

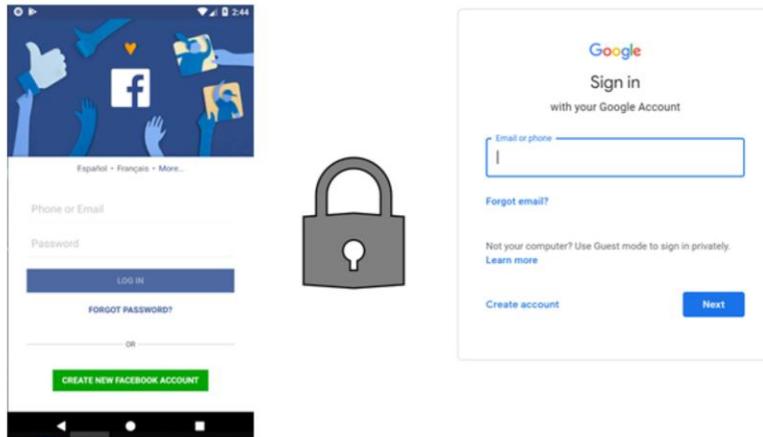
GeneXus[™]
The power of doing.

GeneXus Access Manager - Introduction

Security

GeneXus 16

Security



Como sabemos, a grande maioria das aplicações modernas exige um esquema de segurança, de modo que apenas usuários autorizados possam entrar e também autorizar ou restringir o acesso a partes da aplicação, de acordo com as permissões atribuídas ao usuário.

GeneXus Access Manager - Introduction GeneXus

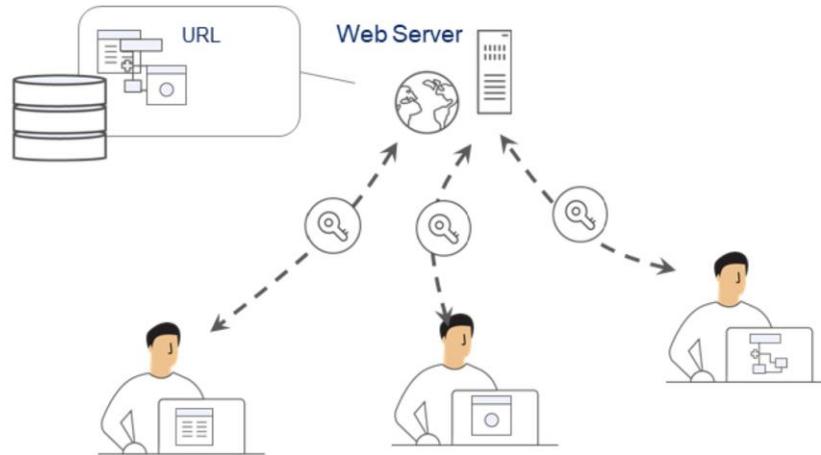
Security

APP	Permission name	Description	Permissions options
<input checked="" type="checkbox"/>	gamexamplechangerespository_Execute	Change Working Repository	Allow
<input type="checkbox"/>	gamexamplechangeyourpassword_Execute	Change Password	Allow
<input checked="" type="checkbox"/>	gamexamplewwwapplications_Execute	Application	Restricted
<input checked="" type="checkbox"/>	gamexamplewwwauthypes_Execute	Authentication Types	Deny
<input type="checkbox"/>	gamexamplewwwconnections_Execute	Connections	Allow

Authentication

Isso significa garantir que todos os usuários que entram sejam devidamente autenticados (isto é, que o usuário é quem eles dizem que são); e autorizado (isto é, uma vez que o usuário é autenticado, o acesso a certas partes da aplicação é permitido ou não).

