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

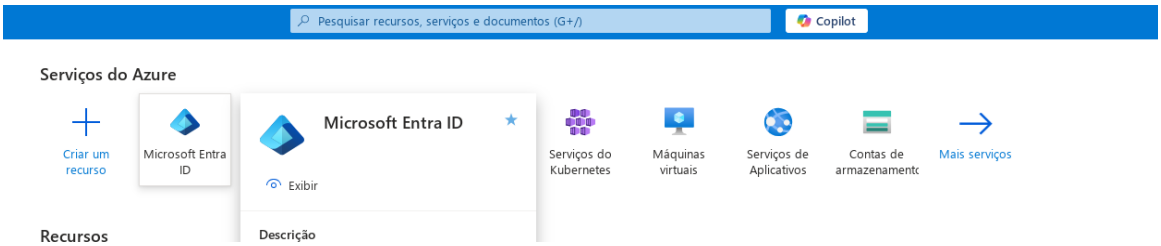
Configurações a serem inseridas na integração:

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

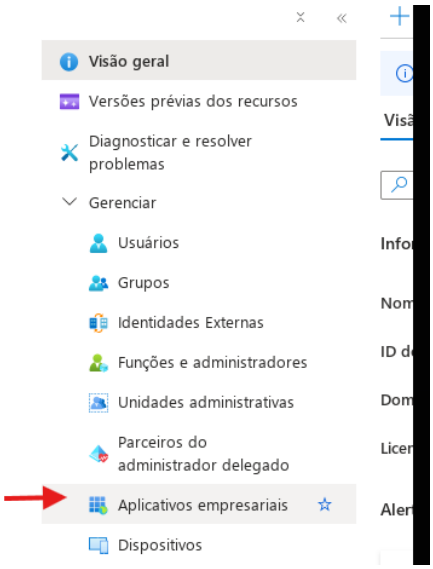
Url de resposta: https://painel-homolog.plugg.to/saml/auth

Configurando Aplicação SAML2:

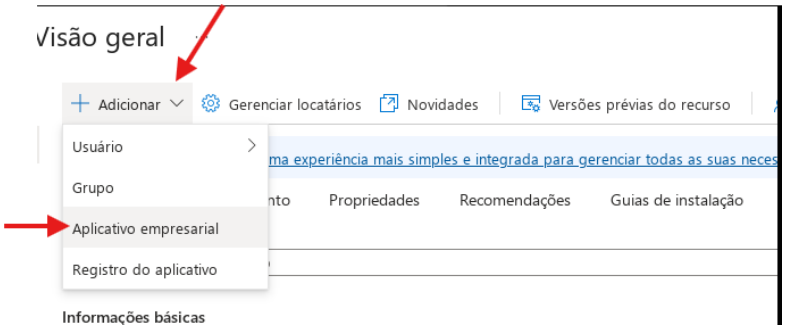
1. Acesse o **portal do Azure Active Directory**.
   Acesse o ícone Entra ID



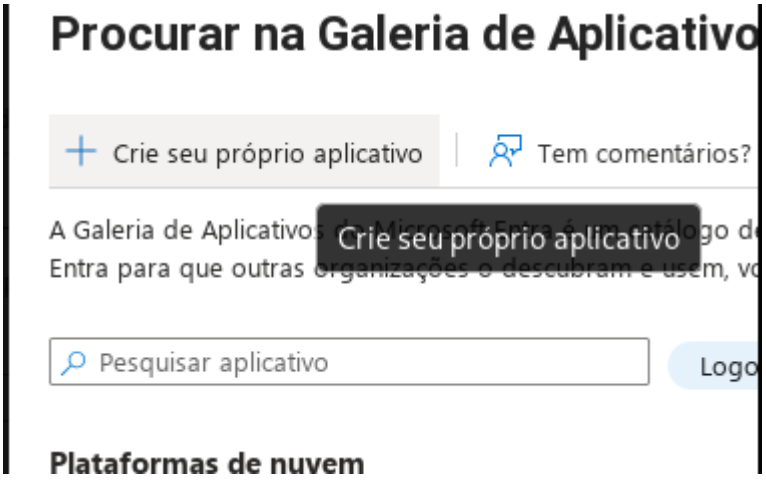
2. Registre uma nova aplicação do tipo **Enterprise Application**.



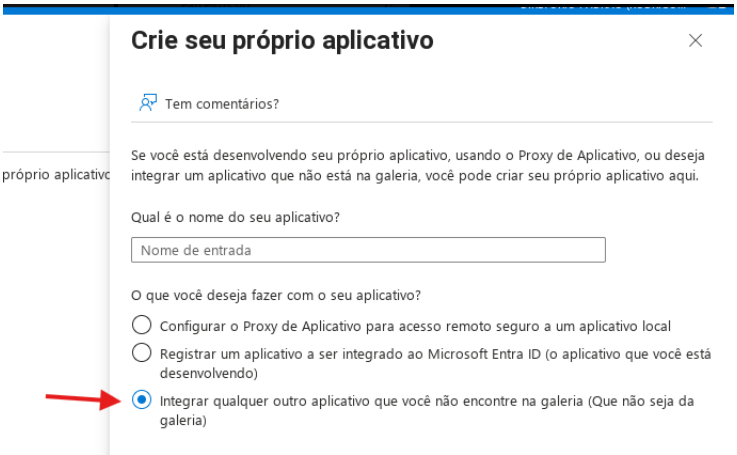
a. Clique em “Adicionar” e depois em “Aplicativo Empresarial”



