GeneXus by Globant

GeneXus Access Manager

Introduction

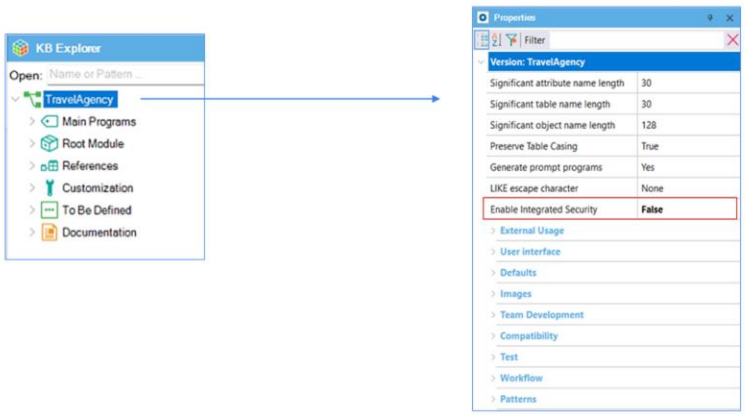
Diego Marranghello

No desenvolvimento de nossas aplicações, existem várias diretrizes de segurança que devem ser levadas em consideração. As mais importantes estão descritas no Open Web Application Security Project, a fundação que gerencia este projeto, que é uma comunidade aberta que define e fornece informações, além de ferramentas, para o desenvolvimento e a verificação de sistemas de computador a partir de uma perspectiva de segurança.

Dentro da fundação existem vários projetos, um dos mais destacados e com maior relevância é o OWASP Top Ten, um documento que trata dos riscos de segurança mais críticos nas aplicações web e móveis. Em um dos pontos do projeto, fala sobre a "Broken Authentication", onde destaca a importância de ter um bom fator de autenticação.

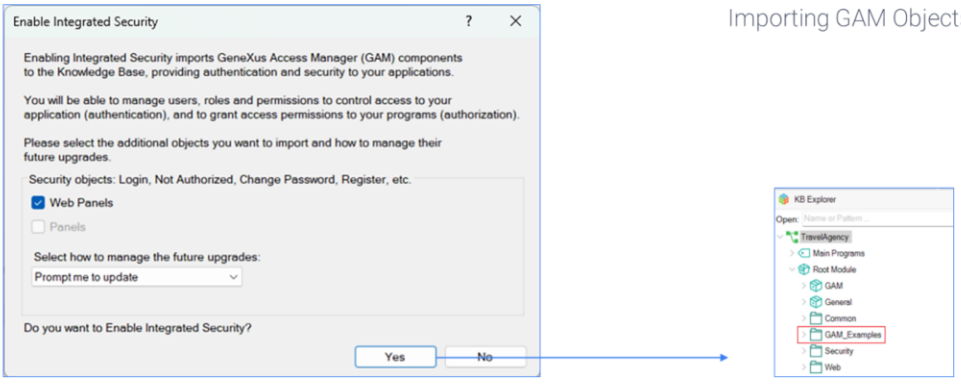
Genexus oferece um módulo denominado "Genexus Access Manager" (GAM) que resolve a autenticação de forma automática. Além desta tarefa, o GAM também permite solucionar problemas de autorização, ou seja, restringir o acesso a diferentes partes da aplicação dependendo das roles ou permissões de cada usuário. O GAM também nos fornece diversos objetos para gerenciar todos os problemas de segurança relacionados com uma aplicação web ou para dispositivos móveis. Por exemplo, objetos que permitem adicionar usuários, atribuir roles, conceder permissões, etc.

