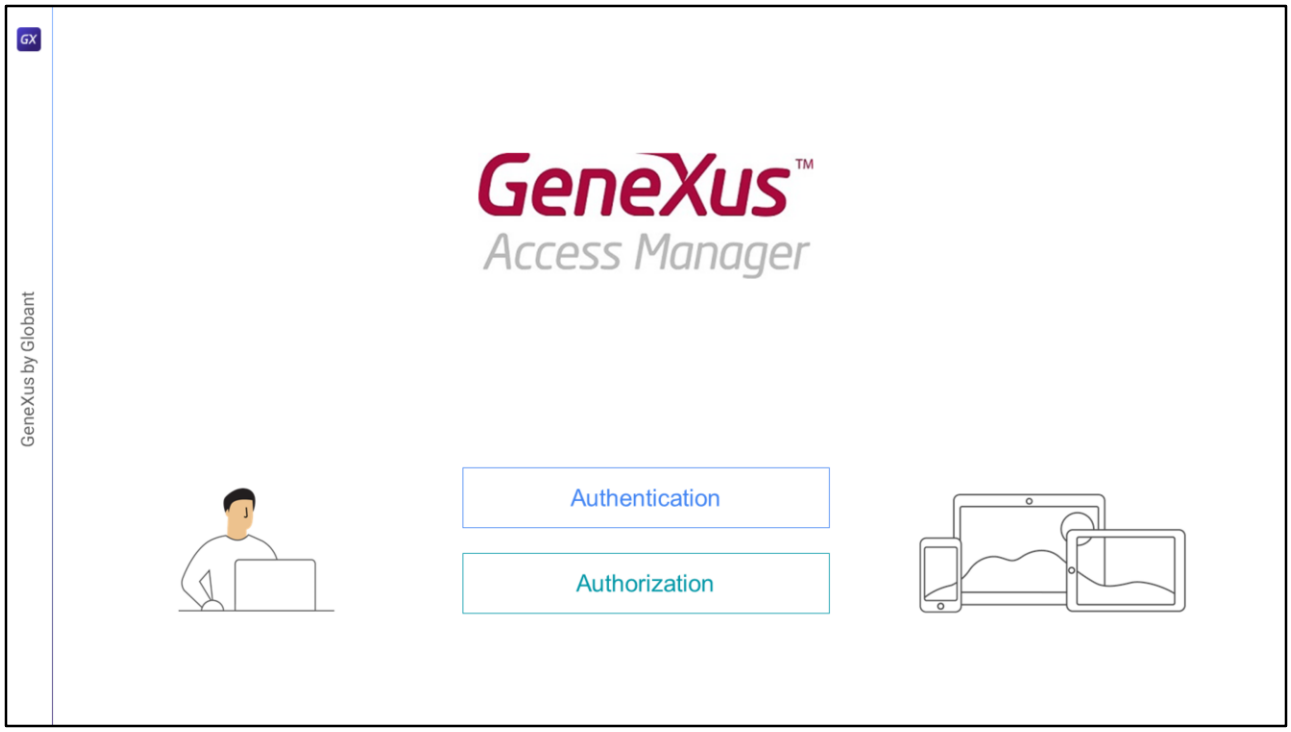
GeneXus by Globant

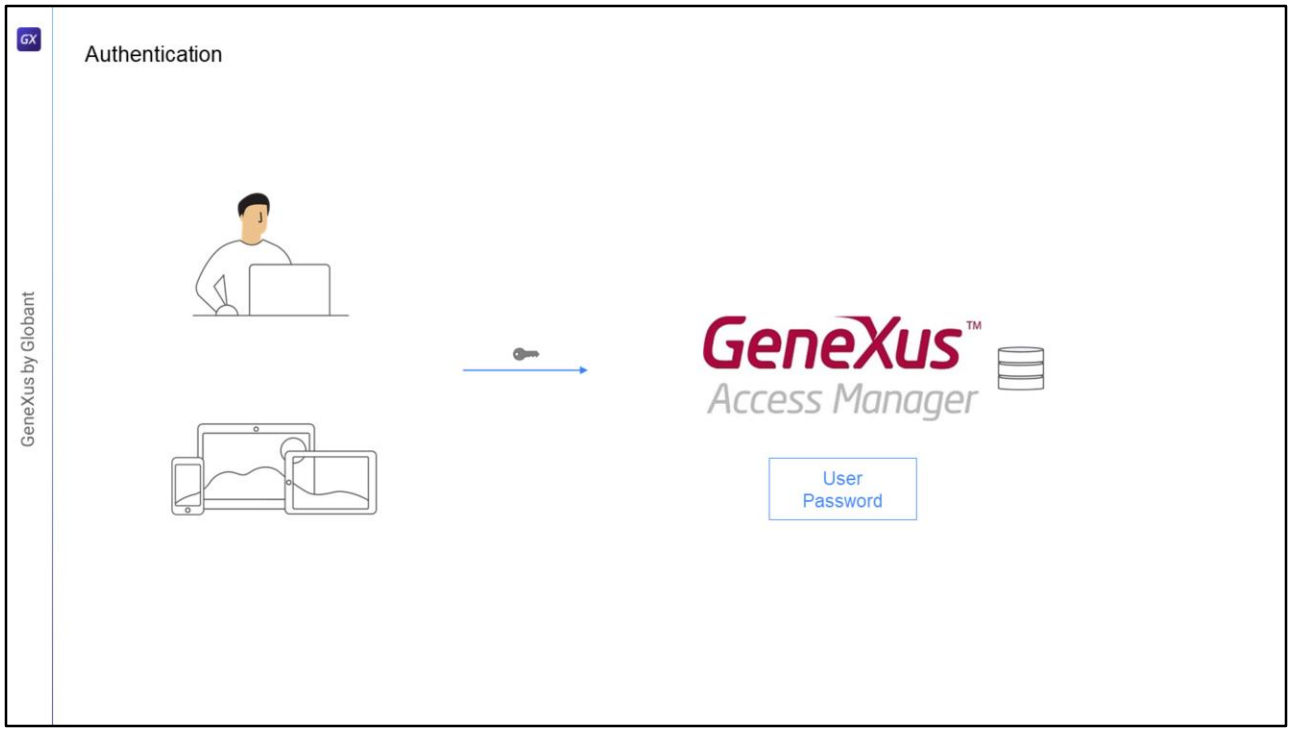
GeneXus Access Manager

Authentication and Authorization

Diego Marranghello



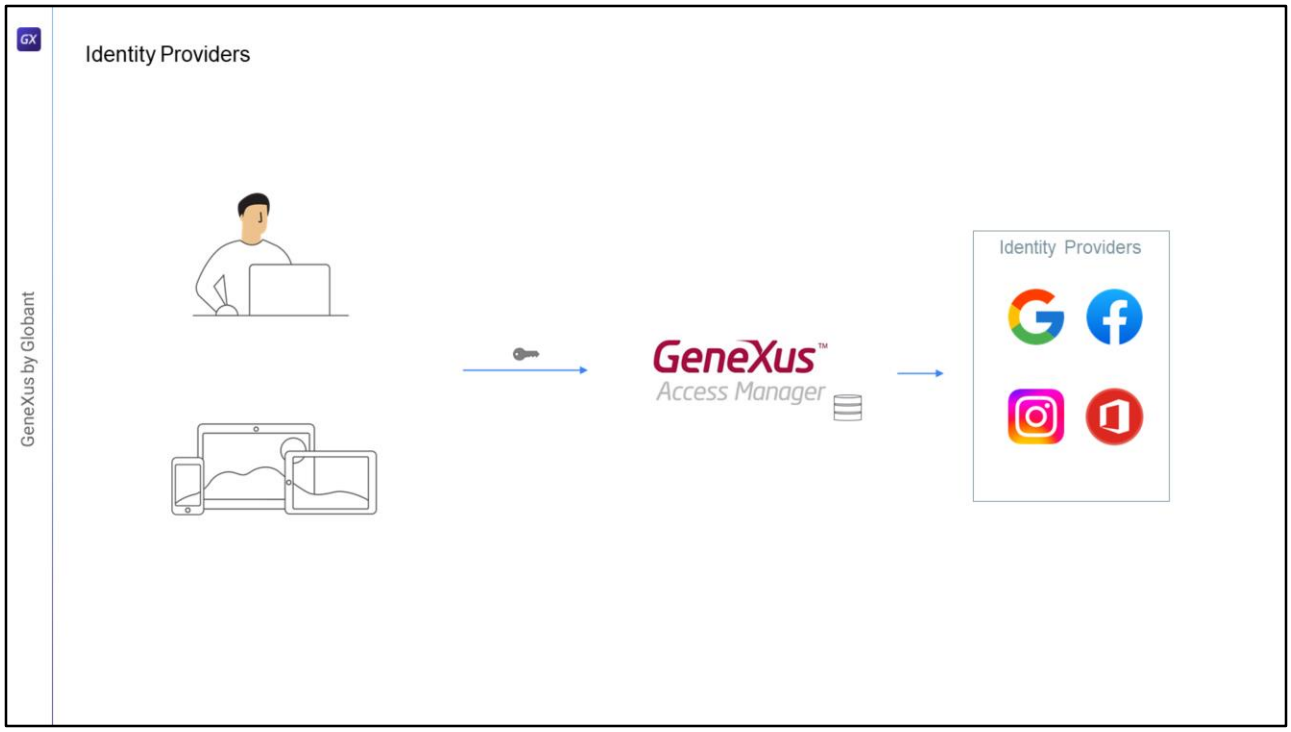
Neste vídeo veremos um pouco mais sobre as características de Autenticação e Autorização utilizadas no GAM.



