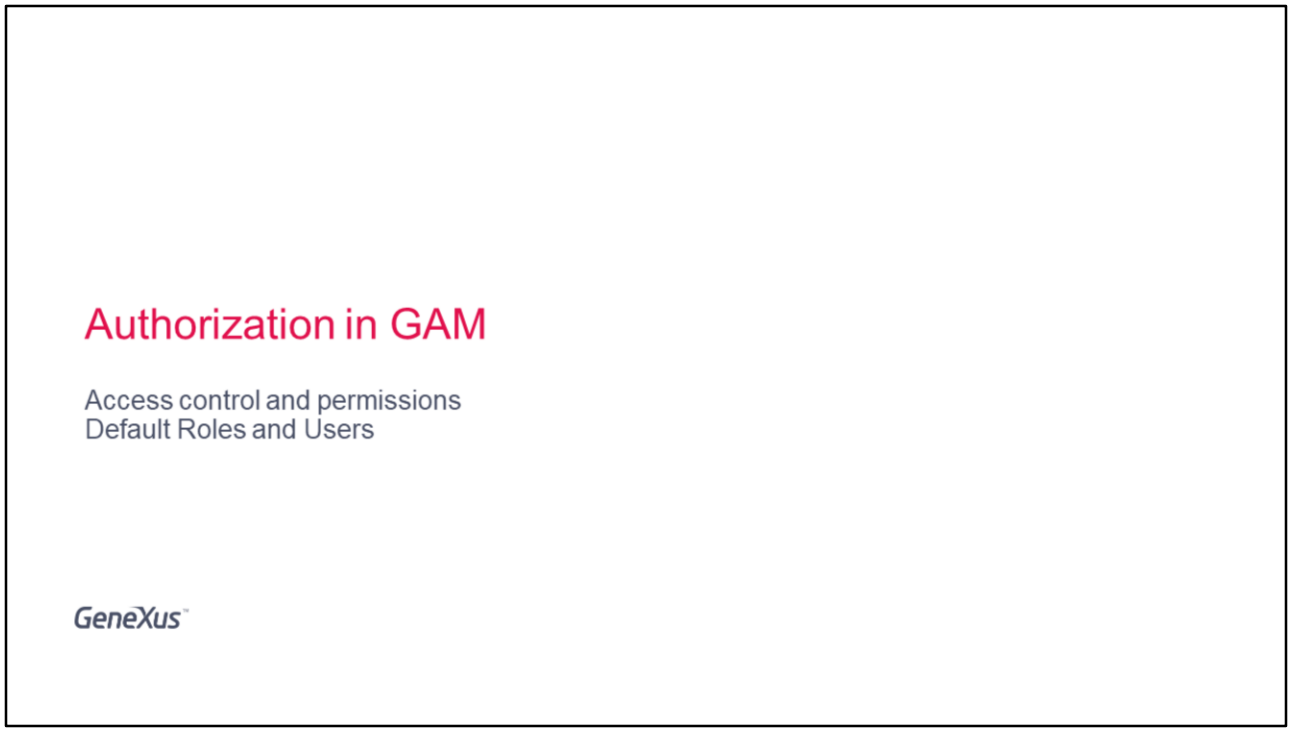

GeneXus™
by Globant

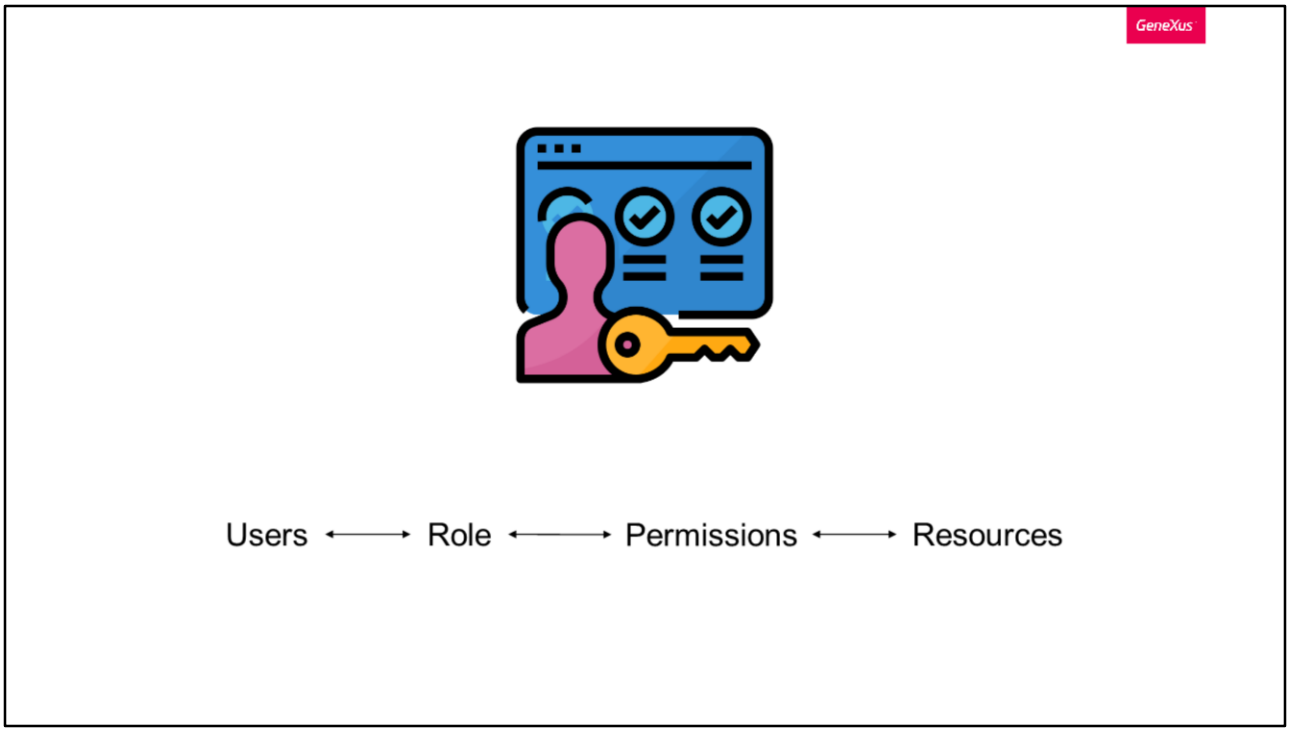
Authorization

Nicolas Adrién

GeneXus



Neste vídeo trataremos os temas relacionados à Autorização no GAM. Controle de acesso e permissões, bem como roles e usuários padrão.

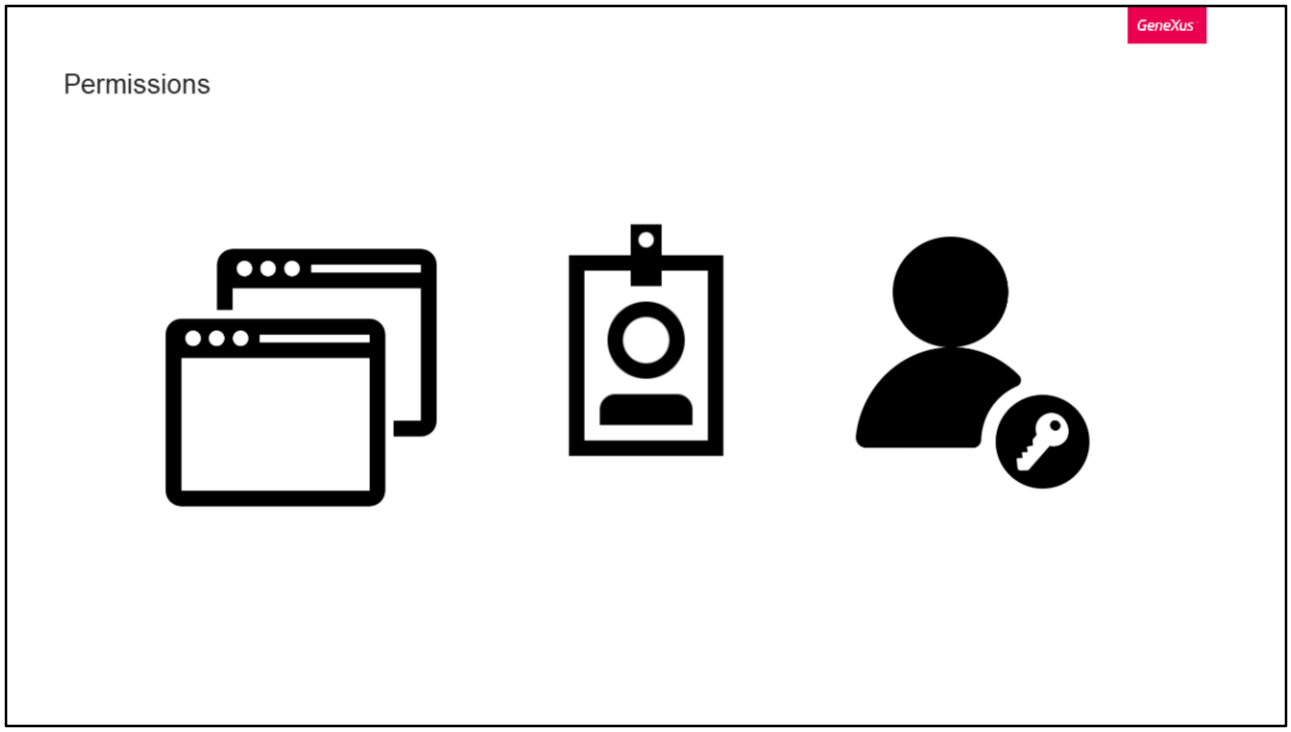


Além da Autenticação, conforme mencionado no curso introdutório, temos o conceito de Autorização.
A autorização é o processo de verificar se um usuário que já foi autenticado possui as permissões necessárias para realizar uma ou mais ações no sistema.

Para isto, como comentamos em vídeos anteriores, o GAM possui um esquema baseado em Roles de Usuário, onde cada usuário tem associada uma ou várias Roles. Também existem os Recursos assegurados e a atribuição de Permissões sobre estes Recursos às Roles.

Os recursos podem ser, por exemplo:

- Web Panels ou painéis Móveis
- Work With para dispositivos móveis.
- Web Components com Acesso por URL habilitado
- Transações WEB
- Entre outros

