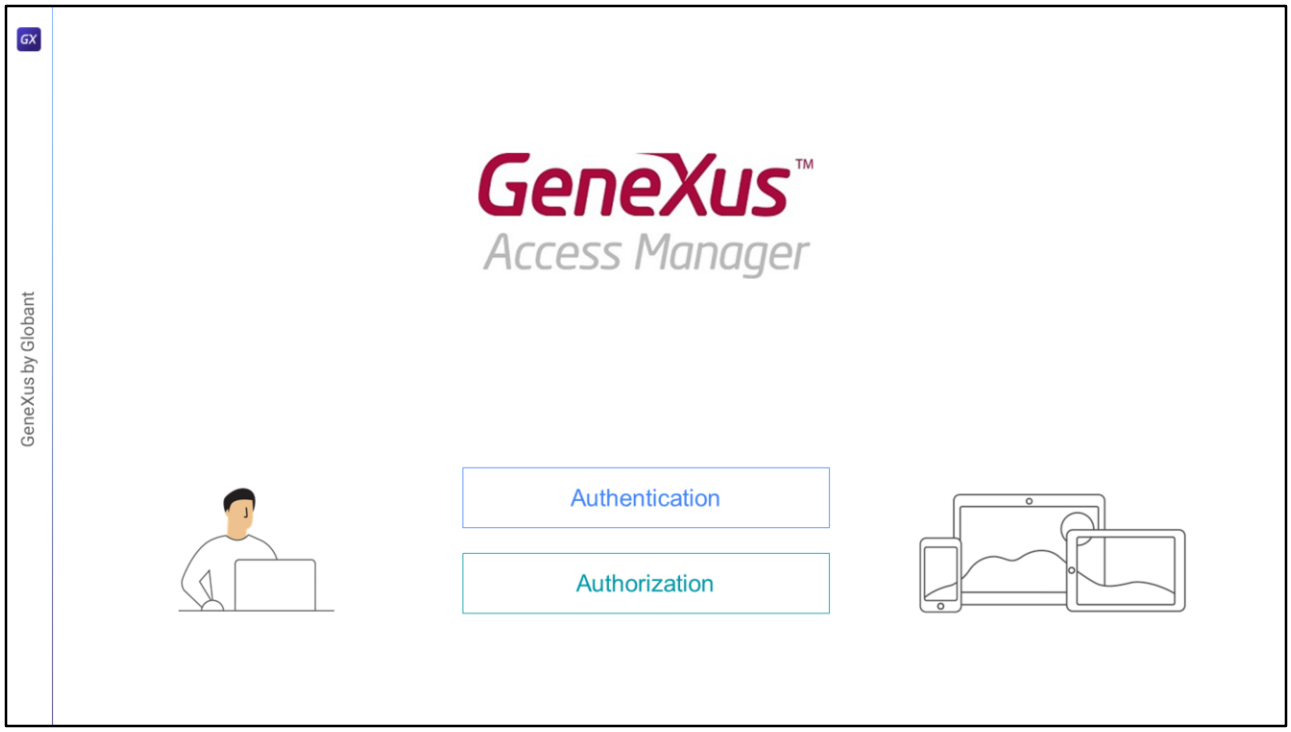
GeneXus by Globant

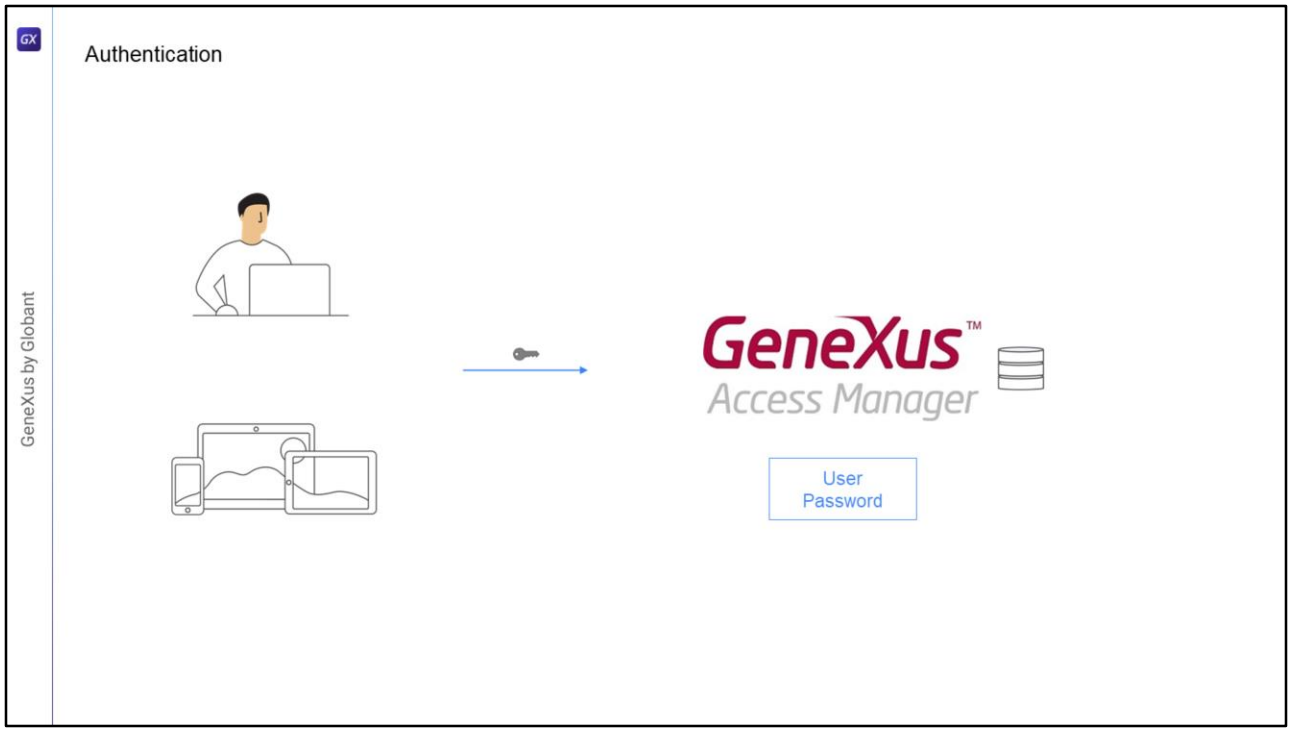
GeneXus Access Manager

Authentication and Authorization

Diego Marranghello



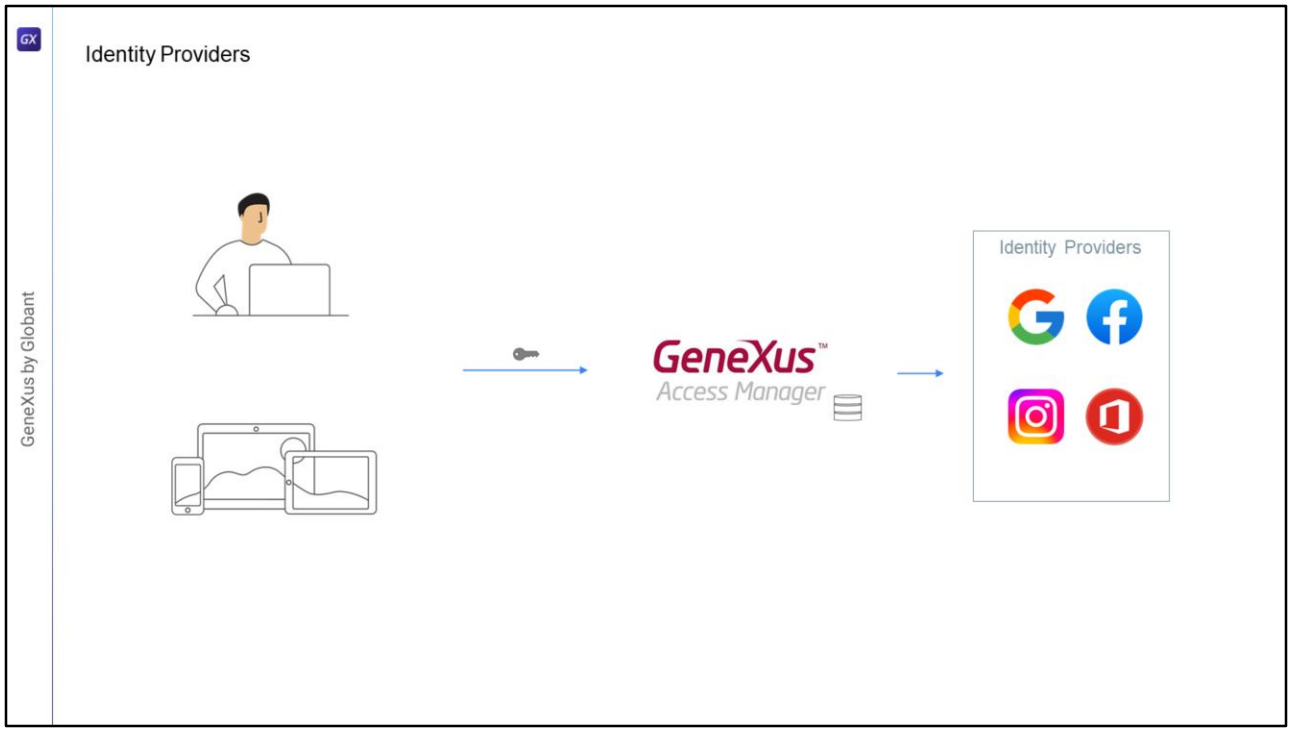
En este video veremos un poco mas de las características de Autenticación y Autorización utilizadas en GAM.



