

使用Office 365配置安全访问以增强防数据丢失

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[Azure上的配置](#)

[安全访问中的配置](#)

[验证](#)

[相关信息](#)

简介

本文档介绍将Office 365防数据丢失与安全访问相集成。

先决条件

- **Office 365 E3 Subscription** 适用于Microsoft租户
 - 开始集成之前，合规性审计如ON在[合规性门户](#)中配置

要求

Cisco 建议您了解以下主题：

- 思科安全访问
- Microsoft Azure企业应用程序和应用程序注册

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全访问
- Microsoft Azure
- Microsoft 365合规性门户

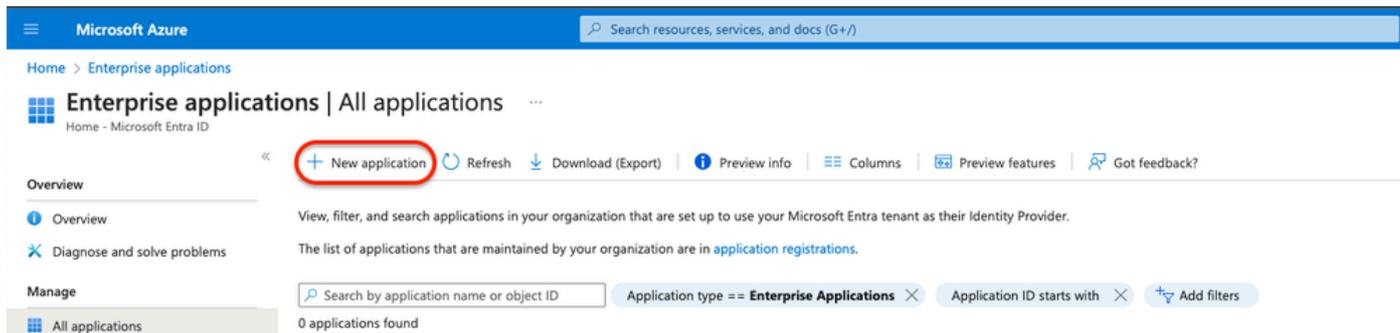
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

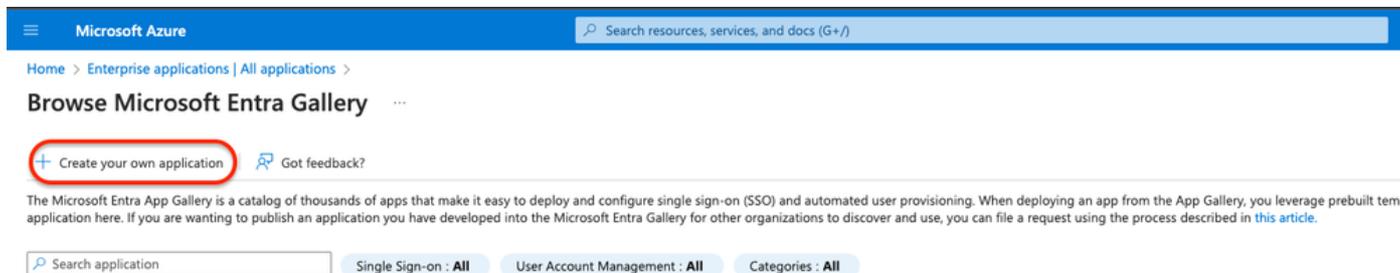
Azure上的配置

要在Azure上启用应用程序，请按照以下步骤进行配置：

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



2. 单击 **Create your own Application。**



3. 提供一个您想要标识应用的名称，并进行选择。 **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.

