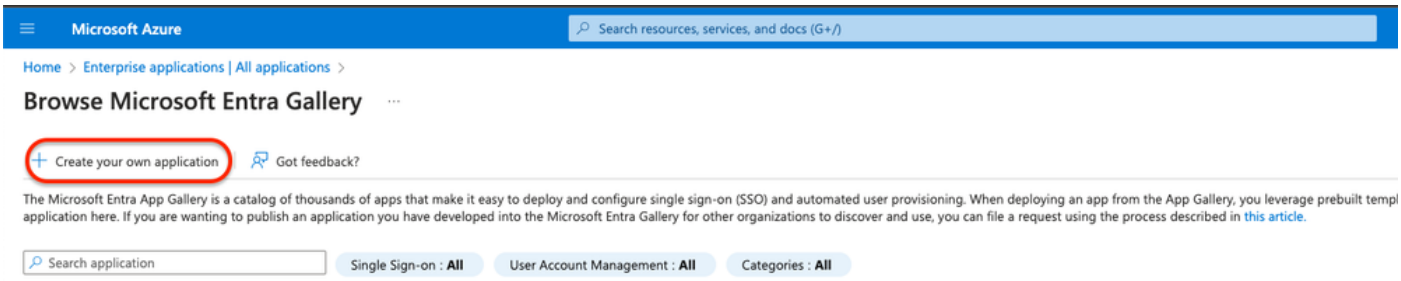
Configuration sur Azure

Pour activer l'application sur Azure, configurez selon les étapes suivantes :

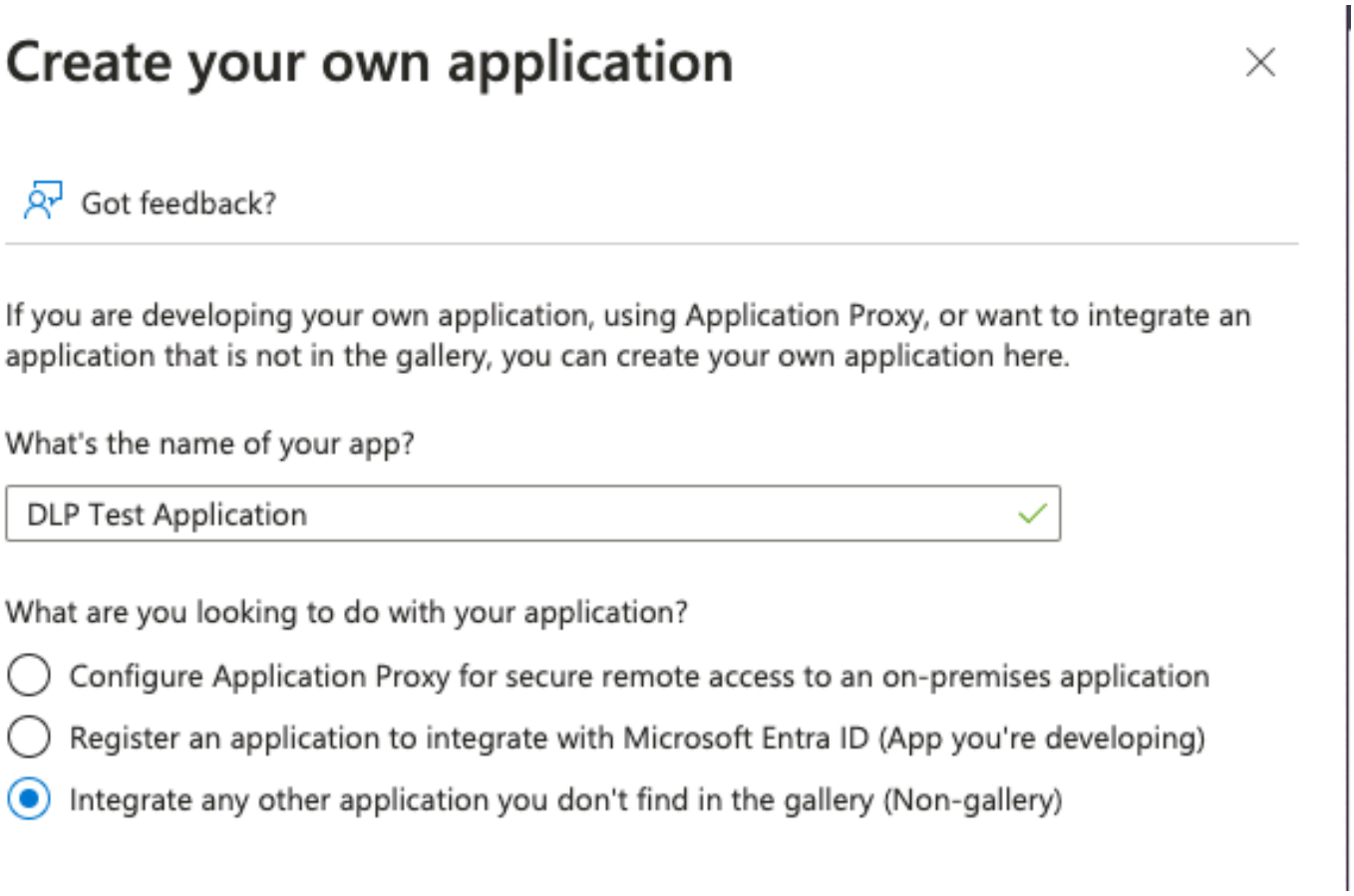
1. Accédez à la **Azure Portal > Enterprise Applications > New Application**.



