Configure Secure Access with Office 365 for Enhanced Data Loss Prevention

Contents

Introduction

This document describes the integration of Data Loss Prevention for Office 365 with Secure Access.

Prerequisites

- **Office 365 E3 Subscription** is present for your Microsoft tenant
- Compliance auditing is configured as **ON** in the compliance portal before you start your integration

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Access
- Microsoft Azure Enterprise Applications and App Registrations

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Access
- Microsoft Azure
- Microsoft 365 Compliance portal

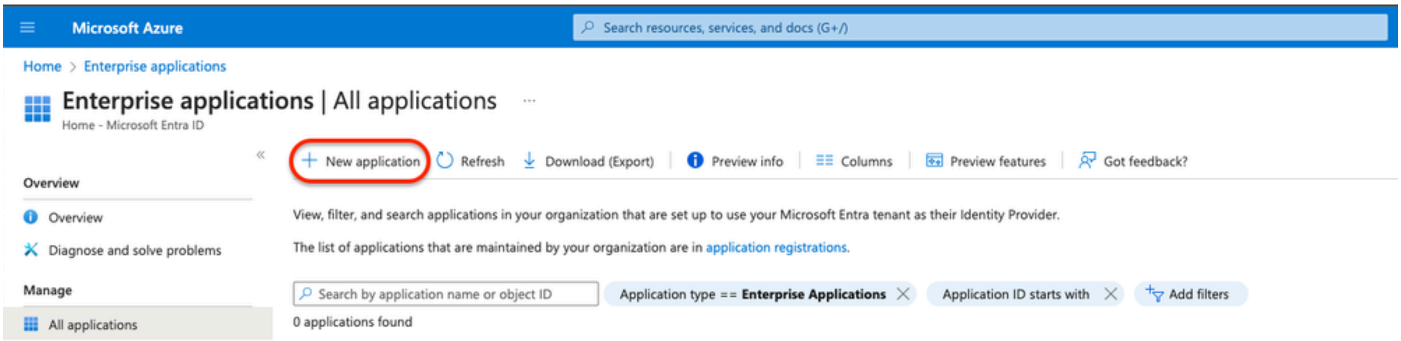
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Configuration on Azure

To enable the application on Azure, configure according to the next steps:

1. Navigate to the **Azure Portal > Enterprise Applications > New Application.**

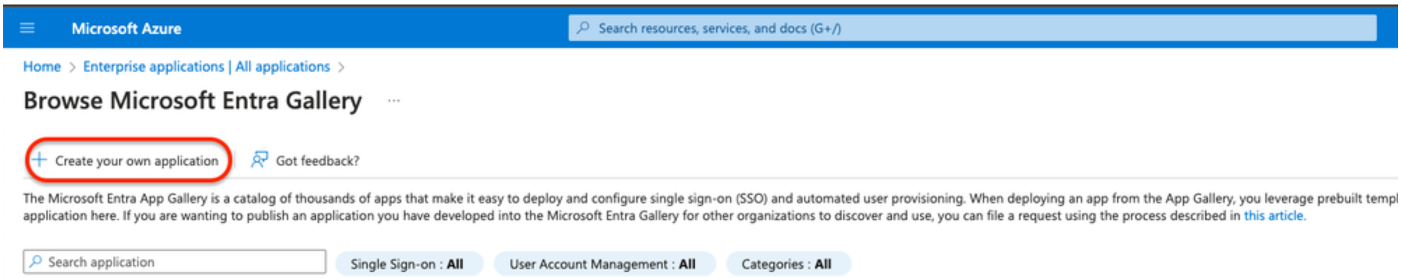

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications
Enterprise applications | All applications
Home - Microsoft Entra ID
New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?
Overview
Overview
Diagnose and solve problems
Manage
All applications
Search by application name or object ID
Application type == Enterprise Applications
Application ID starts with
Add filters

