Configurare l'accesso sicuro con Office 365 per una prevenzione avanzata della perdita di dati

Sommario

Introduzione

Questo documento descrive l'integrazione di Data Loss Prevention per Office 365 con Secure Access.

Prerequisiti

- **Office 365 E3 Subscription** è presente per il tenant Microsoft
  - Il controllo della conformità è configurato come **ON** nel portale della conformità prima di iniziare l'integrazione

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Access
- Registrazioni applicazioni e app aziendali di Microsoft Azure

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Access

  - Microsoft Azure

- Portale conformità Microsoft 365

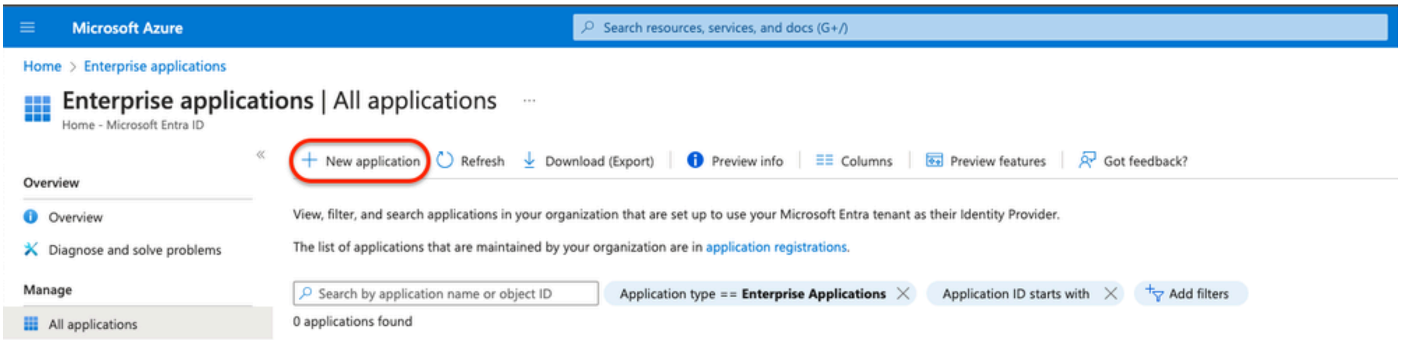
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazione in Azure

Per abilitare l'applicazione in Azure, configurare in base alla procedura seguente:

1. Passare alla finestra di **Azure Portal** > **Enterprise Applications** > **New Application**dialogo.


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
Add filters

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

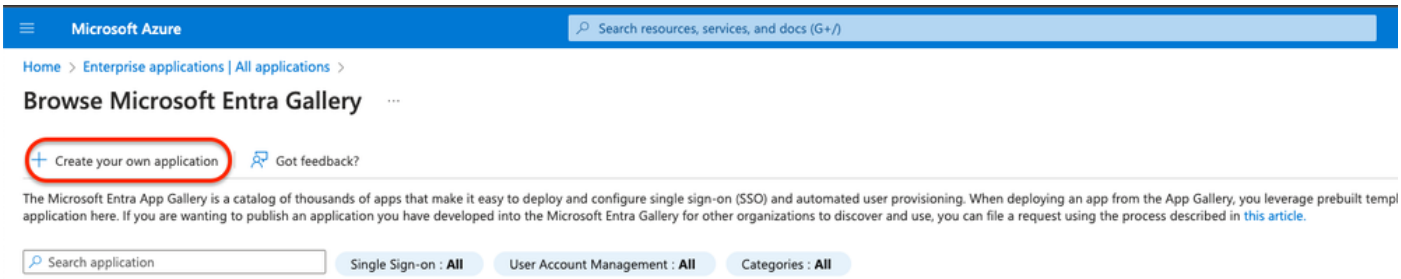
The list of applications that are maintained by your organization are in application registrations.

