

Zone1 Admin Documentation

Table of Contents

Admin Menu	2
Search Listings	3
Flags	4
Rights	5
Roles	6
Groups	8
File Visibility	10

Admin Menu

If your Zone1 account has been given the 'admin' role, you'll have access to the Zone1 Admin menu pictured below:



Search Listings

For those files that can not have a thumbnail generated, generic icons may be uploaded by an administrator and assigned to display per file type, as shown in the image below.



The screenshot shows a web form titled "File Type Category". At the top, there is a text input field labeled "Name" containing the word "Document". Below this is a large rectangular area for uploading an image. To the right of this area, there is a pink text annotation that reads "image uploaded for specific file type". At the bottom of the form, there are two buttons: "Choose File" and "Update". Between these buttons, the text "No file chosen" is displayed.

This can be managed from the 'File Types' and 'File Type Categories' admin pages.

Flags

The system has five non-changing flags for which a file can have:

- nominated for preservation
- selected for preservation
- preserved
- may be university record
- university record

A standard user can assign only the “nominated for preservation” and “may be university record” flag to their items. The rights to add “selected for preservation”, “preserved”, and “university record” flags are managed via the admin interface and can be assigned to a user directly, through a role they have, or through a group they belong to.

Additionally, users with the right to view preserved flag content are allowed to access files with the “preserved” flag regardless of their permissions level.

Rights

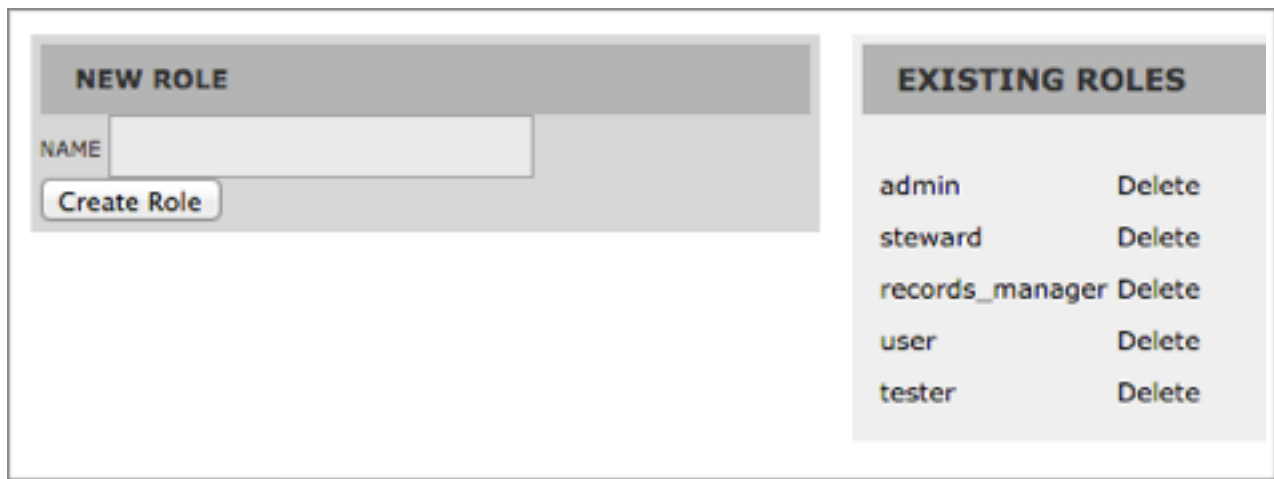
Accessibility is controlled by various rights, that are assigned to a user either directly, through a role (see the “Roles” section), or a group. Here is a full set of base rights and the corresponding functionality when a user has this right:

- `add_preserved`: Can add the “preserved” flag
- `add_nominated_for_preservation_flag`: Can add the “nominated_for_preservation” flag
- `add_selected_for_preservation`: Can add the “selected_for_preservation” flag
- `add_university_record`: Can add the “university_record” flag
- `add_may_be_university_record`: Can add the “may_be_university_record” flag
- `toggle_open`: Can set the access level to open on any content
- `toggle_open_on_owned`: Can set the access level to open on any content owned by yourself
- `toggle_partially_open`: Can set the access level to partial open on any content
- `toggle_partially_open_on_owned`: Can set the access level to partially open on any content owned by yourself
- `toggle_dark`: Can set the access level to dark on any content
- `toggle_dark_on_owned`: Can set the access level to dark on any content owned by yourself
- `manage_disposition`: Can set the disposition attribute on any content
- `delete_items`: Can delete content
- `delete_items_on_owned`: Can delete content owned by yourself
- `view_items`: Can view all content
- `view_items_on_owned`: Can view all content owned by yourself
- `view_preserved_flag_content`: Can view all content with preservation flag
- `delete_comments`: Can delete all comments
- `delete_comments_on_owned`: Can delete comments on content owned by yourself
- `edit_items`: Can edit metadata of all content
- `edit_items_on_owned`: Can edit metadata of all content owned by yourself
- `view_reports`: Can view all reports
- `view_reports_on_owned`: Can view reports on content owned by yourself
- `view_admin`: Can access the admin interface
- `remove_preserved`: Can remove the “preserved” flag
- `remove_nominated_for_preservation`: Can remove the “nominated_for_preservation” flag
- `remove_selected_for_preservation`: Can remove the “selected_for_preservation” flag
- `remove_university_record`: Can remove the “university_record” flag
- `remove_may_be_university_record`: Can remove the “may_be_university_record” flag

