Configureer beveiligde toegang met Office 365 voor uitgebreide preventie van gegevensverlies

Inhoud

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

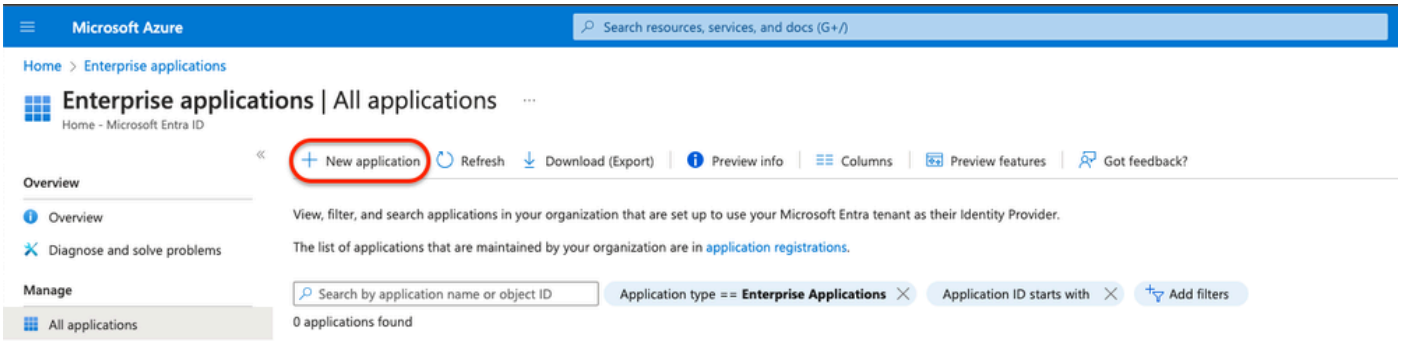
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

