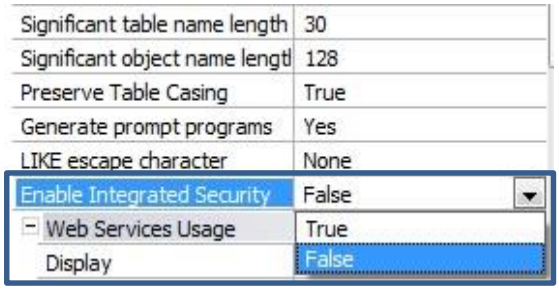
Introdução GAM

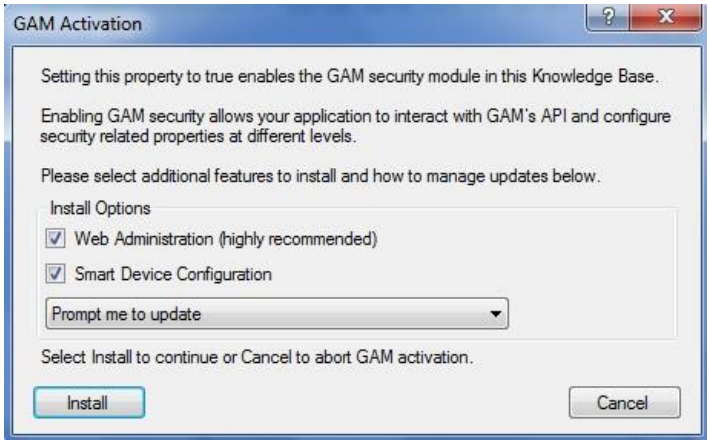
A grande maioria das aplicações modernas necessita de algum esquema de login, autenticação e autorização.

Para atender estas necessidades, Genexus oferece um módulo de segurança, chamado GeneXus Access Manager (GAM) que resolve as funcionalidades de autenticação e autorização para aplicações Web como para aplicações para Smart Devices.

Para se utilizar deste módulo com todos os controles de segurança oferecidos, simplesmente deve-se configurar em nossa base de conhecimento, a nível da versão ativa, a propriedade Enable integrated security com o valor True.



Ao fazê-lo , aparece este diálogo para ativação do GAM e pressionamos o botão “Install”:



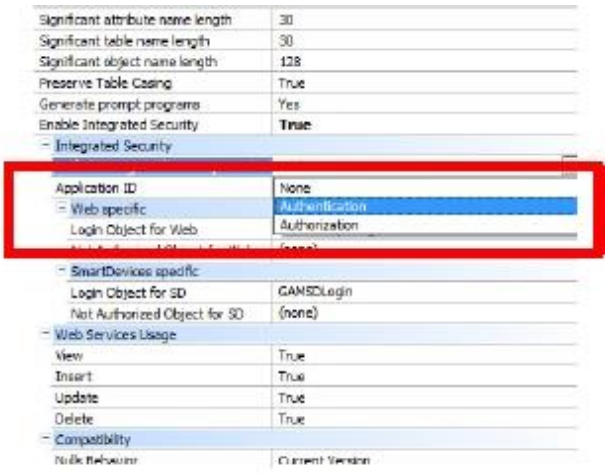
Como consequência será importado um Módulo de segurança desenvolvido com Genexus, que se integrará a nossa aplicação assim permitindo resolver as questões de de segurança de nossa aplicação.

Observamos que na janela de Output, são mostrados vários objetos que estão sendo importados. São estes os objetos correspondentes ao módulo GAM.

Bem. Uma vez habilitada a segurança, você pode selecionar se quer somente a Autenticação ou Autenticação + Autorização.

Conseguimos isso configurando a propriedade **Integrated Security Level**.

Por hora vamos trabalhar somente com Autenticação



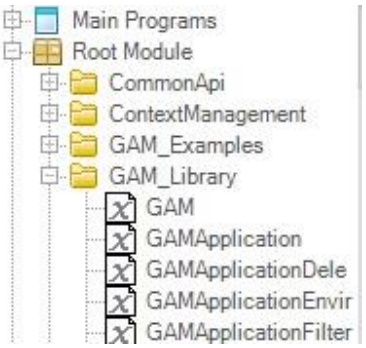
Quando habilitar o GAM, além de importar os objetos, são realizados várias mudanças.

