GeneXus by Globant

GeneXus Access Manager

Introduction

Diego Marranghello

There are several security guidelines to be taken into account when developing our applications. The most important ones are described in the Open Web Application Security Project, the foundation that manages this project, which is an open community that defines and provides information and tools for the development and verification of computer systems from a security perspective.

GeneXus by Globant

OWASP

TOP 10

The foundation has several projects, and among the most renowned and relevant ones is OWASP Top Ten, a document that addresses the most critical security risks to web and mobile applications. One of the project items discusses "Broken Authentication", highlighting the importance of having a good authentication factor.

GeneXus by Globant

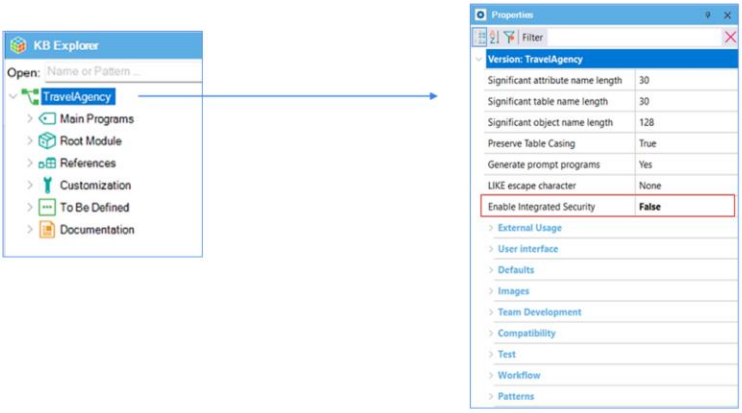
Authentication

GeneXus™ Access Manager

Authorization

GeneXus offers a module called "GeneXus Access Manager" (GAM), which automatically handles authentication. In addition to this task, the GAM allows dealing with authorization concerns, such as restricting access to different parts of the application depending on the roles or permissions of each user. The GAM also provides several objects to manage all the security issues related to a web or mobile application. For example, objects to add users, assign roles, grant permissions, and so on.

Enable Integrated Security

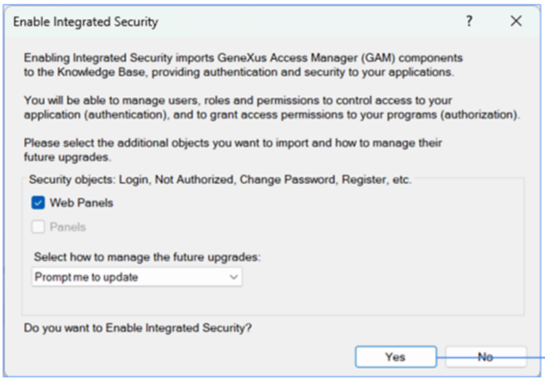


Version: TravelAgency

Significant attribute name length	30
Significant table name length	30
Significant object name length	128
Preserve Table Casing	True
Generate prompt programs	Yes
LIKE escape character	None
Enable Integrated Security	**False**

Security controls are automatically enabled by configuring the "Enable Integrated Security“ property that can be found in the preferences window by selecting the active version of our KB.

Importing GAM Objects



Enable Integrated Security

Enabling Integrated Security imports GeneXus Access Manager (GAM) components to the Knowledge Base, providing authentication and security to your applications.

You will be able to manage users, roles and permissions to control access to your application (authentication), and to grant access permissions to your programs (authorization).

Please select the additional objects you want to import and how to manage their future upgrades.

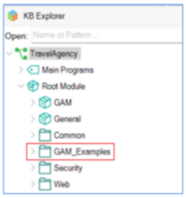
Security objects: Login, Not Authorized, Change Password, Register, etc.

☑ Web Panels

□ Panels

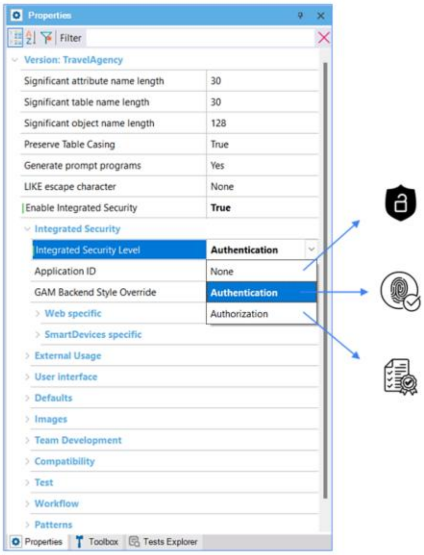
Select how to manage the future upgrades: Prompt me to update

Do you want to Enable Integrated Security?



