

強化されたデータ損失防止のためのOffice 365によるセキュアアクセスの構成

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[Azureの構成](#)

[セキュアアクセスの設定](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、Office 365のデータ損失防止とセキュアアクセスの統合について説明します。

前提条件

- **Office 365 E3 Subscription** Microsoftテナントに存在します
 - コンプライアンス監査は、統合ONを開始する前に[コンプライアンスポータル](#)で設定します

要件

次の項目に関する知識があることが推奨されます。

- シスコセキュアアクセス
- Microsoft Azureエンタープライズアプリケーションとアプリケーションの登録

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- シスコセキュアアクセス

- Microsoft Azure
- Microsoft 365コンプライアンスポータル

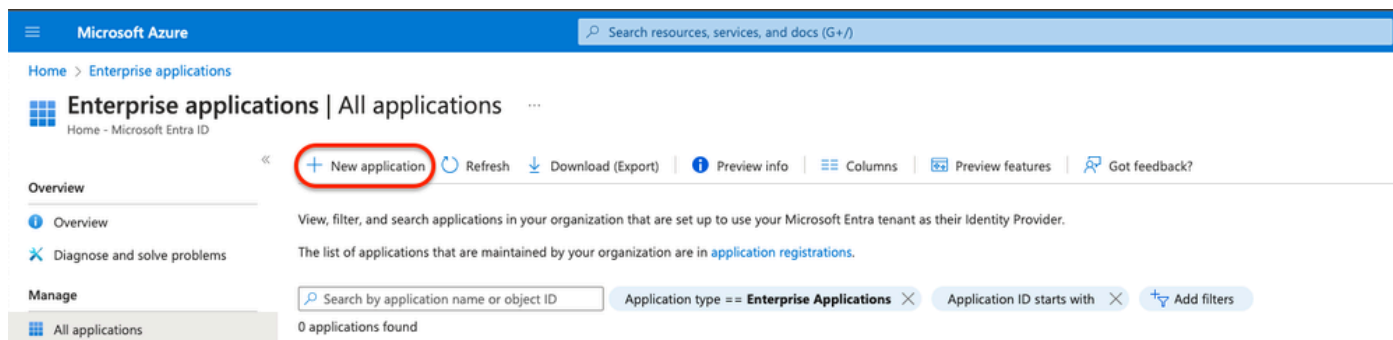
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

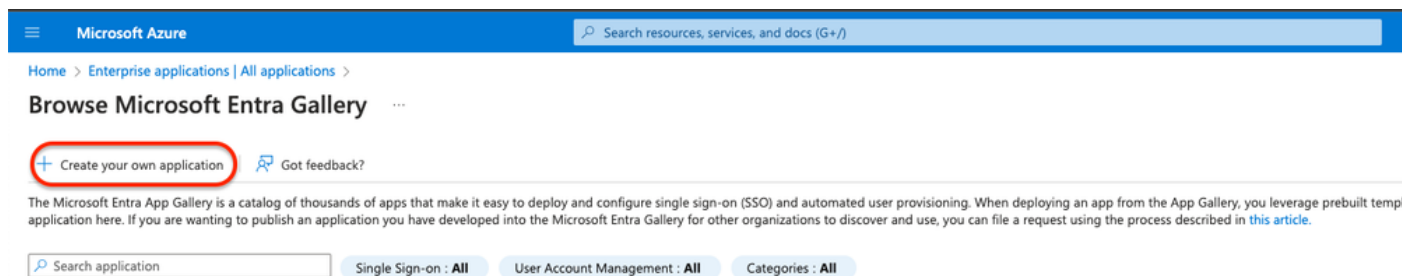
Azureの構成

Azureでアプリケーションを有効にするには、次の手順に従って構成します。

1. **Azure Portal > Enterprise Applications > New Application**に移動します。




2. **Create your own Application**をクリックします。



3. アプリを識別したい名前を付けて選択します。 **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.

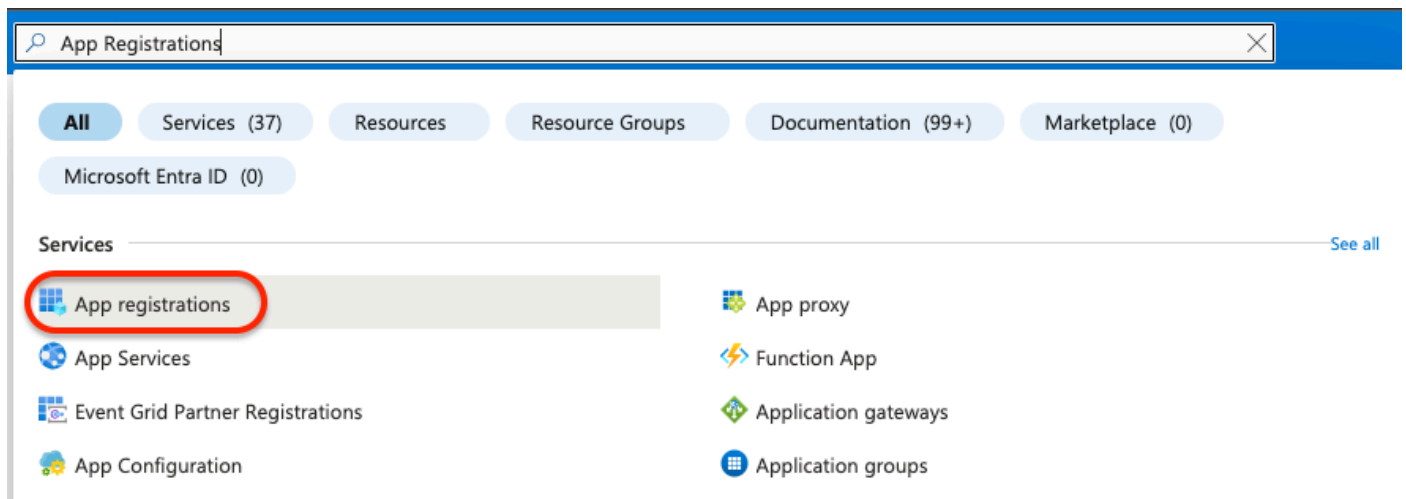
What's the name of your app?

