



Arco

Application administrator manual
DocRoom & Routing security

A new era in document management.

Doma 6

Application administrator manual

DocRoom & Routing security

Document reference: 135964

Author: Arco Training Dept. - Kris Steenackers

Manual Modification Follow-Up

Ref.	Date	Author	Modification description
	11/05/2011	Kris Steenackers	Manual creation
135964	19/12/2011	Kris Steenackers	Added chapter <i>Interesting combinations of security settings</i>

Contents

1	DocRoom Security.....	7
1.1	Introduction.....	7
1.2	Main rules.....	7
1.3	Action profiles.....	8
1.3.1	Overview of all actions	8
1.3.2	How to create an action profile?	11
1.3.3	How to edit an action profile?	12
1.3.4	How to delete an action profile?	13
1.4	Folder security.....	14
1.4.1	How to set security on folder level.....	14
1.4.2	How to view folder security settings.....	15
1.5	Document security	16
1.5.1	How to set security on document level	16
1.5.2	How to view document security settings.....	18
1.5.3	Property Assignee and document and folder security	18
1.6	Case Object security	19
1.6.1	Introduction	19
1.6.2	How to set security on a case object	19
1.6.3	How to view case object security settings	21
1.6.4	Users for which we can define folder, document and case object security	21
2	Routing security.....	22
2.1	Introduction.....	22
2.2	Procedure security	23
2.2.1	Procedure security levels.....	23
2.2.2	How to set procedure security	27
2.2.3	How to edit procedure security	27
2.3	Step executors	28
2.3.1	Introduction	28
2.3.2	Default step executors	28
2.3.3	Conditional step executors.....	29
2.4	Delegate(d) work.....	33
2.4.1	Introduction	33
2.4.2	How to delegate work	34
2.4.3	How to edit a delegation	35
2.4.4	How to remove a user from my delegated work list.....	36
2.4.5	How to see which users have delegated work to me?	37
2.4.6	How to view work delegated to you	37
	In your profile, you can see which users have delegated their work list to you.....	37
3	Other security settings.....	38
3.1	Security on user events.....	38
3.1.1	How to set security on a user event.....	38
3.2	Security on custom screens.....	40
3.2.1	How to set security on a custom screen.....	40
3.3	Security on saved queries.....	42
3.3.1	How to create a secured query and set security on it.....	42
4	Interesting combinations of security settings	44
4.1	Allow a user to select another user in the WebInterface and give the selected user pre-defined rights on the concerned document or folder	44
4.2	Allow edit without check-in / check-out	44
4.3	Allow edit of document only after check-in / check-out.....	44

1 DocRoom Security

1.1 Introduction

Security ensures that data stored in DocRoom and Routing cannot be read or compromised by any individuals without authorization.

Just like Routing security, DocRoom security is based on the user's login and password and the groups and roles a user makes part of. Both DocRoom and Routing use the same user list.

DocRoom security is defined in separate actions. All of these actions are gathered in an *Action Profile*.

This Action Profile is linked to users, groups or roles on document, case object or on folder level.

When using folder security, all items that are added to the folder, will inherit the security settings of the folder. (Except for items with security settings that deviate from the folder security of the folder where they are located)

When setting security on document or case object level, you will change the inherited folder security into an 'own security' of the document or case object.

When such a document or case object is moved to another folder, it keeps its 'own' security settings.

1.2 Main rules

The default way of working is to put security on folder level.

Items that are added to the folder, will inherit the security settings of the folder.

Mind!

Also when you change the security settings of a folder in a later stadium, all sub-items will inherit the new security settings.

By **overriding** the security of a folder item, you can create security settings that deviate from the folder security of the folder where they are located.

When an override has been done, you have changed the inherited folder security into an 'own security' of the folder or the document.

When such an item is moved to another folder, it keeps its 'own' security settings.

1.3 Action profiles

Security is defined in separate actions. All of these actions are gathered in an *Action Profile*. This Action Profile is linked to users, groups or roles on document, case object or folder level.

1.3.1 Overview of all actions

Add Comments	Add comments to a document, folder or case category.
Add File when document is checked out	Add a file to a document is possible after document check-out.
Add File when document is in creation	Add a file to a document is possible when document has the status <i>in creation</i> .
Add File when document is not checked out	Add a file to a document when the document is not checked-out.
Admin case data	User has access to the admin tab of the case where he/she is allowed to change the case metadata of any case on this object.
Admin case status fields	User has access to the admin tab of the case where he/she is allowed to change the case status (step, deadline, ...) of any case on this object.
Can move from folder	User is allowed to move an object from the folder where he/she has these rights.
Check-In other users documents	Check-in documents that are checked-out by other users: Make documents that are reserved for editing by another user available again for edition to all users.
Configure Application	<p>The user has application administrator rights, he can:</p> <ul style="list-style-type: none"> • Create Action Profiles • Create Action Profiles. • View, execute and enable/disable batch jobs. • Manage the file extensions list. • Manage the file servers list. • Manage the lfilters list. • Organize the toolbar. • Execute a batch update of documents. • Use the Doma Admin module. <p>Remark: <i>Configure Application</i> rights are only checked on the root level of the DocRoom tree.</p>
Create Document	Add a new document to the current folder.
Create new document version	Allow the user to check-out a document and create a new version of the document.
Create new file version when the document is not checked out	Check-out a file when the document is not checked-out.
Create Public Property expansion	User can create a property expansion that will be available for all DocRoom users.
Create Shortcut	Create a shortcut in the folder where the user has these rights.
Create Subfolder	Create a subfolder in the current folder.

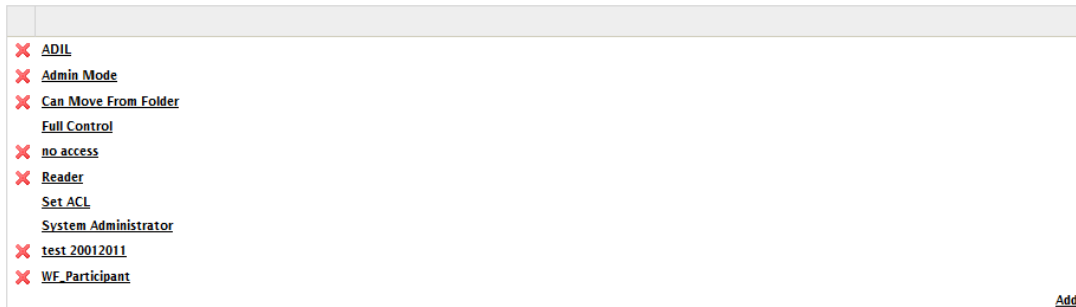
Delete Comments	Delete comments (added by your user only).
Delete Document	Delete the selected document.
Delete File when the document is checked out	Delete a file from a document is possible after document check-out.
Delete File when the document is not checked out	Delete a file from a document is possible when document is not checked-out.
Delete Folder	Delete the selected folder.
Execute User Event: [Name of the event]	User is allowed to execute the mentioned user event. If the user doesn't have rights to execute this user event, he will not see it.
Full Control	Do all actions mentioned in this list.
Manage public saved queries	User is allowed to create/edit/delete public saved queries.
Modify ACL Case	Change the DocRoom security settings of a case category.
Modify ACL Document	Change the security settings of a document.
Modify ACL Folder	Change the security settings of a folder.
Modify Checked out files	Edit files that are checked out. After changes, the user can save the edited file as a new version of the old one. If not selected, the user cannot modify checked out files.
Modify Comments	Change comments (added by your user only).
Modify Files	Edit files without version management (the option Edit appears and allows you to change the file immediately without check-out. The old file will be overwritten by the new one. The new file will get a new revision number (x.x.1will become x.x.2). The old file cannot be viewed anymore.
Modify Meta Data Checked Out Document	Edit the search criteria of the checked-out document. After changes, the user can save the edited document as a new version of the old one. If not selected, the user cannot modify meta data of a checked-out document.
Modify Meta Data Document	Edit document search criteria without version management (the option Edit appears and allows you to change the document meta data immediately without check-out. The old information will be overwritten by the new one. The new information will get a new revision number (x.x.1will become x.x.2).
Modify Meta Data Folder	User is allowed to change folder meta data.
Start Workflow	User is allowed to create a case object.
Unlock Other users Documents	Make documents, that are locked for editing by another user, available again for edition to all users.
View ACL Case	View the DocRoom security settings of the case object.
View ACL Document	View the security settings of the document.
View ACL Folder	View the security settings of the folder.
View Comments	View the comments of the document/folder.
View Document History	View the actions made on the document.



View File History	View the actions made on the file linked to a document.
View Files	View files that are linked to a document.
View Meta Data Document	View the meta data of a document.
View Meta Data Folder	View the search keys of a folder.
View previous document versions	View earlier versions of the document.
View previous file versions	View earlier versions of a file linked to a document.

1.3.2 How to create an action profile?

A new *Action Profile* can be created from the **Admin**-menu in the web interface:

1. Open the **Admin**-menu.
2. Choose the option **Action Profiles**. A new screen will appear.
In this screen you can see a list of all existing *Action Profiles*:

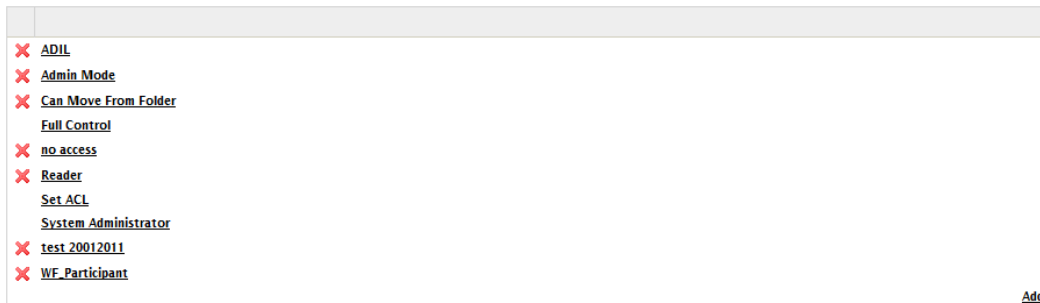


3. Click on **New** to create a new *Action Profile*.
4. Fill in a name for the *Action Profile* in the next screen.
5. Click on **Save** to go to the next screen.
6. Determine which actions a user with this *Action Profile* can do.
Click on the  icon to allow the user with this *Action Profile* to do this action.
Click on the  icon to remove this action from the allowed actions.
7. Click on **Save** to save the new *Action Profile*.
8. The new profile will appear in the list of *Action Profiles*.