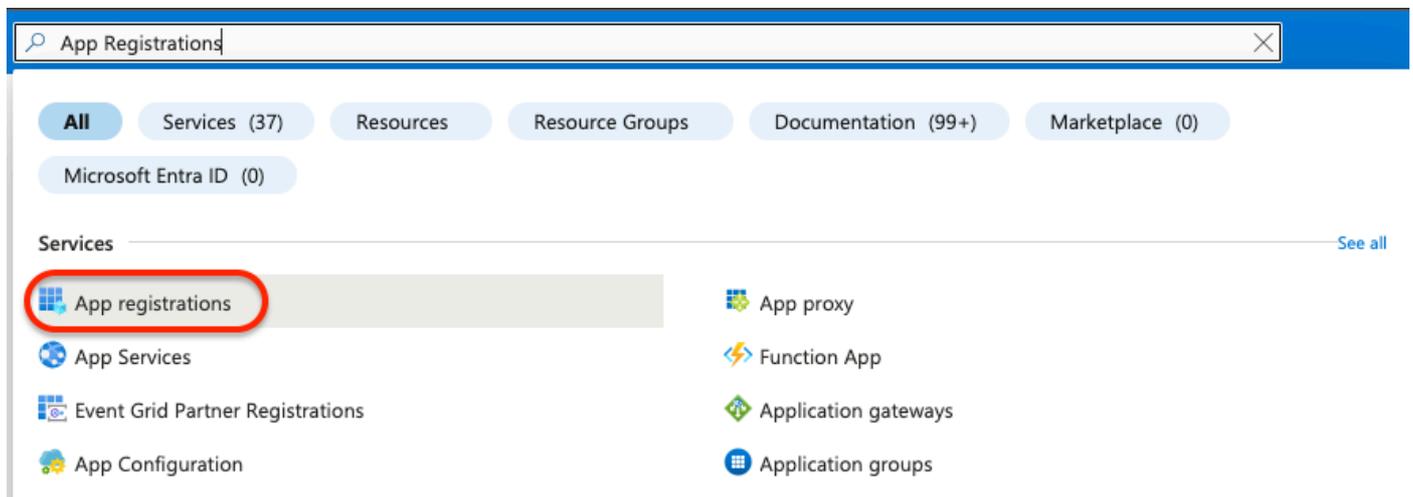
What's the name of your app?

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. 完成后，使用Azure搜索栏查找App Registrations。



The screenshot shows the Azure search interface. At the top, a 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 search results is displayed. The first result, 'App registrations', is highlighted with a red circle. Other results 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. 单击 **All Applications** 并选择三步中创建的应用程序。

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. 选择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 'Display name' is 'DLP Test Application'. The 'Application (client) ID', 'Object ID', and 'Directory (tenant) ID' are all redacted with black bars. The 'Supported account types' are set to 'My organization only'. On the right side, there are links for 'Client credentials', 'Redirect URIs', 'Application ID URI', and 'Managed application in...'. A blue information banner at the top of the main content area provides a notice about the deprecation of ADAL and the Microsoft Graph library, with a 'Learn more' link. At the bottom of the main content area, there are links for 'Get Started' and 'Documentation'.