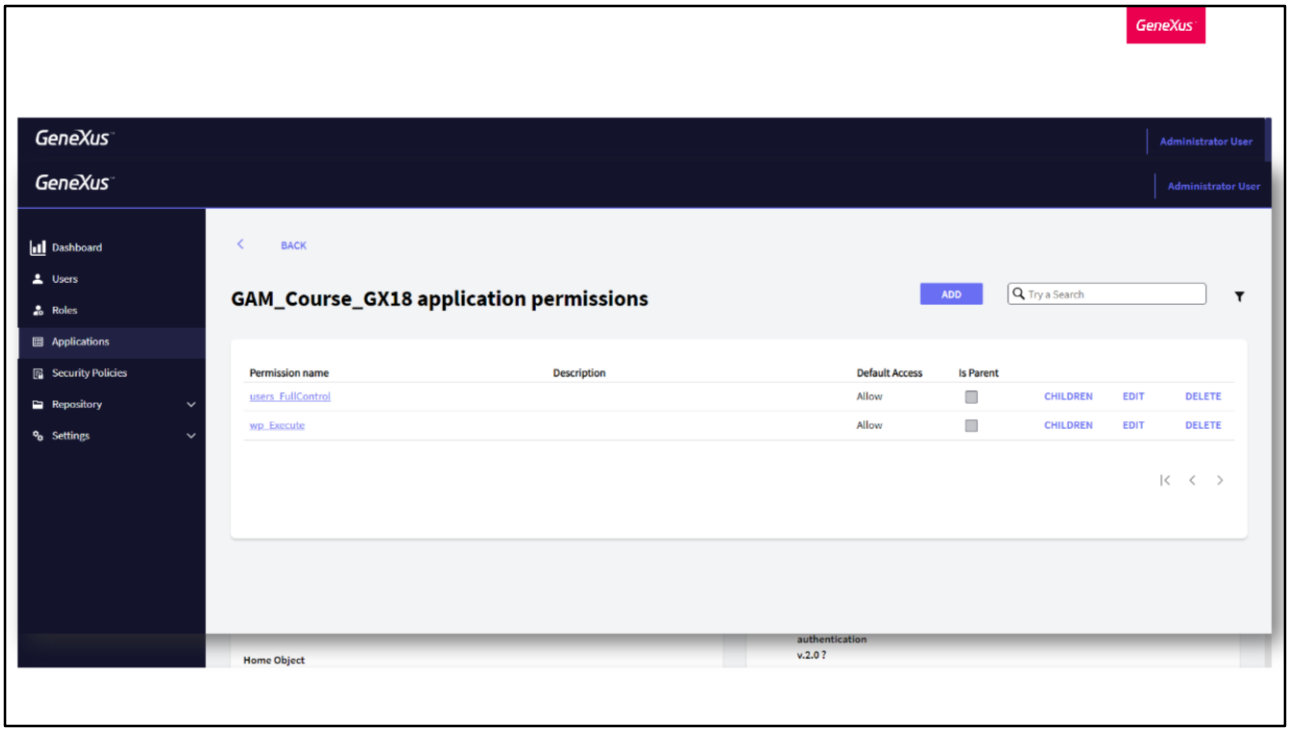


As permissões utilizadas para a autorização podem ser atribuídas em diferentes níveis:

Nível de aplicação: Cada uma das Permissões tem um Tipo de Acesso definido no nível de Aplicação GAM, onde é definido um Tipo de Acesso Predeterminado para cada permissão.

Nível de role: Quando são atribuídas Permissões a Roles, são definidas com um Tipo de Acesso.

E, finalmente, Nível de usuário, que é quando as Permissões são atribuídas aos Usuários e são definidas com um Tipo de acesso, assim como a nível de role.

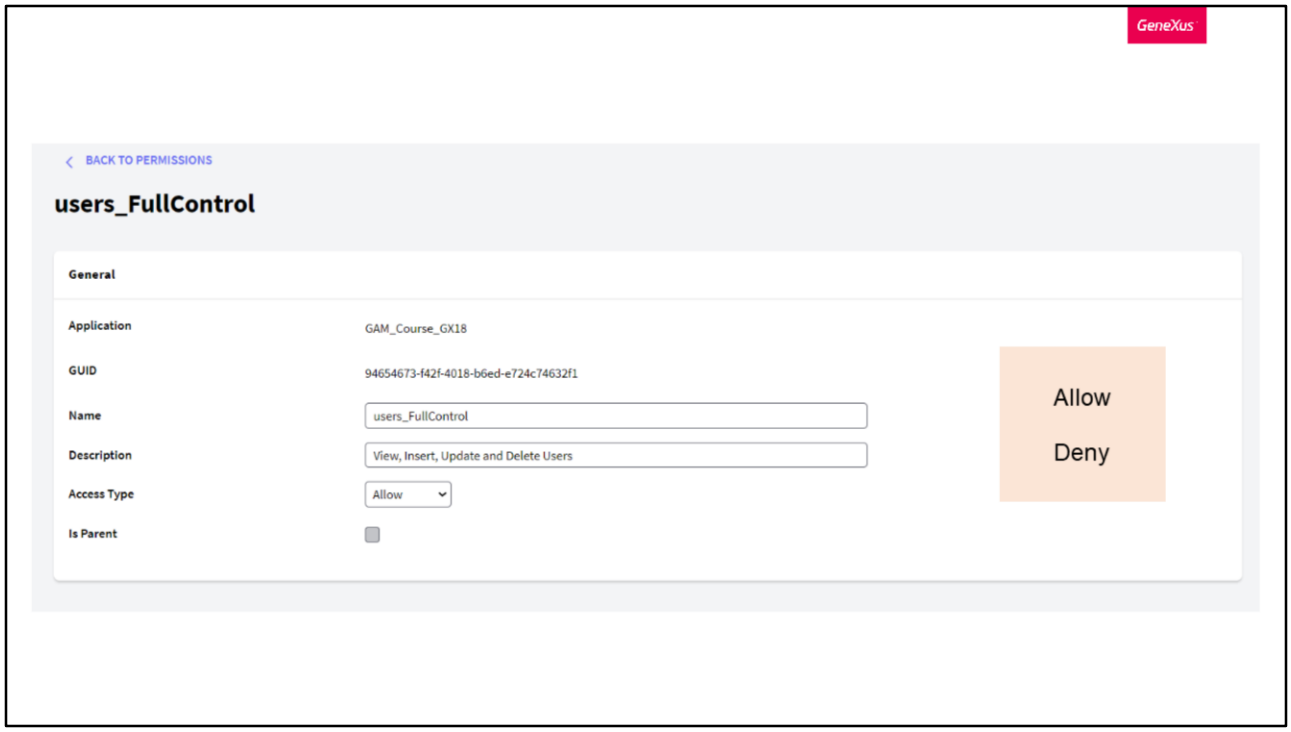


No nível de Aplicação, GAM fornece a facilidade de que a cada aplicação irá gerar automaticamente as permissões.

