3 Rights concepts

An introduction to rights management

More than 100 permissions are necessary to control the user access to all wiki functions and extensions.

Depending on the actions a user needs to take, many of these permissions are related and consequently need to be granted to a certain type of user. A user with read access, for example, needs to also be able to change the user profile and add pages to a watch list. For this reason, BlueSpice uses roles and groups to manage the rights of individual users.

The following entities are part of the rights management system:

- **Permission**: Allows a specific action.
- **Role**: A set of permissions (permissions can only be set by selecting roles).
- **User**: Entity in the wiki instance database. Has a unique user name and user id.
- **User group**: A collection of users. A user is assigned to one or more groups. There are system internal groups (cannot be removed or renamed) and custom groups. In many cases the group name consists of the role and a namespace name
- **Namespace**: Permissions can be set on a namespace level. But not on a per-page-level.

Use case: Managing department information

Anna (HR Manager) and Phil (HR Specialist) are maintaining all content related to the Human Resources department on the company wiki.

Some content is visible to all employees. Other content has to be restricted and only be visible to upper management and to Lea, the company’s legal advisor.

After reviewing the content and access requirements, the company decides to create HR content in two namespaces: All unrestricted content goes in the Main namespace of the wiki. Sensitive information is maintained in a custom namespace called "HR".
Rights concepts

To reflect these specific HR requirements, the wiki administrator needs to complete the following steps:

1. Create the **namespace** (HR:) on the page Special:NamespaceManager:

   ![Add namespace](image)

   After adding the namespace, the new namespace is displayed after pressing the "f5" key.

2. Create the necessary **groups** on the page Special:GroupManager:

   ![Group manager](image)

   - **HR_visitor**: Users in this group have only view permissions to the (HR:) namespace
   - **HR_editor**: Users in this group can create and edit pages in the (HR:) namespace
   - **HR_reviewer**: Users in this group can, additionally, approve documents. For this to work, the function "FlaggedRevs" is activated for the namespace. These groups are initially "empty".
3. Assign **roles** to each group on the page **Special:PermissionManager**. After this, each group has specific sets of permissions:

1. The group HR_visitor:

![Permission manager](image)

The administrator selects the group "HR_visitor" and checks the Role "reader" only in the HR namespace. Since the reader role in the HR namespace is now assigned to the group "HR_visitor", all other groups no longer have any view permissions for this namespace:
2. The group HR_editor: The administrator selects the role editor only in the namespace HR. Since the editor role does not inherit all permissions from the reader role, the administrator also has to check the reader permissions in addition:

3. The group HR_reviewer: The administrator selects the role of reviewer only for the namespace HR. Since the roles HR_visitor and HR_editor have been reserved for the groups HR_visitor and/or HR_editor before, the editor and reader permissions have to be granted as well:
4. **Add users** to the correct user groups: Since Anna needs to be able to edit and approve the documents both in the HR and in the Main namespace, she has to be added to both the “HR_reviewer” and the standard “reviewer” groups:

The administrator also adds the other affected users to the correct groups. The result is the following permissions configuration:
## Rights concepts

<table>
<thead>
<tr>
<th>User</th>
<th>Is in Groups</th>
<th>Roles in Namespace HR</th>
<th>Roles in Namespace Main</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anna (HR manager)</td>
<td>HR_reviewer</td>
<td>reviewer</td>
<td>reviewer</td>
<td>Anna can now read, edit and approve pages in both the HR and the Main namespaces.</td>
</tr>
<tr>
<td></td>
<td>reviewer</td>
<td>reader</td>
<td>editor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reviewer</td>
<td>reader</td>
<td>editor</td>
<td></td>
</tr>
<tr>
<td>Phil (HR specialist)</td>
<td>HR_editor</td>
<td>reader</td>
<td>reviewer</td>
<td>Phil can now read and edit pages in both the HR and the Main namespaces.</td>
</tr>
<tr>
<td></td>
<td>editor</td>
<td>reader</td>
<td>editor</td>
<td></td>
</tr>
<tr>
<td>Edith (CEO)</td>
<td>HR_viewer</td>
<td>reader</td>
<td>editor</td>
<td>Edith can now read pages in the HR namespace and edit pages in the Main namespace.</td>
</tr>
<tr>
<td></td>
<td>editor</td>
<td>reader</td>
<td>editor</td>
<td></td>
</tr>
<tr>
<td>Lea (Legal advice)</td>
<td>HR_viewer</td>
<td>reader</td>
<td>-</td>
<td>Lea can only read pages in the HR namespace.</td>
</tr>
<tr>
<td>All employees</td>
<td>reader</td>
<td>-</td>
<td>reader</td>
<td>All employees can read pages in the Main namespace. They cannot read the pages in the HR namespace.</td>
</tr>
</tbody>
</table>

