PFCG Roles and Authorization Concept

SAP® CRM 7.0

Target Audience

- System administrators
- Technology consultants

Document version: 1.0 – December 2009

THE BEST-RUN BUSINESSES RUN SAP

SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

Disclaimer
Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP’s Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace
You can find this documentation at the following address:
http://service.sap.com/

Terms for Included Open Source Software

This SAP software contains also the third party open source software products listed below. Please note that for these third party products the following special terms and conditions shall apply.

1. This software was developed using ANTLR.

2. gSOAP

Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

3. SAP License Agreement for STLport

SAP License Agreement for STLPort between

SAP Aktiengesellschaft

Systems, Applications, Products in Data Processing

Neurottstrasse 16

69190 Walldorf, Germany

(hereinafter: SAP)

and

you

(hereinafter: Customer)

a) Subject Matter of the Agreement

A) SAP grants Customer a non-exclusive, non-transferrable, royalty-free license to use the STLport.org C++ library (STLport) and its documentation without fee.

B) By downloading, using, or copying STLport or any portion thereof Customer agrees to abide by the intellectual property laws, and to all of the terms and conditions of this Agreement.

C) The Customer may distribute binaries compiled with STLport (whether original or modified) without any royalties or restrictions.

D) Customer shall maintain the following copyright and permissions notices on STLport sources and its documentation unchanged:

Copyright 2001 SAP AG

E) The Customer may distribute original or modified STLport sources, provided that:

o The conditions indicated in the above permissions notice are met;

o The following copyright notices are retained when present, and conditions provided in accompanying permission notices are met:

Copyright 1994 Hewlett-Packard Company

Copyright 1996,97 Silicon Graphics Computer Systems Inc.

Copyright 1997 Moscow Center for SPARC Technology.

Copyright 1999,2000 Boris Fomitchev

Copyright 2001 SAP AG

Permission to use, copy, modify, distribute and sell this software and its documentation for any purposes is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.
Permission to use, copy, modify, distribute and sell this software and its documentation for any purposes is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Moscow Center for SPARC makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.
Boris Fomitchev makes no representations about the suitability of this software for any purpose. This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk. Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.
Permission to use, copy, modify, distribute and sell this software and its documentation for any purposes is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. SAP makes no representations about the suitability of this software for any purpose. It is provided with a limited warranty and liability as set forth in the License Agreement distributed with this copy.
SAP offers this liability and warranty obligations only towards its customers and only referring to its modifications.
b) Support and Maintenance
SAP does not provide software maintenance for the STLport. Software maintenance of the STLport therefore shall be not included.
All other services shall be charged according to the rates for services quoted in the SAP List of Prices and Conditions and shall be subject to a separate contract.
c) Exclusion of warranty
As the STLport is transferred to the Customer on a loan basis and free of charge, SAP cannot guarantee that the STLport is error-free, without material defects or suitable for a specific application under third-party rights. Technical data, sales brochures, advertising text and quality descriptions produced by SAP do not indicate any assurance of particular attributes.
d) Limited Liability
A) Irrespective of the legal reasons, SAP shall only be liable for damage, including unauthorized operation, if this (i) can be compensated under the Product Liability Act or (ii) if caused due to gross negligence or intent by SAP or (iii) if based on the failure of a guaranteed attribute.
B) If SAP is liable for gross negligence or intent caused by employees who are neither agents or managerial employees of SAP, the total liability for such damage and a maximum limit on the scope of any such damage shall depend on the extent to which its occurrence ought to have anticipated by SAP when concluding the contract, due to the circumstances known to it at that point in time representing a typical transfer of the software.
C) In the case of Art. 4.2 above, SAP shall not be liable for indirect damage, consequential damage caused by a defect or lost profit.

D) SAP and the Customer agree that the typical foreseeable extent of damage shall under no circumstances exceed EUR 5,000.

E) The Customer shall take adequate measures for the protection of data and programs, in particular by making backup copies at the minimum intervals recommended by SAP. SAP shall not be liable for the loss of data and its recovery, notwithstanding the other limitations of the present Art. 4 if this loss could have been avoided by observing this obligation.