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

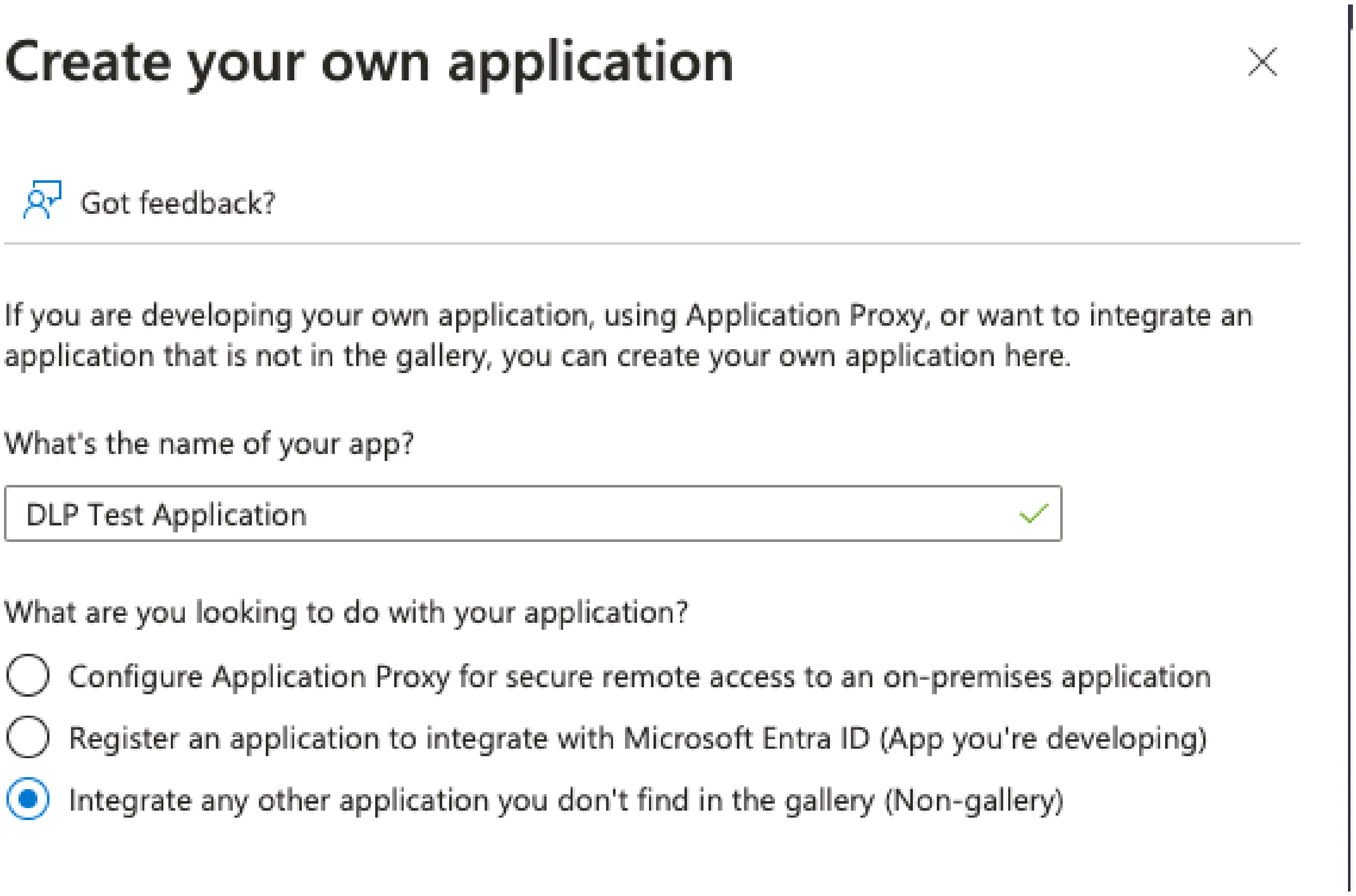
0 applications found

2. Click on **Create your own Application.**


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications | All applications >
Browse Microsoft Entra Gallery
Create your own application
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templ application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in this article.

3. Give a name you desire to identify the app and choose. **Integrate any other application you don't find in the gallery (Non-Gallery).**



