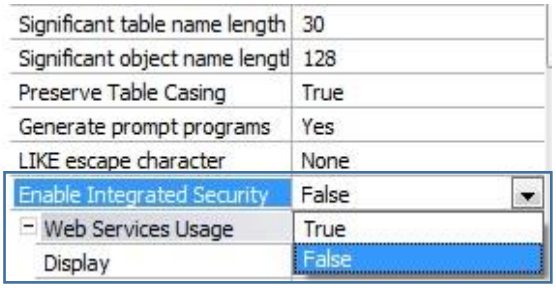
Aplicação do GAM em nossa KB

Anteriormente vimos que o GeneXus oferece um módulo de segurança, chamado GeneXus Access Manager (GAM) que resolve as funcionalidades de autenticação e autorização, tanto para aplicações Web como para aplicações para Smart Devices.

Para dispor do GeneXus Access Manager, com todos os controles de segurança oferecidos, simplesmente terá que configurar em nossa base de conhecimento, a nível da versão ativa, a propriedade Enable integrated Security, com o valor True.



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

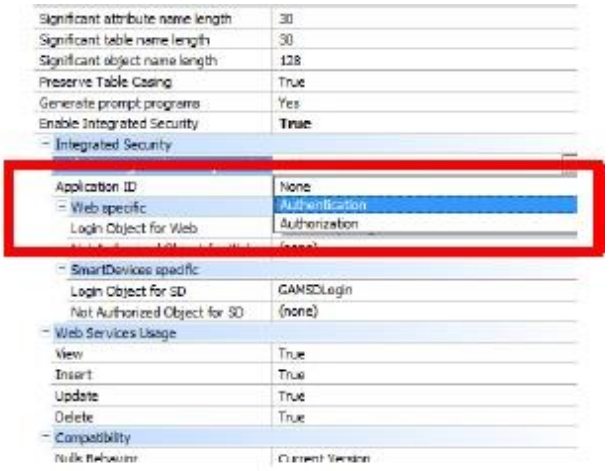
Consequentemente será importado um Módulo de segurança desenvolvido no Genexus, que se integra a nossa aplicação, permitindo assim resolvê-lo referente a segurança do mesmo.

Notamos que na janela de output mostram-se vários objetos está importando. São os objetos correspondentes ao módulo GAM.

Uma vez habilitado a segurança, permite selecionar apenas a Autenticação ou a Autenticação+Autorização.

Isto se consegue configurando a propriedade **Integrated Security Level**.

Agora, vamos trabalhar somente com a Autenticação.



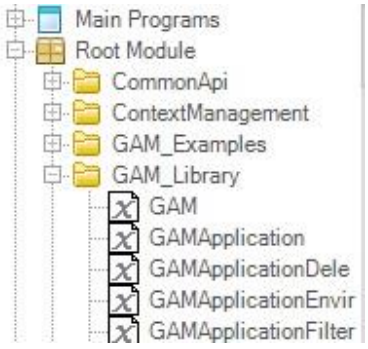
Quando se habilita o GAM, além de importar os objetos, são realizadas várias mudanças.

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

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

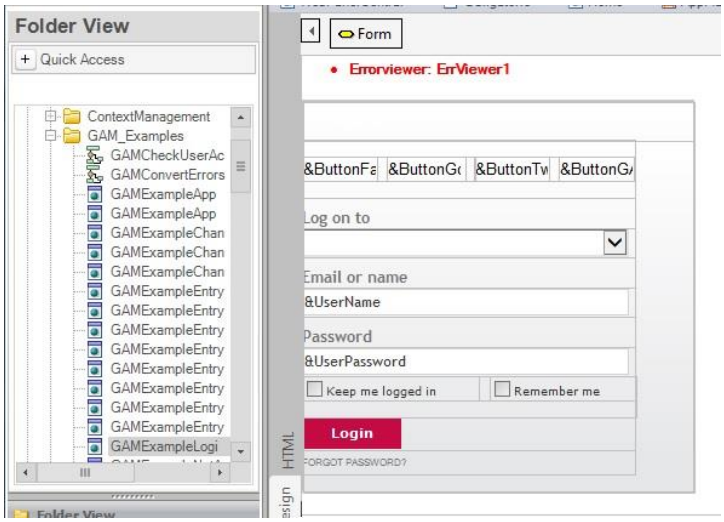
E a propriedade **Login Object for SD**, tem o valor GAMSDLogin, indicando o nome do objeto que realizará o login das aplicações para Smart Devices.

