

Autenticação via SSO (Single Sign-On)

O SSO (Single Sign On) é uma ferramenta de controle de acesso para aplicações distribuídas na web com integração a sistemas corporativos e que utiliza o protocolo OAuth 2.0. Ele é responsável por gerenciar o processo de autenticação e permissões dos usuários em múltiplos serviços, dessa forma, é possível logar em um desses serviços e ter acesso aos demais serviços sem precisar logar em cada um deles. Um exemplo conhecido de sistema que utiliza o SSO é o Gmail (conta Google).

O processo para configurar o login por Redes Sociais, é diferente da autenticação via SSO, [veja aqui](#) como configurar.

Seleção da autenticação

Nos subtópicos abaixo, você verá que há duas formas de configurar a autenticação via SSO dependendo de como foi criado o projeto.

Antes de criar o projeto

A seleção da autenticação pode ser feita durante ou após a [criação do projeto](#) no Cronapp. Na janela de criação do projeto é possível selecionar a opção SSO no campo **Tipo de Autenticação** (Figura 1).

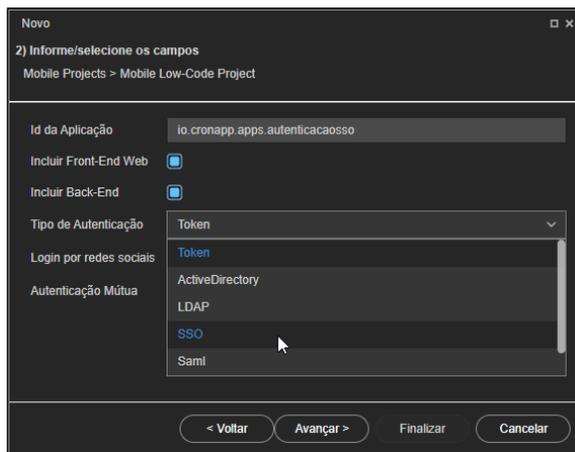


Figura 1 - Seleção do tipo de autenticação na criação do projeto

Ao criar o projeto já como a autenticação do tipo SSO, a view de login virá somente com o botão **Entrar** (Figura 1.1) já configurado para acessar o servidor SSO configurado.



Figura 1.1 - Projeto já criado com SSO

Após criar o projeto

Se a configuração for após a criação do projeto, acesse a aba **Configurações do Projeto** na Janela de [Configurações do Projeto](#) e selecione a opção **SSO (OAuth2)** para exibir o acordeão **Configurações da Autenticação** (Figura 2).

Nesta página

- [Seleção da autenticação](#)
 - [Antes de criar o projeto](#)
 - [Após criar o projeto](#)
- [Configuração](#)

Veja também

- [Configurando o Keycloak com autenticação em 2 fatores](#)

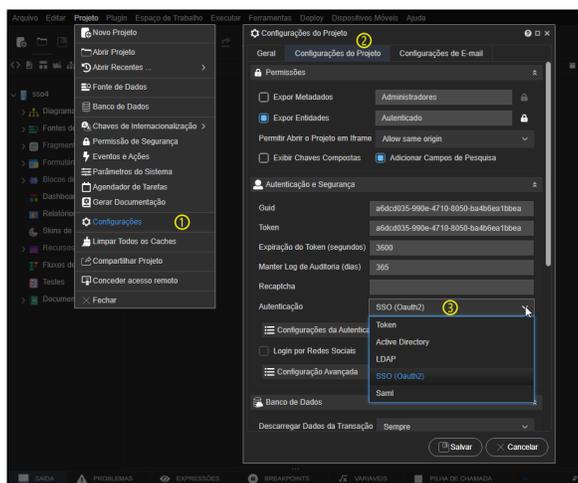


Figura 2 - Seleção do tipo de autenticação após o projeto criado

Após adicionar um botão "Login SSO" na tela de login, é necessário que ele chame uma função com o bloco [Login via SSO \(Oauth2\)](#), a página de login ficará como abaixo (Figura 2.1), contendo duas formas de logar.

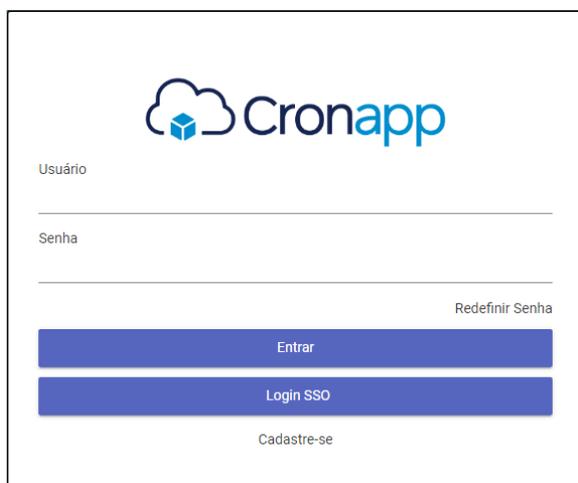


Figura 2.1 - Botão de Login SSO adicionado

Após a configuração do projeto para autenticação via SSO, também é possível fazer autenticação manualmente, através da URL, exemplo:

- **web:** `https://<DOMÍNIO>/#/login`
- **mobile:** `https://<DOMÍNIO>/#/app/login`

Importante

Após a criação do projeto, se for necessário alterar o tipo de autenticação de Token para SSO, por exemplo, será necessário modificar manualmente as páginas de **login web** (Localização: `Formulários /Web/`) e **login mobile** (Localização: `Formulários /Mobile/`), retirando os campos de Entrada de texto ("usuário" e "senha"), os links ("redefinir senha" e "cadastre-se") e o botão "Entrar". Para autenticação via SSO, basta um botão que execute o bloco [Login via SSO \(Oauth2\)](#).

