

# Configureer beveiligde toegang met Office 365 voor uitgebreide preventie van gegevensverlies

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Configuratie op Azure](#)

[Configuratie in beveiligde toegang](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

---

## Inleiding

In dit document wordt de integratie beschreven van Data Loss Prevention voor Office 365 met Secure Access.

## Voorwaarden

- **Office 365 E3 Subscription** is aanwezig voor uw Microsoft-huurder
  - Compliance auditing is geconfigureerd zoals **ON** in het [compliance portal](#) voordat u uw integratie start

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco beveiligde toegang
- Microsoft Azure Enterprise-toepassingen en app-registraties

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco beveiligde toegang

- Microsoft Azure
- Nalevingsportal voor Microsoft 365

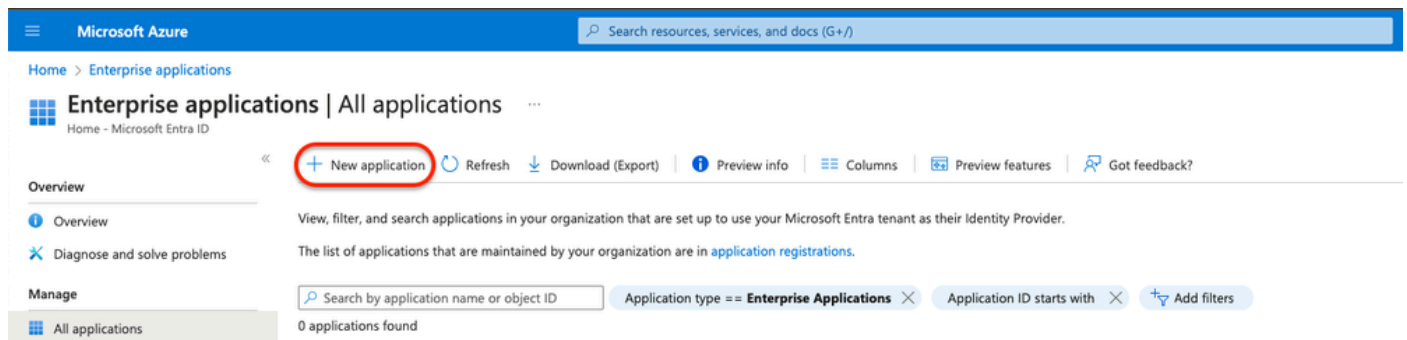
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

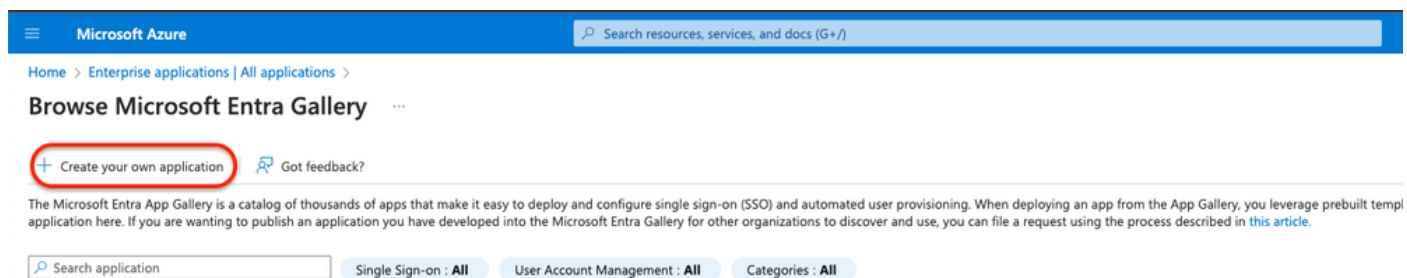
Configuratie op Azure

Om de toepassing op Azure in te schakelen, moet u de volgende stappen uitvoeren:

1. Navigeer naar het **Azure Portal > Enterprise Applications > New Applications** scherm.




2. Klik op **Create your own Application**.



3. Geef een naam die u wenst om de app te identificeren en te kiezen. **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.

