

Lista de Controle de Acesso ou ACL



Lista de Controle de Acesso ou ACL, de acordo com a [Wikipedia definition](#), é “...uma lista que define quem tem permissão de acesso a certos serviços.”

No caso do Joomla, existem dois aspectos distintos para sua Lista de Controle de Acesso que os administradores do site podem controlar:

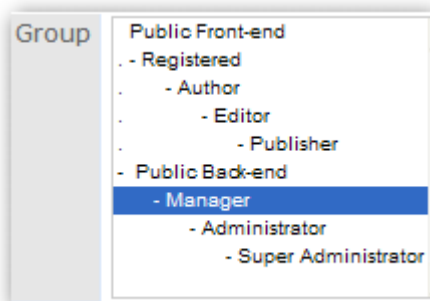
- **Que usuários podem ter acesso a que partes do site?** Por exemplo, uma certa opção de menu estará disponível para um certo usuário? Um usuário cadastrado pode ver, mas o público em geral não. Talvez a opção de menu esteja escondida de todos, exceto de um usuário definido como Editor ou superiores.
- **Que operações (ou ações) podem aplicar um usuário a um objeto específico?** Por exemplo, um usuário cadastrado como "Editor" pode enviar um artigo ou somente editar artigos existentes. Os controles de ACL podem permitir o envio e edição ou mudança na categoria do artigo, adicionar tags ou outro tipo de combinação. submit an article or only edit an existing article.

A implementação da ACL no Joomla foi modificada de forma substancial na série Joomla 2.5 o que permitiu maior flexibilidade para os grupos e permissões.

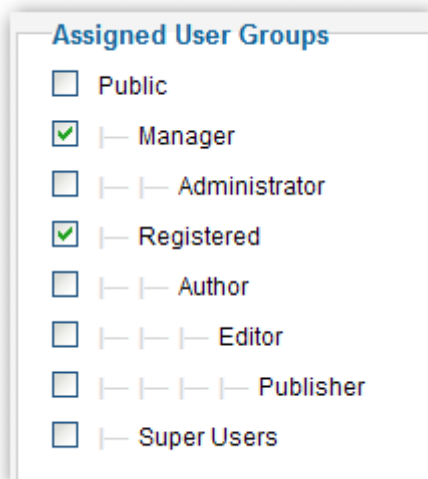
Se o seu cliente tem mais de uma pessoa manutenção do site, você deve considerar a possibilidade de ACL baseada em funções. O que é "baseada em funções" ACL e por que você deve usá-lo em vez da abordagem da ACL 1.5?



Para ser sincero, Joomla 1.5 teve um problema gritante que o impediu de ser adequado para muitos projetos corporativos. O desenvolvedor do site era extremamente limitada no fornecimento de variados papéis para o pessoal para manter o site.



ACL em 1,5



2.5 instala com um conjunto de grupos que se assemelham àsquelas em 1,5

Responsabilidades para diferentes secções do local não poderia ser isolados uns dos outros. Se um usuário precisava de um recurso ou um componente em particular que exigia que o usuário seja um "administrador", nós tivemos que fazer esse usuário um administrador. Quase invariavelmente, que lhe daria mais direitos e acesso a mais áreas do que o que qualquer usuário necessário. Esta limitação é inaceitável para a maioria das empresas.

Felizmente, essa limitação foi removida no 2.5. O problema é ... muitos desenvolvedores de sites não se afastam muito longe do modelo de ACL 1.5.

O que significa olhar baseada em funções como?

Um papel tende a representar alguma tarefa lógica ou conjunto de responsabilidades que pertencem dentro de uma organização ou empresa. É atribuído a um indivíduo e pode ser transferido para ou partilhada por outros indivíduos. A "papel" é um conceito que define uma organização e rotineiramente entende.

Por exemplo, o papel de "o cumprimento da ordem" vai conceder a um usuário a capacidade de acessar pedidos, informações de acesso de envio, alterar o status de uma ordem, e ajustar contagem de inventário para os produtos que estão sendo vendidos. Mas um outro papel pode ser necessária para o gerenciamento de informações de produtos, e outro para acessar informações financeiras de um cliente ou oferecendo reembolsos. Um usuário pode ser atribuído a todos esses papéis, enquanto outro usuário é atribuído a apenas um deles. Todos os recursos de um utilizador são determinados pela agregação de funções que são atribuídas a ele ou ela.

Qualidades típicas de um papel

O acesso e permissões associadas a um papel são apenas o suficiente para a realização de uma tarefa ou conjunto de tarefas relacionadas. Isso permite que o princípio de "menos privilégio."

As tarefas e responsabilidades de um papel são isolados a partir de (e, normalmente, não sobreposição com) as dos outros papéis. Isso permite que o princípio da "separação de funções."

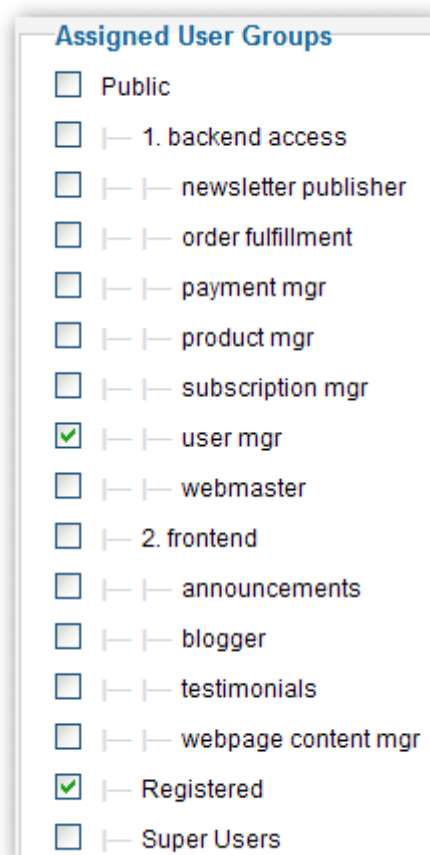
- Um papel representa a combinação de áreas que podem ser de acesso com níveis de permissões.
- Uma pessoa pode ser atribuído a mais do que uma função.
- Mais de uma pessoa pode partilhar o mesmo papel.
- Uma função pode ser facilmente adicionados, removidos ou transferidos entre os usuários.
- Um papel corresponde, em nome e aptidões para o conceito de negócio de que "o papel."

A maioria destes não poderia ser implementado em Joomla 1.5. *Todos* eles podem ser em 2,5. O modelo de ACL de 2,5 nos permite implementar todas essas qualidades, mas não exige nem impor-nos a fazê-lo. Na verdade, a configuração padrão do LCA e parece que emula a ACL de 1,5.

A ACL baseada em funções parece significativamente diferente da ACL chegamos out-of-the box.

Sander Potjer, desenvolvedor do Gerenciador de ACL, me disse que ele prefere para remover a maior parte dos grupos de usuários padrão e reconstruir os grupos de usuários, conforme necessário para um determinado projeto. Para uma solução baseada em funções, isso faz sentido. Até recentemente, isso não poderia ter sido prático. Demasiadas desenvolvedores de extensão falhou em fornecer suporte a ACL básica para seus 1.6 / 1.7 / 2.5 componentes. Como resultado, nós não poderia utilizar um grupo personalizado para acessar esses componentes - tivemos de atribuir um usuário a "gerente" ou mesmo "administrador"! Felizmente, as versões atuais do ACL Manager pode fornecer

automaticamente ACL básica para 2,5 componentes que não dispõem dele. Finalmente, podemos ignorar e até mesmo remover "manager" e "administrador". Se você implementar uma abordagem baseada em papel 100%, sem dúvida, você não precisa mais deles.



O que faz com base em funções nos comprar?

O modelo baseado em função corresponde muito de perto as regras de negócios de uma organização. Os líderes empresariais compreender o conceito de papéis, e um estudo de várias organizações revela que eles preferem para definir e gerenciar o controle de acesso em termos dos vários papéis atribuídos a indivíduos. Se nós modelamos o nosso

ACL de acordo com suas regras de negócios, estaremos entregando aos nossos clientes um CMS que acomoda suas necessidades de pessoal e mudanças futuras.

Considere as realidades que as empresas enfrentam: ao longo do tempo, a equipe e responsabilidades do pessoal mudar. As pessoas vêm e vão, e as responsabilidades se deslocou. Roles pode precisar ser atribuído, removido ou alterado rapidamente. Às vezes, várias pessoas compartilham um papel. Muitas vezes, um membro do pessoal irá reter múltiplos papéis. Papéis devem ser cedidos por indivíduo, e, por vezes, um papel pode ser atribuído ou removido como uma exceção para um cargo ou a uma classe de usuários. Smart Security exige que as pessoas tenham acesso apenas ao que eles precisam.

As empresas esperam ser capaz de fazer tudo isso. Se personalizar a ACL a ser organizado em torno de grupos baseados em função, então nós entregamos aos nossos clientes um sistema de gerenciamento de usuários e funções de usuário que é intuitivo e rápido de administrar.

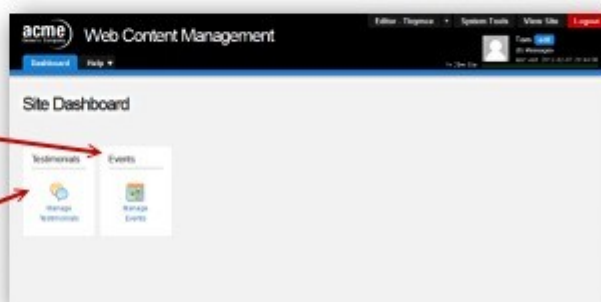
Assigned User Groups

- ☐ Public
- ☐ backend access
- ☐ Events Manager
- ☒ Order Fulfillment
- ☒ Site Auditor
- ☐ Site Statistics
- ☒ Store Manager
- ☐ Testimonials



Assigned User Groups

- ☐ Public
- ☐ backend access
- ☒ Events Manager
- ☐ Order Fulfillment
- ☐ Site Auditor
- ☐ Site Statistics
- ☐ Store Manager
- ☒ Testimonials



Esta captura de tela ilustra três benefícios de um ACL baseada em funções. Em primeiro lugar, a atribuição de funções aos usuários é intuitivo. Ele usa terminologia que é compreensível por parte das empresas. O controle de acesso é segmentado por como a organização entende e define funções. O papel importante do gerenciamento de usuários e atribuir direitos de usuário deve pertencer a pessoa mais adequada - mesmo que essa pessoa não tem um entendimento técnico do sistema. Este sistema baseado em papel é adequadamente intuitiva.

Em segundo lugar, os papéis são livremente agregada e podem ser agregados exclusivamente por usuário. Isto reflecte as realidades do pessoal e de bancos de

voluntários.

Em terceiro lugar, cada usuário do CMS terá acesso somente às partes necessárias para as tarefas que pertencem a esse papel. Se configurar níveis de acesso baseados em funções que correspondem aos grupos baseados em funções, podemos realizar o que você vê aqui: cada usuário vê um backend sob medida para o conjunto de funções atribuídas a ele ou ela.

Uma maneira diferente de pensar sobre ACL

Este artigo apresenta uma maneira diferente de pensar sobre o controle de acesso. Não é um modelo novo. "Controle de acesso baseado em função" (RBAC) foi formalmente descrita em 1996, e é normalmente utilizado por empresas e sistemas de informação. Na verdade, a nova estrutura da ACL do Joomla corresponde ao modelo conhecido como RBAC₁ - ele faz se nós empregamos "grupos de usuários" do Joomla para representar "papéis" em vez de "usuários de tipos" (uma distinção sutil, mas importante). Então, Joomla! que fornecem a base para a construção de um sistema sério de controle de acesso role-base.

Este artigo faz um argumento para a mudança para uma abordagem baseada em funções. Um artigo de acompanhamento vai discutir a implementação e ilustrar uma abordagem de trabalho.

Pode parecer mais seguro não se afastar muito longe do modelo 1.5. Mas as organizações que têm várias pessoas gerenciando seus sites esperar algo melhor. Nós podemos oferecer melhor. E quando trazemos Joomla! para corporações e grandes organizações, é preciso oferecer melhor.

Visão geral da ACL na Versão

Esta seção apresenta grandes alterações ACL entre as versões 2.5 e a série 3.x (que incluirá versões futuras). A tabela abaixo resume as mudanças a partir da versão 2.5.

	Versão 2.5	Versão 3.4
Grupos	Número ilimitado de Grupos definidos pelo usuário	O mesmo que 2,5
Usuários e Grupos	Um usuário pode ser atribuído a vários grupos	O mesmo que 2,5
Níveis de Acesso	Número ilimitado de níveis de acesso definidos pelo usuário	O mesmo que 2,5
Acesso Níveis e Grupos	Grupos são atribuídos aos níveis de acesso. Qualquer combinação de grupos pode ser atribuído a qualquer nível de acesso.	O mesmo que 2,5

ACL separada para Ver e Fazer

O sistema Joomla ACL pode ser considerado como sendo dividido em dois sistemas

completamente separados. Um sistema controla o que as coisas sobre os usuários do site *podem* ver. Os outros controles que os usuários podem *fazer* as coisas (as ações que um usuário pode tomar). A ACL para cada um é configurado de forma diferente.

Como controlar o que os usuários possam ver

A configuração para controlar o que os usuários podem ver é feito da seguinte forma:

- Criar um conjunto de níveis de acesso de acordo com as categorias e / ou a combinação de categorias que deseja Apenas usuários registrados para ver. NB não atribuir quaisquer grupos de usuários aos novos níveis de acesso neste momento.
- Criar um grupo de usuários, com 'registrado' como pai, para cada nível de acesso. Usando os mesmos nomes para os grupos de usuários como os níveis de acesso irá evitar confusão mais tarde.
- Edite seus novos níveis de acesso e atribuir o correto (novo) Grupo de Usuários para cada um. Você também pode querer atribuir o Super User Group (e / ou outros grupos padrão do usuário, mas não 'Guest' User Group) para todos os seus novos níveis de acesso
- Atribua cada item a ser visto com um nível de acesso. Os itens incluem itens de conteúdo (artigos, contatos e assim por diante), itens de menu e módulos.

