GeneXus by Globant

GeneXus Access Manager

Introduction

Diego Marranghello

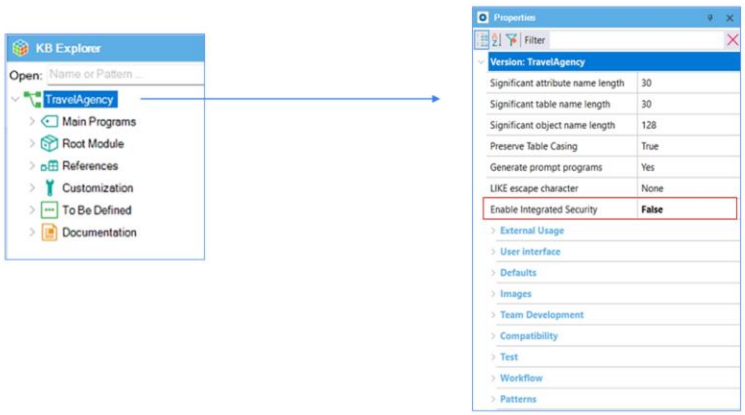
OWASP
Open Web Application Security Project

En el desarrollo de nuestras aplicaciones, existen diversos lineamientos de seguridad que hay que tomar en cuenta. Los más importantes se encuentran descritos en el Open Web Application Security Project, la fundación que gestiona este proyecto, la cual es una comunidad abierta que define y provee información, además de herramientas, para el desarrollo y la verificación de sistemas informáticos desde una perspectiva de seguridad.

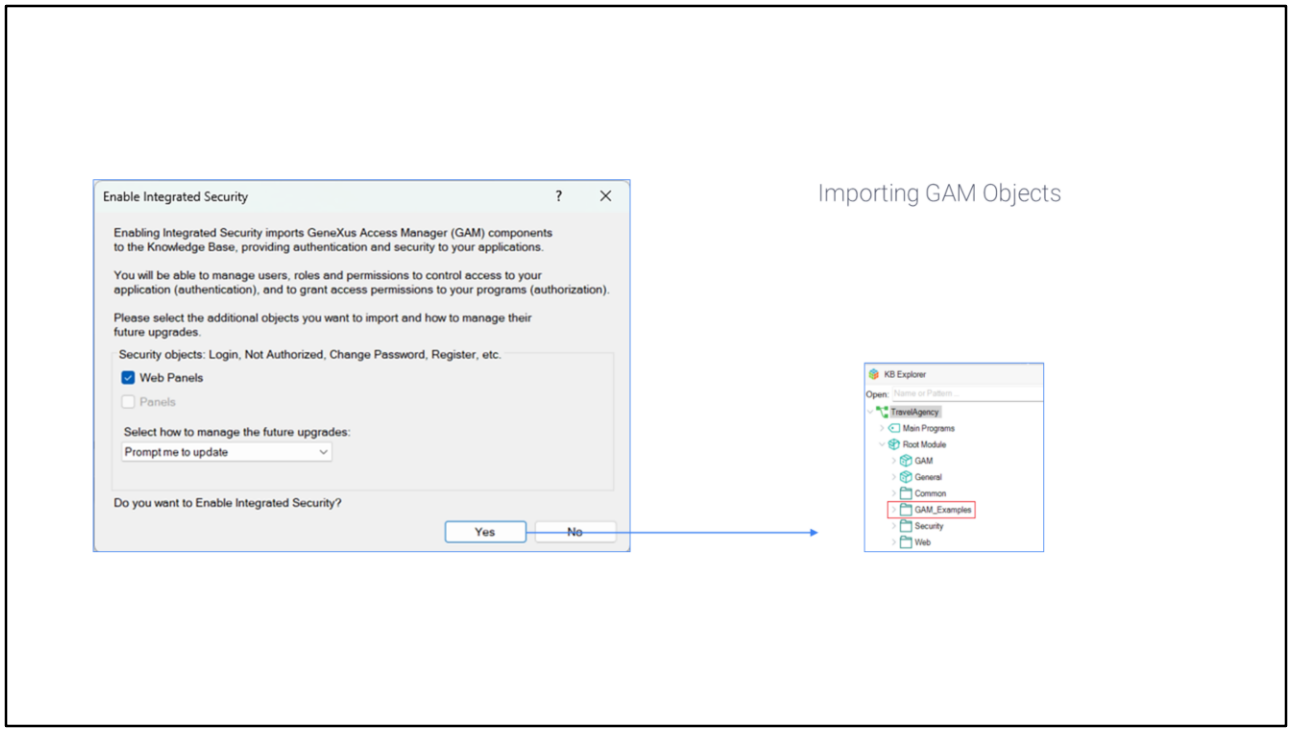
Dentro de la fundación existen varios proyectos, uno de los más destacados y con mayor relevancia es el OWASP Top Ten, un documento que trata sobre los riesgos de seguridad más críticos en las aplicaciones web y móviles. En uno de los puntos del proyecto, habla sobre la "Broken Authentication", donde resalta la importancia de tener un buen factor de autenticación.

