

COMMUNITY ACL

REVOLUTIONIZING JOOMLA! ACCESS CONTROL LEVELS

SUPPORT:
TEL: 269-979-5582
SUPPORT@COREPHP.COM

TABLE OF CONTENTS

INTRODUCTION	4
Real life example: How to setup a school site	5
Groups.....	5
Roles.....	5
Want more?	6
HOW TO INSTALL AND UPGRADE	7
Requirements for installation	7
Backup the database before upgrading	7
Install Community ACL	8
Upload the package file in Extension Manager.....	8
Check that Community ACL plugins are enabled	12
Patch the Menu Files	12
CONFIGURATION	13
Default access tab	13
Access type.....	13
Custom access for default Joomla! groups	14
Synchronization tab	16
Invalid access tab	16
Registration tab	17
HTML override for registration form.....	18
USERS MANAGEMENT	24
Assign users to group/role/function	24
SITES MANAGEMENT	26
Create multi-site synchronization	26
GROUPS MANAGEMENT	28
Creating a new group	28
Edit a group	29

Set access	29
Sections Categories Articles Components Menus Modules	29
Login redirect for frontend and backend	30
Article Submission settings	30
Add users to a group.....	32
Remove users from a group	32
ROLES MANAGEMENT	33
Creating a new role.....	34
Edit a role	34
Set access	34
Sections Categories Articles Components Menus Modules	35
Login redirect for frontend and backend	35
Article Submission settings	36
Add users	37
Remove users	37
FUNCTIONS MANAGEMENT	38
Create a new function.....	38
Edit a function	38
Set access	39
Setting up custom actions – for Components	39
Setting up custom actions – for Content Items	44

INTRODUCTION

One of the most sought-after pieces of functionality missing in Joomla! is the ability to assign access levels and roles to users. Community ACL picks up where Joomla! 1.5 leaves off.

There have been other ACL components released in the past to fill this void, but since they hack the core of Joomla! to a point where it's difficult to upgrade, many shy away from using them.

After working with several clients in real need of a true ACL, and after a year of research and development, we are now providing you the ultimate power of working with ALL your applications and Joomla!

The complete ACL enhancement for Joomla! 1.5

With the new framework of Joomla! 1.5 we have been able to create a new Access Level Control component that does very little to the core (in fact, it only hacks the menu to hide items) and provides you the most powerful solution ever to date.



The power behind Community ACL is endless in what you can do and achieve. You have complete control over your users and what they can/cannot do. Easily assign detailed user access levels and roles, with no fear of upgrade issues.

The power of Groups, Roles and Functions

The Groups with sub roles and powerful functions allow you to pin point access of a users ability to save / edit / navigate / ANYTHING within your site - and do it from the leisure of your home chair.

Works with ANY component!

Community ACL is not built strictly for Joomla! 1.5, but works with ANY component on the market. You can control access to specific parts of a component or just block complete access to the component.

Time to revolutionize the way you work with Joomla!, so lets get started!

REAL LIFE EXAMPLE: HOW TO SETUP A SCHOOL SITE

Community ACL has the power to provide control over any site. The best example that we can provide is schools. Here is an example of how to setup a school site:

Groups

Groups are the root level of all permissions. Any permissions set for a group filter down to the **roles** and are inherited.

For detailed information about groups, please see chapter: "Groups Management".

Following the instructions in the "Groups Management" chapter, create for example the groups:

- ✓ 9th Grade
- ✓ 10th grade
- ✓ 11th grade

Lets use 9th Grade for example – go ahead and disallow a few items under the main group.

For detailed information about setting group access, please see chapter: "Groups Management" > "Set Access".

Roles

In order for the groups to work and be applied to a user, they must have a role attached to it.

For detailed information about roles, please see chapter: "Roles Management".

Following the instructions in the "Roles Management" chapter, create for example the roles:

- ✓ 9th Grade Teachers
- ✓ 9th Grade Students

Each of these roles will have their own permission settings based on how they are going to interact with the site.

For detailed information about setting roles access, please see chapter: "Roles Management" > "Set Access".

This allows for the fullest control over the site, allowing you (the administrator) to fine tune how these users are going to interact with the system.

Want more?

For detailed information and even more control options, please read the individual chapters to understand exactly how to take advantage of the power of Community ACL on your site.

HOW TO INSTALL AND UPGRADE

Please read this chapter to install and upgrade Community ACL the easiest way possible.

With every package that 'corePHP' creates we attempt to make the installation process as easy as possible, but we also recognize that every server is setup differently and this can affect your installation process.

REQUIREMENTS FOR INSTALLATION

With any application there are specific system requirements. Community ACL is not exempt from this. Here are our requirements for installation, so check this before you start:

- ✓ **Joomla! 1.5.14** – Community ACL will not work on any version other than Joomla! 1.5. We suggest that you maintain and update your builds of Joomla! for security purposes.
- ✓ **PHP 5.x** – Although we have had many successes with PHP 4.x we have run into some slight problems. Please see our knowledge base if you are using PHP 4.x and note that we will not support PHP 4.x servers.

BACKUP THE DATABASE BEFORE UPGRADING

If you are **upgrading** your package, continue with the steps below. Otherwise go to directly to the next section: "Install Community ACL".

We highly recommend that you backup your database. Although we have never had any problems with updating – but occasionally we do modify the database. You can create a backup through your servers Cpanel or phpMyAdmin or something similar.

After you've created your backup, uninstall Community ACL Component and Plugin:

1. in your Joomla backend, go to Extensions -> Install/Uninstall -> Components
2. choose Community ACL and click Uninstall (top right).

