eProof Manual for Administrator

CONTENTS

1. INTRODUCTION
***2.* CONFIGURING USERS AND GROUPS**
- *2.1. Creating User Accounts*
- *2.2. Creating User Groups*
- *2.3. Assigning Users to Groups*
- *2.4. Allocating Permissions*

3. SETTING UP NOTIFICATION SYSTEM
- *3.1. Configuring Job/Folder Notifications*
- *3.2. Configuring Global Notifications*
- *3.3. Configuring Notifications for Involved Users*
- *3.4. Inheriting Notification Subscriptions*
- *3.5. Configuring Notifications for Root Folder*
- *3.6. Disabling/Deleting Notification Subscriptions*

1. Introduction

eProof is the premier and distinctive web-based proofing solution that helps conveniently proofread and correct jobs over the Internet from anywhere in the world and at any time.

With eProof you can:

- Publish proofs in the online eProof system to show them to proofing users
- View jobs online on the Internet at any time, in real time
- Monitor correction requests made by users to any objects on the proof: text, images, tables, or to the proof page as a whole, - in real time
- Use a range of standard request development states to facilitate your cooperation with the proofing user
- See changes on the layout highlighted in a different color to easily distinguish between the already altered objects and those still awaiting alteration
- Track correction requests ever made in a job
- View job pages with both current and previous corrections highlighted
- Create subsequent versions of a job to show proof files after requested corrections are applied
- Obtain comprehensive status information for jobs
- Release jobs for production (if you have manager’s rights)
- Share your work in a reliable and secure environment with the advanced security system of eProof

What's more, the eProof user-friendly interface is extremely intuitive, involving basically no learn-how-to practices. You will find no difficulty in finding out what to do next, as you are provided only with those features that you really need for your work in the system.

This manual is designed to guide you through the essential aspects of eProof administration and highlights the three main areas of administrator's activities:

- configuring users and groups
- managing the notification system
- working with color profiles

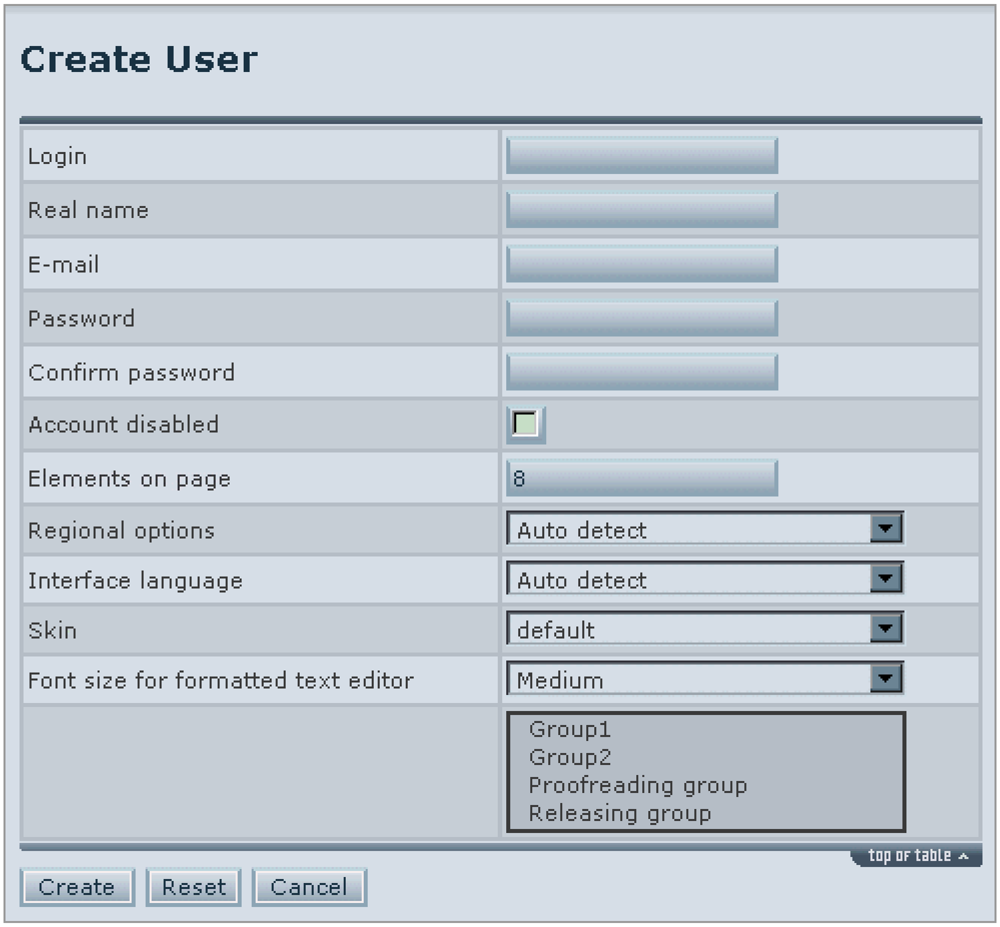
2. Configuring Users and Groups

2.1. Creating User Accounts

User accounts are used to define and authorize system users. A user account includes a login name and a password for identification purposes, both registered in the system. Users with wrong credentials will be denied access to the system as well as to jobs and proofs posted online.

To create user account:

1. Choose Users from the Administration menu. The Web Page eProof - Users featuring a list of user accounts existing in the system and allowing registering a new user account appears on the screen.
2. Click the Create User button. You are taken to the Create User web page where you can define settings for the new user account.