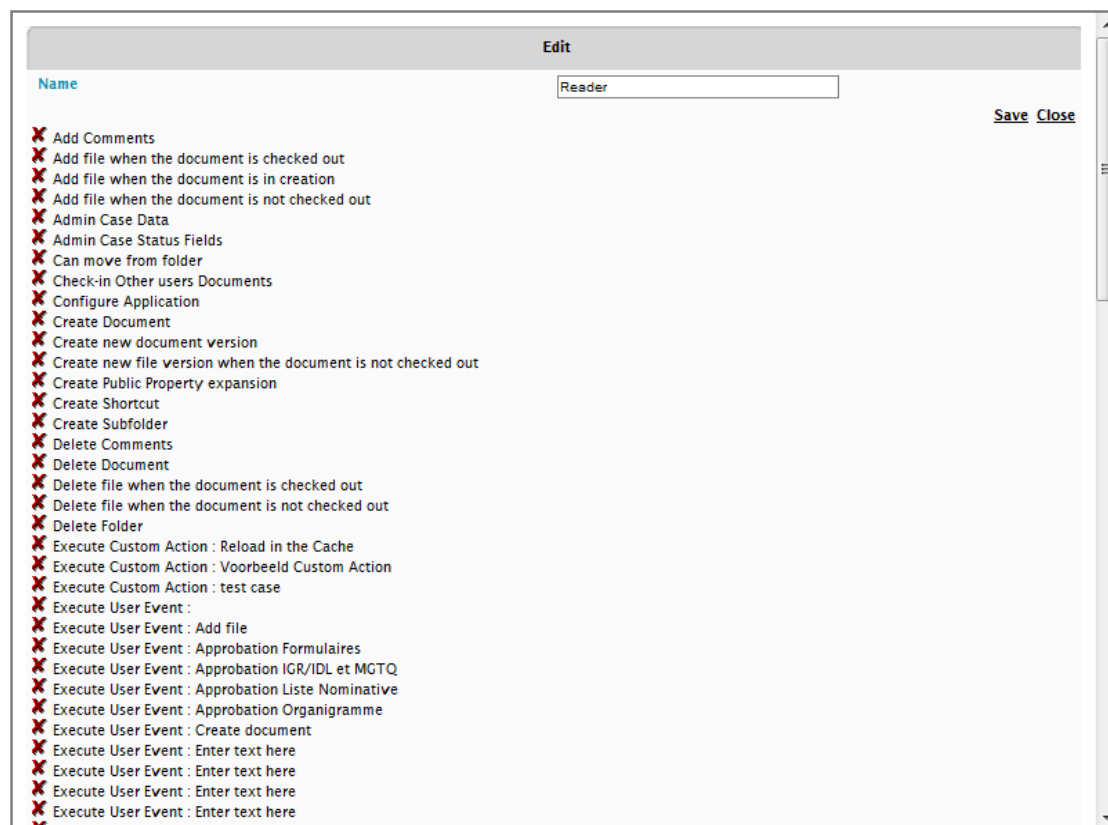
1.3.3 How to edit an action profile?



Existing *Action Profiles* can be edited from the **Admin**-menu in the web interface:

1. Open the **Admin**-menu.
2. Choose the option **Action Profiles**.
The list of *Action Profiles* will be visible.



3. Click on the *Action Profile* you want to edit. The settings of the *Action Profile* will appear.



4. Click on the  and  icons to change the *Action Profile*.
5. Click on **Save** to save the changes.

1.3.4 How to delete an action profile?

1. Open the **Admin**-menu.
2. Choose the option **Action Profiles**. A new screen will appear.
In this screen you can see a list of all existing *Action Profiles*:

✗	<u>ADIL</u>
✗	<u>Admin Mode</u>
✗	<u>Can Move From Folder</u>
	<u>Full Control</u>
✗	<u>no access</u>
✗	<u>Reader</u>
	<u>Set ACL</u>
	<u>System Administrator</u>
✗	<u>test 20012011</u>
✗	<u>WF_Participant</u>

[Add](#)

3. Click on the ✗ icon next to the *Action Profile* you want to delete. The *Action Profiles* you cannot delete are fixed *Action Profiles*.
4. The chosen *Action Profile* will be deleted.

Nice to know

- If the user is not selected in the ACL list, the user will get *No Access*: he/she will not see the objects.
- If no *Action Profile* is defined for a user, the user will browse rights: the user will see the items in the list, but cannot view any of the details of it.
- When more than one *Action Profile* is assigned to the same user, the user will gain all security rights mentioned in the different *Action Profiles*.
- If a user has access to a subfolder of a folder where he/she has no access, both folders will be shown in the Tree Structure. The content of the folder of which the user has no access will not be shown. (If default security is used.)
- When a document is moved to another folder, it will inherit the security of the target folder, except if the document had 'own' security settings, i.e. when the document security settings are different from the security settings of the folder where it is located.
- Document security settings override folder security settings (inherited on document level) when document security is set after the document has been located in the folder.

1.4 Folder security

Folder security defines what a user can do with the selected folder.
By default, folder security is inherited by all folder items, e.g. subfolders, documents and case objects.

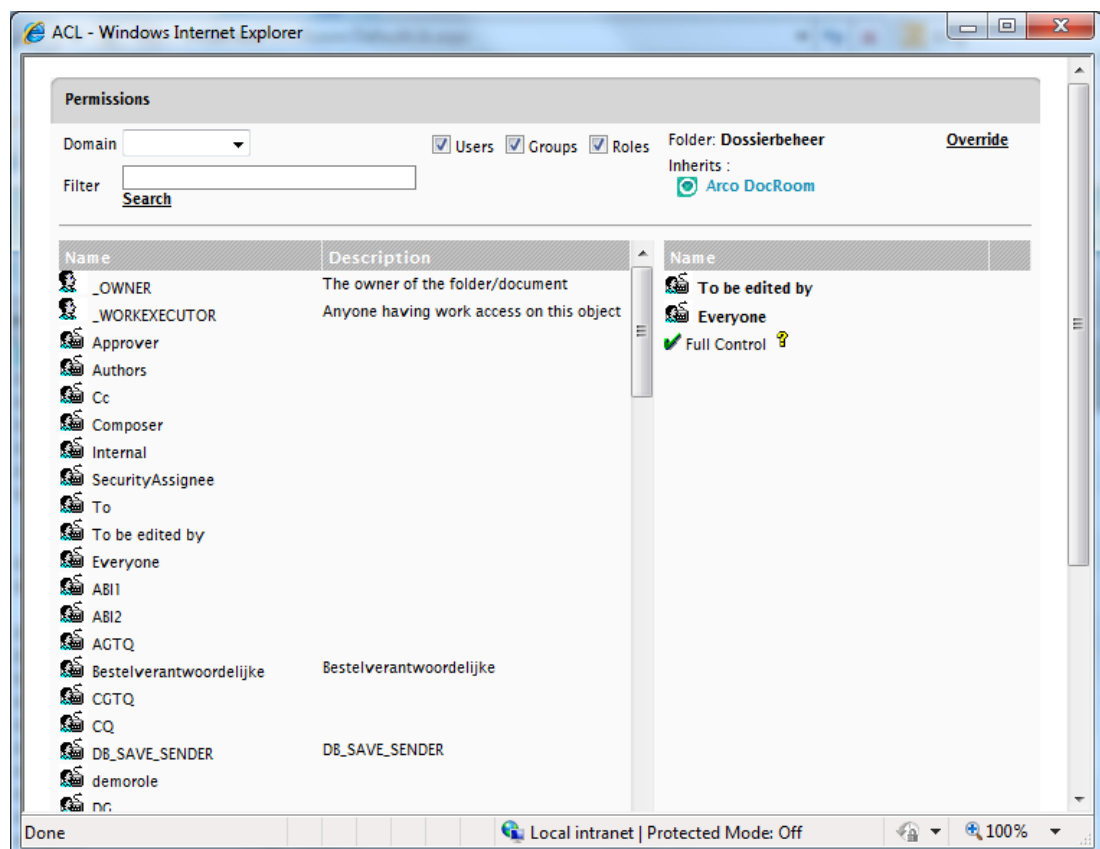
1.4.1 How to set security on folder level

When creating a new folder, the folder will inherit the security settings of the parent folder.
All documents that are added to this folder, will inherit the folder security settings.

These settings can be changed by changing the ACL (= *Access Control List*) settings.