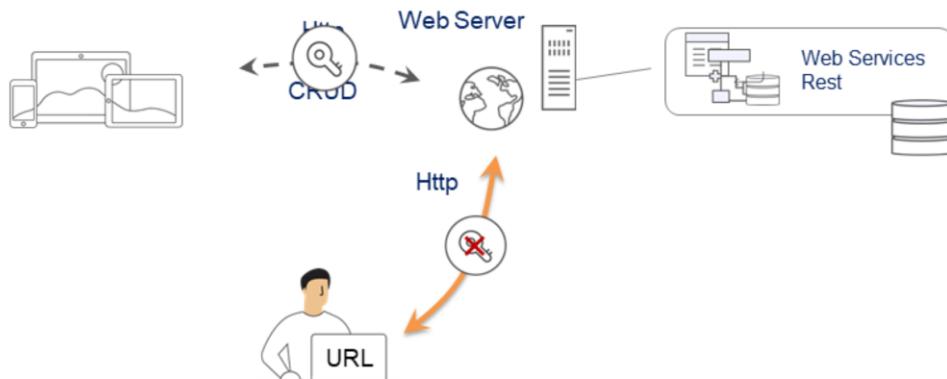
Security in Web Applications



No caso de aplicações Web, como essas aplicações têm vários pontos de entrada, qualquer objeto acessível por URL deve verificar as permissões de autenticação.

Isso implica que cada um desses objetos deve ter a verificação de segurança incorporada para realizar o controle correspondente.

Security in Smart Devices Applications



No caso de aplicativos para Smart Devices, sendo aplicativos distribuídos, uma parte deles é executada no próprio dispositivo e a camada de negócios do aplicativo é conectada por meio de serviços Rest que têm um URL de acesso, de modo que estão expostos a acessos indesejados.

No caso das aplicações web, o que é feito é verificar se apenas usuários devidamente autenticados e autorizados podem acessar a aplicação, evitando a execução de usuários que não tem permissão.

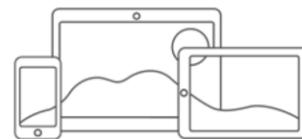
Integrated Security Solution


GeneXus Access Manager



Authentication

Authorization



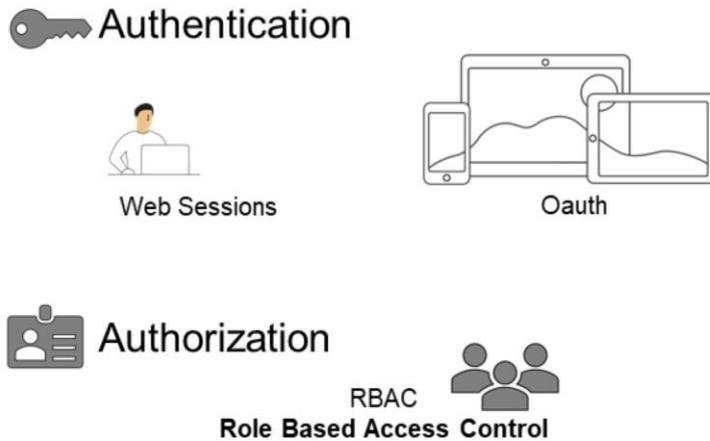
Para atender a essas necessidades, o GeneXus oferece um módulo de segurança, chamado GeneXus Access Manager (GAM), que resolve as funcionalidades de autenticação e autorização, tanto para aplicações Web quanto para dispositivos inteligentes.

O GAM é desenvolvido em GeneXus para que seja facilmente integrado à KB da aplicação e permita resolver de forma centralizada tudo relacionado à Segurança do mesmo. O objetivo é que a solução de segurança seja usada da forma mais declarativa possível no aplicativo, sem criar complexidade adicional.

O GAM também oferece um back-end que permite definir usuários, permissões, políticas de segurança e acesso a objetos, entre outras coisas.

Ele também fornece uma API para acessar muitos desses recursos via código.

