

Overview of ACL in Version  3.x  
(/File:Compat icon 3 x.png)

This section outlines any major ACL changes between versions 2.5 and the 3.0 series (which will include future releases). The table below summarizes the any changes from version 2.5.

	Version 2.5	Version 3.4
<b>Groups</b>	Unlimited user-defined Groups	Same as 2.5
<b>Users &amp; Groups</b>	A User can be assigned to multiple groups	Same as 2.5
<b>Access Levels</b>	Unlimited user-defined Access Levels	Same as 2.5
<b>Access Levels &amp; Groups</b>	Groups are assigned to Access Levels. Any combination of Groups can be assigned to any Access Level.	Same as 2.5

### Separate ACL for Viewing and Doing

The Joomla ACL system can be thought of as being divided into two completely separate systems. One system controls what things on the site users can view. The other controls what things users can *do* (what actions a user can take). The ACL for each is set up differently.

## Controlling What Users Can See

The setup for controlling what users can see is done as follows:

- Create a set of Access Levels according to the Categories and/or the combination of categories you wish only logged in users to see. N.B do not assign any user groups to the **new** Access Levels at this point.
- Create a User Group, with 'Registered' as parent, for each Access Level. Using the same names for the User Groups as the Access Levels will prevent confusion later.
- Edit your new Access Levels and assign the correct (new) User Group to each one. You may also wish to assign the Super User Group(and/or the other default User Groups but not 'Guest' User Group) to all your new Access Levels
- Assign each item to be viewed to one Access Level. Items include content items (articles, contacts, and so on), menu items, and modules.

Any time a user is about to view an item on a Joomla page, the program checks whether the user has access to the item, as follows:

1. Creates a list of all the Access Levels that the User has access to, based on all Groups that the User belongs to. Also, if a group has a parent group, access levels for the parent group are also included in the list.
2. Checks whether the Access Level for the item (article, module, menu item, and so on) is on that list. If yes, then the item is displayed to the user. If no, then the item is not displayed.

Note that Access Levels are set separately for each Group and are not inherited from a group's parent group.

## Controlling What Users Can Do

The system for setting up what users in a User Group can do -- what actions they can take on a given item -- is set up with the Permissions tab of Global Configuration and the Permissions tab of the Options screen of each component. Permissions can also be set up at the Category level for core components and at the Article level for articles.

- If you wish logged in users to Create, Delete, Edit State or Edit Own for specific Categories then:
  - Create a User Group with the Parent as one of your User Groups that has Access to the Category(or Categories) you wish this new User Group to modify.
  - Assign your new User Group to the appropriate Access Level(s). Then change the required permissions for your new user Group either Globally or per Category/Article.
    - When creating a User Group it is good practice to select a parent group that has less permissions than needed for the new group. This is because it is easier to elevate permissions per Component/Category/Article that the extra permissions are needed for than it is to remove permissions from the other Components/Categories/Articles.
      - (example: You have 10 Categories but you want Create permissions for just 1. If you set Global permissions to Allow Create for that group you would need to remove Create permission for all those categories. And you would need to remove the Create permission for that group with any new Category that you add at a later date.)
  - Only create a User Group with one of the default User Groups as parent if none of them have the exact permissions that you need and you wish all Categories

Note that this set up is independent of the setup for viewing but a User Group needs to be assigned to the appropriate Access Level(s) in order for the user in that Group to use those Permissions.

When a user wants to initiate a specific action against a component item (for example, edit an article), the system (after checking the Group the user is in has access) checks the permission for this combination of user, item, and action. If it is allowed, then the user can proceed. Otherwise, the action is not allowed.

The remainder of this tutorial discusses how we control what users can do – what action permissions they have.

## Actions, Groups, and Inheritance

The other side of ACL is granting permissions to users to take actions on objects.

	<b>3.x series</b>
<b>Groups and Actions</b>	Actions allowed for each group are defined by site administrator.
<b>Permission Scope</b>	Permissions can be set at multiple levels in hierarchy: Site, Component, Category, Object.
<b>Permission Inheritance</b>	Permissions can be inherited from parent Groups and parent Categories.

## How Permissions Work

- There are four possible permissions for actions, as outlined below:
- **Not set:** Defaults to "deny" but, unlike the Deny permission, this permission can be overridden by setting a child group or a lower level in the permission hierarchy to "Allow". This permission only applies to the Global Configuration permissions.
  - **Inherit:** Inherits the value from a parent Group or from a higher level in the permission hierarchy. This permission applies to all levels except the Global Configuration level.
  - **Deny:** Denies this action for this level and group. **IMPORTANT:** This also denies this action for all child groups and all lower levels in the permission hierarchy. Putting in Allow for a child group or a lower level will not have any effect. The action will always be denied for any child group member and for any lower level in the permission hierarchy.
  - **Allow:** Allows this action for this level and group and for lower levels and child groups. This does not have any effect if a higher group or level is set to Deny or Allow. If a higher group or level is set to Deny, then this permission will always be denied. If a higher group or level is set to Allow, then this permission will already be allowed.

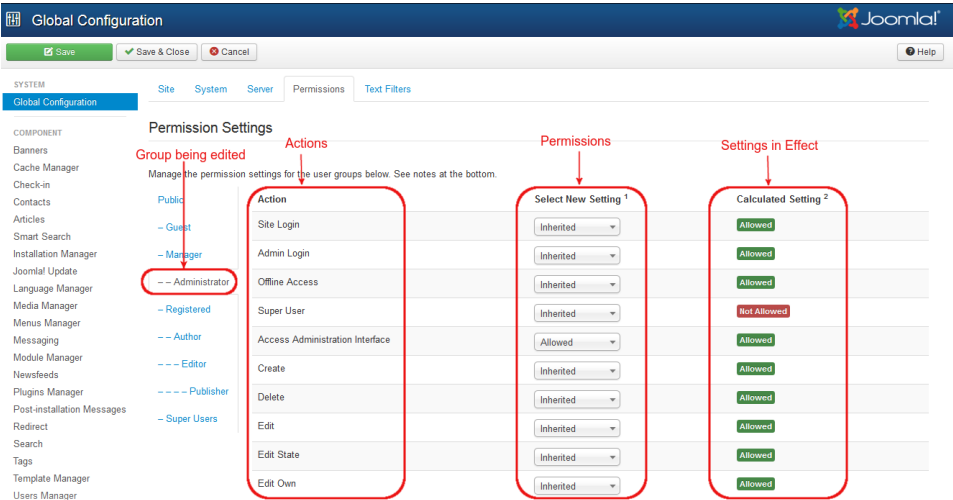
Permission Hierarchy Levels

Action permissions in version 2.5 can be defined at up to four levels, as follows:

1. **Global Configuration:** determines the default permissions for each action and group.
2. **Component Options->Permissions:** can override the default permissions for this component (for example, Articles, Menus, Users, Banners, and so on)
3. **Category:** can override the default permissions for objects in one or more categories. Applies to all components with categories, including Articles, Banners, Contacts, Newsfeeds, and Weblinks.
4. **Article:** Can override the permissions for a specific article. This level only applies to articles. Other components only allow the first three levels.

Global Configuration

This is accessed from Site → Global Configuration → Permissions. This screen allows you set the top-level permission for each group for each action, as shown in the screenshot below.



