

# 향상된 데이터 손실 방지를 위해 Office 365로 보안 액세스 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[Azure의 구성](#)

[Secure Access의 컨피그레이션](#)

[다음을 확인합니다.](#)

[관련 정보](#)

---

## 소개

이 문서에서는 Office 365용 데이터 손실 방지와 보안 액세스의 통합에 대해 설명합니다.

## 사전 요구 사항

- **Office 365 E3 Subscription** Microsoft 테넌트에 대해 존재합니다.
  - 통합을 시작하기 전 ON에 [규정 준수](#) 감사가 [규정 준수](#) 포털에서처럼 구성됩니다

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 보안 액세스
- Microsoft Azure 엔터프라이즈 응용 프로그램 및 응용 프로그램 등록

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 보안 액세스
- Microsoft Azure

- Microsoft 365 규정 준수 포털

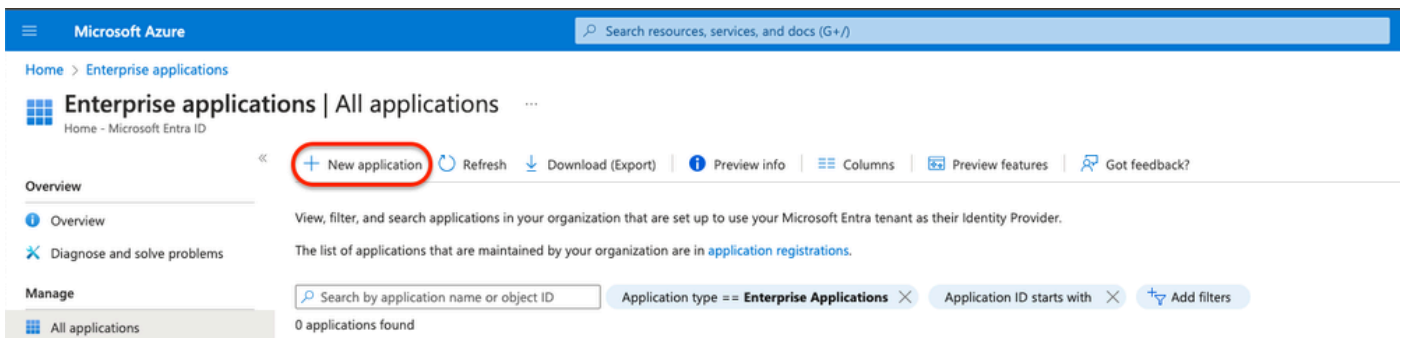
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 구성

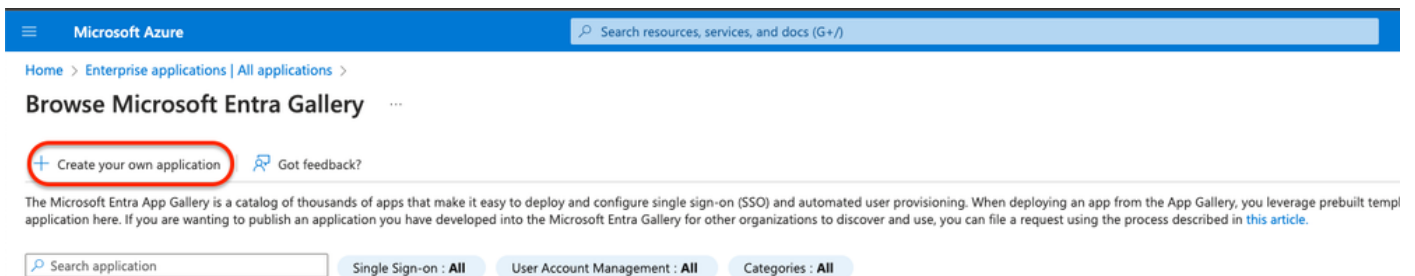
### Azure의 구성

Azure에서 응용 프로그램을 사용하도록 설정하려면 다음 단계에 따라 구성합니다.

1. 로 **Azure Portal > Enterprise Applications > New Application** 이동합니다.




