

Configurando a integração:	2
Etapa 1: Configuração AD.....	2
Configurações a serem inseridas na integração:.....	2
Configurando Aplicação SAML2:.....	2
Configurando Aplicação Microsoft Graph API:	5
Etapa 2: Configuração Plugg.to	11
Configurando API's:	11
Mapeando permissões:.....	12
Logando	13

Configurando a integração:

Para a integração funcionar corretamente é necessário configurar tanto o Active Directory quanto o painel da plugg para inserir as credenciais.

Etapa 1: Configuração AD

Configurações a serem inseridas na integração:

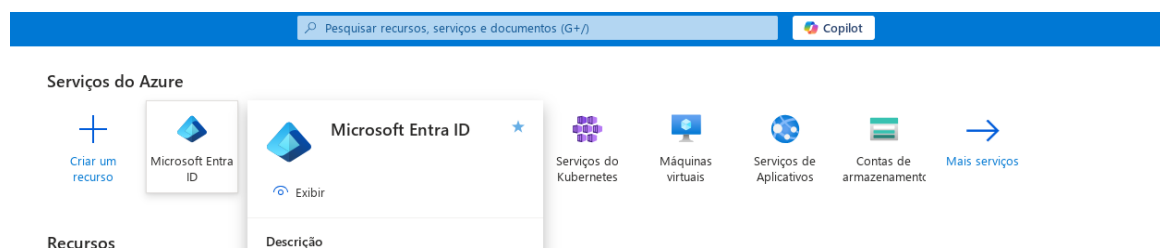
Entity ID: <https://painel.plugg.to/auth/saml2>

Url de resposta: <https://painel-homolog.plugg.to/saml/auth>

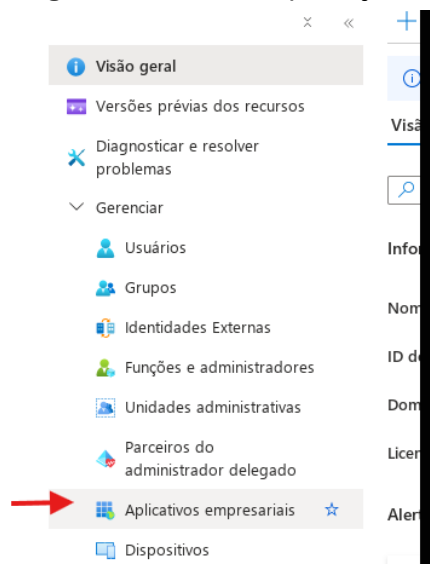
Configurando Aplicação SAML2:

1. Acesse o **portal do Azure Active Directory**.

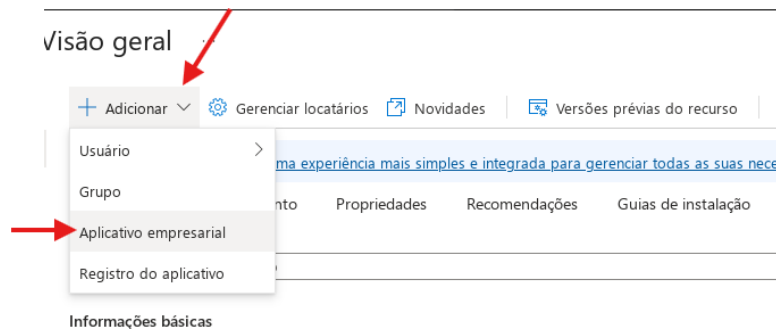
Acesse o ícone Entra ID



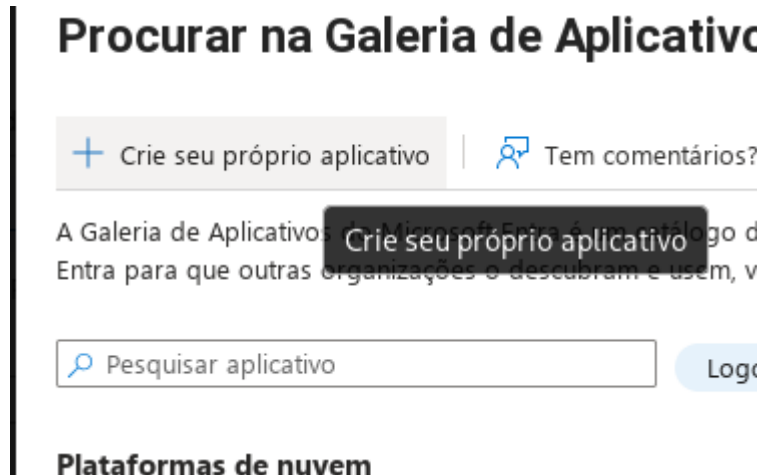
2. Registre uma nova aplicação do tipo **Enterprise Application**.



