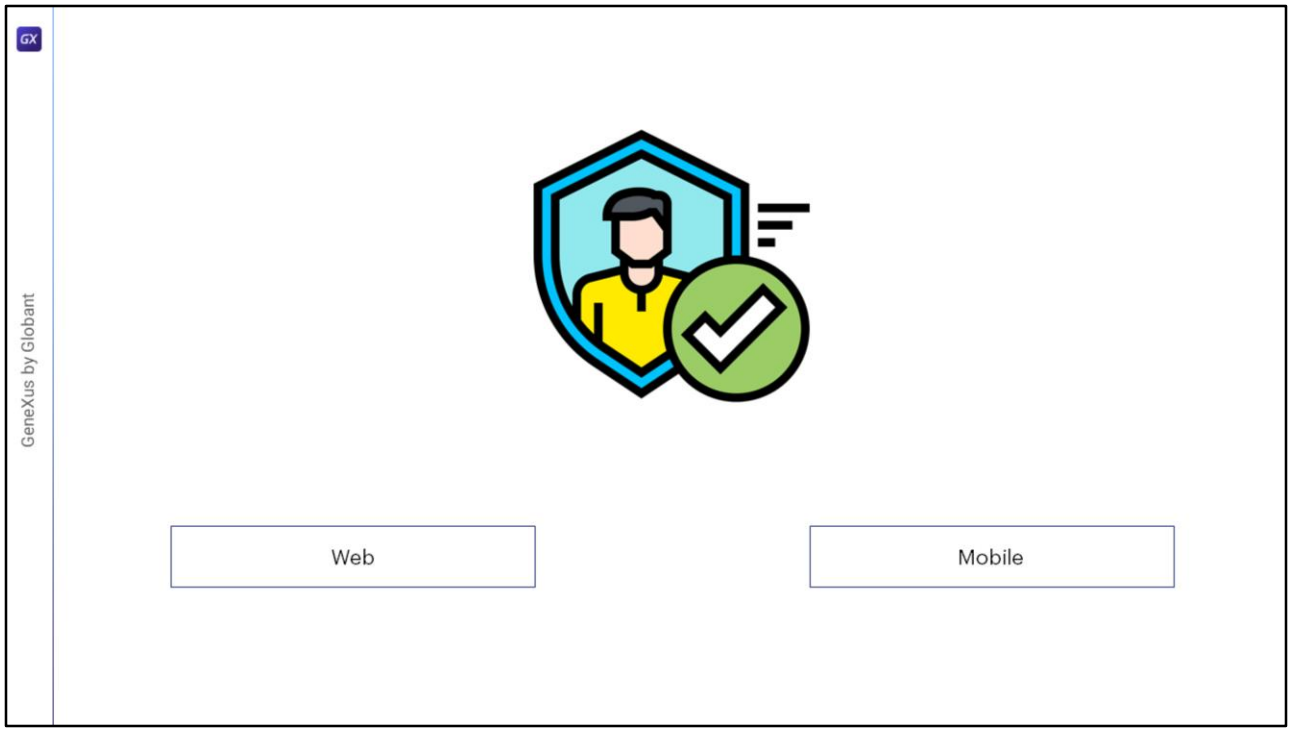

GeneXus by Globant
GeneXus™
by Globant
training.genexus.com

GeneXus by Globant

Authentication

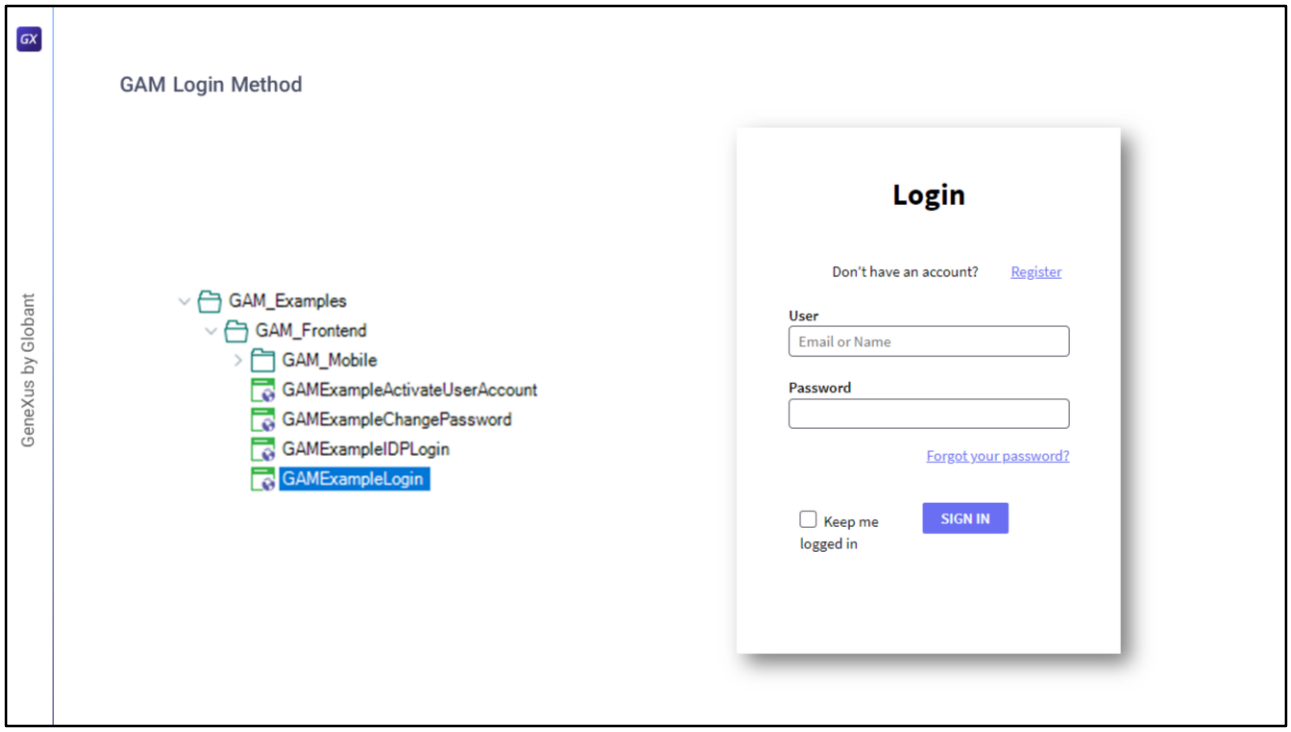
Nicolas Adrién



Como dijimos en videos anteriores, la autenticación es el acto o proceso