Application type == **Enterprise Applications**

Application ID starts with

0 applications found

2. Fare clic su **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

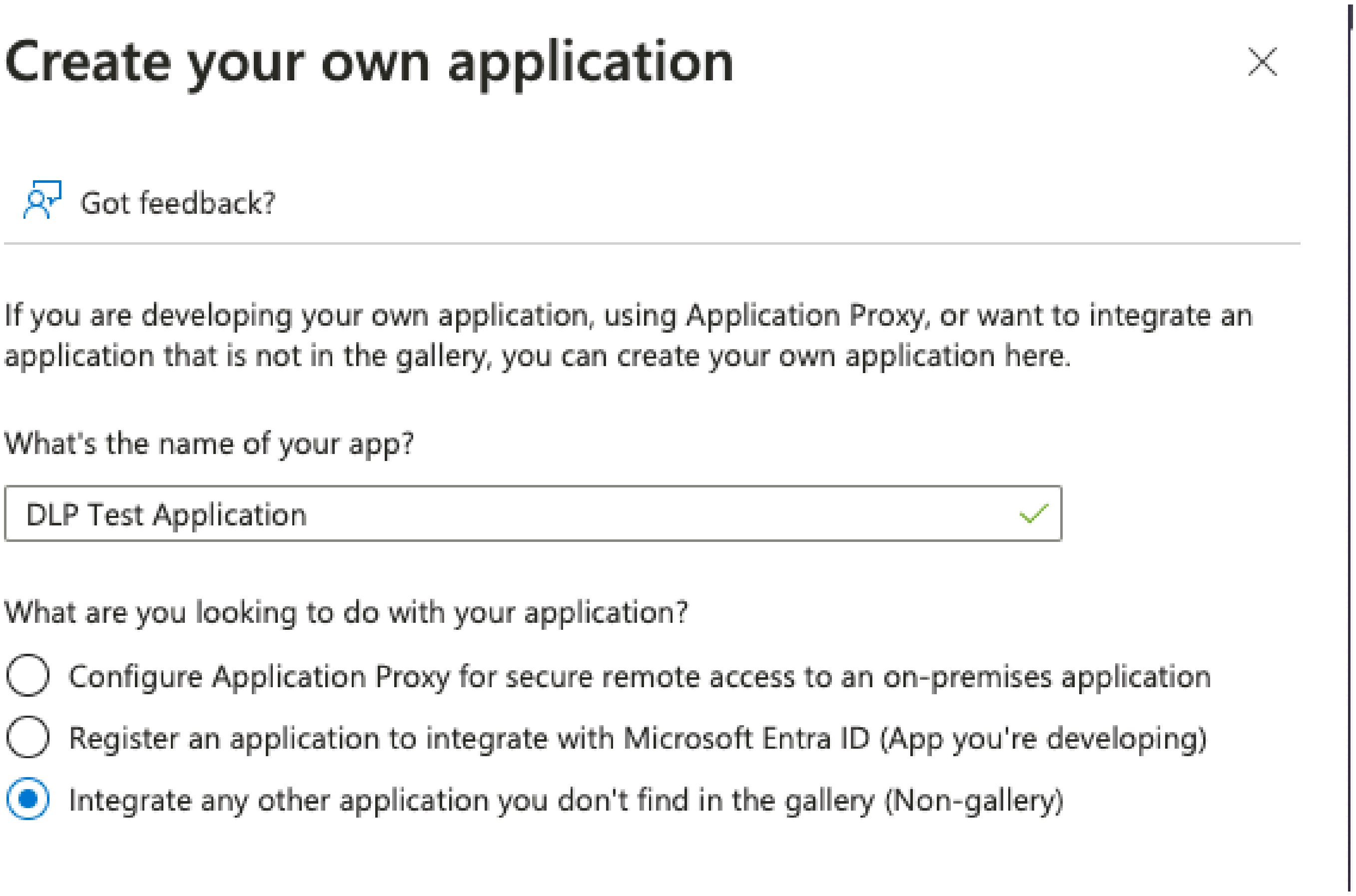
The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templ application here. If you are wanting to publish an application you 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.

Single Sign-on : **All**

User Account Management : **All**

Categories : **All**

3. Dai un nome che vuoi per identificare l'app e scegli. **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

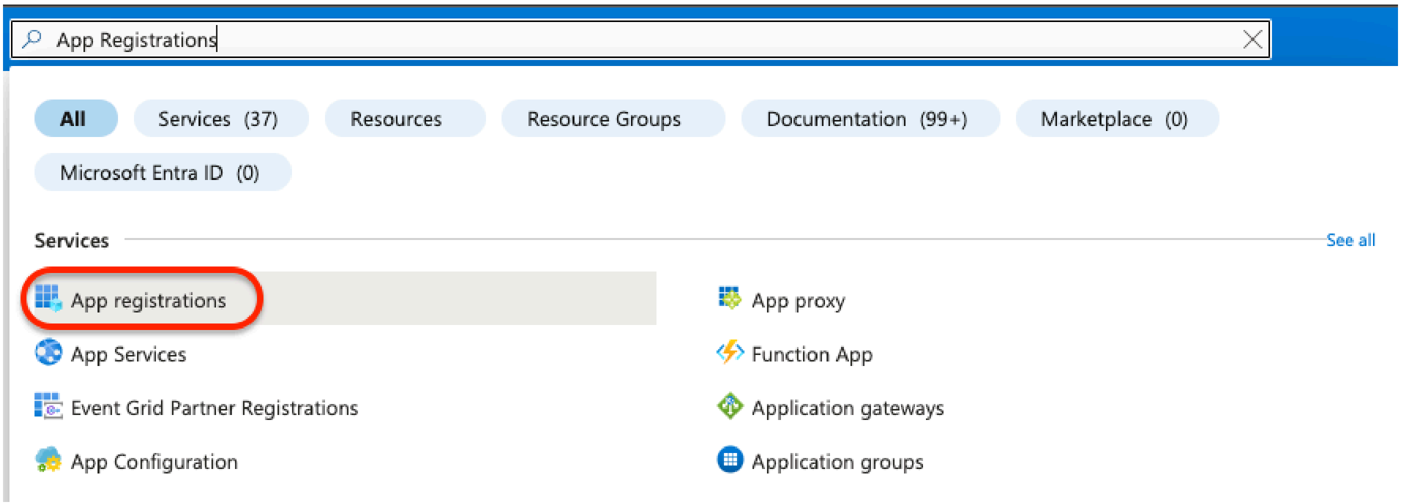
What are you looking to do with your application?

