

使用Office 365設定Secure Access以增強資料遺失防護

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[Azure上的配置](#)

[安全訪問中的配置](#)

[驗證](#)

[相關資訊](#)

簡介

本檔案說明Office 365的Data Loss Prevention與Secure Access的整合。

必要條件

- **Office 365 E3 Subscription** 為您的Microsoft租戶提供
 - 開始整合之前，合規性稽核配置如ON在[合規性門戶](#)中

需求

思科建議您瞭解以下主題：

- Cisco Secure Access
- Microsoft Azure企業應用程式與應用程式註冊

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Secure Access
- Microsoft Azure

- Microsoft 365合規性門戶

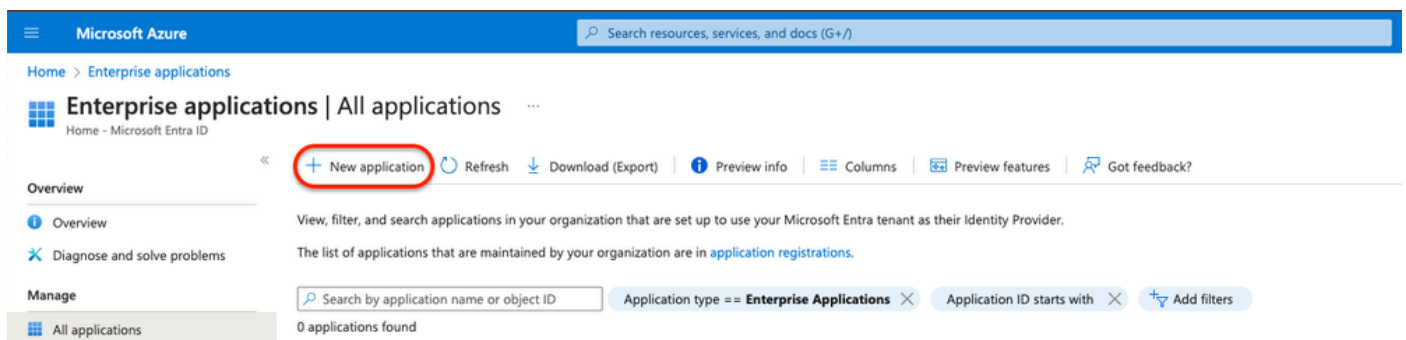
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

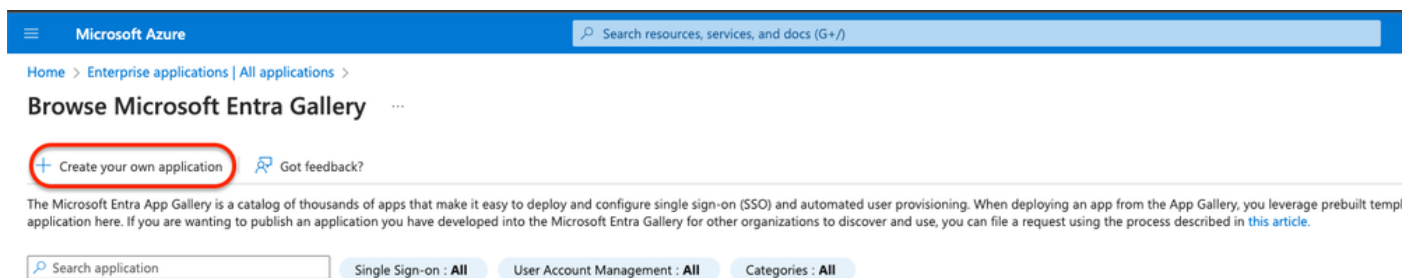
Azure上的配置

要在Azure上啟用應用程式，請按照以下步驟進行配置：

1. 定位至 **Azure Portal > Enterprise Applications > New Application**。




2. 按一下 **Create your own Application**。



3. 輸入您要辨識應用程式的名稱，然後選擇。 **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.

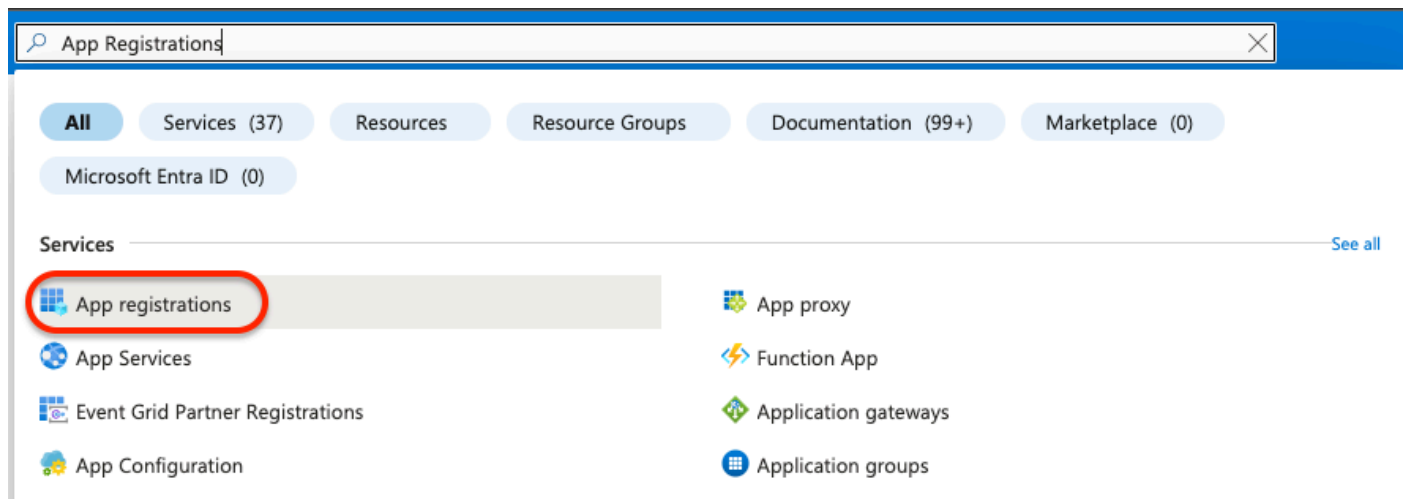
What's the name of your app?