de confirmar que algo (o alguien) es quien dice ser.

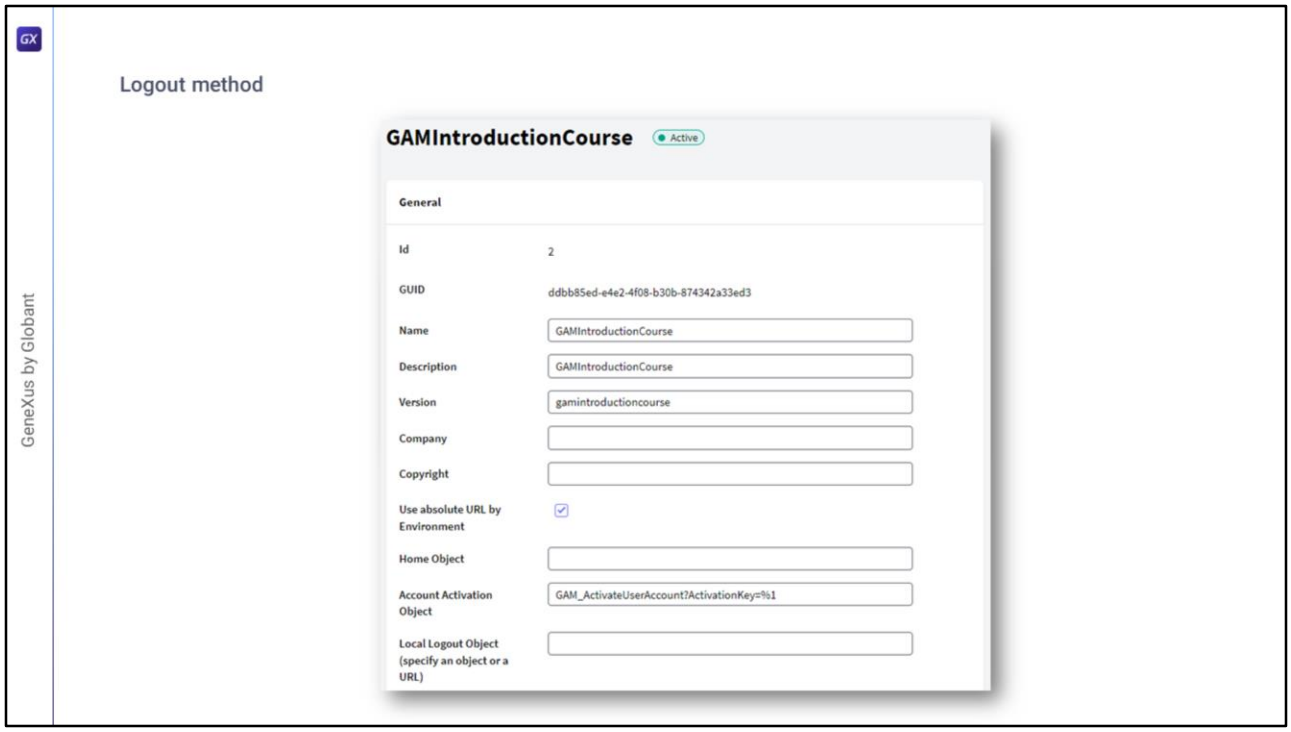
Todos los escenarios de autenticación GAM incluyen la posibilidad de ingresar un nombre de usuario y una contraseña y validar estos datos contra una base de datos existente.