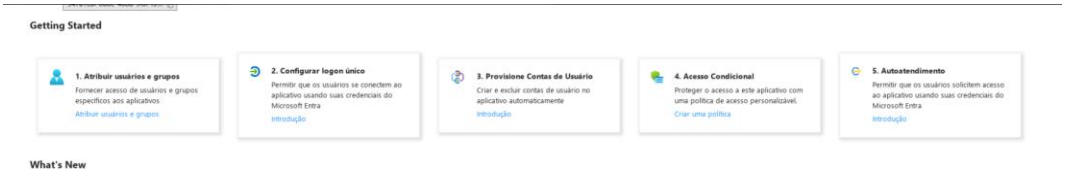
b. Use a opção “+ Criar seu próprio aplicativo”



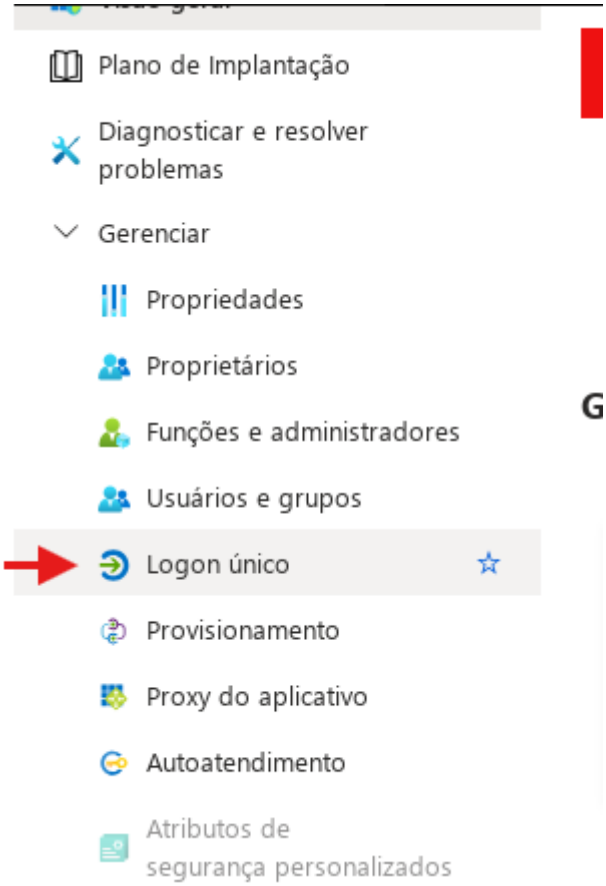
c. Selecione a opção “Integrar qualquer outro aplicativo ...." e defina um nome para esta aplicação



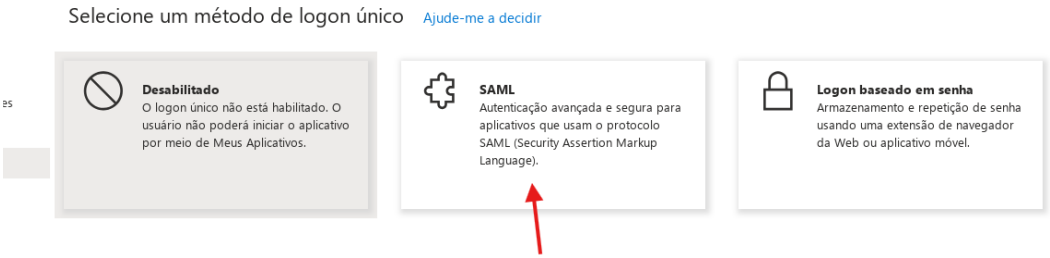
d. Configure a atribuição de usuários e grupos que terão permissão de uso da aplicação:



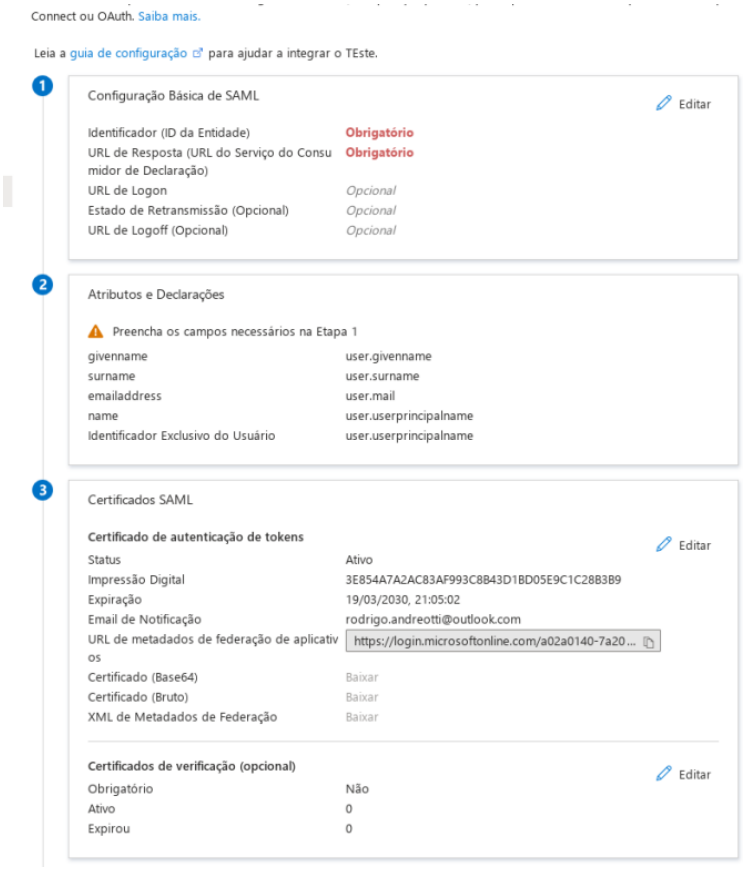
3. Configure o método de autenticação como **SAML 2.0**.
    a. Vá até o menu “Logon único”