A autenticação é o processo de verificar se um usuário é quem diz ser, através da validação de suas credenciais, no caso do GAM: usuário e senha.

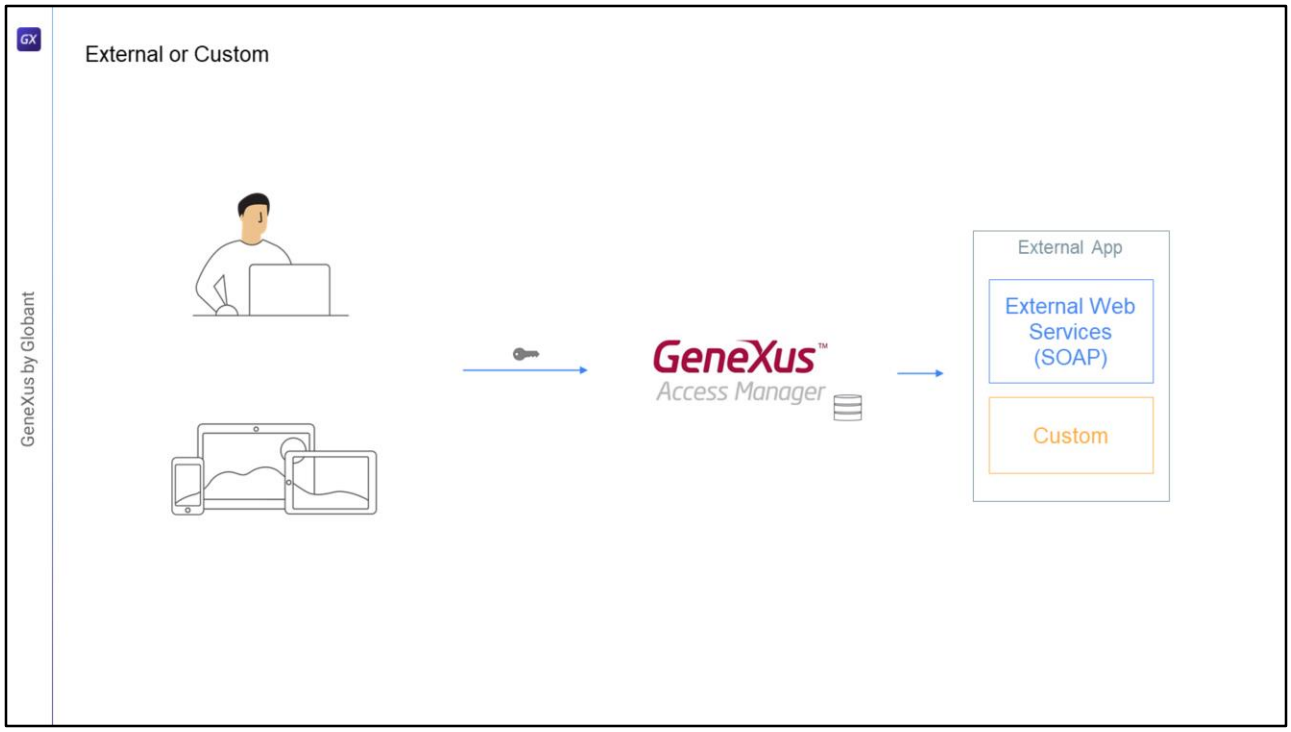
É possível implementar diferentes tipos de autenticação, inclusive podem ser habilitados mais de um simultaneamente.

Os tipos são:
Local: Onde as credenciais do usuário estarão armazenadas na base de dados do GAM na tabela de usuários.



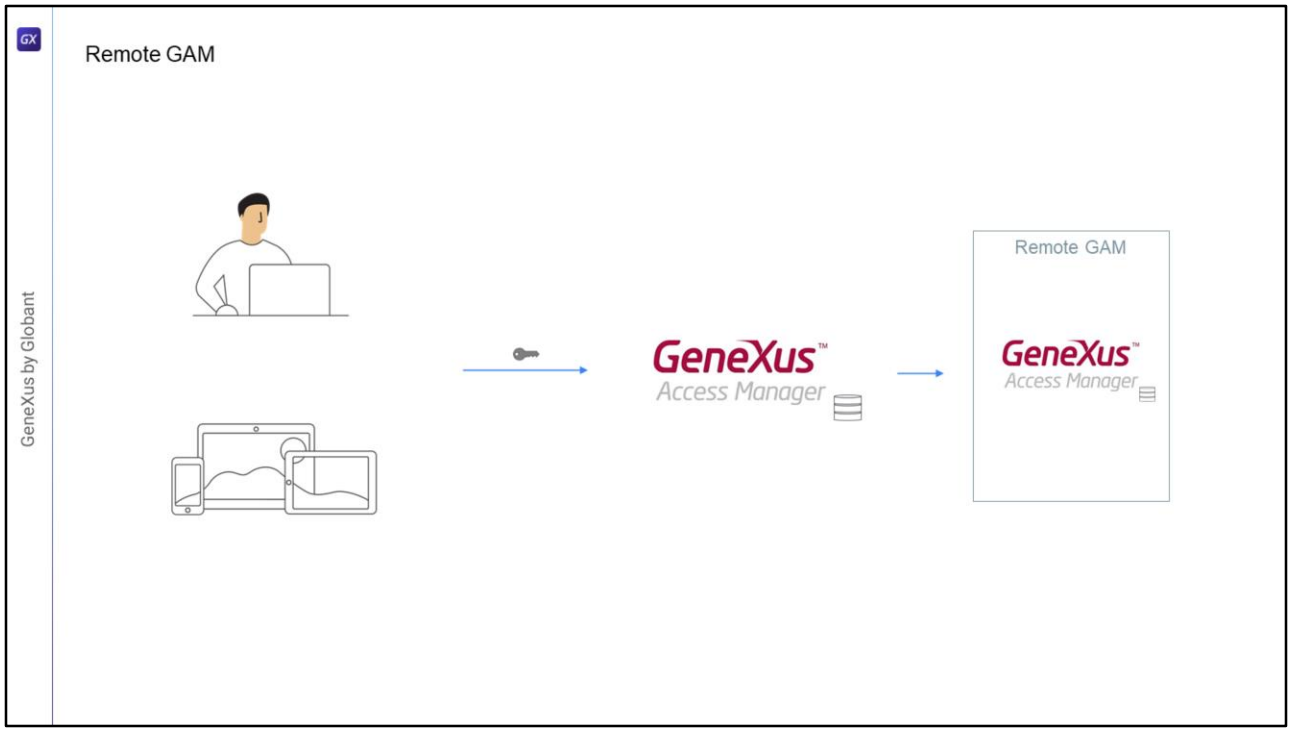
Outra opção é Utilizando um Provedor de Identidade: os Identity Providers que podemos utilizar são vários, por exemplo Google, Facebook, Instagram, Office 365, etc., nestes casos na base de dados do GAM só estará armazenado o ID do usuário na tabela de usuários e isso é utilizado para atribuir, por exemplo, a ROLE a um usuário, e então as credenciais do usuário serão gerenciadas pelo Identity Provider escolhido.