Toda vez que um usuário está prestes a visualizar um item em uma página Joomla, o programa verifica se o usuário tem acesso ao item, como segue:

1. Cria uma lista de todos os níveis de acesso que o usuário tem acesso, com base em todos os grupos que o usuário pertence. Além disso, se um grupo tem um grupo pai, níveis de acesso para o grupo pai também estão incluídos na lista.
2. Verifica se o nível de acesso para o item (artigo, módulo, item de menu, e assim por diante) está nessa lista. Se sim, então o item é exibida para o usuário. Se não, em seguida, o item não é exibido.

Note-se que níveis de acesso são definidos separadamente para cada grupo e não são herdadas do grupo pai de um grupo.

Como controlar o que os usuários podem fazer

O sistema para a criação o que os usuários em um grupo de usuários pode fazer - o que ações eles podem assumir um determinado item - é configurada com o separador Permissões de configuração global e na guia Permissões da tela Opções de cada componente. As permissões também pode ser configurado no nível de categoria de componentes principais e ao nível do artigo para artigos.

- Se você deseja logado aos usuários criar, excluir, editar Estado ou Edite própria para específicas Categorias então:
 - Criar um grupo de usuários com o Pai como um dos seus grupos de usuários que tem acesso à Categoria (ou Categorias) você deseja que esse

novo grupo de usuários para modificar.

- Atribuir o seu novo grupo de usuários para o Nível (s) de acesso apropriado. Em seguida, alterar as permissões necessárias para o seu novo grupo de usuários globalmente ou por Categoria / artigo.
 - Ao criar um grupo de usuários é uma boa prática para selecionar um grupo pai que tem menos permissões do que o necessário para o novo grupo. Isso é porque ele é mais fácil de elevar as permissões por componente / categoria / Article que as permissões adicionais são necessários para que é para remover permissões de os outros componentes / Categorias / Artigos.
 - *(exemplo: Você tem 10 categorias, mas você quer criar permissões para apenas 1. Se você definir permissões globais para Permitir criar para esse grupo seria necessário remover permissão Criar para todas as categorias E você precisa remover a permissão Criar para isso. grupo com qualquer nova categoria que você adiciona em uma data posterior.)*
- Apenas criar um grupo de usuários com um dos Grupos de Usuários padrão como pai, se nenhum deles tem as permissões exatas que você precisa e deseja todas as categorias

Note-se que esta configuração é independente da configuração para visualização, mas um grupo de usuários precisa ser atribuído ao Nível (s) de acesso apropriados para que o usuário nesse grupo para usar essas permissões.

Quando um usuário quer iniciar uma ação específica contra um item de componente (por exemplo, editar um artigo), o sistema (após a verificação do Grupo do usuário está em tem acesso) verifica a permissão para essa combinação de usuário, item, e ação. Se for permitido, então o utilizador pode prosseguir. Caso contrário, não é permitido a ação.

O restante deste tutorial explica como podemos controlar o que os usuários podem fazer - o que eles têm permissões de ação.

Ações, grupos e herança

O outro lado da ACL é conceder permissões aos usuários para executar ações em objetos.

Série 3.x

Grupos e Ações	Ações permitidas para cada grupo são definidas pelo administrador do site.
Permissão Âmbito	As permissões podem ser definidas em vários níveis na hierarquia: Site, Componente, Categoria, Object.
Herança de permissão	As permissões podem ser herdadas de grupos de pais e mães Categorias

Como as permissões de trabalho

Há quatro possíveis permissões para ações, conforme descrito abaixo:

- **Não colocado:** Defaults para "negar", mas, ao contrário da permissão Negar, essa permissão pode ser substituída configurando um grupo filho ou um nível mais baixo na hierarquia permissão para "Permitir". Esta permissão só se aplica às permissões de configuração global.
- **Herdar:** Herda o valor de um grupo pai ou a partir de um nível mais elevado na hierarquia permissão. Esta permissão se aplica a todos os níveis, exceto o nível de configuração global.
- **Negar:** Nega esta ação para este nível e **grupo. IMPORTANTE:** Este também nega esta ação para todos os grupos secundários e todos os níveis inferiores da hierarquia permissão. Colocar em Permitir para um grupo filho ou um nível inferior não terá qualquer efeito. A ação será sempre negado por qualquer membro do grupo filho e para qualquer nível inferior na hierarquia permissão.
- **Permitir:** Permite esta ação para este nível e grupo e para níveis inferiores e grupos filhos. Isto não tem qualquer efeito, se um grupo ou nível mais alto está configurado para Negar ou Permitir. Se um grupo ou nível mais alto está configurado para Negar, então essa permissão será sempre negado. Se um grupo ou nível mais alto está definido para Permitir, então esta permissão já estará permitida.

Níveis de hierarquia de permissões

Permissões de ação na versão 2.5 podem ser definidas em até quatro níveis, como segue:

1. **Configuração Global:** determina as permissões padrão para cada ação e grupo.
2. **Componente Opções> Permissões:** pode revogar as permissões default para este componente (por exemplo, artigos, Menus, Usuários, Banners, e assim por diante).
3. **Categoria:** pode revogar as permissões default para objetos em uma ou mais categorias. Aplica-se a todos os componentes com categorias, incluindo Artigos, Banners, Contatos, Newsfeeds, e Weblinks.
4. **Artigo:** Pode substituir as permissões para um artigo específico. Este nível só se aplica aos artigos. Outros componentes só permitem que os três primeiros níveis.

Configuração Global

Este é acessado a partir do sistema → configuração global → Permissões. Esta tela permite que você defina a permissão de nível superior para cada grupo para cada ação, como mostrado na imagem abaixo.

Global Configuration

Save Save & Close Cancel Help

SYSTEM Site System Server Permissions Text Filters

Global Configuration

COMPONENT

- Banners
- Cache Manager
- Check-in
- Contacts
- Articles
- Smart Search
- Installation Manager
- Joomla! Update
- Language Manager
- Media Manager
- Menus Manager
- Messaging
- Module Manager
- Newsfeeds
- Plugins Manager
- Post-installation Messages
- Redirect
- Search
- Tags
- Template Manager
- Users Manager

Permission Settings

Manage the permission settings for the user groups below. See notes at the bottom.

Group being edited

- Public
- Guest
- Manager
- Administrator**
- Registered
- Author
- Editor
- Publisher
- Super Users

Actions

Action	Permissions	Settings in Effect
Site Login	Inherited	Allowed
Admin Login	Inherited	Allowed
Offline Access	Inherited	Allowed
Super User	Inherited	Not Allowed
Access Administration Interface	Allowed	Allowed
Create	Inherited	Allowed
Delete	Inherited	Allowed
Edit	Inherited	Allowed
Edit State	Inherited	Allowed
Edit Own	Inherited	Allowed

Permissions

Select New Setting ¹

Settings in Effect

Calculated Setting ²

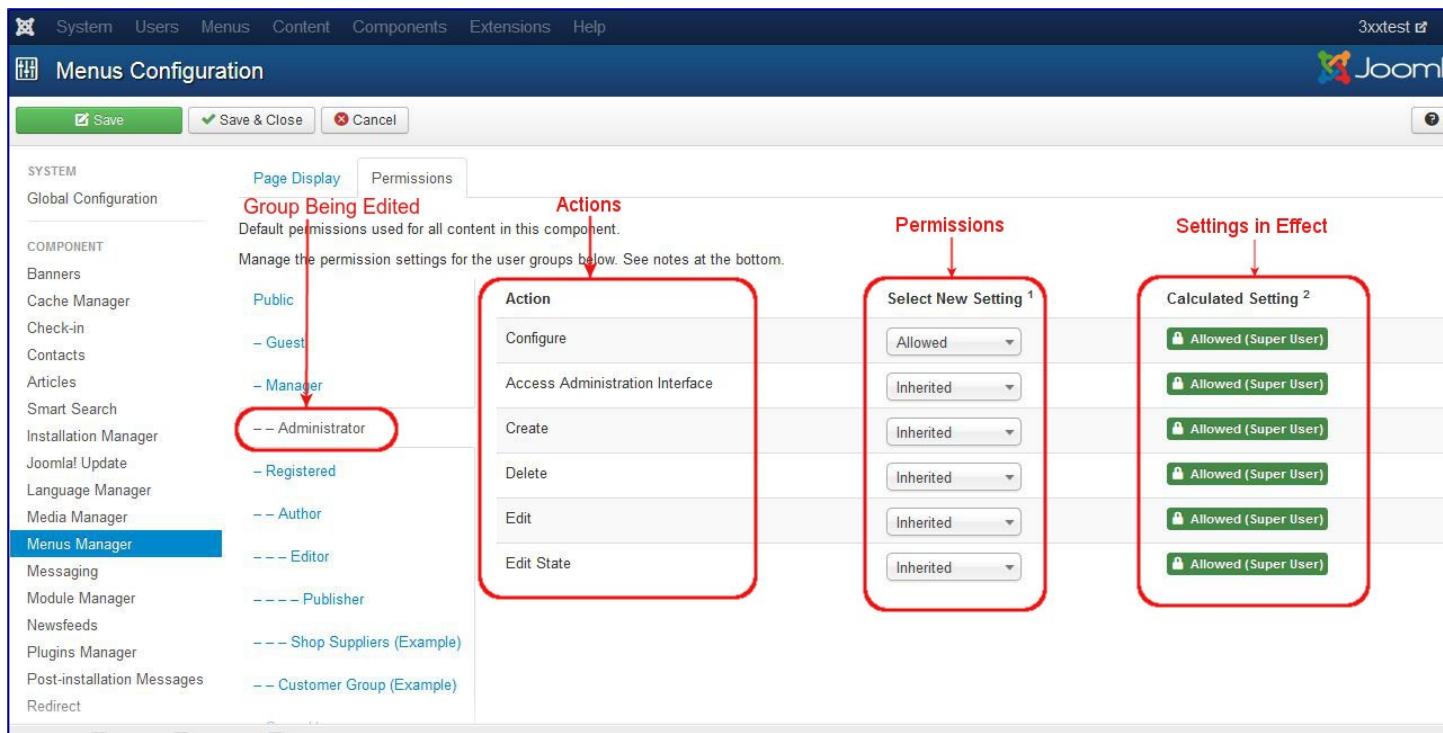
As opções para cada valor são herdadas, permitidos ou negado. A coluna de ajuste calculados mostra a configuração em vigor. Ou é não permitido (o padrão), admitidos, ou negado.

Você trabalha em um grupo de cada vez, abrindo o controle deslizante para esse grupo. Você pode alterar as permissões nos Selecione Configurações Novas caixas de listagem drop-down.

Observe que a coluna de ajuste calculados não é atualizada até que você pressione o botão Salvar na barra de ferramentas. Para verificar se as configurações são o que você quer, pressione o botão Salvar e marque a coluna Configurações Calculado.

Componente Opções-> Permissões

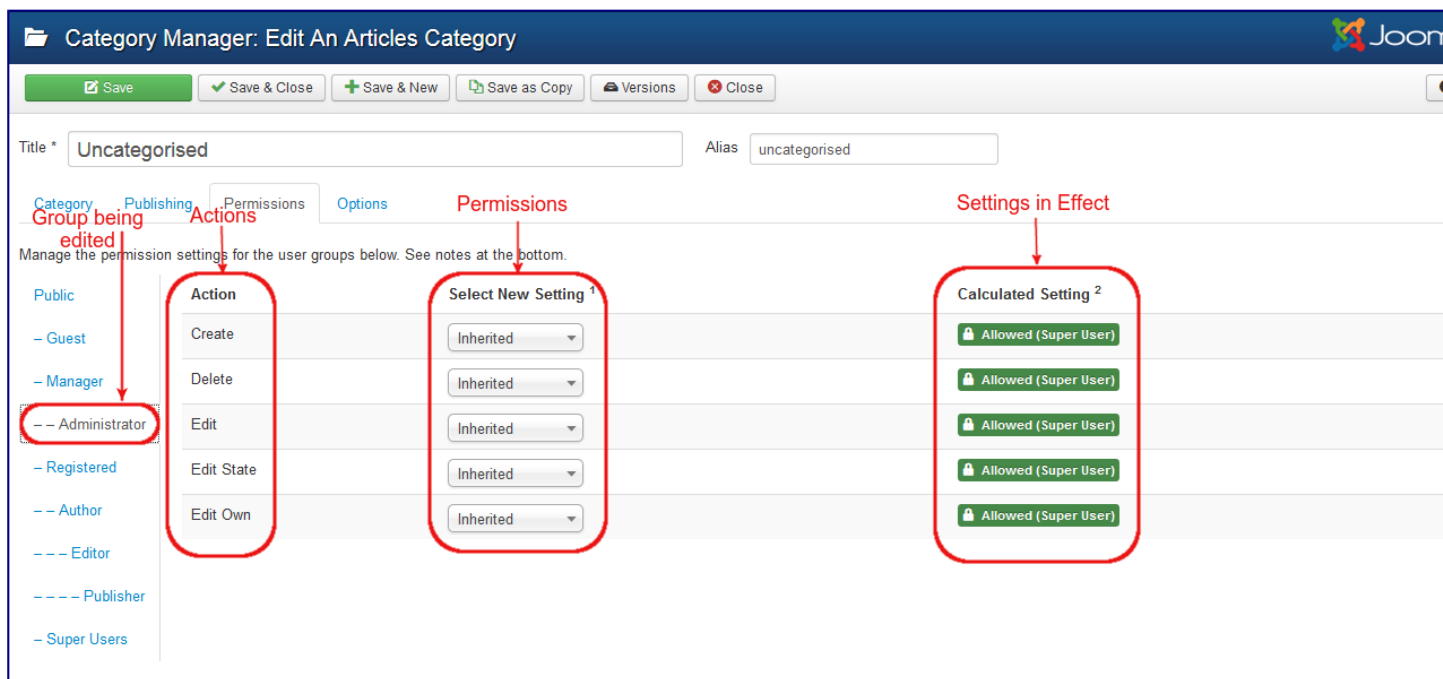
Este é acessada para cada componente, clicando no ícone Opções na barra de ferramentas. Esta tela é semelhante à tela de configuração global acima. Por exemplo, clicando no ícone da barra de ferramentas Opções no Menu Manager mostra os menus de configuração abaixo.