By changing the property to "True", the components of the GeneXus Access Manager will be imported into our KB. Below the Root Module we will find several objects that provide the GAM functions.

Integrated Security Level



Version: TravelAgency

Significant attribute name length	30
Significant table name length	30
Significant object name length	128
Preserve Table Casing	True
Generate prompt programs	Yes
LIKE escape character	None
Enable Integrated Security	**True**
Integrated Security	
Integrated Security Level	**Authentication**
Application ID	None
GAM Backend Style Override	Authentication
Web specific	Authorization
SmartDevices specific	

Once security is enabled, the security level can be selected using the "Integrated Security Level" property that can be found at the KB version or object level.

The default value of this property is "Authentication". Some options for the security level of our application are as follows:

None, i.e., no security mechanism is applied.

Authentication, where the user only needs to be logged in to access.

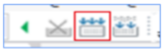
And authorization, where the user not only needs to be logged in but also have the necessary permissions to access each part of the application.

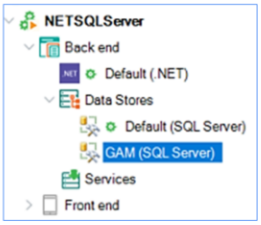
KB

+

GeneXus™
Access Manager

+

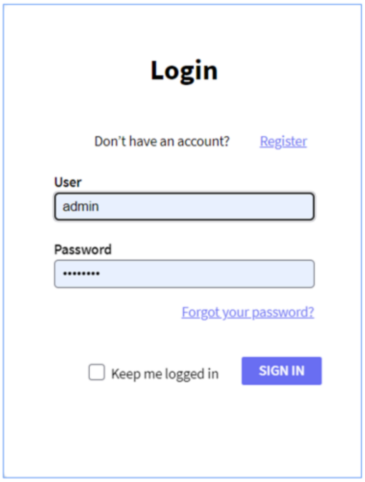




- NETSQLServer
  - Back end
    - Default (.NET)
    - Data Stores
      - Default (SQL Server)
      - GAM (SQL Server)
    - Services
  - Front end

Once the security and level type that our application will use have been applied, we need to “Rebuild all” our KB in order to create the database that the GAM will use.

After enabling security, when running our application a login screen will be displayed for both the web and Smart devices part.



Login

Don't have an account? Register

User: admin

Password: ••••••••

Forgot your password?