Create your own application

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 ✓

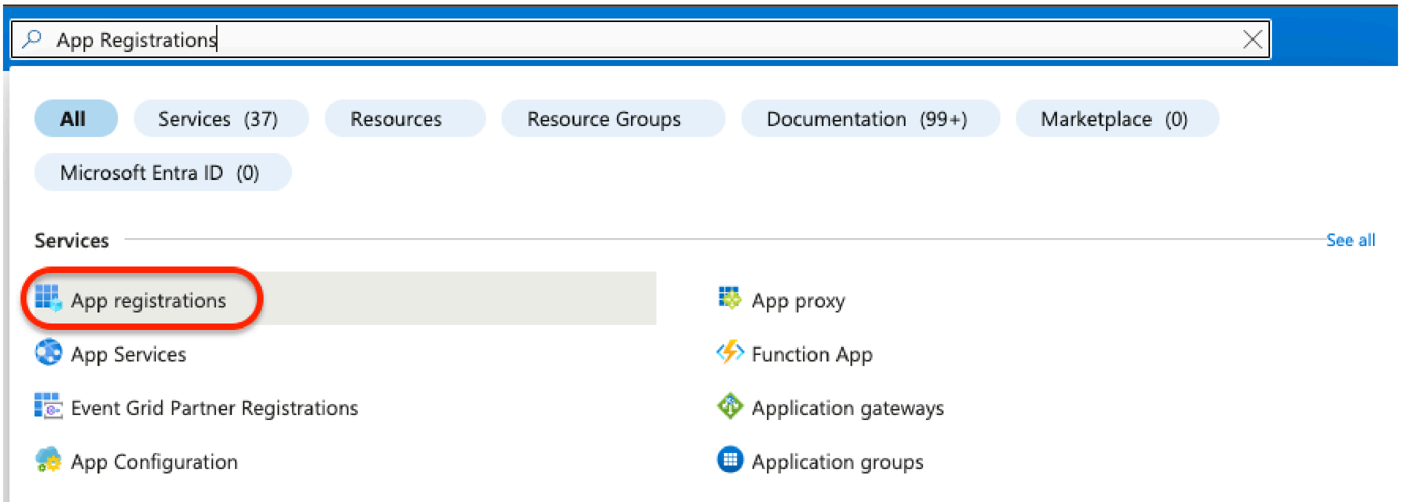
What are you looking to do with your application?

○ 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)

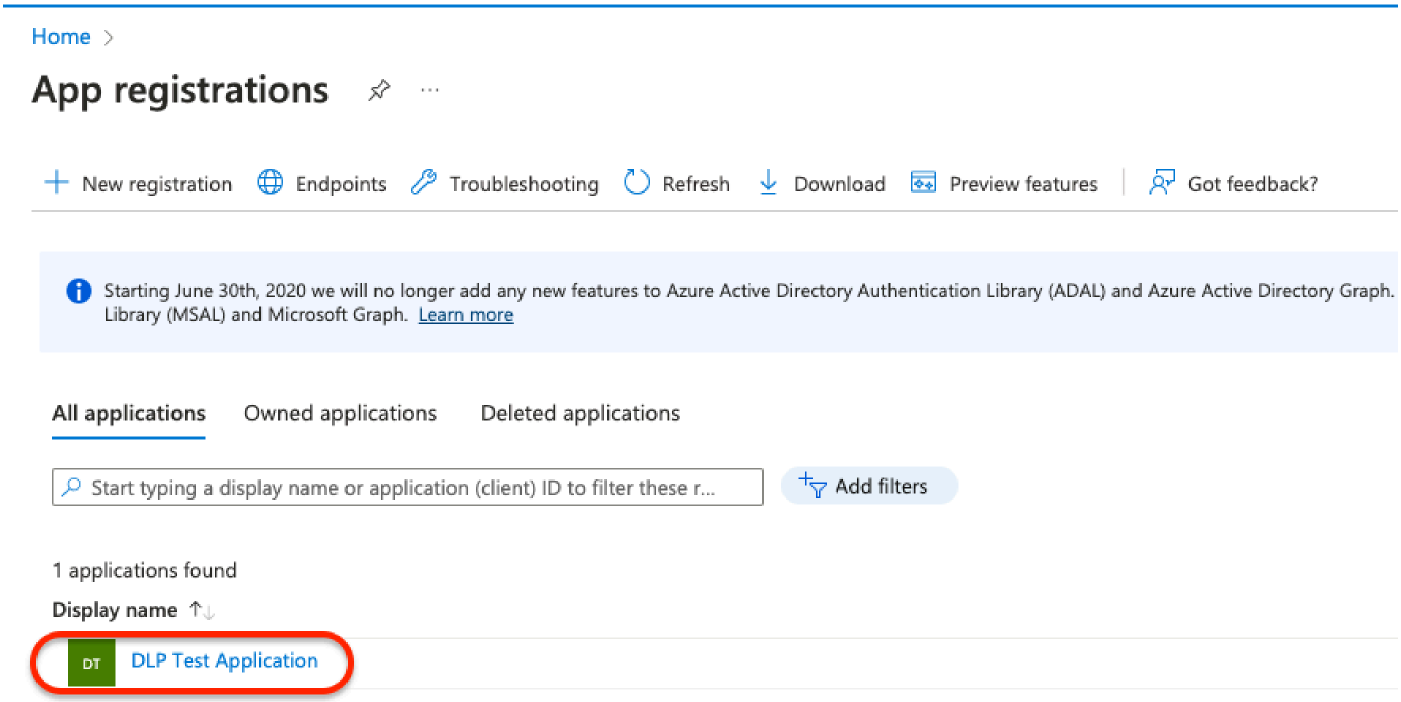
● Integrate any other application you don't find in the gallery (Non-gallery)