La autenticación es el proceso de verificar que un usuario es quien dice ser mediante la validación de sus credenciales, en el caso de GAM: usuario y contraseña.

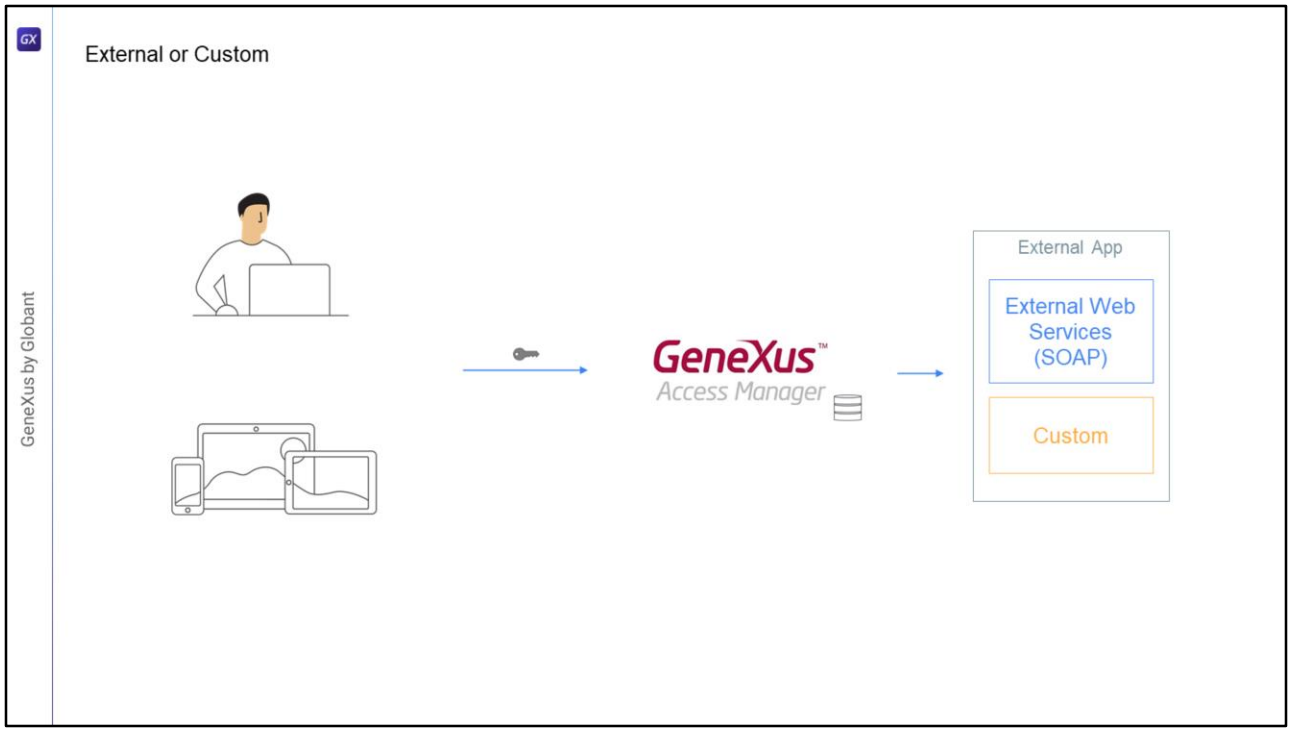
Es posible implementar diferentes tipos de autenticación, incluso pueden habilitarse más de uno en forma simultanea.

Los tipos son:
Local: Donde las credenciales del usuario estarán almacenadas en la base de datos de GAM en la tabla de usuarios.



Otra opción es Utilizando un Proveedor de Identidad: los Identity Providers que podemos utilizar son varios, por ejemplo Google, Facebook, Instagram, Office 365, etc., en estos casos en la base de datos de GAM solo estará almacenado el ID del usuario en la tabla de usuarios, esto se utiliza para asignar por ejemplo el ROL a un usuario, y luego las credenciales del usuario serán gestionadas por el Identity Providers elegido.

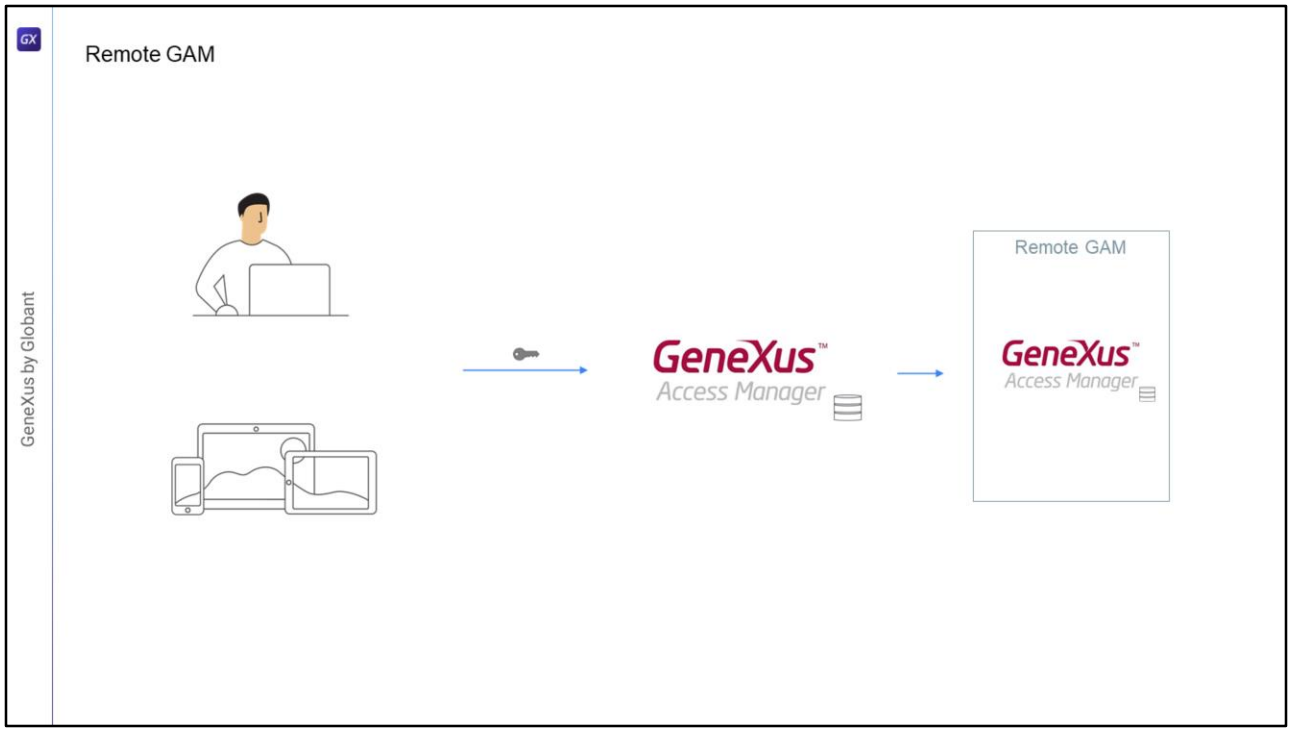
Al momento de autenticar al usuario, este será redireccionado al proveedor de identidad, donde el usuario ingresara sus credenciales, en caso satisfactorio este proveedor retornara a al sitio nuevamente.