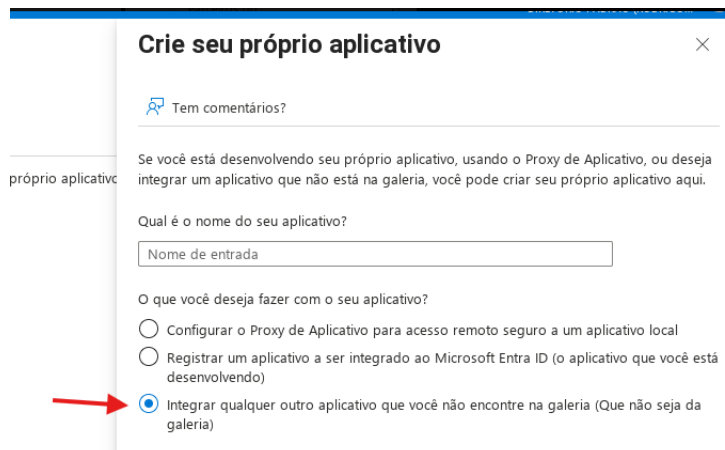
- a. Clique em “Adicionar” e depois em “Aplicativo Empresarial”



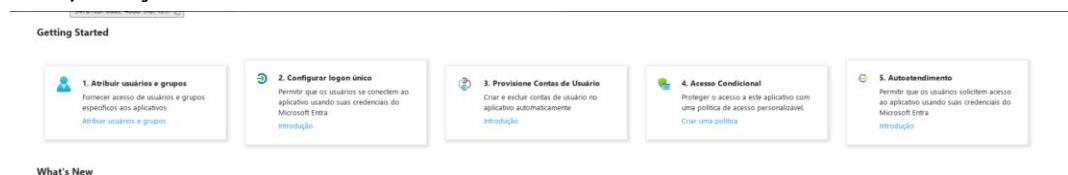
- b. Use a opção “+ Criar seu próprio aplicativo”



- c. Selecione a opção “Integrar qualquer outro aplicativo” e defina um nome para esta aplicação

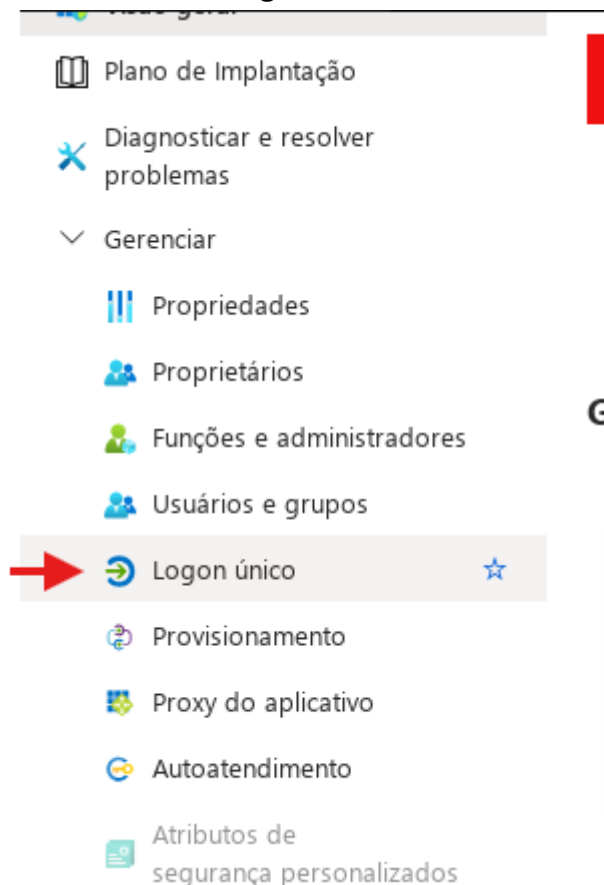


- d. Configure a atribuição de usuários e grupos que terão permissão de uso da aplicação:



3. Configure o método de autenticação como **SAML 2.0**.

a. Vá até o menu “Logon único”



b. Selecione a opção “SAML”



c. Configure a seguinte tela com as informações a seguir:

Entity ID: <https://painel.plugg.to/auth/saml2>

Url de resposta: <https://painel.plugg.to/saml/auth>

Connect ou OAuth. [Saiba mais.](#)

Leia a [guia de configuração](#) para ajudar a integrar o TEste.