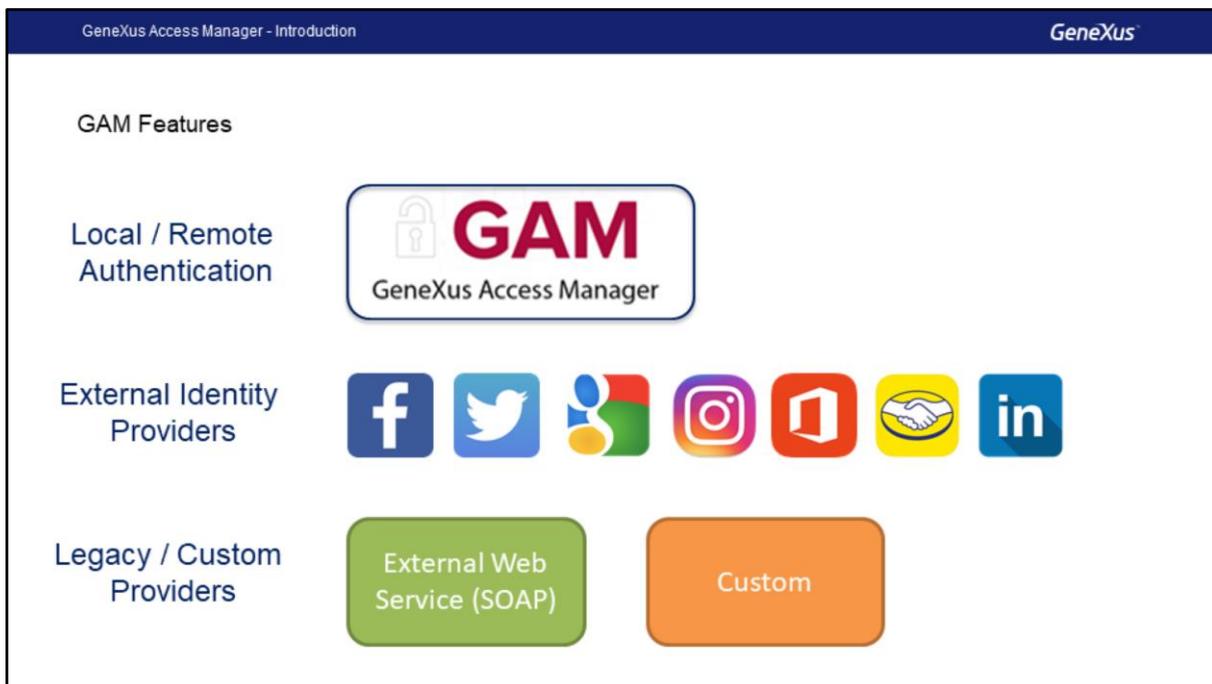
GAM Features



Para resolver a autenticação, internamente é usado:

- **Web sessions** para a segurança de aplicações Web
- **Oauth** para resolver a segurança no caso de aplicativos para SD

No caso de Autorização, sua implementação é baseada em Roles usando o modelo **Role Based Access Control**, onde são encapsulados os métodos, propriedades e tudo o que é necessário para o gerenciamento de autorização na aplicação.



O GAM fornece diferentes tipos de autenticação, os tipos disponíveis são:

Autenticação local usando o GAM onde os usuários e todas as suas credenciais são armazenados em um banco de dados do qual somos proprietários ou remotamente, já que um aplicativo que usa o GAM pode ser um provedor de identidades e, nesse caso, outros aplicativos com GAM podem se conectar remotamente a esse servidor e obter autenticação a partir dele.

Também podemos usar outros provedores externos de identidade, eles fornecem autenticação baseada no protocolo **Oauth 2.0** como **Facebook, Twitter e Google, Instagram, Office 365, Mercado Livre ou LinkedIn**, aqui usamos os mecanismos de autenticação padrão baseados neste protocolo implementado para essas aplicações. Neste caso, não há necessidade de definir usuários locais.

Em muitos casos é necessário integrar nosso aplicativo com outros com os quais temos que trocar informações e é necessário garantir a autenticação dos usuários através de autenticação externa do aplicativo.

Uma forma de autenticação externa é usar um **web service SOAP** fornecido pela outro aplicativo e configurar o GAM para consumir esse web service.

Pode ser possível que o outro aplicativo forneça um programa externo para controlar a autenticação, mas isso não é necessariamente um web service. Neste caso, configuro o GAM para aceitar uma autenticação do tipo Custom.