4. Once done, use the Azure Search Bar to look for **App Registrations.**



App Registrations

5. Click on **All Applications** and choose the application created in step Three.



Home >

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...

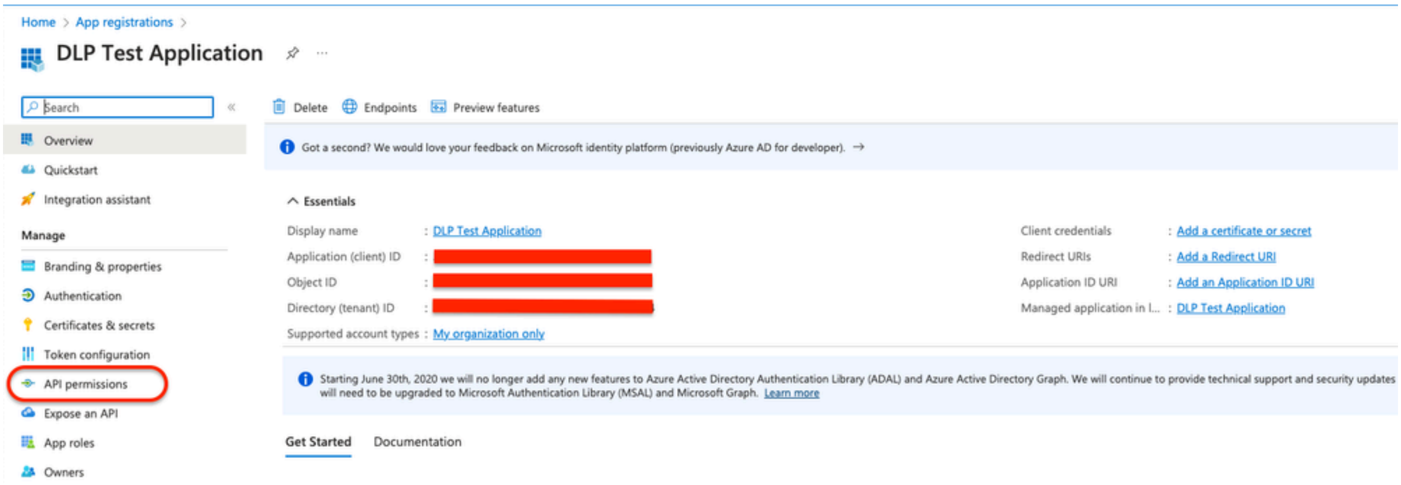
Add filters

1 applications found

Display name ↑↓

DT DLP Test Application

6. Choose **API Permissions**.



Home > App registrations >

DLP Test Application

Search

Delete | Endpoints | Preview features

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

Essentials

Display name : DLP Test Application

Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : My organization only