- ### Configuração Básica de SAML

[Editar](#)

Identificador (ID da Entidade)	Obrigatório
URL de Resposta (URL do Serviço do Consumidor de Declaração)	Obrigatório
URL de Logon	Opcional
Estado de Retransmissão (Opcional)	Opcional
URL de Logoff (Opcional)	Opcional
- ### Atributos e Declarações

⚠ Preencha os campos necessários na Etapa 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Identificador Exclusivo do Usuário	user.userprincipalname
- ### Certificados SAML

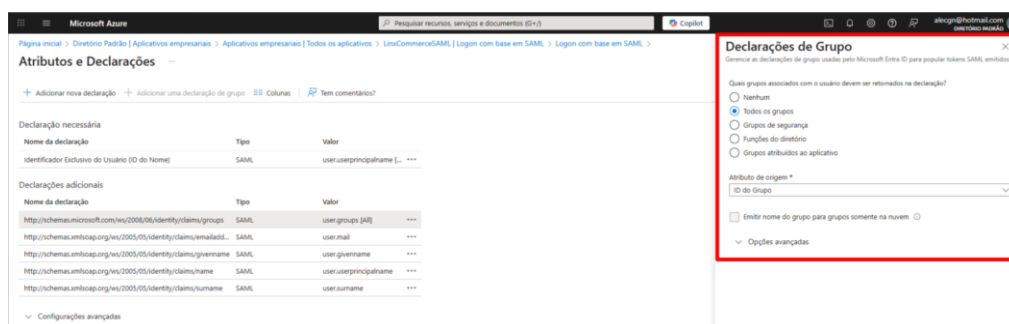
Certificado de autenticação de tokens [Editar](#)

Status	Ativo
Impressão Digital	3E854A7A2AC83AF993C8B43D1BD05E9C1C2883B9
Expiração	19/03/2030, 21:05:02
Email de Notificação	rodrigo.andreotti@outlook.com
URL de metadados de federação de aplicativos	https://login.microsoftonline.com/a02a0140-7a20...
Certificado (Base64)	Baixar
Certificado (Bruto)	Baixar
XML de Metadados de Federação	Baixar

Certificados de verificação (opcional) [Editar](#)

Obrigatório	Não
Ativo	0
Expirou	0

- d. Ainda dentro da tela acima, clique no botão editar referente a seção “Atributos e Declarações” e adicione a permissão de acesso a grupos, conforme abaixo:



- e. Salve as alterações e volte à tela de “Logon único” e copie as informações necessárias para configuração do painel (Ver Item 4 da seção da configuração Plugg.to -> Configurando API's)

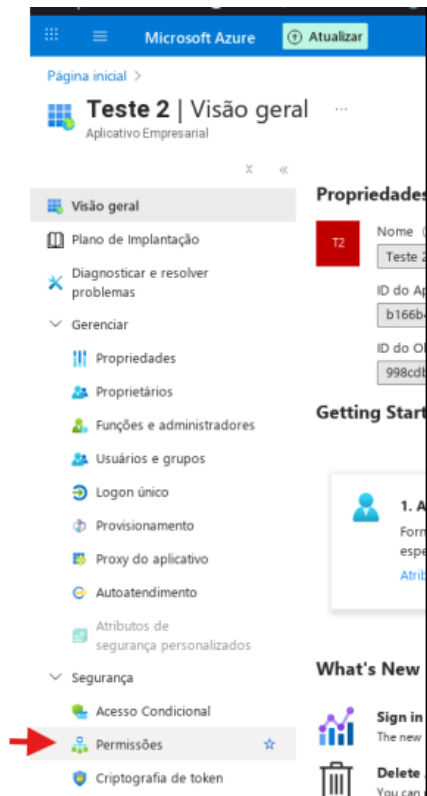
Configurando Aplicação Microsoft Graph API:

Repita os passos 1 e 2 da criação da aplicação apontados no tópico anterior (Configurando Aplicação SAML2)

Após este aplicativo criado é necessário dar as permissões necessárias a ele e criar os tokens de acesso seguindo o seguinte procedimento:

1. Configurando Permissões

a. Acesse o menu “Permissões”



b. Depois acesse “Registro de aplicações”

« [✓ Analisar as permissões](#) [Atualizar](#) | [Alguns comentários?](#)

Permissões

Abaixo está a lista de permissões que foram concedidas para sua organização. Como administrador, você pode con [Saiba mais](#)

Você pode revisar, revogar e restaurar permissões. [Saiba mais](#)

Para configurar as permissões solicitadas para aplicativos que você possui, use o registro do aplicativo. [Registro de aplicativo](#)

Conceder consentimento do administrador para Diretório Padrão

c. Acesse o Menu “Permissões de API”

d. E, então, adicionar permissão:

e. Na tela que é aberta, selecione a opção “API’s que minha organização usa” e procure por “Microsoft Graph”:

Nome	ID do aplicativo (cliente)
Signup	b4bddae8-ab25-483e-8670-df09b9f1d0ea
Azure Resource Graph	509e4652-da8d-478d-a730-e9d4a1996ca4
Azure AD Notification	fc03f97a-9db0-4627-a216-ec98ce54e018
IAM Sunnortability	a57aca87-rbc0-4f3c-8b9e-dc095f1c8978

f. Nós precisaremos de permissões de aplicativo:

Solicitar permissões de API

[← Todas as APIs](#)

Microsoft Graph
<https://graph.microsoft.com/> [Documentos](#)

Que tipo de permissões seu aplicativo requer?

Permissões delegadas

Seu aplicativo precisa acessar a API como o usuário conectado.

Permissões de aplicativo



Seu aplicativo é executado como um serviço de plano de fundo ou daemon sem um usuário conectado.



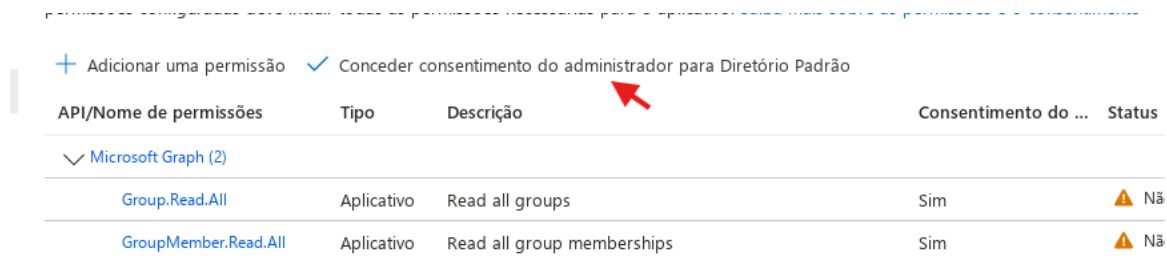
g. Procure pelas permissões de “Groups” e marque as duas abaixo:

- Group.Real.All
- GroupMember.Read.All

Selecionar permissões

group		Consentimen
Permissão		
> Calls		
> Group-Conversation		
> Group-OnPremisesSyncBehavior		
∨ Group (1)		
<input type="checkbox"/> Group.Create ⓘ Create groups		Sim
<input checked="" type="checkbox"/> Group.Read.All ⓘ Read all groups		Sim
<input type="checkbox"/> Group.ReadWrite.All ⓘ Read and write all groups		Sim
∨ GroupMember (1)		
<input checked="" type="checkbox"/> GroupMember.Read.All ⓘ Read all group memberships		Sim
<input type="checkbox"/> GroupMember.ReadWrite.All ⓘ Read and write all group memberships		Sim
> GroupSettings		