□ Keep me logged in

SIGN IN

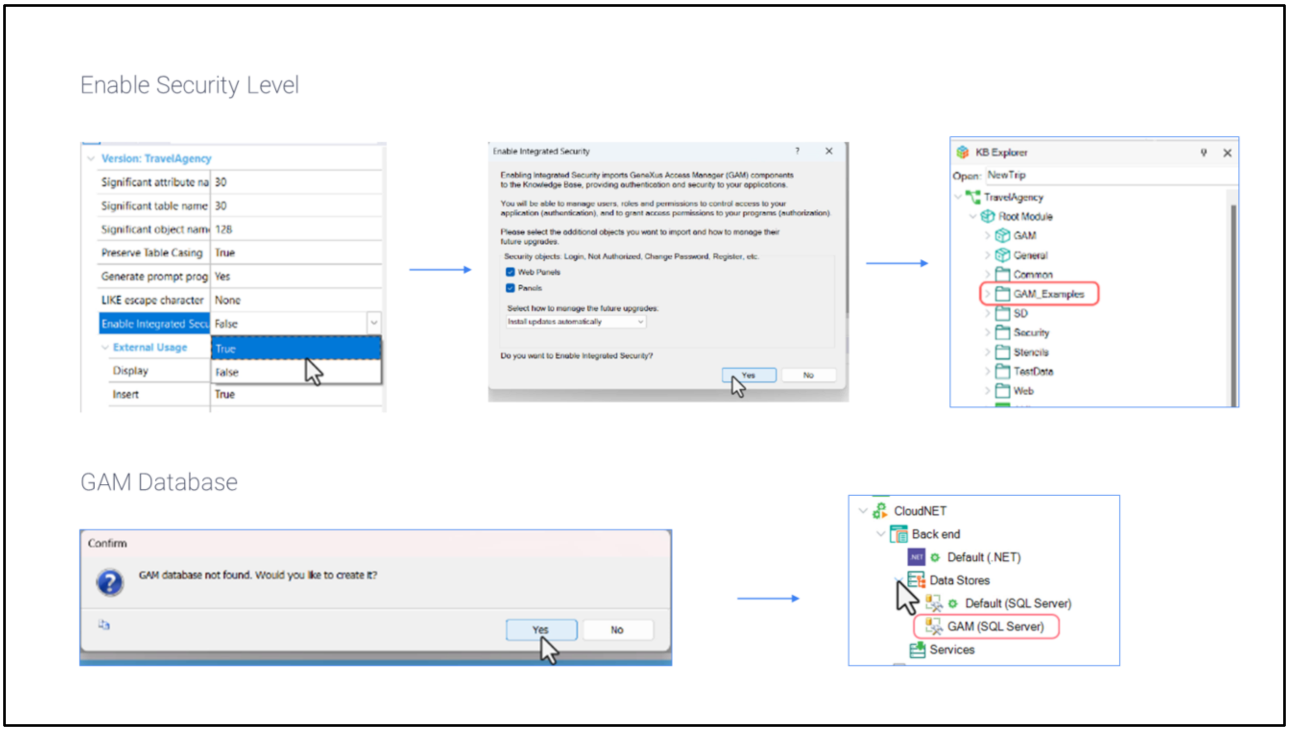
User: admin

Password: admin123

Since we haven't configured users yet, we can use a local user with the following credentials: user: admin and password: admin123. To access the GAM administration console, we must access the "GAM Home" panel.

This panel is GAM's main backend object, where we can configure the users and permissions of our application. Let's see a small demo.

In our example, we want different users to view our backoffice web application depending on their roles. If they authenticate, depending on their roles, they can see certain options.



Enable Security Level

Version: TravelAgency	
Significant attribute na	30
Significant table name	30
Significant object nam	128
Preserve Table Casing	True
Generate prompt prog	Yes
LIKE escape character	None
Enable Integrated Secu	False True False
External Usage	
Display	
Insert	True

Enable Integrated Security

Enabling Integrated Security imports GeneXus Access Manager (GAM) components to the Knowledge Base, providing authentication and security to your applications.

You will be able to manage users, roles and permissions to control access to your application (authentication), and to grant access permissions to your programs (authorization).

Please select the additional objects you want to import and how to manage their future upgrades.

Security objects: Login, Not Authorized, Change Password, Register, etc.

☑ Web Panels

☑ Panels

Select how to manage the future upgrades:

Install updates automatically

Do you want to Enable Integrated Security?

GAM Database

Confirm

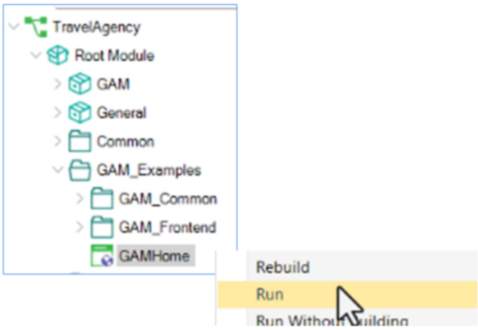
GAM database not found. Would you like to create it?

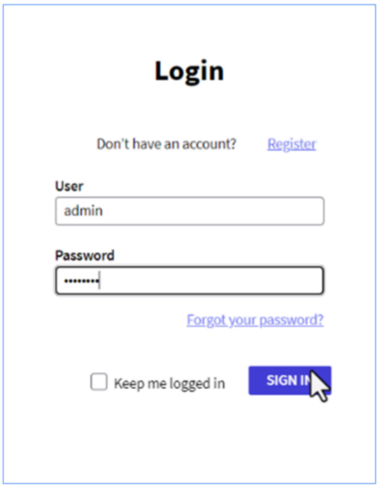
Now we will apply the security module to our Travel Agency KB to demonstrate this. To do so, first we select the active version of the KB. Next, we change the "Enable Integrated Security" property to true. A screen will be displayed requesting permission to import components for managing the GAM module, both for our web application and for Smart devices.

