

Konfigurieren von sicherem Zugriff mit Office 365 für verbesserten Schutz vor Datenverlust

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfiguration auf Azure](#)

[Konfiguration für sicheren Zugriff](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Integration von Data Loss Prevention für Office 365 mit sicherem Zugriff beschrieben.

Voraussetzungen

- **Office 365 E3 Subscription** ist für Ihren Microsoft-Tenant vorhanden.
 - Compliance-Audits werden wie **ON** im [Compliance-Portal](#) konfiguriert, bevor Sie mit der Integration beginnen.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Zugriff von Cisco
- Microsoft Azure Enterprise-Anwendungen und App-Registrierungen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Sicherer Zugriff von Cisco

- Microsoft Azure
- Microsoft 365 Compliance-Portal

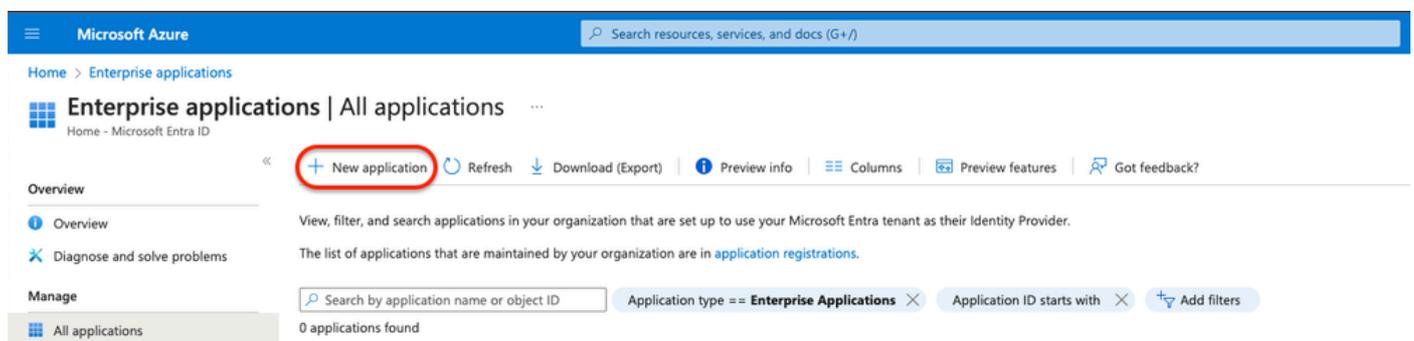
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

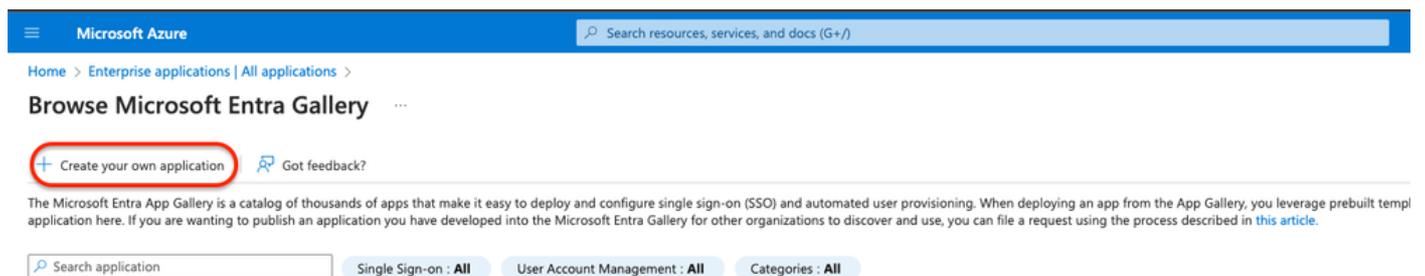
Konfiguration auf Azure

Um die Anwendung auf Azure zu aktivieren, konfigurieren Sie sie wie folgt:

1. Navigieren Sie zum **Azure Portal > Enterprise Applications > New Application**.



2. Klicken Sie auf **Create your own Application**.



3. Geben Sie einen Namen, den Sie wünschen, um die App zu identifizieren und wählen. **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.