Client credentials : Add a certificate or secret

Redirect URIs : Add a Redirect URI

Application ID URI : Add an Application ID URI

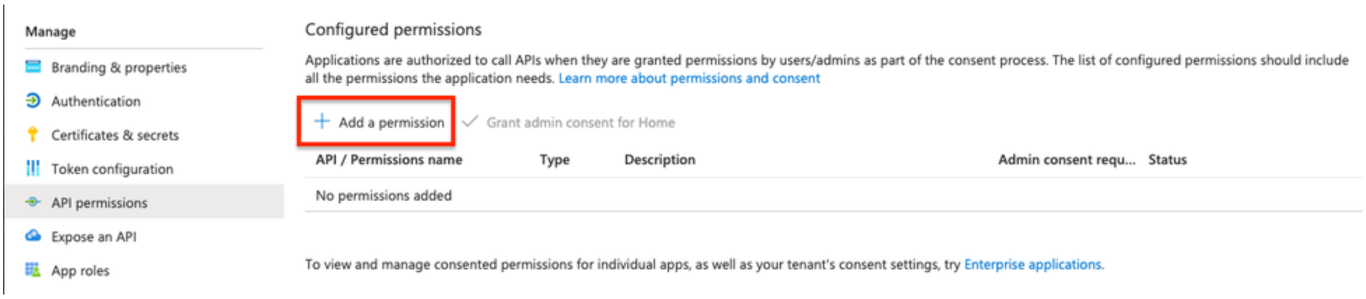
Managed application in l... : DLP Test Application

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. Click on **Add a permission** and choose the required permissions based on the Table.

Note: For that, you must configure the API of **Microsoft Graph**, **Office 365 Management APIs**, and **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

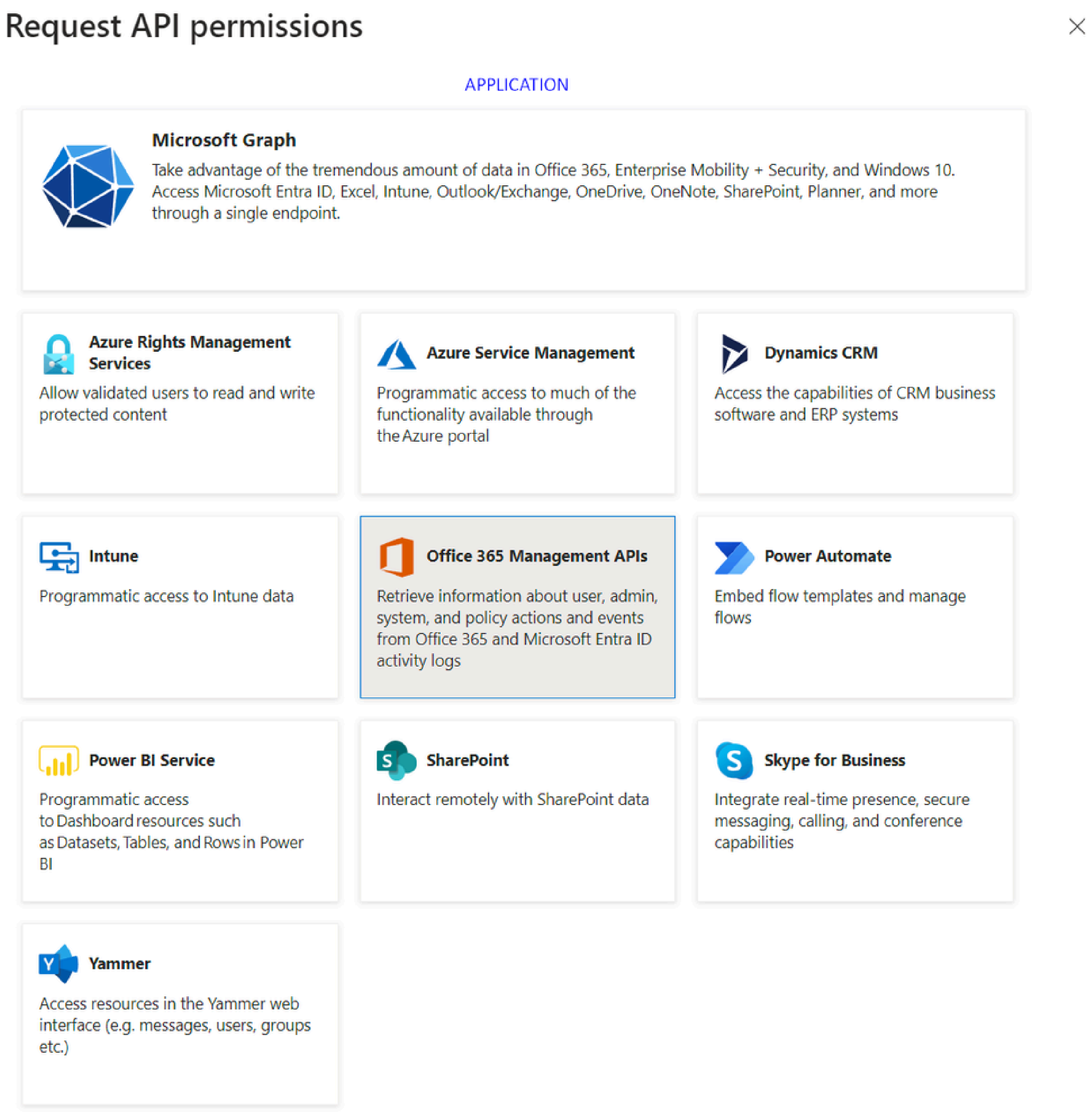
API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