2. 클릭합니다 **Create your own Application**.



3. 앱을 식별하려는 이름을 지정하고 선택합니다. **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.

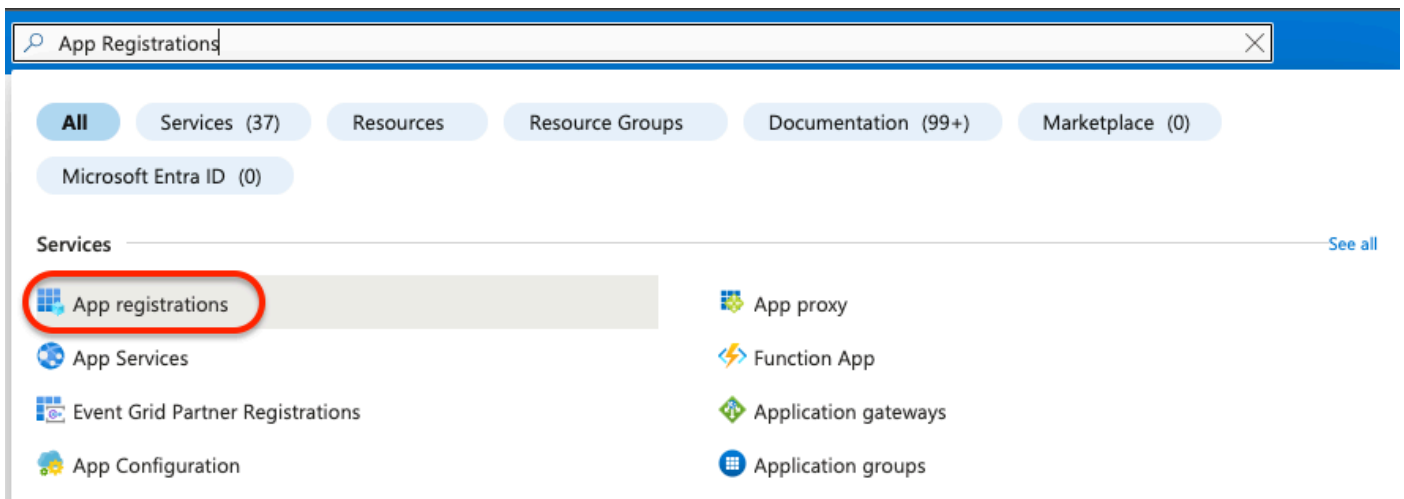
What's the name of your app?

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. 완료되면 Azure Search Bar를 사용하여 검색하십시오App 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 buttons: 'All', 'Services (37)', 'Resources', 'Resource Groups', 'Documentation (99+)', 'Marketplace (0)', and 'Microsoft Entra ID (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. 을 누르고 3 All Applications 단계에서 생성한 애플리케이션을 선택합니다.

# 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. API Permissions 선택합니다.

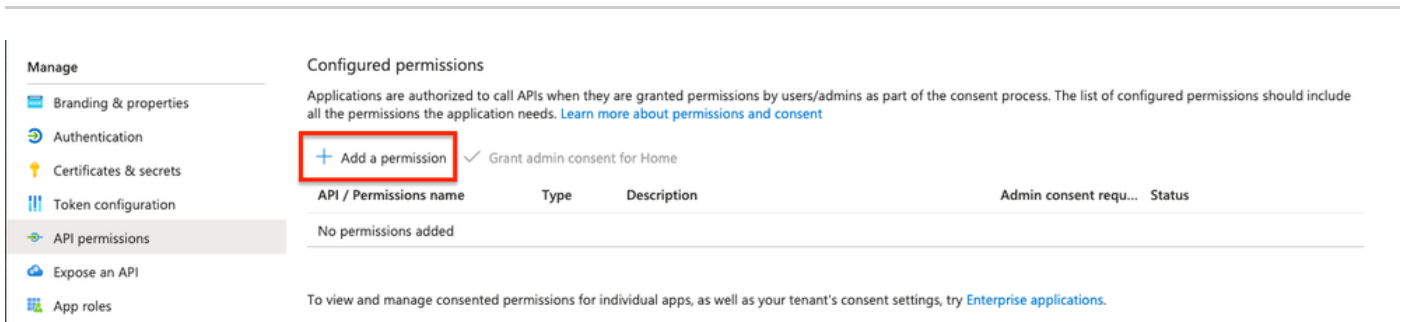
The screenshot shows the Azure portal interface for the 'DLP Test Application'. The left-hand navigation pane is visible, with 'API permissions' selected and circled in red. The main content area displays the 'Essentials' section, which includes the following information:

- 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 I...: DLP Test Application

At the bottom of the Essentials section, there is a notification: "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. 아이콘을 Add a permission 클릭하고 표에 따라 필요한 권한을 선택합니다.

참고: 이를 위해, 및 의 Microsoft GraphAPIOffice 365 Management APIs를 구성해야 SharePoint합니다.



Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles

### Configured permissions

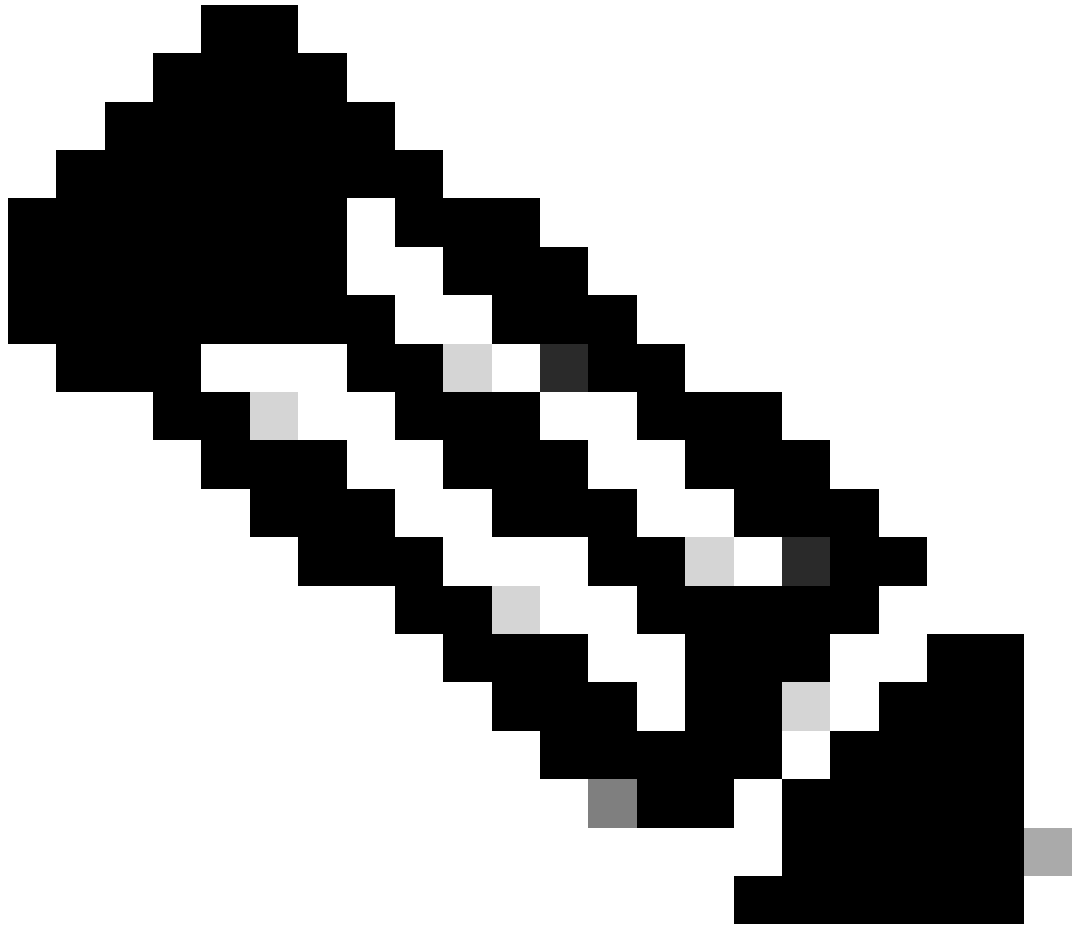
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