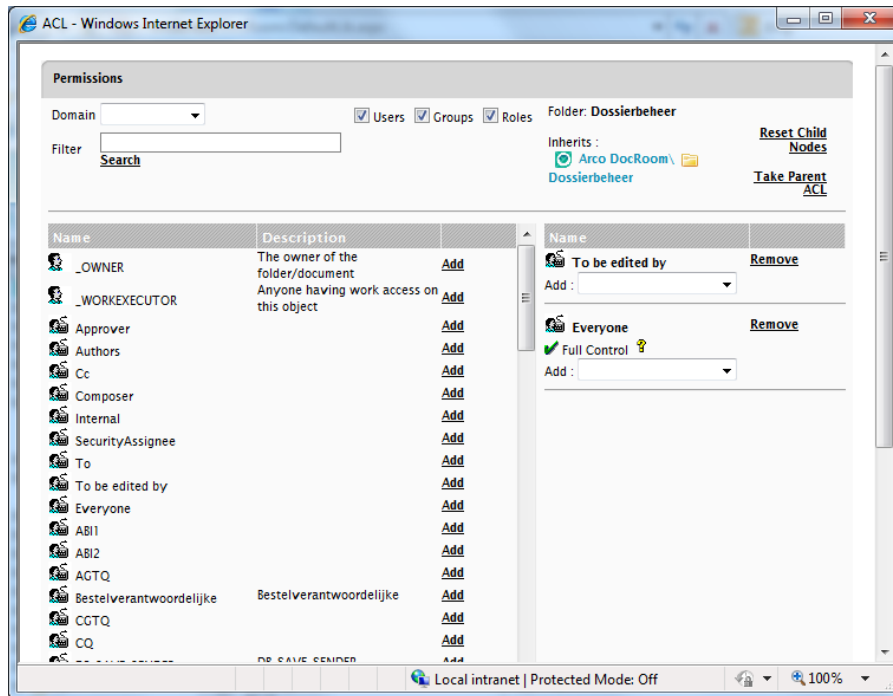
1. Select the folder where you want to change the security settings.
2. Click on the right mouse button.
3. A menu appears: select the option ACL.

The ACL window of the selected folder appears.



4. The security settings of the folder appear in the right column of the ACL window.
5. Click on the option **Override** in the right upper corner of the ACL window.

The ACL window now appears in *Edit mode*.



6. From this screen you can set the security.

- Click on **Take parent ACL** to inherit the security settings of the parent folder.
- You can also define a different security.
 - Select a user/group/role in the left column of the screen by clicking on the **Add** button. The user/group/role will appear on the right side of the screen.
 - Click on the **Remove**-button next to the user/group/role to remove it from the right column. In the right column you can select an *Action Profile* for each user/group/role in the dropdown list. Click on the ? icon to view the settings of the **Action Profile**.

7. Click the option **Close** in the right lower corner of the ACL window to close the window and save the settings.

1.4.2 How to view folder security settings

Folder security settings can be viewed from the Tree Structure in the Web Interface.

1. Select the folder of which you want to view the security settings.
2. Click on the right mouse button.
3. A menu appears: select the option *ACL Management*.
4. The ACL window of the selected folder appears in read-only.

1.5 Document security

Document security defines what a user can do with the selected document.
By default, documents inherit the security of the folder where they are located.
However, when you change the document security, it no longer inherits the security of the folder where it is located.

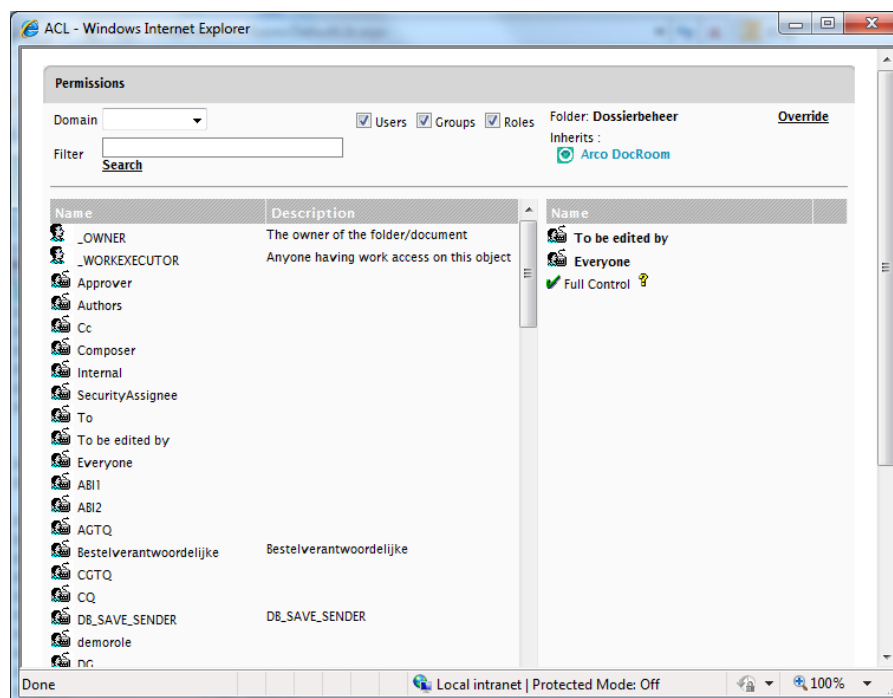
1.5.1 How to set security on document level

By default, when creating a new document, the document will inherit the security settings of the folder where it is located.

These settings can be changed by changing the ACL settings. ACL settings can be viewed from the document detail in the Web Interface:

1. Browse to the document of which you want to change the security settings.
2. Double click on the document title in the document bar to open a pop-up window that contains the document metadata on the left and a preview of the document on the right.
3. Click on the button *ACL Management* (👤) to open the ACL window of the selected document.

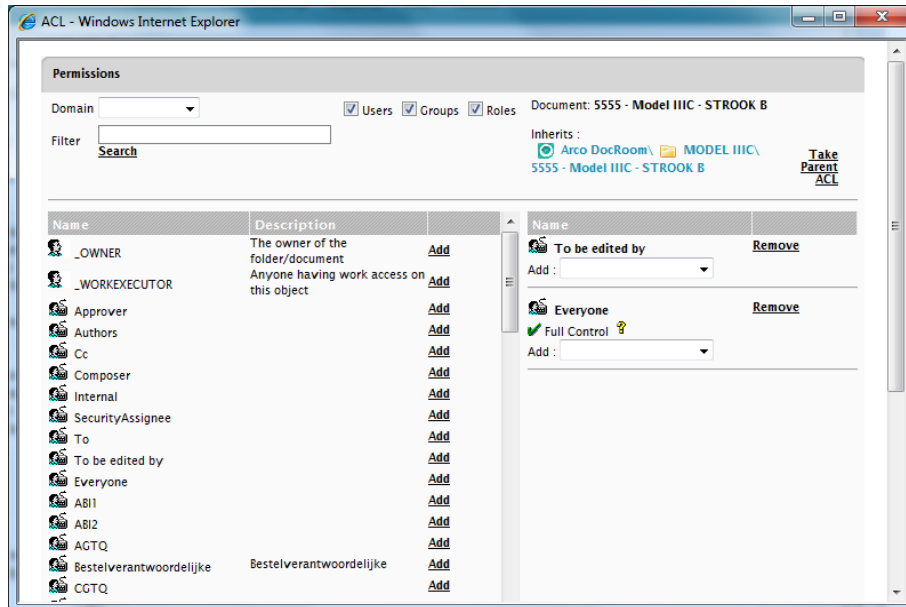
The ACL window of the selected document appears:



The security settings of the document appear in the right column of the ACL window.

4. Click on the option **Override** in the right upper corner of the ACL window.

The ACL window now appears in *Edit mode*:



5. From this screen you can set the security.
 - Click on **Take parent ACL** to inherit the security settings of the folder.
 - You can also define a different security.
 - Select a user/group/role in the left column of the screen by clicking on the **Add** button. The user/group/role will appear on the right side of the screen.
 - Click on the **Remove**-button next to the user/group/role to remove it from the right column.
 - In the right column you can select an *Action Profile* for each user/group/role in the dropdown list. Click on the ? icon to view the settings of the selected *Action Profile*.
6. Click on the option **Close** in the right lower corner of the ACL window to close the window and save the settings.

1.5.2 How to view document security settings

Document security settings can be viewed from the result list in the Web Interface.

1. Select the document of which you want to view the security settings.
2. Click on the right mouse button.
3. A menu appears: select the option *ACL Management*.
4. The ACL window of the selected document appears in read-only.

1.5.3 Property Assignee and document and folder security

We can use a property of the type *Assignee* to allow users to influence the document security, though they don't have the right to set ACL rights on the document.

We have configured a document category with the name document. One of the properties of this category is an assignee field with the name "Reviewers".

When a user adds a document, he/she can select one or more users in the assignee field "Reviewers". All users who are selected in this field, will automatically get edit rights on the document. Other users only have read rights by default.

When working this way, we allow users who don't have the right to change the document security, to select the users who are allowed to edit the document. Thus we allow "normal" users to influence the default document security.

To enable this way of working, we have to do the next configuration:

In the Doma admin module:

- Create a pool property of the type assignee that is searchable. (e.g. reviewers)
- Link this property to a folder category.
- Link the pool property of the type *assignee* also to a document category.

In the DocRoom WebInterface:

- Create a folder of the category where the assignee property is linked to.
- Link an action profile (e.g. edit) to the pool property (reviewers) on folder ACL level.
- Create a new document of this category in the folder where you linked an action profile to the pool property of the type assignee.
- During document insert, you can select the users of the pool property of the type assignee (reviewers). All of these users will get edit rights on the document.

An example:

A user has **Read** rights to all documents of the folder *Training*.

The document *Manual DocRoom* is located in this folder, so this user can only view the document.

One of the document properties is the property *Reviewer* (of the property type *Assignee*)

On folder security level, I have granted **Edit** rights to this assignee *Reviewer*.

When I select the user name in the property *Reviewer*, he will automatically get the **Edit** rights instead of the normal **View** rights.

1.6 Case Object security

1.6.1 Introduction

Since a case object is the result of the creation of a case category, it is influenced by the Routing WorkFlow procedure security settings and by the DocRoom security.

When the procedure of a case object is still active, it can always be found in the Routing result lists. Here, the normal Routing WorkFlow security counts.

When a case object is approached from the DocRoom Library interface (via the tree structure or via a search), the DocRoom security is active.

