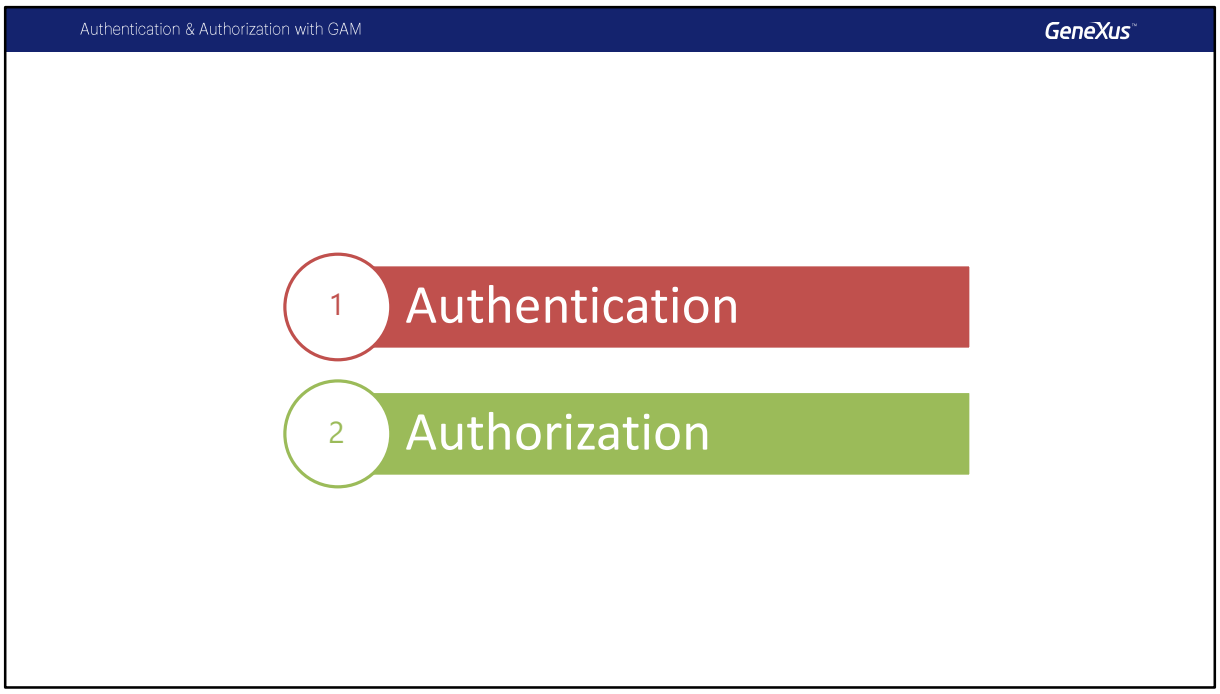
GeneXus™
The power of doing.