○ 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)

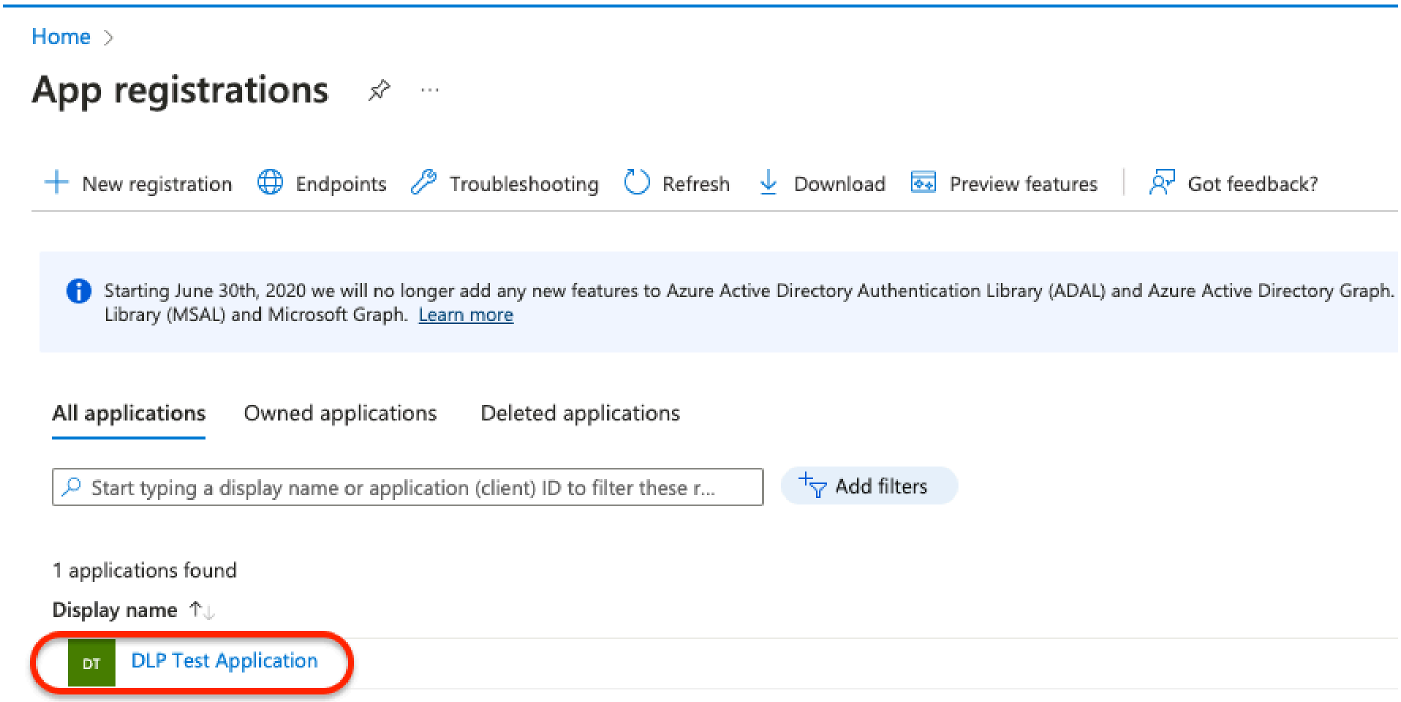
● Integrate any other application you don't find in the gallery (Non-gallery)

