

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración en Azure](#)

[Configuración en Secure Access](#)

[Verificación](#)

[Información Relacionada](#)

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

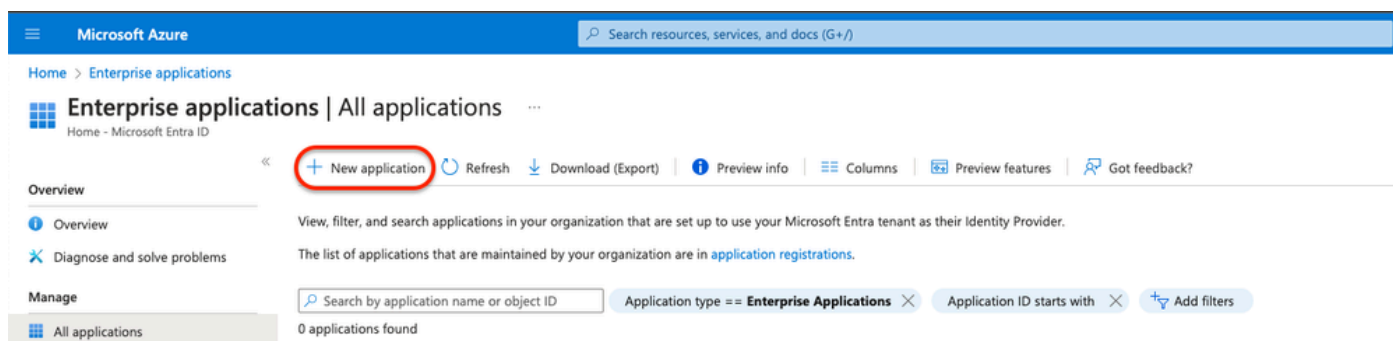
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Configurar

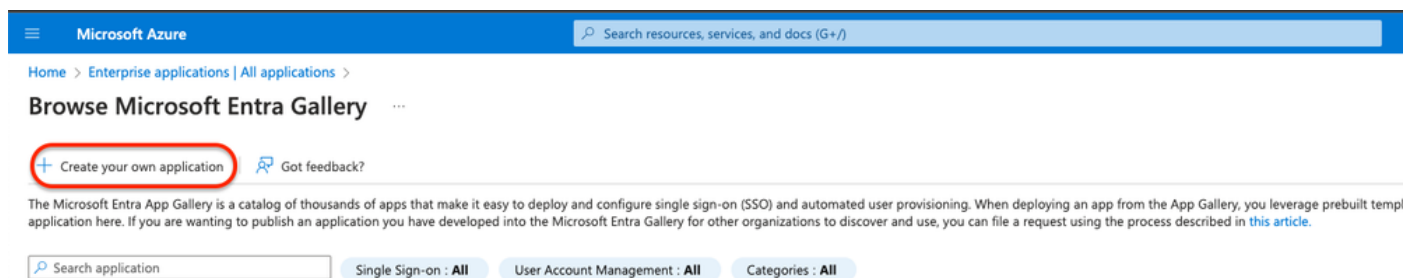
Configuración en Azure

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)**.

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.

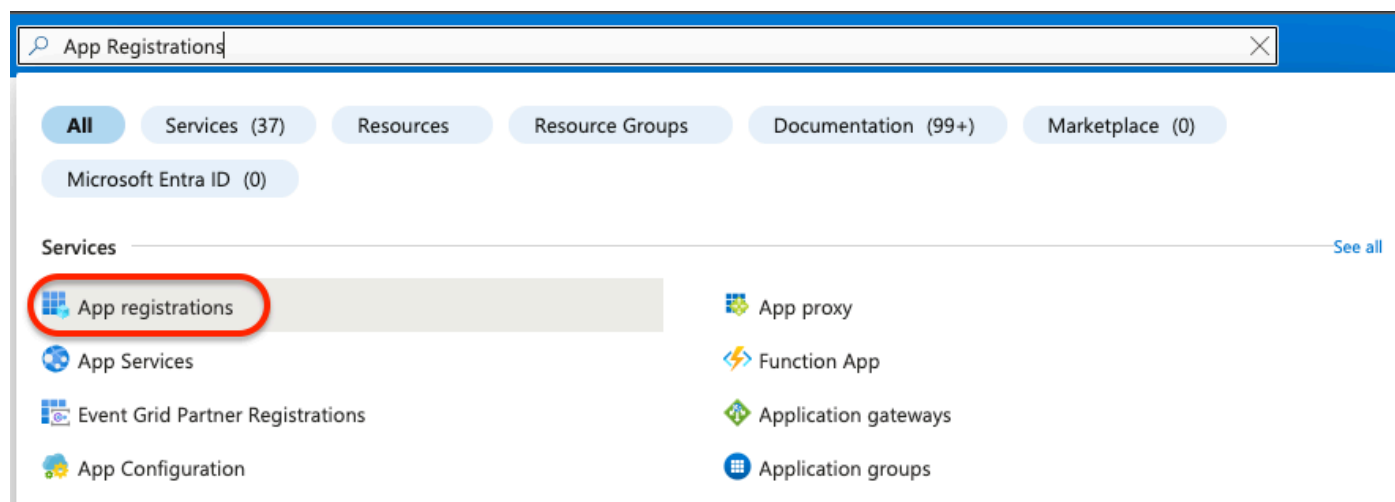
What's the name of your app?

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



The screenshot shows the Azure search interface. The search bar contains the text "App Registrations". Below the search bar, there are several filter buttons: "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".

5. Haga clic en **All Applications** y seleccione la aplicación creada en el paso [Tres](#).

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. Seleccione API Permissions.

Home > App registrations >

DLP Test Application

🗑 Delete 🌐 Endpoints 📄 Preview features

🔍 Search

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

📘 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](#)

📘 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. 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**.

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














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:

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

Type

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

DLP - Test Application | API permissions

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.

- Una vez concedidos los permisos, el estado es visible como **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 [redacted]

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 [redacted] ...
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for [redacted] ...
Files.Read.All	Delegated	Read all files that user can access	No	✓ Granted for [redacted] ...
Files.Read.All	Application	Read files in all site collections	Yes	✓ Granted for [redacted] ...
Sites.Read.All	Delegated	Read items in all site collections	No	✓ Granted for [redacted] ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for [redacted] ...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for [redacted] ...
▼ Office 365 Management APIs (1) ...				
ActivityFeed.Read	Application	Read activity data for your organization	Yes	✓ Granted for [redacted] ...
▼ SharePoint (2) ...				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	✓ Granted for [redacted] ...
User.Read.All	Application	Read user profiles	Yes	✓ Granted for [redacted] ...

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**.

DLP

Name	Status	Action
Microsoft 365	● Authorized	REVOKE

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).