Por exemplo, são habilitados as propriedades para configurar qual será o objeto para Login tanto para aplicações Web como para Smart Devices.

Observemos a propriedade **Login Object for Web.** Tem o valor GAMExampleLogin para indicar que será utilizado esse objeto para login das aplicações Web

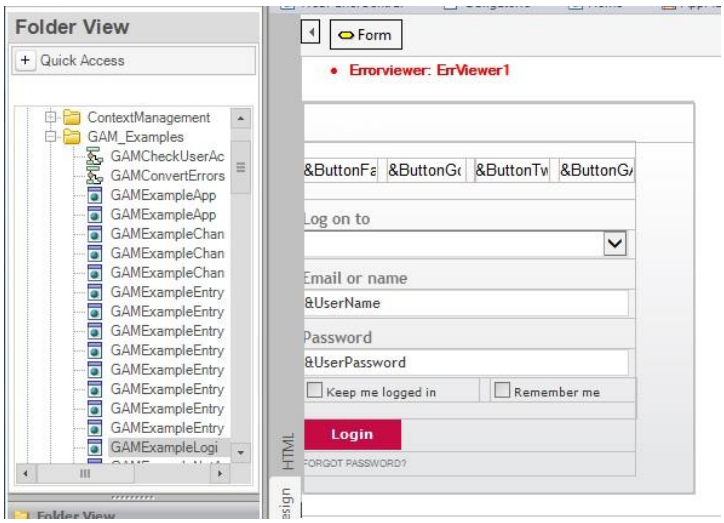
E a propriedade **Login Object for SD**, tem o valor GAMSDLogin, indicando o nome do objeto que realizará o login das aplicações para Smart Devices.

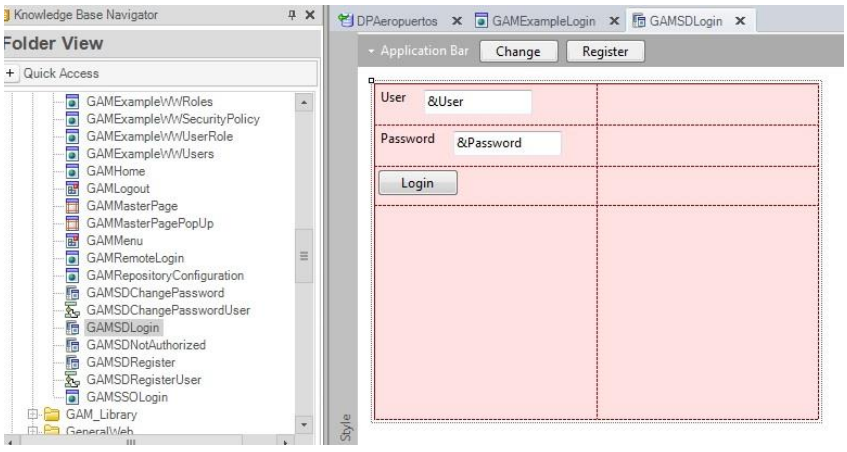
Podemos encontrar os objetos que foram importados ao habilitar nas pastas/folders GAM_Examples e GAM_Library.



A pasta/folder GAM_EXamples contêm todos os objetos de exemplo que foram importados. Observemos que contêm Web Panels e Panels for Smart Devices. Estes objetos serão utilizados para a autenticação e autorização dos usuários.

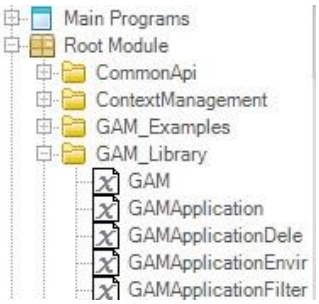
Em particular estão os objetos, GAMExampleLogin e GAMSDLogin que são aqueles que estão configurados, como vimos antes, nas propriedades Login Object for Web e Login Object for Smart Devices.





Mas existem vários objetos que compõem o Backend do GAM. Ou seja, o Backend é uma aplicação Web que utilizamos para administrar e configurar os usuários, suas regras, permissões, etc, e o veremos em alguns minutos.