**+ 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](#).

<b>API/ Permissions Name</b>	<b>Type</b>	<b>Description</b>	<b>Admin Consent Required</b>
<b>Microsoft Graph</b>			
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
<b>Microsoft 365 Management APIs</b>			
ActivityFeed.Read	Application	Read activity data for the Organization	Yes
<b>SharePoint</b>			
Site.FullControl.All	Application	Full control of all site collections	Yes
User.Read.All	Application	Read user profiles	Yes














참고: 권한 대신 `Site.FullControl.All` 를 `Sites.FullControl.All` 선택합니다.

- 
- 이를 위해 응용 프로그램에 따라 사용 권한을 선택하고 다음을 입력해야 합니다.

# Request API permissions




## APPLICATION

 <b>Microsoft Graph</b> 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.		
 <b>Azure Rights Management Services</b> Allow validated users to read and write protected content	 <b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal	 <b>Dynamics CRM</b> Access the capabilities of CRM business software and ERP systems
 <b>Intune</b> Programmatic access to Intune data	 <b>Office 365 Management APIs</b> Retrieve information about user, admin, system, and policy actions and events from Office 365 and Microsoft Entra ID activity logs	 <b>Power Automate</b> Embed flow templates and manage flows
 <b>Power BI Service</b> Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI	 <b>SharePoint</b> Interact remotely with SharePoint data	 <b>Skype for Business</b> Integrate real-time presence, secure messaging, calling, and conference capabilities
 <b>Yammer</b> 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. 필요한 모든 권한이 추가되면 테넌트에 대해 **Grant Admin Consent On(켜기)**을 클릭합니다.



## 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 <b>ssptorg</b>
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for <b>ssptorg</b>
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 <b>ssptorg</b>
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 <b>ssptorg</b>
Office 365 Management APIs (1)				
ActivityFeed.Read	Application	Read activity data for your organization	Yes	⚠ Not granted for <b>ssptorg</b>
SharePoint (2)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	⚠ Not granted for <b>ssptorg</b>
User.Read.All	Application	Read user profiles	Yes	⚠ Not granted for <b>ssptorg</b>

## 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.

- 권한을 부여하면 상태가 다음과 같이 표시됩니다. **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] ...

이제 Azure에 대한 구성이 완료되었으므로 보안 액세스에 대한 구성을 계속할 수 있습니다.

## Secure Access의 컨피그레이션

통합을 활성화하려면 다음 단계에 따라 구성합니다.

- 로 Admin > Authentication 이동합니다.
- 에서 **Platforms**를 클릭합니다Microsoft 365.
- 하위 섹션**Authorize New Tenant** 을DLP 클릭하고 추가합니다Microsoft 365.
- 대화 상자에서 **Microsoft 365 Authorization** 확인란을 선택하여 필수 구성 요소를 충족하는지 확인한 다음 을 클릭합니다Next.
- 테넌트의 이름을 입력한 다음 을 클릭합니다Next.
- Microsoft 365 로그인 페이지로 리디렉션하려면 클릭하십시오Next.
- 관리자 자격 증명으로 Microsoft 365에 로그인하여 액세스 권한을 부여합니다. 그런 다음 Secure Access로 리디렉션되면 통합이 성공했음을 알리는 메시지가 표시되어야 합니다.
- 을(를) **Done** 클릭하여 완료합니다.

다음을 확인합니다.

통합이 성공했는지 확인하려면 [Secure Access](#) Dashboard로 [이동합니다](#).

- 클릭 Admin > Authentication > Microsoft 365

그리고 모든 것이 올바르게 구성된 경우, 상태는 이어야 합니다 Authorized.

DLP

Name	Status	Action
<b>Microsoft 365</b>	✔ Authorized	REVOKE

#### 관련 정보

- [Microsoft 365 테넌트에 SaaS API 데이터 손실 방지 사용](#)
- [Microsoft에서 감사 설정 또는 해제](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.