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

Inhalt

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

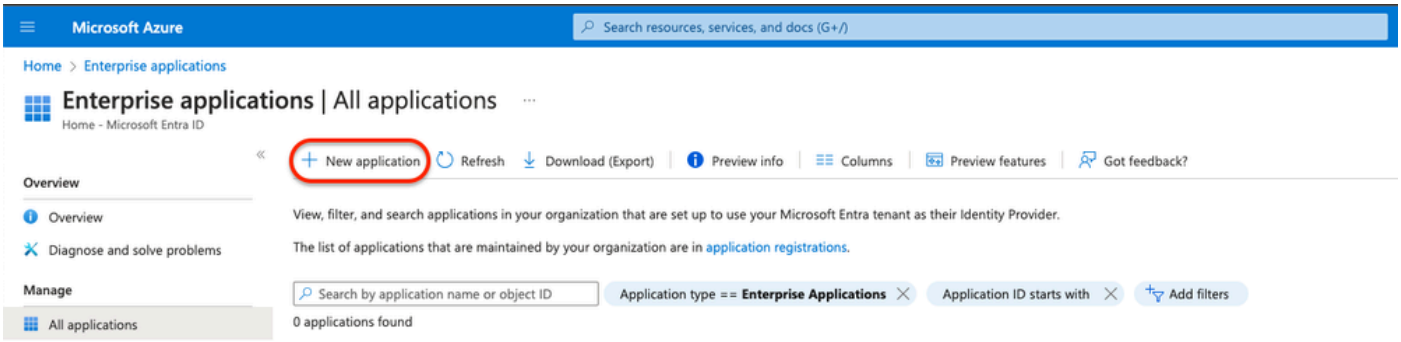
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Konfigurieren