Para acessar essas permissões, basta acessar a Aplicação em questão no Back-end e clicar em Permissões, dentro do submenu “Mais opções”.

Uma vez lá, encontraremos todas as permissões que GeneXus se encarregou de gerar por nós, as quais são compostas por um nome, descrição, acesso padrão e se é pai ou não de outra permissão.

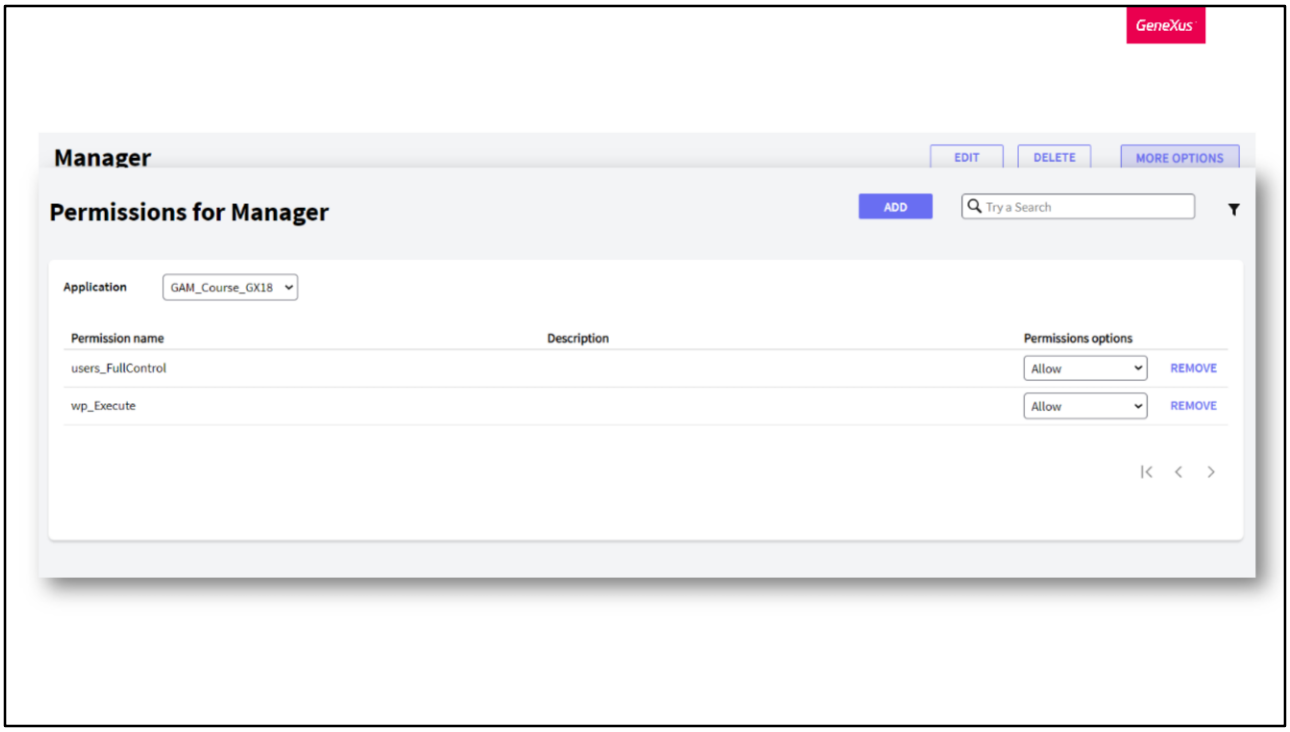
Para este exemplo que vemos em tela, temos uma permissão de execução (por isso termina em Execute) e outra de controle total, mas também podem ser geradas para os modos de Insert, Update e Delete. A permissão de controle total representa a obtenção das permissões mencionadas anteriormente.



No caso de querer editar uma permissão, as opções disponíveis são poder alterar o nome, a descrição e o tipo de acesso.