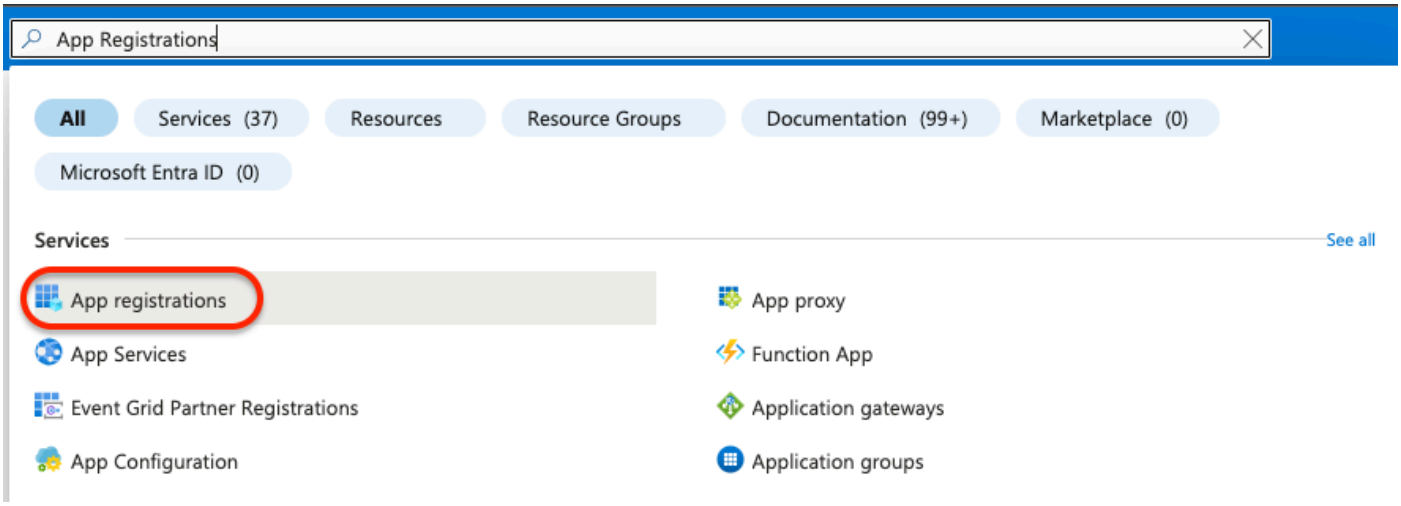
2. Cliquez sur **Create your own Application**.