In addition, the administrator should ensure that Anna is not the only person who can approve content. Otherwise, there would be a problem when Anna is on vacation or has no time for reviewing page edits.

### Related info

- Extension: BlueSpiceNamespaceManager
- Extension: BlueSpicePermission Manager
- Extension: BlueSpiceGroupManager

### 4 Namespace manager

<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 About the Namespace manager</td>
</tr>
<tr>
<td>2 Creating a namespace</td>
</tr>
</tbody>
</table>
About the Namespace manager

The Namespace manager allows a user with administrative rights to create, delete and rename namespaces and to change the settings of these namespaces. Users with edit rights can view the page, but cannot make any changes to it.

The navigation link to the Namespace manager is located under Global actions > Management. This link opens the page Special:NamespaceManager.

Creating a namespace

To create a namespace:

1. **Click** the "Plus" icon at the top of the page. A dialog opens.
2. **Enter** the name for the new namespace and select the namespace options.
You can activate the following options:

1. **Subpages**: namespace can contain subpages (MediaWiki functionality)
2. **Content namespace**: needs to be checked if users will create wiki pages in this namespace (MediaWiki functionality). See also mediawiki.org/wiki/Manual:ContentHandler.
3. The remaining options activate a number of extensions for the namespace: CategoryCheck, Secured page assignments, PageTemplates, Visual editor, Rating, Recommendations, ReadConfirmation, Semantic MediaWiki, FlaggedRevs.

The corresponding talk namespace for the new namespace is automatically created. The ID of each namespace is assigned automatically based on wiki settings and existing namespace IDs.

### Editing and deleting a namespace

**Editing a namespace**: A namespace can be edited by clicking on the "wrench" icon in the table row or above the table when a namespace is selected.

Names of talk namespaces or of system namespaces (File, MediaWiki) cannot be changed.

**Deleting a namespace**: Only custom (user created) namespaces can be deleted.

After clicking on the delete icon, a dialog with the delete options appears.
3. User rights

Rights concepts

- Will be deleted: deletes the pages in this namespace together with the namespace
- Will be moved into "(Pages)" moves the pages of this namespace into the main namespace
- Will be moved into "(Pages) with the suffix "(from [namespace name])" moves and appends the pages with "from [namespace]"

Talk namespaces are deleted with their corresponding namespace and cannot be deleted separately.

Technical details

The interface for the user manager is provided by the extension BlueSpiceNamespaceManager.

Related info

- UserManual:NamespaceManager

3.2 Managing permissions

Contents

1 Access to the permission manager .................................................................................................................. 10
2 Role-based permissions ................................................................................................................................... 10
  2.1 Default roles .............................................................................................................................................. 11
Access to the permission manager

To manage permissions, the extension BlueSpicePermissionManager provides the administrator interface. It is located under *Global actions > Management > Permission manager*. This links to the page `Special:PermissionManager`:

![Permission manager](image)

Role-based permissions

In BlueSpice version 3.0 roles were introduced as a way to manage wiki rights, . The main intention of using roles is to simplify rights management.

Roles represent a *collection of individual permissions* that are necessary to perform certain function on the wiki. For example, for a user who is supposed to only read the wiki, many permissions in addition to the "read" permission are needed: the ability to change their own settings, to search the wiki, to view page ratings, and so on.

All permissions that make up a logical group are encapsulated in a role, in this example the role "reader". If wiki admins want to grant read-only rights to a user group, they only need to assign that group the "reader" role, instead of assigning many individual rights.
By assigning roles to a group, all users belonging to that group will receive the rights contained in these roles. Roles are not assigned directly to users, but to groups instead. Users are then assigned to one or more groups.