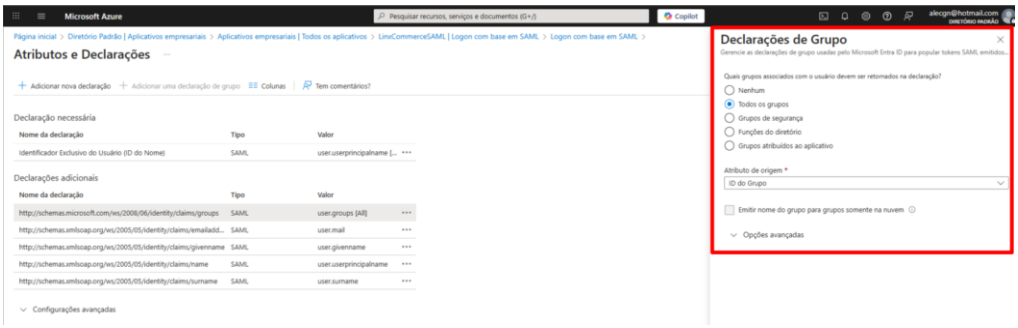
    b. Selecione a opção “SAML”



    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



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:



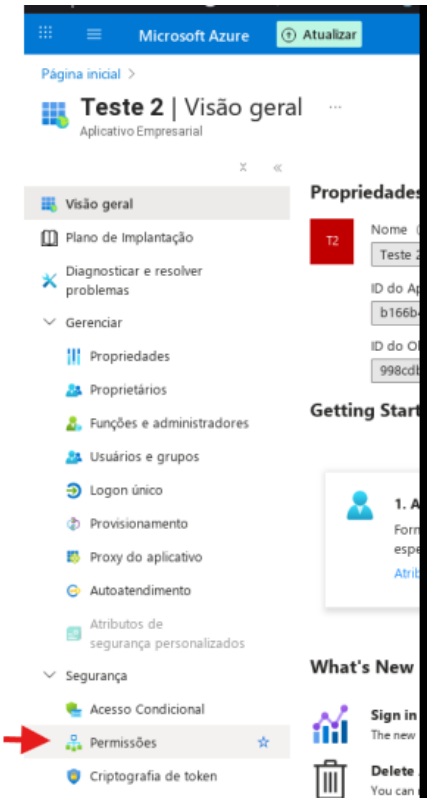
e. Salve as alterações e volte à tela de “Logon único” e copie as informações necessárias para configuração do painel (Ver Item 4 da seção da configuração Plugg.to -> Configurando API’s)

Configurando Aplicação Microsoft Graph API:

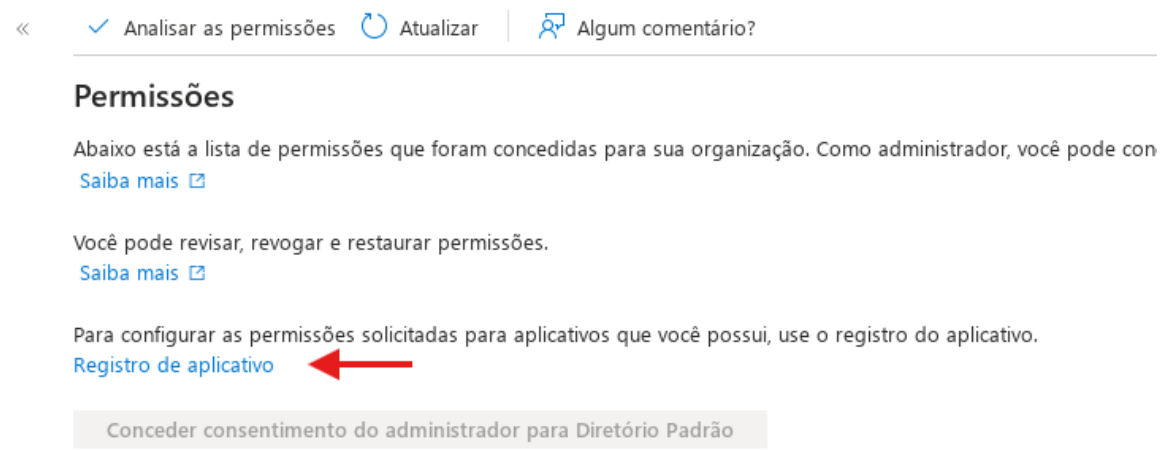
Repita os passos 1 e 2 da criação da aplicação apontados no tópico anterior (Configurando Aplicação SAML2)

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

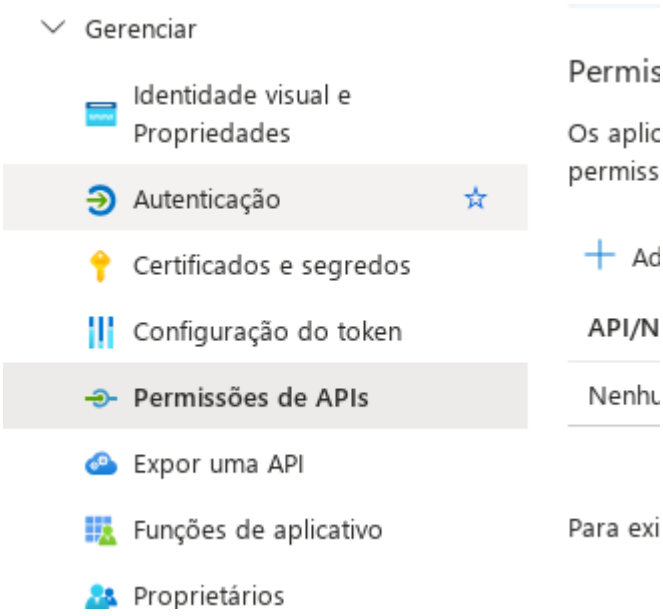
1. Configurando Permissões
    a. Acesse o menu “Permissões”