This means:

- If you have no access to the case object, you will not see it.
- When you have no access to the case object, but you have work on the actual step of it, you will see it if a special user "work executor" is added to the case object security.

In this part, we will discuss the DocRoom security.

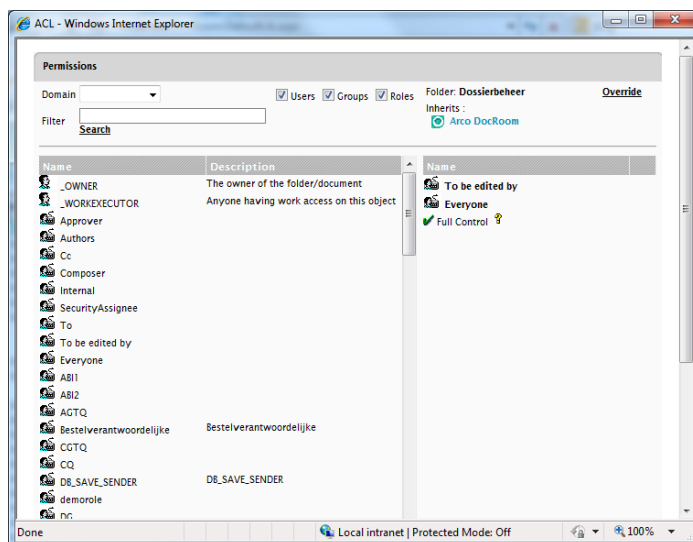
1.6.2 How to set security on a case object

By default, when creating a new case object, it will inherit the security settings of the folder where it is located.

These settings can be changed by changing the ACL settings. ACL settings can be viewed from the document detail in the Web Interface:

1. Browse to the case object of which you want to change the security settings.
2. Double click on the case object title in the case object bar to open a pop-up window that contains the case object metadata on the left and a preview of the case object on the right.
3. Click on the button *ACL Management* (🔑) to open the ACL window of the selected case object.

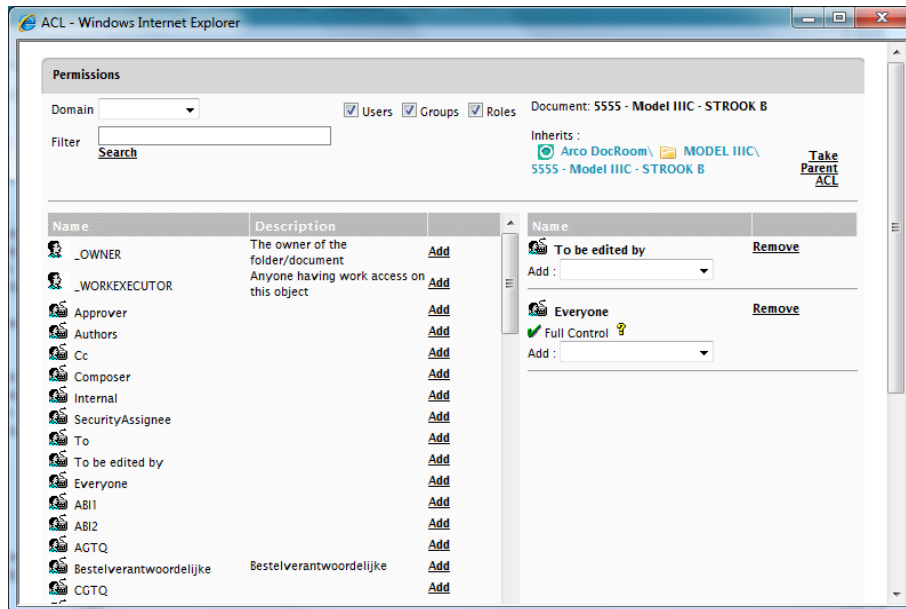
The ACL window of the selected case object appears:



The security settings of the case object appear in the right column of the ACL window.

4. Click on the option **Override** in the right upper corner of the ACL window.


The ACL window now appears in *Edit mode*:



5. From this screen you can set the security.
 - Click on **Take parent ACL** to inherit the security settings of the folder.
 - You can also define a different security.
 - Select a user/group/role in the left column of the screen by clicking on the **Add** button. The user/group/role will appear on the right side of the screen.
 - Click on the **Remove**-button next to the user/group/role to remove it from the right column.
 - In the right column you can select an *Action Profile* for each user/group/role in the dropdown list. Click on the ? icon to view the settings of the selected *Action Profile*.
6. Click on the option **Close** in the right lower corner of the ACL window to close the window and save the settings.

1.6.3 How to view case object security settings

Case object security can be viewed from the result list in the Web Interface.

1. Browse to the case object of which you want to view the security settings.
2. Double click on the case object title in the case object bar to open a pop-up window that contains the case object metadata on the left and a preview of the case object on the right.
3. Click on the button **ACL Management** in the toolbar () to open the ACL window of the selected case object.
4. The ACL window of the selected case object appears.

1.6.4 Users for which we can define folder, document and case object security

DocRoom security can be assigned to:

- One or more named users (synchronized or database user)
- User _OWNER (the owner = creator of the object)
- User _WORKESECUTOR (the user who has Routing work on the object)
- Groups (synchronized from the network)
- Roles (administered in DocRoom)
- Assignee
- Everyone

Or a combination of the items mentioned above.

2 Routing security

Security ensures that data stored in DocRoom and Routing cannot be read or compromised by any individuals without authorization.

2.1 Introduction

Just like DocRoom security, Routing security is based on the user's login and password and the groups and roles a user makes part of. Both DocRoom and Routing use the same user list.

Routing Security is defined on procedure level.

Here we configure what users can do in the web-interface: can they only do their part of the procedure, can they also follow up the dossier when they don't have to do the actual work or do they even have administrator rights so they can administer the dossier?

If they have enough rights, users are also allowed to edit the flow of the procedure by using the Doma admin module.

Next to the security on procedure level, steps of the procedure are assigned to certain users or a group of users. These users execute a step, therefore we refer to them as *step executors*. (called step security in Routing v.4.)

2.2 Procedure security

2.2.1 Procedure security levels

Routing has 7 pre-defined security levels:

1. No Access
2. Start
3. View
4. Edit
5. Own
6. Administer
7. Full control

The first 2 levels can be combined with trail view access rights on step level. Trail view rights enlarge the standard user rights from the moment (step) that the user is involved in the procedure.

Each of the mentioned security rights will be explained below.

2.2.1.1 User levels No Access, Start and View

The first 3 security levels are levels used for end users. They influence the behavior of the Routing dossiers in the web interface. They do not grant access to the procedure in administrator tools such as the Doma admin module.

Web Interface rights

			Security level				
			No Access	No Access + Trail View rights	Start	Start + Trail View rights	View
My Work	See dossier	assigned to the user and started by him	X	X	X	X	X
		assigned to the user and not started by him	X	X	X	X	X
		not assigned to the user and started by him	O	O	O	O	O
		not assigned to the user and not started by him	O	O	O	O	O
	Open dossier in edit mode	assigned to the user and not locked	X	X	X	X	X
		assigned to the user but locked by another user	O	O	O	O	O
	Open dossier in read only	assigned to the user but locked by another user	X	X	X	X	X
		not assigned to the user and started by him	O	O	O	O	O
		not assigned to him and not started by him	O	O	O	O	O
My Dossiers	See dossier	assigned to the user and started by him	NA	NA	X	X	X
		assigned to the user and not started by him	O	O	O	O	O
		not assigned to the user and started by him	NA	NA	X	X	X
		not assigned to the user and not started by him	O	O	O	O	O
	Open dossier in edit mode	assigned to the user, started by him and not locked	NA	NA	O	O	O
		assigned to the user, started by him but locked by another user	NA	NA	X	X	X
	Open dossier in read only	assigned to the user, started by him and not locked	NA	NA	O	O	O
		assigned to the user, started by him, but locked by another user	NA	NA	X	X	X
		not assigned to the user and started by him	NA	NA	O	X	X
		not assigned to the user and not started by him	O	O	O	O	X
Open Dossiers	See dossier	assigned to the user and started by him	NA	X	X	X	X
		assigned to the user and not started by him	X	X	X	X	X
		not assigned to the user and started by him	NA	TV	O	TV	X
		not assigned to the user and not started by him	O	TV	O	TV	X
	Open dossier in edit mode	assigned to the user and not locked	X	X	X	X	X
		assigned to the user but locked by another user	O	O	O	O	O
	Open dossier in read only	assigned to the user but locked by another user	O	X	X	X	X
		not assigned to the user and started by him	NA	NA	O	TV	X
		not assigned to the user and not started by him	O	O	O	TV	X
Archive	See dossier	Started by the user	NA	NA	O	TV	X
		User was step executor during the procedure	O	TV	TV	TV	X

NA = Not Applicable

TV = yes, if Trail View is active for the user

2.2.1.2 Edit

From this level on, also access to the Doma admin tool is allowed. The rights on webinterface level are the same as view rights.

- Web Interface
 - *Same rights as view rights*
- Doma Admin
 - *The procedure on which the user has Edit rights will be listed in the Doma Admin module.*
 - *The user can edit these procedures.*
 - *The user cannot delete these procedures*
 - *User can give No Access, Start or View rights to other users rights.*
 - *User can export the procedure.*
 - *User can create a new version of the procedure.*
- Routing Users Manager
 - No Access

2.2.1.3 Own

- Web Interface
 - *Same rights as view rights*
- Doma Admin
 - *The procedure on which the user has Own rights rights will be listed in the Doma Admin module.*
 - *The user can edit these procedures.*
 - *The user can create procedures.*
 - *The user can delete procedures*
 - *User can give No Access, Start, View or Edit rights to other users rights.*
 - *User can export the procedure.*
 - *User can create a new version of the procedure.*
- Routing Users Manager
 - No Access


2.2.1.4 Administer and Full Control

The highest levels also have access to administrator tools in the web interface, next to access to the administrator client tools such as the Doma admin module and the Routing User Manager.