Enabled Integrated Security



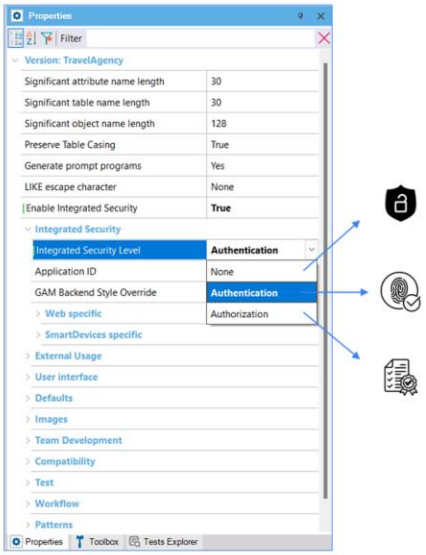
A ativação dos controles de segurança é realizada automaticamente através da configuração da propriedade "Enable Integrated Security" que podemos encontrar na janela de preferências selecionando a versão ativa de nossa KB.

Importing GAM Objects



Ao alterar a propriedade para “True”, serão importados os componentes do Genexus Access Manager para nossa KB. Sob Root Module, encontraremos vários
objetos encarregados de fornecer as funções do GAM.

Integrated Security Level



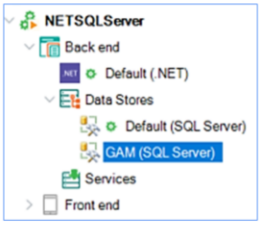
Uma vez habilitada a segurança, é possível selecionar o nível dela utilizando a propriedade "Integrated Security Level" que podemos encontrar no nível da KB ou para cada objeto. O valor padrão desta propriedade é "Authentication". Algumas opções para o nível de segurança de
nossa aplicação são:
Nenhuma, ou seja, não aplica nenhum mecanismo de segurança.
Autenticação, onde o usuário precisa apenas estar logado para acessar.
E autorização, onde o usuário precisa, além de estar logado, ter as permissões necessárias para acessar cada parte da aplicação.

KB

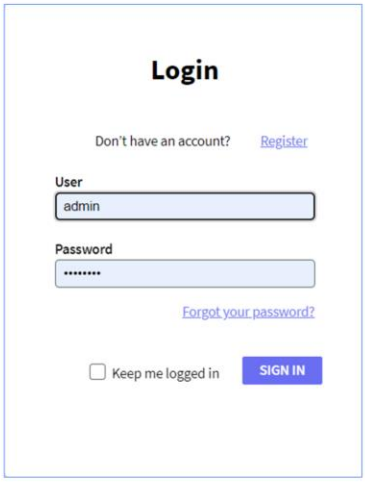
+

GeneXus™
Access Manager

+



Uma vez aplicada a segurança e o tipo de nível que irá utilizar nossa aplicação, precisamos dar um "rebuild all" em nossa KB para que seja criada a base de dados que utilizará o GAM. Depois de ativarmos a segurança, ao executar nossa aplicação, será exibida uma tela de login, tanto para a parte web como para Smart devices.