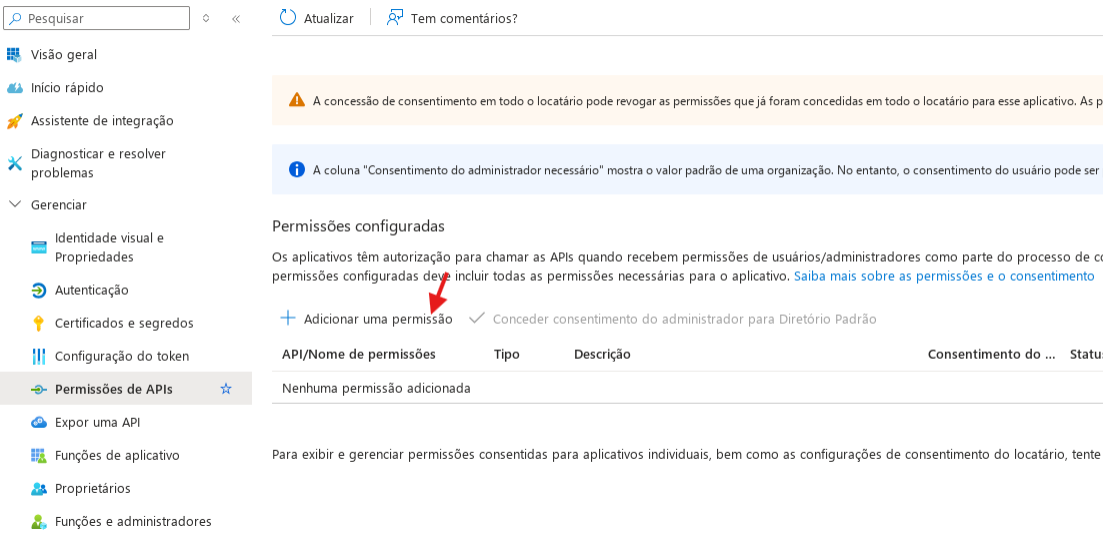
    b. Depois acesse “Registro de aplicações”



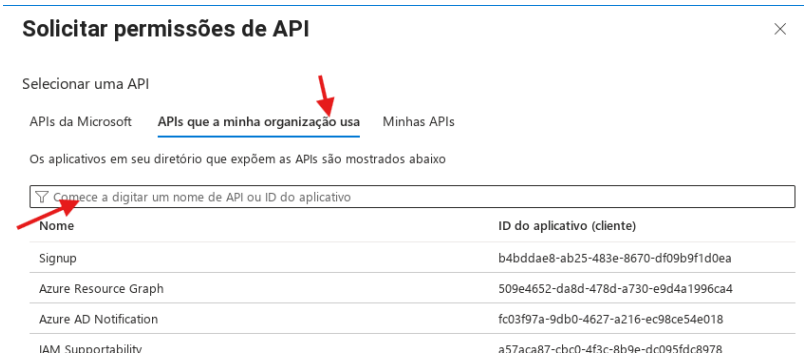
c. Acesse o Menu “Permissões de API”



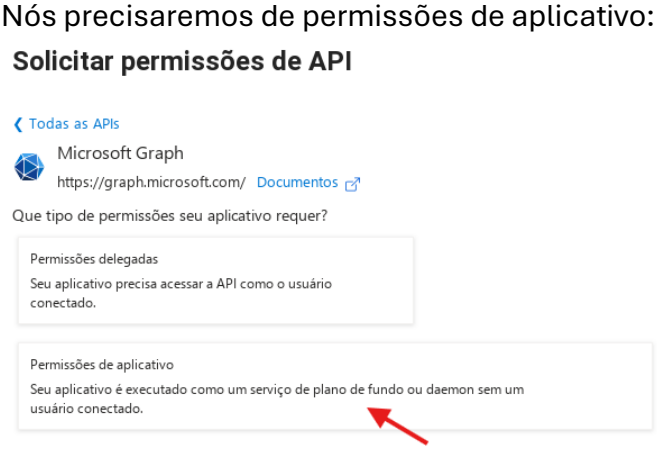
d. E, então, adicionar permissão:



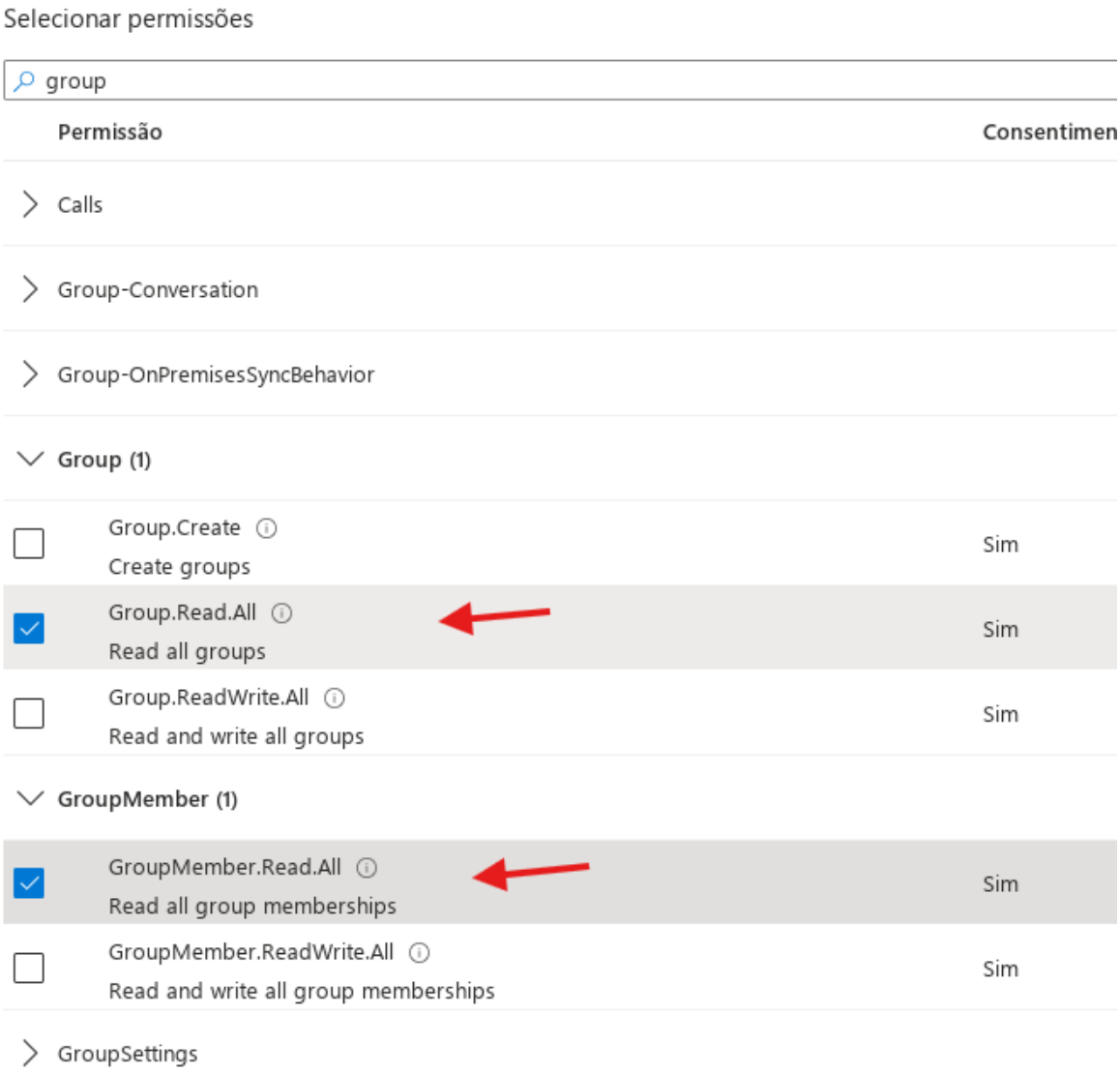
e. Na tela que é aberta, selecione a opção “API’s que minha organização usa” e procure por “Microsoft Graph”:



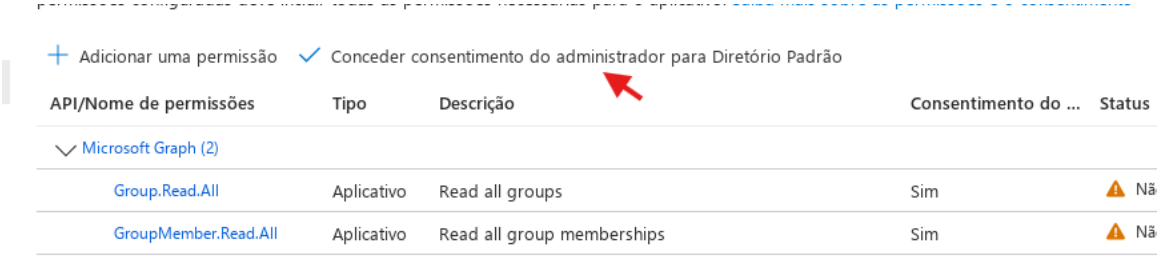
f. Nós precisaremos de permissões de aplicativo:



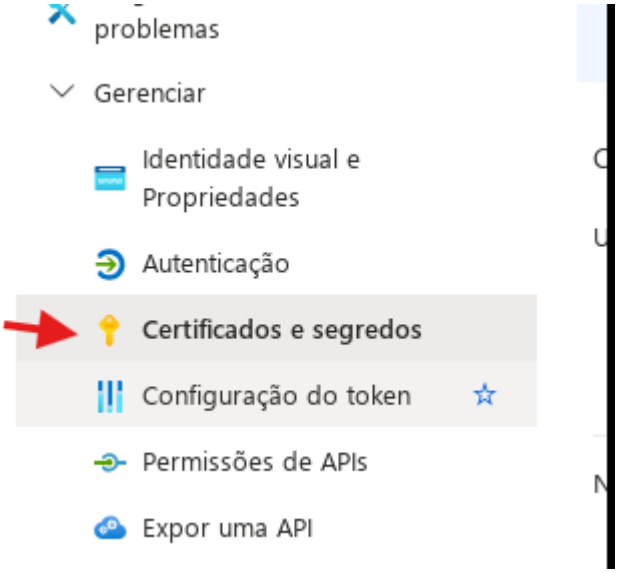
g. Procure pelas permissões de “Groups” e marque as duas abaixo:
- Group.Real.All
- GroupMember.Read.All