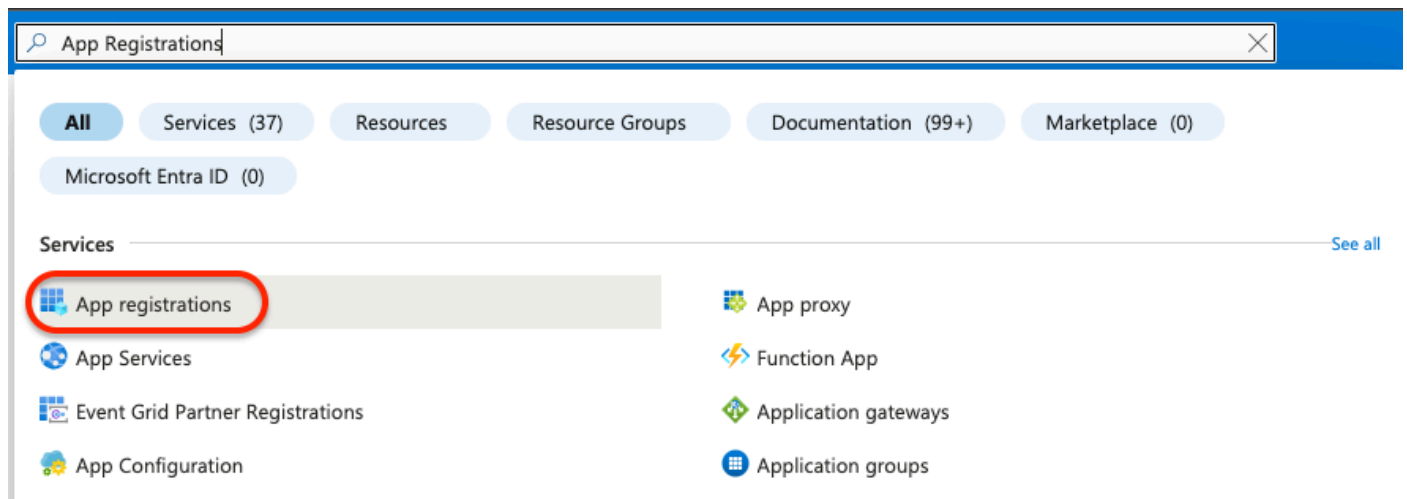
What's the name of your app?

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. Als u dit hebt gedaan, gebruikt u de Azure Search Bar om naar te zoeken **App Registrations**.



The screenshot shows the Azure portal search bar with 'App Registrations' entered. Below the search bar, there are filter tabs: All, Services (37), Resources, Resource Groups, Documentation (99+), Marketplace (0), and Microsoft Entra ID (0). Under the 'Services' section, a list of services is displayed. The 'App registrations' service is highlighted with a red circle. Other services listed 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. Klik op **All Applications** en kies de toepassing die in stap [3.1s](#) gemaakt.

# App registrations

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

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

Start typing a display name or application (client) ID to filter these r...

