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

Contents

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

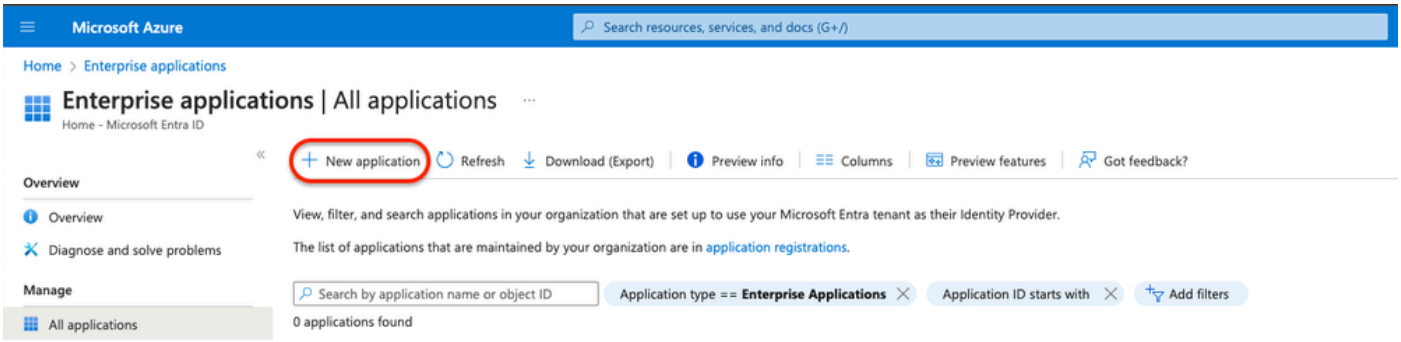
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Configurar