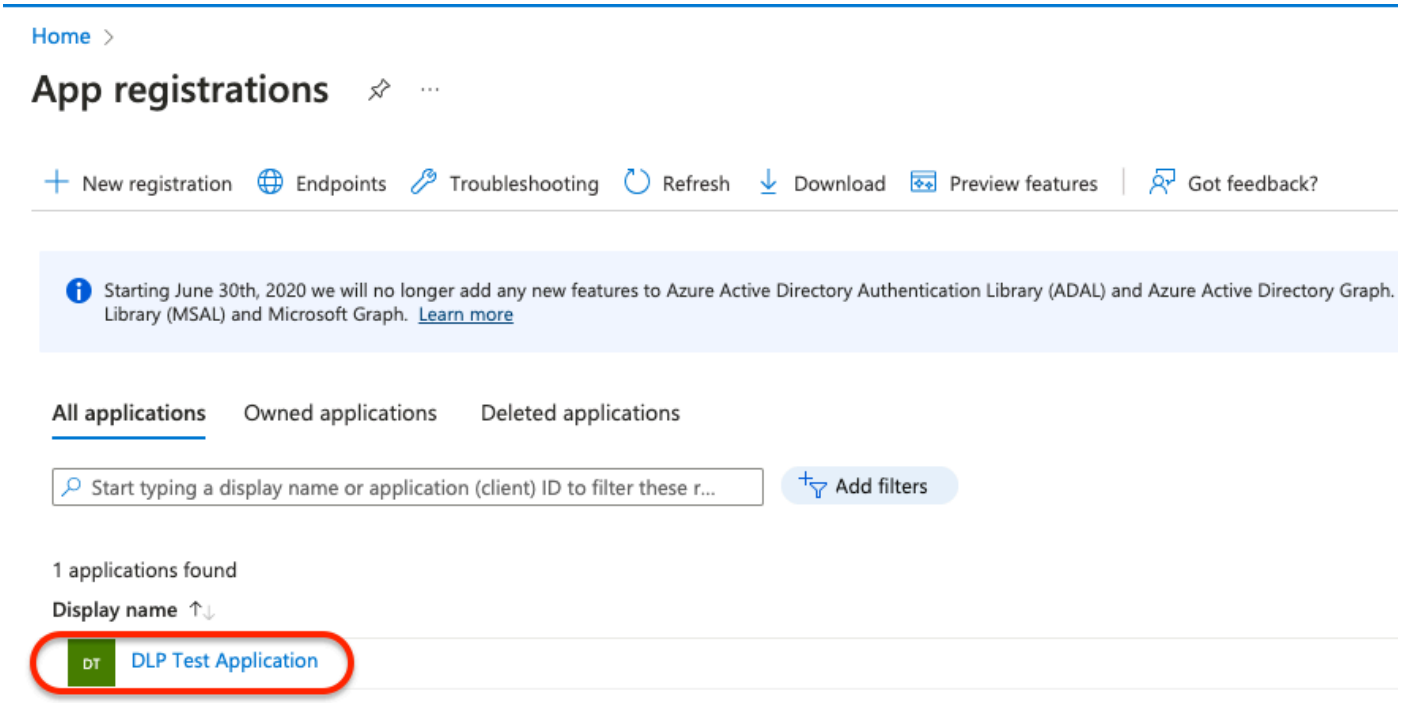
3. Donnez un nom que vous souhaitez identifier l'application et choisissez. **Integrate any other application you don't find in the gallery (Non-Gallery)**.



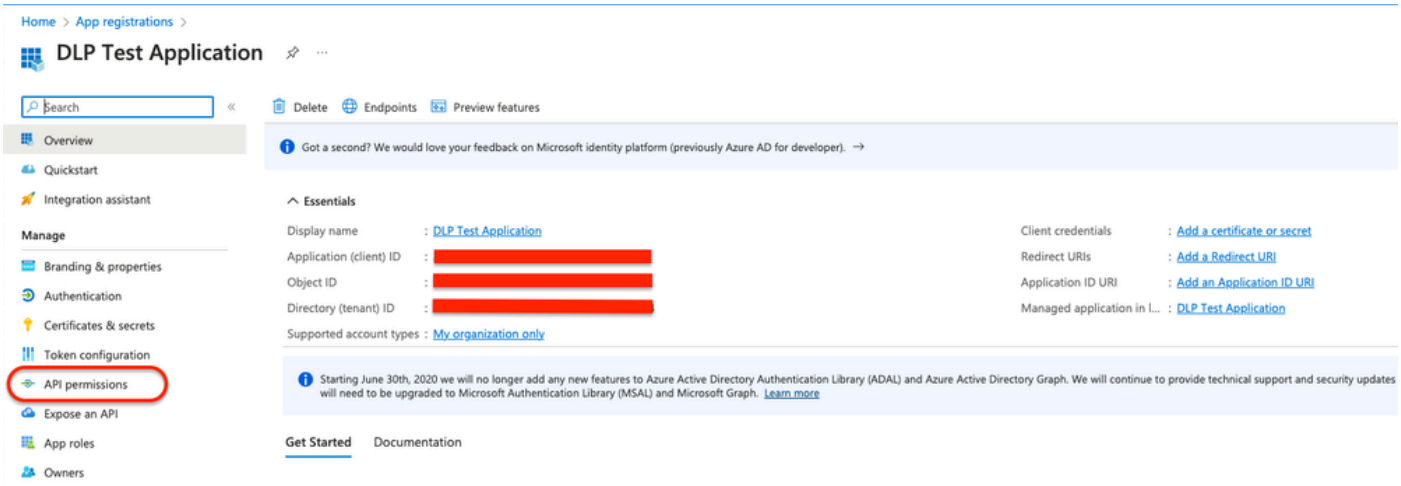
4. Une fois terminé, utilisez la barre de recherche Azure pour rechercher **App Registrations**.