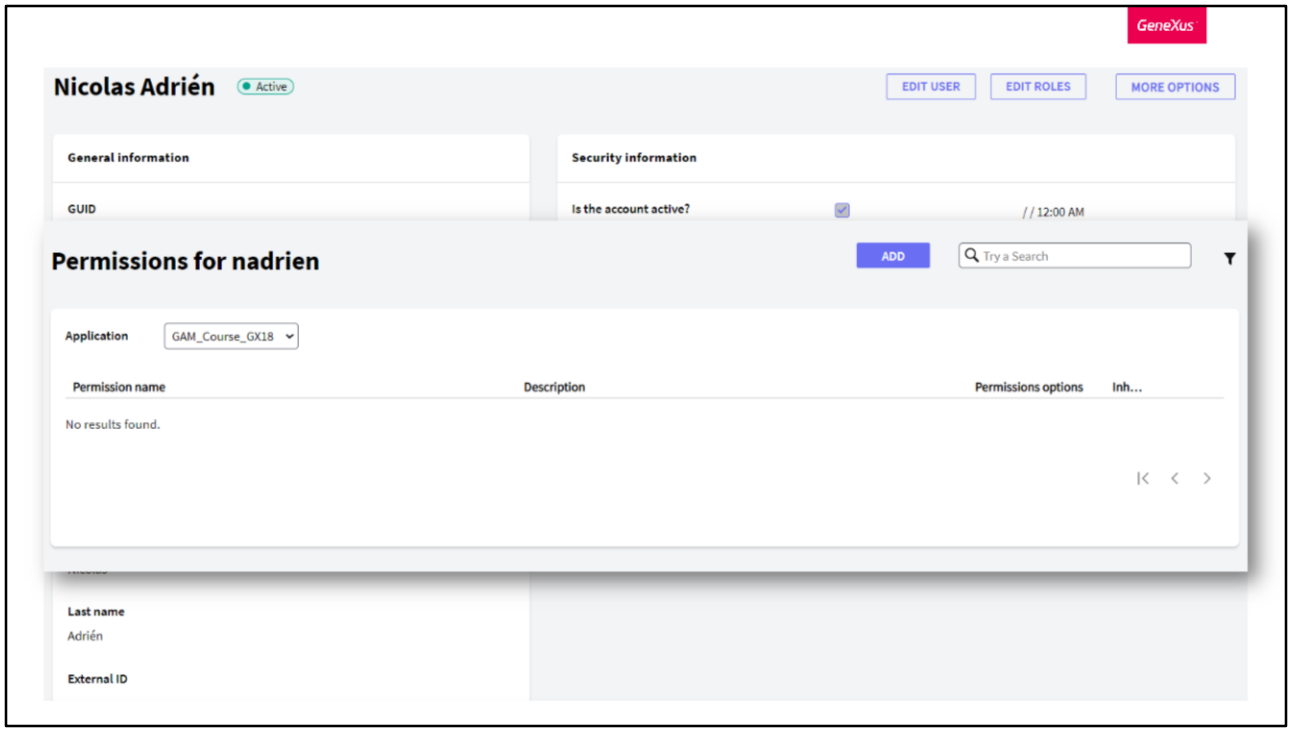
O tipo de acesso de uma permissão define seu uso predeterminado (se é algo público ou restrito). As opções disponíveis são:

- Permitir: Este tipo de acesso habilita a permissão para todos os usuários por padrão. Os usuários que tenham esta permissão concedida com: Tipo de acesso = restrito ou negado, ou que tenham alguma role em que a permissão esteja restrita ou negada, não terão esta permissão.
- Restrito: Os usuários não têm esta permissão por padrão, o que significa que apenas os usuários que têm esta permissão concedida com Tipo de Acesso = Permitir ou têm alguma role em que é permitida esta permissão, têm os direitos correspondentes.



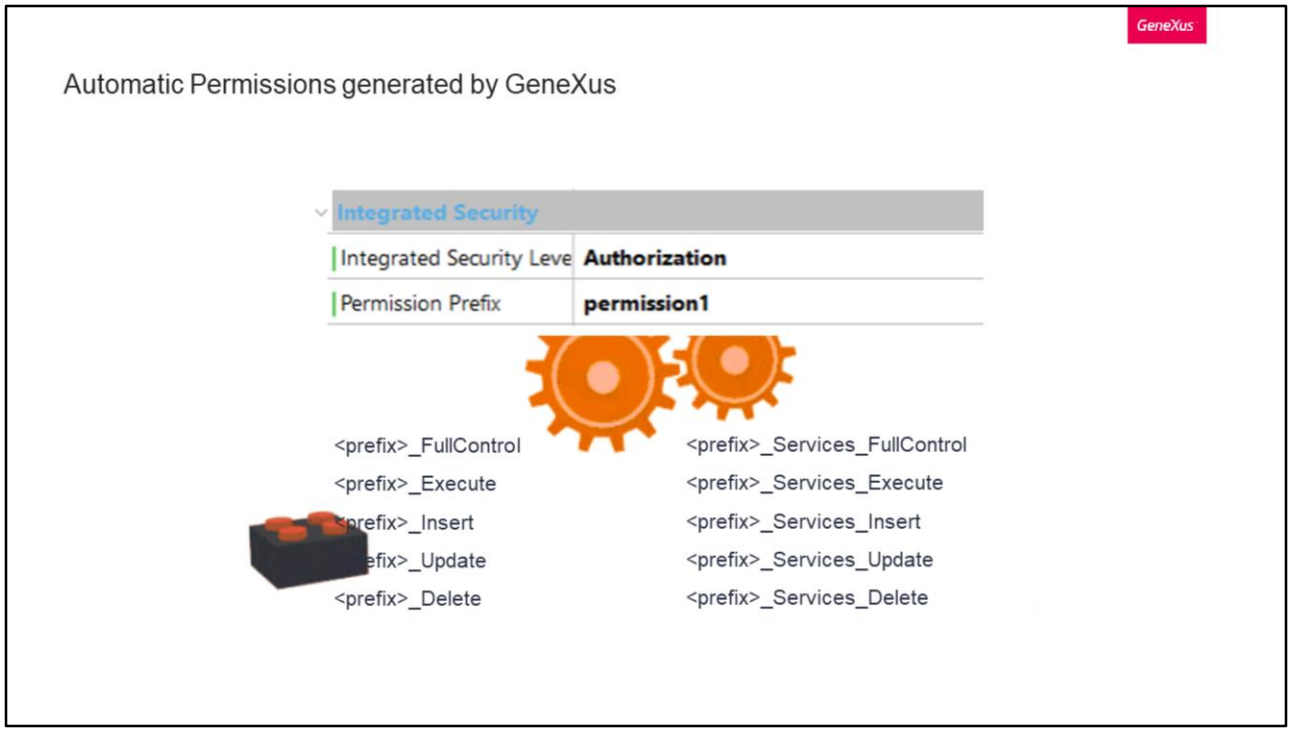
No nível de Role, para adicionar, editar ou excluir permissões, devemos ir para a opção Roles e dentro de uma role podemos gerenciar suas permissões através do submenu "Mais opções".
Como vemos na imagem, GAM nos dá a possibilidade de Adicionar ou Excluir uma permissão, modificar seu nível como dissemos antes (com as opções Permitir, Restrito e Negado) e marcá-la como herdada ou não.

