

Configure o Acesso Seguro com o Office 365 para Prevenção de Perda de Dados Avançada

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuração no Azure](#)

[Configuração no acesso seguro](#)

[Verificar](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a integração da Prevenção de Perda de Dados para Office 365 com Acesso Seguro.

Pré-requisitos

- **Office 365 E3 Subscription** está presente para seu locatário da Microsoft
 - A auditoria de conformidade é configurada como **ON** no [portal de conformidade](#) antes de você iniciar sua integração

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso seguro da Cisco
- Aplicativos Empresariais e Registros de Aplicativo do Microsoft Azure

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Acesso seguro da Cisco

- Microsoft Azure
- Portal de conformidade Microsoft 365

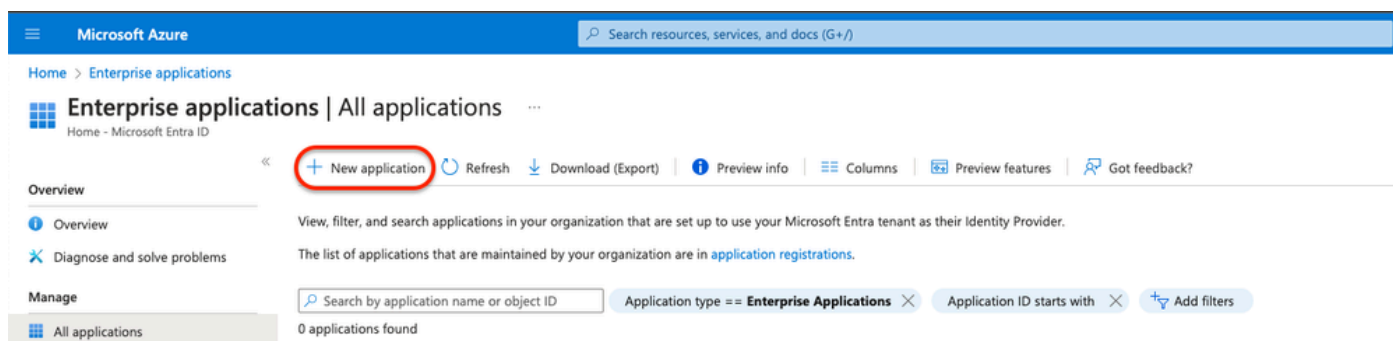
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

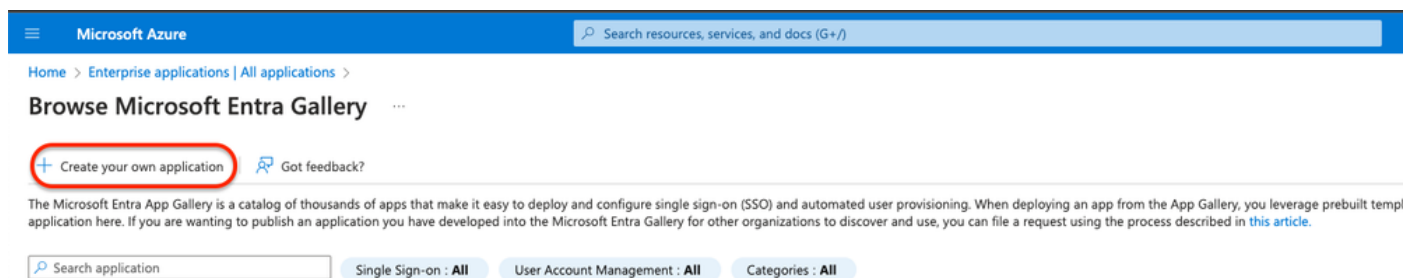
Configuração no Azure

Para habilitar o aplicativo no Azure, configure de acordo com as próximas etapas:

1. Navegue até a **Azure Portal > Enterprise Applications > New Application**.




2. Clique em **Create your own Application**.



3. Dê um nome que você deseja para identificar o aplicativo e escolher. **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.