4. Al termine, usare la barra di ricerca di Azure per cercare **App Registrations**i dati.



App Registrations

5. Fare clic su **All Applications** e scegliere l'applicazione creata al passo 3.



Home >

App registrations

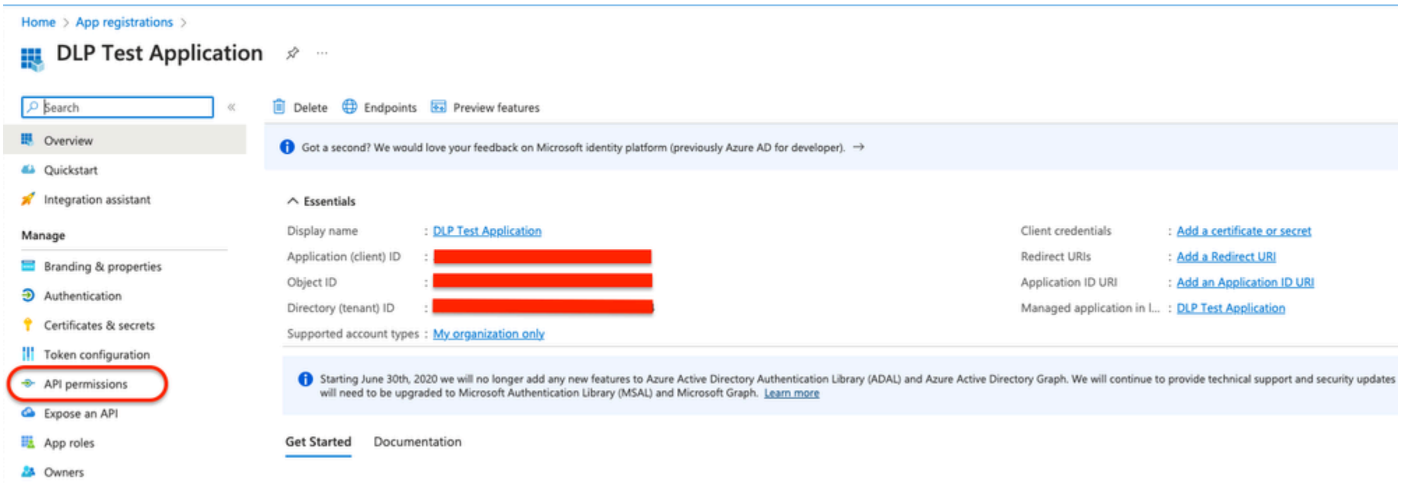
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. Library (MSAL) and Microsoft Graph. Learn more

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. Scegliere **API Permissions**.



Home > App registrations >

DLP Test Application

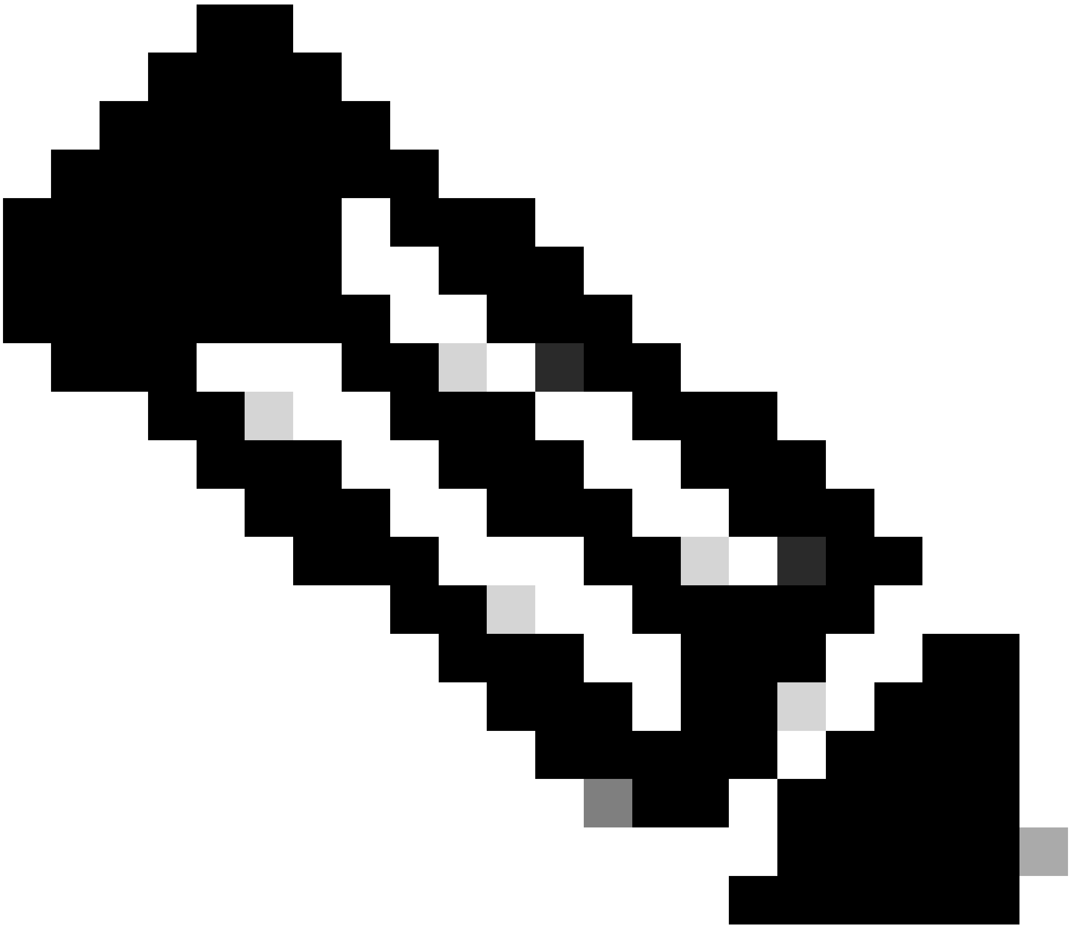
Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