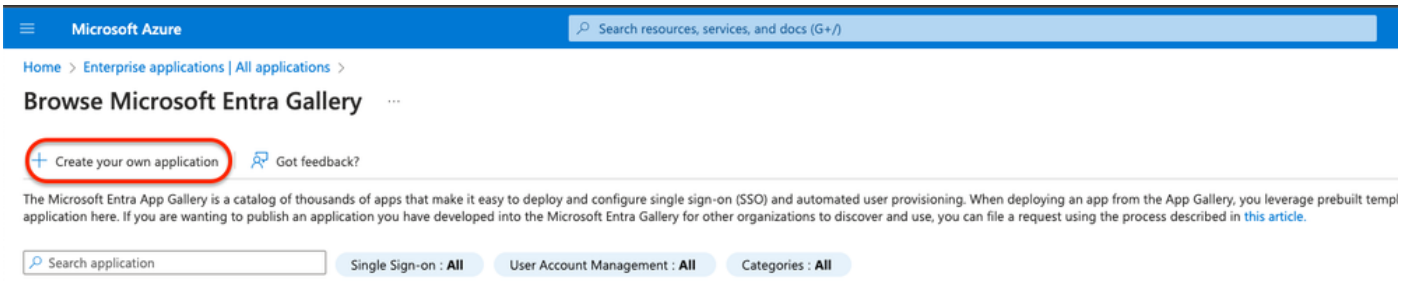
Konfiguration auf Azure

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

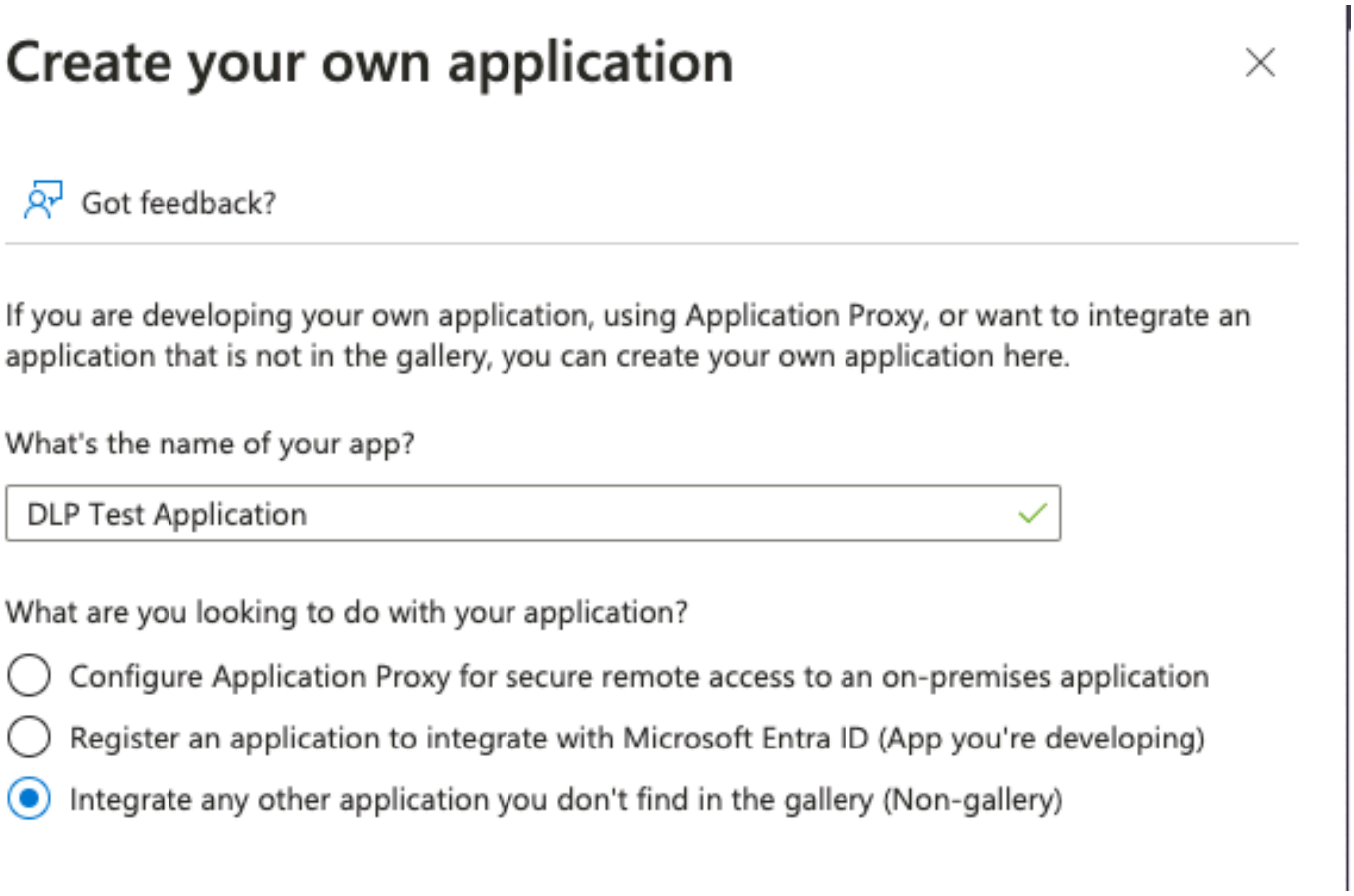
1. Navigieren Sie zum **Azure Portal > Enterprise Applications > New Application**.



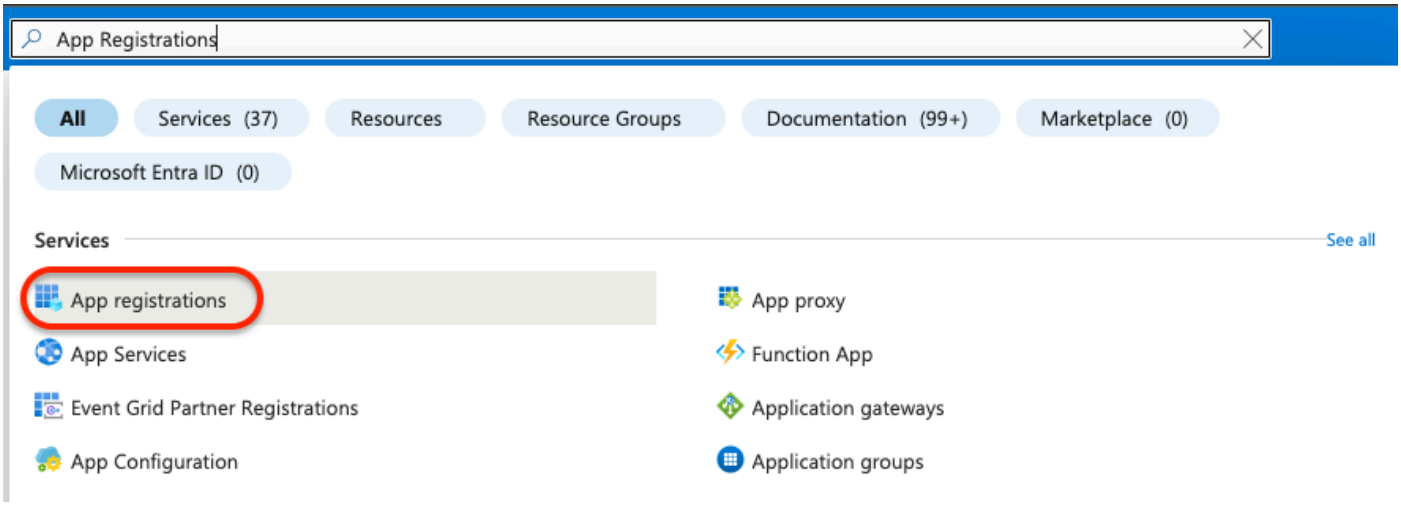
2. Klicken Sie auf **Create your own Application**.