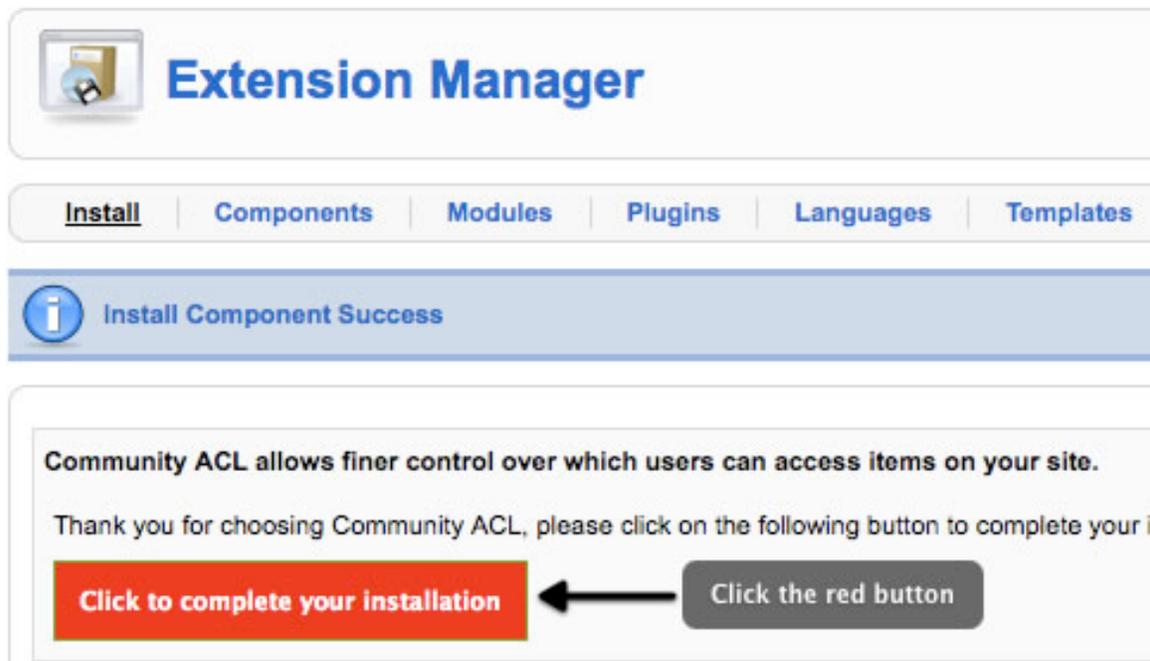
INSTALL COMMUNITY ACL

We can't stress enough that some installations may not go as smooth as others but we have made it to be as simple as possible.

Follow these instructions and you will be up and running in no time. If you do not follow the instructions you will hit some road blocks. So please follow the instructions – it is super easy.

Upload the package file in Extension Manager

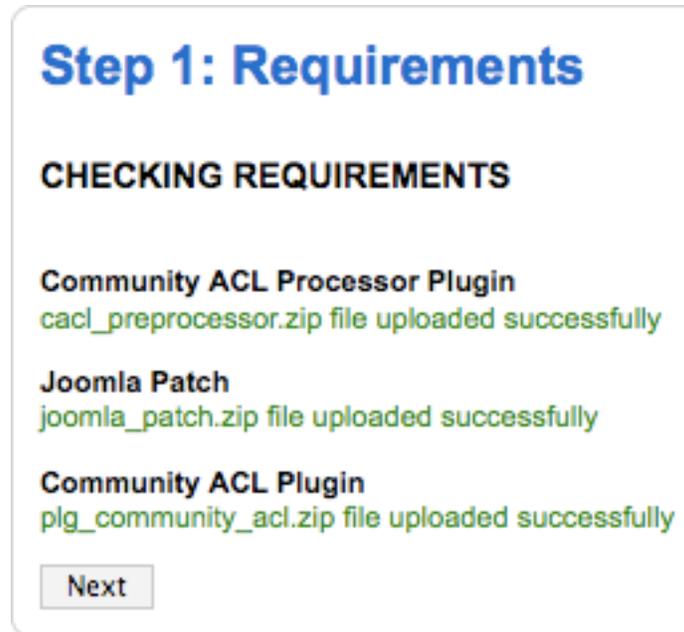
1. In your Joomla backend, go to Extensions -> Install/Uninstall
2. Upload the file for Community ACL (called "Community ACL 1.2.zip" or similar)
3. After it has been successfully installed, click the **red** button to complete your installation (see screenshot).



The screenshot shows the Joomla! Extension Manager interface. At the top, there is a navigation bar with tabs for **Install**, **Components**, **Modules**, **Plugins**, **Languages**, and **Templates**. Below the navigation bar, a blue message box displays an information icon and the text "Install Component Success". Below the message box, a white box contains the following text: "Community ACL allows finer control over which users can access items on your site. Thank you for choosing Community ACL, please click on the following button to complete your i". At the bottom of this white box, there are two buttons: a red button labeled "Click to complete your installation" and a grey button labeled "Click the red button". A black arrow points from the grey button to the red button.

Step 1: Checking Requirements

Click the **Next** button when you see this screen (or similar):



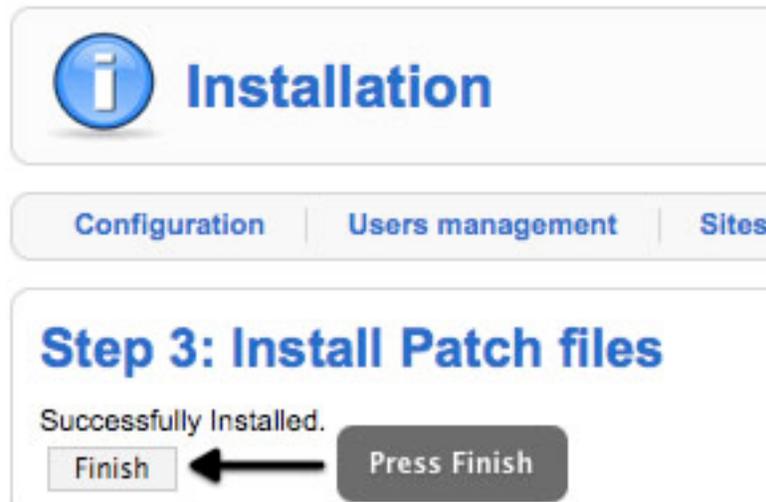
Step 2: Install Joomla! Plugin

Click the **Next** button when you see this screen:



Step 3: Install Patch Files

Click the **Finish** button when you see this screen:



If you at this stage receive the **JFTP: rename: Bad response Rename failed** error, ignore it and proceed.