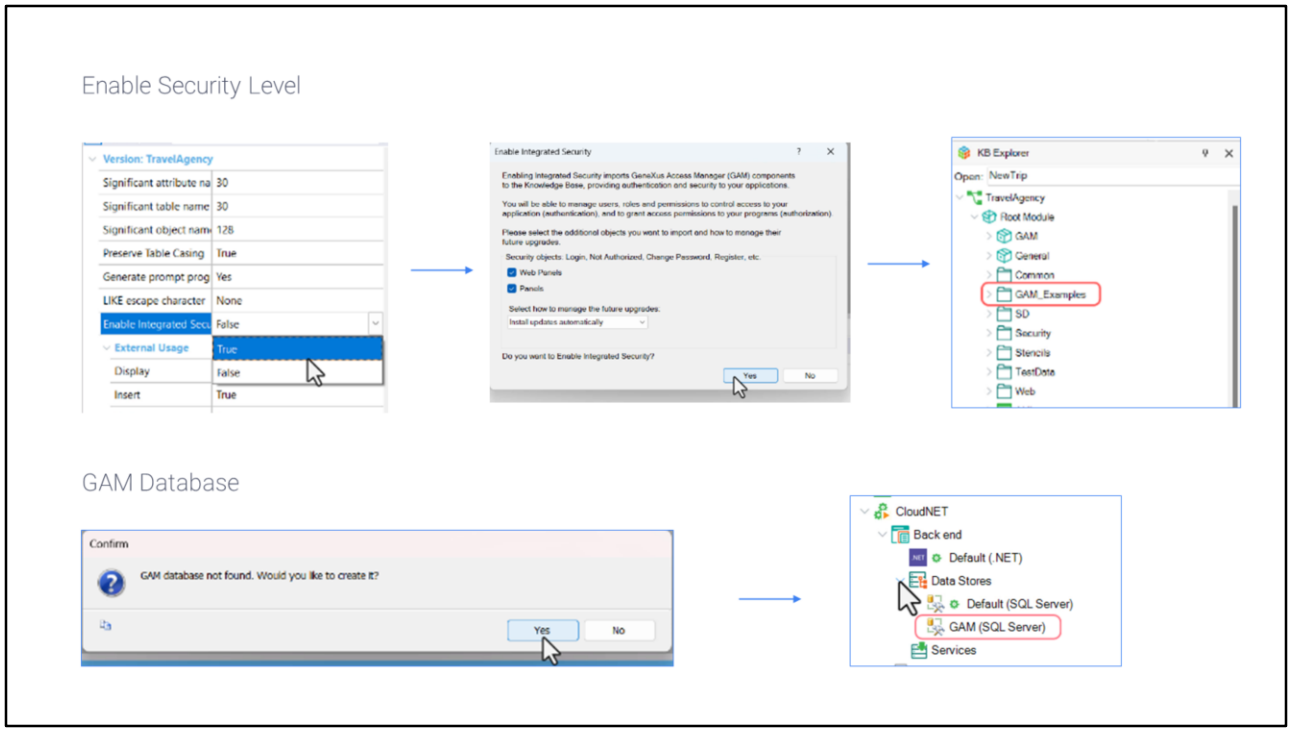
User: admin

Pass: admin123

Como ainda não configuramos usuários, podemos utilizar um usuário local com as seguintes credenciais: usuário: admin e senha: admin123. Para acessar o console de administração do GAM, devemos acessar o panel "GAM Home".

Este panel é o objeto back-end principal do GAM, onde podemos configurar os usuários e as permissões de nossa aplicação. Vejamos uma pequena demonstração.

Em nosso exemplo, queremos que diferentes usuários possam, dependendo de sua role, visualizar nossa aplicação web backoffice. Se eles autenticam, dependendo de sua role, possam ver certas opções.