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

Note: Instead of **Site.FullControl.All** permission choose **Sites.FullControl.All**.

- For that, you need to choose the permission based on the application and type:



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

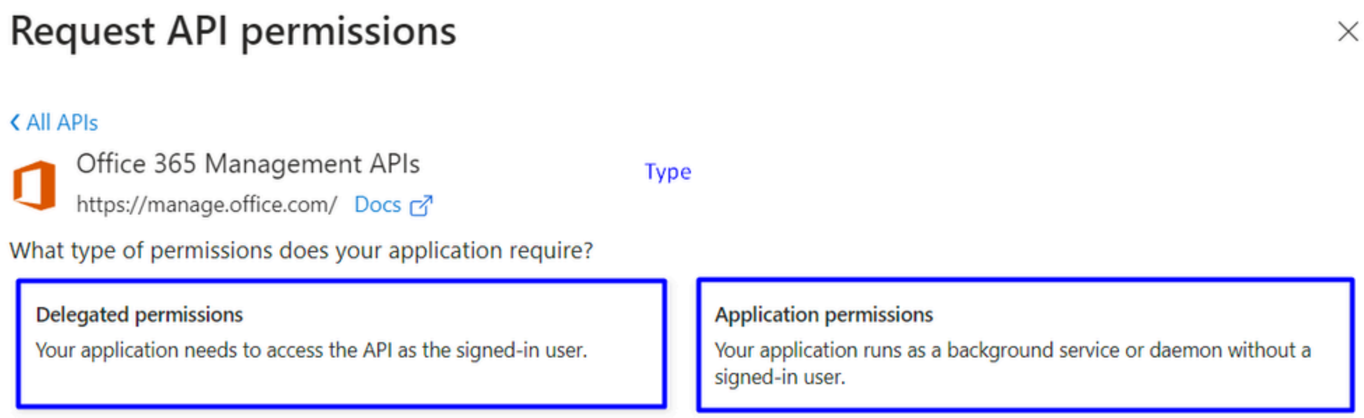
Power Automate
Embed flow templates and manage flows

