HOME

User Manual

DELMIA Process Engineer®

User Management

DELMIA

Foreword

This manual provides an introduction to the basic operations and functions of the User Management.

While developing these functions we have made every effort to create a clearly organized, easy-to-understand program structure.

A user-friendly interface as well as a clear menu guide will enable you to quickly learn how to operate the program and to get familiar with its functions so that you can carry out your planning tasks in a quick and reliable way.

No Liability or Guarantee

Our programs and manuals have been compiled with great care and to the best of our knowledge. They have also been tested in a production setting. However, we assume no liability and provide no guarantee that the software and related descriptions are free of error or are suitable for special purposes.

DELMIA assumes no liability for any damage that may arise from the use of this software. By using this software, the user acknowledges this exclusion from liability and shall hold DELMIA exempt from all claims.

Copyright

Modifications

Moreover, DELMIA retains the right to make modifications and improvements to the product described in this manual at any time without prior notification.

fails to meet the United States government's needs or is inconsistent in any respect with United States Federal law, the United States government agrees to return this software, unused, to DASSAULT SYSTÈMES. The following additional statement applies only to acquisitions governed by DFARS Subpart 227.4 (October 1988): "Restricted Rights – use, duplication, and disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(l)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252-227-7013 (Oct. 1988)."

Table of Contents

1. Introduction

This manual explains how to use the Process Engineer User Management for your planning purposes.

1.1 How to Use this Manual

This manual enables you to get familiar with the operation and functions of the Process Engineer. This manual briefly describes:

- User Management functions

Note

When handling the User Management functions, please also refer to the general introduction to Process Engineer in the General Introduction Manual.

Click General Introduction to access the manual.

1.2 Documentation Conventions and Symbols

The symbols used in this manual are intended to provide you with keys to the contents in an immediately understandable manner.

This symbol is used to introduce key concepts that are covered in the sections immediately following this symbol. As a result, this symbol most frequently appears at the beginning of chapters or sections.

Note

*This symbol is used to mark notes, which provide you with additional information you need to have for further work. You will either find the Note sign at the beginning of a chapter or in a particular text passage in the chapter. Texts bearing this sign are additionally marked with **Note**. The text is always in italics.*

Caution

*This symbol indicates that the text that follows describes particular circumstances that you must avoid to avoid potential errors with the operation of the program or harm to data. You will either find the Caution sign at the beginning of a chapter or near a particular text passage in the chapter. Texts that are introduced by this sign are additionally marked with **Caution**. The text is always in italics.*

This symbol marks examples which serve to illustrate a certain situation.

1 This symbol marks the individual operational steps involved in a particular operating instruction. Operating instructions describe operational steps, for example, how to open a menu or execute a function.

▪ This symbol marks listed subjects. The symbol for listed subjects can be either used to structure a continuous text or to list main subject keywords.

➢ This symbol marks list inside a bulleted or numbered list.

 This symbol marks cross reference information that is available in another manual.

1.3 New Functions in User Management

Password Expiration Feature

A feature that allows you to exempt selected user from the password expiry

Function Rights for Open and Save in ALB

Open and save ALB based on function rights.

2. Overview

User management is part of the administrator's responsibilities.

All of the essential stipulations for user rights are described in the manual. It is necessary to have exact knowledge of the Process Engineer object structure and the plantype sets in order to create good rights management. Besides the user management used for determining the user, group and function permissions, the assignment of rights to access plantype sets, plantypes, and projects is essential.

To be able to assign access rights, the user to whom such access rights shall be granted needs to be defined first. Therefore, DELMIA Process Engineer® allows creating users and assigning access rights to them individually. If several users with identical rights exist, these users can be assigned to groups. The access rights are only assigned on the group level and the users then "inherit" the access rights. How to create users and groups is described in the chapters User Management Interface, respectively.

The following is a comparison of the access rights assignment used in DELMIA Process Engineer® until Version 5.16SP 4 and the new access rights.

2.1 Access Rights

Access Rights Assignment used until DPE Version 5.16SP4
Until the DPE version 5.16SP4 all objects in the DPE data model directly accessible to a user (e.g. creating, changing or deleting objects in the PPR navigator), from the standpoint of access rights administration could be devided into five groups:

- **Group 1 (all Ergocomponents):**
  Certain rights are required to be allowed to create, change and delete such objects. These rights can be administered in connection with the object itself or its type (in that case it is a Slave ErgoPlanType object) (The chapter *Basic information concerning Ergocomponents* in the Administrator Manual explains what Ergocomponents are).

- **Group 2 (Ergoprojects, templates and special security objects: *countries, companies, contracts, licenses* and *ECClassifications*):**
  Certain rights are required to be allowed to create, change and delete objects in this group. The right for creation is administered in connection with the respective function permission, rights to change/delete are administered directly in connection with the object.

- **Group 3 (all ErgoItems):**
  Access rights to objects in this group can be configured (properties of a type: *Own Rights* in the Configuration Manager. Was deactivated in the standard installation). Independent of the assignment of rights, anyone can create such objects. Such objects may be changed if not rights are assigned to them or if the user holds the required rights.

- **Group 4 (Nodes relations, plantypes, CRTokens and MODStatements):**
  Certain rights are required to be allowed to change or delete objects in this group. However, these rights are not administered in connection with the object itself but by a different object).

- **Group 5 (relations and other objects that do not belong in any of the first four groups):**
  No rights are required to be allowed to create, change and delete objects in this group.

Determining Rights in the DPE-Version 5.16SP4

Whenever access rights are assigned, they take immediate effect not only on the object, plantype or type to which they were assigned, but possibly also on the children of this object.

Right Determination at Ergo Components

The most common objects to which access rights are assigned are **Ergo Components.** The first access right found is used in determining rights. The test proceeds as follows:

1) First the user rights to the objects are checked.

➢ If no user-specific object rights are found, in the next step

2) The user rights to the plantypes are checked.

➢ If no user-specific rights for plantypes are found,

3) The group rights to the object are checked.

➢ If no group rights to the object are found

4) The group rights to the plantypes are checked.

➢ If no group rights to the plantypes are found

5) The parent rights are checked. Step 5 signifies:
if no access rights have been assigned for the object or plantype set, this does not mean that access rights will not be checked. Only the user rights for another object, the father, are checked.

- Additive determining of rights for all groups. The group-specific and the "everyone" rights are added. An example of the additive determining of rights is shown in Figure 1.

Somewhat different behavior at objects of group 2, 3, and 4, is to be expected for **non-Ergo Components** (Ergo item, versions, etc.). Only the *Object rights* for users and thereafter for groups are checked here. And if no local access rights are present, the rights are recursively checked at the father down to the Ergo item. The rights of objects in group 5 will not be checked.

General Determination of Rights

The first access right found is used in determining rights. The test proceeds as follows:

6) First the user rights to the objects are checked.

➢ If no user-specific object rights are found, in the next step

7) The group rights to the object are checked.

➢ If no group rights to the object are found

8) The parent rights are checked. Step 3 signifies:
if no access rights have been assigned for the object or plantype set, this does not mean that access rights will not be checked. Only the user rights for another object, the father, are checked.

2.1.1 Access Rights Assignment

Access Rights Assignment as of DPE-Version 5.16SP4
The new, extended access rights concept has become more complex without becoming less straight forward. With the possibility to assign rights to use of types (via the Regular Types), has resulted in an extention of the rights assignment, but in general, the administration of access rights has become more streamlined and easier. The following remains the same:

- The rights assignment for Ergocomponents remains as it is.
- The rights assignment for objects in group 4 (Nodes relations, plantypes, CRTokens, and MODStatements) likewise remains as it is.

The following changes are observed:

The subdivision of the groups has changed.

- For all objects belonging to group 2 (Project, template etc.), group 3 (ErgoItems) or group 5 (relations), you can define *in the configuration* with the ***Own Rights*** setting whether access rights are generally required to access objects of this type. If the value is set to yes, only users holding the corresponding right can change or delete already existing objects. To be able to create such objects no special rights are required.
- The administrator can define exactly, which types of objects are protected by access rights and which are not. This applies both to changing or linking of already existing objects, as well as creating new objects. It is possible to administer access rights for all objects of the same type in connection with a special object. The user interface takes all this information into consideration and proposes only actions for which the current user is sufficiently authorized.

2.1.1.1 New Access Rights Concept

Access rights can be given by User or groups.

In DELMIA Process Engineer® you can give access rights for

- Functions
- Plantypes
- Regular Types and
- Individual objects

Function Permissions
Function permissions assign access rights to the individual functions of the DELMIA Process Engineer. The function is then either accessible or inaccessible to a user or group.

A typical example of function permission is the user management itself. Since not every user creates users, groups, or group affiliations, the access rights to this function must be assigned or restricted.

The function permissions are set in the *user management* dialog.

Use and editing of the user management is described in section User Management Interface.

Access Rights to Plantypes

Access rights to plantypes are used to assign user rights for individual plantypes. To be able to edit, change or create objects of a specific plantype, access rights for the respective plantypes are required. To get access rights for plantypes access rights must have been defined in connection with the plantype set itself. The same applies to creating a project: In addition to the Global Regular Type access right users also need full access to one or several plantype sets or own **at least** a right to change (in this case, projects must be deleted by the administrator).

User rights to plantype sets and individual plantypes are assigned in the system library or in the plantype set of the project. Access rights to the system library also serve as a template for access rights to the plantype set in the project. Note that the access rights in the system library should be assigned with more restriction in comparison to assigning rights in the project plantype set.

Zugriffsrechte aus dem Planungstypensatz der Systembibliothek können an den Planungstypensatz des Projektes überschrieben werden.

How to assign access rights in connection with plantypes is described in section Properties of Regular Types in System Library

Access Rights for Regular Types

The data model has been extended by the new data class XDORegularType. The Regular Types are defined in the plantype set and access rights can be assigned to them similarly to assignment of rights to the plantypes of a plantype set.

In the properties of a type, the *Own rights* function is used to assign access rights to these types.

Using the access rights for Regular Types, user rights for individual types are assigned.

User rights for Global Regular Types are assigned in the system library. User rights to the Regular Types of plantype sets are assigned in the system library or in the plantype set of the project. However, the access rights defined in the system library only serve as a template for the Regular Types of the plantype set in the project. Only if a new project is created, the user rights are also transferred to the Regular Types of the projects. The actual access rights are always defined in the plantype set of the project.

How to assign access rights in connection with Regular Types is described in section Access Rights for Regular Types.

Access rights to objects

By assigning access rights to objects, you can overwrite or in some cases extend access rights which you have previously assigned to the plantypes. If, for example, you have assigned the right *Full access* on the plantype "production view", you can limit these access rights for individual users to the 'objects' "Production view A" and "Production view B" in the PPR Navigator. Viewed as levels of a hierarchy, the access rights for plantypes take effect only on the respective level. Object rights are assigned for access rights on a specific level, i.e. in the project.

How to assign access rights in connection with objects is described in section Assigning Access Rights to Objects.

2.1.2 Determination of Rights

2.1.2.1 General Determination of Rights

When the rights for objects belonging to group 4 (Nodes relations, plantypes, CRTokens and MODStatements) are queried, the access right first located is used. The query is performed as follows:

The first access right found is used in determining rights. The test proceeds as follows:

1) First the user rights to the objects are checked.

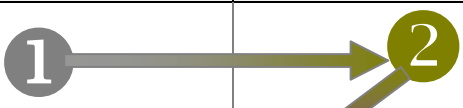
➢ If no user-specific object rights are found, in the next step

2) The group rights to the object are checked.

➢ If no group rights to the object are found

3) The parent rights are checked. Step 3 signifies:
if no access rights have been assigned for the object or plantype set, this does not mean that access rights will not be checked. Only the user rights for another object, the father, are checked.

Table 1: Access Rights

	User right	Group right
Object rights		
Permissions of the father	If no user or group rights exist, the rights belonging to the father apply.	

What fathers are there?

Table 2: Parent Rights

Objects	The parent rights of:
Project	- Does not have a father
Plantype set	Project or no father (library)
Ergo Components	Project
Ergoitem	Project or Ergo Components
PPR relation (global)	Project
PPR relation (owner)	Ergo Components (owner)
SubCompView	Ergo Components

Subcompviewitemlistpro (and derived classes) either have an Ergo Components or the parent group as a parent.

- If there are no local access rights, the rights for the father are recursively checked up to the Ergo Components.
  If you formed groups in the Manufacturing Concept to which you have as-

signed access rights, these access rights apply for the group members as well provided they are not overwritten.

- Restrictive determination of rights. If user-specific rights exist, then they are decisive; all other rights are then not used when determining rights.

2.1.2.2 Determining Rights for Ergo Components

The Ergo Components (Group 1) are the objects of the three views (subassemblies, processes, location, plant, production view, etc.)

The first access right found is used in determining rights. The test proceeds as follows:

1) First the user rights to the objects are checked.

➢ If no user-specific object rights are found, in the next step

2) The user rights to the plantypes are checked.

➢ If no user-specific rights for plantypes are found,

3) The group rights to the object are checked.

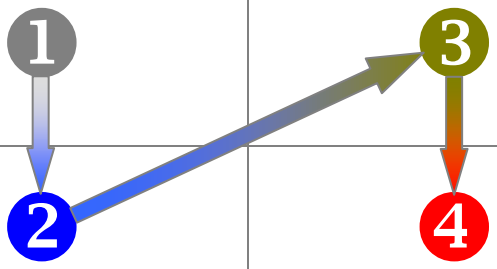
➢ If no group rights to the object are found

4) The group rights to the plantypes are checked.

➢ If no group rights to the plantypes are found

the parent rights are checked. Step 5 signifies:
if no access rights have been assigned for the object or plantype set, this does not mean that access rights will not be checked. Only the user rights for another object, the father, are checked.

Table 3: Determining Rights for Ergo Components

	User right	Group right
Object right		
Type right		
Parent rights	 here **project** If no rights are found in the first four attempts to determine rights, the rights belonging to the father apply.	

- If there are no user-specific rights, then the group-specific rights apply. If there are no group-specific rights, then the rights owned by the father apply.
- Additive determining of rights for all groups. The group-specific and the "everyone" rights are added. An example of the additive determining of rights is shown in Figure 1.

2.1.2.3 Access Rights for Ergoitems, Relations and other Objects

Access rights can also be assigned in connection with objects belonging to the groups 2, 3, and 5. For instance, whether or not access rights can be assigned in connection with Ergoitems or relations, is determined in the configuration.

To make the setting, activate or deactivate the *Own rights* function in the properties dialog of a type.

Note

A type may also inherit the property and therefore does not need to be configured explicitly for assignment of access rights.

If a user is to be allowed to create certain types of objects, such types need to be “localized” in corresponding projects. To localize type “xyz” in a master plantype set, means to create one object of the type “regulartype” in the master plantype set and all slave plantype sets derived from it. As soon as the object has been created, it is included in the query for access rights to objects of this type in the respective project. This query then functions according to the same principle already used for the Ergocomponents:

The first access right found is used in determining rights. The test proceeds as follows:

1) First the user rights to the objects are checked.

➢ If no user-specific object rights are found, in the next step

2) The user rights in the corresponding – RegularType – object to the plantypes are checked.

➢ If no user-specific rights for the RegularType are found,

3) the group rights to the object are checked.

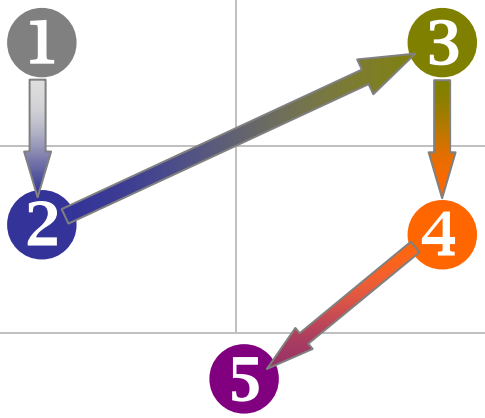
➢ If no group rights to the object are found

4) The group rights in the corresponding – RegularType – object to the plantypes are checked.

➢ If no group rights for the Regular Type are found when the next step is:

5) The parent rights are checked. Step 5 signifies:
if no access rights have been assigned for the object or plantype set, this does not mean that access rights will not be checked. Only the user rights for another object, the father, are checked.

Table 4: Access Rights for Ergoitems, Relations and other Objects

	User right	Group right
Object right		
Type right		
Parent rights	If no rights are found in the first four attempts to determine rights, the rights belonging to the father apply.	

2.1.2.4 Access Rights with New Objects

As long as a new object *is not saved*, it owns **all** rights. The right to create a new object does not have to have to contain the right *Edit*. Therefore a case can appear in which you can create an object but after saving the object in database, the object cannot be edited anymore. In such a case you have to define access rights of new objects before saving.

2.1.2.5 Access Rights with Templates

Previous to version PE5.15, access rights were not copied when using templates were used in a project.