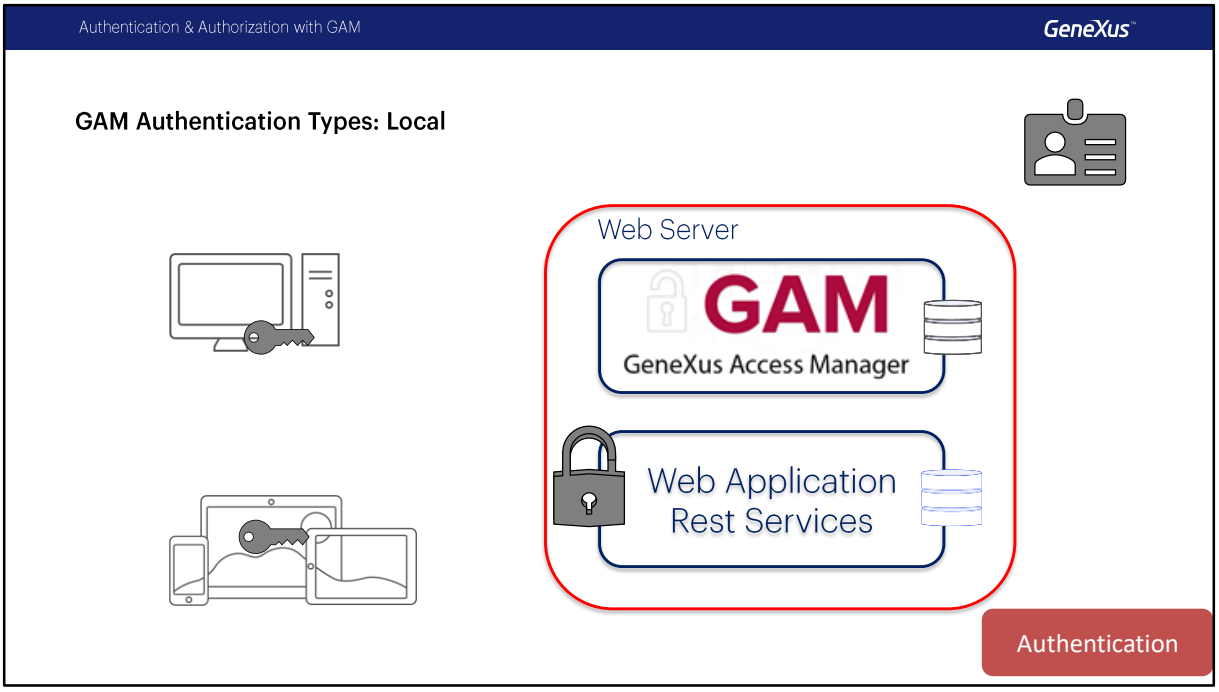
Authentication & Authorization with GAM

Security

GeneXus™ 16



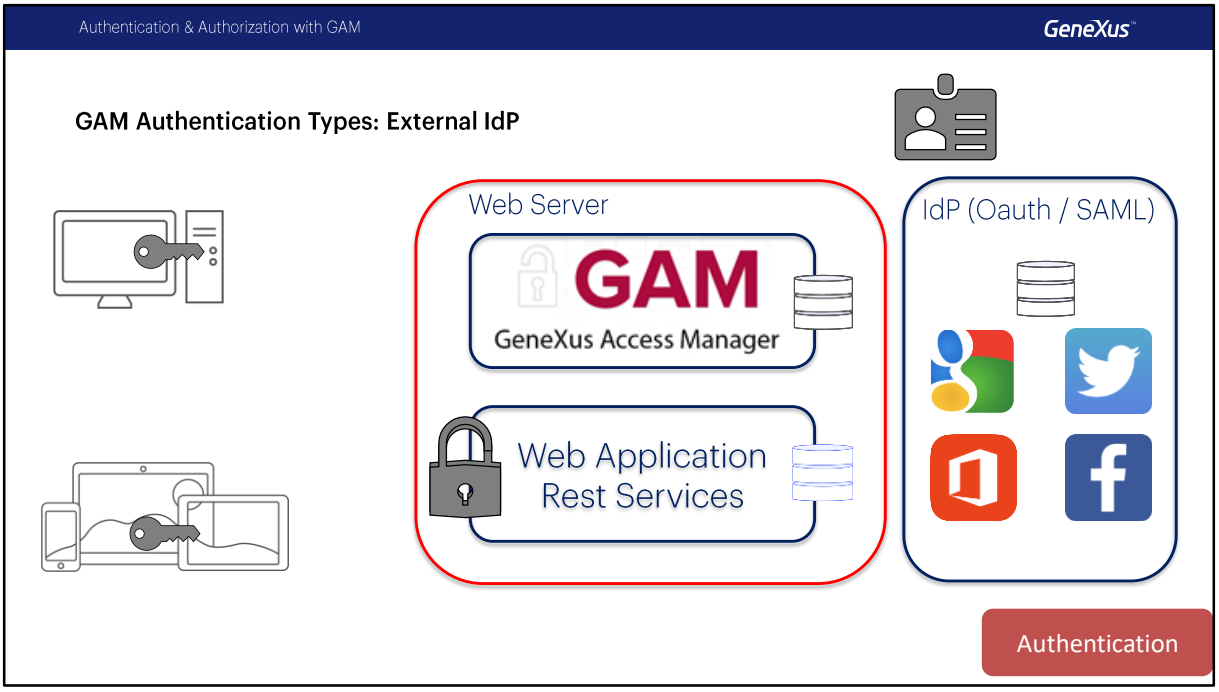
En este video veremos un poco mas de las características de Autenticación y Autorización utilizados en GAM y además veremos una demo donde utilizaremos el Backend Web provisto por esta herramienta.



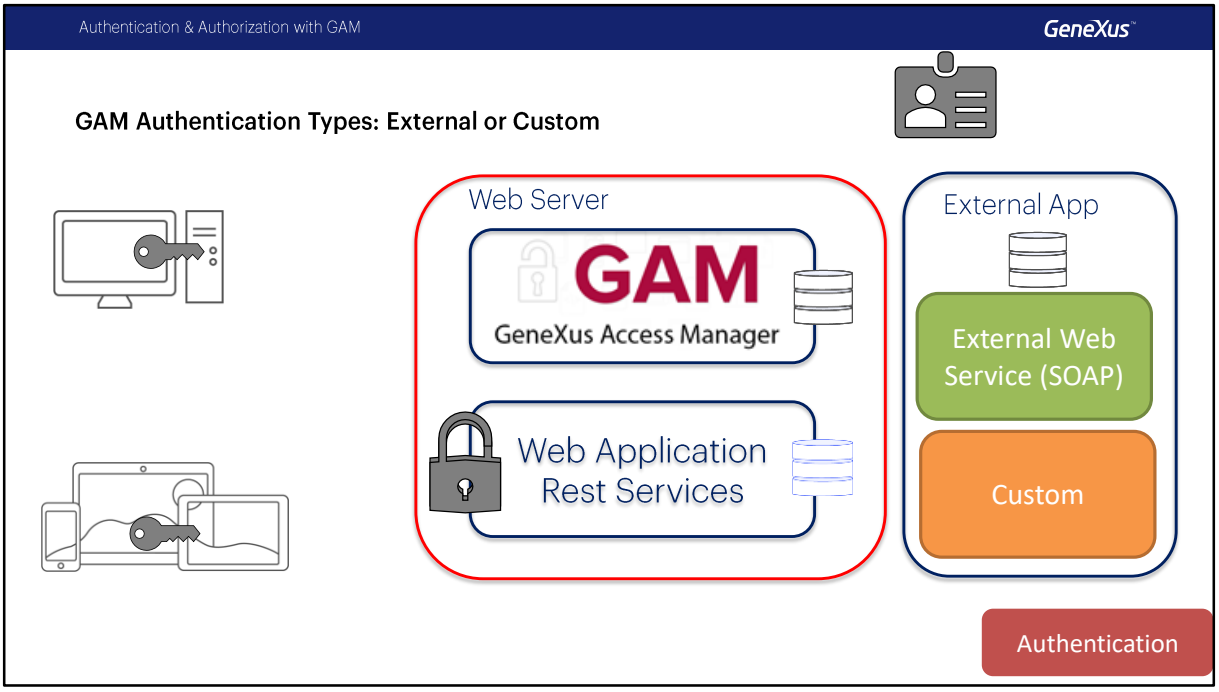
La autenticación es el proceso de verificar que un usuario es quien dice ser, mediante la validación de sus credenciales, en el caso de GAM las credenciales son usuario y contraseña.

Poseemos diferentes tipos de autenticación para implementar, incluso pueden habilitarse varios en forma simultanea.