Likewise, we can choose the way to update these objects, either automatically or by asking us, or to never update them. We select “yes” and the objects will be imported into the "GAM Example" and "GAM Library" folders below "Root Module".

At a general level, we will change the security level to "none" so that any user can view our application. Then, in the version properties, we change a property called "Integrated Security Level". After that, we can change this same property at the object level. For example, in the "Attraction" transaction, we change "Integrated Security Level" to "Authorization" so that only authorized users can access it.

Remember that once GAM is applied, we need to rebuild the KB. This will prompt us to create the GAM database. Once this is done, we will find a new Data Store specifically for GAM.





Login

Don't have an account? Register

User

admin

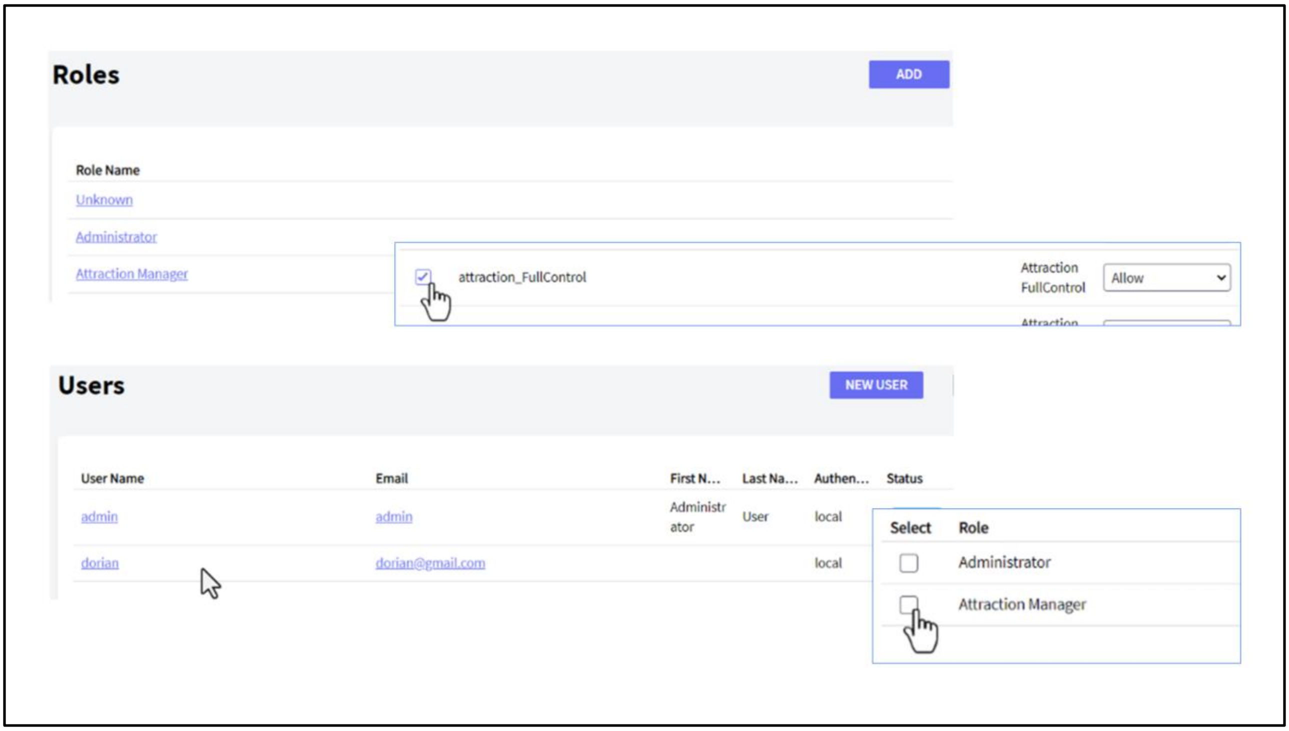
Password

••••••••

Forgot your password?

□ Keep me logged in

We run the "GAM Home" panel and go to the GAM backend, which is its administration console, to be able to add our users and give them permissions through their assigned roles. We log in using the default user (admin) and its password "admin123", keeping in mind that we can change it later.



