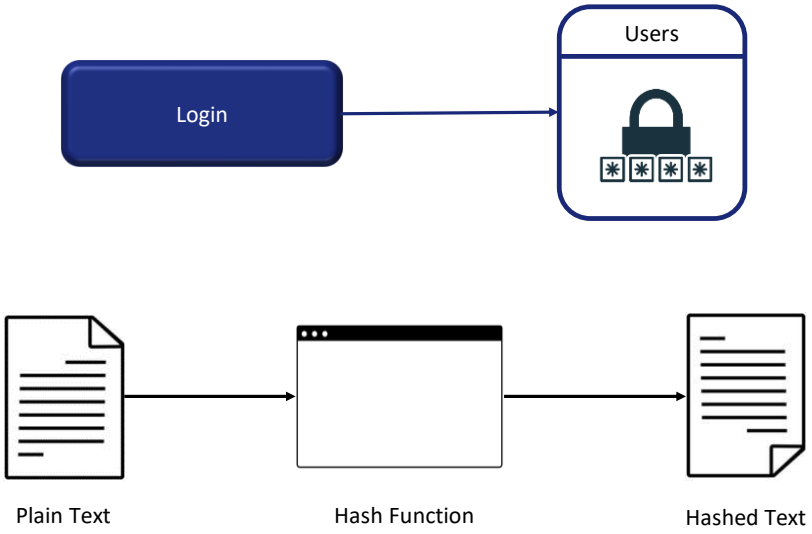
Authentication Types

Nicolas Adrién | GeneXus Training

Authentication types

Como dijimos en videos anteriores, GAM ofrece distintos tipos de autenticación, ya sea internos (contra la base de datos GAM), y externos (como puede ser servicios web, redes sociales, Google o también llamados Remotos).
Entremos en detalle en estos.

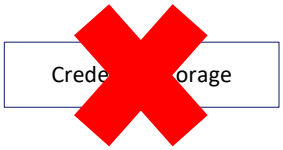


En cuando a los Tipos de Autenticación Internos, tenemos **Autenticación local**, donde las credenciales de los usuarios se almacenan en la tabla "Usuarios" del GAM.

GAM no almacena la contraseña del usuario, pero almacena un hash de la misma. Un hash es un algoritmo tal que, dada una cadena en texto plano, produce siempre la misma cadena resultante y, dada ésta, no se puede obtener la original.

El hash se obtiene a partir de una clave única para cada usuario y un algoritmo denominado SHA-512, en el cual no entraremos en detalle.

Esto significa que cuando se recuperan Usuarios GAM del repositorio, la propiedad de la contraseña siempre tiene un valor vacío.



Cuando se quiere integrar una aplicación con otra para intercambiar información, el primer punto fundamental es resolver el problema de la autenticación.

En el tipo de autenticación Externo, una primer solución es que la aplicación que necesitamos integrar exponga un servicio web SOAP que resuelva la autenticación.

Otro escenario, es el de un programa externo a la aplicación que resuelve los problemas de autenticación, que no necesariamente es un servicio SOAP. La solución para ese escenario es configurar el tipo de autenticación personalizada de GAM en el repositorio de GAM.

En ambos casos, es necesario configurar GAM para aceptar el programa externo como Identity Provider.

Al utilizar cualquiera de estos tipos de autenticación, el GAM Cliente no es el propietario de las credenciales del usuario, solo se almacenará en el Repositorio el nombre de usuario y otra información que dependa de la salida del programa externo.