Create User

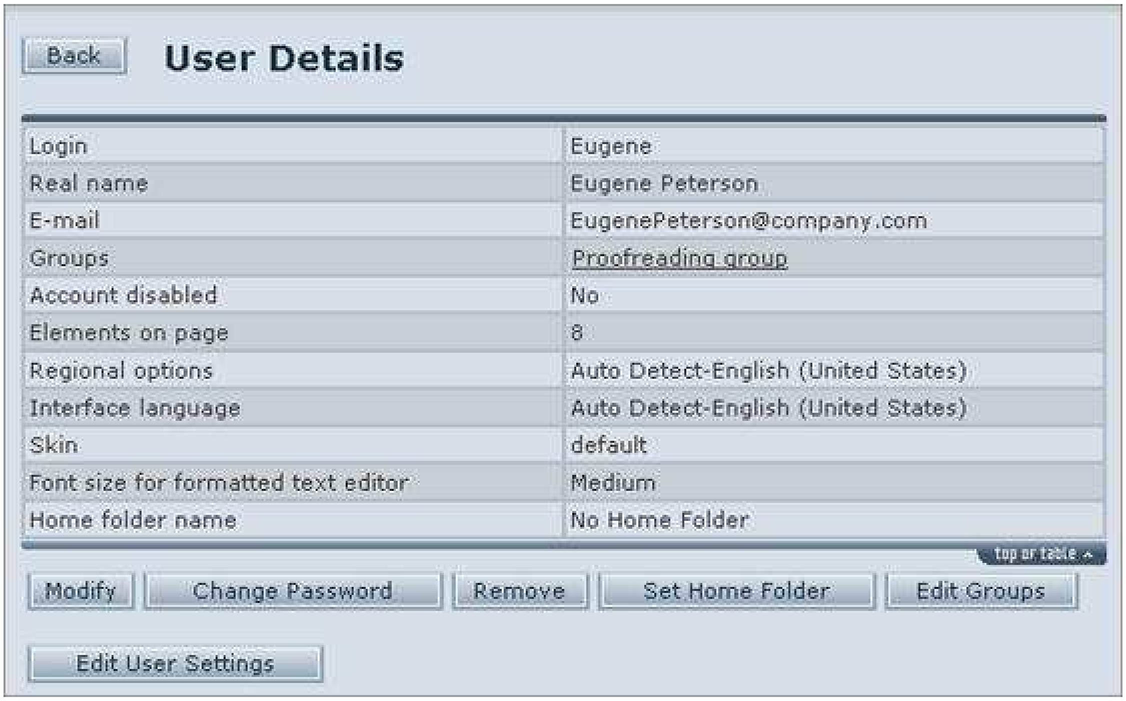
Login	
Real name	
E-mail	
Password	
Confirm password	
Account disabled	□
Elements on page	8
Regional options	Auto detect
Interface language	Auto detect
Skin	default
Font size for formatted text editor	Medium
	Group1 Group2 Proofreading group Releasing group

The user account settings and options are as follows:

Login	The login name used to enter the system
Real Name	The person’s real name
E-mail	The person’s e-mail address
Password	The password to be used by this user for entering the

	system
Confirm Password	Enter the password once again to confirm it.
Account Disabled	Select this check box when you want to disable the current user account. The user will no longer be able to enter the system.
Elements on Page	Specify the maximum number of list elements to show in one portion on page. The default value is 8. Thus, the user will be shown, for example, a portion of eight correction requests in the requests list. To display subsequent portions, the user will have to click button Next.
Regional Options	Choose the user's location from this drop-down list box. This data is essential for defining the currency, numbers, time and date formats. You can choose to leave the default option "Auto-Detect" selected. With the "Auto-Detect" option enabled, the system automatically detects the user's whereabouts.
Interface Language	Select the language of the graphic user interface. You can choose to leave the default option "Auto-Detect" selected. With the "Auto-Detect" option enabled, the system automatically detects the interface lingo of the user's PC and assigns this language to the eProof UI.
Skin	The skin of the eProof user interface for the current user.
Font Size for Formatted Text Editor	Choose between "Small", "Medium", and "Large" as the font size of text extracted from proof and shown in Formatted Text Editor for this user.
Select Initial User Groups	Highlight group(s) to which you want to assign the current user.

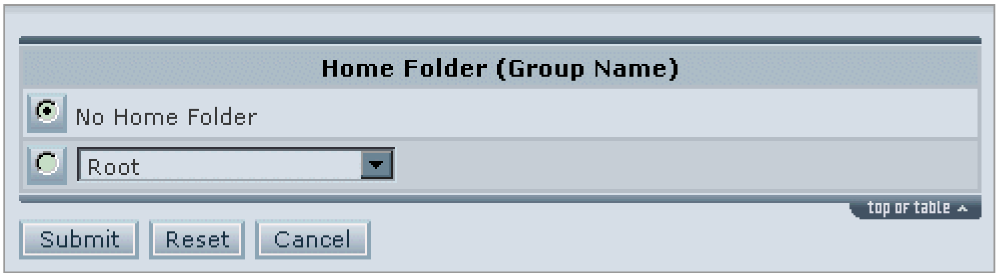
3. Press Create. The User Details page, illustrated below, presents description of the user account you have just created.



User Details

Login	Eugene
Real name	Eugene Peterson
E-mail	EugenePeterson@company.com
Groups	Proofreading group
Account disabled	No
Elements on page	8
Regional options	Auto Detect-English (United States)
Interface language	Auto Detect-English (United States)
Skin	default
Font size for formatted text editor	Medium
Home folder name	No Home Folder

4. Click button Set Home Folder. You switch to page Set Home Folder for User.
5. Select the Home Folder for this user from the drop-down list box.



Home Folder (Group Name)

● No Home Folder

○ Root

Note: The Home Folder option defines the folder that will be shown to the user on logon. No folders above it in folders hierarchy will be available him. Alternatively, you can elect to determine the desired Home folder for all the user group to simplify the account creation process. By default, the user is assigned no Home folder. This setting can be left undefined if you want all folders to be available for the user.

6. Push Submit.
7. Repeat Steps 1 - 6 for each user you want to create.

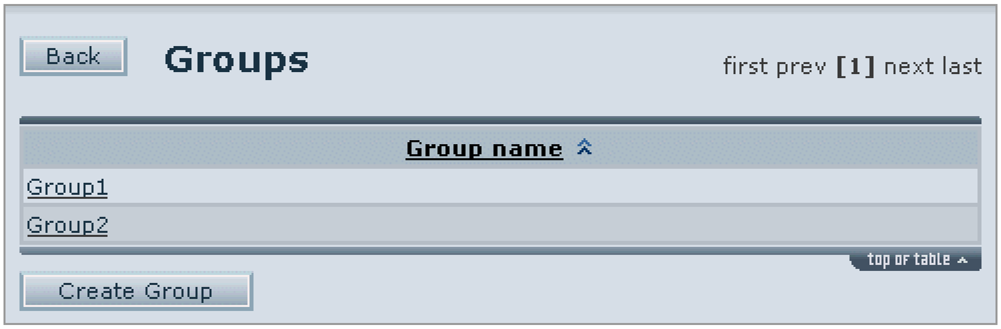
2.2 Creating User Groups

Significantly facilitating the process of user configuration, user groups provide a quick and easy way to allocate identical permissions for multiple user accounts. You are spared multiple user configuration steps and are instead enabled to assign permissions to a group of users as a whole rather than configure each individual user discretely.

Following the instructions below, you may create two user groups: Proofreading group and Releasing group. The Proofreading group will comprise multiple proofreading users and the manager (the user who, in addition to proofing permissions of this group, will also be allowed to release the job). The Releasing group will only include the manager granting this person the permission to release the job. Thus, proofreading users should be included in the Proofreading group, while the manager will belong to both the Proofreading and Releasing groups.

