User Administration



Up to CoPlanner Version 9.1

FURTHER INFORMATION

COPLANNER SOFTWARE & CONSULTING GMBH

SCHUBERTSTRASSE 39, 8010 GRAZ

TEL.: +43 (0) 316 / 38 32 38

FAX: +43 (0) 316 / 38 32 38-17

EMAIL: OFFICE@COPLANNER.COM

CONTENT

Overview 3
Security Type 4
COP Security 4
NT Security 4
Login/Group settings 4
OLAP User 4
SSPI authentication 4
Security on Ribbons 5
Security on Dimensions 5
Security “Blocked Sets” 6

OVERVIEW

The user administration is split up into three areas in the tree:

- Overall (groups/users)
- User groups
- Users



Figure 1: User Administration

The icons in the toolbar have the following meanings:

Button	Action
	Saving the user administration
	Create new user/group
	Call up the wizard to take over group authorizations
	Delete the selected element

Mark a group or a user in the tree and use the button “Create New Element” . Allocate the user name you wish to use. Mark the empty area in the tree or the group/user nod. In doing so, you can create a new group.

Depending on what you have selected in the tree the corresponding setting option appears on the right side of the tree. The following display will appear if you choose the complete overview in the tree:



Figure 2: User Administration - Groups

The “Groups” tab contains detailed information on the groups.

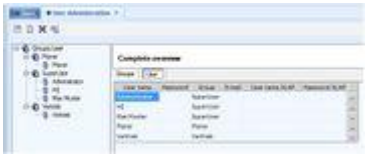


Figure 3: User Administration - Details area where you can make changes

Group selected in the tree

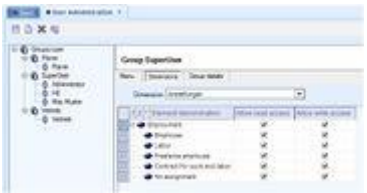


Figure 4: User Administration - Display of a selected group

Here you can make the settings for the menu authorization and the dimension authorization of the group selected in the tree. Group details offer a complete overview of the settings already made. If you wish to rename groups, you can do so within the tree by means of a right mouse click and the popup menu or by pressing the “F2” key.

User selected in the tree



Figure 5: Display of a user

Here you can make the settings for the user selected in the tree. If you wish to rename users, you can do so within the tree by means of a right mouse click and the popup menu or by pressing the “F2” key.

The settings are divided up into three areas:

SECURITY TYPE

COP SECURITY

The user is created in the CoPlanner system, i. e. the password is always allocated in the CoPlanner.

NT SECURITY

The user exists in the domain of your system. The password is the same as the one used for the Windows login. Optionally, you may also enter a user of a different domain / of another computer. In this case the user name must be entered as follows: <domain name>\<user name>. For example, “my company domain\H.Maier“. If you choose to proceed like this, you must also enter the entire path at the login. During the login the system then tries to register the user on this domain.

LOGIN/GROUP SETTINGS

If, as described with the Security Type, COP security is used, the password must be entered and confirmed. Optionally, an e-mail address may be entered as a piece of information. Each user must be allocated to a group since rights are awarded on a group and not on a user level. The group may be defined via combination list field or by means of drag & drop of the user in the tree.

OLAP USER

For the connection to the OLAP server an NT user may be entered. If no user has been entered, the account under which the CoPlanner Server was started, is used, i. e. all dimension elements will then be visible for the user in the OLAP browser and the CoPlanner client (in the case of an OLAP access). If an NT user with a corresponding awarding of authorizations is created in the domain, it should be entered here. As an option, you may also enter the <domain name>\<user name>.

SSPI AUTHENTICATION

It is possible for the CoPlanner client to register at the server with an integrated windows authentication (SSPI). The following steps are required for SSPI: The client can be switched to SSPI in the XML file coplanner.exe.config by means of< add key="Logon.ShowSSPI" value="OnlySSPI"/>.