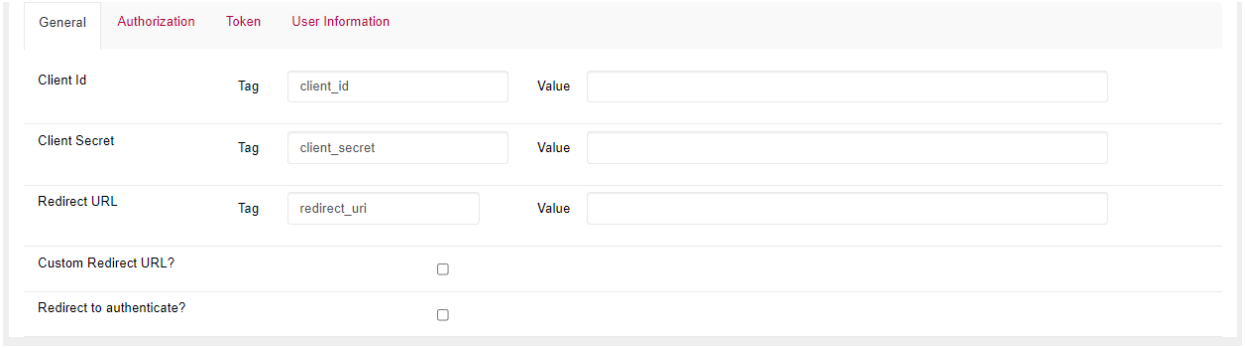
En caso de autenticarse en otros servicios externos, como LDAP, puede usar un programa externo o servicio web para hacer un puente entre la aplicación GAM y LDAP.

Entrado en el resto de tipos de autenticación, primero tenemos a Oauth 2.0.
GAM permite autenticarse con cualquier proveedor de OAuth en versión 2.0, solamente siguiendo unos simples pasos.
Cuando se selecciona este tipo de autenticación, el inicio de sesión de una aplicación se redirige al proveedor de identidad configurado.
El inicio de sesión es mostrado por el proveedor; y allí los usuarios ingresan sus credenciales siendo redirigidos nuevamente a la aplicación.

La definición de este tipo de Autenticación es igual a cualquiera de los otros tipos que ya mencionamos de GAM, solo que este requiere una configuración detallada del protocolo utilizado por el Proveedor. Por lo tanto, para configurar el tipo de autenticación OAuth en GAM, se debe seguir la documentación del proveedor de identidad al que desea conectarse.

Este protocolo también resuelve el SSO entre diferentes aplicaciones clientes.

Authentication types | External



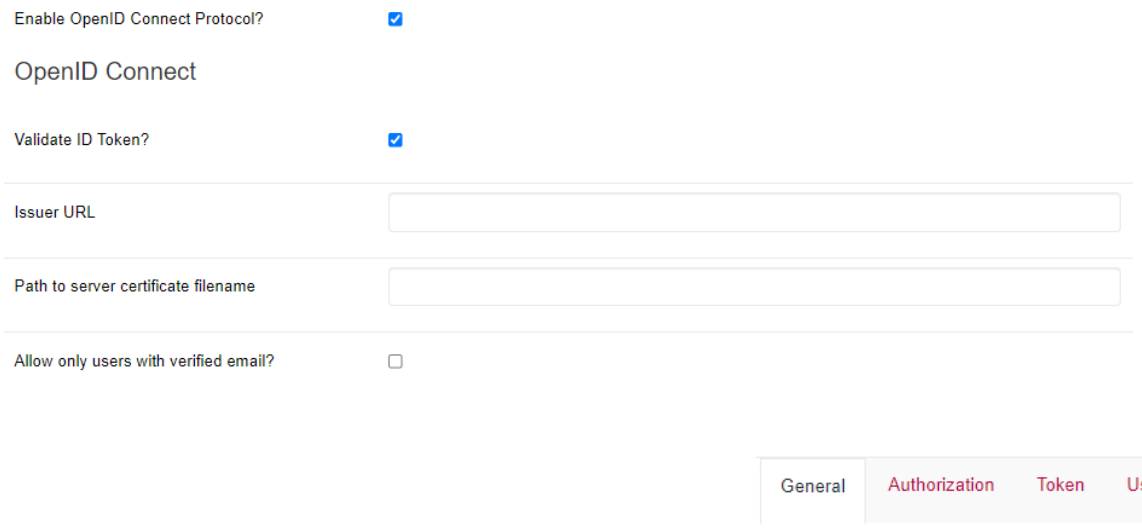
/oauth/gam/callback

Oauth 2.0 tiene un segundo flujo de autenticación el cual permite a través de la opción "Redirigir para autenticar?“ en False la autenticación OAuth 2.0 usando REST sin redireccionar al proveedor de identidad, donde lo que hace GAM es saltearse la redirección configurada en el tab Authorization.