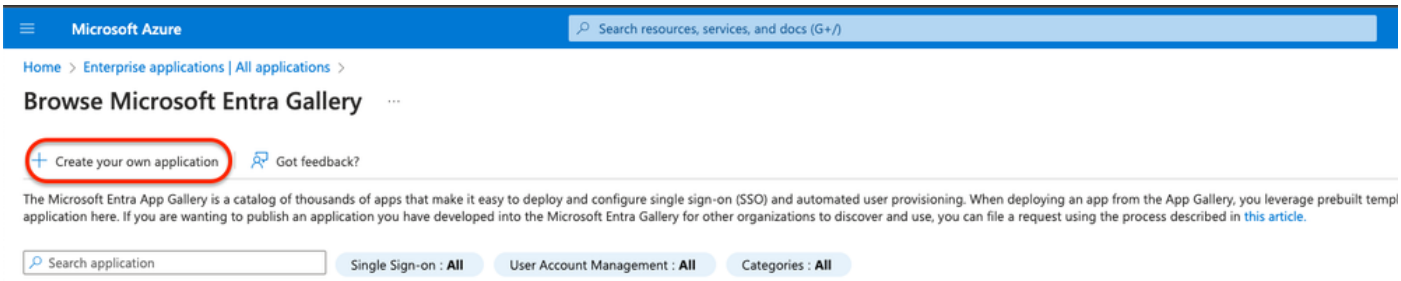
Configuração no Azure

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

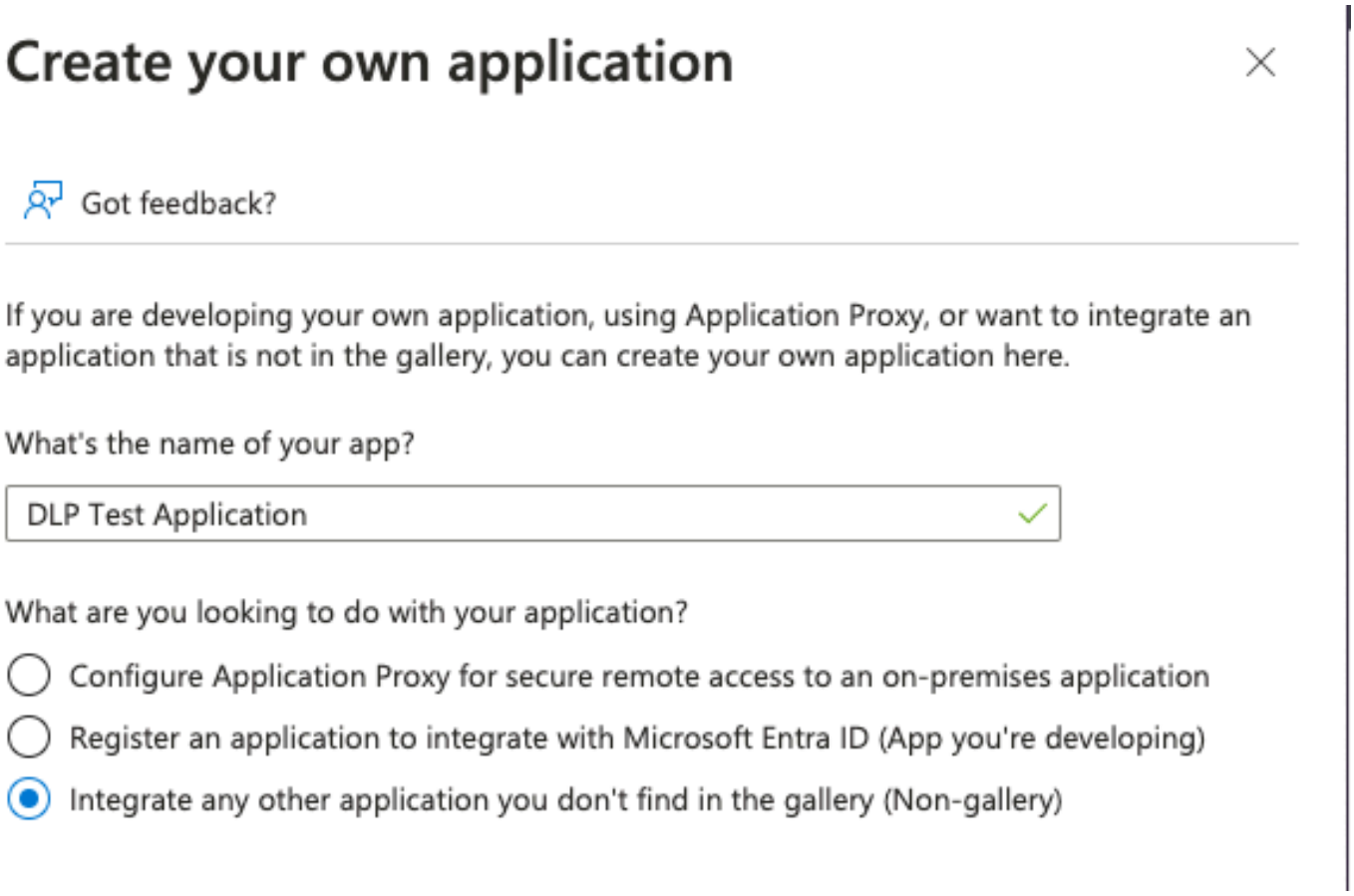
1. Navegue até a **Azure Portal > Enterprise Applications > New Application**.



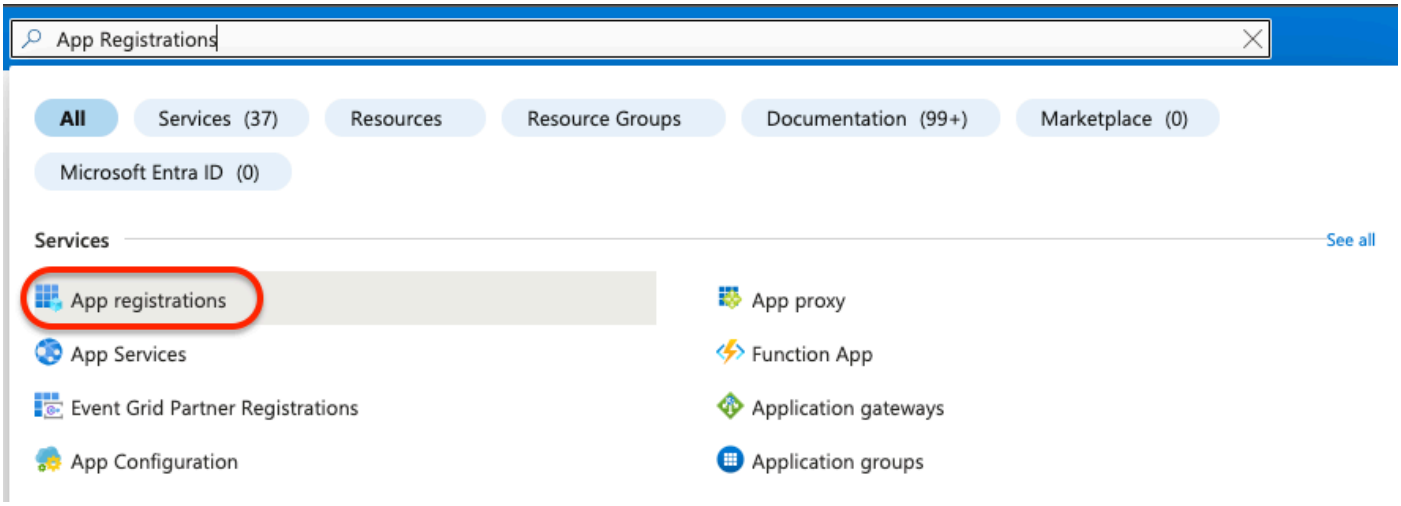
2. Clique em **Create your own Application**.



