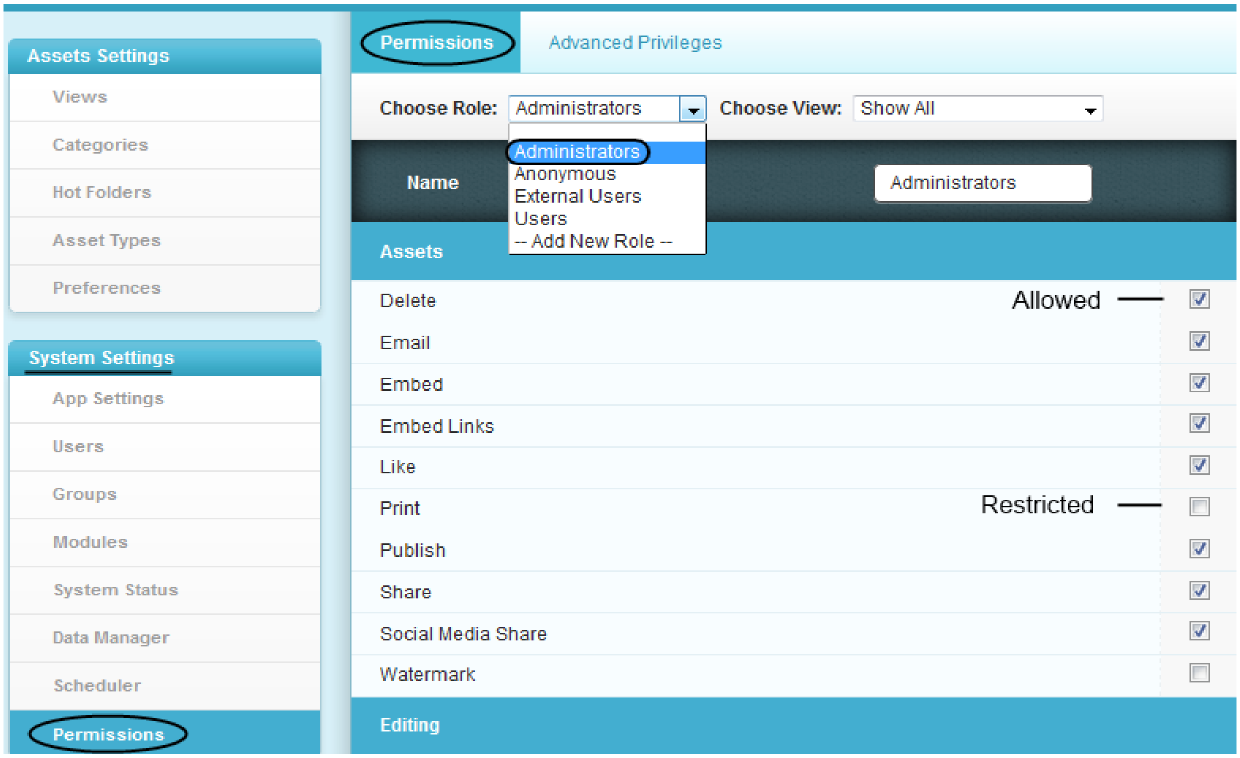
Defining Roles and Custom Permissions

Users are granted or denied access to every feature in EnterMedia based on role assignment and application preferences. Building roles is important for creating the division of privilege between limited accounts, standard users, power players and administrators. By clearly establishing the benefits and limitations of each role before adding users to the system, site administrators can be sure that no user will be able to act outside of a clearly defined context.

To view the default roles or to create a new one go to Settings | (System Settings) Permissions | Permissions (tab) and select an option. The existing settings for administrators and anonymous users can be used to define the minimum and maximum access within the application. The anonymous role is used to set the standard for users who do not have accounts or group assignments within the application. If you want the general public to be able to access a catalog without signing in, this is where to begin. Keep in mind that a private application (set in Data Manager | cagalogsettings | assetviewispublic) will not allow anonymous users to view assets without them being marked for public use. The administration role generally has access to everything. Please note that some areas of the application still require administrator group membership in addition to role assignment.