Genexus ofrece un módulo denominado "Genexus Access Manager" (GAM) que resuelve la autenticación en forma automática. Además de esta tarea, el GAM también permite solucionar problemas de autorización, es decir, restringir el acceso a distintas partes de la aplicación dependiendo de los roles o permisos de cada usuario. El GAM también nos proporciona diversos objetos para administrar todos los problemas de seguridad relacionados con una aplicación web o para dispositivos móviles. Por ejemplo, objetos para agregar usuarios, asignar roles, otorgar permisos, etcétera.

Enabled Integrated Security

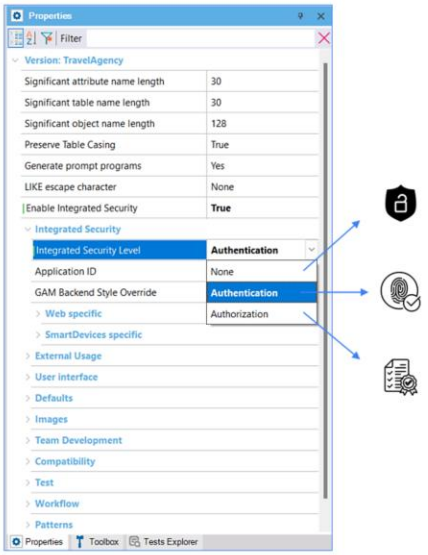


La activación de los controles de seguridad se realiza automáticamente mediante la configuración de la propiedad "Enable Integrated Security" que podemos encontrar en la ventana de preferencias seleccionando la versión activa de nuestra KB.



Al cambiar la propiedad a “True”, se importarán los componentes del Genexus Access Manager a nuestra KB. Bajo Root Module, encontraremos varios objetos encargados de proveer las funciones del GAM.