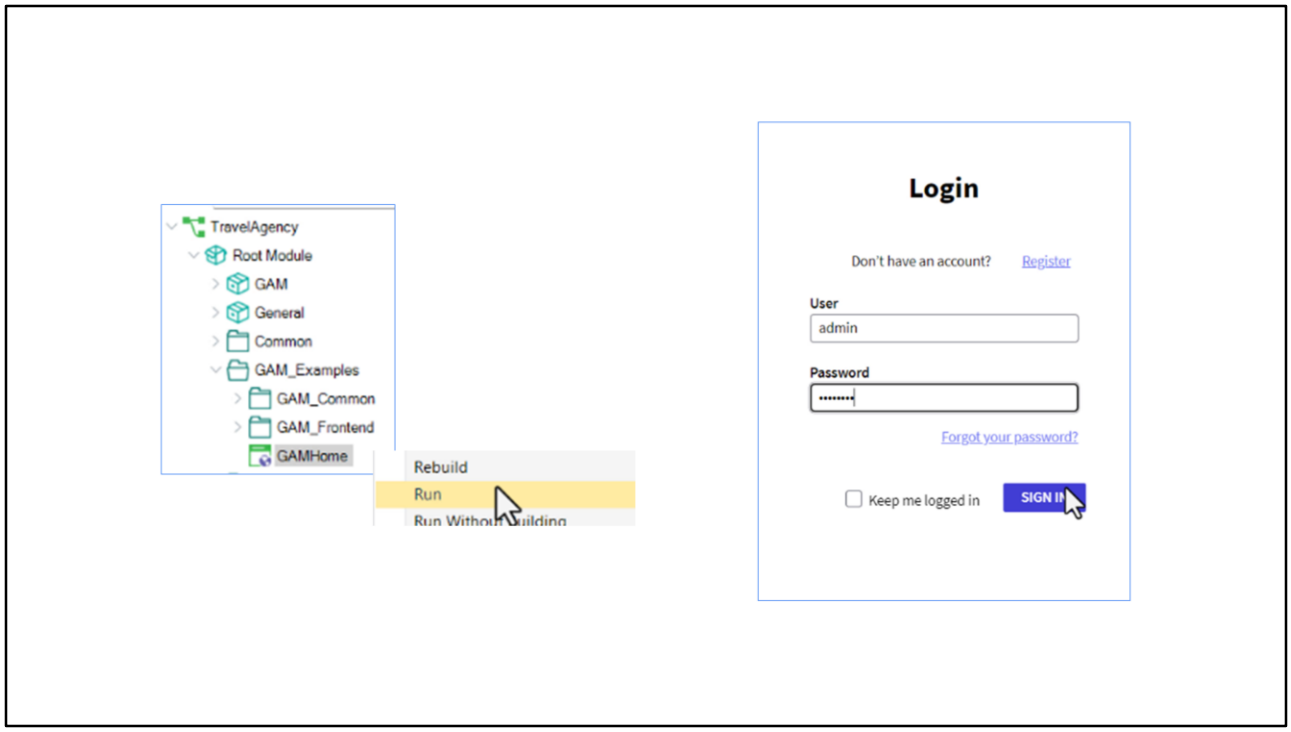


No que segue, aplicaremos o módulo de segurança à nossa KB Travel Agency para resolver isso. Para fazer isso, primeiro nos posicionamos na versão ativa da KB. Posteriormente, alteramos a propriedade "Enable Security" para true. Será exibida uma tela solicitando a permissão para a importação de componentes para a operação do módulo do GAM, tanto para nossa aplicação web quanto para Smart devices.

