

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

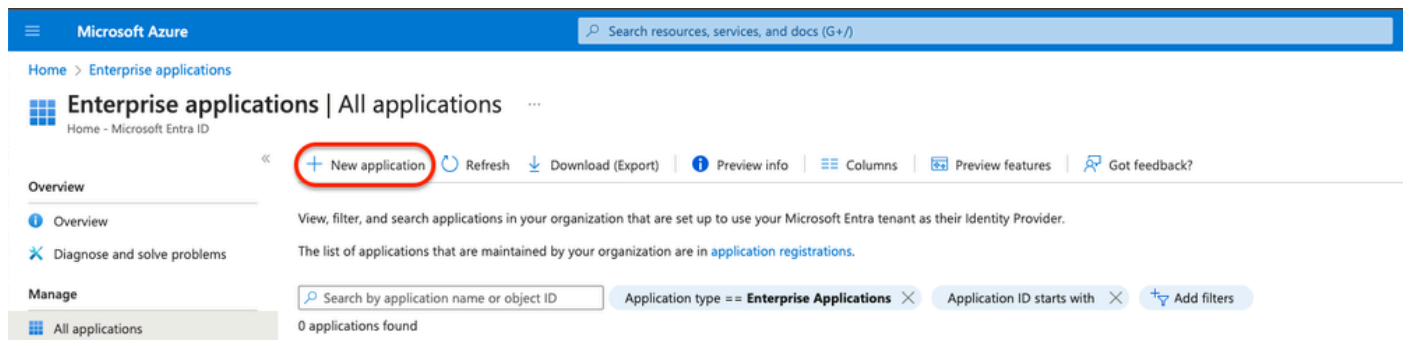
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

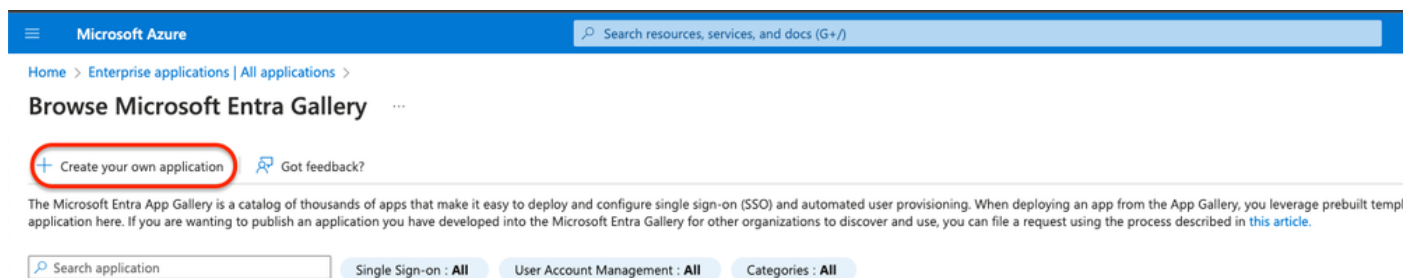
Configuration sur Azure

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).**

Create your own application



 Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

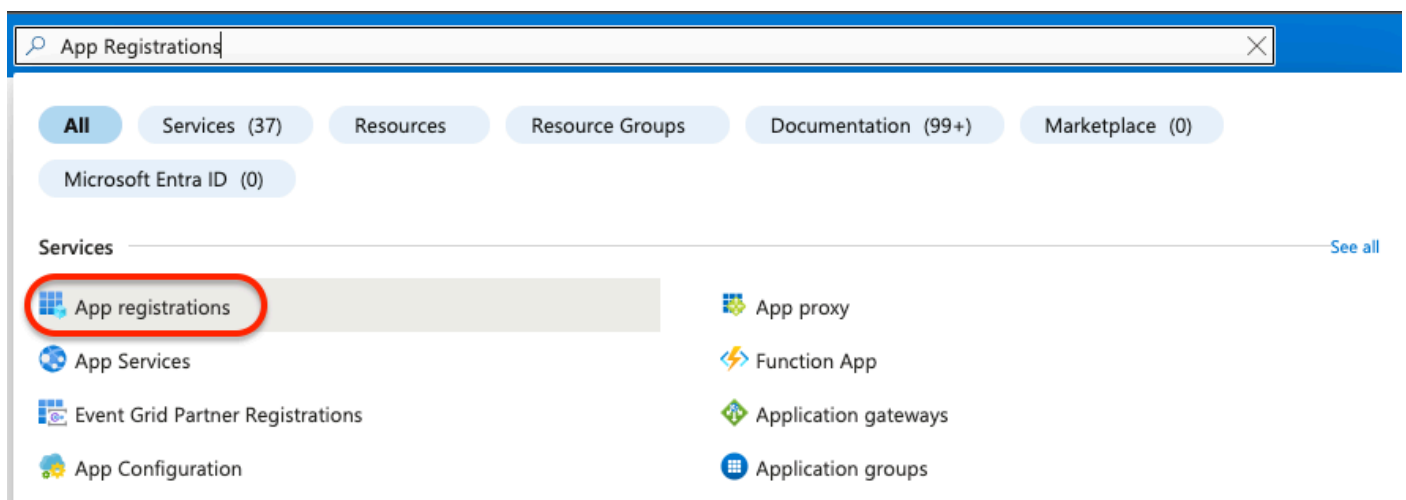
What's the name of your app?