Integrated Security Level

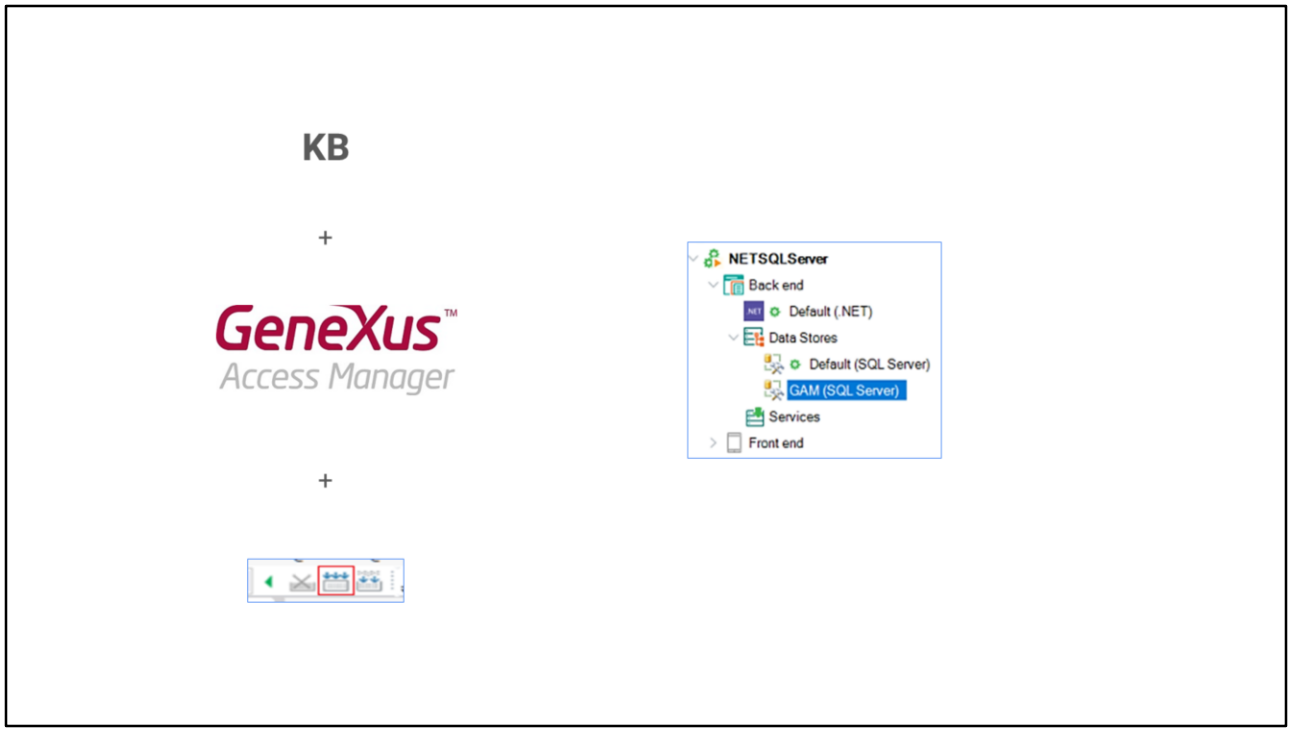


Una vez habilitada la seguridad, se puede seleccionar el nivel de la misma utilizando la propiedad "Integrated Security Level" que podemos encontrar a nivel de la versión de la KB o cada objeto. El valor por defecto de esta propiedad es "Authentication". Algunas opciones para el nivel de seguridad de nuestra aplicación son:

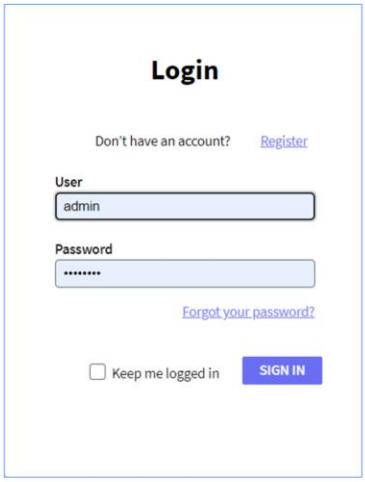
Ninguna, es decir, no aplica ningún mecanismo de seguridad.

Autenticación, donde el usuario necesita solo estar logueado para acceder.

Y autorización, donde el usuario necesita además de estar logueado, tener los permisos necesarios para acceder a cada parte de la aplicación.



Una vez aplicada la seguridad y el tipo de nivel que utilizará nuestra aplicación, necesitamos dar un "rebuild all" a nuestra KB para que se cree la base de datos que utilizará el GAM. Después de que activamos la seguridad, al ejecutar nuestra aplicación se desplegará una pantalla de login tanto para la parte web como para Smart devices.



