Permissions Settings

Related Pages: Groups, Groups Admin, Category, Category Admin, Permissions List, Permission Enforcement Order, Templated Groups and Roles

Understanding Tiki Permissions

onclick=role="">Along with setting the features, setting permissions is one of the basic aspects of Tiki administration. This page describes the basic concepts in Tiki's permission system and how the various aspects interact. A complete list of permissions can be found on the Permissions List page.

How Permissions Work

Main points of the permission system in Tiki

- When Tiki is installed, there are three pre-defined Groups of users:
    - Anonymous: Users that are not logged in are in the Anonymous group.
    - Registered: Users that are logged in are in the Registered group.
    - Admin: The person who installs Tiki is the initial member of the Admin group.
- Administrators (Admin group members) can create and edit Groups of users.
    - Each group can have fully customized access to all site features.
    - Users can be assigned to one or several groups.
    - Groups can have subgroups.
    - Permissions are assigned to groups of users, *not* to individual users.
- Individual objects such as wiki pages can have permissions applied to them directly, for particular user groups.
- If no permissions are specified for a group for an object or content category, then global permisions apply.
- Administrators can create and edit a content Category.
    - Objects can be added to content categories.
    - A content category can then be assigned to a group.
    - Category-based permissions, when used (it's an "advanced" feature), give members of the groups the permissions assigned to them.

In what order are permissions settings applied?

It is important to understand that Tiki uses several types of permissions:

- **Global** permissions: Each site visitor belongs to a **Group** (such as Anonymous or Registered). The permissions you assign to the group define the *global* site-wide permissions for that user.
- **Category** permissions: These permissions define the actions that users can take for objects in a *specific content category*.
- **Object** permissions: These permissions define the actions that user can take for an *individual object*.
- See also: Permission Enforcement Order

***Tip**: The setup of permissions is much easier when you are still learning how to master them if you avoid the level of Category permissions, and you only use Global and Object permissions.*

Permissions are inherited from from the top-down, but override from the bottom-up.

Tiki's permissions model may look like complex... but is also *very* customizable.

ℹ Permissions Example

Consider the following example for a company using Tiki:
You have the groups:

- Anonymous
- Employees

- Board of Directors

Notice that some groups *include* other groups. For example, members of the **Board of Directors** group will include, in addition to their own permissions, the permissions from the Employees, Registered, and Anonymous groups.

You have the categories:

- Financial Information
- Press Releases

You want to give:

- Everyone permission to read most pages
- Employees permission to edit most wiki pages
- Board Members only, access to the company's financial information.

Global (Group) Permissions

First, you need to define the global permissions for each group.

Anonymous

- To let the general public (that is, anonymous visitors) view wiki pages, assign **tiki_p_view** to **Anonymous**.

Employees

- The Employee group includes the **Anonymous** group (that is, everyone) and **Registered** group (that is, users who are logged in). Therefore, the Employee group *inherits* the **tiki_p_view** permission from these groups.

- To let employees edit pages, assign **tiki_p_edit** to **Employees**.

Board of Directors

- The Board of Directors group includes the **Anonymous**, **Registered**, and **Employees** groups. Therefore, the Board of Directors group *inherits* the **tiki_p_view** and **tiki_p_edit** permission from these groups.
  This group does not require any additional permissions.

Category Permissions

Now that the Global permissions are set, you can adjust the permissions for each category. These settings will *override* the Global permissions. The Category permissions can be set for each category from the Settings > Categories (tiki-admin_categories.php) page.

Note: Remember that Category permissions are an advanced feature only recommended for experienced users of Tiki, mastering already how Global and Object permissions work.

Press Releases

Currently, Anonymous can view press releases, and Employees can edit them (as defined by the Global permissions). To allow only the Board of Directors to edit press releases, you must assign permissions to the category. This will override the default group (global) permissions:

- For the Press Releases category, remove **tiki_p_edit** from **Employee**. Now only the **Board of Directors** group can edit wiki pages in the category.
- Anonymous visitors (and all groups that *inherit* the Anonymous group's permissions) can still **view** the pages.

Financial Information

Currently, Anonymous can view Financial Information, and Employees can edit them. But we want *only* the Board of Directors to have access (both view and edit) to these pages. You'll need to make the same adjustments to the

Financial Information category's permissions:

- Remove **tiki_p_edit** from **Employee**. Now only the **Board of Directors** group can edit wiki pages in the category.
- Remove **tiki_p_view** from **Employee**, **Registered**, and **Anonymous**. Now only the Board of Directors can see the pages.