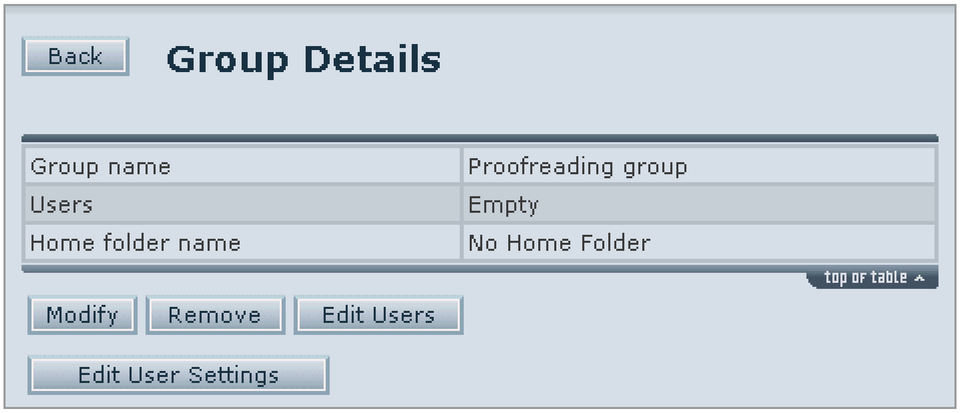
To register user groups:

1. Choose Groups from the Administration menu. Web Page eProof - Groups appears.



Group name
Group1
Group2

2. Click the Create Group button. Web Page eProof - Create Group opens up.
3. In the Group Name text box, enter a name for the current group
4. Press Create. You are shown details of the newly created user group.



Group name	Proofreading group
Users	Empty
Home folder name	No Home Folder

5. Repeat Steps 1 - 4 to create another group. (In this manual, we have called the second group "Releasing group".)

2.3 Assigning Users to Groups

A user can be assigned to one or multiple groups. User groups comprise users who are to be granted identical permissions.

To assign users to groups:

1. Choose Groups from the Administration menu.
2. Click on the desired group name. Web Page eProof - Group Details opens up.
3. Click the Select Users Button. Web Page eProof - Select Users for Groups appears.
4. Select users from the right pane and press the Add User button. Selected users' names appear in the left pane.
5. Click Submit when finished.

Note: Alternatively you may assign user to group whrn creating the user if the desired group already exists. For this on the Web Page eProof - Create User select the desired group from the Select initial user groups List box.

2.4 Allocating Permissions

Permissions define user's access to system objects and to various actions associated with these objects. You are enabled to allow or deny a particular user access to a particular job or particular action within the job. By default, unconfigured users and groups are restricted access to all system objects. Thus, the user accounts and groups created in the previous subsection do not currently have access to any system job or folder.

In this subsection, you will assign permissions to the proofreading and releasing groups. You will allow the Proofreading group proofing and request-creating functions and assign the Releasing group permissions to manage proofreaders' requests and release the job. Once the groups are configured, the users inherit the privileges assigned to their parent groups.

☑ **Permission System Rule 1**: Users inherit privileges of their parent groups. However, users do not unconditionally take over group's privileges, since users may have their own privileges. Refer to Rule 2 below for information on working out verdict privileges for users.

☑ **Permission System Rule 2**: User's own privileges always take priority over those of the parent group.
If a user has an explicit “allow” or “deny” permission, the permission of the parent group (whichever it can be) is neglected, and the user is respectively "allowed" or "denied" the permission, as illustrated in the table below.

User’s own permission	Group’s permission	Verdict for user
Allow	Allow	Allow
Allow	Deny	Allow
Allow	Unconfigured	Allow
Deny	Allow	Deny
Deny	Deny	Deny
Deny	Unconfigured	Deny

However, if the user's privileges are “unconfigured”, the parent group's privileges are taken over to the user with a tendency to restriction, as illustrated in the table next.

User’s own permission	Group’s permission	Verdict for user
Unconfigured	Allow	Allow
Unconfigured	Deny	Deny
Unconfigured	Unconfigured	Deny

As can be observed from the tables above, a user is finally allowed a privilege only if the user has an explicit "allow" privilege or when the user is unconfigured but the parent group is explicitly "allowed" this privilege. If both the user and user group are “unconfigured”, both are denied the respective privilege.

A user may be included into multiple groups whose privileges may be inconsistent. In this case, the groups’ privileges are summed up to form one “aggregate group privilege”, which would then be totted up with the user’s own privilege.

☑ **Permission System Rule 3**: Privileges of different groups are of the same priority. If respective privileges of the groups to which user belongs are consistent, this privilege becomes the “aggregate group privilege”. If inconsistent, however, the privileges are considered with a tendency to restriction. The table below features the inconsistency cases and the resulting verdict:

Privilege of Group1	**Privilege of Group2**	**Privilege of Group3**	**Aggregate Privilege**
Allow	Allow	Deny	Deny
Allow	Allow	Unconfigured	Allow
Deny	Deny	Allow	Deny
Deny	Deny	Unconfigured	Deny
Unconfigured	Unconfigured	Allow	Allow
Unconfigured	Unconfigured	Deny	Deny
Unconfigured	Unconfigured	Unconfigured	Deny

As can be observed from the table above, a privilege is "allowed" only if there is no occurrence of explicit restriction for the privilege and it is "allowed" for at least one of user's groups. The “unconfigured” state of a privilege in all user groups results in denying this privilege.

After the “aggregate group privilege” is worked out, this privilege is summed up with the user's own privilege according to Rule 2.

Note: You will have to consider priorities and sum up privileges only if the groups' users were created and configured by somebody else. Since you might not have the right to configure users discretely, aside from their parent groups, you would not be able to grant users their own permissions. With their own permissions unconfigured, users take over group's permissions unconditionally.

For more information on the eProof permission system and its rules, refer to the white paper.

Prior to starting configuring the groups, you should decide which system element you would set up: the job or the job folder.

Job permissions provide access to the particular job whereas folder permissions refer to all jobs that are or will be included in this folder. For example, a user granted the permission to view a folder would see all jobs of that folder, while the user allowed to view an individual job of that folder would have no access to the other jobs. It is up to you to decide which access scheme is most appropriate in your case.

☑ **Permission System Rule 4**: Jobs inherit permissions of their nesting folders. However, jobs do not unconditionally take over folder's permissions, since jobs may have their own permissions. Refer to Rule 5 below for information on working out verdict permissions for jobs.

☑ **Permission System Rule 5**: Permissions of a job always take priority over those of the nesting folder.
If a job has an explicit “allow” or “deny” permission, the nesting folder’s permission (whichever it can be) is neglected, and the user is respectively allowed or denied access to this job, as illustrated in the table below.

Group or user permission towards:		**Verdict permission towards:**
Job	**Folder**	**Job**
Allow	Allow	Allow
Allow	Deny	Allow
Allow	Unconfigured	Allow
Deny	Allow	Deny
Deny	Deny	Deny
Deny	Unconfigured	Deny

However, if the job’s permissions are “unconfigured”, the nesting folder’s permissions are taken over to the job with a tendency to restriction, as illustrated in the table below.

