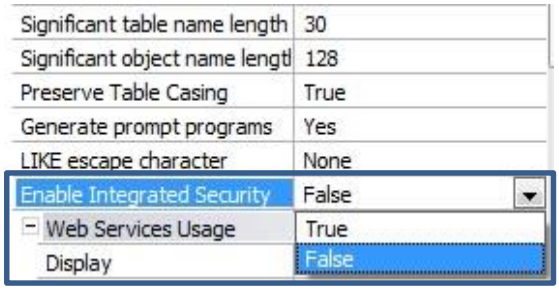
Introducción GAM

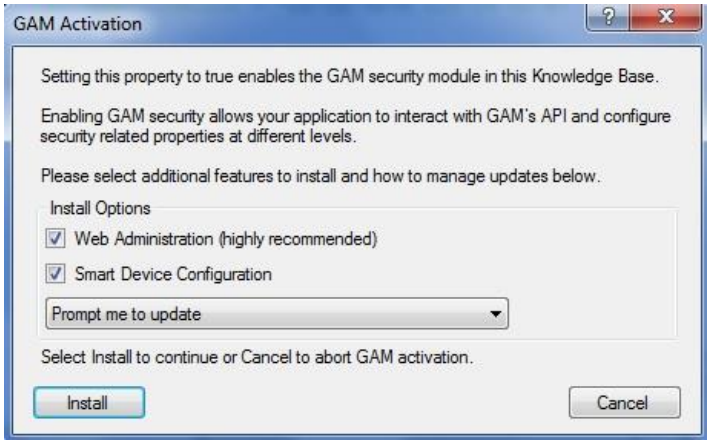
La gran mayoría de las aplicaciones modernas necesitan algún esquema de login, autenticación y autorización.

Para cubrir estas necesidades, GeneXus ofrece un módulo de seguridad, llamado GeneXus Access Manager (GAM) que resuelve las funcionalidades de autenticación y autorización, tanto para aplicaciones Web como para aplicaciones para Smart Devices.

Para disponer de este módulo con todos los controles de seguridad que ofrece, simplemente hay que configurar en nuestra base de conocimiento, a nivel de la versión activa, la propiedad Enable integrated security con el valor True.



Al hacerlo, aparece este diálago para la activación del GAM y presionamos el botón “Install” :



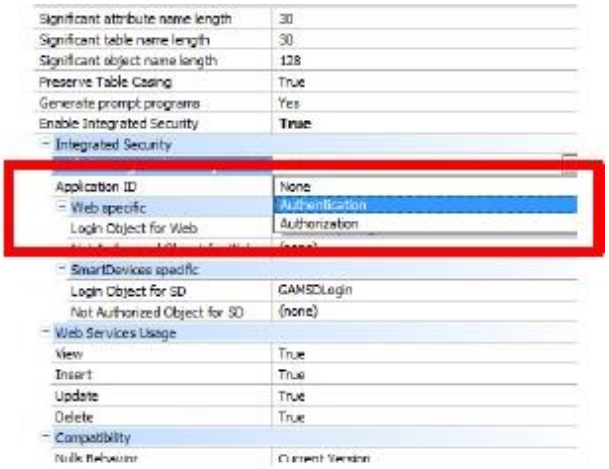
Como consecuencia se importará un Módulo de seguridad desarrollado con GeneXus, que se integra a nuestra aplicación, permitiendo así resolver lo referente a la seguridad de la misma.

Observemos que en la ventana de Output se muestran varios objetos que se están importando. Son los objetos correspondientes al módulo GAM.

Bien. Una vez habilitada la seguridad, se puede seleccionar si se quiere solo Autenticación o Autenticación+Autorización.

Esto se logra configurando la propiedad **Integrated Security Level**.

Por ahora vamos a trabajar solamente con Autenticación.



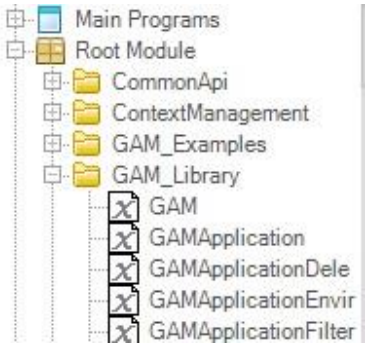
Cuando se habilita el GAM, además de importarse objetos, se realizan varios cambios.

