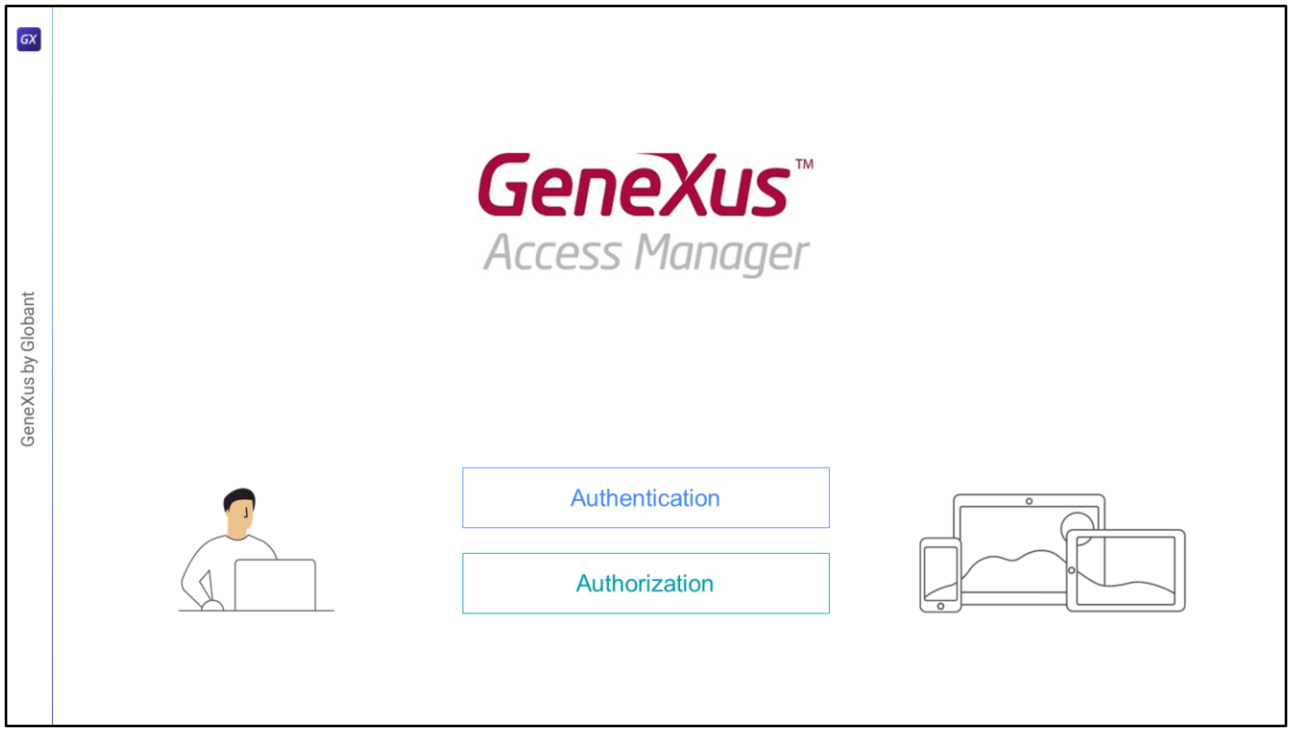
GeneXus by Globant

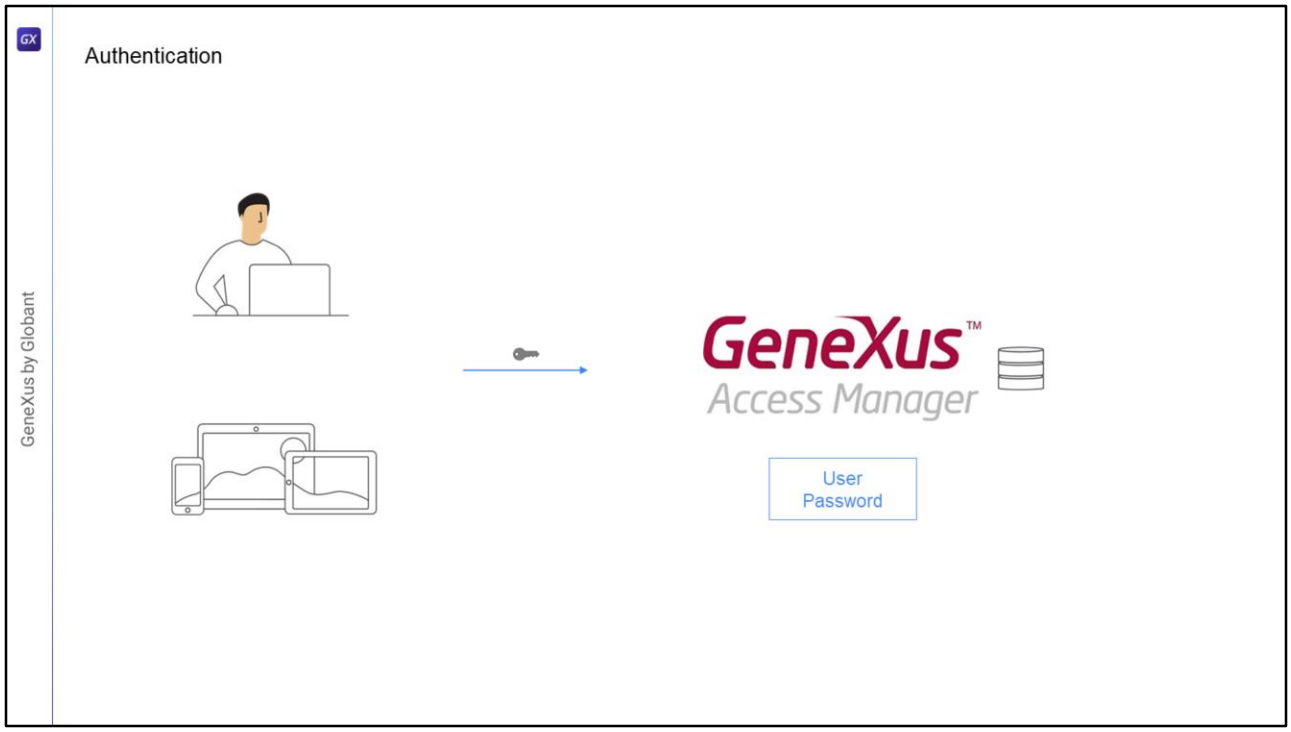
GeneXus Access Manager

Authentication and Authorization

Diego Marranghello



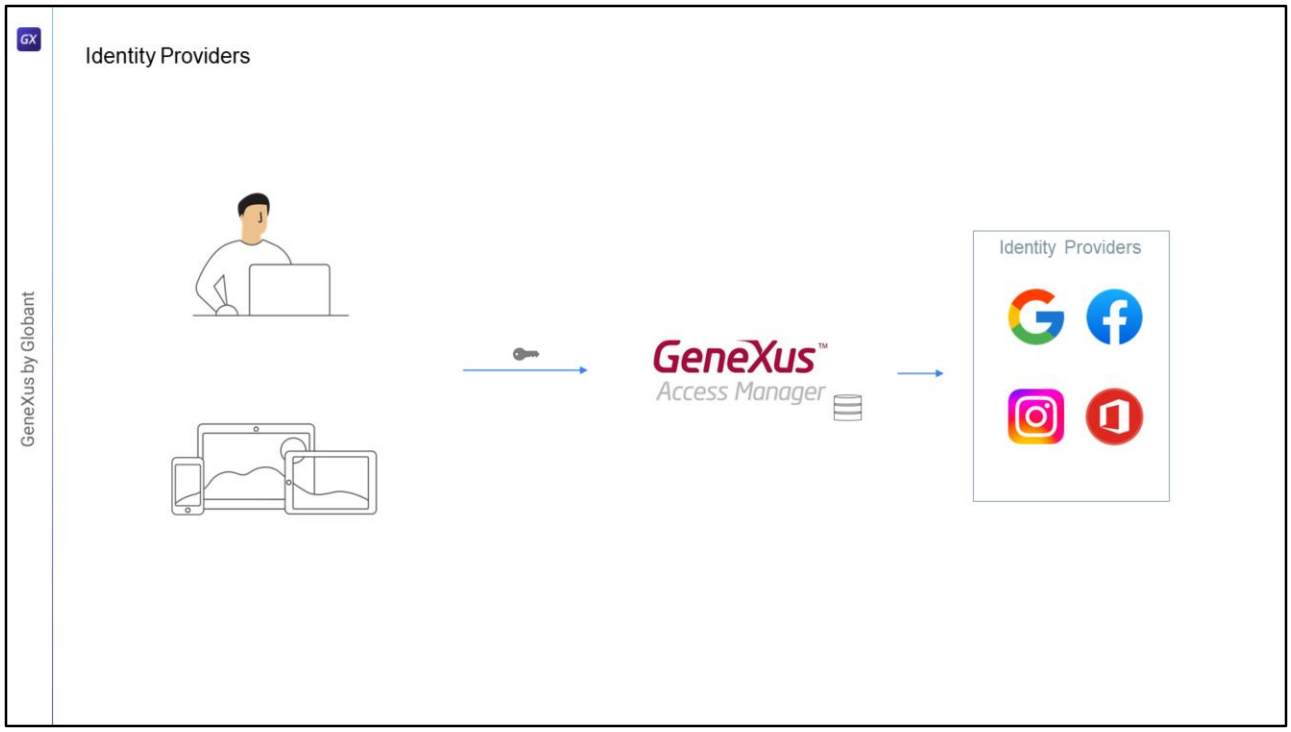
In this video, we will see a little more of the Authentication and Authorization features used in GAM.