Los modos a los que se puede aplicar el GAM dependen del entorno para el que se desarrollan o implementan las aplicaciones. Las opciones disponibles son Web y Móvil.



Veamos el método de Login de GAM.
Como dijimos antes, GAM brinda objetos de ejemplo los cuales podemos utilizar como guía.

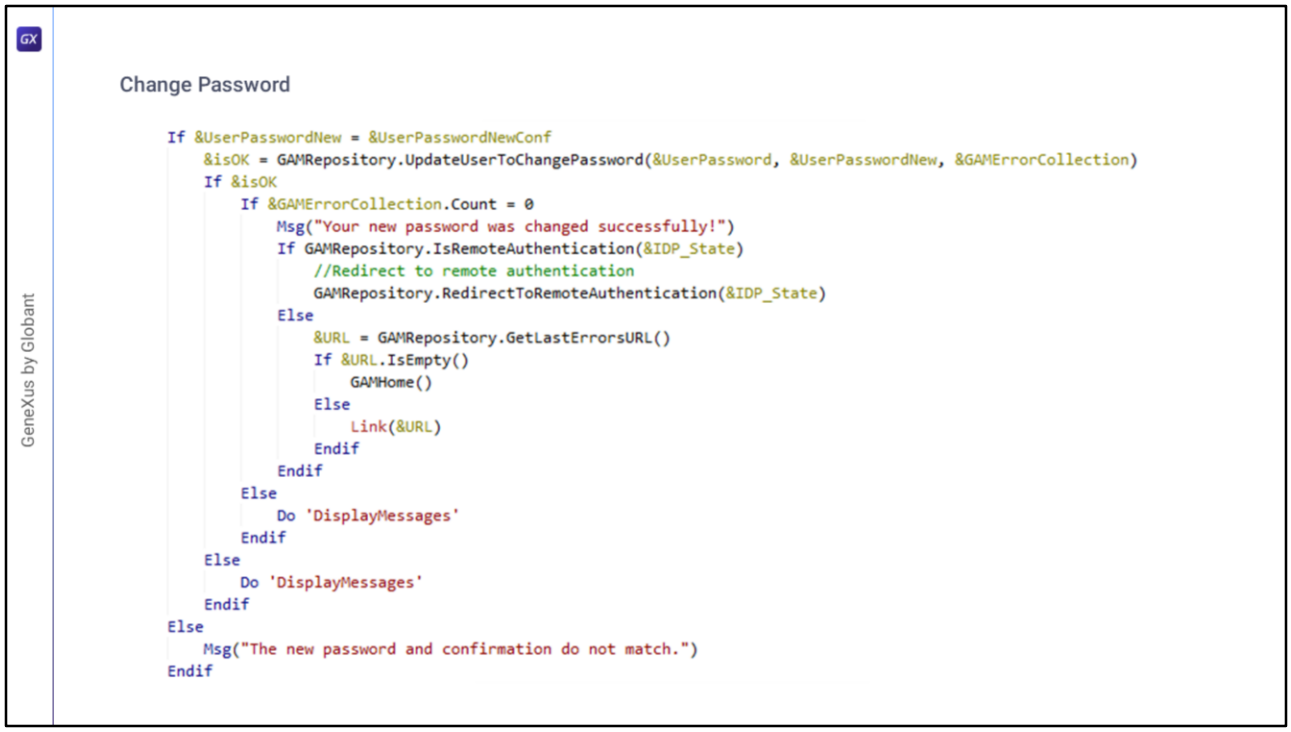
En particular, para el método de GAM existe el objeto **GAMExampleLogin**, el cual realiza la autenticación a través de GAM.
En él se utiliza el método de inicio de sesión de **GAMRepository**, que es un objeto externo que forma parte de la biblioteca GAM, el cual no entraremos en detalle por el momento.



En cuanto al cierre de sesión, una posible implementación puede ser la siguiente.