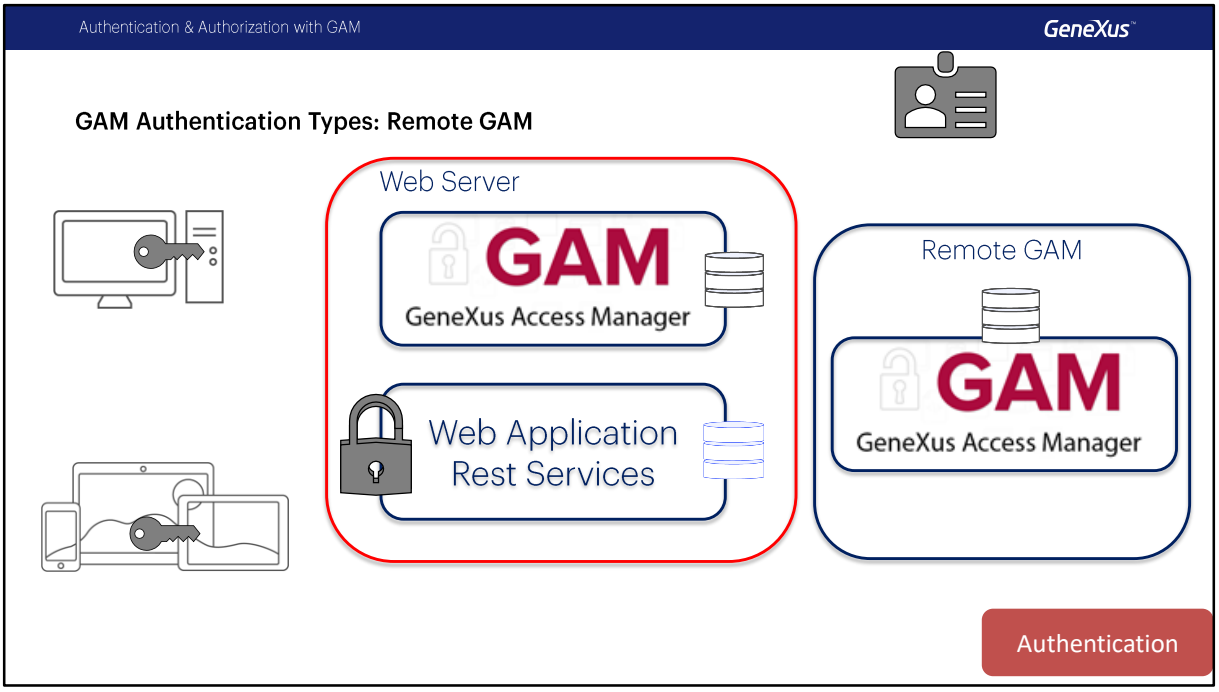
Los tipos son:
Local: en este caso las credenciales del usuario estarán almacenadas en la base de datos de GAM en la tabla de usuarios, por cuestiones de seguridad no se almacena la clave sino que se almacena un Hash obtenido al aplicar un algoritmo SHA-512 a la clave ingresada por el usuario. Luego siempre que se deben validar las credenciales se calcula ese Hash a la contraseña ingresada por el usuario y se lo compara con el Hash almacenado en la tabla. Entre otras cosas esto implica que no tenemos forma de recuperar el valor de la contraseña del usuario ni manipularla de ninguna forma ya que el proceso es irreversible, o sea, dado un hash no se puede obtener el string que lo generó inicialmente.



Otra opción es Utilizando un Proveedor de Identidad Externo que soporte Oauth 2.0 o SAML 2.0: los Identity Providers IdP que podemos utilizar son varios, por ejemplo Google, Facebook, Twitter, Office 365, etc., en estos casos en la base de GAM solo estará almacenado el ID del usuario en la tabla de usuarios, esto se utiliza para asignar por ejemplo a un usuario un ROL y las credenciales del usuario serán gestionadas por el IdP.
AL momento de autenticar al usuario, el usuario será redireccionado al IdP, donde el usuario ingresara sus credenciales, en caso satisfactorio el IdP retornara a al sitio nuevamente.
Las diferencias entre Oauth y SAML tienen que ver con las tecnologías empleadas así como el flujo, pero las alternativas son similares en el sentido de que las credenciales solo se ingresaran en el IdP quien luego de verificarlas retorna el control al sistema que solicito esa validación. En todos estos casos es necesario contar con URLs publicas para lograr las redirecciones necesarias.



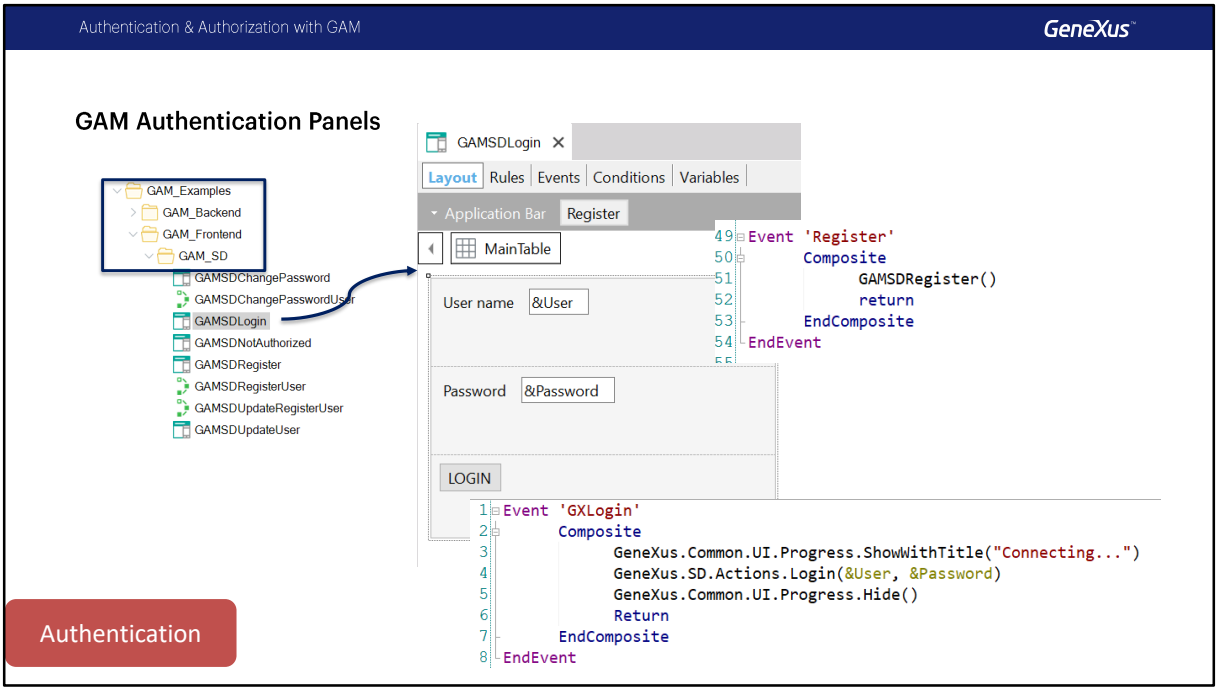
Si utilizamos autenticación Externa, en este caso se configura GAM para interactuar con un proveedor externo que puede utilizar Web Services u otro mecanismo personalizado.
En este caso al igual que en el anterior, en GAM solo se almacena información mínima del usuario ya que la validación de las credenciales de acceso se llevan a cabo en otro sistema.
En estos casos GAM nos provee facilidades para mapear a Roles externos los Roles definidos en GAM.