Authentication is the process of verifying that users are who they claim to be by validating their credentials. In the case of GAM: username and password.

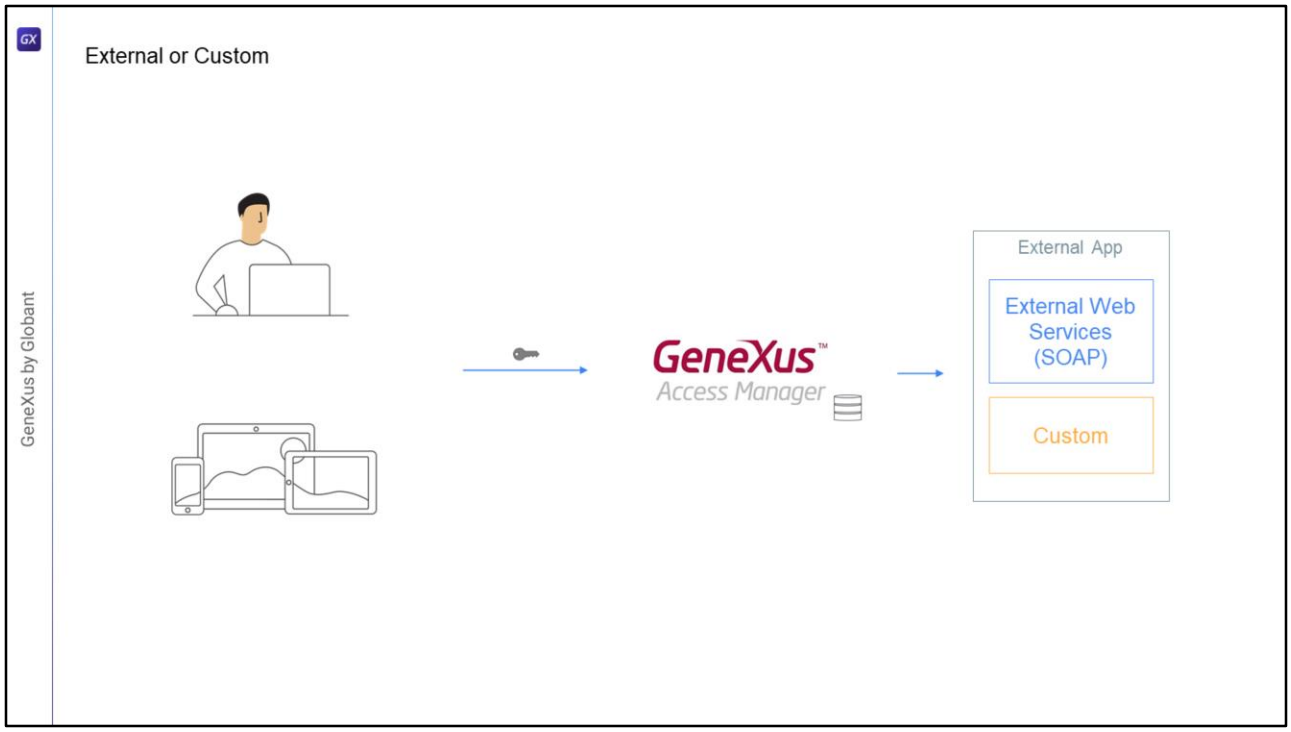
It is possible to implement different types of authentication, and even more than one can be enabled simultaneously.

The types are:
Local: Where the user's credentials will be stored in the GAM database in the user table.



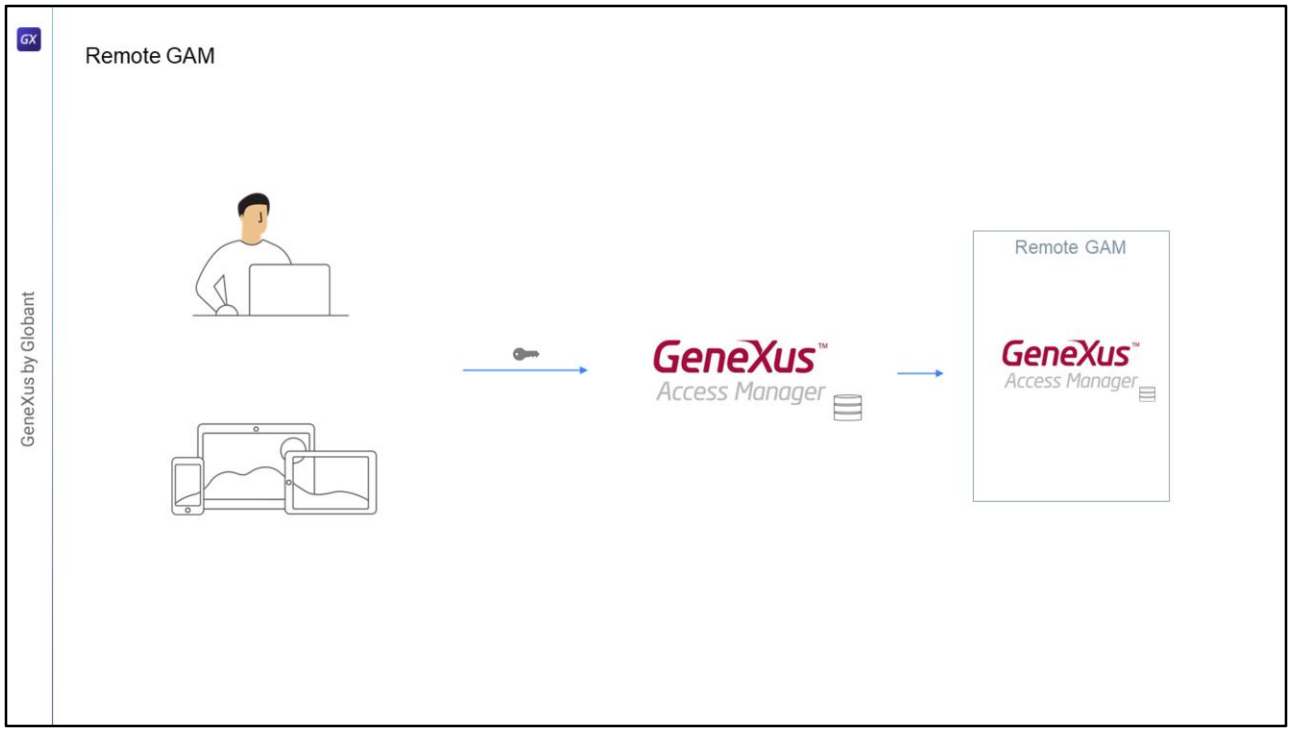
Another option is to use an Identity Provider: there are several Identity Providers that can be used, such as Google, Facebook, Instagram, Office 365, etc. In these cases, the GAM database will only store the user's ID in the user table; this is used to assign, for example, a user's ROLE, and then the user's credentials will be managed by the selected Identity Provider.