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

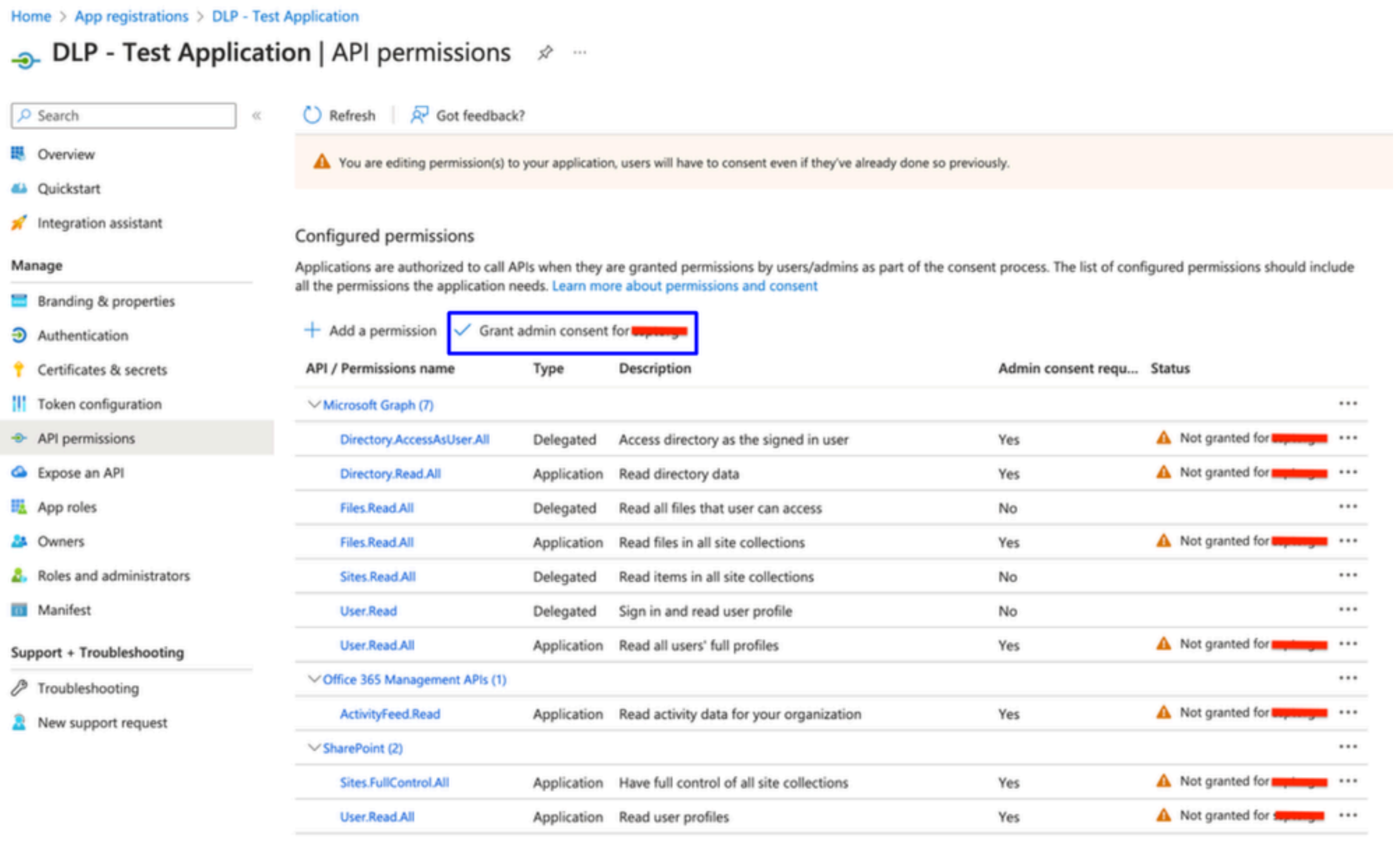
Type

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. Once all the required permissions are added, click on **Grant Admin Consent** for the tenant.

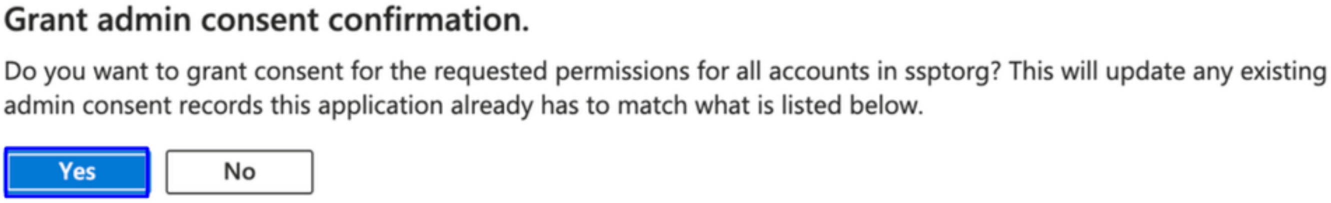


⚠ You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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