(/File:Screenshot\_global\_acl\_J3\_tutorial.jpg)

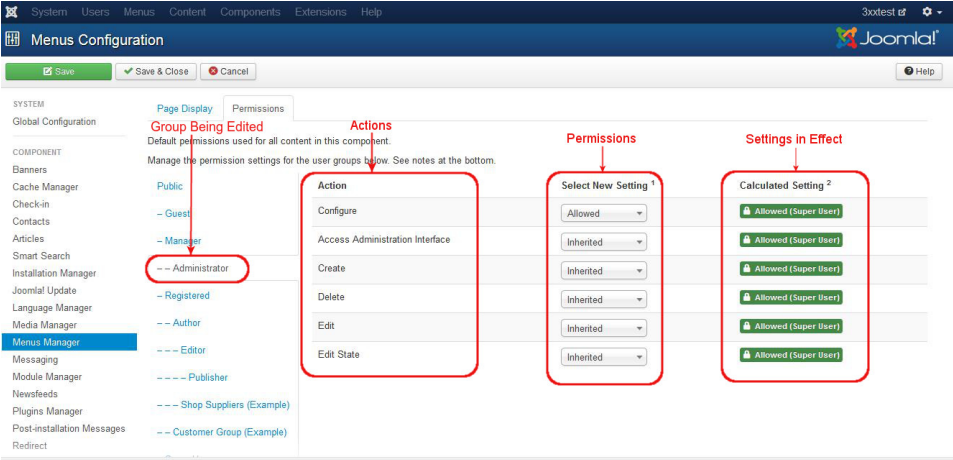
The options for each value are Inherited, Allowed, or Denied. The Calculated Setting column shows you the setting in effect. It is either Not Allowed (the default), Allowed, or Denied.

You work on one Group at a time by opening the slider for that group. You change the permissions in the Select New Settings drop-down list boxes.

Note that the Calculated Setting column is not updated until you press the Save button in the toolbar. To check that the settings are what you want, press the Save button and check the Calculated Settings column.

Component Options->Permissions

This is accessed for each component by clicking the Options icon in the toolbar. This screen is similar to the Global Configuration screen above. For example, clicking the Options toolbar icon in the Menu Manager shows the Menus Configuration below.

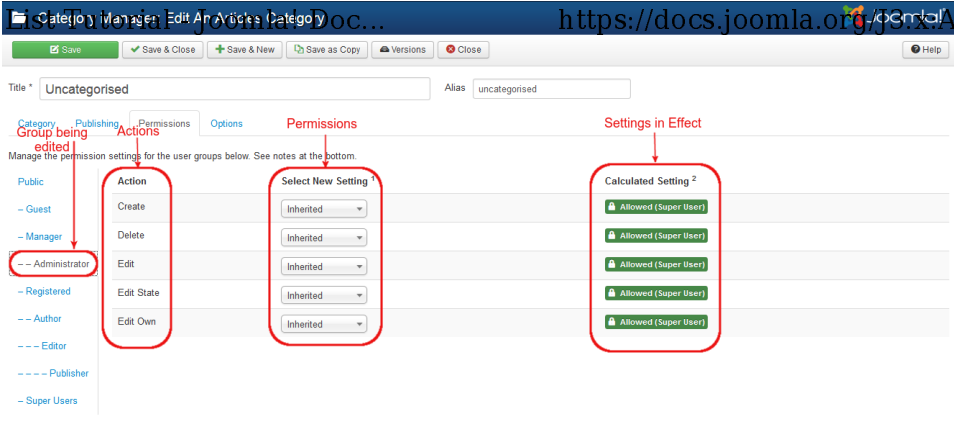


(/File:Screenshot\_menu\_acl\_J3\_tutorial.jpg)

Access to Options is only available to members of groups who have permission for the Configure action in for each component. In the example above, the Administrator group has Allowed permission for the Configure option, so members of this group can access this screen.

Category

Category permissions are accessed in the Category Manager: Edit Category screen, in a tab at the top of the screen. This screen has five permissions, as shown below.



(/File:Screenshot\_category\_acl\_j3\_tutorial.png)

In these screens, you work on the permissions for one User Group at a time. In the example above, we are editing the permissions for the Administrator group.

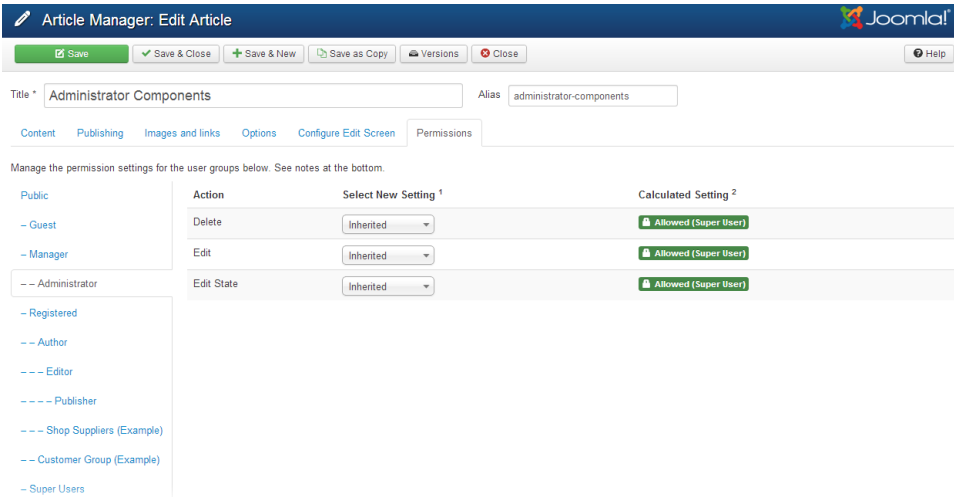
Note that the Configure and Access Component actions do not apply at the category level, so those actions are not included.

Note also that Categories can be arranged in a hierarchy. If so, then action permissions in a parent category are inherited automatically by a child category. For example, if you had a category hierarchy of Animals --> Pets --> Dogs, then the full permission level hierarchy for an article in the Dogs category would be as follows:

- Global Configuration
- Article Manager --> Options --> Permission
- Animals Category
- Pets Category
- Dogs Category
- specific article

Article

Permissions for a single article are access in the Article Manager: Edit Article screen, again in a slider at the bottom of the screen. This screen has three actions, as shown below.



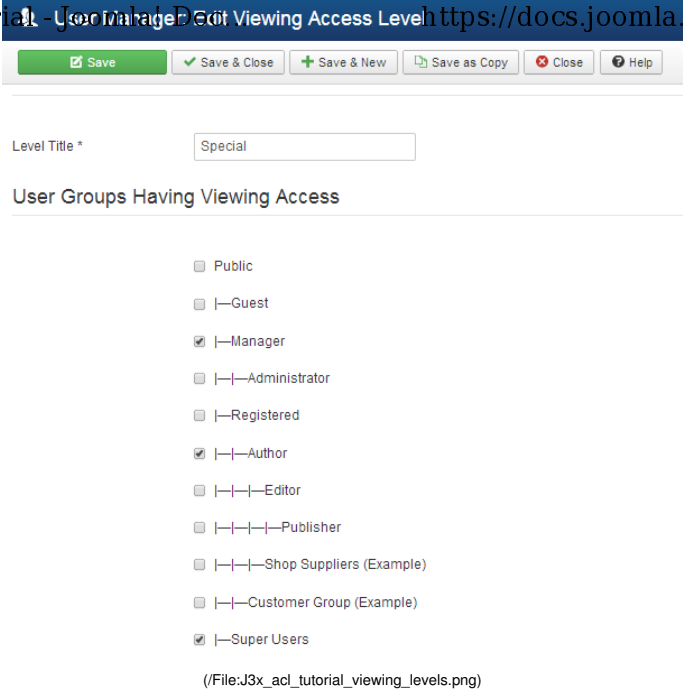
(/File:J3x\_acl\_tutorial\_article\_manager\_article\_permissions.png)

Again, you edit each group by clicking on it to open the slider for that group. You can then change the permissions under the Select New Setting column. To see the effect of any changes, press the Save button to update the Calculated Setting column.