When users are authenticated, they will be redirected to the Identity Provider, where they will enter their credentials; if successful, this provider will return to the site again.

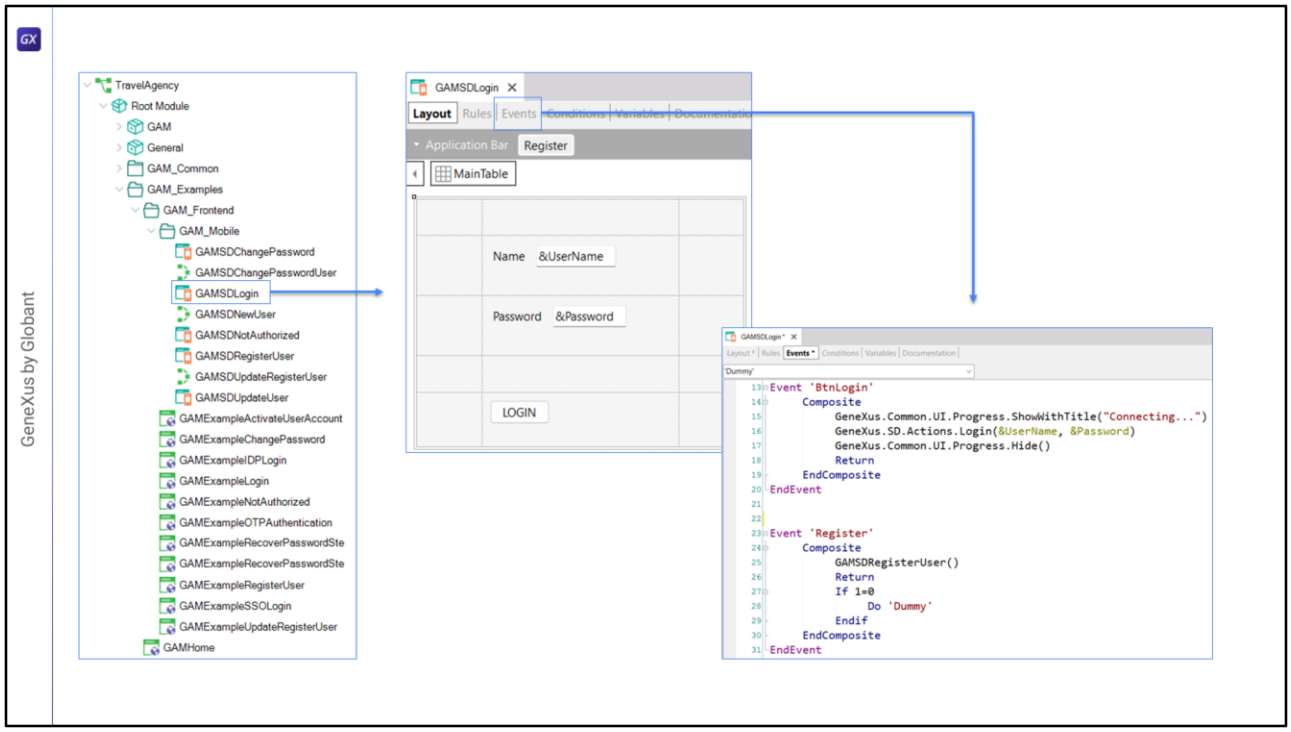


If External authentication is used, GAM must be configured to interact with an external provider, which may use Web Services or another customized mechanism.
In this case, as in the previous one, only minimal user information is stored in GAM, since the validation of access credentials is carried out in another system.

In these cases, GAM facilitates mapping the roles defined in GAM with the external roles.



We can also use Remote GAM since GAM itself is an Identity Provider that will handle the user's credentials. Therefore, we can set up an application using GAM to validate the user's credentials in another GAM instance that will play the role of identity provider.

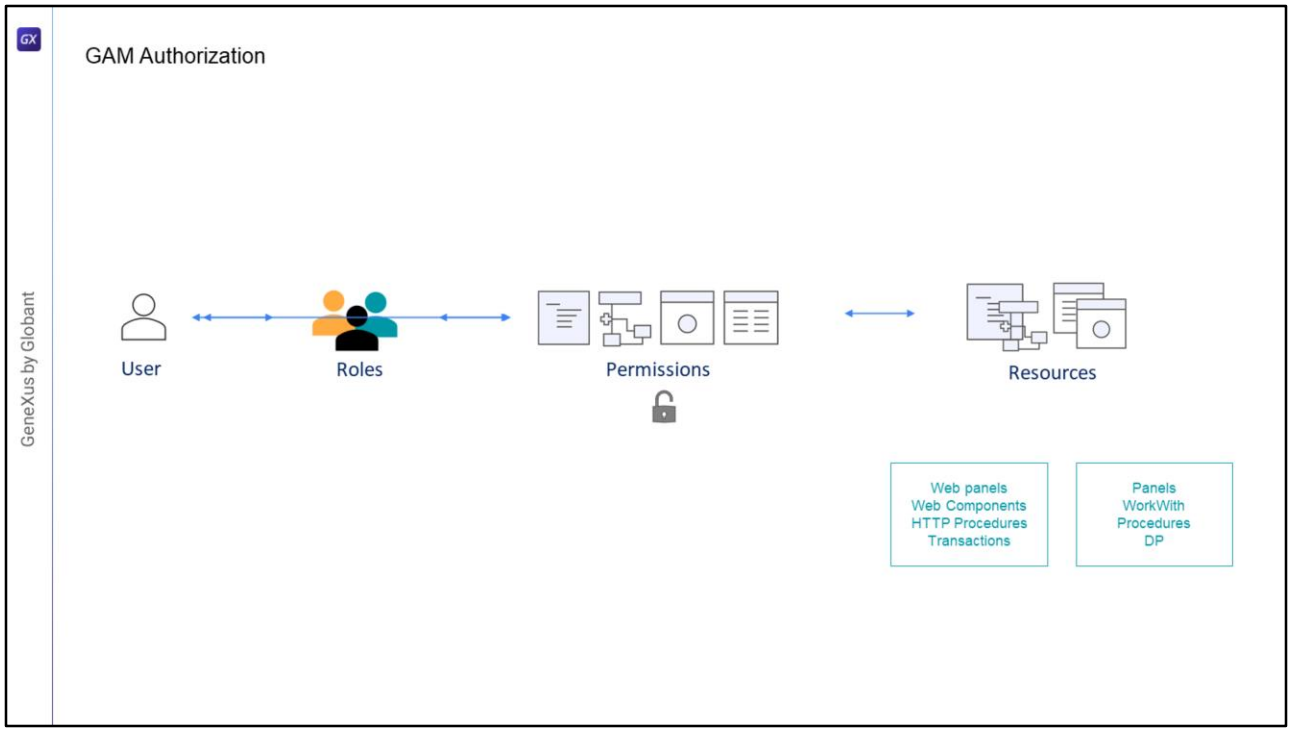


To perform the Authentication, GAM will provide two objects, a Web Panel for the web, and a Panel, which in this case will be used for mobile; these panels can be customized if necessary.

In particular, for mobile, inside the Folder Gam_Examples we will find the Folder Gam_FrontEnd, and inside it another folder named GAM_Mobile with objects that handle login, password change, registration of new users or user data updates.

For example, this is the Login panel –GAMSDLogin– which implements events to handle the login and registration of new users.

An important aspect of this panel is that when the mobile application is offline, this panel must be executed online, which means that the user must have a server connection to access it.



With GAM we can also handle authorization, which is the process of verifying whether a user who has already been authenticated has the necessary permissions to perform some action in the system.

For this, GAM has a scheme based on User Roles. Each GAM user has one or more associated Roles; in addition, we will have secured Resources and the assignment of Permissions on these Resources to the Roles.