Acesso a opções só está disponível para membros de grupos que têm permissão para a ação Configurar na para cada componente. No exemplo acima, o grupo Administrador tem permitido a permissão para a opção Configurar, para que os membros deste grupo podem acessar essa tela.

Categoria

Permissões de categoria são acessados no Gerente de Categoria: tela Editar Categoria, em uma guia na parte superior da tela. Esta tela tem cinco permissões, como mostrado abaixo.



Nestas telas, você trabalha nas permissões para um grupo de usuários de cada vez. No

exemplo acima, estamos editando as permissões para o grupo Administrador.

Note-se que os configurar e componente Access ações não se aplicam no nível de categoria, para que essas ações não estão incluídas.

Note-se também que as categorias podem ser organizadas em uma hierarquia. Se assim for, então permissões de ação em uma categoria pai são herdadas automaticamente por um categoria infantil. Por exemplo, se você tivesse uma hierarquia de categorias de animais → Animais → Cães, em seguida, a hierarquia de nível de permissão total para um artigo na categoria de cães seriam os seguintes:

- Configuração Global
- Article Manager → Opções → Permissão
- Categoria Animais
- Animais de estimação Categoria
- Cães Categoria
- artigo específico

Artigo

Permissões para um único artigo são de acesso no Gerenciador de artigo: Edite tela artigo, novamente em um controle deslizante na parte inferior da tela. Este ecrã tem três ações, como mostrado abaixo.

Article Manager: Edit Article

Save Save & Close Save & New Save as Copy Versions Close

Title * Administrator Components Alias administrator-components

Content Publishing Images and links Options Configure Edit Screen Permissions

Manage the permission settings for the user groups below. See notes at the bottom.

	Action	Select New Setting ¹	Calculated Setting ²
Public			
- Guest	Delete	Inherited	Allowed (Super User)
- Manager	Edit	Inherited	Allowed (Super User)
-- Administrator	Edit State	Inherited	Allowed (Super User)
- Registered			
-- Author			
--- Editor			
---- Publisher			
--- Shop Suppliers (Example)			
-- Customer Group (Example)			
- Super Users			

Mais uma vez, você editar cada grupo, clicando sobre ela para abrir o controle deslizante para esse grupo. Você pode, então, alterar as permissões na coluna Select nova configuração. Para ver o efeito de quaisquer alterações, pressione o botão Salvar para atualizar a coluna de ajuste calculados.

Note que o Configure, componentes Access, e criar ações não se aplicam no nível de artigo, de modo que essas ações não estão incluídas. A permissão para criar um artigo é fixado a um dos níveis mais elevados na hierarquia.

Níveis de Acesso

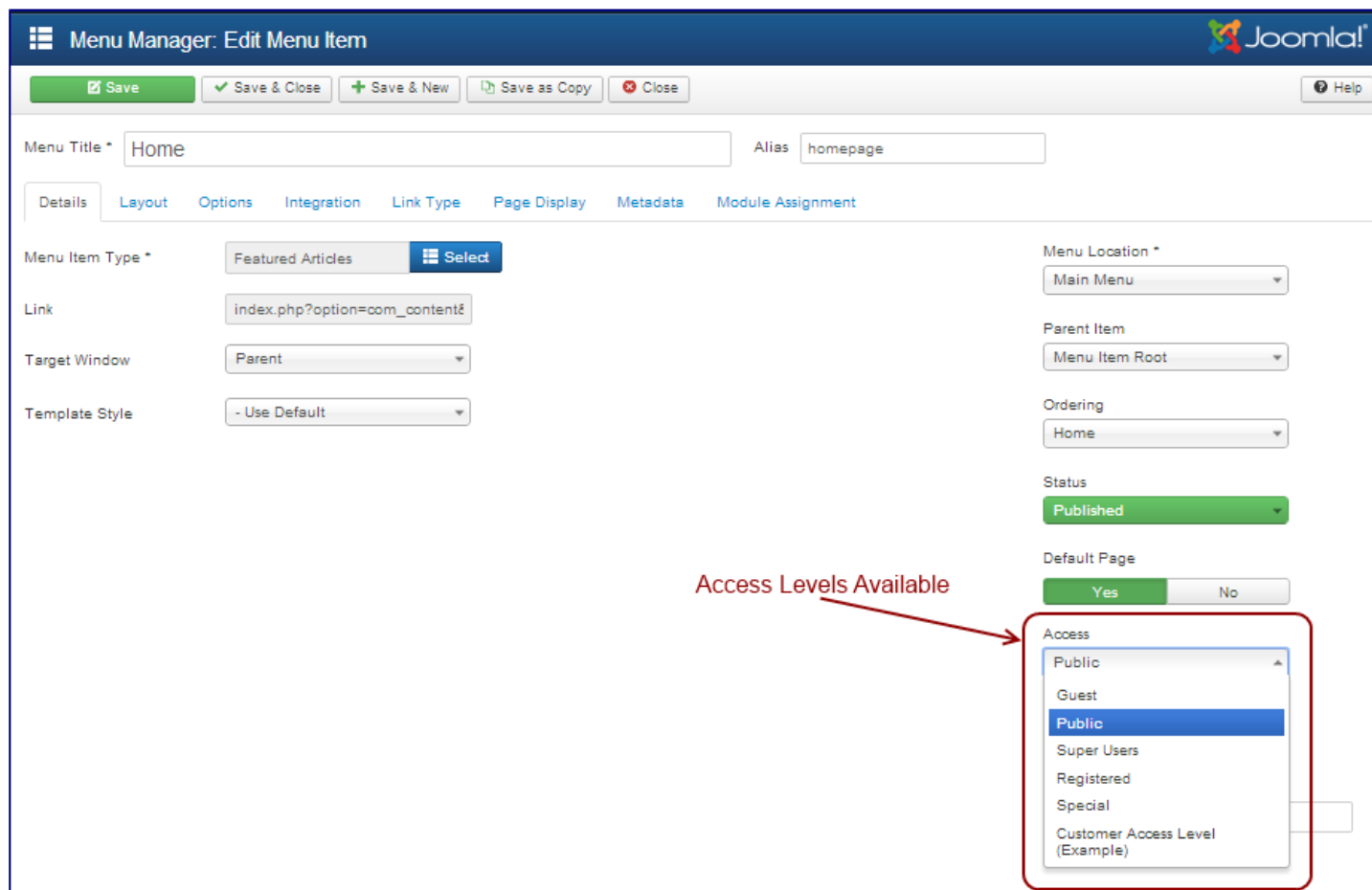
Níveis de acesso em série 3.x são simples e flexível. A tela abaixo mostra o Nível de Acesso Especial.

Basta marcar a caixa para cada grupo que deseja incluir nesse nível. O Nível de Acesso Especial inclui o Manager, Autor, e grupos de superusuários. Ele também inclui grupos secundários desses grupos. Assim, o grupo Administrador é incluído, uma vez que é um grupo filho do grupo Manager. Os grupos editor, e uma loja de Fornecedores estão incluídas, uma vez que são grupos de crianças de Autor. (Observe que poderíamos verificar todos os grupos filhos se nós queria e que não iria doer nada).

Uma vez que níveis de acesso são criados, são utilizados da mesma maneira como na versão 1.5. Cada objeto na extremidade dianteira é atribuído um nível de acesso. Se o

nível for Public, então qualquer um pode acessar esse objeto. Caso contrário, apenas os membros de grupos atribuídos a esse nível de acesso pode acessar esse objeto. Os níveis de acesso são atribuídas aos itens do menu e para os módulos. Cada um só pode ser atribuído a um nível de acesso.

Por exemplo, a tela abaixo mostra a tela de item de menu Editar com a lista de níveis de acesso disponíveis.



Menu Manager: Edit Menu Item

Save Save & Close Save & New Save as Copy Close Help

Menu Title * Home Alias homepage

Details Layout Options Integration Link Type Page Display Metadata Module Assignment

Menu Item Type * Featured Articles Selected

Link index.php?option=com_content&

Target Window Parent

Template Style - Use Default

Menu Location * Main Menu

Parent Item Menu Item Root

Ordering Home

Status Published

Default Page Yes No

Access

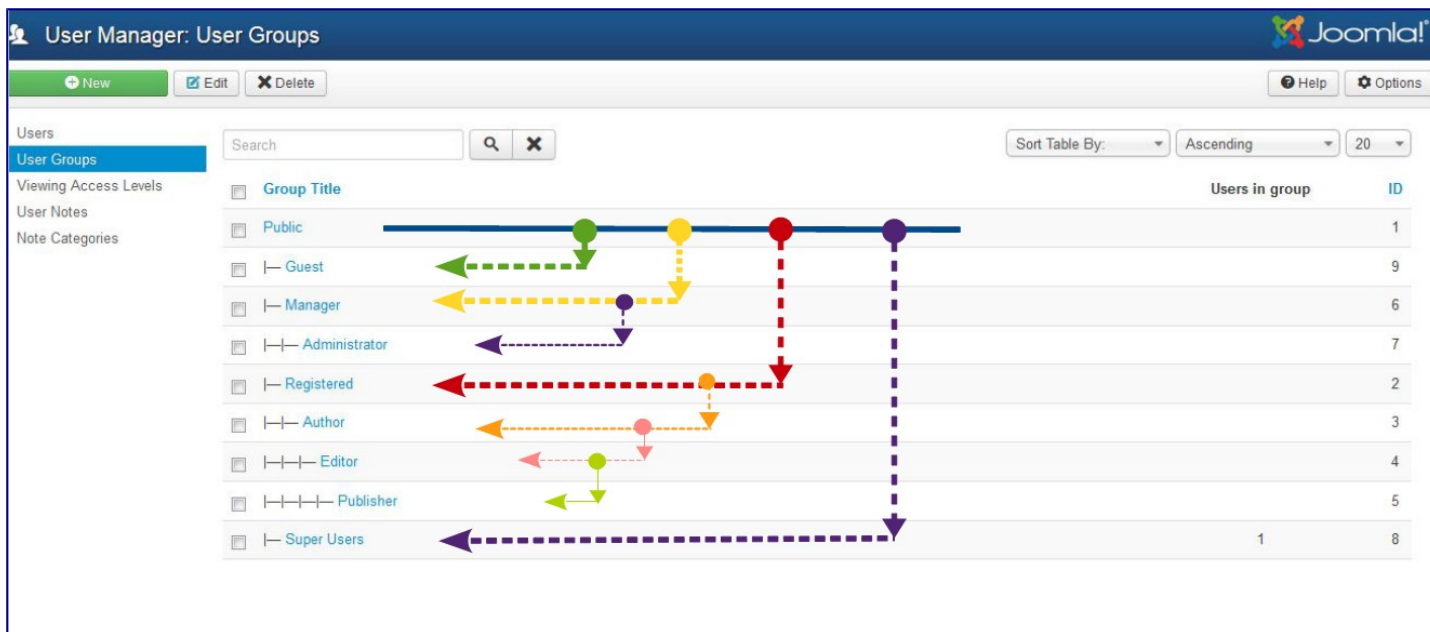
- Public
- Guest
- Public
- Super Users
- Registered
- Special
- Customer Access Level (Example)

Configuração ACL padrão

Quando Joomla! está instalado, estes são definidos para sua configuração padrão inicial. Vamos discutir essas configurações iniciais como uma maneira de entender como funciona o ACL.

Grupos padrão

Versão 3.x permite definir seus próprios grupos. Quando você instalar a versão 3.x, que inclui um conjunto de grupos padrão, seguem abaixo os grupos de usuários padrão básicas. (Grupos de usuários padrão adicionais são instalados com dados de amostra)

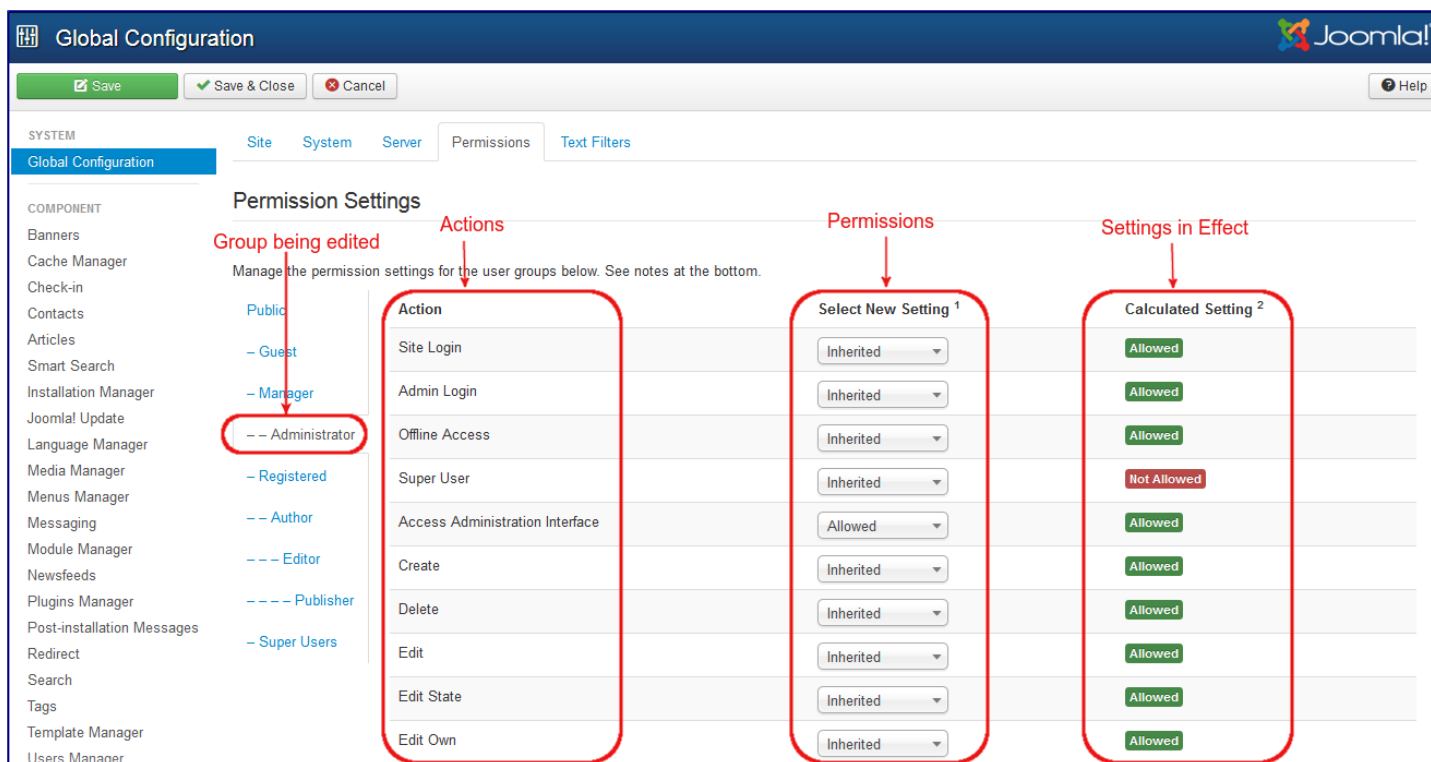


As setas indicam as relações entre pais e filhos. Como discutido acima, quando você definir uma permissão para um grupo pai, essa permissão é automaticamente herdada por todos os grupos filhos. As permissões herdadas, e permitiu que pode ser substituído por um grupo filho. A permissão negado não pode ser substituído e será sempre negar uma ação para todos os grupos filhos.