Group or user permission towards:		**Verdict permission towards:**
Job	**Folder**	**Job**
Unconfigured	Allow	Allow
Unconfigured	Deny	Deny
Unconfigured	Unconfigured	Denied

The eProof powerful permission system allows a wealth of flexibility and options.

Each system user can be configured to have access only to those objects and actions to which this person is entitled.

Example 1. Group is allowed access to Folder1. Folder1 includes Job1.1 and Job 1.2. Since jobs inherit permissions from their parent folder, by default, users can view both Job1.1 and Job1.2.
You may deny access to Job1.1 to one or more users, so that they could only view Job1.2. See More How-To's at the end of this section for instructions on restricting access to jobs and subfolders.

Example 2. Group is allowed access to Folder2. Folder2 includes Subfolder2.1 and Subfolder2.2, each having one or more jobs. Since subfolders inherit permissions from their parent folder, by default, users can view both Subfolder2.1 and Subfolder2.2, as well as their jobs.

You may deny access to Subfolder2.1 to one or more users, so that they could only view Subfolder2.2. Furthermore, you may deny access to one or more jobs inside the "allowed" Subfolder2.2 and allow access to one or more jobs of the "denied" Subfolder2.1. See More How-To's at the end of this section for instructions on restricting access to jobs and subfolders.

For more information on the eProof permission system and its rules, refer to the white paper. See More How-To's at the end of this section for instructions on restricting access to jobs and subfolders.

Once you elect which system object to configure, follow the instructions below to assign access permissions for a folder or individual job to the groups.

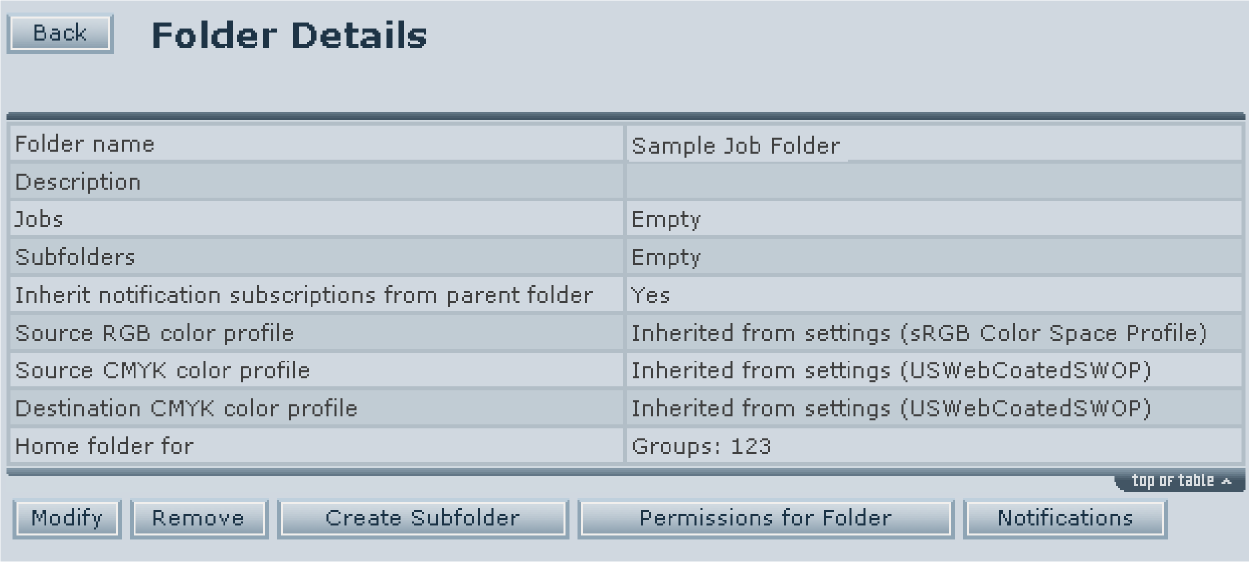
To assign access permissions for folder (job) to user groups:

1. Click the ℹ Information button under the folder or job you want to make accessible to users.
2. Press button Permissions for Folder (in folder details) or Permissions for Job (in job details).
3. From the left-hand drop-down box, select the proofreading group and click Add.
4. Check permission Create/Manage Own Requests. (The Read Folder Details and Read Job Details permissions, which allow access to the current folder and its jobs, are ticked by default.)
5. From the left-hand drop-down box, select the releasing group and click Add.
6. Check permissions Create/Manage Own Requests, Modify Requests of Others, Delete Requests of Others, and Do/Undo Release. (The Read Folder Details and Read Job Details permissions, which allow access to the current folder and its jobs, are ticked by default.)
7. Push Done.

Following Step 1, you click the ℹ Information button under the folder or job that you want to make accessible to users. As a result, the Folder Details or Job Details page offers on the screen. (For the conciseness' sake, we describe pages related to folder configuration in this subsection. Since folder and job setup is very similar, you may refer to page description below when configuring individual jobs.)

Web Page eProof – Folder Details

The Folder Details page, illustrated below, features details of the selected job folder and allows allocating permissions for the current folder. Folder's permissions are taken over to all jobs and subfolders that are or will be included into this folder. If you give the "allow" permission to the folder, the folder's contents will have the permission too (unless explicit restriction is issued for a job or a subfolder; see More How-To's at the end of this subsection for instructions).



