Table of Contents

System Versions

The program runs from SAP_BASIS Version 700, with and without Unicode. It has been developed in Version 700.

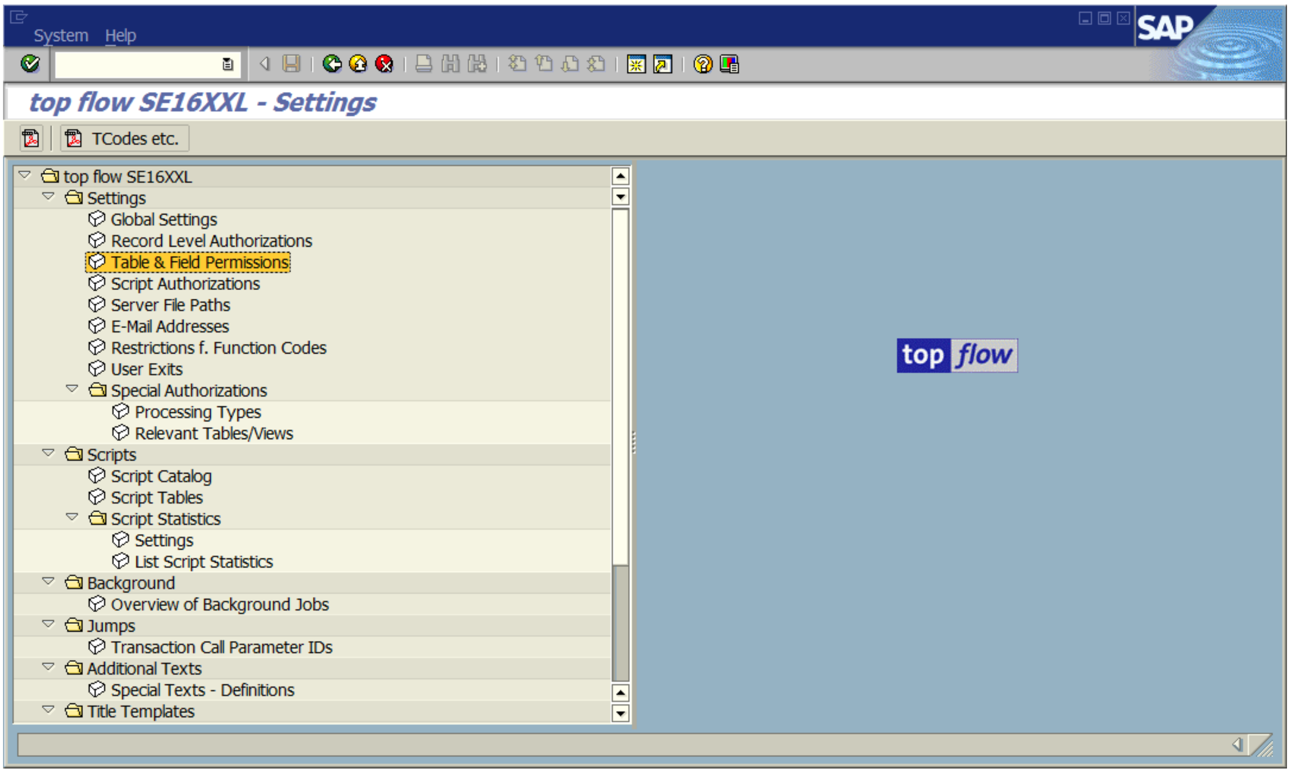
Distributed by top *flow* GmbH – D-88348 Bad Saulgau.

The information contained in the following pages is provided without warranty of any kind. It is subject to change without prior notice. Any data serve information purposes only.
Neither the author nor the distributor are liable for any errors or omissions of the documentation.

top *flow* SE16XXL Permissions

Using the **TableWizard Table & Field Permissions,** you may define which users can access which tables, and which fields for a given table. This makes the **top *flow*** SE16XXL interesting for the more security conscious companies as well.

The SE16XXL Table & Field Permissions are best reached by means of transaction **/TFTO/XXL_SETTINGS**:



The authorization to use the program is based on a set of SAP roles which provide the user with more or less administration rights.
These roles are actually empty. Only the assignment to the user is checked. This assignment can be carried out with the standard transaction **PFCG.**

Instead of the roles, authorization objects **/TFTO/XGLB** or **/TFTO/XCUS** may be assigned (refer to **Transaction Codes, Roles and Authorization Objects**).

In the following page a list of the involved roles will be given.

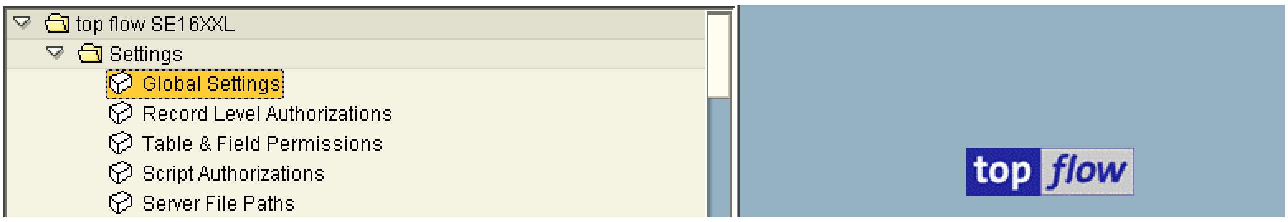
SAP Authorization Roles needed to use the program

SAP Authorization Role	Description
/TFTO/XXL_GLOB_MAINT	Global maintenance of all kinds of SE16XXL settings
/TFTO/XXL_CUSTOM_MAINT	Maintenance of all kind of Table & Field permissions
/TFTO/XXL_CUSTOM_MAINT_ROLES	Maintenance of access roles and their permissions
/TFTO/XXL_CUSTOM_MAINT_USERS	Maintenance of user permissions
/TFTO/XXL_CUSTOM_MAINT_ASSGN	Maintenance of access role assignments to users
/TFTO/XXL_GLOB_DISPL	Global display of all kinds of SE16XXL settings
/TFTO/XXL_CUSTOM_DISPL	Display of all kinds of Table & Field permissions

The first two roles give the user all necessary rights to maintain the permissions.
The following three give only partial rights and can be used to implement a “**four-eyes principle**”, i.e. the administration of permissions is carried out by more than one person, each person having limited administration rights.
The last two roles are just for viewing the permissions. Any kind of maintenance role automatically enables to display all permissions.

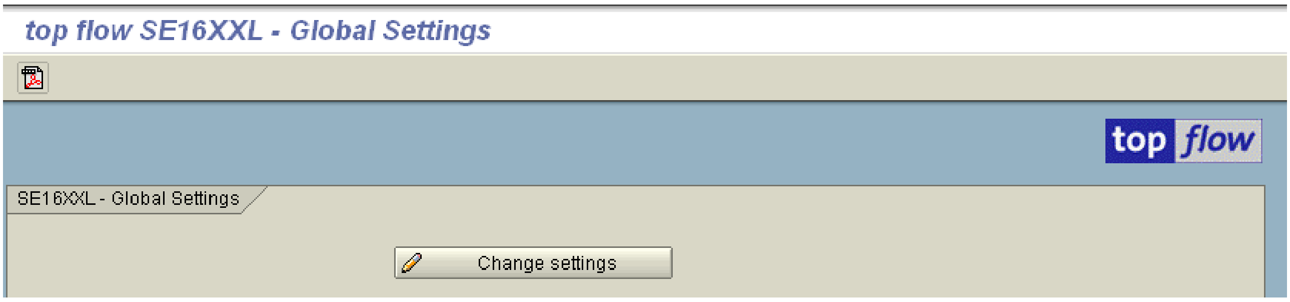
Global setting

The permission functionality is delivered in a deactivated state. It can be activated by calling transaction /TFTO/XXL_SETTINGS (global settings):



- top flow SE16XXL
  - Settings
    - Global Settings
    - Record Level Authorizations
    - Table & Field Permissions
    - Script Authorizations
    - Server File Paths

A double click on Global Settings will display the global settings:



top flow SE16XXL - Global Settings

SE16XXL - Global Settings

Change settings

…

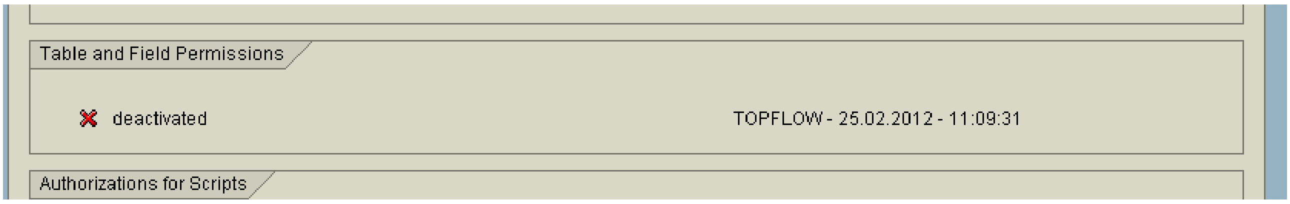


Table and Field Permissions

✗ deactivated TOPFLOW - 25.02.2012 - 11:09:31

Authorizations for Scripts

Press Change settings and then ✓ activate :

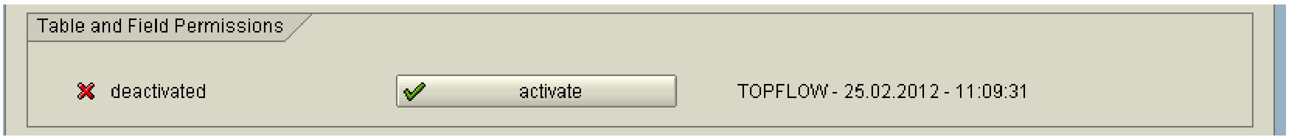


Table and Field Permissions

✗ deactivated ✓ activate TOPFLOW - 25.02.2012 - 11:09:31

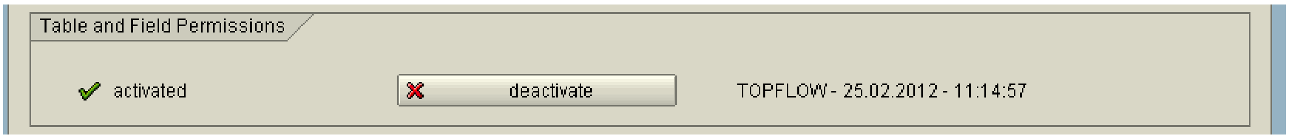


Table and Field Permissions

✓ activated ✗ deactivate TOPFLOW - 25.02.2012 - 11:14:57

Don’t forget to save the settings by pressing Save changes when you are finished.

The activation should be best performed when all permissions have been defined.

Permission Logic

Before describing the program itself, it makes sense to briefly discuss the underlying permission logic.

Originally, the permissions were completely independent of the SAP authorizations. But many companies, especially larger ones, have an integrated authorization concept in which the SE16XXL permissions in their original form did not quite fit.
For this reason, a new way of defining the permissions has been implemented, which allows to assign SE16XXL access roles to SAP authorization roles. Once the access roles have been defined using the present program, they can be assigned to users indirectly by means of the associated SAP roles, just as any other kind of SAP authorization.

The two permission logics, the original one and the new one associated with SAP roles, may be used concurrently, but this probably only makes sense in a transitional period during which the original logic is being phased out.

IMPORTANT: in the following documentation the Tables Wizard access roles will be called either “**access roles**” or just “**roles**” (elementary and complex), whereas the SAP authorization roles will be referred to as “**SAP roles**”.

Original Permission Logic

Tables and fields

You can define permissions at three levels:

1) Pseudo user "*****" (which means "all users");

2) Access roles, which act as abstract users; (these roles don't have anything to do with the standard SAP authorization roles)

3) Individual users.

Each level has two types of permissions, explicit and global (or generic):

- An **explicit** permission describes which fields of a particular database table are allowed to be accessed.

- A **global** permission specifies (either by **name** or by **authorization group**) a series of database tables that are allowed to be accessed.

When a user calls up the **top *flow*** SE16XXL for a particular database table, the following logic is applied:

1) Does the user have an explicit permission for this table?
If yes, the explicit permission is taken, and the user can access the allowed fields.
If not, the search goes on.

2) Does the user have a global permission which covers the current table?
If yes, all fields of the table are allowed.
If not, the search goes on (this is implied in the following steps).

3) If the user has no permission for the current table, the access roles assigned to the user are inspected. Each access role can have the same kind of permission as a user. Since the permissions of the access roles can possibly overlap, the best permission of all is taken. This means that if a given role only allows certain fields of the table, and another role allows all of them, the latter "wins".

4) If neither the user himself, nor his assigned access roles have any permission for the table, then the pseudo user "*" (all users) is taken into account. It also can have permissions like a user. If it has any for the current table, it is taken.

5) If none of the above criteria have been satisfied, the user is not allowed to access the table, and he gets the message "Sorry, you are not authorized".

This can be visualized by means of a table. The check begins with A – if the user has an explicit permission – and proceeds with B, C, D etc., until a definite result has been obtained.
If more than one role is assigned to the user, the ones that allow all fields are considered first. If no such roles exists, because each role only allows some of the fields, then all allowed fields are merged together to form the permission of the user.

Level	**Explicit Permission**	**Global Permission**
User	A	B
Roles of the user	C	D
* (all users)	E	F

To sum the logic up, you define at "all users" level those permissions which all users should have. Then, if you deem it necessary, you can define individual access roles with added permissions, to be assigned selectively to certain users. The permissions of the access roles either enhance or supersede those of "all users".
Finally you can give still more permissions to individual users, adding new permissions or superseding those of the assigned access roles and/or "all users".

Important: you only define which tables are allowed, not which are forbidden.
Forbidden are those that are not allowed.

Views

Views are not considered as separate entities. They inherit the permissions of the database tables from which they are derived.

Forbidden data elements

The above described logic shows how the allowed fields of a table are determined. This could already be sufficient.
But in order to add greater flexibility, permissions at data element level may also be defined. They are used to restrict the fields which can be accessed.
Of course only those fields that are associated to a data element.

Data element permissions are global permissions, stating by name which data elements are forbidden (or allowed). They are also defined at the three levels:

Pseudo user "*****" (all users);
Access roles;
Individual users.

Only the logic is a bit different here.

At the level "all users", the **<u>forbidden</u>** data elements are defined.

At the other two levels, these forbidden elements can be **<u>re-allowed</u>**, either at role or user level (or both). So you can globally define that certain data elements are forbidden, and then allow them just for a limited number of users.

To return to our permission logic, once the allowed fields have been determined, their data elements are compared with the forbidden ones, and if such are found, the associated fields are also considered as "not allowed".

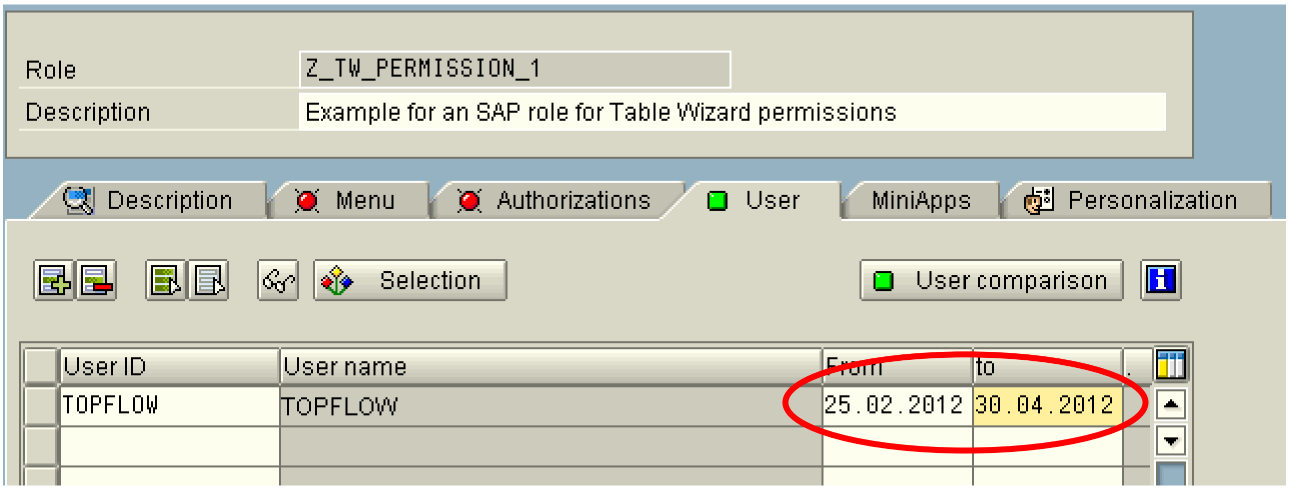
New Permission Logic

In this case, only access roles with their permissions – explicit and/or global – are defined. To each access role an SAP role is associated as an attribute. When the SAP role is assigned by means of transaction PFCG (or SU01) to a user, all access roles associated with the SAP role are indirectly assigned to the user.

The pseudo user "*" (all users) is not strictly necessary in this situation, unless you wish to define "forbidden data elements".

Temporary permissions

The indirect assignment of access roles through an SAP role enables to restrict the assignment to a specific time period, because this is a standard feature of transaction **PFCG**:



Role	Z_TW_PERMISSION_1
Description	Example for an SAP role for Table Wizard permissions

User ID	User name	From	to
TOPFLOW	TOPFLOW	25.02.2012	30.04.2012

Four-eyes principle

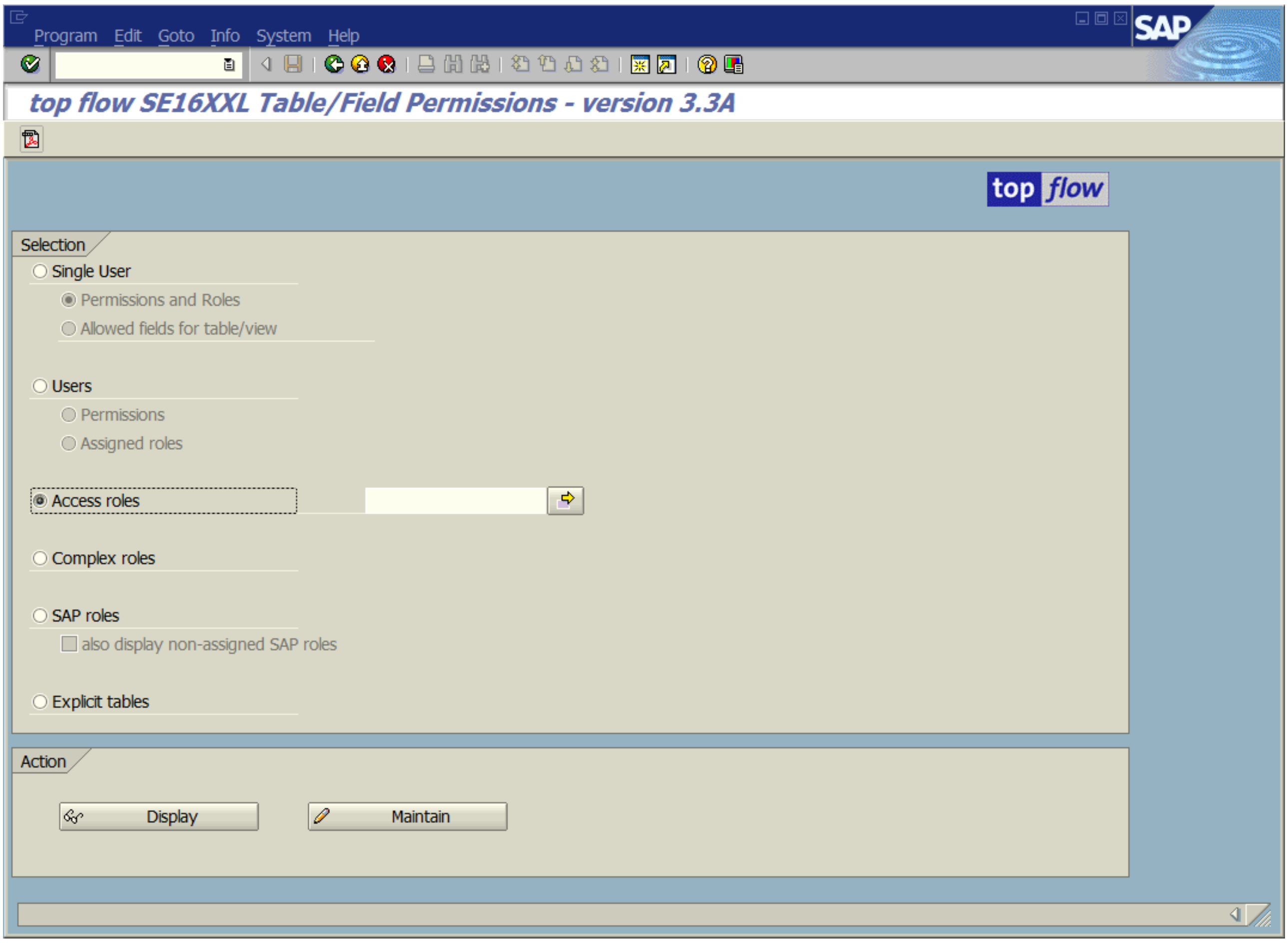
The indirect assignment of roles is also ideal for dividing the maintenance activities upon various persons: one administrator defines the SE16XXL access roles, another one assigns SAP roles to the end users.

We will now describe how the permissions can be configured by means of a brief tutorial. We will start with the more simple scenarios and proceed to the more complicated ones.

Tutorial # 1 – define (elementary) access roles

The definition of access roles is the most important part of the permission logic. If you wish to implement the new logic with SAP roles, you need access roles – otherwise access roles are not mandatory, but still highly recommendable.

To begin with, double click on Table & Field Permissions on the settings screen. The following selection screen will appear:



top flow SE16XXL Table/Field Permissions - version 3.3A

Selection

○ Single User
- ● Permissions and Roles
- ○ Allowed fields for table/view

○ Users
- ○ Permissions
- ○ Assigned roles

● Access roles

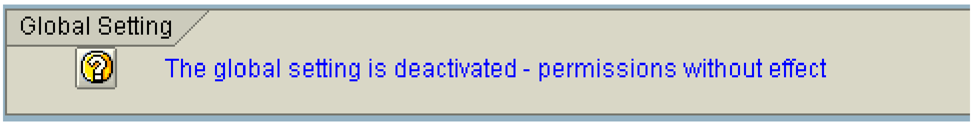
○ Complex roles

○ SAP roles
- □ also display non-assigned SAP roles

○ Explicit tables

Action

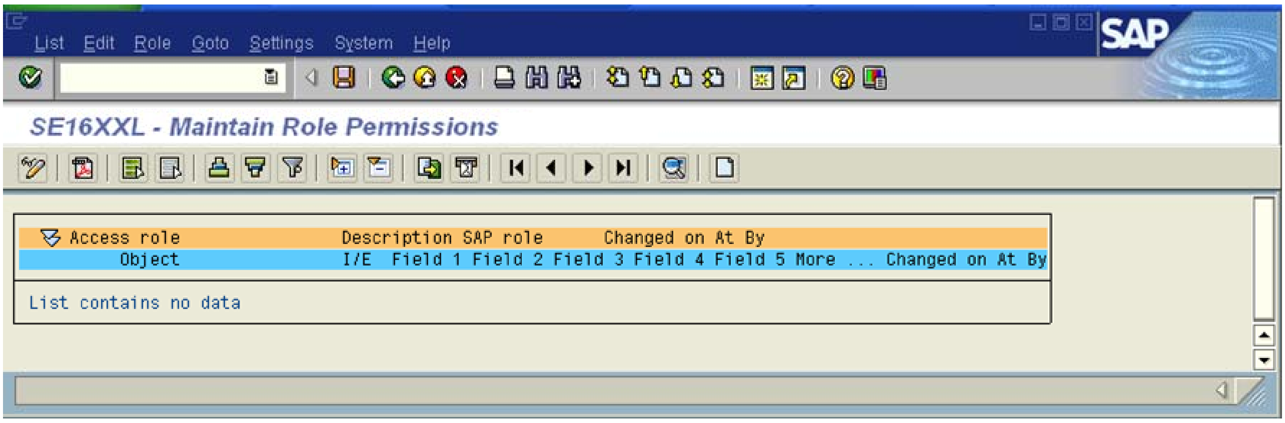
NOTE: if the global setting is deactivated, the following block will also be visible:



Global Setting

The global setting is deactivated - permissions without effect

Choose “Access roles” and press Maintain to get a list of the roles already defined. The first time the list will by empty:

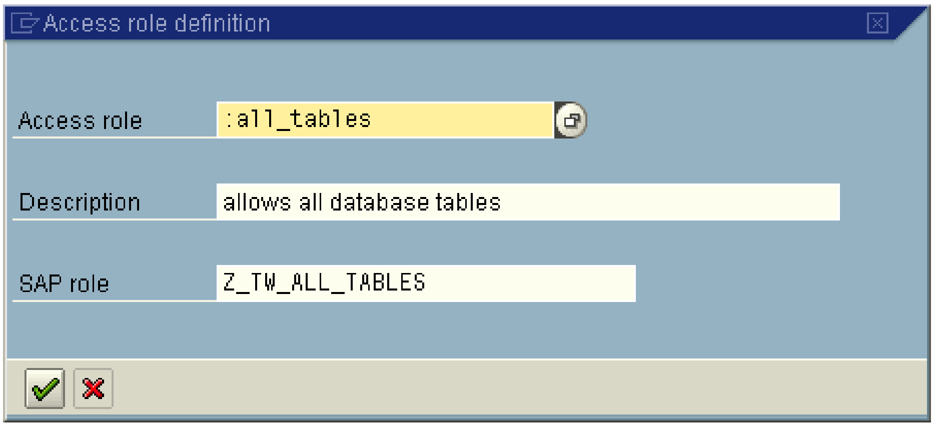


SE16XXL - Maintain Role Permissions

```
Access role                        Description SAP role      Changed on At By
      Object                       I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At By

List contains no data
```

The first access role you wish to create is the one that allows everything, a kind of SAPALL role. You decide to call it ":ALL_TABLES" (roles must begin with a ":").