Configuração Global

Joomla! versão 2.5 será instalado com as mesmas familiares permissões de back-end como o da versão 1.5. No entanto, com 2.5, você pode facilmente mudar estes para atender às necessidades do seu site.

Como discutido anteriormente, as permissões para cada ação são herdadas do nível acima na hierarquia de permissões e do grupo pai de um grupo. Vamos ver como isso funciona. O nível superior para isso é todo o site. Isto é definido nos Site-> global> Configuração-permissões, como mostrado abaixo.



A primeira coisa a notar são os nove ações: Site Login, Admin Login, Super Administrador, Access Component, Criar, Apagar, Modificar, em Editar Estado. e Edite própria. Estas são as ações que um usuário pode executar em um objeto no Joomla. O significado específico de cada ação depende do contexto. Para a tela de configuração global, eles são definidos da seguinte forma:

Site Entrada

Entre para a extremidade dianteira do sítio

Admin Login

Entre a extremidade traseira do sítio

Super Administrador

Concede o status do usuário "super utilizador". Os usuários com essa permissão pode fazer qualquer coisa no site. Somente os usuários com essa permissão pode alterar as configurações de configuração global (esta tela). Essas permissões não pode ser restringido. É importante compreender que, se um usuário é membro de um grupo Super Administrador, quaisquer outras permissões atribuídas a esse usuário são irrelevantes. O usuário pode fazer qualquer ação no site. No entanto, níveis de acesso ainda pode ser atribuído para controlar o que este grupo vê no site. (Obviamente, um usuário Super Admin pode alterar níveis de acesso se eles querem, por isso níveis de acesso não totalmente restringir o que um usuário Super Admin pode ver.)

Access Component

Abra as telas gerente componente (Gerenciador de usuários, gestor de menu, o artigo Manager, e assim por diante)

Crio

Criar novos objetos (por exemplo, usuários, itens de menu, artigos, Weblinks, e

assim por diante)

Excluir

Excluir objetos existentes

Editar

Edite objetos existentes

Editar Estado

Alterar estado de objeto (Publicar, Unpublish, Arquivo e Trash)

Edite própria

Editar objetos que você criou.

Cada grupo para o site tem o seu próprio controle deslizante que é aberta ao clicar no nome do grupo. Neste caso (com os dados de amostra instalados), temos os 7 grupos padrão que tínhamos na versão 1.5 mais dois grupos adicionais chamados "Loja Fornecedores" e "Grupo de clientes". Observe que os nossos grupos são configurados com as mesmas permissões que eles tinham na versão 1.5. Tenha em mente que podemos alterar qualquer uma dessas permissões para fazer a segurança funcionam do jeito que queremos. Vamos passar por isso para ver como ele funciona.

- **Público** tem tudo definido como "não definida", como mostrado abaixo.

Global Configuration

Save Save & Close Cancel Help

SYSTEM Site System Server Permissions Text Filters

Global Configuration

COMPONENT

- Banners
- Cache Manager
- Check-in
- Contacts
- Articles
- Smart Search
- Installation Manager
- Joomla! Update
- Language Manager
- Media Manager
- Menus Manager
- Messaging
- Module Manager
- Newsfeeds
- Plugins Manager
- Post-installation Messages
- Redirect
- Search
- Tags
- Template Manager
- Users Manager

Permission Settings

Manage the permission settings for the user groups below. See notes at the bottom.

Public	Action	Select New Setting ¹
- Guest	Site Login	Not Set
- Manager	Admin Login	Not Set
- - Administrator	Offline Access	Not Set
- - Registered	Super User	Not Set
- - Author	Access Administration Interface	Not Set
- - - Editor	Create	Not Set
- - - - Publisher	Delete	Not Set
- Super Users	Edit	Not Set
	Edit State	Not Set
	Edit Own	Not Set

- Isso pode ser um pouco confuso. Basicamente, "não informado" é o mesmo que "Herdado". Porque Pública é o nosso grupo de alto nível, e por causa de configuração global é o nível mais alto da hierarquia de componentes, não há nada para herdar. Assim, "não informado" é usado em vez de "herdar".
- O padrão neste caso é de nenhuma permissão. Então, como seria de esperar, o grupo Público não tem permissões especiais. Além disso, é importante notar que, uma vez que nada está definido como negado, todas essas permissões podem ser substituídas por grupos filhos ou por níveis mais baixos da hierarquia permissão.
- É **convidado** um grupo de 'criança' do grupo Público tem tudo definido para 'herdados'

Global Configuration

Save Save & Close Cancel

SYSTEM Site System Server Permissions Text Filters

Global Configuration

COMPONENT

- Banners
- Cache Manager
- Check-in
- Contacts
- Articles
- Smart Search
- Installation Manager
- Joomla! Update
- Language Manager
- Media Manager
- Menus Manager
- Messaging
- Module Manager
- Newsfeeds
- Plugins Manager
- Post-installation Messages
- Redirect
- Search
- Tags
- Template Manager
- Users Manager

Permission Settings

Manage the permission settings for the user groups below. See notes at the bottom.

Public	Action	Select New Setting ¹	Calculated Setting ²
- Guest	Site Login	Inherited	Not Allowed
- Manager	Admin Login	Inherited	Not Allowed
-- Administrator	Offline Access	Inherited	Not Allowed
-- Registered	Super User	Inherited	Not Allowed
-- Author	Access Administration Interface	Inherited	Not Allowed
--- Editor	Create	Inherited	Not Allowed
--- Publisher	Delete	Inherited	Not Allowed
- Super Users	Edit	Inherited	Not Allowed
	Edit State	Inherited	Not Allowed
	Edit Own	Inherited	Not Allowed

- Este é o padrão 'Guest User Group' nas opções do Gerenciador de usuários e do Grupo que (não logado) visitantes do seu site são colocados em.
- **Manager** é um grupo "filho" do grupo Público. Isso tem permitido permissões para tudo, exceto Access Component e Super Administrador. Assim, um membro deste grupo pode fazer tudo no final frente e de trás do site, exceto alterar as opções de componentes Permissões Globais e.

Global Configuration

Save Save & Close Cancel

SYSTEM Site System Server Permissions Text Filters

Global Configuration

COMPONENT

- Banners
- Cache Manager
- Check-in
- Contacts
- Articles
- Smart Search
- Installation Manager
- Joomla! Update
- Language Manager
- Media Manager
- Menus Manager
- Messaging
- Module Manager
- Newsfeeds
- Plugins Manager
- Post-installation Messages
- Redirect
- Search
- Tags
- Template Manager
- Users Manager

Permission Settings

Manage the permission settings for the user groups below. See notes at the bottom.

Public	Action	Select New Setting ¹	Calculated Setting ²
- Guest	Site Login	Allowed	Allowed
- Manager	Admin Login	Allowed	Allowed
- - Administrator	Offline Access	Allowed	Allowed
- - Registered	Super User	Inherited	Not Allowed
- - Author	Access Administration Interface	Inherited	Not Allowed
- - - Editor	Create	Allowed	Allowed
- - - - Publisher	Delete	Allowed	Allowed
- Super Users	Edit	Allowed	Allowed
	Edit State	Allowed	Allowed
	Edit Own	Allowed	Allowed

- Os membros do grupo **Administrador** herdar todas as permissões de gerente e também têm permitido para Componentes de Acesso. Assim, os membros desse grupo por padrão pode acessar as telas de opções para cada componente.

Global Configuration

Save Save & Close Cancel Help

SYSTEM Site System Server Permissions Text Filters

Global Configuration

COMPONENT

- Banners
- Cache Manager
- Check-in
- Contacts
- Articles
- Smart Search
- Installation Manager
- Joomla! Update
- Language Manager
- Media Manager
- Menus Manager
- Messaging
- Module Manager
- Newsfeeds
- Plugins Manager
- Post-installation Messages
- Redirect
- Search
- Tags
- Template Manager
- Users Manager

Permission Settings

Manage the permission settings for the user groups below. See notes at the bottom.

	Action	Select New Setting ¹	Calculated Setting ²
Public	Site Login	Inherited	Allowed
- Guest	Admin Login	Inherited	Allowed
- Manager	Offline Access	Inherited	Allowed
- - Administrator	Super User	Inherited	Not Allowed
- Registered	Access Administration Interface	Allowed	Allowed
- - Author	Create	Inherited	Allowed
- - - Editor	Delete	Inherited	Allowed
- - - - Publisher	Edit	Inherited	Allowed
- Super Users	Edit State	Inherited	Allowed
	Edit Own	Inherited	Allowed

- **Registrado** é o mesmo um público exceto para a permissão Permitir para a ação do site Entrada. Isto significa que os membros do grupo registrado pode acessar o site. Desde permissões padrão são herdadas, isso significa que, a menos que um grupo filho substitui essa permissão, todos os grupos filho do grupo Registrado serão capazes de acessar também.

Global Configuration

Save Save & Close Cancel Help

SYSTEM

Global Configuration Site System Server Permissions Text Filters

COMPONENT

Banners

Cache Manager

Check-in

Contacts

Articles

Smart Search

Installation Manager

Joomla! Update

Language Manager

Media Manager

Menus Manager

Messaging

Module Manager

Newsfeeds

Plugins Manager

Post-installation Messages

Redirect

Search

Tags

Template Manager

Users Manager

Permission Settings

Manage the permission settings for the user groups below. See notes at the bottom.

Public

- Guest

- Manager

- - Administrator

- Registered

- - Author

- - - Editor

- - - - Publisher

- Super Users

Action	Select New Setting ¹	Calculated Setting ²
Site Login	Allowed	Allowed
Admin Login	Inherited	Not Allowed
Offline Access	Inherited	Not Allowed
Super User	Inherited	Not Allowed
Access Administration Interface	Inherited	Not Allowed
Create	Inherited	Not Allowed
Delete	Inherited	Not Allowed
Edit	Inherited	Not Allowed
Edit State	Inherited	Not Allowed
Edit Own	Inherited	Not Allowed

- **O autor é um** filho do grupo Registrado e herda suas permissões e também adiciona Criar e editar própria. Desde Autor, Editor e Publisher não têm permissões de back-end, vamos discuti-las abaixo, quando discutimos permissões de front-end.

Global Configuration

SaveSave & CloseCancel

SYSTEM

Global Configuration

COMPONENT

Banners

Cache Manager

Check-in

Contacts

Articles

Smart Search

Installation Manager

Joomla! Update

Language Manager

Media Manager

Menus Manager

Messaging

Module Manager

Newsfeeds

Plugins Manager

Post-installation Messages

Redirect

Search

Tags

Template Manager

Users Manager

SiteSystemServerPermissionsText Filters

Permission Settings

Manage the permission settings for the user groups below. See notes at the bottom.

Public

Guest

Manager

Administrator

Registered

Author

Editor

Publisher

Super Users

Action

Site Login

Admin Login

Offline Access

Super User

Access Administration Interface

Create

Delete

Edit

Edit State

Edit Own

Select New Setting 1

Inherited

Inherited

Inherited

Inherited

Inherited

Allowed

Inherited

Inherited

Inherited

Allowed

Calculated Setting 2

Allowed

Not Allowed

Not Allowed

Not Allowed

Not Allowed

Allowed

Not Allowed

Not Allowed

Not Allowed

Allowed

- **Editor** é uma criança do grupo Autores e adiciona a permissão Editar.