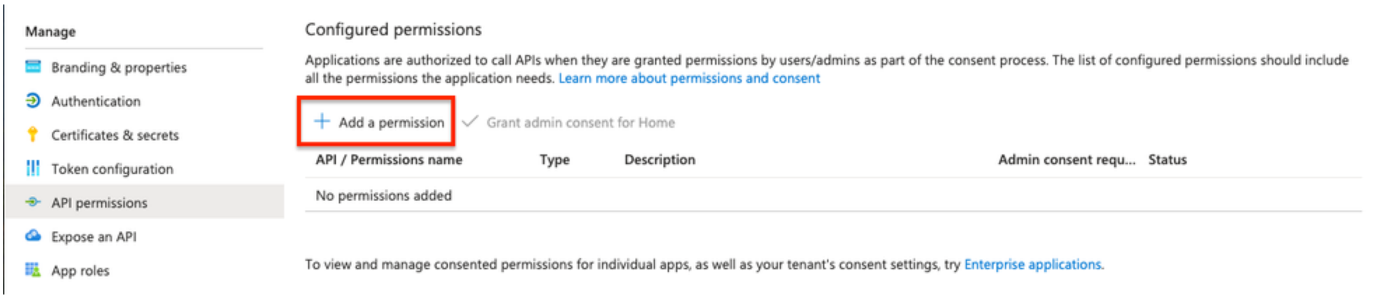
Display name	: DLP Test Application	Client credentials	: Add a certificate or secret
Application (client) ID	: [redacted]	Redirect URIs	: Add a Redirect URI
Object ID	: [redacted]	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: [redacted]	Managed application in l...	: DLP Test 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

7. Fare clic su **Add a permission** e scegliere le autorizzazioni necessarie in base alla tabella.



Nota: a tale scopo, è necessario configurare l'API di **Microsoft Graph**, **Office 365 Management APIs**, e **SharePoint**.



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

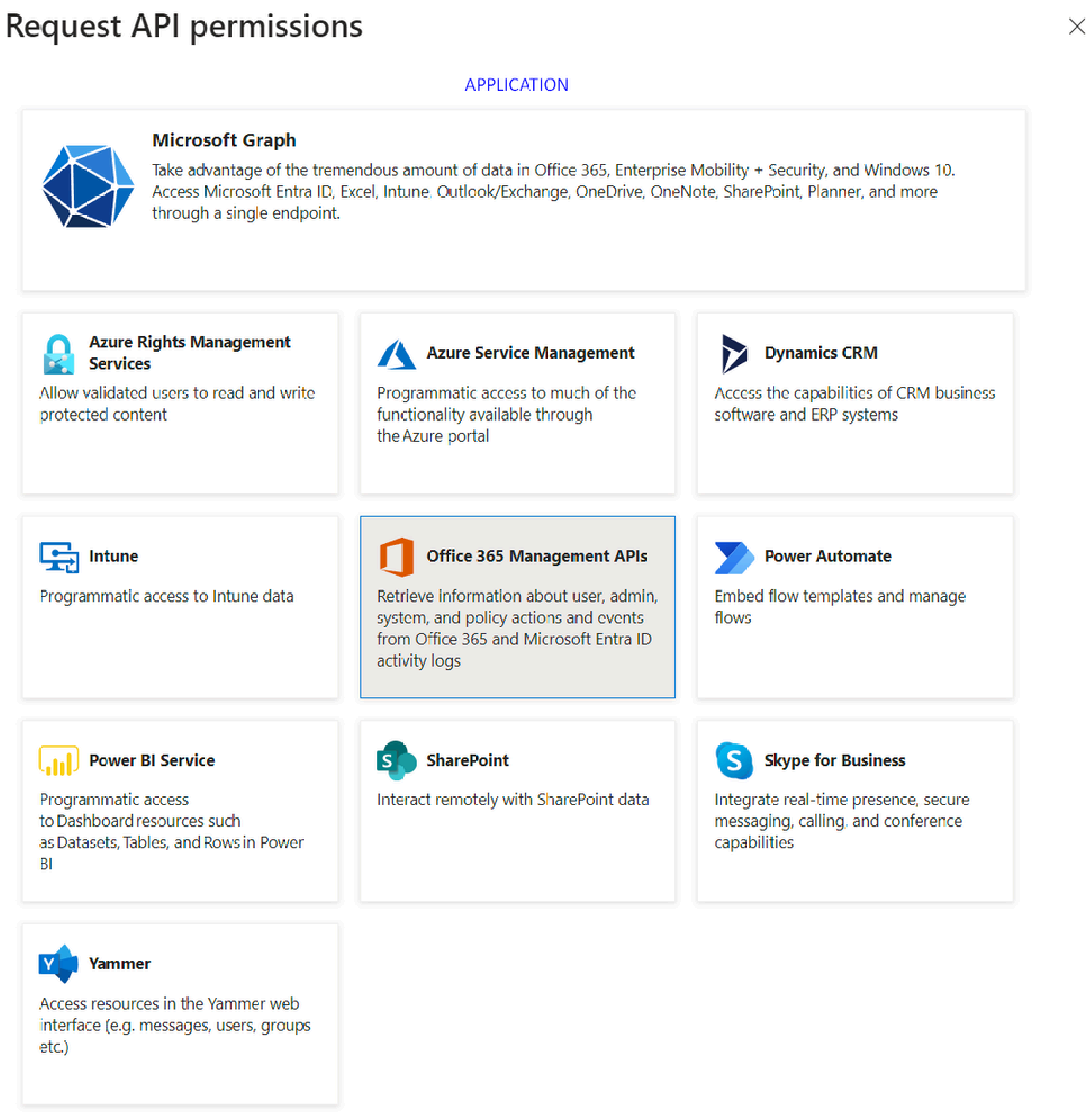
API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