Note that the Configure, Access Component, and Create actions do not apply at the article level, so these actions are not included. Permission to create an article is set at one of the higher levels in the hierarchy.

Access Levels

Access Levels in 3.x series are simple and flexible. The screen below shows the Special Access Level.

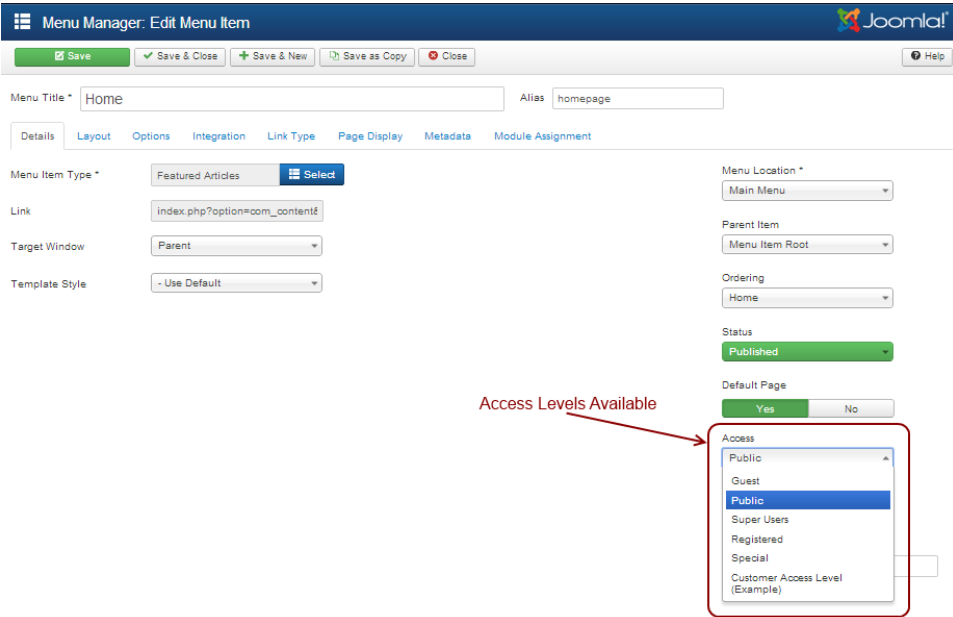


(/File:J3x\_acl\_tutorial\_viewing\_levels.png)

Simply check the box for each group you want included in that level. The Special Access Level includes the Manager, Author, and Super Users groups. It also includes child groups of those groups. So, Administrator group is included, since it is a child group of the Manager group. The Editor, Publisher, and Shop Suppliers groups are included, since they are child groups of Author. (Note that we could check all of the child groups if we wanted and it wouldn't hurt anything.)

Once Access Levels are created, they are used in the same way as in version 1.5. Each object in the front end is assigned an Access Level. If the level is Public, then anyone may access that object. Otherwise, only members of groups assigned to that access level may access that object. Access levels are assigned to Menu Items and to Modules. Each one can only be assigned to one access level.

For example, the screen below shows the Edit Menu Item screen with the list of available access levels.



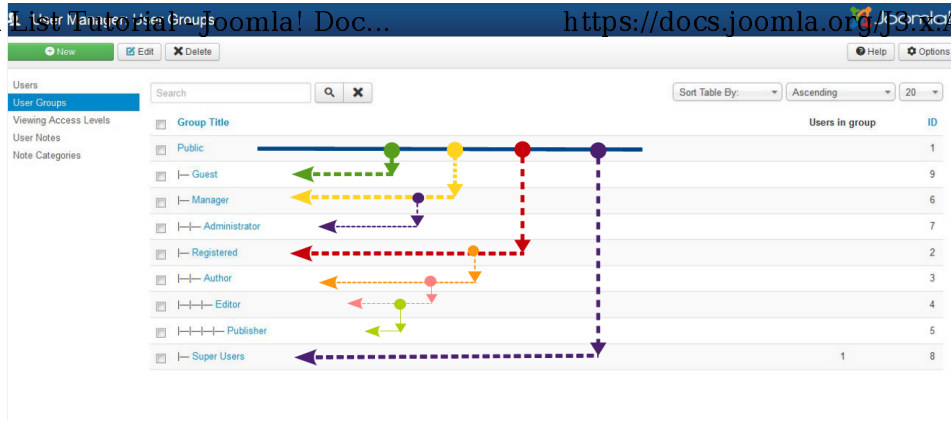
(/File:J3x\_acl\_tutorial\_edit\_menu\_item\_level\_dropdown.png)

Default ACL Setup

When Joomla! is installed, these are set to their initial default settings. We will discuss these initial settings as a way to understand how the ACL works.

Default Groups

Version 3.x allows you to define your own Groups. When you install version 3.x, it includes a set of default groups, shown below are the basic default user groups. (Additional default user groups are installed with sample data)



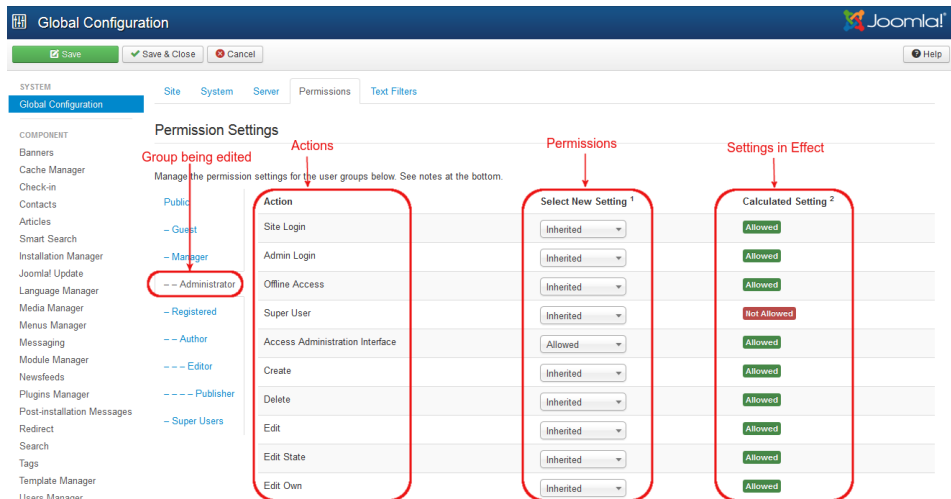
(/File:Screenshot\_usergroups\_acl\_J3\_tutorial.png)

The arrows indicate the child-parent relationships. As discussed above, when you set a permission for a parent group, this permission is automatically inherited by all child groups. The Inherited, and Allowed permissions can be overridden for a child group. The Denied permission cannot be overridden and will always deny an action for all child groups.

## Global Configuration

Joomla! version 2.5 will install with the same familiar back-end permissions as that of version 1.5. However, with 2.5, you can easily change these to suit the needs of your site.

As discussed earlier, the permissions for each action are inherited from the level above in the permission hierarchy and from a group's parent group. Let's see how this works. The top level for this is the entire site. This is set up in the Site->Global Configuration->Permissions, as shown below.