Choose Role: Administrators Choose View: Show All

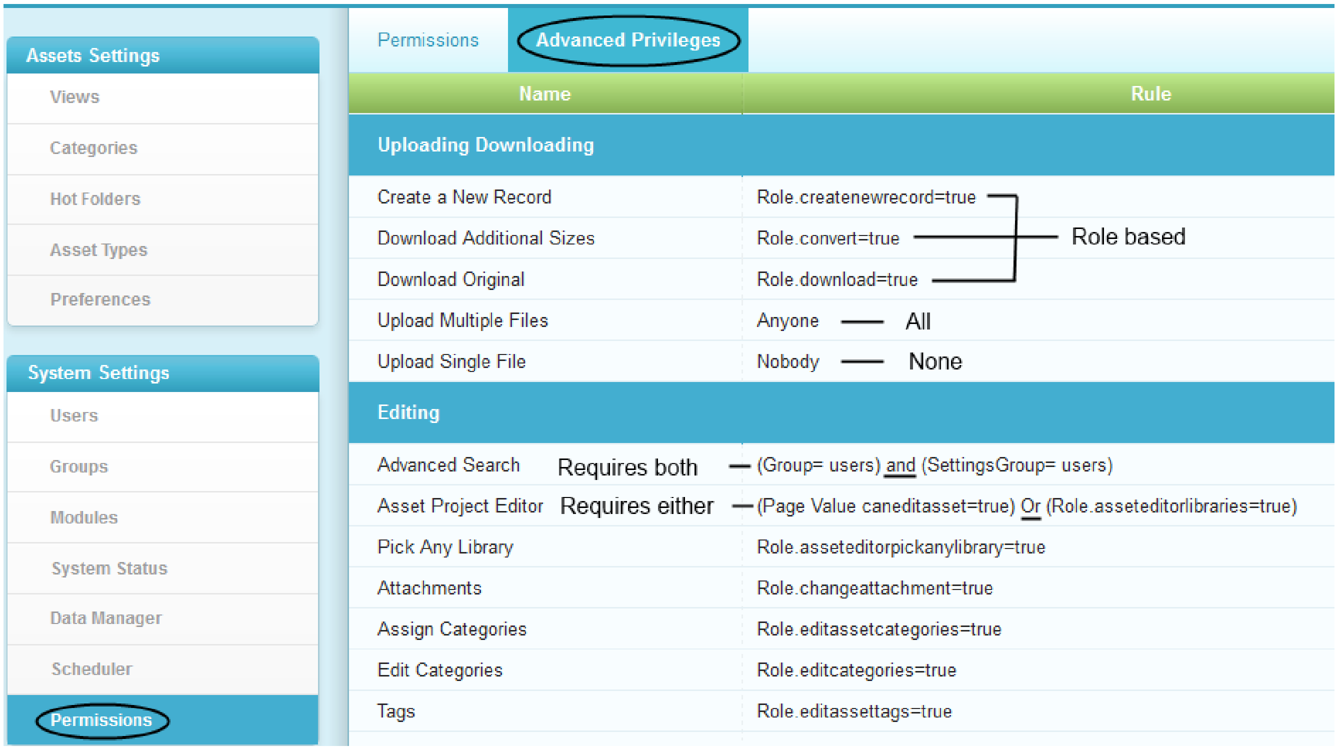
Name: Administrators

Assets

Delete	☑
Email	☑
Embed	☑
Embed Links	☑
Like	☑
Print	□
Publish	☑
Share	☑
Social Media Share	☑
Watermark	□

Roles and users have a one to one ratio within a single catalog. A user can have a different role in another catalog. Each catalog can have an unlimited number of roles. In order to increase the options of an individual user they should be moved to a more permissive role, rather than making changes to the role itself. Individual roles can be tweaked, but be aware that changes to a role will apply to all users.

Permission customizations and application overrides can be established in the Settings | (System Settings) Permissions | Advanced Privileges (tab) area. Here the terms of each permission are determined on a per application basis. 'Role.featureid=true' means that the application will refer to a role when determining whether a user can use a feature. Each permission can be set up to refer to groups or individual users as well. AND / OR logic is also available to create more complex access requirements. IE a user may be required to be a member of both a role or a group in order to access secure metadata, or a user may need to belong to a certain role or an internal group in order to access a second application.