As of version PE5.15 the copying of rights depends on the setting "Browser and menu items > Copy objects with rights“ -- these were previously taken into consideration in general for the copying objects.

Now they are taken into consideration both when copying an entire template into a project and when referencing (single reference usage).

2.1.2.6 Access Rights in the case of New Versions

Whenever new versions are generated, the access rights are copied to them. If access rights are redefined in a version, these access rights only apply to this version and the following versions based on it. If older versions are used, the access rights of those versions apply.

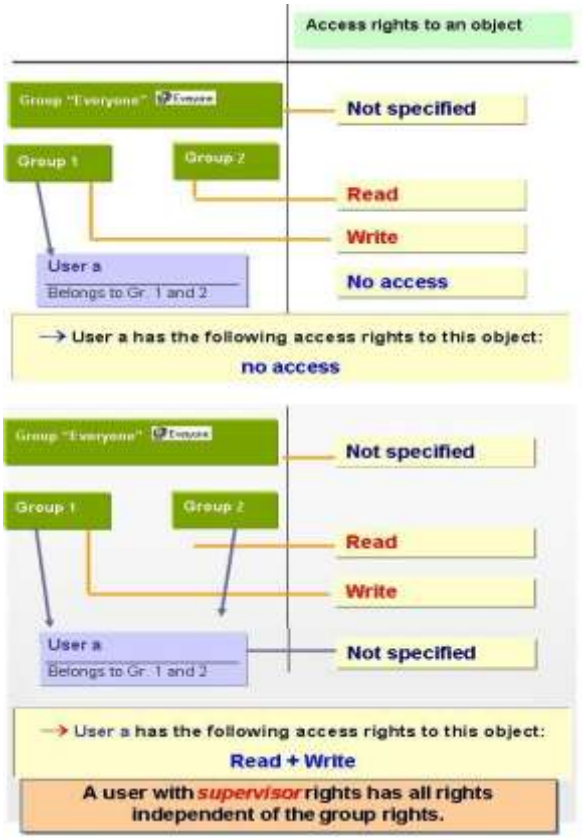


Figure 1: Example of Rights

2.1.3 Defining own Access Rights

The new ***rightvalue*** attribute has been added in the Configuration Manager. All dialogs for assignment of access rights are based on this attribute. The ***rightvalue*** attribute is found on the type *dodefaultimpl* ; and since almost all other types are derivied from *dodefaultimpl*, this attribute is also available on all types.

Figure 2: Opening the User Management

The following figure shows the dialog as implemented in the standard version of DELMIA Process Engineer®.

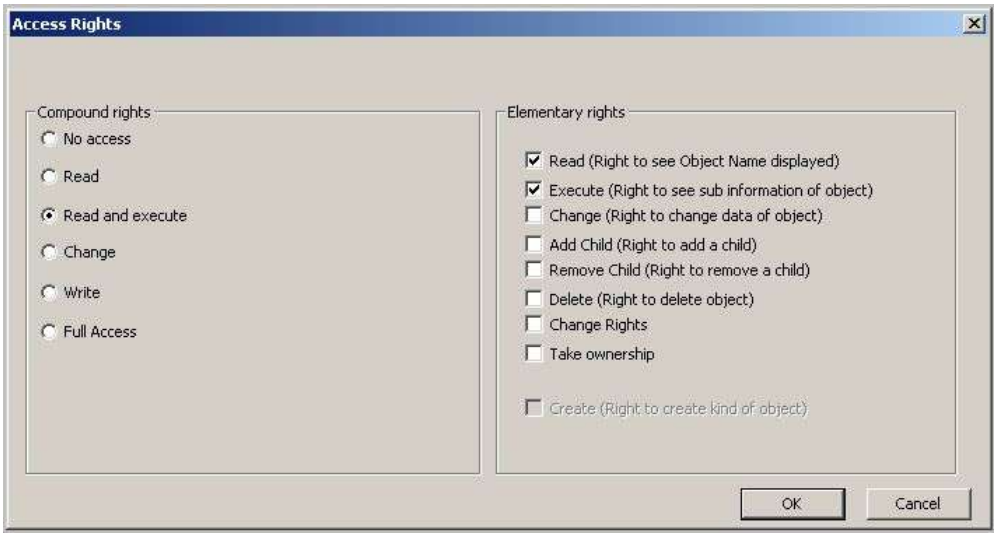


Figure 3: Access Rights Dialog

Left appear the compound rights predefined during installation of DPE. If you activate one of these access rights, the right side will display details of the rights included in this compound right. If you have already assigned access rights in previous versions of DELMIA Process Engineer, you will know this dialog as the user-specific rights definition. The design of this dialog is controlled by the ***rightvalue*** attribute. As of version 5.16SP4 you can adapt this dialog to meet your own requirements.

- Overwrite this attribute in connection with the types or plantypes in which you wish to define the user-specific access rights. Then edit the value list. The values must be entered as described in the following table.
- By default, the value list is structured as follows:

Table 5: Value List Structure

Entry in List of Values	Item Value	Display Order
NOACCESS	0	1
READ	2	2
READ AND EXECUTE	6	3
CHANGE	782	4
WRITE	814	5
FULL ACCESS	1006	6

Except for the internal values there is nothing special in this list of values. How were these internal values generated?

The internal value is comprised of the values from the following table

Table 6: List of Values for Access Rights

Access right	Value
NOACCESS	0
READ	2
EXECUTE	4
CHANGE	8
CREATE	16
DELETE (ERASE)	32

Access right	Value
TAKE OWNERSHIP	64
CHANGE RIGHTS	128
ADD CHILD	256
REMOVE CHILD	512

When you select the access right ***Change***, you will notice that it is comprised of several other access rights.

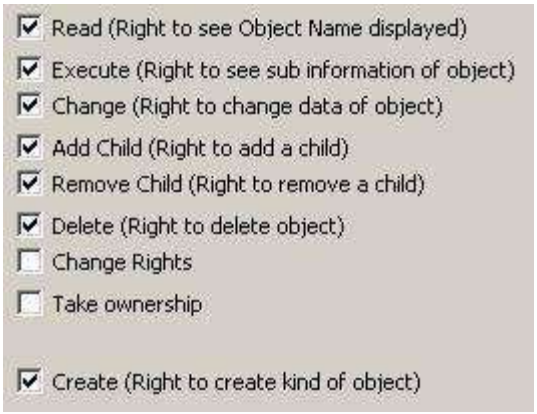


Figure 4: Access Rights

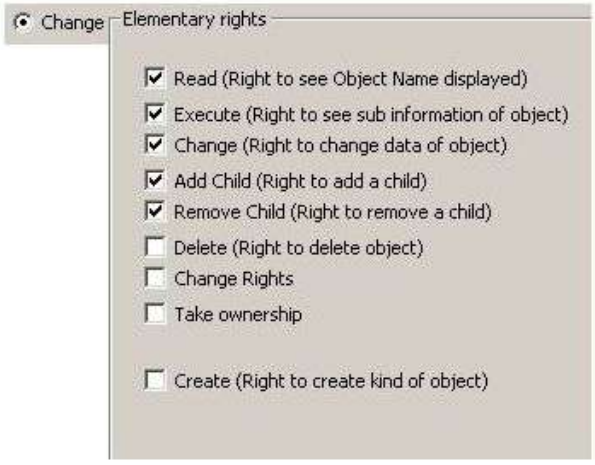


Figure 5: Change Access Rights

If you base the input on the value list shown in Table 4, you can add up the correponding values: Read 2 + Execute 4 + Change 8 + Add child 256 + Remove child 512.

- The sum is 782. This corresponds to the internal value in the value list of the ***rightvalue*** attribute for the right to change.

If the access right ***Write*** is selected, deleting is added as an elementary access right. According to the value list, delete has the value 32. Thus the internal value for the access right *Write* is 814 (782 + 32).

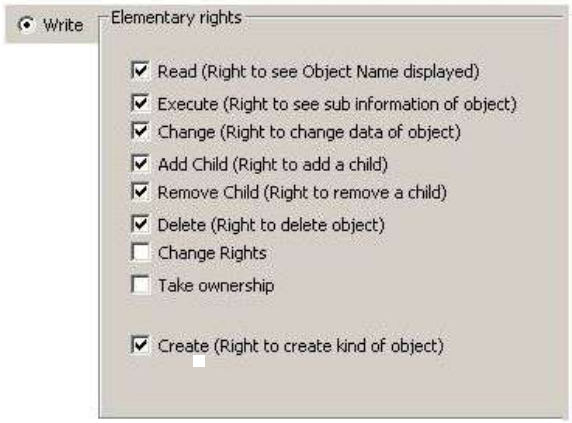


Figure 6: Write Access Right

- These examples show that the right to create an object is not defined as standard.
- To be able to define your own access rights you need to edit the values in the value list of the overwritten ***rightvalue*** attribute. You can delete the values or add new entries. Only the internal value is important.

The following access rights can be defined:

Table 7: Access Rights

Permissions	Description
Read: Read (Right to see object name displayed)	The right to display the object.
Execute: Execute (Right to see sub information of object)	The right to execute functions of the context menu for this object (this right, for example, is necessary in the case of scripts to be able to execute them at all).
Change: Change (Right to change data of object)	The right to change the content of the object, i.e. the object properties can be edited, but no child can be added (for example a link).
Add Child: Add Child (Right to add a child)	The right to add a child (for example, to add a new part to a subassembly). This right also includes the adding of children using relations.
Remove Child: Remove Child (Right to remove a child)	The right to remove a child.
Delete: Delete (Right to delete kind of object)	The right to delete this object.
Change Rights: Change Rights	The user can change the rights of an object (for example, he can assign rights to other users).
Take ownership: Take ownership	The user has the right to change the ownership of an object.
Create: Create (Right to create kind of object)	The right to create an object of this type. You cannot assign this right to objects; it can be used only for plantypes and Regular Types.

2.2 User Management Interface

To open the user management you have to select the “User Management…” menu item in the PPR Navigator **Tools/Database Utilities** menu.

Figure 7: Opening the User Management

Note

*When the application is started for the first time after the installation of the database, the system only knows the user '**admin**' with the password '**admin**'.*

The access template (or the main dialog) of the user management appears afterwards. It consists of a menu bar and two list boxes. The upper list box shows a listing of all users, the lower list box shows a listing of all user groups.

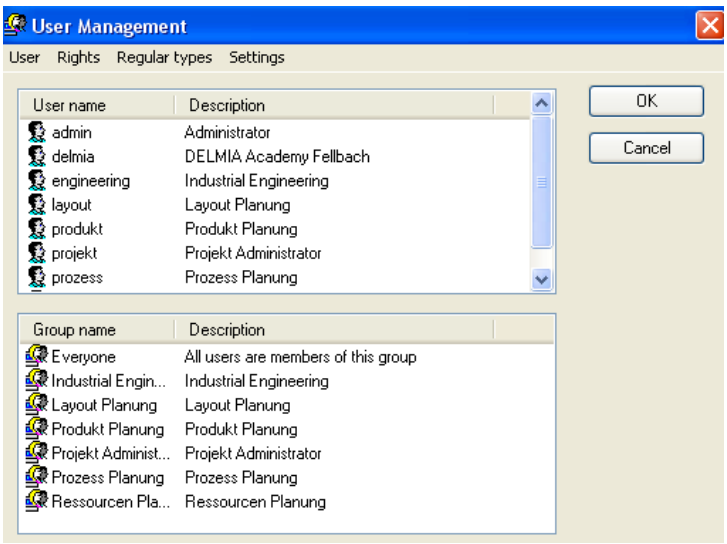


Figure 8: "User Management" Dialog

2.2.1 Menu Bar

The menu bar of the user management has the two entries: "**User**", "**Permissions**"and **Regular Types**. By left-clicking on the "User" entry a popup menu opens consisting of five sub-items. The function of the sub-items will be described in more details below. The "Permissions" entry, on the other hand, does not have any sub-items and enabling it opens the general Permissions dialog. *Please refer to the* Function Permissions. .

Figure 9: The User Management Menu Bar

2.2.1.1 Description of the Menu Items

New User

By left-clicking the *New User...* menu item the Properties-User dialog box opens; here you can enter a new user.

By right-clicking on the user field a context menu opens where you can also enter a new user.

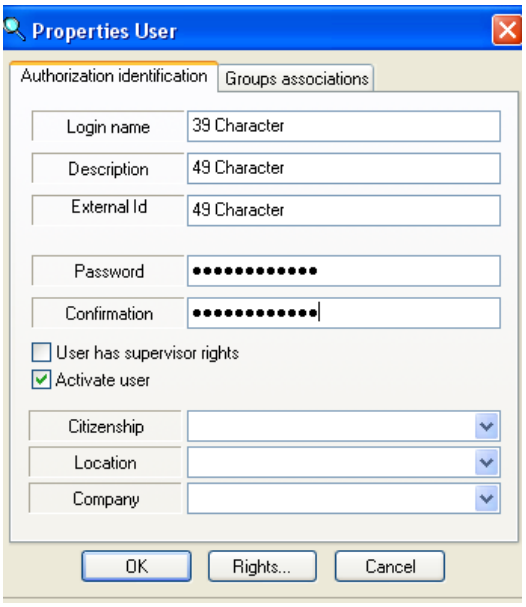


Figure 10: User Dialog

New Group

By left-clicking the **New Group** menu item the New Group dialog box opens; here you can enter a new group.

By right-clicking on the group field a popup menu opens where you can enter a new group, too.

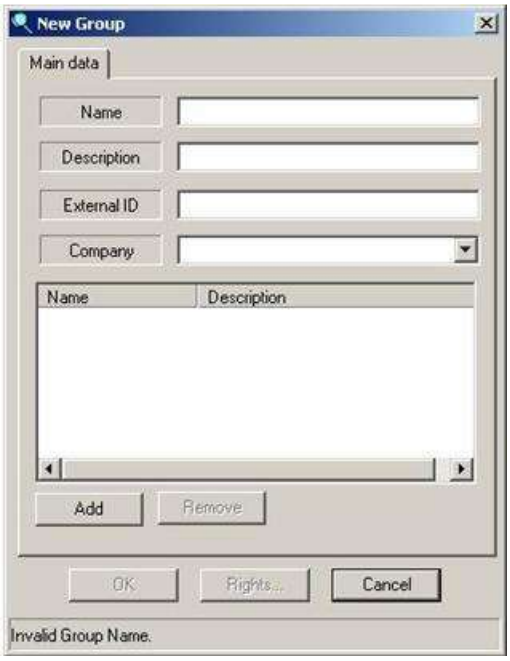


Figure 11: New Group Dialog

Delete

By left-clicking the **Delete** menu item the currently selected entry (user or group) is deleted. If no entry is selected, the menu item is inactive. As with the two menu items described above, you can also delete selected entries by right-clicking.

Properties

By left-clicking the "**Properties**" menu item the Properties-Group or the Properties-User dialog box (The Properties Dialog) of the currently selected entry (user or group) opens. If no entry is selected, the menu item is inactive.

Exit

By left-clicking the *Exit* menu item the user management is closed.

2.2.2 The Properties Dialog

The **Properties** dialog box can be used to edit users or groups, to assign new memberships or new rights.

There are three possibilities to open this dialog box:

- Select an entry (user or group) and by left-clicking the "User"/*Properties* menu item the dialog is opened.
- Double-click the entry to be edited.
- Directly right-click on the entry to be edited and select the *Properties…* entry in the context menu that opens.

2.2.2.1 "Properties-Groups" Dialog

The group-specific "Properties" dialog is used for editing the group properties.

A group is identified by:

- its "**Name**" that represents a clear identification of the group and must absolutely be available,
- its "**Description**" that represents an exact description or designation of the group and its members.