(/File:Screenshot\_global\_acl\_J3\_tutorial.jpg)

The first thing to notice are the nine Actions: Site Login, Admin Login, Super Admin, Access Component, Create, Delete, Edit, Edit State, and Edit Own. These are the actions that a user can perform on an object in Joomla. The specific meaning of each action depends on the context. For the Global Configuration screen, they are defined as follows:

### Site Login

Login to the front end of the site

### Admin Login

Login to the back end of the site

### Super Admin

Grants the user "super user" status. Users with this permission can do anything on the site. Only users with this permission can change Global Configuration settings (this screen). These permissions cannot be restricted. It is important to understand that, if a user is a member of a Super Admin group, any other permissions assigned to this user are irrelevant. The user can do any action on the site. However, Access Levels can still be assigned to control what this group sees on the site. (Obviously, a Super Admin user can change Access Levels if they want to, so Access Levels do not totally restrict what a Super Admin user can see.)

### Access Component

Open the component manager screens (User Manager, Menu Manager, Article Manager, and so on)

### Create

Create new objects (for example, users, menu items, articles, weblinks, and so on)

### Delete

Delete existing objects

### Edit

Edit existing objects

### Edit State

Change object state (Publish, Unpublish, Archive, and Trash)

### Edit Own

Edit objects that you have created.

Each Group for the site has its own slider which is opened by clicking on the group name. In this case (with the sample data installed), we have the standard 7 groups that we had in version 1.5 plus two additional groups called "Shop Suppliers" and "Customer Group". Notice that our groups are set up with the same permissions as they had in version 1.5. Keep in mind that we can change any of these permissions to make the security work the way we want. Let's go through this to see how it works.

Public has everything set to "Not set", as shown below.

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

(/File:Screenshot\_global\_acl\_public\_J3\_tutorial.png)

- This can be a bit confusing. Basically, "Not Set" is the same as "Inherited". Because Public is our top-level group, and because Global Configuration is the top level of the component hierarchy, there is nothing to inherit from. So "Not Set" is used instead of "Inherit".
- The default in this case is for no permissions. So, as you would expect, the Public group has no special permissions. Also, it is important to note that, since nothing is set to Denied, all of these permissions may be overridden by child groups or by lower levels in the permission hierarchy.

- Guest** is a 'child' group of the Public group has everything set to 'Inherited'

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

(/File:Screenshot\_global\_acl\_guest\_J3\_tutorial.png)

- This is the default 'Guest User Group' in the User Manager options and the Group that (non logged in) visitors to your site are placed in.

- Manager** is a "child" group of the Public group. It has Allowed permissions for everything except Access Component and Super Admin. So a member of this group can do everything in the front and back end of the site except change Global Permissions and Component Options.

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

(/File:Screenshot\_global\_acl\_manager\_J3\_tutorial.png)

- Administrator** group members inherit all of the Manager permissions and also have Allowed for Access Component. So members of this group by default can access the Options screens for each component.

The screenshot shows the Joomla! Global Configuration interface, specifically the 'Permission Settings' tab. The left sidebar lists various components, with 'Administrator' highlighted. The main table displays permissions for the 'Administrator' group. The 'Select New Setting' column is circled in red, and a red arrow points to the 'Administrator' group in the left sidebar.

Action	Select New Setting <sup>1</sup>	Calculated Setting <sup>2</sup>
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

(/File:Screenshot\_global\_acl\_administrator\_J3\_tutorial.png)

- Registered** is the same as Public except for the Allow permission for the Site Login action. This means that members of the Registered group can login to the site. Since default permissions are inherited, this means that, unless a child group overrides this permission, all child groups of the Registered group will be able to login as well.

The screenshot shows the Joomla! Global Configuration interface, specifically the 'Permission Settings' tab. The left sidebar lists various components, with 'Registered' highlighted. The main table displays permissions for the 'Registered' group. The 'Select New Setting' column is circled in red, and a red arrow points to the 'Registered' group in the left sidebar.

Action	Select New Setting <sup>1</sup>	Calculated Setting <sup>2</sup>
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

(/File:Screenshot\_global\_acl\_registered\_J3\_tutorial.png)

- Author** is a child of the Registered group and inherits its permissions and also adds Create and Edit Own. Since Author, Editor, and Publisher have no back-end permissions, we will discuss them below, when we discuss front-end permissions.

The screenshot shows the Joomla! Global Configuration interface, specifically the 'Permission Settings' tab. The left sidebar lists various components, with 'Author' highlighted. The main table displays permissions for the 'Author' group. The 'Select New Setting' column is circled in red, and a red arrow points to the 'Author' group in the left sidebar.

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

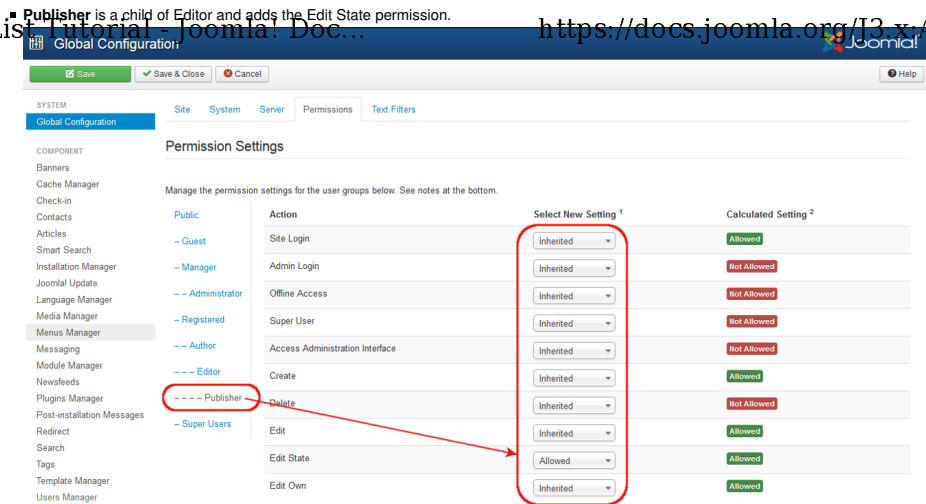
(/File:Screenshot\_global\_acl\_author\_J3\_tutorial.png)

- Editor** is a child of the Authors group and adds the Edit permission.

The screenshot shows the Joomla! Global Configuration interface, specifically the 'Permission Settings' tab. The left sidebar lists various components, with 'Editor' highlighted. The main table displays permissions for the 'Editor' group. The 'Select New Setting' column is circled in red, and a red arrow points to the 'Editor' group in the left sidebar.

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

(/File:Screenshot\_global\_acl\_editor\_J3\_tutorial.png)



(/File:Screenshot\_global\_acl\_publisher\_j3\_tutorial.png)

- **Publisher** is a child of Editor and adds the Edit State permission.
- **Shop Suppliers** is an example group that is installed if you install the sample data. It is a child group of Author.
- **Customer Group** is an example group that is installed if you install the sample data. It is a child group of Registered.
- **Super Users** group has the Allow permission for the Super Admin action. Because of this, members of this group have super user permissions throughout the site. They are the only users who can access and edit values on the Global Configuration screen. Users with permission for the Super Admin action have some special characteristics:
  - If a user has Super Admin permissions, no other permissions for this user matter. The user can perform any action on the site.
  - Only Super Admin users can create, edit, or delete other Super Admin users or groups.

There are two very important points to understand from this screen. The first is to see how the permissions can be inherited from the parent Group. The second is to see how you can control the default permissions by Group and by Action.

This provides a lot of flexibility. For example, if you wanted Shop Suppliers to be able to have the ability to login to the back end, you could just change their Admin Login value to "Allowed". If you wanted to not allow members of Administrator group to delete objects or change their state, you would change their permissions in these columns to Inherited (or Denied).

