Configurar el acceso seguro con Office 365 para una prevención mejorada de la pérdida de datos

Contenido

Introducción

Este documento describe la integración de la Prevención de pérdida de datos para Office 365 con Secure Access.

Prerequisites

- **Office 365 E3 Subscription** está presente para su arrendatario de Microsoft
    - La auditoría de conformidad se configura como **ON** en el portal de conformidad antes de iniciar la integración

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro de Cisco
- Aplicaciones empresariales y registros de aplicaciones de Microsoft Azure

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Acceso seguro de Cisco

- Microsoft Azure
- Portal de cumplimiento de Microsoft 365

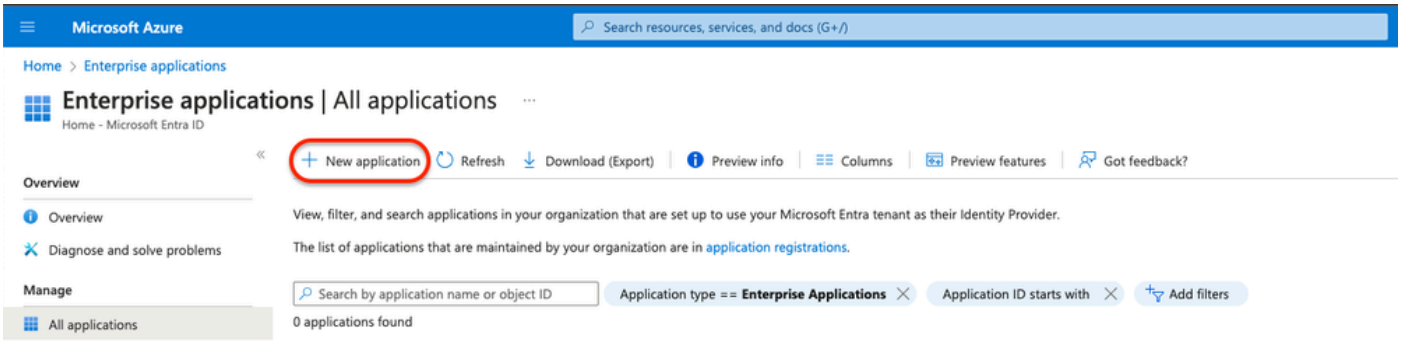
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

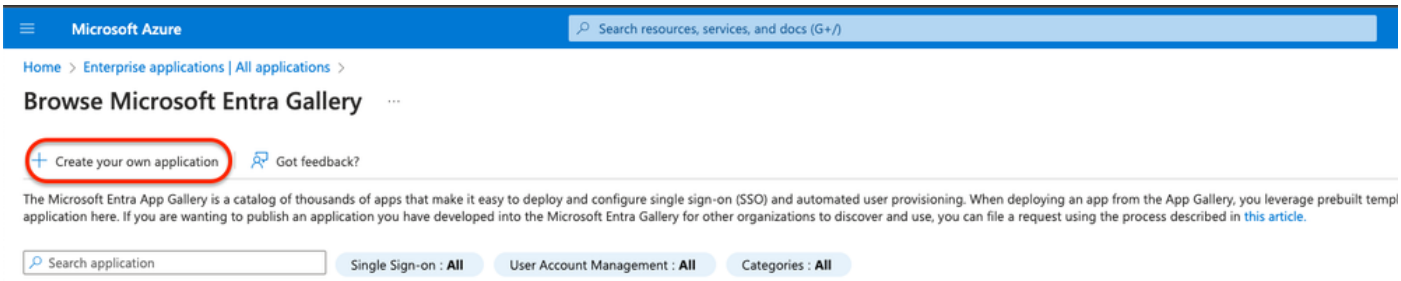
Configuración en Azure

Para habilitar la aplicación en Azure, configure según los siguientes pasos:

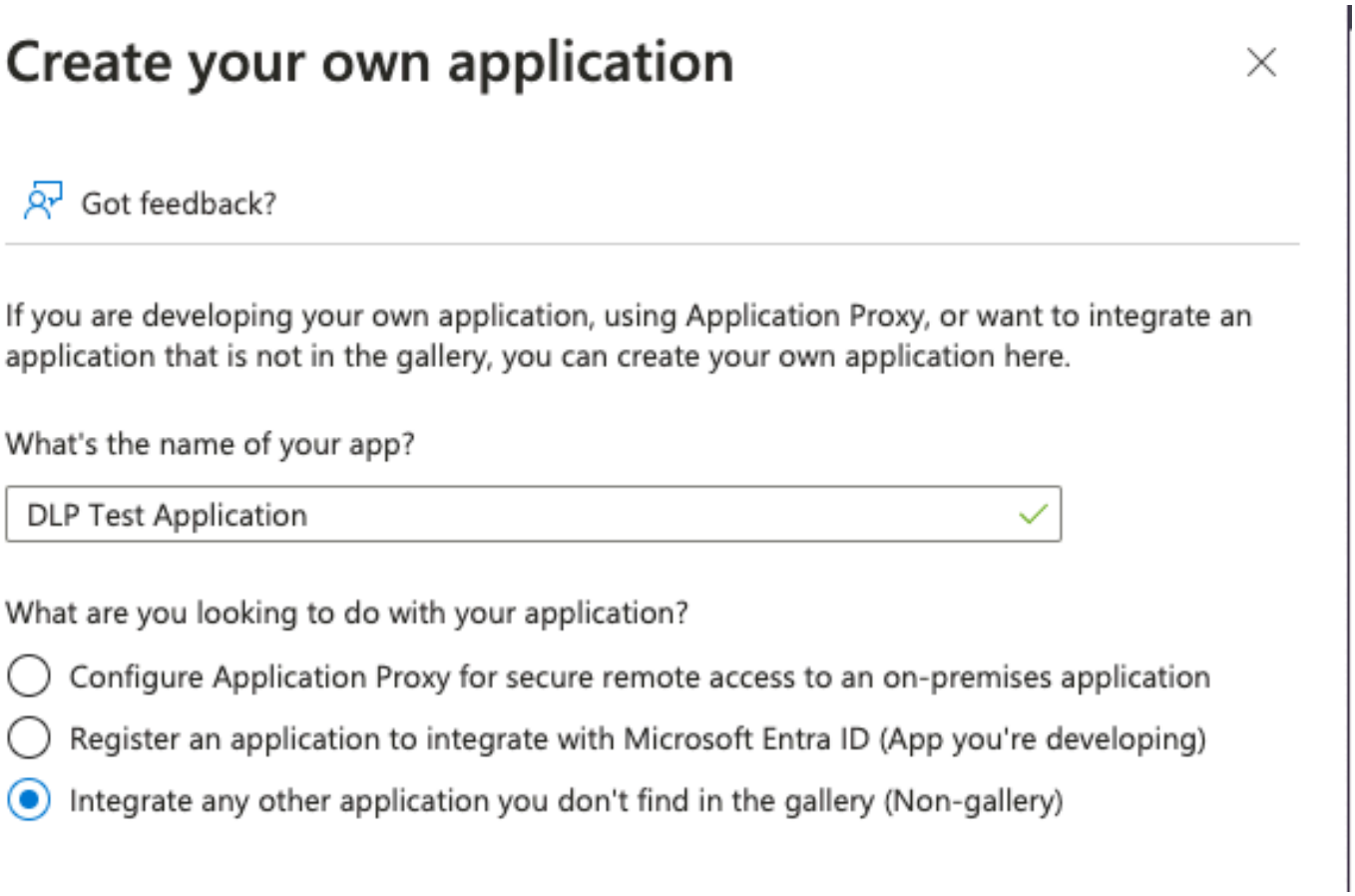
1. Acceda a **Azure Portal > Enterprise Applications > New Application**.



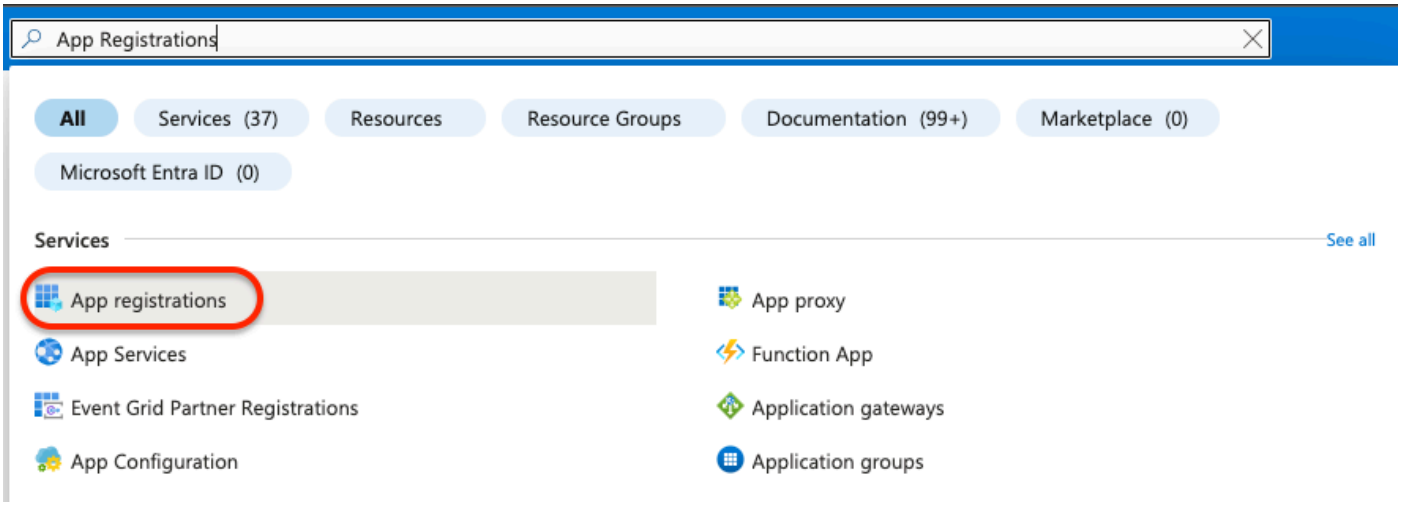
2. Haga clic en **Create your own Application**.



