

# Maintain Custom Transaction Codes in SAP More Effectively



## Applies to:

SAP ECC, BI, and all the other versions of SAP where custom transaction codes can be built. For more information, visit the [Security homepage](#).

## Summary

This article will explain you the process of managing the custom transaction codes more effectively in terms of securing them while providing access to the users.

**Author:** Raghu Boddu

**Company:** IBM India Pvt Ltd

**Created on:** 29 September 2010

## Author Bio



Raghu Boddu is a SAP Certified Technology Professional in SAP Netweaver 7.0 Security and has excellent command over SAP R/3, BI, HR, and GRC. He is good known to the community for easy to understand articles. He has authored many articles for Microsoft knowledgebase and also is an MVP in Windows shell area from 2005-2008.

## Table of Contents

Introduction.....	3
Procedure.....	4
Custom transaction codes .....	4
Parameter transaction codes .....	6
Identifying the authorization group (S_TABU_DIS) .....	6
Identifying the authorization for Organization Unit (S_TABU_LIN) .....	7
Adding S_TABU_LIN values in the role.....	9
Additional Information - Using RSABAPSC ABAP Program .....	10
Related Content .....	11
Disclaimer and Liability Notice.....	12

## Introduction

Custom (starts with Z or Y) transactions are created in the SAP system due to the following reasons:

- Standard SAP may not support that task
- A particular transaction needs to be customized to suit the business requirements.

The custom transaction code will either call an ABAP program internally, or is a parameter transaction which deals with table maintenance (parameter transactions).

The transaction code which has an ABAP program associated will have the authorization restriction as follows:

- Restriction with AUTHORITY-CHECK OBJECT
- Restriction with calling another transaction code

When the **AUTHORITY-CHECK** is added in a program, authorization will be restricted based on an authorization object. However, if the program is calling another transaction code, it may not include any specific authorization objects, in which case the authorization objects of the CALLED transaction should be verified.

## Procedure

### Custom transaction codes

The following process will help in identifying the associated authorization objects that needs to be included in the role along with the transaction code.

1. Login to the system/client.
2. Go to **SE93** transaction code.
3. Enter the transaction code (Z or Y transaction code).
4. Double-click the program which has been associated with the transaction code.

Transaction code	Y00_SD
Package	Z002
Transaction text	Warranty
Program	Y00_SD

5. Click Find button in the program screen.
6. Enter “auth” in the Find text box, select “In main program” option and click Execute.

Find / replace	
Find	auth
<input checked="" type="radio"/> As String	
<input type="radio"/> As a word	
<input type="checkbox"/> Case-sensitive	
<input type="checkbox"/> Replace with	
<input checked="" type="radio"/> In main program	
<input type="radio"/> In program	Y00_SD

This will display all the strings that have Auth included. Find out the lines that display “Authority check” statement and identify the authorization object.

Note: You can double-click on the line to view the specific lines in the program.

Program	Found locs/short description
<input type="checkbox"/> Y00_SD	4 * Author : 13 * Author : 15 * Description : Enable company code parameter for Authority check, 204 PERFORM AUTHORITY_CHECK IN PROGRAM Y00_01 USING P_BUKRS. 205 * PERFORM f_vkorg_auth_chk_p IN PROGRAM y00_ot USING p_vkorg.

Incase, if you don't find any authorization objects, check for the string "Transaction" instead of "Auth". The below screen is an example for the same:

Program	Found locs/short description
<input type="checkbox"/> Y00_MM_F	217 CALL TRANSACTION 'MMS' USING BDCDATA MODE P_MODE UPDATE 'S' MESSAGES INTO IT_MESS.

When the program is calling another transaction, follow the steps mentioned below:

1. Double-click the transaction code in the main program.
2. Click Find button.
3. Enter "auth" as the string and look for the authorization objects associated.

Record the list of authorization objects that are used by the call-in transaction code and ensure to include all of them in the current role.

## Parameter transaction codes

Tables in the SAP environment are treated as critical and hence direct maintenance is not allowed in the production systems using SM30 or SM31 transaction codes.

When a custom table (Z or Y table) requires periodic modification by the business, a Z transaction code is created, which is controlled via a parameter transaction, which will call SM30 or SM31 internally and skips the initial screen, or the application program.

They are further protected by an authorization group. The same will be maintained using **S\_TABU\_DIS**, and **S\_TABU\_LIN** objects.

