The authorization check for dialog users

Short introduction to the basic mode of operation

One has to deal with the following three steps.

I.

The user enters a transaction code like for example *FK01*.

Initially SAP checks if the called transaction code is valid (comparison with table entries in table TSTC), it is also evaluated if the transaction code is locked (via SM01 e.g.)

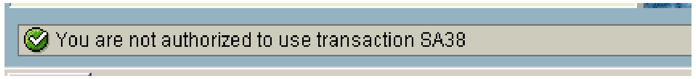
SAP then checks whether the user has a correspondent authorization on the object *S_TCODE.*

The authorization object *S_TCODE* consists of only one field (*TCD*).

The called transaction has to be part of the existing entries.

If the assigned authorization does not meet the requirements, then the user will fail the authorization check already at this stage of procedure.

This is the message that will accompany this step.



You are not authorized to use transaction SA38

If the user successfully passes this check, then SAP continues with the next step (II.).

II.

SAP® then checks whether any values for transaction code authorizations were assigned to the called transaction. This can be looked up in the table **TSTCA**. For a successful pass the user needs a matching authorization.

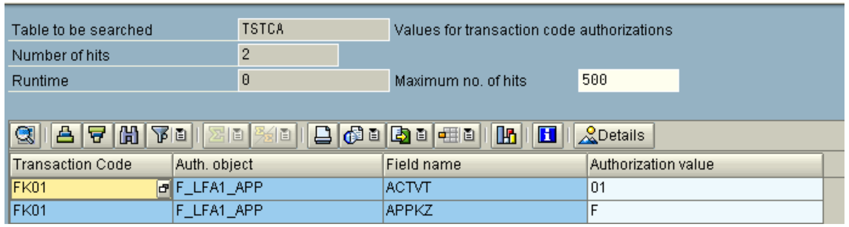
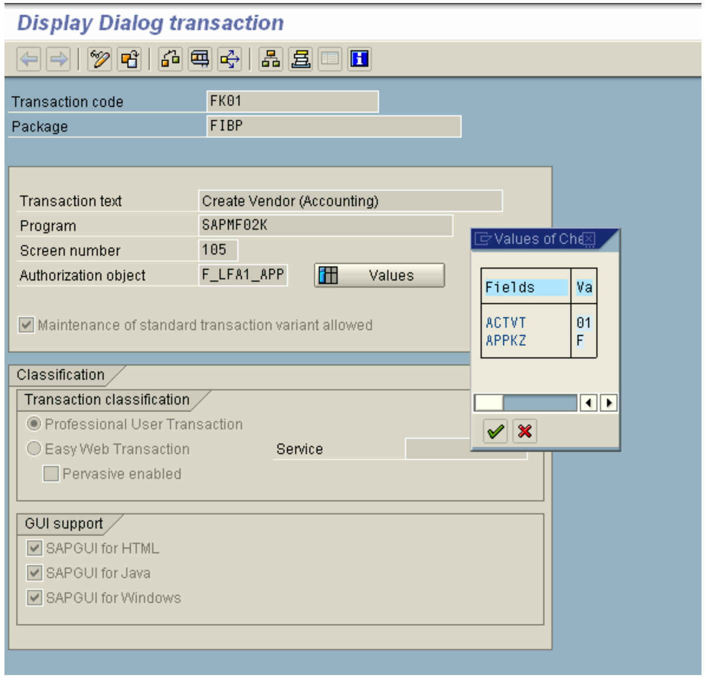


Table to be searched	TSTCA	Values for transaction code authorizations	
Number of hits	2		
Runtime	0	Maximum no. of hits	500

Transaction Code	Auth. object	Field name	Authorization value
FK01	F_LFA1_APP	ACTVT	01
FK01	F_LFA1_APP	APPKZ	F

The above described maintenance is executed with the help of the transaction **SE93**.

There one can define whether an additional authorization check on especially selected authorization objects has to be passed additionally.



Display Dialog transaction

Transaction code	FK01
Package	FIBP

Transaction text	Create Vendor (Accounting)
Program	SAPMF02K
Screen number	105
Authorization object	F_LFA1_APP

☑ Maintenance of standard transaction variant allowed

Classification

Transaction classification

● Professional User Transaction

○ Easy Web Transaction   Service

□ Pervasive enabled

GUI support

☑ SAPGUI for HTML

☑ SAPGUI for Java

☑ SAPGUI for Windows

Values of Che

Fields	Va
ACTVT	01
APPKZ	F

And again if the user fails the way ends right up here. If this step was passed too, SAP® proceeds with the next step.

III.

SAP® checks whether the user has a match for the so-called application authorization.

Every call of a transaction leads to the execution of a SAP® program. The program that is assigned to the transaction can also be reviewed with the call of the transaction **SE93**. And if further authorization checks are executed depends on the source code.

[You might check the source code with the help of the report **RSABAPSC**.]

Within the authority-check the object is listed together with the fields.

The authority-check is always executed with a logical *AND* as a joint of the listed field that are part of the listed authorization object.

One entry as an example of the integrated authority-checks is:

```
…
AUTHORITY-CHECK OBJECT 'F_LFA1_BUK'
ID 'BUKRS' FIELD LFB1-BUKRS
ID 'ACTVT' FIELD B_ACTVT
IF SY-SUBRC <> 0.
      MESSAGE Exxx WITH xxx.
    ENDIF.
…
```

In this case the object *F_LFA1_BUK* (vendor: authorization for company codes) with both of the defined fields is checked.

For the field BUKRS (company code) it is checked if the user has the same value assigned as provided by the variable *LFB1-BUKRS.*

For the field *ACTVT* (activity) it is checked if the user has the same value assigned as provided by the variable *B_ACTVT*.

Only when all values correspond with the requirements, the return value will be set to *0*.

Otherwise the authorization check fails *IF SY-SUBRC <> 0* [means that the return value is not equal 0] and the user will get an error message.

The authority-check may be integrated as a part of the program or may else be executed within an integrated call of a function module. The execution of the authority-check relies on the pass through of the correspondent source code section of course.

If the dialog user has passed these authorization checks successfully, he will be able to execute the called transaction.

Important exceptions

As usual there are some exceptions from the rule.

In this case we have to look at two other adjustments.

1. Disabling of authorization objects

First of all SAP offers the possibility to deactivate checks on authorization objects globally. In case an object is listed in the table **TOBJ_OFF** this object is excluded from any authority-checks. Objects with the initials *S** or *P** cannot be switched off.

2. Check indicator

The second option that is to be considered is the adjustment for the individual transaction. With the help of the transaction **SU24**/**SU22** authorization objects can be maintained to the effect that they will not be checked at the call of a transaction. These settings are located in the tables **USOBX_C** (check table for **USOBT_C**) and **USOBT_C** (relation between transaction and authorization object).

These tables are the customer specific tables that are valid if the profile generator is activated for use. The equivalent SAP tables are the tables **USOBX** and **USOBT**.

The values the check indicator may adopt are:

Y	the authorization object is checked at the call of the transaction the default values are located in the table USOBT_C
N	the authorization object is NOT checked at the call of the transaction
X	the authorization check takes place
U	not maintained
<empty>	not maintained