La otra opción (Custom Redirect URL?), es donde se le especifica a GAM que la URL de retorno indicada es personalizada, la cual si esta en False, este luego le concatenará “/oauth/gam/callback”. En cambio, si esta en True, esta URL la debe implementar el desarrollador y leer las respuestas del IDP.

Ambas propiedades son configurables desde el tipo de autenticación OAuth desde el Backend de GAM.

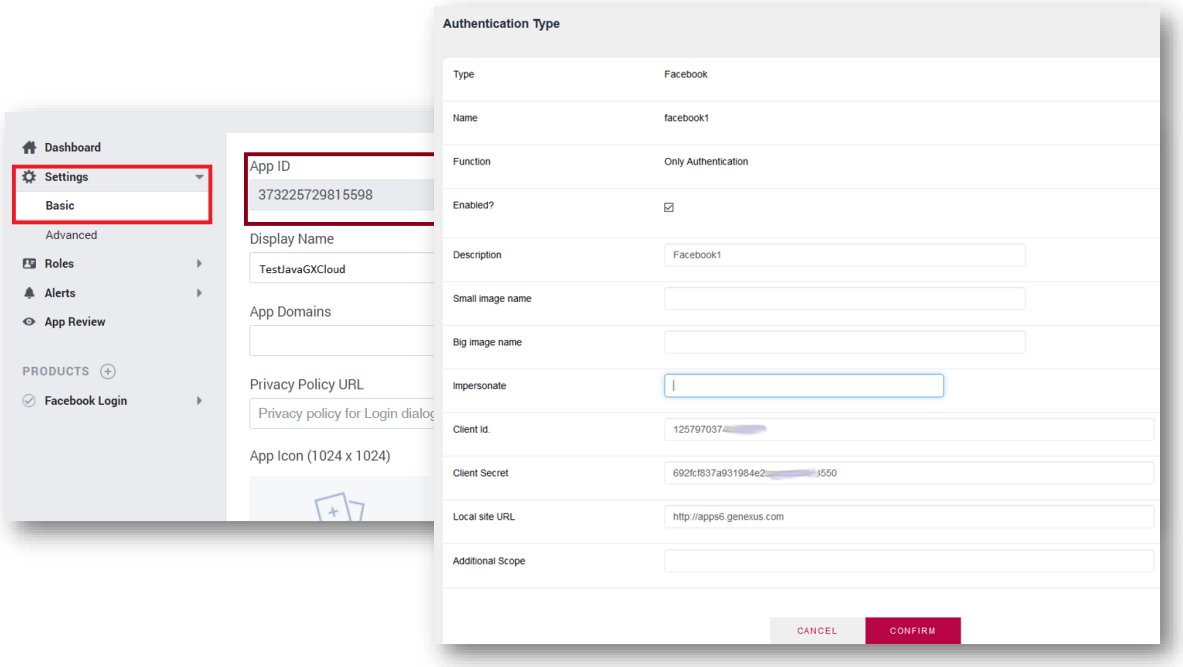
Authentication types | External



Posteriormente tenemos OpenID Connect.
Este es un protocolo de autenticación que funciona con OAuth 2.0 al implementar la autenticación como una extensión del proceso de autorización de OAuth y se está transformando en los mas comunes de la actualidad.
La ventaja que nos proporciona en cuanto a OAuth, es que este protocolo nos permite obtener la información del usuario mientras que en el estándar de OAuth no tenemos como obtener dicha información. Por esta razón, es que ahora no es necesario configurar la sección de User Information en el Authentication Type.