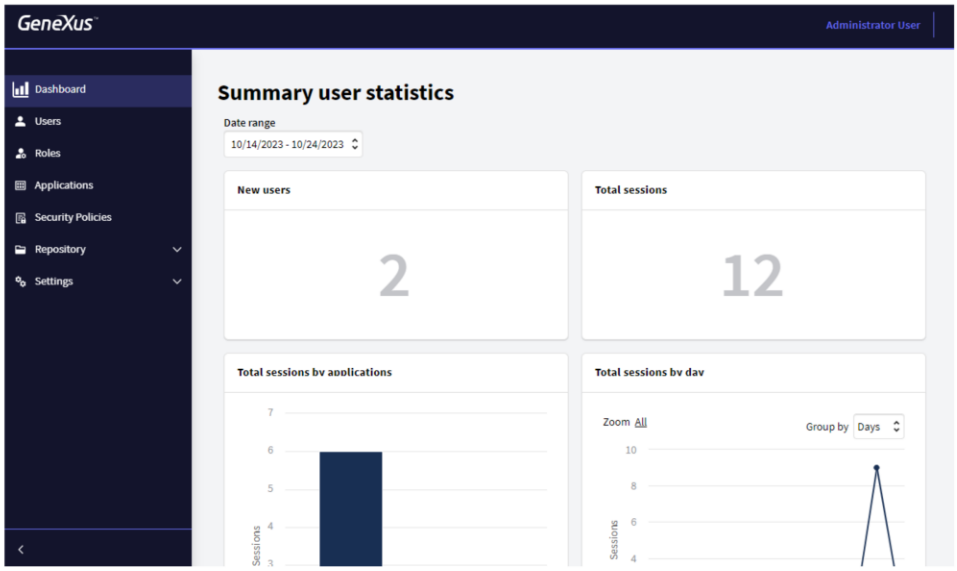
The resources that can be secured are:
Web panels
Web Components with URL Access enabled
Processes with HTTP Protocol, for example, reports with PDF output.
Transactions: in this case, we can not only execute, but also customize the Insert, Update, Delete mode or give Full access to a transaction.

In the case of ONLINE applications for mobile devices, the resources to secure are:
Panels
WorkWith
Processes or Data Providers with Rest protocol

In the case of Offline Applications for mobile devices, we will only have authentication. Since the application is offline, we will not be able to keep the permissions, given that if we modify them some devices may not synchronize, thus making the scheme unfeasible.

GeneXus by Globant

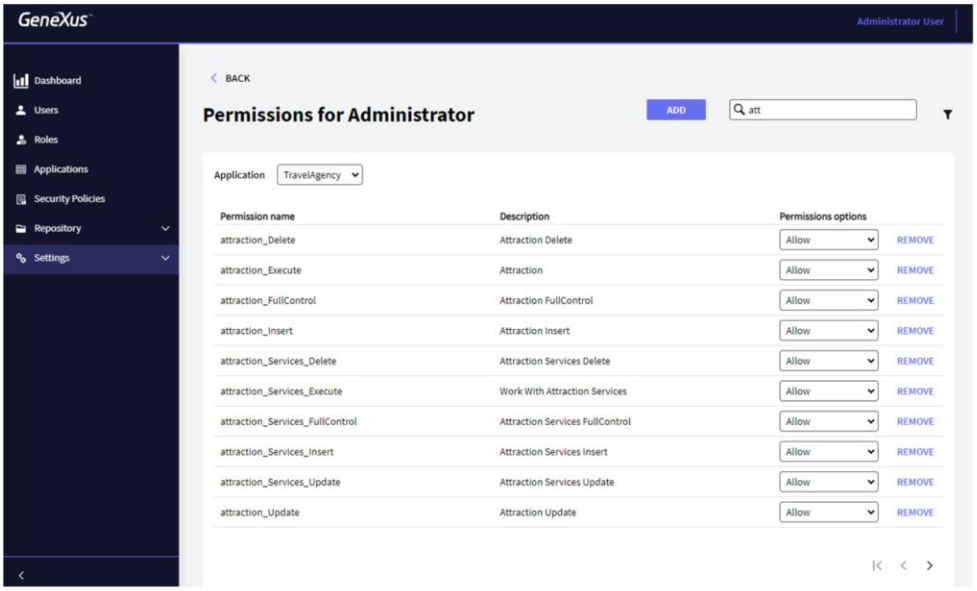
Web BackOffice



To manage all this information, GAM provides a web backoffice, which will allow us to manage users, roles, permissions, and other application settings such as authentication types and other configuration parameters.

GeneXus by Globant

GAM Authorization: Permissions

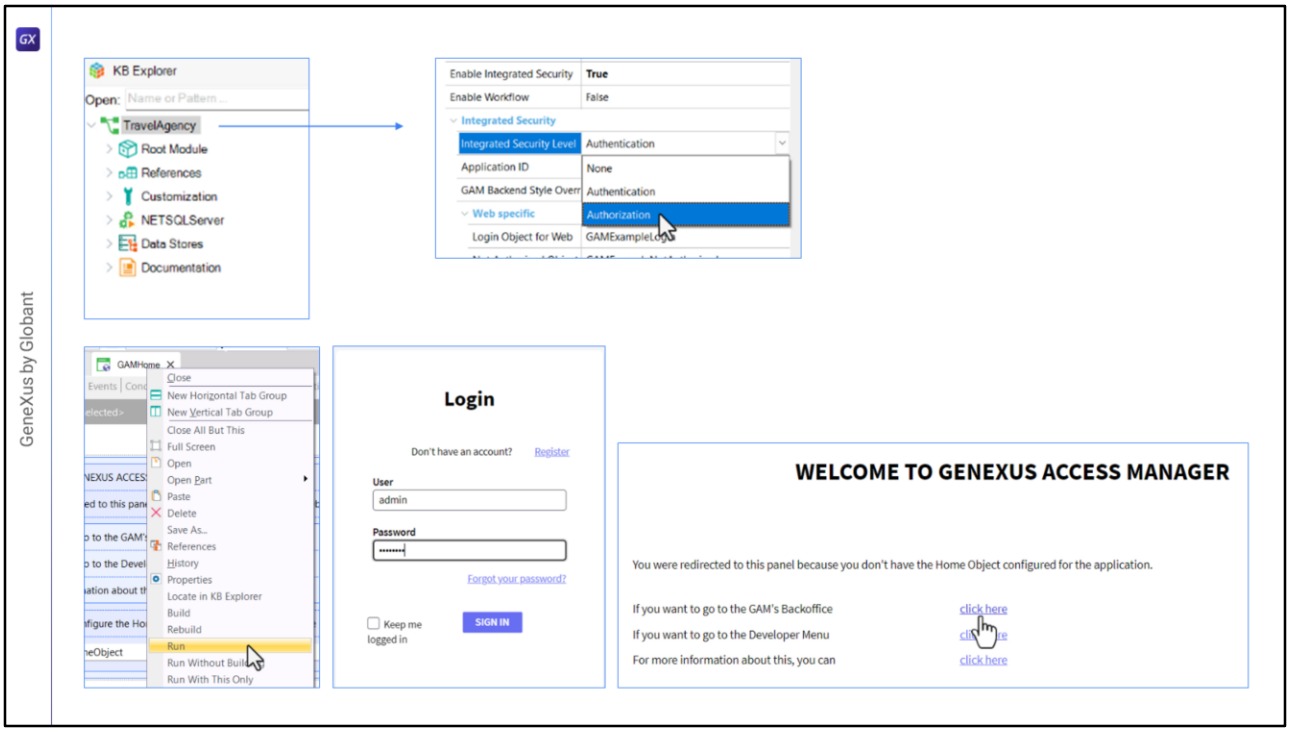


One of the advantages provided by GAM is that for every application it will generate the resources on which the permissions have to be given.

We can see that on one hand we have the permissions of the Attraction transaction; we have one for each mode (insert, update and delete), also one for the execution, and another one that says FullControl.