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 IdP

Para mas información sobre los tipos de autenticación pueden recurrir a la Wiki donde encontraran mucha información, casos de uso y ejemplos detallados.

https://wiki.genexus.com/commwiki/servlet/wiki?15937

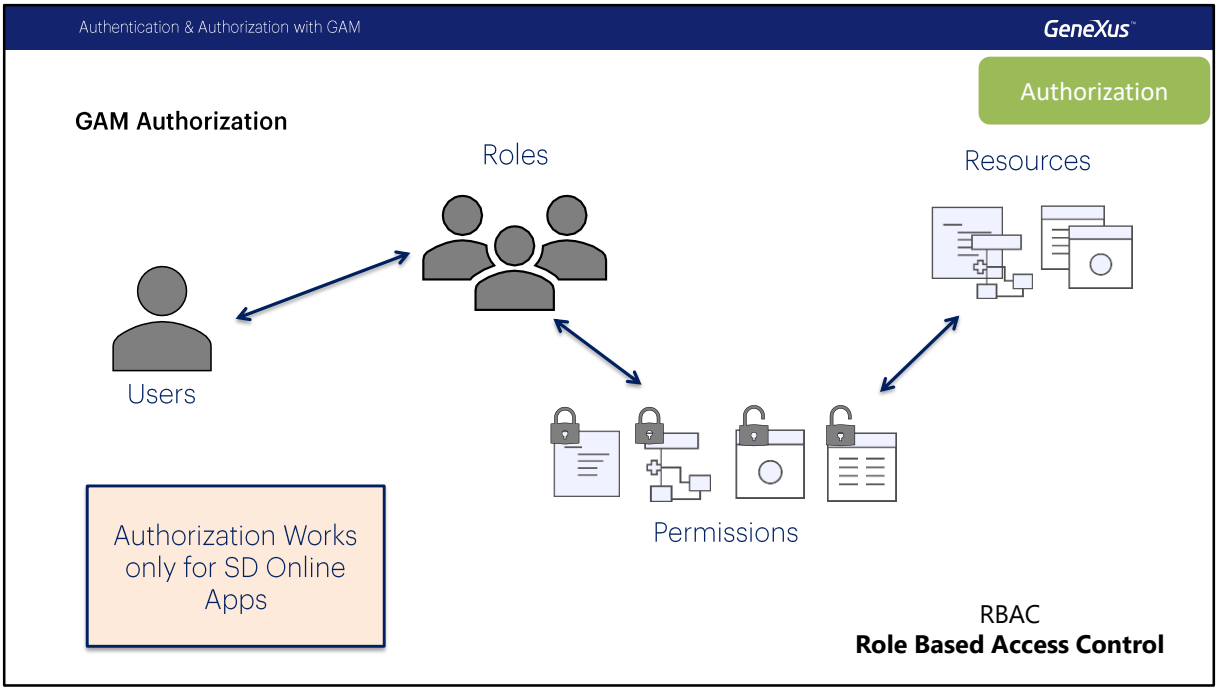


Como parte del mecanismo de Autenticación GAM nos proveerá de dos objetos, un Web Panel y un Panel for Smart Devices ya programados, estos paneles pueden ser personalizados si lo deseamos.

En particular dentro del Folder Gam_Examples encontraremos el Folder Gam_FrontEnd y dentro de este otro folder con nombre GAM_SD 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 SD 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 WEB, en este caso podemos además de ejecutar, personalizar también el modo Insert, Update, Delete o dar acceso Full a una transacción, o sea, ejecución y todos los modos.

En el caso de aplicaciones ONLINE para Smart Devices los recursos a asegurar son:

- Paneles para Smart Devices
- WorkWith for Smart Devices, en este caso el permiso es de ejecución y para las acciones sobre la transacción se manejan sobre la transacción expuesta como business component.