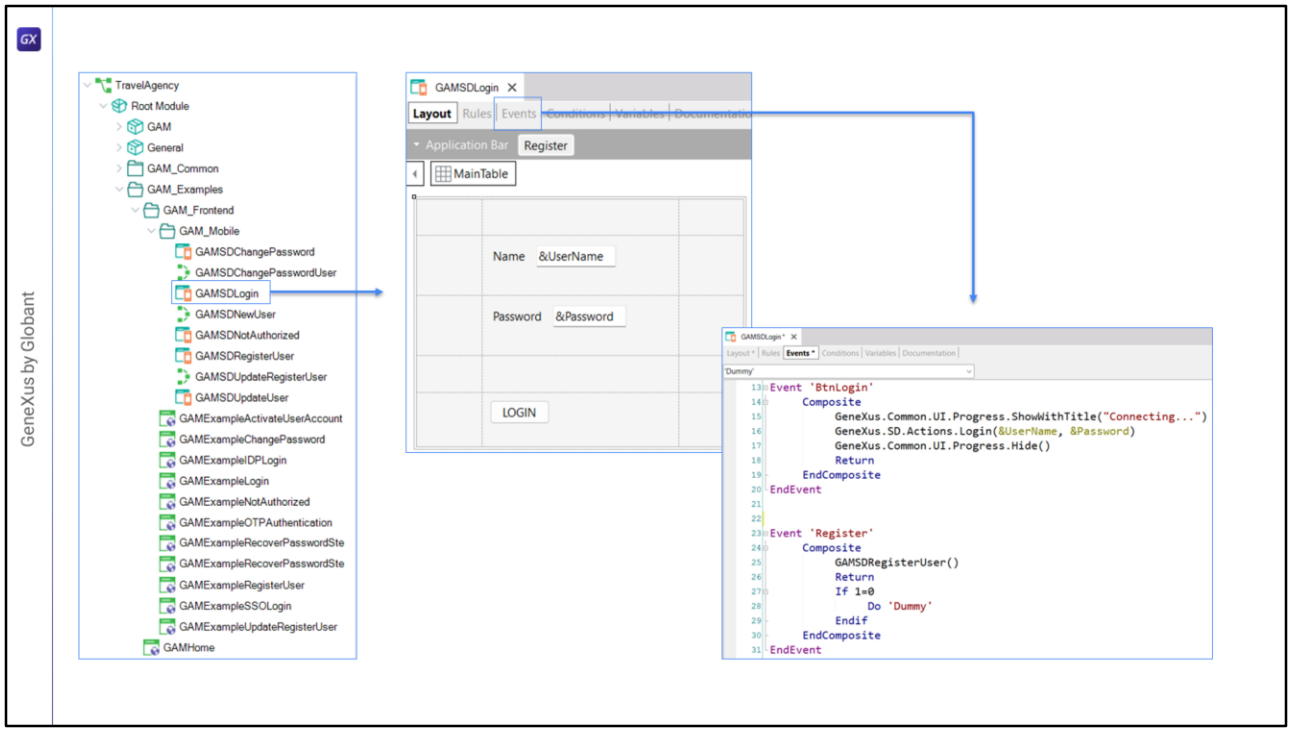
Si utilizamos autenticación Externa, se debe configurar GAM para interactuar con un proveedor externo, el cual puede utilizar Web Services u otro mecanismo personalizado.

En este caso al igual que en el anterior, en GAM solo se almacena información mínima del usuario ya que la validación de las credenciales de acceso se llevan a cabo en otro sistema.

En estos casos GAM nos provee facilidades para mapear los roles definidos en GAM con los roles externos.



También podemos usar GAM Remoto ya que GAM en si es un Identity Provider, que manejara las credenciales del usuario, por lo que podemos configurar que una aplicación utilizando GAM valide las credenciales del usuario en otra instancia de GAM que hará el rol de proveedor de identidad.

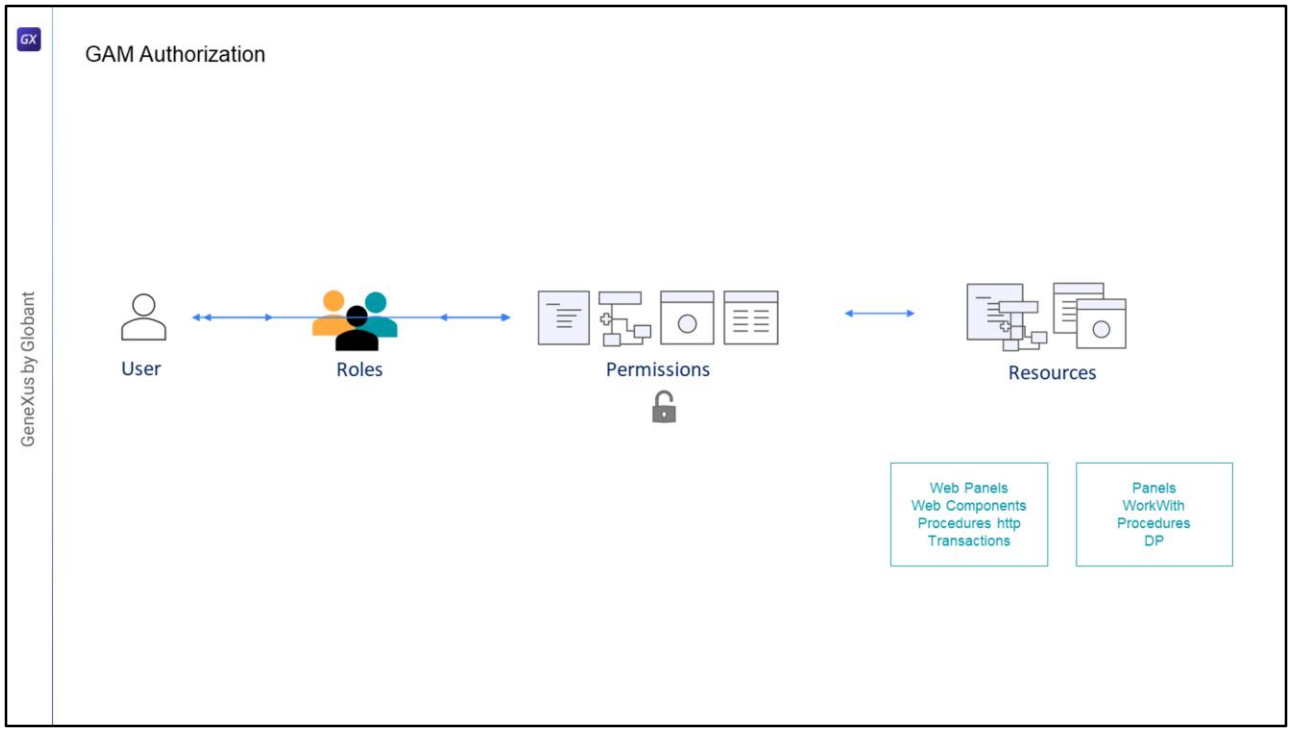


Para realizar la Autenticación, GAM nos proveerá de dos objetos, un Web Panel, para web, y un Panel, que en este caso lo utilizaremos para mobile, estos paneles pueden ser personalizados si lo deseamos.

En particular, para mobile, dentro del Folder Gam_Examples encontraremos el Folder Gam_FrontEnd y dentro de este otro folder con nombre GAM_Mobile con objetos que resuelven el Login, el cambio de contraseña, la registración de nuevos usuarios o la actualización de los datos del usuario.

Por ejemplo este es el panel de Login, GAMSDLogin que implementa eventos para realizar el login y la registración de nuevos usuarios.

Un aspecto importante de este panel es que cuando la aplicación mobile sea Offline, este panel deberá ejecutar Online, o sea que el usuario debe tener una conexión al server para poder acceder.



Con GAM también podremos resolver la autorización, que es el proceso de verificar si un usuario que ya fue autenticado, posee los permisos necesarios para realizar alguna acción en el sistema.

Para esto GAM cuenta con un esquema basado en Roles de Usuario, cada usuario en GAM tiene asociado uno o varios Roles, además tendremos los Recursos asegurados y la asignación de Permisos sobre estos Recursos a los Roles.