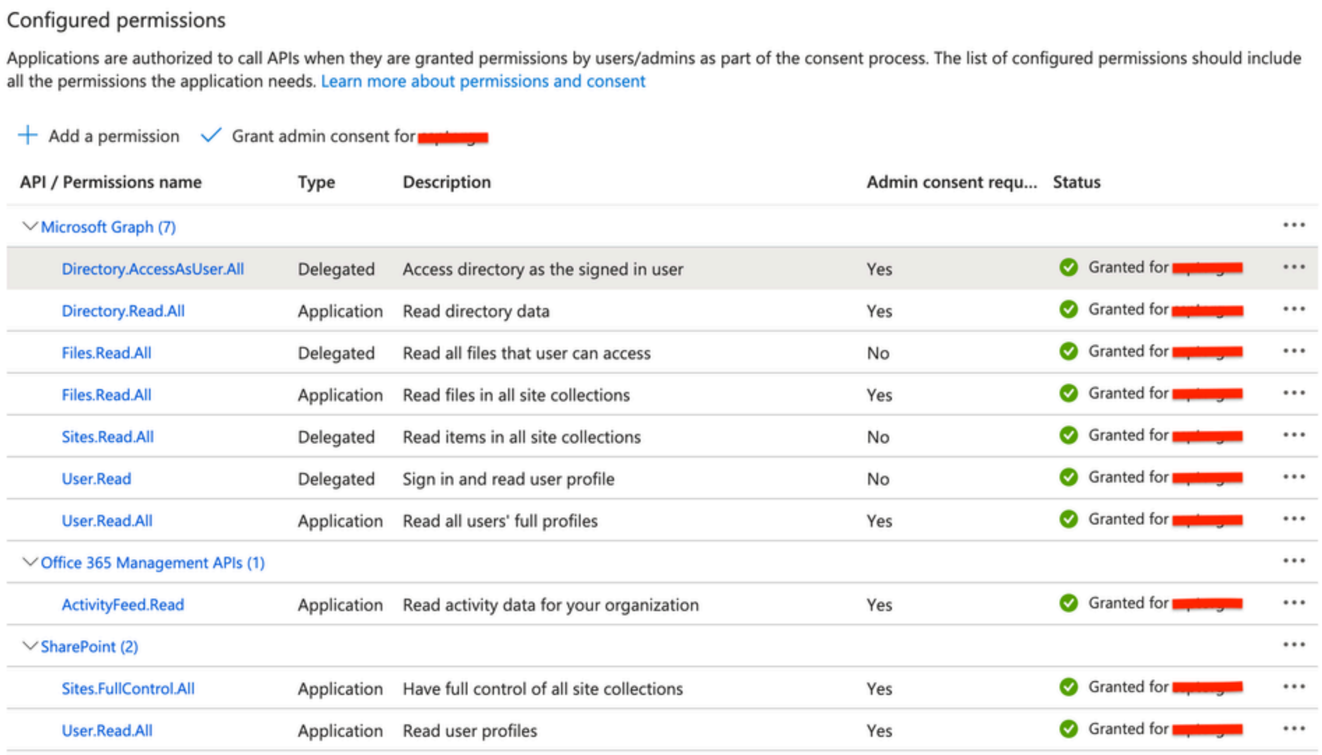
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	⚠ Not granted for [redacted]
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for [redacted]
Files.Read.All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



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.

- Once you grant the permissions, the status is visible as **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

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]	···

Now that the configuration on Azure is completed, you can continue the configuration on Secure Access.

Configuration in Secure Access

To enable the integration, configure according the next steps:

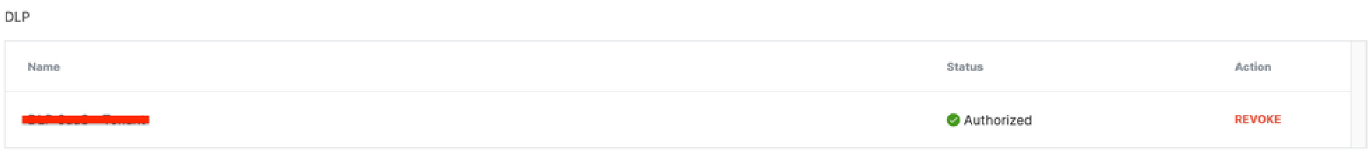
1. Navigate to Admin > Authentication.
2. Under **Platforms**, click**Microsoft 365**.
3. Click **Authorize New Tenant** in the DLP subsection and add **Microsoft 365**.
4. In the **Microsoft 365 Authorization** dialog, check the checkboxes to verify you meet the prerequisites, then click **Next**.
5. Provide a name for your tenant, then click **Next**.
6. Click **Next** to be redirected to the Microsoft 365 login page.
7. Log in to Microsoft 365 with admin credentials to grant access. Then, when you get redirected to Secure Access, you must have a message that indicates your integration was successful.
8. Click **Done** to complete.

Verify

To verify if the integration was successful, navigate to your Secure Access Dashboard:

- Click on **Admin** > **Authentication** > **Microsoft 365**

And if everything is correctly configured, your status must be **Authorized**.



DLP

Name	Status	Action
[redacted]	✓ Authorized	REVOKE

Related Information

- Enable SaaS API Data Loss Protection for Microsoft 365 Tenants
- Turning auditing ON or OFF in Microsoft