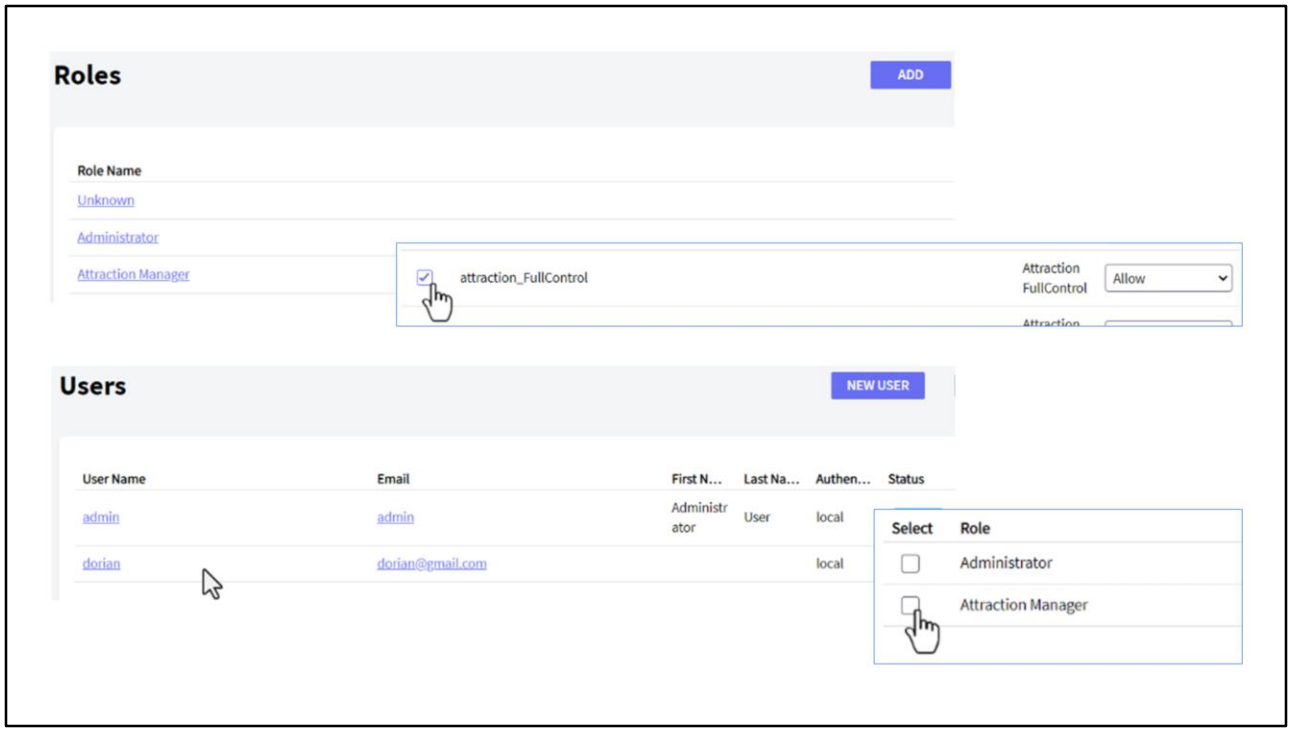
Da mesma maneira, nos concede a possibilidade de escolher a forma de atualizar os referidos objetos, seja automaticamente, que nos pergunte ou que nunca os atualize. Selecionamos que sim e posteriormente serão importados os objetos e podemos encontrá-los na pasta "GAM Example" sob "Root Module ".

No nível geral, mudaremos o nível de segurança para "nenhuma" para que qualquer usuário possa visualizar nossa aplicação. Então, nas propriedades da versão, alteramos uma propriedade chamada "Integrated Security Level". Posteriormente, podemos alterar esta mesma propriedade no nível de objeto. Por exemplo, na transação de "Attraction", alteramos "Integrated Security Level" para "Authorization" para que apenas os usuários autorizados possam acessar.

Lembremos que uma vez que aplicamos o GAM, precisamos fazer um "rebuild" da KB. Isto irá nos pedir para criar a base de dados do GAM. Uma vez realizado, encontraremos um novo Data Store especialmente para o GAM.



Executamos o panel "GAM Home", vamos ao back-end do GAM, que é seu console de administração, para poder adicionar nossos usuários e dar-lhes permissões por meio de sua role atribuída. Acessamos utilizando o usuário padrão (admin) e sua senha "admin123", lembrando que podemos alterá-la posteriormente.