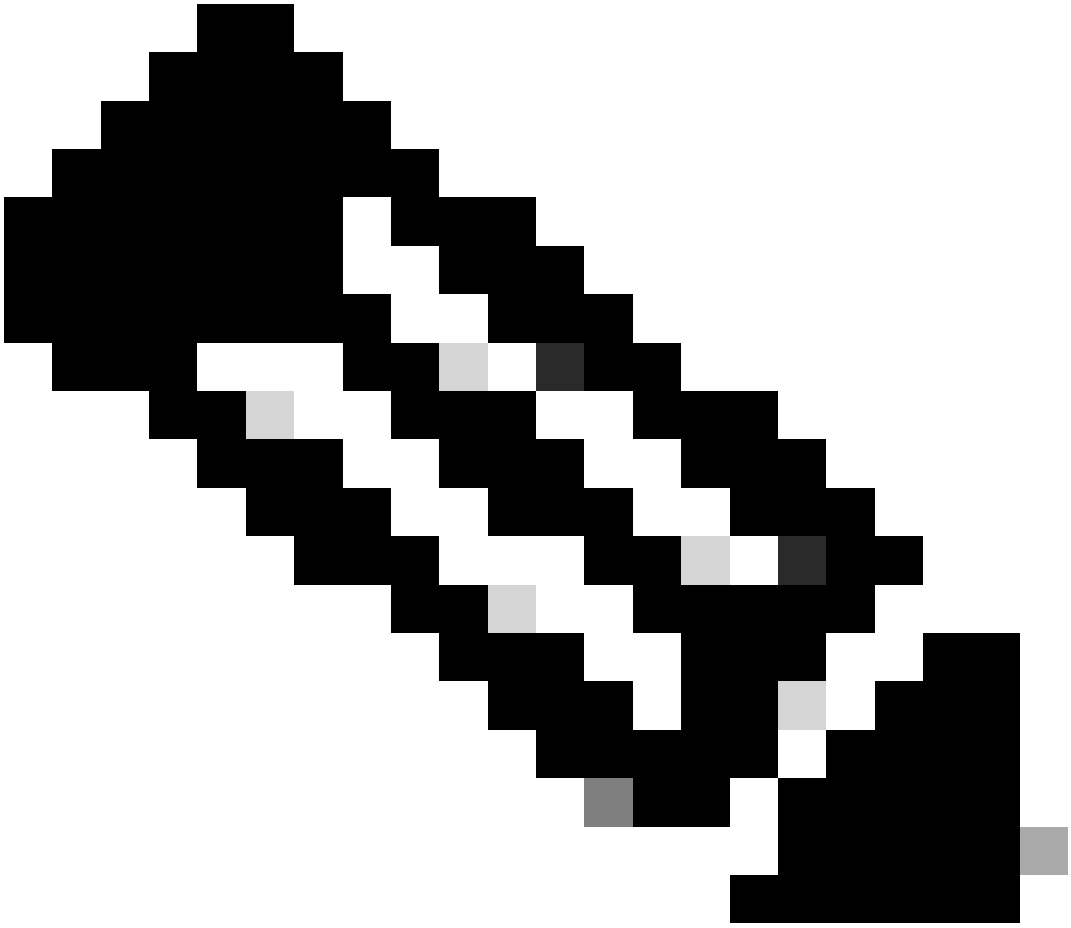
5. Cliquez sur **All Applications** et choisissez l'application créée à l'étape trois.



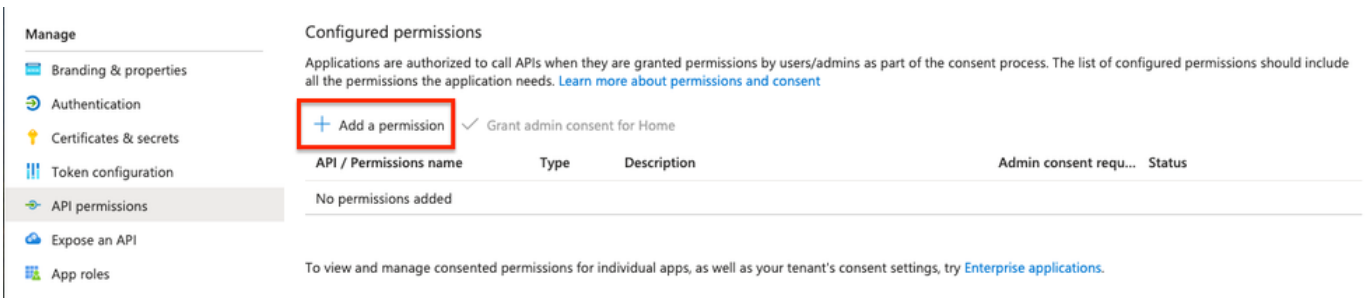
6. Sélectionnez **API Permissions**.