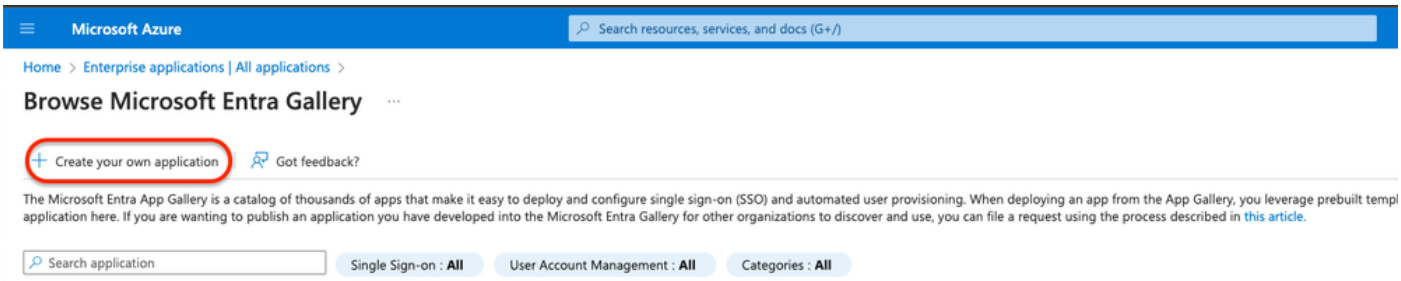
Configuratie op Azure

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

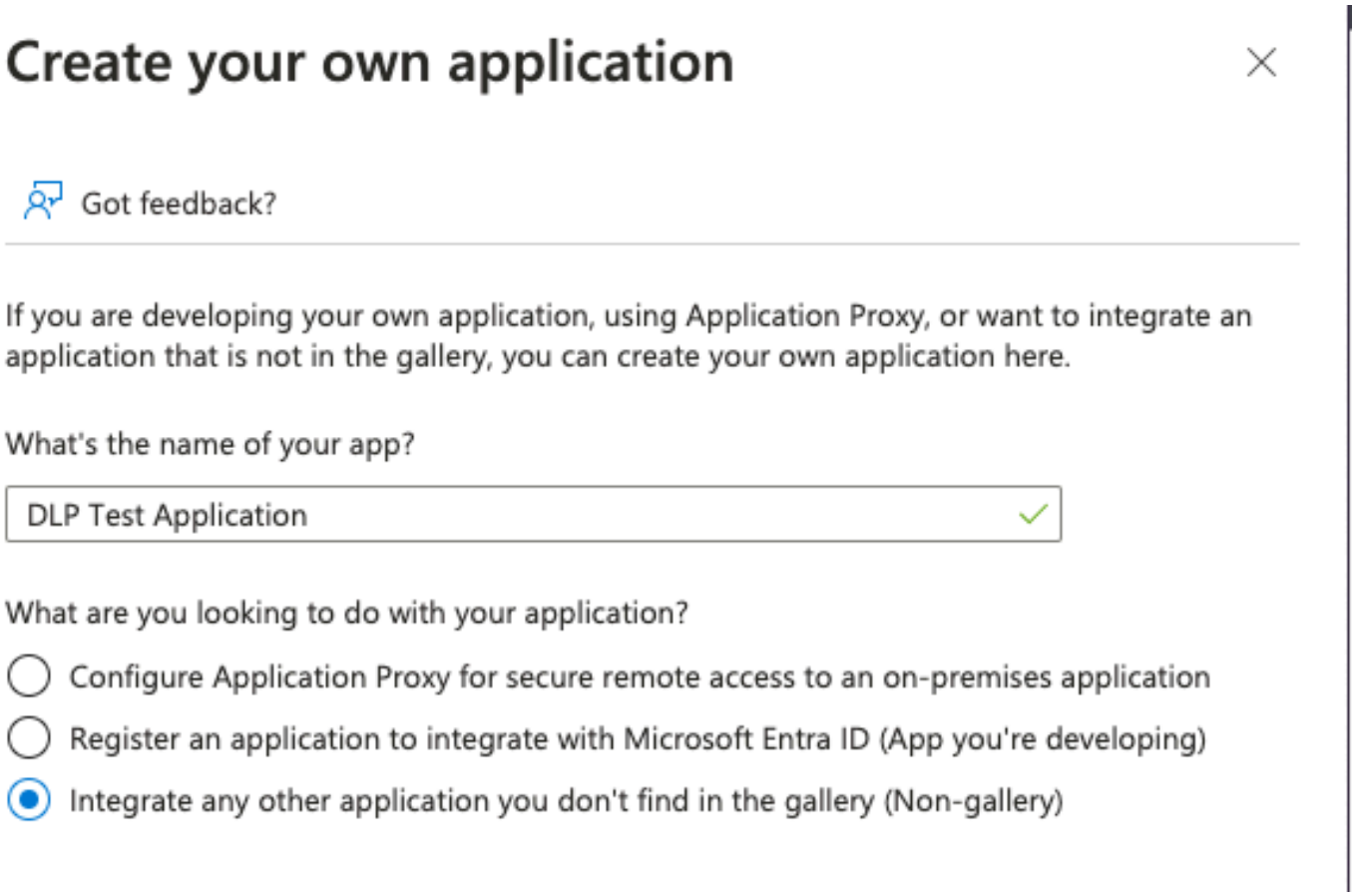
1. Navigeer naar het **Azure Portal > Enterprise Applications > New Application**scherm.



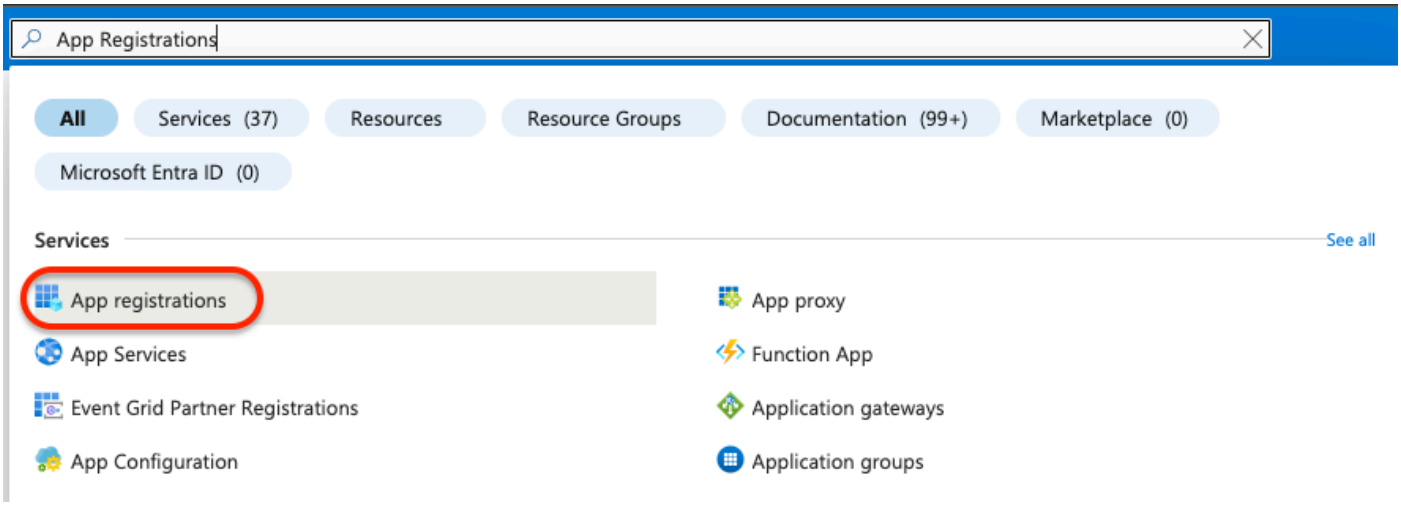
2. Klik op **Create your own Application**.