Role Name
Unknown
Administrator
Attraction Manager

☑ attraction_FullControl — Attraction FullControl: Allow

User Name	Email	First N...	Last Na...	Authen...	Status
admin	admin	Administrator	User	local	
dorian	dorian@gmail.com			local	

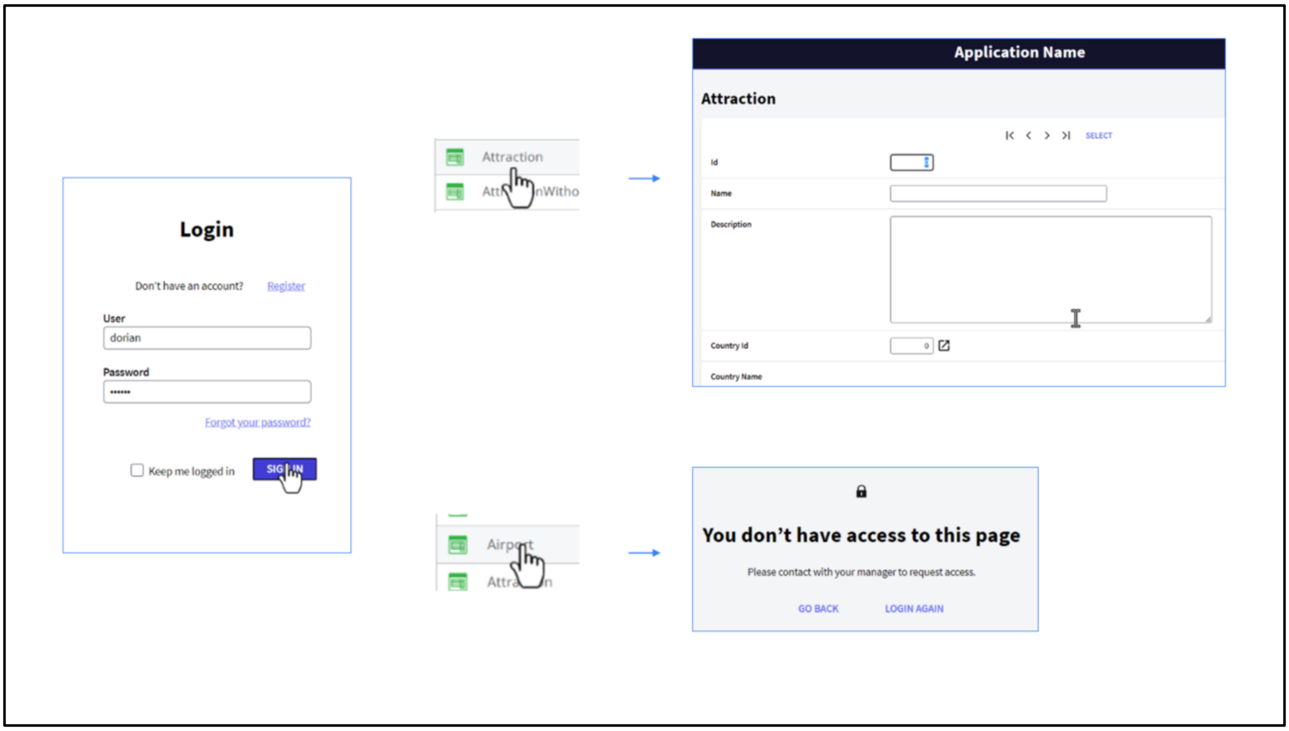
Select	Role
□	Administrator
□	Attraction Manager

We open the administration console, go to "Roles", and add the "Attraction Manager" role that will have permissions to insert, update, or delete an attraction. To do this, we click on the "Add" option, enter the name, and specify the security policy; for now it is enough to leave the default option. We confirm.

Then, we access our role and select "More Options", "Permissions". In this screen, we select the "Travel Agency" application and the "Add" option. In the following screen, the permissions that we can apply to this object are displayed. We select "attraction_Full Control", since this role will be able to perform all these tasks. We click on "Add Selected" and save.

In this way, we have configured our role. Now we need to add a user to have this role assigned to him/her. To do so, we go to the "Users" option and to the "New User" option. We will see that some fields have an asterisk, which indicates that they are mandatory.

We add the user "Dorian" with an email and a password, and add his security policy. We confirm, access the newly created user, "Dorian", and assign him a role. We add a role, indicate that it is "Attraction Manager", and add it with "add selected". Finally, we go back and see that the user already has this new role assigned.