Global Configuration

Save Save & Close Cancel

SYSTEM Site System Server Permissions Text Filters

Global Configuration

COMPONENT

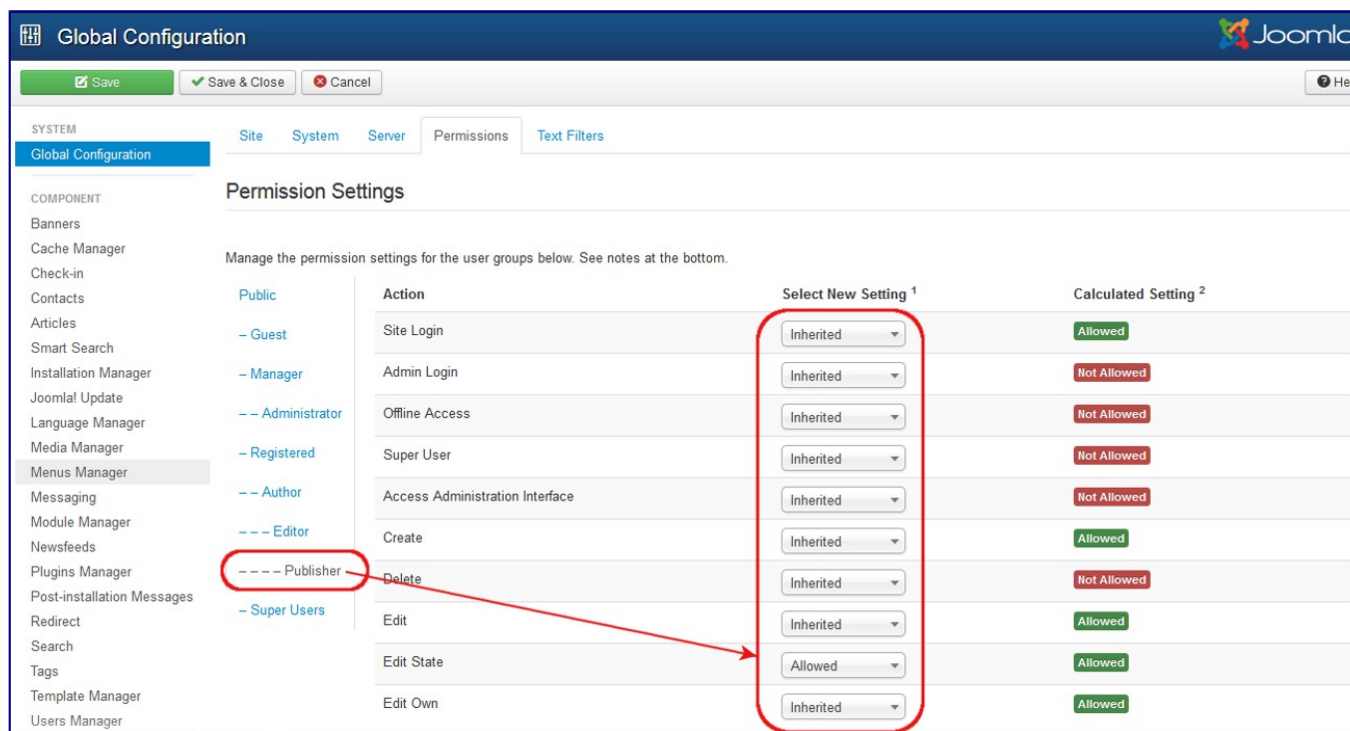
- Banners
- Cache Manager
- Check-in
- Contacts
- Articles
- Smart Search
- Installation Manager
- Joomla! Update
- Language Manager
- Media Manager
- Menus Manager
- Messaging
- Module Manager
- Newsfeeds
- Plugins Manager
- Post-installation Messages
- Redirect
- Search
- Tags
- Template Manager
- Users Manager

Permission Settings

Manage the permission settings for the user groups below. See notes at the bottom.

	Action	Select New Setting ¹	Calculated Setting ²
Public	Site Login	Inherited	Allowed
- Guest	Admin Login	Inherited	Not Allowed
- Manager	Offline Access	Inherited	Not Allowed
- Administrator	Super User	Inherited	Not Allowed
- Registered	Access Administration Interface	Inherited	Not Allowed
- Author	Create	Inherited	Allowed
- - - Editor	Delete	Inherited	Not Allowed
- - - - Publisher	Edit	Allowed	Allowed
- Super Users	Edit State	Inherited	Not Allowed
	Edit Own	Inherited	Allowed

- **Publisher** é um filho do editor e adiciona a permissão Editar Estado.



- **Loja de Fornecedores** é um grupo exemplo que é instalado se você instalar os dados de exemplo. É um grupo filho de Autor.
- **Customer Group** é um grupo de exemplo que é instalado se você instalar os dados de exemplo. É um grupo filho de Registered.
- Grupo **Usuários Super** tem a permissão Permitir para a ação Super Administrador. Devido a isso, os membros deste grupo têm permissões super-utilizador em todo o local. Eles são os únicos usuários que podem acessar e editar valores na tela de configuração global. Os usuários com permissão para a ação Super Administrador têm algumas características especiais:
 - Se um usuário tiver permissões de administrador Super, há outras permissões para este assunto usuário. O usuário pode executar qualquer ação no site.
 - Apenas os usuários Super administrador pode criar, editar ou excluir outros usuários Super administrador ou grupos.

Há dois pontos muito importantes para entender a partir desta tela. A primeira é ver como as permissões podem ser herdadas do grupo pai. A segunda é para ver como você pode controlar as permissões padrão por grupo e por ação.

Isto proporciona uma grande flexibilidade. Por exemplo, se você queria Loja Fornecedores para ser capaz de ter a capacidade para acessar o back-end, você pode simplesmente mudar o seu administrador valor entre a "permitido". Se você queria para não permitir que membros do grupo Administrador para apagar objetos ou mudar seu estado, você mudaria suas permissões nestas colunas para herdados (ou negada).

Também é importante compreender que a capacidade de ter grupos filho é completamente opcional. Ele permite que você poupar algum tempo quando a criação de novos grupos. No entanto, se você gosta, você pode configurar todos os grupos para ter


Pública como o pai e não herdam as permissões de um grupo pai.

Opções e permissões de componentes

Agora, vamos continuar a ver como as permissões padrão de back-end para a versão 2.5 imitar as permissões para a versão 1.5. O grupo Usuários Super em 2,5 é equivalente ao grupo Super Administrador na 1.5.

Basta olhar para a tela de Configurações Globais acima, parece que o grupo Administrador eo grupo Gerenciador têm permissões idênticas. No entanto, na versão 1.5 Os administradores podem fazer tudo, exceto Configuração Global, enquanto Gerenciadores não são permitidos para adicionar usuários ou trabalhar com itens de menu. Isso também é verdade na versão 2.5 configuração padrão. Vamos ver como isso é feito.

Se navegar para usuários-> User Manager e clique no botão Opções na barra de ferramentas, vemos a tela abaixo:

 **Users Configuration** Save & Close

Component

Mass Mail















Permissions


Default permissions used for all content in this component.

Manage the permission settings for the user groups below. See notes at the bottom.

Public

Manager

Action	Select New Setting ¹	Calculated Setting ²
Configure	Inherited 	 Not Allowed
Access Component	Inherited 	 Not Allowed
Create	Inherited 	 Allowed
Delete	Inherited 	 Allowed
Edit	Inherited 	 Allowed
Edit State	Inherited 	 Allowed
Edit Own	Allowed 	 Allowed


Users Configuration
Save & Close

Component
Mass Mail
Permissions

Default permissions used for all content in this component.

Manage the permission settings for the user groups below. See notes at the bottom.

▶ Public

▶ └─ Manager

▼ └─ └─ Administrator

Action	Select New Setting ¹	Calculated Setting ²
Configure	Allowed ▾	✓ Allowed
Access Component	Inherited ▾	✓ Allowed
Create	Inherited ▾	✓ Allowed
Delete	Inherited ▾	✓ Allowed
Edit	Inherited ▾	✓ Allowed
Edit State	Inherited ▾	✓ Allowed
Edit Own	Inherited ▾	✓ Allowed

Esta tela é a mesma que a tela de configuração de permissões globais, exceto que estes valores só afetam a trabalhar com Usuários. Vejamos como isso funciona.

Primeiro, observe que o grupo Administrador tem a permissão Permitir para a ação do administrador, o grupo Manager tem permissão negada para esta ação. Lembre-se que a ação Admin na tela das Configurações Globais dá ao grupo permissões de "super utilizador". Nesta tela, a ação Admin permite que você edite os valores Opções. Assim, o grupo Administrador pode fazer isso, mas o grupo Gerenciador não pode.

Em seguida, observe que o Administrador tem Herdar para a ação Gerenciar eo grupo Gerenciador tem a permissão Negar. Nesta tela, a ação Gerenciar dá um acesso de grupo para o Gerenciador de usuários. Uma vez que o Administrador tem Permitir para a ação Gerenciar por padrão, então a permissão Herdar aqui significa que eles herdarão a permissão Permitir para a ação Gerenciar. Uma vez que o grupo Gerenciador tem a permissão Negar para a ação Gerenciar, membros do grupo gestor não pode acessar o Gerenciador de usuários e, portanto, não pode fazer qualquer uma das outras ações relacionadas ao usuário.

Se você olhar para as opções para o Gerenciador de Menus-> Menu, você vai ver as mesmas configurações padrão como para o Gerenciador de usuários. Mais uma vez, o grupo Administrador pode gerenciar e definir as permissões padrão para objetos gestor de menu enquanto o grupo Gerenciador não pode.

Em suma, podemos ver que as diferentes permissões para os grupos de administrador e gestor são definidas usando os Opções-> Permissões formas nas telas Gerenciador de

usuários e Gerenciador de Menu.

Também é importante compreender que esse mesmo Opções-> Permissões formar para definir permissões padrão está disponível para todos Joomla! objetos, incluindo o Media Manager, Banners, Contatos, Newsfeeds, Redirect, Pesquisa Estatística, Web Links, extensões, módulos, Plugins, Templates, e linguagem. Então, agora você tem a opção de criar grupos de usuários com conjuntos afinadas de permissões de back-end.

Permissões de Front-End

Permissões padrão para o front-end também são definidos através do formulário Opções. Vejamos Content-> Artigo Manager-> Opções> Permissões. Primeiro, vamos olhar para as permissões para Manager, como mostrado abaixo.

Article Manager Options

Save & Close

ArticlesCategoryCategoriesBlog / Featured LayoutsList LayoutsIntegrationText FiltersPermissions

Default permissions used for all content in this component.

Manage the permission settings for the user groups below. See notes at the bottom.

Public

Manager

Action	Select New Setting ¹	Calculated Setting ²
Configure	Inherited	Not Allowed
Access Component	Allowed	Allowed
Create	Inherited	Allowed
Delete	Inherited	Allowed
Edit	Inherited	Allowed
Edit State	Inherited	Allowed
Edit Own	Inherited	Allowed

Gerente permitiu permissão para todas as ações, exceto em Configurar. Assim, os membros do grupo Manager pode fazer tudo com os artigos exceto abrir a tela Opções.

Agora vamos olhar para o administrador, como mostrado abaixo.

► Public		
► Manager		
▼ Administrator		
Action	Select New Setting ¹	Calculated Setting ²
Configure	Allowed ▼	✓ Allowed
Access Component	Inherited ▼	✓ Allowed
Create	Inherited ▼	✓ Allowed
Delete	Inherited ▼	✓ Allowed
Edit	Inherited ▼	✓ Allowed
Edit State	Inherited ▼	✓ Allowed
Edit Own	Inherited ▼	✓ Allowed

Administrador tem permitido Configure, então os administradores podem editar esta tela Opções.

Ambos os grupos podem criar, excluir, editar e alterar o estado de artigos.

Agora, vamos olhar para a grupos Publisher, Editor, e Autor e ver como as suas permissões estão definidas.

Autores têm apenas Criar e editar permissões próprios, como mostrado abaixo.

▼ Author		
Action	Select New Setting ¹	Calculated Setting ²
Configure	Inherited ▼	⊖ Not Allowed
Access Component	Inherited ▼	⊖ Not Allowed
Create	Allowed ▼	✓ Allowed
Delete	Inherited ▼	⊖ Not Allowed
Edit	Inherited ▼	⊖ Not Allowed
Edit State	Inherited ▼	⊖ Not Allowed
Edit Own	Inherited ▼	✓ Allowed

Isto significa que os autores podem criar artigos e pode editar artigos que eles criaram. Eles não podem excluir os artigos, alterar o estado de artigos publicados, ou editar artigos criados por outros.

Editores têm as mesmas permissões Autores com a adição de permissão para a ação Editar, como mostrado abaixo.

▼ Editor		
Action	Select New Setting ¹	Calculated Setting ²
Configure	Inherited ▼	Not Allowed
Access Component	Inherited ▼	Not Allowed
Create	Inherited ▼	Allowed
Delete	Inherited ▼	Not Allowed
Edit	Allowed ▼	Allowed
Edit State	Inherited ▼	Not Allowed
Edit Own	Inherited ▼	Allowed

Então editores podem editar artigos escritos por qualquer pessoa.

Os editores podem fazer tudo Editores pode fazer além de terem a permissão para a ação Editar Estado, como mostrado abaixo.

▼ Publisher		
Action	Select New Setting ¹	Calculated Setting ²
Configure	Inherited ▼	Not Allowed
Access Component	Inherited ▼	Not Allowed
Create	Inherited ▼	Allowed
Delete	Inherited ▼	Not Allowed
Edit	Inherited ▼	Allowed
Edit State	Allowed ▼	Allowed
Edit Own	Inherited ▼	Allowed

Então Publishers pode mudar o estado publicado de um artigo. Os estados possíveis incluem Publicado, não publicado, arquivados, e Trashed.

Todos esses grupos têm permissão Herdar para Configurar e Access Component. Lembre-se que Autor é uma criança do grupo registrado, e não Registrada não tem nenhuma permissões padrão, exceto para Login. Desde Registrado não tem permissão para Configurar e Access Component, e desde que a permissão do autor para estas ações é "Herdado", então Autor não tem essas permissões também. Esta mesma permissão é passada de Autor para Editor e do Editor para Publisher. Então, por padrão, nenhum desses grupos têm permissão para trabalhar com artigos no back-end.