Object Permissions

But what if you want one item in the Financial Information category, to be visible to the public? You can override all other permissions, by assigning specific permissions to the *object* itself. For example, the ABC Company may have a public disclosure form, issued by the government, that it needs to make public (but that only the government can change or update):

- For the individual item, remove **tiki_p_edit** from the **Employee** and **Board of Directors** group. Since this form is issued by the government, no one should be able to change it.
- Anonymous visitors (and all groups that *inherit* the Anonymous group's permissions) can still **view** the pages.

Object Permissions can be tricky.

For example using version 10, if you wanted to hide one wiki page made by admin from the Anonymous group you would select the page's permissions (from the admin menu : Wiki/List Pages/then click the Key icon for your page in the list).

Using the object permission page of the wiki page, you turn off the "*Can view page/pages (tiki_p_view)*" attribute and save.

However, after loging off, and connecting as Anonymous you can still see the page.

It turns out that you have to turn off the "*Can view page/pages (tiki_p_view)*" **AND** "*Can admin the wiki* *(tiki_p_admin_wiki)*" attributes to hide the wiki page from the Anonymous group.

Managing permissions

Warning

While entering a filter, JQuery will rebuild the list. Do not press enter or you'll start all over.

The interface has three tabs. The first tab is for assigning permissions.

The second tab is to select which groups should be included in the table for assigning permissions, because, when the list of groups is large, assigning permissions could be slow.

The third tab is to filter the number of features that should be shown in the nterface. This is specially needed when managing category permissions, to avoid having a list bigger than needed for our purposes in specific cases.

In addition, this new interface to manage permissions includes several features:

onclick=role="">

onclick=role="">

onclick=role="">

1. You can assign or remove all object permissions on all child categories if this box is checked.
2. You can filter the whole list of permissions dynamically to list only those containing som text
3. You can expand or collapse at will any of the sections of permissions

4. You can select one by one the permissions to be assigned or checking the box at the column title (group name) level, and that selection will propagate to all the checkbox shown in that column.

Permissions by section

onclick=role="">

Today

←

→

September 2025

SU	MO	TU	WE	TH	FR	SA
31	01	02	03	04	05	06
07	08	09	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	01	02	03	04

Demo site for testing

- demo

Category permissions

Permissions can be restricted via the category feature. Basically, you can already assign all the permissions you need as described above. The full granularity of permissions can be assigned to categories (and thus inherited when objects belong to a given category).

If an object has no specific (object) permissions, then:

1. If the object is not part of any category with specific permissions, global permissions apply.
2. If the object is part of at least one category with specific permissions, the permissions on that object are the sum of the permissions granted to all of the object's categories which have specific permissions.

For example, if...

1. wiki page *Foo* has no specific permissions
2. the set of categories *Foo* is in is category #3 and category #5
3. and category #3 has no specific (category) permissions

... then:

1. If category #5 has no with specific permissions, global permissions apply.
2. If category #5 has specific permissions, the permissions on Foo are the permissions on category #5.

Because adding a category to an object can provide additional rights, it is important to protect who can assign categories to prevent undesired escalation. For example, if the site contains public and private information, someone with access to edit private information should not be able to make it available publicly by changing the categories. To resolve this issue, multiple permissions can be assigned to the categories.

o begin with, tiki_p_modify_object_categories allows to determine if the user is allowed to modify the categories of th object at all. Without this permission, it will be impossible to modify the categories. Typically, it is safe to grant this permission widely.

Then, there is higher granularity available for each category. tiki_p_add_object and tiki_p_remove_object determine if the user can add or remove elements from the category. Categories on which permissions are specified should also specify who can assign to or remove from those categories. When a user has the tiki_p_modify_object_categories permission on an object and modifies that object, but lacks the tiki_p_add_object permission on a certain category, the user will see a checkbox for that category, but the checkbox will be disabled.

Additionally, some category changes may be allowed in certain contexts by defining Category Transitions, which would allow to change a category only from a certain state. A group of transitions create a workflow.

Workspaces

Workspaces further facilitate management of large and complex Tiki sites.

Admin permissions and special permissions

When a group has an admin permission on a feature such as tiki_p_admin_sheet, the group will lost his admin permission for an object with local perms or categories permissions.

Customising the permissions list (re-ordering it) for power users.

Since Tiki19 it is possible to customise and re-order the list of the permissions displayed under Setting => Permissions (tiki-objectpermissions.php). Super user can edit a yaml file located at : tiki-objectpermissions_order.yml.

Note

Some information on this page is from **Tiki for ~~Dummies~~ Smarties**, copyright (C) by Rick Sapir, published by KeyContent.org, and available under a Creative Commons Attribution-Share Alike License.

Alias

- ACL
- ACLs
- permission
- Permission
- perm
- perms
- right
- rights
- global permissions
- global permission
- object permission
- object permissions
- privilege
- privileges
- category permission
- category permissions