Na pasta/folder Folder GAM_Library observamos que há objetos externos os quais tem as configurações necessárias para executar APIs do GAM. As APIs são funções que permitem a comunicação da nossa KB com a base de dados do GAM, que é outra base de dados diferente da associada a nossa aplicação . A base de dados do GAM contêm a informação dos usuários, regras, etc.



Algo importante para ter em conta, é que quando habilitamos o GAM logo devemos executar a ação **Rebuild all** na KB.

Neste momento do proceso é solicitado criar a base de dados associado ao GAM.
Colocamos Yes

Logo terminado o Rebuild all, podemos executar a aplicação com o GAM aplicado.
Pressionamos então a tecla F5.

Tentemos, por exemplo, acessar o Work With Country.

Vemos que primeiro se executa um objeto de Login.

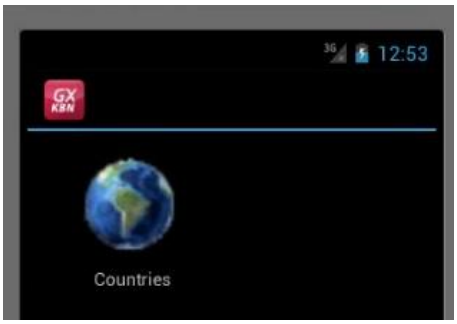
A execução deste objeto é automática cada vez que requerido.

Neste caso como não temos definido nenhum tipo de autenticação a utilizar como por exemplo poderia ser: facebook, o twitter… por padrão somente está habilitada a autenticação local e podemos entrar com o usuário: “admin” e senha: “admin123”.

O objeto de login é executado pelo simples fato de termos configurado as propriedades para habilitar o GAM sem termos precisado programar nada mais. Isto é assim porque fazendo uso do GAM, se realiza um **controle de acesso automático em cada objeto**.

Vamos agora executar a aplicação para Smart Devices. Vemos que aqui também aparece o painel de login. Entramos então com o usuário admin e senha admin123 .

Uma vez então que são digitados os dados do login, seremos redirecionados para o objeto que está tratando de executar, neste caso o Dashboard.

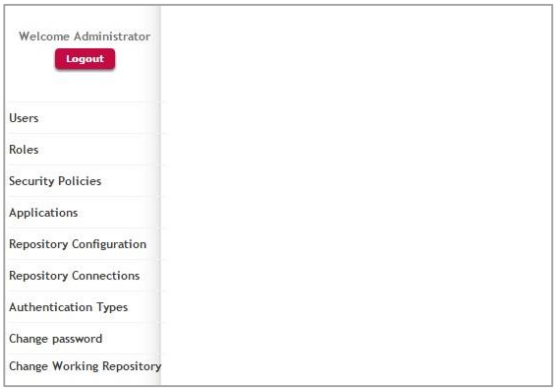


Este é então o comportamento padrão tanto para aplicações Web como Smart Devices.

Como comentávamos antes, entre os objetos que são importados ao habilitar o GAM, há um grupo que implementa o Backend para administrar usuários, regras, etc.

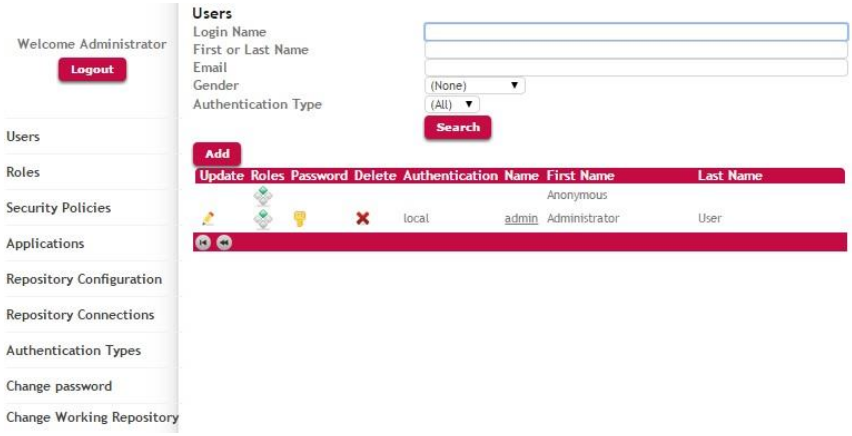
Para acessar o Backend em tempo de execução a partir do Developer Menu devemos executar o GAMHome que é o objeto principal do Backend do GAM.