The reason is that the installer attempts to move files on your site's FTP site, however existing permissions conflict with the ability to perform the operation. Therefore, you would have to manually move files on your site, via FTP.

Step 4: Install Community Builder Plugin (optional)

This stage will only display if **Community Builder** has been installed on your website.

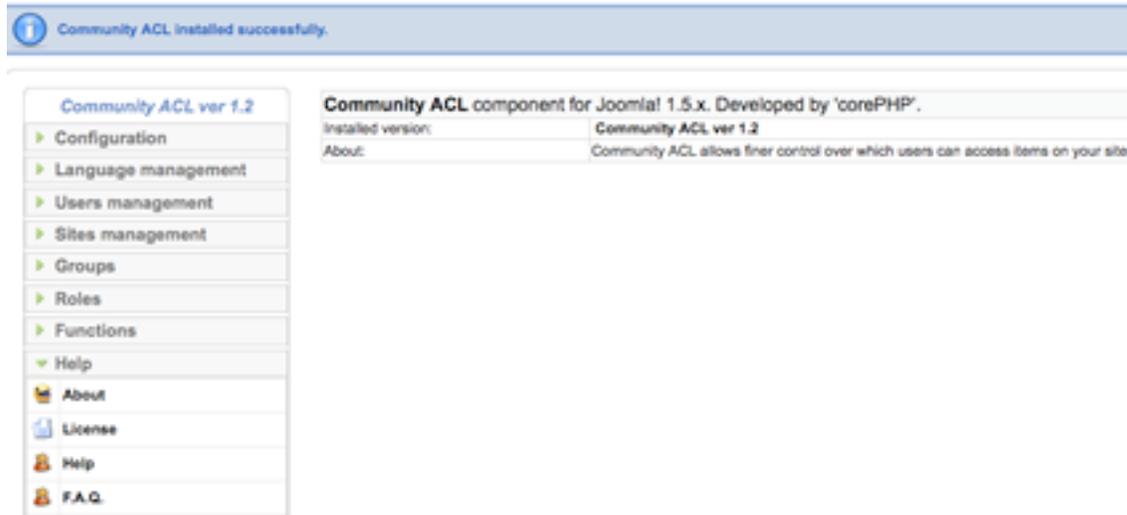
Step 4: Install Community Builder Plugin

Extracting Files...

Would you like to install Community Builder Plugin?

Click **Yes** to install the Community Builder Plugin, or click **No** to skip the Community Builder Plugin.

Finished: Community ACL installed



If no error messages, skip to the next step “Check that plugins are enabled”.
If you have error messages after installation, please read the following information.

If you have an error message on your “Community ACL installed successfully” screen:

1. Unzip the Community ACL installation package and browse to the folder called ‘site’.
2. Unzip the file ‘joomla_patch.zip’ and browse to joomla_patch > libraries > joomla > application > module, where you will find a file called helper.php
3. In your FTP, browse to libraries > joomla > application > module and replace the existing helper.php on your FTP site with the file provided in the extracted joomla_patch folder.
4. Refresh your Joomla backend and your error messages are now gone.

Check that Community ACL plugins are enabled

Go to Extensions > Plugin Manager and look for:

1. **User – Community ACL**
If Community Builder is already installed on your site, ensure that this plugin is installed and enabled
2. **System – Community ACL Preprocessor**
3. **System – Community ACL**
4. **User Registration Community ACL**
5. **System – Community ACL JomSocial**
Only if you have JomSocial installed (the zip filename is cacl_joomsocial.zip)

Patch the Menu Files

1. Unzip the Community ACL installation package (the same .zip file you previously uploaded in the Extension Manager) and browse to the folder called 'site'.
2. Unzip the file 'joomla_patch.zip' and go to:
Libraries/joomla/application/module
Patch the existing helper.php on your FTP site with the file provided in the extracted joomla_patch folder.

NOTE: If you now get a blank page or a php error message saying "Memory Size exhausted" when you try to log in to the backend of your site, make sure your `memory_limit` is set to 16M or more on your server.

SETUP is now complete! :)

CONFIGURATION

This menu item serves to manage the component's settings.
Access it via: Components > Community ACL > Configuration

In this chapter you will get a brief overview of the 3 tabs under Configuration as well as learn how CommunityACL...

- ✓ ...allows you to define "default allow" or "default deny" user access to site for easier administration
- ✓ ...synchronizes with Joomla! users and Community Builder fields
- ✓ ...synchronizes your settings to your other sites for quicker administration

DEFAULT ACCESS TAB

Under this area Community ACL allows you to set your default parameters that will be transparent across the board for the usage of Community ACL.

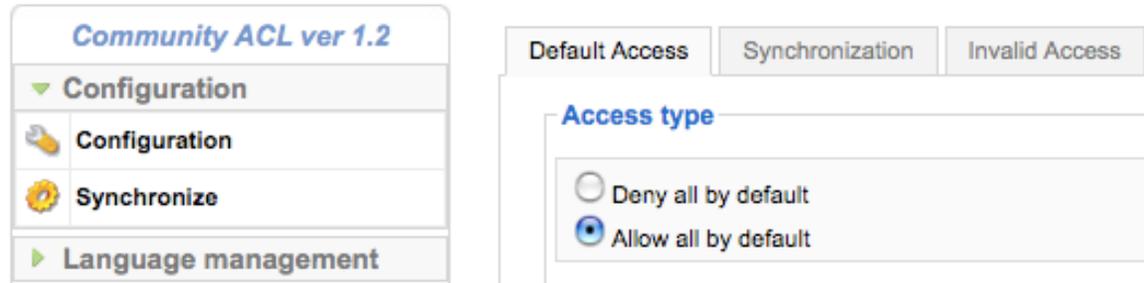
If you installed CommunityACL for the first time, you have no groups, roles or functions set yet.

You will set up your groups, roles and functions in the following chapters, but first lets take a look at some basic (and important!) information about the Default Access types and how they operate:

Access type

The "Default Access" tab allows you to define what group, role and/or function must be applied to a user, depending on the user type, if he/she doesn't have any.