Press 🗋 and define the access role:



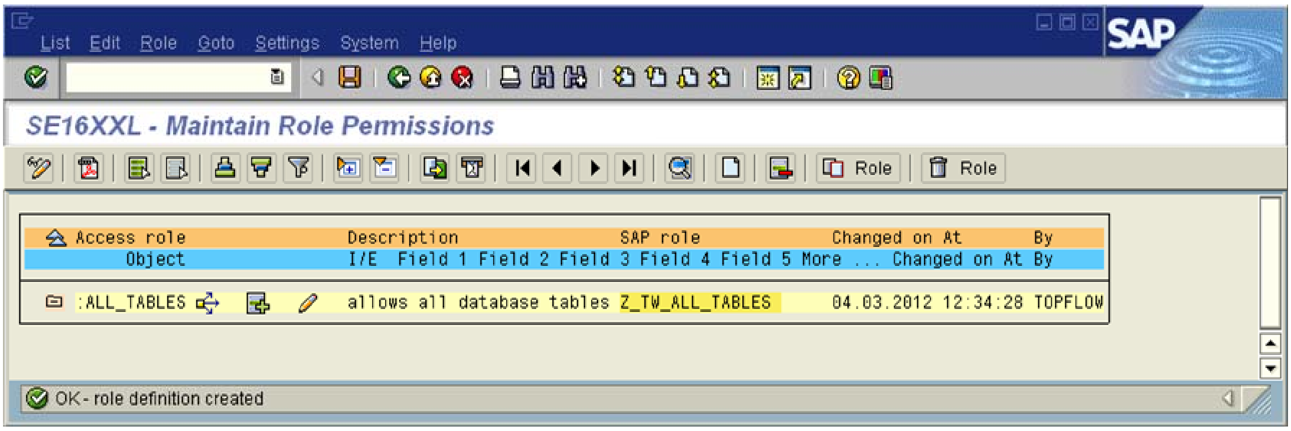
Access role definition

Access role: :all_tables

Description: allows all database tables

SAP role: Z_TW_ALL_TABLES

The SAP role is only necessary if you intend to implement the new logic. Otherwise the field can be left empty. The list changes accordingly:

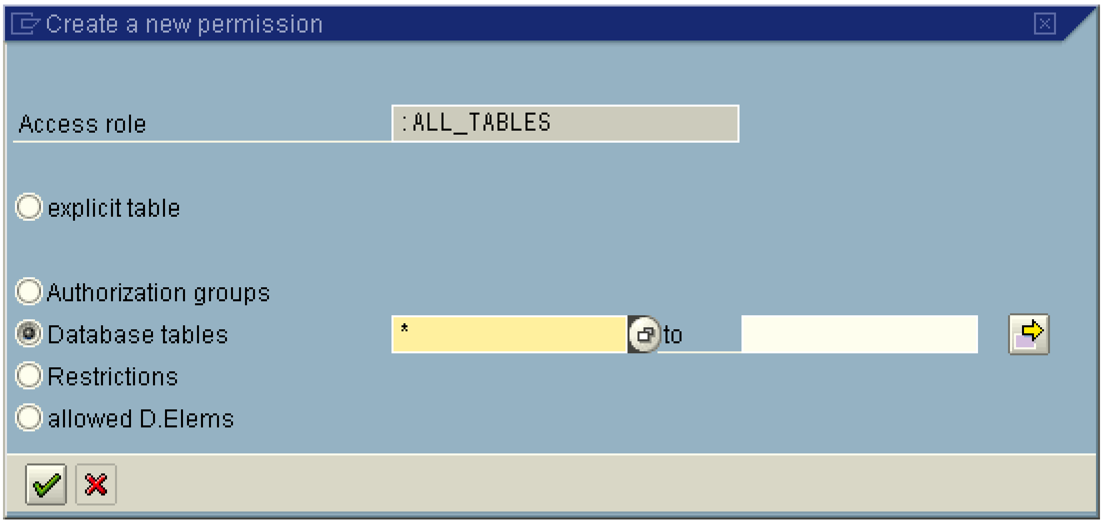


SE16XXL - Maintain Role Permissions

```
Access role                 Description                 SAP role          Changed on At        By
      Object                I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At By

:ALL_TABLES                 allows all database tables Z_TW_ALL_TABLES   04.03.2012 12:34:28 TOPFLOW
```

OK - role definition created

The access role is now defined but still “empty”. It is necessary to define the global permission that allows all database tables. To achieve this, click on the ⊞ icon at the right of the access role name. On the ensuing popup, choose “**Database tables**”:



Create a new permission

Access role: :ALL_TABLES

○ explicit table

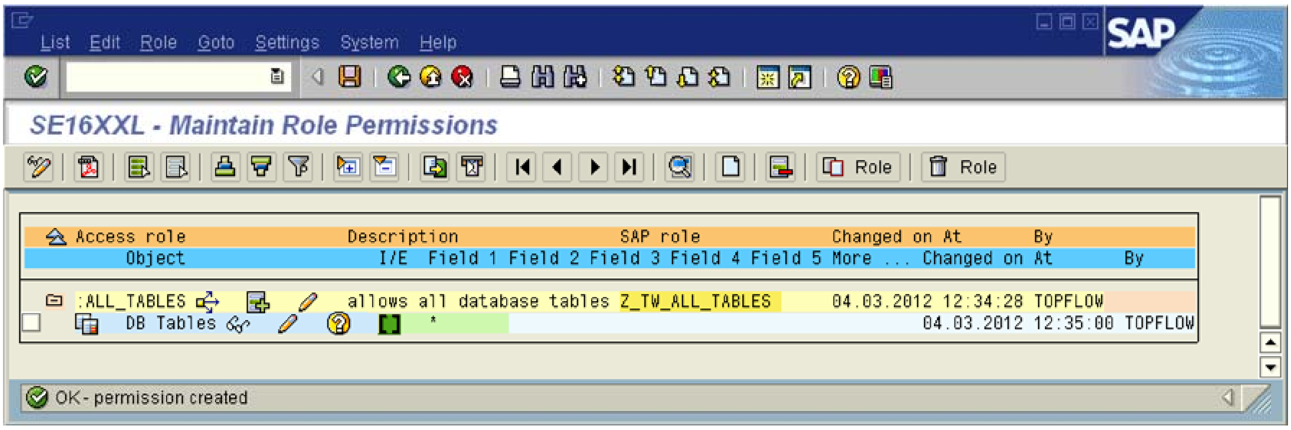
○ Authorization groups

● Database tables: * to

○ Restrictions

○ allowed D.Elems

Enter **“*”** (to denote all tables) and press ✓ to complete the definition.
The list is updated correspondingly:



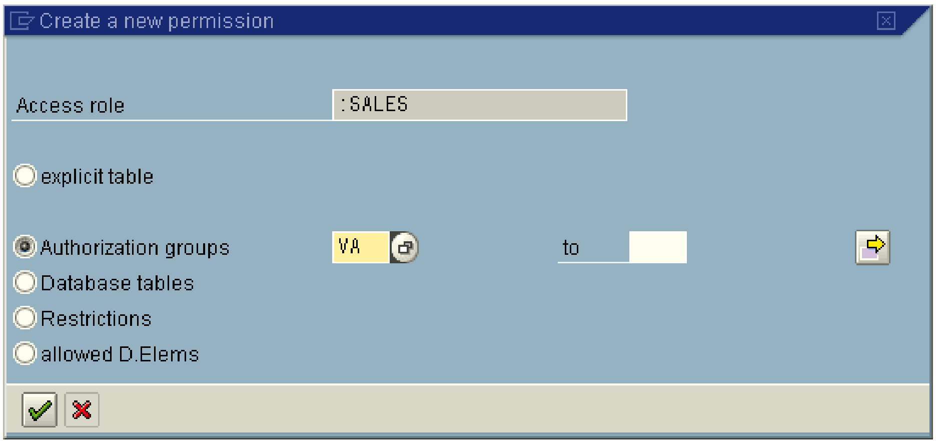
SE16XXL - Maintain Role Permissions

```
   Access role                  Description                 SAP role           Changed on At        By
          Object                         I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At     By

   :ALL_TABLES                  allows all database tables Z_TW_ALL_TABLES     04.03.2012 12:34:28 TOPFLOW
□       DB Tables                          *                                   04.03.2012 12:35:00 TOPFLOW
```

OK - permission created

A role that allows everything is necessary for the IT department, but you also need more specific roles for other departments, such as Sales or Planning.

So we proceed by defining an access role – named :SALES – for the Sales Department. The definition itself is carried out as already described above. Since most sales relevant tables have authorization group **VA**, we assign this auth. group to the role. To do this, we click on the ⊞ icon as we have already done, but choose “Authorization groups” and enter VA this time:



Create a new permission

Access role :SALES

○ explicit table

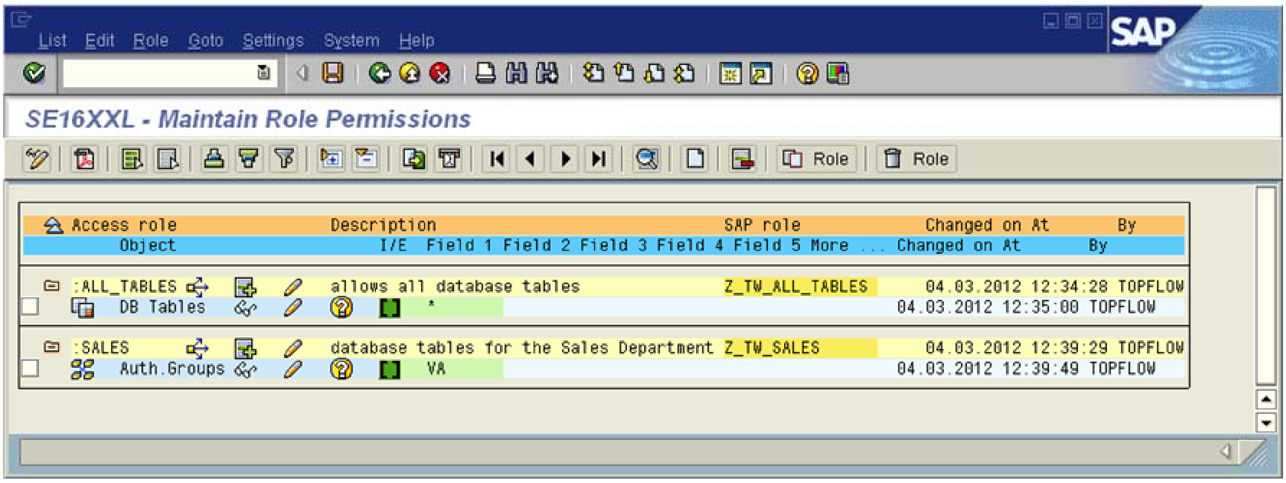
● Authorization groups VA to

○ Database tables

○ Restrictions

○ allowed D.Elems

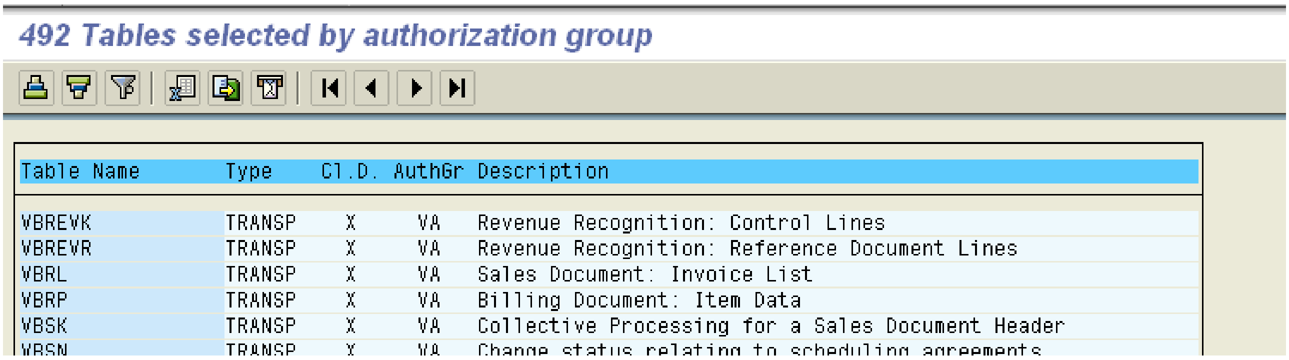
Our list of access roles now looks like this:



SE16XXL - Maintain Role Permissions

```
Access role                   Description                       SAP role               Changed on At          By
        Object                     I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At        By

:ALL_TABLES                   allows all database tables        Z_TW_ALL_TABLES        04.03.2012 12:34:28 TOPFLOW
        DB Tables                        *                                       04.03.2012 12:35:00 TOPFLOW

:SALES                        database tables for the Sales Department Z_TW_SALES      04.03.2012 12:39:29 TOPFLOW
        Auth.Groups                      VA                                      04.03.2012 12:39:49 TOPFLOW
```

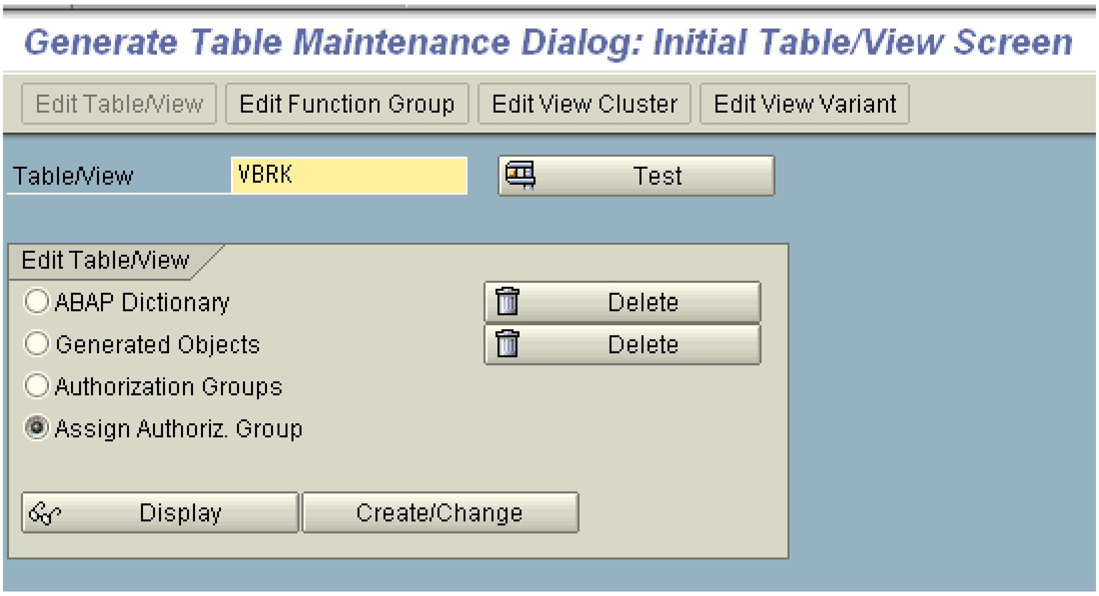
We would like to take a look at the list of selected tables to make sure all sales relevant tables have been taken into account. Such a list is easily produced by clicking on the ? icon at the right of the “Auth.Groups” line:



492 Tables selected by authorization group

Table Name	Type	Cl.D.	AuthGr	Description
VBREVK	TRANSP	X	VA	Revenue Recognition: Control Lines
VBREVR	TRANSP	X	VA	Revenue Recognition: Reference Document Lines
VBRL	TRANSP	X	VA	Sales Document: Invoice List
VBRP	TRANSP	X	VA	Billing Document: Item Data
VBSK	TRANSP	X	VA	Collective Processing for a Sales Document Header
VBSN	TRANSP	X	VA	Change status relating to scheduling agreements

While inspecting the list of selected tables, we notice that **VBRK** (invoice header) is missing from the list. Indeed VBRK belongs to authorization group **MA** – use standard transaction **SE54** to determine the authorization group of a given table:



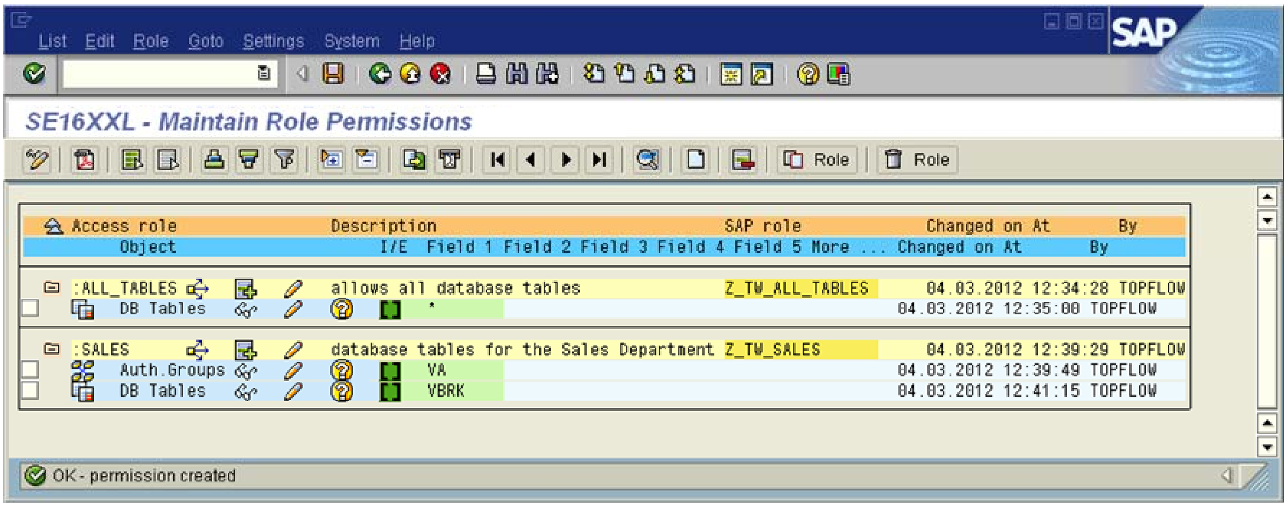
Generate Table Maintenance Dialog: Initial Table/View Screen

Table/View: VBRK

Edit Table/View

○ ABAP Dictionary
○ Generated Objects
○ Authorization Groups
● Assign Authoriz. Group

In order to also cover this database table, we add a corresponding permission by name:



SE16XXL - Maintain Role Permissions

```
Access role                     Description                            SAP role          Changed on At        By
     Object                          I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At        By

:ALL_TABLES                     allows all database tables             Z_TW_ALL_TABLES   04.03.2012 12:34:28 TOPFLOW
     DB Tables                       *                                                 04.03.2012 12:35:00 TOPFLOW

:SALES                          database tables for the Sales Department Z_TW_SALES      04.03.2012 12:39:29 TOPFLOW
     Auth.Groups                     VA                                                04.03.2012 12:39:49 TOPFLOW
     DB Tables                       VBRK                                              04.03.2012 12:41:15 TOPFLOW
```

OK - permission created

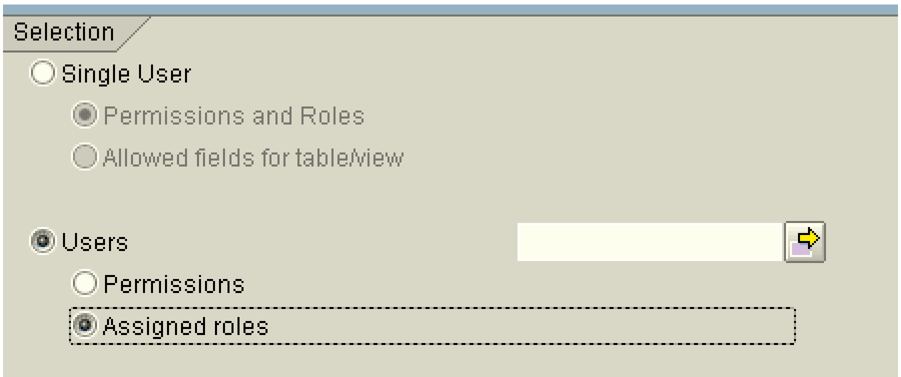
Now we can press the 💾 button and thus save our work – if we forget, the program will remind us when we try to leave it.

Conclusion: we have defined two (elementary) access roles, one covering all database tables for the IT department, the other one allowing only sales relevant database tables for the Sales department.

In the next tutorials we will first assign these roles to users **directly** and then – through their associated SAP roles – **indirectly**.

Tutorial # 2 – assign access roles to users (directly)

In order to assign access roles directly to users, call the Table & Field Permissions again and choose “Users” and “Assigned roles”:



Selection

○ Single User

● Permissions and Roles

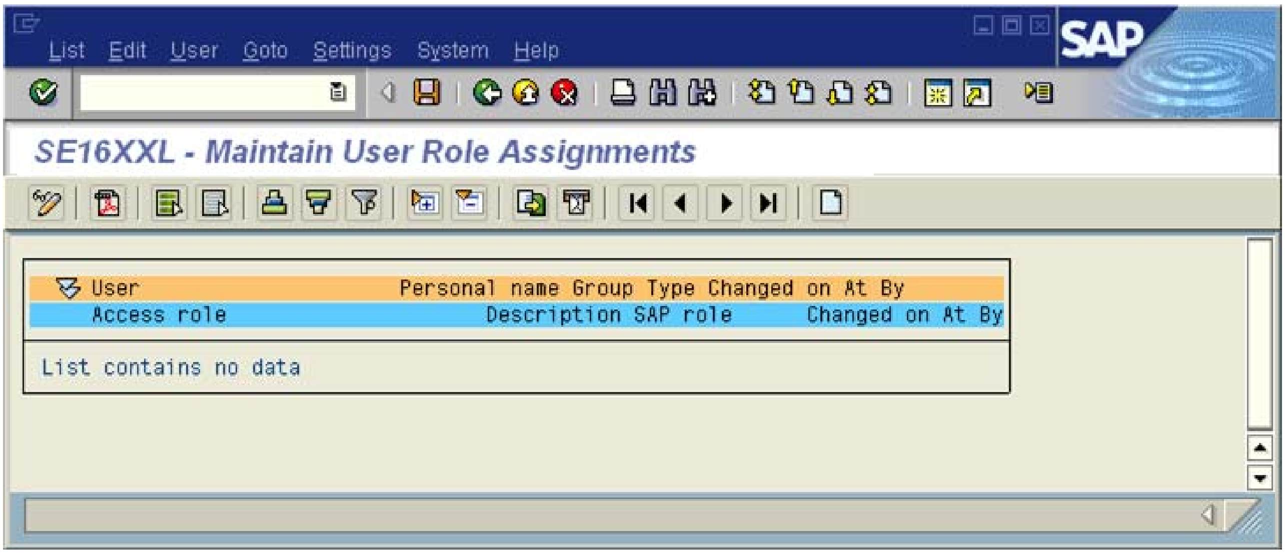
○ Allowed fields for table/view

● Users

○ Permissions

● Assigned roles

As an alternative you may switch to this list without leaving the program by choosing ***Goto → Users & assigned roles.*** Both ways, the list of users and assigned roles appears – empty at first:

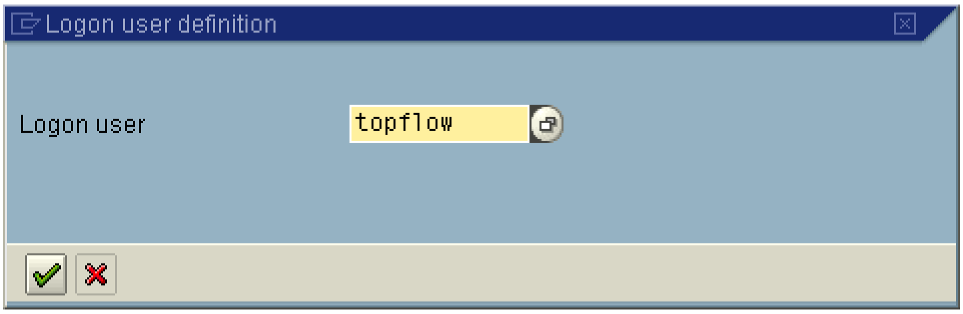


SE16XXL - Maintain User Role Assignments

```
User                             Personal  name Group Type Changed on  At  By
    Access role                            Description SAP role        Changed on  At  By

List contains no data
```

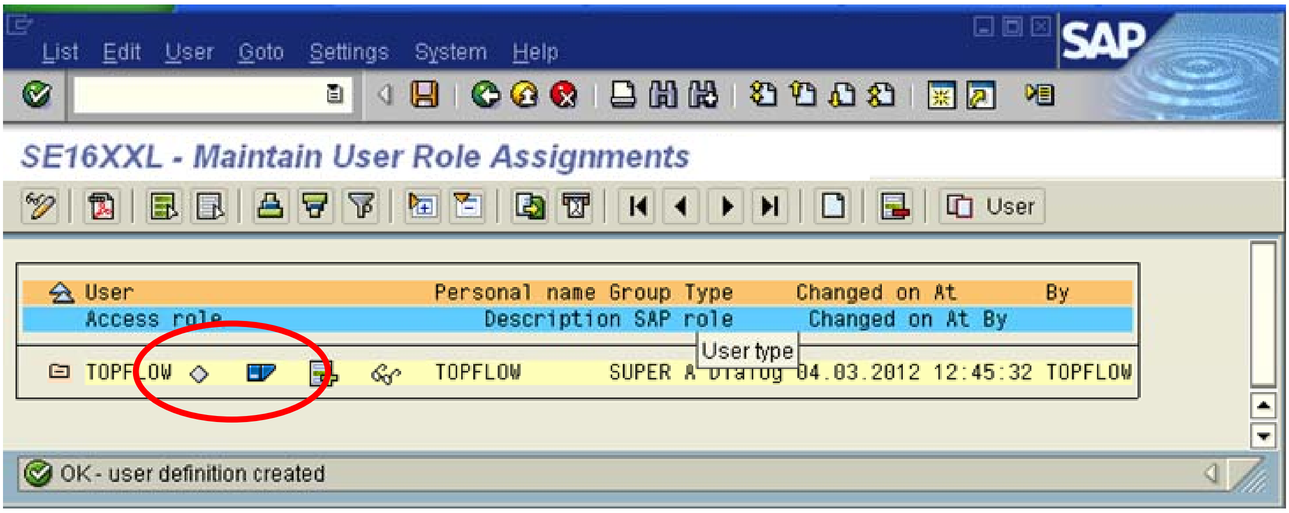
In order to assign an access role to a user, the user himself must be defined first. This definition is only necessary when assigning roles directly, because the program needs to know which users are considered from the point of view of the SE16XXL permissions. As we will see later on, no such definition is necessary when the assignment is performed indirectly by means of SAP roles.

We press the 🗋 icon on the application toolbar to define a user:



Logon user topflow

After entering the logon user and pressing ✓, we obtain the following:



SE16XXL - Maintain User Role Assignments

```
User                       Personal name Group Type    Changed on At         By
   Access role                   Description SAP role    Changed on At By
                                                 User type
TOPFLOW ◇   ▰   ⊞   TOPFLOW       SUPER  A  Dialog 04.03.2012 12:45:32 TOPFLOW
```

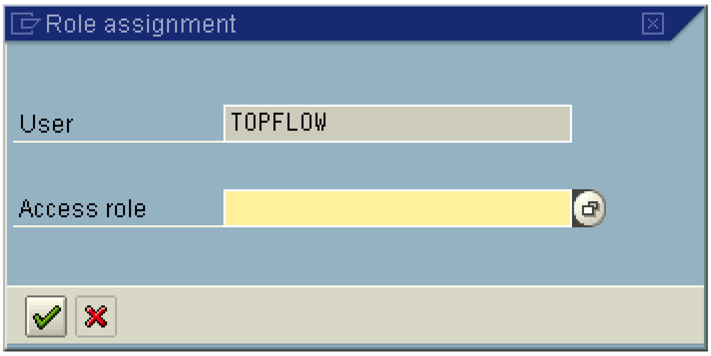
OK - user definition created

Notice the two icons at the right of the user:

▰ signifies that this is a real SAP user (you can create non-existent users using the "copy" function);

◇ signifies that the user is also defined as SE16XXL Permissions user.