No momento de autenticar o usuário, ele será redirecionado para o provedor de identidade, onde o usuário irá inserir suas credenciais e em caso de sucesso, este provedor retornará ao site novamente.

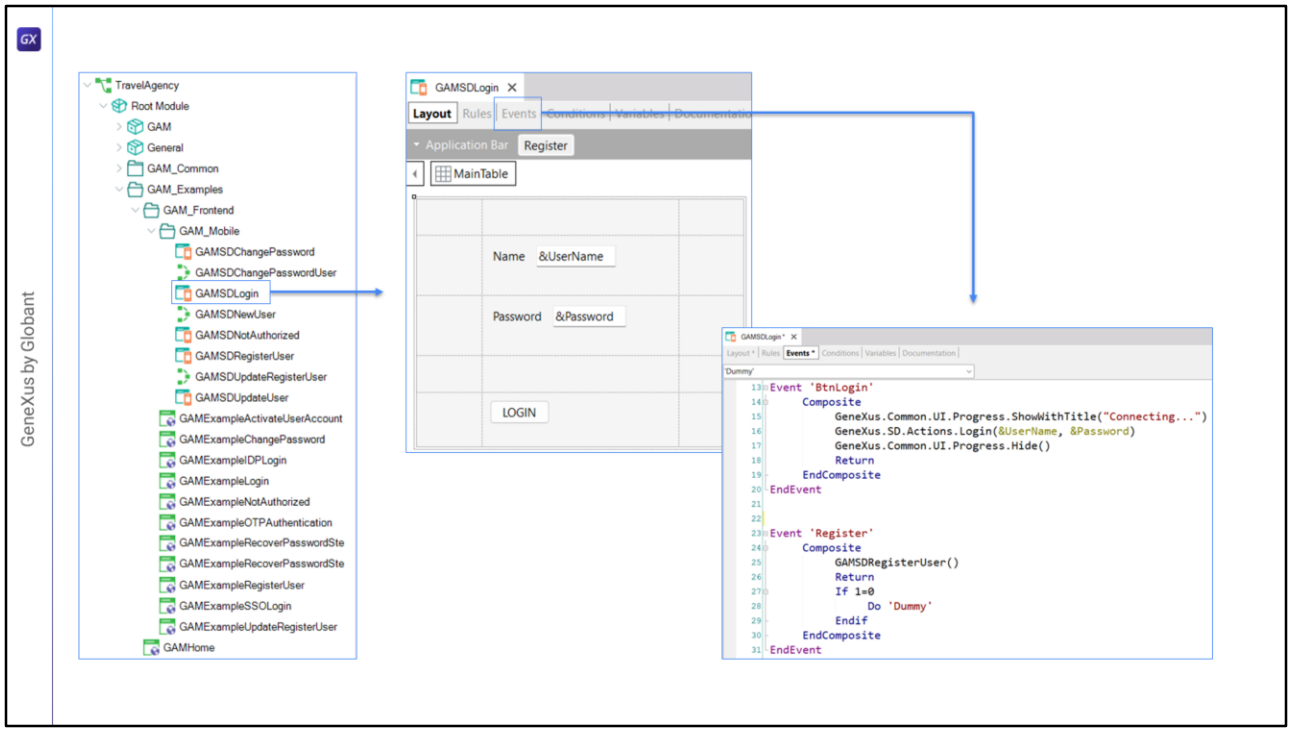


Se utilizarmos autenticação Externa, deve ser configurado o GAM para interagir com um provedor externo, que pode utilizar Web Services ou outro mecanismo personalizado. Neste caso, tal como no anterior, no GAM só é armazenada informação mínima do usuário, uma vez que a validação das credenciais de acesso é realizada em outro sistema.

Nestes casos o GAM nos fornece facilidades para mapear as roles definidas no GAM com as roles externas.



También podemos usar GAM Remoto já que o próprio GAM é um Identity Provider, que irá gerenciar as credenciais do usuário, então podemos configurar que uma aplicação utilizando GAM valide as credenciais do usuário em outra instância do GAM que desempenhará a função de provedor de identidade.

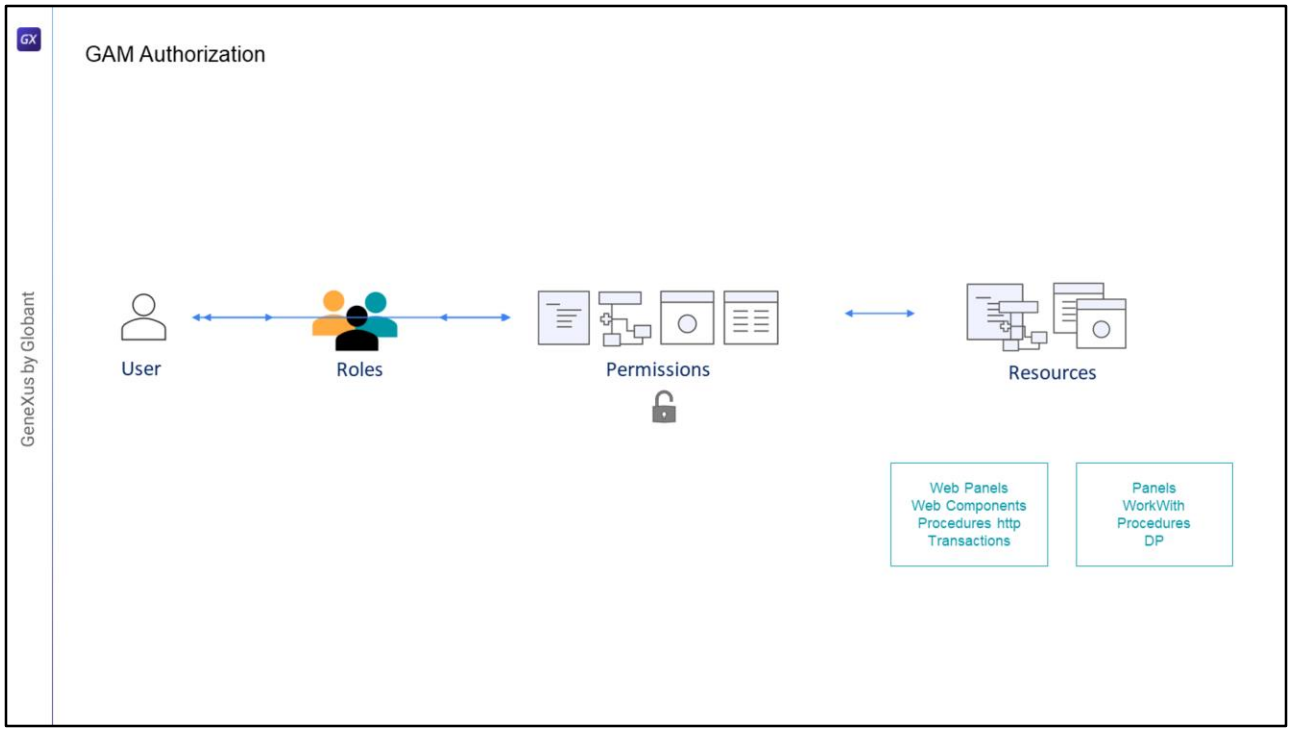


Para realizar a Autenticação, GAM irá nos fornecer dois objetos, um Web Panel, para web, e um Panel, que neste caso utilizaremos para mobile, estes painéis podem ser personalizados se desejarmos.

Em particular, para mobile, dentro da pasta Gam_Examples encontraremos a pasta Gam_FrontEnd e dentro desta outra pasta com nome de GAM_Mobile com objetos que resolvem o Login, a alteração de senha, o registro de novos usuários ou a atualização dos dados do usuário.

Por exemplo, este é o panel de Login, GAMSDLogin, que implementa eventos para efetuar o login e o registro de novos usuários.

Um aspecto importante deste panel é que quando a aplicação mobile for Offline, este panel deverá ser executado Online, ou seja, o usuário deverá ter uma conexão com o server para poder acessar.



Com GAM também podemos resolver a autorização, que é o processo de verificar se um usuário que já foi autenticado possui as permissões necessárias para realizar alguma ação no sistema.

Para isso, o GAM possui um esquema baseado em Roles de Usuário, cada usuário no GAM tem associada uma ou várias Roles, também teremos os Recursos protegidos e a atribuição de Permissões sobre estes Recursos às Roles.