Vejamos que a esquerda há um menu, onde se pode acessar as diferentes opções de Backend.



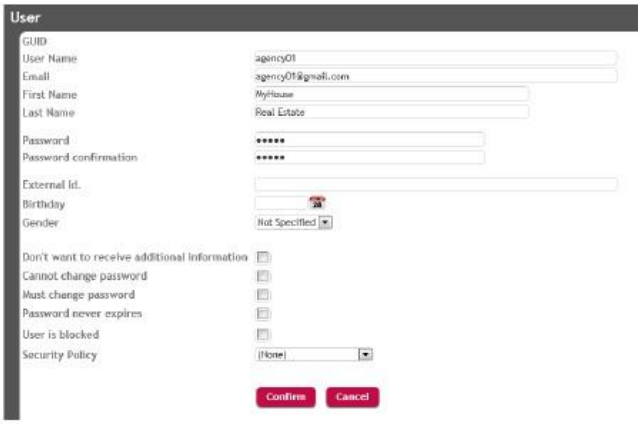
Entremos na opção Users.

Aqui veremos todos os usuários definidos. Por padrão somente aparece o usuario admin que é criado automaticamente com a aplicação do GAM, e é o que estamos utilizando para nos logarmos.



Vamos definir um novo usuário, para um dos agentes de viagens que irão utilizar o aplicativo que você está construindo.

Para isto pressionamos o botão Add ...e entramos com os dados do usuario…



Indicamos então que a autenticação é local, definimos o nome do usuários que será “pjones”, o e-mail será pjones@gmail.com, o nome é “Peter”, o apelido “Jones”, e definimos a senha que será “pjones123”, e confirmamos “pjones123”.

E assim foi definido o nosso usuário.

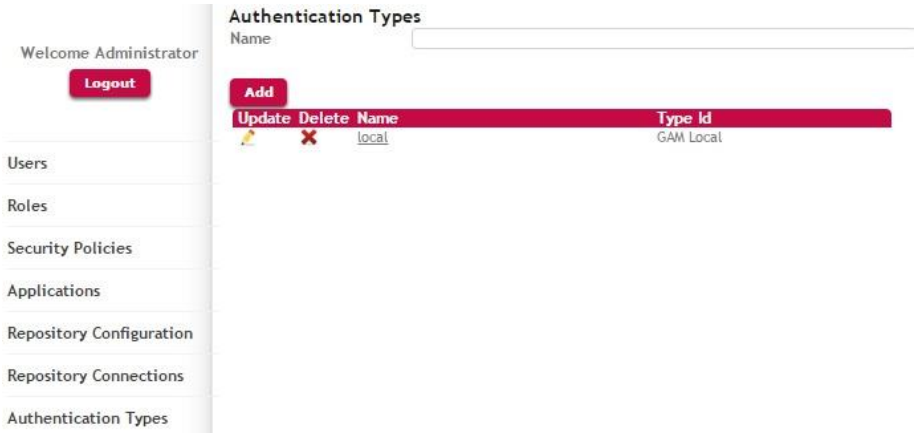
Agora podemos associar uma função para o usuário.

Assim que pressionamos Role, vamos escolher a função de Administrator.

Pressionamos Add, e desta forma associamos a função Administrador ao usuário pjones.

Bem. Agora voltamos para a opçãoAuthentication Types e vemos que por padrão somente está habilitada a autenticação local.

Aqui é onde devemos definir os diferentes tipos de autenticação que queremos utilizar em nossa aplicação como por exemplo, Facebook, o twitter.



Assim vimos neste vídeo que podemos implementar aplicações Genexus seguras fácilmente já que o Genexus nos fornece o GAM, GeneXus Access Manager, que nos oferece uma solução completa e integrada para resolver a Autenticação e Autorização de nossas aplicações tanto Web como para Smart Devices.