Autenticação via SSO (Single Sign-On)

O SSO (Sigle 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 co mo 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).

Novo		n x
2) Informe/selecione os ca	ampos	
Mobile Projects > Mobile L	.ow-Code Project	
ld da Aplicação	io.cronapp.apps.autenticacaosso	
Incluir Front-End Web		
Incluir Back-End		
Tipo de Autenticação	Token	~
Login por redes sociais		
Autenticação Mútua	ActiveDirectory	
,	LDAP	
	SSO	
	Saml	
	< Voltar Avançar > Finalizar Cance	lar

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.

Cronapp	
Entrar	

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

Arquivo Editar I	Projeto Plugin Espaço de Trabalho E	xecutar	Ferrament	as Deploy Dispositivos	Móveis Ajuda		
- ~ ~	Novo Projeto		Config	urações do Projeto 👩		Ø□×	
	Cabrir Projeto		Geral	Configurações do Proje	to Configurações de E-mail		
◇ 16 17 14 14	Abrir Recentes >		A Perm				=
	E Fonte de Dados						
Diagrams	🗟 Banco de Dados			por Metadados	Administradores	<u> </u>	
> To Fonter de	Schaves de Internacionalização >			por Entidades		•	
Eragment	A Permissão de Segurança		Permiti	r Abrir o Projeto em Iframe	Allow same origin	~	
> E Formulár	🕈 Eventos e Ações			bir Chaves Compostas	Adicionar Campos de Pesquisa		
> Blocos de	ma Parâmetros do Sistema						
Dashboar	Agendador de Tarefas		Le Auter	nticação e Segurança		^	
Relatório	Gerar Documentação		Guid		a6dcd035-990e-4710-8050-ba4b6ea1bb	ea	
 Skins de 	🌣 Configurações 🛛 🕦		Token		a6dcd035-990e-4710-8050-ba4b6ea1bb	ea	
> III Recursos	📩 Limpar Todos os Caches		Expiraç	ão do Token (segundos)	3600	= 1	
71 Fluxos de	🖻 Compartilhar Projeto		Manter	Log de Auditoria (dias)	365	= !	
🛃 Testes	Conceder acesso remoto		Recent	cha		_	
> Documen	× Fechar		Recapt	-			
			Autenti	cação	SSO (Oauth2)	Ъ.	
			≣c	onfigurações da Autentica	Token		
				gin por Redes Sociais	Active Directory		
			:= c	onfiguração Avançada	LDAP		
			😤 Banc	o de Dados	Sami	2	
			Danaar	ranar Dadaa da Transasão			
			Descal	regai Dados da Transação	i sempre		
						ancelar	
E saina							
	- Contrastor	-	- ones	48 1000			

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.

	Cronapp	
Usuário		
Senha		
		Redefinir Senha
	Entrar	
	Login SSO	
	Cadastre-se	

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://<DOMINÍO>/#/login
- mobile: https://<DOMINÍO>/#/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.

🗘 Configu	rações do Projeto					0 = ×
Geral	Configurações do Pr	ojeto	Configurações de E-mail			
Manter I	Log de Auditoria (dias)					
Recapto	ha					
Autentic	ação					
≣ Co						
ID do	Cliente			Segredo do Cliente		
	do Token de Acesso		ľokenUri	URI de Autorização do Usuário	userAuthorizationUri	
	de Logout do Usuário			URI de Informações do Usuário	userInfoUri	
Esco	pos	openid	profile email	Chave Principal Customizada Oauth2		
					Salvar X Ca	incelar

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.

okta		
Sign In		
1 Username	0	
Password	0	
Remember me		
Sian In		

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 oslogs da aplicação (*run time*) para obter detalhes.