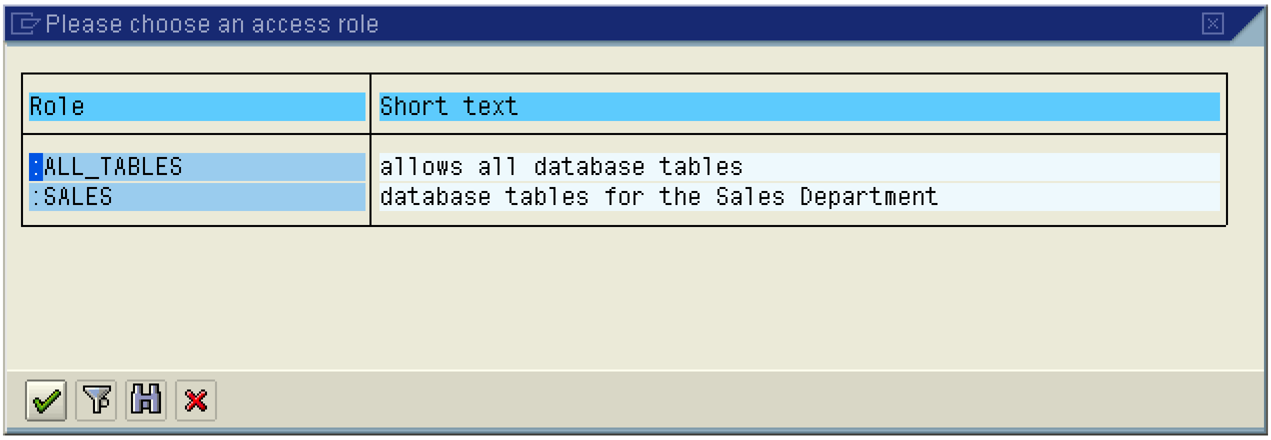
We are now ready to assign an access role to the user. A new role assignment is created with a click on the ⊞ icon of the user line:



User TOPFLOW

Access role

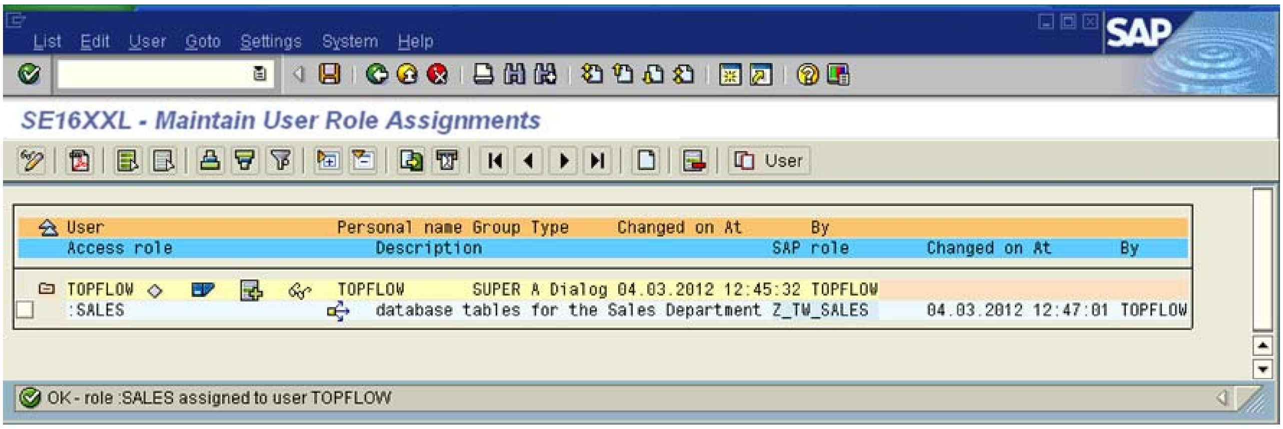
The value help (F4) provides a list of the available access roles:



Please choose an access role

Role	Short text
:ALL_TABLES	allows all database tables
:SALES	database tables for the Sales Department

Just as an example we choose :SALES – the list changes accordingly:



SE16XXL - Maintain User Role Assignments

```
User                              Personal name Group Type      Changed on At         By
Access role                           Description                           SAP role        Changed on At         By

TOPFLOW                           TOPFLOW       SUPER A Dialog 04.03.2012 12:45:32 TOPFLOW
:SALES                                database tables for the Sales Department Z_TW_SALES      04.03.2012 12:47:01 TOPFLOW
```

OK - role :SALES assigned to user TOPFLOW

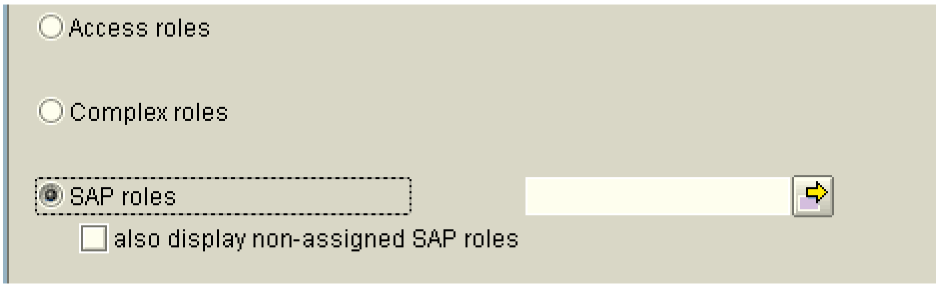
As you may imagine, it is possible to assign any number of access roles to a user.

NOTE: the present example is based on the assumption that the administrator is authorized to define users **and** to assign access roles to them. If these authorizations belong to different persons, the one authorized to carry out the assignments will have to wait until the users have been defined by the other one.

We will now describe the indirect assignment of access roles.

Tutorial # 3 – assign access roles to users (indirectly)

The best way to perform such an assignment is by calling the Table & Field Permissions and choosing **SAP roles**:



○ Access roles

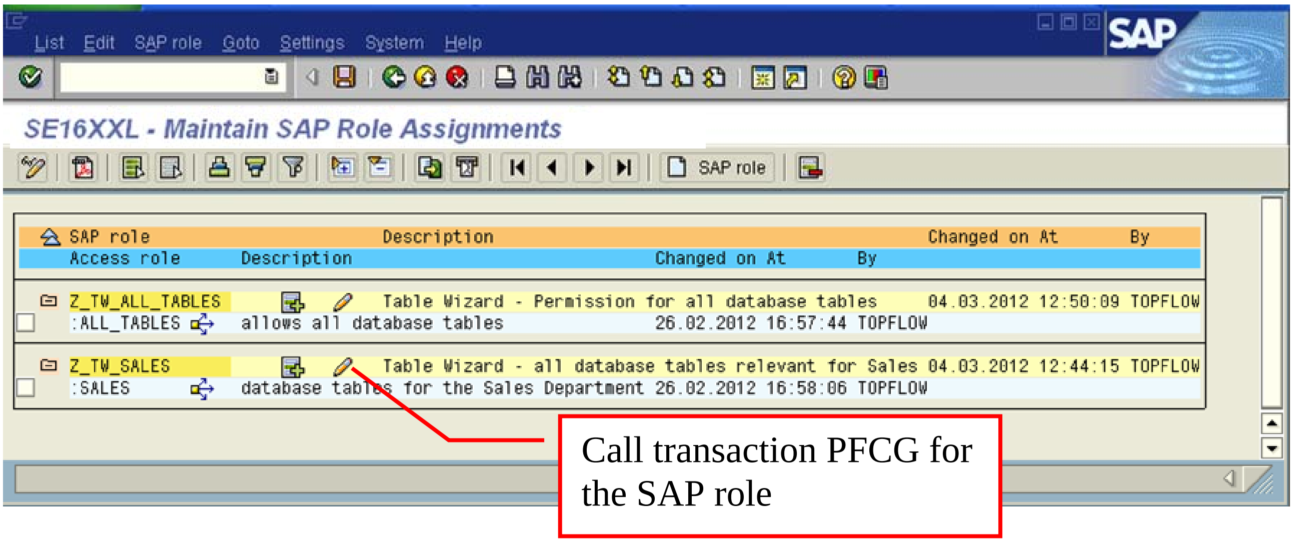
○ Complex roles

● SAP roles

□ also display non-assigned SAP roles

The standard list only takes into account SAP roles associated with SE16XXL roles. To select all SAP roles, also check the ☑ also display non-assigned SAP roles option.

In our example the list looks like this:



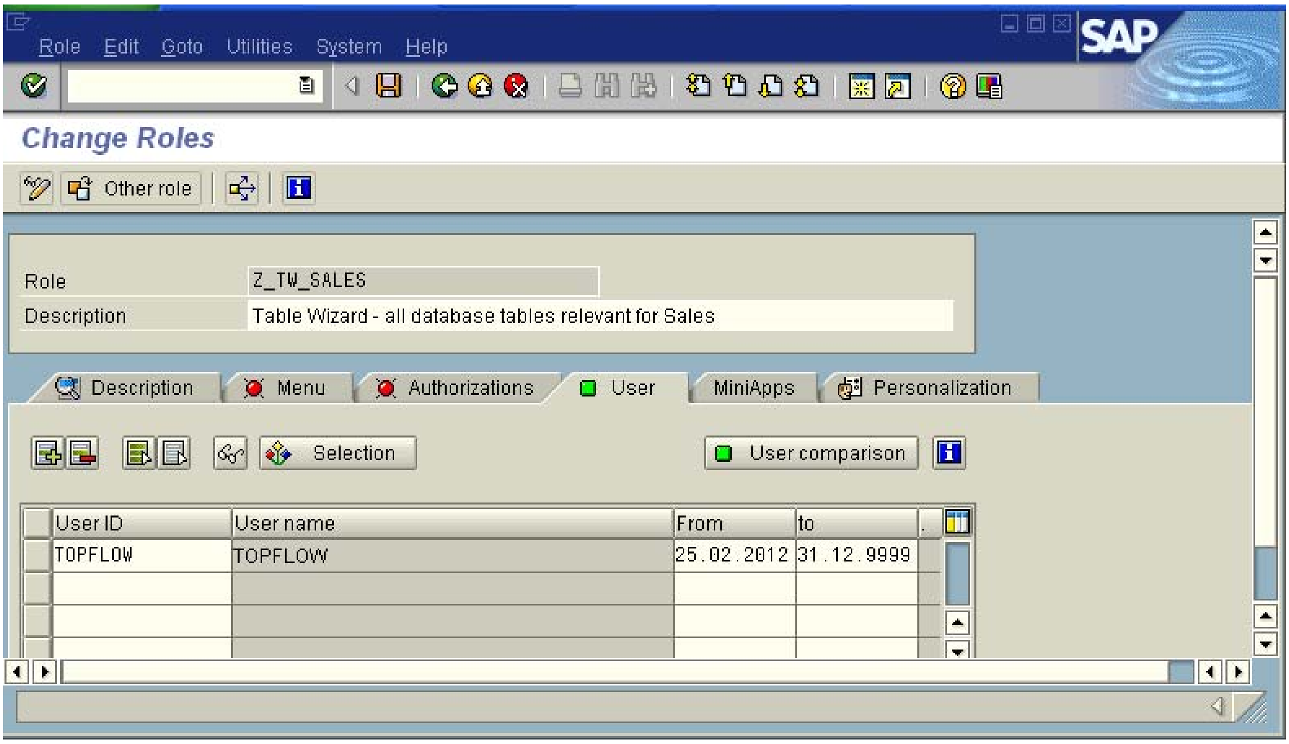
SE16XXL - Maintain SAP Role Assignments

```
SAP role                      Description                                     Changed on At          By
   Access role      Description                             Changed on At          By

Z_TW_ALL_TABLES                  Table Wizard - Permission for all database tables   04.03.2012 12:50:09 TOPFLOW
   :ALL_TABLES      allows all database tables              26.02.2012 16:57:44 TOPFLOW

Z_TW_SALES                       Table Wizard - all database tables relevant for Sales 04.03.2012 12:44:15 TOPFLOW
   :SALES           database tables for the Sales Department 26.02.2012 16:58:06 TOPFLOW
```

Call transaction PFCG for the SAP role

It shows each SAP role and the associated SE16XXL access roles. Associate further access roles by clicking on the ⊞ icon at the right of each SAP role.

In this tutorial we are interested in performing an indirect assignment of access roles to users. This is achieved by assigning one or more users to an SAP role, thereby assigning to these users all access roles associated with the SAP role. By clicking on the ✎ icon at the right of the SAP role we call standard transaction **PFCG** (you need the corresponding authorization):



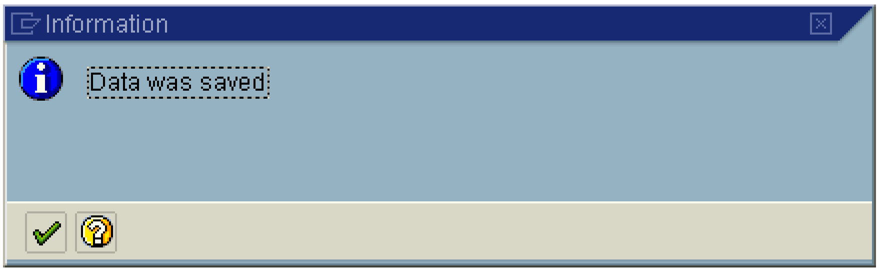
Change Roles

Role Z_TW_SALES

Description Table Wizard - all database tables relevant for Sales

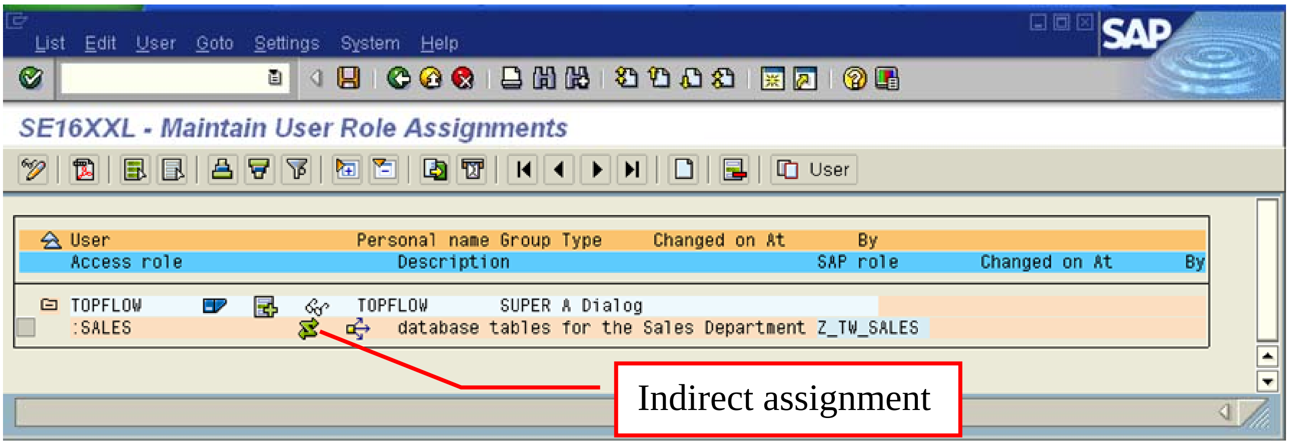
User ID	User name	From	to
TOPFLOW	TOPFLOW	25.02.2012	31.12.9999

After pressing 💾, we exit from PFCG. The following message informs us that the assignment has been carried out for real:


Information

Data was saved

To see the indirect assignment, we call up the list of **users and roles** by means of menu function ***Goto → Users & assigned roles***:



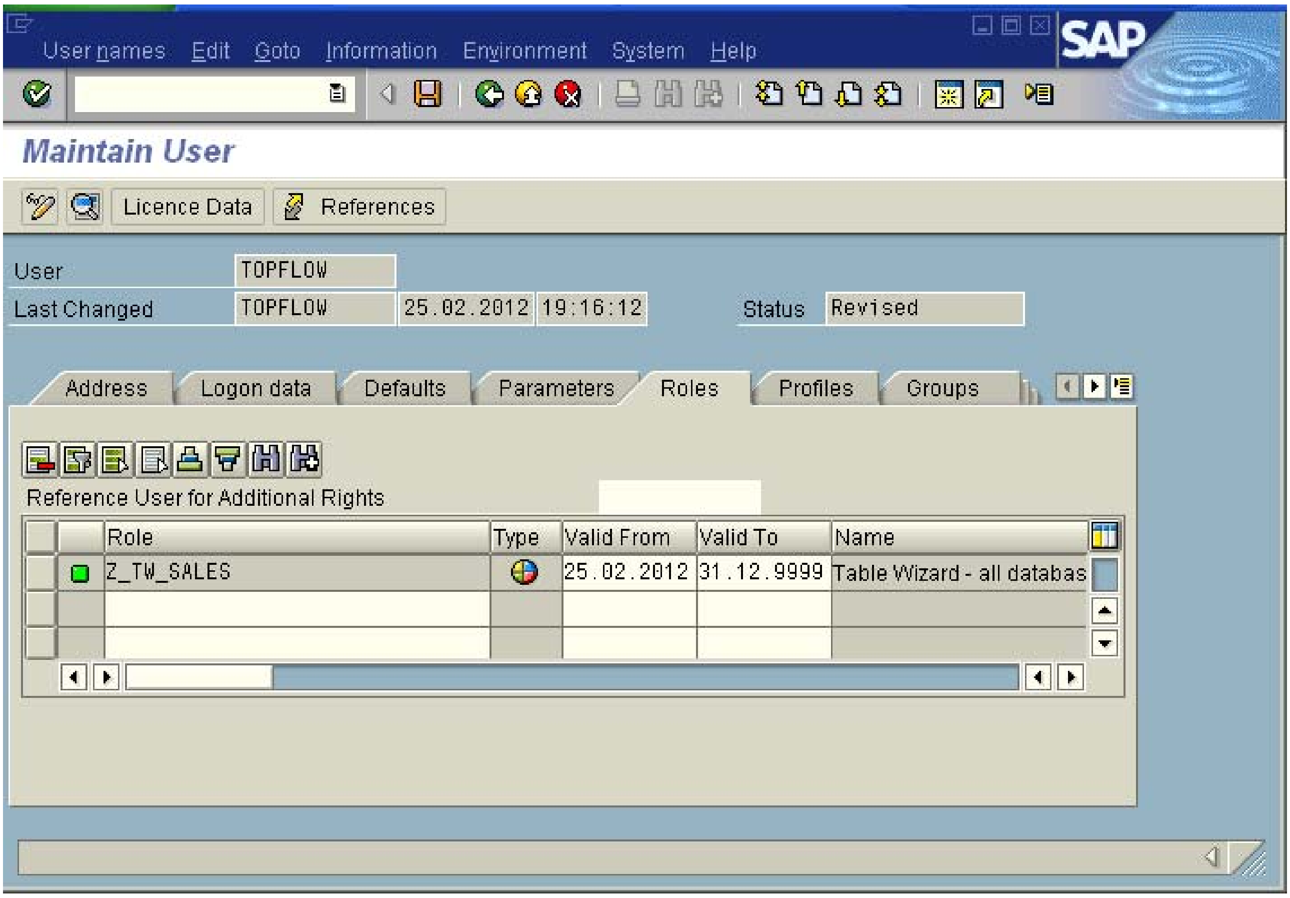
SE16XXL - Maintain User Role Assignments

```
User                          Personal name Group Type    Changed on At       By
     Access role                       Description                         SAP role        Changed on At       By

TOPFLOW                       TOPFLOW       SUPER A Dialog
:SALES                          database tables for the Sales Department Z_TW_SALES
```

Notice that the list is slightly different from the one we have seen in **tutorial # 2**.

- Firstly, no ◇ icon is at the right of the user, which means that the user has not been defined as SE16XXL permission user (we assume that tutorial # 2 has not taken place).
- Secondly, the access role is marked with an ⇄ icon, signalizing that the assignment has been carried out indirectly.
- Thirdly, the colors are different.

Another way to assign an SAP role to a user is standard transaction SU01, which may also be called from the list of **Users & assigned roles** by using menu function ***User → Display SAP user (SU01)***.



User	TOPFLOW
Last Changed	TOPFLOW 25.02.2012 19:16:12
Status	Revised

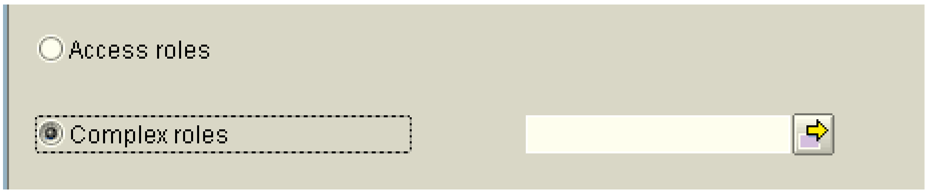
Reference User for Additional Rights

	Role	Type	Valid From	Valid To	Name
🟩	Z_TW_SALES	●	25.02.2012	31.12.9999	Table Wizard - all databas

Tutorial # 4 – define a complex role

A complex role is for access roles what the composite role is for SAP roles, i.e. a collection of elementary access roles which can all be assigned together. A complex role does not have any permissions itself – the elementary access roles contained in the complex role do.

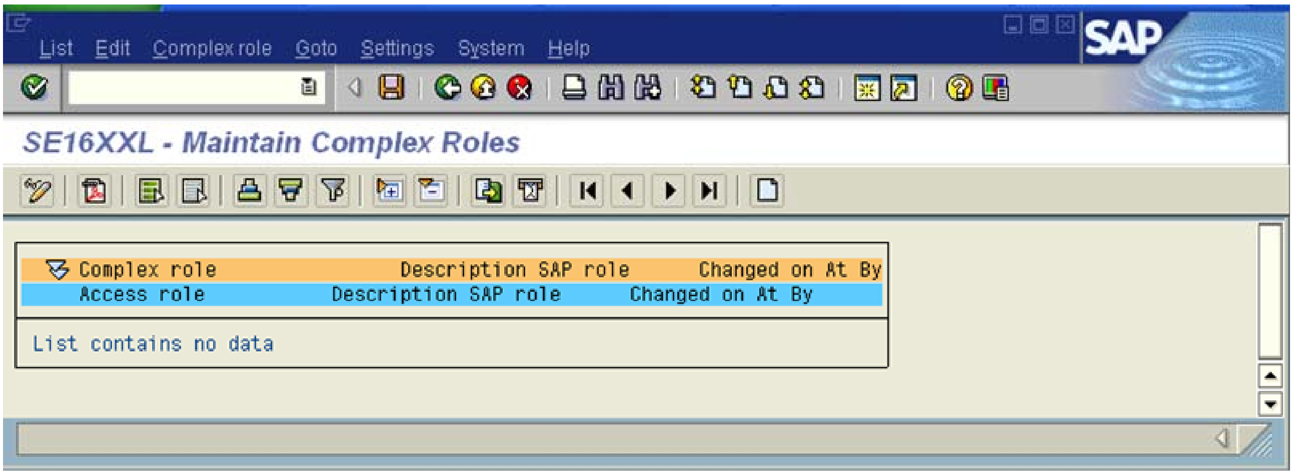
To define a complex role, we call the program and choose “**Complex roles**”:



○ Access roles

● Complex roles

The corresponding list will be shown – empty at first:

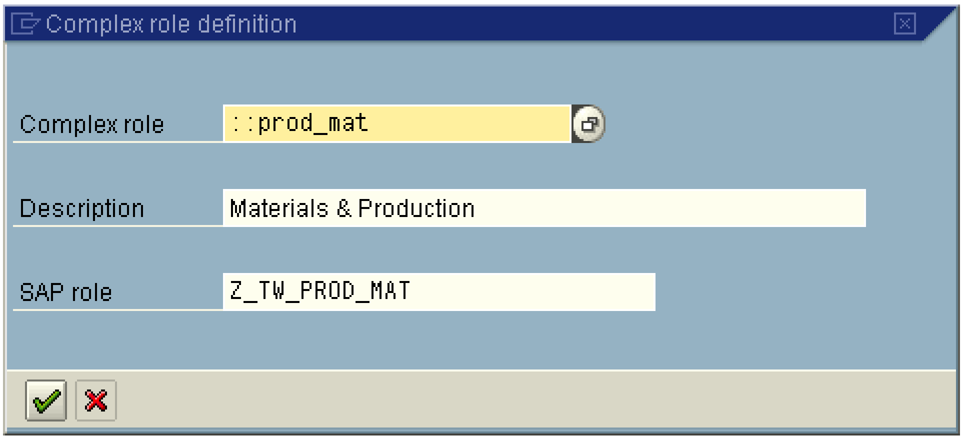


SE16XXL - Maintain Complex Roles

Complex role	Description SAP role	Changed on At By
Access role	Description SAP role	Changed on At By

List contains no data

We press 🗋 to define a new complex role (the name must begin with “::”):



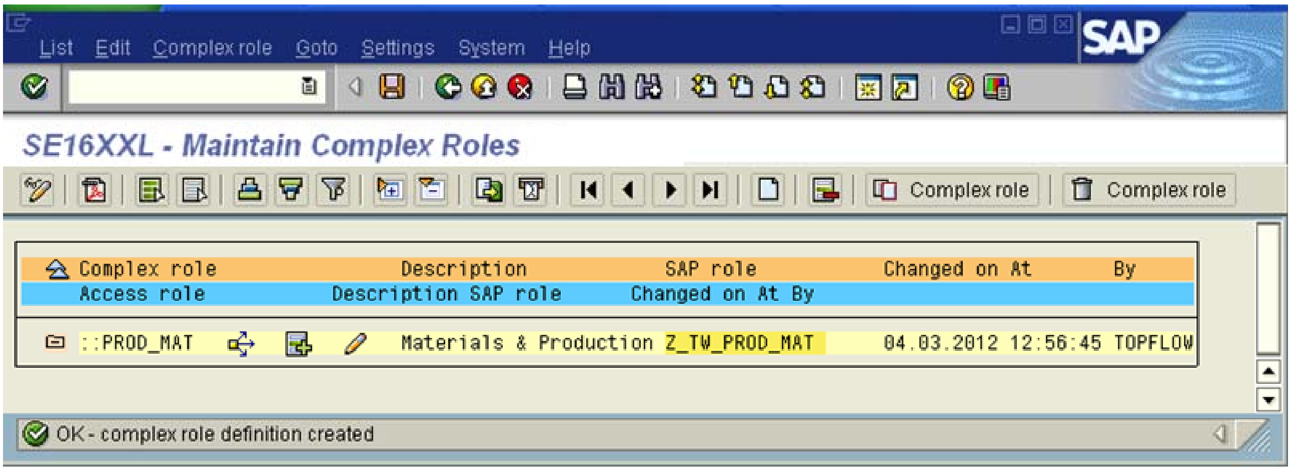
Complex role definition

Complex role ::prod_mat

Description Materials & Production

SAP role Z_TW_PROD_MAT

The list is updated accordingly:

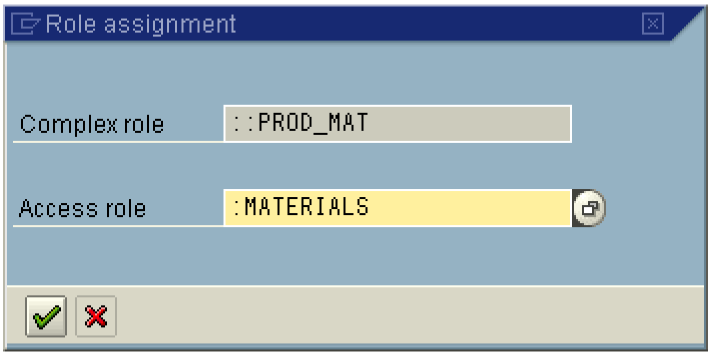


SE16XXL - Maintain Complex Roles

```
Complex role            Description          SAP role           Changed on At        By
    Access role        Description SAP role     Changed on At By

::PROD_MAT                    Materials & Production Z_TW_PROD_MAT      04.03.2012 12:56:45 TOPFLOW
```

OK - complex role definition created

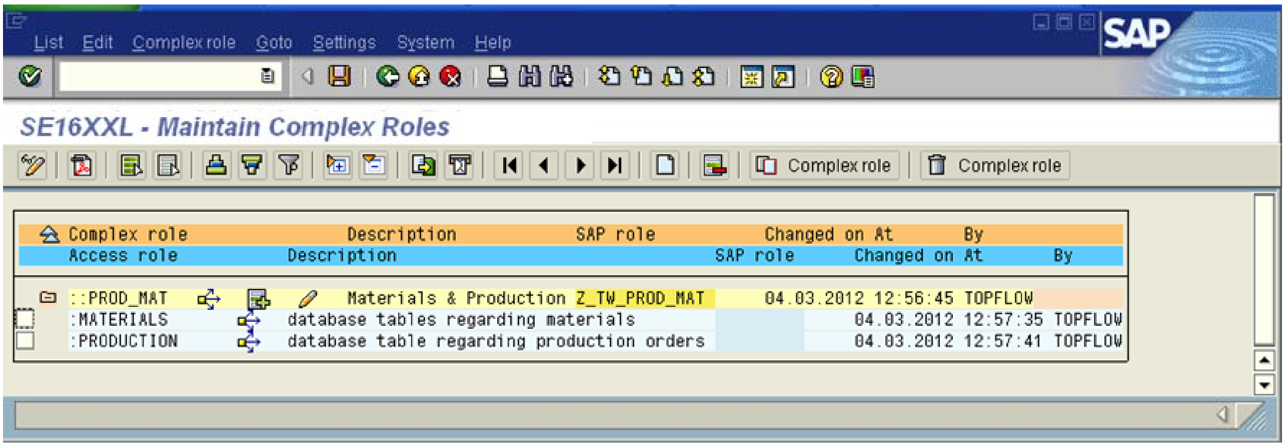
Now we assign two elementary access roles to our newly created complex role. A click on the icon is all that is needed:



Complex role ::PROD_MAT

Access role :MATERIALS

We repeat the operation for access role :PRODUCTION. The result is as follows:



SE16XXL - Maintain Complex Roles

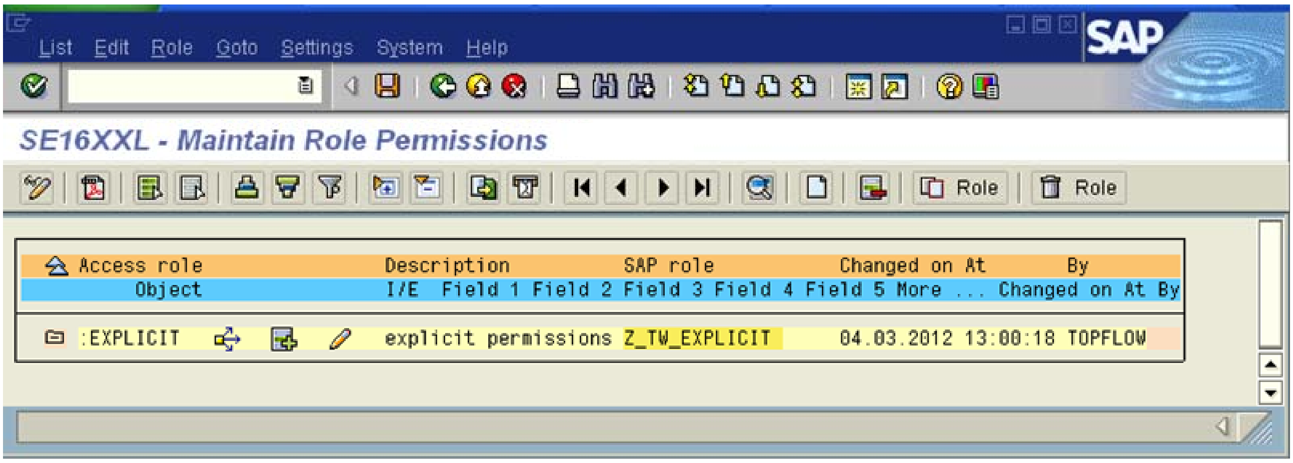
```
  Complex role               Description           SAP role            Changed on At       By
  Access role           Description                           SAP role     Changed on At        By

  ::PROD_MAT                    Materials & Production Z_TW_PROD_MAT      04.03.2012 12:56:45 TOPFLOW
□ :MATERIALS            database tables regarding materials                    04.03.2012 12:57:35 TOPFLOW
□ :PRODUCTION           database table regarding production orders             04.03.2012 12:57:41 TOPFLOW
```

Instead of assigning the two elementary roles to a user, you can assign the complex role. Just as for elementary roles, this assignment can be direct or indirect through the associated SAP role.