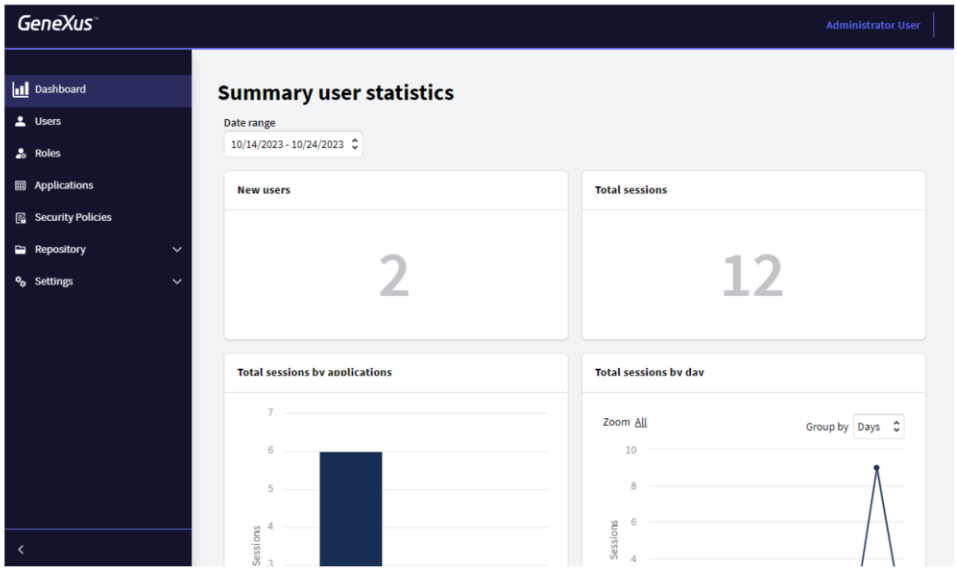
Os recursos que podemos proteger são:
Web Panels
Web Components com acesso por URL habilitado
Processos com Protocolo HTTP, por exemplo relatórios com saída em PDF
Transações, neste caso podemos, além de executar, personalizar também o modo Insert, Update, Delete ou dar acesso Full a uma transação.

No caso de aplicações ONLINE para dispositivos móveis, os recursos a proteger são:
Panels
WorkWith
Processos ou Data Providers com protocolo Rest

No caso de Aplicações para dispositivos móveis Offline teremos apenas a autenticação, pois sendo offline a aplicação, não poderemos manter as permissões, pois se as modificarmos pode ocorrer que alguns dispositivos não sincronizem, inviabilizando o esquema.

GeneXus by Globant

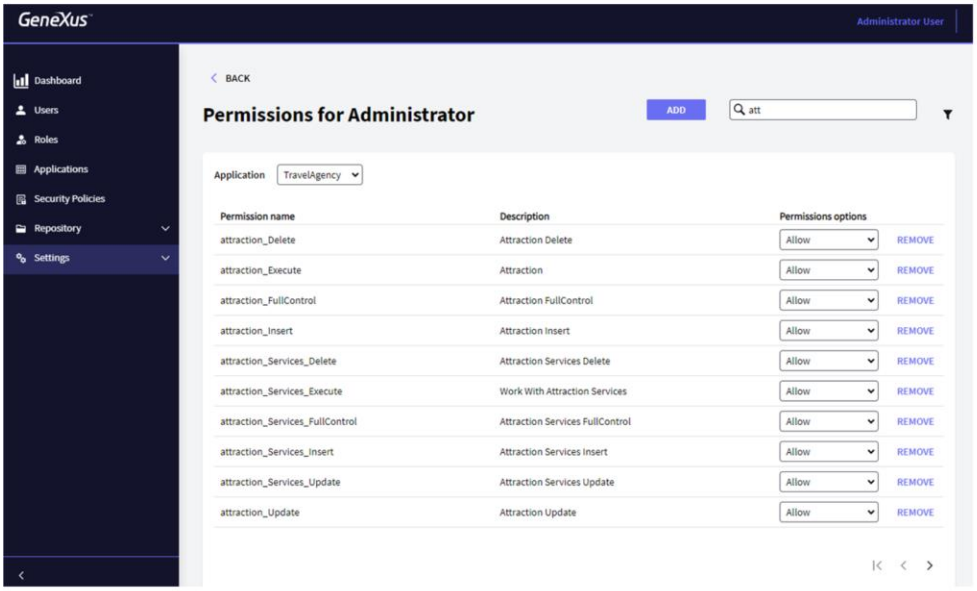
BackOffice Web



Para gerir toda esta informação, GAM fornece um backoffice web, que nos permitirá gerenciar usuários, roles, permissões e outras configurações da aplicação como os tipos de autenticação e outros parâmetros de configuração.

GeneXus by Globant

GAM Authorization: Permissions

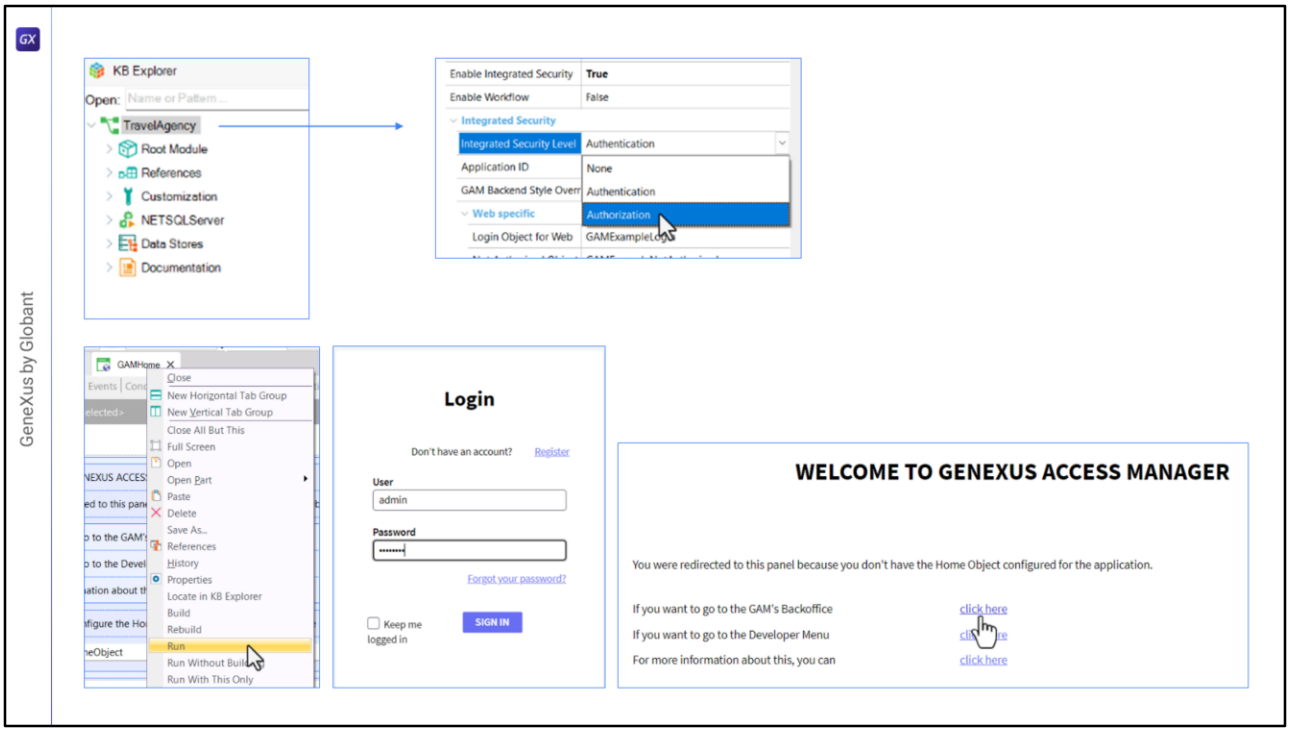


Uma das facilidades que o GAM nos oferece é que para cada aplicação ele será responsável por gerar os recursos sobre os quais há depois que dar as permissões.

Podemos ver que temos por um lado as permissões da transação Atraction, temos uma para cada modo (insert, update e delete), também uma para a execução, e outra que diz FullControl.

Depois vemos também que aparecem recursos com o nome Atraction_Services, estes referem-se à transação quando é utilizada como BC e exposta como REST, ou quando é utilizada no objeto WorkWith

Ao selecionar uma role com FullControl estamos concedendo todas as permissões sobre essa transação, execução e cada um dos modos que serão adicionados automaticamente.



