

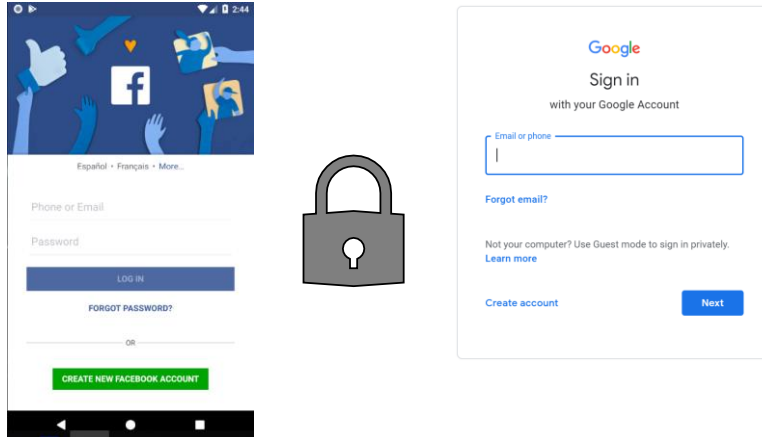
GeneXus[™]
The power of doing.

GeneXus Access Manager - Introduction

Security

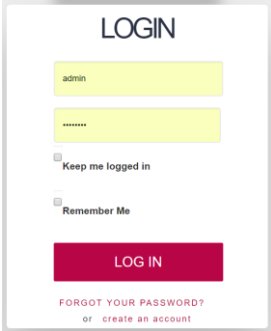
GeneXus™ 16

Security



Como ya sabemos , la gran mayoría de las aplicaciones modernas necesitan un esquema de seguridad, para que solo puedan ingresar los usuarios permitidos y también autorizar o restringir el acceso a partes de la aplicación, según los permisos asignados al usuario.

Security



LOGIN

admin

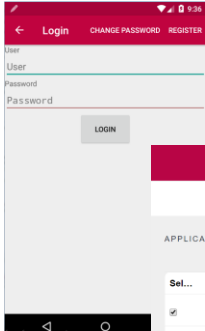
.....

Keep me logged in

Remember Me

LOG IN

FORGOT YOUR PASSWORD?
or create an account



Login CHANGE PASSWORD REGISTER


User

User


Password

Password

LOGIN



Authorization



Authentication

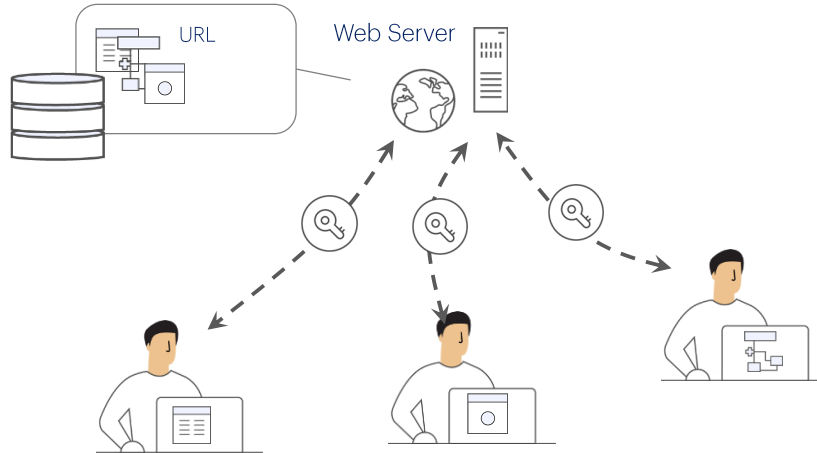
Add Permission ← BACK + ADD SELECTED

APPLICATION: GAM Backend ROLE: BackedUser

Sel..	Permission name	Description	Permissions options
<input checked="" type="checkbox"/>	gamexamplechangerespository_Execute	Change Working Repository	Allow
<input type="checkbox"/>	gamexamplechangeyourpassword_Execute	Change Password	Allow
<input checked="" type="checkbox"/>	gamexamplewapplications_Execute	Application	Restricted
<input checked="" type="checkbox"/>	gamexamplewauthitypes_Execute	Authentication Types	Deny
<input type="checkbox"/>	gamexamplewconnections_Execute	Connections	Allow

Esto significa asegurar que todos los usuarios que ingresen estén debidamente autenticados (es decir, que el usuario sea quien dice ser); y autorizados (es decir, una vez que el usuario se autentica, se le permita el acceso o no a ciertas partes de la aplicación).