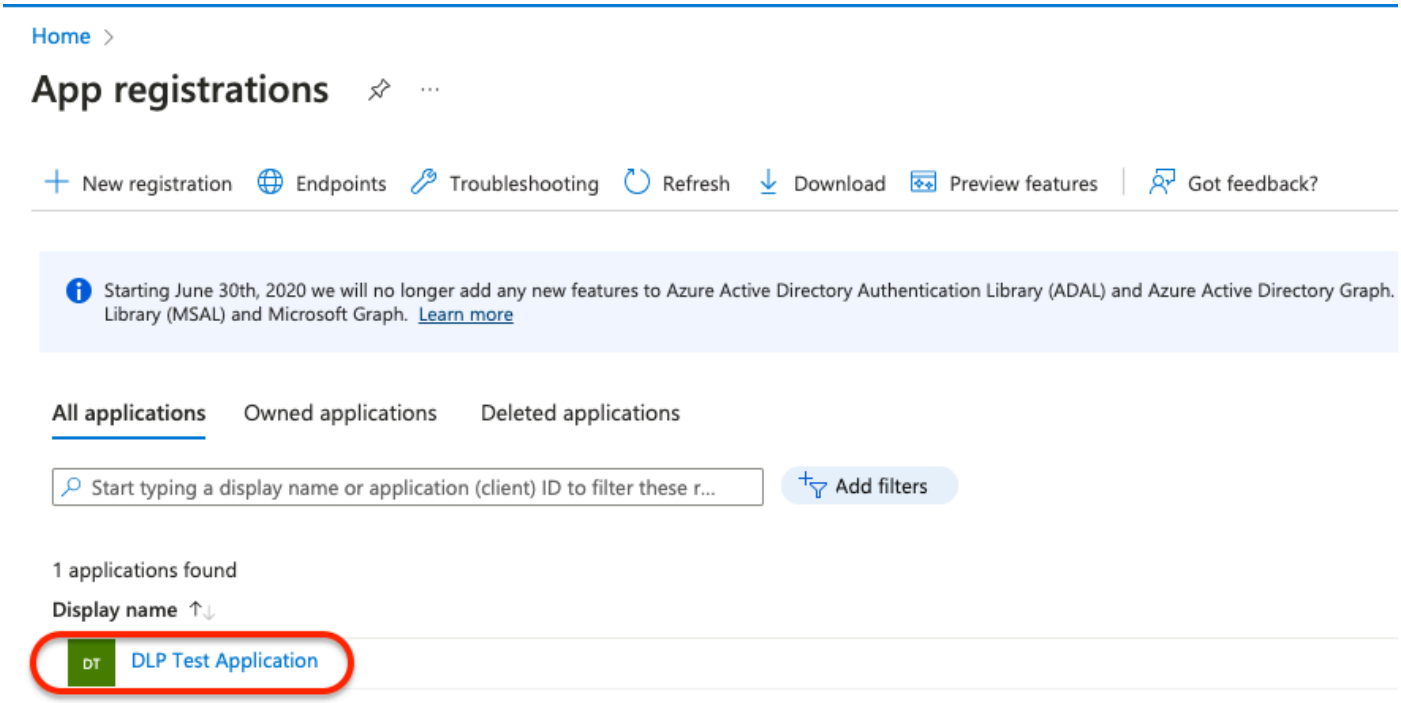
3. Geef een naam die u wenst om de app te identificeren en te kiezen. **Integrate any other application you don't find in the gallery (Non-Gallery)**.



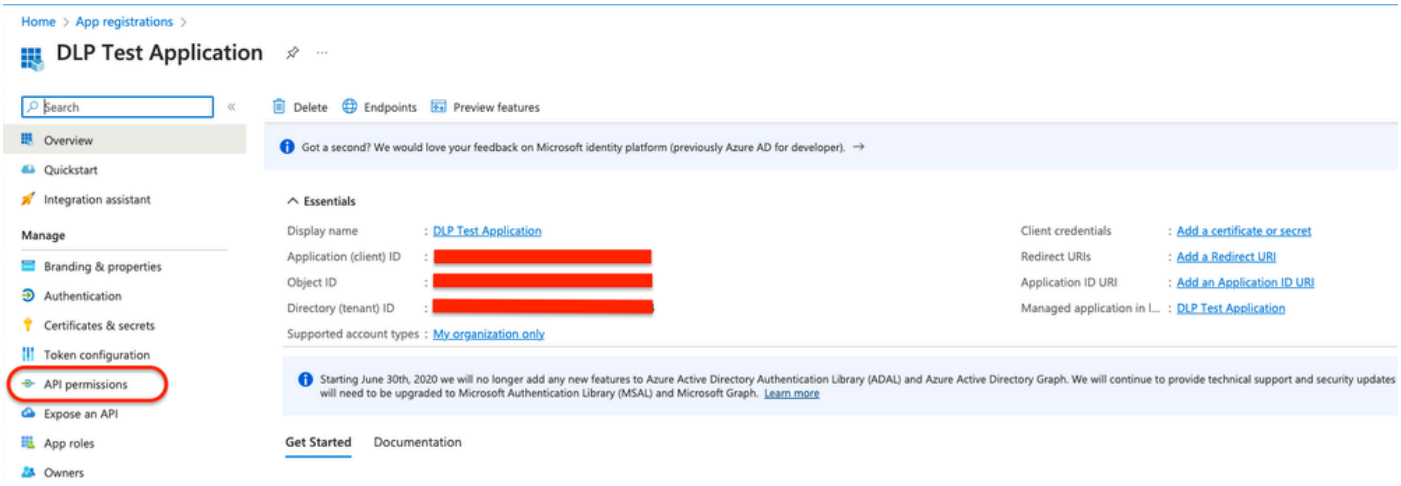
4. Als u dit hebt gedaan, gebruikt u de Azure Search Bar om naar te zoeken **App Registrations**.