Then we also see that there are resources named Attraction_Services; these refer to the transition when it is used as BC and exposed as REST, or when it is used in the WorkWith object.

When selecting a role with FullControl we are giving all permissions on that transaction, execution, and each of the modes that will be shown as inherited.



Let's take a look at what we've talked about in GeneXus.

In the KB that we are seeing, we have previously set the Enable Integrated security property to true, in the knowledge base version node.
And we left everything by default, so the security level is set to Authentication.

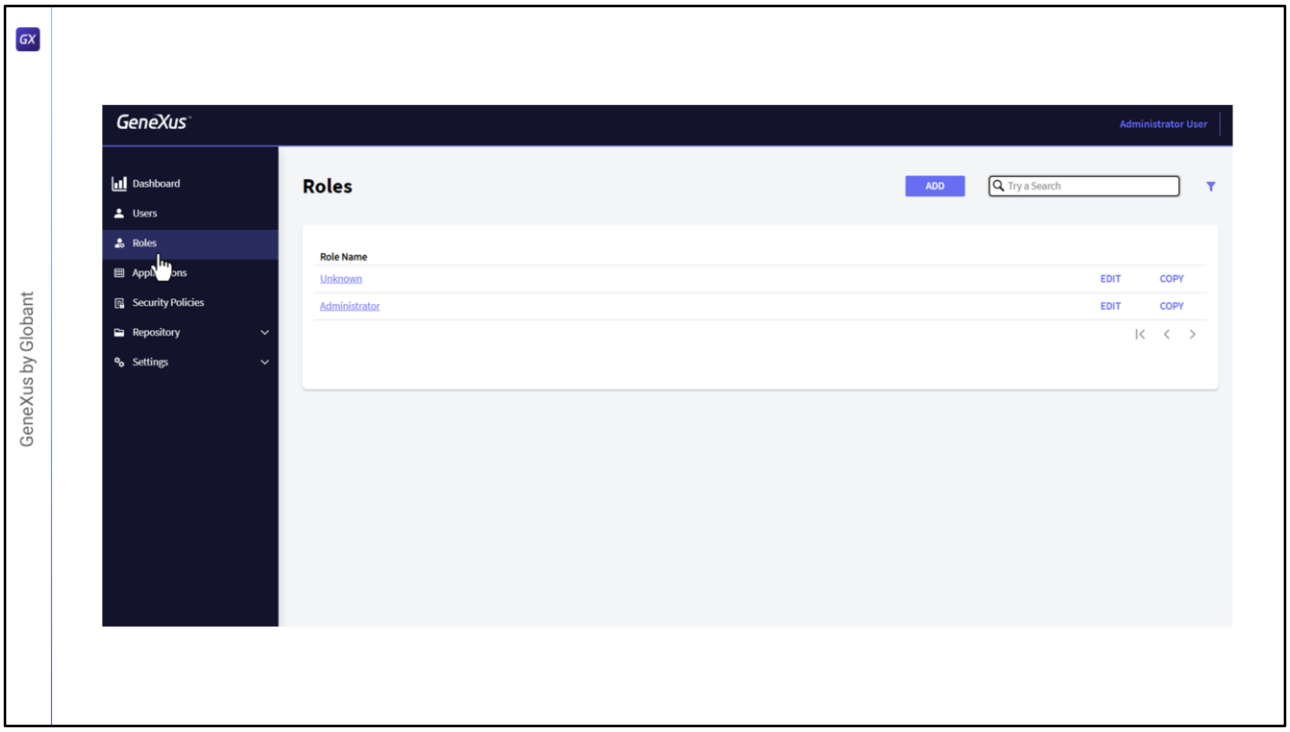
Now we will change it to Authorization; after changing this property we have to do a Rebuild All of the application.

So now our application is ready to not only authorize, but also authenticate users; that is to say, manage their permissions.

First we are going to execute the GAMHome object, which must have the main program property set to true so that we can execute it directly.

It will ask for login, so we use the only user that we have created by default: admin and the password admin123.

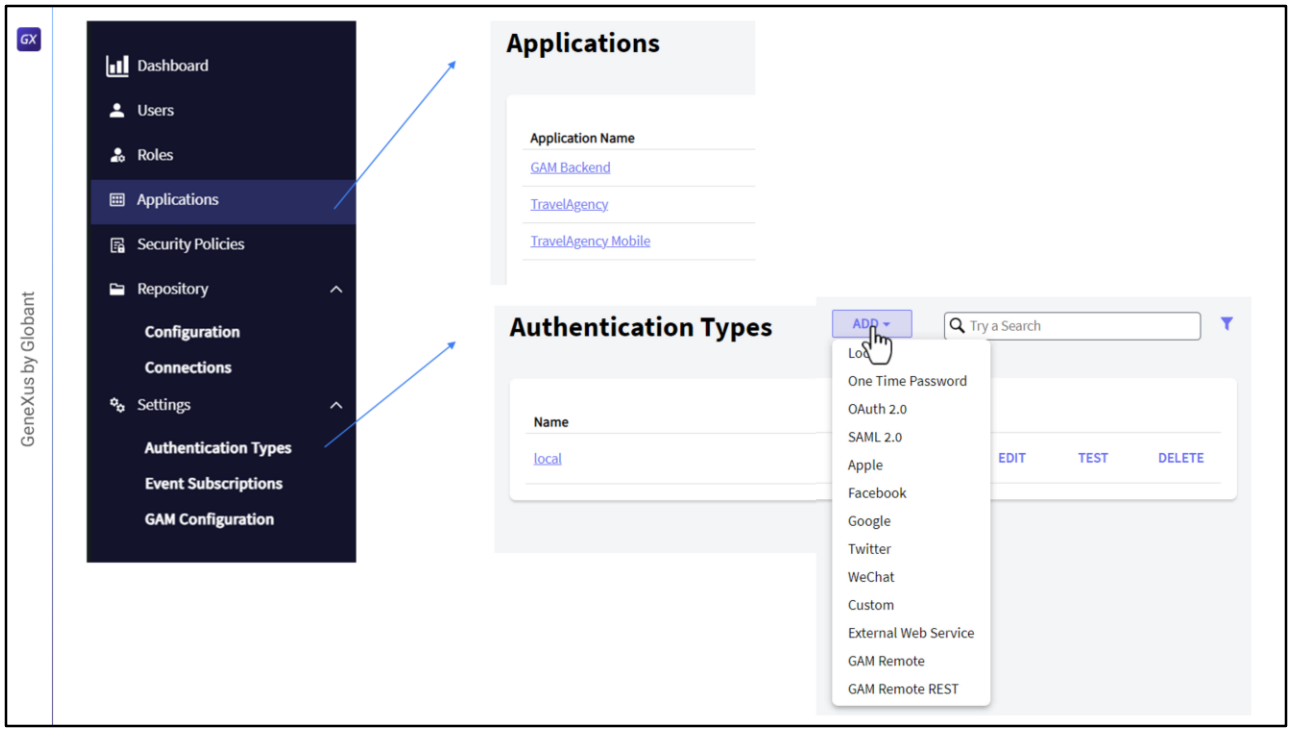
We select to enter the GAM Backoffice, go to the Users section where we can create or edit the users information.



Then we have Roles, where we can define the roles we want; by default, there are 2 roles defined. The Administrator role has access to all the functionalities of the back end as well as to permissions on all the objects of the front end.