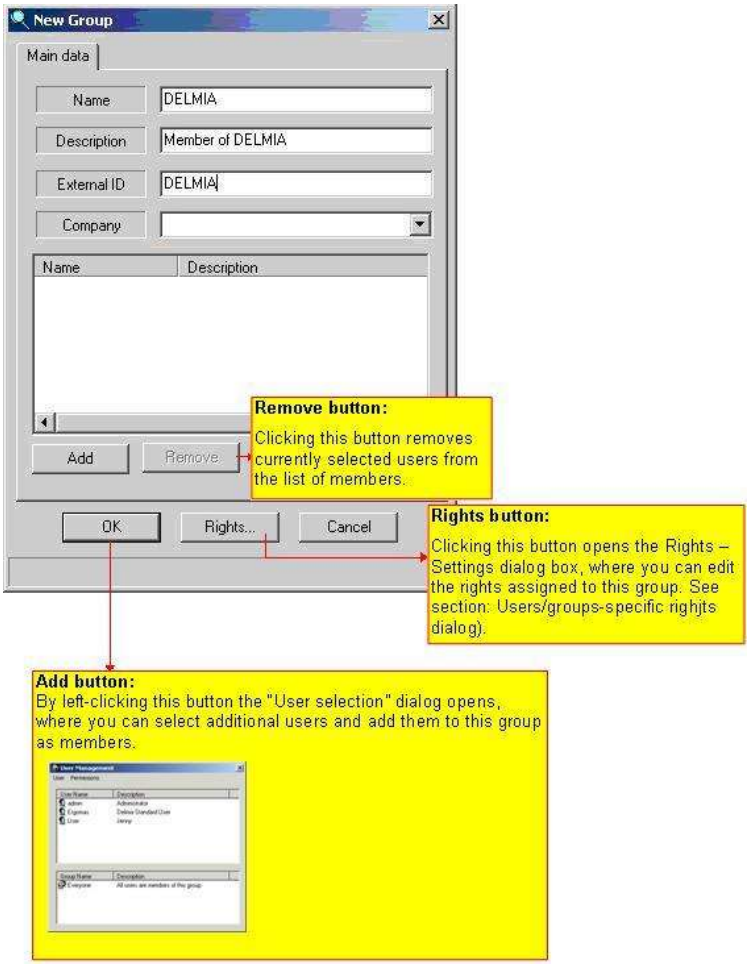


Figure 12: "User Management" Dialog Box

2.2.2.2 "Properties-User" Dialog

The user-specific "Properties" dialog is called to edit the properties of a user. The dialog consists of the Authorization identification and Groups Associations tabs. These tabs are described in more detail in the following sub-chapters.

The "Rights..." button can be clicked independent of the currently active tab. The "User rights settings on dialog" dialog box is then opened. *Please refer to the* Users/Groups-Specific "Rights" Dialog. Here, you can edit the user rights.

"Authorization identification" tab

A user is identified by the properties defined in the "Authorization identification" tab.

- The "**Login Name**" must always be entered, as it represents the unambiguous identification of the user.
- The "**Description**" does not necessarily have to be entered, but it does give a more exact description of the user, however, and can therefore be assigned more easily.
- The "**Password**" and the "**Confirmation**" of the password enable the exact authentication of the user to be verified when starting the user management or the DELMIA Process Engineer application.
  There is a minimum size for each password of ***1 character***. All users without password cannot logon after upgrade. The administrator has to enter a initial password in the user management for these users before they can logon.

- The **"Externe ID"** is required for importing and exporting projects, and it does not have to be entered. If you leave the field blank when creating a new user, the registration name will be entered automatically. This entry can later be overwritten or changed.

Figure 13: Properties-User Dialog

By checkmarking the "**User has supervisor rights**" checkbox the user has all rights independent of the settings. Thus, only the administrators should have supervisor rights.

When and which entries in nationality, place and enterprise must be made, *please refer to the* Security Guidelines.

In the "Group Associations" tab the group membership of a user can be determined. A user can be a member of multiple groups. The following actions can be performed:

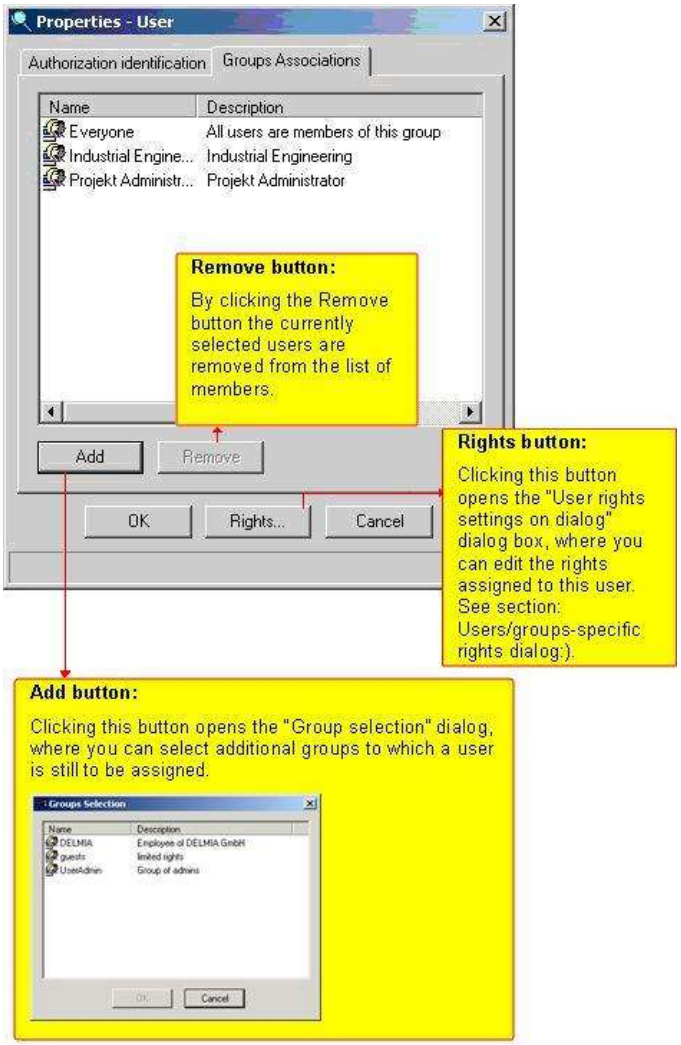


Figure 14: Properties-User dialog: Group Associations Tab

2.2.2.3 Additional User and Group Properties

The additional user and group properties can be accessed by “User Management…” (Tools->Database Utilities->User Management). The additional user properties are separated into two groups represented by two pages in the properties dialog (see Figure **Error! Reference source not found.**15 and Figure REF _Ref104271333 \h **Error! Reference source not found.**16). The additional group properties are shown in Figure 15.

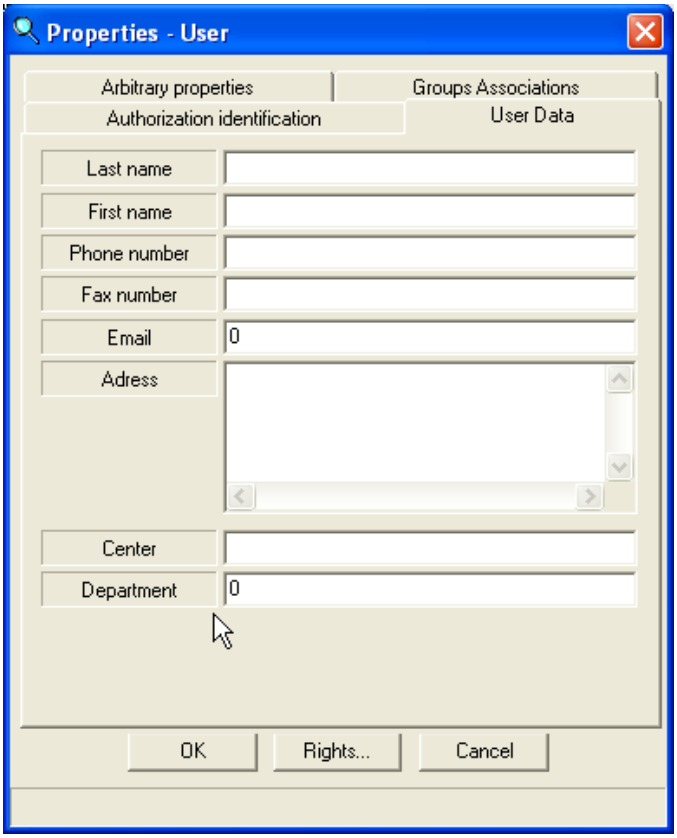


Figure 15: Use Properties: "User Data"

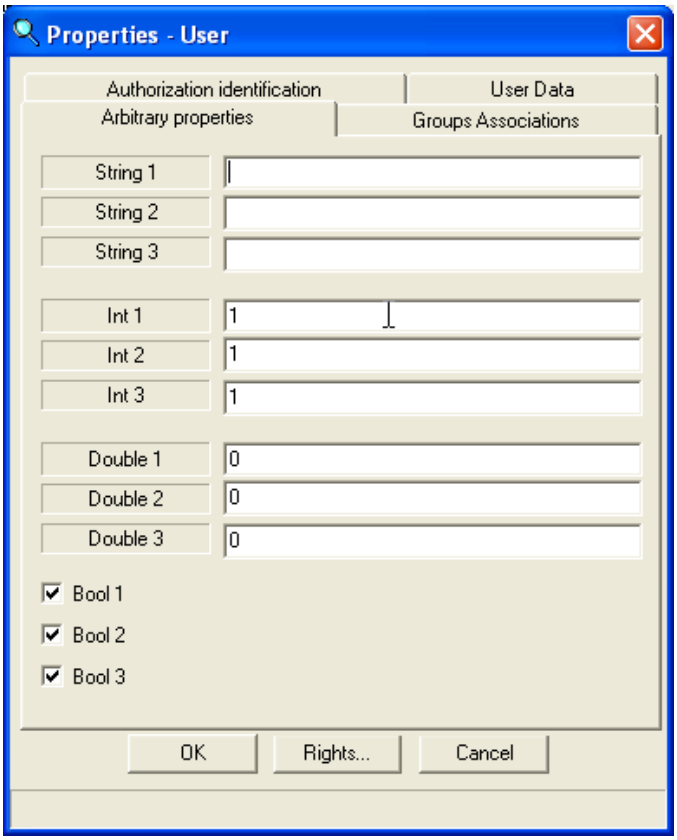


Figure 16: User properties "Arbitrary Properties"

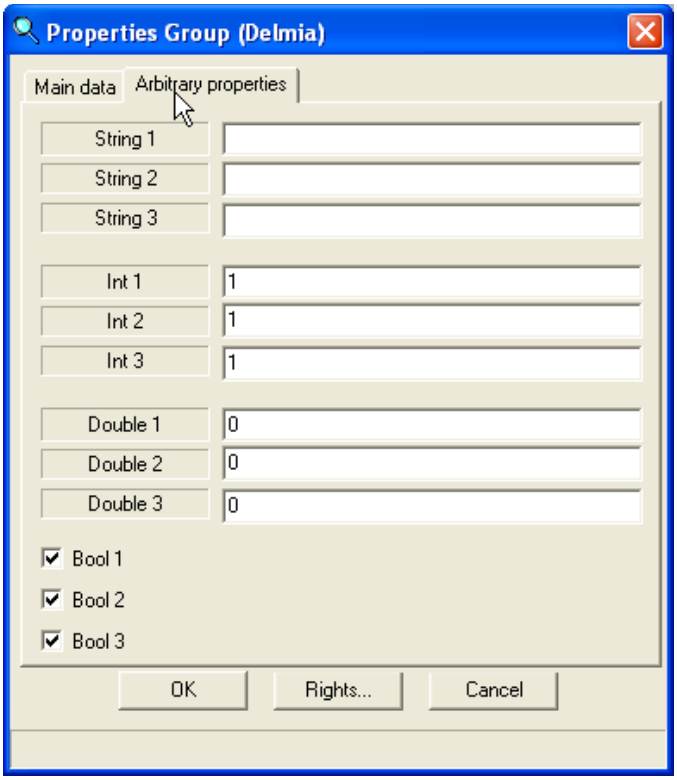


Figure 17: Group properties "Arbitrary properties"

To activate the additional user and group properties, the following steps is performed using the configuration manager:

- Go to Tools->Database Utilities->Configuration Manager).
- Type "user" (singleuser) two new pages have to be created (see **Error! eference source not found.** 18). One of the new pages has to be named as "User Data" (see **Error! Reference source not found.**19) and the other one have to be named "Arbitrary Data"(see **Error! Reference source not found.**20).

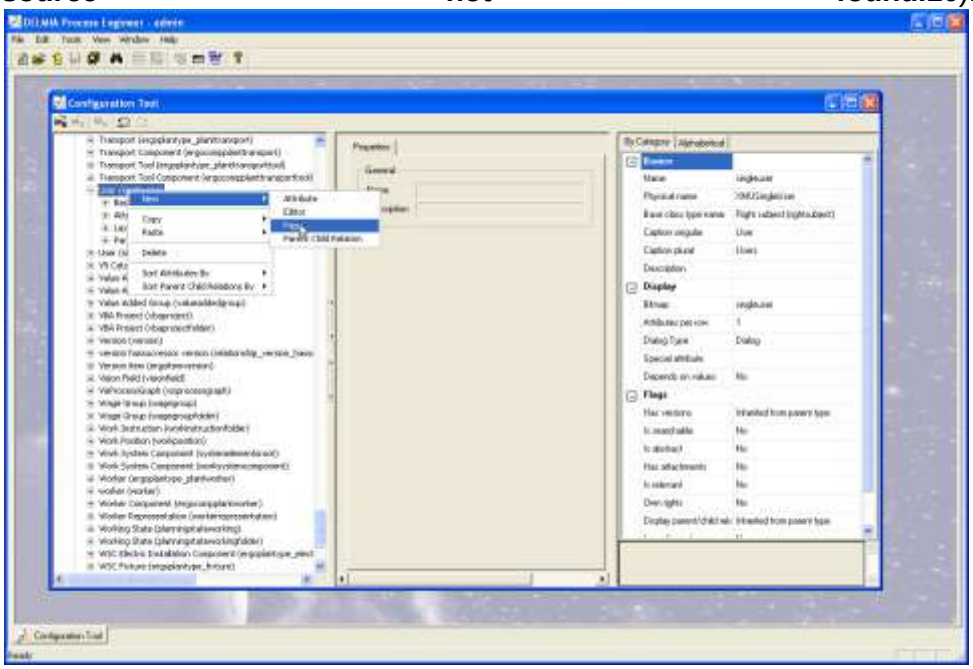


Figure 18: Create New Page for User

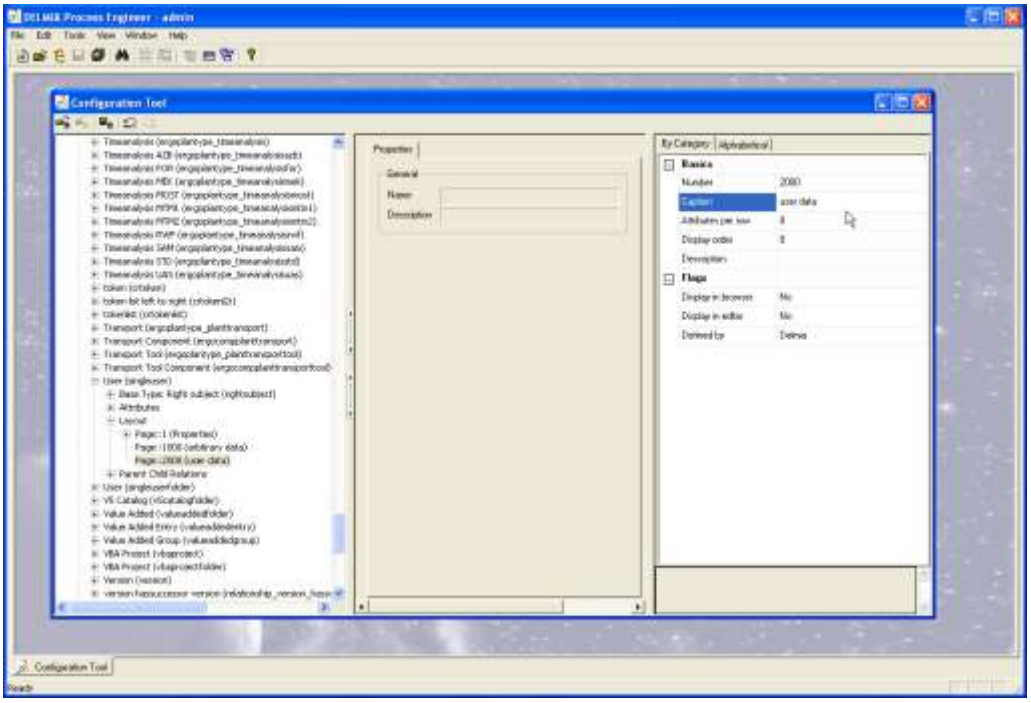


Figure 19: Change Caption to User Data

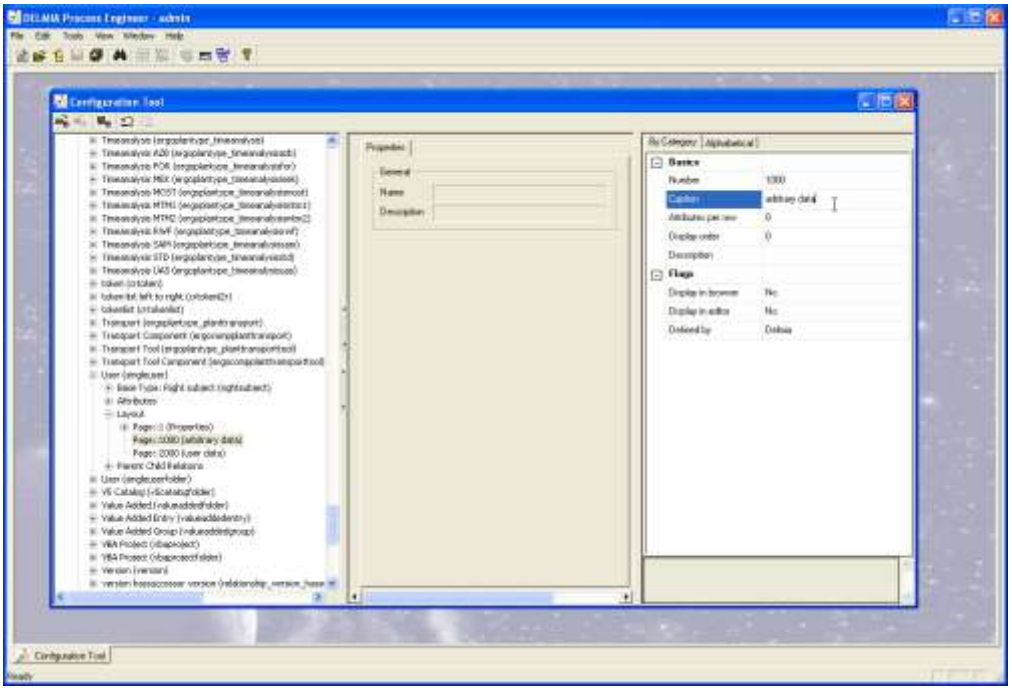


Figure 20: Change Caption to Arbitrary Data

Similarly, On type “group” (group of user) only one page has to be created. It must also be named as “Arbitrary Data”.