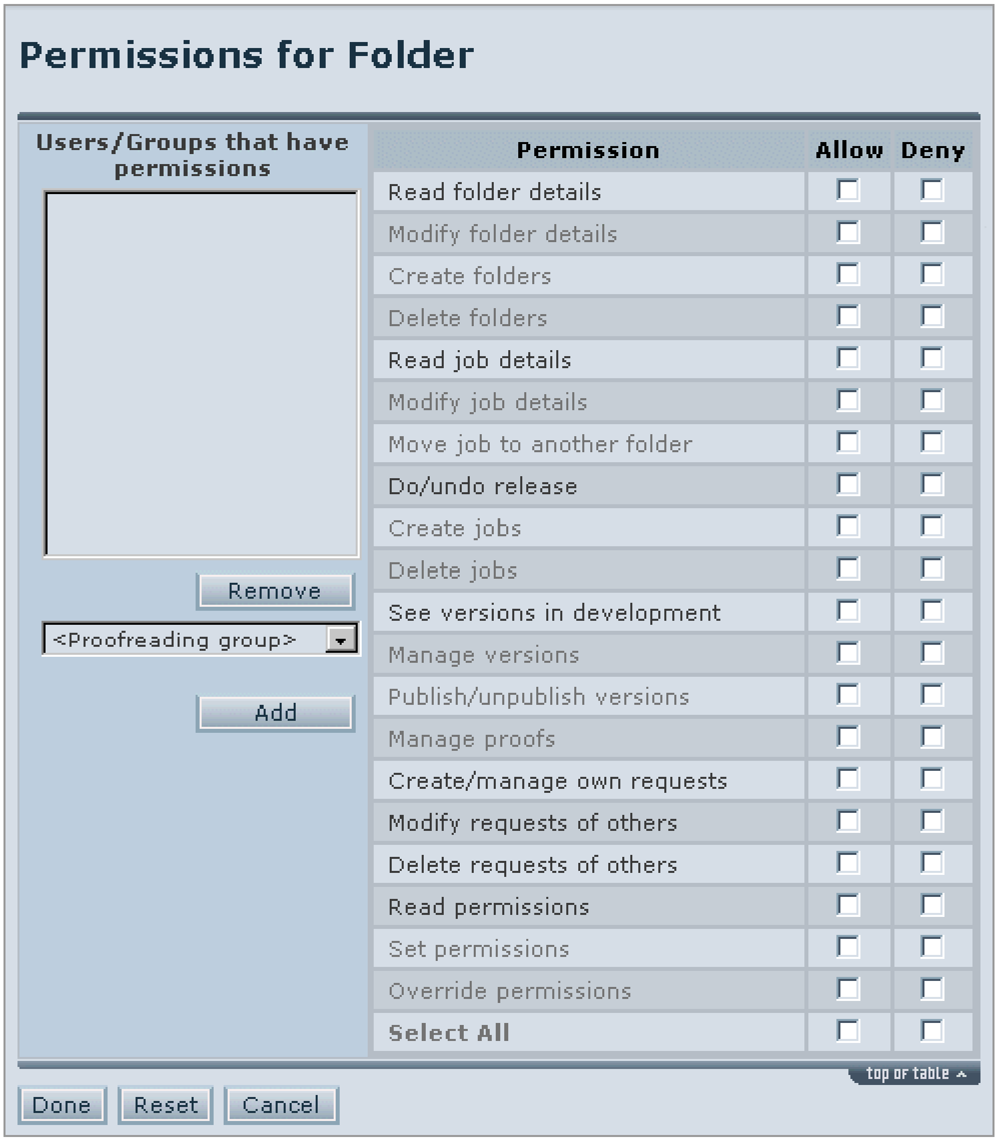
Folder Details

Folder name	Sample Job Folder
Description	
Jobs	Empty
Subfolders	Empty
Inherit notification subscriptions from parent folder	Yes
Source RGB color profile	Inherited from settings (sRGB Color Space Profile)
Source CMYK color profile	Inherited from settings (USWebCoatedSWOP)
Destination CMYK color profile	Inherited from settings (USWebCoatedSWOP)
Home folder for	Groups: 123

The page provides the folder name and description as well as titles of the jobs assigned to this folder. You can click a job to view the job details. Press button Permissions for Folder. You are taken to page Permissions for Folder.

Web Page eProof – Permissions for Folder

The Permissions for Folder page, illustrated below, allows assigning permissions for the current folder to groups and individual users.



Permissions for Folder

Users/Groups that have permissions

Permission	Allow	Deny
Read folder details	□	□
Modify folder details	□	□
Create folders	□	□
Delete folders	□	□
Read job details	□	□
Modify job details	□	□
Move job to another folder	□	□
Do/undo release	□	□
Create jobs	□	□
Delete jobs	□	□
See versions in development	□	□
Manage versions	□	□
Publish/unpublish versions	□	□
Manage proofs	□	□
Create/manage own requests	□	□
Modify requests of others	□	□
Delete requests of others	□	□
Read permissions	□	□
Set permissions	□	□
Override permissions	□	□
Select All	□	□

The Permissions for Folder table comprises two panes. The left-hand pane features groups and users that are already configured and allows selecting new groups and users for configuration.

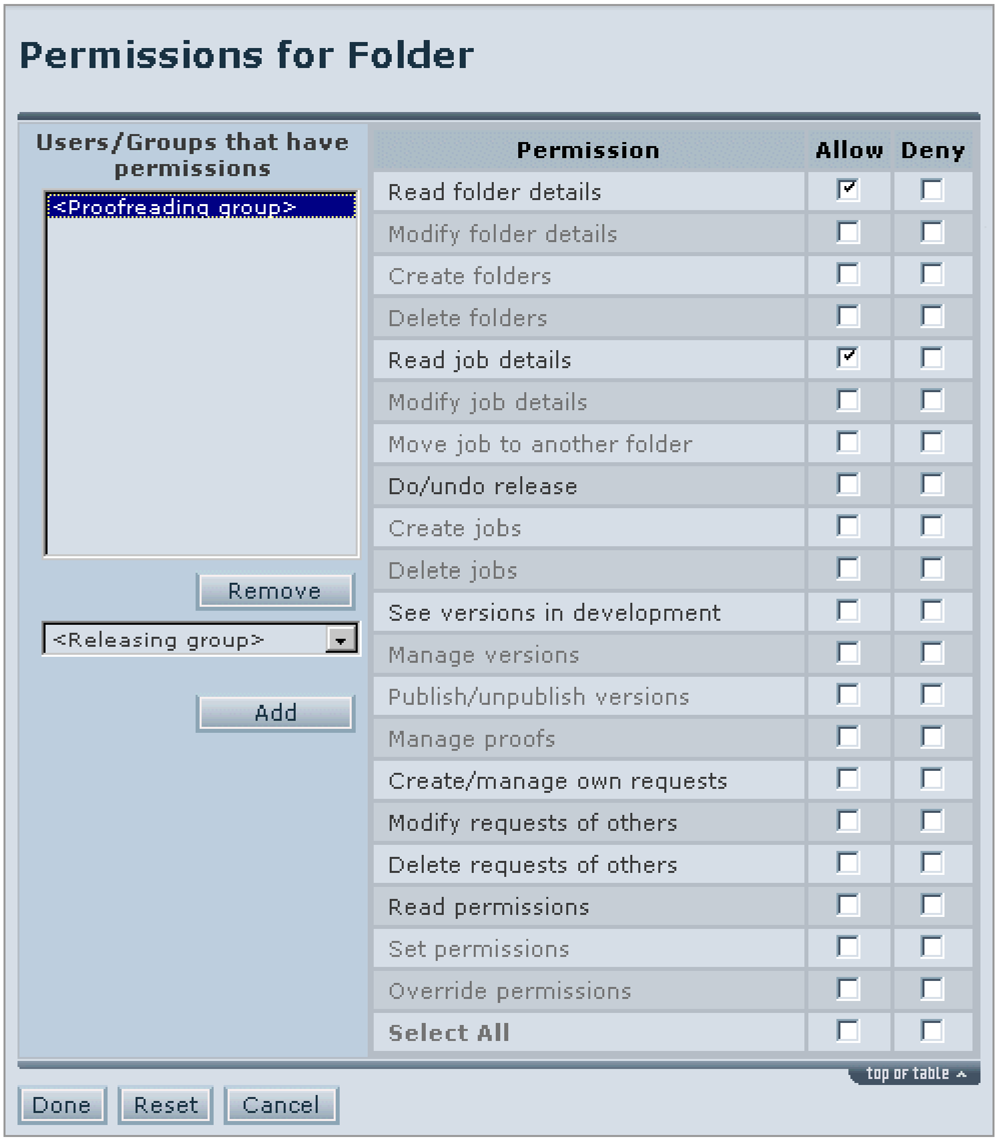
The right-hand pane provides a list of folder permissions, which you can assign to groups or users selected at the left. There are two columns: Allow and Deny. The Allow column lets check permissions in order to allow the corresponding actions. The Deny column allows to restrict permissions by leaving ticks at the corresponding check boxes.