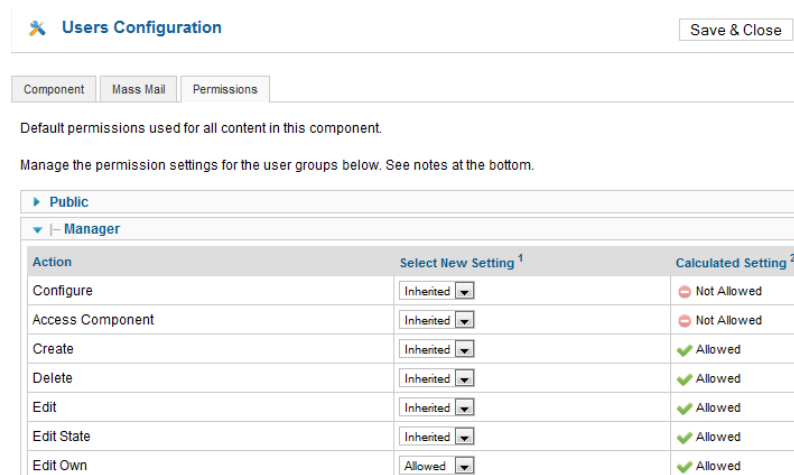
It is also important to understand that the ability to have child groups is completely optional. It allows you to save some time when setting up new groups. However, if you like, you can set up all groups to have Public as the parent and not inherit any permissions from a parent group.

## Component Options & Permissions

Now, let's continue to see how the default back-end permissions for version 2.5 mimic the permissions for version 1.5. The Super Users group in 2.5 is equivalent to the Super Administrator group in 1.5.

Just looking at the Global Configuration screen above, it would appear that the Administrator group and the Manager group have identical permissions. However, in version 1.5 Administrators can do everything except Global Configuration, whereas Managers are not permitted to add users or work with menu items. That is also true in the default version 2.5 configuration. Let's see how this is accomplished.

If we navigate to Users->User Manager and click the Options button in the toolbar, we see the screen below:



(/File:Screenshot\_acl\_tutorial\_20110111-09.png)

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 <sup>1</sup>	Calculated Setting <sup>2</sup>
Configure	Allowed	Allowed
Access Component	Inherited	Allowed
Create	Inherited	Allowed
Delete	Inherited	Allowed
Edit	Inherited	Allowed
Edit State	Inherited	Allowed
Edit Own	Inherited	Allowed

(/File:Screenshot\_acl\_tutorial\_20110111-10.png)

This screen is the same as the Global Configuration Permissions screen, except that these values only affect working with Users. Let's look at how this works.

First, notice that the Administrator group has Allow permission for the Admin action and the Manager group has Deny permission for this action. Remember that the Admin action in the Global Configuration screen gives the group "super user" permissions. In this screen, the Admin action allows you to edit the Options values. So, the Administrator group can do this but the Manager group cannot.

Next, notice that the Administrator has Inherit for the Manage action and the Manager group has Deny permission. In this screen, the Manage action gives a group access to the User Manager. Since the Administrator has Allow for the Manage action by default, then the Inherit permission here means they inherit the Allow permission for the Manage action. Since the Manager group has Deny permission for the Manage action, members of the Manager group cannot access the User Manager and therefore cannot do any of the other user-related actions.

If you look at the Options for Menus->Menu Manager, you will see the same default settings as for the User Manager. Again, the Administrator group can manage and set default permissions for Menu Manager objects whereas the Manager group cannot.

In short, we can see that the different permissions for the Administrator and Manager groups are set using the Options->Permissions forms on the User Manager and Menu Manager screens.

It is also important to understand that this same Options->Permissions form for setting default permissions is available for all Joomla! objects, including Media Manager, Banners, Contacts, Newsfeeds, Redirect, Search Statistics, Web Links, Extensions, Modules, Plugins, Templates, and Language. So you now have the option to create user groups with fine-tuned sets of back-end permissions.

Front End Permissions

Default permissions for the front end are also set using the Options form. Let's look at Content->Article Manager->Options->Permissions. First, let's look at the permissions for Manager, as shown below.

Article Manager Options

Save & Close

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

Manager

Action	Select New Setting <sup>1</sup>	Calculated Setting <sup>2</sup>
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

(/File:Screenshot\_acl\_tutorial\_20110111-11a.png)

Manager has allowed permission for all actions except Configure. So members of the Manager group can do everything with Articles except open the Options screen.

Now let's look at Administrator, as shown below.

Public

Manager

Administrator

Action	Select New Setting <sup>1</sup>	Calculated Setting <sup>2</sup>
Configure	Allowed	Allowed
Access Component	Inherited	Allowed
Create	Inherited	Allowed
Delete	Inherited	Allowed
Edit	Inherited	Allowed
Edit State	Inherited	Allowed
Edit Own	Inherited	Allowed

(/File:Screenshot\_acl\_tutorial\_20110111-12a.png)

Administrator has Allowed for Configure, so Administrators can edit this Options screen.

Both groups can create, delete, edit, and change the state of articles.

▼ Author		
Action	Select New Setting <sup>1</sup>	Calculated Setting <sup>2</sup>
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

(/File:Screenshot\_acl\_tutorial\_20110112-07.png)

This means that Authors can create articles and can edit articles they have created. They may not delete articles, change the published state of articles, or edit articles created by others.

Editors have the same permissions as Authors with the addition of permission for the Edit action, as shown below.

▼ Editor		
Action	Select New Setting <sup>1</sup>	Calculated Setting <sup>2</sup>
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

(/File:Screenshot\_acl\_tutorial\_20110112-08.png)

So Editors can edit articles written by anyone.

Publishers can do everything Editors can do plus they have permission for the Edit State action, as shown below.

▼ Publisher		
Action	Select New Setting <sup>1</sup>	Calculated Setting <sup>2</sup>
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

(/File:Screenshot\_acl\_tutorial\_20110112-09.png)

So Publishers can change the published state of an article. The possible states include Published, Unpublished, Archived, and Trashed.

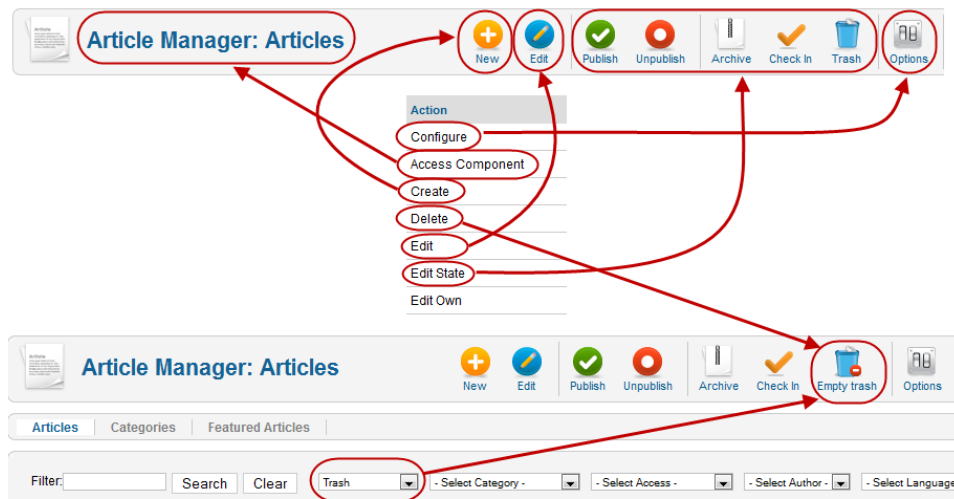
All of these groups have Inherit permission for Configure and Access Component. Remember that Author is a child of the Registered group, and Registered does not have any default permissions except for Login. Since Registered does not have permission for Configure and Access Component, and since Author's permission for these actions is "Inherited", then Author does not have these permissions either. This same permission is passed from Author to Editor and from Editor to Publisher. So, by default, none of these groups are allowed to work with articles in the back end.