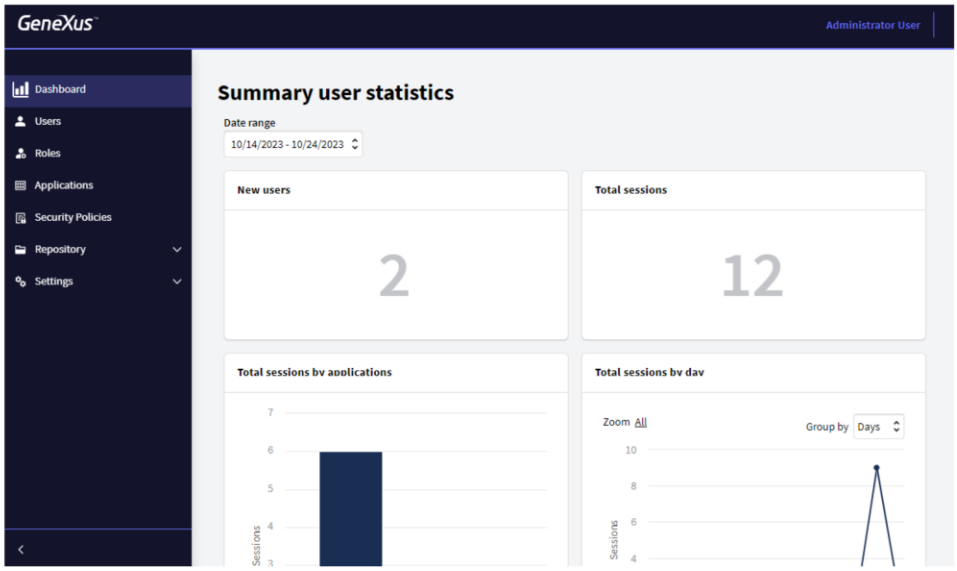
Los recursos que podemos asegurar son:
Web Panels
Web Components con Acceso por URL habilitado
Procesos con Protocolo HTTP, por ejemplo reportes con salida a PDF
Transacciones, en este caso podemos además de ejecutar, personalizar también el modo Insert, Update, Delete o dar acceso Full a una transacción.

En el caso de aplicaciones ONLINE para dispositivos móviles los recursos a asegurar son:
Panels
WorkWith
Procesos o Data Providers con protocolo Rest

En el caso de Aplicaciones para dispositivos móviles Offline solo contaremos con la autenticación, ya que al ser offline la aplicación no podremos mantener los permisos, ya que si los modificamos puede que algunos dispositivos no se sincronicen por lo que el esquema es inviable.

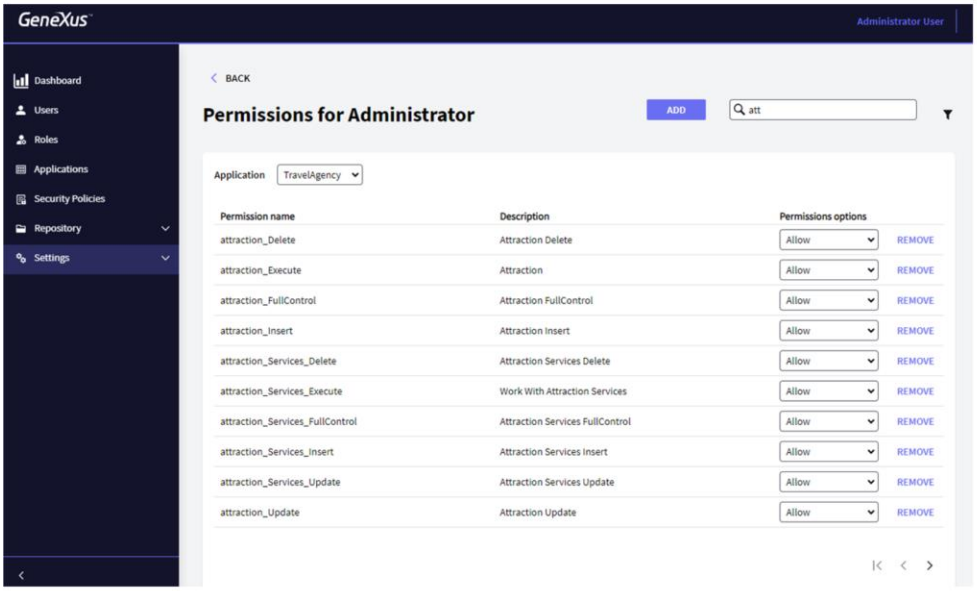
GeneXus by Globant

BackOffice Web



Para manejar toda esta información, GAM nos provee un backoffice web, que nos permitirá administrar usuarios, roles, permisos y otras configuraciones de la aplicación como son los tipos de autenticación y demás parámetros de configuración.

GAM Authorization: Permissions



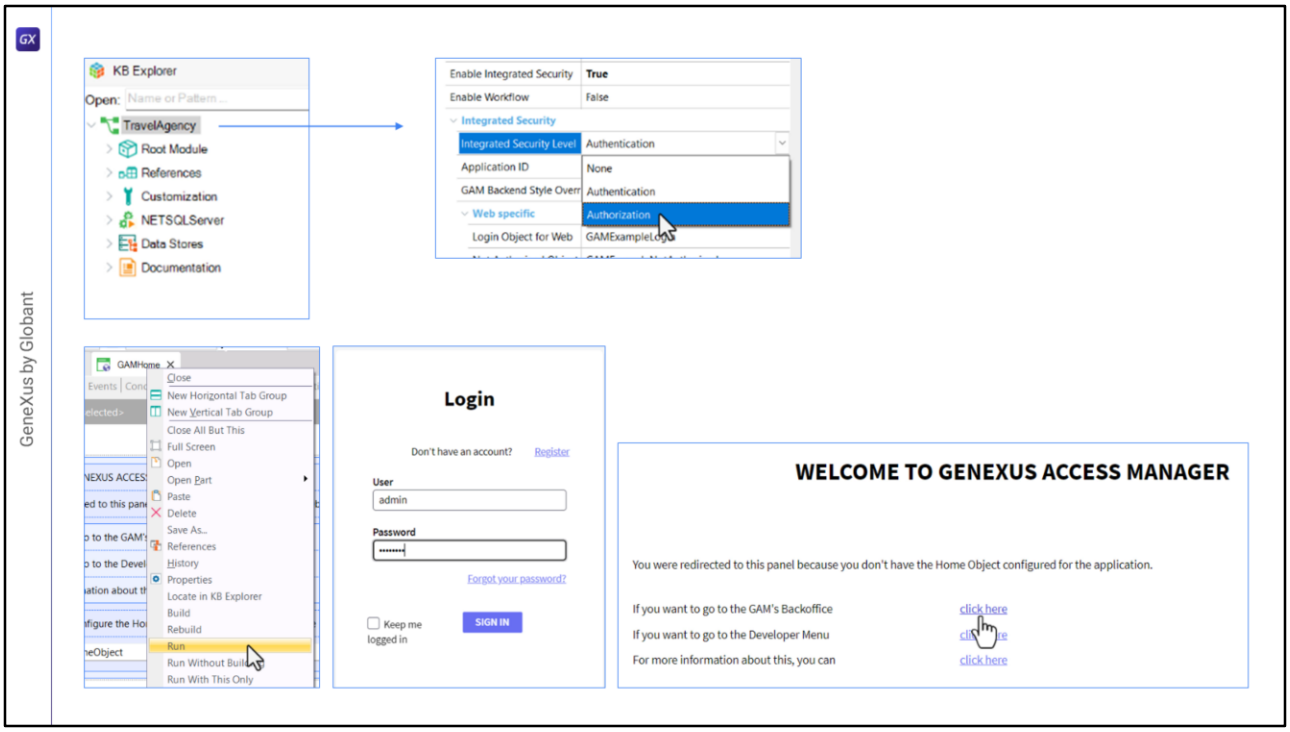
GeneXus by Globant

Una de las facilidades que nos brinda GAM es que para cada aplicación se encargara de generar los recursos sobre los cuales hay luego que dar los permisos.

Podemos ver que tenemos por un lado los permisos de la transacción Atraction, tenemos uno para cada modo (insert, update y delete) , además uno para la ejecución, y otro que dice FullControl.

Luego también vemos que aparecen recursos con el nombre Atraction_Services, estos se refieren a la transición cuando es utilizada como BC y expuesta como REST, o cuando se utiliza en el objeto WorkWith

Al seleccionar un rol con FullControl estamos dando todos los permisos sobre esa transacción, ejecución y cada uno de los modos los cuales se mostraran como heredados.