There are two types of settings that Community ACL can be set to:



Deny all by default

This setting will deny EVERYTHING by default. This means that in your groups and roles you will need to create permissions to allow the users to gain access to the modules / plugins etc.

Do not be surprised when you toggle this switch on that your entire site goes blank. This is normal. You will just need to create a group and role with permissions and add it to Public in the Custom Access for Joomla! Groups. Read more about this in the next section.

Allow all by default

This setting allows EVERYTHING by default. This means in your groups and roles you will be denying access to the users on what portions of the site they have access to.

Everything will show on the frontend unless you create a group/role and apply it to the Public in the Custom Access for Joomla! groups section. Read on in the next section more about this.

Custom access for default Joomla! groups

So you don't want to go through the hassle of setting up specific groups and settings for users and apply it to them separately? But later you want to get more defined with your users? Don't worry, that is easy.

This global permission system makes about 60% of sites easy to configure, and for the other 40% we have added the ability to edit large amount of users easily as well. Read more in each specific chapter.

In this section of the Default Access tab you can assign the Groups/Roles and functions for the default Joomla! groups.

Custom Access for Joomla! groups

This rules will work only if user does not belong any CACL group or role.

Public (not logged):	Group: <input type="text" value="Public Group"/>	Role: <input type="text" value="Public roles"/>	Function: <input type="text" value="None"/>
Registered:	Group: <input type="text" value="10th Grade"/>	Role: <input type="text" value="Student"/>	Function: <input type="text" value="None"/>
Author:	Group: <input type="text" value="10th Grade"/>	Role: <input type="text" value="Teacher"/>	Function: <input type="text" value="None"/>
Editor:	Group: <input type="text" value="None"/>	Role: <input type="text" value="None"/>	Function: <input type="text" value="None"/>
Publisher:	Group: <input type="text" value="None"/>	Role: <input type="text" value="None"/>	Function: <input type="text" value="None"/>
Manager:	Group: <input type="text" value="None"/>	Role: <input type="text" value="None"/>	Function: <input type="text" value="None"/>
Administrator:	Group: <input type="text" value="None"/>	Role: <input type="text" value="None"/>	Function: <input type="text" value="None"/>

For example:

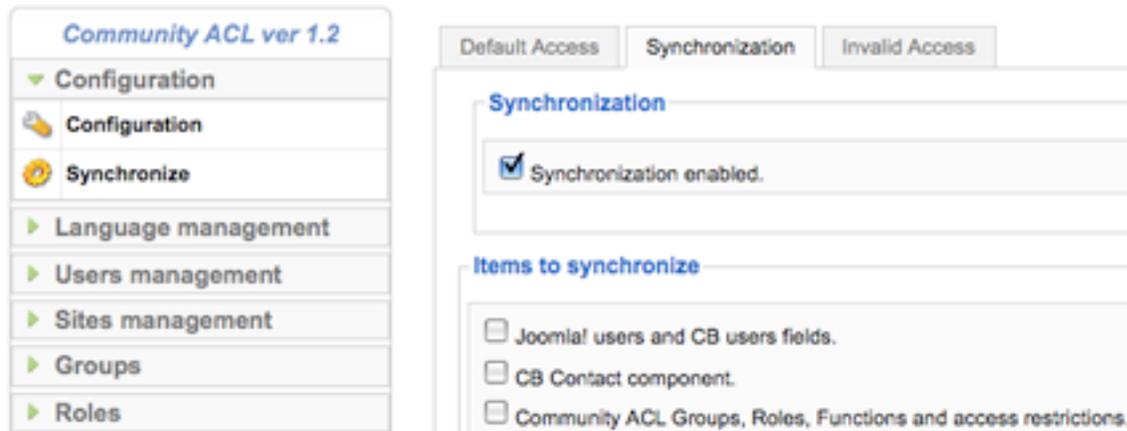
- ✓ If you setup specific permissions for the frontend users in the Groups and Roles, here you would choose them to apply to the **Public (not logged)** users.
- ✓ If you want all your **Registered** users to fall under a specific rule pattern you would assign it here. This way you don't have to do that for all your users.

The ONLY rule for this kind of setup is:

- ✓ Make sure that the individual Authors, Editors etc do NOT have a group/role/function assigned to them under their user details (see Users Management chapter).

This because **the individual settings will override the universal** – meaning that Community ACL will ignore the universal assignments under “Custom Access for Joomla! groups” and instead assign the user to the group you assigned to him/her under the user details.

SYNCHRONIZATION TAB



Important – Do **not** enable synchronization until all the sites to be synchronized are entered. See chapter “Sites Management” for more information.

The "Synchronization" tab allows you to switch on/off synchronization and specify the elements to be synchronized. For example:

- Joomla! users and Community Builder users fields.
- Community Builder Contact component.
- Community ACL Groups, Roles, Functions and access restrictions.

To activate:

1. Tick the “Synchronization enabled” box
2. Choose which items you want to synchronize and click Save (top right).

INVALID ACCESS TAB

If a user is restricted from accessing a page/article on your website, here is where you can set the url you want to redirect them to instead or choose to show them a “Forbidden content” message.

Default Access Synchronization Invalid Access

Invalid Access

Redirect URL:

Redirect URL (Administration):

Forbidden content: Show title with `no access` message

- Show only title
- Show title with `no access` message
- Show title and introtext
- Show title and introtext with appended `no access` message

For single article view only the Redirect URL applies, i.e. the user gets automatically redirected to the URL you specify in this tab.

The 'Forbidden content' drop-down menu only applies to when the menu/article view is in a **blog layout** (arrows on screenshot to the right shows example of Blog Layout options when creating a new menu item in Joomla!).

In the drop-down menu you set what you want to be shown on the page if user doesn't have access.

 Menu Item: [New]

Select Menu Item Type



REGISTRATION TAB

This tab is activated in 2 scenarios:

1. Community Builder and the Community Builder Plugin are installed, or...
2. the HTML overrides are activated (see next chapter for more info)

#	Group	Role	Function	Delete
1	Basic Members	30 Days Trial	None	

Under the “Registration” tab you can set up multiple groups, roles and functions to be automatically assigned to users when they register/create an account on your site.