NOTE:

Make sure the caption is “User Data” and “Arbitrary Data”, if the caption is different, than the tabs will not be displayed in User/Group properties dialog.

2.2.2.4 Changing the Password

If the user does not have the right to call the user management. (*Please refer to the* Function Permissions) the user is, however, able to change his own password.

1) Go to **Tools** < **Change Password**.

Figure 21: Change Password Menu Item

2) A dialog box with three input fields opens where you can enter the old and the new password.

3) Click **OK.**
If the new password does not meet all configured rules, then a message pops-up. The message describes the rules to change a password in "Change Password" window. *Please refer to the* Password Rules.

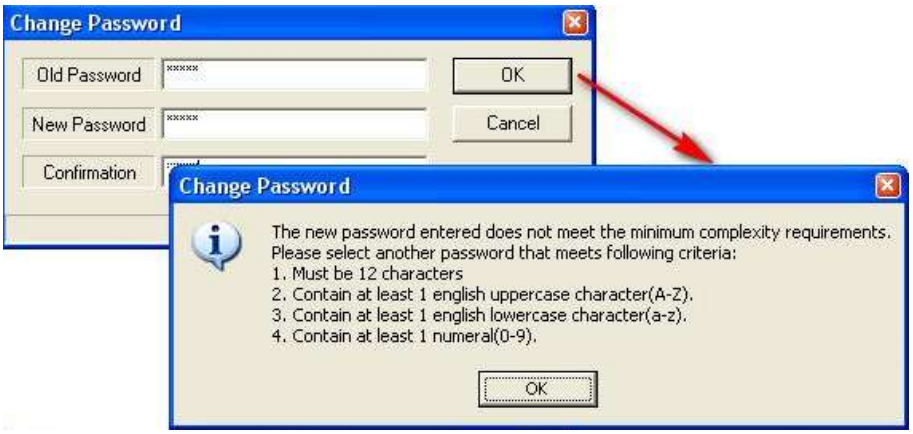


Figure 22: Password Strength Checking

4) Once the new entered password meets minimum complexity requirements, the password gets changed and the success message "**Your Password has been changed successfully** "comes up. This check will not be done for users with supervisor privilege.

5) The password expiry time period can be configured and before expiry you will start getting notification for changing the password from the date set for password expiry reminder date.
If you do not change the password till the expiry date then you will be forced to change the password. The change password dialog will be displayed and you will be forced to give a new password once the password expiry date is reached. You cannot login to DPE without changing the password once the password is expired. Password expiry date is valid for user with supervisor privilege.

6) The failed user login attempts will be logged into log file and it includes machine identifier, user identifier, date, and time of the occurrence.
The failed login attempts are logged into xml file (DELMIA->EPLOGGER), using xml tag named as "LoginFailed", the blocked user is also logged using xml tag named as "UserBlocked". The description key has login failed information. *Please refer to* Administration_Manual.
After a configured number of successive failed login attempts to a given

account, the account will be disabled until the intervention by an administrator.
If administrator account is disabled for giving wrong password then another user with supervisor privilege can activate the account.

7) Admin can enable or disable the user by **Activate User** check box in **User Properties'** dialog box
If user gets disabled due to successive wrong password.

Figure 23: Activate User

Password Rules

1) Select **Tools** > **Database Utilities > User Management** > **Settings.**
2) Select **Is Enabled** in **Settings** dialog box.

- **Is Enabled**: – This checks the password against the rules set by administrator.
- **Minimum Length of password**: Length of password as 12 (characters).
- **Password expiry (in days)** – Duration by which the password will expire. The days are counted from the first successful login.
- **Allowed number of login failed attempts** – This is the number of attempts you can try with incorrect password.
- **Password expiry reminder (in days)** – The number of days before the expiry date, you will be notified about expiry of password.
- **Upper-case, Digits, Lower-case, Special** – These are the type of characters required in the password to meet the complexity requirement set by the administrator.
- Close and save **Settings** by clicking **OK**.

3) Click **OK** in **User Management** dialog box to save changes.

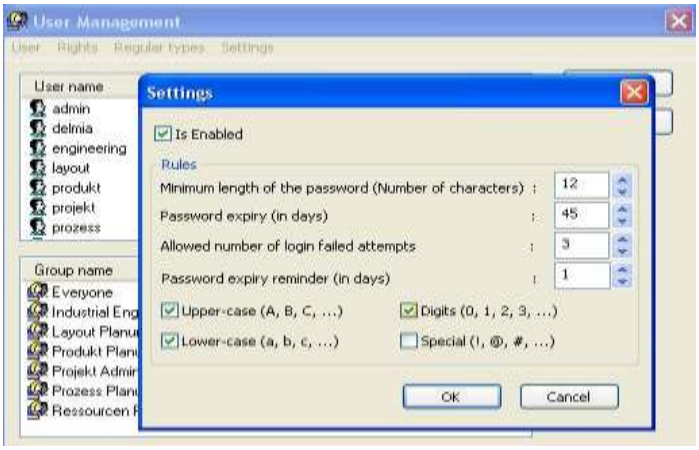


Figure 24: Password Rules

Note

The settings menu entry is enabled only for super users.

2.2.2.5 Password Expiration Feature

The Password Expiration Exemption check box in the User Properties dialog box enables you to exempt selected users from password expiry. If you select the check box, there is no password expiry check. When a new user is created, the check box is not selected by default.

The password modified date is not updated for these selected users. The user is not check for any password expiry. If the passwork expiration check box is not selected, the last password changed date is considered for the password expriration check.

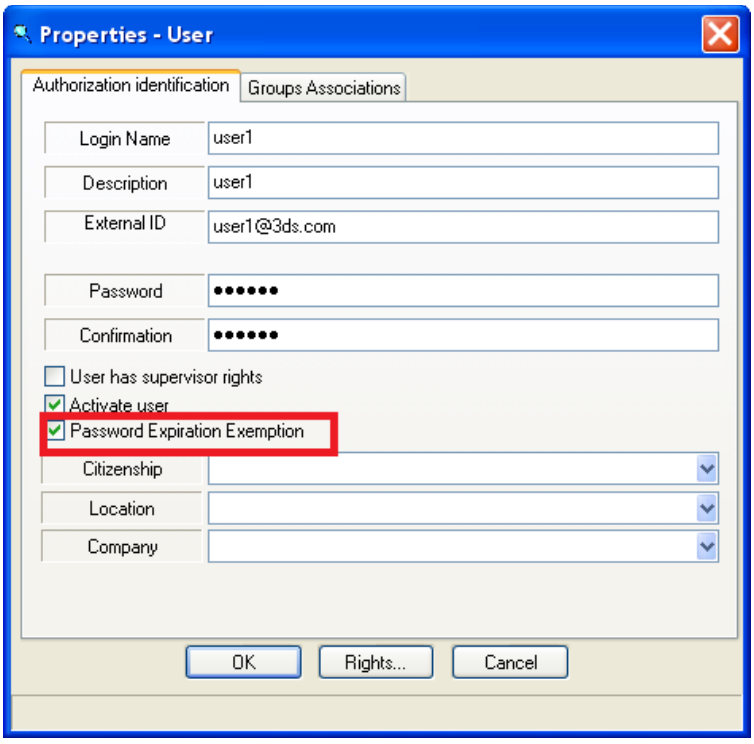


Figure 25: Password Expiration Exemption

2.3 Function Permissions

2.3.1 General “Rights” Dialog

The dialog "Functions" opens if you activate the menu item "Rights" in the "User management“ dialog. In the general “Permissions” dialog **all groups and all users** are displayed **that have been assigned rights for selected functions.** Using the dialog box you can get a quick overview of the existing rights assignments.

In the rights management you can assign **function** rights.

Access rights can be determined for superordinated functions or specifically for individual components of these functions.

Functions:

By double-clicking the function entry or by left-clicking the plus sign + you can open the sub-folders.

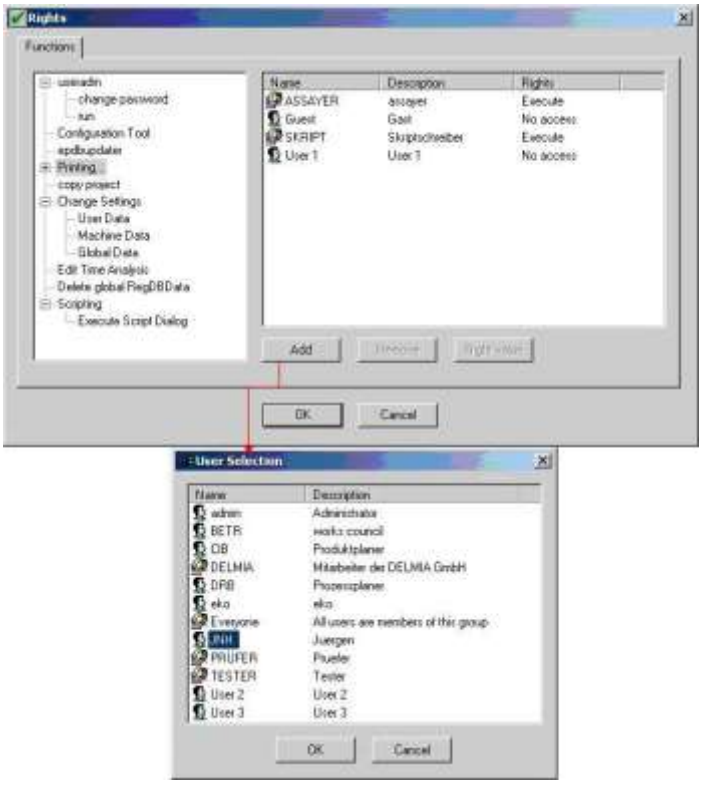


Figure 26: General Rights, Functions Tab

If an entry is selected in the left column of the dialog box, the groups or users that have already been assigned rights for the selected function are displayed in the right column assuming that rights were previously assigned. As long as no group or user has been selected, no type of access is shown.

Add Button

By left-clicking the **Add** button the “Users/Groups Selection” dialog opens showing all groups/users to whom no rights have been assigned yet for the function entry selected.

Remove Button

By clicking the **Remove** button the currently selected users or groups are removed without confirmation.

Button Access Type *(right value)*

This button is active only after a group or user has been selected. You can activate (execute) or deactivate (no access) the function permissions for the selected users or groups in the "Access Rights" dialog.

Figure 27: Access Rights

OK and Cancel Button

Using these buttons you can save the changes made (***OK***) or you can exit the dialog without saving (***Cancel***). The dialog is always exited after clicking one of the buttons.

Note

Rights of superordinated entries are mandatory. The rights in the components serve to refine the assignment for individual users or groups. However, you cannot undermine or sap superordinated rights

Procedure for Assigning Rights

1) Select a function.

2) Add the groups and users to which you want to assign special rights to the selected function with the *Add* button.

3) Select one or more of the groups or users to be added.

4) You can assign access rights to the current selection with the *Access Rights* button.
   Two access rights are available in function permissions:
   Function can not be executed = *no access* or
   Function can be executed = *execute*.

2.3.2 Users/Groups-Specific “Rights” Dialog

Using the **Properties/Rights** function you can determine access rights for each user and each group.

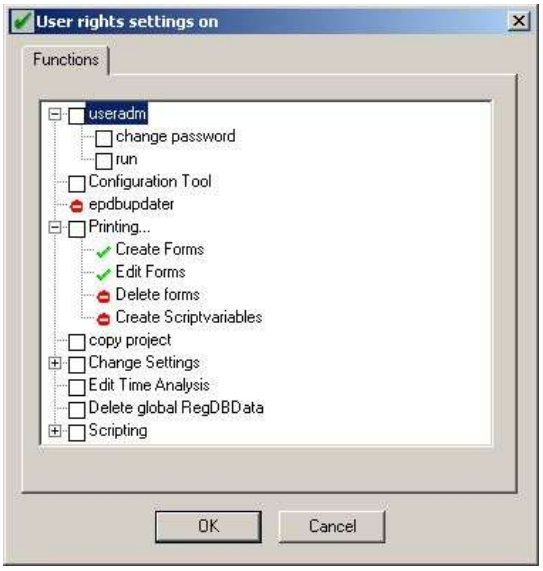


Figure 28: User Rights - Settings Dialog for Users/Groups

In order to assign function permissions to a group or user in the **User Rights dialog**, you must select the respective function. You can activate or deactivate the function permission by clicking the left or right mouse button.

The following table shows how to use the mouse buttons.

Table 8: Mouse Buttons Description

Icon	Meaning	Mouse button	Description
✔	Execute	Left mouse button:	Function permission is activated
⛔	No access	Right mouse button:	Function permission is deactivated
☐	Nothing assigned	Double click right or left mouse button.	No function permission assigned

The assignment of rights is explained again in detail below. Afterwards, you will be shown in an example how rights are inherited and added.

Administrator or a User with Administrator Rights:

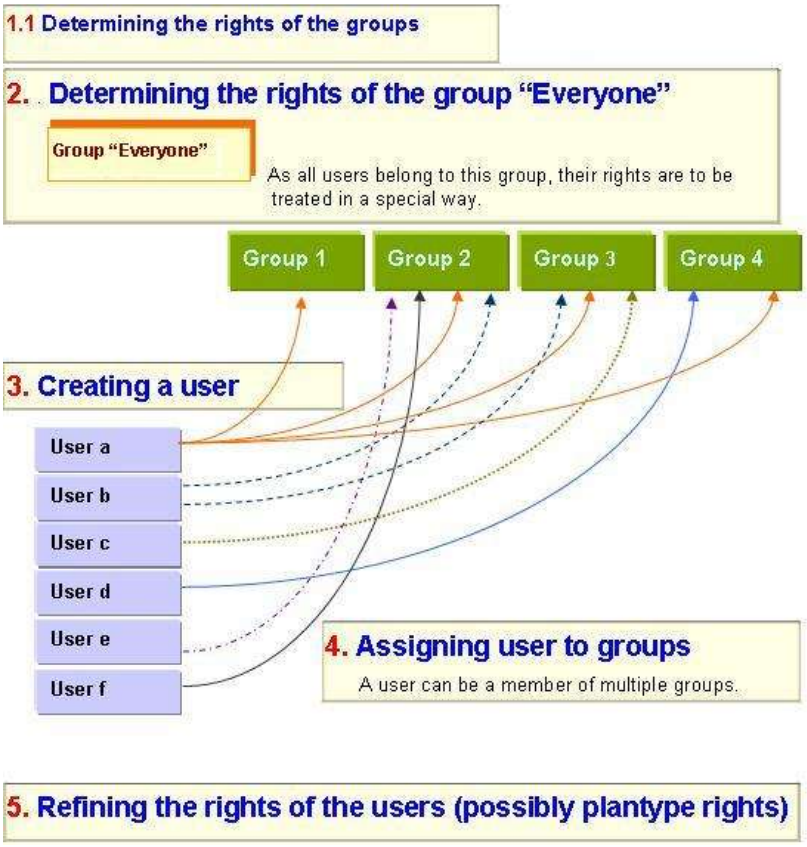


Figure 29: Procedure when Creating Groups and Users

The exactly descriptions for the Function permission can be found in the Appendix: *Please refer to the* Appendix

Function Permissions.

2.4 Regular Types

2.4.1 The Regular Types Dialog in the User Management

If you activate the menu item **Regular types** in the "User management" dialog, the "Created And Not Created Regular Types" dialog will open. In this dialog, **all types to which access rights may be assigned**, are shown. In order to assign access rights for types in configuration manager the property **Own Rights** has to be set on Yes or property **Own Rights** is inherited by a base type.