Algo a destacar sobre isto é que se adicionarmos uma permissão a uma role, por transitividade esta permissão também será concedida a todos os usuários que tenham essa role.



Finalmente, o último nível é por Usuários.
Assim como por Roles, primeiro é acessado o Usuário e depois ao editá-lo, temos a opção de editar permissões dentro do submenu “Mais opções”.

Aqui são tratados exatamente da mesma forma que por Roles, como acabou de ser mencionado.
Um detalhe a destacar é que as permissões concedidas neste nível prevalecem sobre as permissões concedidas no nível de role, sem importar o tipo de acesso que se tenha, o nível de Usuário sempre vencerá.



Muitas das permissões vistas nas imagens anteriores correspondiam a permissões automáticas geradas por GeneXus.

Ao realizar Build, estas permissões são geradas e então são verificadas em tempo de execução.

Isto, supondo que se tem a propriedade Nível de segurança integrada definida com o valor Autorização, é claro.

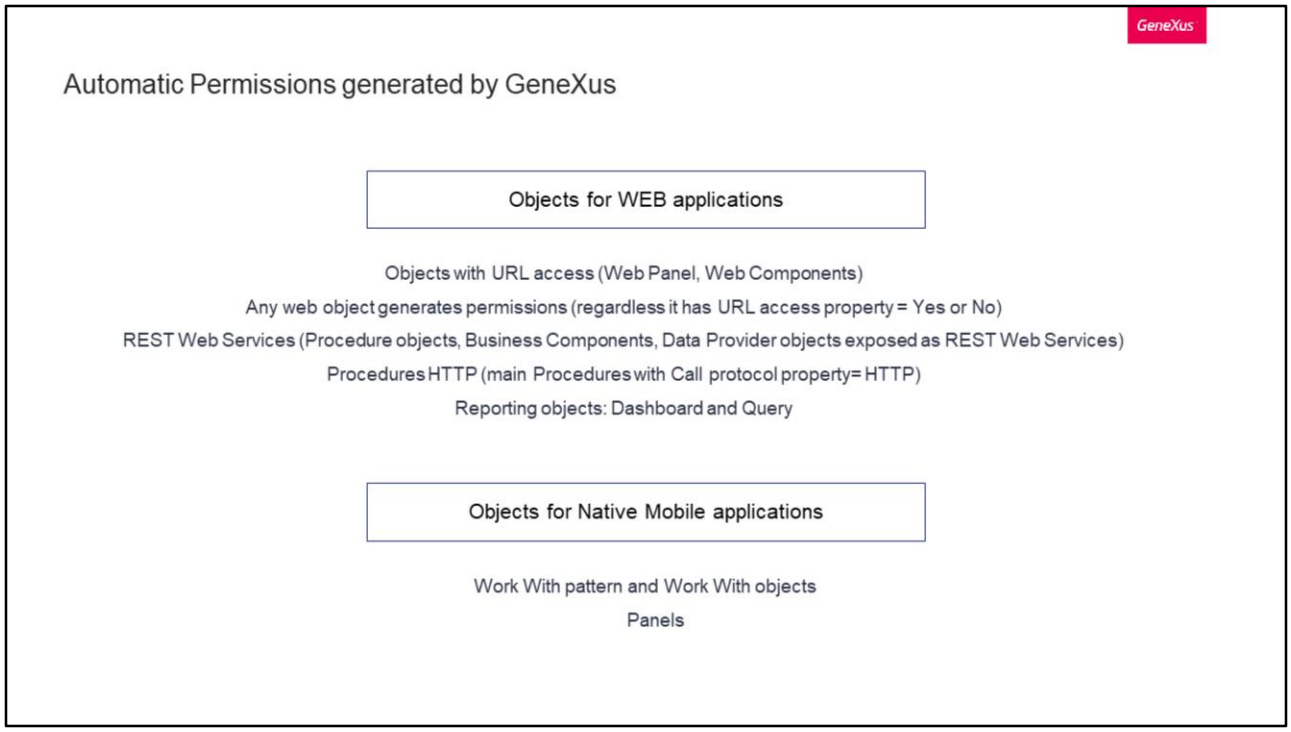
O código para verificar estas permissões é incluído no código gerado, e o usuário apenas declara (através da propriedade Permission Prefix) qual é a permissão que será verificada. Algo positivo a destacar sobre isto é que, como pode ser visto, nada precisa ser programado, basta declarar as permissões necessárias para executar o objeto.

As permissões automáticas podem ser descritas da seguinte forma:
Em primeiro lugar temos as Permissões de execução onde cada objeto da KB (exceto o Menu) expõe uma permissão de acesso. Mais adiante entraremos em detalhes sobre quais são os objetos que expõem as permissões.

Em segundo lugar, temos as Permissões para a execução das diferentes modalidades de uma transação.

Quando é especificado um prefixo de permissão em qualquer transação web (suponhamos que seja "prefix"), é criado um conjunto de permissões no Repositório GAM, nomeado da seguinte forma:
prefix.FullControl é o pai do restante das permissões e a representação de cada permissão é dada pela ação concatenada ao prefixo.

Em terceiro lugar temos as Permissões de Serviços.
Se "prefix" for o prefixo de permissão de um componente de negócios exposto como REST, as seguintes permissões são geradas automaticamente.



Na placa anterior, dissemos que cada objeto da KB (exceto o Menu) expõe uma permissão de acesso. Vamos ver quais são estes objetos.