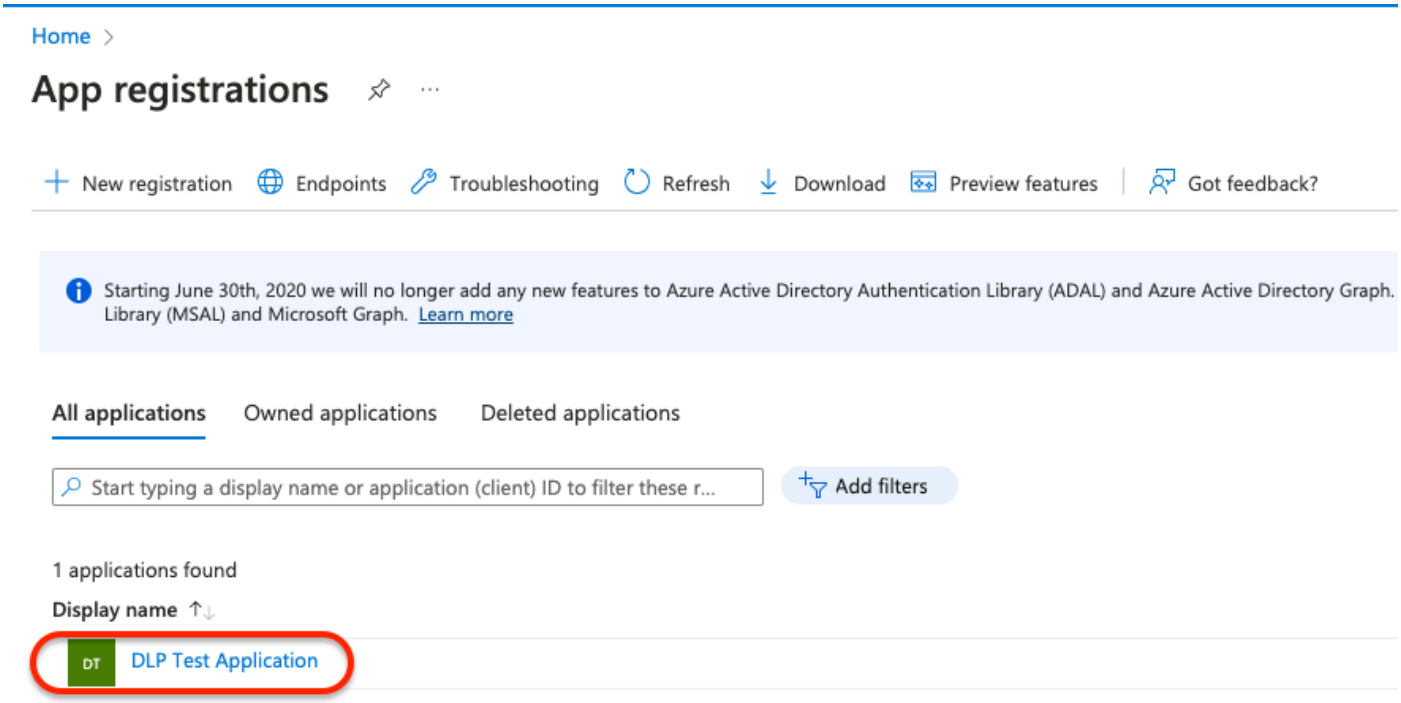
3. Dê um nome que você deseja para identificar o aplicativo e escolher. **Integrate any other application you don't find in the gallery (Non-Gallery)**.



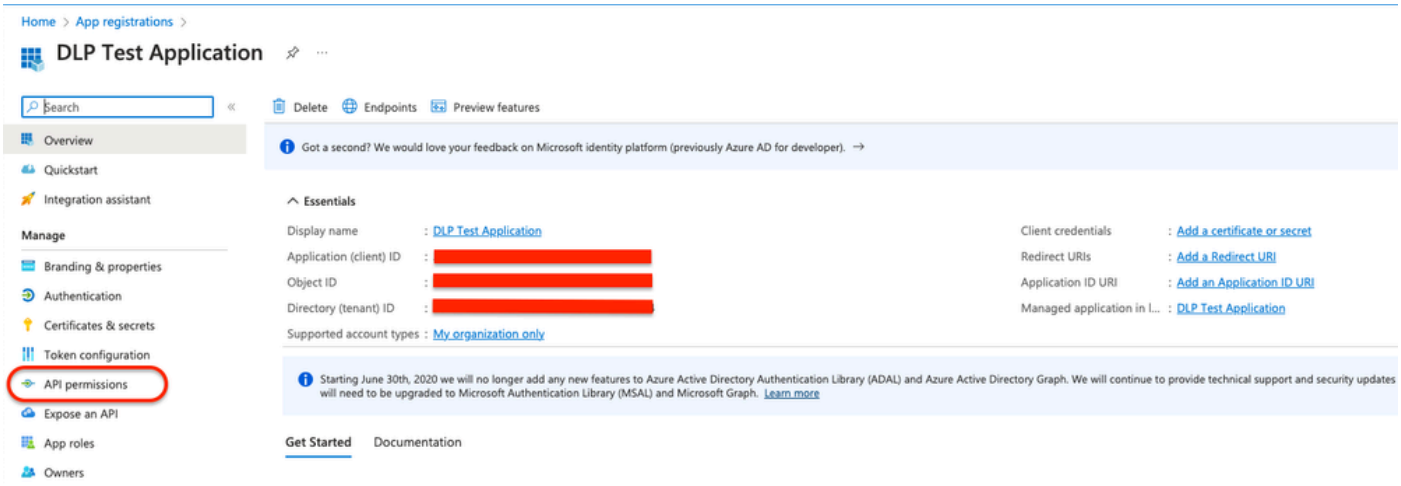
4. Depois de concluído, use a Barra do Azure Search para procurar **App Registrations**.