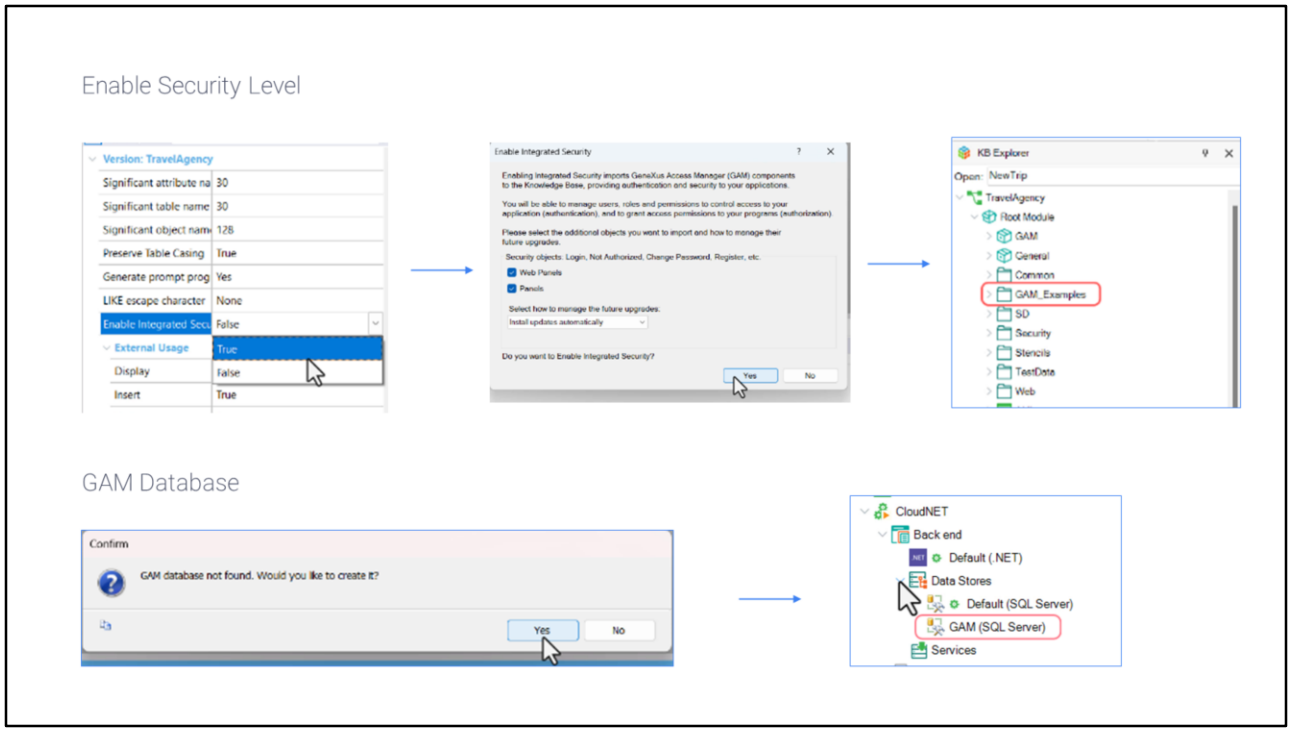
User: admin

Pass: admin123

Como aún no hemos configurado usuarios, podemos utilizar un usuario local con las siguientes credenciales: usuario: admin y contraseña: admin123. Para acceder a la consola de administración del GAM, debemos acceder al panel "GAM Home".

Este panel es el objeto backend principal del GAM, donde podemos configurar los usuarios y los permisos de nuestra aplicación. Veamos una pequeña demostración.

En nuestro ejemplo, queremos que diferentes usuarios puedan, dependiendo de su rol, visualizar nuestra aplicación web backoffice. Si se autentican, dependiendo de su rol, puedan ver ciertas opciones.