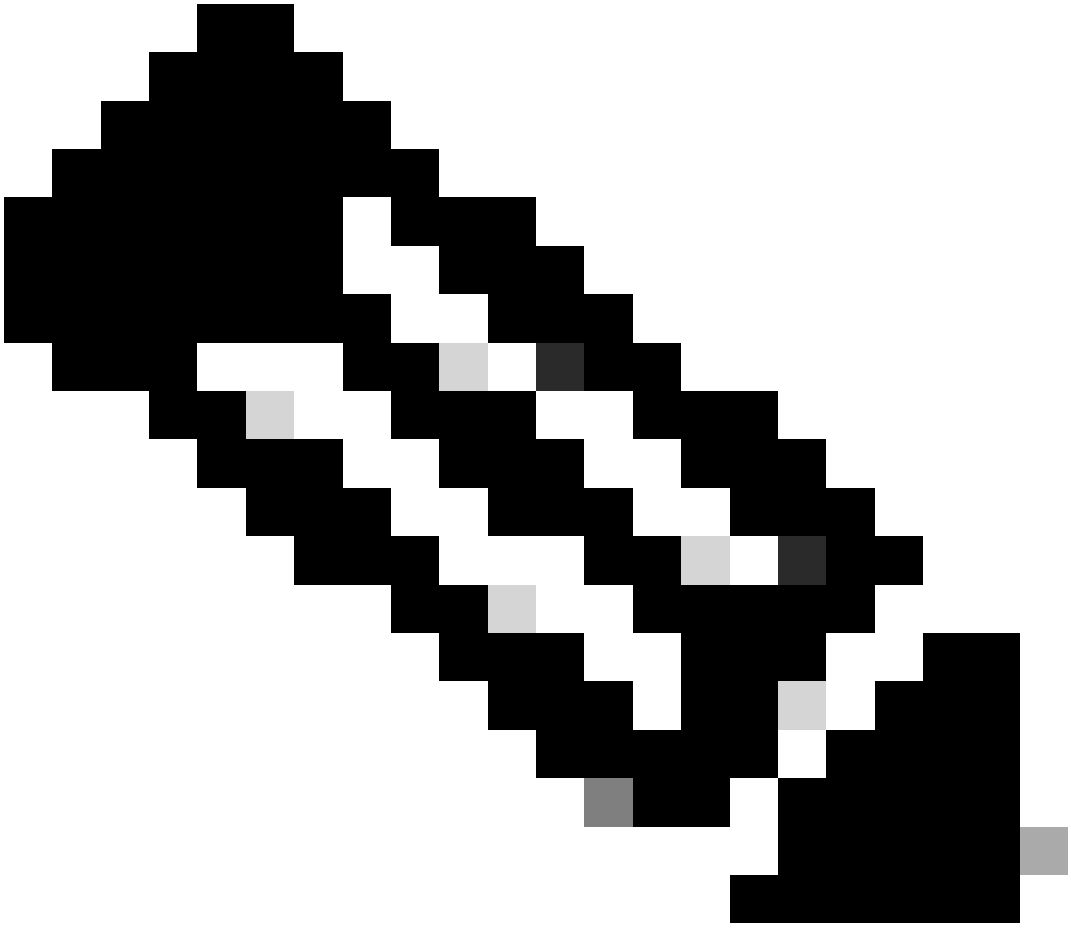
7. Cliquez sur **Add a permission** et choisissez les autorisations requises en fonction du tableau.



Remarque : pour cela, vous devez configurer l'API de **Microsoft Graph**, **Office 365 Management APIs**, et **SharePoint**.