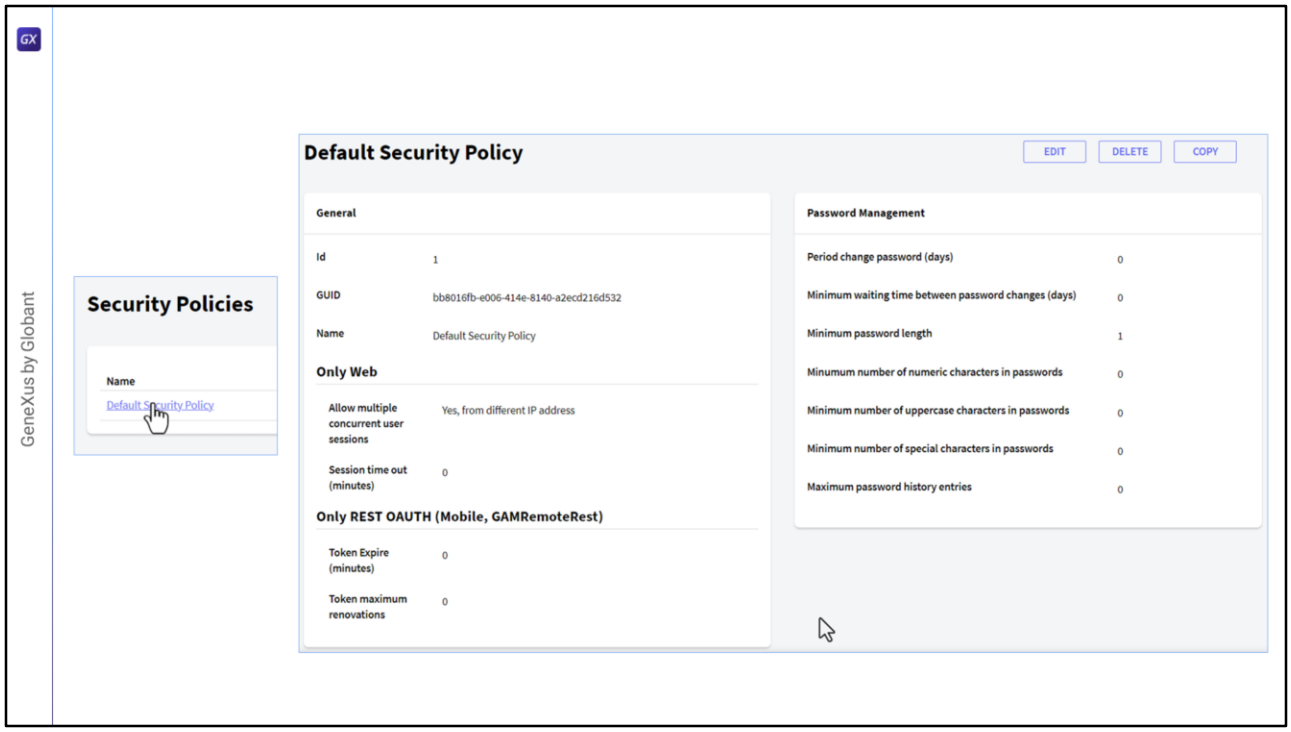
The other role is Unknown. This role is used when we allow users to self-register in the application; that is, self-registered users are associated with this role.

We can change the default role used in this case.

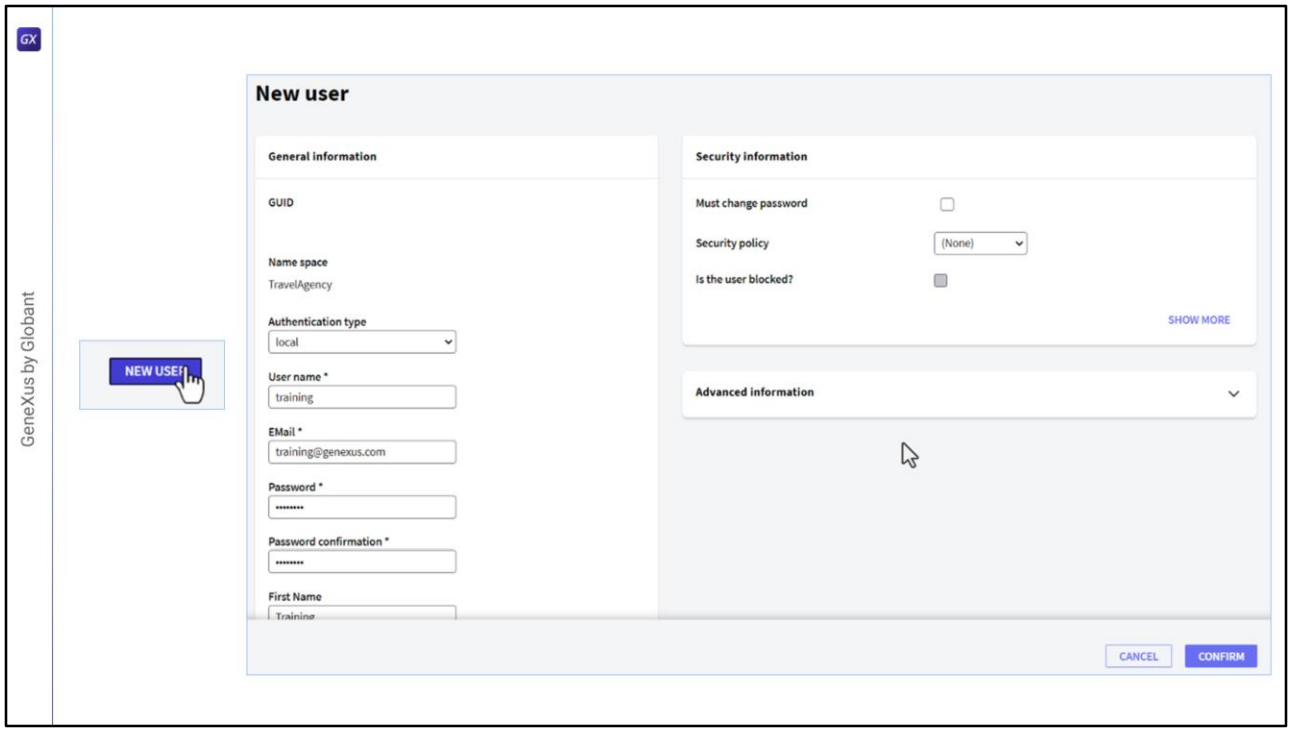


And in this menu we have access to the whole GAM configuration.
Here are the applications. Note that in this case there are 3 applications defined: the GAM application containing the whole GAM back end, the WEB application, and the Mobile application, which in this case have the same name. We are going to edit and change the mobile one to distinguish them.

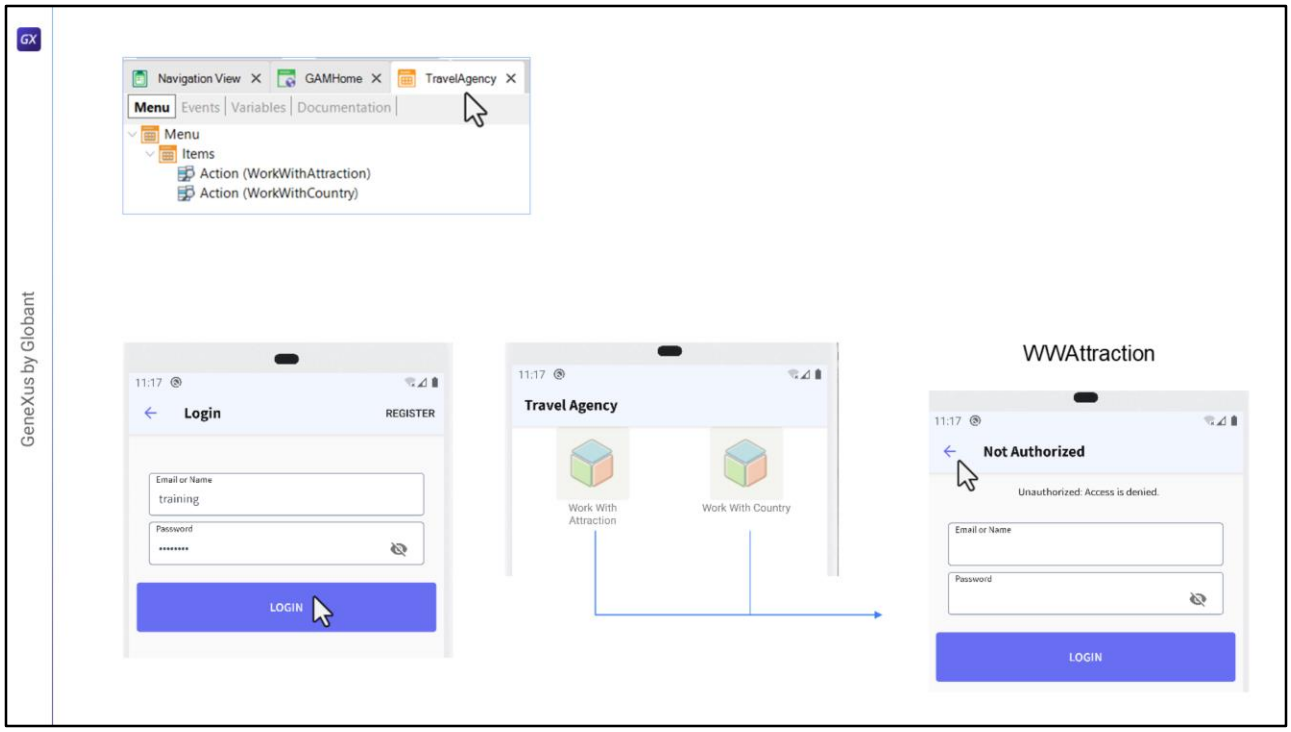
From the menu we can also configure, for example, the administration of the authentication types we mentioned. By default, Local authentication is used, but with Add we could add another type, and here we choose the type we want to add.