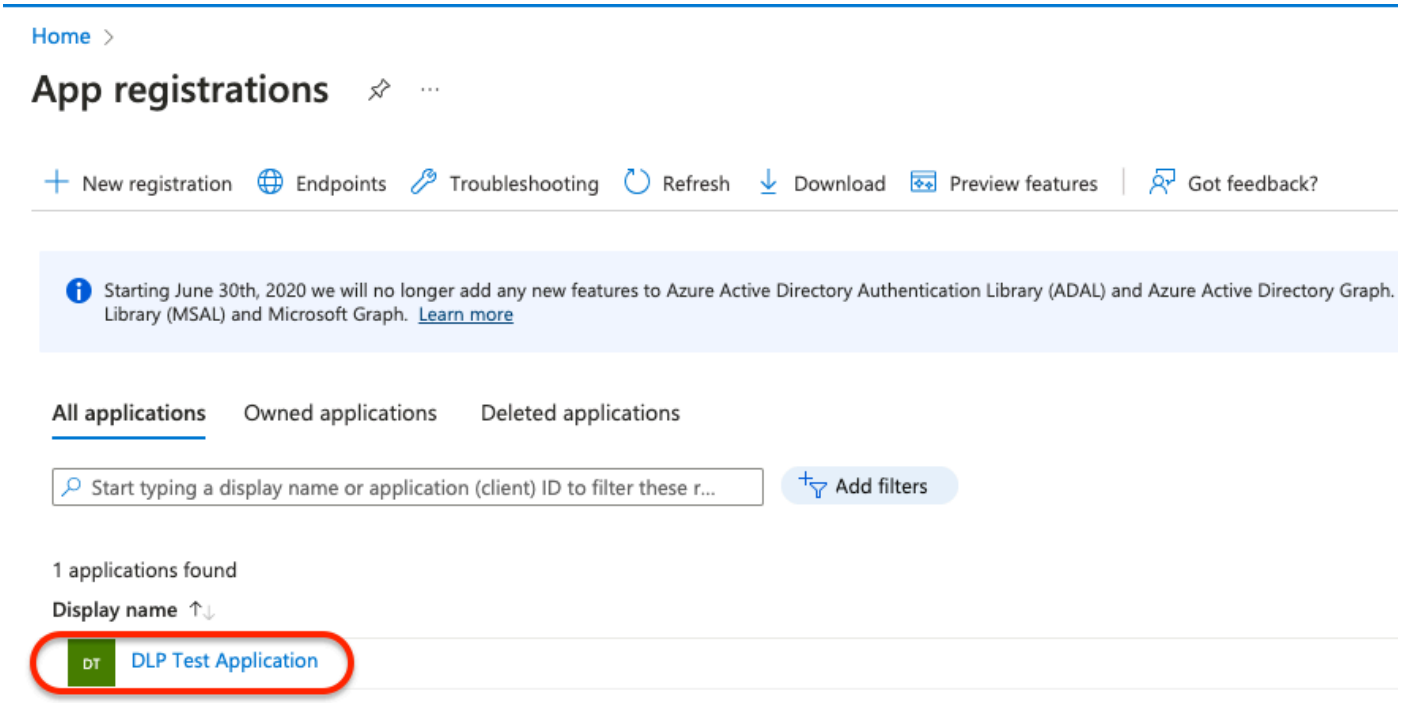
3. Geben Sie einen Namen, den Sie wünschen, um die App zu identifizieren und wählen. **Integrate any other application you don't find in the gallery (Non-Gallery)**.



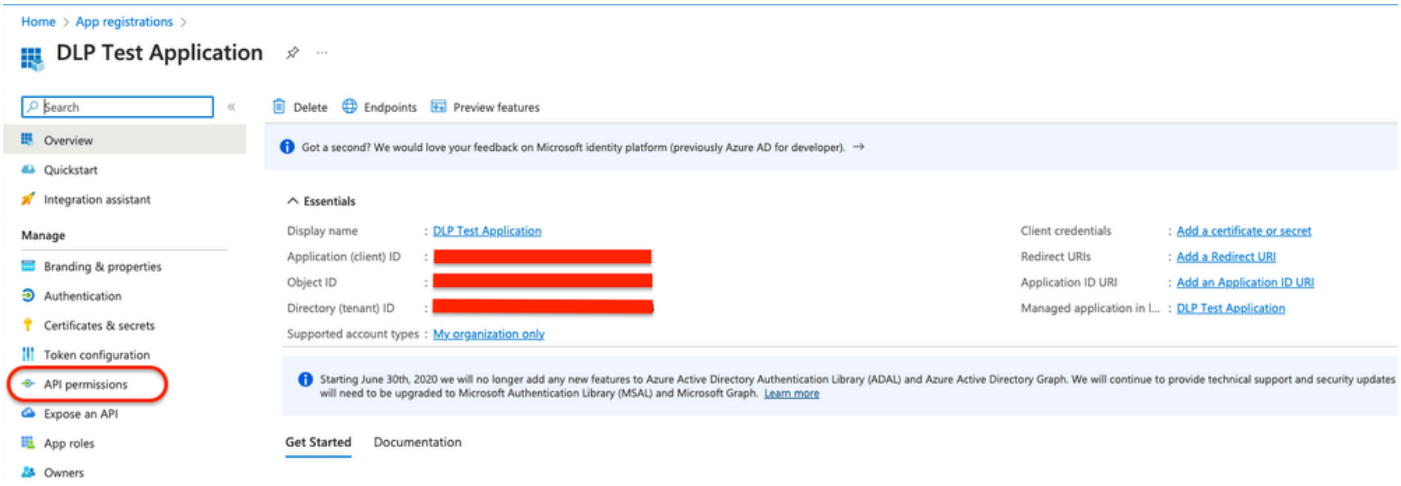
4. Verwenden Sie anschließend die Azure-Suchleiste, um nach zu suchen **App Registrations**.