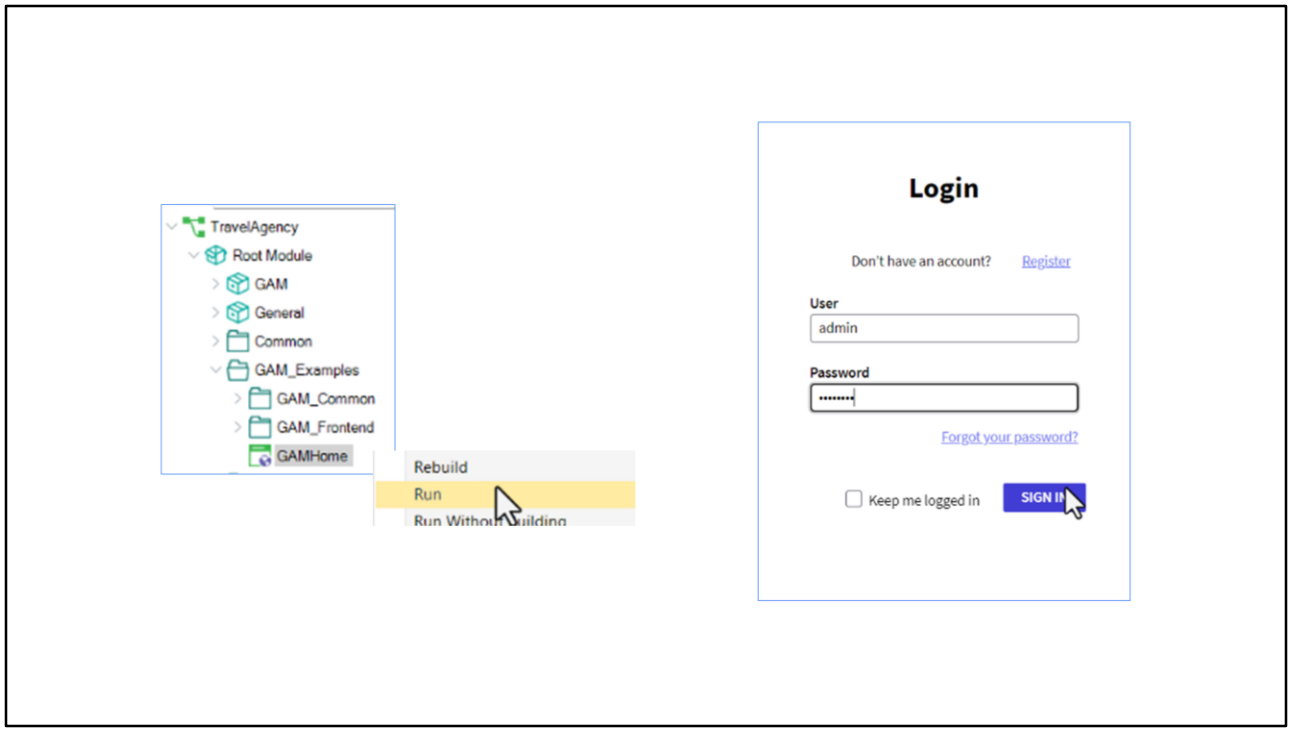


En lo que sigue, aplicaremos el módulo de seguridad a nuestra KB Travel Agency para solventar esto. Para ello, primero nos posicionamos en la versión activa de la KB. Posteriormente, cambiamos la propiedad "Enable Security" a true. Se desplegará una pantalla solicitando el permiso para la importación de componentes para el manejo del módulo del GAM, tanto para nuestra aplicación web como para Smart devices.