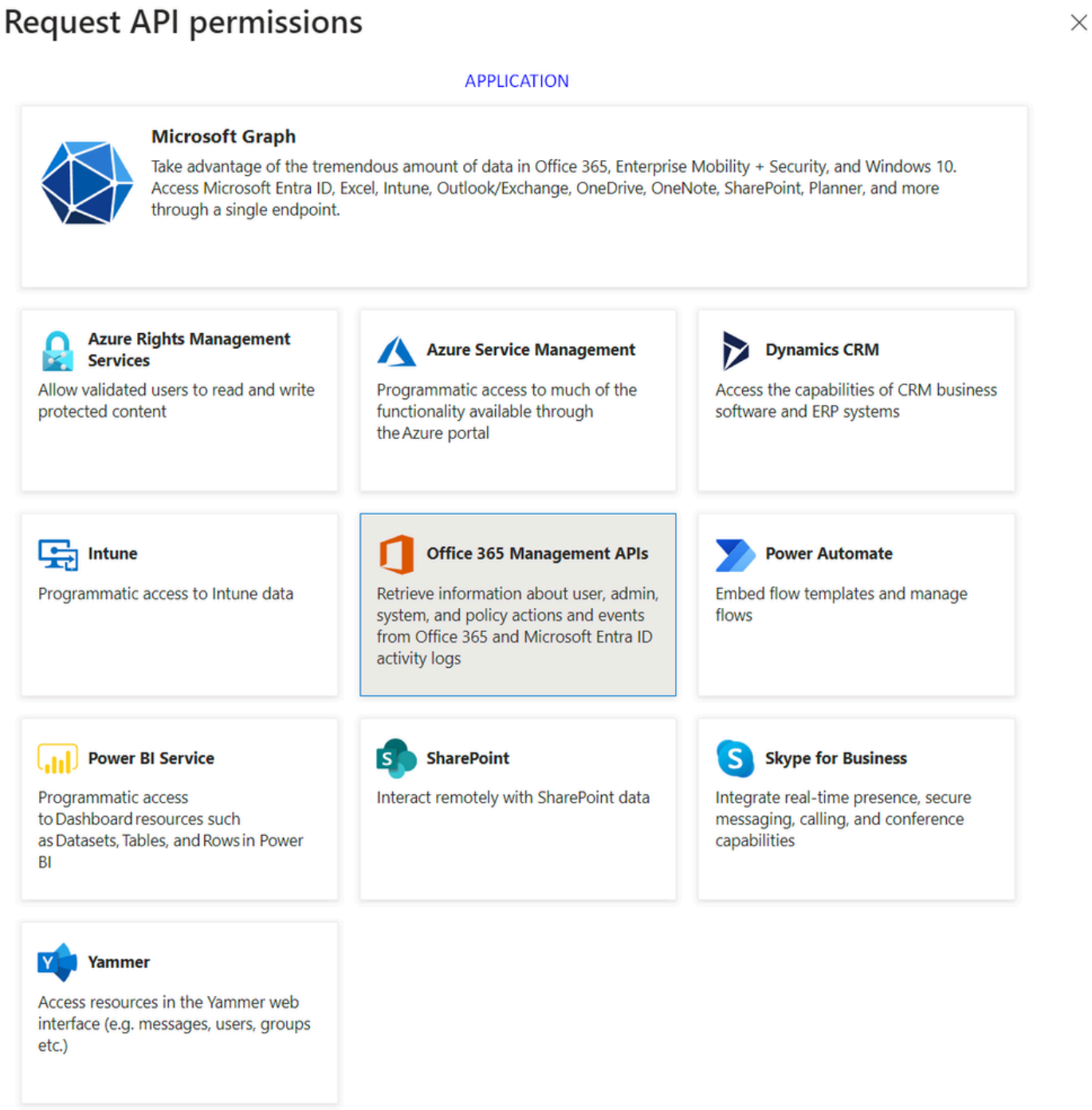


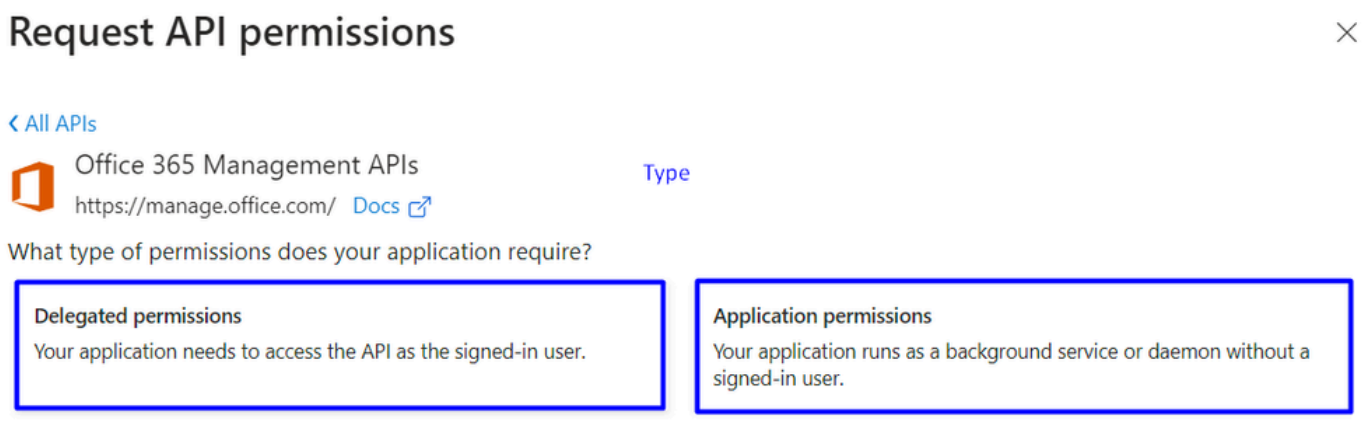
API/ Permissions Name	Type	Description	Admin Consent Required
Microsoft Graph			
Directory.AccessAsUser.All	Delegated	Access directory as the signed-in user	Yes
Directory.Read.All	Application	Read directory data	Yes
Files.Read.All	Delegated	Read all files that user can access	No
Files.Read.All	Application	Read files in all site collections	Yes
Sites.Read.All	Delegated	Read items in all site collections	No
User.Read	Delegated	Sign in and read user profile	No
User.Read.All	Application	Read all users' full profiles	Yes
Microsoft 365 Management APIs			
ActivityFeed.Read	Application	Read activity data for the Organization	Yes
SharePoint			
Site.FullControl.All	Application	Full control of all site collections	Yes
User.Read.All	Application	Read user profiles	Yes