There are security policies, and we'll see how the default policy is configured. For example, for mobile we can select the expiration time for security tokens. Here, the period is in days to force users to change their password, minimum password length, and so on. There are many parameters that we can predefine, and we can create several policies, including one for backoffice users, another one for mobile users, etc. We can manage it in a flexible way.



Now, we're going to create a new user.
We go to users, Add, enter training as User name, and as email we enter training@genexus.com. We set the password to training, confirm the password again, set the first name to training and the last name to GeneXus, leave the rest as default. Finally, we assign a policy –the only one we have– and confirm.



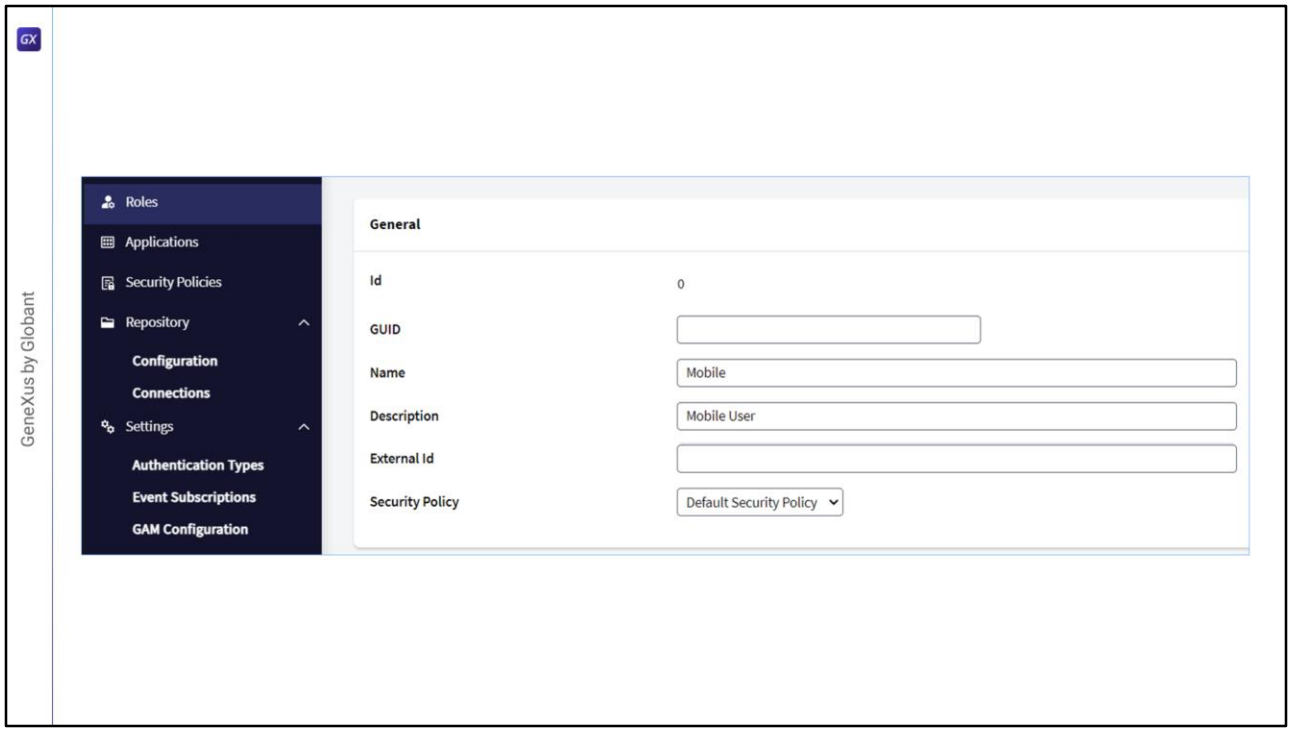
In our KB, we have created a Menu object, set as startup object, and with the following WorkWith objects as Items –the country object and the attraction object.

When executed, it opens the application in the emulator, and the first thing it asks for are the access credentials.
We enter the user that we have just created: user training, and the same password.

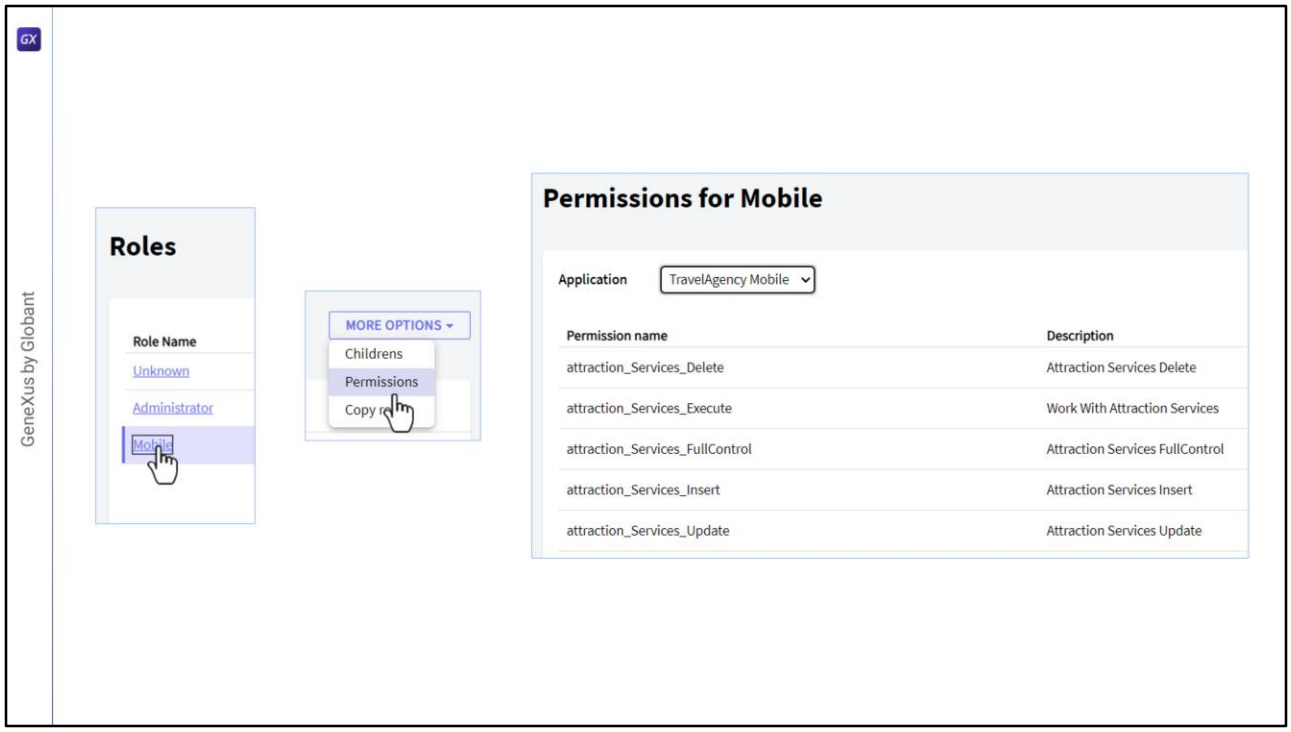
And there we can access the menu with the items that we had entered.
In this case, the menu does not require special permissions and we can see it if the user is authenticated.