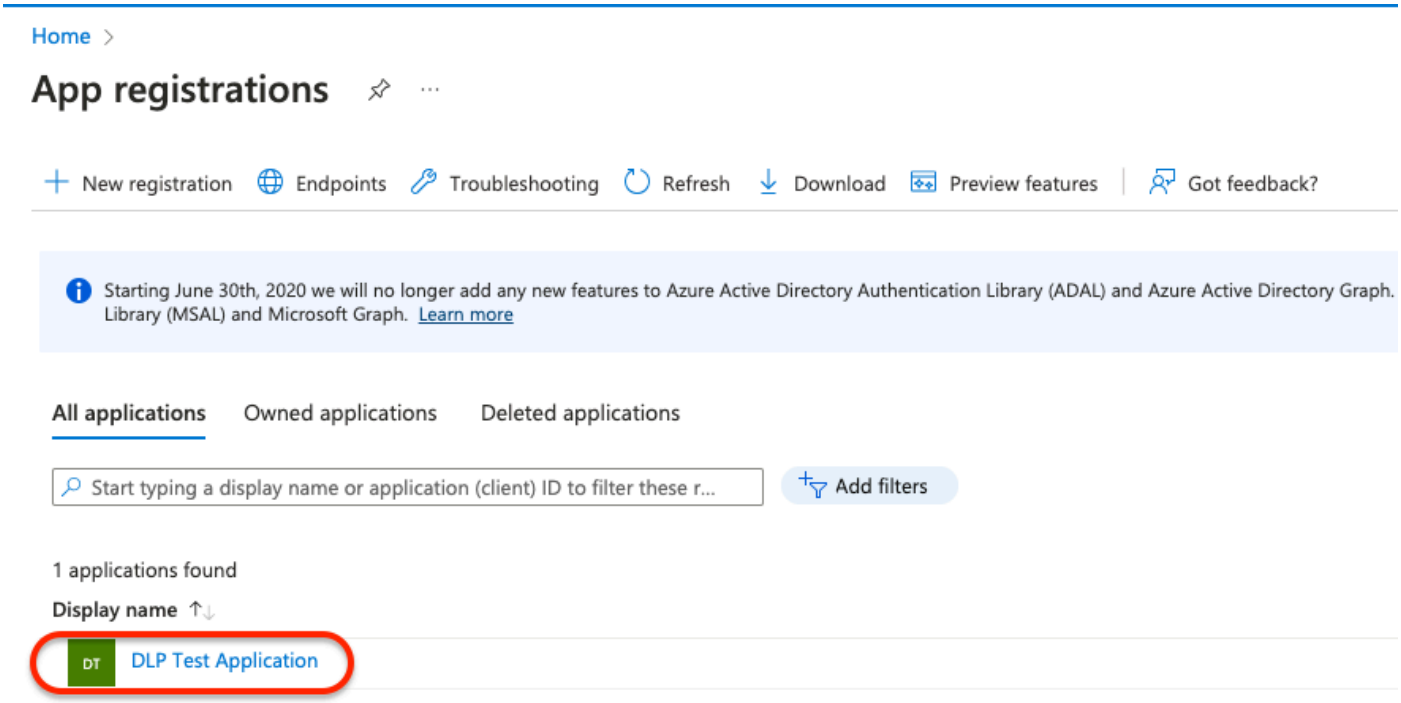
3. Dé un nombre que desee para identificar la aplicación y elegir. **Integrate any other application you don't find in the gallery (Non-Gallery)**.



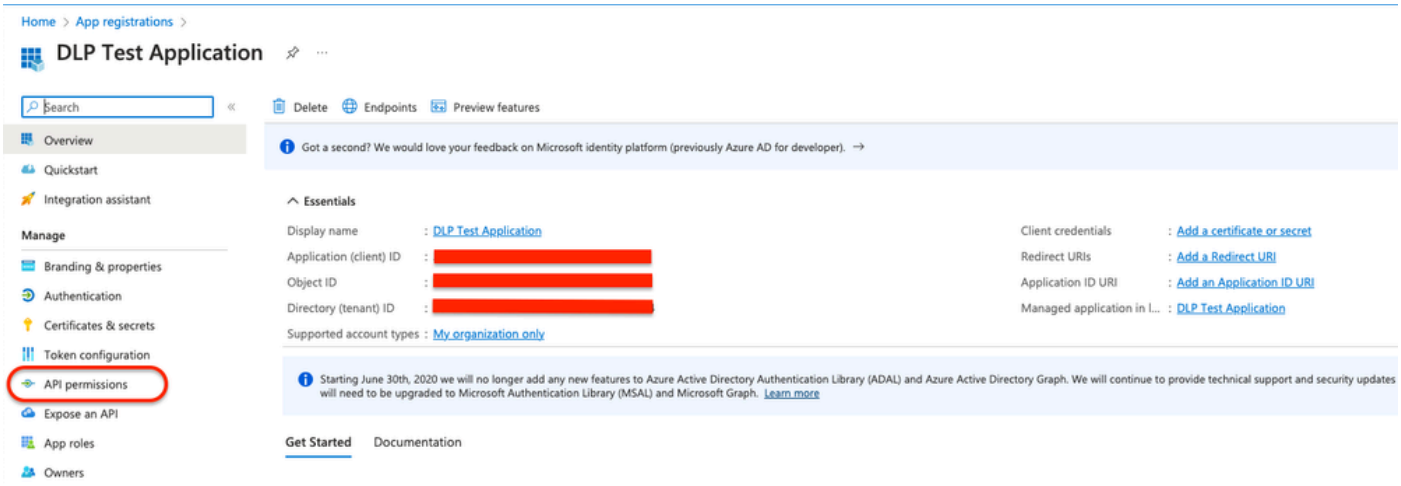
4. Una vez hecho esto, use la barra de búsqueda de Azure para buscar **App Registrations**.