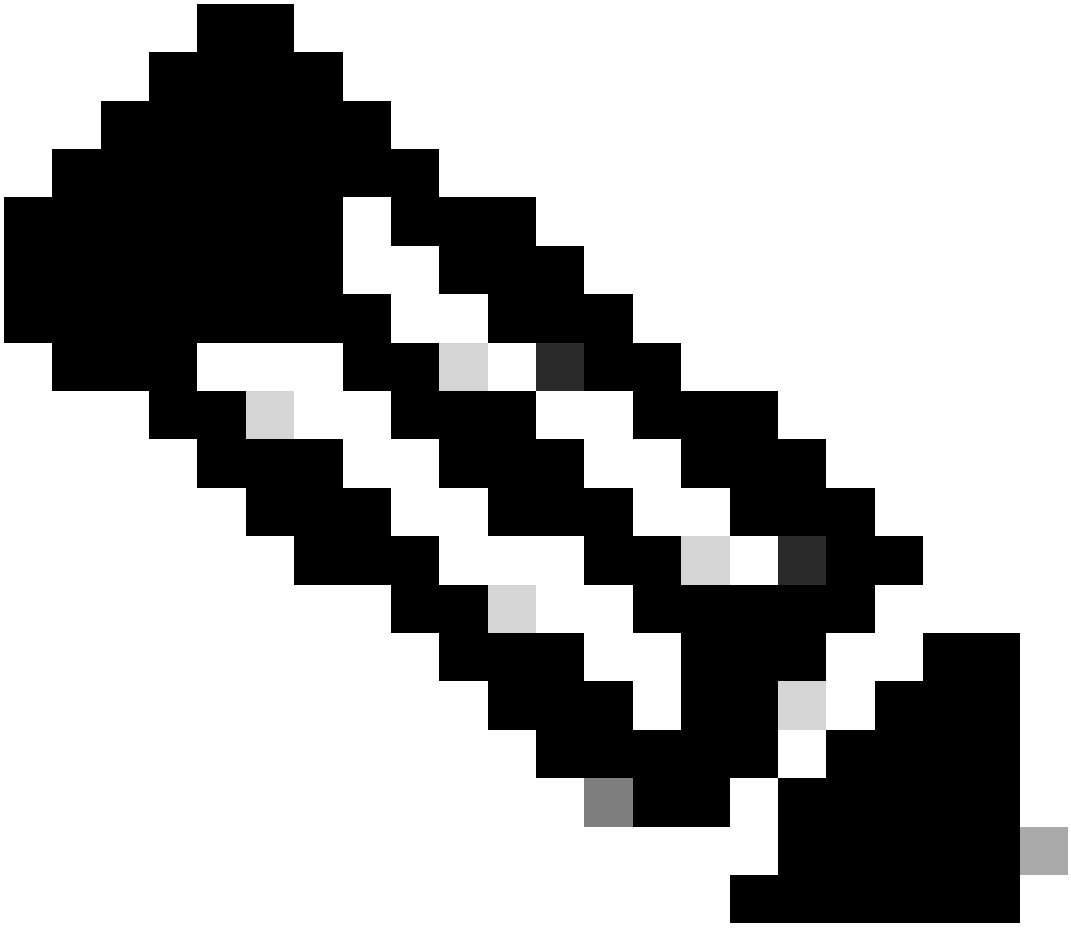
5. Clique em **All Applications** e escolha o aplicativo criado na etapa Três.