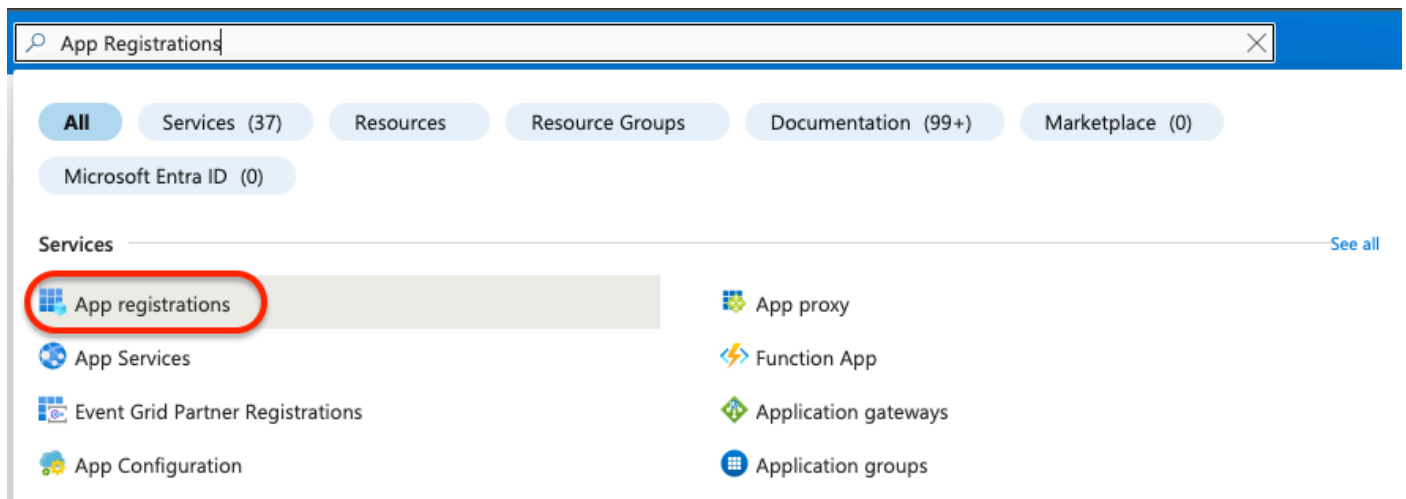
What's the name of your app?

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. Depois de concluído, use a Barra do Azure Search para procurar **App Registrations**.



The screenshot shows the Azure Search bar with the search term "App Registrations". Below the search bar, there are several filter buttons: "All", "Services (37)", "Resources", "Resource Groups", "Documentation (99+)", and "Marketplace (0)". Under the "Services" section, the following items are listed:

- App registrations (highlighted with a red circle)
- App proxy
- App Services
- Function App
- Event Grid Partner Registrations
- Application gateways
- App Configuration
- Application groups

5. Clique em **All Applications** e escolha o aplicativo criado na etapa [Três](#).

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. Escolha API Permissions.

Home > App registrations >

DLP Test Application

🗑️ Delete 🌐 Endpoints 📄 Preview features

🔍 Search

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

📘 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](#)

📘 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. Clique em Add a permission e escolha as permissões necessárias com base na Tabela.

Observação: para isso, você deve configurar a API de **Microsoft Graph**, **Office 365 Management APIs**, e **SharePoint**.

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














Observação: em vez da **Site.FullControl.All** permissão, escolha **Sites.FullControl.All**.

-
- Para isso, você precisa escolher a permissão com base no aplicativo e digitar:

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. Depois que todas as permissões necessárias forem adicionadas, clique **Grant Admin Consent** em para o espaço.

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.

- Depois que você conceder as permissões, o status ficará visível como **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 ██████████

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 ██████████ ...
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for ██████████ ...
Files.Read.All	Delegated	Read all files that user can access	No	✓ Granted for ██████████ ...
Files.Read.All	Application	Read files in all site collections	Yes	✓ Granted for ██████████ ...
Sites.Read.All	Delegated	Read items in all site collections	No	✓ Granted for ██████████ ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for ██████████ ...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for ██████████ ...
▼ Office 365 Management APIs (1) ...				
ActivityFeed.Read	Application	Read activity data for your organization	Yes	✓ Granted for ██████████ ...
▼ SharePoint (2) ...				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	✓ Granted for ██████████ ...
User.Read.All	Application	Read user profiles	Yes	✓ Granted for ██████████ ...

Agora que a configuração no Azure foi concluída, você pode continuar a configuração no Secure Access.

Configuração no acesso seguro

Para habilitar a integração, configure de acordo com as próximas etapas:

- Navegue até Admin > Authentication.
- Em **Platforms**, clique em **Microsoft 365**.
- Clique **Authorize New Tenant** na subseção DLP e adicione **Microsoft 365**.
- Na caixa de **Microsoft 365 Authorization** diálogo, marque as caixas de seleção para verificar se você atende aos pré-requisitos e clique em **Next**.
- Forneça um nome para o locatário e clique em **Next**.
- Clique **Next** para ser redirecionado à página de login do Microsoft 365.
- Faça login no Microsoft 365 com credenciais de administrador para conceder acesso. Em seguida, quando for redirecionado para o Secure Access, você deverá receber uma mensagem indicando que sua integração foi bem-sucedida.
- Clique **Done** para concluir.

Verificar

Para verificar se a integração foi bem-sucedida, navegue até o [Painel de Acesso Seguro](#):

- Clique em **Admin > Authentication > Microsoft 365**

E se tudo estiver configurado corretamente, seu status deverá ser **Authorized**.

DLP

Name	Status	Action
Microsoft 365	● Authorized	REVOKE

Informações Relacionadas

- [Habilitar proteção contra perda de dados de API SaaS para usuários do Microsoft 365](#)
- [Ativando ou desativando a auditoria no Microsoft](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.