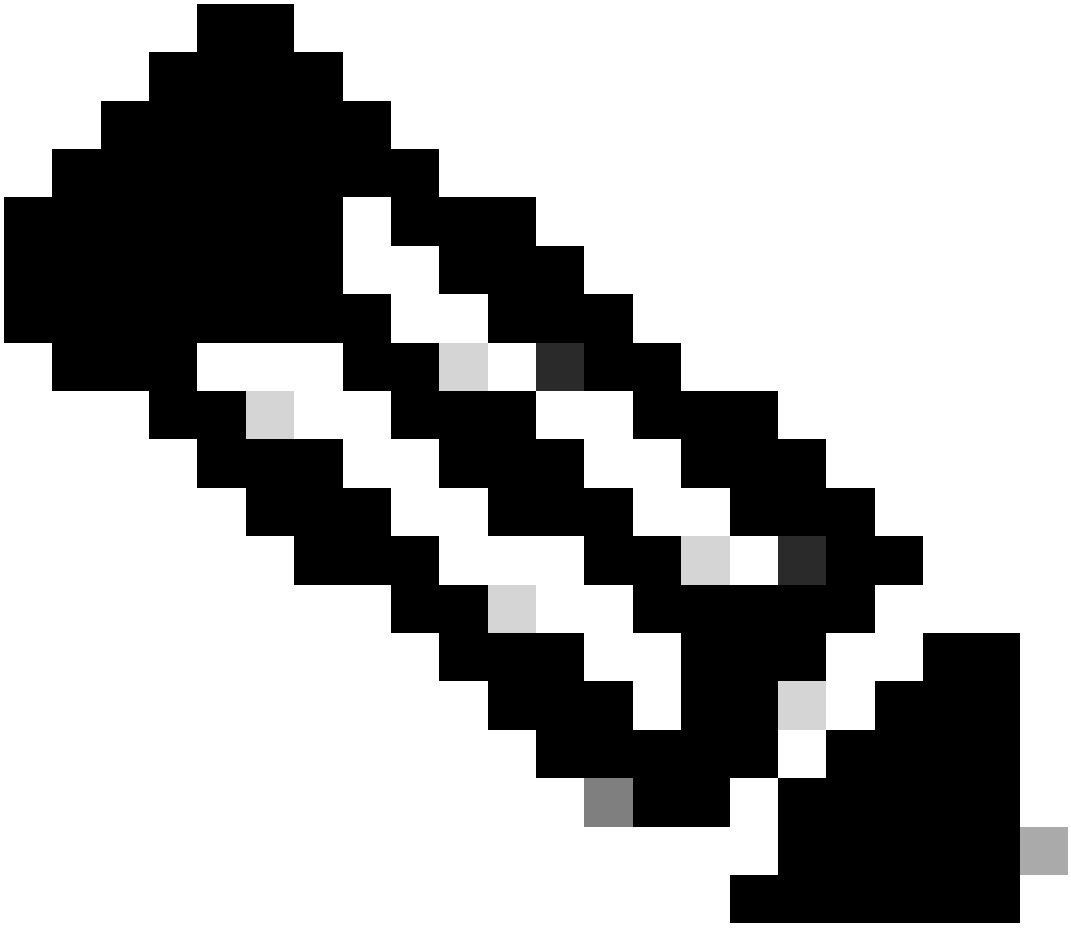
5. Haga clic en **All Applications** y seleccione la aplicación creada en el paso Tres.