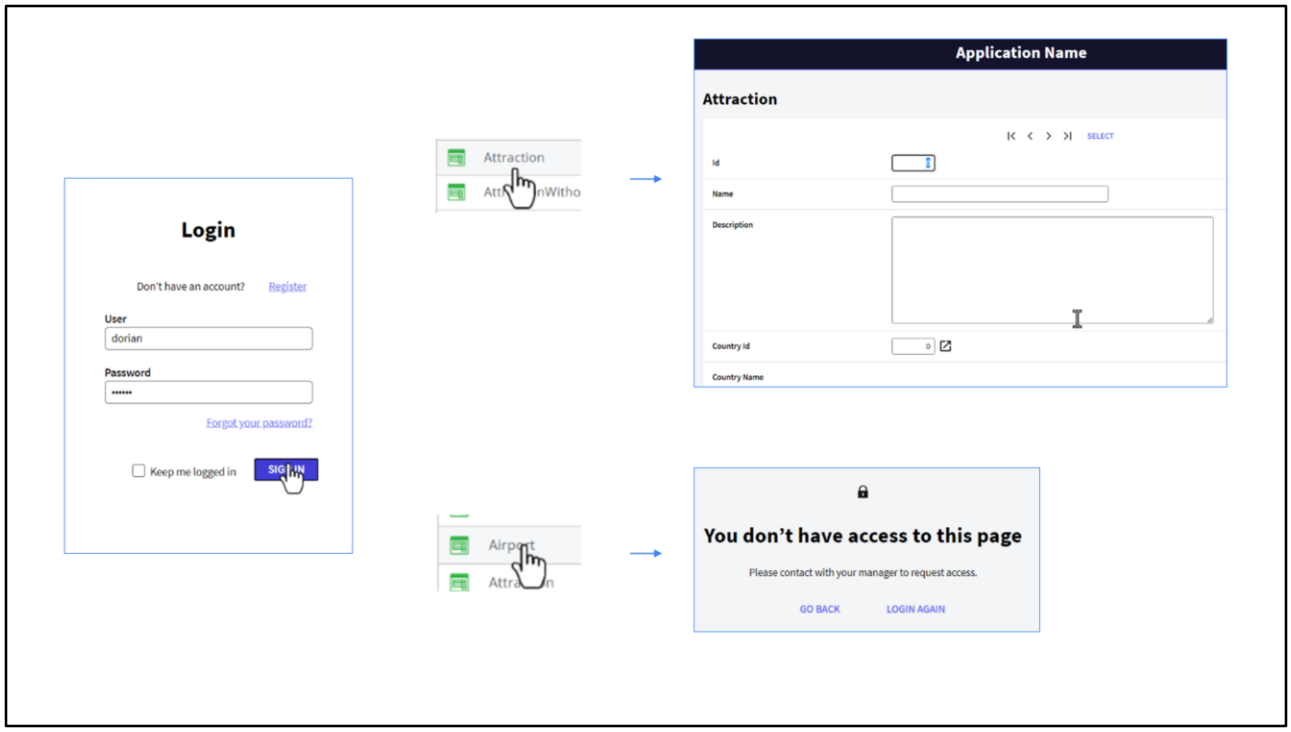
Entrando no console de administração, primeiro vamos em “Roles” e adicionaremos a role "Attraction Manager" que terá as permissões para poder inserir, atualizar ou remover alguma atração. Para isso, clicamos na opção "Add" e colocamos o nome e indicamos a política de segurança, por enquanto basta deixar a opção padrão. Confirmamos.

Depois, entramos em nossa role e selecionamos “More Options” "Permissions". Nesta tela, selecionamos a aplicação "Travel Agency" e a opção "Add". Na próxima tela, são exibidas as permissões que podemos aplicar a este objeto. Selecionamos "attraction_FullControl", pois esta role poderá realizar todas essas tarefas. Clicamos em "Add Selected" e salvamos.

Com isto, configuramos nossa role. Agora precisamos adicionar um usuário para que tenha atribuída essa role. Para fazer isso, vamos para a opção "Users" e para a opção "New User". Veremos que alguns campos possuem asterisco, que indica que são obrigatórios.

Adicionamos o usuário "Dorian" com um e-mail, uma senha e adicionamos sua política de segurança. Confirmamos. Entramos no usuário recém-criado, "Dorian", e vamos atribuir sua role. Adicionamos role e indicamos que seja “Attraction Manager” e adicionamos com "add