It is important to remember that these permissions are only default settings for categories and articles and for any child groups that are created. So they can be overridden for child groups, for categories, and for specific articles.

Also, note that there are no Denied permissions for any actions in the default settings. This allows you to add Allowed permissions at any level. Remember, once you have an action set for Denied, this action will be denied at all lower levels in the hierarchy. For example, if you set the Admin Login for Registered to Denied (instead of Inherited), you could not grant Publishers Allowed permissions for this action.

Article Manager & Actions Diagram

The diagram below shows how each action in the permissions form relates to the various options on the Article Manager screen.



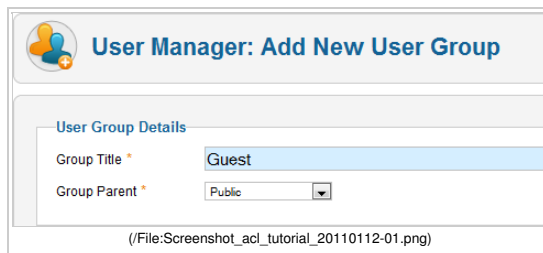
(/File:Screenshot\_acl\_tutorial\_20110111-16.png)

- **Configure** allows you to view and change the Options for the component.
- **Access Component** allows you to navigate to the Article Manager. Without this permission, no other actions are possible.
- **Create** allows you to add new articles.
- **Delete** allows you to delete trashed articles. Note that the Delete icon only shows in the toolbar when you have the "Select State" filter set to "Trash".
- **Edit** allows you to edit existing articles.
- **Edit State** allows you to Publish, Unpublish, Archive, or Trash articles.
- **Edit Own** is the same as Edit except that it only applies to articles written by you.

### Allowing Guest-Only Access to Menu Items and Modules

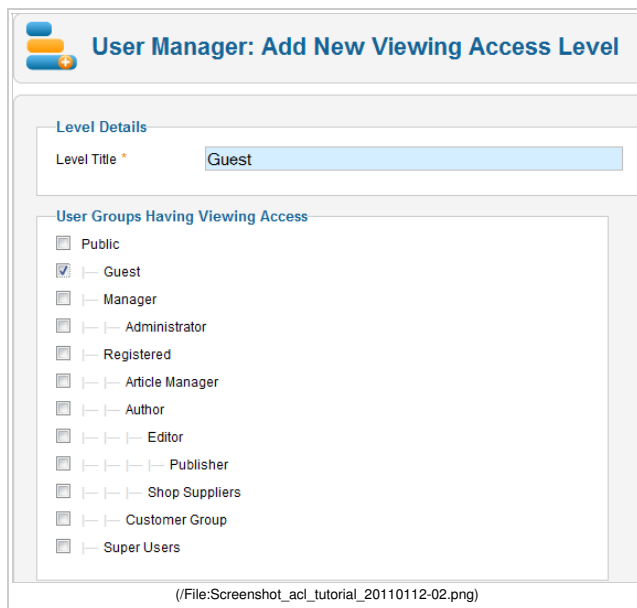
Version 1.6 introduced the ability to create a View Access Level that is only for guests of the site (meaning a user who is not logged in). The example below shows how you can set up this new feature.

1. Create a new user group called Guest. Make it a child of the Public group as shown below.



(/File:Screenshot\_acl\_tutorial\_20110112-01.png)

2. Create a new access level called Guest and grant only the Guest group access to this level, as shown below.

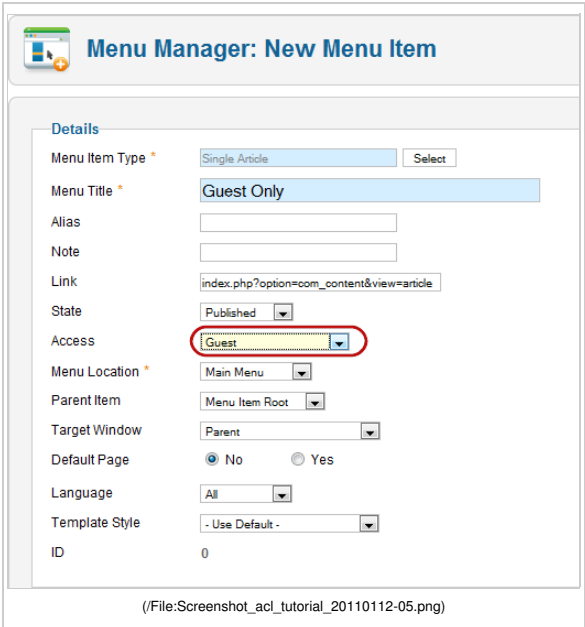


(/File:Screenshot\_acl\_tutorial\_20110112-02.png)

3. Navigate to User Manager – Options – Component and change the Guest User Group from the default value of "Public" to "Guest", as shown below.



Now, if we assign a menu item, module, or other object to the Guest access level, only non-logged in users will have access. For example, if we create a new menu item with access level of Guest, as shown below,



this menu item will only be visible to non-logged-in visitors to the site.

If required other user groups like Author can be granted access in the Guest access level, this would allow Authors to view articles in the front end for editing.

**N.B. Login/logout in front end (for changing data in session) to see the change.**

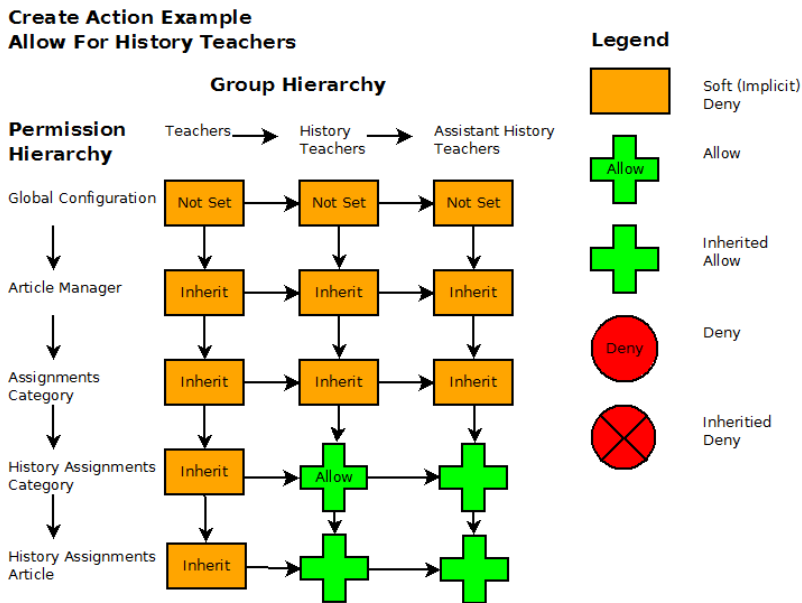
Using Permission and Group Levels Together

As discussed above, it is possible to define groups in a hierarchy, where each child group inherits action permissions (for example, the create permission) from its parent group. Action permissions are also be inherited from the permission level above. For example, a permission in the Article Manager is inherited from the same permission in the Global Configuration, and a permission in a child Category is inherited from the parent Category permission.

This dual inheritance can be confusing, but it can also be useful. Let's consider an example as follows. We have a school with a group hierarchy of Teachers → Assistant History Teachers. We also have a category hierarchy of Assignments → History Assignments. We want History Teachers and Assistant History Teachers to have the following permissions:

- both groups can create new articles only in the History Assignments category.
- only History Teachers (not Assistant History Teachers) can Publish or otherwise have Edit State permission.