Configuração

Após seguir os passos da Figura 2.1, acesse a aba **Configurações da Autenticação** e preencha os campos informados na Figura 3.

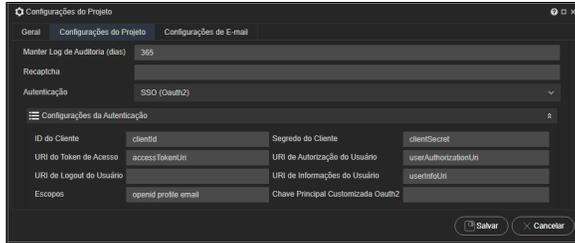


Figura 3 - Aba Configurações da Autenticação da janela de Configurações do Projeto

- **ID do Cliente:** o ID do cliente encontrado nas configurações do provedor de autenticação SSO.
- **Segredo do Cliente:** valor do segredo do cliente encontrado nas configurações do provedor de autenticação SSO.

Alguns provedores SSO só exibem o segredo no momento da criação, Caso tenha perdido, será necessário excluir o antigo e criar um novo.

- **URI do Token de Acesso:** URI do provedor OAuth2 que fornece o *token* de acesso para a aplicação.
- **URI de Autorização do Usuário:** URI para o qual o usuário será redirecionado, se for necessário, para autorizar o acesso ao recurso.
- **URI de Logout do Usuário:** após o usuário fazer o logout da aplicação será direcionado para a URI inserida. Na próxima vez que o usuário precisar logar na aplicação, deverá fazer o login via SSO novamente.
- **URI de Informações do Usuário:** URI para obter detalhes atuais do usuário.
- **Escopos:** define os dados concedido para o provedor SSO, sendo possível adicionar novos escopos, separando-os com o caractere espaço " " .

Cuidado ao alterar as informações dos Escopos, se for inserido algo que não exista, gerará um erro.

Alguns provedores SSO exigem parâmetros específicos para funcionar, dessa forma, acesse a documentação do seu provedor SSO para garantir a configuração correta.

Exemplo: A depender de como o provedor Azure esteja configurado, ele exigirá o parâmetro "Read.User", assim, o campo Escopo deve ser preenchido da seguinte forma: `openid profile email User.Read`

- **openid:** fornece *tokens* para autenticação;
- **profile:** fornece o acesso às informações sobre o usuário, como: nome, sobrenome, nome preferencial e ID de objeto;
- **email:** concede acesso ao endereço de e-mail principal do usuário.
- **Chave Principal Customizada Oauth2:** campo opcional que permite definir qual o identificador do usuário será retornado após a autenticação. Caso não seja preenchido, uma lista padrão retornará com os dados do usuário: id, e-mail, nome e outros.

Por fim, após feita a configuração e clicar no botão de login, o usuário será direcionado para o serviço de autenticação via SSO (exemplo na figura 3.1) e que após logar, retornará para a aplicação já com o usuário autenticado.

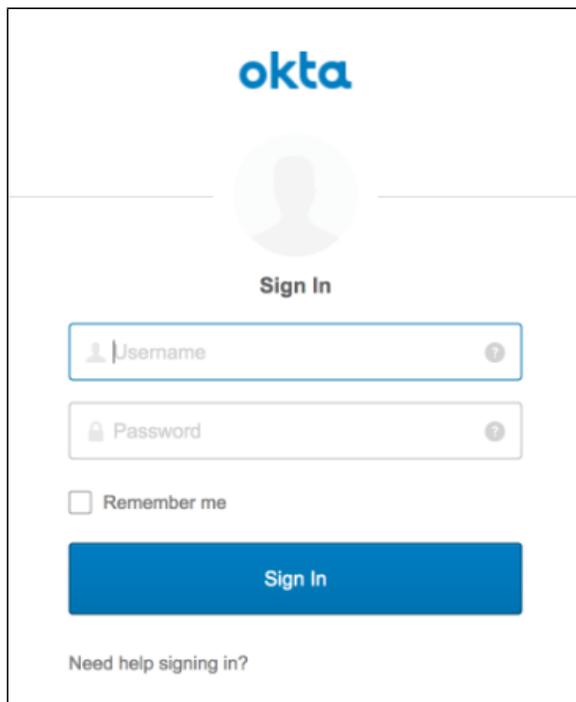


Figura 3.1 - Redirecionamento para a página do servidor de SSO configurado

Caso ocorra algum erro de autenticação via SSO, analise o log no Console do depurador (*dev time*) ou os logs da aplicação (*run time*) para obter detalhes.