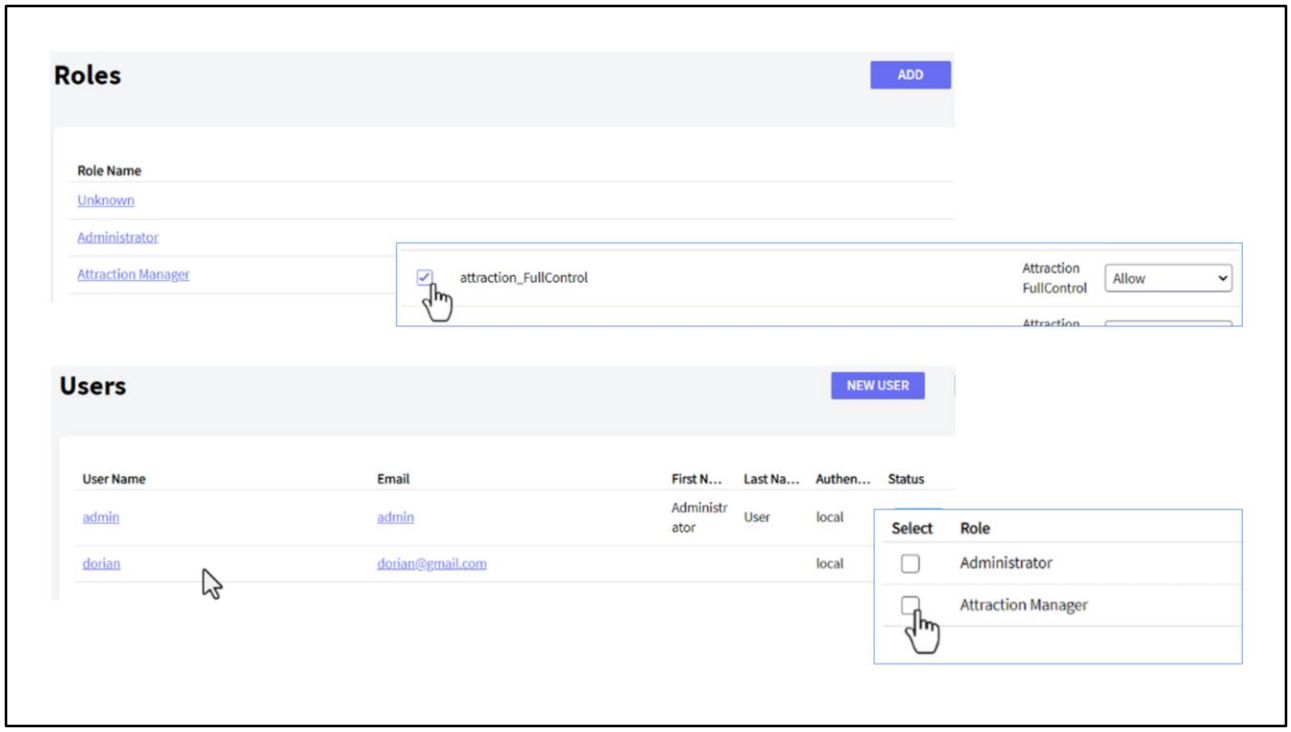
De igual manera, nos otorga la posibilidad de elegir la forma de actualizar dichos objetos, ya sea automáticamente, que nos pregunte o que nunca los actualice. Seleccionamos que sí y posteriormente se importarán los objetos y los podremos encontrar en las carpetas "GAM Example" y "GAM Library" debajo de "Root Module ".

A nivel general, cambiaremos el nivel de seguridad a "ninguno" para que cualquier usuario pueda visualizar nuestra aplicación. Entonces, en las propiedades de la versión, cambiamos una propiedad llamada "Integrated Security Level". Posteriormente, podemos cambiar esta misma propiedad a nivel de objeto. Por ejemplo, en la transacción de "Atracción", cambiamos "Integrated Security Level" a "Authorization" para que solo los usuarios autorizados puedan acceder.

Recordemos que una vez que aplicamos el GAM, necesitamos hacer un "rebuild" a la KB. Esto nos solicitará que creemos la base de datos del GAM. Una vez realizado, encontraremos un nuevo Data Store especialmente para el GAM.



Ejecutamos el panel "GAM Home", vamos al backend del GAM, el cual es su consola de administración, para poder agregar nuestros usuarios y darles permisos mediante su rol asignado. Accedemos utilizando el usuario por defecto (admin) y su contraseña "admin123", recordando que podemos cambiarlo posteriormente.