With the aid of this dialog, you can determine which types will appear in the folder for the global regular types of the system library. This determines the access rights for higher order, cross-project objects.

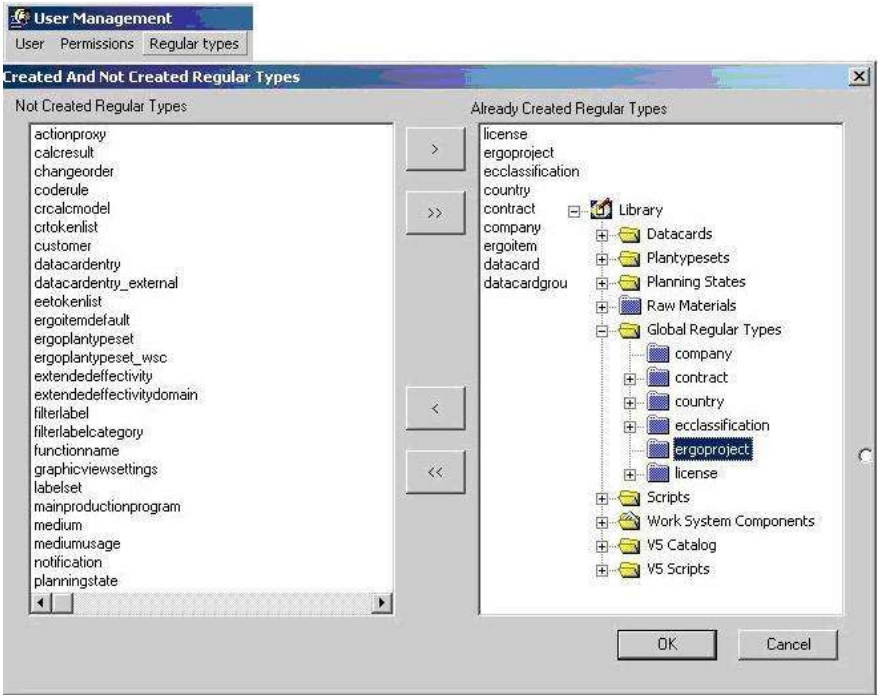


Figure 30: "Created and Not Created Regular Types" Dialog

- The left list in the "Created And Not Created Regular Types" dialog shows all types to which access rights can be assigned.
- The right list in the "Created And Not Created Regular Types" shows all types already assigned to the Global Regular Types folder.
- The buttons with the single arrows allow to move individual types between the lists, the button with the double arrows allow to move the entire list.

The Global Regular Types Folder

In the **Global Regular Types** folder of the system library you may assign to users who do not hold superuser rights the right to create safety-related data objects, such as for companies, lands or contracts.

The following types are required:

- Country, company, contract, ecclassification, licence, and ergoproject.

With the aid of the Regular Type **ergoproject** you define the user´s access to a project.

Beside security relevant data objects you can add also here more data objects. **Global Regular Types** are always needed whenever access rights are to be defined as cross project.

2.4.1.1 Properties of Regular Types in System Library

Figure 31: Regular Data Types

In Properties of a **Regular Types** you can only activate checkbox *"***Apply Rights to Objects in CCZ** *also"*. CCZ stands for Configuration Control Zone and means, that for an object and its children (ergo components, ergoitems

and relations) a configuration is available which is different from project (ergo project) and other types. In the **Configuration Control Zone** *(CCZ)* there is an object which is **Owner** and whose children (and children of children) are in a relationship with the Owner but at the same time they are dependent on him. If a child is also indicated as *Owner* then a new CCZ is created. You specify in configuration of a type, whether a type or a plantype is *Owner* or *Member.*

What cause an activating of "**Apply Rights To Objects In CCZ Also"?**

This entry does not have effects for *Global Regular Types* and ergo components. If this entry is activated however on ergoitems, the rights of ergo components with the linked ergo item is taken over and not those rights of the project. By an example this circumstance can be described:

Attachments are ergo items and can be attach on every ergo component and project. They are not visible in project library but they are stored in database. If you assign access rights for attachments with the help of **Regular Types** by activation of **Apply Rights To Objects In CCZ** *Also* the access rights are considered independently of project access rights and in each case access rights of ergo component are used.

2.5 Access Rights to plantypes, Regular Types, and Objects

If you do not have rights to an object, this object is either not displayed or you cannot access the object. The users and the groups of the user management have to be assigned to the individual objects and plantypes.

In the following sections the assignment of access rights is described.

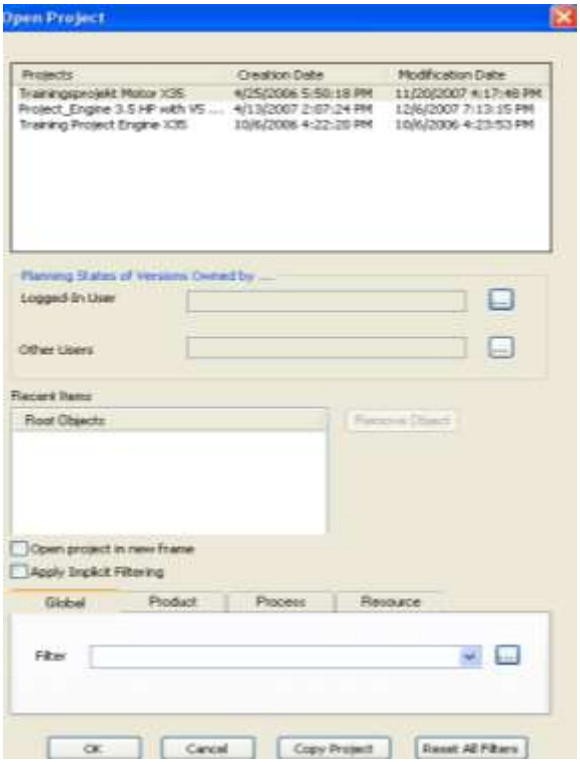


Figure 32: The Open Project Dialog if no Access Rights are Defined for a Project.

As explained in Figure 32 the user does not have access rights to projects. For this reason no projects are displayed in the *Open Project* dialog.

How you can define access rights for objects is displayed in details below. For this purpose DELMIA Process Engineer offers three possibilities:

- Assignment of rights on plantype level
- Assignment of rights on Regular Types
- Assignment of rights for individual objects

On the plantype level or to Regular Types, access rights can be assigned in the system library (general library) or in the project library. Access rights to project plantype sets, on the other hand, are effective only in the project.

Note

Access rights assigned in the system library, whether to plantypes or Regular Types, are only considered templates for the project.

2.5.1 Assigning Access Rights to Plantypes

In the Process Engineer the rights to plantypes are assigned in the following way:

If you open the context menu of the plantype, you will find two entries that refer to rights

- Permissions and
- Permissions...

Figure 33: Definition of Permissions for Plantypes

2.5.2 Assigning Access Rights to Individual Plantypes

Permissions... menu item

Using the **Permissions...** menu item you can assign access rights to the selected object.

1) Click **Permissions..** in the context menu of a type.

- Then the window **Data Object Permissions** opens, in which you can assign the user rights for this object.

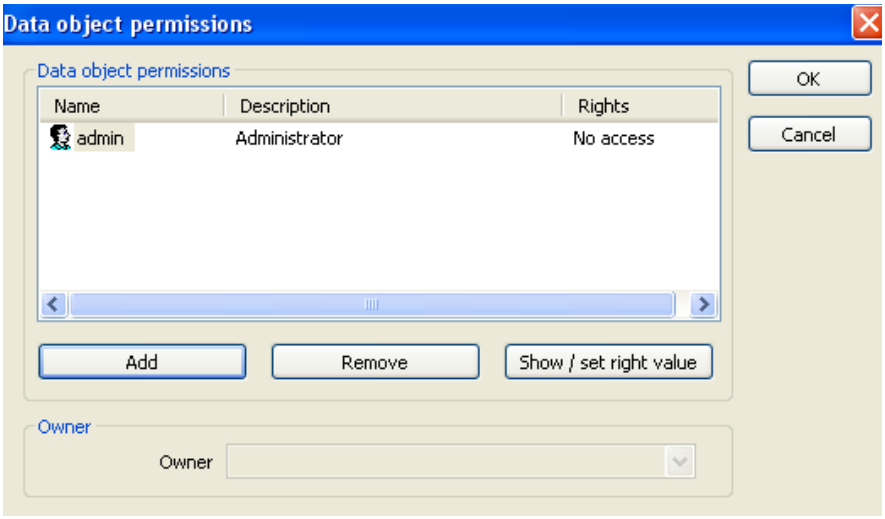


Figure 34: Data Type Permissions Dialog

The assignment of users is performed in the same way as in the case of data objects. The procedure is therefore described in the section: Assigning Access Rights to Individual Objects and Assigning Access Rights to Individual Objects

2.5.3 Passing on Rights to other Plantypes

2.5.3.1 Rights Menu Item

With this menu item, the rights of a selected plantype are passed on to other plantypes (of the same plantype set).

You have three possibilities to determine or to remove the rights of other plantypes:

Remove Rights
Using this menu item you can remove user rights from multiple types at the same time.

Proceed as follows:

1) Select a plantype and open the **Rights/Remove** rights in the context menu.

2) In the dialog ***Data* Object Permissions** you can specify which user or group from which specific permissions are to be removed. For this purpose add the user(s)/group(s) using the **Add** button to the empty display field of the dialog. Using the **Type of Access** field you can determine the access rights to be removed. Whenever you call the dialog the display area is empty. Quit the dialog using the **OK** button.

3) A dialog (Figure 35) opens where you can select the plantypes from which the previously selected right should be removed. Remove the access rights for each selected entry (grey background). If rights are removed that do not belong to this type, nothing will happen. How is the selection made?

- If you want to select all entries, you have to mark all entries in the corresponding view by holding down the mouse button.
- In the case of an individual or group selection press the Ctrl or the Shift key while holding down the mouse button; this procedure is already familiar to you from the Windows browser.

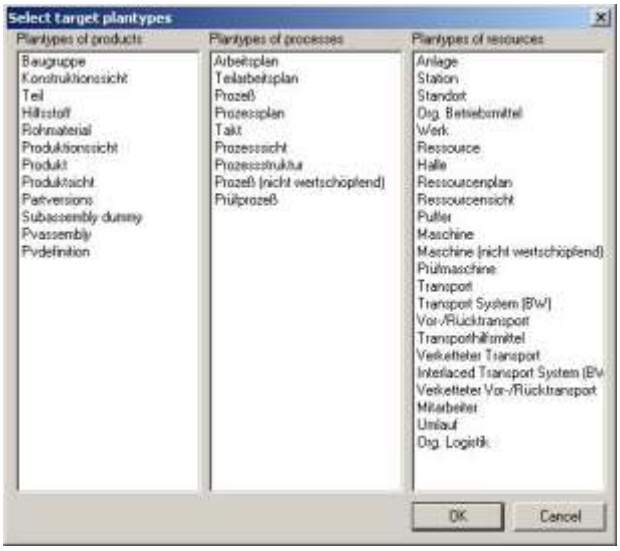


Figure 35: Dialog for Selecting one or Multiple Plantypes

Add Rights

Using this menu item you can add user rights to other types. This change affects all selected types. The procedure is the same as in the case of **Remove rights**.

Overwrite Rights

Using this menu item all rights of the **selected** types are transferred to the selected types in the dialog that is opened.

You have, for example assigned access rights to a type using the **Permissions**... menu item. These access rights also apply to other types. By clicking on **Rights/Overwrite rights** the dialog opens, where you can transfer access rights to other types.

2.5.3.2 Defining Access Rights

Access Rights defined for a Plantype

Table 9: Access Rights for Plantype

S.No.	Access Rights	Description
1	No access	The user does not have access to the object
2	Read	The user can display the object (is often called management right)
3	Change	The user can edit the object and, in contrast to the write access right, he can change its properties
4	Full Access:	The user has all rights (read, change, delete)

All of the access rights assignable to objects may be defined. The only difference is that the right to create objects of the respective type cannot be assigned.

Create: The right to create an object of this type.

2.5.4 Access Rights for Regular Types

2.5.4.1 Regular Types

DELMIA Process Engineer® has been extended by the new data class XDORegularType. The Regular Types are defined in the plantype set and access rights can be assigned to them similarly to assignment of rights to the plantypes of a plantypeset.

Eigene Rechte

In the properties of a type, the **Own Rights** function is used to assign access rights to these types.

In the Process Engineer the rights to plantypes are assigned in the following way:

If you open the context menu of the plantype, you will find two entries that refer to rights. *Please refer to the* Figure 36.

- Permissions and
- Permissions**…:**

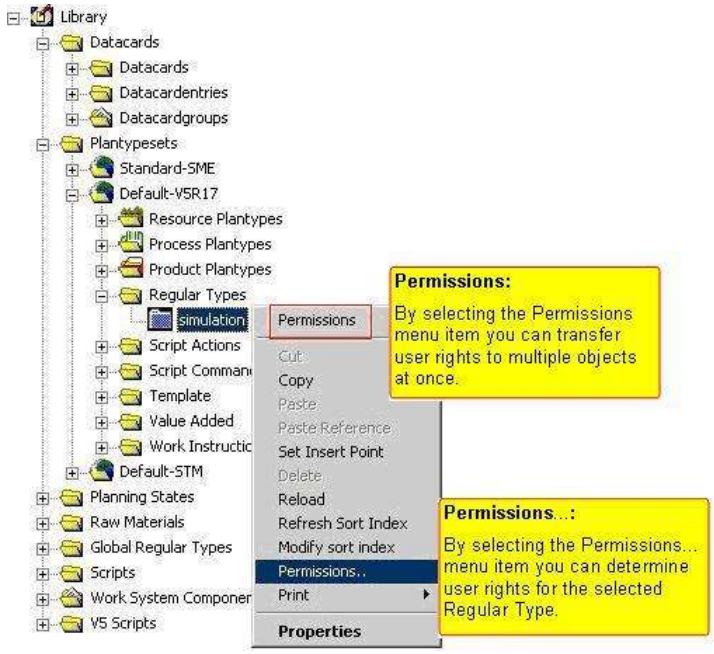


Figure 36: Definition of Permissions for Regular Types

2.5.4.2 Manage Regular Types in plantypeset of sytemlibrary

1) Open systemlibrary and select the plantypeset in which you want to log on Regular Types

2) In context menu select **Manage Regular Types**

Figure 37: Manage Regular Types in Plantype Set of Systemlibary

- Diaolog „Created And Not Created Regular Types“ will be opened

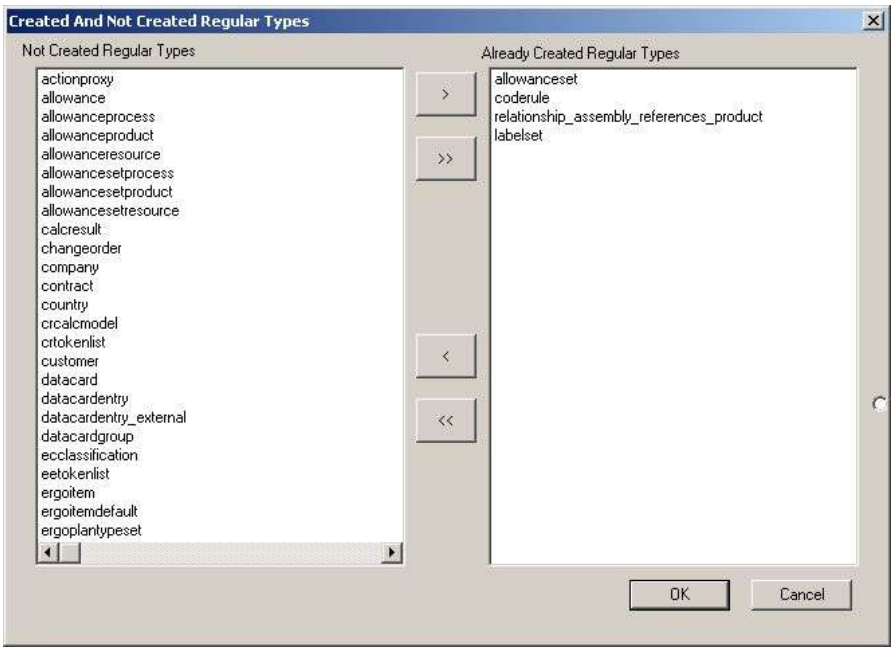


Figure 38: Dialog “Created And Not Created Regular Types“ in planetypeset

- Left side of dialog “Created And Not Created Regular Types“ shows all types which can be assigned with access rights.
- Ride side of dialog “Created And Not Created Regular Types“ shows all types which are already assigned to directory Global Regular Types.

With a button with simple arrow you can move individual types into the other relative list; with a button with double arrow you can move the whole list.