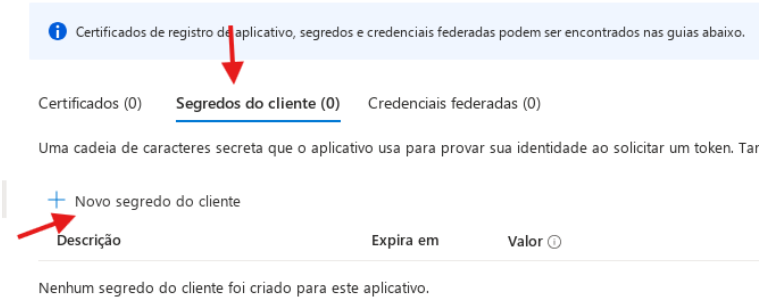
h. Por fim, conceda as permissões com administrador do diretório usando o botão “Conceder consentimento do administrador para Diretório Padrão”:



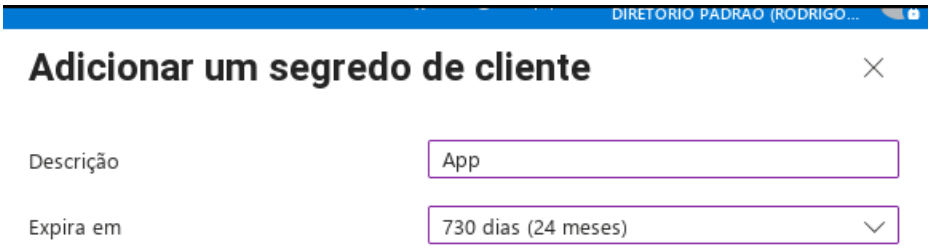
2. Criar client_secret para a aplicação
   a. Agora navegue até a aba “Certificados e segredos”



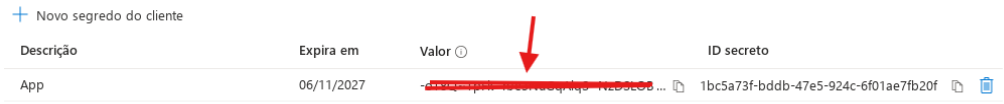
   b. Clique na aba “Secredos do Cliente” e depois em “Novo segredo do Cliente”



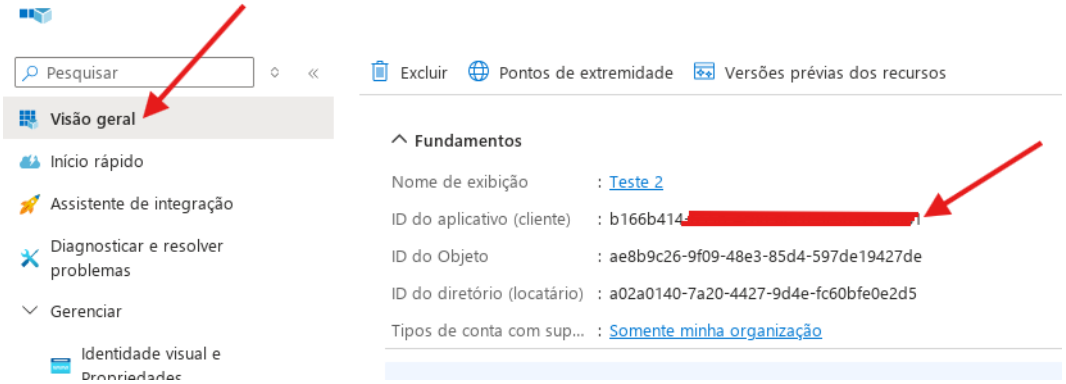
c. Defina um nome para o secredo e um período de duração para ele de acordo com suas políticas internas:



d. Copie os detalhes do segredo recém criado:



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



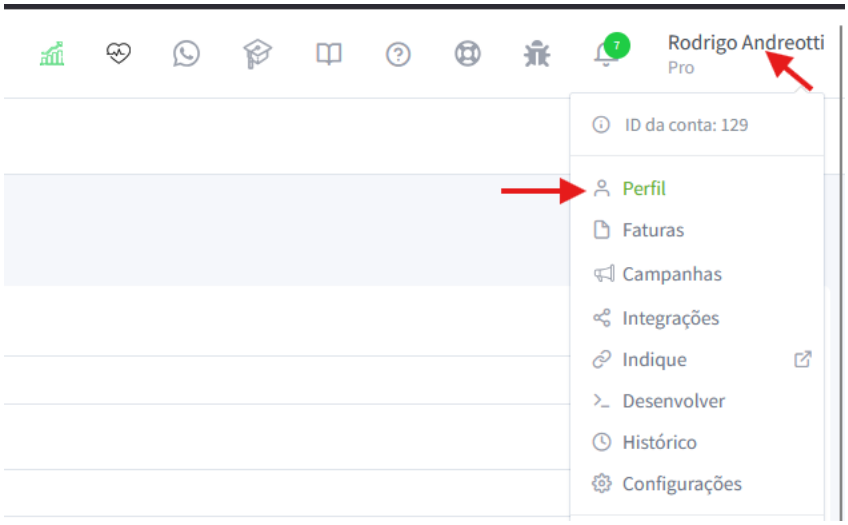
Importante: Os segredos de aplicativo para microsoft tem validade, é importante que essa validade entre no planejamento da sua equipe de TI para que seja renovada dentro do prazo estipulado na hora da criação do segredo.