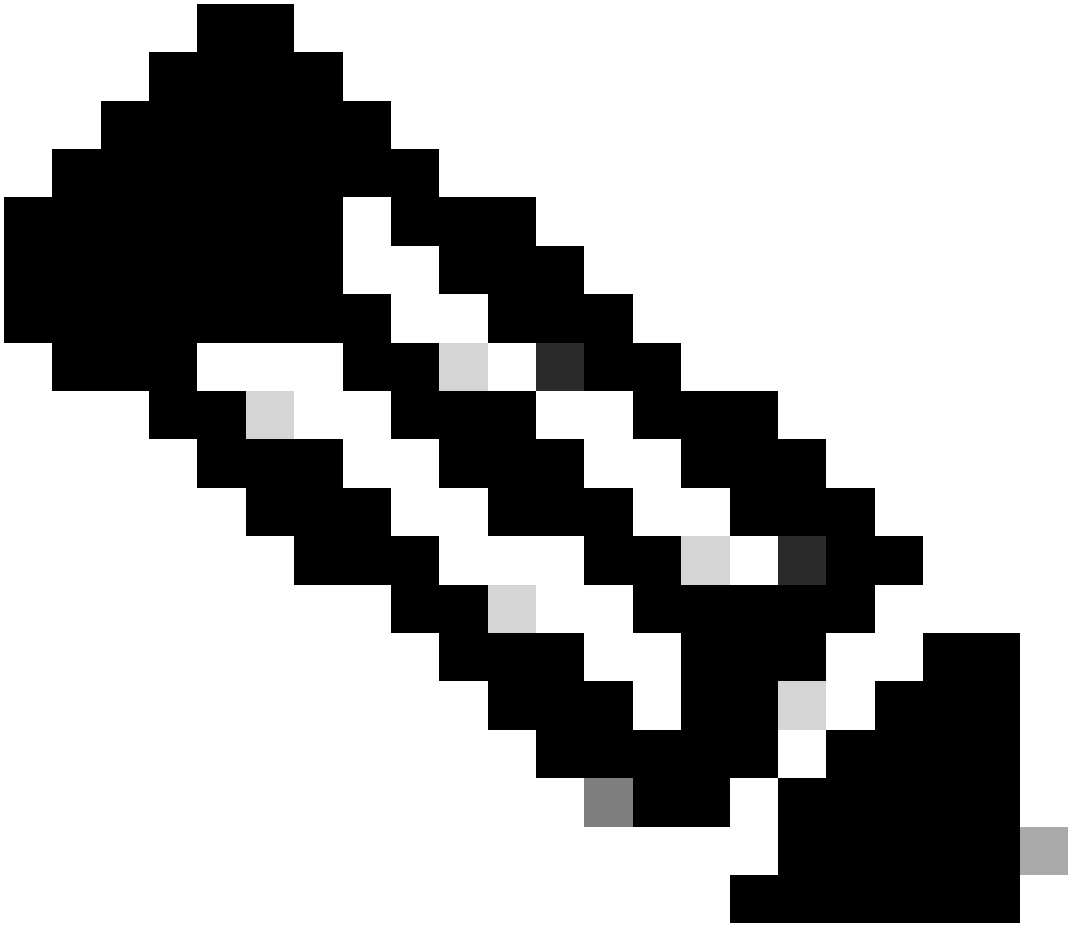
5. Klicken Sie auf **All Applications** und wählen Sie die Anwendung erstellt in Schritt Drei.