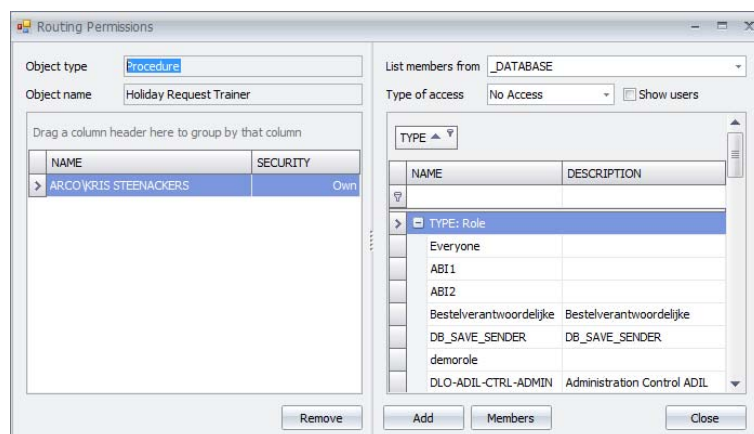
Currently, there is no functional difference between the levels Administer and Full Control.

- Web Interface
 - Same rights as view rights
 - User can administer the dossier from the web interface:
 - Edit dossier
 - Unlock dossier
 - Finish dossier
 - Delete dossier
 - Move work to another step
 - Assign work to another user
- Doma Admin
 - The procedure on which the user has Own rights rights will be listed in the Doma Admin module.
 - The user can edit these procedures.
 - The user can create procedures.
 - The user can delete procedures
 - User can give No Access, Start, View, Edit or Own rights to other users rights.
 - User can export the procedure.
 - User can create a new version of the procedure.
- Routing Users Manager (Not used anymore for Doma v 6.1.6)
 - User can synchronize Routing security with network users and groups
 - User can manage roles
 - User can manage role relationships

2.2.2 How to set procedure security


1. Open the Doma admin module.
2. Make sure that the tab *Procedure* is selected.
3. Click on the button  in the toolbar.
4. The routing permissions window appears:

The right part of the screen shows all configuration items.
The left part of the screen shows the actual security settings.



5. Do the next steps to configure the security:
 1. **List members from:** Select the synchronized domain or _DATABASE: this is a filter that shows domain users or database users.
 2. **Type of access:** select here which of the 7 Routing security levels will be assigned to the selected user(s).
 3. **Show users:** check this option to show users in the list. If this is not selected, only groups and roles are shown.
 4. In the list below this fields, select the user (s) (by scrolling or by using the filter) to whom you want to assign the selected security level.
 5. **Add:** Click here to add the selected user(s) and the assigned security level to the Routing permissions list at the left.
6. Close the window after configuration.

2.2.3 How to edit procedure security

1. Open the Doma admin module.
2. Make sure that the tab *Procedure* is selected.
3. Click on the button  in the toolbar.
4. The routing permissions window appears:
 - a. The right part of the screen shows all configuration items.
 - b. The left part of the screen shows the actual security settings.
5. Edit the procedure security.

2.3 Step executors

2.3.1 Introduction

On step level, you have to define the step executor(s). When a user is a member of the step executor list, he will see the dossier of this step in the list *My Work*.

If a step has more than one step executor, each of these users will see the dossier in the list *My Work*.

When the step is assigned to more than one user, and one of the users opens the step detail, the step will be locked by this user. Other users will still see the dossier, but they can only open it in read-only.

2.3.2 Default step executors

Users on object level

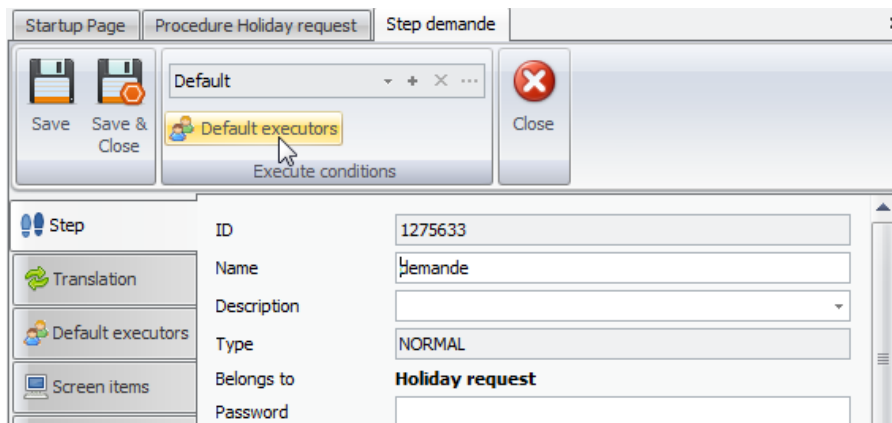
_OWNER	The owner (creator) of a folder or a document
_WORK EXECUTOR	Anyone having work access on this object

Users on workflow step executor level

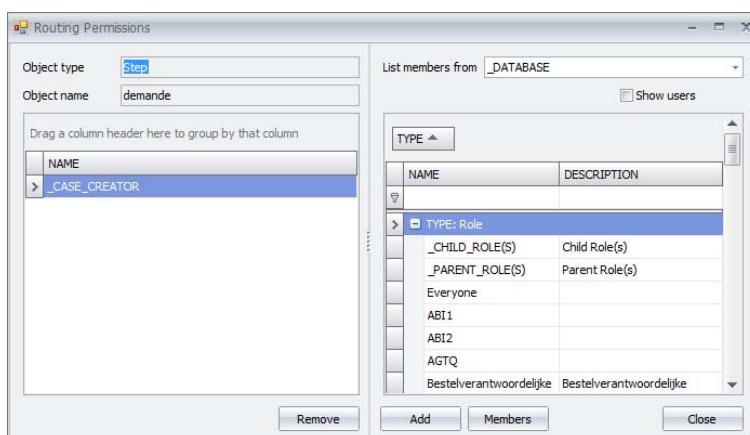
Named user
_CASE CREATOR
_STEP_EXECUTOR
Everyone
Assignee
group
Role
_CHILD_ROLE(S)
_PARENT_ROLE(S)
_STRUCTURE_ROLE

2.3.2.1 How to set step executors

1. Open the Doma administrator module.
2. Open the procedure detail.
3. Open the step detail by selecting the tab Steps; then double click on the step in the procedure overview to open the step detail in a new tab.
4. The step detail appears in a new tab. When the tab Step is selected, the button Default executors will be visible in the toolbar:



5. Click on the button **Default executors** to define the default executors of the selected step.
6. The Routing Permissions window appears in a pop-up window:



7. Select one or more users in the right frame, then click on the **Add** button to copy them to the Routing Permissions overview at the left side.
8. Close the Routing Permissions window.

2.3.3 Conditional step executors

It is also possible to define conditional step executors.
This allows us to assign steps to different users, based upon a condition.

E.g. in an invoice approval procedure,

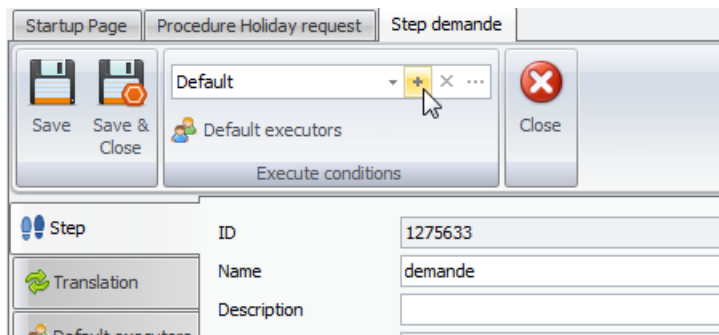
In this case, you can assign the step to other step executors. The step will be assigned to these other step executors if the condition where they are linked to has been reached. The condition is always based on property values.

When you define conditional security, the system will first check if the condition has been reached. If this is the case, the step will be assigned to the step executors who are linked to the conditional security.

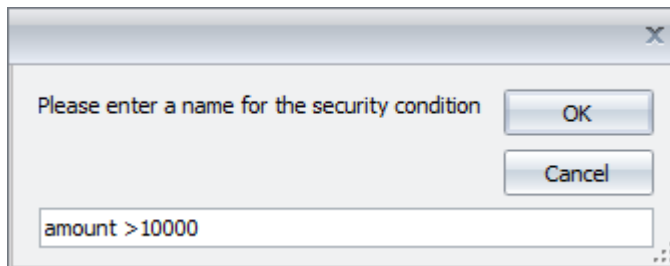
When the condition has not been reached, the system will check the next condition. If there is no condition left, the default security of the step will be used.