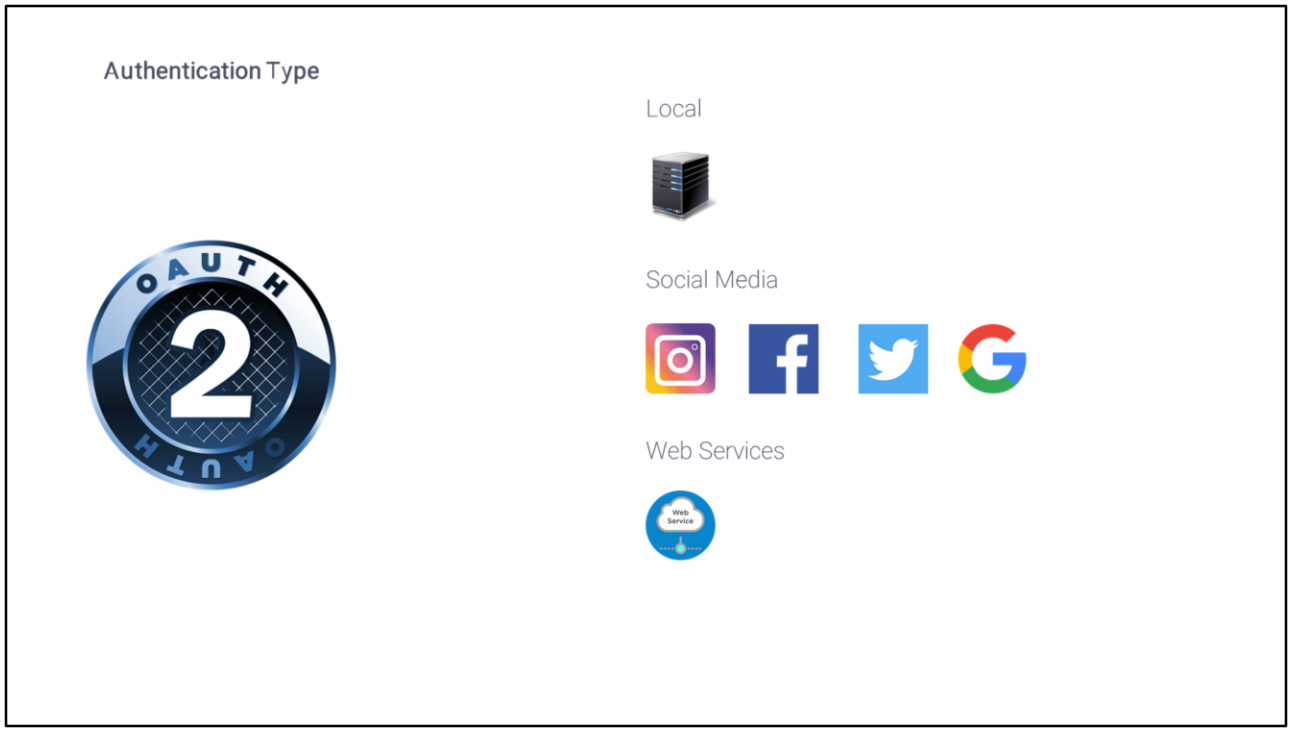
selected". Voltamos e visualizamos que o usuário já tem esta nova role atribuída.



Agora vamos novamente à nossa aplicação backoffice, onde administramos uma agência de viagens.

Ao executar a aplicação, a partir do Launchpad selecionamos a transação Attraction, nos pedirá as credenciais de acesso, fazemos login com o usuário Dorian e podemos acessar sem problemas. Dadas as permissões, podemos também inserir, atualizar ou remover qualquer uma das atrações.

Se formos à transação Airport e colocarmos como segurança autorização, como fizemos com Attraction, e tentarmos entrar em Airport a partir do Launchpad, nos dirá que não estamos autorizados, pois apenas demos permissão para acessar as atrações.



Com isto vemos como GeneXus nos permite administrar a autenticação e autorização da aplicação. Até agora, utilizamos apenas a autenticação dos usuários locais, mas podemos utilizar outro tipo de autenticação, como Facebook, Twitter, Google ou algum outro serviço externo.

Cabe destacar que a versão atual de Genexus pode realizar a autenticação com qualquer provedor que utilize OAuth 2.0. OAuth é um padrão para conceder acesso a sites web ou aplicações a partir de outro site web, mas sem conceder as senhas.

Uma de suas vantagens é que verifica-se a identidade do usuário e emite um token para a aplicação para conceder acesso, o que torna muito mais segura a autenticação em nossa aplicação.

Para saber mais sobre o Genexus Access Manager, visite nossa WIKI.