Vamos ver tudo isso que falamos no GeneXus.

Na KB que estamos vendo, já definimos anteriormente a propriedade Enable Integrated security como true, no nó da versão da base de conhecimento.
E deixamos tudo por padrão, então o nível de segurança está em Authentication.

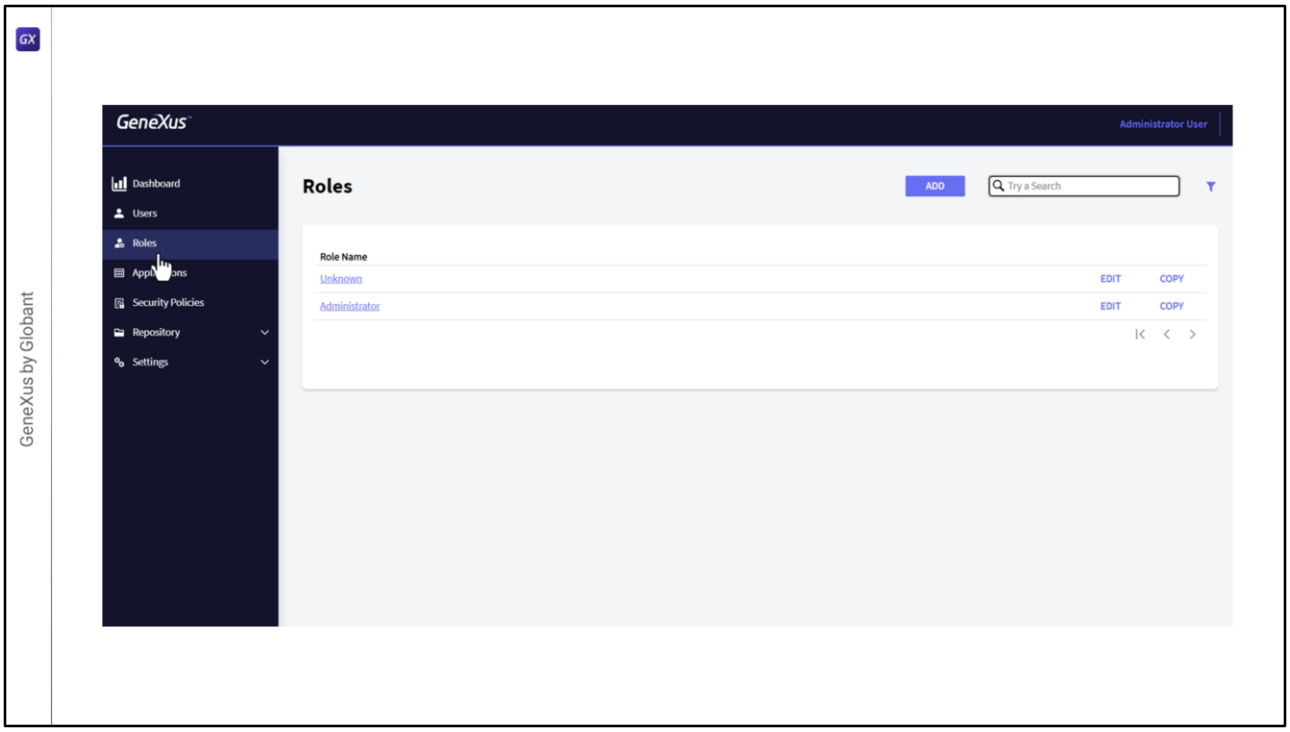
Agora vamos mudar para Authorization, após alterar esta propriedade devemos fazer um Rebuild All da aplicação.

Então agora nossa aplicação está pronta para, além de autorizar, autenticar os usuários, ou seja, gerenciar suas permissões.

Primeiro vamos executar o objeto GAMHome, que deve ter a propriedade main program definida como true para que possamos executá-lo diretamente.

Nos pedirá o login, usamos o único usuário que temos criado por padrão: admin, e a senha admin123.

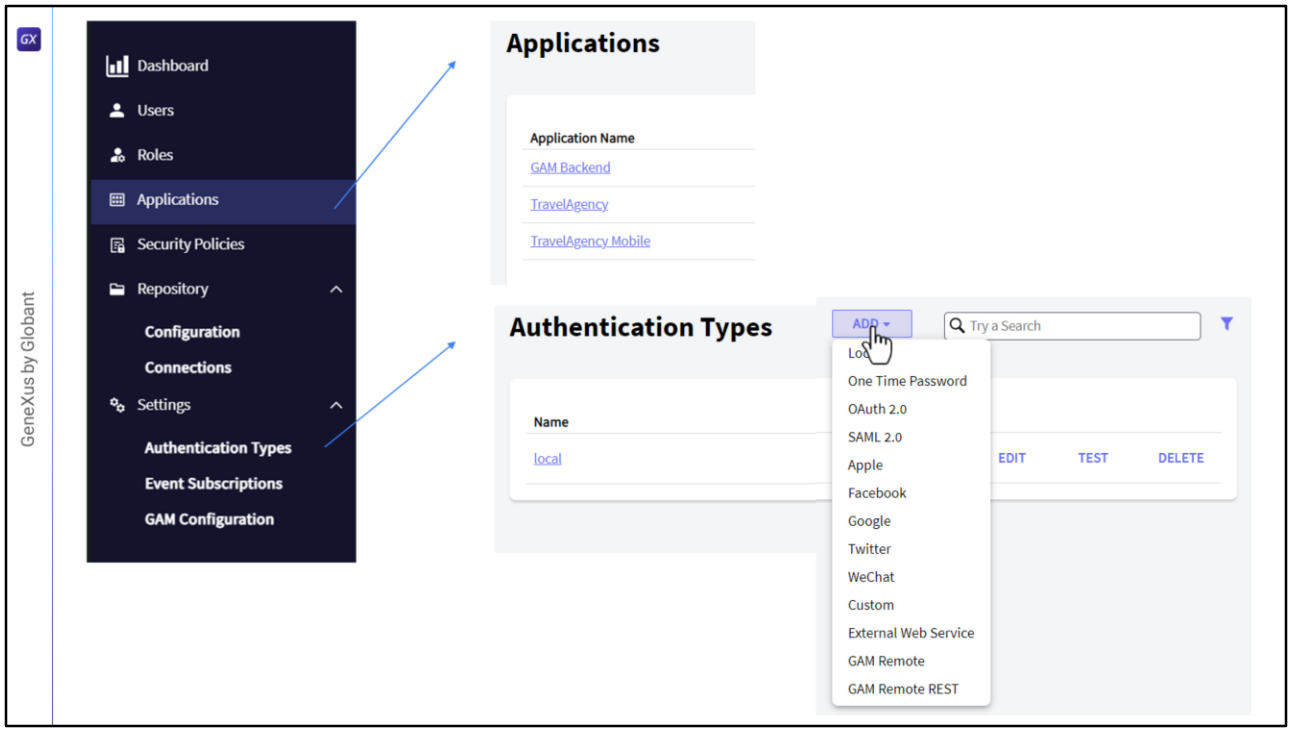
Selecionamos entrar no Backoffice do GAM, vamos para a seção de Usuários, e aqui podemos criar ou editar a informação dos usuários.



Depois temos Roles, aqui podemos definir as roles que queremos, por padrão existem 2 roles definidas, Administrator que tem acesso a todas as funcionalidades tanto do backend quanto permissões sobre todos os objetos do front end.

A outra role é Unknown, esta role serve quando permitimos que os usuários se autorregistrem na aplicação, ou seja, quando os usuários se autorregistram eles ficam associados a esta role.