F) The exclusion or the limitation of claims in accordance with the present Art. 4 includes claims against employees or agents of SAP.

4. Adobe Document Services

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and / or other countries. For information on Third Party software delivered with Adobe document services and Adobe LiveCycle Designer, see SAP Note 854621.

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE TEXT	Keys on the keyboard, for example, F2 or ENTER.

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Contents

1 Introduction

In the CRM role concept there is a dependency between Business Roles and PFCG roles. The idea is, that each business role has a corresponding PFCG role containing only those authorization objects needed to fulfill the task being part of the Business Role.

The question now is how to determine the needed authorizations if you have enhanced a business role or created your own business role from scratch. Possible enhancements are new/enhanced UI components or changes in the navigation profile or in the business role.

This document first explains the authorization concept and then gives you detailed step by step descriptions how to create/update your PFCG role.

2 Architecture

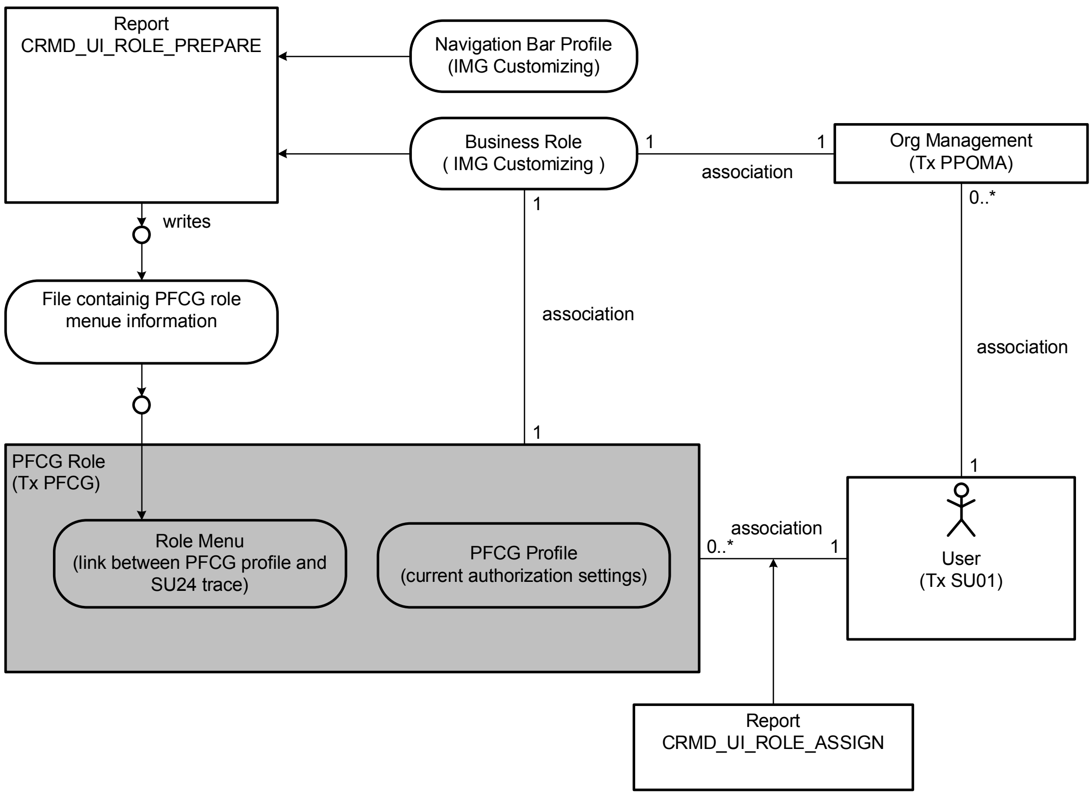
Overview

This chapter introduces the parts involved in this process and shows their dependencies.