Vamos a ver todo esto que hablamos en GeneXus.

En la KB que estamos viendo, ya prendimos previamente la propiedad Enable Integrated security en true, en el nodo de la versión de la base de conocimiento.
Y dejamos todo por defecto, por lo que el nivel de seguridad está en Authentication.

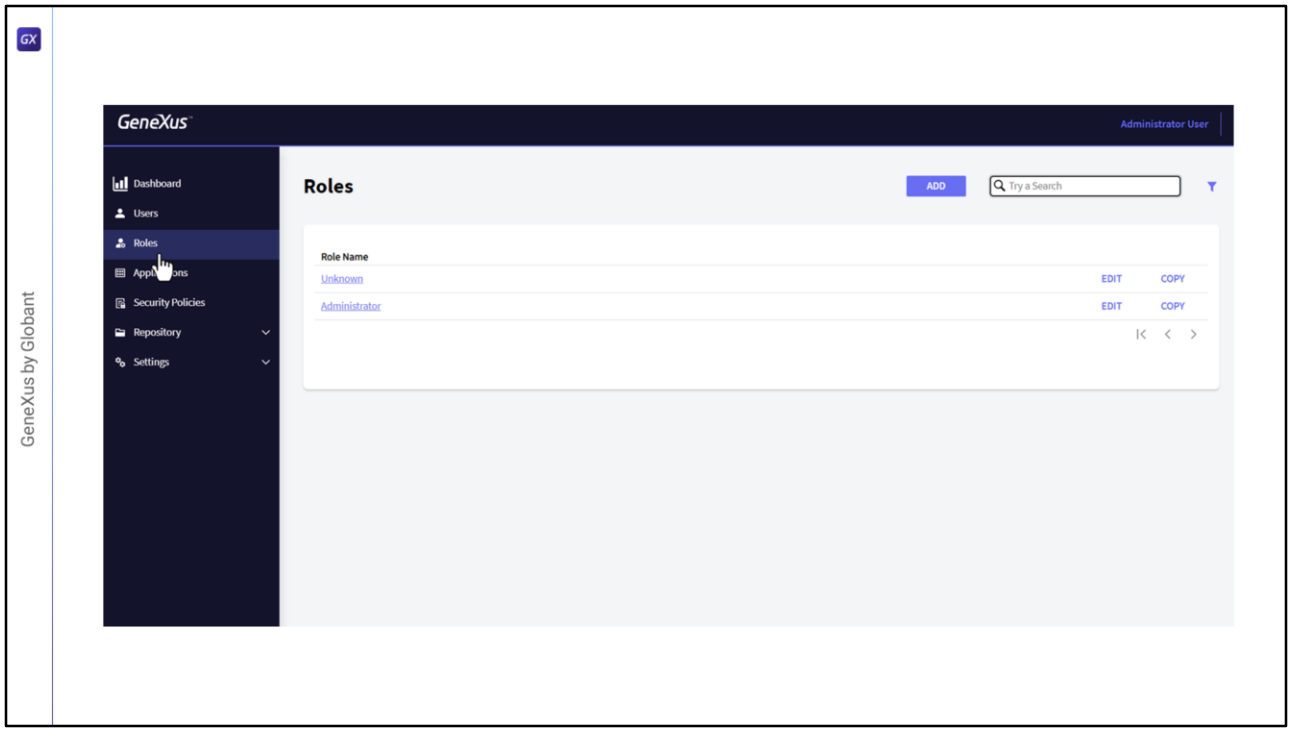
Ahora lo cambiaremos a Authorization, luego de cambiar esta propiedad hay que hacer un Rebuild All de la aplicación.

Entonces ahora nuestra aplicación esta lista para, además de autorizar, autenticar a los usuarios, o sea manejar sus permisos.

Primero vamos a ejecutar el objeto GAMHome, el cual deberá tener la propiedad main program en true para que podamos ejecutarlo directamente.

Nos pedirá el login, usamos el único usuario que tenemos creado por defecto: admin, y la contraseña admin123.

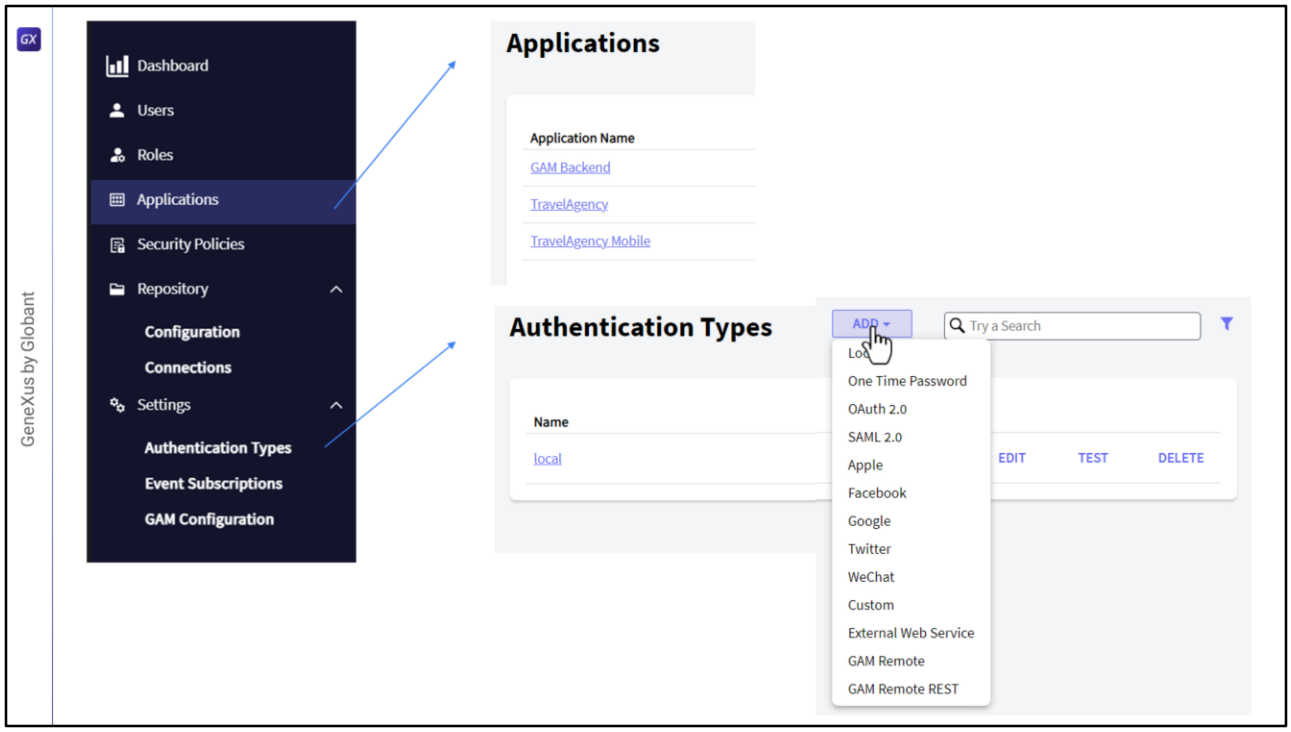
Seleccionamos para ingresar al Backoffice del GAM, vamos a la sección de Usuarios, y aquí podemos crear o editar la información de los usuarios.



Luego Tenemos Roles, aquí podemos definir los roles que deseemos, por defecto hay 2 roles definidos, Administrator que tiene acceso a todas las funcionalidades tanto del backend como permisos sobre todos los objetos del front end.

El otro rol es Unknown, este rol sirve cuando permitimos que los usuarios se auto registren en la aplicación, o sea cuando se auto registran los usuarios quedan asociados a este rol.