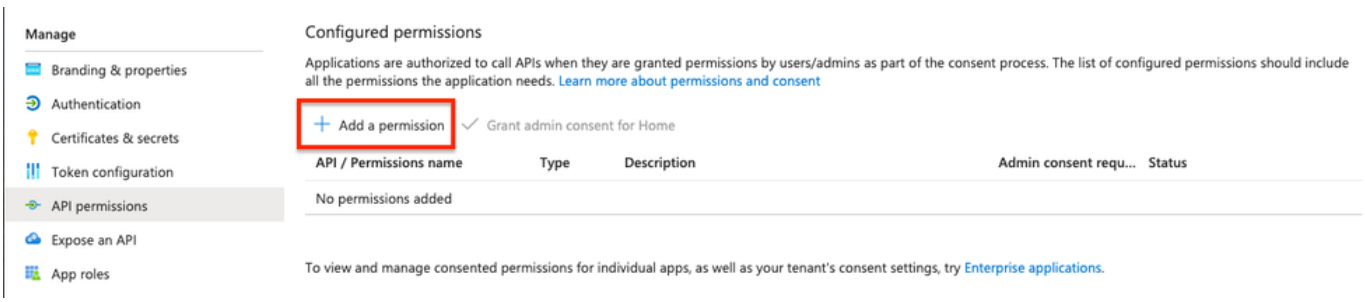
6. Seleccione **API Permissions**.



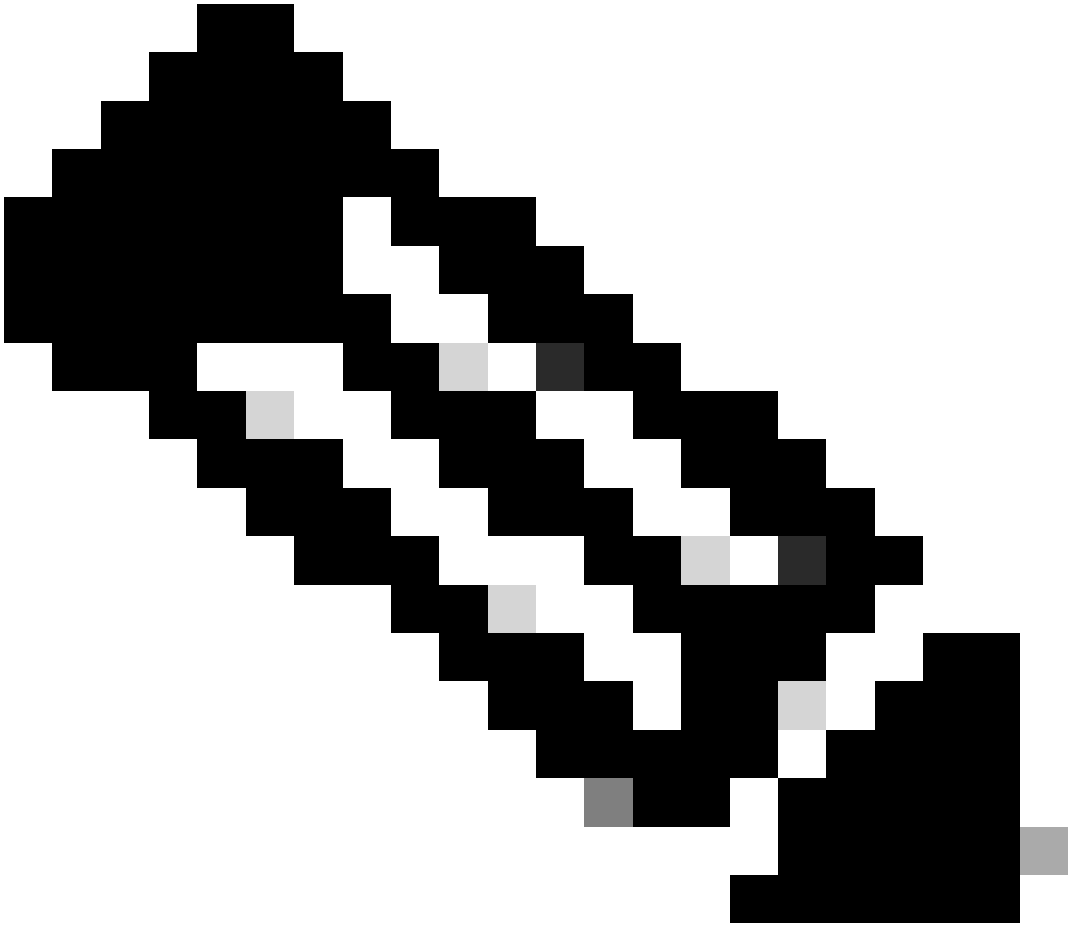
7. Haga clic en **Add a permission** y seleccione los permisos necesarios según la tabla.



Nota: Para ello, debe configurar la API de **Microsoft Graph**, **Office 365 Management APIs**, y **SharePoint**.