Architecture

The graphic below shows and explains the following dependencies:

- Between the PFCG role menu and the business role
- Between the user and the PFCG role

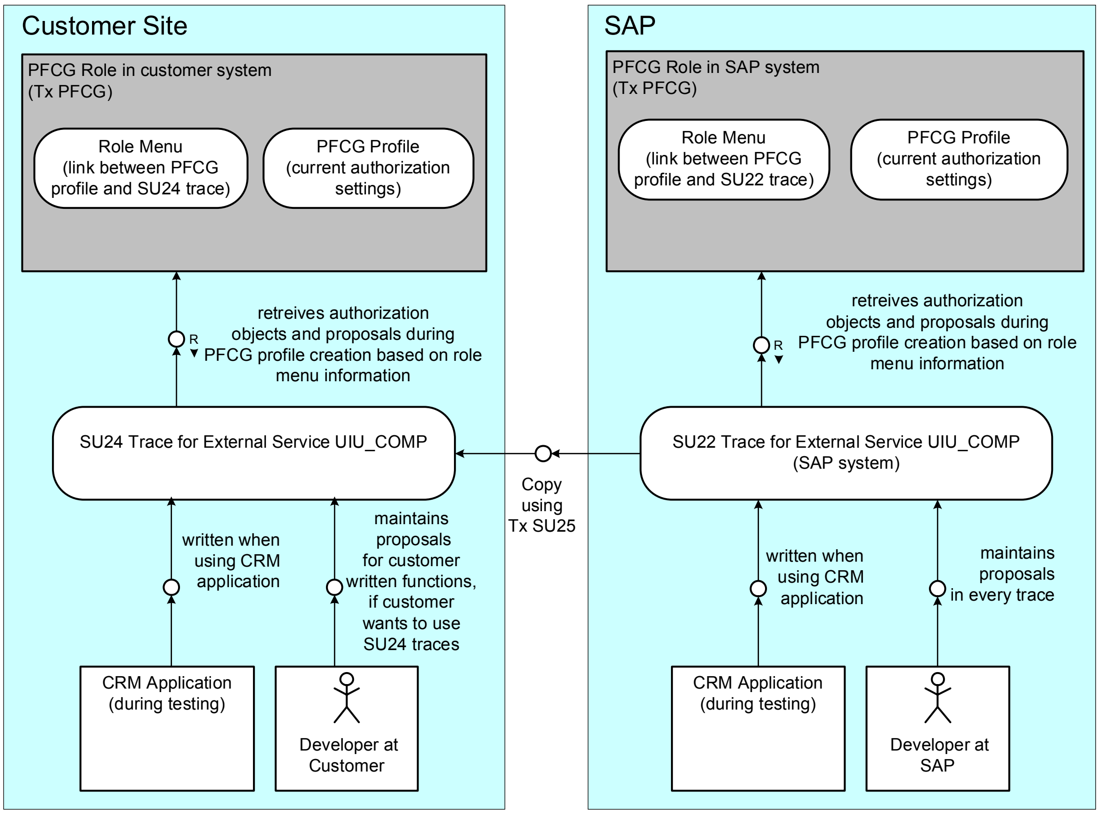


Component	Description
User	CRM uses the standard user maintenance (SU01). Authorizations are provided using PFCG profiles/roles assigned to the users.
Organizational Management	Users are (usually) indirectly assigned to business roles using the organizational management. If a position in