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. 完了したら、Azure Search Barを使用してApp Registrationsを探します。



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. All Applications をクリックし、手順3で作成したアプリケーションを選択します。

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. 「API Permissions」を選択します。

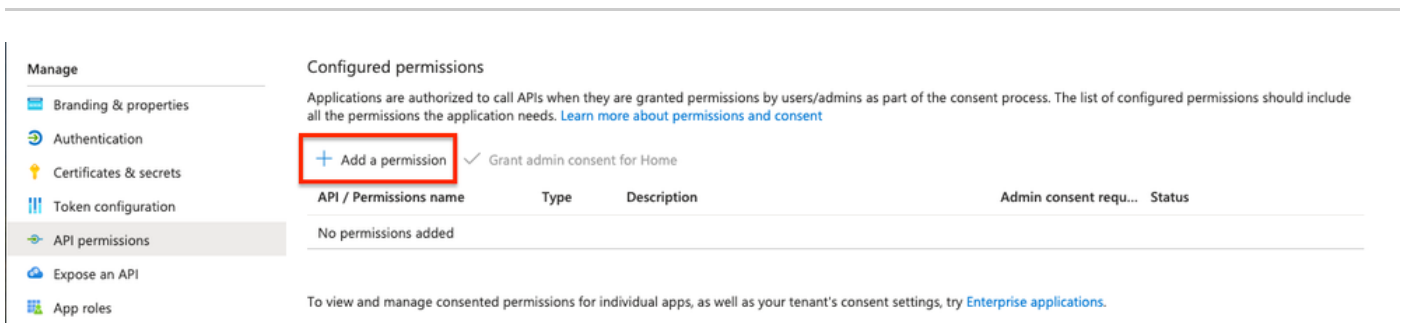
The screenshot shows the Azure portal interface for the 'DLP Test Application'. The left-hand navigation pane is visible, with 'API permissions' selected and circled in red. The main content area displays the 'Essentials' section, which includes a table of application details:

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

Below the table, there is a notice about the upgrade from ADAL to MSAL and a 'Supported account types' section set to 'My organization only'. At the bottom, there are links for 'Get Started' and 'Documentation'.

7. Add a permission をクリックし、表に基づいて必要な権限を選択します。

注：そのためには、Microsoft Graph、Office 365 Management APIs、および SharePointのAPIを設定する必要があります。



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:Site.FullControl.All 権限ではなく、 Sites.FullControl.Allを選択してください。

-
- そのためには、アプリケーションとタイプに基づいて権限を選択する必要があります。

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. 必要な権限をすべて追加したら、テナントの「Grant Admin Consent on」をクリックします。

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.

- 権限を付与すると、ステータスは次のように表示されます **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] ...

Azureの構成が完了したので、Secure Accessで構成を続行できます。

セキュアアクセスの設定

統合を有効にするには、次の手順に従って設定します。

- Admin > Authenticationに移動します。
- [Platforms]で、[Microsoft 365]をクリックします。
DLP
 - サブセクション**Authorize New Tenant** をクリックし、**Microsoft 365**を追加します。
Microsoft 365 Authorization
 - ダイアログで、チェックボックスをオンにして前提条件を満たしていることを確認し、**Next**をクリックします。
 - テナントの名前を入力し、**Next**をクリックします。
Next
 - クリックすると、Microsoft 365のログインページにリダイレクトされます。
 - 管理者クレデンシャルを使用してMicrosoft 365にログインし、アクセスを許可します。その後、セキュアアクセスにリダイレクトされたら、統合が成功したことを示すメッセージが表示されます。
- クリックし**Done** で完了します。

確認

統合が正常に完了したことを確認するには、[セキュアアクセスダッシュボード](#)に移動します。

- クリック **Admin > Authentication > Microsoft 365**

すべてが正しく設定されていれば、ステータスは**Authorized**になります。

DLP

Name	Status	Action
Microsoft 365	● Authorized	REVOKE

関連情報

- [Microsoft 365テナントのSaaS APIデータ損失保護を有効にする](#)
- [Microsoftでの監査のオンまたはオフ](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。