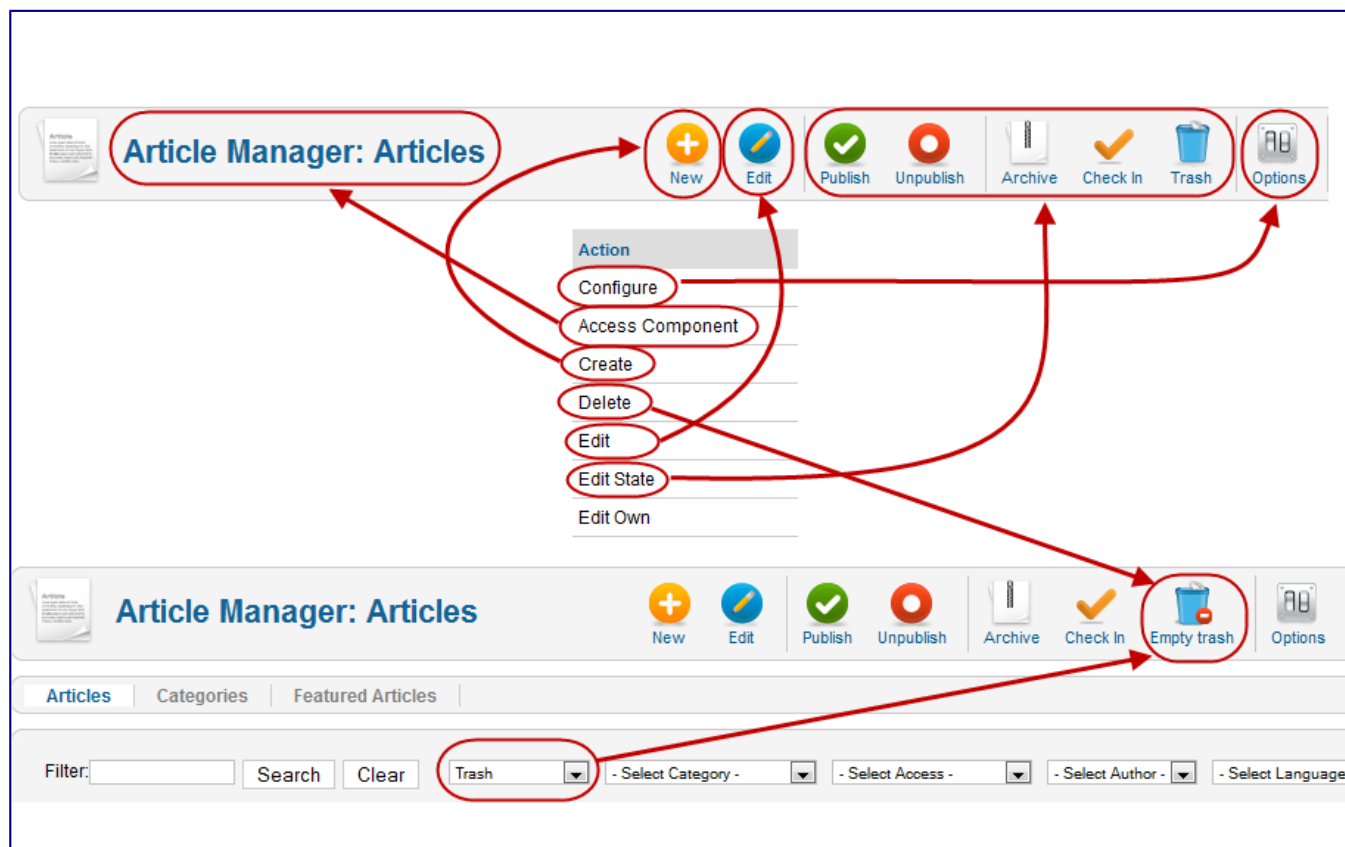
É importante lembrar que essas permissões são apenas configurações padrão para categorias e artigos e para quaisquer grupos filho que são criados. Assim, eles podem ser substituídos por grupos filhos, por categorias, e para artigos específicos.

Além disso, observe que não há permissões negadas para quaisquer ações nas configurações padrão. Isso permite que você adicione permissões permitidas em qualquer nível. Lembre-se, uma vez que você tem um conjunto de ações para negado, esta ação será negada a todos os níveis mais baixos da hierarquia. Por exemplo, se você definir o

Admin Login para Registered para negado (em vez de Herdado), você não poderia conceder permissões de estimacão Publishers para essa ação.

Artigo Manager & ações Diagrama

O diagrama abaixo mostra como cada ação na forma permissões relaciona-se com as várias opções na tela do Gerenciador de artigo.

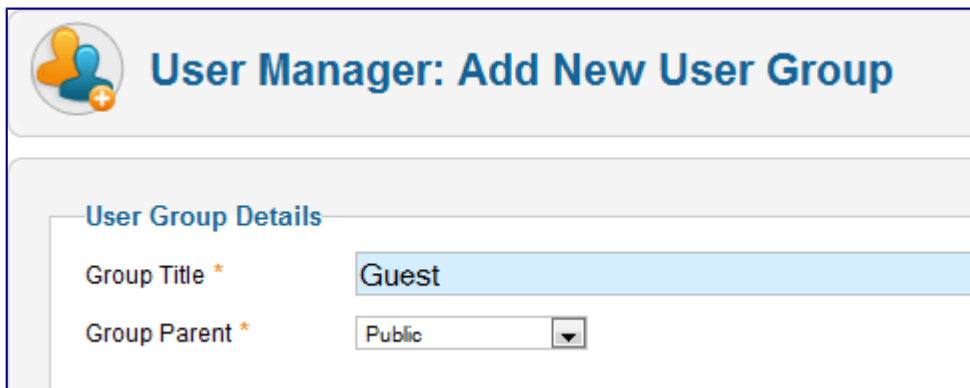


- **Configure** permite visualizar e alterar as opções para o componente.
- **Componente de acesso** permite que você navegue até o Gerenciador de artigo. Sem essa permissão, não são possíveis outras ações.
- **Criar** permite que você adicione novos artigos.
- **Excluir** permite excluir artigos lixeira. Observe que o ícone Excluir mostra apenas na barra de ferramentas quando você tem o filtro "Selecionar Estado" definida como "Trash".
- **Editar** permite editar artigos existentes.
- **Editar Estado** permite a você Publicar, Unpublish, Archive, ou artigos de lixo.
- **Editar própria** é o mesmo que Editar, exceto que ele só se aplica a artigos escritos por você.

Permitindo-Guest Apenas Acesso a itens do menu e Módulos

Versão 1.6 introduziu a capacidade de criar uma visualização de acesso nível que é apenas para os hóspedes do site (o que significa um usuário que não está logado). O exemplo abaixo mostra como você pode configurar esse novo recurso. *(NB Passos 1 a 3 não são necessários para 3.x Joomla! Como eles existem na instalação padrão*

1. Criar um novo grupo de usuários chamado Guest. Torná-lo um filho do grupo Public como mostrado abaixo.



The screenshot shows the 'User Manager: Add New User Group' interface. It features a header with a logo and the title. Below is a section titled 'User Group Details' containing two fields: 'Group Title' with the value 'Guest' and 'Group Parent' with a dropdown menu set to 'Public'.

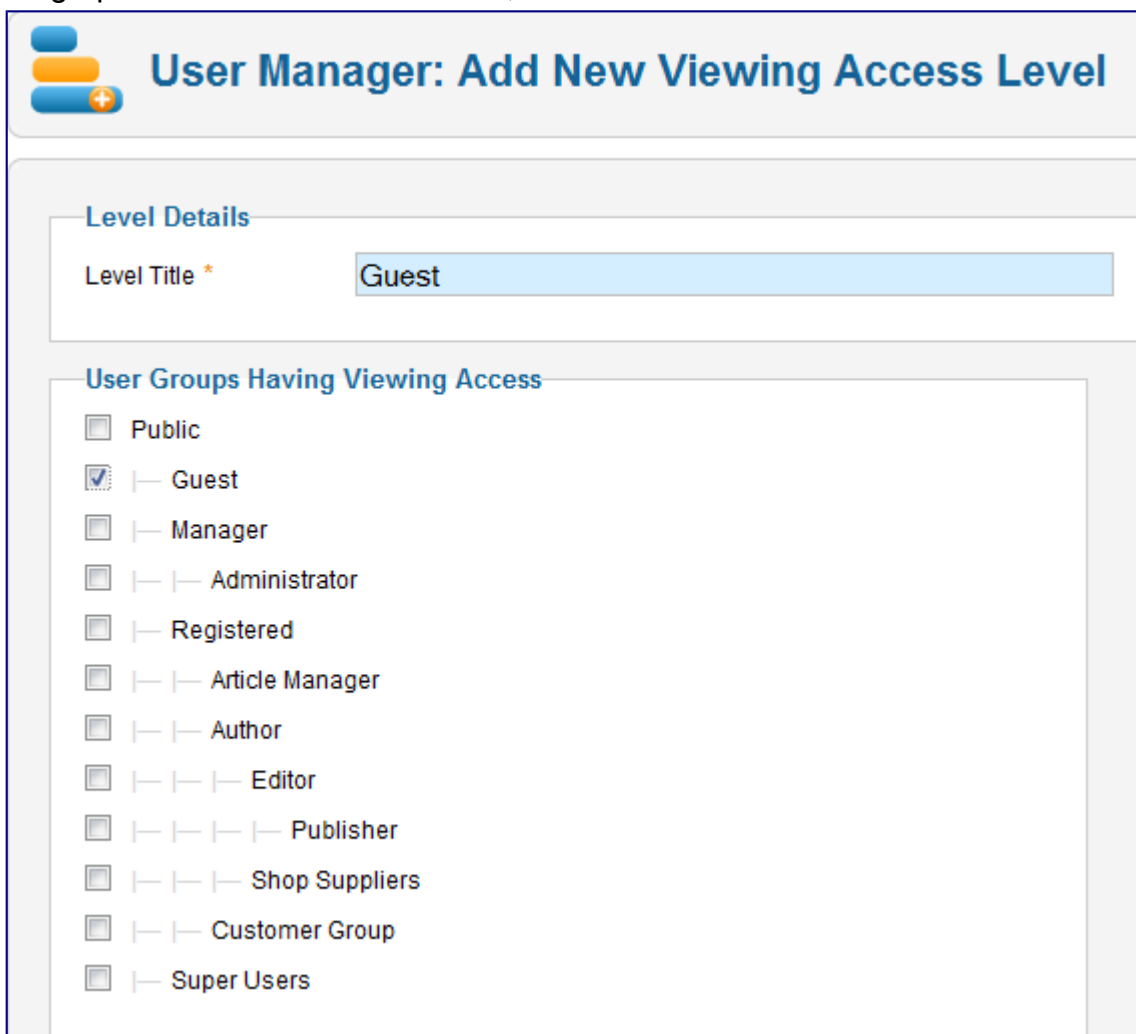
User Manager: Add New User Group

User Group Details

Group Title *

Group Parent * ▼

2. Criar um novo nível de acesso chamado de Clientes e conceder apenas o acesso do grupo dos visitantes a este nível, como mostrado abaixo.



The screenshot shows the 'User Manager: Add New Viewing Access Level' interface. It features a header with a logo and the title. Below is a section titled 'Level Details' with a 'Level Title' field set to 'Guest'. Underneath is a section titled 'User Groups Having Viewing Access' with a list of user groups, each with a checkbox. The 'Guest' group is checked.

User Manager: Add New Viewing Access Level


Level Details

Level Title *

User Groups Having Viewing Access

- ☐ Public
- ☒ Guest
- ☐ Manager
- ☐ Administrator
- ☐ Registered
- ☐ Article Manager
- ☐ Author
- ☐ Editor
- ☐ Publisher
- ☐ Shop Suppliers
- ☐ Customer Group
- ☐ Super Users

3. Navegue até Usuário Gerente → Opções → Component e mudar o Guest User Group a partir do valor padrão de "público" para "Guest", como mostrado abaixo.


Users Configuration

Component
Mass Mail
Permissions

Allow User Registration
☐ No
☒ Yes


New User Registration Group
- Registered

Guest User Group
- Guest

New User Account Activation
Self

Frontend User Parameters
☐ Hide
☒ Show

Agora, se atribuir um item de menu, módulo ou outro objeto para o nível de acesso dos visitantes, apenas para não-usuários logados terão acesso. Por exemplo, se criar um novo item de menu com o nível de acesso do Guest, como mostrado abaixo,


Menu Manager: New Menu Item

Details

Menu Item Type *
Single Article
Select

Menu Title *
Guest Only

Alias

Note

Link
index.php?option=com_content&view=article

State
Published

Access
Guest

Menu Location *
Main Menu

Parent Item
Menu Item Root

Target Window
Parent

Default Page
☒ No
☐ Yes

Language
All

Template Style
- Use Default -

ID
0

este item de menu só será visível para os visitantes não registrados no site.

Se necessários outros grupos de utilizadores como autor pode ser concedido o acesso no nível de acesso dos visitantes, isso permitiria que autores para ler artigos no front-end

para a edição.

NB login / logout na extremidade dianteira (*para mudar os dados na sessão*) para ver a alteração.