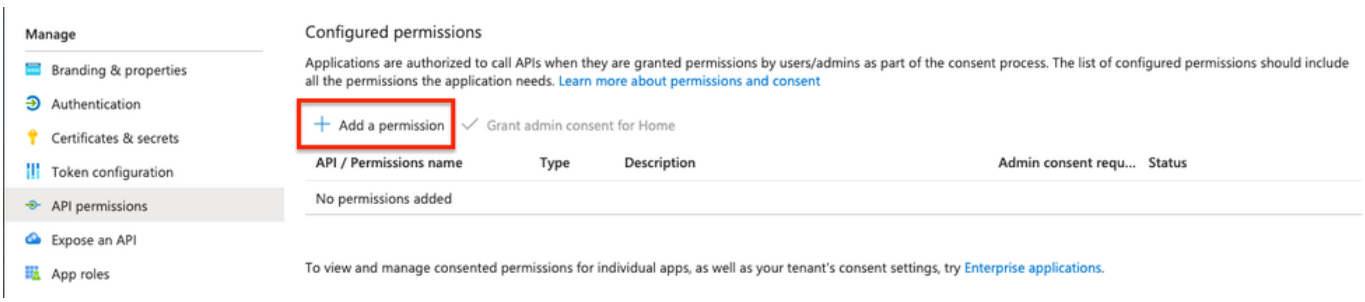
6. Escolha **API Permissions**.



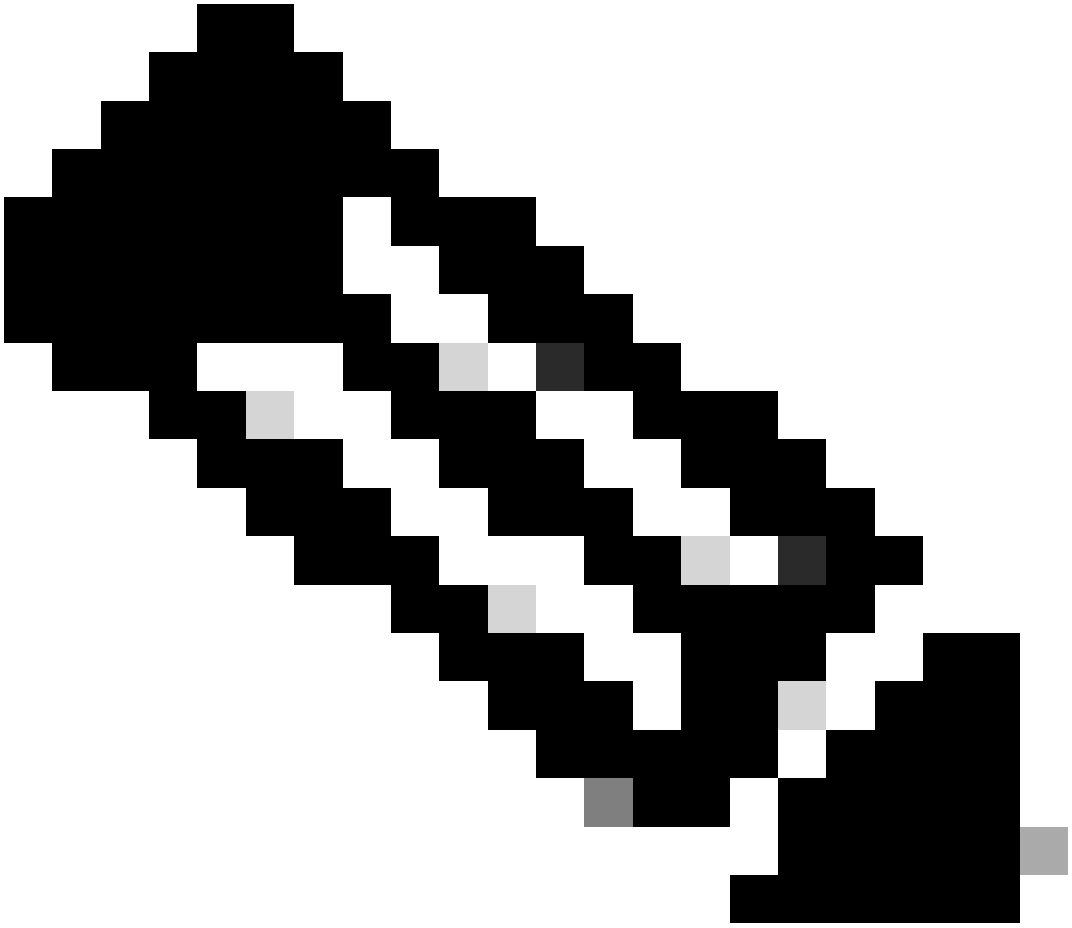
7. Clique em **Add a permission** e escolha as permissões necessárias com base na Tabela.