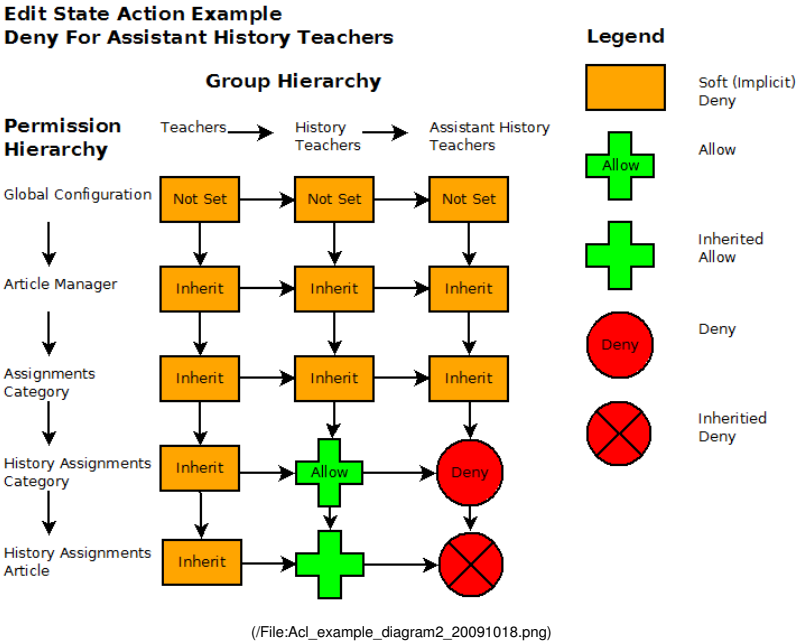
This ACL scheme is very easy to implement. The diagram below shows how this would be set up for the Create Action.



In the diagram, the Permission Hierarchy is shown down the left side and the Group hierarchy is shown across the top. Permissions are inherited down and to the right, as shown by the arrows. To implement the desired permissions, we leave the Global Configuration blank (Not Set) for all three groups. Similarly, in the Article Manager and Assignments Category, we leave the Create permission to Inherit for all the groups. As shown in the diagram, this means that these groups do not have Create permission for articles in general or for articles in the Assignments group.

To sum up so far, we have not set any special permissions to get to this point. Now, in the History Assignments category permissions screen, we set the Create permission to Allow for the History Teachers group. This setting overrides the Soft (Implicit) Deny that we had by default and gives members of this group permission to create content (articles and child categories) for this category. This Allow setting also is inherited by the Assistant History Teachers group.

Next, we need to grant History Teachers the Edit State permission while denying this permission to Assistant History Teachers. This is done as shown in the diagram below.



This configuration is the same as the one above except that this time we set the Edit State permission in the History Assignments category to Deny for the Assistant History Teachers group. This means that Assistant History Teachers will not be able to Publish or Unpublish articles in this category.

Note that this was accomplished by setting just two permissions in the History Assignments category: Allow for the History Teachers group and Deny for the Assistant History Teachers group.

ACL Action Permission Examples

Here are some examples of how you might set up the ACL for some specific situations.

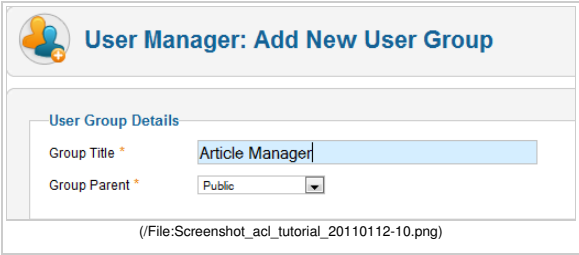
Back-end Article Administrator

Problem:

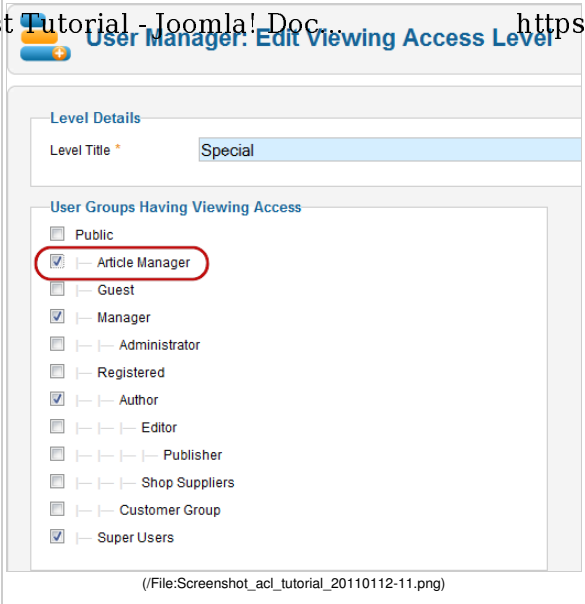
We want to create a group called "Article Administrator" with back-end permissions only for articles and not for any other back-end menu options. Members of this group should be able to use all of the features of the article manager, including setting article permissions.

Solution:

- 1. Create a new group called Article Administrator and make its parent group Public, as shown below.

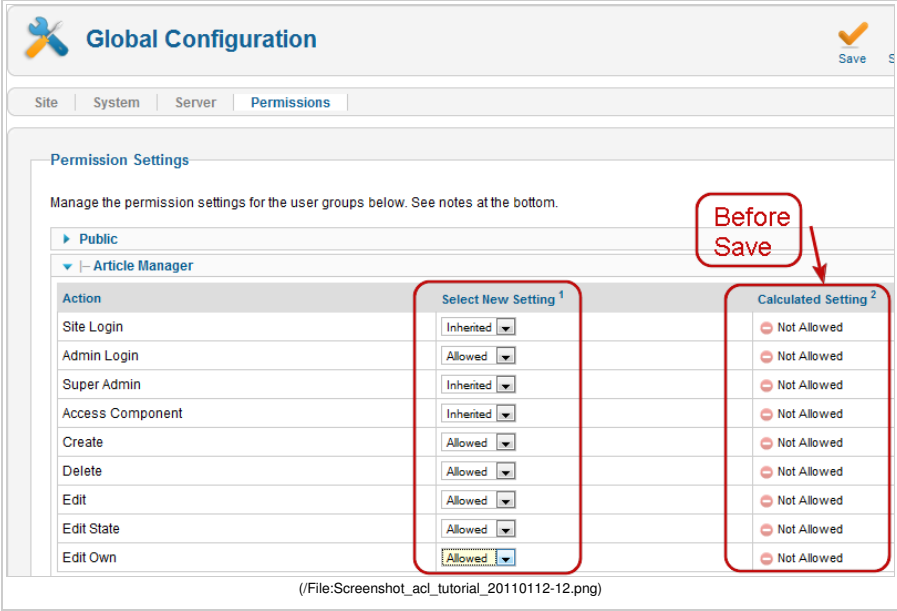


- Because its parent group is Public, it won't have any permissions by default.
- 2. In Users → Access Levels, edit the Special Access level to add the new group. That way they can get access to the back end menu items and modules (This assumes that the modules for the admin menu and quickicons have the Special Access level assigned to them, which is the default.)