Usando Permissão e Níveis agrupar

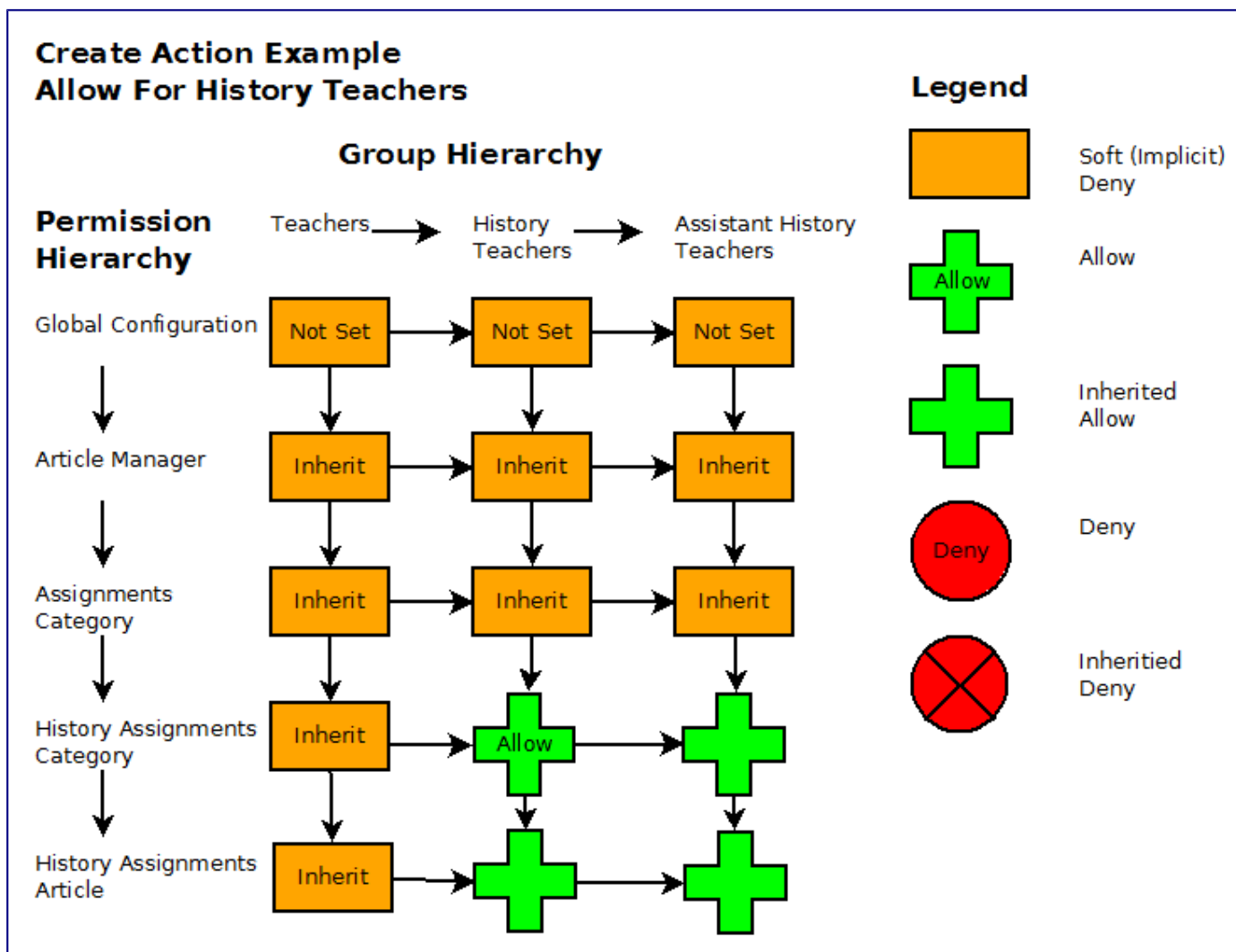
Como discutido acima, é possível definir grupos em uma hierarquia, onde cada grupo filho herda as permissões de ação (por exemplo, a permissão criar) de seu grupo pai.

Permissões de ação também são herdadas do nível de permissão acima. Por exemplo, uma permissão no Gerenciador de artigo é herdada da mesma permissão na configuração global, e uma permissão em uma Categoria filho é herdado do pai Categoria permissão.

Esta dupla herança pode ser confuso, mas também pode ser útil. Vamos considerar um exemplo a seguir. Temos uma escola com uma hierarquia de grupo de Professores de História → → Assistentes de Professores de História. Nós também temos uma hierarquia de categorias de Atribuições → História Atribuições. Queremos Professores de História e assistente de Professores de História de ter as seguintes permissões:

- ambos os grupos pode criar novos artigos somente na categoria Trabalhos de História.
- única Professores de História (não Assistentes de Professores de História) podem publicar ou não tem permissão Editar Estado.

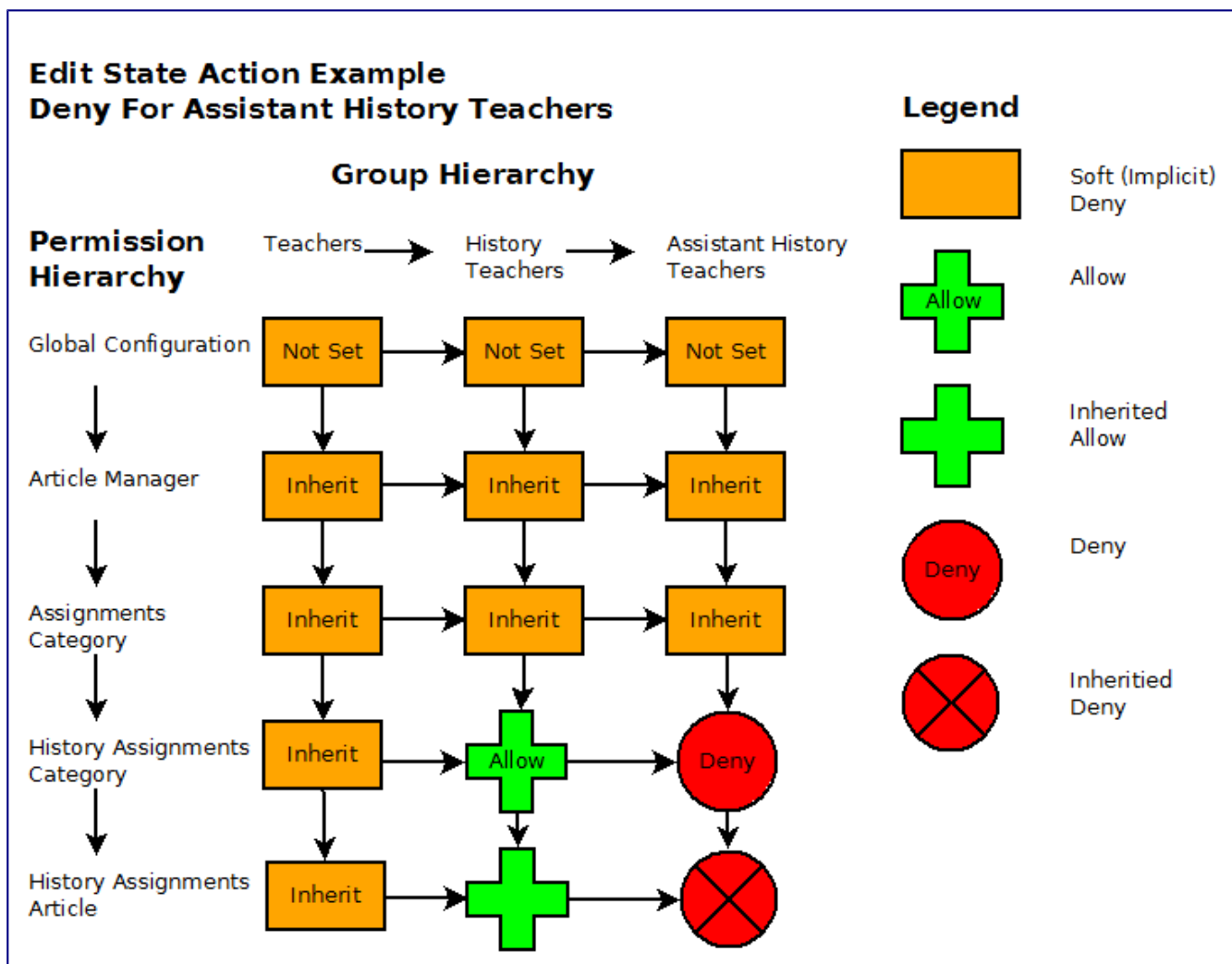
Este esquema de ACL é muito fácil de implementar. O diagrama abaixo mostra como isso seria configurado para a Ação Criar.



No diagrama, a Hierarquia permissão é mostrado pelo lado esquerdo ea hierarquia de grupo é mostrado na parte superior. As permissões são herdadas para baixo e para a direita, conforme mostrado pelas setas. Para implementar as permissões desejadas, deixamos a configuração global em branco (não definido) para os três grupos. Da mesma forma, no artigo Manager e Atribuições Categoria, deixamos a permissão Criar para Herdar para todos os grupos. Como mostrado no diagrama, isto significa que estes grupos não têm permissão para criar em artigos em geral ou para o grupo de artigos em Atribuições.

Para resumir, até agora, nós não definimos quaisquer permissões especiais para chegar a este ponto. Agora, na tela de permissões de categoria Trabalhos de História, nós definir a permissão Criar para Permitir para o grupo Professores de História. Esta definição substitui a Soft (implícita) Negar que tivemos por padrão e dá aos membros deste grupo permissão para criar conteúdo (artigos e categorias filho) para esta categoria. Esta configuração Permitir também é herdada pelo grupo Professores de História Assistant.

Em seguida, precisamos de conceder Professores de História a permissão Editar Estado ao negar essa permissão para Assistentes de Professores de História. Isto é feito como se mostra no diagrama a seguir.



Esta configuração é a mesma que a anterior excepto que desta vez, defina a permissão Editar Estado na categoria Trabalhos de História para Negar para o grupo Professores de História Assistant. Isto significa que professores assistentes de história não vai ser capaz de publicação e retirada artigos nesta categoria.

Note-se que este foi realizado, definindo apenas duas permissões na categoria Trabalhos de História: Permitir para o grupo Professores de História e Negar para o grupo Professores de História Assistant.

Exemplos de ações de permissão ACL

Aqui estão alguns exemplos de como você pode configurar a ACL para algumas situações específicas.

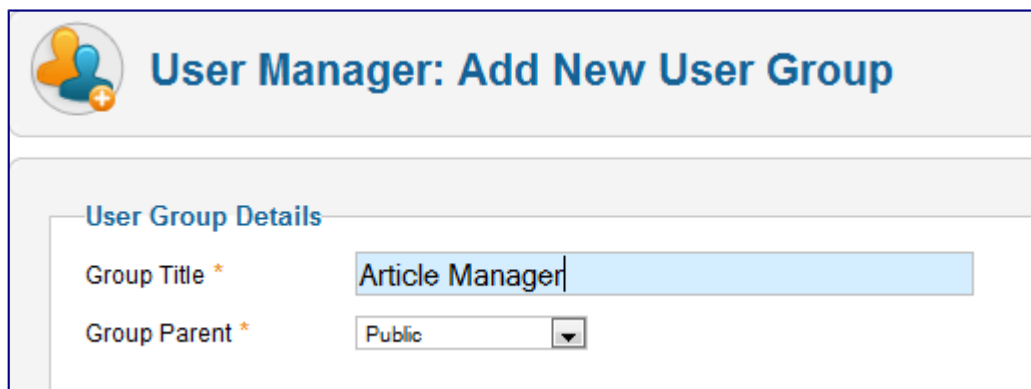
Back-end artigo Administrator

Problema:

Queremos criar um grupo chamado "artigo Administrator" com permissões de back-end só para artigos e não para quaisquer outras opções de menu de back-end. Os membros deste grupo deve ser capaz de usar todos os recursos do gerenciador de artigo, incluindo permissões artigo ajuste.

Solução:

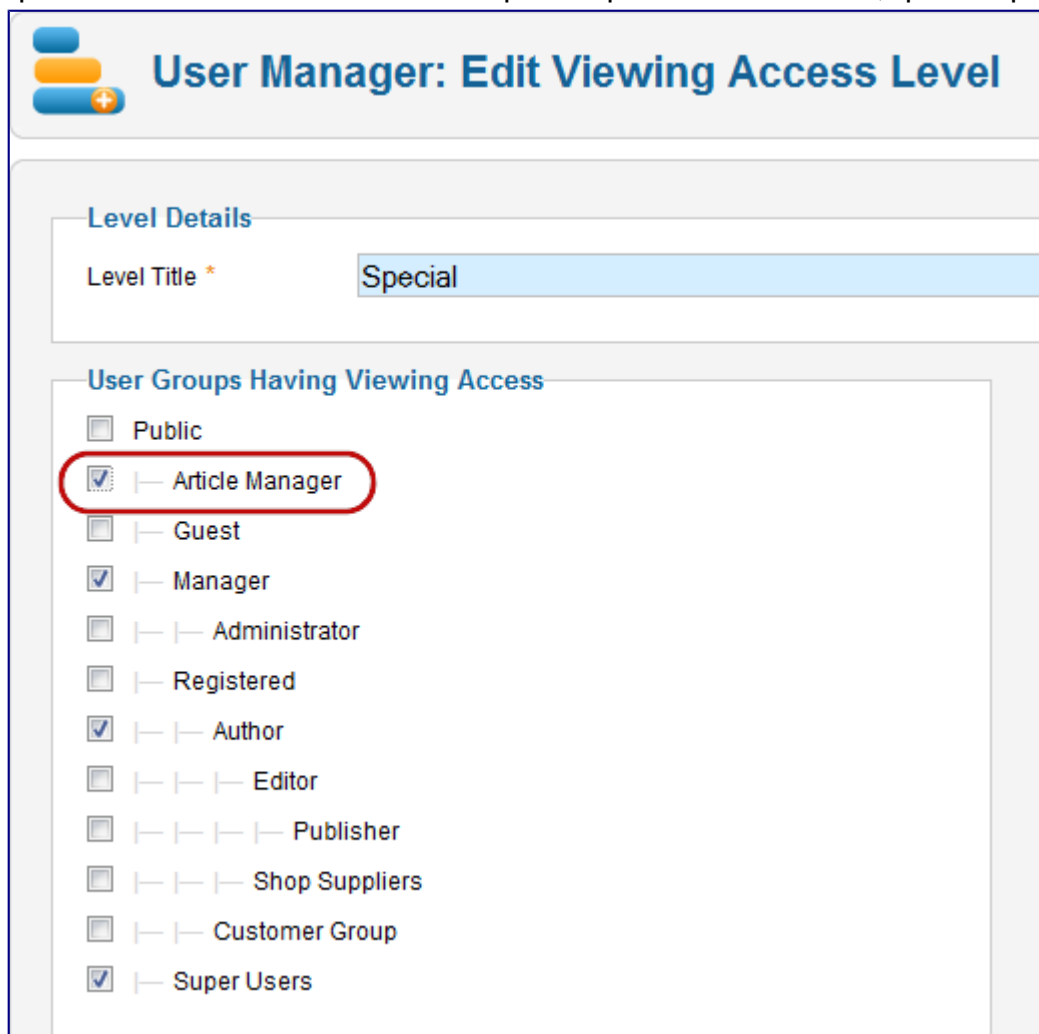
1. Criar um novo grupo chamado artigo Administrador e fazer seu grupo pai Pública, como mostrado abaixo.