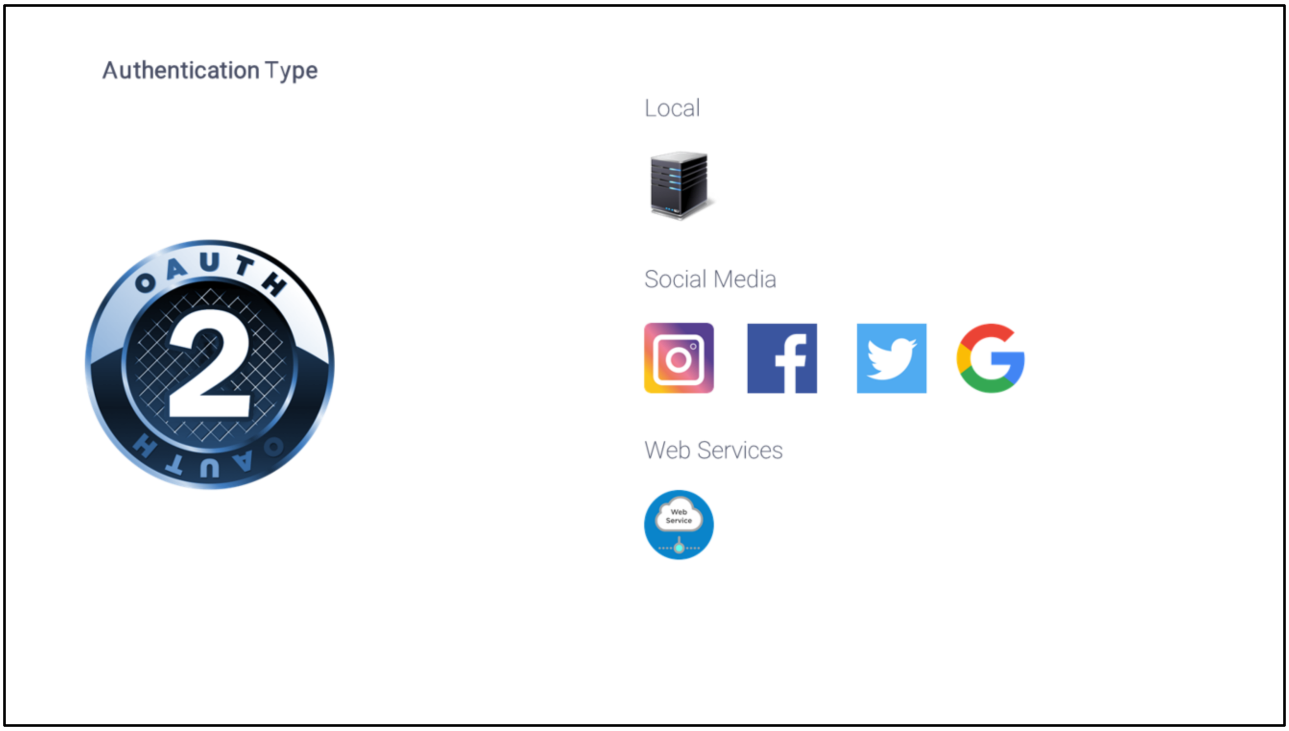
You don't have access to this page

Please contact with your manager to request access.

Now let's go to our backoffice application again, where we manage a travel agency.

When we run the application, from the Launchpad we select the Attraction transaction; it will ask for the access credentials, so we log in with the user Dorian, and access without problems. With the required permissions we can also enter, update, or delete these attractions.

If we go to the Airport transaction and set authorization as security—just like we did with Attraction—and try to enter Airport from the Launchpad, we will be told we are not authorized, since we only gave permissions to access the attractions.



Authentication Type

Local

Social Media

Web Services

We’ve seen how GeneXus allows managing application authentication and authorization. So far, we have only used local user authentication, but we can use other types of authentication, such as Facebook, Twitter, Google or some other external service.

Note that the current version of GeneXus can authenticate with any provider that uses OAuth 2.0. OAuth is a standard for granting access to websites or applications from another website, but without granting passwords.

One of its advantages is that it verifies the user's identity and issues a token for the application to grant access, which makes our application authentication much more secure.

wiki.genexus.com

To learn more about the GeneXus Access Manager, visit our wiki.