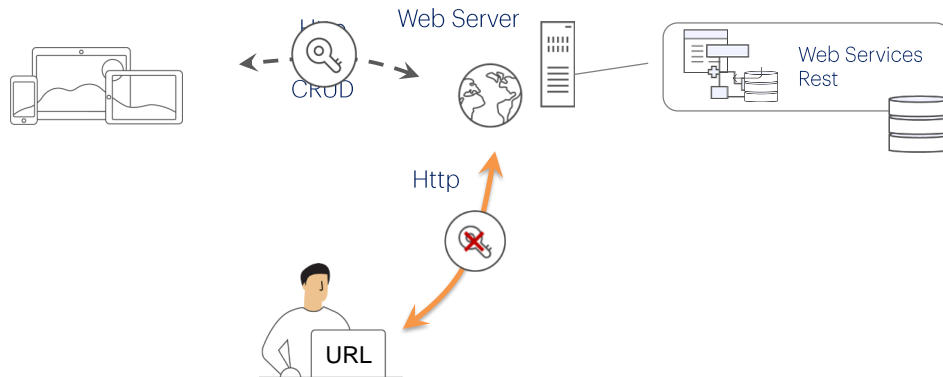
Security in Web Applications



En el caso de las aplicaciones Web, como estas aplicaciones tienen varios puntos de entrada, cualquier objeto accesible por URL debe chequear permisos de autenticación.

Eso implica que cada uno de estos objetos tienen que tener incorporado el chequeo de seguridad para hacer la verificación correspondiente.

Security in Smart Devices Applications



En el caso de las aplicaciones para Smart Devices, al ser aplicaciones distribuidas, una parte de ellas se ejecuta en el propio dispositivo y la capa de negocios de la aplicación se resuelve a través de servicios Rest que tienen una URL de acceso, por lo que están expuestos a accesos indeseados.

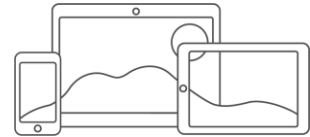
Al igual que para las aplicaciones web, lo que se hace es verificar que solamente usuarios debidamente autenticados y autorizados puedan acceder a la aplicación, evitando la ejecución de usuarios que no cumplan con esto.

Integrated Security Solution



Authentication

Authorization



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.

El GAM está desarrollado en GeneXus por lo que se integra fácilmente a la KB de la aplicación y permite resolver de manera centralizada todo lo referente a la Seguridad de la misma. El objetivo es que la solución de Seguridad se utilice lo más declarativamente posible dentro de la aplicación, sin crear complejidad adicional.

El GAM también provee un backend que permite definir usuarios, permisos, políticas de seguridad y acceso a objetos, entre otras cosas.

Además provee una API para poder acceder a muchas de estas funcionalidades en forma programática.

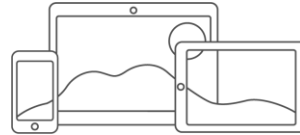
GAM Features



Authentication



Web Sessions



Oauth



Authorization

RBAC



Role Based Access Control

Para resolver la Autenticación, internamente se usa:

- **Web sessions** para la seguridad de aplicaciones Web
- **Oauth** para resolver la seguridad en el caso de aplicaciones para SD

En el caso de la Autorización, su implementación está basada en Roles utilizando el modelo **Role Based Access Control** mediante el cual se encapsulan los métodos, propiedades y todo lo necesario para el manejo de autorización en la aplicación.

GAM FeaturesLocal / Remote
AuthenticationExternal Identity
ProvidersLegacy / Custom
Providers

El GAM provee diferentes Tipos de Autenticación, los tipos disponibles son:

Autenticación local usando GAM donde los usuarios y todas sus credenciales son almacenados en una base de datos de la cual somos propietarios o también en forma **Remota**, ya que una aplicación que use GAM puede ser convertirse en proveedor de identidades y en este caso, otras aplicaciones con GAM pueden conectarse remotamente a este server y obtener la autenticación desde allí.

Podemos utilizar también a otros proveedores de identidad externos, estos proveen una autenticación basada en el protocolo **Oauth 2.0** como **Facebook, Twitter y Google, Instagram, Office 365, Mercado Libre o LinkedIn**, aquí se utilizan los mecanismos de autenticación estándar basados en este protocolo implementado por estas aplicaciones. En este caso no hay necesidad de definir usuarios locales.