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

Nota: anziché il **Site.FullControl.All** permesso, scegliete **Sites.FullControl.All**.

- A tale scopo, è necessario scegliere l'autorizzazione in base all'applicazione e digitare:



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

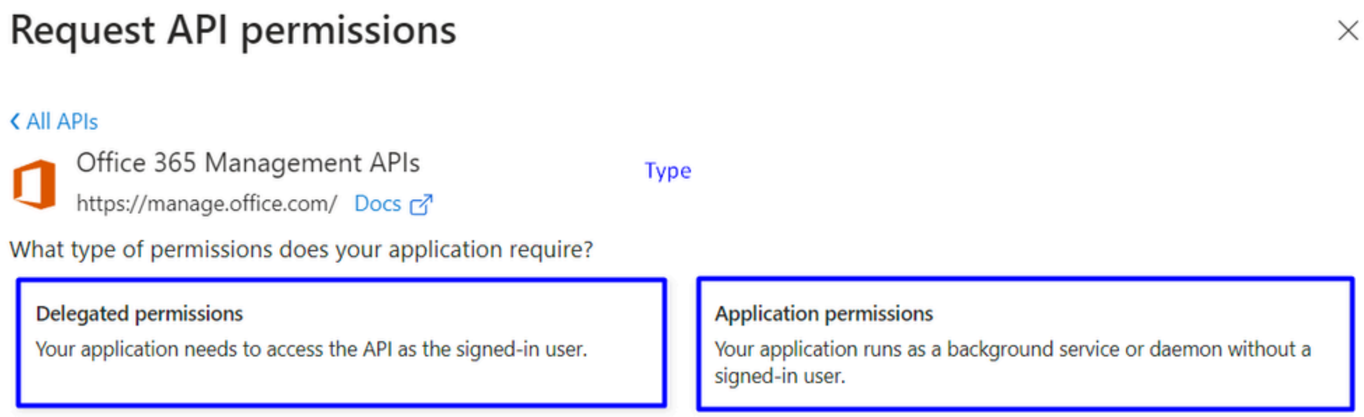
Power Automate
Embed flow templates and manage flows