GeneXus Access Manager - Introduction GeneXus

GAM Features

The screenshot displays the GeneXus Access Manager interface. At the top, it says 'GeneXus Access Manager - Introduction' and 'GeneXus'. The main content is titled 'GAM Features'. On the left, there is a small icon of a person at a computer. The central part shows a table of permissions:

Permission name	Description	Permissions options	Inherited
gamexamplechangeyourpassword_Execute	Change Password	Allow	DELETE
gamexamplewapplications_Execute	Application	Allow	DELETE
gamexamplewauthypes_Execute	Authentication Types	Restricted	DELETE

Below the permissions table is a 'Speakers' section with a search bar and a table of speakers:

Id	Full Name	Image	Company Name	Country Id	Country
12	García, Alejandro		GeneXus	5	Uruguay
15	Cerdas, Amanda		Century 21 Knowledge Proq.	5	Uruguay
23	Bachmann, Armin		GeneXus	5	Uruguay
2	Gorda, Breggan		GeneXus	5	Uruguay

To the right of the speakers table is a 'Speaker' profile form for Armin Bachmann, with fields for Name, Surname, Full Name, Image, and CVMini. Below the form is a bio: 'Mr. Bachmann is a graduate of Computer Science Engineering from the School of Engineering of the University of the Republic of Uruguay, and member of GeneXus support team since 1999.'

On the far right, there is a mobile app interface titled 'Work With Speaker' showing a list of speakers and a detailed profile for Armin Bachmann with a photo and bio.

Com a Autorização, definimos as permissões de execução dos objetos e as permissões nos modos de operação das transações.

A definição é feita para cada objeto, dando permissões para cada função e, dependendo da função que o usuário atribuiu, serão as permissões efetivas no objeto.

Essa validação é feita nos seguintes objetos da Web:

- Web Panels
- Web Components com a propriedade URL Access=Yes
- Transações

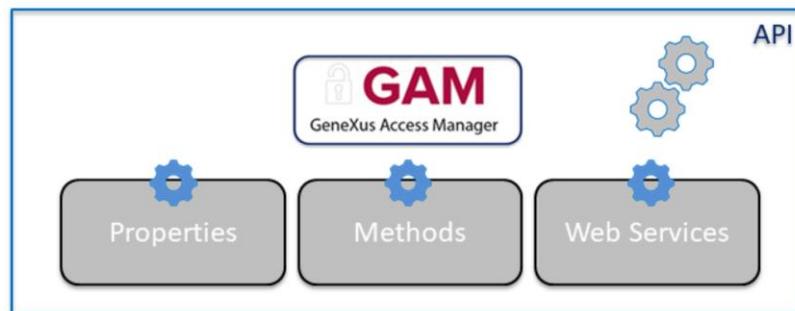
Além disso, são verificadas as permissões nos modos Insert, Update, Delete e Display das transações Web.

E para Smart Devices, nos objetos:

- Work With for Smart Devices
- Panels for Smart Devices.

E as ações de Insert, Update e Delete no Work With for Smart Devices.

GAM Features



O GAM também expõe uma API (Application Program Interface) para acessar suas propriedades e métodos, caso seja necessário fazê-lo a partir de nosso aplicativo e uma série de serviços da Web que podem ser usados por outros aplicativos. Vamos ver isso no nível avançado.

Enable Integrated Security



The screenshot shows the GeneXus IDE interface. On the left, the 'KB Explorer' tree is expanded to show the 'EventDay' module. The 'EventDay_Version16' node is selected. On the right, the 'Properties' window is open, showing the configuration for the selected version. The 'Enable Integrated Security' property is set to 'True'.

Property	Value
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

Para ativar o GAM, você deve ir até o nível da versão ativa da KB e configurar a propriedade **Enable Integrated Security** como True.

Na versão Trial, ele está localizado no primeiro nó do KB Explorer com o nome da KB.

GeneXus Access Manager - Introduction GeneXus

Integrated Security Level

The screenshot displays the GeneXus Access Manager interface. On the left, a tree view shows the project structure under 'EventDay_Version16', including 'Net Environment', 'Generators', and 'DataStores'. Below it, the 'KB Explorer' shows a tree view with 'EventDay', 'Root Module', 'Components', 'Data', 'DP', 'GeneXus', and 'Panels'. The 'Company' object is selected under 'Transactions'. In the center, a configuration table shows the 'Integrated Security Level' set to 'Authentication'. On the right, the 'Properties' window shows the 'Company' object's details, with the 'Integrated Security Level' also set to 'Authentication'.