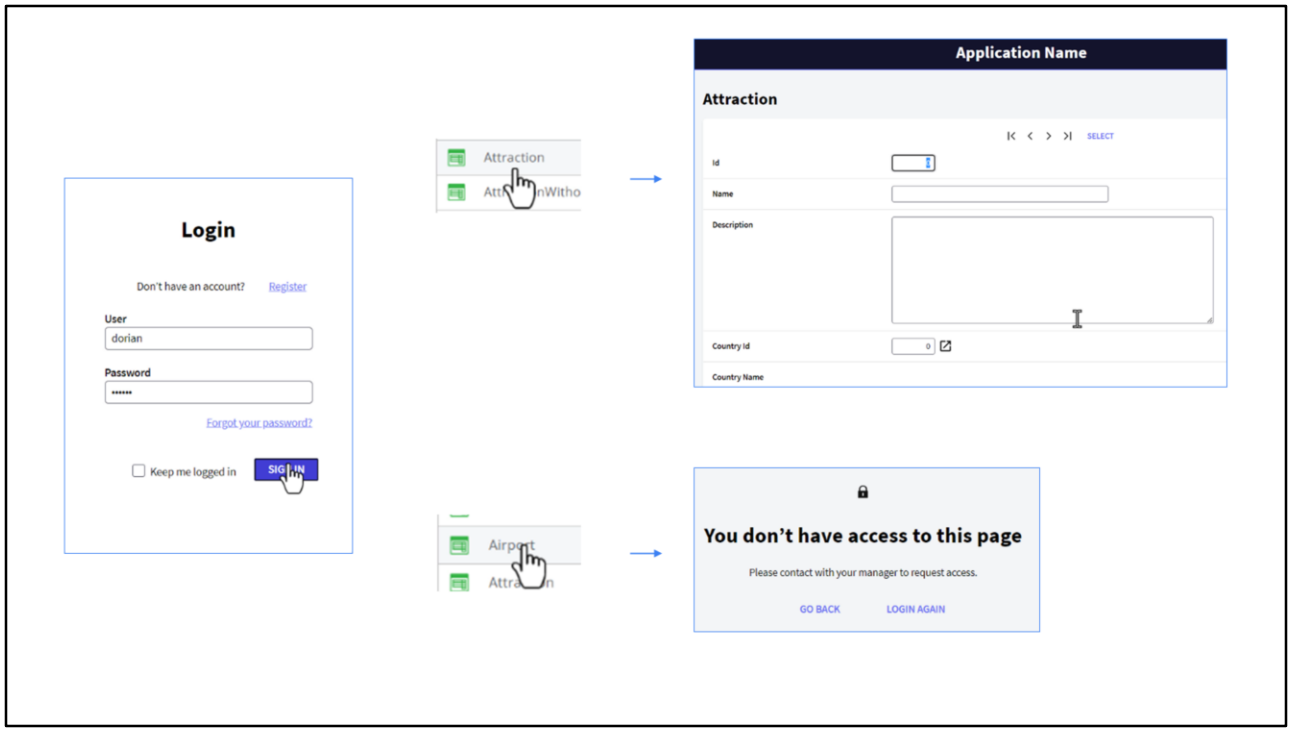
Entrando a la consola de administración, primero vamos a “Roles” y agregaremos el rol "Atracción Manager" que tendrá los permisos para poder insertar, actualizar o borrar alguna atracción. Para ello, damos clic en la opción "Add" y colocamos el nombre e indicamos la política de seguridad, por ahora basta dejar la opción por defecto. Confirmamos.

Después, entramos a nuestro rol y seleccionamos “More Options” "Permissions". En esta pantalla, seleccionamos la aplicación "Travel Agency" y la opción "Add". En la siguiente pantalla, se despliegan los permisos que podemos aplicar a este objeto. Seleccionamos "attraction_Full Control", ya que este rol podrá realizar todas esas tareas. Damos clic en "Add Selected" y salvamos.

Con esto, tenemos configurado nuestro rol. Ahora necesitamos agregar un usuario para que tenga asignado dicho rol. Para ello, vamos a la opción "Users" y a la opción "New User". Veremos que algunos campos tienen asterisco, lo cual indica que son obligatorios.

Agregamos al usuario "Dorian" con un email, una contraseña y le agregamos su política de seguridad. Confirmamos. Entramos al usuario recién creado, "Dorian", y le vamos a asignar su

