Security with GeneXus Access Manager

In general, applications imply restricted usage for duly authorized users. This calls for some type of login aspect for verifying user authentication and for the occasional authorization or restriction of use for specific functionalities, depending on the user profile.

To fulfill such requirements, GeneXus provides a security model called GeneXus Access Manager (GAM) that solves authentication and authorization functionalities for both web applications and smart device applications.

This module is made available with all its security controls by simply configuring the "Enable Integrated Security" property -in the Preferences window of our knowledge base, at the active version level- with True value.



) 🕑 🖉 🕲 😁

This will cause the import of the GeneXus Access Manager to be integrated in our application, thus allowing us to solve the security issue. This will also imply the addition, to our KB, of two folders under the Root Module that contain several objects.

GeneXus

nable Integrated Security	?	×
Enabling Integrated Security imports GeneXus Access N to the Knowledge Base, providing authentication and se		
You will be able to manage users, roles and permissions application (authentication), and to grant access permiss		zation).
Please select the additional objects you want to import a future upgrades.	nd how to manage their	
Additional Components		
Web backend panels and Web security objects. If y a new theme will be imported also.	you select this option,	
Smart Devices security panels		
Select how to manage the future upgrades:		
Prompt me to update \checkmark		
Do you want to Enable Integrated Security?		
	Yes	No

3000000

Once our security is enabled, we may select whether all we want is just Authentication or if we prefer Authentication and Authorization. This is done by setting up the **Integrated Security Level** property.

		GeneXus
Properties	# X	
}≣ A2 Filter	×	
 Version: Travel_Agency 		
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	
V Integrated Security		
Integrated Security Level	Authentication 🗸	
Application ID	None	
> Web specific	Authentication	
> SmartDevices specific	Authorization	
> External Usage		
> Compatibility		

000000

Something important to bear in mind is that when we enable the GAM we must then execute the **Rebuild all** action in the KB. This is meant to create the database that the GAM will use.

Once the GAM is applied, when we execute the application, the first thing displayed will be a login object. This is valid for both web applications and smart device applications.

GeneXus



000000

Only local authentication will be enabled by default, where we may access with the user: "admin" and the password: "admin123". But we may also define other authentication types such as Facebook, Twitter or an external service like, for example, a web service.

In order to access the Backend in runtime we must execute –from the Developer Menu- the GAMHome that is the main object of the GAM's backend. Through this backend we may set up users and different permits on our application's objects.

				GeneXu
GENEXUS ACCESS MANAGER	US	ERS ROLES SETTINGS+	ŝ.	A <u>Administrat</u>
SHOW FILTERS Users	Q Try a Se	arch	+ A	DD
User Name admin	First Name Administrator	Last Name User	Authentication	EDIT
		FIRST/ PREV/ NEXT		

The GeneXus Access Manager allows the implementation of secure applications, as it provides us with a fully integrated solution for solving the Authentication and Authorization of our web and smart device applications. To learn more on how to use GAM in GeneXus go to the following wiki link:

GeneXus

http://wiki.genexus.com/commwiki/servlet/wiki?24746,Toc%3AGeneXus+Access +Manager+%28GAM%29,