En muchas ocasiones es necesario integrar nuestra aplicación con otras con las que tenemos que intercambiar información y es necesario asegurar la autenticación de los usuarios mediante una autenticación externa a la aplicación.

Una forma de autenticación externa es utilizar un **web service SOAP** que provee la otra aplicación y configurar al GAM para que consuma ese web service.

Puede ser posible que la otra aplicación provee un programa externo para resolver la autenticación, pero que no necesariamente es un web service. En ese caso configuro el GAM para aceptar una autenticación del tipo Custom.

GAM Features

The screenshot displays the GeneXus Access Manager interface. On the left, there is a 'Speakers' table with columns for Id, Full Name, Image, Company Name, Country Id, and Country. The table lists several speakers, including Garrido, Alejandro; Cardoso, Amando; Bachmann, Armin; and Gonda, Breogan. In the center, a 'Speaker' form is shown for Armin Bachmann, with fields for Name, Surname, Full Name, Image, and CVMini. On the right, a 'Work With Speaker' mobile app interface is shown, displaying a list of speakers and a detailed profile for Armin Bachmann, including his photo and bio.

Permission name	Description	Permissions options	Inherited
gamexamplechangeyourpassword_Execute	Change Password	Allow	DELETE
gamexamplewvapplications_Execute	Application	Allow	DELETE
gamexamplewvauthypes_Execute	Authentication Types	Restricted	DELETE

Id	Full Name	Image	Company Name	Country Id	Country
12	Garrido, Alejandro		GeneXus	5	Uruguay
15	Cardoso, Amando		Century 21 Knowledge Prop.	5	Uruguay
23	Bachmann, Armin		GeneXus	5	Uruguay
2	Gonda, Breogan		GeneXus	5	Uruguay

Con la Autorización, definimos los permisos ejecución de los objetos y los permisos sobre los modos de operación de las transacciones.

La definición se hace otorgando para cada objeto, permisos a cada rol y en función de cuál sea el rol que tenga asignado el usuario, serán los permisos efectivos sobre el objeto.

Esta validación se realiza sobre los siguientes objetos Web:

- Web Panels
- Web Components con la propiedad URL Access=Yes
- Transacciones

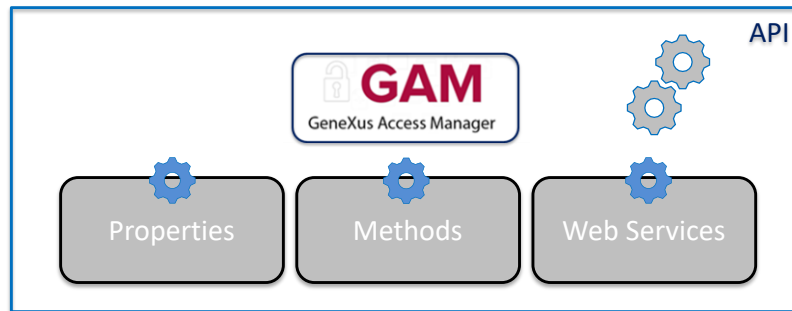
Además, se verifican los permisos sobre los modos Insert, Update, Delete y Display de las Transacciones Web

Y para Smart Devices de los objetos:

- Work With for Smart Devices
- Panels for Smart Devices.

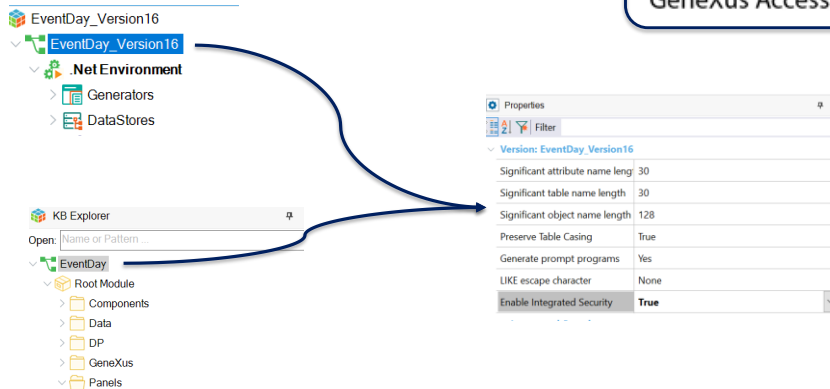
Y las acciones de Insert, Update y Delete sobre los Work With for Smart Devices.