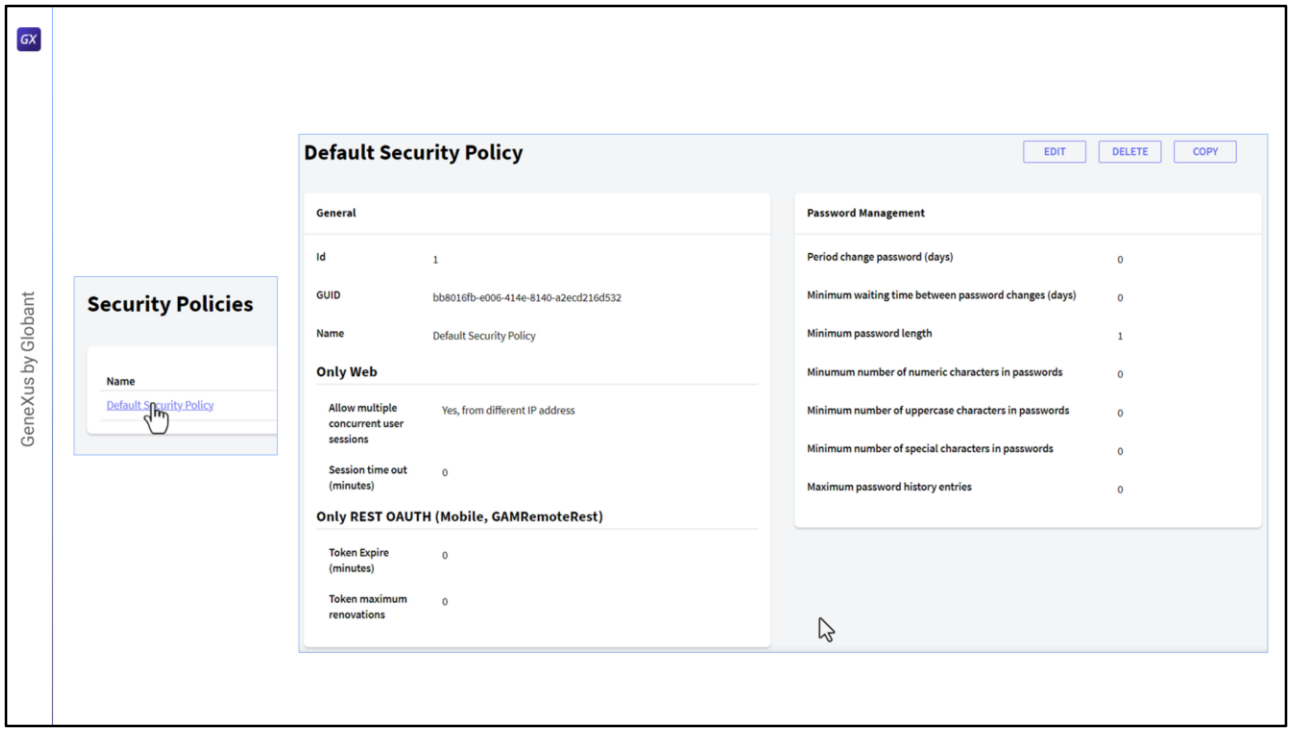
Podemos cambiar cual es el rol por defecto que se usa en este caso.



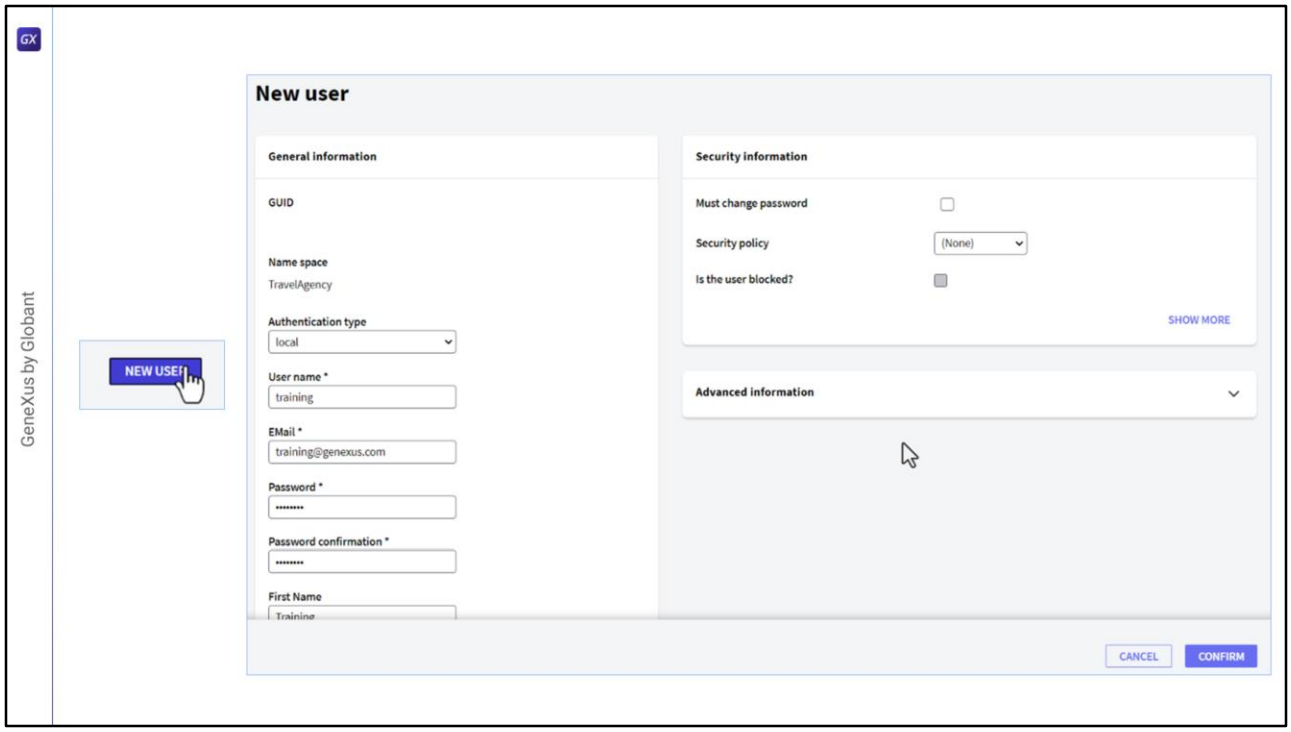
Y en este menú tenemos acceso a toda la configuración de GAM.

Tenemos las aplicaciones, vean que en este caso tenemos definidas 3 aplicaciones, la aplicación GAM que tiene todo el backend de GAM, la aplicación WEB y la aplicación Mobile, que en este caso ambas tienen el mismo nombre, vamos a editar y cambiar la de mobile para diferenciar.

En el menú tenemos acceso además a configurar por ejemplo a la administración de los tipos de autenticación que vimos, por defecto se usa la autenticación Local, pero con Add podríamos agregar otro tipo, y acá elegimos el tipo que queremos agregar.