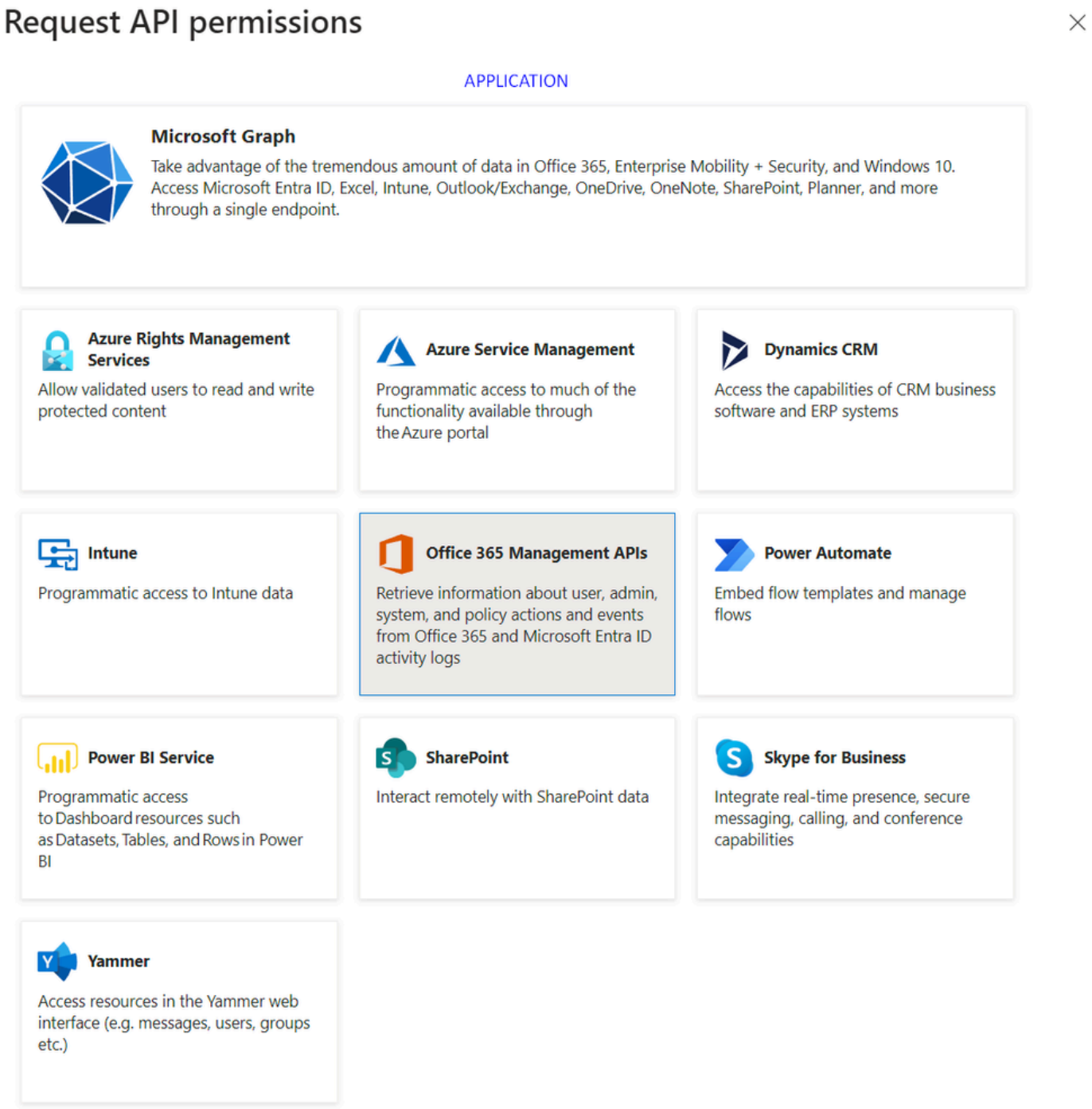


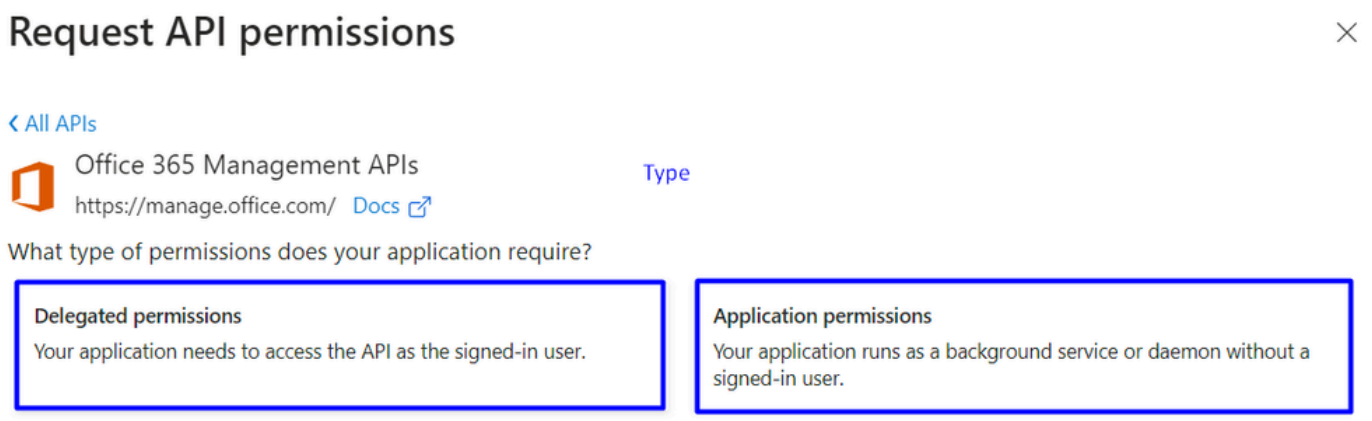
API/ Permissions Name	Type	Description	Admin Consent Required
Microsoft Graph			
Directory.AccessAsUser.All	Delegated	Access directory as the signed-in user	Yes
Directory.Read.All	Application	Read directory data	Yes
Files.Read.All	Delegated	Read all files that user can access	No
Files.Read.All	Application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