GAM Features



El GAM también expone una API (Application Program Interface) para acceder a sus propiedades y métodos en caso de que sea necesario hacerlo desde nuestra aplicación y una serie de servicios Web que pueden ser utilizados desde otras aplicaciones. Esto lo veremos en el nivel avanzado.

Enable Integrated Security



Para habilitar el GAM se debe ir a nivel de la versión activa de la KB y configurar la propiedad **Enable Integrated Security** en el valor True.
En la version Trial se encuentra en el primer nodo de KB Explorer con el nombre de la KB.

Integrated Security Level

The screenshot displays the GeneXus Access Manager interface. On the left, the 'KB Explorer' shows a tree view with 'EventDay_Version16' selected. Below it, the 'EventDay' folder is expanded, showing 'Root Module', 'Components', 'Data', 'DP', 'GeneXus', and 'Panels'. In the center, a properties window for 'EventDay_Version16' is shown, with the 'Integrated Security Level' dropdown menu set to 'Authentication'. On the right, the 'Properties' window for the 'Company' business component is shown, with the 'Integrated Security Level' dropdown menu also set to 'Authentication'. A logo for 'GAM GeneXus Access Manager' is visible in the top right corner.

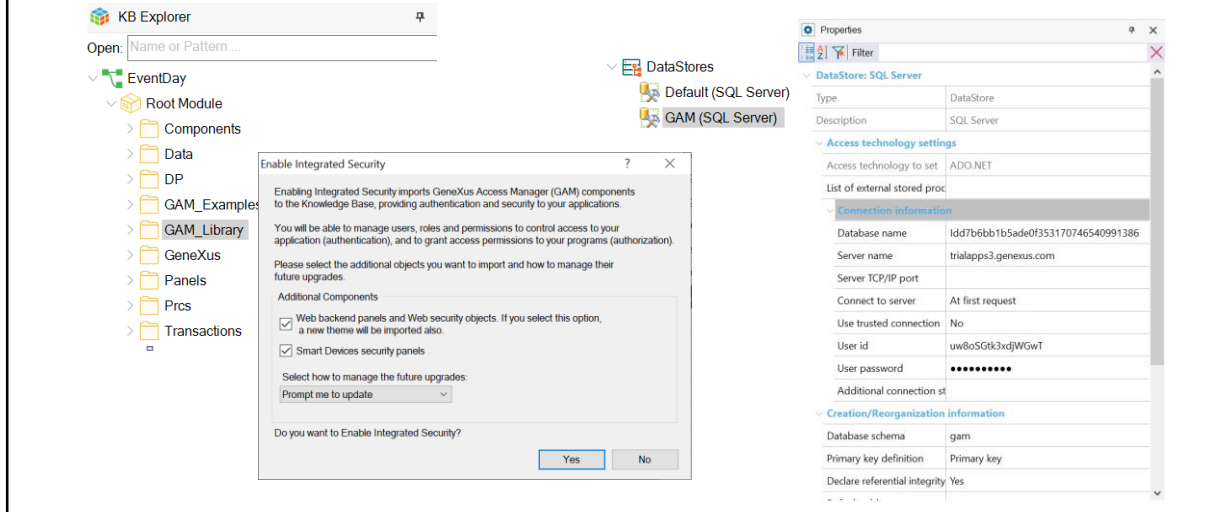
Una vez que hayamos habilitado GAM, veremos otra propiedad llamada **Integrated Security Level** que permite indicar el valor por defecto de la seguridad de los objetos de la KB.

Esta propiedad se encuentra también a nivel de objeto por lo que será posible personalizar la forma en que se implementará la seguridad en ese objeto.

Hay tres valores posibles:

- **None:** indica que el objeto será público, es decir no tendrá seguridad.
- **Authentication:** indica que sólo usuarios autenticados podrán ejecutarlo.
- **Authorization:** indica que el usuario además de haberse autenticado, tendrá que estar autorizado para ejecutar dicho objeto, es decir tener el rol adecuado para ejecutarlo.

GAM Integration



Una vez que tengamos las propiedades de seguridad configuradas se van a importar en forma automática los objetos de GAM en la KB y luego deberemos hacer un Rebuild All de la misma.

Al hacerlo, se abrirá un cuadro de diálogo que nos avisa que se instalará el módulo GAM en nuestra KB, con la solución lista tanto para web como para Smart Devices.