HTML override for registration form

If you have the HTML overrides activated (see instructions further down for how to execute the HTML overrides), you’ll see both the “Registration” tab and the “Registration Membership Types” tab.

#	Group	Role	Function	Delete
---	-------	------	----------	--------

The HTML overrides adds the feature for Community ACL to **display the groups and roles at the frontend during registration.**

That way, your new users can specify which Community ACL group(s) and role(s) they would like to be assigned to. (This has been a really popular request!)

To show you how your users will see this when implemented on your site, this how the Joomla registration normally looks for your website visitors:

Registration

Name:	<input type="text"/>	*
Username:	<input type="text"/>	*
E-mail:	<input type="text"/>	*
Password:	<input type="text"/>	*
Verify Password:	<input type="text"/>	*

Fields marked with an asterisk (*) are required.

This is how the Joomla registration form looks when you have created the HTML overrides:

Registration

Name: *

Username: *

E-mail: *

Password: *

Verify Password: *

Community ACL User Setup

Membership Type Add

Fields marked with an asterisk (*) are required.

The membership types/names you add under the **Registration Membership Types** tab (and after you click Save), will then be visible under the Registration tab, where you can specify further what you want new members to be assigned to, based on their choice when they register.

Default Access Synchronization Invalid Access **Registration Membership Types** Registration

Setup Details

#	Group	Role	Function	Membership Type	Delete
1	10th Grade	Teacher	None	teacher	
2	10th Grade	Student	None	student	
3	10th Grade	Parent/Guardian	None	parent/guardian	
	<input type="text" value="10th Grade"/>	<input type="text" value="test"/>	<input type="text" value="None"/>	<input type="text" value="teacher"/>	<input type="button" value="Add"/>

#	Membership Type	Add
1	teacher	
2	student	
3	parent/guardian	

Enter new membership type below:

How to execute the HTML override

1. Unzip Community ACL package: Community ACL Version 1.2.zip
2. Locate the folder: site/HTML override/**com_user**
3. Using an FTP Client, upload the entire folder 'com_user' to templates/TEMPLATE_NAME/html/

How to test the new feature

1. On the frontend of your website, go to the Login Module (please be advised that this only works for the **Joomla! login module**, NOT the Community Builder login module)
2. Click on 'Create an account' link:
3. You will now see a form similar to the following layout:

Login

Username

Password

Remember Me

- [Forgot your password?](#)
- [Forgot your username?](#)
- [Create an account](#)



Registration

Name: *

Username: *

E-mail: *

Password: *

Verify Password: *

Community ACL User Setup

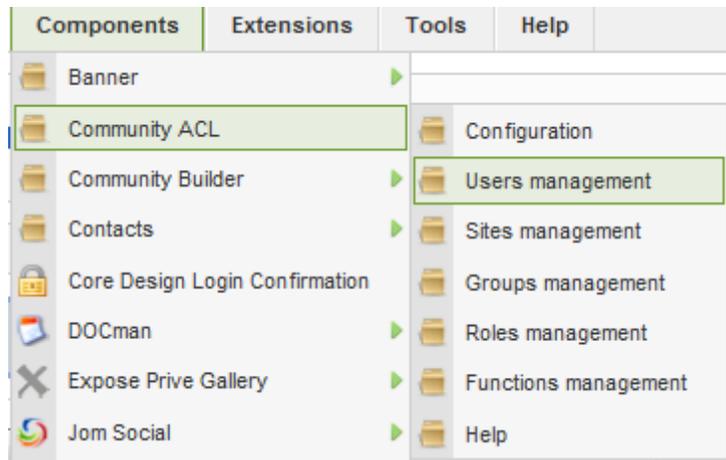
#	Membership Type	Add
	<input type="text" value="teacher"/>	<input type="button" value="Add"/>

Fields marked with an asterisk (*) are required.

4. Complete the form, select the groups and roles you would like to be assigned to (click Add after each membership type you want to add)
5. When form is complete, click the 'Register' button.

Check Community ACL to confirm success

1. Go to the backend and access the Community ACL - User Manager:



2. Search for the user you just added from the frontend registration form.
3. Examine the Community ACL Details of the newly created user and you see that all Group(s), Role(s) and Function(s) are all assigned to the user just like it was setup/selected during registration.

USERS MANAGEMENT

Here you can see all the registered users of your site as well as their names, groups, log status and more.

<ul style="list-style-type: none"> ▶ Configuration ▶ Language management ▼ Users management  User Manager ▶ Groups 	<table border="1"> <thead> <tr> <th>#</th> <th><input type="checkbox"/></th> <th>Name</th> <th>Username</th> <th>Logged In</th> <th>Enabled</th> <th>Group▲</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="checkbox"/></td> <td>10th Grade teacher</td> <td>teacher10</td> <td>✓</td> <td>✓</td> <td>Publisher</td> </tr> <tr> <td>2</td> <td><input type="checkbox"/></td> <td>10th Grade Student</td> <td>student10</td> <td></td> <td>✓</td> <td>Registered</td> </tr> <tr> <td>3</td> <td><input type="checkbox"/></td> <td>Parents</td> <td>parent10</td> <td></td> <td>✓</td> <td>Registered</td> </tr> </tbody> </table>	#	<input type="checkbox"/>	Name	Username	Logged In	Enabled	Group▲	1	<input type="checkbox"/>	10th Grade teacher	teacher10	✓	✓	Publisher	2	<input type="checkbox"/>	10th Grade Student	student10		✓	Registered	3	<input type="checkbox"/>	Parents	parent10		✓	Registered
#	<input type="checkbox"/>	Name	Username	Logged In	Enabled	Group▲																							
1	<input type="checkbox"/>	10th Grade teacher	teacher10	✓	✓	Publisher																							
2	<input type="checkbox"/>	10th Grade Student	student10		✓	Registered																							
3	<input type="checkbox"/>	Parents	parent10		✓	Registered																							

- To **add** a new user: User Manager > click “New” (top right)
- To **edit** an existing user: User Manager > click the name of the existing user

ASSIGN USERS TO GROUP/ROLE/FUNCTION

When adding a new user, or editing an already existing user, you can define the group, function and role for this user in the "Community ACL Details" section.