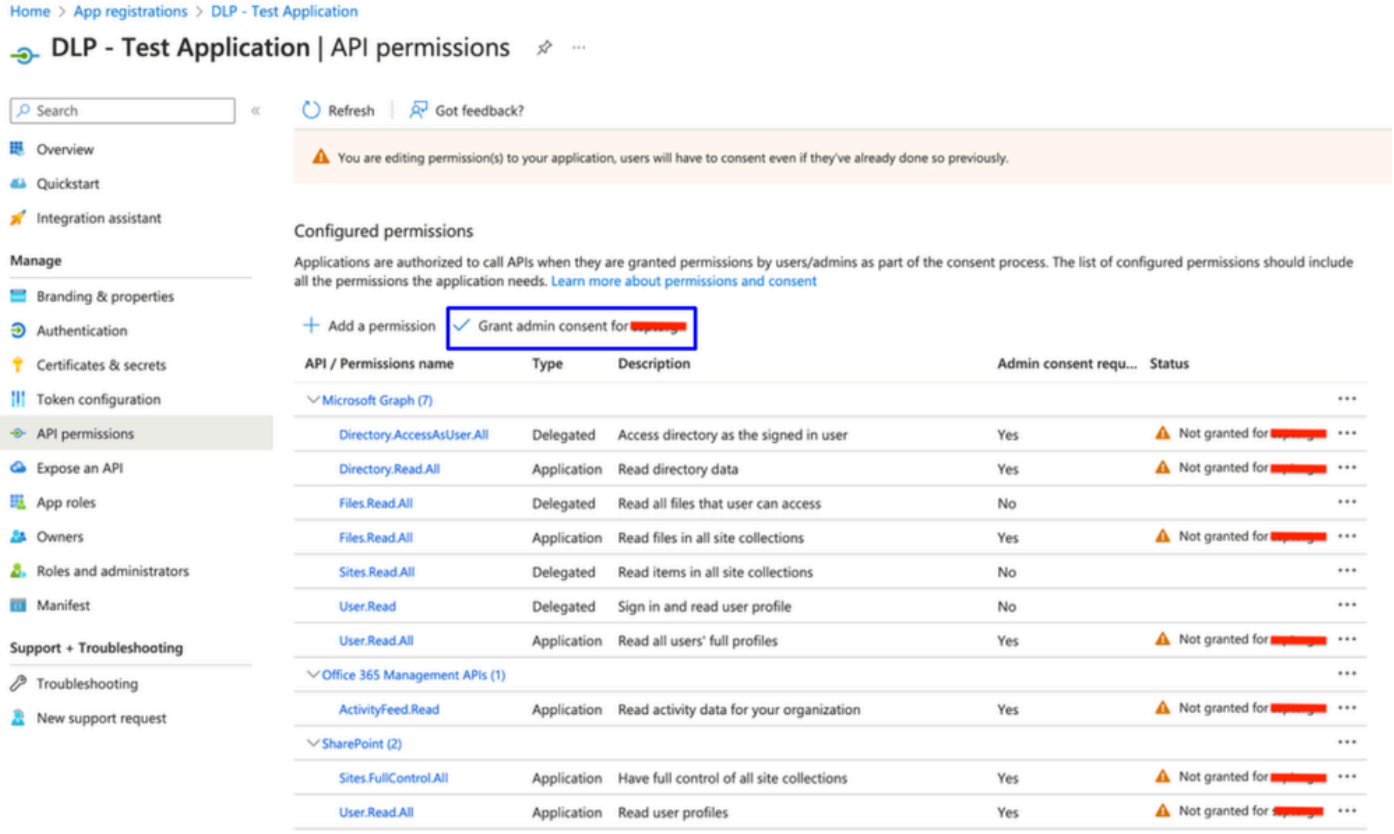
Remarque : au lieu d'**Site.FullControl.All** autorisation, choisissez **Sites.FullControl.All**.

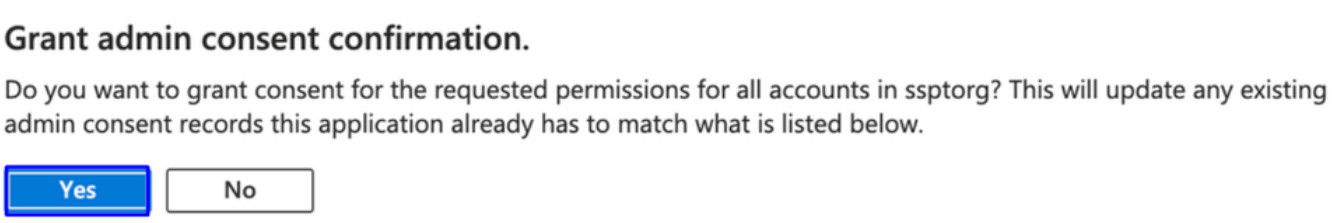
- Pour cela, vous devez choisir l'autorisation en fonction de l'application et tapez :