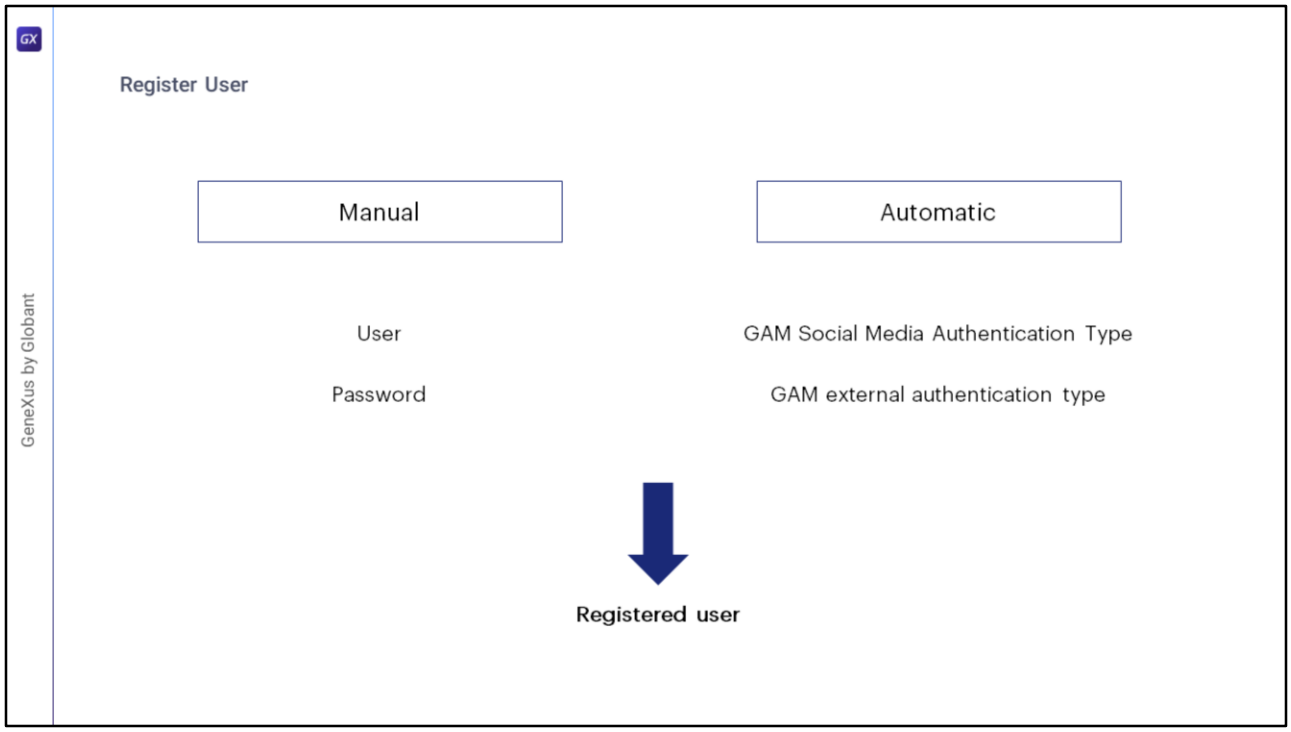
La primera instrucción carga en el repositorio de la base de datos GAM los datos del usuario, y en caso de errores estos se reciben en el SDT &Errors.
La segunda instrucción transfiere el flujo hacia el Web Panel GAMExampleLogin. Eso es todo.

El cierre de sesión de la aplicación se configura utilizando el backoffice web de GAM en la configuración de la aplicación (o mediante programación, utilizando la API de GAM).
Su propósito es determinar la URL del objeto a ser redirigido luego de ejecutar el Logout en las aplicaciones SSO.



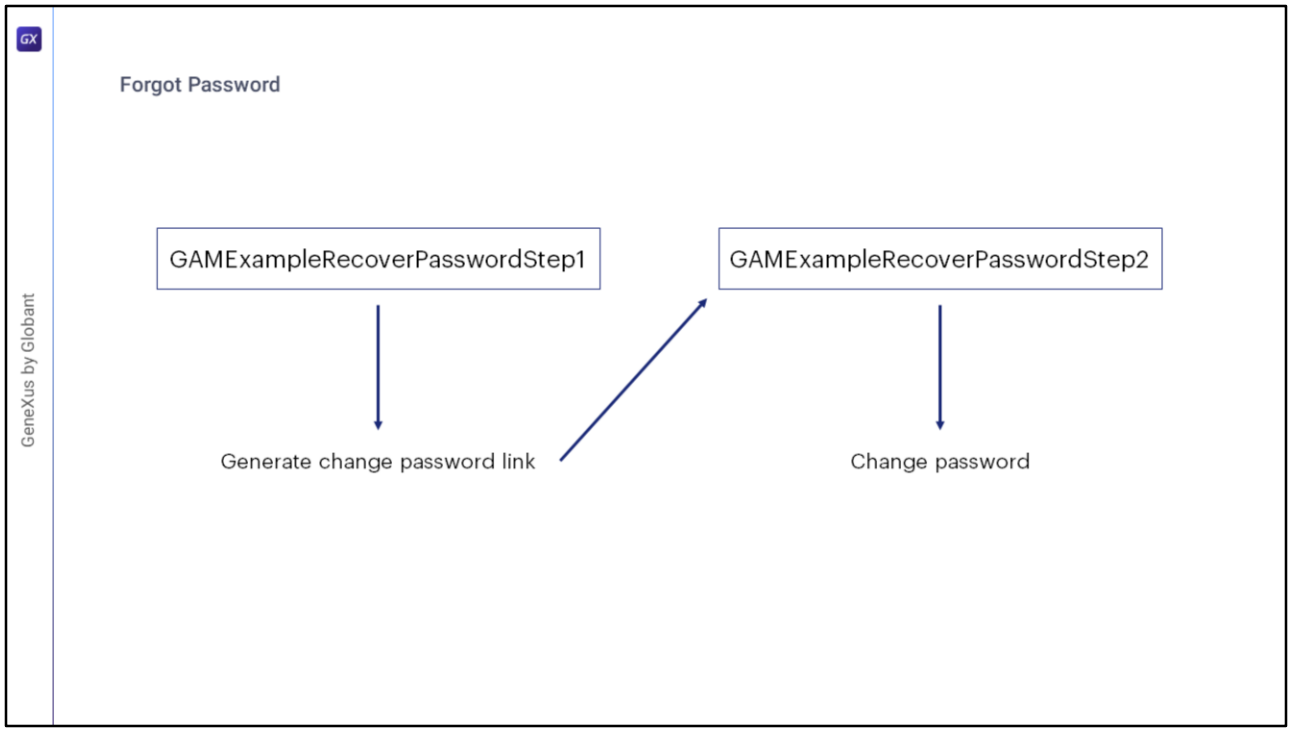
Como ya mencionamos la existencia de los ejemplos de GAM, este también proporciona uno para el cambio de contraseña.