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

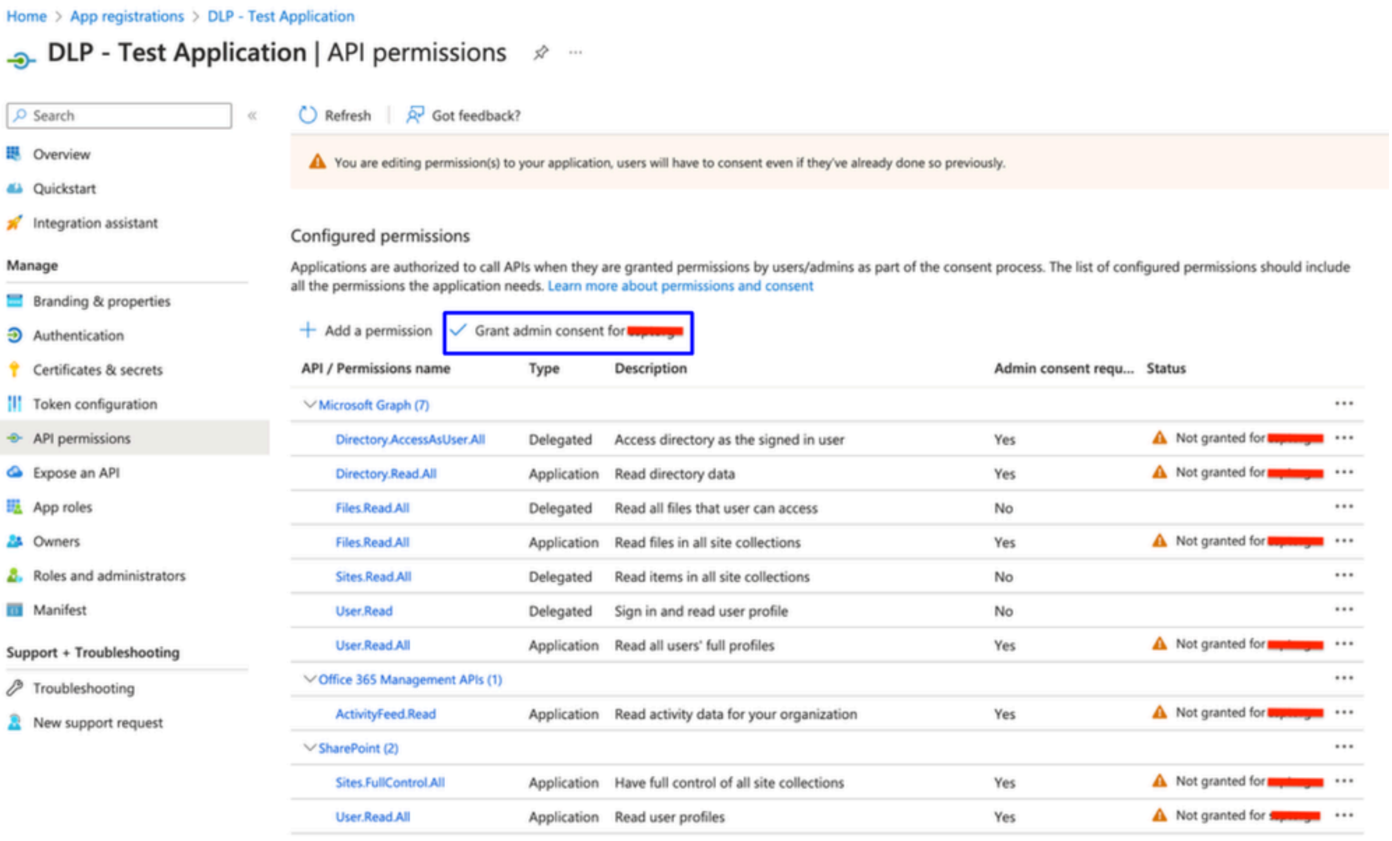
Type

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 volta aggiunte tutte le autorizzazioni richieste, fare clic su **Grant Admin Consent** on per il tenant.



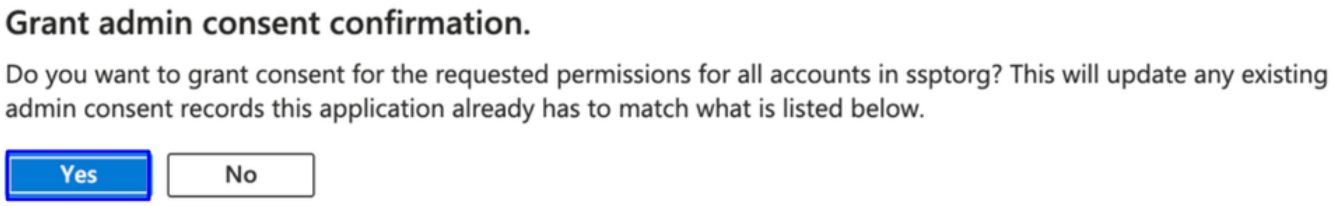
DLP - Test Application | API permissions