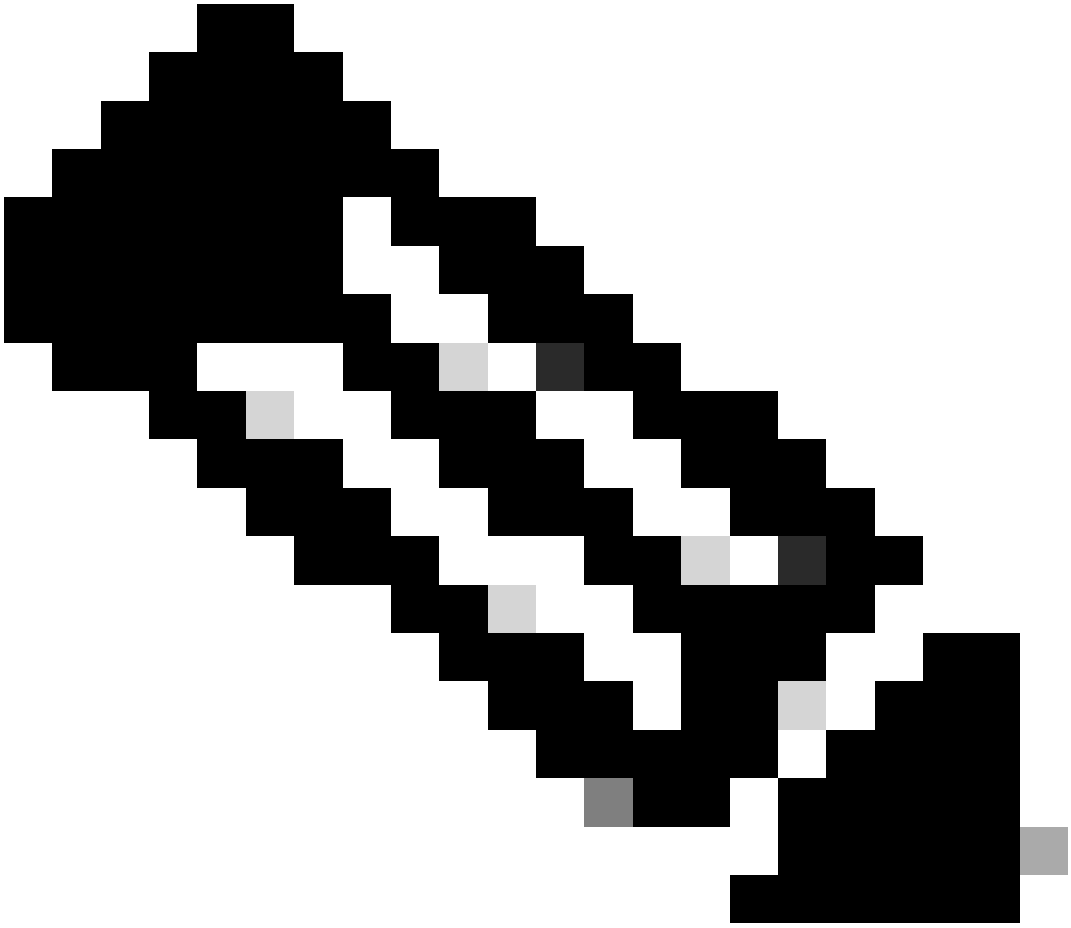
5. Klik op **All Applications** en kies de toepassing die in stap 3 is gemaakt.



