CHALLENGE 1:

For this challenge, first it is necessary to activate GAM in our knowledge base. To do so, we select Tools/GeneXus Access Manager/Enable Integrated Security.

Some options can be selected, but we will leave them all with their default values. This will import the GeneXus objects associated with the GAM examples so that they will work without having to make changes.

As you can see in the output, the GAM modules and objects associated with security are being imported.

At the KB level, we can see that the *Enable integrated security* property is set to `true`, which means that GAM is enabled in the KB.

Once GAM is imported, we build the application so that the objects are generated considering the new authentication levels. Again, this process takes some time so we will move forward until it is finished.

Since this is the first build of the application, we are asked to reorganize to create the application tables.

This process takes a few minutes, so we will skip it to accelerate the solution.

Once the objects have been generated and deployed taking into account the GAM configuration, we can access the GAM login panel, which is GAMExampleLogin. Here we can use the default administrator credentials, which are admin/admin123.

After selecting to go to the GAM Backoffice we see that the main view is the dashboard. As the letter of the challenge indicated, we proceed to create users through their option.

We are going to use the default authentication type, which is local. The name of the first user was Dave, so we enter his personal data.

Then we do the same with Nate.

Lastly, we create and assign the roles to these users.
We click on Add. The first role will be Manager.

The second one, Assistant.

Now that we have created the roles, we will assign them to the users.

Dave will be assigned the Manager role, and Nate the Assistant role.

That's it. The process is analogous for the other two users.