Community ACL Details

#	Group	Role	Function	Delete
1	Students	Grade 1	None	

Students ▼

Grade 1 ▼

None ▼

Add

Email notification when new content is submitted No Yes



Learn more about how to create Groups, Roles and Functions in the chapters: “Groups Management” and “Roles Management” and “Functions Management”

Unlike Groups and Roles, you cannot assign a user **Function** under the “Functions management” menu item.

In order to assign a user to a Function, please follow the instructions below:

1. Access the Users Management menu item
2. Click the name of the user you wish to assign to the function
3. Under Community ACL Details (see screenshot above), select a Group, Role and the Function.
Please note: in order to assign a user to a Function, you also need to select a Group and a Role
4. Click Add (marked with arrow in screenshot above)
5. Click Save (top right)

SITES MANAGEMENT

Allows you to synchronize with multiple websites, allowing for one master site for your access levels.

Here you can enter the sites which already have the component installed with which you want to synchronize users, roles, functions and site elements access to.

CREATE MULTI-SITE SYNCHRONIZATION

To add the site you want to synchronize with, go to "Sites Management" and click "New".

When entering new sites, or editing the already existing sites, make sure you have entered the correct parameters. It can be done by means of the "Check DB Details" button.

Site Details

Name:	<input type="text"/>	Name is URL of your site.	<input type="button" value="Check DB Details"/>
Published:	<input type="text" value="Yes"/>		
Description:	<input type="text"/>	Description of your site.	

MySQL DB details	
Database host:	<input type="text"/> A database host of your site. If a database is located on the same hosting as your main site - try to fill localhost here. Contact your ISP for details.
Database name:	<input type="text"/> Name of the database your site is using.
Database user:	<input type="text"/> Database user name, which have rights to connect to database. Contact your ISP for details
Database password:	<input type="text"/> A database password. Contact your ISP for details.
Tables prefix:	<input type="text"/> Select a tables prefix for this site. Usually it is 'jos_'.

Important: one of the sites must be marked as "Main Site". The same site has to be marked as "Main Site" on all sites you are synchronizing to.

[Sites management](#) | [Groups management](#) | [Roles management](#) | [Functions management](#) | [Help](#)

One site must be set to Main Site

#	<input type="checkbox"/>	Name	Main Site	Published	DB host	DB name	DB user	Table prefix
1	<input type="checkbox"/>	Site 1			localhost	dbname	user	
2	<input type="checkbox"/>	Site 2			localhost	dbname	user	

On the main site you must enter all the sites which are to be synchronized, as all the information required for the elements synchronization will be saved on that site.

GROUPS MANAGEMENT

In this chapter you will learn about how to manage your access groups and how to:

- ✓ create/edit a group and add/remove users in a group
- ✓ define access to sections, categories, articles, component, modules and menus.

You will also learn that:

- ✓ if access is denied or allowed to a **section**, the category and the article within that section inherit the access level
- ✓ if access is denied or allowed to a **category**, the articles in that category inherit the access
- ✓ if you want to deny/allow users access, they must belong to a Group and a Role (see separate “Role Management” chapter). Most importantly, a Group requires at least one role

CREATING A NEW GROUP

#	<input type="checkbox"/>	Name
1	<input type="checkbox"/>	Students
2	<input type="checkbox"/>	Teachers

1. Click on “New Group” in the left menu
2. Enter the name and description of your group and click Save

EDIT A GROUP

Access via Groups management > List of Groups. Under the Tools column, click [Edit]:

#	<input type="checkbox"/>	Name	Published	Tools
1	<input type="checkbox"/>	Students		[Edit] [Set access] [Add users] [Remove users]

When you are done editing, click Save.

SET ACCESS

This section also includes **Login redirect for frontend and backend** and **Article Submission settings**, both on a group level.

Note – You can decide to leave the Set Access blank (recommended) and do the permissions setup at Roles. Read more in the chapter “Roles Management”.

First define a common access for all the **roles** which form this group: if **all the roles** of a certain group should not have access to an element, you should forbid access to this element on a **group** level.

Under the Tools column, click [Set access] for the group you want to set permissions for and see the next chapters for more information:

#	<input type="checkbox"/>	Name	Published	Tools
1	<input type="checkbox"/>	Students		[Edit] [Set access] [Add users] [Remove users]

Sections|Categories|Articles|Components|Menus|Modules

Important – If you forbid access to a **section**, then you forbid access to all its categories and articles too; the same applies to **categories**.

1. Go to one of the first 6 available tabs: Sections/Categories/Articles/Components/Menus/Modules depending on what item you want to set access for.

Sections
Categories
Articles
Components
Menus
Modules

Add New Item

- Uncategorized
- About Joomla!
- News
- FAQs
- 10th Grade

Lists of Allowed Items

#	Section	Published	ID	Delete	
				<input type="button" value="Clear All"/>	
1	10th Grade		5		

2. Select the item(s) you want to set this group to have access to and click Add. When you are done, click Save.

Login redirect for frontend and backend

Here you can set the url to where you want the users in this group to be redirected to after they have logged in.

Article Submission settings

Here you set what is visible or not to the users in this group when they submit an article from the frontend of your website. (also available for Roles, see separate chapter)

Sections	Categories	Articles	Components	Menus	Modules	Redirect	Article Submission
Items		Choices					
Show Frontpage		<input checked="" type="radio"/> Yes <input type="radio"/> No					
Show Start Publishing		<input checked="" type="radio"/> Yes <input type="radio"/> No					
Show Finish Publishing		<input checked="" type="radio"/> Yes <input type="radio"/> No					
Show Author Alias		<input checked="" type="radio"/> Yes <input type="radio"/> No					
Show Access Level		<input checked="" type="radio"/> Yes <input type="radio"/> No					
Show Metadata Fields		<input checked="" type="radio"/> Yes <input type="radio"/> No					

Select which items to be Hidden(No) / Displayed(Yes) and click Save.