- If you leave the dialog with **OK**, all Regular Types on the right side of this digalog in directory Regular Types are created. You will find in all projects in which the plantypeset is used the same Regular Type. A requirement of access rights should take place at Regular Types in project. Access rights, which are assigned to Regular Types of Systemlibrary, are transfered only on new created projects.

2.5.5 Assigning Access Rights to Individual Regluar Types

2.5.5.1 Access Rights Menu Item

Using the **Access rights** menu item, you can assign access rights to a selected object.

1) In the context menu of a type, click access rights.

- The **Data Object Permissions** window opens, in which you can assign the access rights for this object.

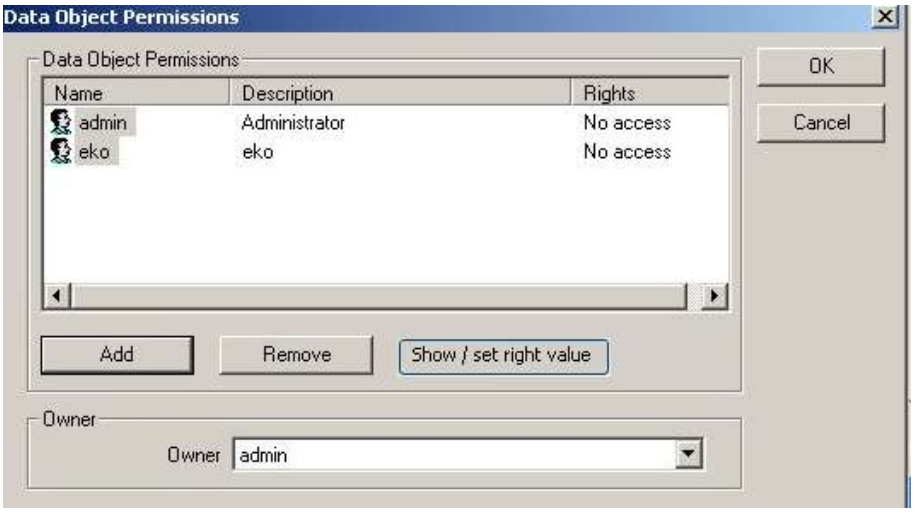


Figure 39: Dialog Rights – Data Types

The assignment of users is identical for Regular Types and data objects. The procedure is therefore described in section: *Assigning access rights to objects;* Assigning Access Rights to Individual Objects

2.5.6 Passing on Rights to other Regular Types

2.5.6.1 Permissions Menu Item

Using this menu item, the rights of a selected Regular Type are passed on to other Regular Types (of the same plantype set).

There are three possibilities for defition or removal of rights of other plantypes:

Removing Rights

This menu item allows to remove user rights from several types at the same time. Proceed as follows:

1) Select a Regular Type and open the option **Rights / Removing rights** from the context menu.

2) In the **Data Object Permissions** dialog you can specify the user or group from which specific permissions are to be removed. To do so, add the user(s)/group(s) to the empty field in the dialog using the **Add** button with **Access type** you can define the access rights to be removed. Upon each call-up of the dialog, the display is empty. Close the dialog by clicking *OK*.

3) A dialog opens (Figure 40) in which you can select the plantypes in which the previously selected right is to be removed. In every entry that is selected (highlighted in gray), the access rights are removed. If rights are

removed that had not been assigned to this type, nothing will happen. How to select?

- If you wish to select all entries, you only need to move over all entries while keeping the mouse button pressed.
- If you select individual entries or a group of entries use the mouse button and the Ctrl or the Shift button, respectively, as known from Windows Explorer.

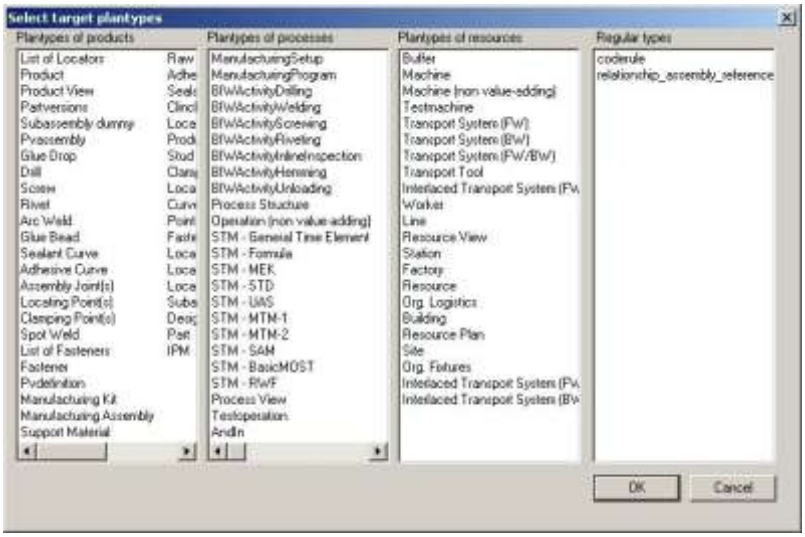


Figure 40: Dialog for Selection of one or Several Regular Types

Adding Rights

This menu item allows to add access rights to other plantypes. The change applies to all selected types. The procedure is identical with that for **Removing rights**.

Overwriting Rights

This menu item confers all rights of the **selected** type on all types selected in a dialog that opens.

You may, for instance have assinged rights to a type using the **Access rights**... menu item. These access rights also apply to other types. Selecting **Rights** / **Overwriting rights** will open a dialog (Figure 40) in which you can confer access rights on other types.

2.5.6.2 Defining Access Rights

Access Rights defined for a Plantype

S.No	Access Rights	Decsription
1	No access	The user has no access to the object.
2	Read:	The user can display the object (often referred to as the “management right”)
3	Change	The user can edit the object and change its properties
4	Full access	The user has all rights (read, change, create, delete).
5	User-specific:	Section “Defining own Access Rights” explains how to define user-specific access rights.

All of the access rights assignable to objects may be defined. The only difference is that the right to create objects of the respective type cannot be assigned.

Create: The right to create an object of this type.

2.6 Assigning Access Rights to Objects

To specifically assign rights to certain objects right-click the corresponding object and select by left-clicking the **Permissions…** menu item.

If you open the context menu of the node, you will find two entries that refer to rights. *Please refer to the* Figure 41.

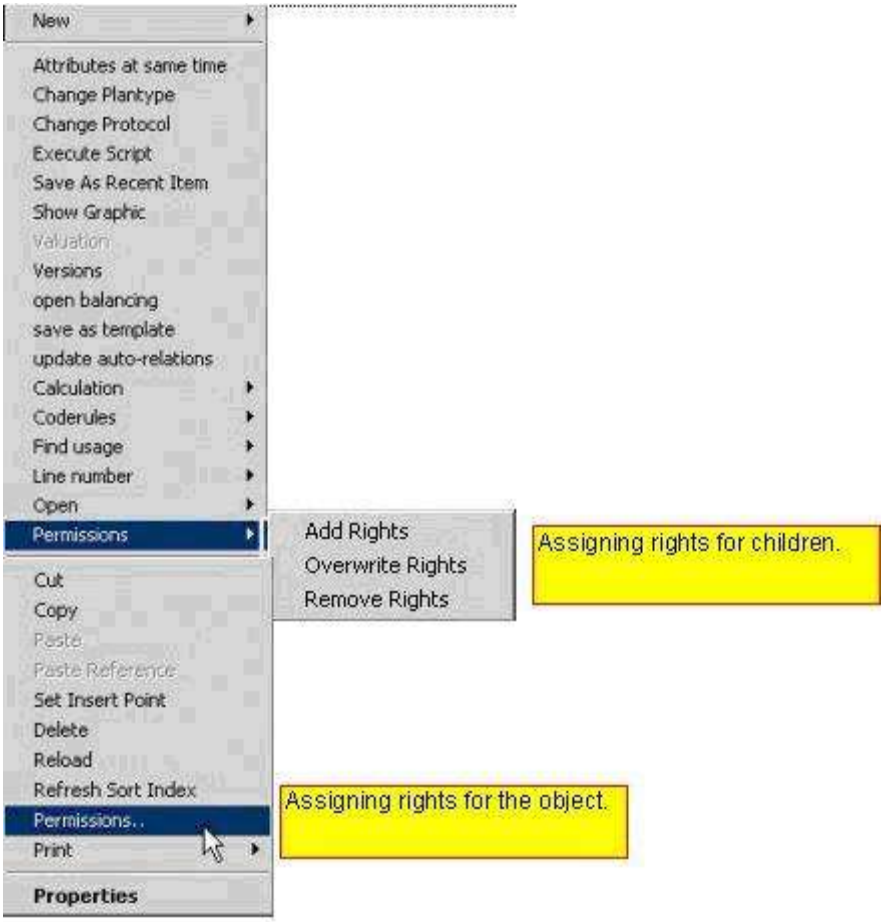


Figure 41: Assigning Rights

2.6.1 Assigning Access Rights to Individual Objects

Permissions... menu item
Using the **Permissions...** menu item you can assign access rights to the selected object.

1) Click **Permissions** in the context menu of an object.

- The **Data Object Permissions** window opens, where you can assign user rights to this object.

If you do not have a “user management” function right you can only read access rights, but you cannot change them.

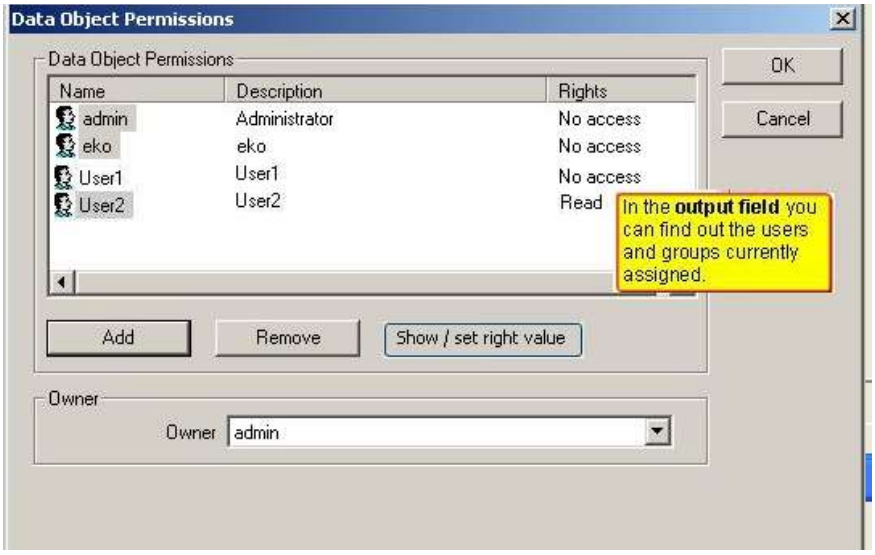


Figure 42: Data Object Permissions Dialog

Add and Remove Buttons

Click **Add** to add a new user or a new group from the **User selection** or click "**Remove**" to delete a current assignment.

Figure 43: User Selection for a Data Object

Button Change Rights

This button is active only after a group or user has been selected. You can change the access rights of the selected entries in the "Access Rights" dialog .

Category Owner

If user A has created an object himself, he is the object **owner**. For user A all rights to this object are the same as for all other objects of this type. As owner or creator of an object there are no additional rights assigned with regard to this object; the owner right is for information purposes only and can be changed by the administrator at any time.

Determining or Changing the Type of Access of a User (Group)

To determine the type of access of a user (group) open the context menu of the same object again and enable the **Right value** entry. In the output field of this window you can see the existing user assignment.

Figure 44: User Assignment

To find out the current access rights (type of access) of a user, mark the entry.

To change access rights proceed as follows:

2) Mark the user

3) Click Button **Right value**

4) Determine the new type of access. *Please refer to the* Figure 45.

Access Rights defined for an Object

Table 10: Access Rights Description

S.No	Access Rights	Description
1	No access	The user does not have access to the object
2	Read and execute	The user can display the object and its properties (is often called management right)
3	Write	The user can edit the object
4	Change:	The user can edit the object and, in contrast to the write access right, he can change and delete its properties.
5	Full Access	The user has all rights (read, change, delete)

User Specified: *Please refer to the* Defining own Access Rights.

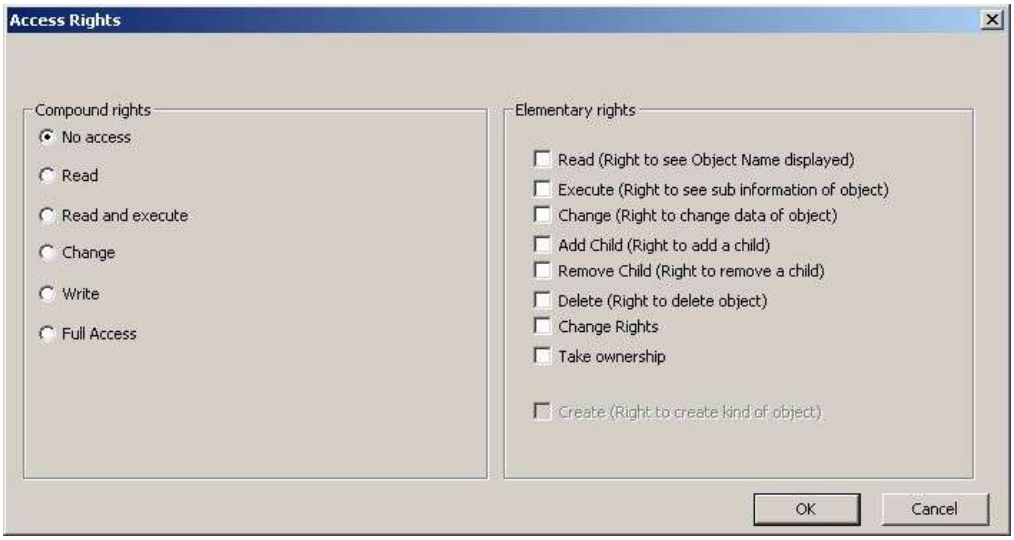


Figure 45: The User Specified Type of Access for Object Rights

2.6.2 Passing on Rights to Children

Caution

This function can be deactivated as of Version R12.

In order to prevent copying rights to children you must make an entry in the registration editor (master and all slave servers).

5) Under
HKEY_LOKAL_MACHINE \ SOFTWARE \ DELMIA \ IPDSERVER
you can generate a new character sequence with the name:
RightsToCopyByNew.
You can enter 0 or 1 as the value.

- If **value = 0:** the rights are not **NOT** copied to the child.
- If **value = 1:** the rights are copied to the child.
  The access rights of parent nodes are automatically transferred to their children.

The existing rights are copied only if a new child object is created for this object.

Note

This applies only to new child objects: *Existing access rights to the object (only Ergo Components, no projects) are automatically transferred to the child if you create a new child for this object in the corresponding structure. In order to check the rights to an object, call up the menu item Access Rights.*

Example

In the example, another object (child) is added to the **Resource rights** in the structure. Please refer to the Figure 47. **User 1** has the right to makes changes to the object Resource rights. If a new child is created for this resource, the rights of **User 1** (Please refer to the Figure 46) are automatically transferred to this child. Of course, the rights of Admin, DRB, and Guest are also transferred.

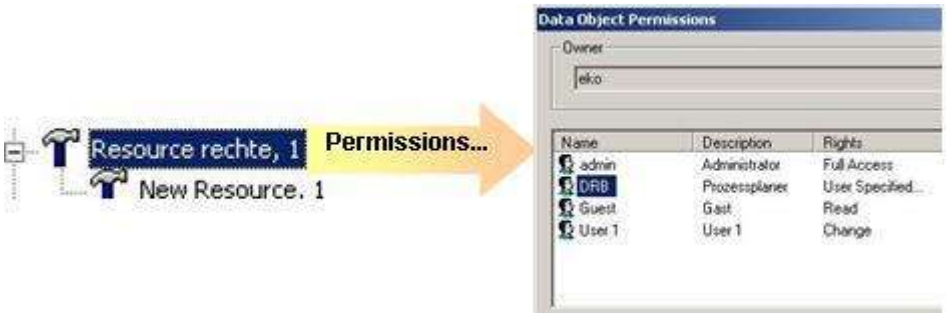


Figure 46: Adding a New Object to the Resource

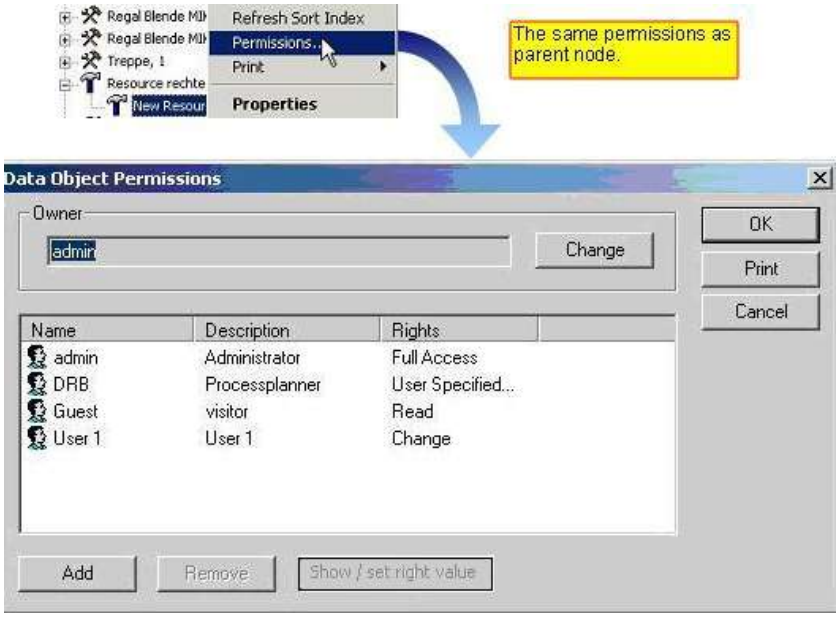


Figure 47: Data Type Permissions Dialog for a New Resource

2.6.3 Permissions Menu Item

Using this menu item the corresponding structure (children) inherits rights of a selected hierarchical level. You can use this function on every hierarchical level of a project and you can individually determine the rights for a user on every hierarchical level.