Tutorial # 5 – define an explicit permission for a table

Up to now we have defined permissions for all fields of the database tables involved. This was because we addressed the tables either by name or by authorization group. But – as we already mentioned at the beginning – it is possible to define permissions at field level – i.e. for specific fields of a database table, and not for the table as a whole. A typical example is table MBEW, in which the fields VERPR and STPRS seem to be most sensitive.

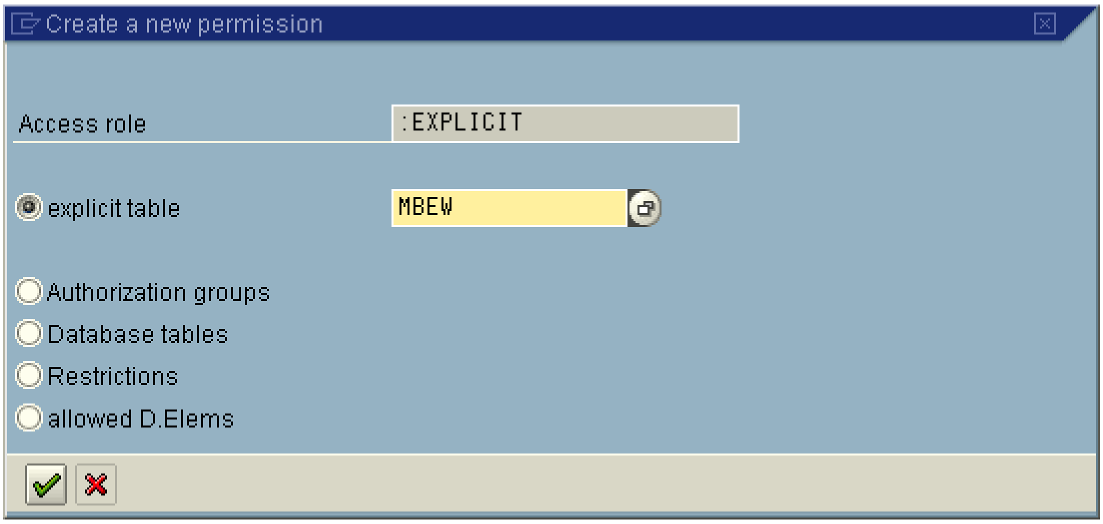
We start by defining a new role called :EXPLICIT.



SE16XXL - Maintain Role Permissions

Access role	Description	SAP role	Changed on At	By
Object	I/E Field 1 Field 2 Field 3 Field 4 Field 5 More ...		Changed on At	By
:EXPLICIT	explicit permissions	Z_TW_EXPLICIT	04.03.2012 13:00:18	TOPFLOW

As usual we click on to define a new permission:



Create a new permission

Access role :EXPLICIT

● explicit table MBEW

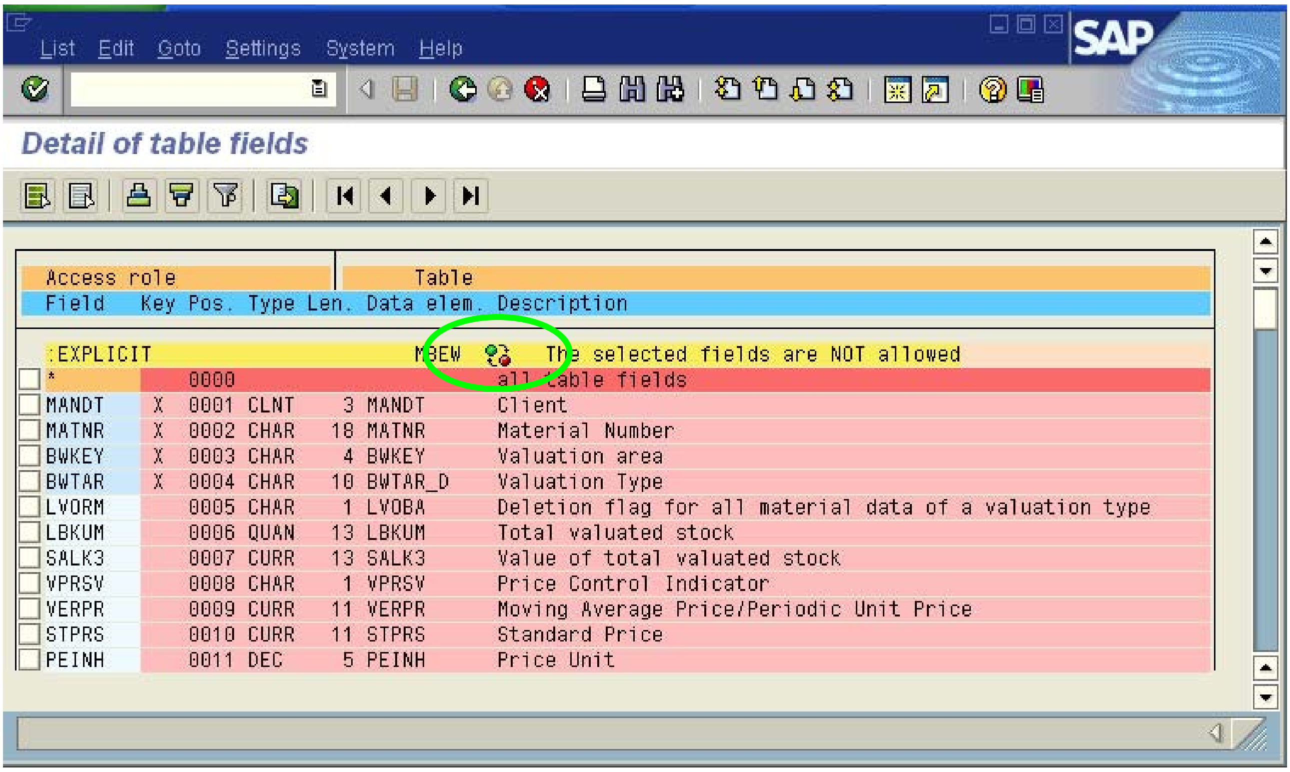
○ Authorization groups

○ Database tables

○ Restrictions

○ allowed D.Elems

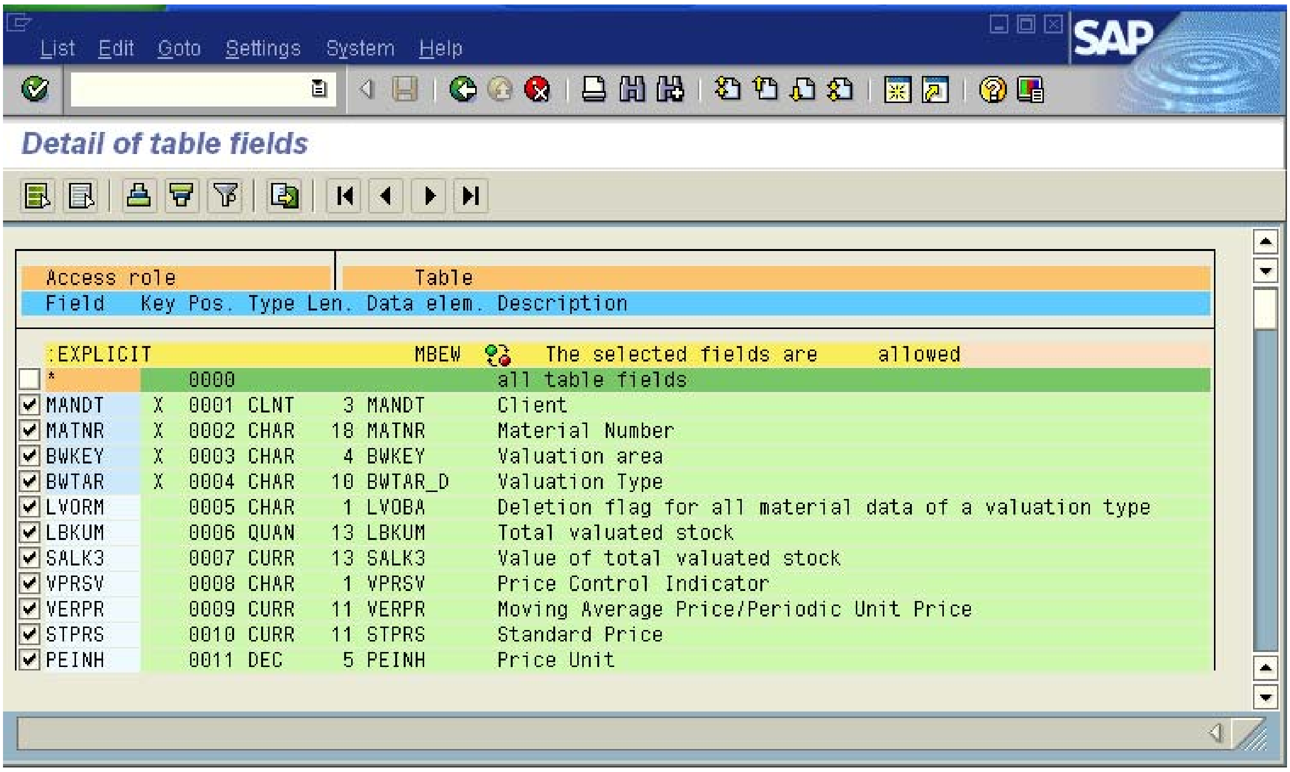
This time we choose “explicit table”. The following list of the table fields appears:



Detail of table fields

	Access role					Table	
	Field	Key	Pos.	Type	Len.	Data elem.	Description
	:EXPLICIT					MBEW	The selected fields are NOT allowed
□	*		0000				all table fields
□	MANDT	X	0001	CLNT	3	MANDT	Client
□	MATNR	X	0002	CHAR	18	MATNR	Material Number
□	BWKEY	X	0003	CHAR	4	BWKEY	Valuation area
□	BWTAR	X	0004	CHAR	10	BWTAR_D	Valuation Type
□	LVORM		0005	CHAR	1	LVOBA	Deletion flag for all material data of a valuation type
□	LBKUM		0006	QUAN	13	LBKUM	Total valuated stock
□	SALK3		0007	CURR	13	SALK3	Value of total valuated stock
□	VPRSV		0008	CHAR	1	VPRSV	Price Control Indicator
□	VERPR		0009	CURR	11	VERPR	Moving Average Price/Periodic Unit Price
□	STPRS		0010	CURR	11	STPRS	Standard Price
□	PEINH		0011	DEC	5	PEINH	Price Unit

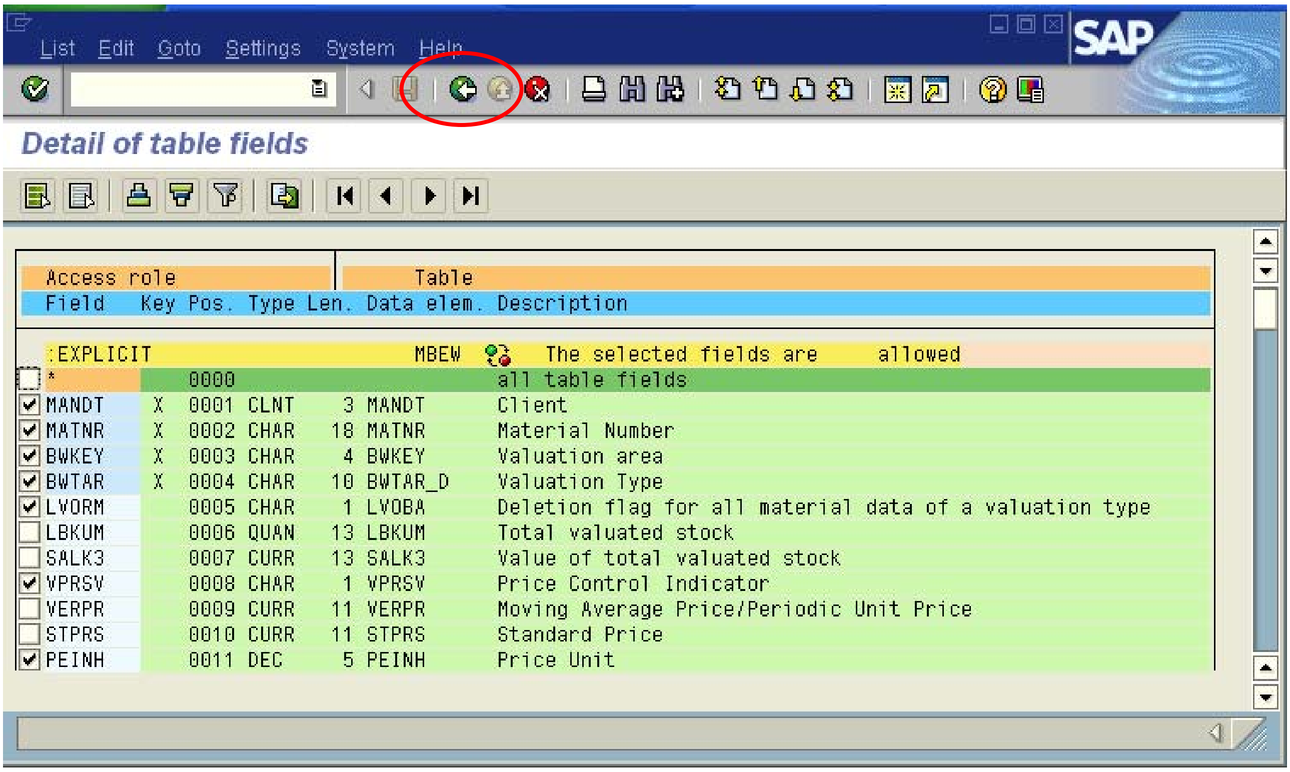
We want to be particularly restrictive in this case, so we switch definition mode by clicking on the icon:



Detail of table fields

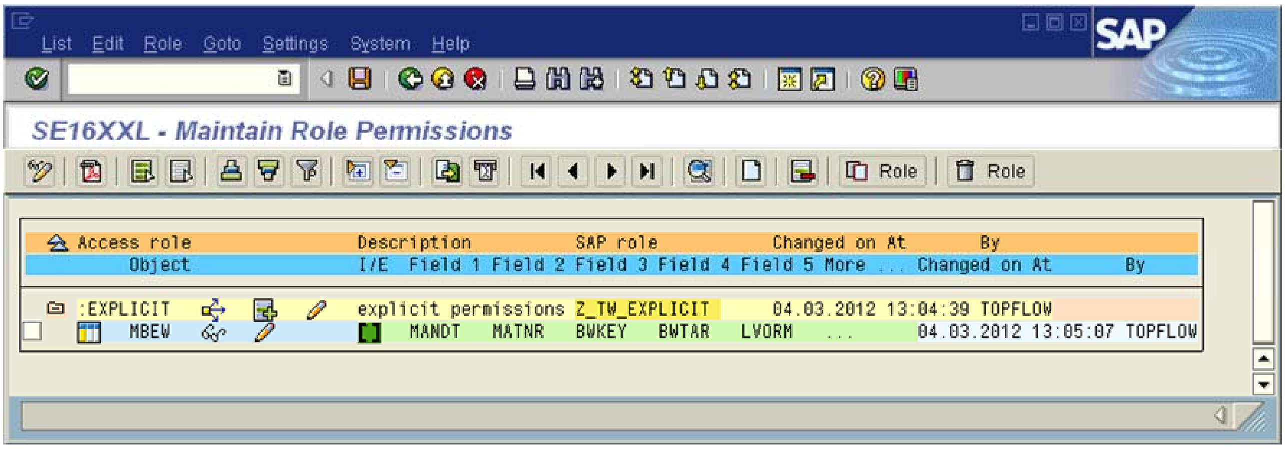
	Access role					Table	
	Field	Key	Pos.	Type	Len.	Data elem.	Description
	:EXPLICIT					MBEW	The selected fields are allowed
□	*		0000				all table fields
☑	MANDT	X	0001	CLNT	3	MANDT	Client
☑	MATNR	X	0002	CHAR	18	MATNR	Material Number
☑	BWKEY	X	0003	CHAR	4	BWKEY	Valuation area
☑	BWTAR	X	0004	CHAR	10	BWTAR_D	Valuation Type
☑	LVORM		0005	CHAR	1	LVOBA	Deletion flag for all material data of a valuation type
☑	LBKUM		0006	QUAN	13	LBKUM	Total valuated stock
☑	SALK3		0007	CURR	13	SALK3	Value of total valuated stock
☑	VPRSV		0008	CHAR	1	VPRSV	Price Control Indicator
☑	VERPR		0009	CURR	11	VERPR	Moving Average Price/Periodic Unit Price
☑	STPRS		0010	CURR	11	STPRS	Standard Price
☑	PEINH		0011	DEC	5	PEINH	Price Unit

After pressing the button we select only those fields which we consider “safe”:



```
 Access role        Table
 Field    Key Pos.  Type Len. Data elem. Description

 :EXPLICIT                   MBEW     The selected fields are      allowed
□ *              0000                   all table fields
☑ MANDT     X    0001 CLNT     3 MANDT      Client
☑ MATNR     X    0002 CHAR    18 MATNR      Material Number
☑ BWKEY     X    0003 CHAR     4 BWKEY      Valuation area
☑ BWTAR     X    0004 CHAR    10 BWTAR_D    Valuation Type
☑ LVORM          0005 CHAR     1 LVOBA      Deletion flag for all material data of a valuation type
□ LBKUM          0006 QUAN    13 LBKUM      Total valuated stock
□ SALK3          0007 CURR    13 SALK3      Value of total valuated stock
☑ VPRSV          0008 CHAR     1 VPRSV      Price Control Indicator
□ VERPR          0009 CURR    11 VERPR      Moving Average Price/Periodic Unit Price
□ STPRS          0010 CURR    11 STPRS      Standard Price
☑ PEINH          0011 DEC      5 PEINH      Price Unit
```

We exit by means of the green button . The list is updated accordingly:


List Edit Role Goto Settings System Help
SE16XXL - Maintain Role Permissions
Role
Role

```
 Access role              Description             SAP role          Changed on At        By
       Object             I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At         By

  :EXPLICIT               explicit permissions Z_TW_EXPLICIT       04.03.2012 13:04:39 TOPFLOW
□      MBEW                    MANDT   MATNR   BWKEY   BWTAR   LVORM   ...      04.03.2012 13:05:07 TOPFLOW
```

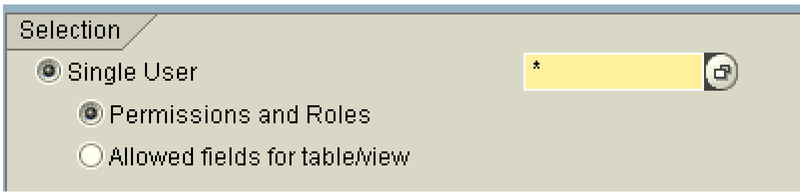
From now on all users to whom the access role is assigned (either directly or indirectly) will only see the allowed fields of table MBEW.

IMPORTANT: if two roles are assigned to a user, one allowing only some fields of a table, the other allowing all fields, the role allowing all fields "wins". Therefore care should be taken that tables with explicit permissions are not also available as a whole (all fields) in other roles. In our example MBEW should only be addressed in one role.

Tutorial # 6 – define forbidden data elements

Up to now, only tables and their fields have been discussed. But, as already mentioned at the beginning, it is also possible to define particular data elements which are forbidden, independently of the database table being considered.
In the present tutorial we will demonstrate how this definition is carried out.

We call Table & Field Permissions and choose “Single User” and “Permissions and Roles” – as user we enter “*” (this is a conventional name for “all users”):



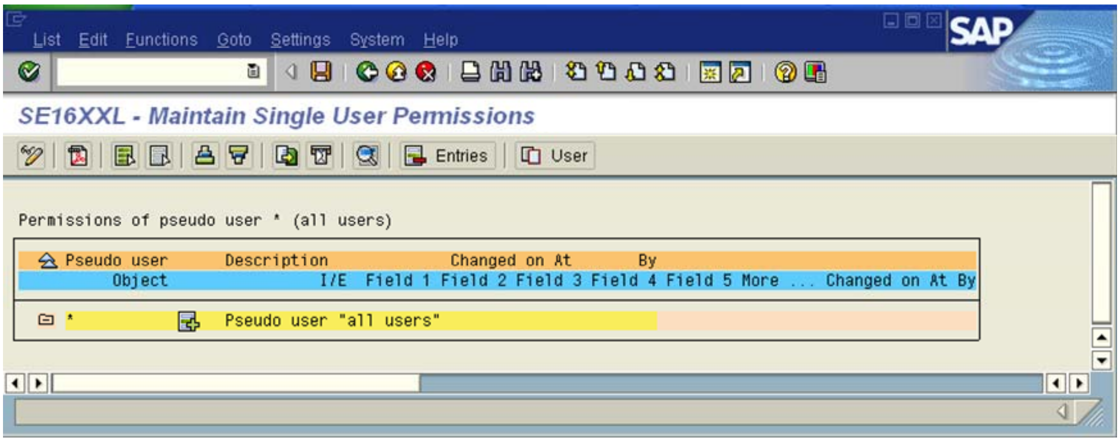
Selection

● Single User *

● Permissions and Roles

○ Allowed fields for table/view

User “*” is predefined and therefore does not need to be defined explicitly:

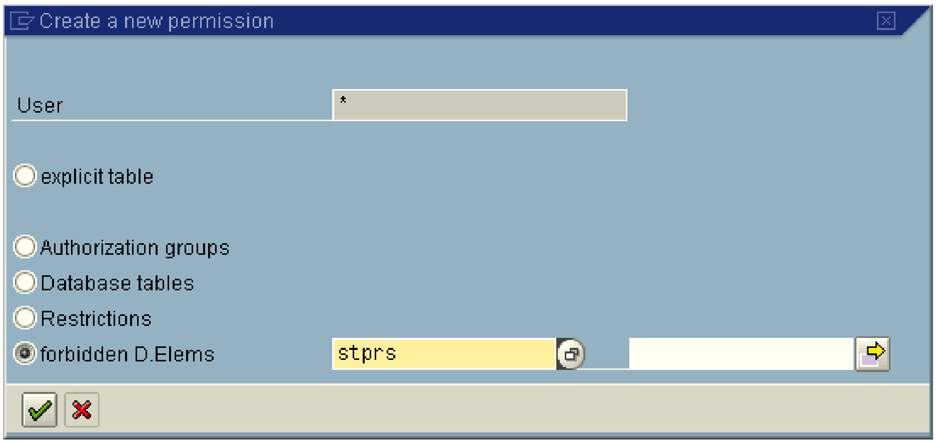


SE16XXL - Maintain Single User Permissions

Permissions of pseudo user * (all users)

Pseudo user	Description	Changed on At	By
Object	I/E Field 1 Field 2 Field 3 Field 4 Field 5 More ...	Changed on At	By
*	Pseudo user "all users"		

After clicking on at the right of the name, we choose “forbidden D.Elems”:



Create a new permission

User *

○ explicit table

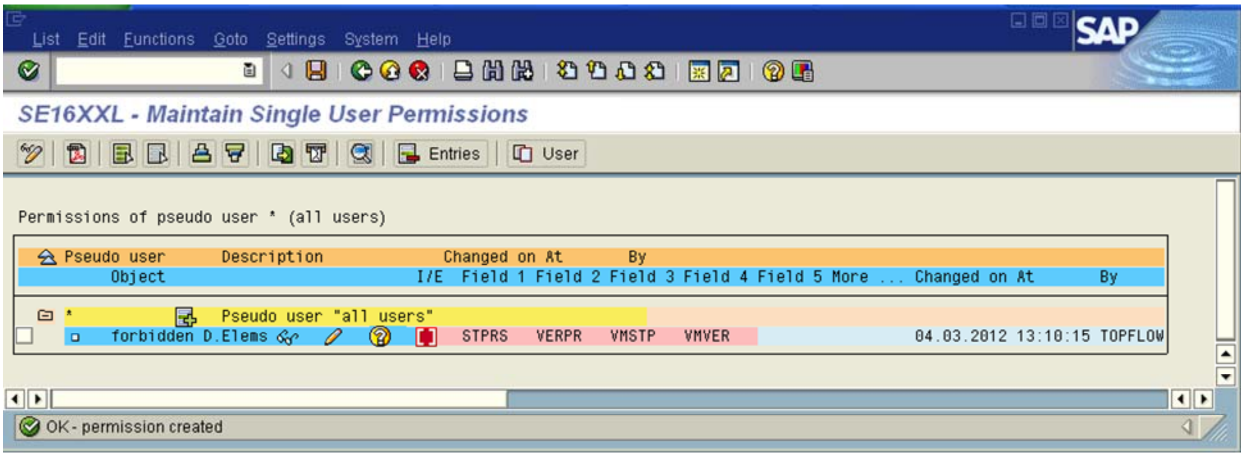
○ Authorization groups

○ Database tables

○ Restrictions

● forbidden D.Elems stprs

By means of the multiple selection button (⇨) more data elements can be entered. The result is:

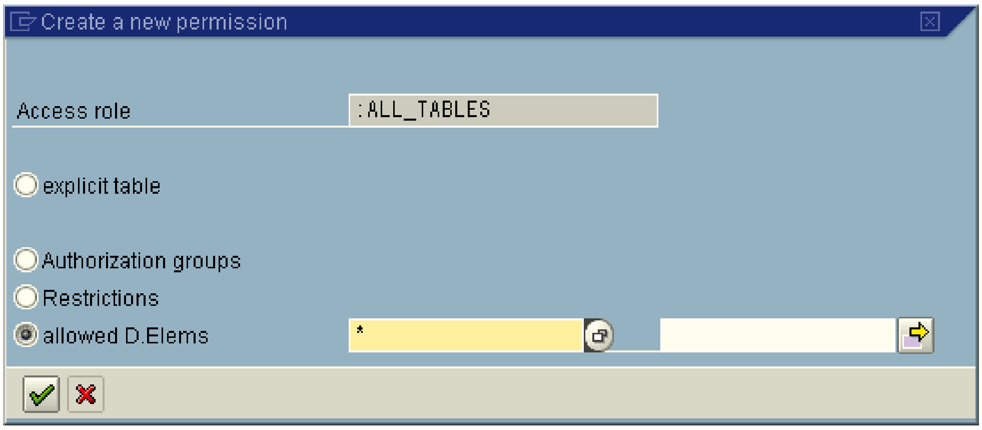

List Edit Functions Goto Settings System Help
SAP
SE16XXL - Maintain Single User Permissions
Entries
User

```
Permissions of pseudo user * (all users)

  Pseudo user       Description                  Changed on At         By
        Object                              I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At       By

  *                   Pseudo user "all users"
  □ forbidden D.Elems                             STPRS   VERPR   VMSTP   VMVER                   04.03.2012 13:10:15 TOPFLOW
```

OK - permission created

From now on, all database table fields associated with the forbidden data elements will not be visible to SE16XXL users.