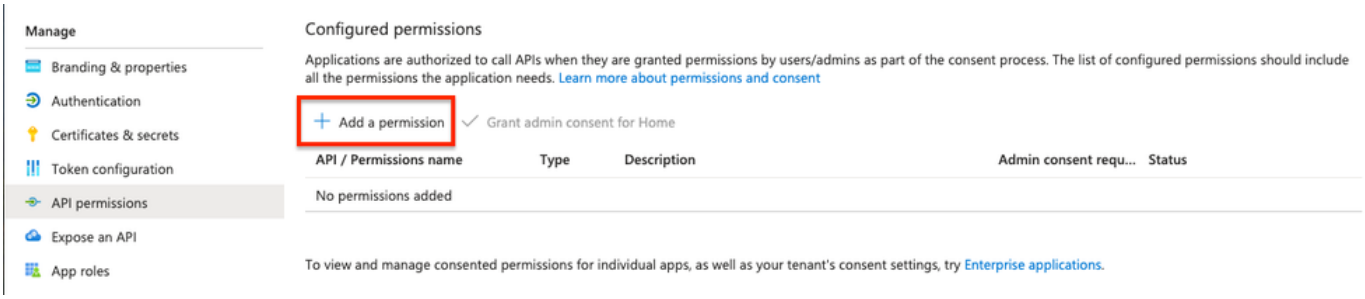
6. Kies **API Permissions**.



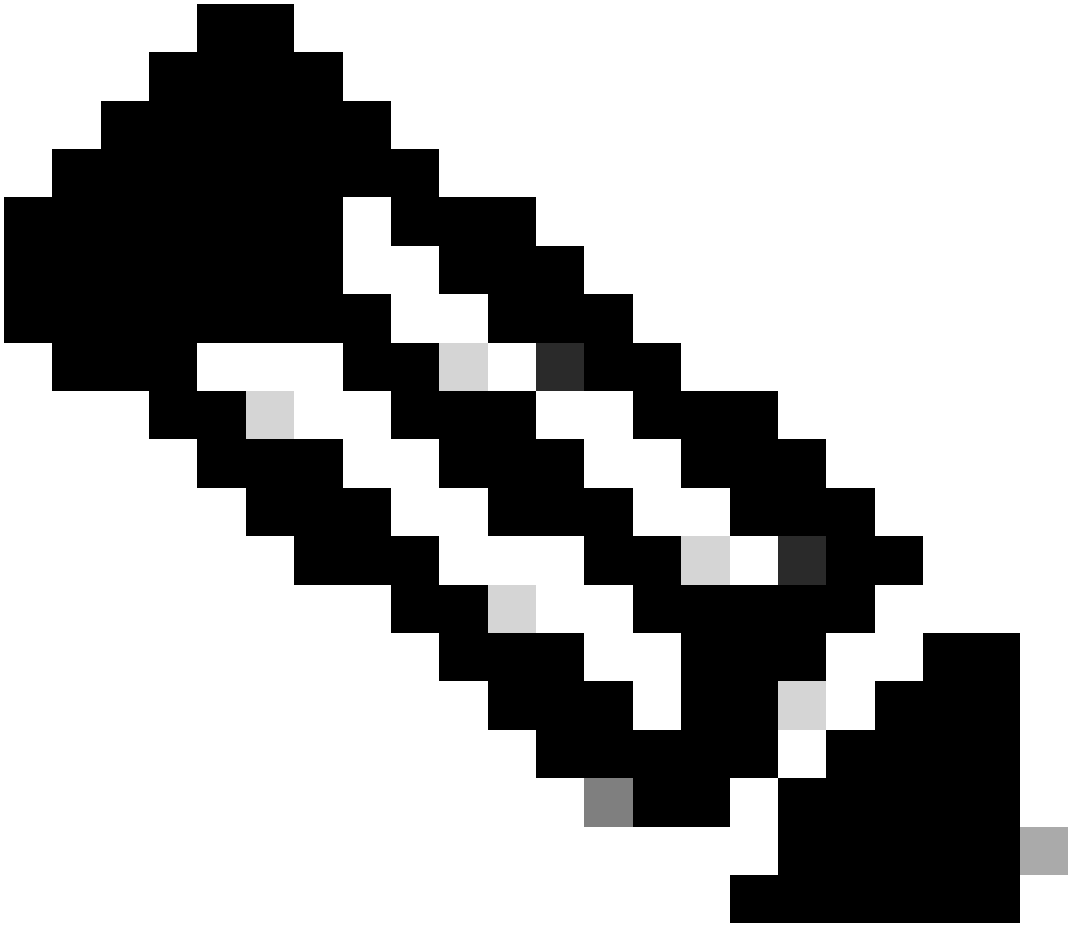
7. Klik op **Add a permission** en kies de gewenste rechten op basis van de tabel.