The screenshot shows the 'User Manager: Add New User Group' interface. It features a header with a logo and the title. Below is a section titled 'User Group Details' containing two fields: 'Group Title' with the value 'Article Manager' and 'Group Parent' with a dropdown menu set to 'Public'.

Porque seu grupo pai é público, não terá quaisquer permissões por padrão.

2. Em Usuários → Níveis de Acesso, edite o nível de acesso especial para adicionar o novo grupo. Dessa forma, eles podem ter acesso aos itens de menu back-end e módulos (Isso pressupõe que os módulos para o menu de administração e quickicons ter o nível de acesso especial que lhes é atribuído, que é o padrão.)



The screenshot shows the 'User Manager: Edit Viewing Access Level' interface. It features a header with a logo and the title. Below is a section titled 'Level Details' with a 'Level Title' field set to 'Special'. Underneath is a section titled 'User Groups Having Viewing Access' which lists various user groups with checkboxes. The 'Article Manager' group is highlighted with a red circle and has its checkbox checked. Other groups include Public, Guest, Manager, Administrator, Registered, Author, Editor, Publisher, Shop Suppliers, Customer Group, and Super Users.

Por padrão, os itens de menu de back-end e os módulos estão definidos para acesso especial, por isso, se você esquecer de adicionar o novo grupo para o nível de acesso especial, você não vai ver todos os módulos ou itens de menu quando

você efetuar login como um usuário de o novo grupo.

3. No site de configuração global → → permissões, clique no grupo Administrador artigo e alterar as permissões para permitido para as seguintes ações: Admin Login, Criar, Apagar, Modificar, em Editar Estado, e Edite própria. A tela abaixo mostra o que irá mostrar antes de pressionar Salvar.

Global Configuration

Site | System | Server | **Permissions**

Permission Settings

Manage the permission settings for the user groups below. See notes at the bottom.

Public

Article Manager

Action	Select New Setting ¹	Calculated Setting ²
Site Login	Inherited	Not Allowed
Admin Login	Allowed	Not Allowed
Super Admin	Inherited	Not Allowed
Access Component	Inherited	Not Allowed
Create	Allowed	Not Allowed
Delete	Allowed	Not Allowed
Edit	Allowed	Not Allowed
Edit State	Allowed	Not Allowed
Edit Own	Allowed	Not Allowed

Depois de salvar, as Calculados As permissões devem mostrar como mostrado abaixo.

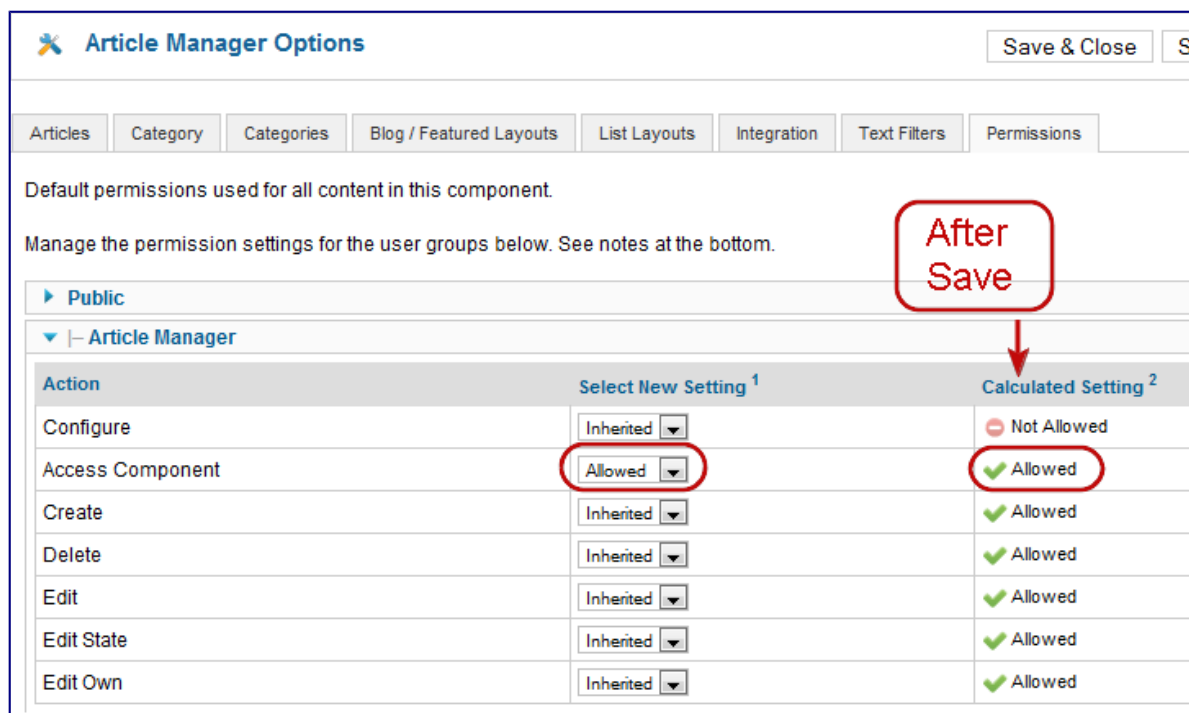
Article Manager

Action	Select New Setting ¹	Calculated Setting ²
Site Login	Inherited	Not Allowed
Admin Login	Allowed	Allowed
Super Admin	Inherited	Not Allowed
Access Component	Inherited	Not Allowed
Create	Allowed	Allowed
Delete	Allowed	Allowed
Edit	Allowed	Allowed
Edit State	Allowed	Allowed
Edit Own	Allowed	Allowed

Note-se que a permissão para o componente de acesso é herdada, que se traduz em não permitido. Isso é importante. Isto significa que este grupo só será capaz de acessar os componentes se dar ao grupo "permitido" a permissão para Componentes de Acesso. Então, só temos que mudar a um componente que queremos dar-lhes acesso e não tem que alterar as configurações para os componentes onde nós não queremos que eles tenham acesso. Se tivéssemos um

caso em que queria dar um acesso de grupo para tudo, exceto para um componente, podemos definir o padrão de estimação e, em seguida, definir o componente para uma negado. Observe também que nós não demos o grupo do site Entrada permissão, para que os usuários neste grupo não será capaz de fazer login no front end. (Se quiséssemos para permitir que, teríamos apenas mudar a permissão de estimação para o Site Login.)

4. Em Gerenciador de artigo → Opções → permissões, alterar as permissões para permitido para esse grupo para a ação de componentes Access, como mostrado abaixo.



Article Manager Options [Save & Close] [S...]

Articles | Category | Categories | Blog / Featured Layouts | List Layouts | Integration | Text Filters | Permissions

Default permissions used for all content in this component.

Manage the permission settings for the user groups below. See notes at the bottom.

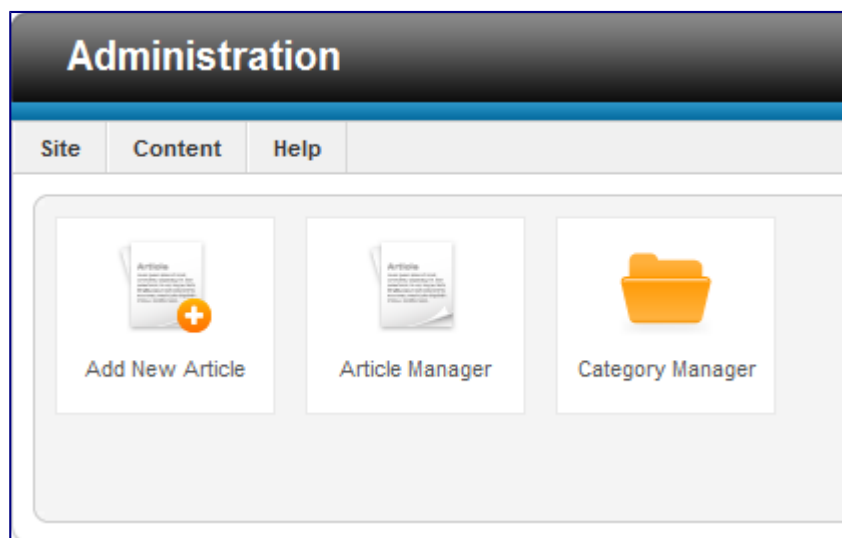
Public

Article Manager

Action	Select New Setting ¹	Calculated Setting ²
Configure	Inherited	Not Allowed
Access Component	Allowed	Allowed
Create	Inherited	Allowed
Delete	Inherited	Allowed
Edit	Inherited	Allowed
Edit State	Inherited	Allowed
Edit Own	Inherited	Allowed

Todas as outras permissões desejadas são herdadas.

Isso é tudo que você precisa fazer. Os membros desse grupo podem acessar o back-end e fazer tudo no artigo Manager, mas não pode fazer qualquer outra coisa no back-end. Por exemplo, a tela abaixo mostra o que um usuário no Gerenciador de artigo vai ver quando eles login para o back-end.



Níveis de acesso ACL Ver Exemplos

Um conceito básico da utilização de níveis de acesso é que todos os itens com o mesmo acesso poderá ser visto pelo mesmo grupo de usuários. Em outras palavras, se dois itens têm o mesmo acesso, você não pode ter um visível por um usuário e não podem ser visualizados por outro usuário. Por outro lado, é fácil ter uma visão Grupo qualquer número de itens com diferentes níveis de acesso.

Da mesma forma, cada grupo tem exatamente a mesma combinação de níveis de acesso, mas um usuário pode ser um membro de mais de um grupo. Dependendo da situação, você pode querer ter usuários em apenas um grupo ou você pode precisar de ter um usuário em mais de um grupo.

Isto significa que nós podemos precisar de grupo nossos artigos para que os itens de modo que todos os itens de um grupo têm o mesmo nível de sensibilidade. Aqui estão alguns exemplos.

Exemplo hierárquica

Neste exemplo, os níveis de acesso são hierárquicos, por exemplo, como códigos de habilitação de segurança do governo. Digamos, por exemplo, temos os seguintes conjuntos de documentos classificados: Classificada, Segredo, e Top Secret. Usuários têm correspondentes códigos clearance. Usuários com depuração Classificados só pode ver documentos classificados e não pode ver secreto ou Top Secret. Usuários com afastamento secreto pode ver documentos classificados e secreto, mas não Top Secret. Usuários com Top Secret pode ver todos os documentos.

Neste caso, você poderia criar três níveis de acesso: Classificada, Segredo, e Top Secret e os mesmos três grupos. Os usuários só seria membros de um grupo, como segue:

Do utilizador	Grupo	Níveis de Acesso
C1, C2, C3	Classificado	Classificado
S1, S2, S3	Segredo	Classificadas, Segredo
TS1, TS2, TS3	Confidencial	Classificadas, Segredo, Top Secret

Neste caso, todos os usuários estão em exatamente um grupo, mas alguns grupos têm acesso a mais de um nível de acesso de itens. Em outras palavras, temos um relacionamento um-para-um entre usuários e grupos, mas um relacionamento um-para-muitos entre os grupos e níveis de acesso.

Segurança Exemplo equipe

Outro caso de uso possível é um conjunto de equipes não-hierárquicas. Vamos dizer que nós temos três equipes, T1, T2 e T3. Alguns usuários estão apenas em um time, mas outros podem ser em duas ou mais equipes. Neste caso, podemos configurar os nossos níveis de acesso e grupos pela equipe. Documentos para cada equipe tem o nível de acesso para essa equipe, e do Grupo para a equipe tem apenas o nível de um acesso. Quando um usuário está em mais de uma equipe, eles são adicionados ao grupo para cada equipa, como segue:

Do utilizador	Descrição	Grupo	Níveis de Acesso
U1	Equipe 1 membro	T1	T1
U2	Team 2 membro	T2	T2
U3	Um membro da equipa 3	T3	T3
U1-2	Membro das equipas 1 e 2	T1, T2	T1, T2
U1-3	Membro das equipas de 1 e 3	T1, T3	T1, T3
U1-2-3	Membro das equipas de 1,2 e 3	T1, T2, T3	T1, T2, T3

Exemplo híbrido

Em uma situação do mundo real, você pode ter uma combinação destes dois acordos. Digamos, por exemplo, temos gerentes e funcionários. A equipe só pode ver documentos e gerentes da equipe podem ver documentos gerente e os funcionários. Ambos os tipos de usuários podem ser atribuídos a equipes bem, caso em que eles podem ver todos os documentos para essa equipe. Além disso, dizem que os gerentes podem acessar alguns, mas não todos, os documentos da equipe. A equipe só pode acessar documentos da equipe se eles são membros dessa equipe.

Neste exemplo, podemos configurar os seguintes níveis de acesso:

Nível de acesso	Descrição	Grupos
Gerente	Documentos gerente da equipe não-	Gerente
Funcionários	Non-equipe documentos de pessoal	Manager, Staff
Team1	Team1 documentos sensíveis (sem acesso fora da equipe)	Team1
Team1-Manager	Team1 documentos que podem ser acessados por todos os gestores	Team1, Gerente
Team2	Team2 documentos sensíveis (sem acesso fora da equipe)	Team2
Team2-Manager	Team2 documentos que podem ser acessados por todos os gestores	Team2, Gerente

Em seguida, os usuários podem ser atribuídos a grupos como segue:

Tipo de usuário	Grupo
Manager em nenhuma equipe	Gerente
A equipe em nenhuma equipe	Funcionários
Manager na equipa 1	Manager, Team1
A equipe na equipa 1	Staff, Team1
Manager em equipes 1 e 2	Manager, Team1, Team2
Os funcionários em equipes 1 e 2	Staff, Team1, Team2

Fontes:

<http://magazine.joomla.org/issues/issue-aug-2012/item/825-A-Case-for-Role-Based-ACL>

https://docs.joomla.org/J3.x:Access_Control_List_Tutorial