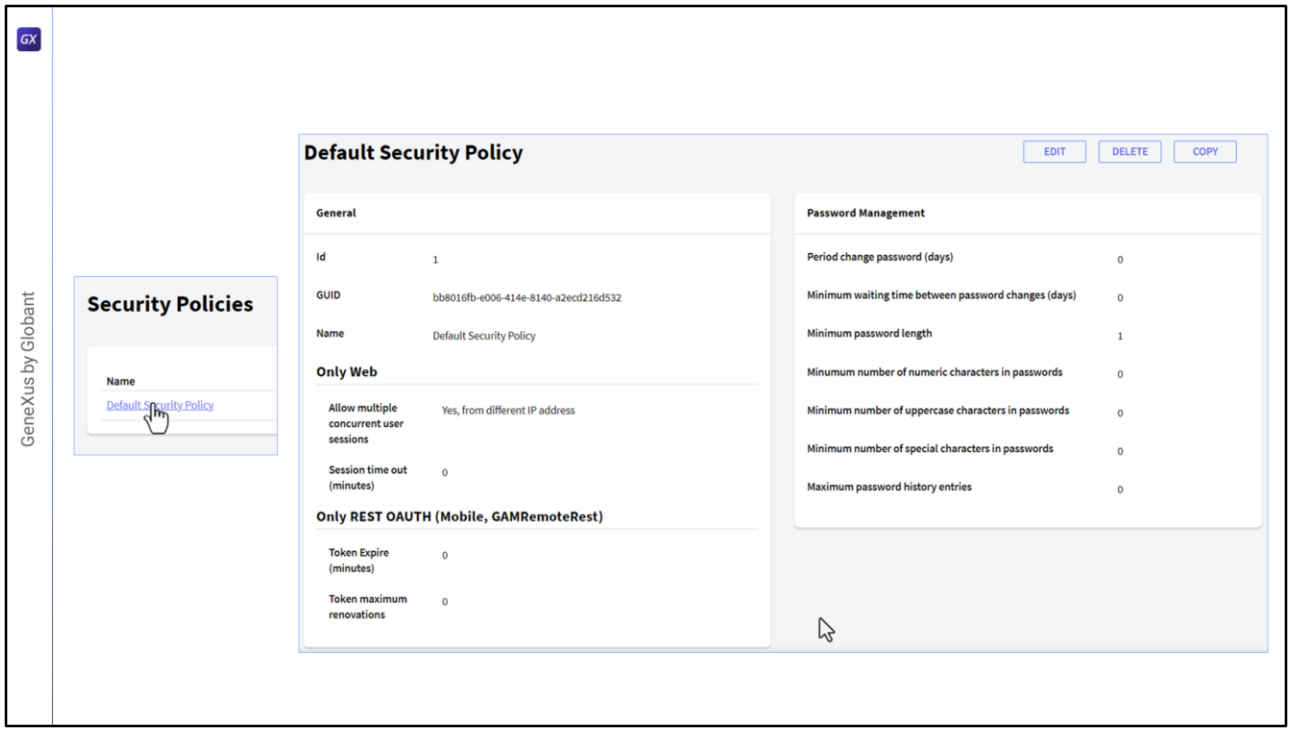
Podemos alterar qual é a role padrão que se usa neste caso.



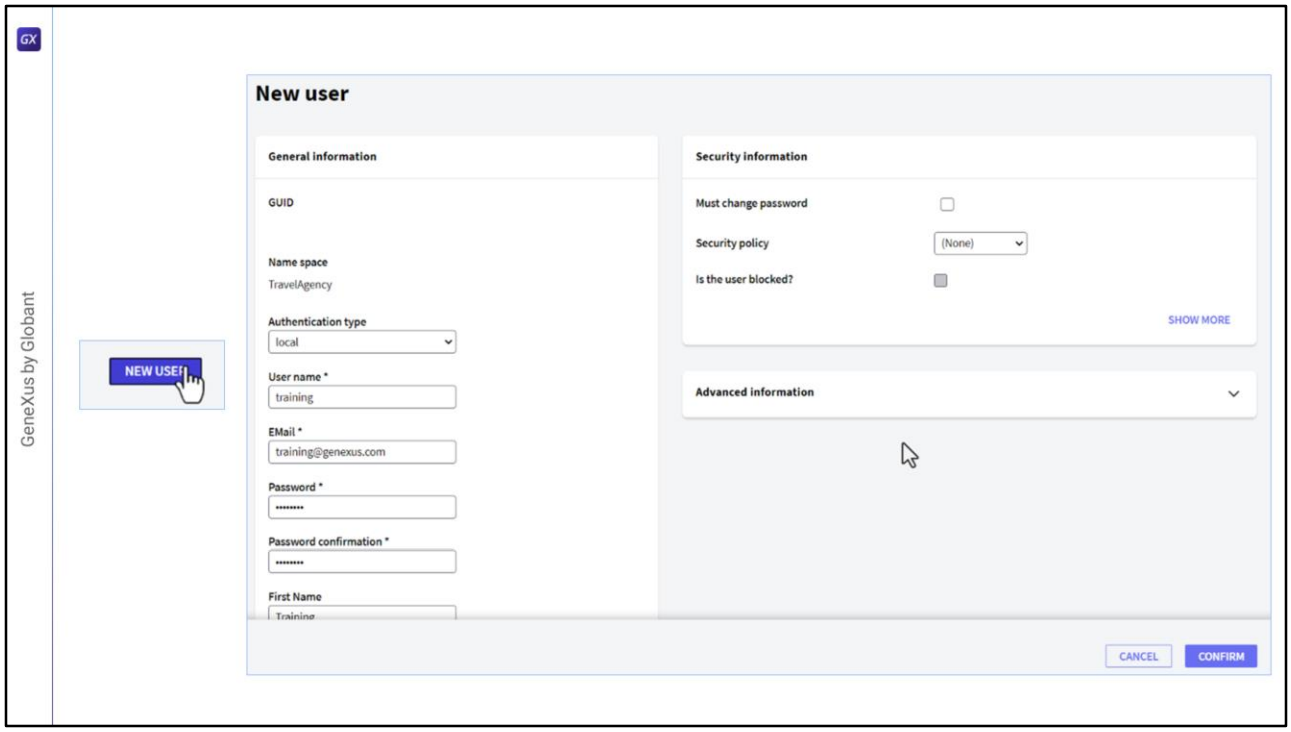
E neste menu temos acesso a toda a configuração do GAM.

Temos as aplicações, vejam que neste caso temos definidas 3 aplicações, a aplicação GAM que tem todo o backend do GAM, a aplicação WEB e a aplicação Mobile, que neste caso ambas têm o mesmo nome, vamos editar e mudar a de mobile para diferenciar.

No menu temos acesso também para configurar, por exemplo, a administração dos tipos de autenticação que vimos, por exemplo é usada a autenticação Local, mas com Add poderíamos adicionar outro tipo, e aqui escolhemos o tipo que queremos adicionar.