Para que el protocolo funcione, se debe activar la propiedad Validate ID Token, e incluir quien es el proveedor y el certificado publico local en un servidor.
Con esta información, se obtiene un JSON Web Token firmado y devuelto por el proveedor, llamado ID Token.

Authentication types | External



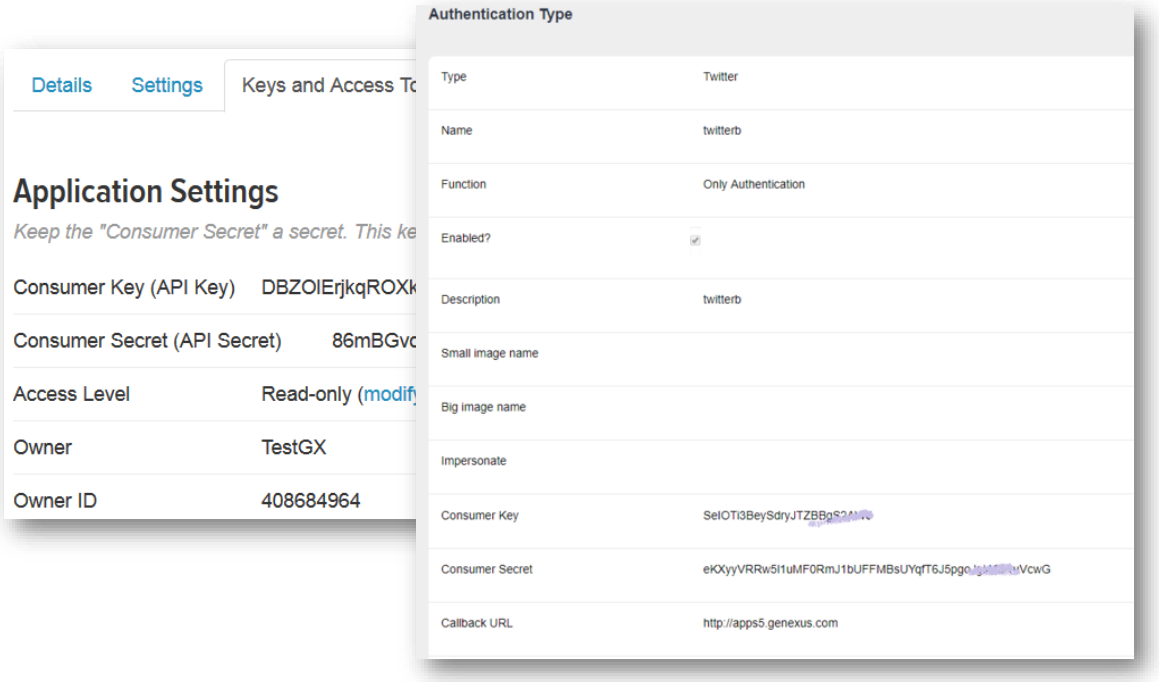
En segundo lugar tenemos a Facebook.

En este tipo se deben seguir dos pasos:
En primer lugar se debe crear una "aplicación de cliente de Facebook" en su sitio y obtener un ID y clave (denominada "Secreto") para su aplicación.
En segundo lugar, se debe definir el "Tipo de autenticación de Facebook" en el backend o la API de GAM.

Realizando estos pasos detalladamente ya se tiene configurado el tipo de autenticación correctamente.

Este tipo se puede usar en aplicaciones web y aplicaciones móviles nativas, y por detrás se resuelve mediante Oauth 2.0.