Por ejemplo, se habilitan propiedades para configurar cuál será el objeto para Login tanto para aplicaciones Web como para Smart Devices.

Observemos la propiedad **Login Object for Web .** Tiene el valor GAMExampleLogin para indicar que se utilizará ese objeto para el login de las aplicaciones Web.

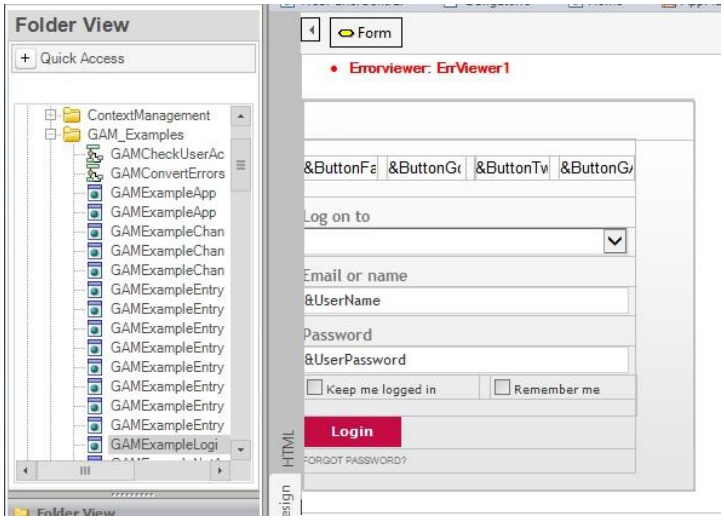
Y la propiedad **Login Object for SD**, tiene el valor GAMSDLogin, indicando el nombre del objeto que realizará el login de las aplicaciones para Smart Devices.

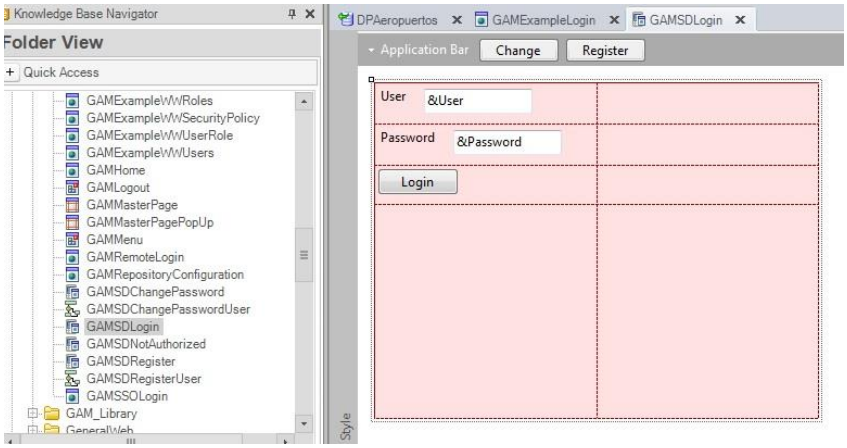
Los objetos que se importaron al habilitar el GAM, podemos encontrarlos en los folders GAM_Examples y GAM_Library.



El folder GAM_EXamples contiene todos los objetos de ejemplo que se importan. Observemos que contiene Web Panels y Panels for Smart Devices . Estos objetos van a ser utilizados para la autenticación y autorización de los usuarios.

En particular están los objetos, GAMExampleLogin y GAMSDLogin que son los que quedan configurados, como vimos antes, en las propiedades Login Object for Web y Login Object for Smart Devices.

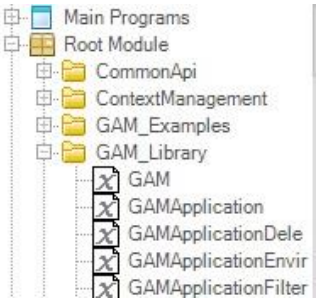




Pero además hay varios objetos que conforman el Backend del GAM. Es decir, el Backend es una aplicación Web que se utiliza para administrar y configurar los usuarios, sus roles, permisos, etc., y lo vamos a ver en unos minutos.