Component	Description
	the organizational management is assigned to a business role using the info type *Business Role*, then in turn all users are assigned to this business role as well. For information about other ways to assign business roles, see Determination of Business Roles
Navigation Bar Profile	Used to define work centers, logical links etc. Provides common settings used in business roles.
Business Role	Uses and adopts the navigation bar profile (e.g. work centers can be turned off) to the needs of the particular business functions. There is (usually) an assignment to one PFCG role.
Report CRMD_UI_ROLE_ASSIGN	Assigns PFCG roles to the user based on user assignments in the organizational management (positions in the organizational management in turn are assigned to business roles)
PFCG Role	Contains tailored authorizations for the business role. The authorizations are retrieved from SU22/SU24 traces (at SAP/customer) based on the PFCG role menu. Note Every user has to be assigned to the PFCG role SAP_CRM_UIU_FRAMEWORK—in addition to the business role specific PFCG role Usually there is a 1:1 relation between business roles and PFCG roles. There are cases where this is not suitable. It is then possible to assign the same PFCG role to several business roles in Customizing or even to omit the PFCG role.
PFCG Role Menu	Is imported from a file created by report CRMD_UI_ROLE_PREPARE in the PFCG transaction. Each role menu entry is linked to a SU22/SU24 trace. The menu contains all traces and in turn all the authorizations needed to run a specific business role.
Report CRMD_UI_ROLE_PREPARE	Creates the role menu file based on the settings in Customizing. This information represents the link between the business role settings and the SU24 traces.

The next graphic shows and explains the following dependencies:

- Between the PFCG role and the SU22/24 traces
- Between the PFCG role and the CRM Web Client based application



Component	**Description**
PFCG Profile	Contains authorization objects needed for a particular business role. The profile retrieves authorization objects from SU22/SU24 trace during profile creation. Only traces that are connected to the PFCG role via the role menu are read.
SU22 Trace	Authorization traces delivered by SAP. The CRM user interface uses the external trace type UIU_COMP.
SU24 Trace	Authorization traces maintained by the customer. These traces are copied from the SAP namespace (SU22) using transaction SU25.

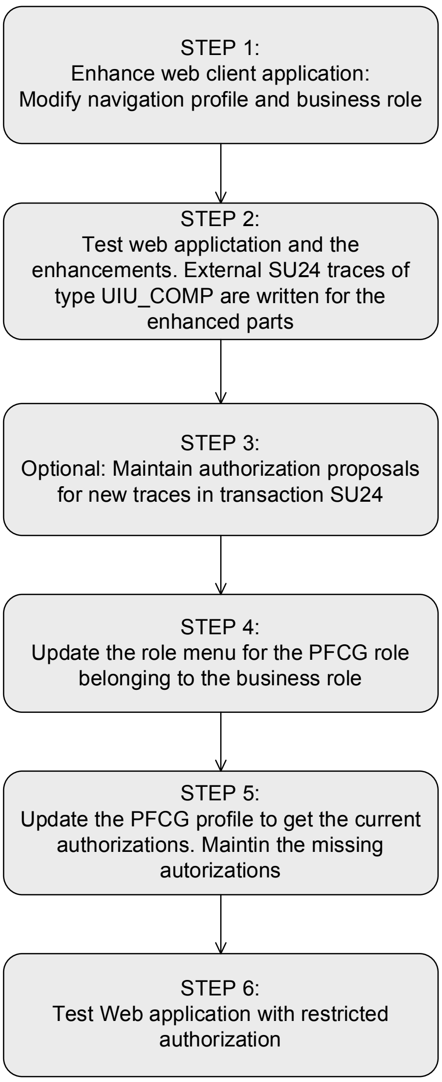
CRM Application	Available UI functions are controlled in Customizing. Authorizations are controlled by PFCG roles.
	
	SU22 (at SAP) and SU24 (at the customer) traces are written if they are turned on when the application performs an authorization check.
	
	Turning trace on/off:
	
	TA: RZ11
	`auth/authorization_trace = Y: active`
	`auth/authorization_trace = N: inactive`
	
	The more functions were executed in the application, the better is the coverage of the authorization check in the SU22/24 trace.

Maintaining Authorizations

This chapter gives you some hints on how to update your PFCG profiles after changing navigation profile or business role settings.

Prerequisite for the steps described in this chapter is that you have already copied the SAP SU22 traces into your SU24 namespace using the transaction SU25. Please see *Define Authorization Role* in SPRO for further details on this topic. You should also have an own business role by copying an existing business role which you are adjusting/enhancing according to your business requirements.