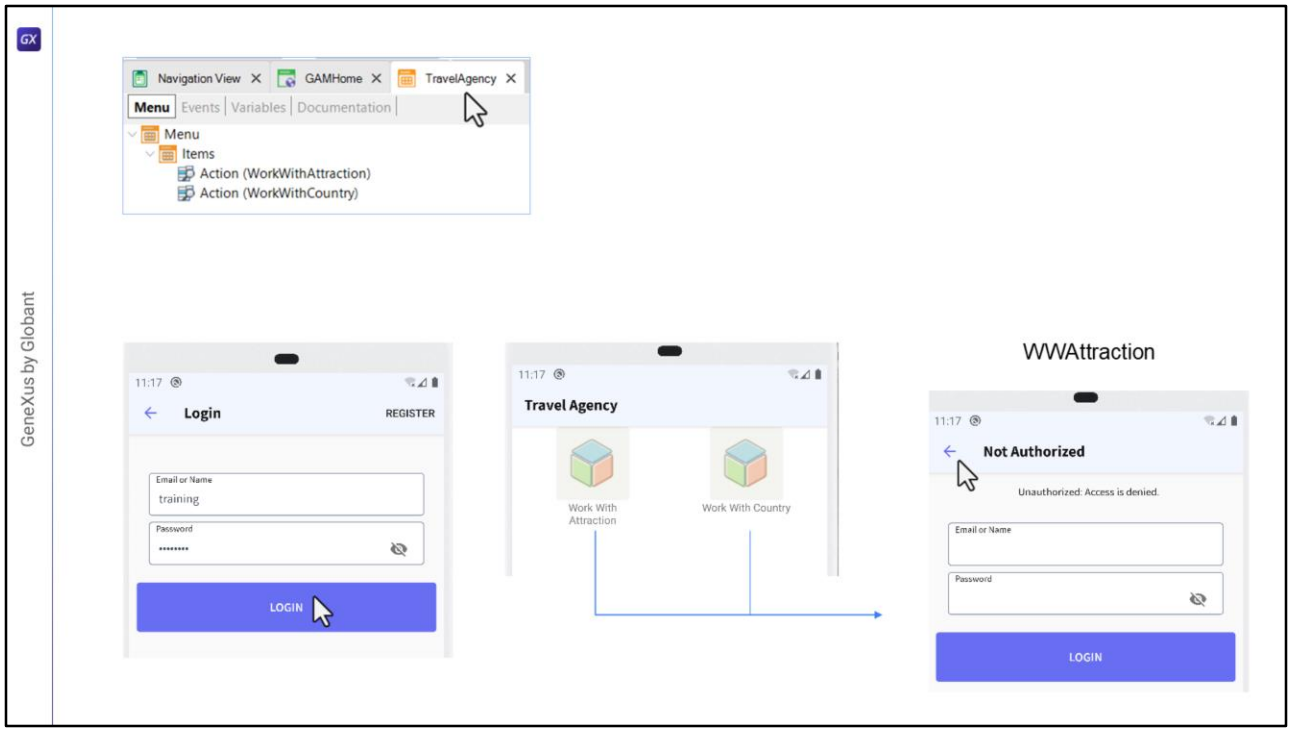


Temos, por exemplo, políticas de segurança, vamos ver como está configurada a política default, por exemplo para mobile podemos escolher o tempo de expiração dos tokens de segurança. Aqui, por exemplo, temos o período em dias para obrigar o usuário a alterar a senha, o comprimento mínimo da senha, etc. Muitos parâmetros que podemos predefinir, e podemos criar várias políticas, uma para usuários do backoffice, outra para usuários mobile, etc., podemos tratar de forma flexível.



Bem, o que vamos fazer é criar um novo usuário.

Vamos em usuários, Adicionar e vamos inserir training como User Name, como e-mail inserimos training@genexus.com, como senha colocamos training, confirmamos novamente a senha, para nome training e sobrenome GeneXus, o restante deixamos tudo por default, atribuímos uma política, a única que temos e confirmamos.



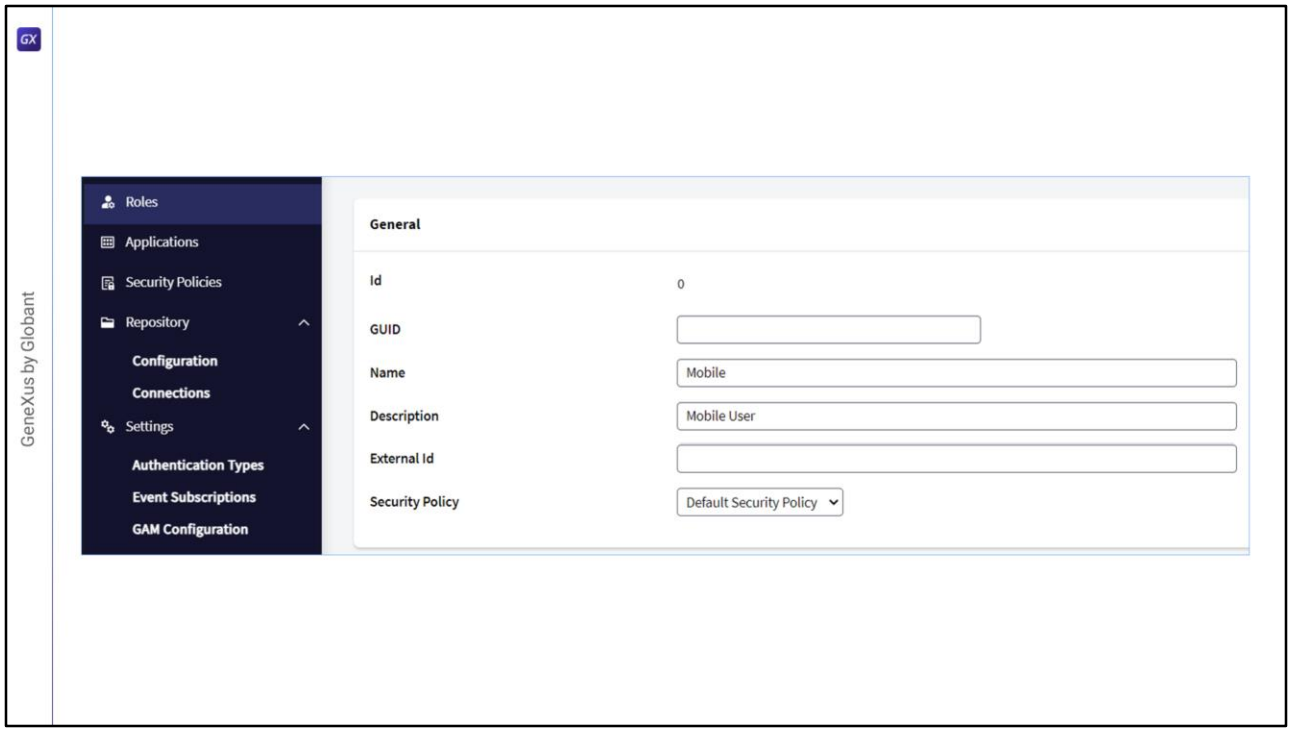
Em nossa KB, criamos um objeto Menu, declarado como startup object, e que tem os seguintes objetos WorkWith como Items, o de país e o de atração.

Ao executar, abre a aplicação no emulador, e a primeira coisa que nos pede são as credenciais de acesso.
Inserimos o usuário que acabamos de criar: usuário training e mesma senha.

E aí permite o acesso ao menu com os itens que havíamos inserido. Neste caso, o menu não requer permissões especiais, somente se o usuário estiver autenticado podemos visualizá-lo.

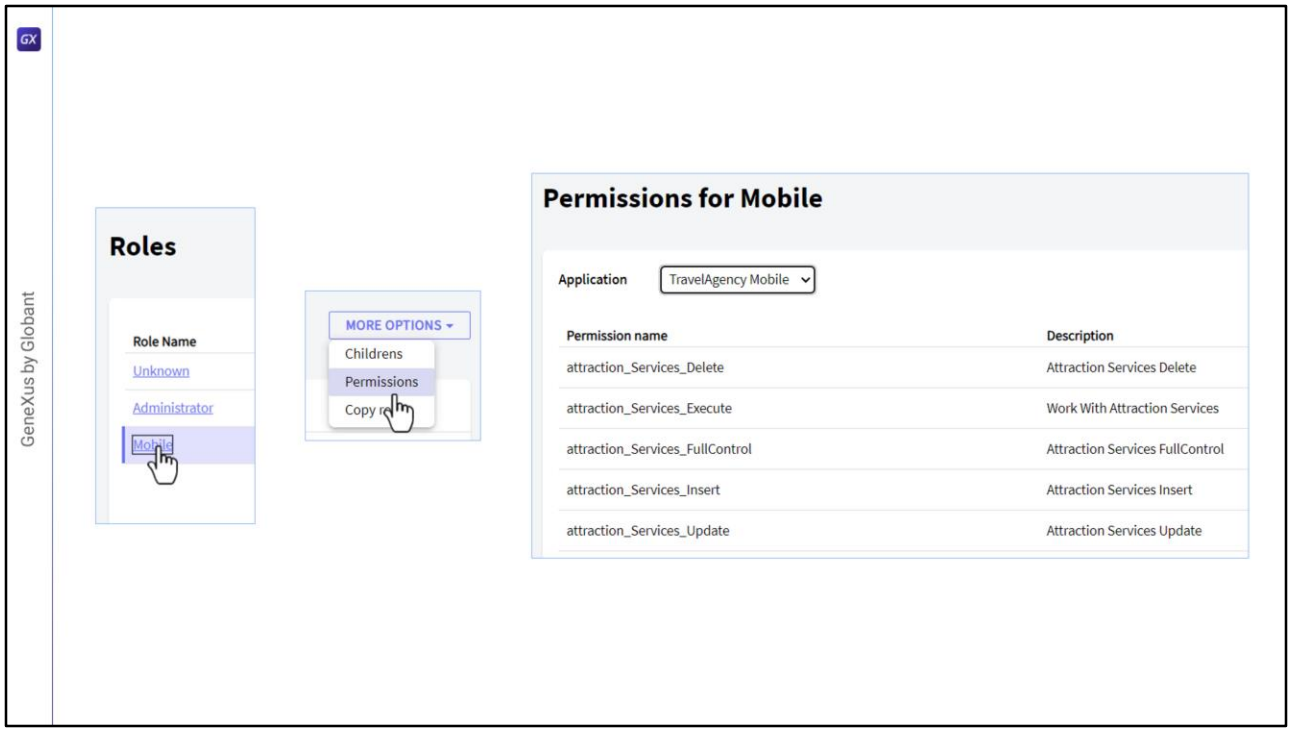
Mas se quisermos acessar as opções, por exemplo as Atrações, dá acesso não autorizado.
Em países, o mesmo.