Basically, permissions for folder are identical to job permissions. The only difference lies in a number of additional, folder-specific, permissions (four permissions at the top of the list). Permissions for folder and their definitions are as follows.

Read folder details	Permits user to view subfolders and jobs of current folder, as well as read folder details. If permission "Read job details" is also allowed, user will be able to view the contained jobs, read their details, and view their proofs.
Modify folder details	Permits user to edit folder details (name, description).

Create folders	Permits user to make new subfolders in current folder. Permissions for these subfolders are inherited from their parent folder by default.
Delete folders	Permits user to remove folder. Jobs contained in the folder will be deleted as well.
Read job details	Permits user to view job, read its details, view published versions and their proofs.
Modify job details	Permits user to edit job details (name, brand, country).
Move or copy job to another folder	Permits user to move and copy job to another folder.
Do/Undo release	Permits user to do and undo release of job
Create jobs	Permits user to create jobs in current folder and copy jobs to this folder.
Delete jobs	Permits user to remove job.
See versions in development	Permits user to view unpublished versions.
Manage versions	Permits user to create, modify, and delete versions in job.
Publish/Unpublish versions	Permits user to publish and unpublish versions in job. (Can be assigned only if the previous permission is allowed.)
Manage proofs	Permits user to upload proof files as well as replace and delete existing files in job.
Create/manage own requests	Permits user to create correction requests as well as modify and delete them.
Modify requests of others	Permits user to edit requests created by other users.
Delete requests of others	Permits user to remove requests created by other users.
Read permissions	Permits user to view permissions assigned to other users within current job or folder.
Set permissions	Permits user to assign permissions within current job or folder.
Override permissions	Permits user to re-allocate permissions in emergency cases, e.g. when permissions set exclude anyone's access to system objects. (This function is currently not implemented.)
Select All	Mark this check box to select ALL permissions in the Allow column.

From the left-hand drop-down list box, select the group to which you want to assign proofreading permissions and click Add. The group becomes selected and appears in the upper Users/Groups that Have Permissions area. The right-hand Permissions pane shows ticks in the Allow column at those permissions that are checked by default for the selected group, as shown below.



Permission	Allow	Deny
Read folder details	☑	□
Modify folder details	□	□
Create folders	□	□
Delete folders	□	□
Read job details	☑	□
Modify job details	□	□
Move job to another folder	□	□
Do/undo release	□	□
Create jobs	□	□
Delete jobs	□	□
See versions in development	□	□
Manage versions	□	□
Publish/unpublish versions	□	□
Manage proofs	□	□
Create/manage own requests	□	□
Modify requests of others	□	□
Delete requests of others	□	□
Read permissions	□	□
Set permissions	□	□
Override permissions	□	□
Select All	□	□

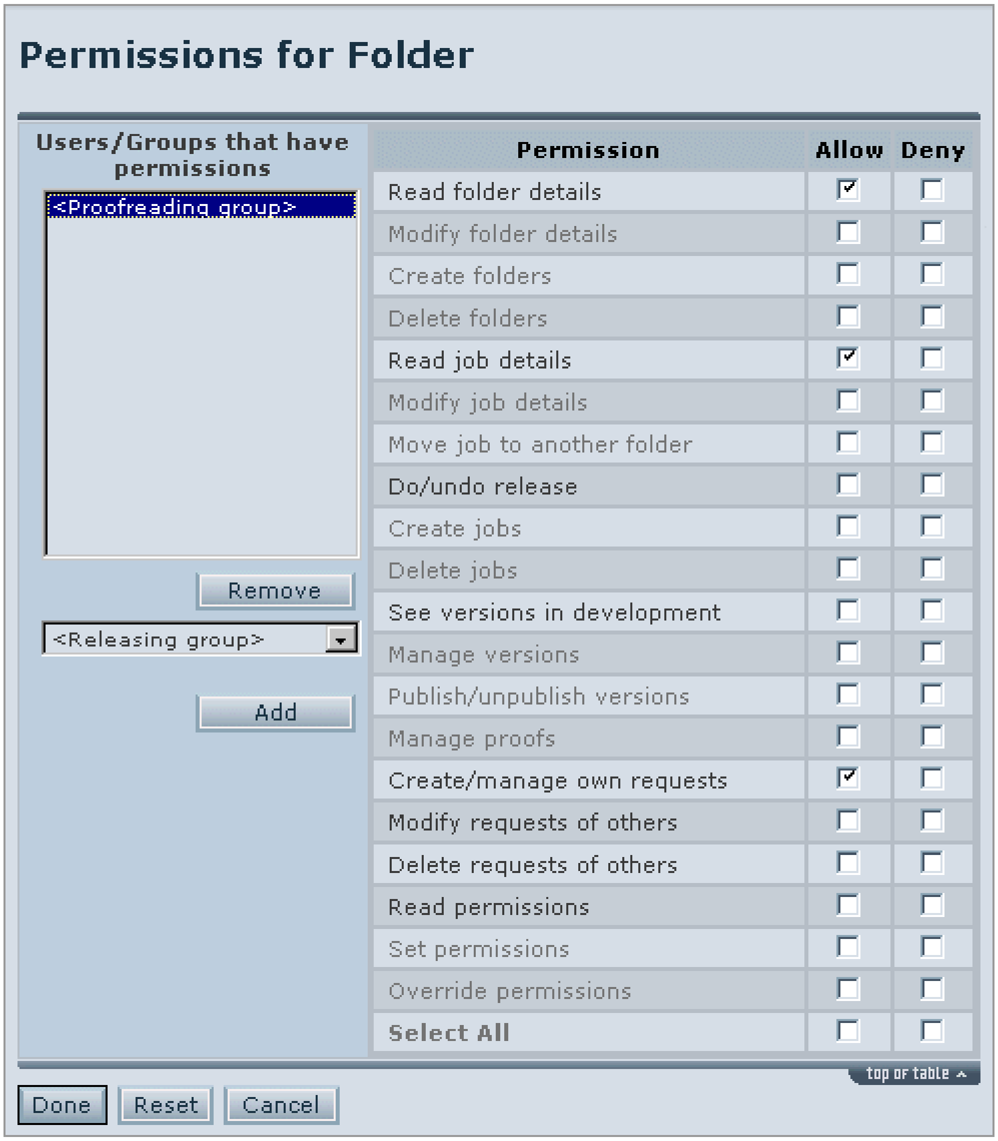
Note: The default permissions appear initially selected to facilitate the process of configuration. These privileges are most likely to be assigned to system users. Although the permissions are checked by default, they are not applied until you confirm them by clicking button Done.