In contrast to the assignment of rights in the case of plantypes, the assignement of rights to children in the case of objects is actually only possible to their own children.

Note

Only use the rights function if a structure available for the selected hierarchical level.

You have three possibilities to determine the rights of children: *Please refer to the* Figure 41

- Remove Rights
- Add Rights
- Overwrite Rights

Remove Rights

Using this menu item you can remove previously assigned user rights for a structure. This change affects all children of the selected hierarchical level to which the user has been assigned rights (not to WSCs).

Add Rights
Using this menu item you can add user rights that a user has for a structure. This change affects all children (not to WSCs) of the selected hierarchical level to which the user has rights..

Overwrite Rights
Using this menu item all rights of the existing user are transferred to the selected structure to its children, even if an individual user previously did not have any rights to certain children of the structure.

Example

Example

A selected structure on the second hierarchical level has five additional equal hierarchical levels with corresponding structures (children of the corresponding structure).

A specific user only has, for example, a read right on two of these equal hierarchical levels. If you now execute the **Overwrite Rights** function on the highest hierarchical level of the selected structure, this particular user is assigned the read right for all children of the entire structure, thus also in the three additional hierarchical levels. In the same way all existing users would get, corresponding to the definition of their rights, rights to all children of the entire structure.

Caution

*Rights assigned on the children level are overwritten. If such a user is assigned full access to the parent node only, but no access to the child node, the user as well as all other users and groups, who are assigned rights to the parent node, are assigned full access to the children node after executing the **Overwrite Rights** function.*

2.6.3.1 Changed View for Nodes

The view of parent nodes with children changes if children cannot be displayed because of missing access rights.

If you assign **user 2** read rights to **process plan 1** and **user 2** has no access to **process plan 2**, in the Process View only **process plan 1** is displayed to **user 2.** If additional process plans are created in the Process View to which the user, however, has no access right, the process symbol in the Process View is marked with an exclamation mark. In the Process View only process plans are displayed to which the user has at least read rights (*Please rrefer to the* PPR Navigator Manual for more detailed information).

2.7 Copying Access Rights in the Project Plantype Set

Access rights that were assigned to random individual plantypes in the plantype set of a project can be transferred to other projects with the same plantype set. Access rights to plantypes are assigned to certain users who, according to assigned access rights, should have access to the respective plantypes or, for example, should be permitted to read them.

A plantype set consists of the three plantypes **Resources, processes** and **products**, to which individual plantypes are assigned in a hierarchical fashion.

As in the **Resource view**

- The plantypes resource view, station and machines
- Or in the case of the Process plantype, the plantypes process view, work plan and cycle.

Example

Example of a PlanTypeSet

Figure 48: Example – Overview of Plantype set Standard PRO

2.7.1 Copying Access Rights

The access rights for plantypes of a project plantype set can be copied using the context function **Copy Rights To Another PTS** and can only be copied in projects with the same plantype set.

For example, you have assigned access rights for certain users in the plantype set of a project for the plantypes Resources, Process and Product view, such as read rights. Now you want to copy these access rights to another project with the same plantype set; for example, say you have created a new project and the same users should again have the same access rights to it.

1) You therefore select the plantype set in the initial project (project 'Temperature Sensor AF20' in the example) and open the context menu.

2) Select **Copy Rights to Another PTS.**

3) In the **Copy rights to PTS** dialog determine for which projects the access rights are to be copied.

Figure 49: Open the Context Function for Copying Access Rights

In the **Copy rights to PTS** dialog you can determine for which project the rights should be overwritten. All projects with the same master PlanTypeSet are displayed in the dialog, which are available for selection.

In the example the right to read is to be copied for the new project '*Project A'* to the three views, Resource, Process, and Product views.

Projects for which the rights should be overwritten are shown in the right display window (selected projects). Two buttons are provided for this:

4) If you want to show all projects at once in the right display window, you do not need to select any project, but simply click on the button with the double arrow. Individual projects are shown in the right display window using the button with the single arrow; to do this you have to select the project first (left display window).

5) Projects can also be removed from this display window in the same way by using the two buttons with the arrows pointing in opposite directions.

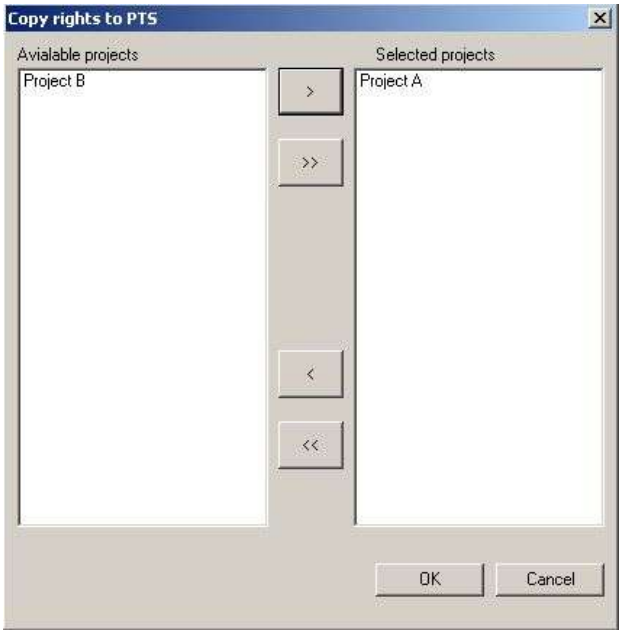


Figure 50: Assign Projects Dialog

6) Confirm the entries by clicking **OK**, and the rights will be transferred for the selected projects.

2.7.1.1 Executing Controls

The copied access rights have been transferred to the new project.

You can execute a simple control:

1) Open the plantype set in the new project and select Resource view, for example, under the plantype Resources.

2) Open the context menu and select **Access rights**.

3) The **Rights – data** dialog shows the users with the copied access rights. You can execute this control for each plantype for which access rights are copied.

PlanTypeSets are usually created and administered in the system library. Using the context function **Copy Rights To Slave PTS**, you can again overwrite the access rights assigned for the project for each plantype set in the system library.

Please read the chapter entitled **Copying rights of a plantype set** in the System Library Manual.

Figure 51: Run a Check for Copied Rights

Matrix of Rights

Table 11: Matrix of Rights

Rights	Rights								
	Read	Execute	Change	Add child	Create	Delete child	Delete object	Change rights	Change owner
Display object	x	x							
Change attribute	x	x	x						
Object new	x	x	x		x				
Delete object	x	x					x		
Change rights	x	x						x	x
Rights dialog function rights									
No access									
Execute		x							
Rights dialog object rights									
No access									
Read	x								
Change	x	x	x	x		x			
Write	x	x	x	x		x	x		
Full Access	x	x	x	x		x	x	x	x
Rights	**Read**	**Execute**	**Change**	**Add child**	**Create**	**Delete child**	**Delete object**	**Change rights**	**Change owner**
Rights dialog Content of rights - selection									
No access									
Read	x								
Change	x	x	x	x		x			
Write	x	x	x	x	x	x	x		

Full Access	x	x	x	x	x	x	x	x	x

2.7.2 Actions and the Necessary Rights (Specific)

Table 12: The Matrix of Rights II

Action	Rights									
		Read	Execute	Change	Add child	Create	Remove child	Delete object	Change rights	Change owner
Creating an ErgoComponent										
Under a project	- plantype set project - project - ergocomp. plantype	x x x			x	x				
Under another ErgoComponent	- **plantype set project** - ergocomp. parent - ergocomp. plantype	x x x		x	x	x				
In the Project Library	- **plantype set project** - ergocomp. plantype	x x		x	x	x				
Deleting an ErgoComponent										
Under a project	- plantype set project - ergocomp. - ergocomp using the object to be deleted (Relation, Stüli)	x x x					x x	x		
In the Project Library	- plantype set project - ergocomp. - ergocomp using the object to be deleted (Relation, Stüli)	x x x					x x	x		
Bills of materials entries										
Create	- ergocomp. parent - ergocomp. child	x x			x					

Action	Rights									
		Read	Execute	Change	Add child	Create	Remove child	Delete object	Change rights	Change owner
Delete	- ergocomp. parent	x					x			
Linked objects										
Create a link	- Target object - Actual object	x x			x x					
Delete a link	- Target object - Actual object	x x					x x			
Create a project	- Library Plantypesets (template)	x		x		x				
Start configuration manager	- **Function right** "configurationtool"		x							
Conversion tool										
Start conversion tool	- **Function right** "epdbupdater"		x							
Convert project	- Library PlanTypeSet (template) - For all system items conFigure types included in the project	x x		x x		x x				
Settings dialog										
	Function right: Change settings/Global data		x							
	Function right: Change settings/Machine data		x							
	Function right: Change settings/User data		x							
Printing										
	Function right: Printing/Create forms		x							
	Function right: Printing/Edit		x							

Action	Rights									
		Read	Execute	Change	Add child	Create	Remove child	Delete object	Change rights	Change owner
	forms									

Note

Function rights: Function rights are assigned by the user management

2.7.3 Creating Rights

For a new project access rights have to be defined and assigned to the users. Rights assigned once in a project can be revised at any time. In the previous sections it has been explained how you can create function rights for users and groups and how you can assign plantype sets, objects and types.

It has proved helpful to take function rights as an example when creating groups or when structuring group rights. This, however, is not mandatory.

Another possibility is to create groups according to departments and to assign different rights to these groups. The more differentiated the structure is set up the easier it is to assign the individual users.

This section shows on the one hand how you can assign access rights to a new project and on the other hand how you can redefine existing access rights in a project.

What needs to be observed in the case of new projects?

- The plantype set of the General Library is assigned at least **read rights**.
- The plantype set is assigned at least **read rights.**
- Create a new project and assign user and group rights to **project nodes**.

If you assign the function permission create project, you must also assign complete access or write permissions to one or more plantype sets.

Example

This is illustrated using an example:

Initial Situation
A new group "**User Admin**" is created.

Table 13: Group User Admin

Description	Membership	Rights / Function Rights
Group UserAdmin		**All** function rights: **Execute**
User 1	Member in group UserAdmin	Not specified
User 2	Member in group UserAdmin	In the case of user management No access right Otherwise: Not specified

First Opening

- **User 1** cannot open projects and cannot create new projects.
- **User 2** cannot open projects and cannot create new projects.

Now read rights are assigned to the project node

Group **UserAdmin:** full access:

User 1: read right

User 2: read right

Second Opening

- **User 1** can open and edit the project and the user management.
- **User 2** can open the project, but **cannot** open the user management.
- **User 1** and **user 2** can only read the project.

Thus it appears that:

- **Rights are inherited** (for example, the UserAdmin group has had the right to open and to edit the user management; user 1 + 2 have inherited the right due to their group membership.)
- **Superordinated rights can be overwritten by directly assigning rights** (user 2 had no access right to the user management.) Although the group right for the project was set to *full access*, both users could only read the project.
- **For guests or groups with guest status (only read right, otherwise no further rights)** it is sufficient to assign read rights to a project node. This group does not need access rights to the plantype set.

2.8 Special Note on Scripts

Please refer to the Scripting Manual for details concerning creation and use of scripts.

2.8.1 Permissions in Scripting

The user is given different rights for executing a script with the **Run As Owner** function.

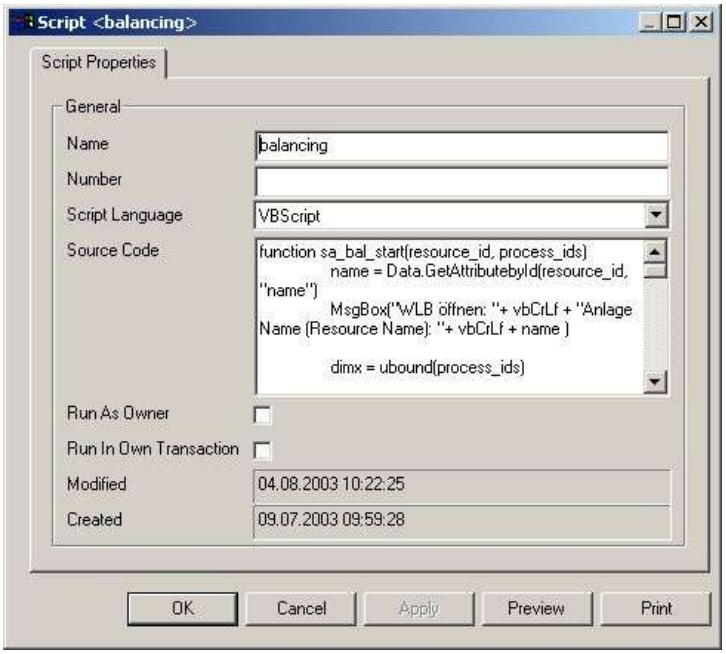


Figure 52: Run As Owner

2.8.1.1 Executing a Script as the Script Owner

With the Run As Owner function, you can now start a script independently of the execution type as if the script owner were the present user. The following rights are to be granted:

- The right to create, write, and change scripts.
- The right to execute interactive scripts.

The script writer is in possession of administrator rights; these rights are transferred to the script executor by the Run As Owner function.

- Activate the Run As Owner function in the script dialog.

Note

The introduction of the function Run As Owner brings on additional tasks for the administrator. For this reason, administrators are recommended to create a separate group for users who are entitled to write and execute interactive scripts.

2.8.1.2 Interactive Execution of Scripts

The interactive execution of scripts can be limited by the (script) administrator as follows:

Table 14: Interactive Execution of Scripts

Function	Required Access Right
Display scripts in dialog “Execute script”	Right to “execute” script object
Display scripts in context menu of an object	Right to “execute” script actions and script objects
Display VBA macros in the context menu of an object	Right to “execute” script actions

2.8.1.3 Function Rights for Scripts and VBA Macros

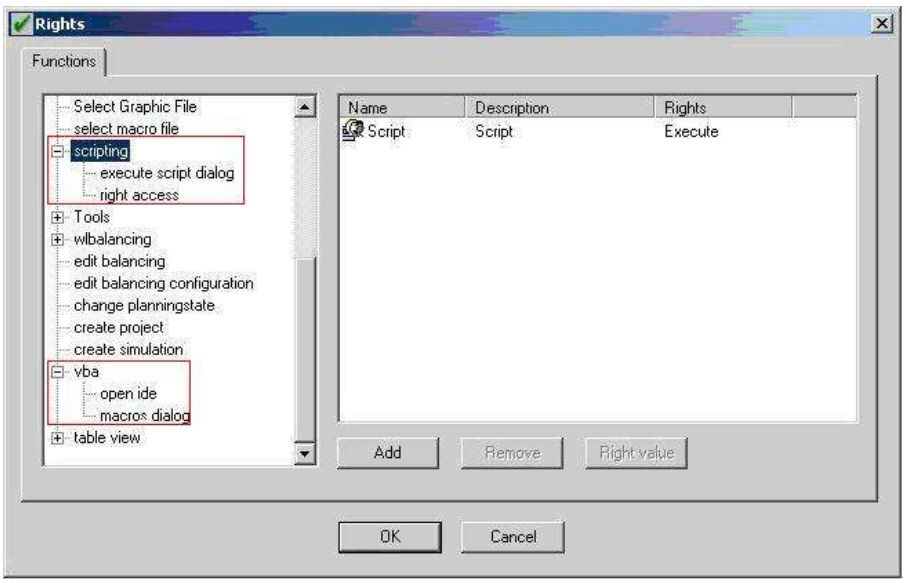


Figure 53: Function Rights

In the following table the function rights are described:

Table 15: Function Rights Description

Function Right	Description	Comment
Scripting Execute script dialog	Grants the right to execute scripts via a dialog.	This allows to deactivate the context menu “Execute script” for “normal” users. Opening the dialog and selection of the correct script requires knowledge about which scripts can be applied to which nodes. The (script) administrator should nonetheless have the possibility to execute scripts quickly, without having to generate (pseudo) script actions before.
Scripting Right Access	Grants access to the database for the access rights. A script can then read from the database for the access rights and write to it.	Additionally the right to *Change rights* is required for the object and / or plan-type level.
VBA Macros dialog	Grants the right to display the default VBA macro dialog.	Similar to “Execute script dialog”, however, for VBA macros.
VBA Open IDE	Grants the right to open the VBA IDE and to edit a VBA project.	

