

Configurar SSO para Yapoli no Azure AD

Para configurar um acesso SSO na Yapoli via Azure AD é necessário fazer o vínculo no Azure antes de cadastrar na Yapoli para definir os parâmetros.

Para tal, siga os seguintes passos:

Passo 1

No Azure AD vá em App registrations > New Registration

A tela abaixo deve ser mostrada. Informe um nome qualquer a seu gosto, verifique qual o conjunto de usuários deve ter permissão de acesso no "Supported account types" e, no "Redirect URI", selecione plataforma "Web" e informe a seguinte url: ***https://<<dominio-da-plataforma-na-yapoli>>/login-oauth***, exemplo: *https://cliente.yapoli.com/login-oauth*. Se o login for feito por domínio personalizado, informe este domínio, ex: *https://cliente.com/login-oauth*.

Clique em "Register".

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Diretório Padrão only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform	▼	e.g. https://example.com/auth
-------------------	---	-------------------------------

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#) 

[Register](#)

Passo 2

Para criar uma senha através da qual a Yapoli possa se autorizar no seu domínio, vá até Certificates & Secrets e, na aba "Client Secrets" clique em "New Client Secret". Uma janela se abrirá à direita, escolha a seu critério um identificador para essa senha e quanto tempo para que a senha expire. Após isso o valor da senha gerada será exibido na lista uma única vez. Clique para copiar essa senha e armazene-a para utilizá-la no cadastro da Yapoli.

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
-------------	---------	-------	-----------

No client secrets have been created for this application.

Passo 3

Vá até "Token Configuration" e clique em "Add optional claim". No menu que aparecer à direita clique em "Access" e na lista que abrir abaixo marque "preferred_username". Ao final, clique em "Add".

Obs: Esse passo é necessário para que o nome preferencial seja o identificador do usuário. Esses identificador precisa ser o e-mail do usuário que é utilizado para entrar na plataforma Yapoli.

The screenshot shows the 'Add optional claim' configuration page in the Azure portal. The page is titled 'YapoliValidacao | Token configuration'. On the left, there is a navigation pane with various options like 'Overview', 'Quickstart', 'Integration assistant', 'API', 'Branding & properties', 'Authentication', 'Certificates & secrets', 'Token configuration', 'API permissions', 'Expose an API', 'App roles', 'Owners', 'Roles and administrators', 'Manifest', 'Port + Troubleshooting', 'Troubleshooting', and 'View support request'. The main content area is titled 'Optional claims' and contains a table with columns 'Claim' and 'Description'. Below the table, there are two buttons: '+ Add optional claim' and '+ Add groups claim'. On the right side, there is a panel titled 'Add optional claim' with a sub-section 'Token type' where 'Access' is selected. Below this, there is a list of optional claims with checkboxes and descriptions. The 'preferred_username' claim is checked. At the bottom of the panel, there are 'Add' and 'Cancel' buttons.

Passo 4

Vá até "API permissions" e clique em "Add a permission". No menu à direita que abrir, selecione "Microsoft Graph" e "Delegated Permissions". Na lista que aparecer marque as opções "email", "openid" e "profile". Clique em "Add permissions".

The screenshot shows the 'Request API permissions' dialog in the Azure portal. It is for the 'Microsoft Graph' API. The 'Delegated permissions' section is active, showing a list of permissions to be requested. The permissions listed are:

Permission	Admin consent required
<input checked="" type="checkbox"/> email (View users' email address)	No
<input type="checkbox"/> offline_access (Maintain access to data you have given it access to)	No
<input checked="" type="checkbox"/> openid (Sign users in)	No
<input checked="" type="checkbox"/> profile (View users' basic profile)	No

At the bottom of the dialog, there are 'Add permissions' and 'Discard' buttons.

Passo 5

Vá até "Overview". Primeiro copie e armazene o "Application (client ID)" (primeiro print). Depois, no menu superior clique em "Endpoints". Na lista que aparecer (print 2) copie as URLs que aparecerem nas opções "OAuth 2.0 authorization endpoint (v2)" e "OAuth 2.0 token endpoint (v2)". Copie e armazene os valores destas URLs assim como fez com a senha no passo 2 e com o application ID

The screenshot shows the 'Endpoints' page in the Azure portal for the application 'YapoliValidacao'. The page displays the following information:

- Display name: YapoliValidacao
- Application (client) ID: 0968b9fe-6aee-408b-8980-f78e250bdd31
- Object ID: f6481fc2-b583-41ef-bcd4-1e4578504b77
- Directory (tenant) ID: 999137ef-aafc-40b2-b879-2a9356095647
- Client credentials: 0.certificate_1.secret
- Redirect URIs: 1.web_0.spa_0.public.client
- Application ID URI: Add an Application ID URI
- Managed application in L.: YapoliValidacao

At the bottom, there are links for 'Get Started' and 'Documentation'.

Endpoints

OAuth 2.0 authorization endpoint (v2)

`https://login.microsoftonline.com/999137ef-aafc-40b2-b879-2a9356095647/oauth2/v2.0/authorize`

OAuth 2.0 token endpoint (v2)

`https://login.microsoftonline.com/999137ef-aafc-40b2-b879-2a9356095647/oauth2/v2.0/token`

Passo 6

Vá até a plataforma Yapoli, entre com um perfil com permissão de administrar clientes. Vá até o Manager > Advanced Settings > Single Sign-On.

Clique no "+" para adicionar um novo e preencha os seguintes campos da forma abaixo (os campos omitidos seguem o padrão de documentação de SSO da Yapoli):

- Client ID: Inclua o application ID copiado no passo 5
- Scope: Insira: *openid email profile*
- Authorization URL: insira o valor copiado de "OAuth 2.0 authorization endpoint (v2)" no passo 5
- Token URL: insira o valor copiado de "OAuth 2.0 token endpoint (v2)" no passo 5
- Secret Key: insira a senha copiada no passo 2 (**atenção**: esta senha não poderá mais ser obtida nem pelo Azure, nem pela Yapoli após finda essa operação)
- Tipo de solicitação: FORM
- Identificação: ID_TOKEN
- Campo de identificação: Insira: *preferred_username*

Clique em SAVE

Após feitos estes passos vá até a página de login da Yapoli. Uma opção com o nome do SSO inserido no passo 6 deve ser apresentado.

Obs: todos os passos podem estar traduzidos noutra idioma. Consideramos aqui a configuração em inglês.