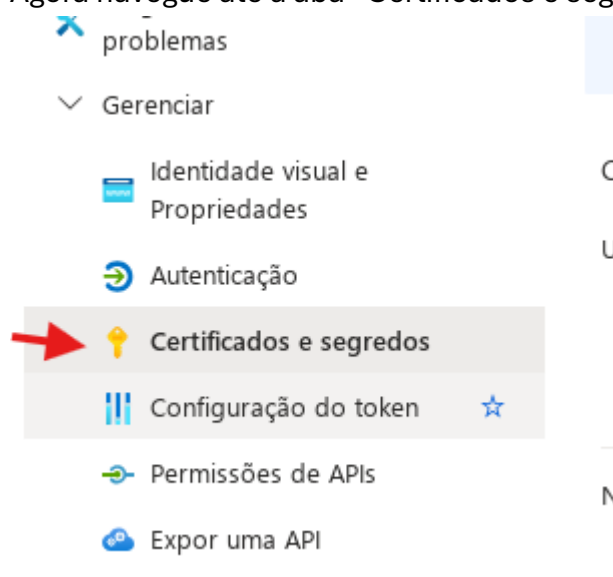
- h. Por fim, conceda as permissões com administrador do diretório usando o botão “Conceder consentimento do administrador para Diretório Padrão”:



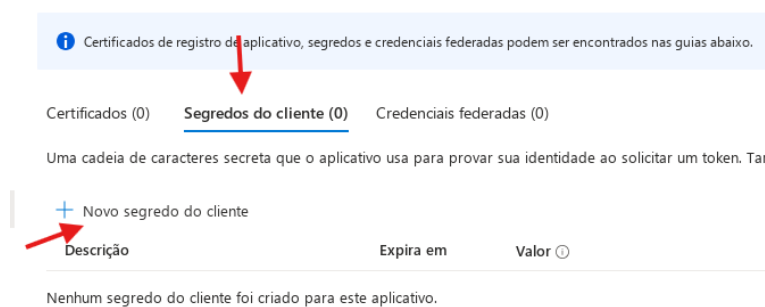
API/Nome de permissões	Tipo	Descrição	Consentimento do ...	Status
+ Adicionar uma permissão ✓ Conceder consentimento do administrador para Diretório Padrão				
Microsoft Graph (2)				
Group.Read.All	Aplicativo	Read all groups	Sim	⚠ Nã
GroupMember.Read.All	Aplicativo	Read all group memberships	Sim	⚠ Nã

2. Criar client_secret para a aplicação

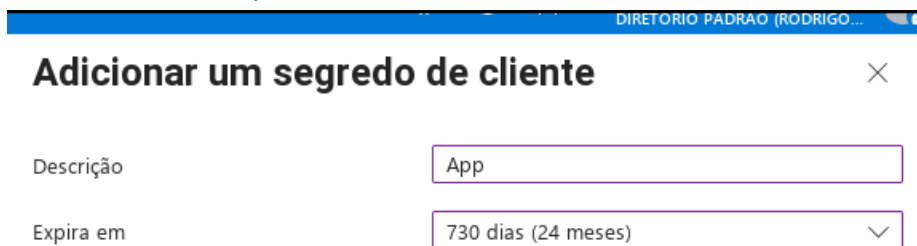
- a. Agora navegue até a aba “Certificados e segredos”



- b. Clique na aba “Segredos do Cliente” e depois em “Novo segredo do Cliente”



- c. Defina um nome para o segredo e um período de duração para ele de acordo com suas políticas internas:

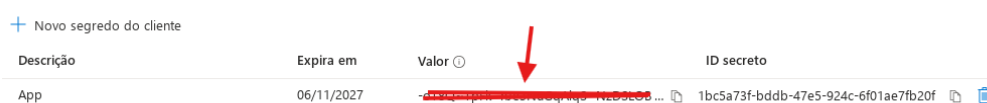


Adicionar um segredo de cliente ✕

Descrição

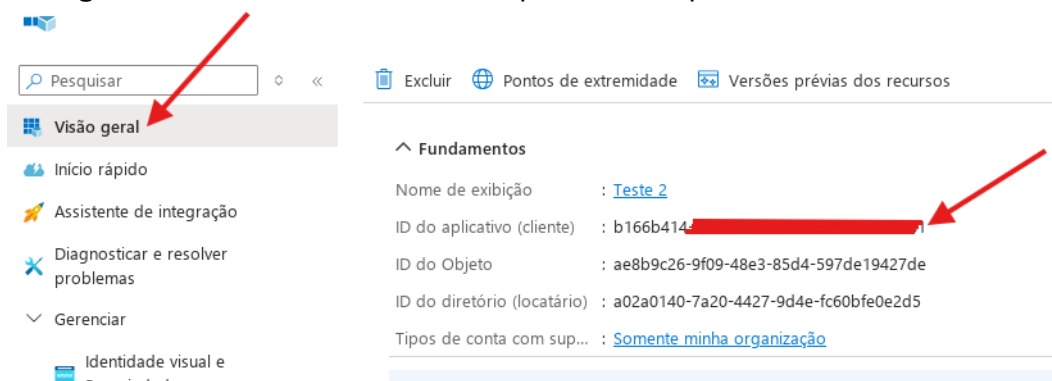
Expira em ▾

- d. Copie os detalhes do segredo recém criado:



Descrição	Expira em	Valor	ID secreto
App	06/11/2027	[REDACTED]	1bc5a73f-bddb-47e5-924c-6f01ae7fb20f

- e. Navegue até a aba “Visão Geral” e copie o ID do aplicativo criado



Visão geral

Nome de exibição : [Teste 2](#)

ID do aplicativo (cliente) : b166b414-[REDACTED]

ID do Objeto : ae8b9c26-9f09-48e3-85d4-597de19427de

ID do diretório (locatário) : a02a0140-7a20-4427-9d4e-fc60bfe0e2d5

Tipos de conta com sup... : [Somente minha organização](#)

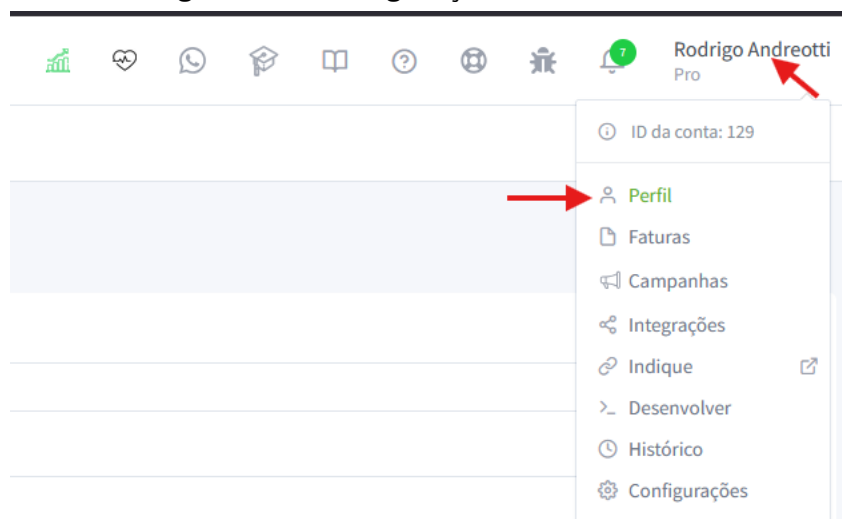
Importante: Os segredos de aplicativo para microsoft tem validade, é importante que essa validade entre no planejamento da sua equipe de TI para que seja renovada dentro do prazo estipulado na hora da criação do segredo.

Etapa 2: Configuração Plugg.to

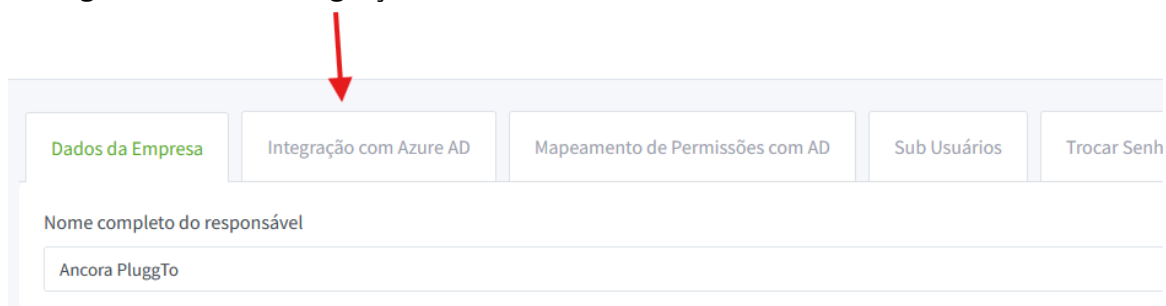
Configurando API's:

Quando a configuração do AD é concluída, precisamos inserir as credenciais obtidas na API dentro do painel da Plugg.to, para isso teremos o seguinte passo a passo:

1. Logar no painel da Plugg com o usuário admin da conta
2. Navegar até as configurações de Perfil:



3. Navegar até a aba "Integração com Azure AD"



- Do lado esquerdo configure as credenciais da aplicação criada para SAML2 e do lado direito as credenciais da aplicação criada para Graph API:

Configuração Azure AD / SAML

Configure a integração com Azure Active Directory para permitir login via SSO.