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

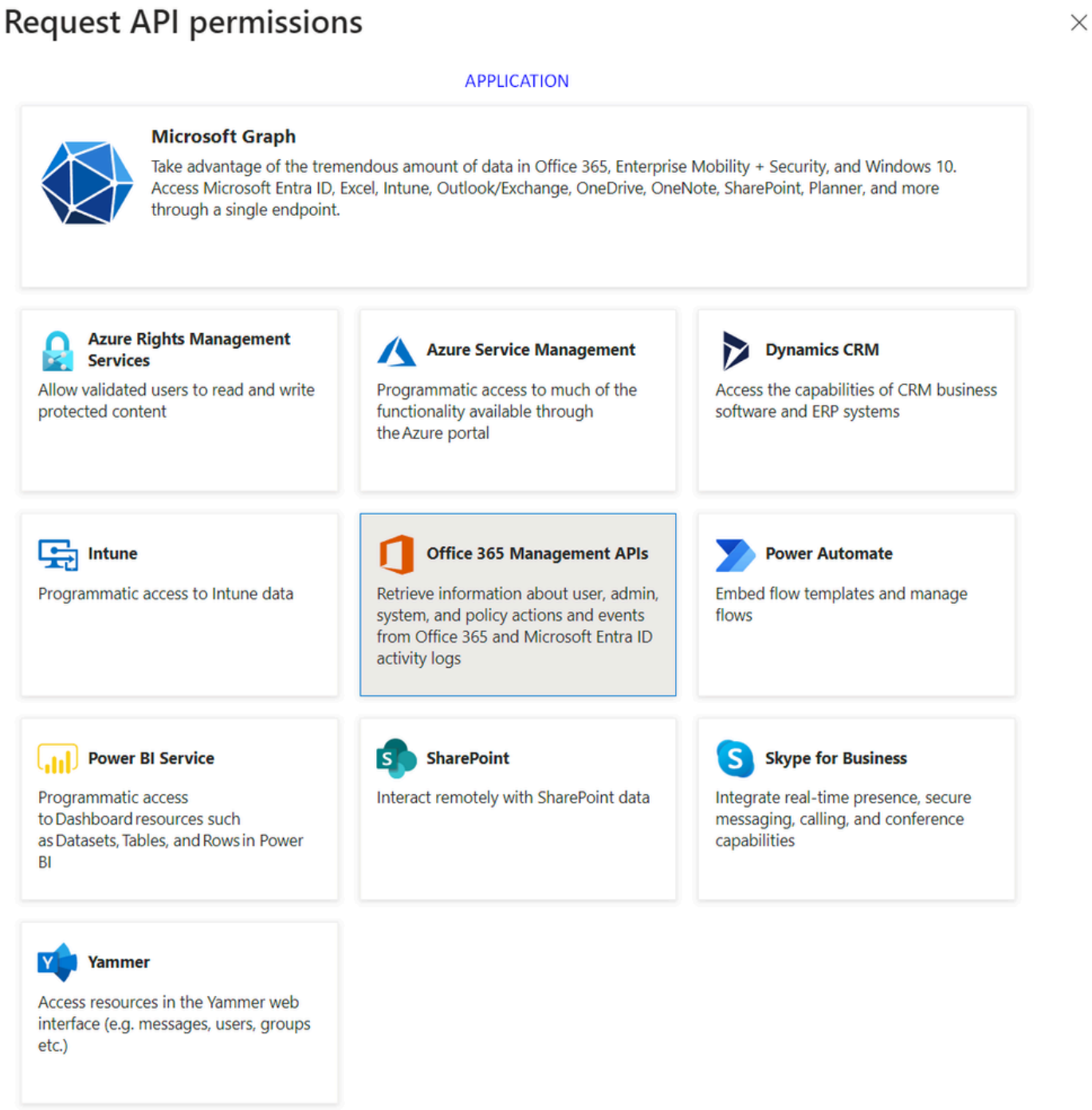


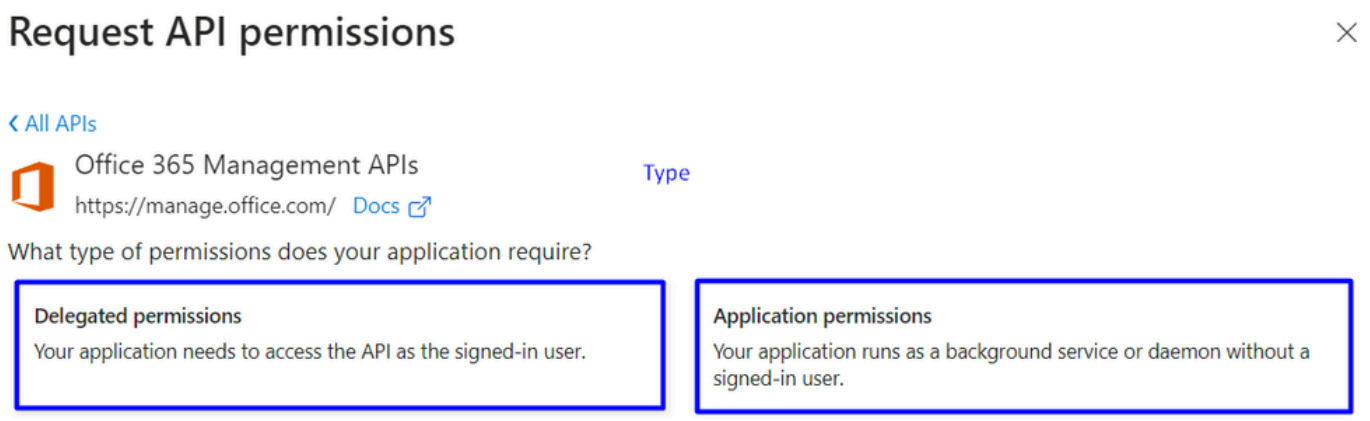
API/ Permissions Name	Type	Description	Admin Consent Required
Microsoft Graph			
Directory.AccessAsUser.All	Delegated	Access directory as the signed-in user	Yes