2.3.3.1 How to configure a condition on step executor level

1. Open the Doma administrator module.
2. Open the procedure detail.
3. Open the step detail by selecting the tab Steps; then double click on the step in the procedure overview to open the step detail in a new tab.
4. The step detail appears in a new tab. When the tab Step is selected, the button Default executors will be visible in the toolbar. Above this toolbar, a dropdown list with the value *Default* is shown.
5. Click on the + button next to the list:

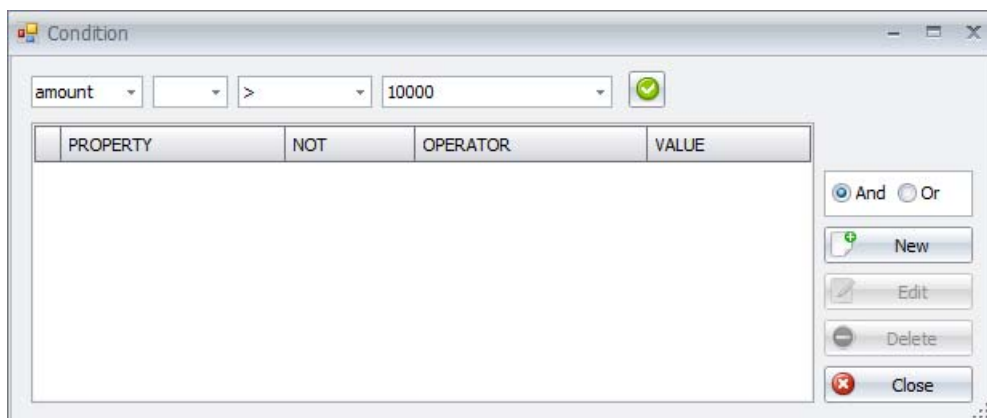


6. The next window appears:




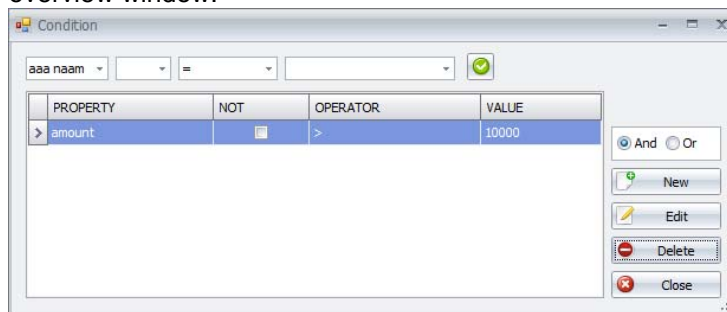
Enter a name for this condition. Then click in the OK button.

7. The condition definition window appears as a pop-up window: define your condition:

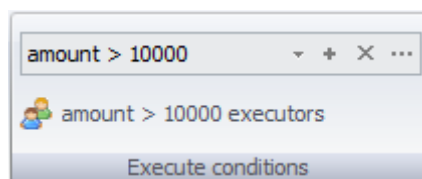


- a. Select the property on which the condition is based in the left upper dropdown list.
- b. Complete your condition.

- c. Click on the Save condition button  to save the condition to the condition overview window:

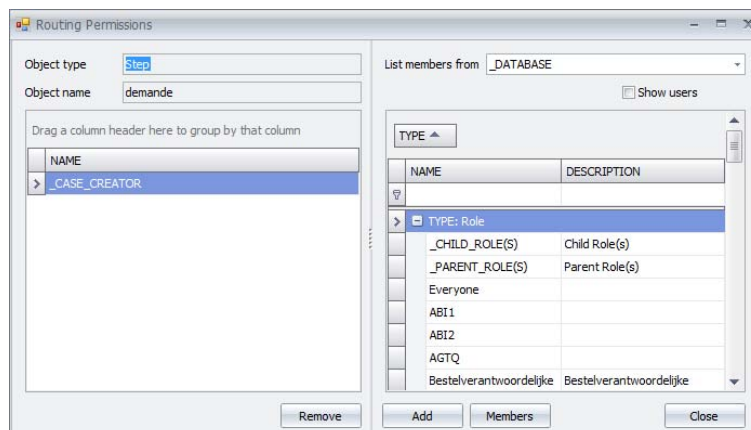


- d. Add another condition if necessary or click on the Close button to save your condition.
e. The conditional security is now shown in the dropdown list in the security part of the toolbar:




2.3.3.2 How to set conditional step executors

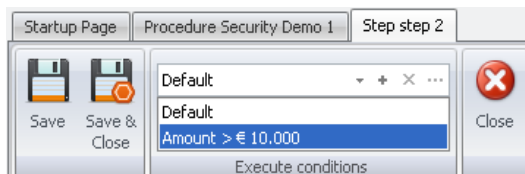
1. Click on the button with the reference to the condition (in the example **amount > 10000**) to define the conditional executors of the selected step.
2. The Routing Permissions window appears in a pop-up window:



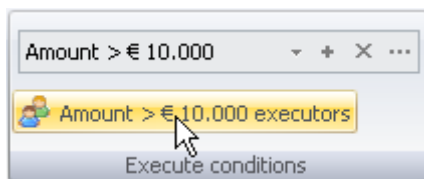
3. Select one or more users in the right frame, then click on the **Add** button to copy them to the Routing Permissions overview at the left side.
4. Close the Routing Permissions window.

2.3.3.3 How to edit a condition on step executor level

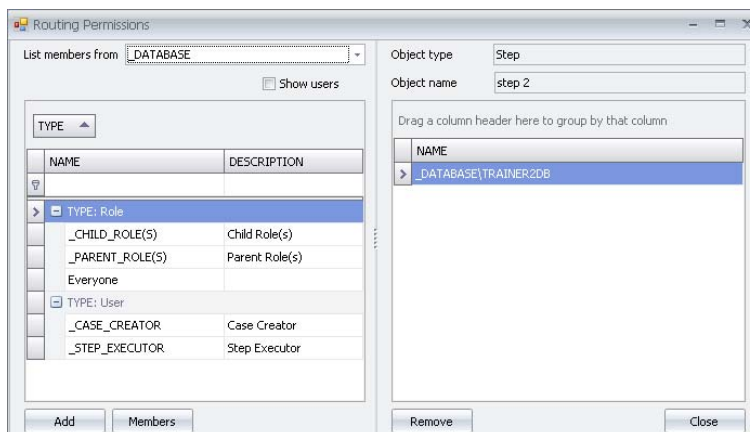
1. Open the Doma administrator module.
2. Open the procedure detail.
3. Open the step detail by selecting the tab Steps; then double click on the step in the procedure overview to open the step detail in a new tab.
4. The step detail appears in a new tab. When the tab Step is selected, the button Default executors will be visible in the toolbar. Above this toolbar, a dropdown list with the value *Default* is shown.
5. Open this list by clicking on the reversed triangle button  at the right of this field. You will see all conditional security definitions in the list:



6. Select the conditional security definition that you want to edit in the list. It now appears in the rectangle under the list. Click on this button to open the configuration details.



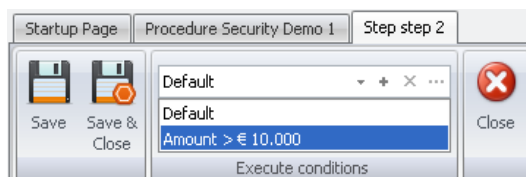
7. The Routing Permissions window appears. Here you can change the security settings that are linked to the condition.




Close the window after changes.

2.3.3.4 How to delete a condition on step executor level

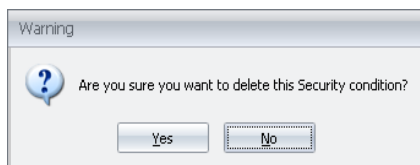
1. Open the Doma administrator module.
2. Open the procedure detail.
3. Open the step detail by selecting the tab Steps; then double click on the step in the procedure overview to open the step detail in a new tab.
4. The step detail appears in a new tab. When the tab Step is selected, the button Default executors will be visible in the toolbar. Above this toolbar, a dropdown list with the value *Default* is shown.
5. Open this list by clicking on the reversed triangle at the right of this field. You will see all conditional security definitions in the list:



6. Select the conditional security definition that you want to delete in the list. It now appears in the rectangle under the list. Click on the delete button  at the right of the list.



7. A warning message message appears:



Click Yes to delete – the condition will be immediately removed from the list.

Click No to cancel.

2.4 Delegate(d) work

2.4.1 Introduction

Users can delegate their work list to other users: they can allow other users to treat work that was initially assigned to themselves.

When a user delegates his/her work to someone else, this work will also appear in the work list of the user to whom they have delegated the work.

2.4.2 How to delegate work

How to delegate your Routing work list to another user

- Click on your user name in the navigation bar to open the *My Preferences* window.



- The *My preferences* window appears:

- Select the tab **Delegates** (1), then click on the add icon (2) in the list Delegated from me

- A new window appears.

- Select whether you want to assign your work list to a user, a role or a group in the dropdown list **To** (1).
- Then select the user, group or role in the field next to it. Enter the (a part of the) name of the user (group, role) and click on the magnifying glass next to the field. If only one

item is found, it is immediately copied to the field, if there are more possibilities, a selection field appears.(2).

- If you want to limit the delegation to a certain procedure, then select this procedure in the field **procedure** (3). If this field is left empty, all your work is delegated to the user(s) in the *To* field.
- By default, the *manual* mode is selected in the field **Mode** (4). This means that the delegation starts on save and ends when you delete it. Select *Timed* to enter a start and end date. The delegation then starts and ends on the dates defined in the delegation.
- Click on the **Save** button (5) to save your settings.

- The delegation is now shown in the overview in the list **Delegated from me**.

Profile	Member of	Preferences	Delegates	
Delegated from me:				
To	Procedure	Mode	Begin	End
Admin		Manual		
Delegated to me:				
From	Procedure	Mode	Begin	End
No delegates found				

2.4.3 How to edit a delegation

How to edit delegations.

- Click on your user name in the navigation bar to open the *My Preferences* window.



- The **My preferences** window appears:

- Select the tab **Delegates** (1), then click on the **edit icon** (pencil icon) next to the delegation you want to change(2) in the list *Delegated from me*.

- The delegation details appear. Make your changes and save.

2.4.4 How to remove a user from my delegated work list

How to remove a user from the list "My delegates".

- Click on your user name in the navigation bar to open the *My Preferences* window.



- The **My preferences** window appears:

- Select the tab **Delegates** (1), then click on the **delete icon** ✖ next to the delegation you want to delete (2) in the list *Delegated from me*.

2.4.5 How to see which users have delegated work to me?

- Click on your user name in the navigation bar to open the *My Preferences* window.



