

Nova Permissão de Segurança

O sistema de permissões de segurança é um mecanismo de autenticação e autorização de usuários. Usuários podem fazer login com as informações contidas no Banco de Dados ou podem usar um provedor de login externo. Os provedores de login externo suportados incluem o Active Directory, OpenID-connect, Facebook, Google, Microsoft Account, Twitter, Github, Certificados digitais e ICP Brasil, podendo também ser personalizado para qualquer provedor de login externo compatível com OAuth 2.0.

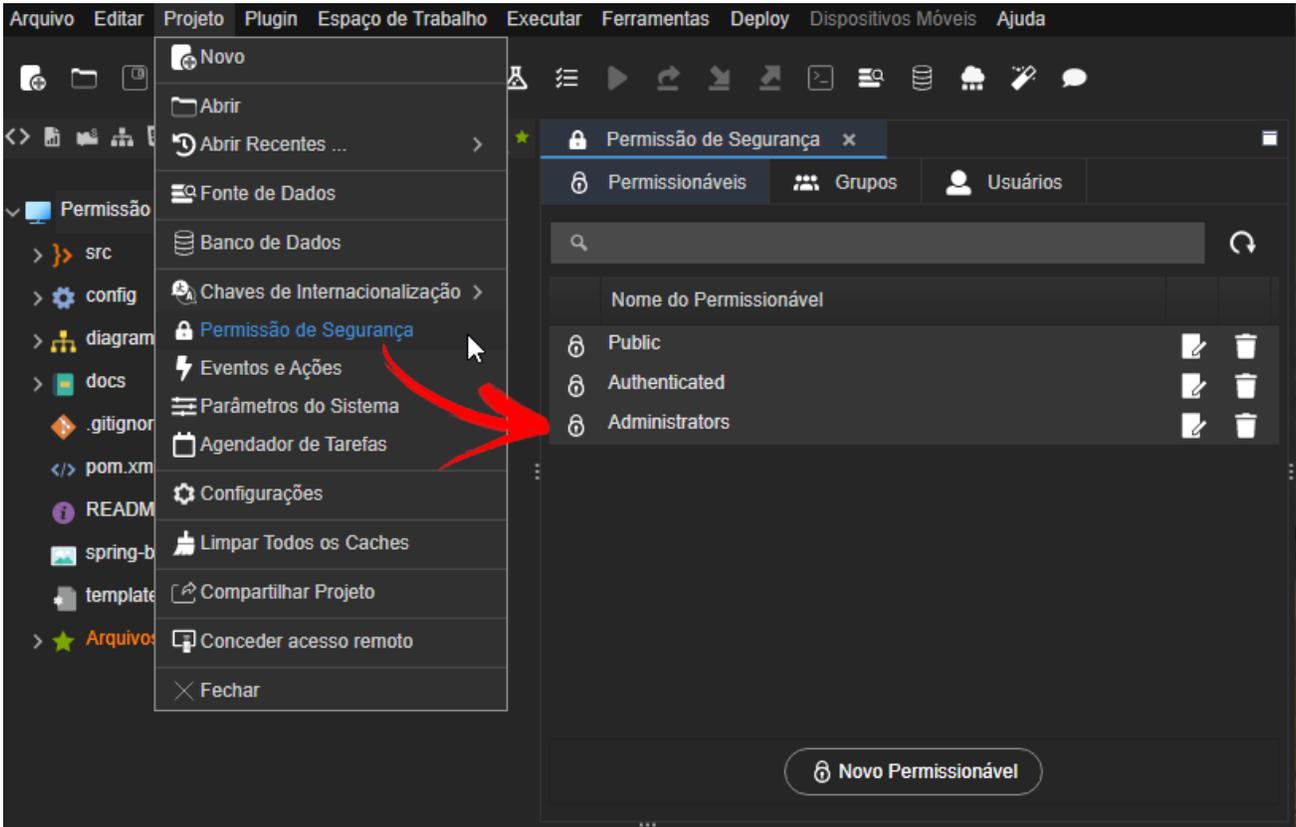


Figura 1 - Acesso a nova janela de permissões de segurança

Modelo de dados das permissões de segurança

Por padrão, o sistema de permissões e segurança armazena informações de usuário em um banco de dados usando o JPA. Para muitos aplicativos, essa abordagem funciona bem. No entanto, você pode preferir usar um mecanismo de persistência ou esquema de dados diferente, tornando o modelo extensível e personalizável.