GAM además está preparado para ejecutar en una base de datos independiente de la base de datos de la aplicación si así lo deseamos, no deberemos preocuparnos por esta estructura en ese caso ya que cuenta con un Schema propio y estará asociado a un Data Store Independiente en la KB, con lo cual toda la configuración es independiente. Además GAM se encargará de inicializar y luego mantener toda la base de datos actualizada.

DEMO: Integrate GAM into Knowledge Base

A continuación vamos a ir a GeneXus y vamos a utilizar GAM.

Enable Integrated Security

The screenshot shows the GeneXus KB Explorer interface on the left and the Properties dialog on the right. The KB Explorer shows a tree view with 'EventDay' selected. The Properties dialog shows the 'Version: EventDay' section with various settings. The 'Enable Integrated Security' property is highlighted in blue and set to 'True'. Below it, the 'Integrated Security' section is also highlighted in blue and set to 'True', with 'Integrated Security Level' set to 'False'.

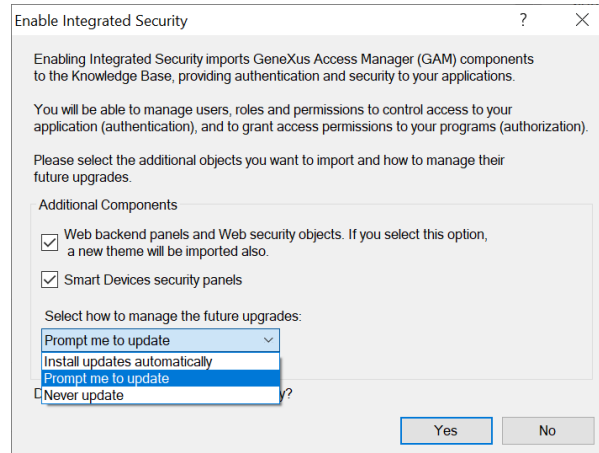
Version: EventDay	
Significant attribute name length	30
Significant table name length	30
Significant object name length	128
Preserve Table Casing	True
Generate prompt programs	Yes
LIKE escape character	None
Enable Integrated Security	True
Integrated Security	
Integrated Security Level	False

Vamos a ir a las propiedades de la Base de Conocimientos.

hacemos click sobre EventDay. el nombre de la KB.

vamos a habilitar GAM, ponemos en la propiedad Enable Integrated Security el valor True.

Enable Integrated Security



Este dialogo nos indica que se va a proceder con la integración.

Aquí podemos indicar si deseamos que se integre el backend web y con este otro si deseamos que se integre la seguridad para los paneles de Smart Devices.

Con este combo podemos elegir como deseamos que se actualice este modulo, puede ser automático, podemos elegir que nos pregunte o que nunca se actualice. presionamos Yes.

Además, en background se están importando los objetos de GAM.

Integrated Security Level

Integrated Security Level <table border="1"> <tr> <td>Integrated Security Level</td> <td>Authentication</td> </tr> <tr> <td>Application ID</td> <td>None</td> </tr> </table>		Integrated Security Level	Authentication	Application ID	None		
Integrated Security Level	Authentication						
Application ID	None						
Web specific <table border="1"> <tr> <td>Login Object for Web</td> <td>Authorization</td> </tr> </table>		Login Object for Web	Authorization				
Login Object for Web	Authorization						
Application ID	b3356369-b037-4216-982e-cbf8cfdc6a73						
Web specific <table border="1"> <tr> <td>Login Object for Web</td> <td>GAMEExampleLogin</td> </tr> <tr> <td>Not Authorized Object for</td> <td>GAMEExampleNotAuthorized</td> </tr> </table>		Login Object for Web	GAMEExampleLogin	Not Authorized Object for	GAMEExampleNotAuthorized		
Login Object for Web	GAMEExampleLogin						
Not Authorized Object for	GAMEExampleNotAuthorized						
SmartDevices specific <table border="1"> <tr> <td>Login Object for SD</td> <td>GAMSDLogin</td> </tr> <tr> <td>Not Authorized Object for</td> <td>GAMSDNotAuthorized</td> </tr> <tr> <td>Change Password Object f</td> <td>GAMSDChangePassword</td> </tr> </table>		Login Object for SD	GAMSDLogin	Not Authorized Object for	GAMSDNotAuthorized	Change Password Object f	GAMSDChangePassword
Login Object for SD	GAMSDLogin						
Not Authorized Object for	GAMSDNotAuthorized						
Change Password Object f	GAMSDChangePassword						