Directory.Read.All	Application	Read directory data	Yes
Files.Read.All	Delegated	Read all files that user can access	No
Files.Read.All	Application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



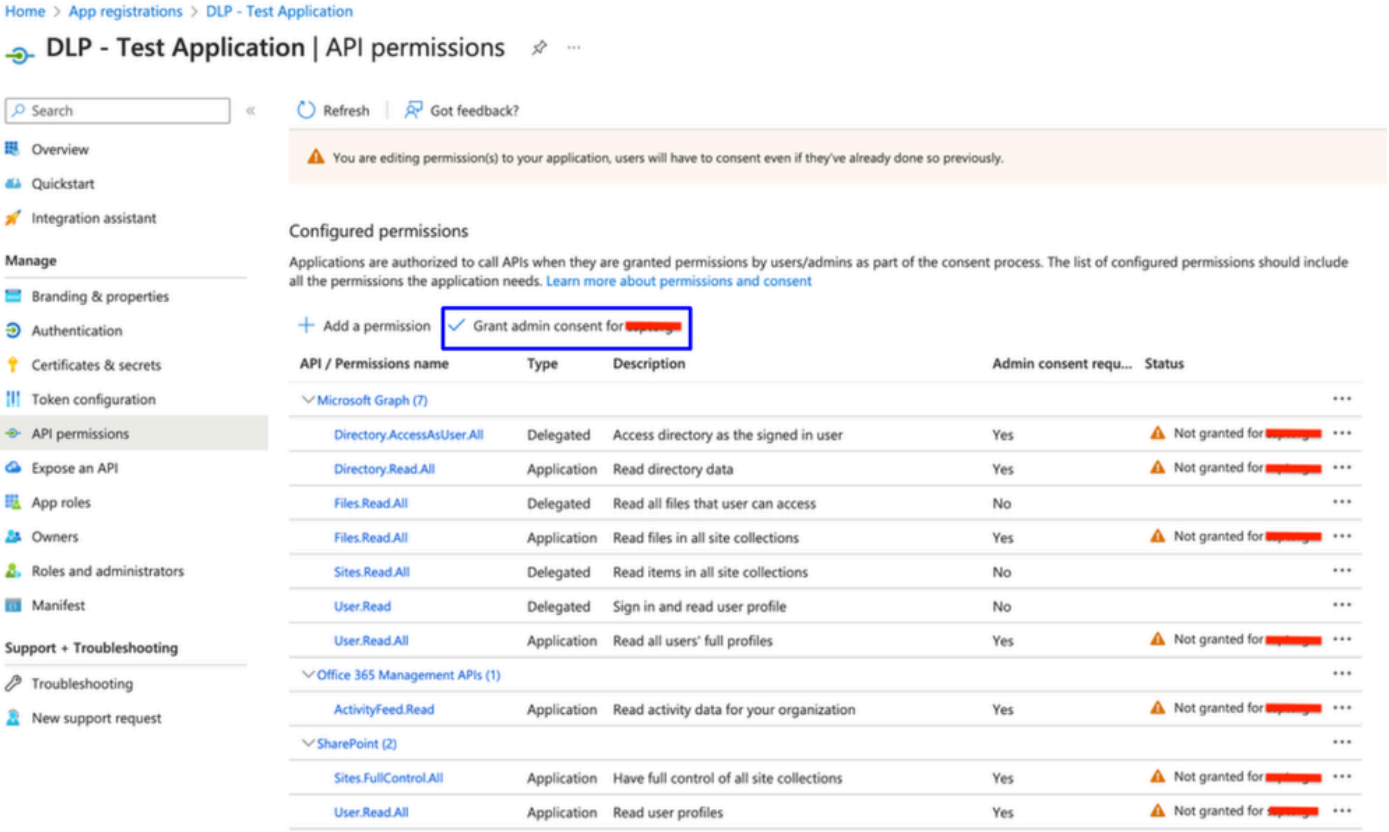
Observação: em vez da **Site.FullControl.All** permissão, escolha **Sites.FullControl.All**.