⚠ 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

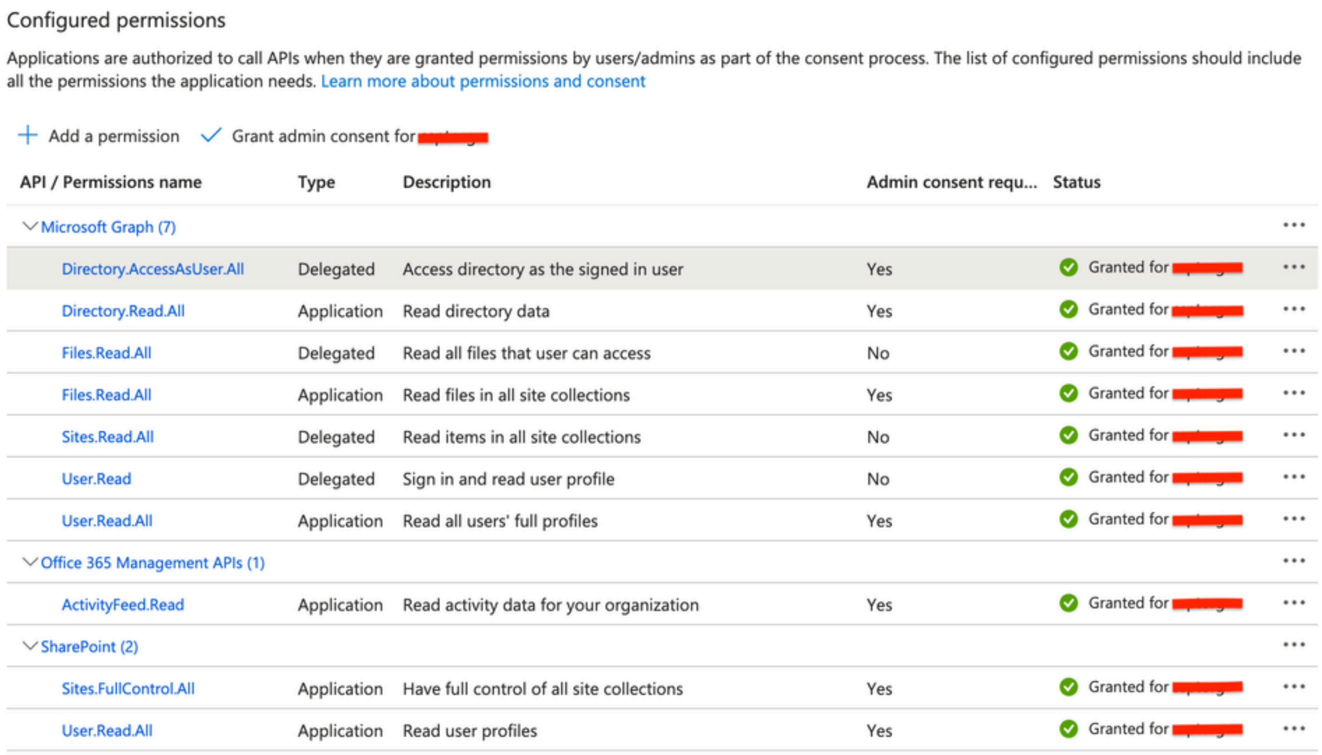
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				···
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	⚠ Not granted for [redacted] ···
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for [redacted] ···
Files.Read.All	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.

- Dopo aver concesso le autorizzazioni, lo stato viene visualizzato come **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]	...

Ora che la configurazione in Azure è stata completata, è possibile continuare la configurazione in Accesso sicuro.

Configurazione in Secure Access

Per abilitare l'integrazione, configurare come segue:

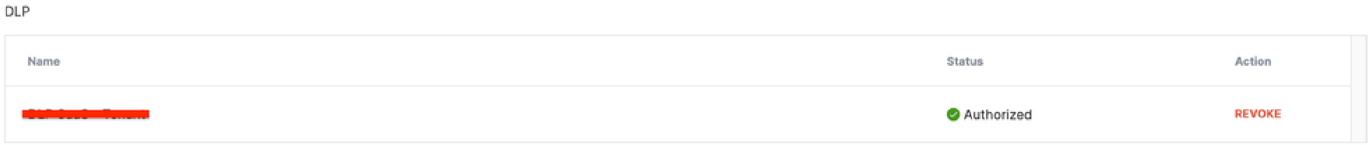
- Passare a Admin > Authentication.
- In **Platforms**, fare clic**Microsoft 365** su.
- Fate clic **Authorize New Tenant** nella DLP sottosezione e aggiungete **Microsoft 365**.
- Nella finestra di **Microsoft 365 Authorization** dialogo, selezionare le caselle di controllo per verificare che siano soddisfatti i prerequisiti, quindi fare clic su **Next**.
- Fornire un nome per il tenant, quindi fare clic su **Next**.
- Fare clic su **Next** per essere reindirizzati alla pagina di accesso a Microsoft 365.
- Accedere a Microsoft 365 con le credenziali di amministratore per concedere l'accesso. Quando si viene reindirizzati a Secure Access, è necessario che venga visualizzato un messaggio che indica che l'integrazione è stata completata correttamente.
- Fare clic **Done** per completare.

Verifica

Per verificare se l'integrazione è riuscita, passare al Dashboard di accesso sicuro:

- Fare clic su **Admin > Authentication > Microsoft 365**

Se la configurazione è corretta, lo stato deve essere **Authorized**impostato su.



DLP

Name	Status	Action
[redacted]	✓ Authorized	REVOKE

Informazioni correlate

- [Abilita protezione da perdita di dati API SaaS per tenant Microsoft 365]()
- [Attivazione o disattivazione del controllo in Microsoft]()