Add filters

1 applications found

Display name ↑↓

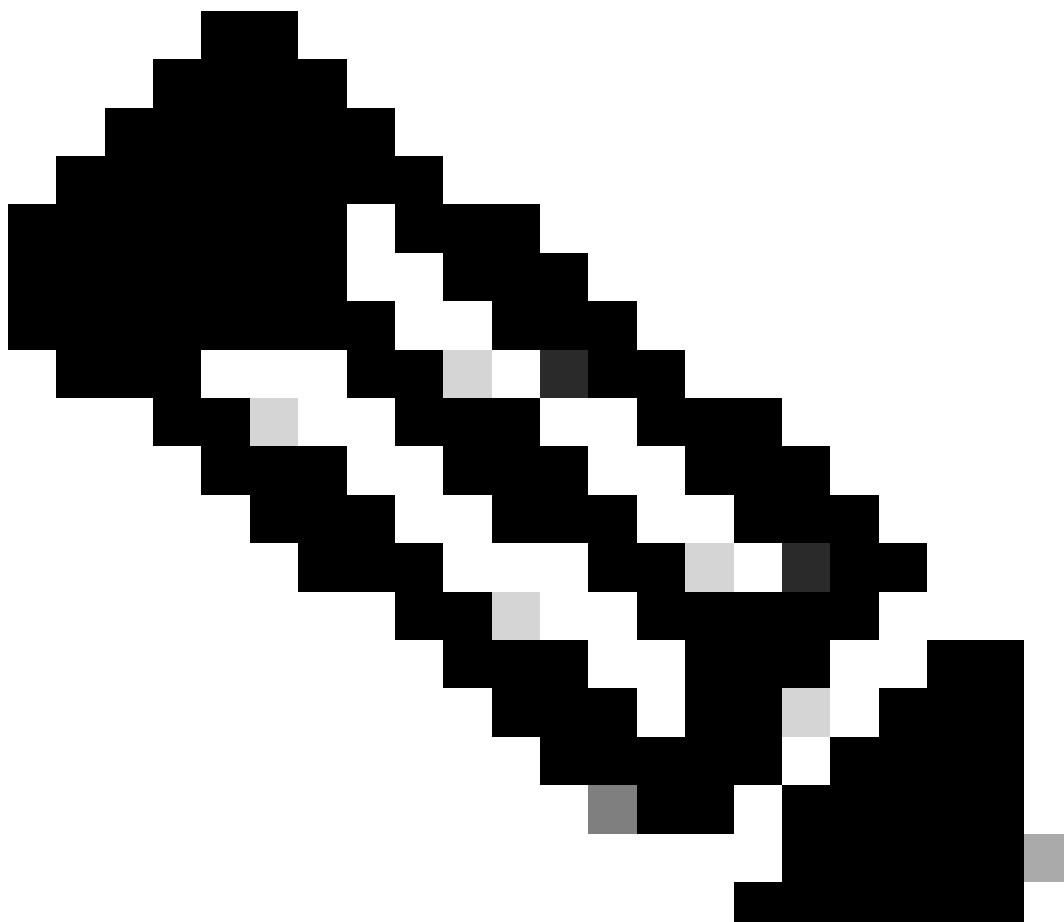
DT DLP Test Application

## 6. Kies API Permissions.

The screenshot shows the 'API permissions' page for the 'DLP Test Application'. The left-hand navigation pane has 'API permissions' selected and circled in red. The main content area displays the application's details under the 'Essentials' section, including the display name 'DLP Test Application', application (client) ID, object ID, and directory (tenant) ID, all of which are redacted with black bars. To the right, there are links for 'Add a certificate or secret', 'Add a Redirect URI', 'Add an Application ID URI', and 'Managed application in...'. A notice at the bottom of the main area states that starting June 30th, 2020, new features will not be added to ADAL and Azure Active Directory Graph, and that technical support and security updates will be provided for MSAL and Microsoft Graph. The 'Get Started' and 'Documentation' links are visible at the bottom of the page.

## 7. Klik op Add a permission en kies de gewenste rechten op basis van de tabel.

**Opmerking:** hiervoor moet u de API van **Microsoft Graph**, **Office 365 Management APIs**, en **SharePoint** configureren.



**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](#).

<b>API/ Permissions Name</b>	<b>Type</b>	<b>Description</b>	<b>Admin Consent Required</b>
<b>Microsoft Graph</b>			
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
<b>Microsoft 365 Management APIs</b>			
ActivityFeed.Read	Application	Read activity data for the Organization	Yes
<b>SharePoint</b>			
Site.FullControl.All	Application	Full control of all site collections	Yes
User.Read.All	Application	Read user profiles	Yes














**Opmerking:** In plaats van **Site.FullControl.All** toestemming kiezen **Sites.FullControl.All**.

- 
- Hiervoor moet u de toestemming kiezen op basis van de toepassing en het type:

# Request API permissions



## APPLICATION

 <b>Microsoft Graph</b> 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.		
 <b>Azure Rights Management Services</b> Allow validated users to read and write protected content	 <b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal	 <b>Dynamics CRM</b> Access the capabilities of CRM business software and ERP systems
 <b>Intune</b> Programmatic access to Intune data	 <b>Office 365 Management APIs</b> Retrieve information about user, admin, system, and policy actions and events from Office 365 and Microsoft Entra ID activity logs	 <b>Power Automate</b> Embed flow templates and manage flows
 <b>Power BI Service</b> Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI	 <b>SharePoint</b> Interact remotely with SharePoint data	 <b>Skype for Business</b> Integrate real-time presence, secure messaging, calling, and conference capabilities
 <b>Yammer</b> 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. Zodra alle vereiste toestemmingen worden toegevoegd, klik **Grant Admin Consent** op voor de huurder.