En el Folder GAM_Library observemos que hay external objects los cuales tienen las configuraciones necesarias para ejecutar APIs del GAM. Las APIS son funciones que permiten que se comunique nuestra KB con la base de datis del GAM, que es otra base de datis

diferente de la asociada a nuestra aplicación. La base de datis del GAM contiene la información de los usuarios, roles, etc.



Algo importante de tener en cuenta, es que cuando habilitamos el GAM, luego debemos ejecutar la acción **Rebuild all** en la KB.

Es en este momento que nos solicitan crear la base de datos asociada al GAM.
Ponemos Yes.

Luego de terminado el Rebuild all, podemos ejecutar la aplicación con el GAM aplicado.
Presionemos entonces la tecla F5
Intentemos, por ejemplo, acceder a Work With Country.

Vemos que primero se ejecuta un objeto de login.

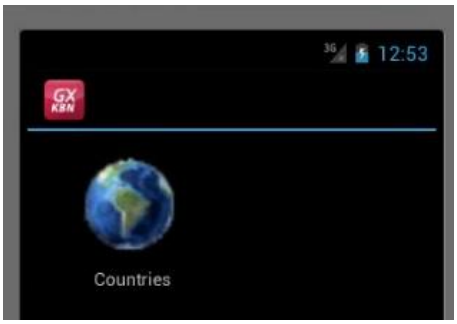
La ejecución de este objeto es automática cada vez que se requiere.

En este caso como no hemos definido ningún tipo de autenticación a utilizar como por ejemplo podrían ser: facebook o twitter… por defecto solo está habilitada la autenticación local y podemos ingresar con el usuario: “admin” y password: “admin123”.

El objeto de login se ejecutó por el simple hecho de haber configurado las propiedades para habilitar el GAM y no hemos tenido que programar nada más. Esto es así porque haciendo uso del GAM, se realiza un **control de acceso automático en cada objeto**.

Vayamos ahora a ejecutar ahora la aplicación para Smart Devices. Vemos que aquí también aparece primero el panel de login. Ingresamos entonces con el usuario admin y password admin123.

Una vez entonces que se ingresan los datos de login, se redirecciona al objeto que se estaba tratando de ejecutar, en este caso al Dashboard.

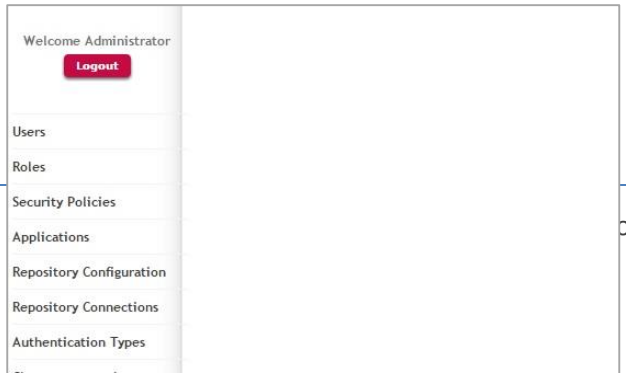


Este es entoncesel comportamiento por defecto tanto para aplicaciones Web como para Smart Devices.

Como comentábamos antes, entre los objetos que se importan al habilitar el GAM, hay un grupo que implementa el Backend para administrar usuarios, roles, etc.

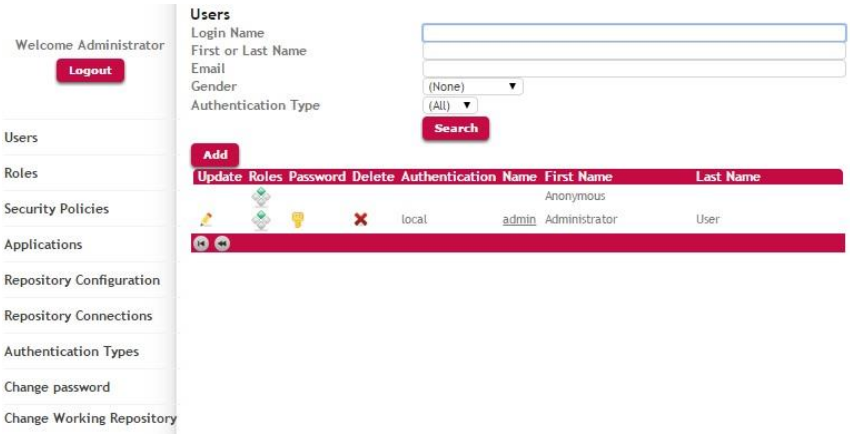
Para acceder al Backend en tiempo de ejecución, desde el Developer Menu, debemos ejecutar el GAMHome que es el objeto principal del Backend del GAM.