Although some data elements have now been forbidden, it is still possible to allow them for particular access roles and/or users. To show how this is done we will enhance the previously defined role :ALL_TABLES by choosing “allowed D.Elems”:



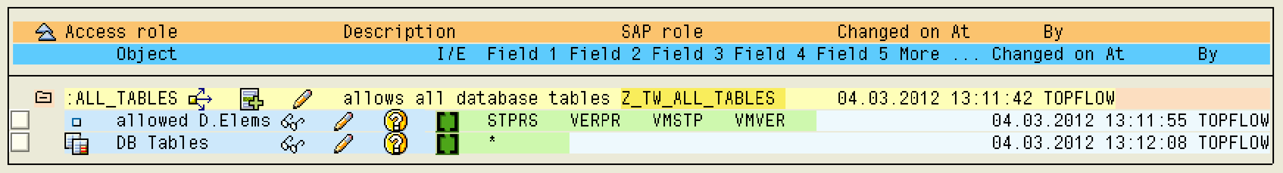
Create a new permission

Access role :ALL_TABLES

○ explicit table

○ Authorization groups
○ Restrictions
● allowed D.Elems *

The access role now presents itself as follows:



```
  Access role                 Description                SAP role          Changed on At        By
        Object                              I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At       By

  :ALL_TABLES                 allows all database tables Z_TW_ALL_TABLES   04.03.2012 13:11:42 TOPFLOW
  □ allowed D.Elems                               STPRS   VERPR   VMSTP   VMVER                   04.03.2012 13:11:55 TOPFLOW
    DB Tables                                     *                                               04.03.2012 13:12:08 TOPFLOW
```

These six tutorials should be sufficient to give you an idea of how the program works. We will now take a closer look at the various lists and functions of the tool.

General remarks

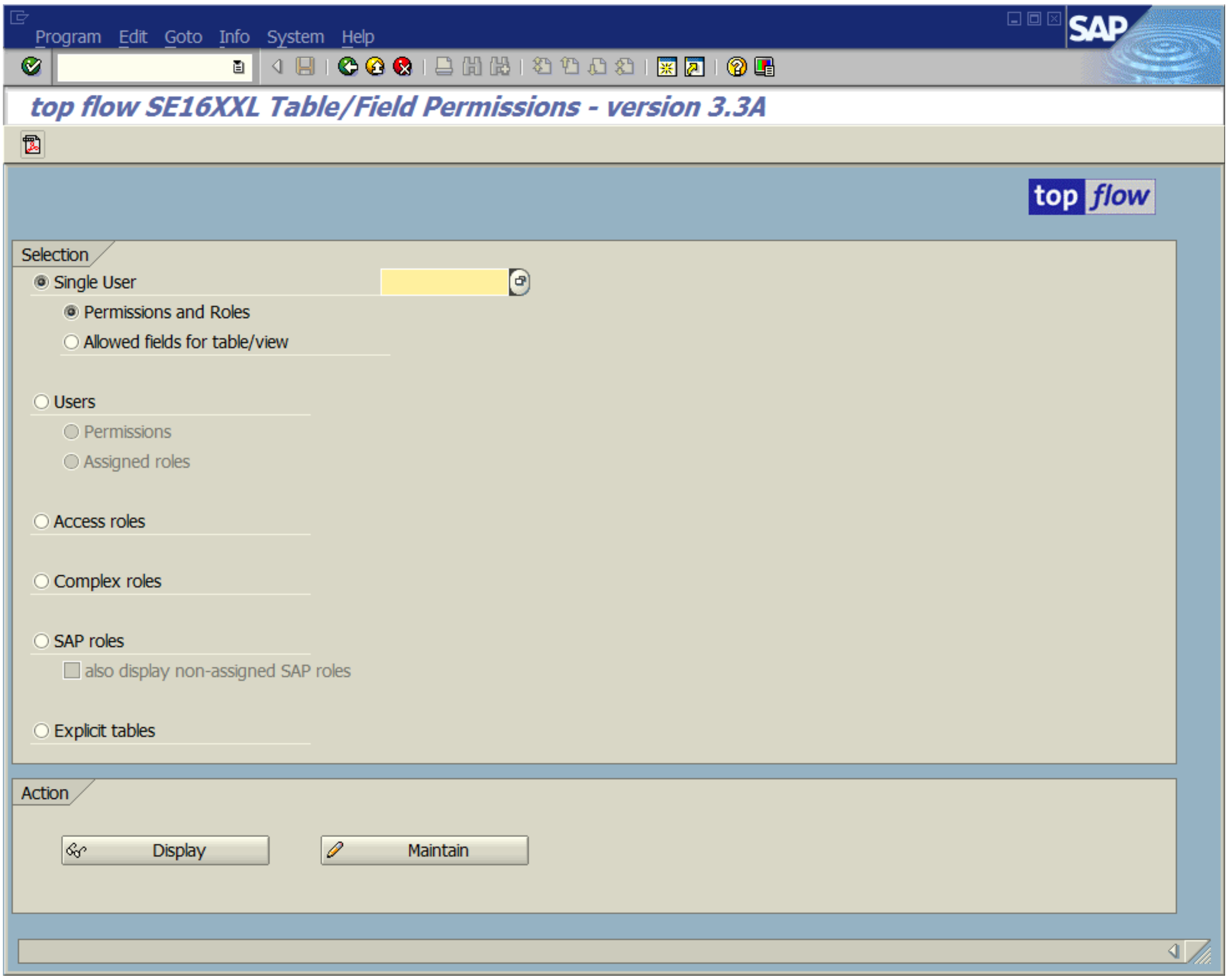
The program offers a series of lists each depicting a particular view of the permissions situation. Throughout these lists, icons are used to denote characteristics or functions. The most frequently used icons are listed below:

Icon	Meaning
▦	Explicit permission for a table and its fields
▤	Global permission – database table names
⌘	Global permission – authorization groups
☒	Global permission – restrictions
□	Forbidden (or allowed) data elements
[ ]	Selected items allowed
[■]	Selected items excluded
][	Forbidden data elements
👓	Display item in detail
⇨	Where used (X-ref)
?	List of tables (or data elements) selected by the permission
✎	Change item
⊞	Add new permission or assignment
⊟	Delete selected entries
🔍	Detailed list of the allowed fields of a table for a given user
🗋	Define a new user or access role
🗑	Delete a user or access role definition
▰	Existing SAP logon user
△	User not defined in SAP
◇	User defined in SE16XXL Permissions
⊕	Access role
✤	Complex role
⇄	Indirect assignment of a role through an SAP role
⊞	Field allowed
⊟	Field not allowed

All operations carried out in the program – except the ones performed externally using transactions **PFCG** or **SU01** – do not take effect until you **save your work** by pressing the 💾 button on the system function bar.

We will now begin with the description of the Table & Field Permission tool.

Selection Screen



top flow SE16XXL Table/Field Permissions - version 3.3A

Selection

● Single User

● Permissions and Roles

○ Allowed fields for table/view

○ Users

○ Permissions

○ Assigned roles

○ Access roles

○ Complex roles

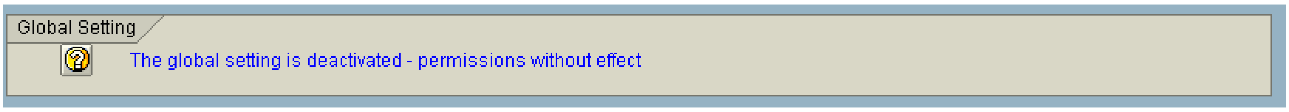
○ SAP roles

□ also display non-assigned SAP roles

○ Explicit tables

Action

If the associated global setting is deactivated, the following block will also be visible to warn you about the situation:


Global Setting

The global setting is deactivated - permissions without effect

This is just a warning – the maintenance of permissions is possible in any case.

Regardless of the button you press to start, either Display or Maintain, you can switch from maintenance to display mode (and vice versa) any time you wish by pressing the ✎ button on the application toolbar.

Single User – Permissions and Roles

Select this option for an overview of the permission situation of a particular user. The ensuing block list displays all related information.   More …

Single User – Allowed fields for table / view

This option is useful to get an overview of the permission situation of a particular user in regard to a single database table or view. The resulting list shows if the user has any permission at all, and if yes, how it is configured.   More …

Users – Permissions

Check this option to obtain a list of users and their directly associated permissions. This option is not relevant if you implement the new logic with SAP roles. More …

Users – Assigned roles

This option produces a list of users and their assigned access roles, both elementary and complex. Roles indirectly assigned through an SAP role are also shown. More …

Access roles

Select this option to obtain a list of elementary access roles and their associated permissions. This is the list you will probably use most often.   More …

Complex roles

This option produces a list of complex roles and their associated elementary roles. More …

SAP roles

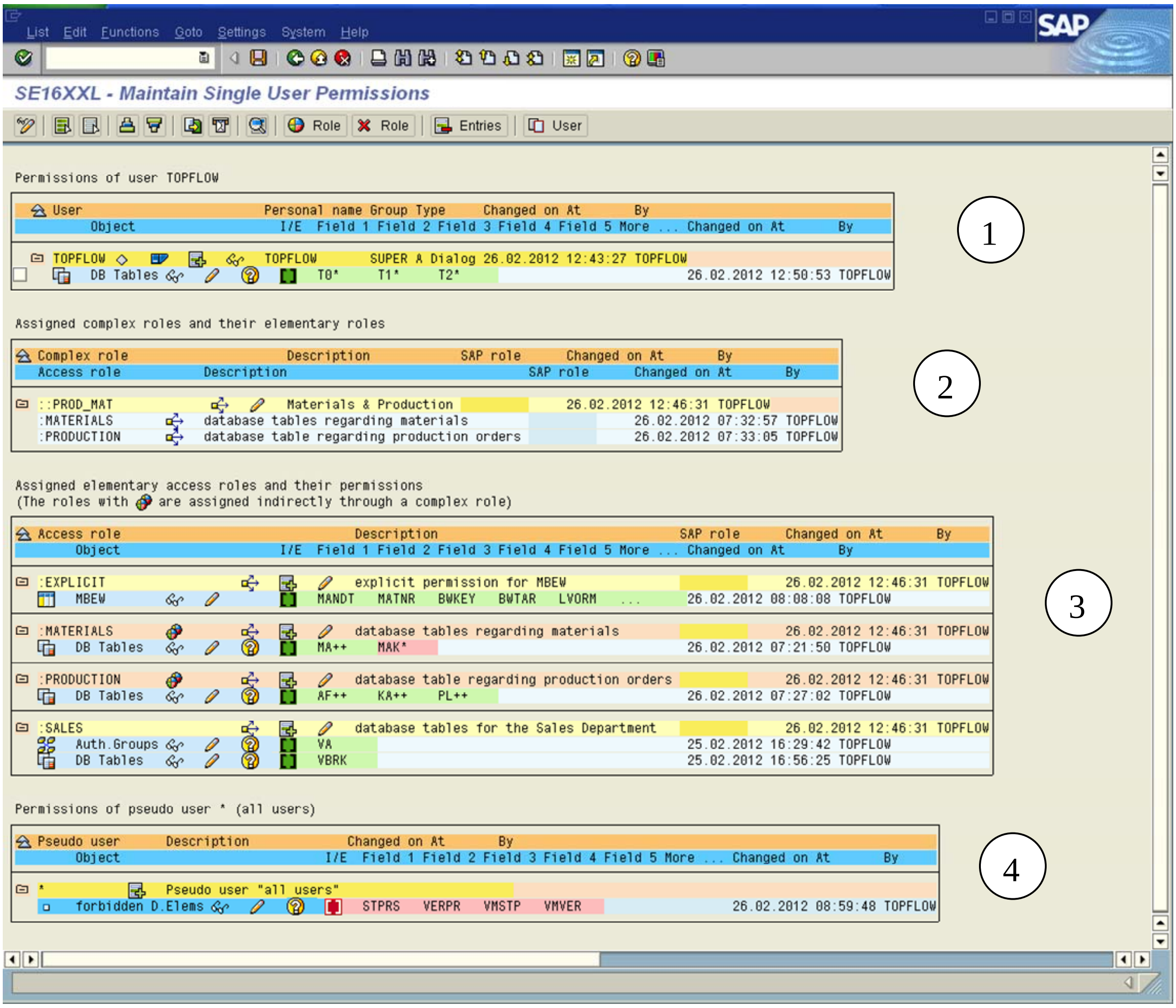
This option is only relevant if you wish to implement the new permission logic based on SAP roles. It shows selected SAP authorization roles together with the associated access roles.   More …

Explicit tables

Use this option to get an overview of all database tables that have an explicit permission.   More …

Single User – Permissions and Roles

A typical block list showing the permissions of a user might look like this:


List Edit Functions Goto Settings System Help
SAP
SE16XXL - Maintain Single User Permissions
Role
Role
Entries
User
1
2
3
4

```
Permissions of user TOPFLOW

 User                             Personal name Group Type      Changed on At         By
       Object                         I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At          By

 TOPFLOW                          TOPFLOW        SUPER A Dialog 26.02.2012 12:43:27 TOPFLOW
       DB Tables                           T0*     T1*     T2*                      26.02.2012 12:50:53 TOPFLOW

Assigned complex roles and their elementary roles

 Complex role                    Description              SAP role      Changed on At         By
 Access role          Description                                SAP role      Changed on At         By

 ::PROD_MAT                      Materials & Production                  26.02.2012 12:46:31 TOPFLOW
 :MATERIALS           database tables regarding materials                         26.02.2012 07:32:57 TOPFLOW
 :PRODUCTION          database table regarding production orders                  26.02.2012 07:33:05 TOPFLOW

Assigned elementary access roles and their permissions
(The roles with   are assigned indirectly through a complex role)

 Access role                                   Description                     SAP role      Changed on At         By
     Object                           I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At          By

 :EXPLICIT                                      explicit permission for MBEW                   26.02.2012 12:46:31 TOPFLOW
     MBEW                                  MANDT   MATNR   BWKEY   BWTAR   LVORM   ...  26.02.2012 08:08:08 TOPFLOW

 :MATERIALS                                     database tables regarding materials            26.02.2012 12:46:31 TOPFLOW
     DB Tables                             MA++    MAK*                                 26.02.2012 07:21:50 TOPFLOW

 :PRODUCTION                                    database table regarding production orders     26.02.2012 12:46:31 TOPFLOW
     DB Tables                             AF++    KA++    PL++                         26.02.2012 07:27:02 TOPFLOW

 :SALES                                         database tables for the Sales Department       26.02.2012 12:46:31 TOPFLOW
     Auth.Groups                           VA                                           25.02.2012 16:29:42 TOPFLOW
     DB Tables                             VBRK                                         25.02.2012 16:56:25 TOPFLOW

Permissions of pseudo user * (all users)

 Pseudo user      Description               Changed on At         By
     Object                                 I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At          By

 *                Pseudo user "all users"
     forbidden D.Elems                           STPRS   VERPR   VMSTP   VMVER                 26.02.2012 08:59:48 TOPFLOW
```

Four blocks are visible:

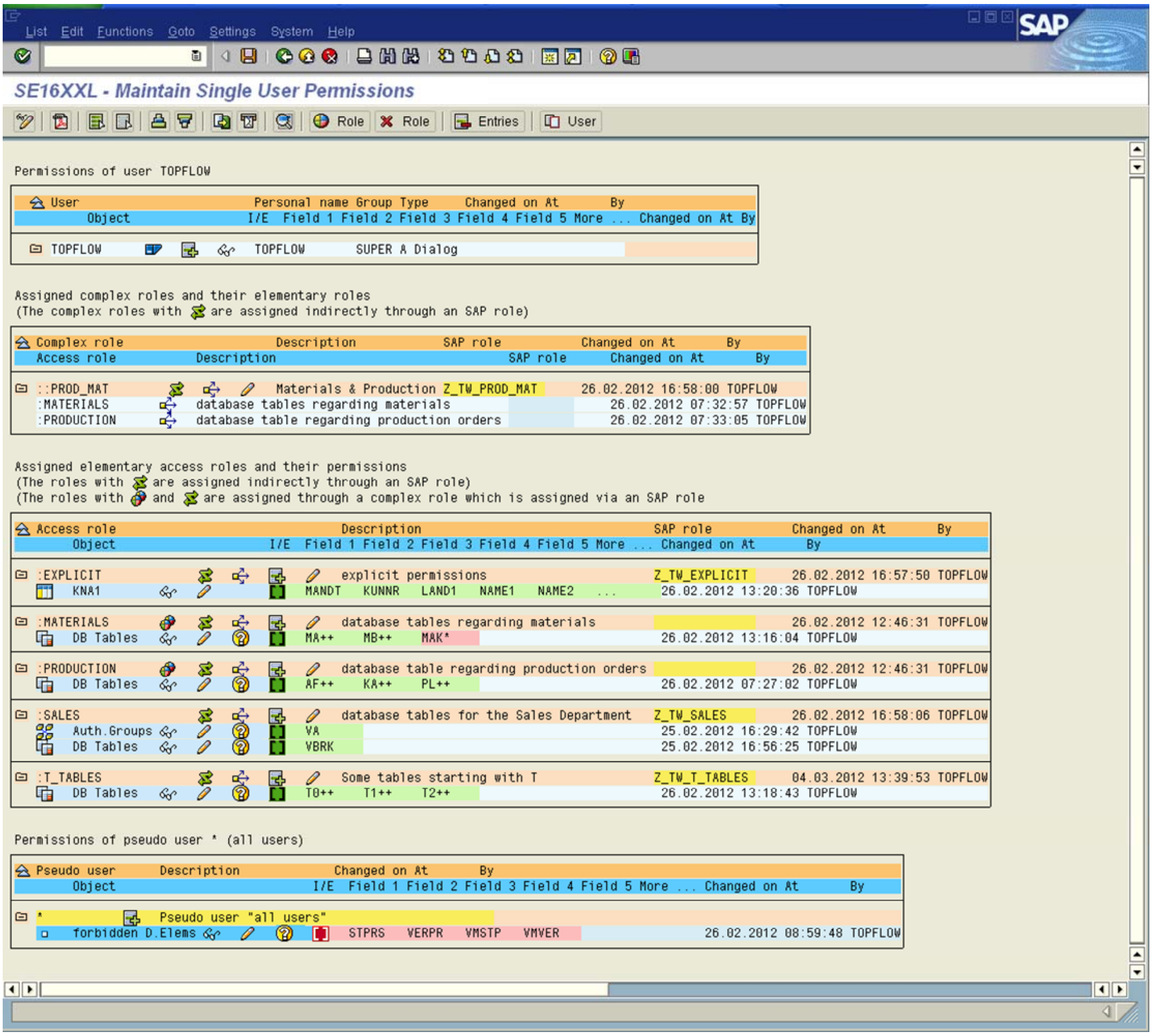
1) the definition of the user and the directly assigned permissions;

2) a list of assigned complex roles, if any;

3) a list of assigned elementary roles – possibly assigned by means of complex roles;

4) the permissions of pseudo user “*” (all users).

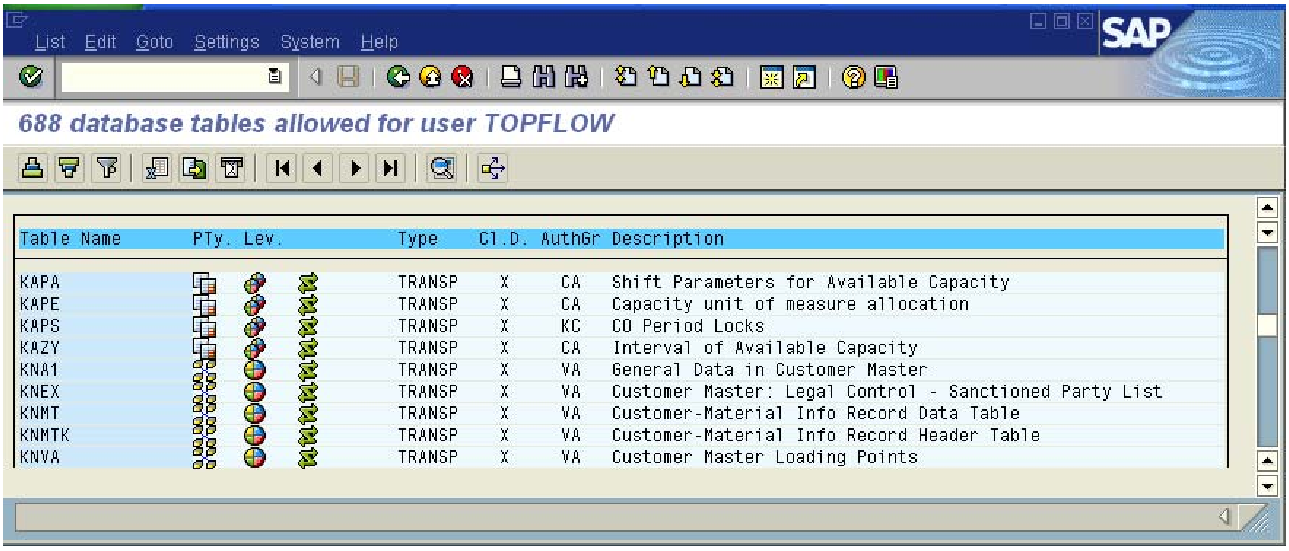
The above example implies the direct assignment of permissions and roles.
An implementation involving SAP roles would present a slightly different picture:


List Edit Functions Goto Settings System Help
SAP
SE16XXL - Maintain Single User Permissions
Role
Role
Entries
User

```
Permissions of user TOPFLOW

 User                          Personal name Group Type     Changed on At        By
        Object                I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At By

 TOPFLOW                      TOPFLOW       SUPER A Dialog

Assigned complex roles and their elementary roles
(The complex roles with  are assigned indirectly through an SAP role)

 Complex role                  Description          SAP role          Changed on At        By
 Access role          Description                             SAP role          Changed on At        By

 ::PROD_MAT                    Materials & Production Z_TW_PROD_MAT   26.02.2012 16:58:00 TOPFLOW
 :MATERIALS           database tables regarding materials                      26.02.2012 07:32:57 TOPFLOW
 :PRODUCTION          database table regarding production orders               26.02.2012 07:33:05 TOPFLOW

Assigned elementary access roles and their permissions
(The roles with  are assigned indirectly through an SAP role)
(The roles with  and  are assigned through a complex role which is assigned via an SAP role

 Access role                             Description                      SAP role          Changed on At        By
        Object                        I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At        By

 :EXPLICIT                            explicit permissions              Z_TW_EXPLICIT     26.02.2012 16:57:50 TOPFLOW
      KNA1                            MANDT   KUNNR   LAND1   NAME1   NAME2   ...     26.02.2012 13:20:36 TOPFLOW

 :MATERIALS                           database tables regarding materials                 26.02.2012 12:46:31 TOPFLOW
      DB Tables                       MA++    MB++    MAK*                            26.02.2012 13:16:04 TOPFLOW

 :PRODUCTION                          database table regarding production orders          26.02.2012 12:46:31 TOPFLOW
      DB Tables                       AF++    KA++    PL++                            26.02.2012 07:27:02 TOPFLOW

 :SALES                               database tables for the Sales Department Z_TW_SALES 26.02.2012 16:58:06 TOPFLOW
      Auth.Groups                     VA                                              25.02.2012 16:29:42 TOPFLOW
      DB Tables                       VBRK                                            25.02.2012 16:56:25 TOPFLOW

 :T_TABLES                            Some tables starting with T       Z_TW_T_TABLES     04.03.2012 13:39:53 TOPFLOW
      DB Tables                       T0++    T1++    T2++                            26.02.2012 13:18:43 TOPFLOW

Permissions of pseudo user * (all users)

 Pseudo user       Description             Changed on At        By
        Object                       I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At        By

 *                 Pseudo user "all users"
      forbidden D.Elems               STPRS   VERPR   VMSTP   VMVER                        26.02.2012 08:59:48 TOPFLOW
```

NOTE: when using SAP roles, the actual assignment is carried out by means of transaction **PFCG** (or **SU01**). As a consequence, the assignment functions available in the present list – like Role and ✖ Role – are irrelevant and should not be used.

The above described overview is useful to get an idea of the permissions of a single user. But it would be difficult to deduce from it exactly which database tables are allowed for the user in question.
To this end the menu function ***Functions → List all allowed tables*** is available.
In our example, it produces the following list:

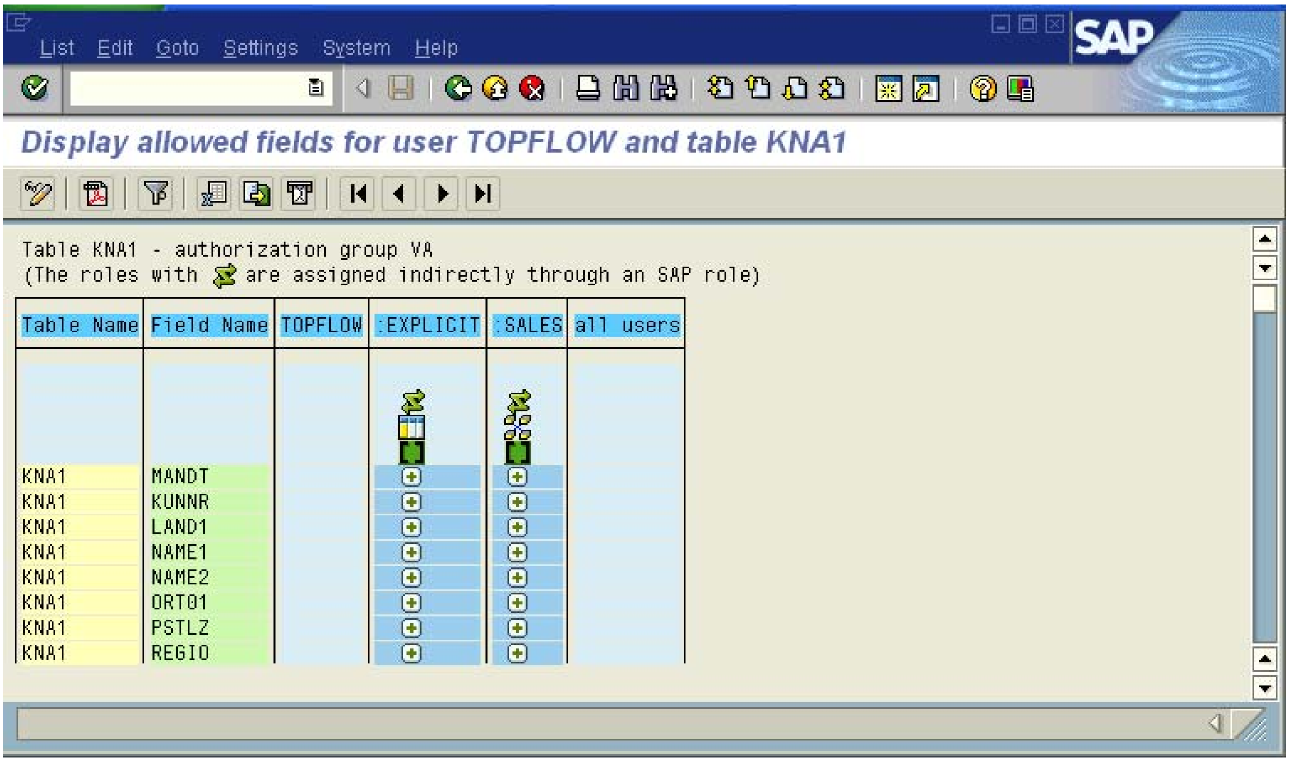


688 database tables allowed for user TOPFLOW

Table Name	PTy.	Lev.		Type	Cl.D.	AuthGr	Description
KAPA				TRANSP	X	CA	Shift Parameters for Available Capacity
KAPE				TRANSP	X	CA	Capacity unit of measure allocation
KAPS				TRANSP	X	KC	CO Period Locks
KAZY				TRANSP	X	CA	Interval of Available Capacity
KNA1				TRANSP	X	VA	General Data in Customer Master
KNEX				TRANSP	X	VA	Customer Master: Legal Control - Sanctioned Party List
KNMT				TRANSP	X	VA	Customer-Material Info Record Data Table
KNMTK				TRANSP	X	VA	Customer-Material Info Record Header Table
KNVA				TRANSP	X	VA	Customer Master Loading Points

Table KNA1 is a good example of what happens when a table is addressed by more than one role. It has an explicit permission in role :EXPLICIT, but also a global permission in role :SALES (through authorization group VA). As already stated, the widest permission is taken.