Authentication types | External

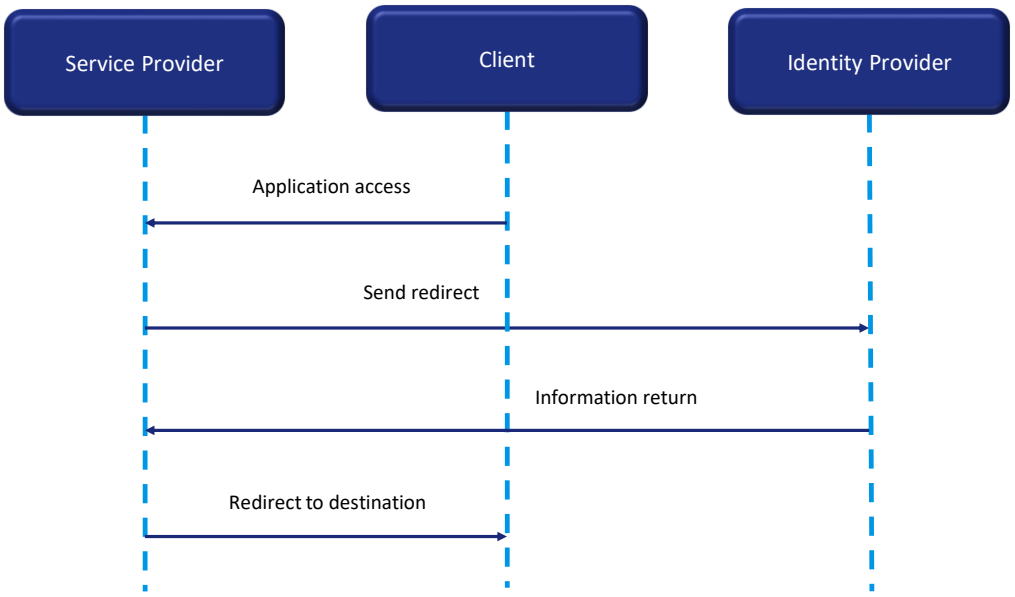


Después tenemos a Twitter.

Este caso se ejecuta de igual manera que Facebook.
Como paso 1 se debe crear una aplicación de Twitter en su sitio, y obtener la clave y secreto del consumidor para esa aplicación.
Como paso 2 se define el tipo de autenticación de Twitter utilizando el backend GAM.

Nuevamente como en Facebook, este tipo de autenticación se puede utilizar en aplicaciones web y también en aplicaciones móviles nativas.

En la Wiki de GeneXus se puede encontrar con detalle este y todos los tipos de autenticación existentes para GAM.



GAM permite autenticarse utilizando cualquier proveedor SAML versión 2.0.

SAML es un mecanismo de comunicación seguro basado en XML para comunicar identidades entre organizaciones.

Uno de los casos de uso que resuelve SAML también es SSO, por lo que evita la necesidad de mantener varias credenciales en varias ubicaciones y aumenta la seguridad al tiempo que reduce las tareas de tiempo de administración.

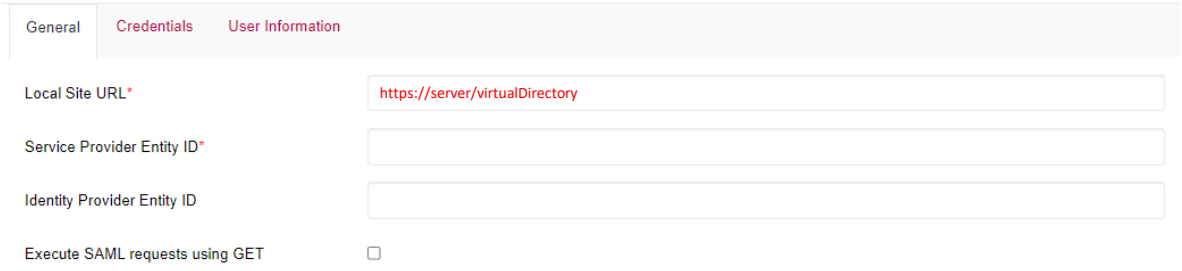
En SAML participan dos entidades aparte del cliente: un proveedor de servicios y un proveedor de identidad.
Un flujo de inicio de sesión se realiza, a grandes rasgos, de la siguiente manera:
En primer lugar el usuario intenta acceder a una aplicación alojada en un proveedor de servicios.
Este Proveedor genera una solicitud de autenticación y la envía a través de un redireccionamiento al navegador del usuario.
El proveedor de identidad recibe la solicitud, autentica al usuario solicitando credenciales de acceso válidas o comprobando que existen cookies de sesión correctas, y genera la respuesta para ser devuelta al navegador del usuario.
Finalmente, el usuario es redirigido a la URL de destino.