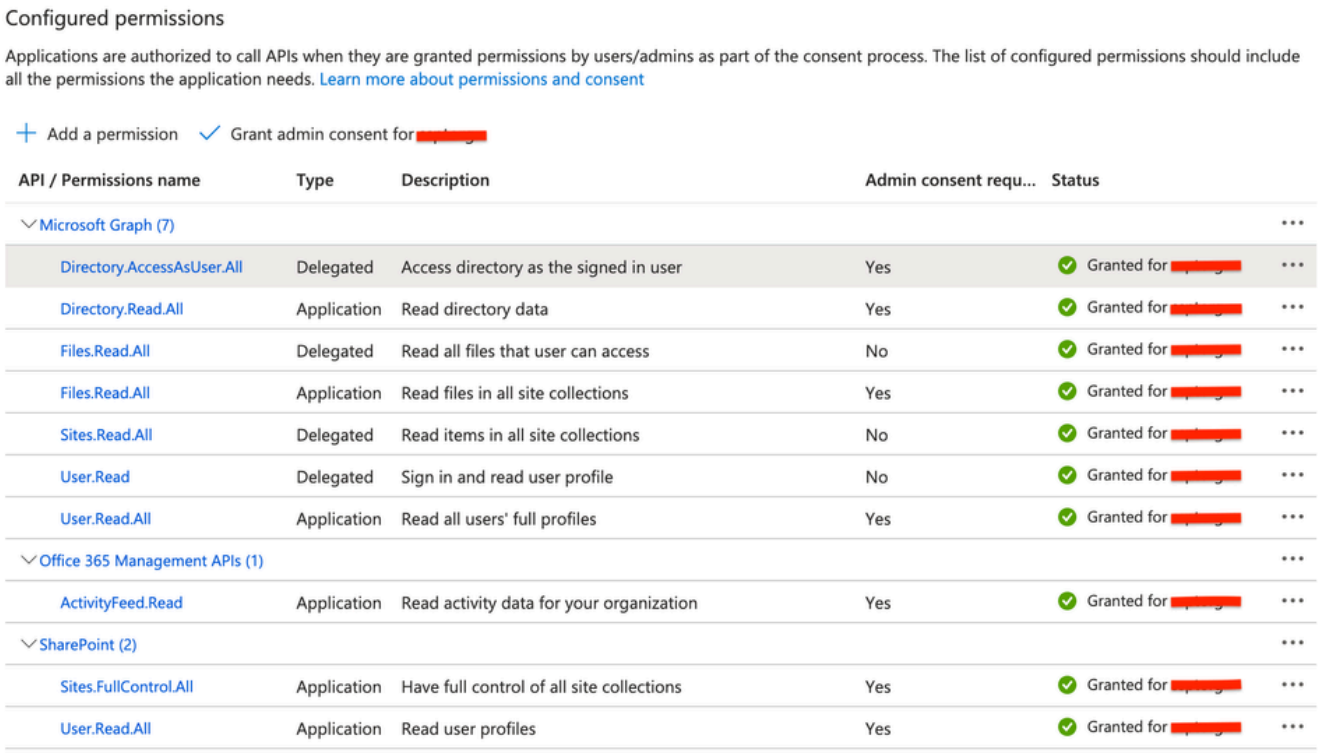


8. Une fois toutes les autorisations requises ajoutées, cliquez **Grant Admin Consent** sur pour le locataire.





- Une fois que vous accordez les autorisations, l'état est visible sous la forme **Granted**



Maintenant que la configuration sur Azure est terminée, vous pouvez poursuivre la configuration sur Secure Access.

Configuration dans Secure Access

Pour activer l'intégration, procédez comme suit :

- Accédez à Admin > Authentication.
- Sous **Platforms**, cliquez sur**Microsoft 365**.
- Cliquez sur **Authorize New Tenant** la sousDLP-section et ajoutez **Microsoft 365**.
- Dans la boîte de **Microsoft 365 Authorization** dialogue, cochez les cases pour vérifier que vous remplissez les conditions requises, puis cliquez sur **Next**.
- Entrez un nom pour votre locataire, puis cliquez sur **Next**.
- Cliquez sur **Next** pour être redirigé vers la page de connexion de Microsoft 365.
- Connectez-vous à Microsoft 365 avec les informations d'identification d'administrateur pour accorder l'accès. Ensuite, lorsque vous êtes redirigé vers Secure Access, vous devez recevoir un message indiquant que votre intégration a réussi.
- Cliquez **Done** pour terminer.

Vérifier

Pour vérifier si l'intégration a réussi, accédez à votre tableau de bord d'accès sécurisé :

- Cliquez sur **Admin > Authentication > Microsoft 365**

Et si tout est correctement configuré, votre état doit être **Authorized**.

Informations connexes

- Activer la protection contre la perte de données de l'API SaaS pour les locataires Microsoft 365
- Activation ou désactivation de l'audit dans Microsoft

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.