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

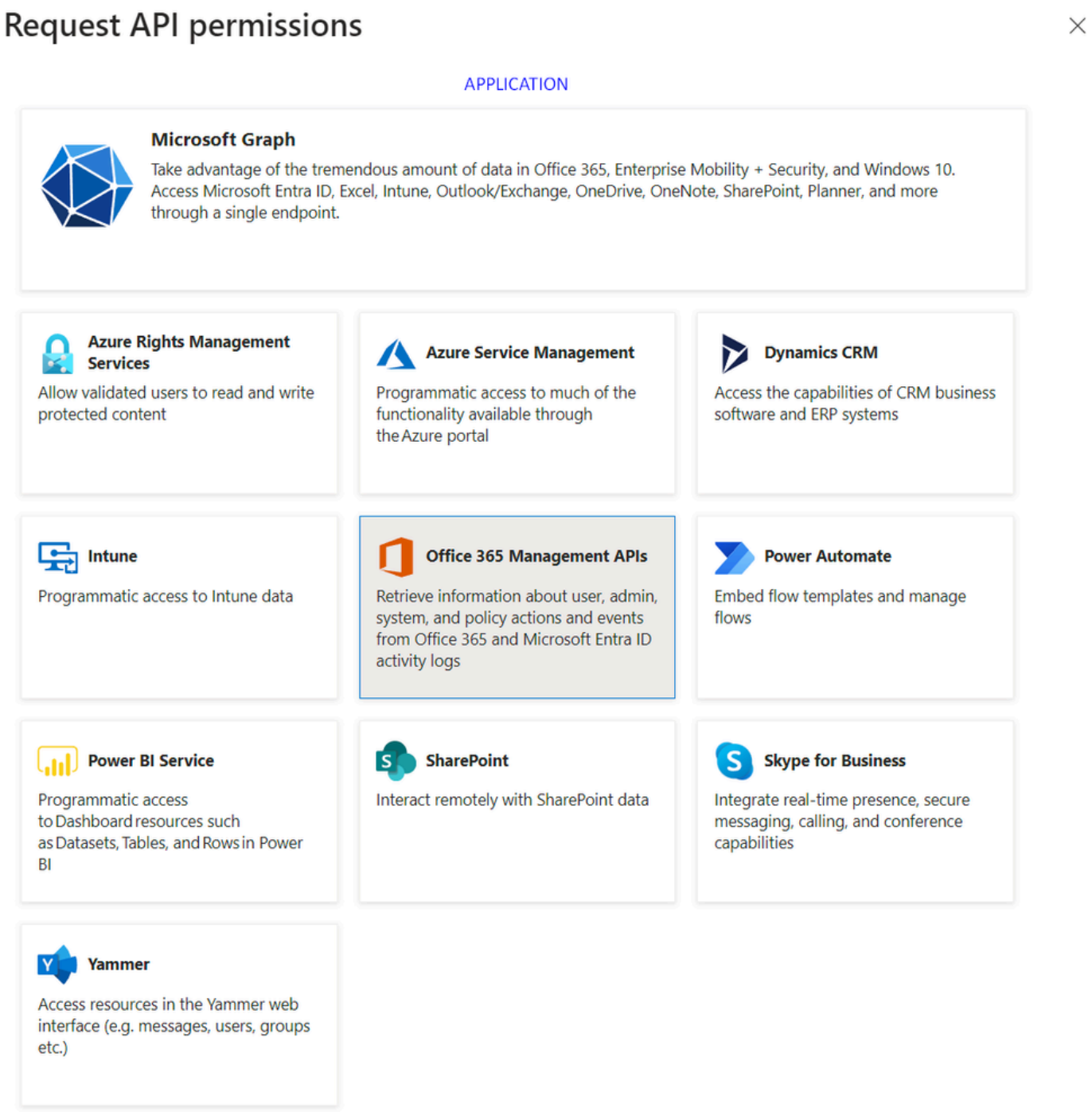


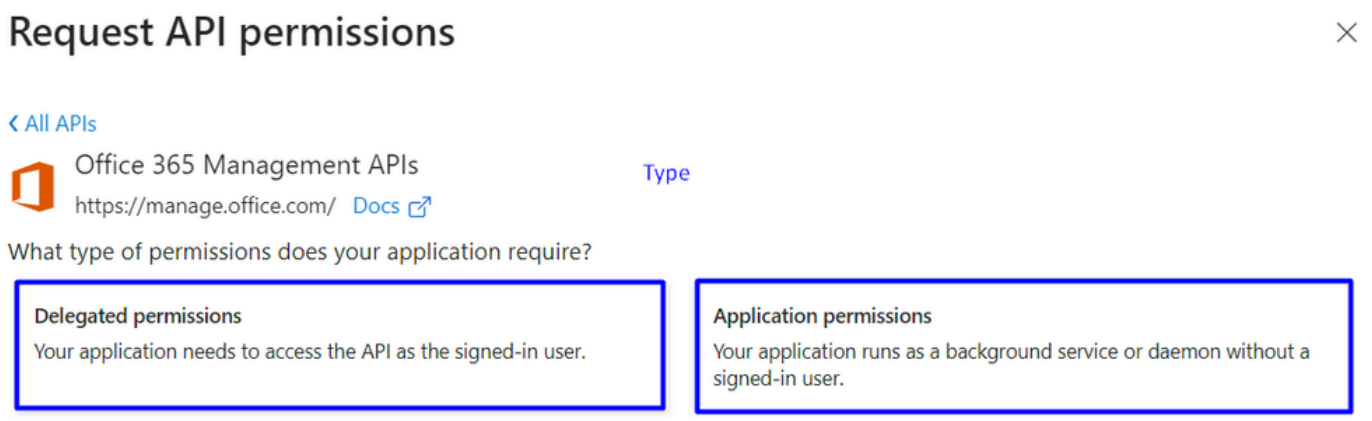
API/ Permissions Name	Type	Description	Admin Consent Required
Microsoft Graph			
Directory.AccessAsUser.All	Delegated	Access directory as the signed-in user	Yes