The selected permissions are Read Folder Details and Read Job Details. These permissions allow viewing information about the current folder and its jobs and viewing the jobs and their proof files.

Tip: With no other permissions set, the two default permissions provide users with "read-only" access to the selected system object. The users are only allowed to view the current folder or job in the system.

As can be observed from the picture above, some permissions may be dimmed. The dimmed permissions are disabled, so you cannot assign these permissions to users or groups. Since you have limited rights for creating and configuring users/groups in the system, you are allowed a restricted number of permissions at your disposal. The selection of the "full-color" permissions comprises options mostly relating to proofreading and releasing. These are most probable types of activity that you might need to permit your users within the eProof system. The choice of permissions you are enabled to assign is up to administrator.

Check permission Create/Manage Own Requests in the Allow column to permit users of the selected group to make, modify, and delete their correction requests. Each user is only allowed to manage requests created by him/herself. The Permissions for Folder table should now look something like the picture below.



Permissions for Folder

Users/Groups that have permissions

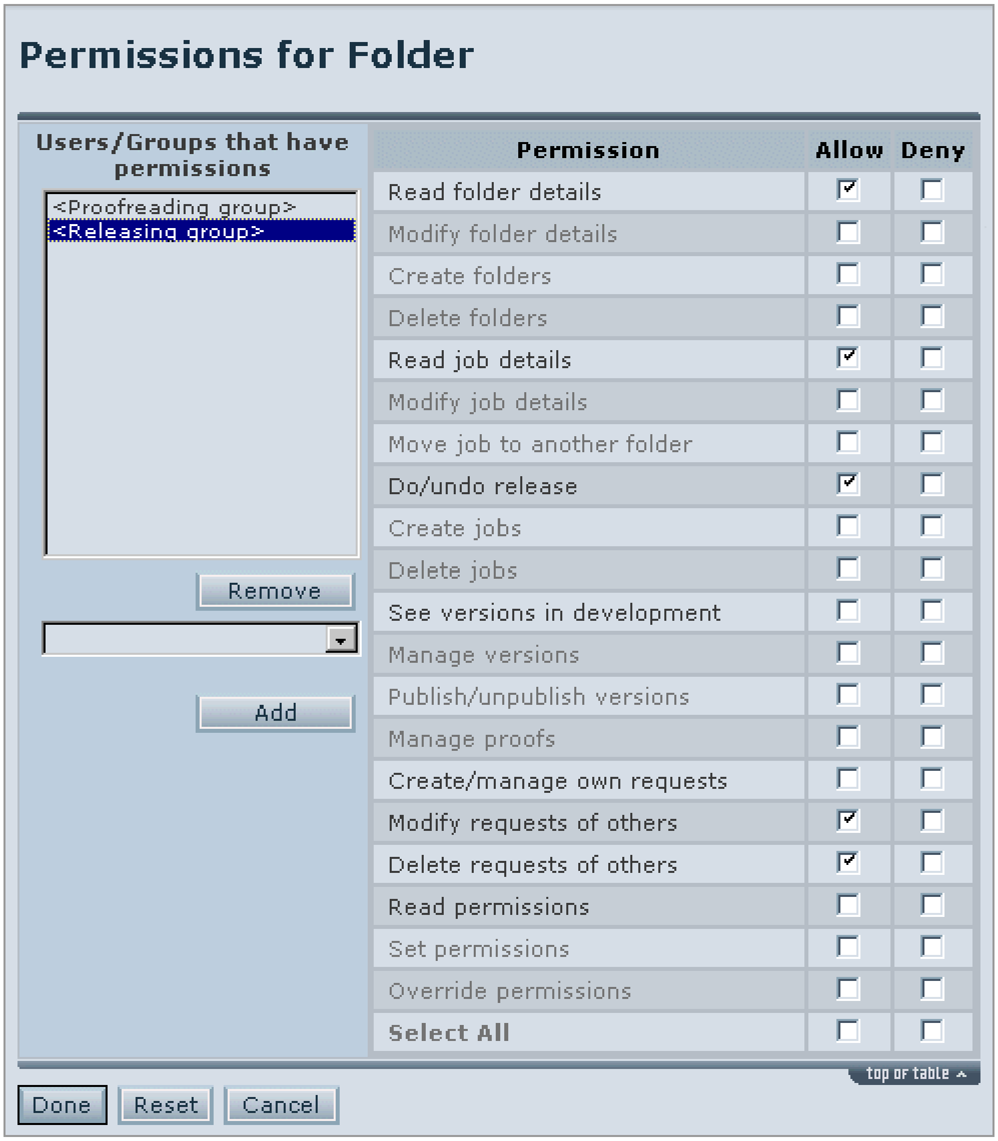
<Proofreading group>

<Releasing group>

Permission	Allow	Deny
Read folder details	☑	□
Modify folder details	□	□
Create folders	□	□
Delete folders	□	□
Read job details	☑	□
Modify job details	□	□
Move job to another folder	□	□
Do/undo release	□	□
Create jobs	□	□
Delete jobs	□	□
See versions in development	□	□
Manage versions	□	□
Publish/unpublish versions	□	□
Manage proofs	□	□
Create/manage own requests	☑	□
Modify requests of others	□	□
Delete requests of others	□	□
Read permissions	□	□
Set permissions	□	□
Override permissions	□	□
Select All	□	□

From the left-hand drop-down box, select the group to which you want to assign releasing permissions and click Add. The group becomes selected and appears in the upper Users/Groups that Have Permissions area. The right-hand Permissions pane shows ticks at the two permissions set by default.

In the Allow column, mark check boxes Do/Undo Release, Modify Requests of Others, and Delete Requests of Others. According to these permissions, users of this group will be able to alter and delete correction requests submitted by other users. They are also permitted to make release of the jobs of the current folder. The Permissions for Folder table should now look something like the picture below.