Use the button to get a detailed picture of the situation:



Display allowed fields for user TOPFLOW and table KNA1

Table KNA1 - authorization group VA
(The roles with are assigned indirectly through an SAP role)

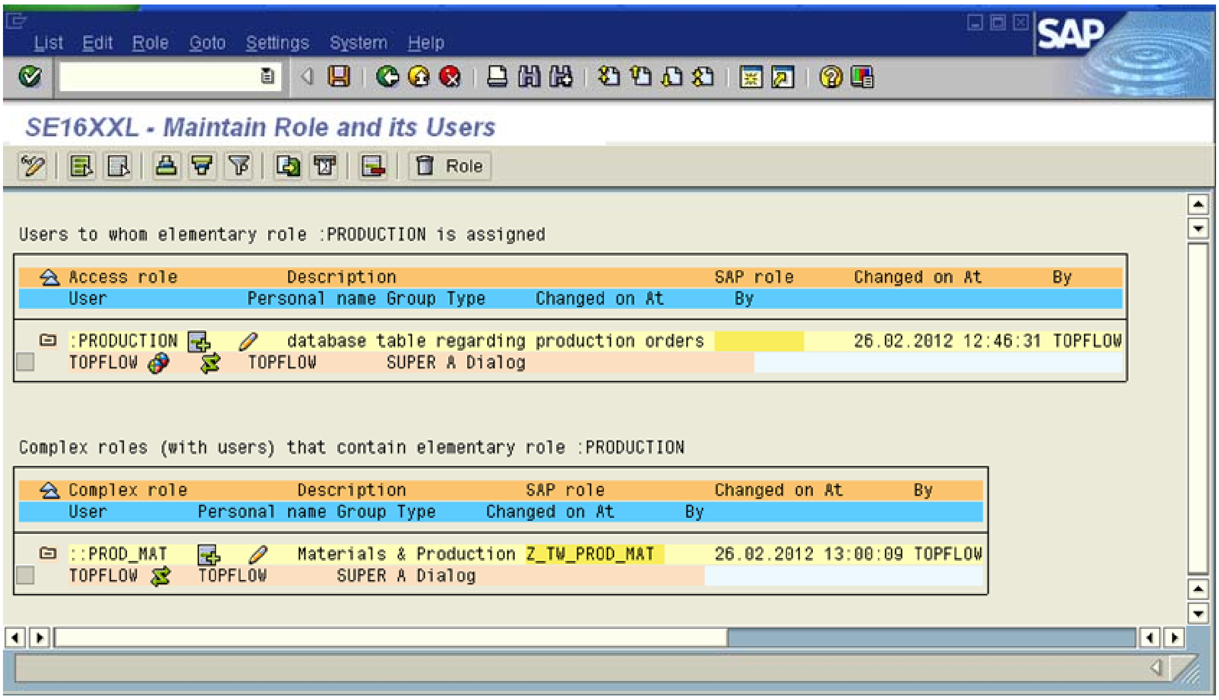
Table Name	Field Name	TOPFLOW	:EXPLICIT	:SALES	all users
KNA1	MANDT		⊕	⊕	
KNA1	KUNNR		⊕	⊕	
KNA1	LAND1		⊕	⊕	
KNA1	NAME1		⊕	⊕	
KNA1	NAME2		⊕	⊕	
KNA1	ORT01		⊕	⊕	
KNA1	PSTLZ		⊕	⊕	
KNA1	REGIO		⊕	⊕	

The green fields are allowed.

Navigation

It is possible to navigate from one list to another. This is useful to get a better picture of the current permissions situation. In our example of user TOPFLOW, you may navigate to the definition of complex role ::PROD_MAT by just clicking on the name. The same applies to the elementary roles.

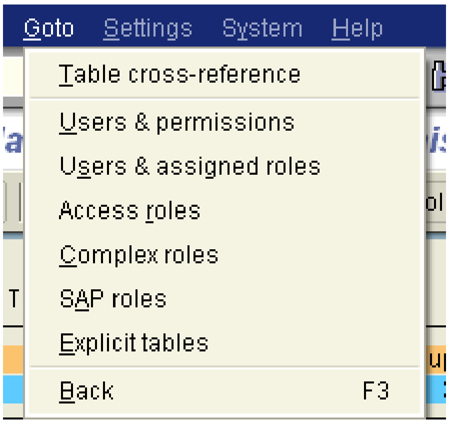
Even more interesting are the “where used” lists, which can be reached by clicking on the corresponding icon.
If for example you do this for access role :PRODUCTION, you will get the following list, showing both the assigned users and the associated complex role(s):



SE16XXL - Maintain Role and its Users

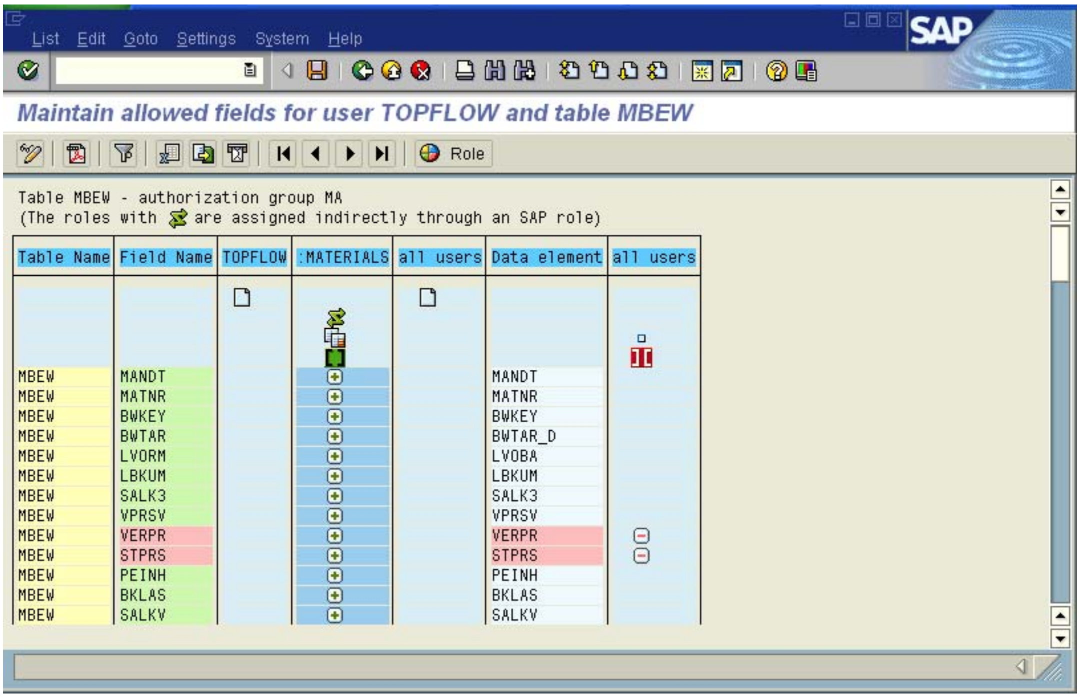
```
Users to whom elementary role :PRODUCTION is assigned

Access role         Description                            SAP role      Changed on At        By
User                Personal name Group Type     Changed on At        By

:PRODUCTION         database table regarding production orders           26.02.2012 12:46:31 TOPFLOW
TOPFLOW             TOPFLOW       SUPER A Dialog


Complex roles (with users) that contain elementary role :PRODUCTION

Complex role            Description             SAP role            Changed on At        By
User              Personal name Group Type     Changed on At        By

::PROD_MAT              Materials & Production  Z_TW_PROD_MAT       26.02.2012 13:00:09 TOPFLOW
TOPFLOW           TOPFLOW       SUPER A Dialog
```

Another possibility is to make use of the ***Goto*** menu functions:



Single User – Allowed fields for table / view

This function is also available in most lists (button). It provides you with a detailed list of the fields of the table in question – showing which are allowed and which are not, and why.
We will make an example with user TOPFLOW and table MBEW:



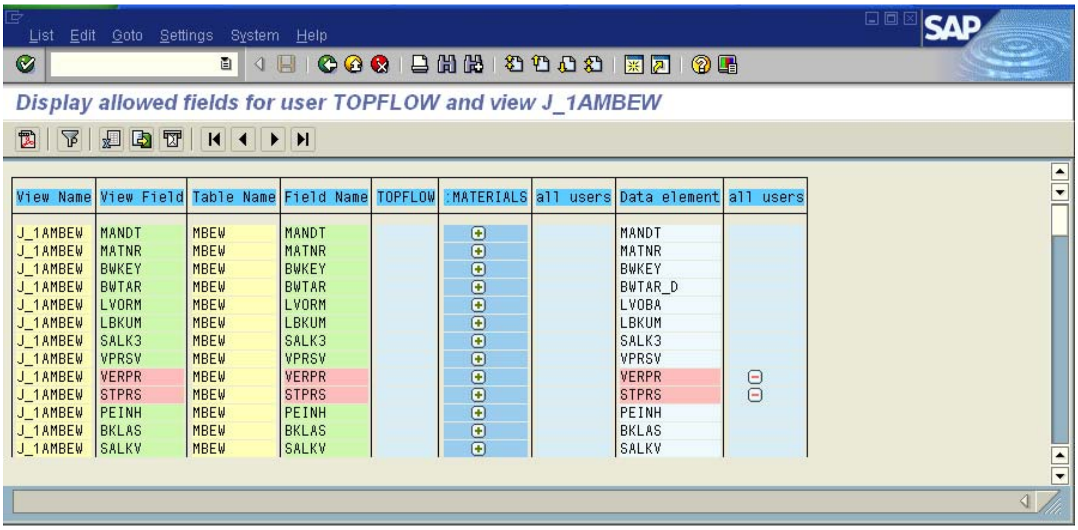
Maintain allowed fields for user TOPFLOW and table MBEW

Table MBEW - authorization group MA
(The roles with are assigned indirectly through an SAP role)

Table Name	Field Name	TOPFLOW	:MATERIALS	all users	Data element	all users
MBEW	MANDT		⊕		MANDT	
MBEW	MATNR		⊕		MATNR	
MBEW	BWKEY		⊕		BWKEY	
MBEW	BWTAR		⊕		BWTAR_D	
MBEW	LVORM		⊕		LVOBA	
MBEW	LBKUM		⊕		LBKUM	
MBEW	SALK3		⊕		SALK3	
MBEW	VPRSV		⊕		VPRSV	
MBEW	VERPR		⊕		VERPR	⊖
MBEW	STPRS		⊕		STPRS	⊖
MBEW	PEINH		⊕		PEINH	
MBEW	BKLAS		⊕		BKLAS	
MBEW	SALKV		⊕		SALKV	

The fields in red are not allowed.

A similar list can also be produced for a view (only in display mode):

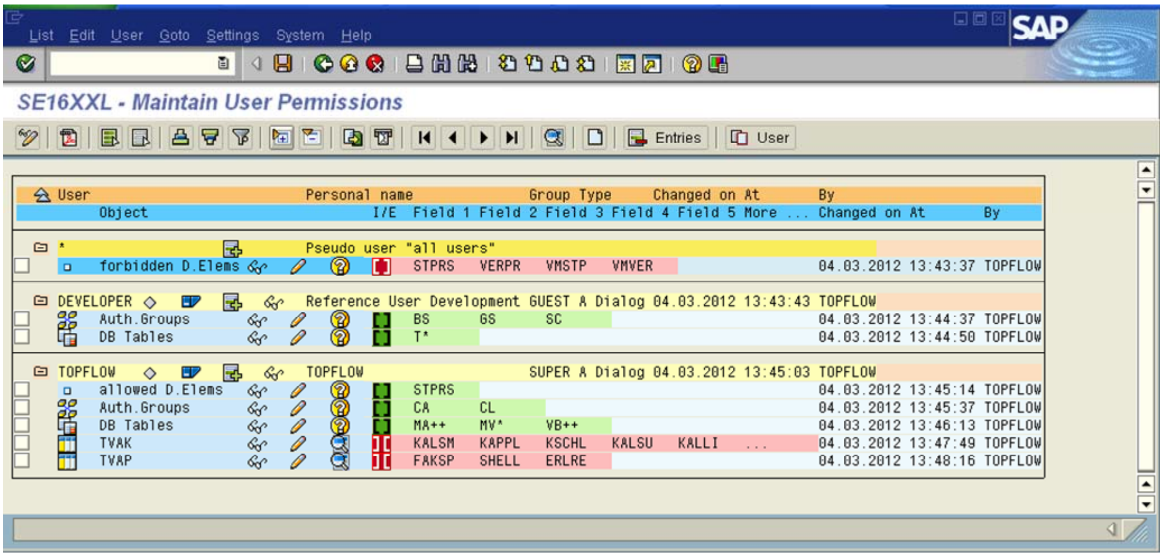


Display allowed fields for user TOPFLOW and view J_1AMBEW

View Name	View Field	Table Name	Field Name	TOPFLOW	:MATERIALS	all users	Data element	all users
J_1AMBEW	MANDT	MBEW	MANDT		⊕		MANDT	
J_1AMBEW	MATNR	MBEW	MATNR		⊕		MATNR	
J_1AMBEW	BWKEY	MBEW	BWKEY		⊕		BWKEY	
J_1AMBEW	BWTAR	MBEW	BWTAR		⊕		BWTAR_D	
J_1AMBEW	LVORM	MBEW	LVORM		⊕		LVOBA	
J_1AMBEW	LBKUM	MBEW	LBKUM		⊕		LBKUM	
J_1AMBEW	SALK3	MBEW	SALK3		⊕		SALK3	
J_1AMBEW	VPRSV	MBEW	VPRSV		⊕		VPRSV	
J_1AMBEW	VERPR	MBEW	VERPR		⊕		VERPR	⊖
J_1AMBEW	STPRS	MBEW	STPRS		⊕		STPRS	⊖
J_1AMBEW	PEINH	MBEW	PEINH		⊕		PEINH	
J_1AMBEW	BKLAS	MBEW	BKLAS		⊕		BKLAS	
J_1AMBEW	SALKV	MBEW	SALKV		⊕		SALKV	

Users – Permissions

A list of the defined users and their permissions might look like the following:



SE16XXL - Maintain User Permissions

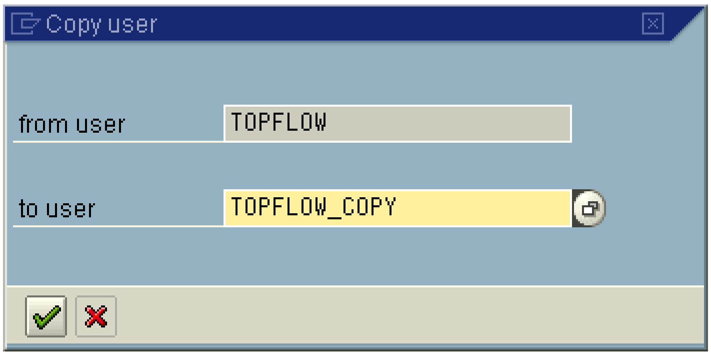
```
User                        Personal name            Group Type     Changed on At         By
      Object                        I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At       By

*                           Pseudo user "all users"
      forbidden D.Elems                  STPRS   VERPR   VMSTP   VMVER                    04.03.2012 13:43:37 TOPFLOW

DEVELOPER                   Reference User Development GUEST A Dialog 04.03.2012 13:43:43 TOPFLOW
      Auth.Groups                        BS      GS      SC                               04.03.2012 13:44:37 TOPFLOW
      DB Tables                          T*                                               04.03.2012 13:44:50 TOPFLOW

TOPFLOW                     TOPFLOW                    SUPER A Dialog 04.03.2012 13:45:03 TOPFLOW
      allowed D.Elems                    STPRS                                            04.03.2012 13:45:14 TOPFLOW
      Auth.Groups                        CA      CL                                       04.03.2012 13:45:37 TOPFLOW
      DB Tables                          MA++    MV*     VB++                             04.03.2012 13:46:13 TOPFLOW
      TVAK                               KALSM   KAPPL   KSCHL   KALSU   KALLI   ...      04.03.2012 13:47:49 TOPFLOW
      TVAP                               FAKSP   SHELL   ERLRE                            04.03.2012 13:48:16 TOPFLOW
```

This list only shows the permissions assigned directly to users. Permissions that are derived from assigned access roles are not displayed here.

IMPORTANT: If you are implementing the permission logic based on SAP roles this list should contain at most the pseudo user **"*"**, which is predefined. No other users should be visible.

Making a copy of a user

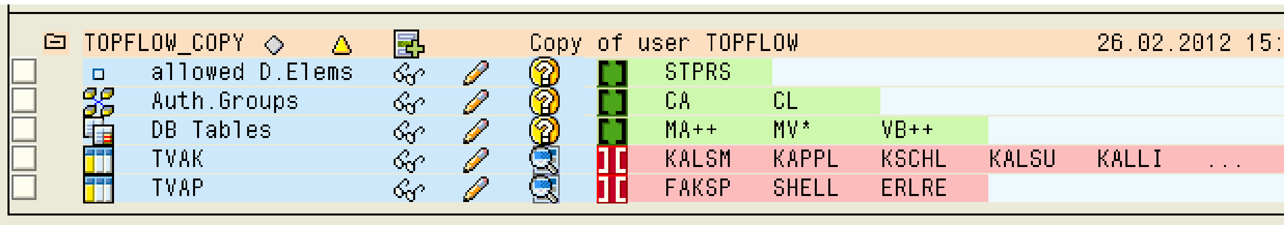
Before changing the permissions of a user it may be a good idea to make a copy in order to be able to undo the changes if something goes wrong.
Use function User to perform this operation. A **non-existing user** is best entered as target:



from user TOPFLOW

to user TOPFLOW_COPY

The copy has the same permissions as the original user:

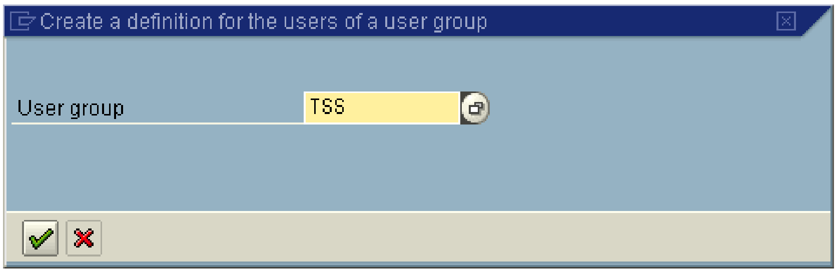


```
TOPFLOW_COPY                     Copy of user TOPFLOW                 26.02.2012 15:
  allowed D.Elems                STPRS
  Auth.Groups                    CA     CL
  DB Tables                      MA++   MV*    VB++
  TVAK                           KALSM  KAPPL  KSCHL  KALSU  KALLI  ...
  TVAP                           FAKSP  SHELL  ERLRE
```

NOTE: not only the permissions of the original user but also the assigned access roles, both elementary and complex, are copied. This does not apply to roles indirectly assigned through SAP roles, because these assignments lie outside of the responsibility of this tool.

Defining many users in one operation

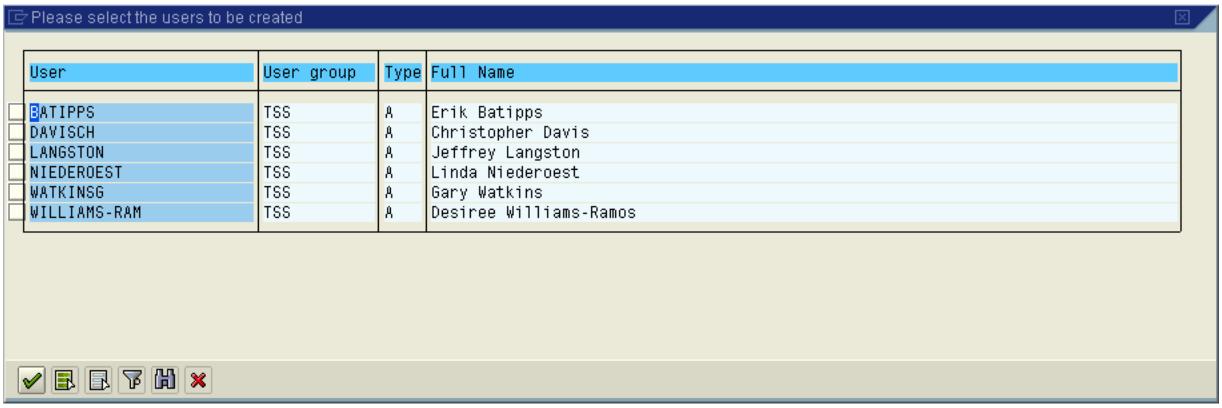
It may sometimes be necessary to create a definition for many users. Doing this one at a time can be cumbersome. But there is a faster way – menu function ***Users → Create a def. for the users of a group***:



Create a definition for the users of a user group

User group: TSS

From the ensuing list you may select the users to be defined:



Please select the users to be created

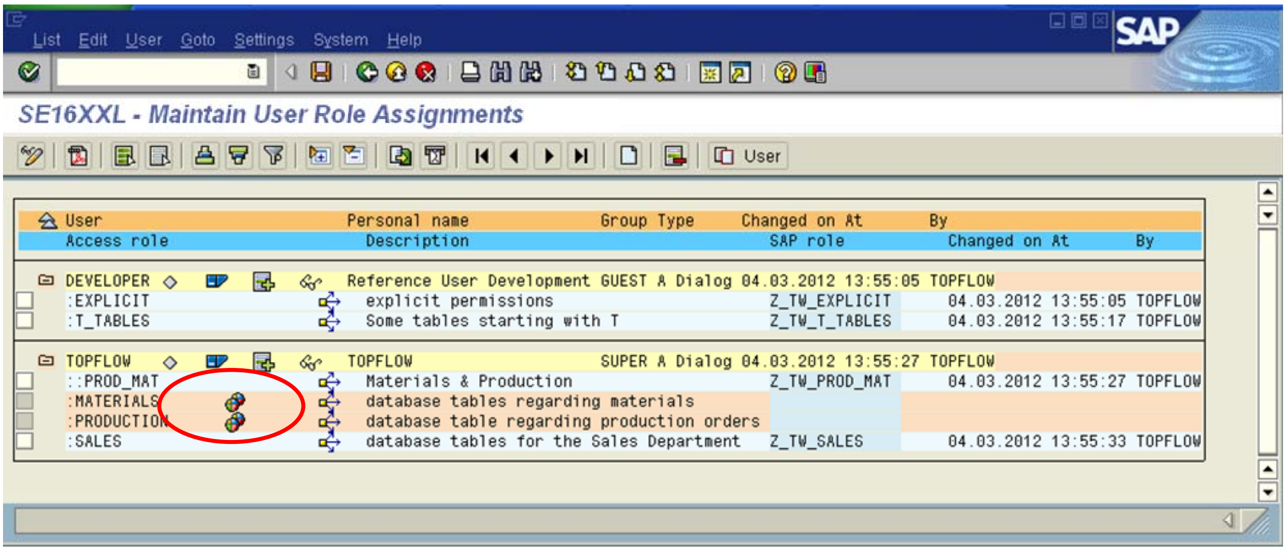
User	User group	Type	Full Name
□ BATIPPS	TSS	A	Erik Batipps
□ DAVISCH	TSS	A	Christopher Davis
□ LANGSTON	TSS	A	Jeffrey Langston
□ NIEDEROEST	TSS	A	Linda Niederoest
□ WATKINSG	TSS	A	Gary Watkins
□ WILLIAMS-RAM	TSS	A	Desiree Williams-Ramos

As already mentioned, this functionality is not needed if you implement the permission logic based on SAP roles.

Users – Assigned roles

This list is always important, because however you implement your permission logic, you always get an overview of the involved users and their (directly or indirectly) assigned access roles.

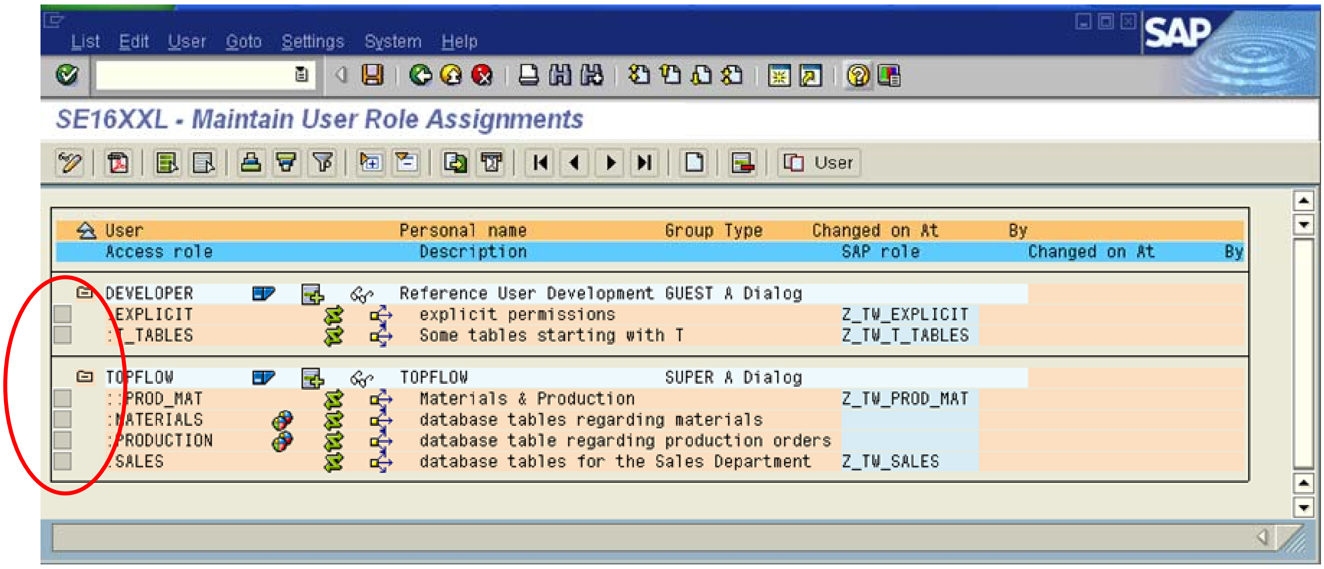
With directly assigned access roles the list might be similar to the following:



SE16XXL - Maintain User Role Assignments

```
User                          Personal name             Group Type   Changed on At         By
    Access role                   Description                    SAP role      Changed on At        By

DEVELOPER                     Reference User Development GUEST A Dialog 04.03.2012 13:55:05 TOPFLOW
□  :EXPLICIT                      explicit permissions           Z_TW_EXPLICIT  04.03.2012 13:55:05 TOPFLOW
□  :T_TABLES                      Some tables starting with T    Z_TW_T_TABLES  04.03.2012 13:55:17 TOPFLOW

TOPFLOW                       TOPFLOW                   SUPER A Dialog 04.03.2012 13:55:27 TOPFLOW
□  ::PROD_MAT                     Materials & Production         Z_TW_PROD_MAT  04.03.2012 13:55:27 TOPFLOW
□  :MATERIALS                     database tables regarding materials
□  :PRODUCTION                    database table regarding production orders
□  :SALES                         database tables for the Sales Department Z_TW_SALES 04.03.2012 13:55:33 TOPFLOW
```

Notice the elementary roles assigned by means of a complex role (🔗).
The same list using SAP roles would look like this:



SE16XXL - Maintain User Role Assignments

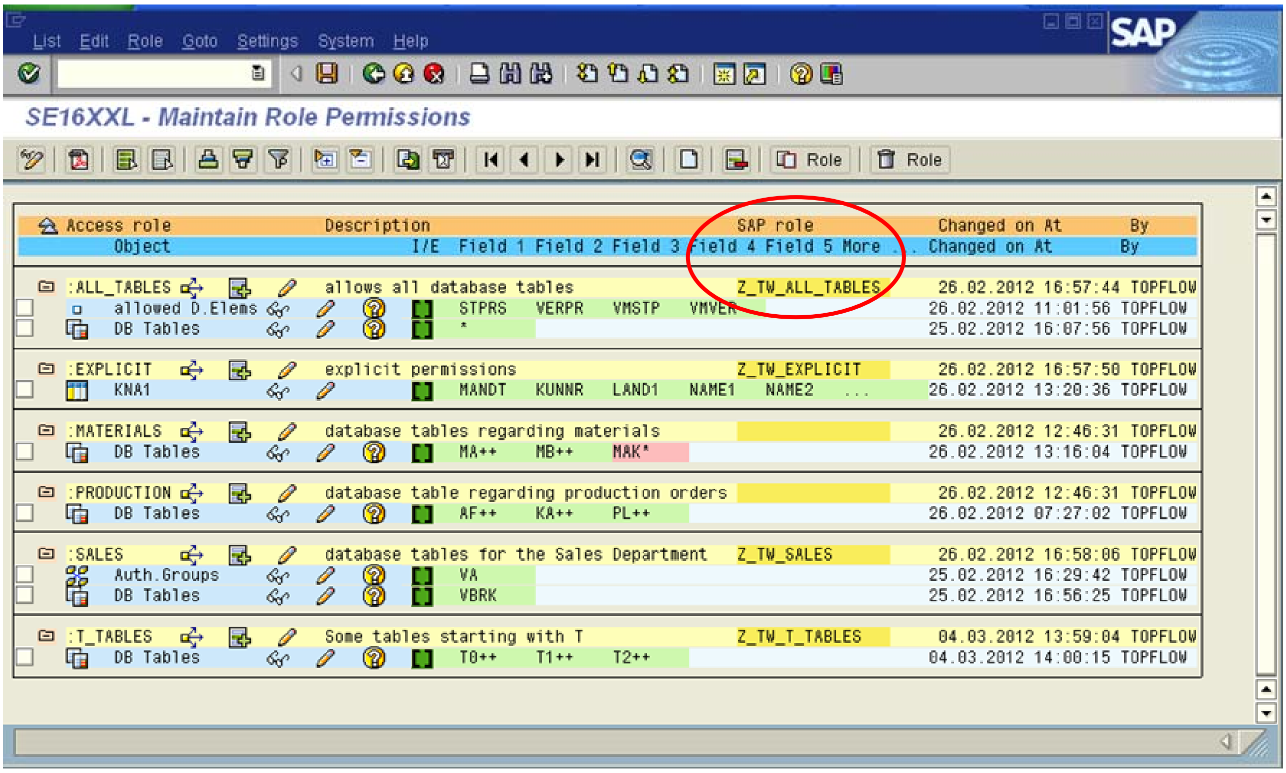
```
User                          Personal name             Group Type   Changed on At         By
    Access role                   Description                    SAP role      Changed on At        By

DEVELOPER                     Reference User Development GUEST A Dialog
□  :EXPLICIT                      explicit permissions           Z_TW_EXPLICIT
□  :T_TABLES                      Some tables starting with T    Z_TW_T_TABLES

TOPFLOW                       TOPFLOW                   SUPER A Dialog
□  ::PROD_MAT                     Materials & Production         Z_TW_PROD_MAT
□  :MATERIALS                     database tables regarding materials
□  :PRODUCTION                    database table regarding production orders
□  :SALES                         database tables for the Sales Department Z_TW_SALES
```

Notice in this case that none of the assignments are selectable, because the assignments are carried out externally to the program using transaction **PFCG**.