El mecanismo de este es bastante simple de entender, y consiste en utilizar los métodos provistos por GAM como lo es **UpdateUserToChangePassword**.
No vamos a entrar en detalle de la implementación de este método, pero posteriormente a su llamado solo se controla si hubo errores o no en el proceso. En caso de que no, además se chequea si la autenticación era remota, con el fin de finalizar el proceso de Login en las aplicaciones externas si fuera el caso, y si no, es redirigido al home de GAM.



En cuanto al registro de usuario, existen dos formas de realizarlo:
La primera es manual, donde un usuario GeneXus se registra en GAM y allí se crea un usuario y contraseña para tener acceso a la aplicación. Esto ocurre en el caso de Tipo de Autenticación GAM Local.

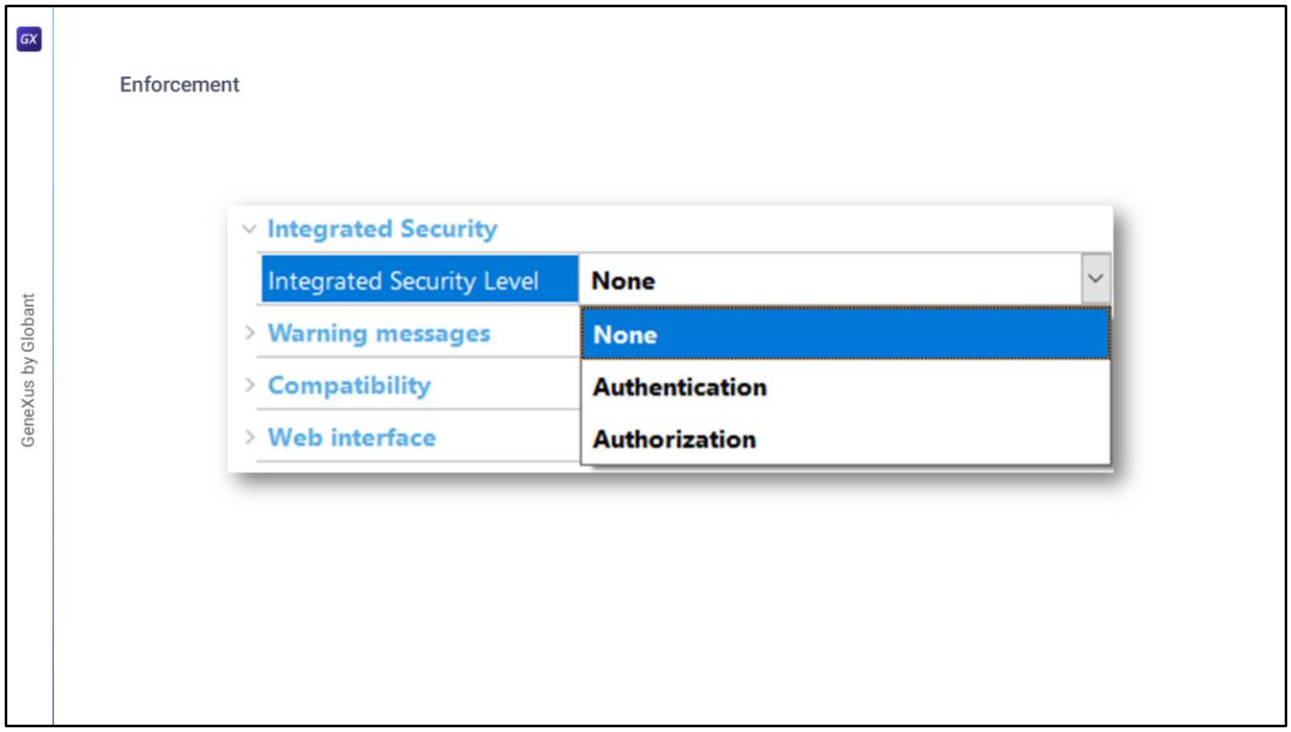
La segunda forma es automática y es el caso de Tipo de autenticación de GAM por redes sociales o autenticación externa, donde el registro de usuario se realiza cuando el usuario ingresa a la aplicación por primera vez.