Directory.Read.All	Application	Read directory data	Yes
Files.Read.All	Delegated	Read all files that user can access	No
Files.Read.All	Application	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



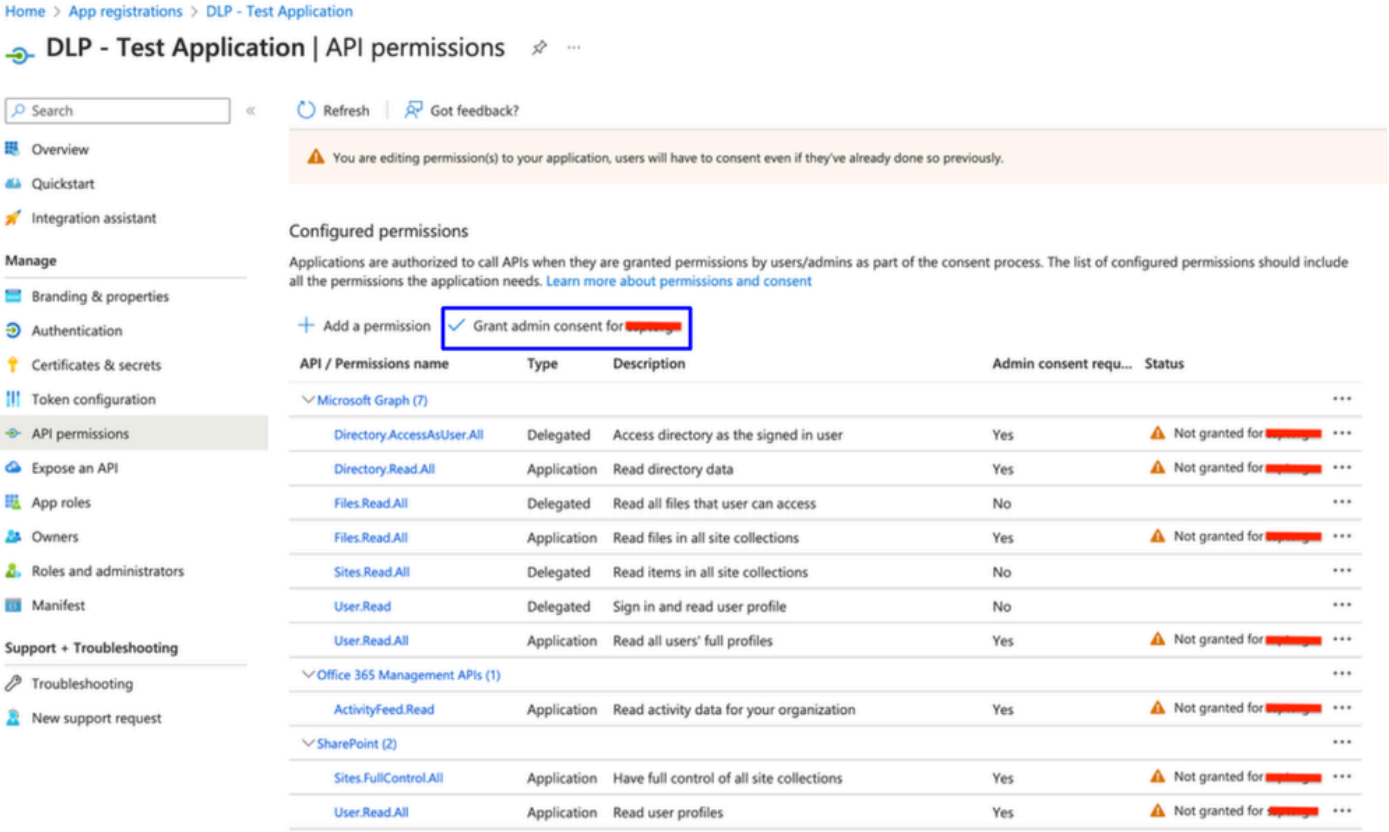
Opmerking: In plaats van **Site.FullControl.All** toestemming kiezen **Sites.FullControl.All**.