Options for value:

NoSSPI	SSPI is not used.
OnlySSPI	Authentication is only possible via SSPI.
OptionalSSPI	Optionally, authentication is possible with SSPI.

If this authentication is used, the windows user who executes the CoPlanner client must only be able to register at the server on which the CoPlanner server is running. In this case it is not necessary to enter the user name/password. However, the user must exist as an NT user in the user administration (<domain name>\<user name>) and have the corresponding rights regarding the plan selected. Authentication is done through port 11000. Therefore, it must be ensured that both client and server are authorized to communicate via this port.

SECURITY ON RIBBONS

By means of this security, internal process logics can be displayed. Settings can be made via User Administration/Groups Administration/Menu Authorization. Here, individual roles are allocated or denied to ribbon buttons.

Hint Whether commands are available in the ribbon, web or tree is indicated directly at the menu item via the navigation designer!

On the “menu” tab you can determine which items of the menu shall be visible to the various user groups. Uncheck those menu items which you do not wish to be available for the various groups.

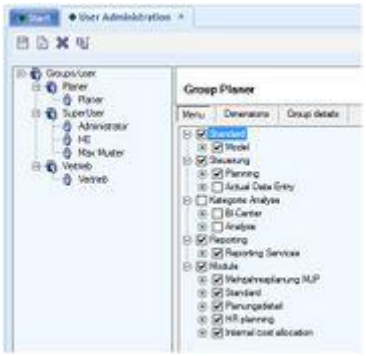


Figure 6: User Administration - Security on Ribbons

According to the above-referenced authorization a user of the “Planner” group may not open any dimensions.

SECURITY ON DIMENSIONS

By means of this security, internal areas of responsibility are secured (e. g. persons in charge of cost centers). Settings are possible through User Administration/Groups Administration/Dimension Authorizations. These authorizations do not apply to the dimensions themselves but to values in the tables which are booked regarding the dimension. Technically speaking, blocked sets are provided by the server dynamically with SecurityFlags: Writing denial: The dataset is allocated the integer value “1” in “COPSYS_LOCKED”. This value (1) is not saved. Reading denial: The dataset is removed from the target quantity.

Hint Aggregation values are always displayed WITHOUT security!

Example: Role “A” may not book sales (sales table) for the product “racing bicycles". Sales of the product “racing bicycle XT” may not be viewed.

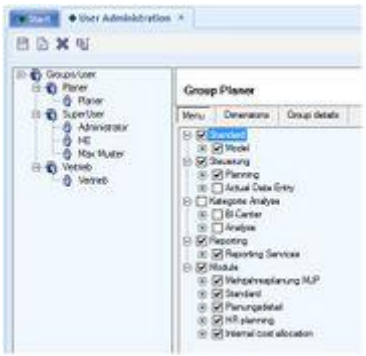


Figure 7: User Administration - Security regarding Dimensions

Use the “Dimensions” tab in order to determine writing and reading rights in the various dimensions. Select the desired dimension from the dimensions menu and uncheck all those elements which you do not want to be available to the user selected. You may choose between read-only authorization and an authorization for both reading and writing.

Hint Please note that if you wish to enable a writing or reading right for a sub-element, you must by all means also enable the elements on the level above. Otherwise, the element will not be displayed.



Figure 8: Security regarding dimensions, reading right

Based on the settings above, the user of the “Planner” group may only read the profit and loss account according to the type of expenditure format but may not make any changes.

Hint In order to be able to login as a newly created user, the program must be closed and then reopened.



Figure 9: User Administration - CoPlanner Login

SECURITY “BLOCKED SETS”

This security system is primarily intended for PowerUsers and system administrators. It can be used to secure the planning model. For this purpose, relational single datasets are protected from being deleted (= COPSYS_ID remains intact). Datasets may be changed. In the developer mode available through the context menu of the dataset, in dimension maintenance and in input masks (only line mode). In the field “COPSYS_LOCKED” of the dataset the integer value 2 is entered.