Diagrama de dados

O modelo de dados das permissões de segurança é representado pelo seguinte diagrama de dados:

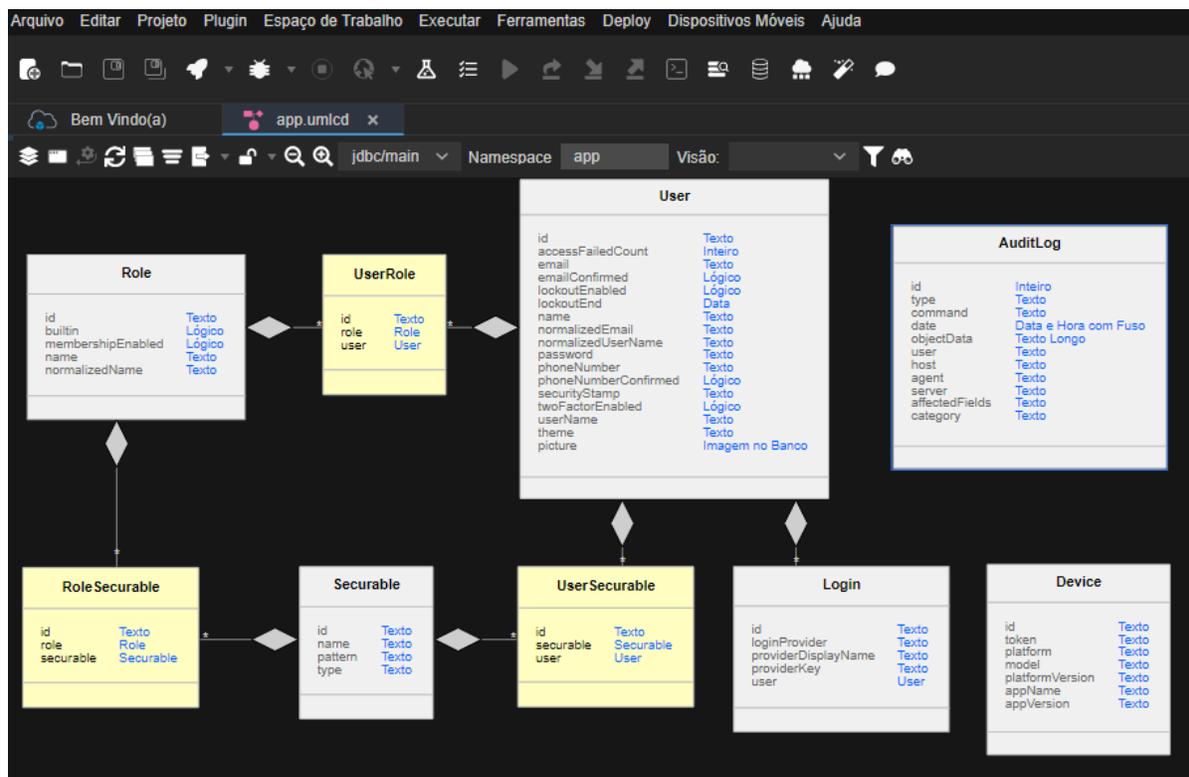


Figura 2 - Tabelas geradas junto com o sistema

Tipos de Entidade

O modelo de dados das permissões de segurança consiste dos seguintes tipos de entidade (Figura 2):

Nome da Entidade	Descrição
User	Representa um usuário
Role	Representa um papel
Login	Representa um login e seu provedor para um usuário
Securable	Representa um conjunto de objetos ao qual você quer aplicar controle de acesso
View	Representa um objeto do tipo View ao qual você quer aplicar controle de acesso
RoleSecurable	Associa um conjunto de objetos a um papel, permitindo que todos os usuários contidos em um papel tenham acesso a esse conjunto de objetos
UserSecurable	Associa um conjunto de objetos a um usuário, permitindo que o usuário tenha acesso a esse conjunto de objetos
UserRole	Associa um usuário a um papel

Relacionamentos dos tipos de entidade

Os tipos de entidade são relacionados entre si das seguintes formas:

- Cada User pode ter múltiplos Securables associados, e cada Securable pode estar associado a múltiplos Users. Esse relacionamento muitos-para-muitos é representado pela entidade UserSecurable.
- Cada User pode ter múltiplos Logins associados.
- Cada User pode ter múltiplos Roles associados, e cada Role pode estar associada a múltiplos Users. Esse relacionamento muitos-para-muitos é representado pela entidade UserRole.
- Cada Role pode ter múltiplos Securables associados, e cada Securable pode estar associado a múltiplos Roles. Esse relacionamento muitos-para-muitos é representado pela entidade RoleSecurable.
- Cada Securable pode ter múltiplos Views associados.