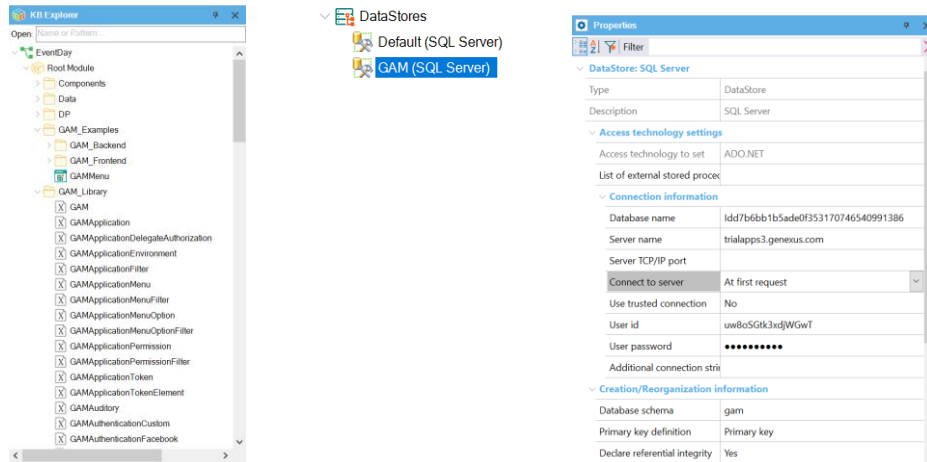
Ahora vean que tenemos disponible la propiedad Integrated Security Level.

En esta propiedad podemos indicar si deseamos habilitar solo autenticación que es el valor por defecto, si deseamos autorización o si no deseamos tener seguridad. esto a nivel de base de conocimiento.

Además se asigna un Application ID que se utilizara en el repositorio de GAM para identificar a la aplicación.

Ahora ya tenemos las propiedades donde indicamos los objetos de login, uno en caso de error de autorización y otro para cambiar la contraseña.

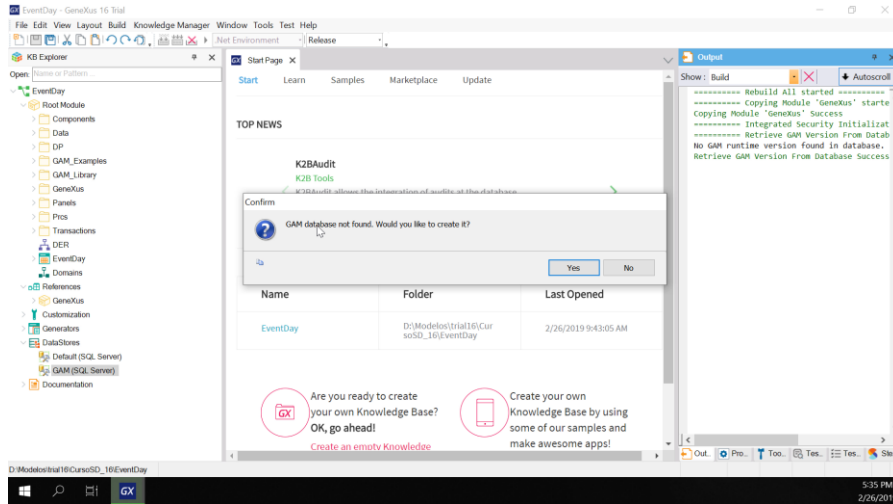
GAM Objects & Data Store



En la KB ya podemos ver que se crearon algunos folders en el root module. Gam_Examples que son objetos de ejemplo que podemos modificar. Acá estarán los objetos del backend y del frontend tanto para web como para SD. Y Gam_Library con la API, estos son todos objetos externos.

Además tenemos un nuevo Data Store, GAM, con la información de esa conexión. Por defecto se asume la misma base que el Data Store default pero tenemos un schema propio para las tablas.