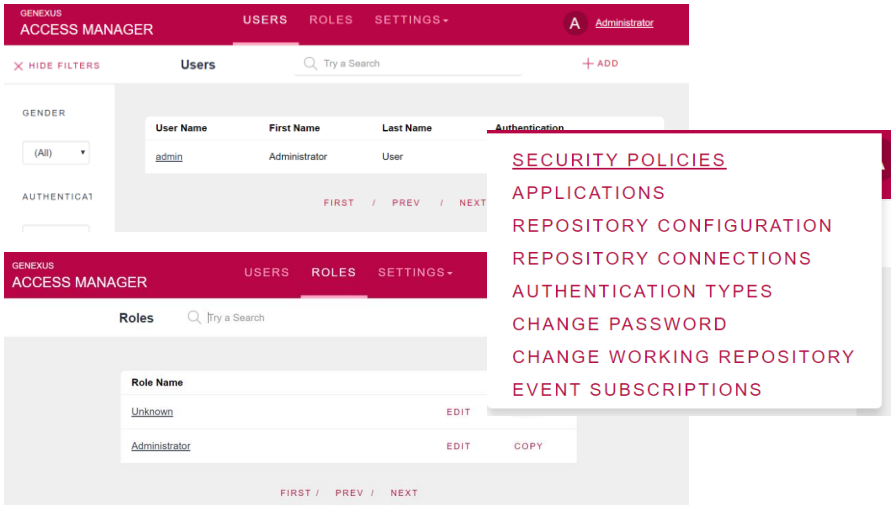
- Procesos o Data Providers con protocolo Rest

En el caso de Aplicaciones para Smart Devices 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. Como ya mencionamos, el panel de Login, GAMSDLogin debe ejecutar siempre en forma OnLine, es decir que para acceder el dispositivo debe estar conectado, para que se realice la validación de las credenciales, una vez que el usuario fue autenticado de ahí en mas puede trabajar en forma desconectada, hasta que se venza la sesión iniciada.

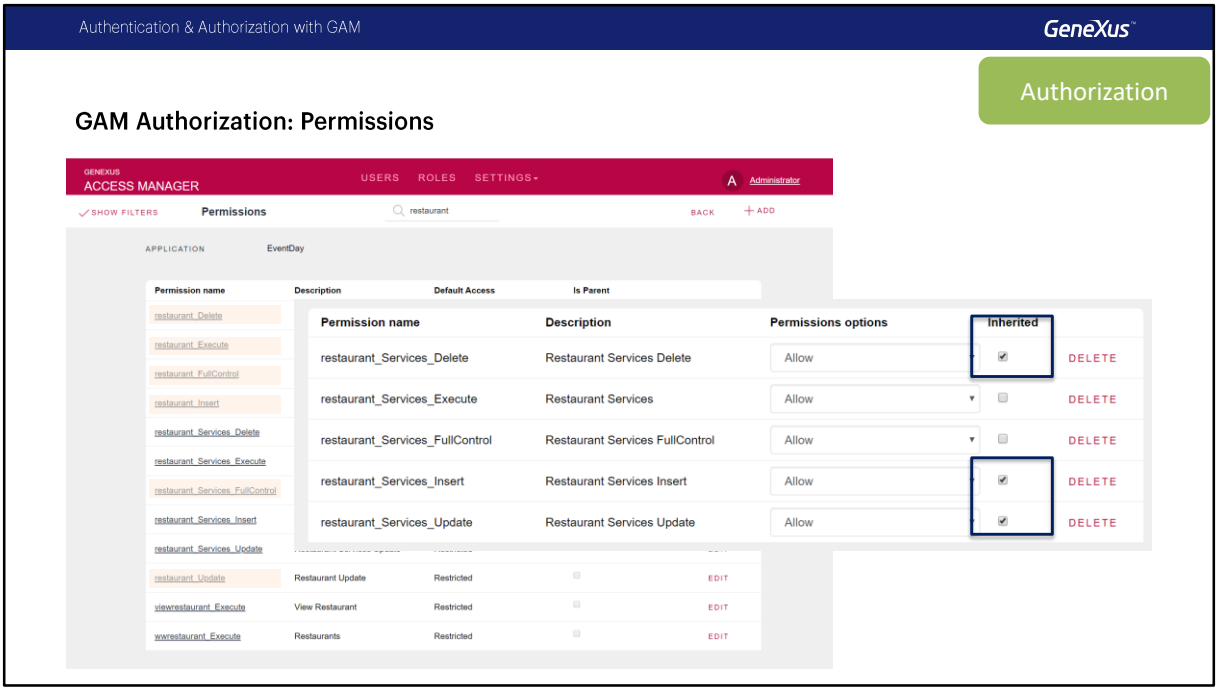
GeneXus

Authorization

GAM: Backend Web



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



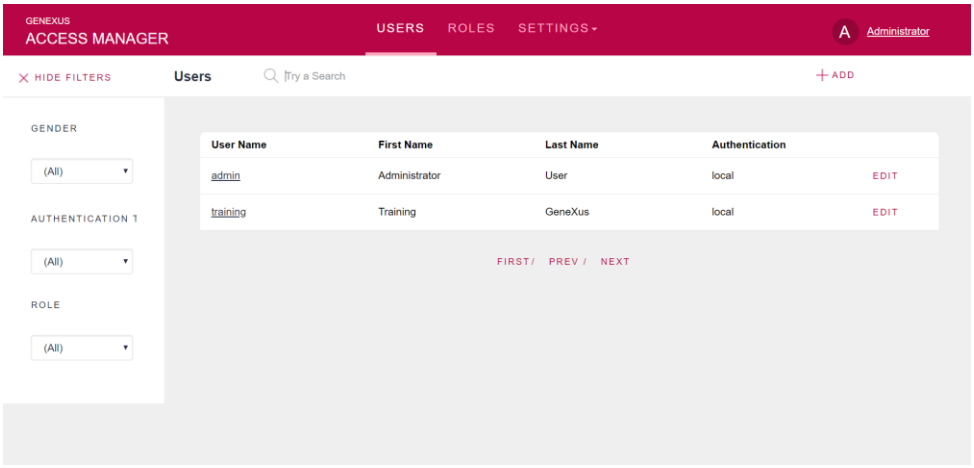
Una de las facilidades que nos brinda GAM es que para cada aplicación se encargara de generar los recursos sobre los cuales hay luego que dar los permisos.