Isso ocorre porque configuramos a aplicação para nível de segurança Autorização, mas ainda não demos nenhuma autorização ao usuário, apenas o criamos.



Vamos voltar à tela Web para gerenciar essas permissões.

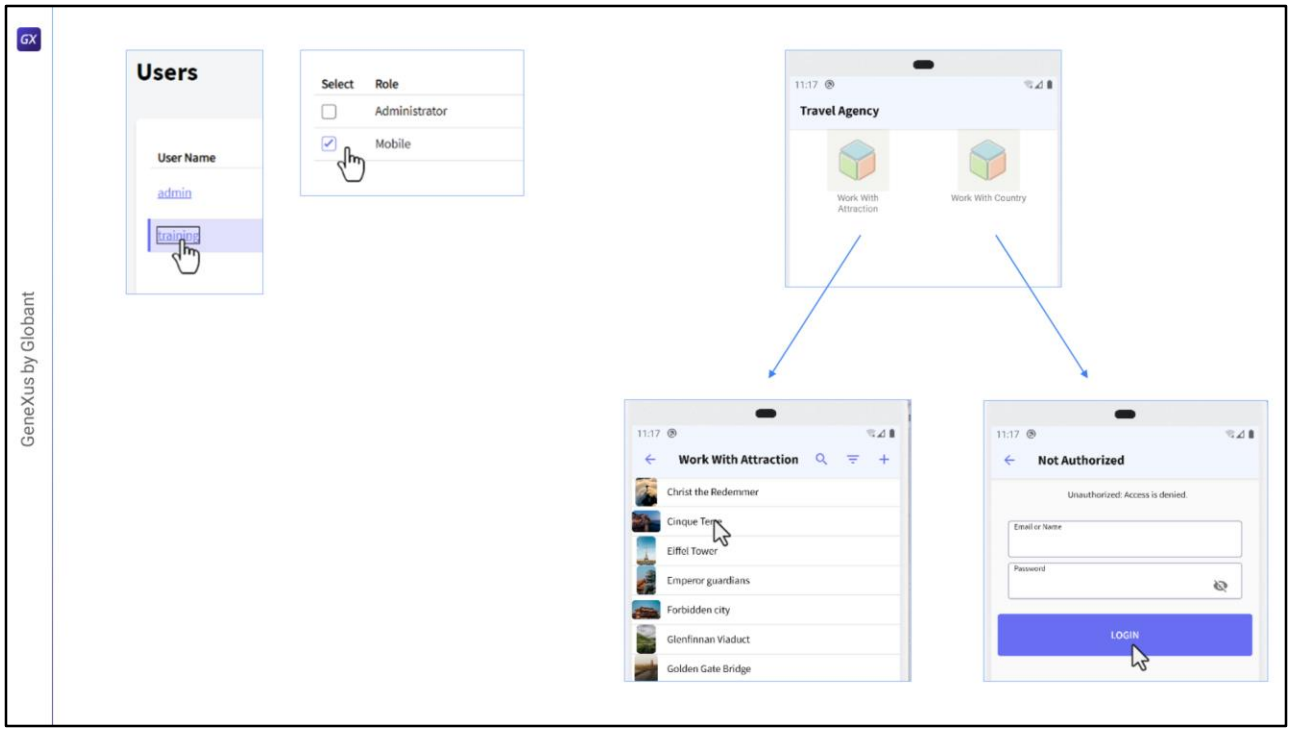
Agora vamos criar uma Role, vamos colocar Role “Mobile”, a descrição Mobile User. Também associamos uma política à Role e confirmamos.



Bem, agora precisamos acessar a Role e conceder permissões sobre alguns recursos.
Selecionamos a aplicação TravelAgency e pressionamos Add.
Ali nos mostra uma lista com todos os recursos sobre os quais podemos dar permissões.

Vamos adicionar uma para acessar as atrações, procuramos atraction, selecionamos Atraction_Services_FullControl.

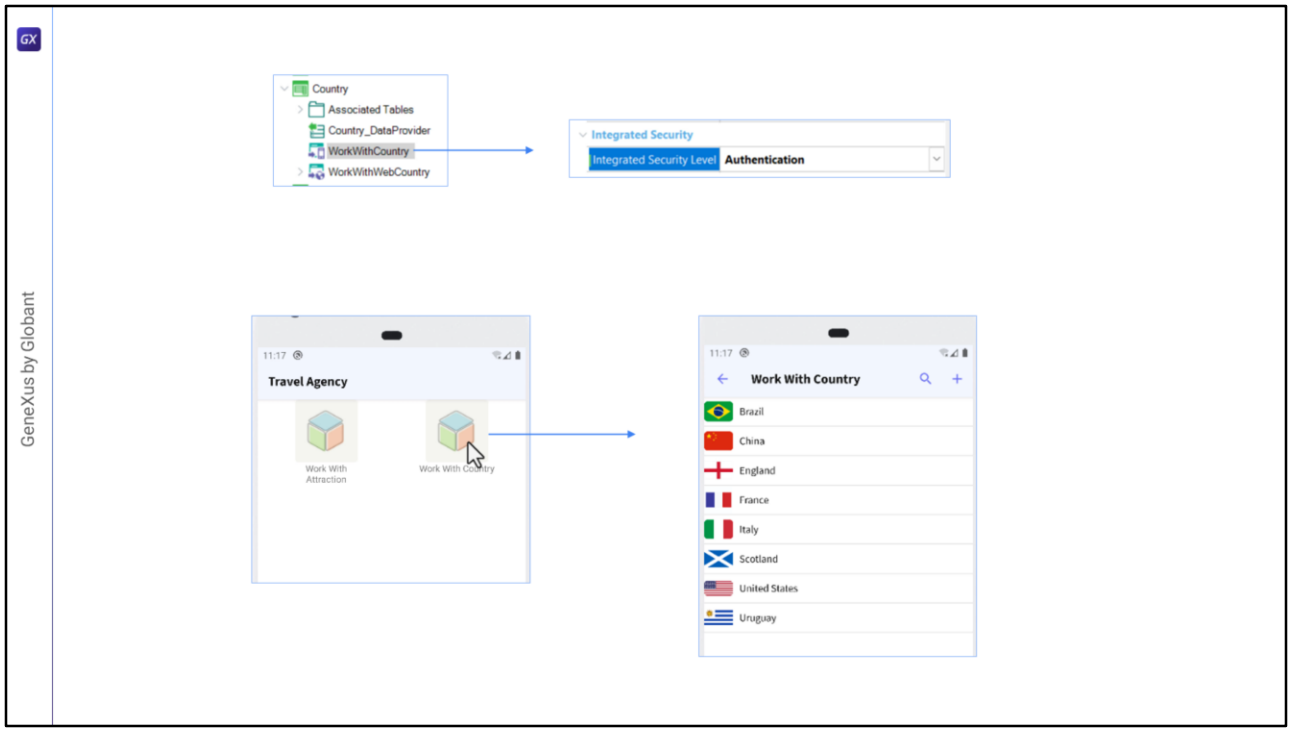
E ao selecionar fullcontrol, vemos que são herdadas todas as permissões sobre as atrações.



Agora vamos associar ao usuário que criamos esta role.
Clicamos no nome de usuário, depois em Roles, na opção Add e selecionamos Mobile.
Add Selected e pronto.

E agora se formos ao emulador e acessarmos as atrações, aí sim nos mostra a lista. E se quisermos, nos permite entrar em modo Insert também, já que lhe demos permissão full.

Agora, se formos a países, nos dá acesso não autorizado, isto ocorre porque para países ainda não demos nenhuma permissão.



Por exemplo, poderíamos querer que para os países não fossem verificadas as permissões, então no WorkWith Country, no nível de segurança, podemos usar a opção de somente autenticação, outra opção seria colocar None.
Vamos executar a aplicação para que assuma essa alteração.

E agora se acessarmos Países, nos mostra a lista.
Bem, esta foi apenas uma pequena amostra de toda a flexibilidade que o GAM nos oferece para lidar com autorização e autenticação dos usuários.
Lembrem-se que a autorização é apenas para aplicações OnLine.


GeneXus by Globant
GeneXus™
by Globant
training.genexus.com