<p>Configurações SAML</p> <p>Entity ID</p> <input type="text" value="ID da entidade Azure AD"/> <p>URL de Login SSO</p> <input type="text" value="URL de Login SSO Azure AD"/> <small>URL de Login SSO Azure AD</small> <p>URL de logoff SSO</p> <input type="text" value="URL de logoff SSO Azure AD"/> <p>Metadata URL</p> <input type="text" value="https://login.microsoftonline.com/tenant-id/federationmetadata/..."/> <small>URL dos metadados do Azure AD para configuração automática</small>	<p>Configurações do Open Graph API</p> <p>Client ID</p> <input type="text" value="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"/> <p><small>Client ID do Open Graph API Azure AD</small></p> <p>Client Secret</p> <input type="text" value="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"/> <small>Client Secret do Open Graph API Azure AD</small>
---	---

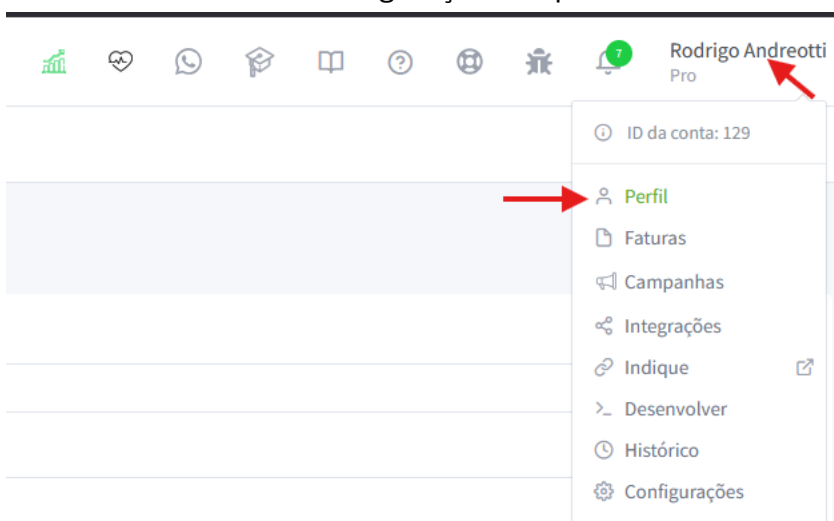
[Salvar Configuração](#)

- Clique em salvar as configurações. Neste momento iremos validar se conseguimos conexão com ambas as integrações e se tudo correr bem, salvaremos as credenciais.

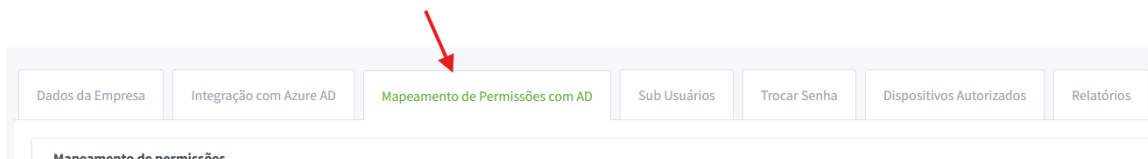
Mapeando permissões:

Depois de configurar com sucesso a integração com os endpoints, precisamos atrelar os grupos de trabalho do AD com as permissões efetivas da Plugg.to e para isso podemos realizar o seguinte procedimento:

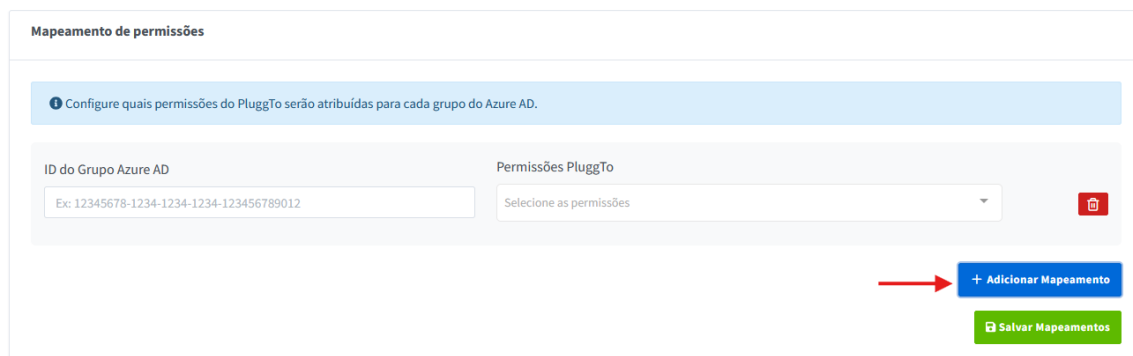
- Acessar novamente a configurações de perfil.



2. Acessar a aba “Mapeamento de Permissões com AD”



3. Nesta aba clique em adicionar mapeamento:



4. Aparecerá uma nova linha para inserir os dados de atrelamento. Copie o ID do grupo no AD e cole no campo da esquerda.

5. No campo da direita selecione todas as permissões que usuários desse grupo terão:



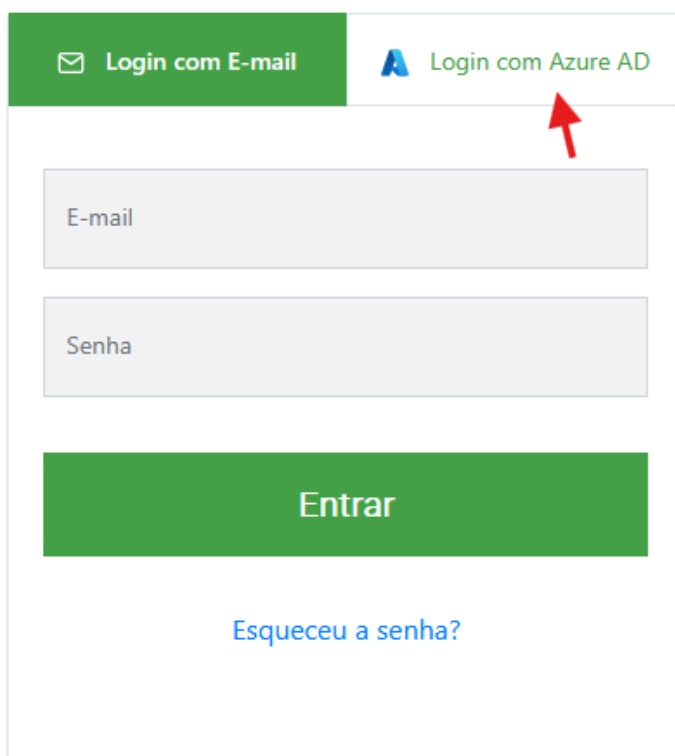
6. Repita o procedimento para todos os grupos necessários e, por fim, salve o Mapeamento

Logando

Após todos os procedimentos acima já é possível logar usando o AD no nosso painel.

1. Faça logoff e vá para a tela de login do painel

2. Selecione a aba "Login com Azure AD"

A login form with two tabs at the top: "Login com E-mail" (selected) and "Login com Azure AD". Below the tabs are two input fields for "E-mail" and "Senha". A green "Entrar" button is positioned below the input fields. At the bottom, there is a blue link for "Esqueceu a senha?". A red arrow points to the "Login com Azure AD" tab.

✉ Login com E-mail **A** Login com Azure AD

E-mail


Senha

Entrar

[Esqueceu a senha?](#)

3. Informe o seu plugg ID e clique em “Entrar com SSO”



✉ Login com E-mail  Login com Azure AD

Login com Azure AD

Entre com sua conta corporativa

Seu PluggID
7234

Entrar com SSO

Precisa configurar SSO para sua empresa?
Entre em contato com o administrador.

4. Isso irá te redirecionar para a tela de login do Azure AD, se tudo estiver configurado corretamente tanto do lado da plugg, quanto do lado do Azure, você deve conseguir logar sem problemas.