Con la Biblioteca de ejemplos GAM se distribuyen dos objetos: **GAMExampleRecoverPasswordStep1** y **GAMExampleRecoverPasswordStep2**, que brindan una solución para el caso de olvido de contraseña. La idea es que el usuario GeneXus complete estas muestras de acuerdo a sus necesidades.

La idea básica de estos objetos es que con el primero, el usuario de la aplicación tenga la posibilidad de ingresar su nombre de usuario o correo electrónico con el fin de cambiar su contraseña a través de él.
Como la idea es preservar la confidencialidad del usuario, a su correo electrónico se envía un enlace con destino al segundo objeto web por el cual finalmente podrá cambiar la contraseña.

En la Wiki de GeneXus se puede conocer más detalles sobre la implementación de esto.

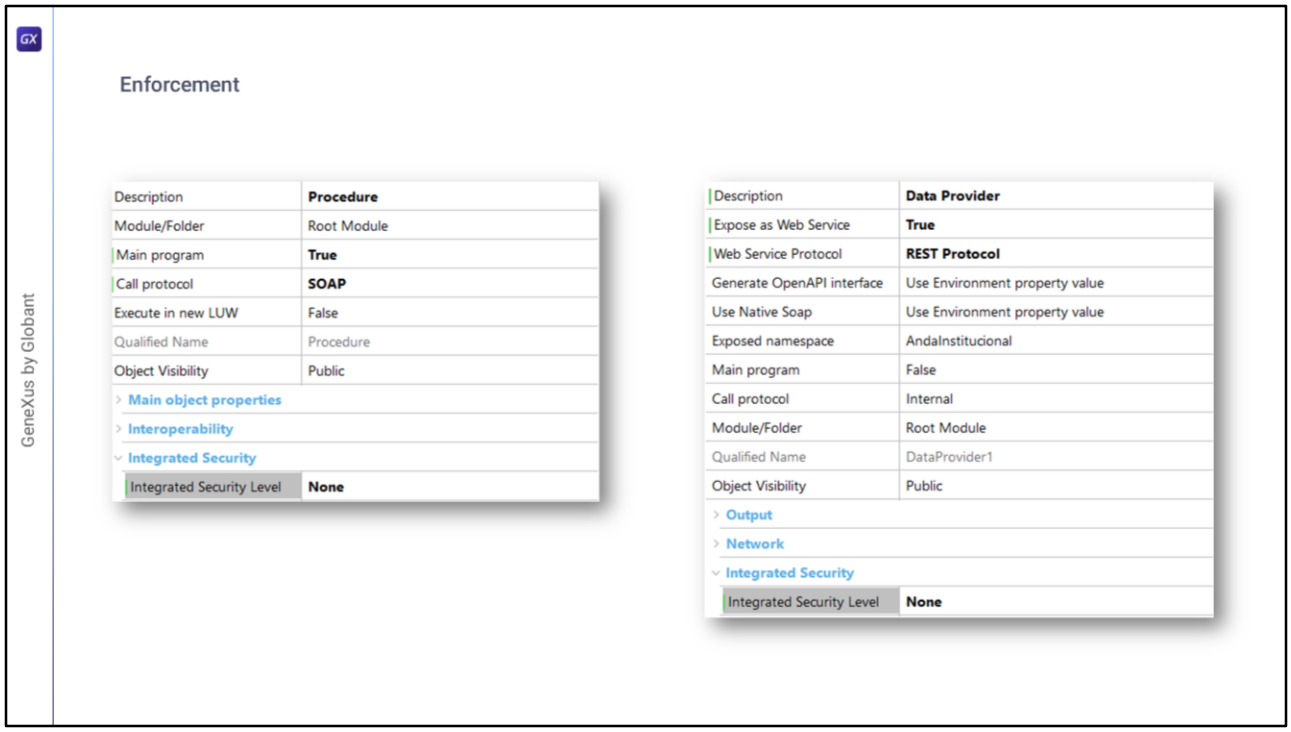


En todos los webpanels que requieren autenticación, GAM verifica la misma automáticamente sin necesidad de pedirle al usuario loguearse en cada momento.
La forma más fácil para configurar y definir esto, es seteando la propiedad **Integrated Security Level** con valor **Authentication** en las propiedades de los objetos que queramos que solo se accedan autenticados.

Al activar esta propiedad con dicho valor, se hará cumplir la seguridad.
En el caso de objetos web, la verificación también se realiza en cada llamada AJAX que se ejecuta. Este es el valor predeterminado en el nivel de versión.

Si el usuario no está autenticado, se mostrará un Objeto de inicio de sesión para la propiedad Web o un Objeto de inicio de sesión para la propiedad SD (dependiendo de la aplicación), para permitir que el usuario se autentique y acceda a la aplicación.