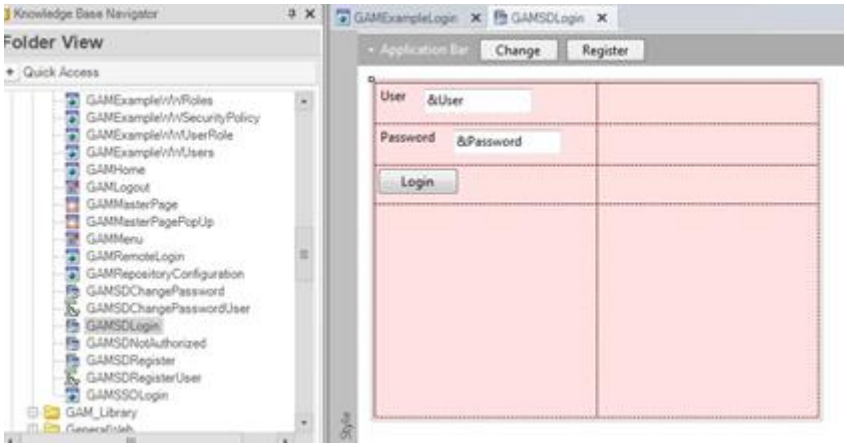
Ao habilitar o GAM, podemos encontrar os objetos importados, nos folders GAM_Examples e GAM_Library.



O folder GAM_EXamples contém todos os objetos do exemplo que foi importado. Observamos que contém Web Panels e Panels for Smart Devices. Estes objetos irão ser utilizados para a autenticação e autorização dos usuários.

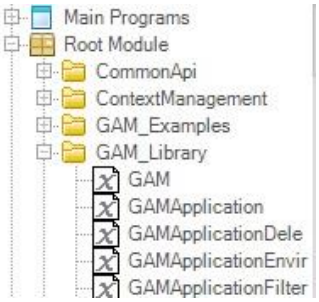
Particularmente, são os objetos que estão no GAMExampleLogin e GAMSDLogin que estão configurados, como vimos antes, nas propriedades do Login Object for Web e Login Object for Smart Devices.





Há vários objetos que compõem o Backend do GAM. Ou seja, o Backend é uma aplicação Web utilizada para administrar e configurar os usuários, suas funções, permissões, etc., e iremos ver em poucos minutos.

No folder GAM_Library, observemos que há objetos externos, os quais tem as configurações necessárias para executar APIs do GAM. As APIs, são funções que permite que a comunicação com a nossa KB e 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, contém as informações dos usuários, funções, etc.



Algo importante a considerar, é que quando habilitamos o GAM, logo devemos executar a ação Rebuild all na KB.

É nesse momento que é solicitado criar a base de dados associada ao GAM.
Colocamos Yes.

Logo, terminado o Rebuild all, podemos executar a aplicação com o GAM aplicado.
Pressionamos então a tecla F5. Agora tente, por exemplo, acessar o Work With Speaker.

Vemos que primeiro executa o objeto de login.

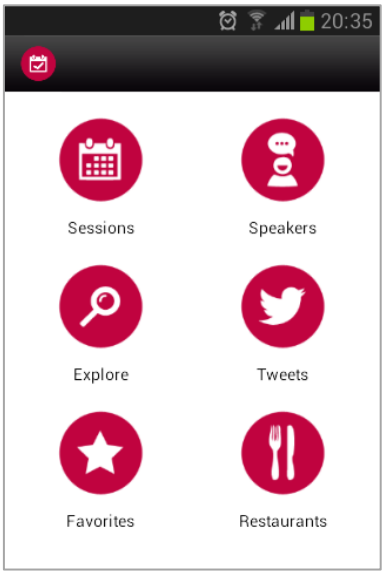
A execução deste objeto é automática sempre que necessário.

Neste caso, como não definimos nenhum tipo de autenticação a ser utilizado, por exemplo, poderia ser: Facebook ou twitter… por padrão somente está habilitado a autenticação local e podemos acessar com o usuário: “admin” e senha: “admin123”.

O objeto login é executado simplemente porque foi configurado nas propriedades para habilitar o GAM e não tem que programar mais nada. Isto é, porque o GAM utiliza um **controle de acesso automático em cada objeto.**

Vamos agora executar a aplicação para Smart Devices. Vemos que também aparece primeiro a panel do login. Acessamos então com o usuário: admin e a senha: admin123.

Uma vez que inseridos os dados de login, é redirecionado ao objeto que estava tentando executar, neste caso o Dashboard.

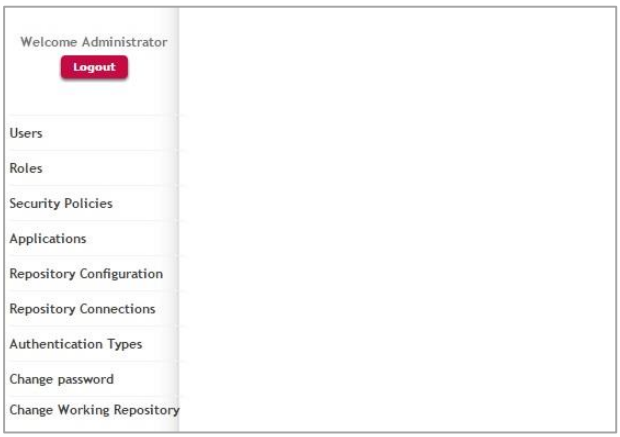


Este é o comportamento por padrão tanto para aplicações Web como para Smart Devices.