Access roles

This is the most important list of the permission tool. If you implement the permissions using SAP roles, you need to define access roles with the related permissions. If you choose the original modus operandi instead, you might do without access roles, but this is not advisable. So regardless of your implementation, you will most certainly create a series of access roles with well defined permissions.

A typical list of access roles might have the following appearance:



SE16XXL - Maintain Role Permissions

```
  Access role                    Description                           SAP role        Changed on At        By
      Object                     I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More . . Changed on At        By

  :ALL_TABLES                    allows all database tables            Z_TW_ALL_TABLES  26.02.2012 16:57:44 TOPFLOW
□     allowed D.Elems                 STPRS   VERPR   VMSTP   VMVER                    26.02.2012 11:01:56 TOPFLOW
□     DB Tables                       *                                                25.02.2012 16:07:56 TOPFLOW

  :EXPLICIT                      explicit permissions                  Z_TW_EXPLICIT    26.02.2012 16:57:50 TOPFLOW
□     KNA1                            MANDT   KUNNR   LAND1   NAME1   NAME2   . . .    26.02.2012 13:20:36 TOPFLOW

  :MATERIALS                     database tables regarding materials                    26.02.2012 12:46:31 TOPFLOW
□     DB Tables                       MA++    MB++    MAK*                             26.02.2012 13:16:04 TOPFLOW

  :PRODUCTION                    database table regarding production orders             26.02.2012 12:46:31 TOPFLOW
□     DB Tables                       AF++    KA++    PL++                             26.02.2012 07:27:02 TOPFLOW

  :SALES                         database tables for the Sales Department Z_TW_SALES    26.02.2012 16:58:06 TOPFLOW
□     Auth.Groups                     VA                                               25.02.2012 16:29:42 TOPFLOW
□     DB Tables                       VBRK                                             25.02.2012 16:56:25 TOPFLOW

  :T_TABLES                      Some tables starting with T           Z_TW_T_TABLES    04.03.2012 13:59:04 TOPFLOW
□     DB Tables                       T0++    T1++    T2++                             04.03.2012 14:00:15 TOPFLOW
```

The attribute “**SAP role**” is only necessary if you implement the new logic.

Since this list is probably the one used most often, we will take a closer look at the available functions.

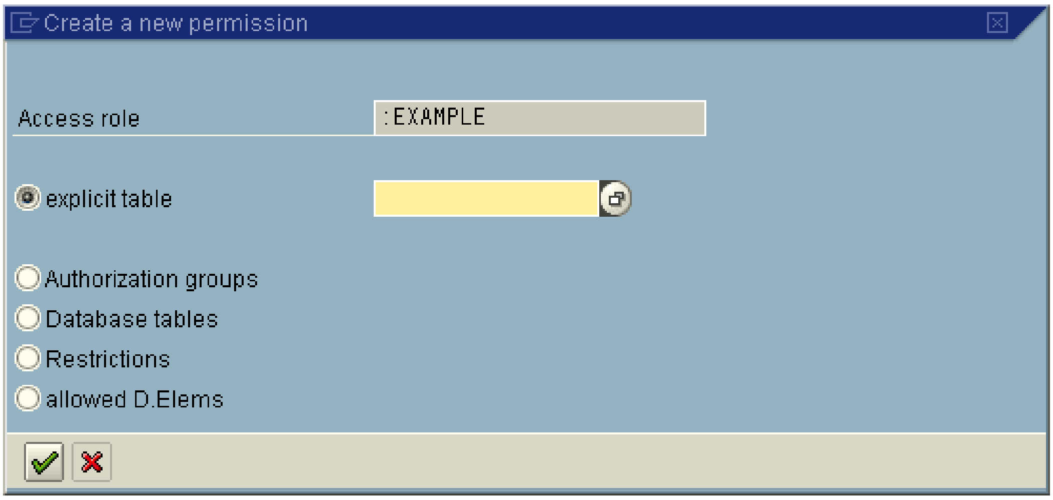
We will begin with the functions needed to create, change, copy and delete access roles. Some functions are available as buttons on the application toolbar.

Functions pertaining to access roles

Function	Description
	Display assignments of a role (the icon is at the right of the role)
□	Create a new access role definition
✎	Change an existing access role (icon at the right of the role)
Role	Copy an existing role with its permissions. The direct assignments to users are not copied. The SAP role attribute of the original role is not copied.
Role	Delete an access role with all permissions and assignments
Role → Delete many roles	Menu function to delete many access roles in one operation

Adding permissions to an access role

Click on the icon at the right of a role to add a new kind of permission to it. The first time, when the role is brand new, the ensuing popup looks like the following:



Create a new permission

Access role :EXAMPLE

● explicit table

○ Authorization groups

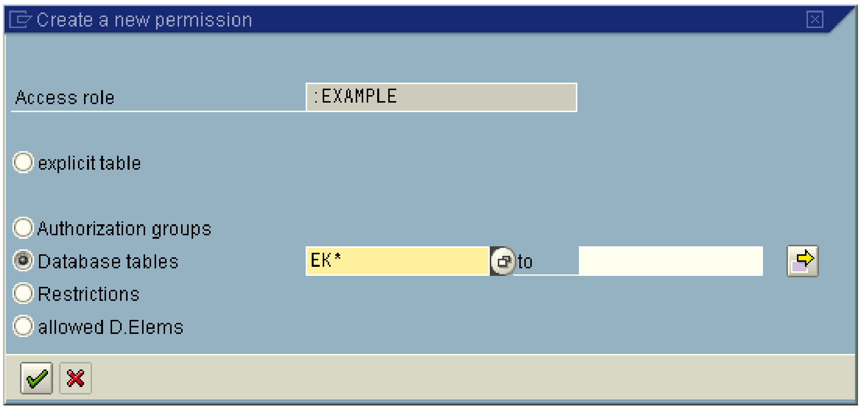
○ Database tables

○ Restrictions

○ allowed D.Elems

All kinds of permissions are available to be chosen.

Suppose you choose "Database tables", i.e. you wish to select the tables by name:



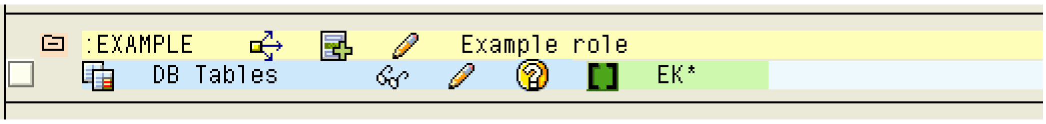
Create a new permission

Access role :EXAMPLE

○ explicit table

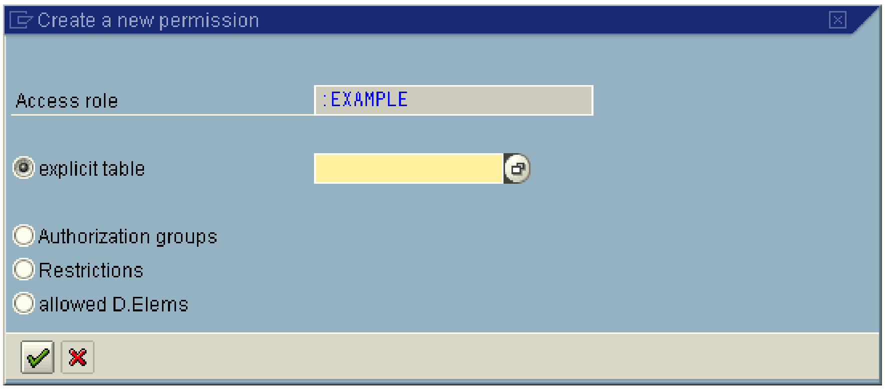
○ Authorization groups
● Database tables EK* to
○ Restrictions
○ allowed D.Elems

On the list the access role will now be followed by the new permission:



:EXAMPLE Example role
□ DB Tables EK*

If you now click on the ⊞ icon again, you will notice that “Database tables” is not available anymore:



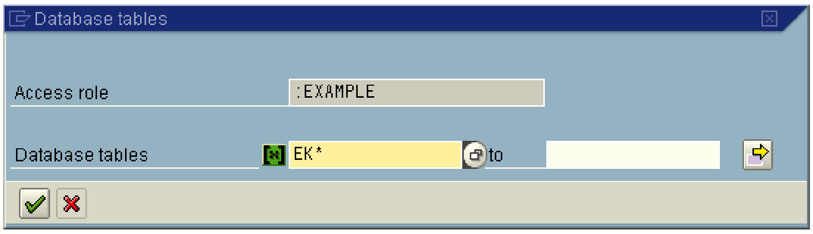
Create a new permission

Access role :EXAMPLE

● explicit table

○ Authorization groups
○ Restrictions
○ allowed D.Elems

This is because this “kind” of permission has already been assigned. In order to add new selection criteria to “Database tables”, you have to click on the ✎ icon on the corresponding permission line. A matching popup will appear, allowing you to add or change the criteria:



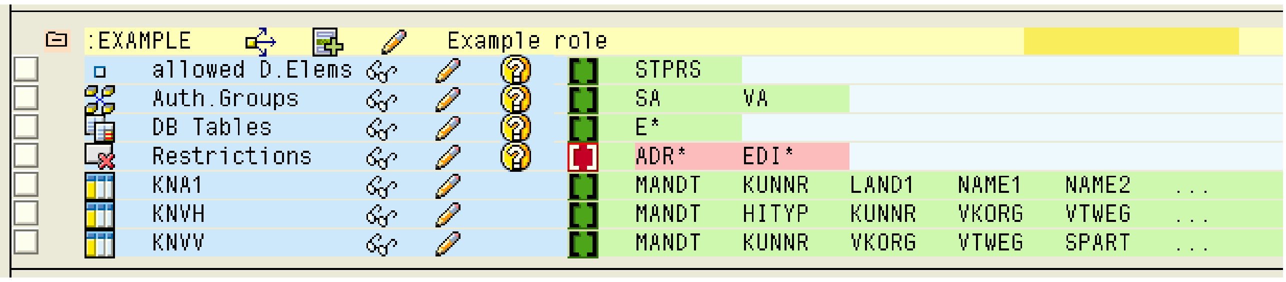
Database tables

Access role :EXAMPLE

Database tables EK* to

All kinds of permissions behave like this with the exception of explicit tables.

Each explicitly defined table permission occupies a separate line on the list, showing the first fields of the permission. To make a more complicated example, the permissions associated with a given access role might look like the following:



```
   :EXAMPLE                          Example role
□     allowed D.Elems                   STPRS
□     Auth.Groups                       SA       VA
□     DB Tables                         E*
□     Restrictions                      ADR*     EDI*
□     KNA1                              MANDT    KUNNR    LAND1    NAME1    NAME2    ...
□     KNVH                              MANDT    HITYP    KUNNR    VKORG    VTWEG    ...
□     KNVV                              MANDT    KUNNR    VKORG    VTWEG    SPART    ...
```

The “Restrictions” are a special kind of global permission. They restrict the other two kinds of global permissions, “DB Tables” and “Auth.Groups”.

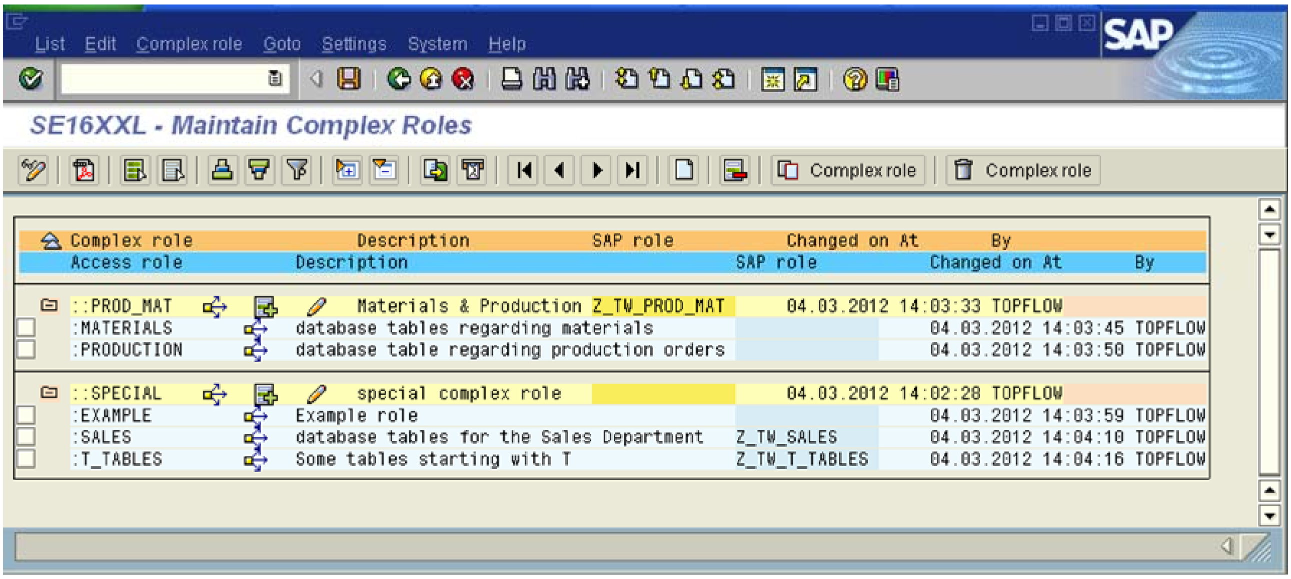
Other useful functions

Function	Description
👓	Display a global or explicit permission
❓	List the database tables selected by a global permission
🗑	Delete the selected permissions of one or more roles

NOTE: As in all lists of this tool you can navigate to other lists by using the ***Goto*** menu functions. This way, if you have changed something, you can see possible effects of your changes on the permission environment without having to save your work.

Complex roles

The list shows complex roles and their assigned elementary roles. A typical list might have the following appearance:



SE16XXL - Maintain Complex Roles

Complex role	Description	SAP role	Changed on At	By
Access role	Description	SAP role	Changed on At	By
::PROD_MAT	Materials & Production	Z_TW_PROD_MAT	04.03.2012 14:03:33	TOPFLOW
□ :MATERIALS	database tables regarding materials		04.03.2012 14:03:45	TOPFLOW
□ :PRODUCTION	database table regarding production orders		04.03.2012 14:03:50	TOPFLOW
::SPECIAL	special complex role		04.03.2012 14:02:28	TOPFLOW
□ :EXAMPLE	Example role		04.03.2012 14:03:59	TOPFLOW
□ :SALES	database tables for the Sales Department	Z_TW_SALES	04.03.2012 14:04:10	TOPFLOW
□ :T_TABLES	Some tables starting with T	Z_TW_T_TABLES	04.03.2012 14:04:16	TOPFLOW

Complex roles can be convenient to give a certain structure to the many elementary roles you may have defined. But they are not absolutely necessary. Indeed many companies do without them.

In fact there is no “right” way to define permissions. There are many different ways to do it. For example, you might define elementary roles that exactly meet the needs of each department. Or you can break these up into small portions, each containing at most from five to ten database tables, and then group these together by means of complex roles. Or you may use a mixture of both.

With the introduction of SAP roles, even more possibilities open up. It is possible to associate the same SAP role to several access roles, or to have a one-to-one correspondence between access roles and SAP roles. Instead of defining complex roles with this tool, you may then group your associated SAP roles together into a composite SAP role.

Personally, I would try to define relatively small and straightforward elementary roles and then group them together by means of either complex roles or SAP roles which would then be assigned to the users. But this is not necessarily the best solution to your problems.

Functions pertaining to complex roles

Function	Description
⇄	Display user assignments of a complex role (the icon is at the right of the role)
🗋	Create a new complex role definition
✎	Change an existing complex role (icon at the right of the role)
⧉ Complex role	Copy an existing complex role with its elementary role assignments. The direct assignments to users are not copied. The SAP role attribute of the original role is not copied.
🗑 Complex role	Delete a complex role with all elementary role assignments. The elementary roles themselves are not deleted.
Complex role → Delete many complex roles	Menu function to delete many complex roles in one operation

Functions for adding or deleting elementary role assignments

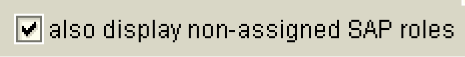
Function	Description
➕	Add a new elementary role assignment to the complex role (the icon is at the right of the complex role)
➖	Delete selected role assignments of one or more complex roles

By clicking on the ⇄ icon to the right of a complex or elementary role you navigate to a “Where used” list of the involved role.

SAP roles

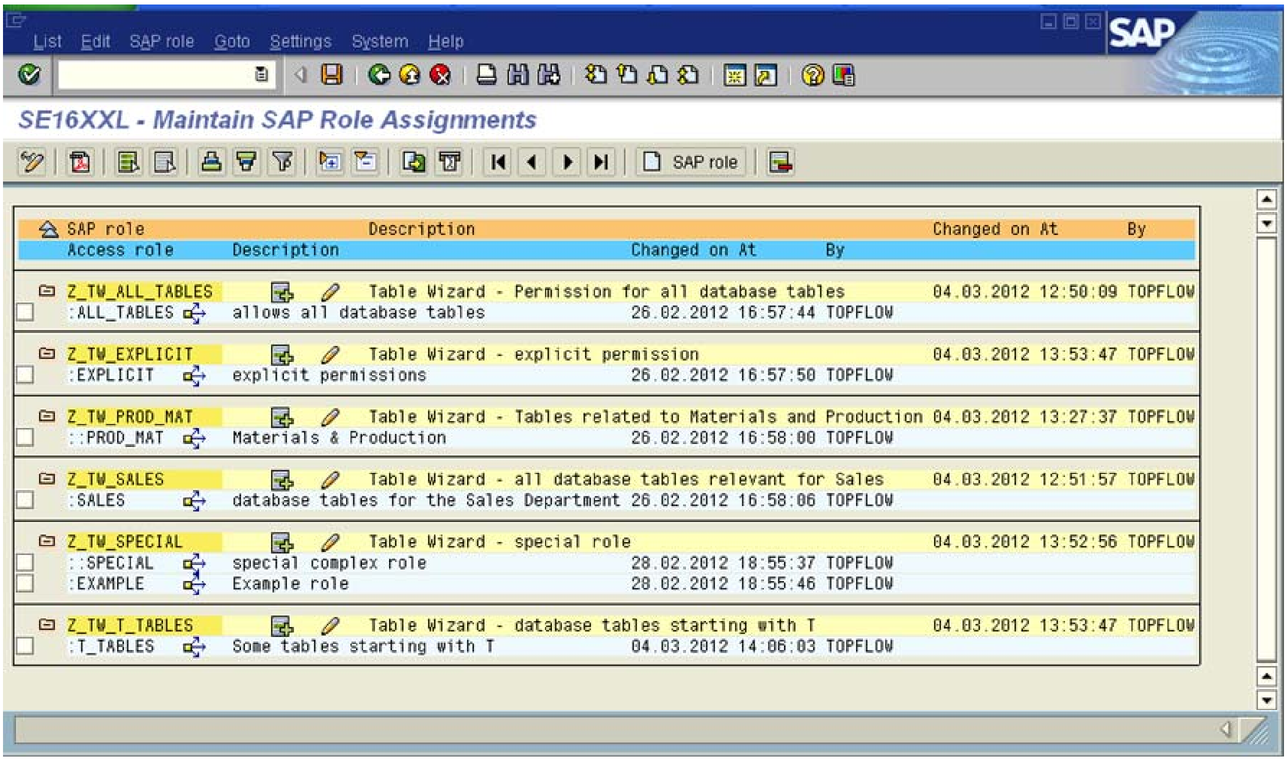
This new list has been added to give you a better overview of the SAP roles involved in your permission implementation. Starting from this list, you can easily call standard transaction **PFCG** to either create a new SAP role or change an existing one. It is also a practical way to associate SAP roles to access roles, both elementary and complex.

The list normally shows only those SAP roles that are associated to access roles.
If you wish to select also non-assigned SAP roles, check the following option on the selection screen:



☑ also display non-assigned SAP roles

A typical list of SAP roles might look like the following:



SE16XXL - Maintain SAP Role Assignments

```
  SAP role                          Description                                            Changed on At        By
  Access role     Description                                   Changed on At         By

  Z_TW_ALL_TABLES                   Table Wizard - Permission for all database tables      04.03.2012 12:50:09 TOPFLOW
□ :ALL_TABLES     allows all database tables                    26.02.2012 16:57:44 TOPFLOW

  Z_TW_EXPLICIT                     Table Wizard - explicit permission                     04.03.2012 13:53:47 TOPFLOW
□ :EXPLICIT       explicit permissions                          26.02.2012 16:57:50 TOPFLOW

  Z_TW_PROD_MAT                     Table Wizard - Tables related to Materials and Production 04.03.2012 13:27:37 TOPFLOW
□ ::PROD_MAT      Materials & Production                        26.02.2012 16:58:00 TOPFLOW

  Z_TW_SALES                        Table Wizard - all database tables relevant for Sales  04.03.2012 12:51:57 TOPFLOW
□ :SALES          database tables for the Sales Department      26.02.2012 16:58:06 TOPFLOW

  Z_TW_SPECIAL                      Table Wizard - special role                            04.03.2012 13:52:56 TOPFLOW
□ ::SPECIAL       special complex role                          28.02.2012 18:55:37 TOPFLOW
□ :EXAMPLE        Example role                                  28.02.2012 18:55:46 TOPFLOW

  Z_TW_T_TABLES                     Table Wizard - database tables starting with T         04.03.2012 13:53:47 TOPFLOW
□ :T_TABLES       Some tables starting with T                   04.03.2012 14:06:03 TOPFLOW
```

Each SAP role is followed by the associated access roles, elementary and complex. For the purpose of permissions, composite SAP roles are treated in the same way as simple SAP roles.

Functions for maintaining SAP roles

Function	Description
🗋 SAP role	Create a new SAP role with transaction **PFCG**
✎	Change an existing SAP role with transaction **PFCG** (the icon is at the right of the SAP role) Once in PFCG, you can also assign the SAP role to users or delete existing assignments.

NOTE: While most functions of the permission tool only change the definitions in a **virtual** way (i.e. the changes must be **saved** to take effect), using transaction **PFCG** means the changes are **real** – they are carried out **directly on the database**.

Functions for associating SAP roles to access roles

Function	Description
⊞	Assign the SAP role to an existing access role (the icon is at the right of the SAP role)
⊟	Clear the **SAP role attribute** of the selected access roles (this dissolves the association between access role and SAP role)

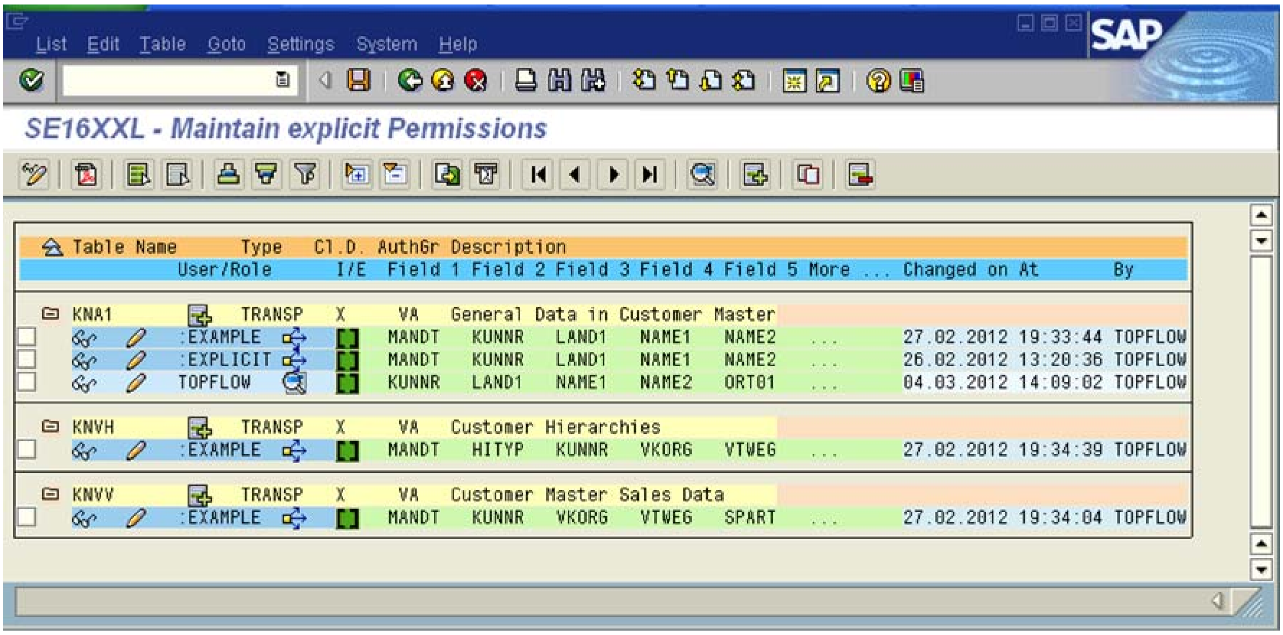
By clicking on the ⇄ icon to the right of a complex or elementary access role, you navigate to a “Where used” list of the involved role.