Each right can be assigned to a user directly, through a role the user has, or through a group the user belongs to. See the sections “Roles”, “Groups”, and “File Visibility” to understand more about rights and accessibility.

Roles

Roles can be created via the admin, shown in the screenshot below.

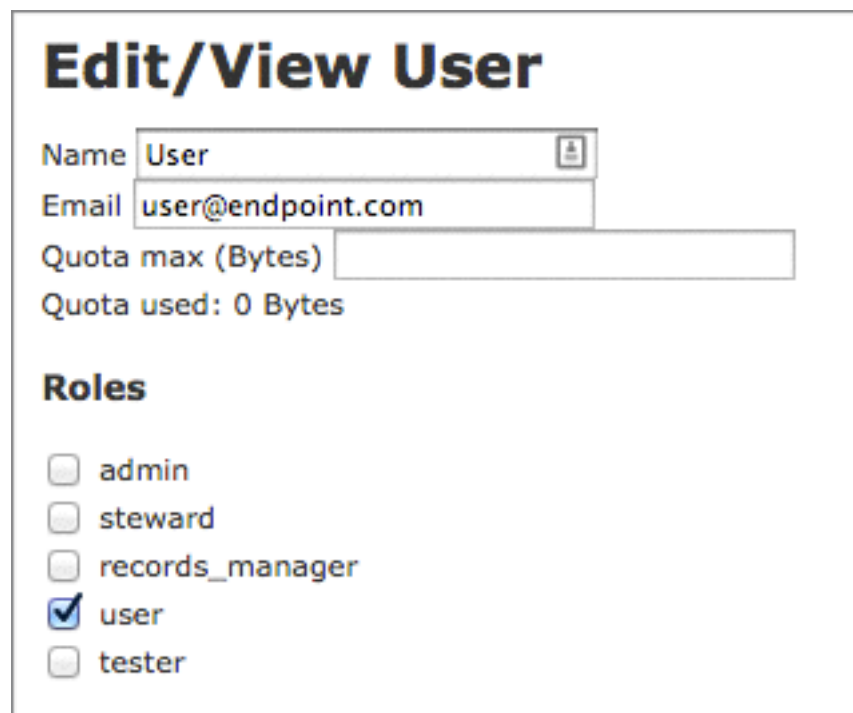


The screenshot displays the Roles management interface. On the left, under the 'NEW ROLE' header, there is a form with a 'NAME' label and an input field. Below the input field is a 'Create Role' button. On the right, under the 'EXISTING ROLES' header, there is a table listing existing roles and their corresponding 'Delete' actions.

NEW ROLE	
NAME	<input type="text"/>
<input type="button" value="Create Role"/>	

EXISTING ROLES	
admin	Delete
steward	Delete
records_manager	Delete
user	Delete
tester	Delete

Once a role is created, users may be assigned to this role via the admin interface, as shown in the screenshot below.



The screenshot displays the 'Edit/View User' interface. It features a title 'Edit/View User' and several input fields for user information: 'Name' (with the value 'User'), 'Email' (with the value 'user@endpoint.com'), and 'Quota max (Bytes)' (with an empty input field). Below these fields, it shows 'Quota used: 0 Bytes'. Under the 'Roles' section, there is a list of roles with checkboxes: 'admin', 'steward', 'records_manager', 'user' (which is checked), and 'tester'.

Edit/View User

Name

Email

Quota max (Bytes)

Quota used: 0 Bytes

Roles

- ☐ admin
- ☐ steward
- ☐ records_manager
- ☒ user
- ☐ tester

After a role has been created and users assigned to the role, rights can be assigned to the role from the interface as shown in the screenshot below.

Edit Role

Name

☒ **add_preserved**
Ability to add PRESERVED flag.

☒ **add_selected_for_preservation**
Ability to add SELECTED_FOR_PRESERVATION flag.

☐ **add_may_be_university_record**
Ability to add MAY_BE_UNIVERSITY_RECORD flag.

☐ **toggle_open_on_owned**
Ability to set access level to open on content owned by you.