En la imagen vemos los que se generaron relacionados a Restaurant.
Ahí podemos ver que tenemos por un lado los permisos de la transacción Restaurant, tenemos uno para cada modo (insert, update y delete) , además ejecución, y otro que indica FullControl.
Luego también vemos que aparecen recursos con el nombre Restaurant_Services, estos se refieren a la transición cuando es utilizada como BC y expuesta como REST pero además también es el prefijo que se utiliza en el objeto WorkWith For Smart Devices.
Al autorizar a un rol con FullControl le estamos dando sobre esa transacción todos los permisos, ejecución y cada uno de los modos los cuales se mostraran como Heredados.

Demo: GAM Backend & Authorization

Vamos a ver todo esto que hablamos en GeneXus.

GAM Backend: Users



Vamos a ver todo esto que hablamos en GeneXus.

En la demo anterior solo vimos que nos pedía login, tanto en Web como en la aplicación para Smart Devices, esto es porque habíamos dejado el valor default en el nivel de seguridad que era Authentication.

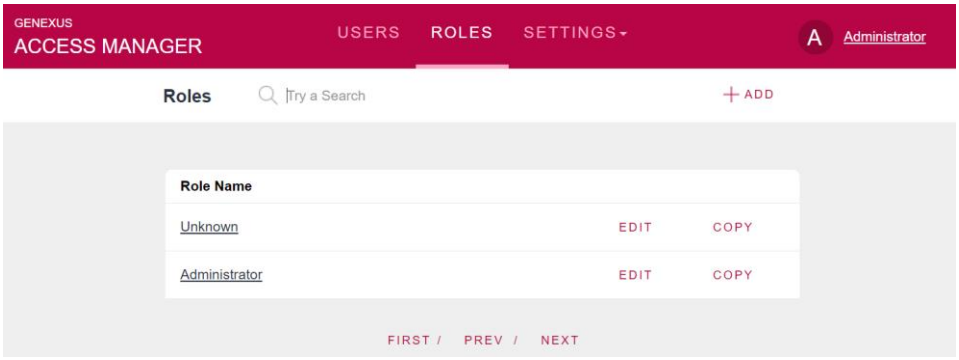
Yo ya prepare la KB para que ejecute en forma OnLine nuevamente y además configure el Nivel de Seguridad en Authorization, luego de hacer cambios en esta propiedad hay que hacer un Rebuild All de la aplicación.

Entonces ahora nuestra aplicación esta lista para autenticar y autorizar a los usuarios.

Primero vamos a entrar al Backend Web de GAM, el objeto es GAMHome.

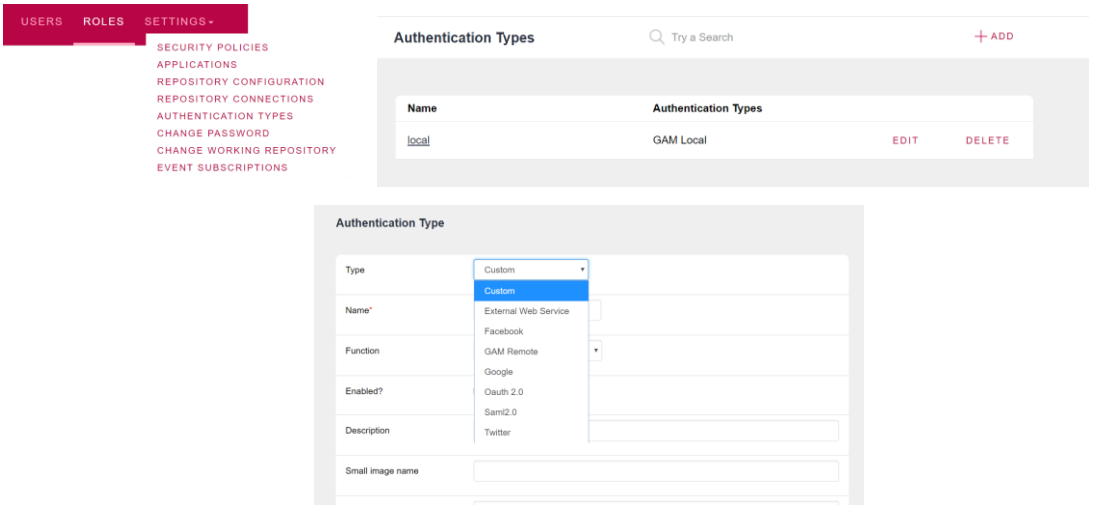
Nos pedirá el login, usamos el único usuario que tenemos que es admin, la contraseña es admin123, en mi caso el navegador esta recordando las credenciales.
Bien, lo primero que vemos es el panel de administración de Usuarios, aquí podemos crear o editar la información de los usuarios.

GAM Backend: Roles



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, cuando se auto registran los usuarios quedan asociados al rol Unknown. Nosotros podemos cambiar cual es el rol por defecto que se usa en este caso.

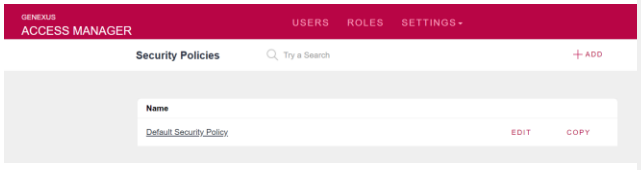
GAM Settings: Authentication Types

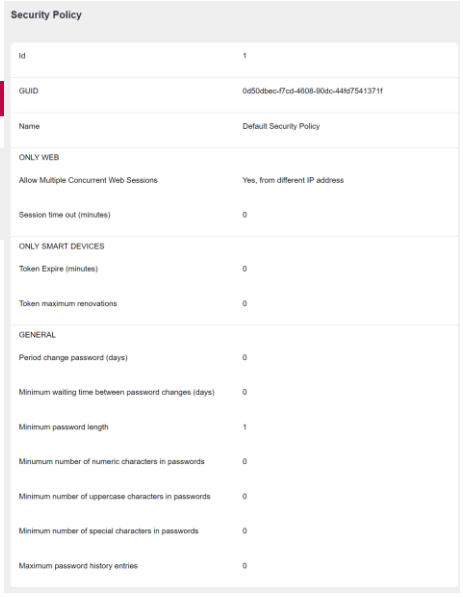


Y en este menú tenemos acceso a toda la configuración de GAM.
Tenemos las aplicaciones, vean que en este caso tenemos definidas 3 aplicaciones, la aplicación GAM que tiene todo el backend de GAM, la aplicación WEB y la aplicación EventDay SD.