- The **My preferences** window appears:

- Select the tab **Delegates**, there you see which users have delegated their work to you in the list **delegated to me**.

2.4.6 How to view work delegated to you

All delegated work also appears in your work list.

If you want to make a distinction between work that is originally assigned to you and delegated work, you can visualize the column **Work List**.

This column will show to which user the work is assigned under the header **Assigned to**.

With the filter of this column, you can filter your work.

In your profile, you can see which users have delegated their work list to you.

3 Other security settings

Next to the DocRoom security settings of folders and documents and the Routing procedure security settings, also other settings can be configured.
Below you see an overview of other security settings in DocRoom and Routing.

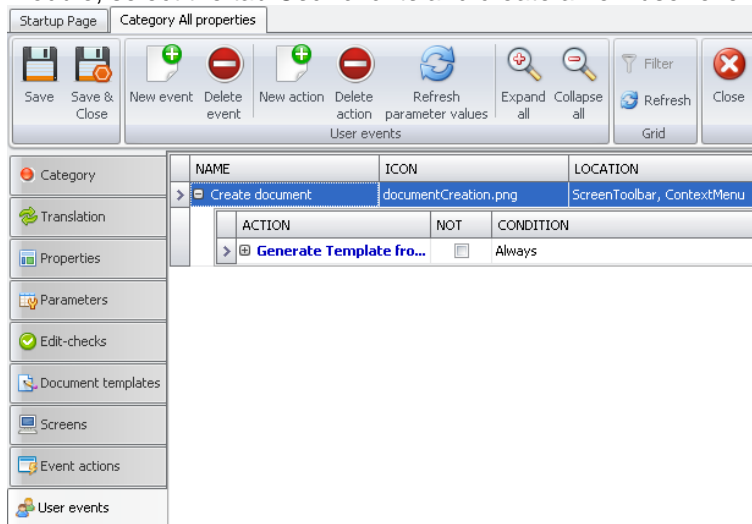
3.1 Security on user events

A user event is an action that can be triggered by the user: he/she can click on a toolbar button or a menu-item to start the action.

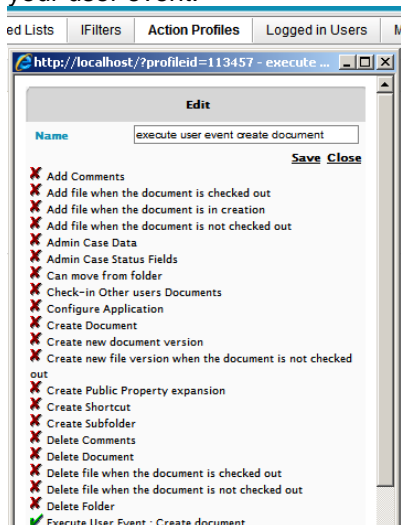
During the configuration of a user event, it is possible to link security settings to it. This way, you can define which users are allowed to use this user event.

3.1.1 How to set security on a user event

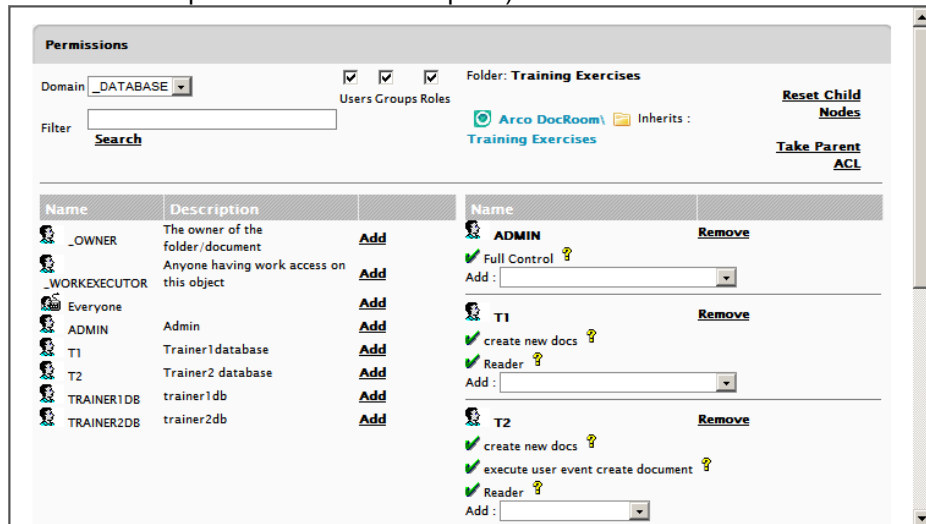
1. First create your user event on object level: open the object detail in the Doma admin module, select the tab *User events* and create a new user event.



2. Create a new action profile (or adapt an existing one) that allows a user to activate your user event.

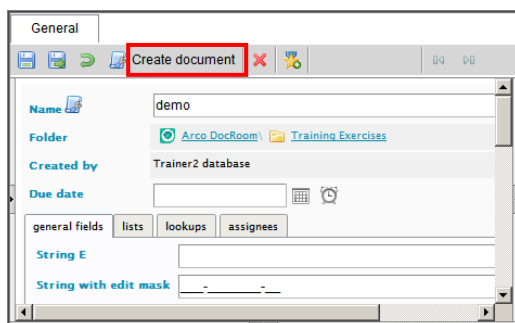


3. Assign this action profile in the DocRoom webinterface:
 - a. On the folder levels where you want the user event to be available when a document is created in this folder.
 - b. To the users who you want to allow to execute this user event. (Users who don't have this profile won't see the option).

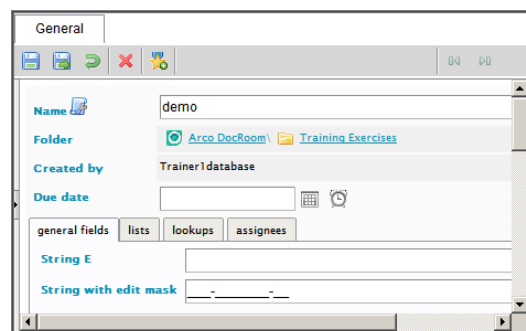


As a result, certain users will see the user action, others won't:

User T2 sees the user action:



User T1 doesn't see the user action:

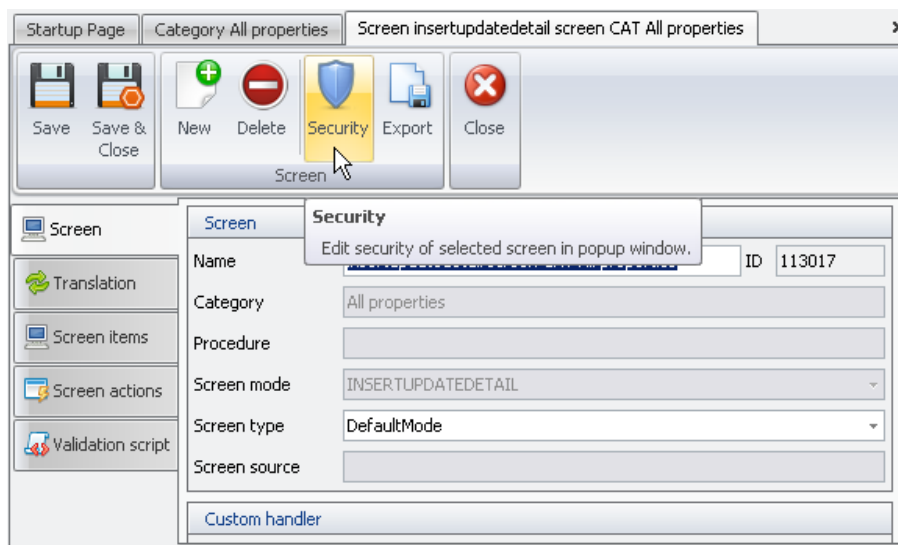


3.2 Security on custom screens

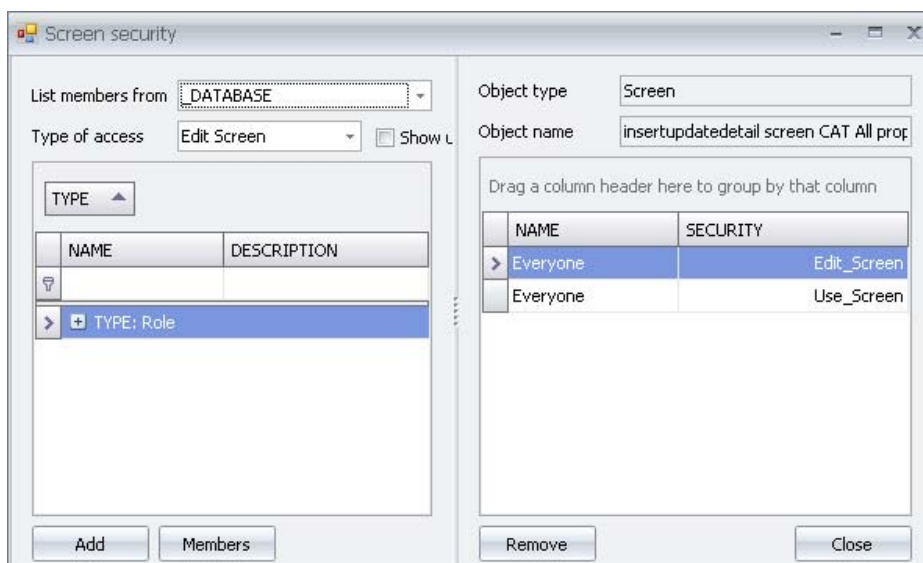
DocRoom allows application administrators to create custom screens. It is possible to link security to a custom screen, so that only those users will see the custom screen. When a user has no view rights on a custom screen, he will automatically view the default result list instead. Next to view rights, also edit rights can be granted to users.

3.2.1 How to set security on a custom screen

1. Open the detail of a custom screen in the Doma admin module. In the toolbar, you will see a Security button. Click on this button to open the security configuration window of this custom screen.