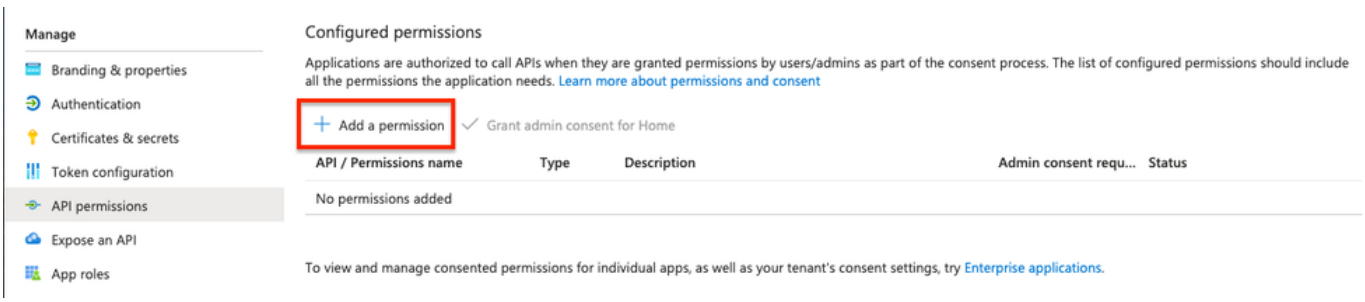
6. Wählen Sie **API Permissions**.



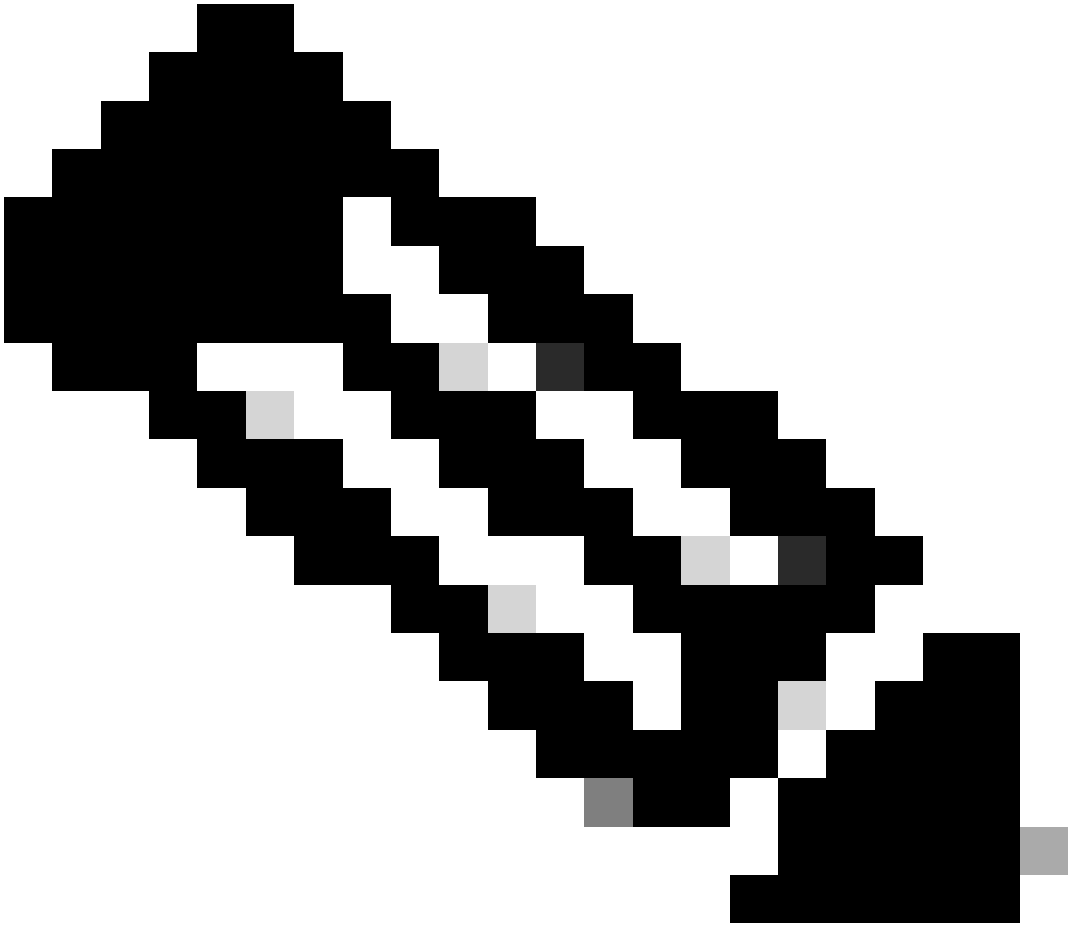
7. Klicken Sie auf **Add a permission** und wählen Sie die erforderlichen Berechtigungen basierend auf der Tabelle.