Explicit tables

This list is relevant only in case you have defined explicit permissions at field level. It shows the database tables for which explicit permissions have been defined. Each table is followed by the users and / or access roles which have the permission.

In case you base your implementation on SAP roles, the list should **only** contain access roles and **no** users.

A typical list might have the following appearance:



SE16XXL - Maintain explicit Permissions

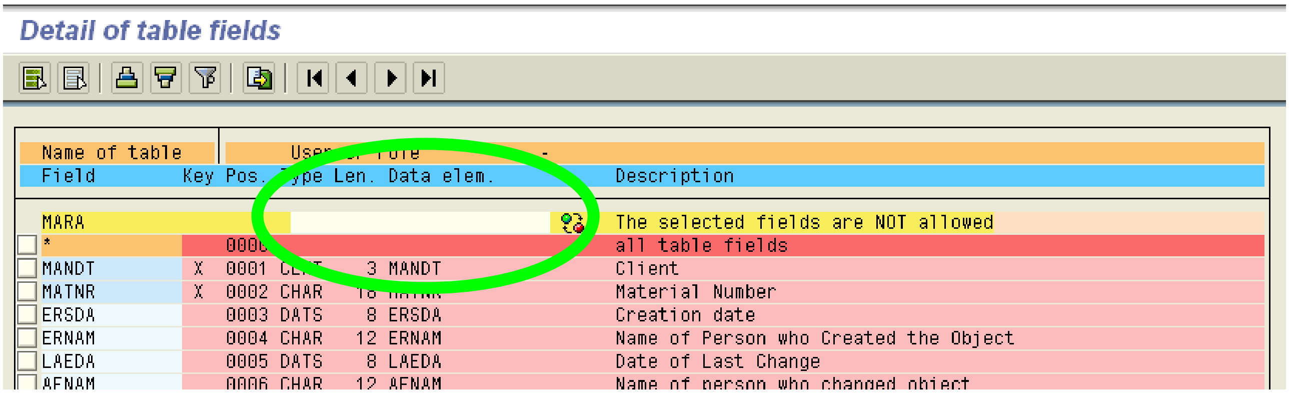
```
  Table Name       Type    Cl.D. AuthGr Description
             User/Role      I/E   Field 1 Field 2 Field 3 Field 4 Field 5 More ... Changed on At        By

  KNA1             TRANSP   X       VA   General Data in Customer Master
□            :EXAMPLE             MANDT   KUNNR   LAND1   NAME1   NAME2   ...     27.02.2012 19:33:44 TOPFLOW
□            :EXPLICIT            MANDT   KUNNR   LAND1   NAME1   NAME2   ...     26.02.2012 13:20:36 TOPFLOW
□            TOPFLOW              KUNNR   LAND1   NAME1   NAME2   ORT01   ...     04.03.2012 14:09:02 TOPFLOW

  KNVH             TRANSP   X       VA   Customer Hierarchies
□            :EXAMPLE             MANDT   HITYP   KUNNR   VKORG   VTWEG   ...     27.02.2012 19:34:39 TOPFLOW

  KNVV             TRANSP   X       VA   Customer Master Sales Data
□            :EXAMPLE             MANDT   KUNNR   VKORG   VTWEG   SPART   ...     27.02.2012 19:34:04 TOPFLOW
```

Available functions

Function	Description
✚	Create a new permission (use the button on the application toolbar to create a permission for a table not yet on the list)
✎	Change an existing explicit permission
⊟	Delete selected permissions

Function	Description
⧉	Copy an existing explicit permission
👓	Display an explicit permission
🔍	Detailed list of the allowed fields of a table for a given user
⇆	“Where used” list for a given access role

When creating a new permission (or copying an existing one), the list of fields is output without the owner (user or access role):

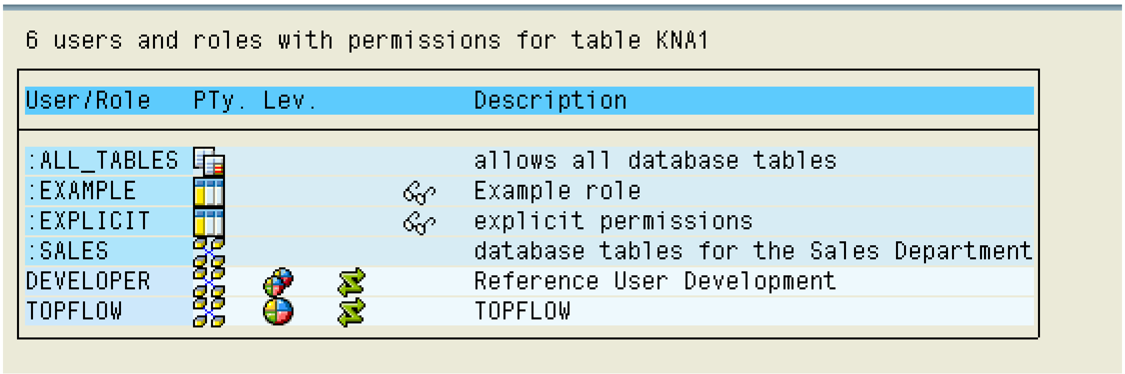


```
Detail of table fields

 Name of table        User or role              -
 Field          Key Pos.  Type Len. Data elem.          Description

 MARA                                                   The selected fields are NOT allowed
□ *                 0000                                all table fields
□ MANDT         X   0001  CLNT    3 MANDT               Client
□ MATNR         X   0002  CHAR   18 MATNR               Material Number
□ ERSDA             0003  DATS    8 ERSDA               Creation date
□ ERNAM             0004  CHAR   12 ERNAM               Name of Person who Created the Object
□ LAEDA             0005  DATS    8 LAEDA               Date of Last Change
□ AENAM             0006  CHAR   12 AENAM               Name of person who changed object
```

You must enter the name of a user or of an elementary access role.

Table cross-reference

Use the menu function ***Table → Table cross-reference*** to get a list of the access roles and users which have **any kind** of permission for the involved table:



```
6 users and roles with permissions for table KNA1

User/Role   PTy. Lev.            Description

:ALL_TABLES                      allows all database tables
:EXAMPLE                         Example role
:EXPLICIT                        explicit permissions
:SALES                           database tables for the Sales Department
DEVELOPER                        Reference User Development
TOPFLOW                          TOPFLOW
```

Forbidden Data Elements

As already seen in tutorial # 6, it is possible to define data elements that are forbidden independently of the database table or view being considered.

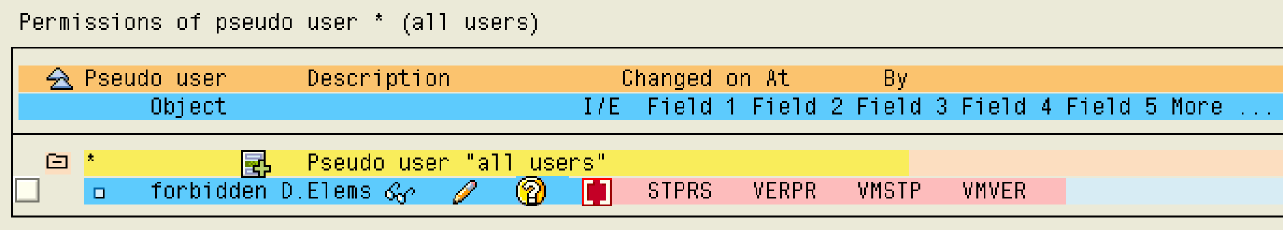
Which data elements are forbidden is defined at the level of the **pseudo user "*"** (that represents all users) – for specific users and / or access roles this prohibition can be overridden by defining the **allowed** data elements.

If you make use of this functionality, it may be interesting to determine for a given forbidden data element which users and / or roles have a special permission for it.

Data element cross-reference

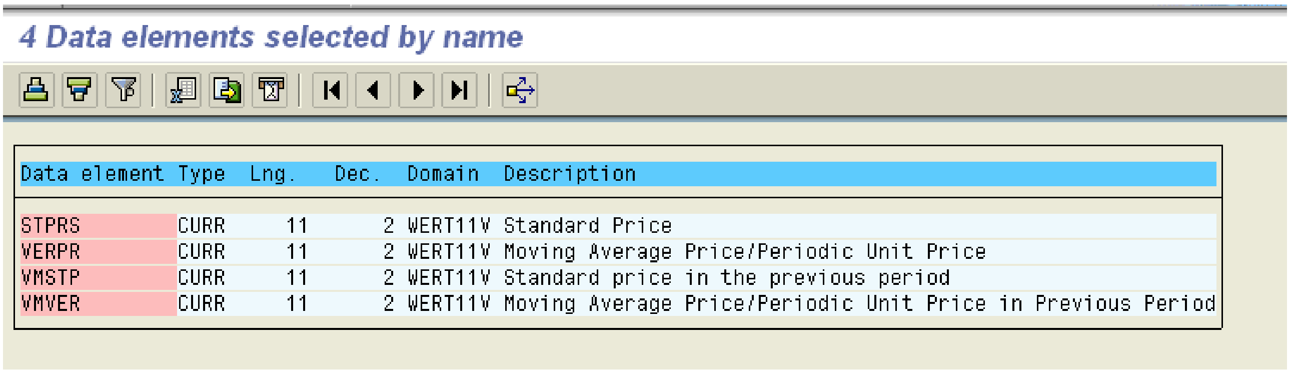
You can find this information as follows:

In the permission list of the pseudo user „*", click on the ? icon on the line „forbidden D.Elems":



```
Permissions of pseudo user * (all users)

  Pseudo user        Description                  Changed on At        By
          Object                              I/E  Field 1 Field 2 Field 3 Field 4 Field 5 More ...

  *                  Pseudo user "all users"
□  forbidden D.Elems                              STPRS   VERPR   VMSTP   VMVER
```

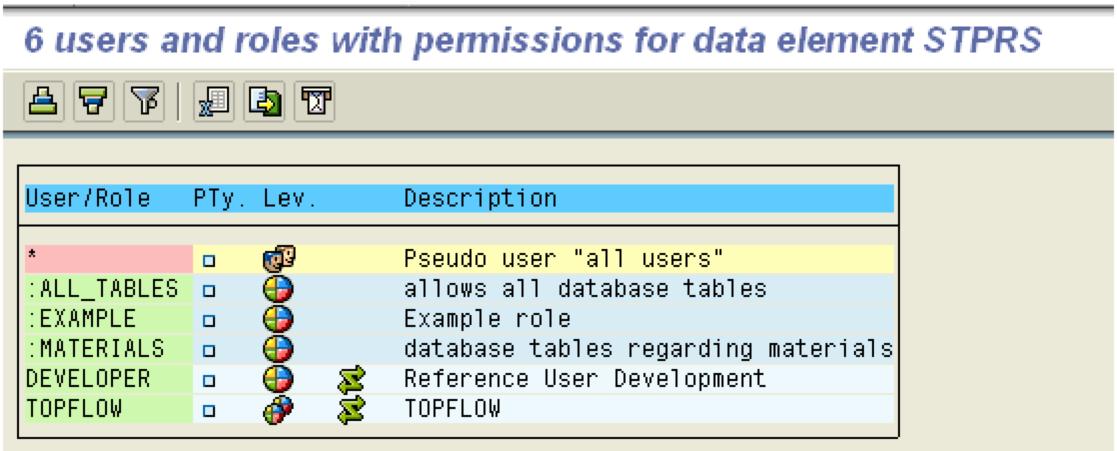
As a result, the list of the forbidden data elements appears:



4 Data elements selected by name

Data element	Type	Lng.	Dec.	Domain	Description
STPRS	CURR	11	2	WERT11V	Standard Price
VERPR	CURR	11	2	WERT11V	Moving Average Price/Periodic Unit Price
VMSTP	CURR	11	2	WERT11V	Standard price in the previous period
VMVER	CURR	11	2	WERT11V	Moving Average Price/Periodic Unit Price in Previous Period

In order to get the cross-reference list, set the cursor on a line and press the ⇆ button on the application toolbar. The following list will appear:

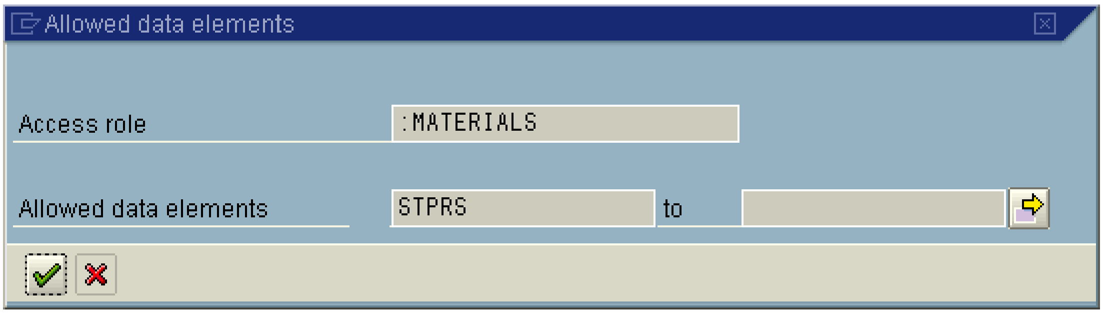


6 users and roles with permissions for data element STPRS

User/Role	PTy.	Lev.	Description
*	□		Pseudo user "all users"
:ALL_TABLES	□		allows all database tables
:EXAMPLE	□		Example role
:MATERIALS	□		database tables regarding materials
DEVELOPER	□		Reference User Development
TOPFLOW	□		TOPFLOW

Notice that the users obtain the permission indirectly (⇄) through an SAP role.

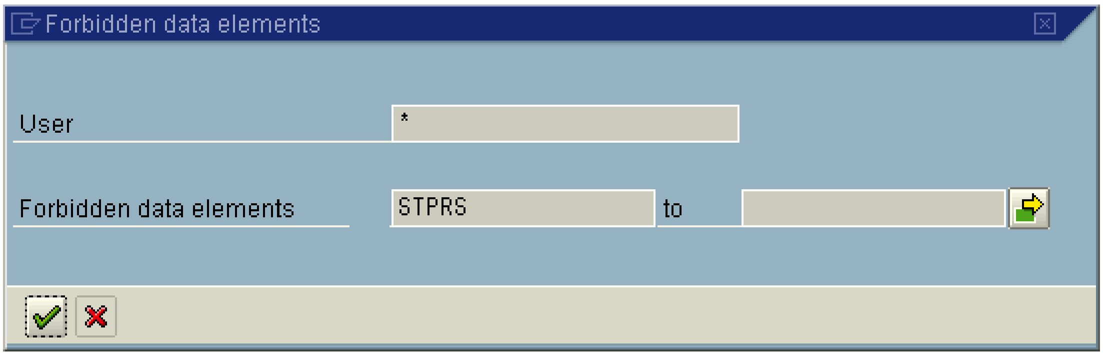
When you double click on a user (or access role), you get a popup showing the definition of the permission:



Allowed data elements

Access role	:MATERIALS		
Allowed data elements	STPRS	to	

If you double click on the "*" on the first line, you get the definition of the forbidden data elements:



Forbidden data elements

User	*		
Forbidden data elements	STPRS	to	

Click on ⇨ for more details.

Download

The permission data are stored in the database. But it still makes sense to download a copy of them now and then, as a preventive measure against accidental destruction. Furthermore you can download the data on one system and upload them (selectively) on another.
It is also advisable to download the permissions before making major changes, in order to be able to return to the original settings if necessary.

IMPORTANT: In case your implementation is based on SAP roles, only access roles and complex roles are relevant for you.

In the relevant user and role lists, use menu function ***List → Download data***.
The function is available both in maintain and display mode.

The way the download function works depends on the list from which you call it:

- if you are in a user list, i.e. ***Users & Permissions*** or ***Users & Assigned roles***, then all information associated with the selected users is stored in the download file, i.e. the permissions of the users, the associated roles (either elementary or complex), the roles assigned to the complex roles, and the permissions of all involved elementary roles. And of course the permissions of the pseudo user "*".

- If you are in a role list, either ***Access roles*** or ***Complex Roles***, then only the permissions of the elementary roles, possibly the complex roles associated with the elementary ones, and the roles associated with these etc. are stored in the file. No user information is stored in this case.

This means that when you download roles, you only get role related data on the file, whereas if you download users, you get all the data involved, i.e. also the roles.

Since it could be that not all defined roles are assigned to users, it is advisable to perform two download operations, one with all users, and the other with all roles.
The role download should be performed in the ***Access roles*** selection in order to also get those roles that are not associated with a complex one.

Upload

The upload functionality can be used to transport permissions to another system or another client or to restore corrupted or accidentally deleted permissions.

The menu function ***List*** → ***Upload data*** is only available in maintain mode.

Don't worry about calling this function since it does not overwrite existing data without asking you. And even if you have accidentally overwritten some permissions or assignments, all this is done in virtual memory first and only takes effect after you press the save button (💾).

If you base your permissions on SAP roles, only access roles and complex roles are of interest to you, since the user assignments are managed externally to this program in transaction PFCG.

The effect of the function depends on the list from where you call it. While the download function stores all related data into the file, the upload function only creates or replaces the data of the list you are in, with the exception of roles, which may be created if not existing.

IMPORTANT: administrators with limited authorizations may not be able to perform all kinds of upload operations.

If you are in ***Users & Permissions***, only users and their (explicit or global) permissions are created or replaced.

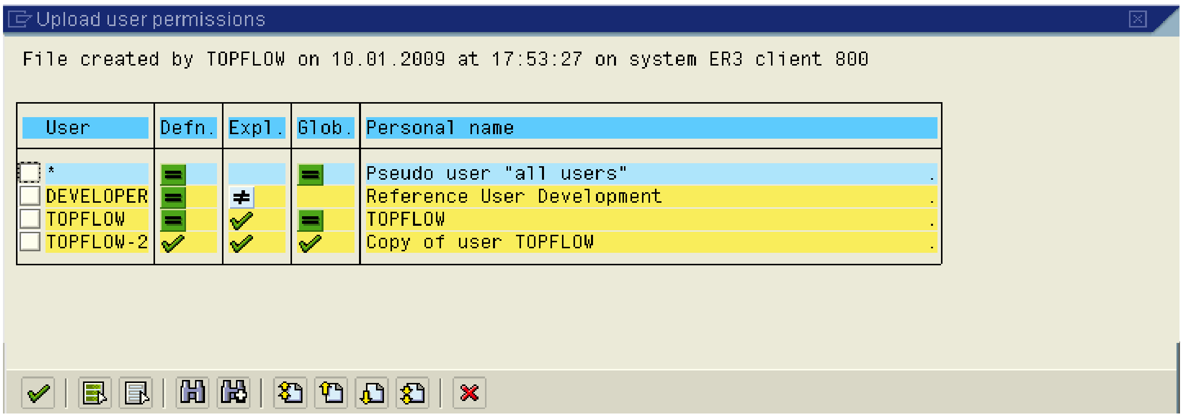
In ***Users & Assigned roles*** the role assignments are created or replaced. If an assigned role is missing, it is completely created. This also applies to complex roles, i.e. if an assigned complex role does not exist, it is created, and if some of its originally assigned roles do not exist, they are also completely created. So if you download on one system, and upload on another that does not contain any permission data yet, all information accessory to a user is created together with the user definition itself.

In ***Access roles*** (these are elementary roles), the roles and their permissions are created or replaced. No assignments to users or complex roles are created or replaced.

In ***Complex roles*** the complex roles are created or replaced. Assigned roles that do not exist are completely created. Already existing ones are left unchanged. No assignments to users are created or replaced.

The following example will show you how it works.

Suppose you have downloaded the user definitions and then made some changes. Afterwards you decide to restore the definitions to their original state. To achieve this you execute the program selecting "***Users & Permissions***". After calling the upload function the following popup appears:



File created by TOPFLOW on 10.01.2009 at 17:53:27 on system ER3 client 800

	User	Defn.	Expl.	Glob.	Personal name
□	*	=		=	Pseudo user "all users"
□	DEVELOPER	=	≠		Reference User Development
□	TOPFLOW	=	✓	=	TOPFLOW
□	TOPFLOW-2	✓	✓	✓	Copy of user TOPFLOW

Defn. describes the definition.
Expl. is related to the explicit table permissions.
Glob. describes the global permissions.

The meaning of the icons is as follows:

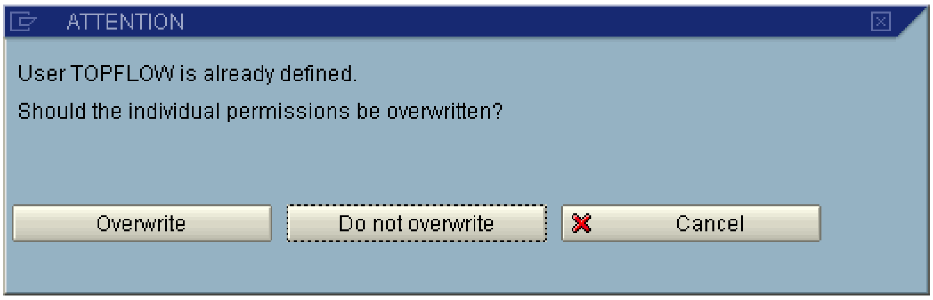
= The current values and the values on the file are identical.

≠ The current values and the values on the file differ.

✓ Only values on file exist.

No icon means that neither the user nor the file has such a permission.

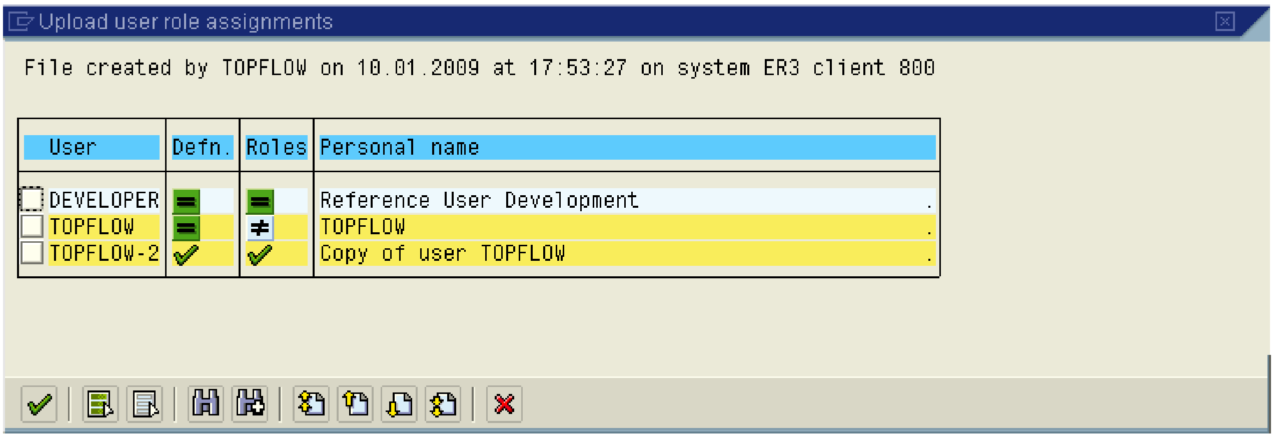
To create or replace a user definition, just check the corresponding box and press ENTER. In case the user already exists, a popup like the following will appear:



User TOPFLOW is already defined.

Should the individual permissions be overwritten?

Uploading in the "***Users & Assigned roles***" list works in a similar fashion:

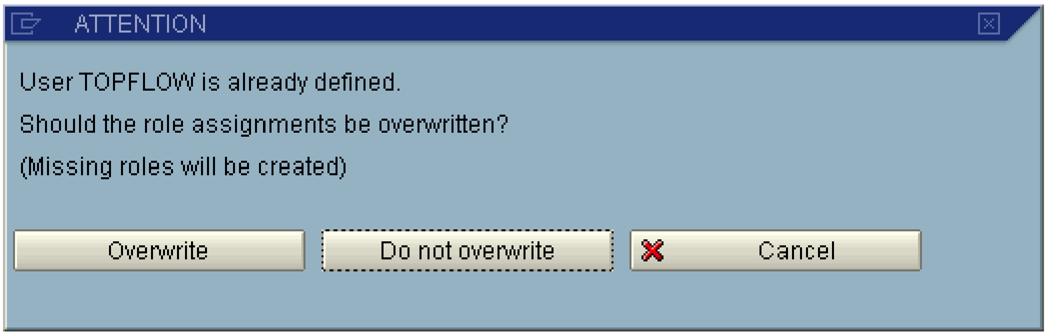


Upload user role assignments

```
File created by TOPFLOW on 10.01.2009 at 17:53:27 on system ER3 client 800
```

	User	Defn.	Roles	Personal name
□	DEVELOPER	=	=	Reference User Development
□	TOPFLOW	=	≠	TOPFLOW
□	TOPFLOW-2	✓	✓	Copy of user TOPFLOW

When you upload an existing user, the following popup will ensue:



ATTENTION

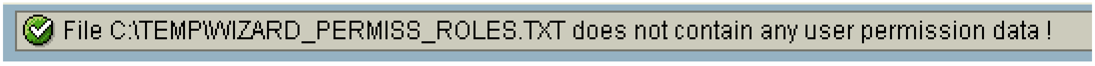
User TOPFLOW is already defined.

Should the role assignments be overwritten?

(Missing roles will be created)

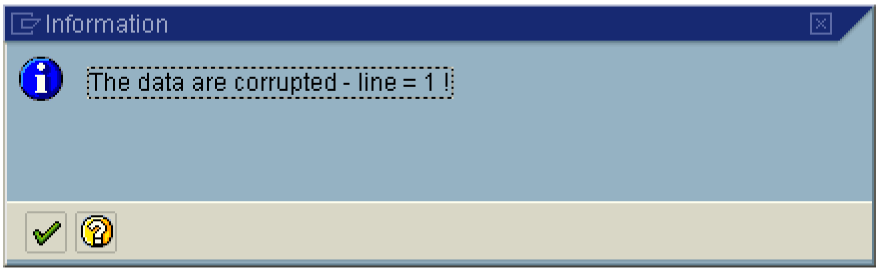
In a similar way you can upload elementary and complex roles.

If you use a file containing only roles to upload user definitions, the program issues the following message:



File C:\TEMP\WIZARD_PERMISS_ROLES.TXT does not contain any user permission data !

If you select the wrong file altogether, you could get the following message:



Information

The data are corrupted - line = 1 !

In case you wish to transfer all permissions from one system to another you might proceed as follows:

On the source system:

- download all users;
- download all roles if some roles are not assigned to users.

On the target system:

- upload the elementary roles;
- upload the complex roles, if any exist;
- upload the user permissions;
- upload the user role assignments.

In case you implement permissions based on SAP roles, only the access roles are relevant for download and upload.

The user assignments have to be transferred from the source system to the target system by using the **SAP transport system** (Menu function ***Role*** → ***Transport*** in transaction **PFCG**).

In such a situation you may dispense with the download / upload functionality altogether and also transfer the SE16XXL access roles by using a workbench transport request. How permissions may be transported is discussed on the following page.

Transport

Instead of using download and upload you can also transport permissions from one system to another.

The menu function is ***List → Transport data*** (only available in maintain mode).

If you base your permissions on SAP roles, only access roles and complex roles are of interest to you, since the user assignments are managed externally to this program in transaction PFCG.

The working of the function depends on the list from where you call it:

1) ***Single Use*** list: the definition of the user together with the permissions and role assignments are transported. The roles are not transported.

2) ***Users → Permissions***: the definitions of selected users are transported, together with their permissions. Optionally, the role assignments are also transported. The roles themselves, as in single user mode, are not transported.

3) ***Users → Assigned roles***: the other way around – the definitions and role assignments are transported, the permissions are only optionally taken into account.

4) ***Access roles***: only the role definitions and their permissions are transported.

5) ***Complex roles***: the definitions of the complex roles and their elementary role assignments are transported. The elementary roles themselves are not considered.

In the remaining lists the transport function is not available.

CAUTION: the transport functionality is not as flexible as download/upload. By using the latter you can choose what should be “imported”. This possibility is not available with a transport – in this case all data in the transport request are written to the database, without exception. So it’s better not to transport any accessory data in order to avoid overwriting existing entries.

R3TR TABU is used as transport object. The transport itself should be a workbench request.