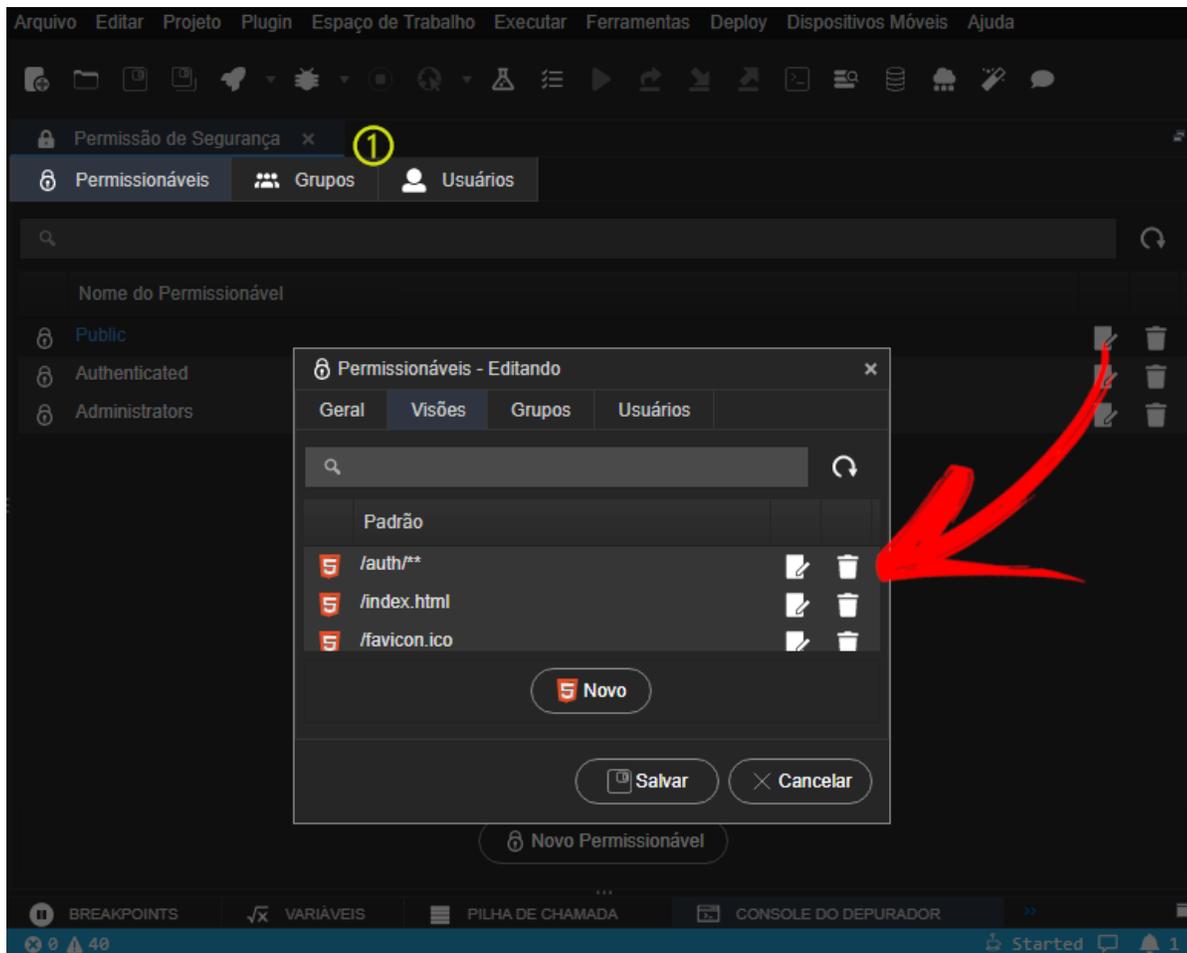
Personalizando as permissões de segurança

Por padrão, as permissões de segurança podem ser personalizadas durante o desenvolvimento da aplicação e durante a sua execução.

Durante o desenvolvimento, acesse o menu Projeto > Permissão de segurança (Figura 1).

Tela principal do sistema de permissão de segurança

A tela principal do sistema de permissão de segurança é composta das abas (item 1 figura abaixo) de Permissionáveis (Securable), Grupos (Role) e Usuários (User).



Permissionáveis

Mostra os perfis de permissões do projeto, podendo editar ou adicionar novos perfis. Por padrão, o Cronapp cria automaticamente os perfis: Public, Authenticated e Administrators.

Ao editar um dos permissionáveis (figura 3), é possível editar seu nome (aba Geral), adicionar diversas permissões na camada de view (aba Visões), definir os grupos de usuários que pertencem a esse perfil (aba Grupo) ou selecionar os usuários individualmente (Usuários),

Grupos

Figura 3 - Configuração dos Permissionáveis

As permissões dadas a um Grupos de acesso serão passadas aos usuários que estão vinculados a esse grupo,

Nas configurações de um grupo é possível: alterar o nome, indicar se o grupo pode ter membros e se o grupo é predefinido. Além disso, a aba Usuários (nas configurações do grupo) permite selecionar os usuários para esse grupo.

Por padrão, o Cronapp possui os grupos Administrators (administradores do sistema), Anonymous Users (usuários não logados) e Authenticated Users (usuários logados).

Usuários

Os usuários cadastrados podem receber permissões específicas ou ser adicionado em grupos.