Como mencionamos antes, entre os objetos que são importados ao habilitar o GAM, há um grupo destes objetos, que implementa o backend para administrar os usuários, funções, etc.

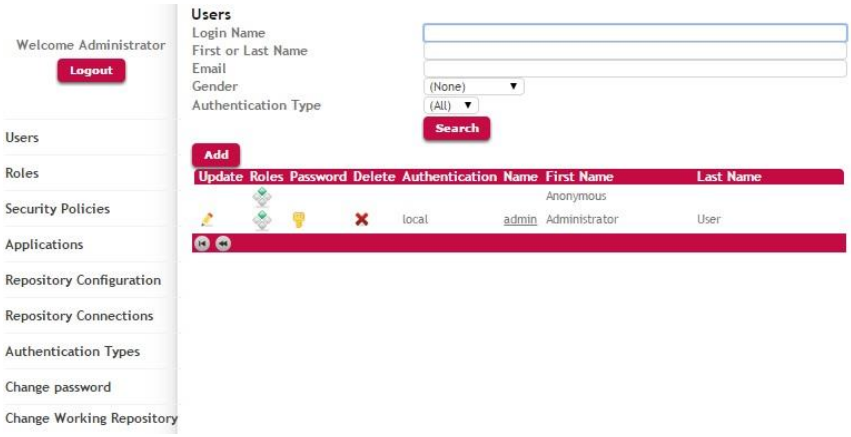
Para acessar o Backend em tempo de execução, desde o Developer Menu, devemos executar o GAMHome, que é o objeto principal do Backend do GAM.

Vejamos que na esquerda há um menú, onde pode-se acessar as diferentes opções do Backend.

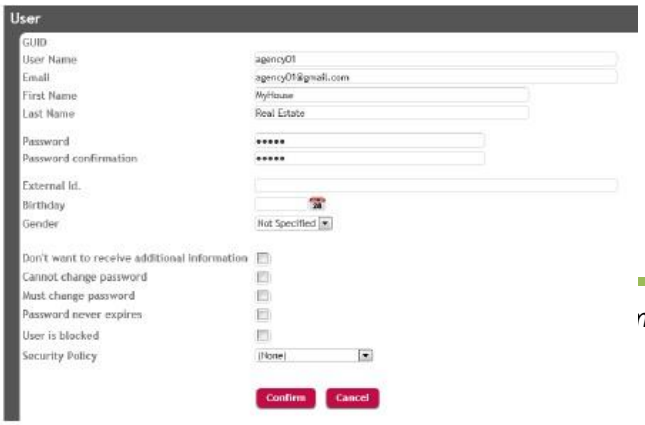


Escolhemos a opção Users.

Aqui, iremos ver todos os usuários definidos. Por padrão somente está o usuário admin que é criado automáticamente com a aplicação do GAM, e é o que estamos utilizando para nos logarmos.



Vamos definir um novo usuário, para um dos organizadores do evento, que irá utilizar a aplicação que estamos construindo.
Para isso, pressionamos o botão Add… e inserimos os dados do usuário…



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

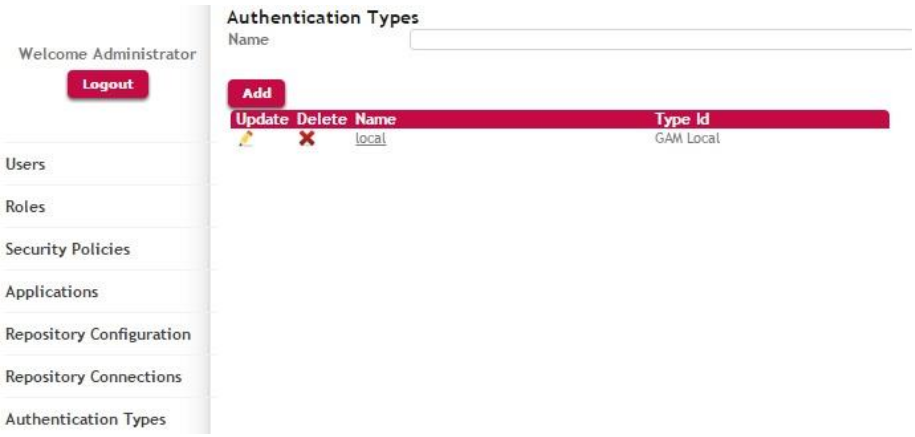
Agora, vamos associar uma função ao nosso usuário.

Assim, que pressionamos Role, e escolhemos o rol Administrator.

Pressionamos Add, e desta forma associamos o rol Administrator ao usuário pjones.

Agora vejamos a opção Authentication 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 ou twitter.



Desta forma, vimos neste vídeo que podemos implementar aplicações seguras no Genexus, já que o mesmo nos fornece o GAM, Genexus Access Manager, que nos dá uma solução completa e integrada para resolver a Autenticação e Autorização de nossas aplicações tanto Web como para Smart Devices.