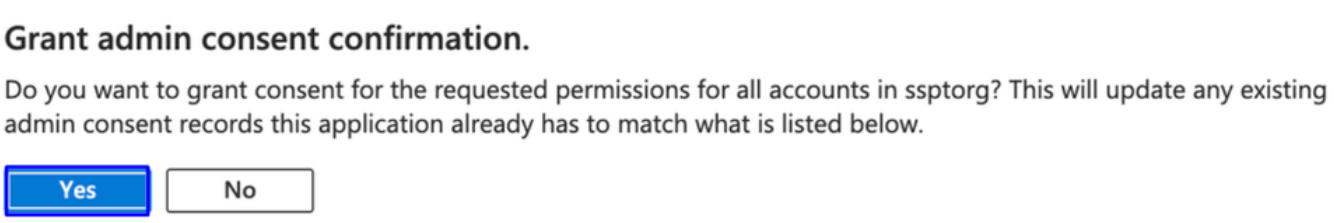
- Hiervoor moet u de toestemming kiezen op basis van de toepassing en het type:



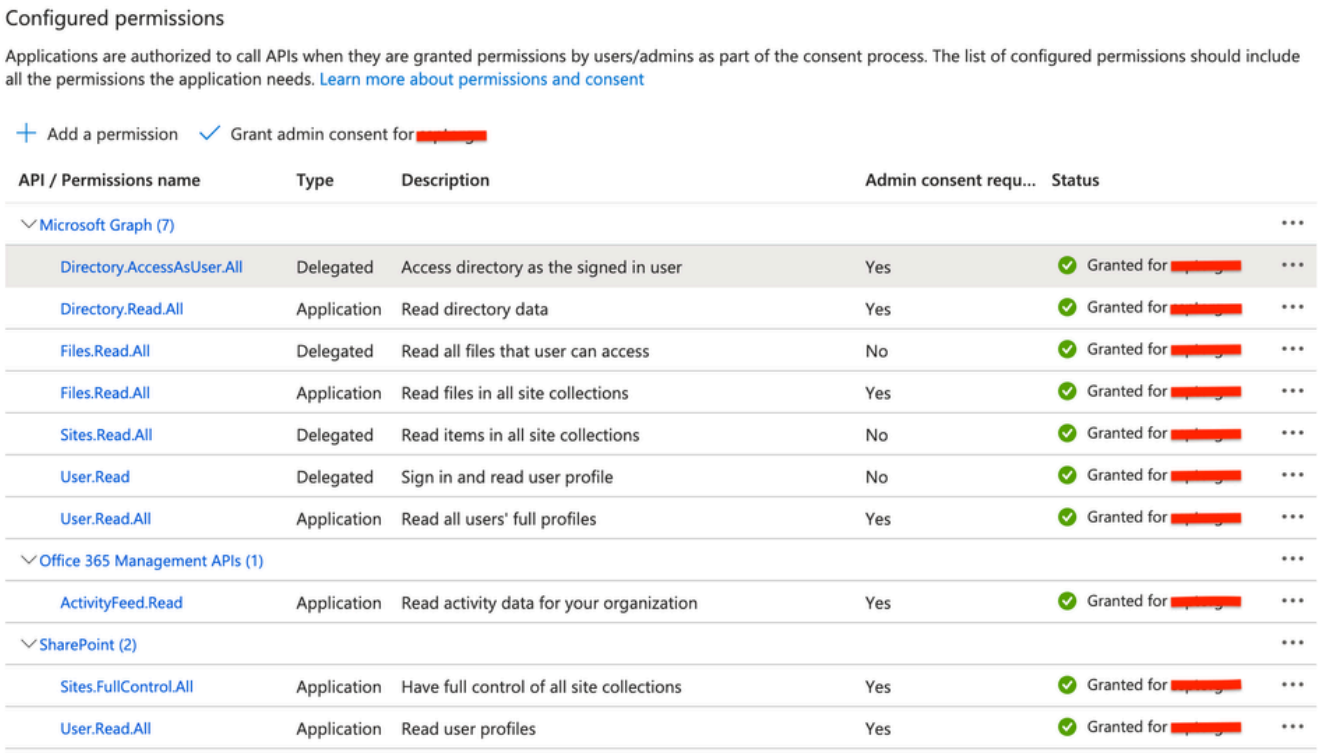


8. Zodra alle vereiste toestemmingen worden toegevoegd, klik **Grant Admin Consent** op voor de huurder.





- Zodra u de machtigingen verleent, is de status zichtbaar als **Granted**



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.

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.