Veamos que a la izquierda hay un menu, donde se pueden acceder a las diferentes opciones del Backend.



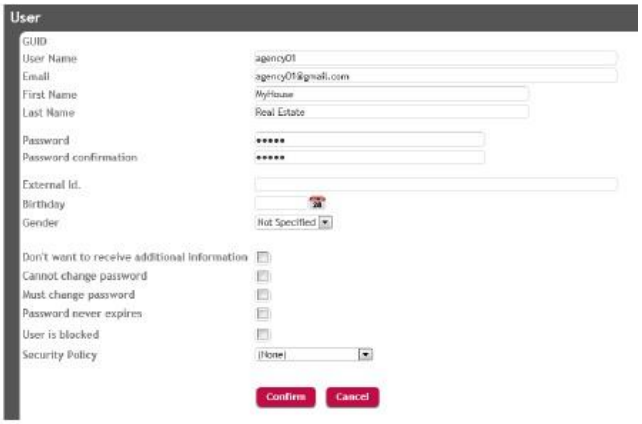
Ingresemos a la opción Users.

Aquí vamos a ver todos los usuarios definidos. Por defecto solo está el usuario admin que es el que se crea automáticamente con la aolicación del GAM, y es el que estamos utilizando nosotros para loguearnos.



Vamos a definir un nuevo usuario, para uno de los agentes de viaje que va a utilizar la aplicación que estamos construyendo.

Para esto presionamos el botón de Add ...e ingresamos los datos del usuario…



Indicamos entonces que la autenticación es local, definimos el nombre del usuario que será “pjones”, el email será pjones@gmail.com, el nombre es “Peter”, el apellido “Jones”, y definimos la password que será “pjones123”, y confirmamos la password “pjones123”.

Y quedó definido nuestro usuario.

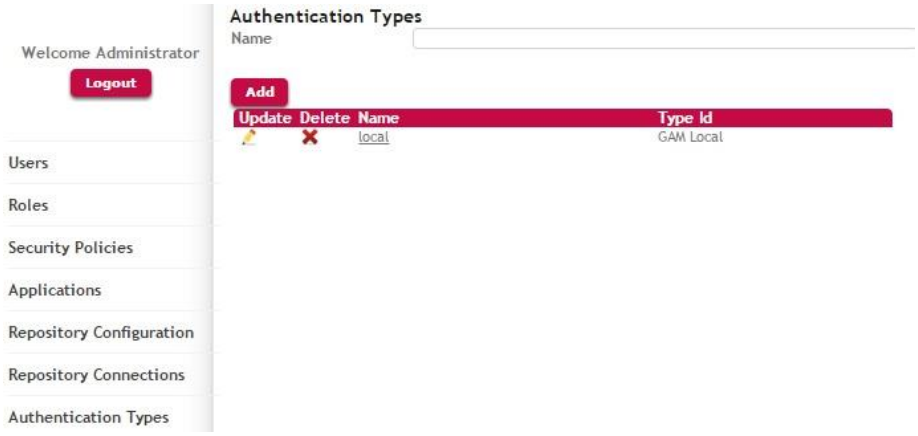
Ahora, le vamos a asociar un Rol a nuestro usuario.

Así que presionamos Role, y vamos a elegir el rol Administrator

Presionamos Add, y de esta forma le asociamos el rol Administrador al usuario pjones.

Bien. Ahora vayamos a la opción Authentication Types, y vemos que por defecto solo está habilitada la autenticación local.

Aquí es donde debemos definir los diferentes tipos de autenticación que queremos utilizar en nuestra aplicación como por ejemplo, facebook o twitter.



De esta forma hemos visto en este video que podemos implementar aplicaciones GeneXus seguras fácilmente ya que GeneXus nos proveer el GAM, GeneXus Access Manager, que nos

brinda una solución completa e integrada para resolver la Authenticación y Autorización de nuestras aplicaciones tanto Web como para Smart Devices.