Para aplicações web temos:

- Objetos web com acesso por URL, como os Web Panel e Web Components
- A partir de GeneXus Evolution 3, qualquer objeto web gera permissões, independentemente de possuir propriedade de acesso URL com valor Sim ou Não
- Serviços web REST, como procedimentos, Business Components ou Data Providers de dados expostos como serviços web REST
- Procedimentos HTTP, que são Main com propriedade de protocolo de chamada com valor HTTP

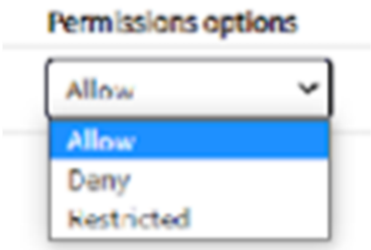
E finalmente,

- Objetos de informes, como Dashboard e Querys

Para aplicações móveis nativas, temos Work With pattern e Work With objects, e também os Painéis.

GeneXus

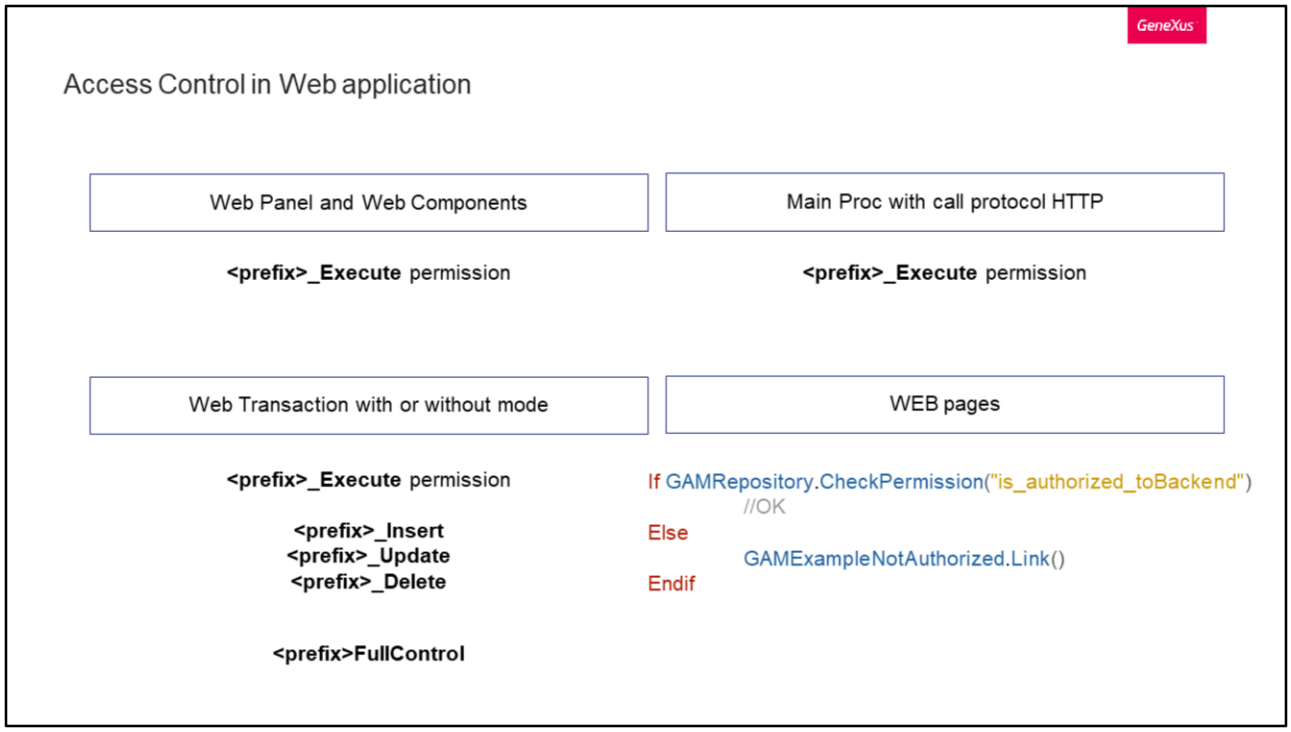
Permission denial



GAM permite especificar negação de permissões. Ou seja, indicar que uma permissão não pode ser utilizada em uma sessão cujo usuário tenha a referida role.
Já vimos a opção anteriormente onde tínhamos, além das opções de Permitir e Restringir, Negar.

Um usuário que tenha uma role com permissão de Tipo de acesso = Negar não terá esta permissão, independentemente de a permissão estar permitida no nível da aplicação (de forma predeterminada) ou se tiver outra role onde a permissão esteja permitida.

A única maneira em que é possível conceder esta permissão ao usuário é com Tipo de acesso = Permitir.



Vejamos cenários em que é realizado o controle de acesso.

Primeiro temos os Web Panel e Web Components (que só têm acesso a partir da url - URL access = true)
Neste caso, é validado se o usuário possui permissão para executar o objeto. No caso de não ter, não deve ver nenhum dado do formulário.
Para isto, GAM verifica se o usuário possui a permissão <prefix>_Execute, onde prefix é o Prefixo de permissão definido para o objeto.
No caso de ser detectado um erro de permissão, será realizado um redirecionamento automático para o Objeto de “Não Autorizado” para objetos web no caso de serem aplicações web.