3. User Access Rights

User Access Rights for Pages, Groups and Attributes

In user manual Administration you have already learnt in description of properties for pages, groups and attributes that starting from Version DPE 5.17 you can define own user rights for these display elements. Description of pages, groups and attributes can be pre-defined for any individual user.

Caution

Precondition for rights on attributes, pages or groups to being considered correctly is that the option "OwnRights" on type "proxycfgelement" is set to Yes.

3.1 Procedure

The procedure should be displayed on the basis of an example.

To display pages, groups and attributes user specifically proceed in following way:

1) Select pages, groups or attributes from those you want to assign access rights and set the option **Own rights** on **Yes**.

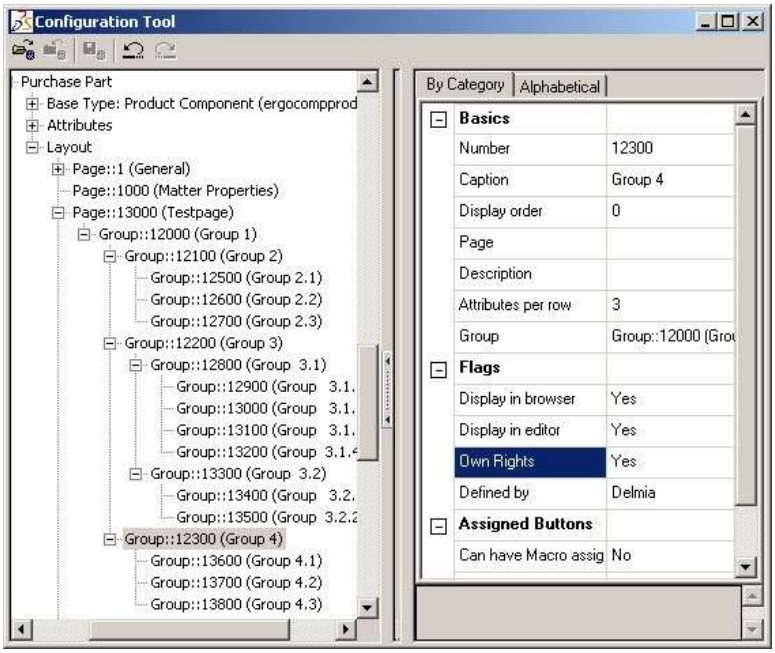


Figure 54: Coonfig Tool

- For this reason in context menu of relative pages, groups or attributes the function **Permissions** is activated.

2) Click **Permissions** in context menu.

Figure 55: Context Menu

- Dialog **Rights – Data objects** opens in which you can select the user to who you want to assign the access rights.

Figure 56: Data Objects Dialog

3) With the button **Add** you select users or groups to who you want to assign access rights.

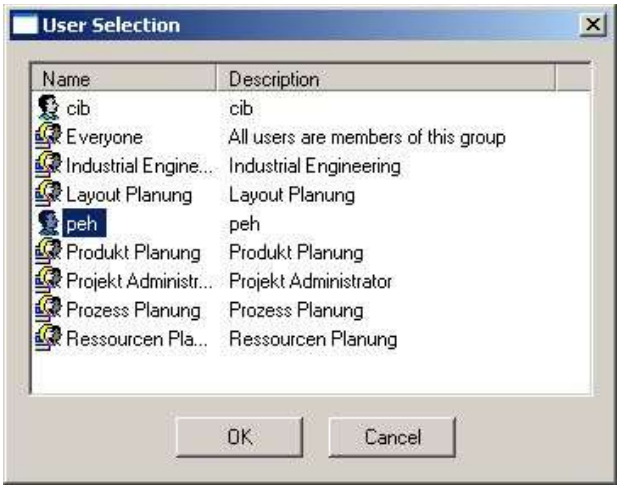


Figure 57: User Selection

Procedure with assigning of rights:

4) Select a function.

5) Add with button **Add** groups and users to who you want to assign special rights at the selected function.

6) Select on or more of the evenly added groups or users.

7) With the button **Access Right**s you assign access rights to the preceding selection.
With functions rights three access rights are available for you:

- Object cannot be shown = No Access
- The right to display the object = Read
- Full Access = Write

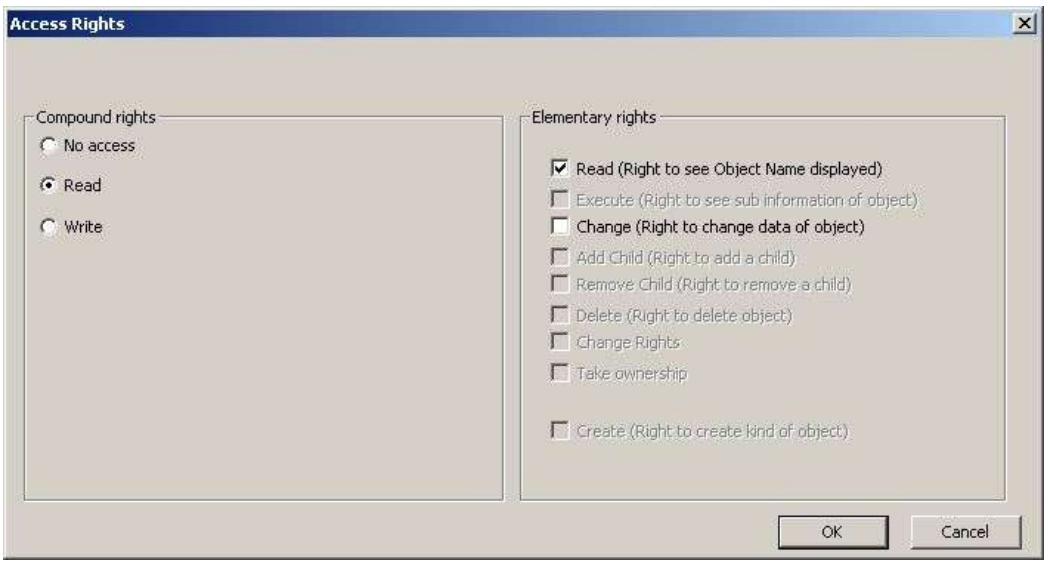


Figure 58: Access Rights

8) After the selection click button  and specify the access rights.

In order to check the evenly built configuration you have two possibilities:

- Preview in middle part of configuration manager.
- You sign in as evenly configured user in DELMIA Process Engineer® and check in PPR-Navigator result of the configuration.

3.1.1 Preview for User Specific Configuration

To activate a preview open context menu with a right click on the middle part of configuration manager.

Figure 59: Preview Open Context Menu

Three entries are available:

- Display all pages (also the inherited)
- Display only the pages which are indicated as **Display Editor**
- Preview for user specific configuration

In order to receive a preview of user specific configuration click **Preview for User.**

- Dialog **Select Single User** opens in which you select the user for who you create the preview.

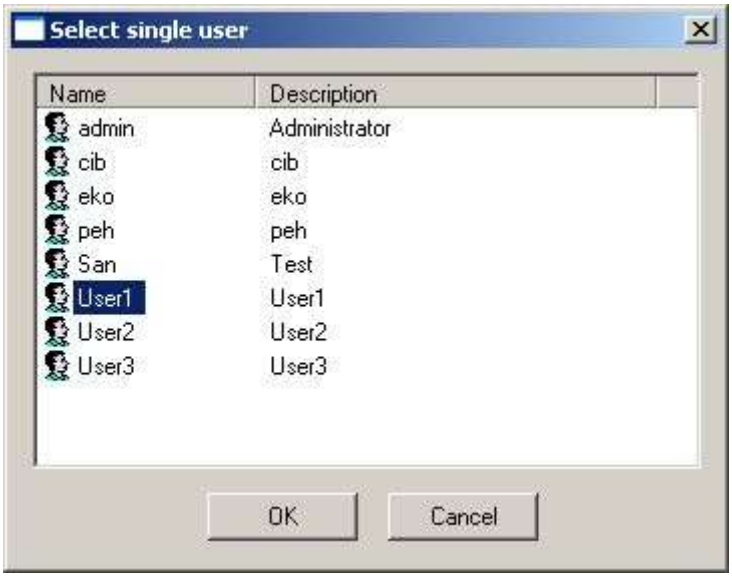


Figure 60: Select Single User

What is to be considered?

If option Own Rights is activated on a type or plantype but afterwards no user is assigned this object is not shown.

Appendix

3.2 Function Permissions

Figure 61: Function Permissions

Table 16: Function Permissions Descriptions

Function Permissions	Description	Comments
useradm		
useradm/change password	You can change your location after logging in with this function permission (*Please refer to the* Security Manual).	You can change password with this function permission. This permission is for e.g. users with guest status - in order to prevent guest users from changing their passwords
useradm/run	This function permission allows you to call up the MultiUserManagement - module.	The module is used to view/edit users/groups.
useradm/edit user and groups	With this function permission you are allowed to create, delete, and edit user and group data. This function permission alone does not allow one to create, edit, or delete an administrator. Only administrators can create other administrators.	e. g. Properties, setting group affiliations, creating new users and groups, allocating function permissions. This function permission replaces the function permission: useradm/remove user, useradm/add user, useradm/ edit.
useradm/change location	With this function permission you can change your own residence after log on.	
Useradm/manage gobal regular types	This function permission allows you to manage global regular types.	
Configuration Tool	This function permission allows you to use the configuration tool.	
Epdbupdater	This function permission allows you to use the data converter.	Besides the Superuser, only users with the function permission “epdbupdater” may use the E4 data converter. If a normal user does not hold this permission, an error message will be displayed and the conversion is denied.
printing		
printing/create forms	This function permission allows you to create new print forms, printing of lists and graphics forms for objects.	The function is found under Tools / Print Forms / New object or New list or New graphic.
printing/edit forms	This function permission allows you to edit existing print forms, printing of lists and graphics forms for objects.	
printing/delete forms	This function permission allows you to delete existing print forms for objects.	The function is found under Tools / Print Forms / Delete object.
printing/create scriptvariables	This function permission allows you to create new script variables for print forms.	The function is found under Tools / Print Forms / Script variables.
printing/external data sources	This function permission allows you to prepare queries for printing.	The function is found under Tools / Print Forms / external data sources.
printing/object wizard	This function permission allows you to create a practically endless variety of reports on PPR-Navigator data	The function is found under Tools / Print Forms / Object Wizards.

Function Permissions	Description	Comments
	structures.	
copy project	This function permission allows you to copy projects.	Only for users that have this permission, the button “Copy project” in the “Open Project” dialog is activated.
change settings		
change settings/user data	This function permission allows you to edit the registry key HKEY_CURRENT_USER/DELMIA/Software/ergoplan.	The administration of non-object-specific permanent settings (Session Data) is done with Tools/Settings/Maintenance.
change settings/machine data	This function permission allows you to edit the registry key HKEY_LOCAL_MACHINE/DELMIA/Software/ergoplan.	
change settings/global data	This function permission allows you to edit global (applicable to all users) common database entries.	
change settings/user db data	This function permission allows you to edit user-specific database entries.	
Edit Time Analysis	This function permission allows you to edit the time analysis.	If you do not hold this permission, an error message will appear as soon as you try to edit the time analysis.
delete global regdbdata	This function permission allows you to delete global common database entries.	
Versions_allows_delete	For administrative functions, this function permission can be used to delete versions that are set to “indelible” in the planning status.	The planning status allows to set that versions cannot be deleted in this planning status.
Edit Graphic	This function permission allows you to edit the graphics.	
Show Graphic	This function permission allows you to display the graphics.	Show graphic is available for instance in the context menu of the product and resource structure.
Edit External Graphic	This function permission allows you to edit the graphics externally	e.g. using CATIA
Select Graphic File	This function permission allows you to assign an existing graphic to a WSC object.	
Select Macro File	This function permission allows you to assign an ISEGRIM macro to a WSC object.	
Automatic Line Balancing	This function permission allows you to activate the **Open** and **Save** function rights for ALB. If the **Open** and **Save** functions are enabled and the automatic line balancing function is deactivated, then the **Open** and **Save** functions are disabled; it is not possible to open or save ALB.	

Function Permissions	Description	Comments
Open	This function permission allows you to open ALB in an activated state.	
Save	This function permission allows you to save in ALB.	If this function is deactivated, then the **Save** and **Save as** commands do not work in ALB.
scripting		
scripting/execute script dialog	Grants the right to execute scripts via a dialog.	This allows to deactivate the context menu “Execute script” for “normal” users. Opening the dialog and selection of the correct script requires knowledge about which scripts can be applied to which nodes. The (script) administrator should nonetheless have the possibility to execute scripts quickly, without having to generate (pseudo) script actions before.
scripting/right access	Grants access to the database for the access rights.	A script can then read from the database for the access rights and write to it. Additionally the right to Change rights is required for the object and / or plantype level.
scripting/execute external script	Grants the right to execute external script.	
tools		
tools/pprloader	DPE administration clients: pprloader.exe	
tools/ptimex	DPE administration clients: ptimex.exe	
edit balancing	This function permission allows you to edit the ALB Balancing.	
change planningstate	This function permission allows you to change the planning state of an object in the “Change planning state” dialog.	Version coding of objects
vba		
vba/open ide	Grants the right to open the VBA IDE and to edit a VBA project.	
vba/macros dialog	Grants the right to display the default VBA macro dialog.	Similar to “Execute script dialog”, however, for VBA macros.
WIbalancing		
wlbalancing/delete balancing	This function permission allows you to delete the balancing.	Objects may be created of balancing processes. If a balancing object is created, it can only be deleted by a user who has the respective function permission.
open configuration	This function permission allows you to open the wlb balancing configuration.	
first level	**Save**: This function permission allows you to save a level 1 workload balancing. **Open**: This function permission al-	

Function Permissions	Description	Comments
	lows you to open a level 1 workload balancing.1 **Set valid**: This function permission allows you to set a level 1 workload balancing as valid.	
second level	**Save**: This function permission allows you to save a level 2 workload balancing. **Open**: This function permission allows you to open a level 2 workload balancing.1 **Set valid**: This function permission allows you to set a level 2 workload balancing as valid.	
third level	**Save**: This function permission allows you to save a level 3 workload balancing. **Open**: This function permission allows you to open a level 3 workload balancing.1 **Set valid**: This function permission allows you to set a level 3 workload balancing as valid.	
edit balancing configuration	This function permission allows you to edit the ALB balancing configuration.	To allow proper performance of balancing, the respective data is set in the configuration of the balancing. Open the balancing configuration using the context menu of a project. The configuration will only be available if you hold this function permission.
table view		
table view/general access	With this function right, you can use the function table view/general access.	
table view/table view profiles	With this function right, you can create profiles for user groups on a plantype set.	
cleanup graphic directory	With this function right, you can use the function cleanup graphic directory.	Redundant files can be removed from this directory with this function. *Please refer to the* Administrator Manual.
number processes	Using this function right, you can number the processes in the process graph consecutively and display the numbering during the actual process. Assignment of numbering is done by attribute name or nameshort.	You can open the function with the right mouse button in the Process Graph.
versioning		

Function Permissions	Description	Comments
versioning/CheckOut without consistency checks	Use this function permission to check out or check out (deep) versions without consistency checks.	
versioning/Create without consistency checks	With this function permission you can create or create (deep) versions without consistency checks. This function can be found in the context menu when creating a version.	
template		
template/copy associated resources	This function permission becomes effective if one copies processes from one template to another. If one has this function permission, whether the associated resources should also be copied is queried upon copying.	
security overlay properties	This function permission allows you to edit the security dialog.	This function can be found in the menu Tools / Setting / Security Dialog.
regular project <- > mcm project	With this function permission you can make an MCM project out of a regular project and vice versa.	This function can be found in the menu Tools / Regular Project <--> MCM Project.
graphic		
graphic/create preview graphic	With this function permission you can create graphic files in the ...cgr format, which can be used in DPM-V5.	
Create global filter	With this function permission you can create a global filter.	
Create personal filter	With this function permission you can create a personal filter.	
Versionhistory_allow_delete	For administrative functions, this function permission can be used to delete versions that are set to “indelible” in the planning status.	The planning status allows to set that versions cannot be deleted in this planning status.
Acess finder global profiles	With this function permission you can save finder search profiles into global database instead of user database.	

List of Figures

List of Tables

Index