☐ **toggle_partially_open_on_owned**
Ability to set access level to partially open on content owned by you.

example of rights that can be assigned to roles

Once a role has been created and assigned to a user, that user may perform the allowed rights assigned to that role. See the “Rights” section of the documentation for a full list of assignable rights.

Tester Role

The ‘tester’ role is used to provide accounts with the ability to switch between being in an ‘admin’ role and another non-admin role. Any user who has the ‘tester’ role will be able to see and use the ‘Toggle off/on Admin’ button at the top of the page. When toggled off, the ‘admin’ role is removed from the current user’s roles so that they can operate in any non-admin role they also have assigned to their account. When toggled on, the ‘admin’ role will be added back to the user’s roles so that they’ll once again be permitted to see and perform admin functionalities.

For example, if an admin needs to test a particular feature as the ‘steward’ role, they can update their roles to include ‘admin’ (which can’t be deselected), ‘tester’, and ‘steward’. Then when they click the admin toggle button their ‘admin’ role is removed, leaving them with ‘steward’ and ‘tester’, and since ‘tester’ doesn’t have any rights associated with it they’re left with nothing but the rights of a ‘steward’. The same process can be used to test as a ‘records_manager’ or a ‘user’ (or any future roles that are added via the roles admin page).

Groups

Groups are similar to roles in that they represent a subset of users. Groups are different to roles in that users are invited to join a group and must accept the invitation to receive the benefits of the group.

Groups act on two levels:

- A user that has the right to edit group rights may assign rights to that group. Any users in the group can then have a specific set of rights assigned to them. This is very similar to role and rights assignment, except that users must accept an invitation to join a group. The screenshot below shows an example of a group edit page for an administrator, where rights may be assigned to this group.

The screenshot shows a web interface for editing a group named 'berkman_test'. At the top, there is a header bar with the group name and a close button. Below this, there is a 'Name' field containing 'berkman_test'. A checkbox labeled 'Assign rights to this group' is present, with a note below it stating 'Note: This is a dangerous field to play with.' Below the checkbox is a table with three columns: 'Members', 'Owner', and 'Remove'. The table lists six users: Daniel Collis Puro, Laura Miyakawa, J S Diaz, J Diaz, Andrea Goethals, and Wendy Gogel. Each user has a checked checkbox in the 'Owner' column and an unchecked checkbox in the 'Remove' column. Below the table is a large text area with the placeholder text 'Enter emails, one per line'. At the bottom of the form are two buttons: 'UPDATE' and 'DELETE'.

Members	Owner	Remove
Daniel Collis Puro	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Laura Miyakawa	<input checked="" type="checkbox"/>	<input type="checkbox"/>
J S Diaz	<input checked="" type="checkbox"/>	<input type="checkbox"/>
J Diaz	<input type="checkbox"/>	<input type="checkbox"/>
Andrea Goethals	<input type="checkbox"/>	<input type="checkbox"/>
Wendy Gogel	<input type="checkbox"/>	<input type="checkbox"/>

- A user without the right to edit group rights that creates a group may assign file access to one or more files to a group they created. See “File Visibility” for more information. The screenshot below shows an example of a group edit page for a standard user. Note that a standard user may not assign rights to a group.

Test Group

Name

Test Group

Members

Steph

Admin (Invited by you less than a minute ago.) (Re-send invite)

Owner

☒

☐

Remove

☐

☐

Enter emails, one per line

UPDATE

DELETE

File Visibility

File accessibility is controlled by several facets, described below.

The right to view all items (refer to “Rights” section, “view_items” right) can be assigned to a user directly, to a user through a role that user has, or to a user through a group that user belongs to. This permission is managed through the Zone1 admin interface.

Additionally, an owner of a file may mark it as “Partially Open” and may specify one or more groups of users that can view the file.

A file marked as “Dark” is only visible to the owner of the file and any user that has the right to view all items assigned to the user directly, to a role the user has, or to a group the user belongs to.

Additionally, a user with a right to view preserved flag content may view any file that has the preserved flag, regardless of its permissions status. This right is managed through the Zone1 admin.

The path of logic for whether a file is visible to a user is:

- If a file is marked as “Open”, it is visible to all. Note that regular users may not mark files as “Open” unless they have been given this right.
- If a file is marked as “Partially Open”, it is visible to the owner, any users in any group that the owner has given access to view the file, and any users that have been assigned the right to view all items either directly, through a role they have, or through a group they belong to. If the file has a preserved flag, it is also visible to any users that have the right to view preserved flag content.
- If a file is marked as “Dark”, it is visible to the owner and any users that have been assigned the right to view all items either directly, through a role they have, or through a group they belong to. If the file has a preserved flag, it is also visible to any users that have the right to view preserved flag content.