But if we want to access the options, such as the Attractions, it shows a message indicating unauthorized access.
It is the same for countries.

This is because we configured the application at Authorization security level, but we haven't given any authorizations to the user yet, we just created it.



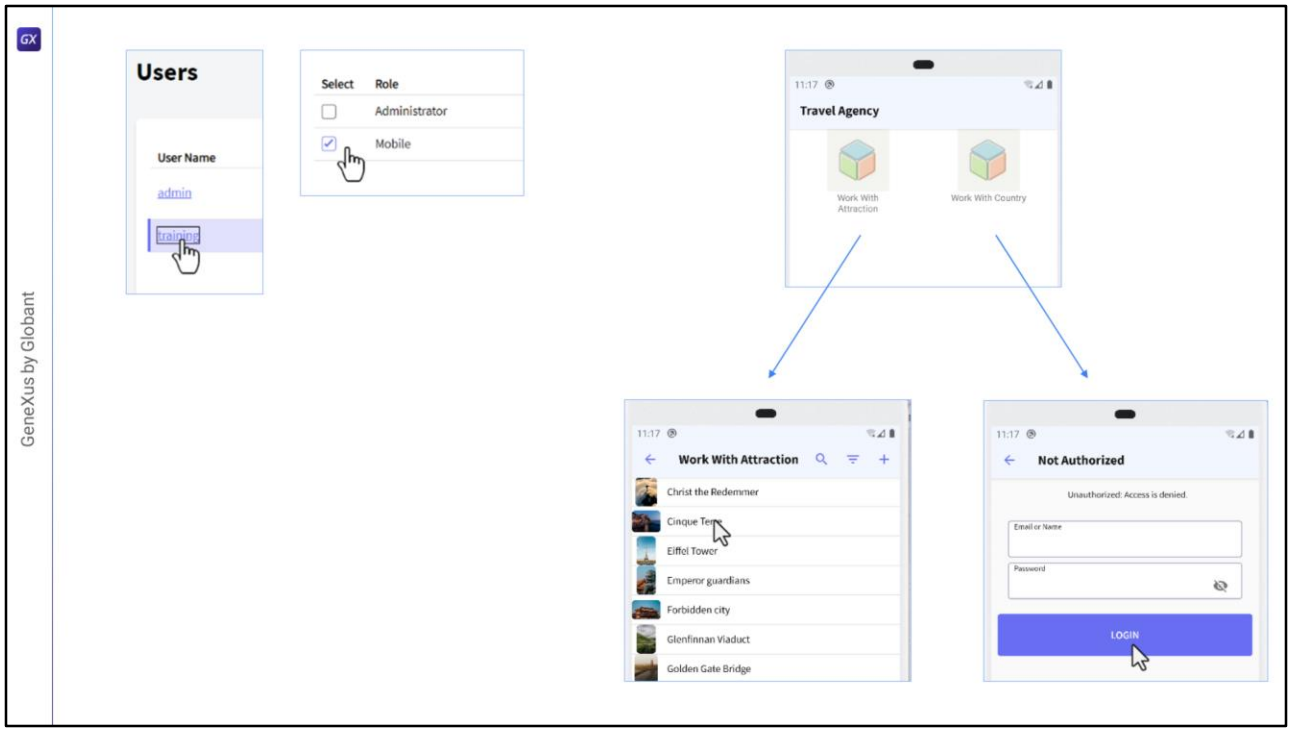
Let's go back to the Web screen to handle these permissions.
Now we are going to create a Role. We enter the “Mobile” Role, with the description Mobile User. We also associate a policy with the Role and confirm.



OK, now we need to access the Role and give it permissions over some resources.
We select the TravelAgency application and select Add.
There it shows a list with all the resources over which we can give permissions.

We are going to add one to access to the attractions, so we look for attraction and select Attraction_Services_FullControl.
When selecting FullControl, we see that all the permissions on the attractions will be inherited.

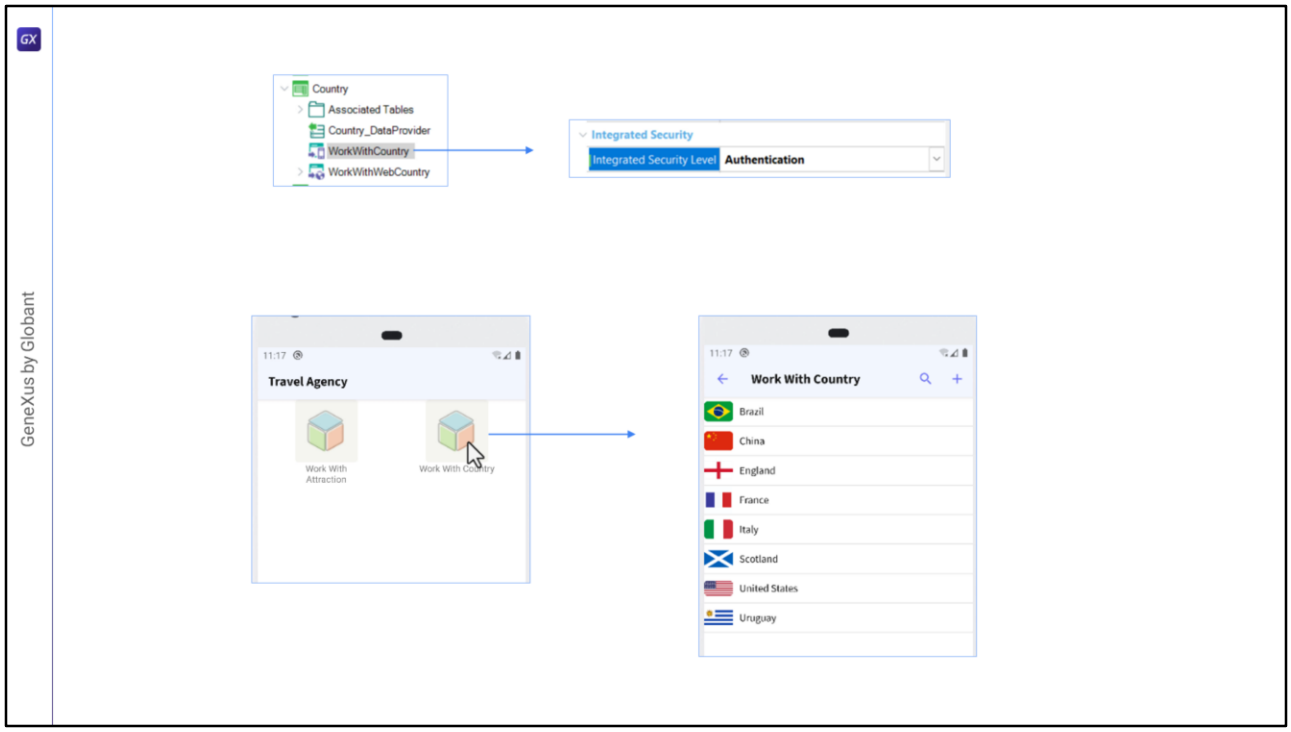
We save.



Now we are going to associate this role with the user that we created.
We click on the username, then on Roles, on the Add option, and select Mobile.
Add Selected and that's it.

If we go to the emulator and access the attractions, the list will be displayed. Also, we can enter in Insert mode if we want to, since we gave it full permission.

Now if we go to countries it shows an unauthorized access message; this is because for countries we have not given any permissions yet.



For example, we may want permissions not to be checked for countries. Then in the Country WorkWith we can use the option to only authenticate; another option would be to set None.

Let's run the application so that it takes this change.

If we access Countries, it will show the list.

Well, this was just a small sample of all the flexibility that GAM provides to manage user authorization and authentication.

Remember that authorization is only for online applications.


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