See the below screen shot for an example:

The screenshot shows the configuration for transaction code ZM\_YAA\_S. The fields are as follows:

Transaction code	ZM_YAA_S
Package	Y_SI
Transaction text	Error Table for Interface
Default values for	
Transaction	SM30
<input checked="" type="checkbox"/> Skip initial screen	
Obsolete: Use default values for transaction	
Screen	0
From module pool	

## Identifying the authorization group (S\_TABU\_DIS)

When the custom transaction code is a parameter transaction, the authorization group for table should be added to the role. Below are the steps which will help you to identify the authorization group:

1. Go to SE93, and enter the tcode.
2. Scroll down and copy the view name:

Default Values	
Name of screen field	Value
VIEWNAME	YAA_S0
UPDATE	x

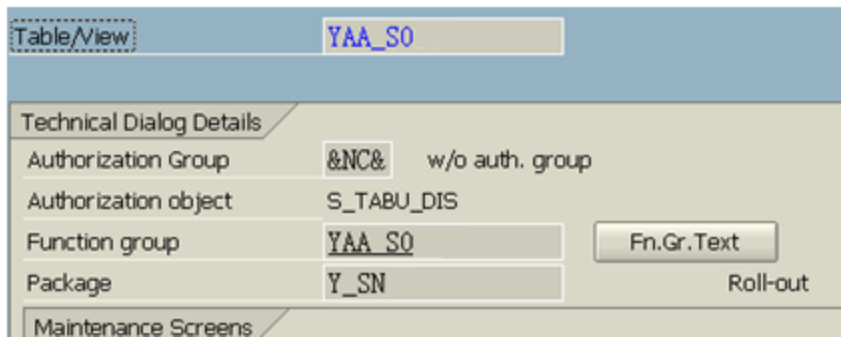
3. Go to SE11, enter the view name and click **Display** button.

The screenshot shows the SE11 object maintenance screen for the view YAA\_S0. The selected object type is 'View'.

<input type="radio"/> Database table	
<input checked="" type="radio"/> View	YAA_S0
<input type="radio"/> Data type	
<input type="radio"/> Type Group	
<input type="radio"/> Domain	
<input type="radio"/> Search help	
<input type="radio"/> Lock object	

Buttons: Display, Change

4. Click **Utilities(M)** menu option, and select **Table Maintenance Generator** option.
5. Check the Authorization group:



The Authorization Group that you find here should be maintained in **S\_TABU\_DIS** for the role in which the transaction code is added.

Note: S\_TABU\_DIS should not have authorization group FC31 (FI Posting Period) and FC01 (FI Organization unit) with activity 01, and 02. These are assigned in very limited roles due to its criticality.

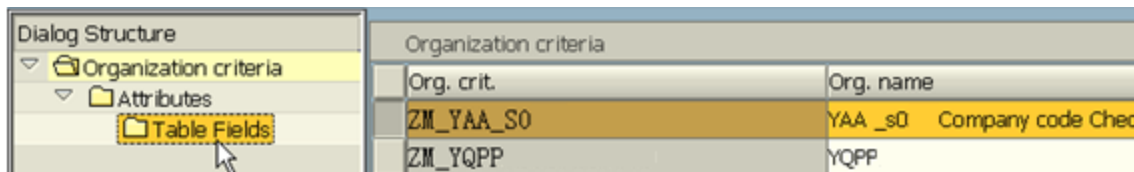
Also, ensure that a **DISPLAY** role doesn't have **01**, or **02** activities for **S\_TABU\_DIS** object.

#### Identifying the authorization for Organization Unit (S\_TABU\_LIN)

1. Goto **SPRO** transaction code.
2. Click SAP Reference IMG button.
3. Navigate to SAP Customizing Implementation Guide, SAP Web Application Server, System administration, Users and Authorization, Line-oriented Authorizations.
4. Select Define organizational criteria
5. Click Check mark, when you are prompted with "Caution: The table is cross-client" message.
6. Scroll down and find the authorization under the Org.Crit option

Organization criteria	
Org. crit.	Org. name
ZM_YAA_S0	YAA_s0 Company code Check

7. Select the entry, and double-click Table Fields option in the left pane



- Select Organization criterion: Attribute from the list and click check mark icon.

Determine Work Area: Entry

Work Area  
ZM\_YAA\_S0

Organization criterion  
ZM\_YAA\_S0

Organization criterion: Attrib  
COMPANY CODE CHECK

Further select cond. Append

- Identify the field on which the S\_TABU\_LIN restriction should be added:

Organization crit. ZM\_YAA\_S0

Org. crit. name YAA\_s0 Company code Check

Attrib. COMPANY CODE CHECK

Name Company Code Check - S0

View/table YAA\_S0

Table Fields

Field Name BUKRS

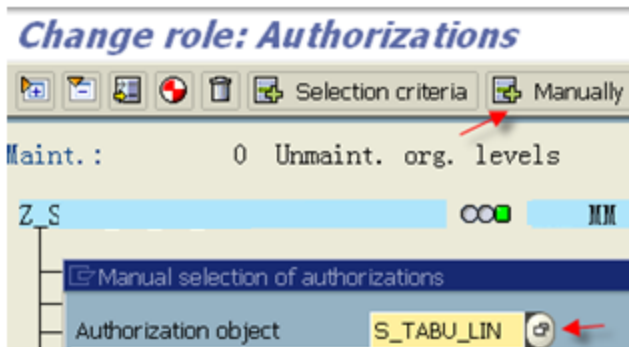
Domain BUKRS



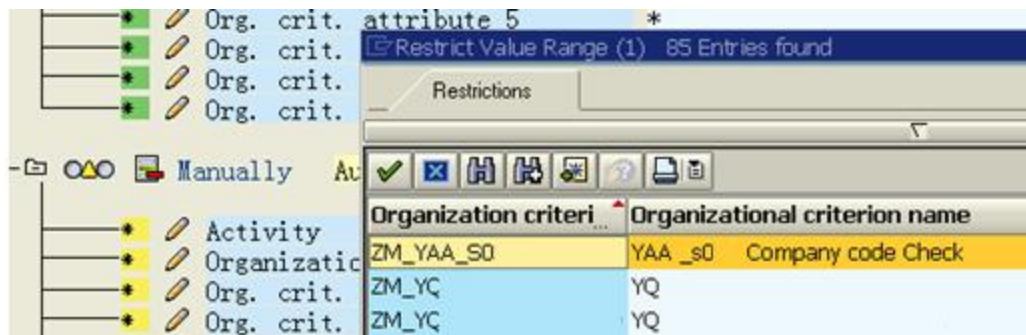
## Adding S\_TABU\_LIN values in the role

Once you identify the Organization criteria, go to the role and add **S\_TABU\_LIN** object manually, if it is added in the role (If the existing S\_TABU\_LIN has different values, do not change the same and add a new one manually again.)

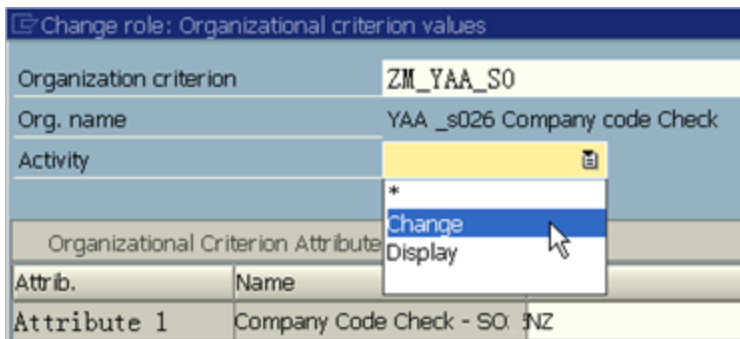
1. Click Manually button and enter S\_TABU\_LIN and click the check mark



2. Click Pencil icon for Activity and select the Organization Criteria as shown below:



3. Select the activity, and enter the company code to which the data should be restricted: (You can check the organizational level values to know the company code information.)



4. Click Transfer (F5).
5. Continue with the other changes/generate the profile.

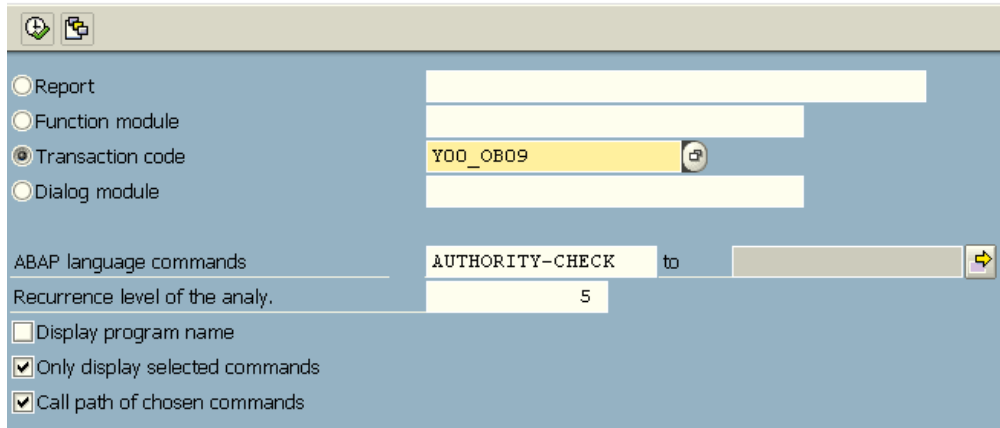
Note: A display role should not have either \*, or Change Activity.

### Additional Information - Using RSABAPSC ABAP Program

The “**RSABAPSC**” program can be used to trace the authority-check commands used in a program and its sub programs.

It allows specifying the recurrence level, which is “5” by default.

#### *Statistical program analysis to find ABAP lang. commands*



The screenshot shows the SAP dialog box for statistical program analysis. It features a top bar with navigation icons. Below, there are radio buttons for selecting the analysis type: Report, Function module, Transaction code (selected), and Dialog module. To the right of these are input fields, with 'Y00\_OB09' entered in the Transaction code field. Below this is a section for 'ABAP language commands' with 'AUTHORITY-CHECK' entered and a 'to' field. The 'Recurrence level of the analy.' is set to '5'. At the bottom, there are checkboxes for 'Display program name' (unchecked), 'Only display selected commands' (checked), and 'Call path of chosen commands' (checked).

However, it is advised to specify a value which is not more than 10.

## Related Content

For more information, visit the [Security homepage](#).

## Disclaimer and Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.