Name	Rule
Uploading Downloading	
Create a New Record	Role.createnewrecord=true
Download Additional Sizes	Role.convert=true
Download Original	Role.download=true
Upload Multiple Files	Anyone
Upload Single File	Nobody
Editing	
Advanced Search	(Group= users) and (SettingsGroup= users)
Asset Project Editor	(Page Value caneditasset=true) Or (Role.asseteditorlibraries=true)
Pick Any Library	Role.asseteditorpickanylibrary=true
Attachments	Role.changeattachment=true
Assign Categories	Role.editassetcategories=true
Edit Categories	Role.editcategories=true
Tags	Role.editassettags=true

Role based

All

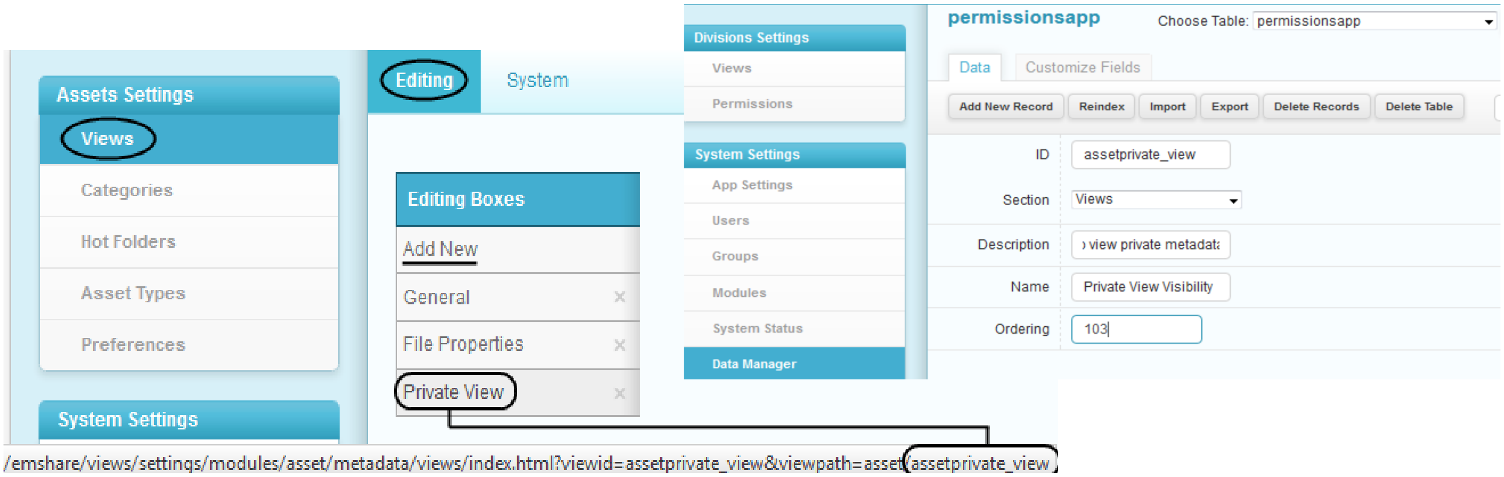
None

Requires both

Requires either

In some cases, an administrator may want to create a custom permission. A common example of this is adding a private metadata view to the asset metadata viewing area. The General and File Properties ship by default and are public to all users. This can also be changed by creating a custom permission.

For an example, create an additional view called 'Private View' in the Settings | Views | Editing (tab) by clicking 'Add New' under editing boxes. By default the system will assign an internal to the field of 'assetprivate_view'. Confirm the ID by hovering over the new view and reading the url at the bottom of the browser. When this is done proceed to the Data Manager and drop down to the permissionsapp (table). Click 'Add New Record' and fill in the appropriate information. Once all of the blanks are filled in the permission must be set in the Application Preferences area. By default the permission is turned off for all users.



Choose Table: permissionsapp

ID	assetprivate_view
Section	Views
Description	› view private metadat:
Name	Private View Visibility
Ordering	103

/emshare/views/settings/modules/asset/metadata/views/index.html?viewid=assetprivate_view&viewpath=asset/assetprivate_view