Default roles

By default, BlueSpicePermissionManager includes a number of pre-defined roles that serve most user needs on the wiki. The individual permissions contained in a role can be seen by clicking the info icon in front of the role name. It opens a dialog with a permissions list for the role:

- **bot** - typically assigned only to the *bot* group
- **admin** - all available rights. It should be assigned only to wiki-admin groups
- **maintenanceadmin** - very similar to the *admin* role, used for user groups that are responsible for maintaining wiki integrity
- **author** - all permissions necessary for creating content on the wiki
- **editor** - create content, edit and delete content, create reviews
- **reviewer** - all reviewing actions
- **accountmanager** - user account management rights
- **structuremanager** - move (rename) pages, create and delete namespaces
Rights concepts

- **reader** - basic read-only access
- **accountselfcreate** - this role must be assigned to the "*" groups to allow users to self-create user accounts
- **commenter** - cannot create and edit content, can only comment on existing content

The roles matrix

The permission manager consists of the group tree (1) and the role matrix (2):

![Permission manager screenshot](image)

The **group tree** (on the left) shows all existing groups:

- **Group "*"**: all non-logged-in (anonymous) users
- **Group "user"**: all logged-in users, the default group for all users
- **Subgroups of group "user"**: all groups that are defined on the wiki, either by default, by MediaWiki, or custom groups created by the wiki admins. System groups, created by MediaWiki, can be hidden by unchecking the "Show system groups" checkbox above the tree.

The columns in the **role matrix** are:

- **Role information** (info icon): Clicking the icon shows all the permissions in a role. This list is exportable.
## Role name

**Wiki:** Assignment of a role to the entire wiki. By assigning the role in this column, a user group gets permissions in this role on the wiki (all namespaces).

**Individual namespaces:** The following columns list every (applicable) namespace on the wiki.

- Roles can be assigned to individual namespaces. For example, the group *user* can get the *editor* role only in the namespace *Public*. *Users in this group cannot edit content in any other*. By granting a role to a particular group in a particular namespace, means that all other groups will lose permissions from this role, eg. granting role "reader" in namespace "Private" to group "sysop" means that all users in any other groups won't be able to read pages in "Private" namespace, even if they have "reader" role granted on the wiki level ("Wiki" column).
- The same role can be granted to multiple groups for the same namespace.
- Additional namespaces can be added in the matrix by clicking on the arrow in table header, then "Columns". Then the namespaces can be selected.

### Role inheritance

By default, all roles granted to the (*) group will be granted to the *user* group, and all roles granted to the *user* group are granted to its subgroups. If a group inherits the role from an upper-level group field, this is indicated in the role matrix with a green background, but the checkbox is empty.

### Technical info

#### Logging

Every change to the roles is logged in the MediaWiki log book, found under Special:Log under Permission Manager log type. These logs are available only to wiki administrators (users in groups with the role *admin*).

#### Backups

All changes to the role matrix are backed up. By default, the last 5 backups are kept. This limit can be changed in BlueSpiceConfigManager, under configs for the extension BlueSpicePermissionManager.

### Related info

- UserManual:PermissionManager
- Managing groups
- Rights concepts
3.1 Managing groups

Accessing the group manager

The interface for the Group manager is provided by BlueSpiceGroupManager. It allows adding, renaming and deleting groups. An administrator can go to Global actions > Management > Group manager. This opens the page Special:GroupManager:

![Group manager interface](image)

Functionality

The group manager has the following features:

- **Viewing groups**: it provides a list of all user groups
- **Creating new groups**: Clicking on the "plus" button opens a dialog for adding a new group.
- **Renaming groups**: A group can be renamed by selecting it and then clicking the wrench icon. System groups and groups declared by other extensions cannot be renamed.
- **Deleting a group**: A group can be deleted by selecting it and then clicking the "x" button. System groups cannot be deleted.
Assigning roles and users to groups

To assign users to groups, use the User manager. To assign roles (permissions) to groups, use the Permission manager.

Related info

- UserManual:BlueSpiceGroupManager
- Managing permissions