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.

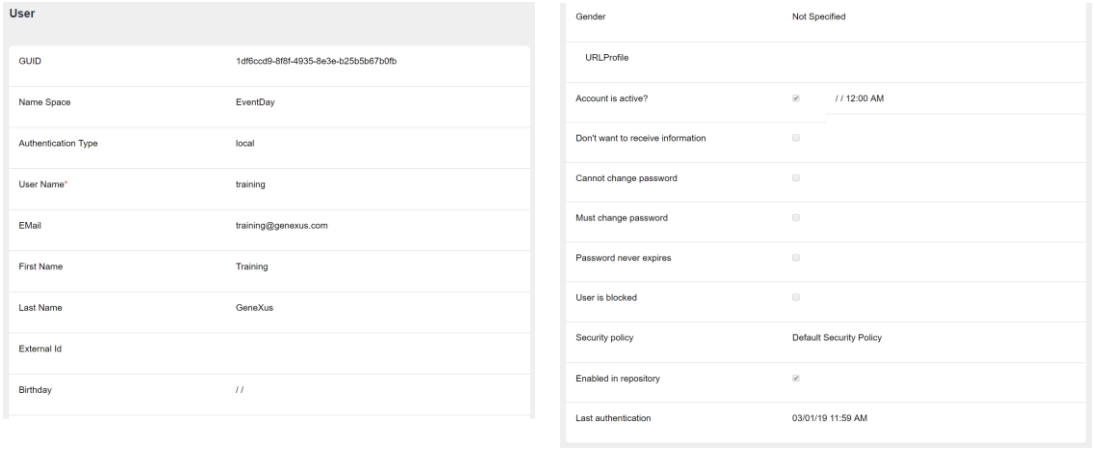
GAM Settings:



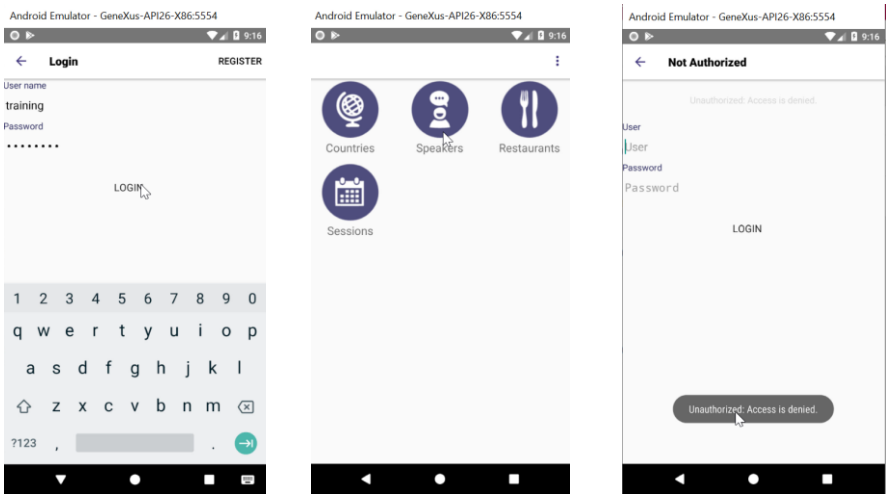


Tenemos por ejemplo políticas de seguridad, veamos como esta configurada la política default, por ejemplo para Smart Devices podemos elegir el tiempo de expiración de los tokens de seguridad. Acá por ejemplo en General, tenemos el periodo en días para obligarle a cambiar la contraseña al usuario, el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

GAM Backend: New User

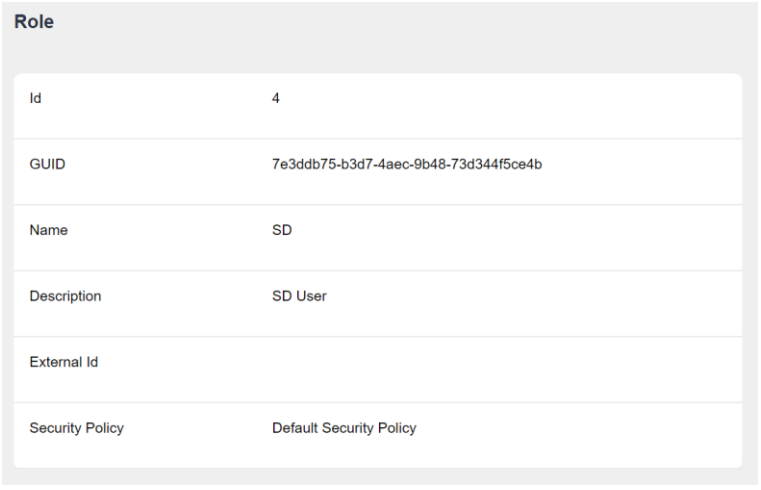


Bien, lo que vamos a hacer es crear un nuevo usuario.
Vamos a usuarios, Agregar y vamos a ingresar training como User Name, como mail ingresamos training@genexus.com , de contraseña ponemos training, confirmamos de vuelta la contraseña, de nombre training y apellido GeneXus , el resto dejamos todo por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