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

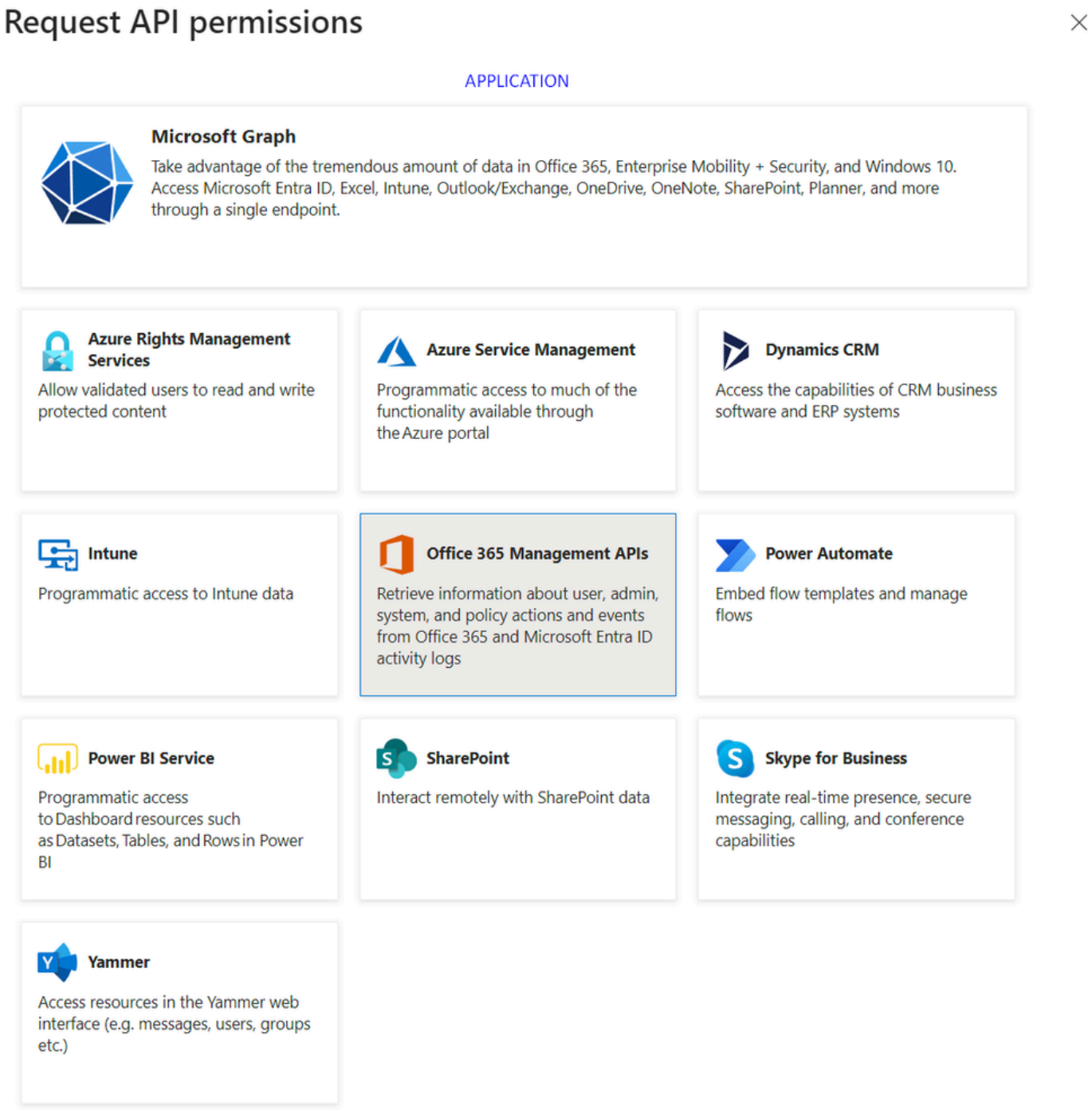


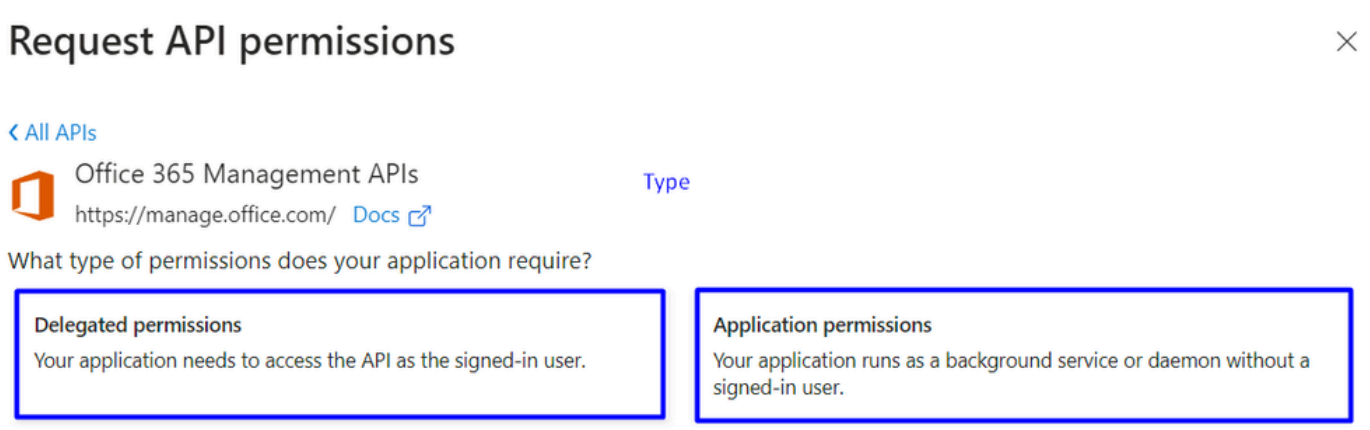
API/ Permissions Name	Type	Description	Admin Consent Required
Microsoft Graph			
Directory.AccessAsUser.All	Delegated	Access directory as the signed-in user	Yes