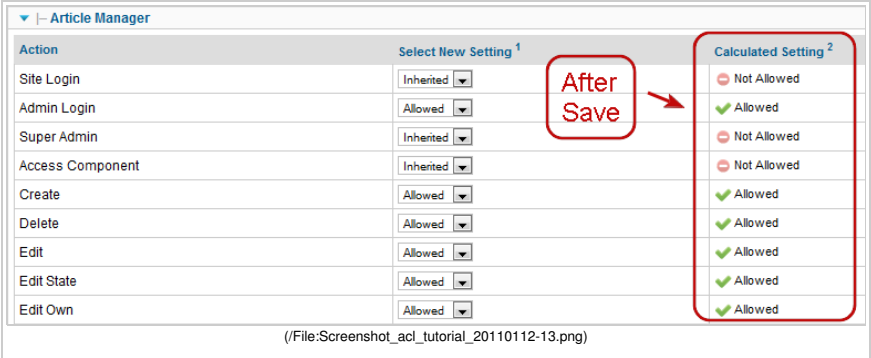


By default, the back-end menu items and modules are set to Special access, so if you forget to add the new group to the Special access level, you won't see any modules or menu items when you log in as a user of the new group.

3. In Site → Global Configuration → Permissions, click on the Article Administrator group and change the permissions to Allowed for the following actions: Admin Login, Create, Delete, Edit, Edit State, and Edit Own. The screen below shows what will show before you press Save.

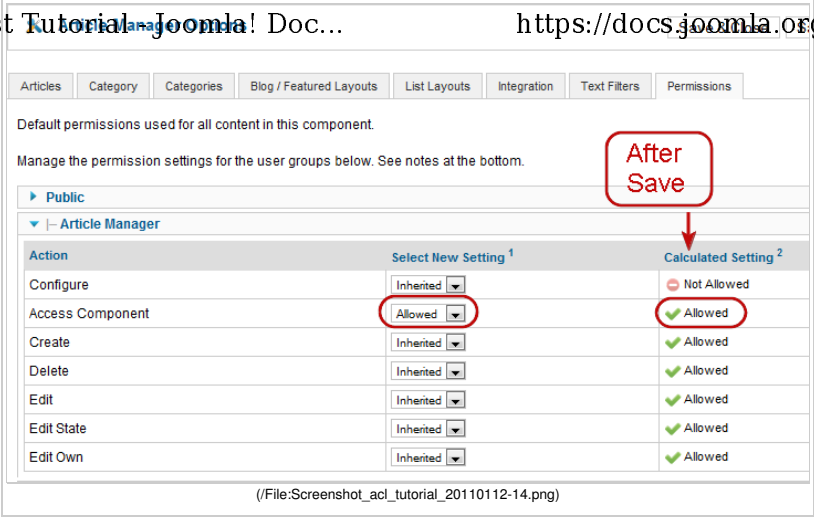


After you save, the Calculated Permissions should show as shown below.



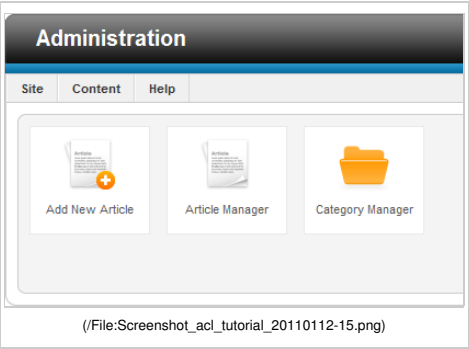
Note that the permission for the Access Component is Inherited, which translates to Not Allowed. This is important. This means that this group will only be able to access components if we give the group "Allowed" permission for Access Component. So we only have to change the one component we want to give them access to and don't have to change any settings for the components where we don't want them to have access. If we had a case where we wanted to give a group access to everything except for one component, we could set the default to Allowed and then set the one component to Denied. Also note that we did not give the group Site Login permission, so users in this group will not be able to log into the front end. (If we wanted to allow that, we would just change the permission to Allowed for Site Login.)

4. In Article Manager → Options → Permissions, change permissions to Allowed for this group for the Access Component action, as shown below.



All of the other desired permissions are inherited.

That's all you need to do. Members of this group can login to the back end and do everything in Article Manager but can't do anything else in the back end. For example, the screen below shows what a user in the Article Manager will see when they login to the back end.



ACL View Access Levels Examples

A basic concept of using Access Levels is that all items with the same Access will be viewable by the same group of users. In other words, if two items have the same Access, you can't have one viewable by one user and not viewable by another user. On the other hand, it is easy to have one Group view any number of items with different Access levels.

Similarly, each Group has exactly the same combination of Access levels, but one User can be a member of more than one group. Depending on the situation, you may want to have users only in one Group or you may need to have a User in more than one Group.

This means that we may need to group our items so that items so that all items in a group have the same level of sensitivity. Here are some examples.

Hierarchical Example

In this example, Access levels are hierarchical, for example, like government security clearance codes. Say for example we have the following sets of classified documents: Classified, Secret, and Top Secret. Users have corresponding clearance codes. Users with Classified clearance can only see Classified documents and cannot see Secret or Top Secret. Users with Secret clearance can see Classified and Secret documents but not Top Secret. Users with Top Secret can see all documents.

In this case, you would create three Access levels: Classified, Secret, and Top Secret and the same three Groups. Users would only be members of one group, as follows:

User	Group	Access Levels
C1, C2, C3	Classified	Classified
S1, S2, S3	Secret	Classified, Secret
TS1, TS2, TS3	Top Secret	Classified, Secret, Top Secret

In this case, all users are in exactly one group, but some groups have access to more than one Access Level of items. In other words, we have a one-to-one relationship between users and groups, but a one-to-many relationship between Groups and Access Levels.

Team Security Example

Another possible use case is a set of non-hierarchical teams. Let's say we have three teams, T1, T2, and T3. Some users are only on one team, but others might be on two or more teams. In this case, we could set up our Access Levels and Groups by team. Documents for each team have the access level for that team, and the Group for the team has only the one access level. When a User is on more than one team, they get added to the group for each team, as follows:

User	Description	Group	Access Levels
U1	Team 1 member	T1	T1
U2	Team 2 member	T2	T2
U3	Team 3 member	T3	T3
U1-2	Member of teams 1 and 2	T1, T2	T1, T2
U1-3	Member of teams 1 and 3	T1, T3	T1, T3
U1-2-3	Member of teams 1,2, and 3	T1,T2, T3	T1, T2, T3

Hybrid Example

In a real-world situation, you might have a combination of these two arrangements. Say for example we have Managers and Staff. Staff can only see Staff documents and Managers can see Manager and Staff documents. Both types of users can be assigned to teams as well, in which case they can see all of the documents for that team. In addition, say that Managers can access some, but not all, team documents. Staff can only access team documents if they are members of that team.

Access Level	Description	Groups
Manager	Non-team manager documents	Manager
Staff	Non-team staff documents	Manager, Staff
Team1	Sensitive Team1 documents (no access outside team)	Team1
Team1-Manager	Team1 documents that can be accessed by all managers	Team1, Manager
Team2	Sensitive Team2 documents (no access outside team)	Team2
Team2-Manager	Team2 documents that can be accessed by all managers	Team2, Manager

Then, users could be assigned to groups as follows:

User Type	Group
Manager on no teams	Manager
Staff on no teams	Staff
Manager on team 1	Manager, Team1
Staff on team 1	Staff, Team1
Manager on teams 1 and 2	Manager, Team1, Team2
Staff on teams 1 and 2	Staff, Team1, Team2

Categorie (/Special:Categories): Joomla! 1.6 (/Category:Joomla!\_1.6) Joomla! 2.5 (/Category:Joomla!\_2.5) Joomla! 3.x (/Category:Joomla!\_3.x)  
Tutorials (/Category:Tutorials) Access Control (/Category:Access\_Control) Access Management (/Category:Access\_Management)  
Needs to be marked for translation (/Category:Needs\_to\_be\_marked\_for\_translation)