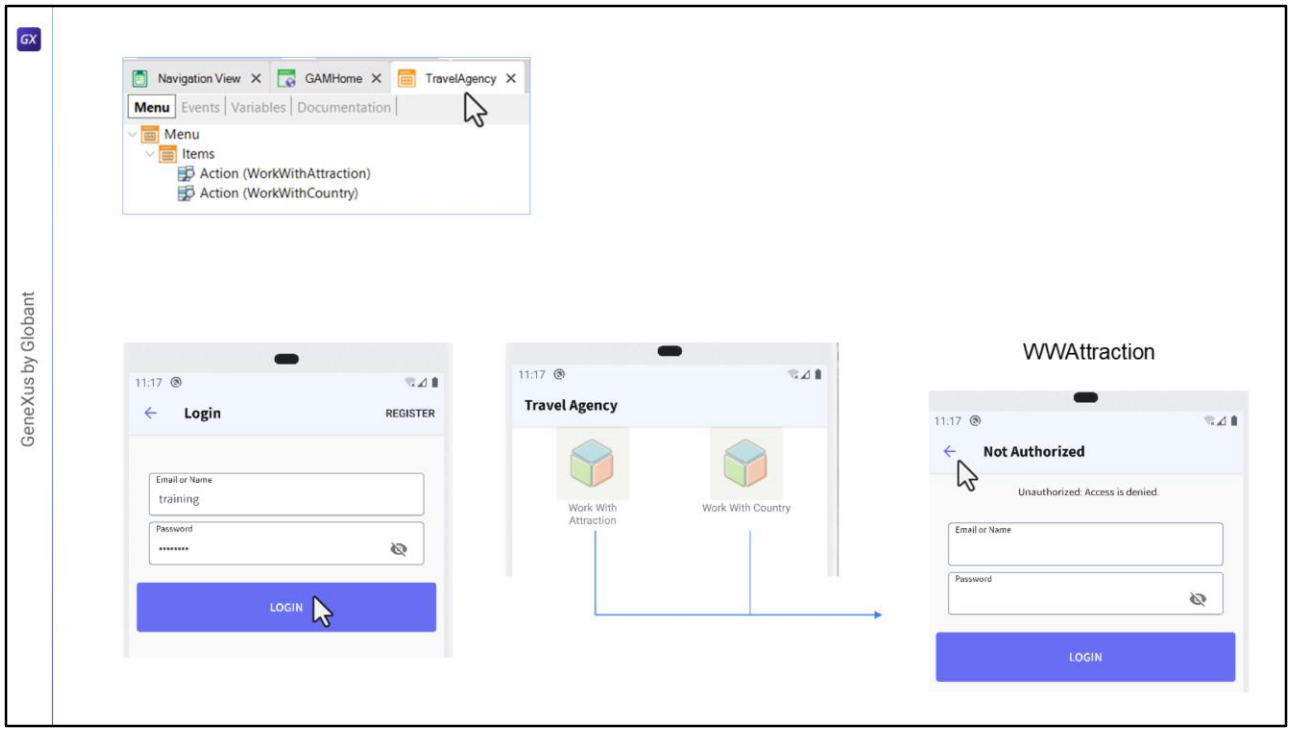


Tenemos por ejemplo políticas de seguridad, veamos como esta configurada la política default, por ejemplo para mobile podemos elegir el tiempo de expiración de los tokens de seguridad. Acá por ejemplo, tenemos el periodo en días para obligarle a cambiar la contraseña al usuario, el largo mínimo de la contraseña, etc. Un montón de parámetros que podemos predefinir, y podemos crear varias políticas, una para usuarios de backoffice, otra para usuarios mobile, etc, lo podemos manejar de forma flexible.



Bien, lo que vamos a hacer es crear un nuevo usuario.

Vamos a usuarios, Agregar y vamos a ingresar training como User Name, como mail ingresamos training@genexus.com , de contraseña ponemos training, confirmamos de vuelta la contraseña, de nombre training y apellido GeneXus , el resto dejamos todo por default, asignamos una política, la única que tenemos y confirmamos.



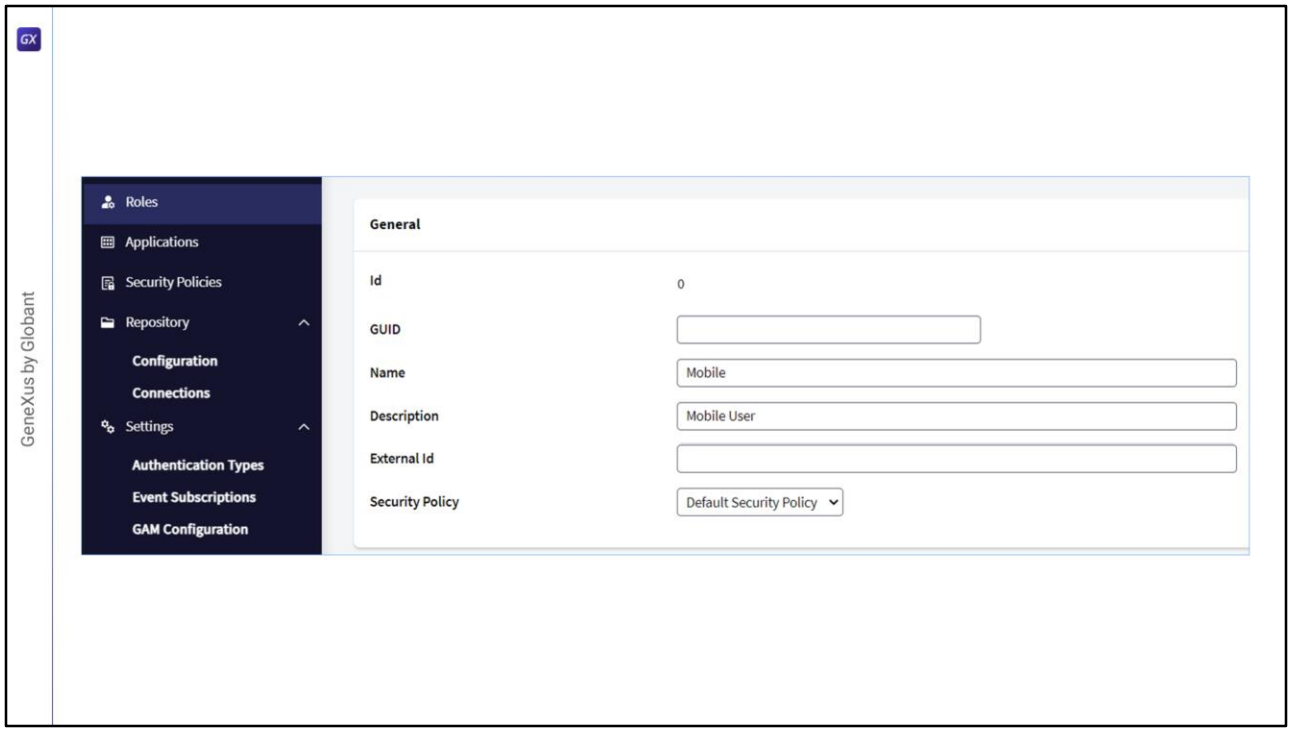
En nuestra KB, tenemos creado un objeto Menu, declarado como startup object, y que tiene los siguientes objetos WorkWith como Items, el de país y el de atracción.

Al ejecutar, nos abre la aplicación en el emulador, y lo primero que nos pide son las credenciales de acceso.
Ingresamos el usuario que acabamos de crear: usuario training, y misma contraseña.

Y ahí deja acceder al menú con los ítems que teníamos ingresados. En este caso, el menú no requiere permisos especiales, solo con que el usuario este autenticado lo podemos ver.

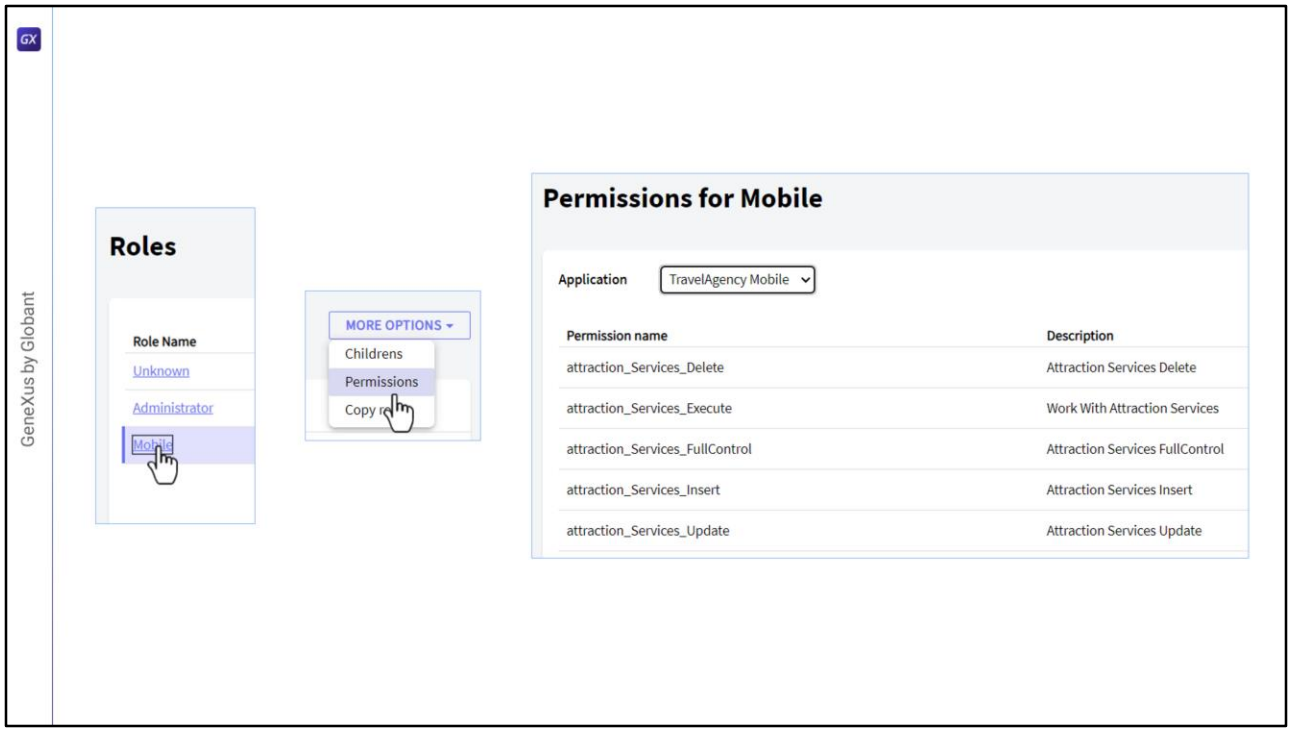
Pero si queremos acceder a las opciones, por ejemplo a las Atracciones, da acceso no autorizado.
En países, lo mismo.