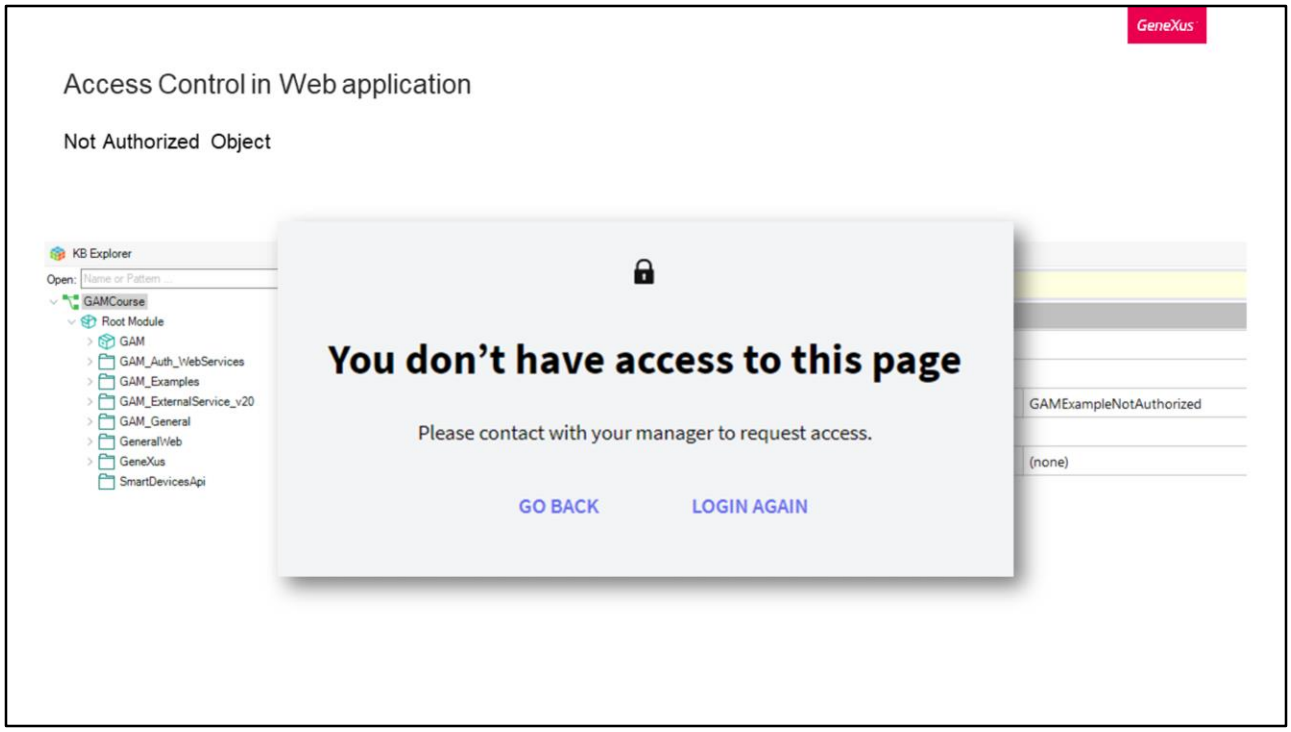
Depois temos o acesso a um processo principal com protocolo de chamada HTTP. Um exemplo disto pode ser um relatório em PDF que é exibido no navegador.
Aqui é validado se o usuário tem permissão para executar este objeto. GAM verifica se o usuário possui a permissão <prefix>_Execute, onde prefix é o Prefixo de permissão definido para o objeto.
Em caso de erro, será exibido o erro 401, lançado pelo servidor de aplicações que deve ser capturado pelo programador.
No caso de um relatório em PDF, é considerado o objeto “Não autorizado” para objetos Web.

Em terceiro lugar, temos o acesso a uma Transação web com ou sem modalidade.
Primeiro é validado se o usuário tem permissão para executar o objeto. Neste caso, GAM verifica se o usuário novamente possui a permissão <prefix>_Execute, onde o prefixo neste caso é o definido para a Transação. Esta permissão permite ao usuário exibir os dados da transação (somente em modo de visualização).
Se o usuário executa uma ação sobre a transação, seja Confirmar ou Excluir, serão necessárias outras permissões conforme vemos em tela.
De fato também temos a permissão que agrupa todas as permissões e também pode ser utilizada.
Em caso de erro, será exibida uma mensagem de erro de GeneXus se a Transação não recebe como parâmetros KEY e mode. Isto pode ser visto com mais detalhes na Wiki de GeneXus.

Finalmente temos o último ponto. Acesso restrito a um grupo de páginas WEB.
Existem alguns casos onde o nível de autorização necessário é apenas para permitir ou negar para um grupo de usuários o acesso a um conjunto de páginas web da aplicação.

Por exemplo, se dividirmos nossa aplicação nos módulos front-end e back-end, provavelmente apenas alguns usuários autorizados sejam os que podem acessar o back-end.
Uma maneira de fazer isto é usar uma Master Page para as páginas dele e programar o seguinte no evento de Start desta.
Além disso, deve ser definida a propriedade da aplicação “Exigir permissões de acesso” com valor verdadeiro.

A outra opção é definir as permissões automáticas como filhos dessa permissão "is_authorized_toBackend" e isso seria o suficiente.



Na placa anterior, nomeamos bastante o objeto Não autorizado. Vejamos como podemos configurá-lo.
No nível de versão, podemos encontrar a propriedade Not Authorized Object tanto para Web quanto para Mobile. Ali é onde podemos configurar qual objeto de nossa base de conhecimento é aquele que queremos definir para que a aplicação redirecione para ele quando o usuário não estiver autorizado.

Por padrão, teremos que para Web seja utilizado o exemplo de GAM. É possível aproveitá-lo e utilizá-lo, com a possibilidade de modificar seu design.
No caso de utilizar um próprio, ele deve ter configurada a propriedade de nível de segurança integrada como "Nenhum".

SLIDE DE CIERRE