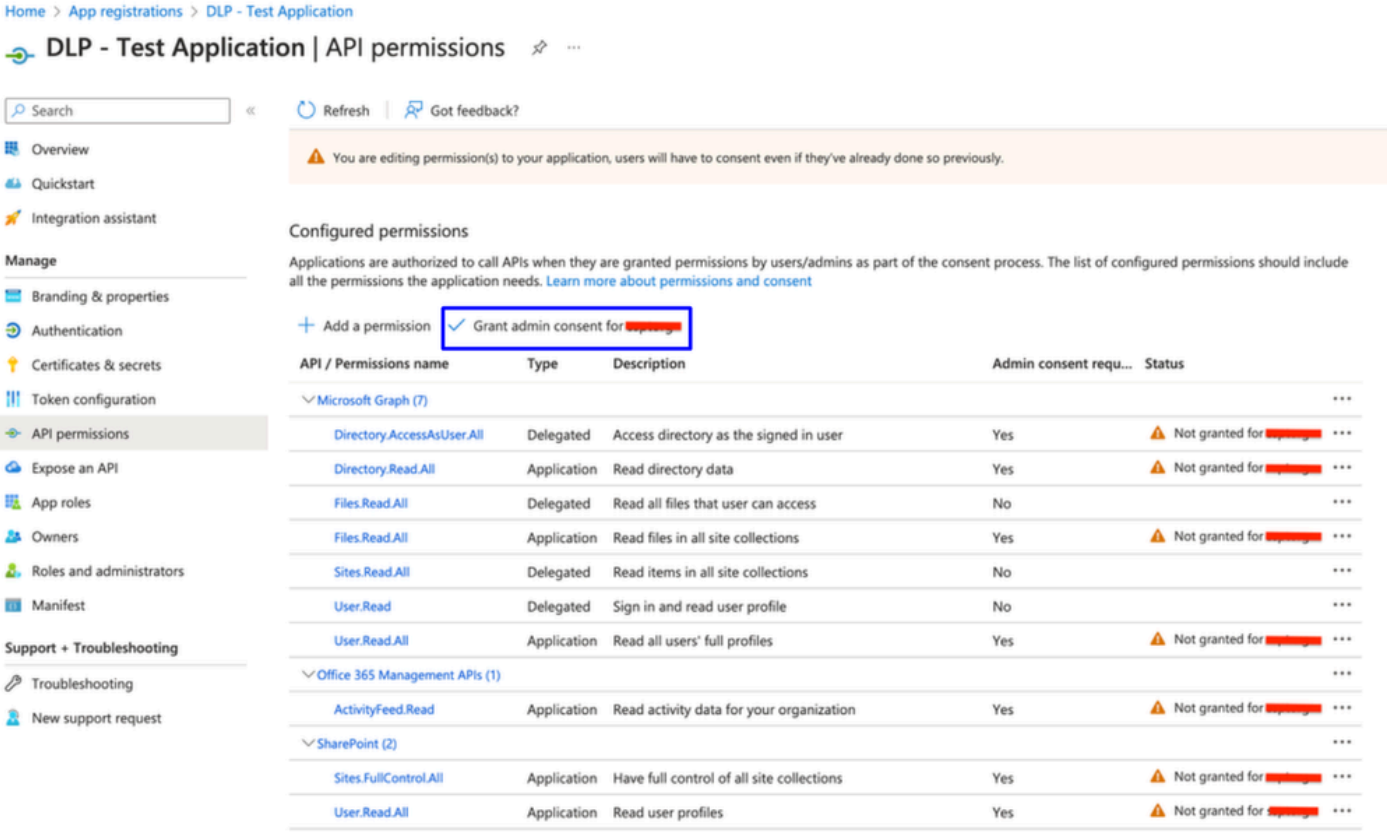
Nota: En lugar de **Site.FullControl.All** permiso, elija **Sites.FullControl.All**.

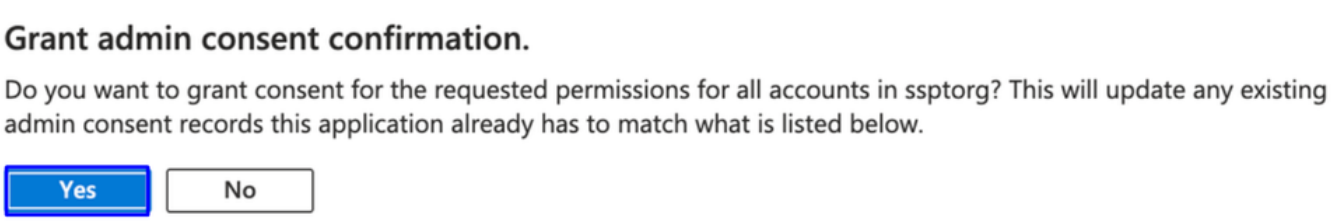
- Para ello, debe elegir el permiso en función de la aplicación y el tipo:



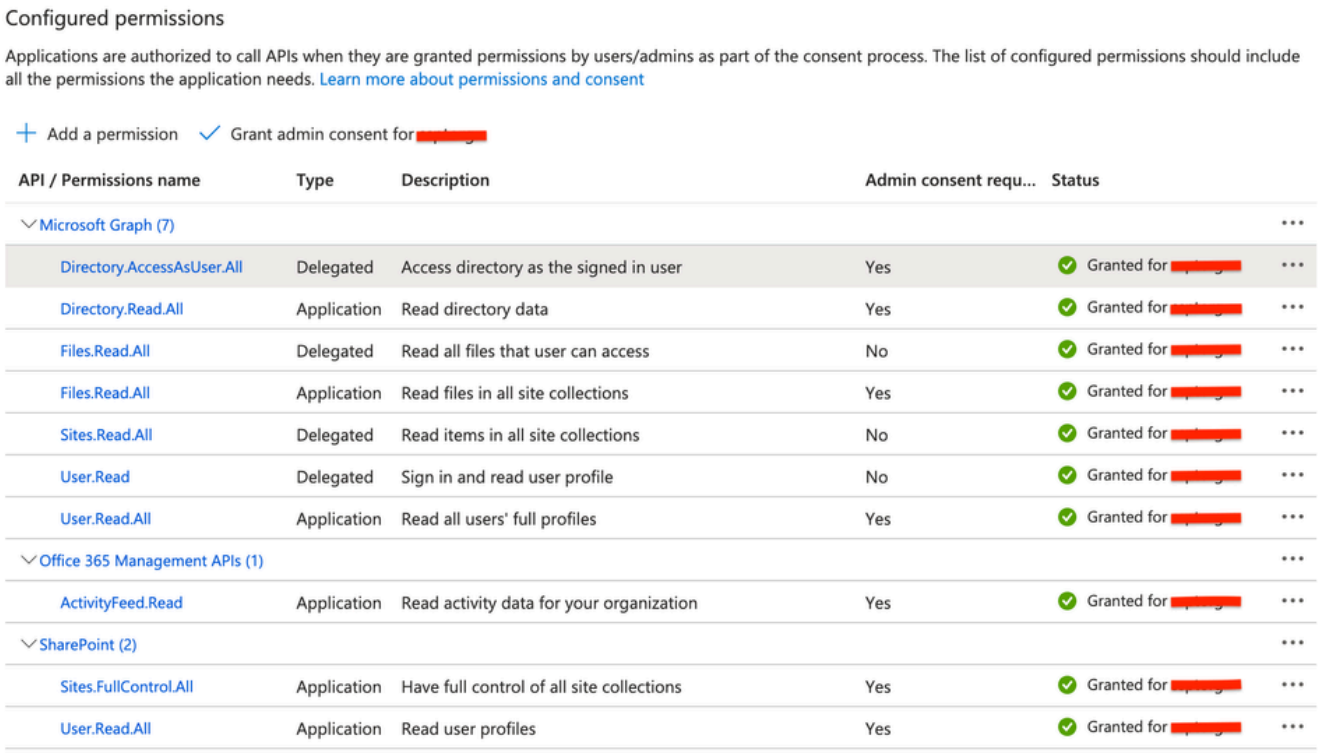


8. Una vez agregados todos los permisos necesarios, haga clic **Grant Admin Consent** en para el arrendatario.





- Una vez concedidos los permisos, el estado es visible como **Granted**



Ahora que la configuración en Azure se ha completado, puede continuar la configuración en Secure Access.

Configuración en Secure Access

Para habilitar la integración, realice la configuración de acuerdo con los siguientes pasos:

- Desplácese hasta Admin > Authentication.
- En **Platforms**, haga clic**Microsoft 365** en.
- Haga clic **Authorize New Tenant** en la DLP subsección y agregue **Microsoft 365**.
- En el cuadro de **Microsoft 365 Authorization** diálogo, active las casillas de verificación para comprobar que cumple los requisitos previos y, a continuación, haga clic en **Next**.
- Proporcione un nombre para el arrendatario y haga clic en **Next**.
- Haga clic **Next** para ser redirigido a la página de inicio de sesión de Microsoft 365.
- Inicie sesión en Microsoft 365 con credenciales de administrador para conceder acceso. A continuación, cuando se le redirija a Secure Access, debe tener un mensaje que indique que la integración se ha realizado correctamente.
- Haga clic **Done** para finalizar.

Verificación

Para verificar si la integración se realizó correctamente, navegue hasta el panel de acceso seguro:

- Haga clic en **Admin > Authentication > Microsoft 365**

Y si todo está correctamente configurado, su estado debe ser **Authorized**.

Información Relacionada

- Habilitar la protección contra pérdida de datos API SaaS para arrendatarios de Microsoft 365
- Activar o desactivar la auditoría en Microsoft

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).