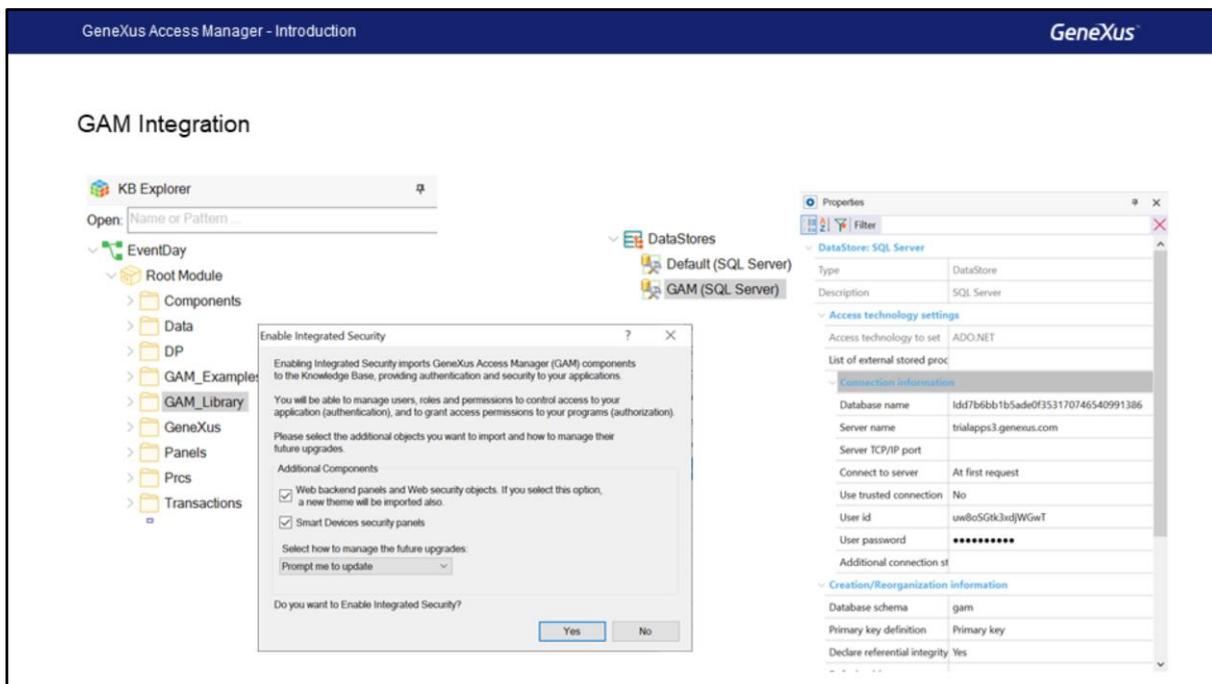
Properties	
BusinessComponent: Company	
Name	Company
Description	Company
Module/Folder	Transactions
Business Component	True
Qualified Name	Company
Object Visibility	Public
Integrated Security	
Integrated Security Level	Authentication
Network	None
Connectivity Support	Authentication
Business Component	Authorization

Depois de ativarmos o GAM, veremos outra propriedade chamada **Integrated Security Level**, que permite indicar o valor padrão da segurança dos objetos da KB.

Essa propriedade também está no nível do objeto, portanto, será possível personalizar a maneira como a segurança será implementada nesse objeto.

Existem três valores possíveis:

- **None:** indica que o objeto será público, isto é, não terá segurança.
- **Authentication:** indica que somente usuários autenticados podem executá-lo..
- **Authorization:** indica que o usuário, além de ter se autenticado, terá que ser autorizado a executar o respectivo objeto, ou seja, ter o papel apropriado para executá-lo.



Quando tivermos as propriedades de segurança configuradas, serão importados automaticamente os objetos do GAM no KB e, em seguida, teremos que fazer um Rebuild All da KB.

Ao fazer isso, uma caixa de diálogo será aberta informando que o módulo GAM será instalado em nosso banco de dados, com a solução pronta para Web e Smart Devices.

O GAM também está preparado para rodar em um banco de dados independente do banco de dados do aplicativo, se desejarmos. Não devemos nos preocupar com essa estrutura nesse caso, porque ela possui seu próprio Schema e será associada a um Data Store Independente na KB, com o qual toda a configuração é independente. Além disso, o GAM será responsável pela inicialização e manter o banco de dados inteiro atualizado.

DEMO: Integrate GAM into Knowledge Base

Em seguida vamos no GeneXus e vamos utilizar o GAM.

GeneXus™

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