2. The security configuration window opens in a pop-up screen.
 - a. The left part of the screen shows the list of available users.
 - b. The right part of the screen shows the actual security configuration.



3. Define the security settings:

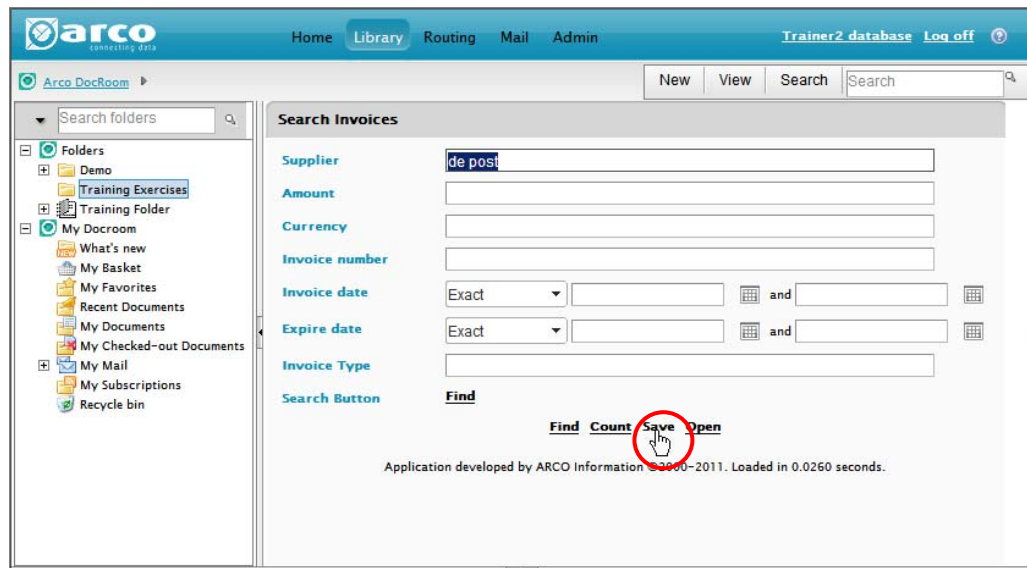
- a. Select whether you list members from the database or from a synchronized network
- b. Select the type of access:
 - i. Edit screen: the user is allowed to edit the screen in the Doma admin module
 - ii. Use screen: the user is allowed to use the screen in the Doma WebInterface. If the user isn't allowed to use the screen, he/she will be redirected to another custom screen that he/she is allowed to see or to the default screen.
- c. Select a user/group/role from the list.
- d. Click on the button Add.
- e. The selected user/group/role and the selected security level now appear in the actual security configuration overview at the right.

3.3 Security on saved queries

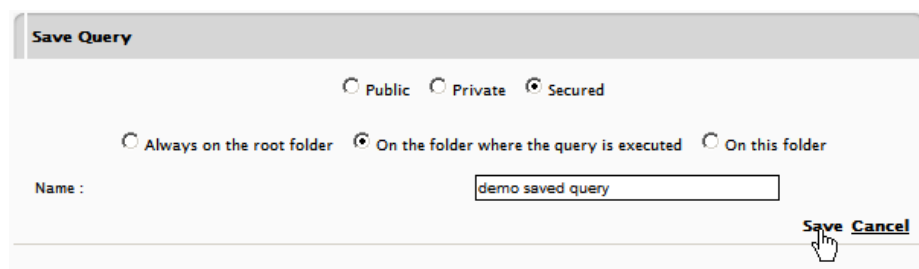
Saved queries can be registered as *public*, *private* or *secured*. If a query is secured, the creator of the query can define which users are allowed to execute the query.

3.3.1 How to create a secured query and set security on it

1. Define a query in the DocRoom WebInterface and click on the Save option.



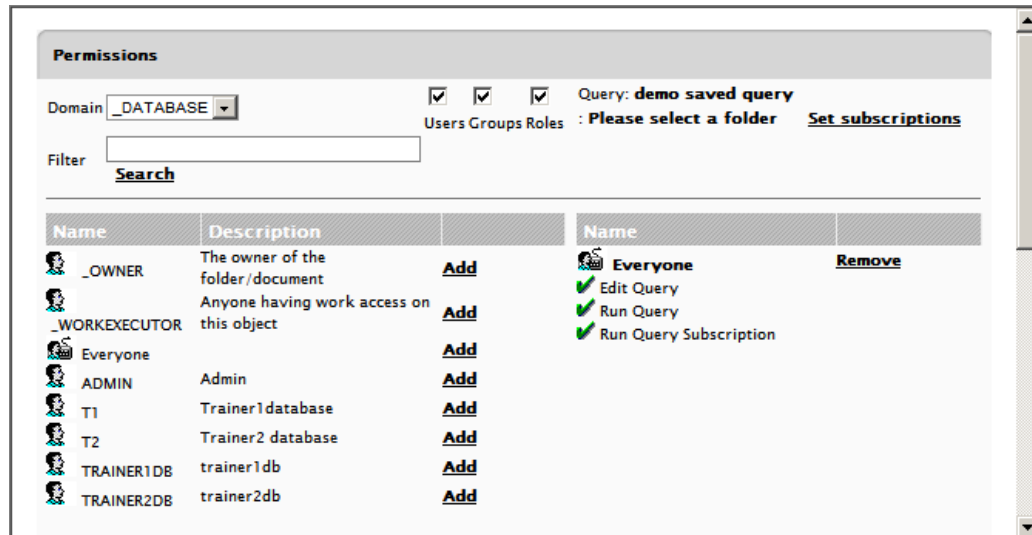
2. A new screen appears:
 - a. select the option *Secured*.
 - b. define where the saved query will be executed (on the folder where the query is executed in this example).
 - c. enter a clear name for the query.
 - d. click on the Save option to save the query.



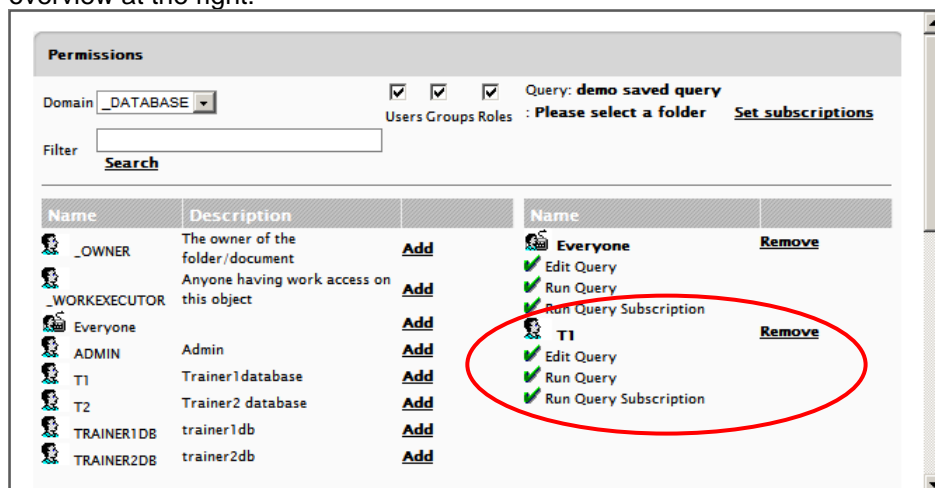
3. The link ACL Management now appears in the left lower corner – click on it to open the security configuration screen of the saved query:



4. The security configuration screen of the saved query appears.
 - a. The left part of the screen shows the list of available users.
 - b. The right part of the screen shows the actual security configuration.



5. Define the security settings:
 - a. Select whether you list members from the database or from a synchronized network
 - b. Select a user/group/role by clicking on the option **Add** next to it.
 - c. The selected user/group/role is copied to the actual security configuration overview at the right:



- d. By default, this user has the next rights:
 - i. Edit query: the user is allowed to edit the query in the Doma WebInterface and can save the changes.
 - ii. Run query: the user can execute the query (the query is shown to the user in the list of saved queries .)
 - iii. Run query subscription: the user can subscribe to the query, so he/she will automatically receives a mail when new result are found by the query.
 - iv. Click on the icon next to the right to disable one of the rights. When disabled, the icon appears in front of it.
6. Close the window.
7. Save the query.

4 Interesting combinations of security settings

How can I configure the system to ...

4.1 Allow a user to select another user in the WebInterface and give the selected user pre-defined rights on the concerned document or folder

1. Create a pool property of the type assignee in the Doma admin module.
2. Link this pool property to the category where you want to allow this kind of access.
3. Define the access rights for this assignee in the document security.

When a user selects another user in the assignee property of the document, the user will get the access rights that are linked to this assignee.

4.2 Allow edit without check-in / check-out

1. Open the Admin-menu.
2. Choose the option Action Profiles.
3. The list of Action Profiles will be visible.
4. Click on the Action Profile you want to edit. The settings of the Action Profile will appear.
5. Make sure that the next settings are set in your action profile:

- ✓ Create New Document Version
- ✓ Modify Checked Out Files
- ✓ Modify Meta Data Checked Out Folder
- ✓ View Files
- ✓ View Meta Data Document
- ✓ View Meta Data Folder
- ✓ View Previous Document Versions
- ✓ View Previous File Versions

4.3 Allow edit of document only after check-in / check-out

1. Open the Admin-menu.
2. Choose the option Action Profiles.
3. The list of Action Profiles will be visible.
4. Click on the Action Profile you want to edit. The settings of the Action Profile will appear.
5. Make sure that the next settings are set in your action profile:

- ✓ Modify Files
- ✓ Modify Meta Data Document
- ✓ Modify Meta Data Folder
- ✓ View Files
- ✓ View Meta Data Document
- ✓ View Meta Data Folder