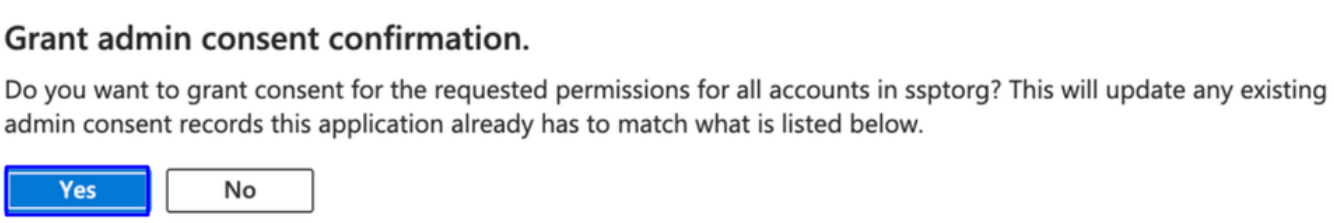
- Para isso, você precisa escolher a permissão com base no aplicativo e digitar:



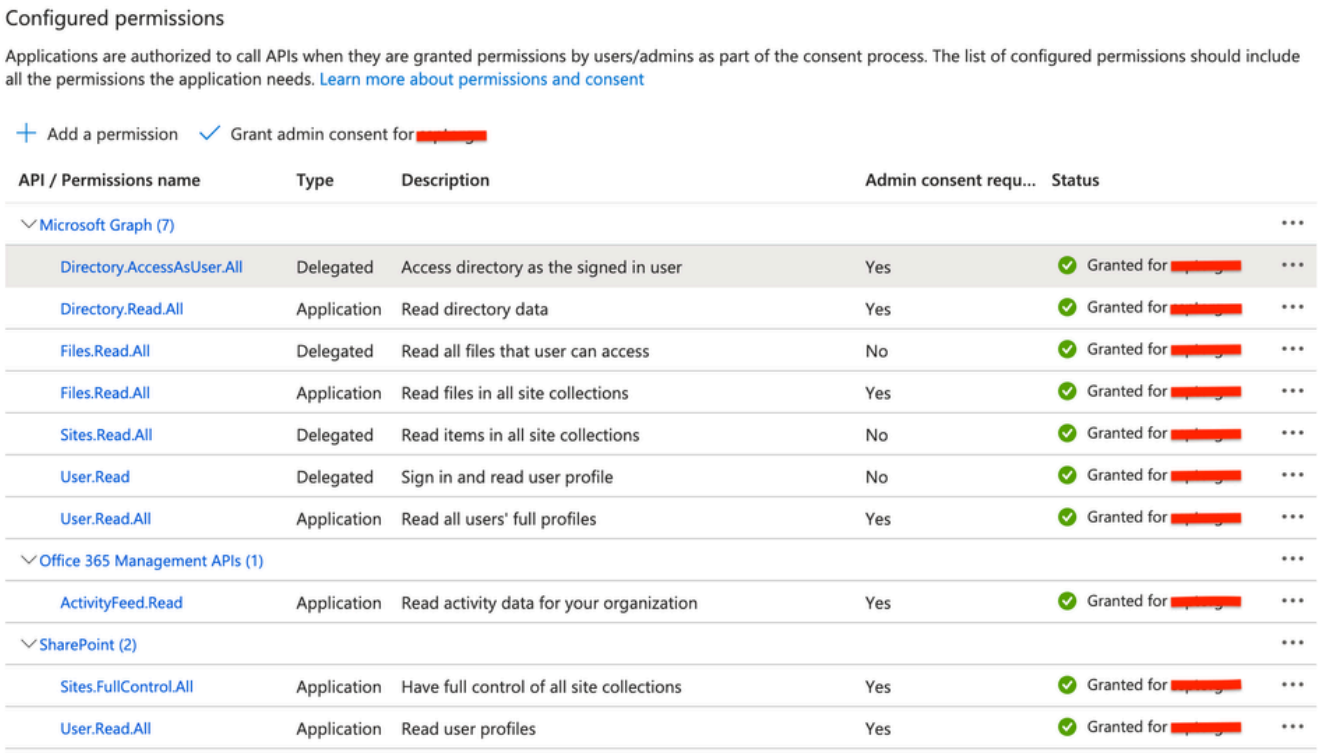


8. Depois que todas as permissões necessárias forem adicionadas, clique **Grant Admin Consent** em para o espaço.





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



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 subseçãoDLP 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**.

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.