En el caso de elegir la opción Authorization, no solo se comprobará si el usuario esta autenticado en el sistema o no, sino que también se comprobará si tiene permisos para acceder a dicho objeto.



Si la propiedad Integrated Security Level se define a nivel de versión, los procedimientos o Data Providers de tipo Web Service, tomaran también ese valor y capaz no es lo que se busca.

Para definir un valor especifico o simplemente desactivar la propiedad, se hace como cualquier otro objeto desde el menú Propiedades sobre el objeto.

Otra forma de realizar esto, pero de forma manual, la podemos encontrar en los objetos de ejemplos de GAM, donde se realiza con el código que vemos en pantalla.

En los distintos External Objects que trae incorporado GAM, tenemos GAMSession, el cual tiene un método para el chequeo de sesión.
Además de verificar el resultado booleano de este método, se puede utilizar una variable de tipo **GAMSession**, con la cual podemos utilizar los distintos métodos disponibles del External Object.
En este caso en particular, se utiliza **IsAnonymous** para corroborar si en la sesión se está autenticado o no.

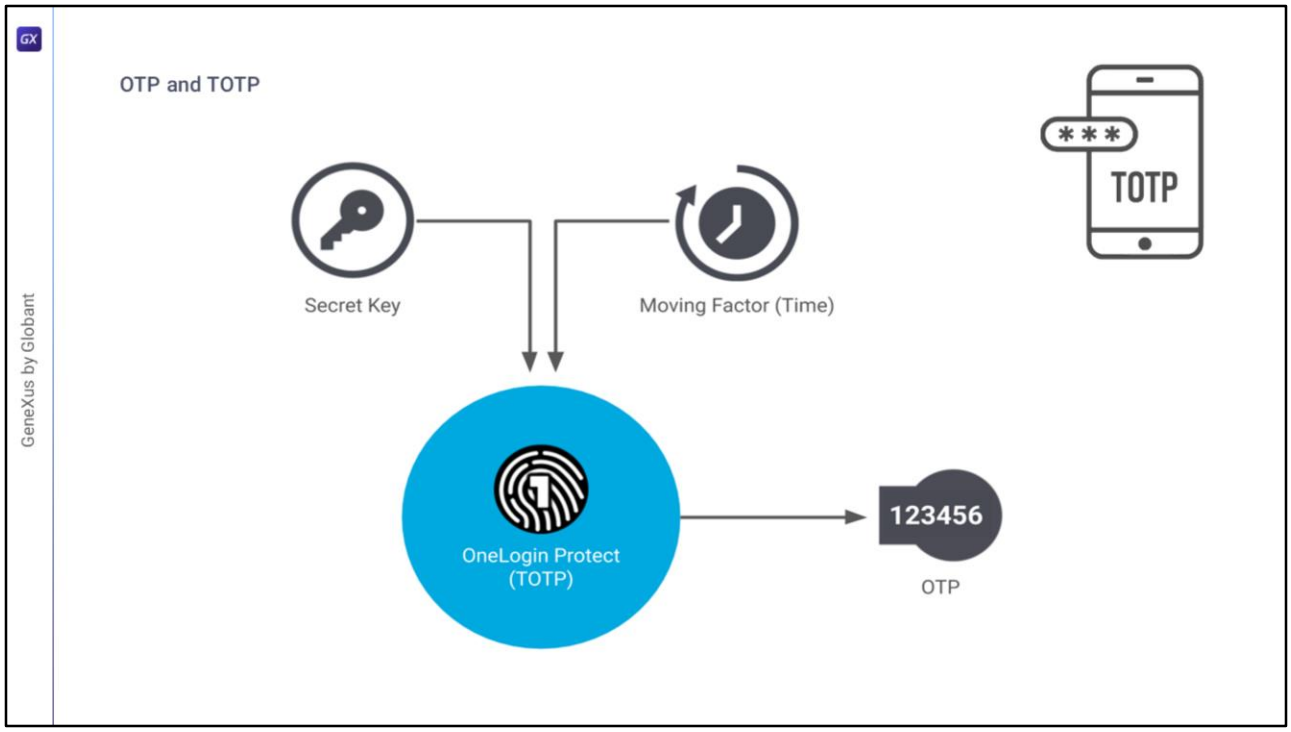
Brindar acceso seguro a aplicaciones y software basado en la nube es un desafío constante para las empresas de todas las industrias.
Una de las formas con las que se ha contrarrestado el robo de contraseñas y otros tipos de ciberataques es mediante el uso de contraseñas de un solo uso (u OTP como son sus siglas).

OTP es una forma de autenticación multifactor donde para cada autenticación, es posible generar una contraseña temporal y enviarla por correo electrónico o SMS al usuario especificado en el formulario de inicio de sesión.

¿Cómo funciona?
Cuando un usuario se autentica en una aplicación web, se genera una contraseña y se envía un correo electrónico/SMS con la contraseña generada. Por defecto, GAM envía contraseñas por correo electrónico; sin embargo, se puede personalizar cómo se envían los códigos a los usuarios (por ejemplo, enviando las contraseñas por SMS).
Estos mismos pasos se aplican para las aplicaciones móviles.