## 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 <b>ssptorg</b>
Directory.Read.All	Application	Read directory data	Yes	Not granted for <b>ssptorg</b>
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 <b>ssptorg</b>
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 <b>ssptorg</b>
Office 365 Management APIs (1)				
ActivityFeed.Read	Application	Read activity data for your organization	Yes	Not granted for <b>ssptorg</b>
SharePoint (2)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	Not granted for <b>ssptorg</b>
User.Read.All	Application	Read user profiles	Yes	Not granted for <b>ssptorg</b>

## 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

- Zodra u de machtigingen verleent, is de status zichtbaar als **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) ...				
<a href="#">Directory.AccessAsUser.All</a>	Delegated	Access directory as the signed in user	Yes	✓ Granted for ██████████ ...
<a href="#">Directory.Read.All</a>	Application	Read directory data	Yes	✓ Granted for ██████████ ...
<a href="#">Files.Read.All</a>	Delegated	Read all files that user can access	No	✓ Granted for ██████████ ...
<a href="#">Files.Read.All</a>	Application	Read files in all site collections	Yes	✓ Granted for ██████████ ...
<a href="#">Sites.Read.All</a>	Delegated	Read items in all site collections	No	✓ Granted for ██████████ ...
<a href="#">User.Read</a>	Delegated	Sign in and read user profile	No	✓ Granted for ██████████ ...
<a href="#">User.Read.All</a>	Application	Read all users' full profiles	Yes	✓ Granted for ██████████ ...
▼ Office 365 Management APIs (1) ...				
<a href="#">ActivityFeed.Read</a>	Application	Read activity data for your organization	Yes	✓ Granted for ██████████ ...
▼ SharePoint (2) ...				
<a href="#">Sites.FullControl.All</a>	Application	Have full control of all site collections	Yes	✓ Granted for ██████████ ...
<a href="#">User.Read.All</a>	Application	Read user profiles	Yes	✓ Granted for ██████████ ...

Nu de configuratie op Azure is voltooid, kunt u de configuratie op Secure Access voortzetten.

## Configuratie in beveiligde toegang

Configureer volgens de volgende stappen om de integratie in te schakelen:

- Navigeer naar Admin > Authentication.
- Klik onder **Platforms** op **Microsoft 365**.
- Klik **Authorize New Tenant** in de DLP subsectie en voeg **Microsoft 365** toe.
- Schakel in het **Microsoft 365 Authorization** dialoogvenster de selectievakjes in om te controleren of u aan de voorwaarden voldoet en klik vervolgens op **Next**.
- Geef een naam voor uw huurder, dan klik **Next**.
- Klik hierop **Next** om naar de Microsoft 365-inlogpagina te worden doorgestuurd.
- Log in op Microsoft 365 met beheerdersreferenties om toegang te verlenen. Vervolgens, wanneer u wordt omgeleid naar Secure Access, moet u een bericht hebben dat aangeeft dat uw integratie is geslaagd.
- Klik om **Done** te voltooien.

## Verifiëren

Om te verifiëren of de integratie succesvol was, navigeer dan naar uw [Secure Access Dashboard](#):

- Klik op **Admin > Authentication > Microsoft 365**

En als alles correct wordt geconfigureerd, moet uw status worden **Authorized**aangepast.

DLP

Name	Status	Action
<b>Microsoft 365</b>	● Authorized	<b>REVOKE</b>

Gerelateerde informatie

- [SaaS API Data Loss Protection inschakelen voor Microsoft 365-huurders](#)
- [Auditing in- of uitschakelen in Microsoft](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.