Permissions for Folder

Users/Groups that have permissions

<Proofreading group>
<Releasing group>

Permission	Allow	Deny
Read folder details	☑	□
Modify folder details	□	□
Create folders	□	□
Delete folders	□	□
Read job details	☑	□
Modify job details	□	□
Move job to another folder	□	□
Do/undo release	☑	□
Create jobs	□	□
Delete jobs	□	□
See versions in development	□	□
Manage versions	□	□
Publish/unpublish versions	□	□
Manage proofs	□	□
Create/manage own requests	□	□
Modify requests of others	☑	□
Delete requests of others	☑	□
Read permissions	□	□
Set permissions	□	□
Override permissions	□	□
Select All	□	□

Since the user assigned to the current Releasing group also belongs to the Proofreading group, the user inherits permissions from both groups. Therefore, even with permission Create/Manage Own Requests unconfigured for the current group, the user will be able to make and manage his or her own requests, since the corresponding permission is allowed for the other group.

Occasionally, you might need to assign some other permissions. Check those permissions in the Permissions pane.

When you are finished, click Done. The permissions are assigned, and you are taken back to the Folder Details page.

More How-To's:
To deny access to a job or subfolder:

1. Click the ⓘ Information button under the job or subfolder you want to make inaccessible to a group or individual user.
2. Press button Permissions for Job in job details or Permissions in folder details.
3. Highlight the group or user in question in the left-hand Groups/Users that Have Permissions area. If the target user/group is not shown in the left-hand area, choose the user or group from the drop-down list box and click Add.

4. In the Deny column, mark check box Read Job Details to deny access to job or Read Folder Details to deny access to folder (and all folder's jobs).
5. Push Done.

3. Setting Up Notification System

eProof notification system is an advanced and flexible system designed to notify users of various eProof events. Notifications can describe events from any job/folder as well as user and system management events and be sent to any user or group. Notification subscriptions are configured by administrator.

There are three types of notification subscriptions in eProof:

- Job/Folder Notifications
- Global Notifications
- Notifications for Involved Users

Job/Folder notifications inform of actions related to jobs and folders. Global notifications deal with user and system management.

Notification for involved users is actually an offshoot of global notifications. They determine whether and which global notifications should be sent to a user that was the object of the action. To receive these notifications, the user may not be subscribed for global notifications but should be configured to receive notifications for involved user. For example, " An account was created for you", "Your account was modified", "Your rights were updated" are notifications sent to the involved user.

Notifications can be sent immediately or dispatched as a daily digest.

3.1 Configuring Job/Folder Notifications

Can be configured either in user/group details or in job/folder details.

To set job/folder notifications in user/group details:

1. Choose Administration / Users (Groups) / particular user (group) / Notifications.
2. Click Add Folder / Job Notifications.
3. Select the particular job or folder from which this user (group) will receive notifications in the corresponding drop-down combo box.
4. Check the desired notification events in the Send Immediately or Send as Daily Digest columns.
5. Click Done when finished.

To set job/folder notifications in job/folder details:

1. Click the Information button under the desired job or folder.
2. In Job/Folder Details page click on the Notifications button
3. Press button Add Notifications.
4. Select the particular user or group to receive notifications in the corresponding drop-down combo box.
5. Check the desired notification events in the Send Immediately or Send as Daily Digest columns.
6. Click Done when finished.

3.2 Configuring Global Notifications

Can be configured both for groups and for users.

To set global notifications for group/user:

1. Choose Administration / Groups (Users) / particular group (user) / Notifications.
2. Click button Add Global Notifications.
3. Check the desired notification events in the Send Immediately or Send as Daily Digest columns.
4. Click Done when finished.

3.3 Configuring Notifications for Involved Users

Can be configured both for all system users and for users of individual group(s).

To set notifications for involved users of an individual group:

1. Choose Administration / Groups / particular group / Notifications.
2. Click button Add Involved Users Notifications
3. Check the desired notification events.
4. Click Done when finished.

To set notifications for involved users for the whole system:

1. Choose Administration / Notifications for Involved Users.
2. Check the desired notification events.
3. Click Done when finished.

3.4 Inheriting Notification Subscriptions

For more convenience, notification subscriptions can be inherited from parent folder or from parent group. Parent folder propagates its subscriptions to child jobs and subfolders, whereas parent group assigns its subscriptions to child users/groups. As a folder/group is specifically configured to receive notifications, their child objects can just be set to inherit the subscriptions from the parent, saving admin's time for configuring all child objects separately.

While group-to-user inheritance is unconditional, folder-to-job inheritance can be enabled (default) or disabled.

To set job/folder to inherit notification subscriptions from parent folder at creation time:

1. Choose Job Selection / Create Job (Create Folder).
2. The Inherit Notification Subscriptions from Parent Folder option is enabled by default. Do not disable this option.
3. Proceed with creating the job (folder) and click Create when finished.

There's a number of general notification settings applicable to the whole system. These settings enable you to activate/deactivate using email notifications in eProof and specify a number of other options.

To configure general notification system settings:

1. Choose Administration / Settings.
2. Here you can define the following options:

Property	Description
Support emails	Defines the email addresses included in the notification messages as eProof support staff addresses. If users have any

	questions or want to modify subscriptions, they'll use this(these) address(es) specified in their messages.
Use mail notifications	Determines whether the notification system is enabled in eProof.
Email sending mode	Specifies the way messages to multiple recipients are dispatched. The same emails can be sent to each user discretely, i.e. multiple recipients - multiple identical messages. Or, single message can be sent to all users subscribed for this notification. In the single message approach, users can be shown either all in the To field or others in the CC field.
Maximum recipients for one letter	In case single message approach is opted in the option above, here you can specify the maximum number of recipients for one letter.
Digest send time	Specifies the local time of daily notification dispatch in the format of 24.00.

3.5 Configuring Notifications for Root Folder

Notifications for the top Root folder are shown in the Administration menu. Subscriptions for this folder are configured the same way as for any other folder. Admin can create basic notifications for the Root and then set child folders/jobs to inherit these subscriptions, adding specific notifications for users/groups separately.

3.6. Disabling/Deleting Notification Subscriptions

Existing notification subscriptions can be disabled or deleted. While you can choose subscriptions to be deleted, disabling applies to all user/group's subscriptions (they can be enabled any time). Please note that you can only delete subscriptions that were created for user/group individually rather than inherited from parent group. Inherited subscriptions cannot be deleted in child objects.

To disable or delete notification subscriptions for group/user:

1. Choose Administration / Groups (Users) / particular group (user) / Notifications.
2. To delete: Check the subscriptions you want to delete and click button Delete Selected.
3. To disable: Click button Disable Notifications. All subscriptions are disabled.