La contraseña autogenerada no debe estar caducada y se puede utilizar para **un solo** inicio de sesión.
Sin embargo, OTP debe tener una fecha de vencimiento por razones de seguridad, y es el administrador de la aplicación quien puede establecer dicho tiempo.

Para permitir que un usuario use OTP con GAM, el usuario debe existir en este, estando registrado previamente, y se debe haber validado la autenticidad del método utilizado para recibir la OTP, ya sea el correo electrónico o SMS para verificar que realmente es del usuario registrado.

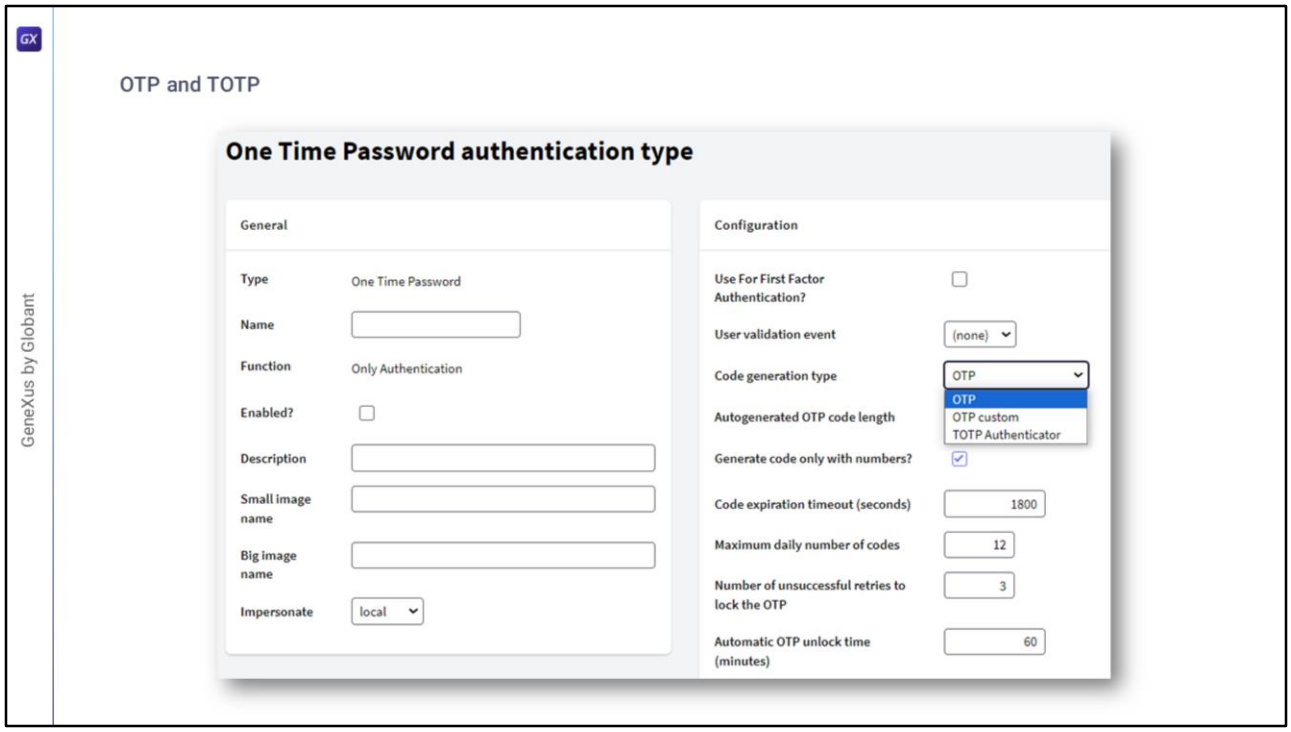


La otra forma con la que se ha contrarrestado el robo de contraseñas y otros tipos de ciberataques es mediante el uso de contraseñas de un solo uso basadas en el tiempo (o TOTP como son sus siglas).

La contraseña de un solo uso basada en el tiempo es un algoritmo que genera claves de contraseña de un solo uso (OTP) que utilizan la hora actual como fuente de unicidad. Por lo tanto, en el GAM, TOTP se encuentra como un tipo de generación de Código OTP.

Este método de autenticación ofrece la ventaja de que no necesitan recordar una contraseña, ya que se genera un nuevo código cada vez que desean iniciar sesión. Además, agrega otro nivel de seguridad porque el código es válido por un corto período de tiempo.

En caso de que alguien intente autenticarse con un nombre de usuario que no le pertenece, este método agrega otro nivel de dificultad debido a que los usuarios necesitan una aplicación en su teléfono móvil para obtener estos códigos.



La activación y configuración de estos métodos en el GAM se puede realizar a través de la opción de menú Authentication Type en el Backoffice de GAM.


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