Authentication types | External

SSO SAML

Do not use self-signed certificate

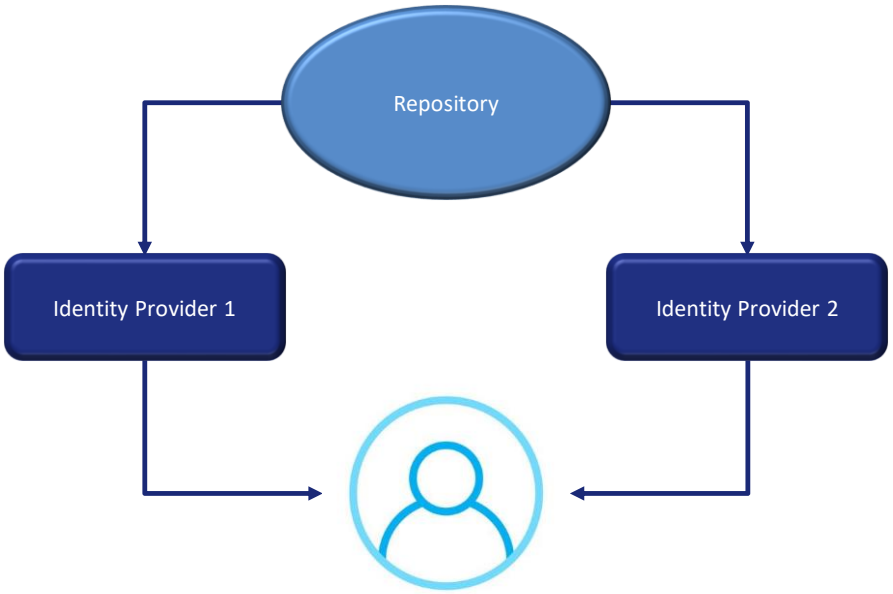
Use https protocol and include server and virtual directory



Algo a mencionar en SAML es lo siguiente:

- En cuanto a certificados, lo recomendable es no usar certificados auto firmados.
- La propiedad Local Site URL debe tener protocolo https e incluir server y directorio virtual como vemos en pantalla.

GAM Impersonation



Cuando el Repositorio de GAM permite a los usuarios finales autenticarse con diferentes proveedores de identidad, de forma predeterminada se asignan a diferentes Usuarios de GAM. Por cuestiones de seguridad, los usuarios pueden autenticarse utilizando diferentes mecanismos dependiendo de la fuente de acceso que se utilice. Sin embargo, la información de inicio de sesión debe asignarse al mismo usuario lógico de GAM.

La Suplantación (Impersonation) permite que el repositorio tenga dos mecanismos de autenticación diferentes pero que convergen en el mismo usuario.
Esto es útil para casos, por ejemplo, en los que no es posible utilizar el mismo tipo de autenticación desde la intranet y desde internet, pero se quiere que el usuario sea el mismo.
También se utiliza cuando se quiere migrar de un tipo de autenticación a otro, donde en ese caso el tipo de autenticación "suplantada" es la que se está migrando.

Según el tipo de autenticación, existen distintos criterios para mapear usuarios que se encuentran detallados en la Wiki de GeneXus.

Para cerrar este tema, pasaremos a una serie de demos con el fin de mostrar los casos de forma practica con más detalle.

training.genexus.com
wiki.genexus.com
training.genexus.com/certifications