Creating GAM Database



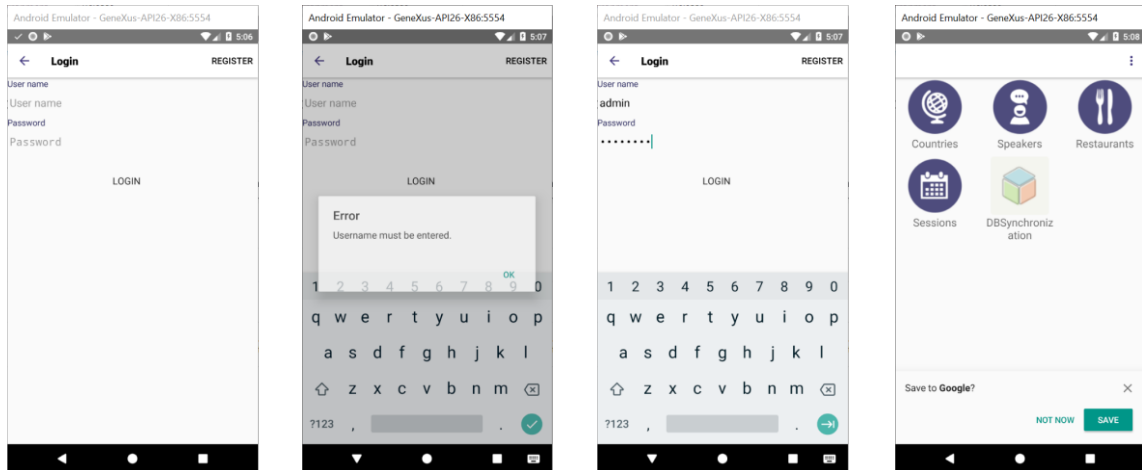
Bien, como termino el proceso de importación, vamos a hacer un Rebuild All de la aplicación.

GeneXus nos indica que la base de datos de GAM no se encontró y si deseamos crearla, vamos a poner que si.

bien, ahí se crea la base de datos con todas las tablas y luego se inicializa la base de datos.

vamos a esperar que termine de generar.

Login in Smart Devices



Bien, ya tenemos la aplicación.

Y ahora si vamos al emulador, lo primero que vemos es la pantalla de login.

Y si deseamos ingresar sin usuario nos da un error. todo esto nos provee GAM en forma automática.

Para ingresar vamos a usar un usuario que se crea por defecto, "admin", la contraseña es "admin123".

Y ahí si se abre nuestra aplicación, no vamos a guardar las credenciales.

Y la aplicación sigue funcionando normalmente.

Login in Web

The screenshot displays the GeneXus Access Manager web interface. At the top, there is a dark blue header with the text "GeneXus Access Manager - Introduction" on the left and the "GeneXus™" logo on the right. Below the header, the main content area is divided into three sections:

- DEVELOPER MENU:** A red header with white text. Below it, there are three tabs: "Web Objects", "Install iOS Apps", and "Install Android Apps". Under "Web Objects", there is a "Browse Web Objects" section with a grid of 15 icons representing various web objects, including "ChatMessages", "Device", "GAMEexampleChange...", "GAMEexampleChange...", "GAMEexampleLogin", "GAMEexampleNotAuth...", "GAMEexampleRegister", "GAMEexampleWWWApp", "GAMEexampleWWWAuth...", "GAMEexampleWWWCon...", "GAMEexampleWWWDev", "GAMEexampleWWWRep...", "GAMEexampleWWWRoles", "GAMEexampleWWWSec", "GAMEexampleWWWUsers", "GAMHome", "GAMSSOLogin", "Home", "WWComperly", "WWComperly", and "WWCoerity".
- LOGIN:** A central white login form with a red "LOG IN" button. The form includes fields for "User Name" and "Password", checkboxes for "Keep me logged in" and "Remember Me", and a red "LOG IN" button. Below the button, there is a link for "FORGOT YOUR PASSWORD? or create an account".
- Application Name:** A red header with white text. Below it, there is a "Recents Home" section with a list of links: "Companies", "Countries", "Restaurants", "Rooms", "Sessions", "Session Favorites", "Speakers", "Tracks", and "Users".

Ahora si vamos al web. acá tenemos el Developer Menu.

Si intentamos ingresar a un objeto, por ejemplo a home nos va a redirigir a la pantalla de login.

vamos a usar el mismo usuario. "admin". "admin123". y accedemos.

Y ahí si recién podemos acceder a los objetos y la web sigue funcionando normalmente.

Con esto terminamos la introducción, en el próximo video veremos mas detalles de GAM.

GeneXus™

Videos	training.genexus.com
Documentation	wiki.genexus.com
Certifications	training.genexus.com/certifications