Directory.Read.All	Application	Read directory data	Yes
Files.Read.All	Delegated	Read all files that user can access	No
Files.Read.All	Application	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



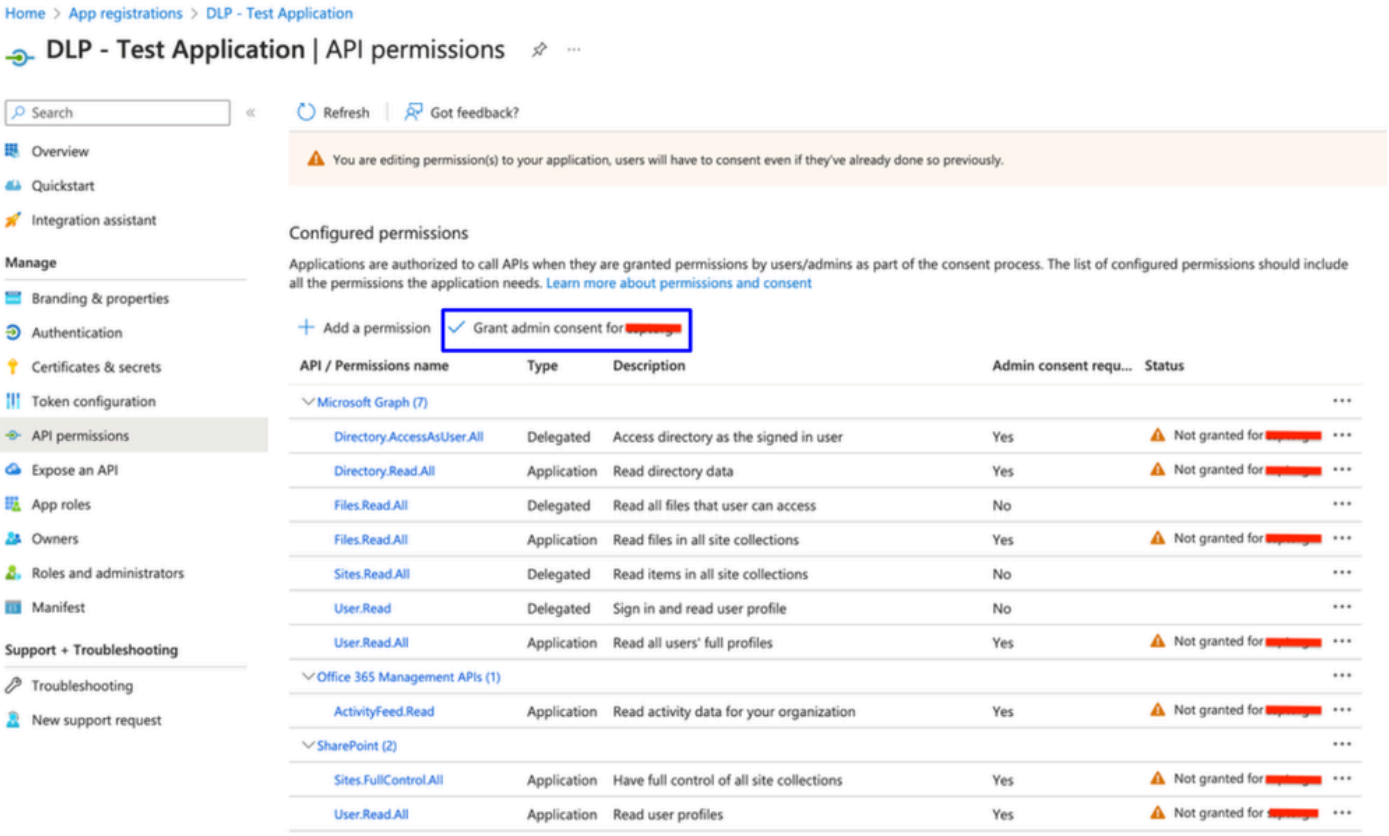
Hinweis: Anstelle der **Site.FullControl.All** Berechtigung wählen **Sites.FullControl.All**.