7. 单击Add a permission 并根据表选择所需的权限。

注意：为此，必须配置 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

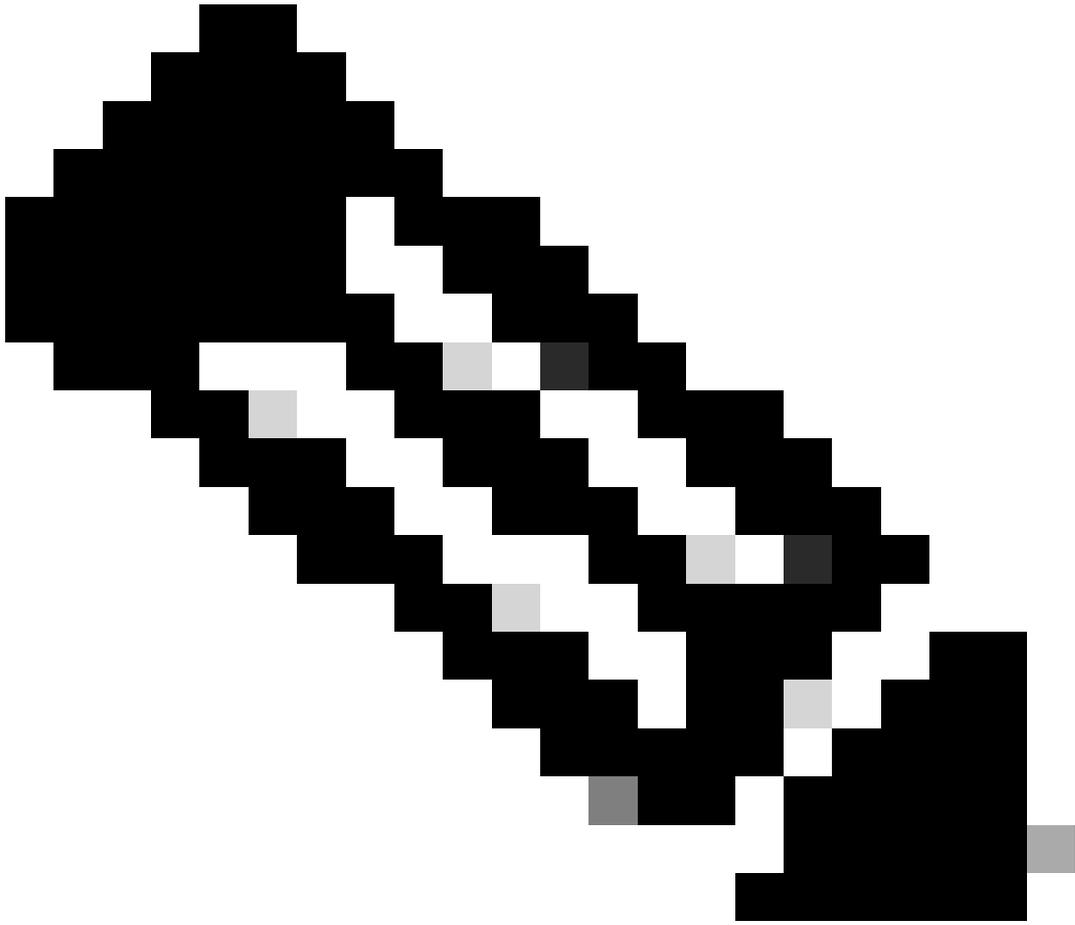
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ 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



注意：选择 `Sites.FullControl.All`而不是`Site.FullControl.All` 权限。

-
- 为此，您需要根据应用程序和类型选择权限：

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. 添加所有所需权限后，单击 **Grant Admin Consent** 打开，进入租户。

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.

- 授予权限后，状态将显示为 **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] ...

现在，Azure上的配置已完成，您可以继续在Secure Access上进行配置。

安全访问中的配置

要启用集成，请按照以下步骤进行配置：

- 导航到Admin > Authentication。
- 在Platforms下，单击Microsoft 365。
- 在DLP子部分中单击Authorize New Tenant 并添加Microsoft 365。
- 在Microsoft 365 Authorization 对话框中，选中复选框以验证是否符合必备条件，然后单击 Next。
- 为您的租户提供一个名称，然后单击Next。
- 单击Next以重定向到Microsoft 365登录页。
- 使用管理员凭据登录到Microsoft 365以授予访问权限。然后，当您被重定向到“安全访问”时，您必须有消息表明您的集成成功。
- 单击Done 完成操作。

验证

要验证集成是否成功，请导航到[安全访问控制面板](#)：

- 点击 **Admin > Authentication > Microsoft 365**

如果一切配置正确，您的状态必须为 **Authorized**。

DLP

Name	Status	Action
	 Authorized	REVOKE

相关信息

- [为Microsoft 365租户启用SaaS API数据丢失保护](#)
- [在Microsoft中打开或关闭审核](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。