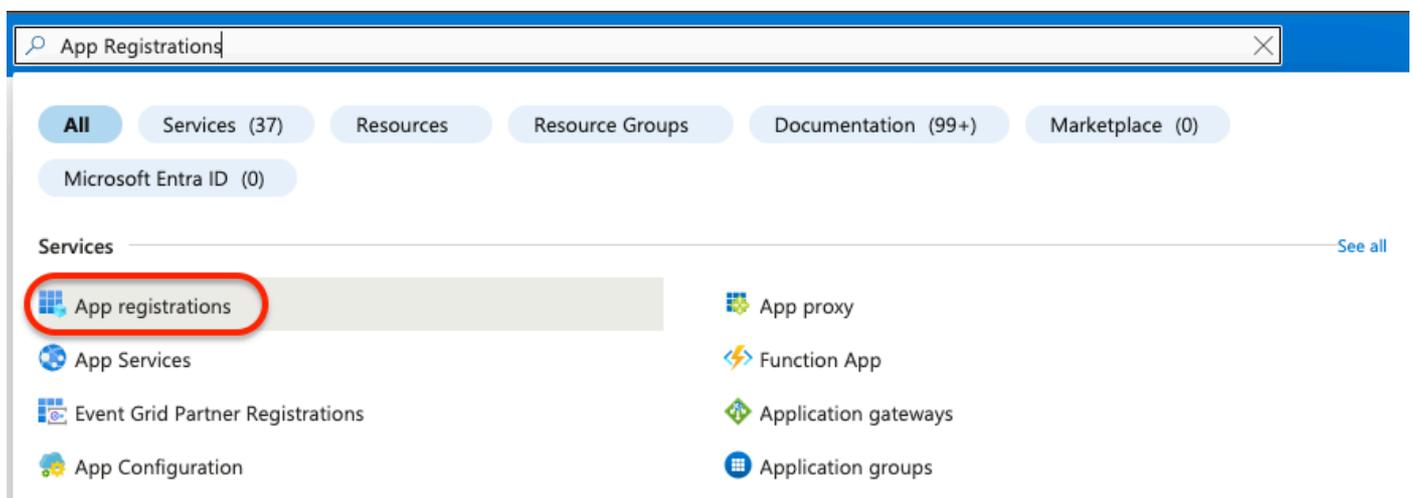
What's the name of your app?

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. Verwenden Sie anschließend die Azure-Suchleiste, um nach zu suchen **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. Klicken Sie auf **All Applications** und wählen Sie die Anwendung erstellt in Schritt [Drei](#).

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. Wählen Sie API Permissions.

Home > App registrations >

DLP Test Application

Delete Endpoints Preview features

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions**
 - Expose an API
 - App roles
 - Owners

i 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](#)

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. 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](#)

Get Started Documentation

7. Klicken Sie auf Add a permission und wählen Sie die erforderlichen Berechtigungen basierend auf der [Tabelle](#).

Hinweis: Hierzu müssen Sie die API von **Microsoft Graph**, **Office 365 Management APIs** und **SharePoint** konfigurieren.

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



Hinweis: Anstelle der **Site.FullControl.All** Berechtigung wählen **Sites.FullControl.All**.

-
- Dazu müssen Sie die Berechtigung basierend auf der Anwendung auswählen und Folgendes eingeben:

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. Nachdem Sie alle erforderlichen Berechtigungen hinzugefügt haben, klicken Sie für **Grant Admin Consent** den Tenant auf .

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.

- Sobald Sie die Berechtigungen erteilt haben, wird der Status angezeigt als **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] ...

Nachdem die Konfiguration auf Azure abgeschlossen ist, können Sie die Konfiguration auf Secure Access fortsetzen.

Konfiguration für sicheren Zugriff

Um die Integration zu aktivieren, konfigurieren Sie sie wie folgt:

- Navigieren Sie zu Admin > Authentication.
- Klicken Sie unter **Platforms** auf **Microsoft 365**.
- Klicken Sie **Authorize New Tenant** in den DLP Unterabschnitt und fügen Sie **Microsoft 365**.
- Aktivieren Sie im **Microsoft 365 Authorization** Dialogfeld die Kontrollkästchen, um zu überprüfen, ob Sie die Voraussetzungen erfüllen, und klicken Sie dann auf **Next**.
- Geben Sie einen Namen für Ihren Tenant ein, und klicken Sie dann auf **Next**.
- Klicken Sie auf **Next**, um zur Microsoft 365-Anmeldeseite weitergeleitet zu werden.
- Melden Sie sich bei Microsoft 365 mit Administratoranmeldeinformationen an, um den Zugriff zu gewähren. Wenn Sie dann zu Secure Access umgeleitet werden, müssen Sie eine Nachricht erhalten, die anzeigt, dass die Integration erfolgreich war.
- Klicken Sie **Done** zum Abschließen.

Überprüfung

Um zu überprüfen, ob die Integration erfolgreich war, navigieren Sie zu Ihrem [Secure Access Dashboard](#):

- Klicken Sie **Admin > Authentication > Microsoft 365**

Und wenn alles richtig konfiguriert ist, muss Ihr Status **Authorized**.

DLP

Name	Status	Action
Microsoft 365	● Authorized	REVOKE

Zugehörige Informationen

- [Schutz vor Datenverlust für SaaS-API für Microsoft 365-Tenants](#)
- [Aktivieren oder Deaktivieren der Überwachung in Microsoft](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.