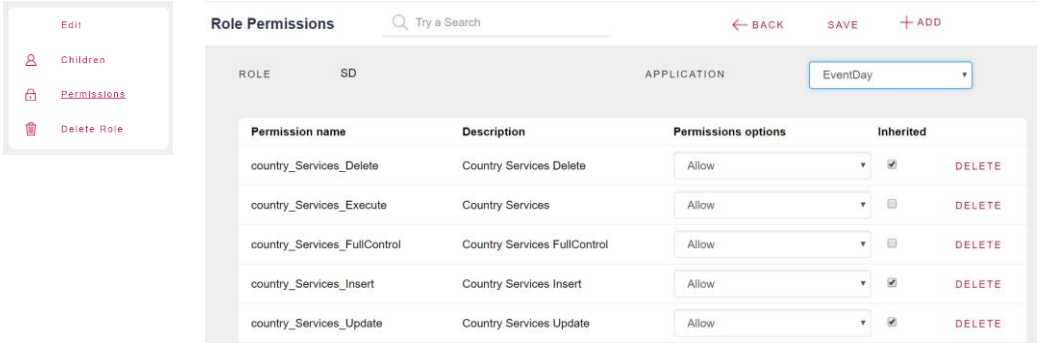
Ahora puedo ir al emulador y acceder en la app con este usuario.
Ingresamos training, usuario y contraseña son iguales.
Y ahí me deja acceder al menú, en este caso, el menú no requiere permisos especiales, solo con que el usuario este autenticado lo podemos ver.
Pero si queremos acceder a las opciones, por ejemplo oradores, me da acceso no autorizado.
En países, lo mismo.
Esto es porque configuramos la aplicación para nivel de seguridad Autorización, y no le hemos dado ninguna autorización al usuario, solo lo creamos. De hecho ni siquiera le asignamos un rol.

GAM Backend: New Role



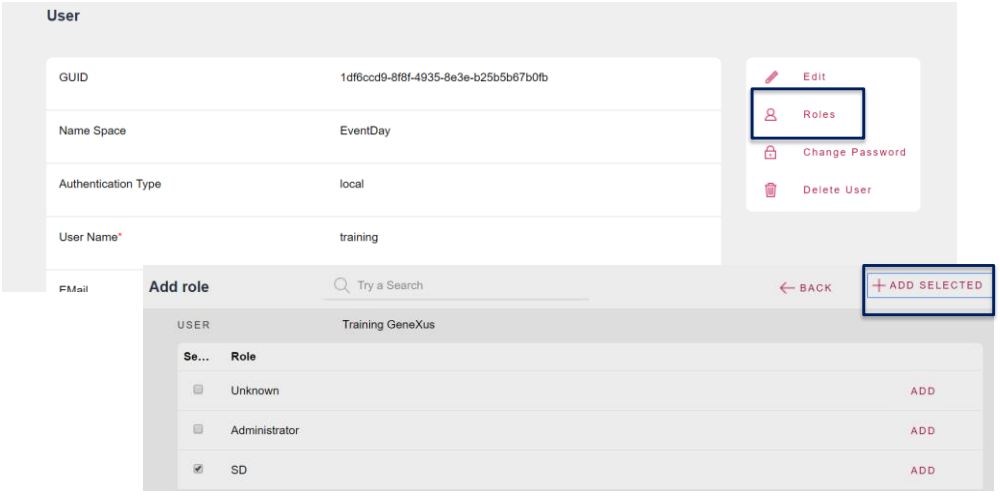
Ahora vamos a crear un Rol, vamos a poner Rol SD, la descripción SD User. Asociamos también una política al Rol y confirmamos.

GAM Backend: Add Permissions to Role



Bien, ahora tenemos que acceder al Rol y darle permisos sobre algunos recursos.
Seleccionamos la aplicación EventDay y presionamos Add.
Ahí nos muestra una lista con todos los recursos sobre los que podemos dar permisos.
Y podemos ir seleccionando varios. Luego de seleccionar algunos, presionamos en Add Selected para volver.
Vamos a agregar uno para acceder a países, buscamos country, seleccionamos Country_Services_FullControl. Grabamos.

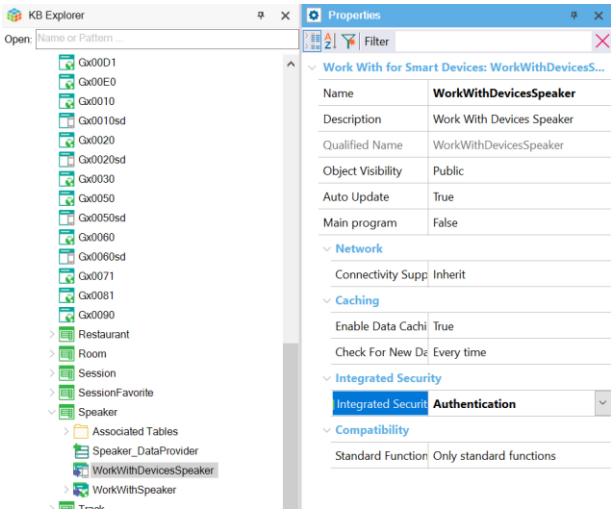
GAM Backend: Add Role to User



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

Y ahora si vamos al emulador y accedemos a Países, ahí si nos muestra la lista. Y nos deja ingresar en modo Insert también.
Pero si vamos a Oradores, no le dimos permiso sobre esto. Así que nos da acceso no autorizado de nuevo.

Custom Security Level



Por ejemplo podríamos desear que para los oradores , no se chequearan los permisos, entonces en el Work With Devices Speaker podemos usar la opción de solo autenticación , podríamos poner None también.
Vamos a correr la aplicación para que tome este cambio.

Ok. Ya termino. Volvamos al emulador.
Y ahora si accedemos a Oradores, nos muestra el panel.
Bien, esto fue solo una pequeña muestra de toda la flexibilidad que nos brinda GAM para manejar la autorización. Recuerden que la autorización solo es para aplicaciones OnLine.

Con esto terminamos el tema.

GeneXus™

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