DLP Test Application 

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Microsoft Entra ID (App you're developing)
- 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**.



The screenshot shows the Azure search interface. The search bar at the top contains the text 'App Registrations'. Below the search bar, there are several filter buttons: 'All', 'Services (37)', 'Resources', 'Resource Groups', 'Documentation (99+)', and 'Marketplace (0)'. Under the 'Services' section, a list of results is displayed. The first result, 'App registrations', is highlighted with a red circle. Other results include 'App proxy', 'App Services', 'Function App', 'Event Grid Partner Registrations', 'Application gateways', 'App Configuration', and 'Application groups'. A 'See all' link is visible at the end of the Services section.

5. Cliquez sur **All Applications** et choisissez l'application créée à l'étape [trois](#).

Home >

App registrations

+ New registration Endpoints Troubleshooting Refresh Download Preview features | Got feedback?

i Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications Owned applications Deleted applications

Add filters

1 applications found

Display name ↑↓

DT DLP Test Application

6. Sélectionnez API Permissions.

Home > App registrations >

DLP Test Application

Delete Endpoints Preview features

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions**
 - Expose an API
 - App roles
 - Owners

i Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: DLP Test Application	Client credentials	: Add a certificate or secret
Application (client) ID	: [REDACTED]	Redirect URIs	: Add a Redirect URI
Object ID	: [REDACTED]	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: [REDACTED]	Managed application in l...	: DLP Test Application

Supported account types : [My organization only](#)

i Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

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**.

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) ✓ Grant admin consent for Home

API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

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 :

Request API permissions



APPLICATION

 Microsoft Graph Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.		
 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal	 Dynamics CRM Access the capabilities of CRM business software and ERP systems
 Intune Programmatic access to Intune data	 Office 365 Management APIs Retrieve information about user, admin, system, and policy actions and events from Office 365 and Microsoft Entra ID activity logs	 Power Automate Embed flow templates and manage flows
 Power BI Service Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI	 SharePoint Interact remotely with SharePoint data	 Skype for Business Integrate real-time presence, secure messaging, calling, and conference capabilities
 Yammer Access resources in the Yammer web interface (e.g. messages, users, groups etc.)		

Request API permissions



< All APIs



Office 365 Management APIs

Type

<https://manage.office.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

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

DLP - Test Application | API permissions

Search

Refresh | Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for **ssptorg**

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	Not granted for ssptorg
Directory.Read.All	Application	Read directory data	Yes	Not granted for ssptorg
Files.Read.All	Delegated	Read all files that user can access	No	
Files.Read.All	Application	Read files in all site collections	Yes	Not granted for ssptorg
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	Not granted for ssptorg
Office 365 Management APIs (1)				
ActivityFeed.Read	Application	Read activity data for your organization	Yes	Not granted for ssptorg
SharePoint (2)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	Not granted for ssptorg
User.Read.All	Application	Read user profiles	Yes	Not granted for ssptorg

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in ssptorg? This will update any existing admin consent records this application already has to match what is listed below.

Yes

No

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

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for ██████████

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (7) ...				
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	✓ Granted for ██████████ ...
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for ██████████ ...
Files.Read.All	Delegated	Read all files that user can access	No	✓ Granted for ██████████ ...
Files.Read.All	Application	Read files in all site collections	Yes	✓ Granted for ██████████ ...
Sites.Read.All	Delegated	Read items in all site collections	No	✓ Granted for ██████████ ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for ██████████ ...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for ██████████ ...
▼ Office 365 Management APIs (1) ...				
ActivityFeed.Read	Application	Read activity data for your organization	Yes	✓ Granted for ██████████ ...
▼ SharePoint (2) ...				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	✓ Granted for ██████████ ...
User.Read.All	Application	Read user profiles	Yes	✓ Granted for ██████████ ...

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**.

DLP

Name	Status	Action
Microsoft 365	● Authorized	REVOKE

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.