Etapa 2: Configuração Plugg.to

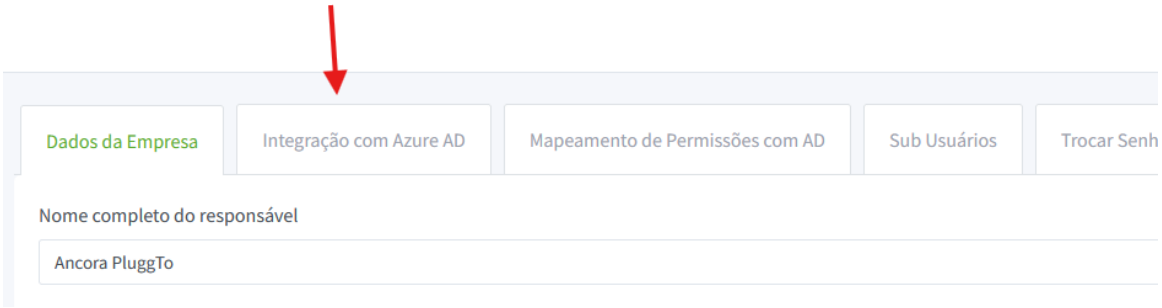
Configurando API's:

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:

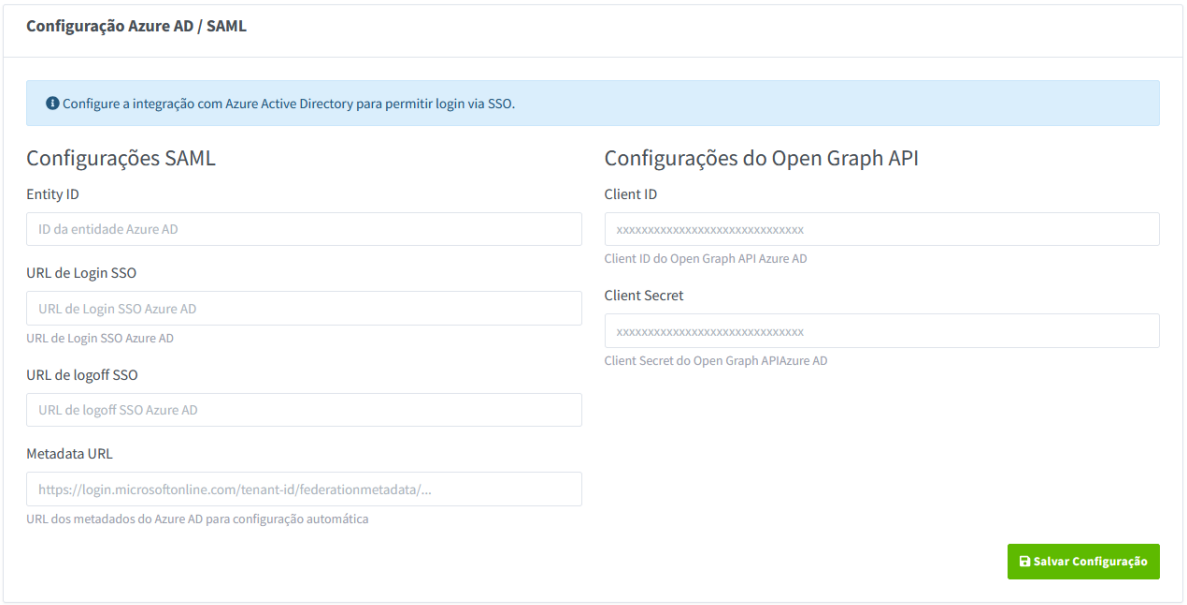
1. Logar no painel da Plugg com o usuário admin da conta
2. Navegar até as configurações de Perfil:



3. Navegar até a aba “Integração com Azure AD”



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

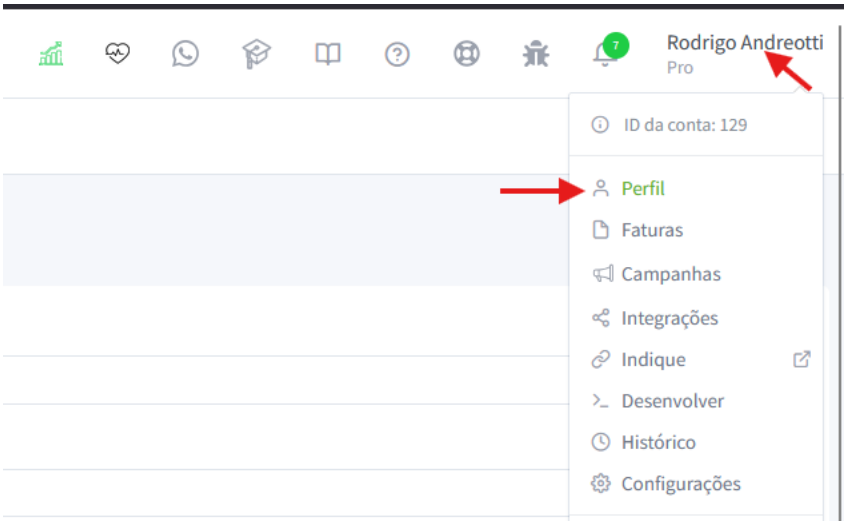


5. Clique em salvar as configurações. Neste momento iremos validar se conseguimos conexão com ambas as integrações e se tudo correr bem, salvaremos as credenciais.