Esto es porque configuramos la aplicación para nivel de seguridad Autorización, pero aún no le hemos dado ninguna autorización al usuario, solo lo creamos.



Volvamos a la pantalla Web para manejar estos permisos.

Ahora vamos a crear un Rol, vamos a poner Rol “Mobile”, la descripción Mobile User. Asociamos también una política al Rol y confirmamos.

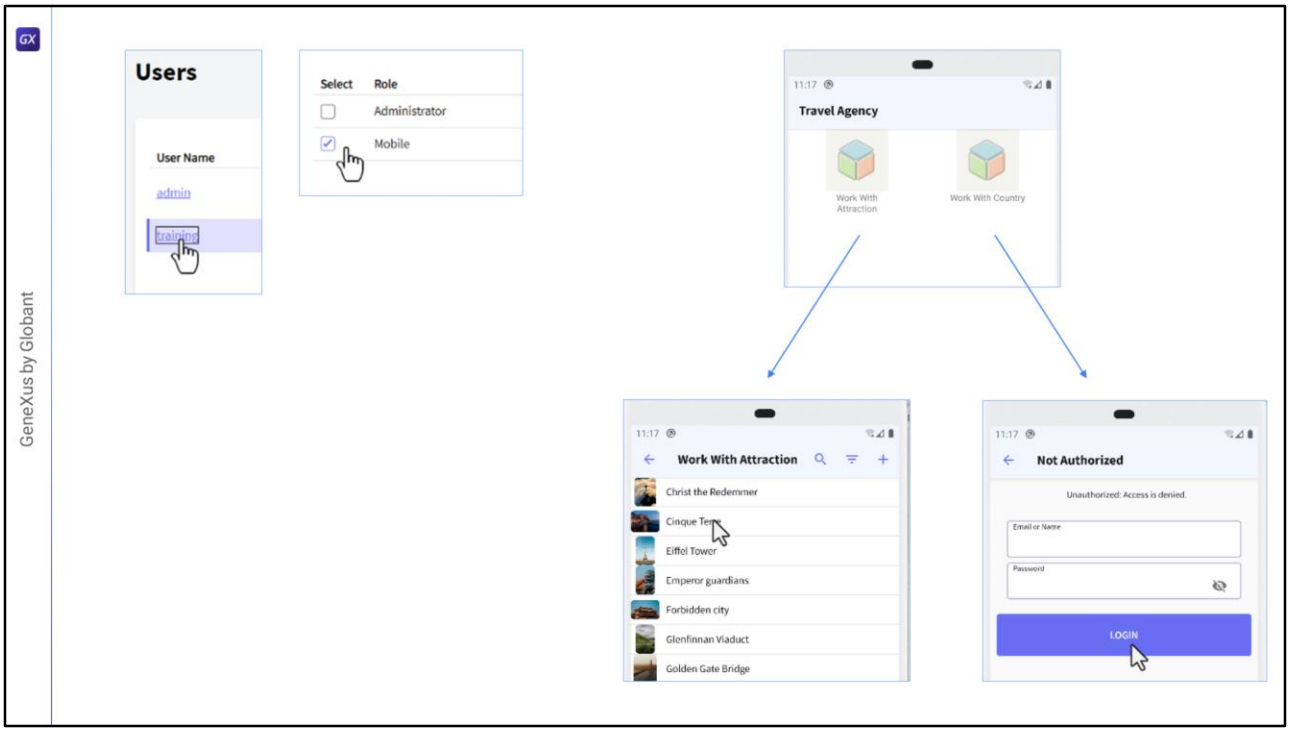


Bien, ahora tenemos que acceder al Rol y darle permisos sobre algunos recursos.
Seleccionamos la aplicación TravelAgency y presionamos Add.
Ahí nos muestra una lista con todos los recursos sobre los que podemos dar permisos.

Vamos a agregar uno para acceder a las atracciones, buscamos atraction, seleccionamos Atraction_Services_FullControl.

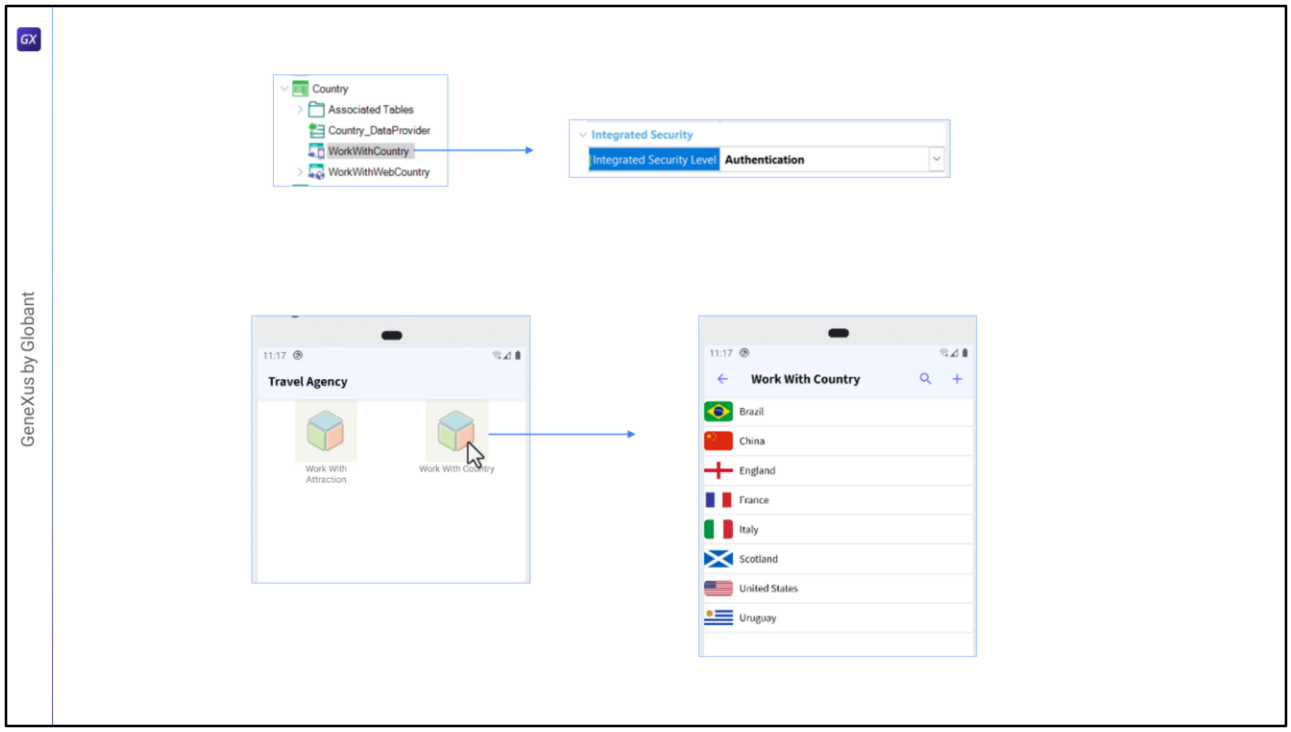
Al seleccionar fullcontrol, vemos que se heredaran todos los permisos sobre las atracciones.

Grabamos.



Ahora vamos a asociar al usuario que creamos este rol.
Hacemos clic en el nombre de usuario, luego en Roles, en la opción Add, y seleccionamos Mobile.
Add Selected y listo.

Y ahora si vamos al emulador y accedemos a las atracciones, ahí sí nos muestra la lista. Y si queremos nos deja ingresar en modo Insert también, ya que le dimos permiso full.
Ahora si vamos a países nos da acceso no autorizado, esto porque para países no dimos ningún permiso aún.



Por ejemplo podríamos desear que para los países no se chequearan los permisos, entonces en el WorkWith Country podemos usar la opción de solo autenticación, otra opción sería poner None.
Vamos a correr la aplicación para que tome este cambio.

Y ahora si accedemos a Países, nos muestra el listado.
Bien, esto fue solo una pequeña muestra de toda la flexibilidad que nos brinda GAM para manejar la autorización y autenticación de los usuarios.
Recuerden que la autorización solo es para aplicaciones OnLine.


GeneXus by Globant
GeneXus™
by Globant
training.genexus.com