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. 完成後，使用 Azure 搜尋欄查詢 App Registrations。



The screenshot shows the Azure portal search interface. The search bar at the top contains the text 'App Registrations'. Below the search bar, there are several filter tabs: 'All', 'Services (37)', 'Resources', 'Resource Groups', 'Documentation (99+)', and 'Marketplace (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'. A 'See all' link is visible at the end of the Services section.

5. 按一下 **All Applications** 並選擇步驟三建立的應用模組。

Home >

App registrations

+ New registration Endpoints Troubleshooting Refresh Download Preview features | Got feedback?

i 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

Add filters

1 applications found

Display name ↑↓

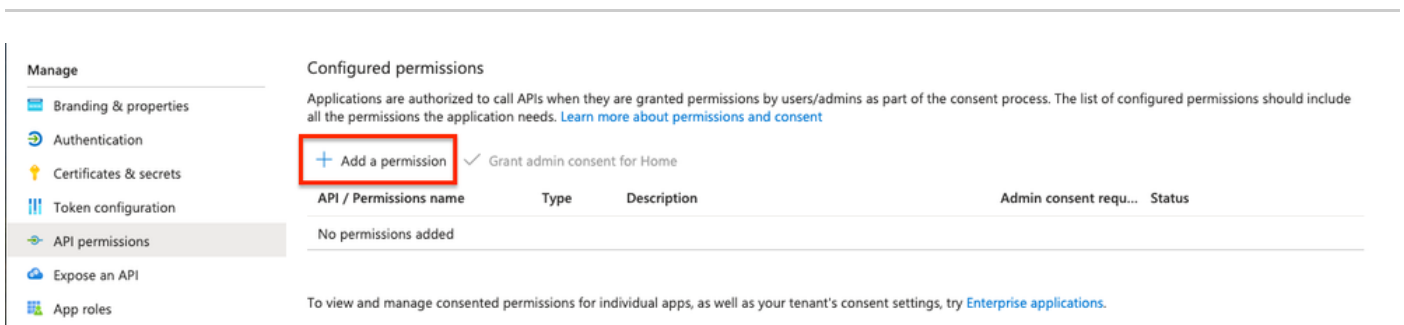
DT DLP Test Application

6. 選擇API Permissions。

The screenshot shows the 'API permissions' page for the 'DLP Test Application'. The left-hand navigation pane has 'API permissions' selected and circled in red. The main content area displays the application's details under the 'Essentials' section. The 'Application (client) ID', 'Object ID', and 'Directory (tenant) ID' fields are redacted with red bars. To the right, there are links for 'Add a certificate or secret', 'Add a Redirect URI', 'Add an Application ID URI', and 'Managed application in L...'. A notice at the bottom of the main area states that starting June 30th, 2020, new features will not be added to ADAL and Azure Active Directory Graph, and that technical support and security updates will be provided for MSAL and Microsoft Graph. The 'Get Started' and 'Documentation' links are visible at the bottom of the main content area.

7. 按一下Add a permission 並根據表格選擇必要的許可權。

注意：為此，必須配置 Microsoft Graph、Office 365 Management APIs和 SharePoint的API。



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














附註：選擇 Sites.FullControl.All 而不是 Site.FullControl.All 許可權。

-
- 為此，您需要根據應用程式和型別選擇許可權：

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

Type

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

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. 增加所有所需許可權後，按一下 **Grant Admin Consent** 打開租戶。

DLP - Test Application | API permissions

Search

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.

- 一旦您授予許可權，狀態會顯示為 **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] ...

現在，Azure上的配置已完成，您可以繼續在Secure Access上進行配置。

安全訪問中的配置

要啟用整合，請按照以下步驟進行配置：

- 導航到Admin > Authentication。
- 在Platforms下，按一下Microsoft 365。
- 在DLP子Authorize New Tenant 段落中按一下並加入Microsoft 365。
- 在Microsoft 365 Authorization 對話方塊中，選中相應的覈取方塊以驗證是否符合前提條件，然後按一下 Next。
- 為您的租戶提供一個名稱，然後按一下Next。
- 按一下Next以重定向到Microsoft 365登入頁。
- 使用管理員憑據登入到Microsoft 365以授予訪問許可權。然後，當您被重定向到Secure Access時，您必須看到一條指示整合成功的消息。
- 點選Done 完成操作。



驗證

要驗證整合是否成功，請導航到[安全訪問控制台](#)：

- 按一下 **Admin > Authentication > Microsoft 365**

如果所有配置都正確，則您的狀態必須為**Authorized**。

DLP

Name	Status	Action
	 Authorized	REVOKE

相關資訊

- [為Microsoft 365租戶啟用SaaS API資料丟失保護](#)
- [在Microsoft中開啟或關閉稽核](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。