This is an example of what logged in group members see if all set to Yes:

Publishing

Section:

Category:

Show on Front Page: No Yes

Author Alias:

Start Publishing:

Finish Publishing:

Access Level:

Ordering: New Article defaults to the first position. Ordering can be changed after this Article has been saved.

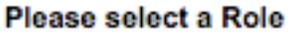
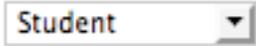
Metadata

Description:

Keywords:

ADD USERS TO A GROUP

Note: You can not add new users until you have created one or more **Roles**. Please see chapter “Roles Management” for more information on how to do this.

1. Under the Tools column, click [Add users] 
2. Select a Role from the list (If list is empty, see note above) 
3. Click Continue 
4. Click in the check box to select the user(s) to be included in this group
5. Click Add (top right)

REMOVE USERS FROM A GROUP

1. Under the Tools column, click [Remove users] for the group you want to remove user(s) in.
2. Click in the check box to select the user(s) to be removed from this group.
3. Click Remove (top right)

ROLES MANAGEMENT

Roles allows you to organize **different access levels within a group**. You can assign unlimited number of roles to a group – for example, the group ‘10th Grade’ can have the Roles ‘Teacher’, ‘Student’ and/or ‘Parent’.

Sites management		Groups management		<u>Roles management</u>	
#	<input type="checkbox"/>	Name	Published	Ordering	Group
1	<input type="checkbox"/>	Teacher		▼ 1	10th Grade
2	<input type="checkbox"/>	Student		▲ ▼ 2	10th Grade
3	<input type="checkbox"/>	Parent		▲ 3	10th Grade
4	<input type="checkbox"/>	Teacher		▼ 1	11th Grade
5	<input type="checkbox"/>	Student		▲ ▼ 2	11th Grade

Setting up a role is a process identical to setting up a group. The difference is that a Role **needs to be assigned to an existing Group**.

Recommended: do all the permissions setup under **Roles**, such as deny/allow access to Sections, Categories, Articles, Components, etc.

In this chapter you will learn how to:

- ✓ Add/edit/delete role(s)
- ✓ Define access to sections, categories and articles
- ✓ Deny or grant access to the components and modules within the site, on both the front end and back end

Important to know is that:

- ✓ If you deny or allow access to a **section**, the category and the article within that section inherit the access level
- ✓ If you deny or allow access to a **category**, the articles in that category inherit the access

CREATING A NEW ROLE

1. Click New Role (left menu) or New (top right)
2. Enter the Role details and select the Group this Role will be assigned to
3. Click Save

EDIT A ROLE

1. Click [Edit] under the Tools column
2. Edit the Details
3. Click Save

SET ACCESS

This section also includes **Login redirect for frontend and backend** and **Article Submission settings**, both on a role level.

Under the Tools column, click [Set access] for the role you want to set permissions for:

#	<input type="checkbox"/>	Name	Published	Tools
1	<input type="checkbox"/>	Students		 [Edit] [Set access] [Add users] [Remove users]

You will then see something similar to the following screen (depending on the content of your site):

Sections
Categories
Articles
Components
Menus
Modules

Add New Item

- Uncategorized
- About Joomla!
- News
- FAQs
- 10th Grade

Lists of Allowed Items

#	Section	Published	ID	Delete	
				<input type="button" value="Clear All"/>	
1	10th Grade		5		

Sections|Categories|Articles|Components|Menus|Modules

Important – If you forbid access to a **section**, then you forbid access to all its categories and articles too; the same applies to **categories**.

1. Go to one of the first 6 available tabs: Sections/Categories/Articles/Components/Menus/Modules depending on what item you want to set access for.
2. Select the item(s) you want to set this role to have access to and click Add. When you are done, click Save.

Login redirect for frontend and backend

Here you can set the url to where you want the users in this group to be redirected to after they have logged in.

Article Submission settings

Here you set what is visible or not to the users in this group when they submit an article from the frontend of your website.

Publishing

Section:

Category:

Show on Front Page: No Yes

Author Alias:

Start Publishing:

Finish Publishing:

Access Level:
Registered
Special

Ordering: New Article defaults to the first position. Ordering can be changed after this Article has been saved.

Metadata

Description:

Keywords:

(also available for Groups, see separate chapter)

Sections	Categories	Articles	Components	Menus	Modules	Redirect	Article Submission
Items		Choices					
Show Frontpage		<input checked="" type="radio"/> Yes <input type="radio"/> No					
Show Start Publishing		<input checked="" type="radio"/> Yes <input type="radio"/> No					
Show Finish Publishing		<input checked="" type="radio"/> Yes <input type="radio"/> No					
Show Author Alias		<input checked="" type="radio"/> Yes <input type="radio"/> No					
Show Access Level		<input checked="" type="radio"/> Yes <input type="radio"/> No					
Show Metadata Fields		<input checked="" type="radio"/> Yes <input type="radio"/> No					

1. Select which items you would like this group to see Hidden (No)/
Displayed (Yes)
2. Click on Save/Apply

ADD USERS

1. Under the Tools column, click [Add users]
2. Click in the check box to select the user(s)
3. Click Add

REMOVE USERS

1. Under the Tools column, click [Remove users]
2. Click in the check box to select the user(s)
3. Click Remove

FUNCTIONS MANAGEMENT

Using functions you can define how your users interact with content.

For example, you can easily create:

- one function that allows people to add, edit, publish and comment on articles as well as remove them
- another function that only lets users comment

Then, when you assign your users into groups, you don't have to go through each person in detail – just assign them the function you created and you're good to go.