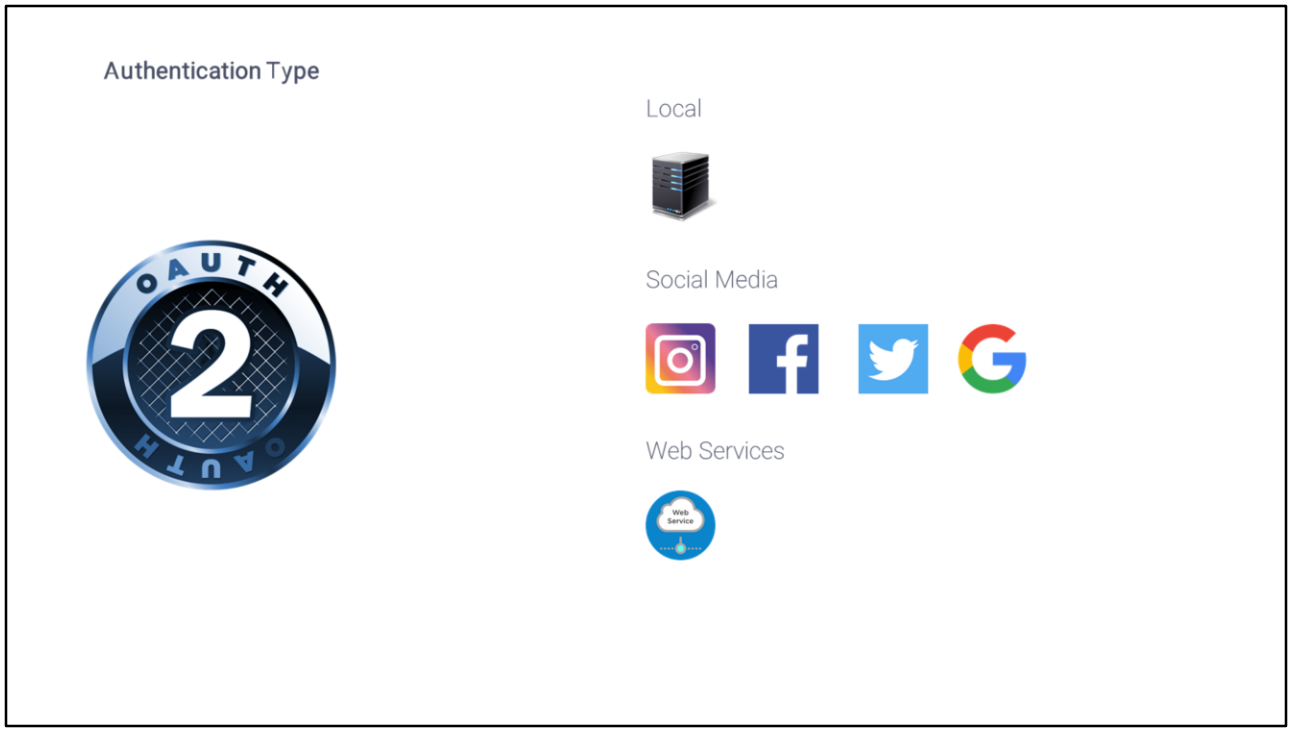
rol. Agregamos rol, e indicamos que sea “Attraction Manager” y agregamos con "add selected". Regresamos y visualizamos que el usuario ya tiene este nuevo rol asignado.



Ahora vayamos nuevamente a nuestra aplicación backoffice, donde gestionamos una agencia de viajes.

Al ejecutar la aplicación, desde el Launchpad seleccionamos la transacción Attraction, nos pedirá las credenciales de acceso, nos logueamos con el usuario Dorian, y podemos acceder sin problemas. Dados los permisos podemos también ingresar, actualizar o eliminar dichas atracciones.

Si vamos a la transacción Airport, y ponemos como seguridad autorización, al igual que lo hicimos con Attraction, e intentamos ingresar a Airport desde el Launchpad, nos dirá que no estamos autorizados, ya que sólo dimos permisos para acceder a las atracciones.



Con esto vemos como GeneXus nos permite administrar la autenticación y autorización de la aplicación. Hasta ahora, solo hemos utilizado la autenticación de los usuarios locales, pero podemos utilizar otro tipo de autenticación, como Facebook, Twitter, Google o algún otro servicio externo.

Cabe destacar que la versión actual de Genexus puede realizar la autenticación con cualquier proveedor que utilice OAuth 2.0. OAuth es un estándar para otorgar acceso a sitios web o aplicaciones desde otro sitio web, pero sin otorgar las contraseñas.

Una de sus ventajas es que se verifica la identidad del usuario y emite un token a la aplicación para otorgar acceso, lo cual hace mucho más segura la autenticación en nuestra aplicación.

Para saber más sobre el Genexus Access Manager, visita nuestro WIKI.