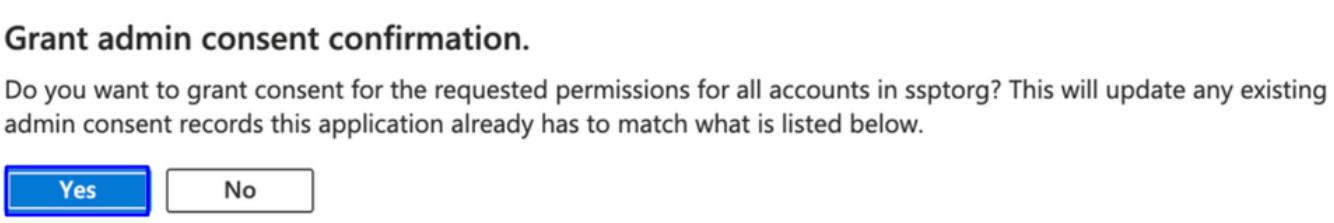
- Dazu müssen Sie die Berechtigung basierend auf der Anwendung auswählen und Folgendes eingeben:



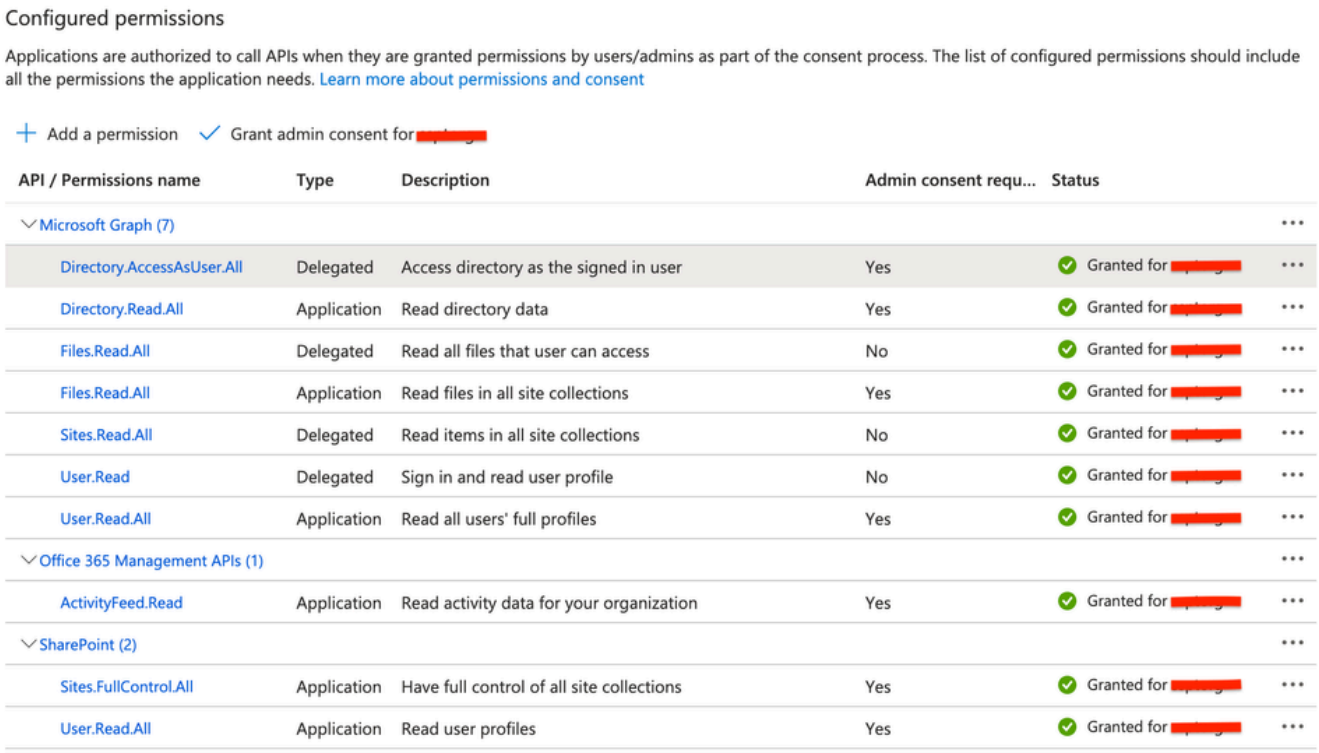


8. Nachdem Sie alle erforderlichen Berechtigungen hinzugefügt haben, klicken Sie für **Grant Admin Consent** den Tenant auf .





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



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**.

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.