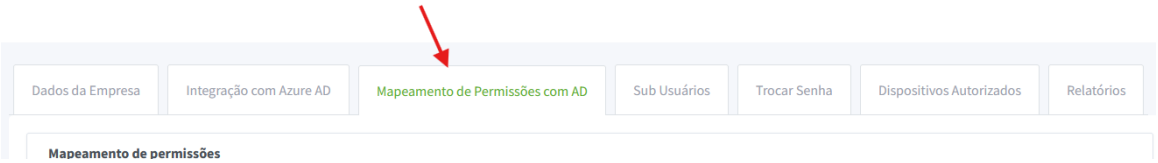
Mapeando permissões:

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:

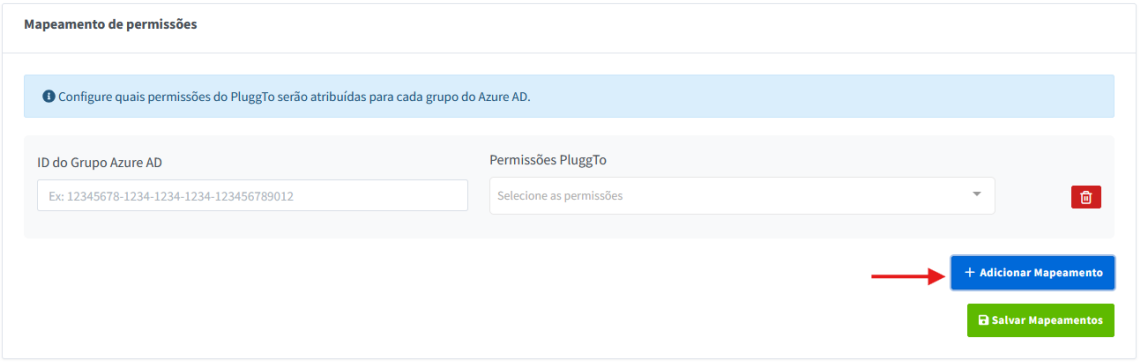
1. Acessar novamente a configurações de perfil.



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:

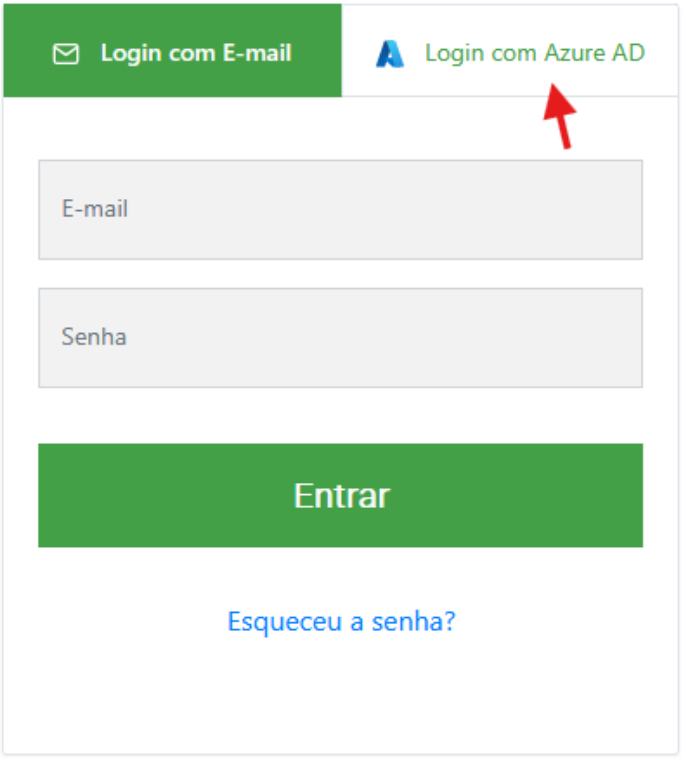
6. Repita o procedimento para todos os grupos necessários e, por fim, salve o Mapeamento

Logando

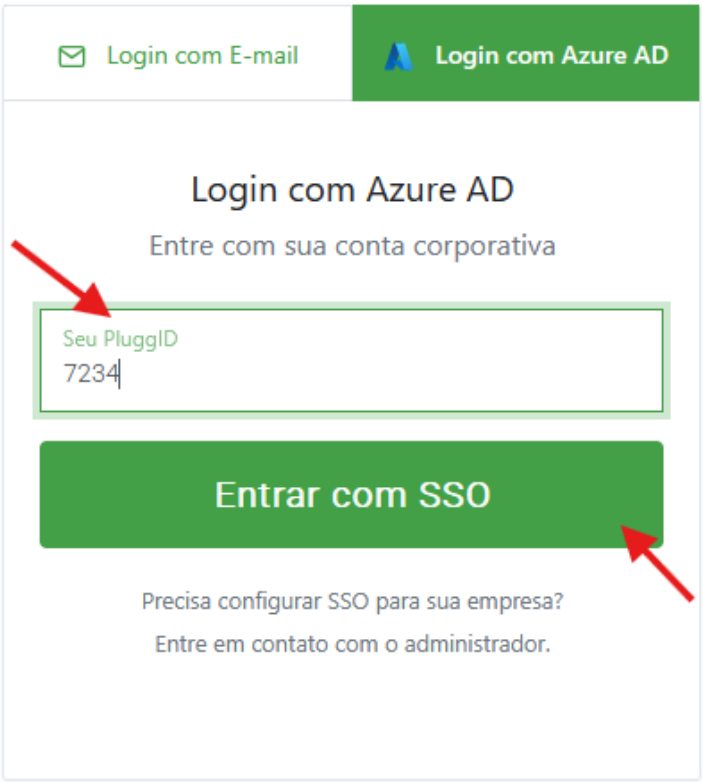
Após todos os procedimentos acima já é possível logar usando o AD no nosso painel.

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

2. Selecione a aba “Login com Azure AD”



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



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.