In this chapter you'll learn how to you can:

- ✓ control how a user interacts with Sections, Categories and Articles by disallowing or allowing access for them to add/edit/publish it
- ✓ create, edit and set actions for a function
- ✓ allow/deny access to a specific part, component or variables in the url
- ✓ create functions with multiple access rights to a variety of components

CREATE A NEW FUNCTION

1. Click New functions (left menu) or New (top right)
2. Enter the Function details and click Save



EDIT A FUNCTION

1. Click on the function name or click [Edit] under the Tools column
2. Edit the function details and click Save

SET ACCESS

Click on [Set actions] under the Tools column, you will then see:

Allowed Actions for components

Component: All actions Custom Actions

Custom action:

Key: Value:

Allow all values except this value
 Any value

Front End
 Back End

#	Component	Key	Value	Front End	Back End	Delete Clear All
1	Articles	Any key	Any value	✓	✓	<input type="button" value="Delete"/>

1. In the drop-down menu, select a Component
2. You now have two options: setting permissions (for the component you've selected) for **All actions** or **Custom actions**:
 - a. To set permissions for all actions, choose the radio button 'All Actions', tick the checkbox called 'Any Value' and click Add.
 - b. To set permissions for specific actions, choose the radio button 'Custom Actions' and read the next chapter for more information about how to specify the Custom Actions.

Setting up custom actions – for Components

Custom actions allows you to have extra fine-grained control over who can do what on your site.

For information about how to assign a user to a function, see chapter Users Management -> Assign users to group/role/function

In this chapter you'll learn how easy it is to know what to provide for the **key** and the **value** under the Custom action.

Custom action:

Key: Value:

Allow all values except this value

Any value

Note: The Action will only work if all the pairs of key/value coincide in the request.

Lets give you an example: you want to deny/allow access to edit a specific article:

1. Access the article from your Joomla backend and examine the URL. For example: `http://www.domain.com/administrator/index.php?option=com_banners&task=edit&cid[]=1`
2. In the above URL you see '`...option=com_banner...`' – this means that the component is called BANNER (see Quick Reference Guide further down in this chapter). So select Banner from the component drop down list.
3. From the same URL, you also see '`...task=edit...`' (see Quick Reference Guide further down in this chapter). Now, in order to setup a function to allow access to edit this article (and all other articles under Banner):
 - a. In the field called 'Key' add the value '**task**'
 - b. In the field called 'Value' add the value '**edit**'

Please note: The above would allow users the ability to edit any article under Banner. If that's exactly what you want, then this is the stage where you click the Add button and then Save. If you want to deny/allow access to a **specific** article, then keep on reading.

4. Looking at the url we used above, you see '`... cid[]=1`' Now, in order to setup a function to allow/deny access to edit this specific article (with the id of 1):
 - a. Click 'Add another key-value pair'
 - b. In the field called 'Key' add the value '**cid**'
 - c. In the field called 'Value' add the value '**1**'

5. Click the Add button and then Save.

The screenshot shows the ACL configuration interface for the 'Banners' component. The 'Component' dropdown is set to 'Banners'. The 'Custom Actions' radio button is selected. The 'Custom action' section shows a key-value pair with 'Key: cid' and 'Value: 1'. There are checkboxes for 'Only allow this value' and 'Any value'. Below this, 'Front End' and 'Back End' are both checked. At the bottom, a table shows the configuration:

#	Component	Key	Value	Front End	Back End	Delete
1	Banners	cid	1	✓	✓	✗

Another example is the url:

`/index.php?option=com_config?section=com_contact_details`

Looking at the url above, you can break it down to:

- **option=com_config** means the Configuration Manager component (to select from the Component drop-down menu)
- **section=com_contact_details** means Key=**section** and Value=**com_contact_details**

One last example: in this scenario you have a category for which you want to allow/forbid the user access to edit:

`/index.php?`

`option=com_categories§ion=com_content&task=edit&cid[]=25`

1. Choose the Category Manager in the drop-down menu
2. Type **section** in the Key field and **com_content** in the Value field. Click "Add another key-value pair"
3. Type **task** in the Key field and **edit** in the Value field. Click "Add another key-value pair"
4. Type **cid** in the Key field and **25** in the Value field. Click Save.

Quick reference guides

Hint: You can tell the value of the component by identifying what the value of "option" is in the URL – ex. `index.php?option=com_search&Itemid=26` means the `option=com_search`. Therefore the component is the Search component.

Components

To make it easier for you to quickly see, based on the url, which component to choose from the drop down menu you can use the following list as a quick reference for some of the common components:

Component	Option Value
Banners	com_banners
Configuration Manager	com_config
Contacts	com_contact
Search	com_search
Weblinks	com_weblinks
Articles	com_content
Category Manager	com_categories
Section Manager	com_sections
Front Page Manager	com_frontpage
Community ACL	com_community_acl

Keys and Values

These Keys/Values can be combined or used individually, depending on which Component you've selected and what action you want to allow/deny.

See the following list as a basic reference guide and please note that not all keys/values apply to all component.

Action	Key	Value
Access	task	accesspublic
	task	accessregistered
	task	accessspecial
Archiving	task	archive
	task	unarchive
Copying	task	copy
Copying Saving	task	copysave
Creating new	task	add
Deleting	task	remove
Editing	task	edit
Frontpage	task	toggle_frontpage
Locking	task	block
	task	unblock
Logout	task	logout
Moving	task	movesect
Moving saving	task	movesectsave
Publication	task	publish
	task	unpublish
Reset	task	reset
Saving	task	apply
	task	save
	task	save2new
	task	save2copy

Action	Key	Value
	task	go2menu
	task	go2menuitem
Show Search Results	search_results	1
Sorting	task	orderup
	task	orderdown
	task	saveorder
Viewing	task	preview

Setting up custom actions – for Content Items

Under the Actions for Content Items tab, select any Section(s), Article(s) or Categories for which you want to either deny or allow the access to Add/Edit/Publish, then click Save (top right).

Hint: The individual Select All buttons selects all the Sections, Categories or Articles beside it. You can also hold the Ctrl key down and click the Sections, Categories or Articles of your choice if you would like to select more than one at a time.

If you select a category, it means that users tied to this Function will be allowed/restricted to Add/Edit/Publish all articles under that category.

If you forbid a Section ex. “About Joomla!” it implies that all categories and articles under the section “About Joomla!” will be forbidden. Likewise, if you forbid a Category, all articles under that particular category will be forbidden.

For information about how to assign a user to a function, see chapter Users Management -> Assign users to group/role/function