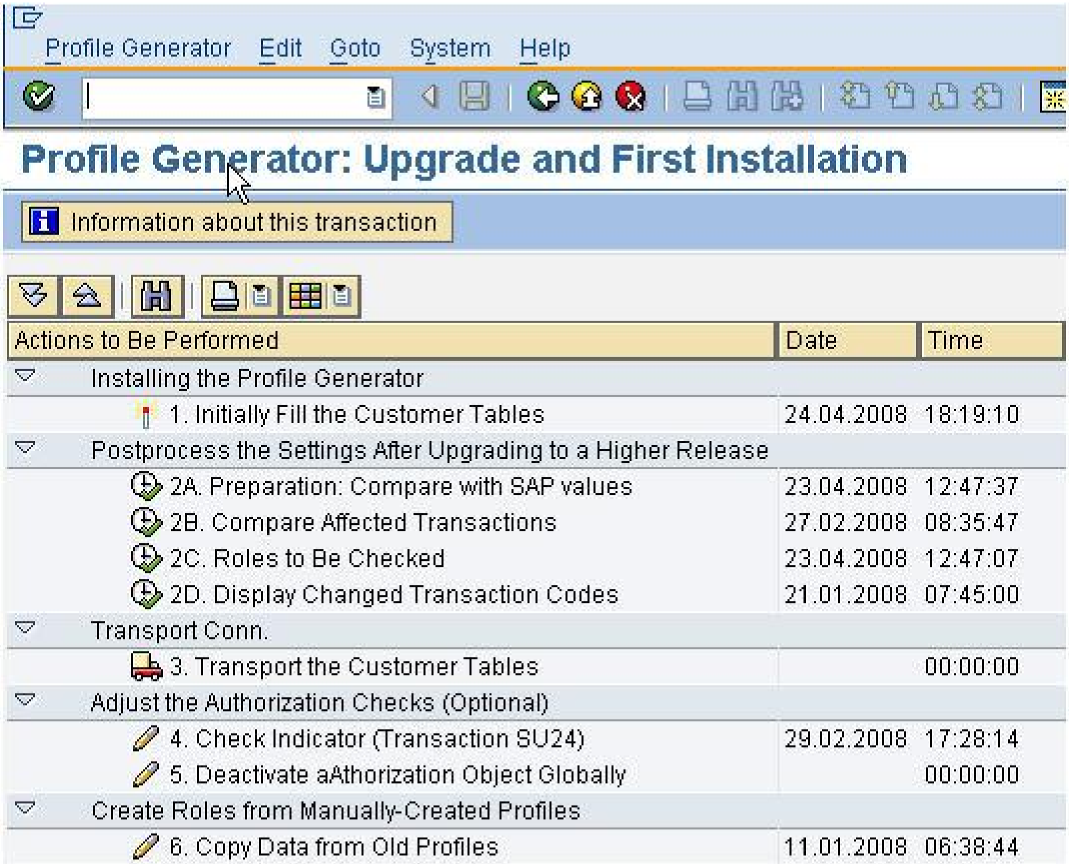
The following diagram depicts the main steps one usually performs to keep the business role and the corresponding PFCG role in sync.



Prerequisites

You need authorization traces delivered by SAP before you can create PFCG profiles for a business role.

If not done yet, copy the SAP SU22 traces into your namespace. For that you have to use transaction SU25. See *Define Authorization Role* in SPRO for further details.



Step1: Enhancing Web Client Application

This step involves the development of new UI components, enhancements of existing UI component, changes in the business role or navigation bar customizing. It is out of scope of this document to describe these activities in detail. This step is just mentioned since it may significantly influence the authorizations needed to run your application.

Step2: Testing Web Application (Full Authorization)

Once you have finished developing your business role you have to test it. By testing it, you do not only validate functional correctness but also write SU24 authorization traces (if they are turned on). These traces will be used in STEP 5 where you are determining the authorization needed by your business role. It is therefore important in this step to test all processes which may execute additional authorization checks.

Before start testing, make sure that the SU24 trace is turned on:

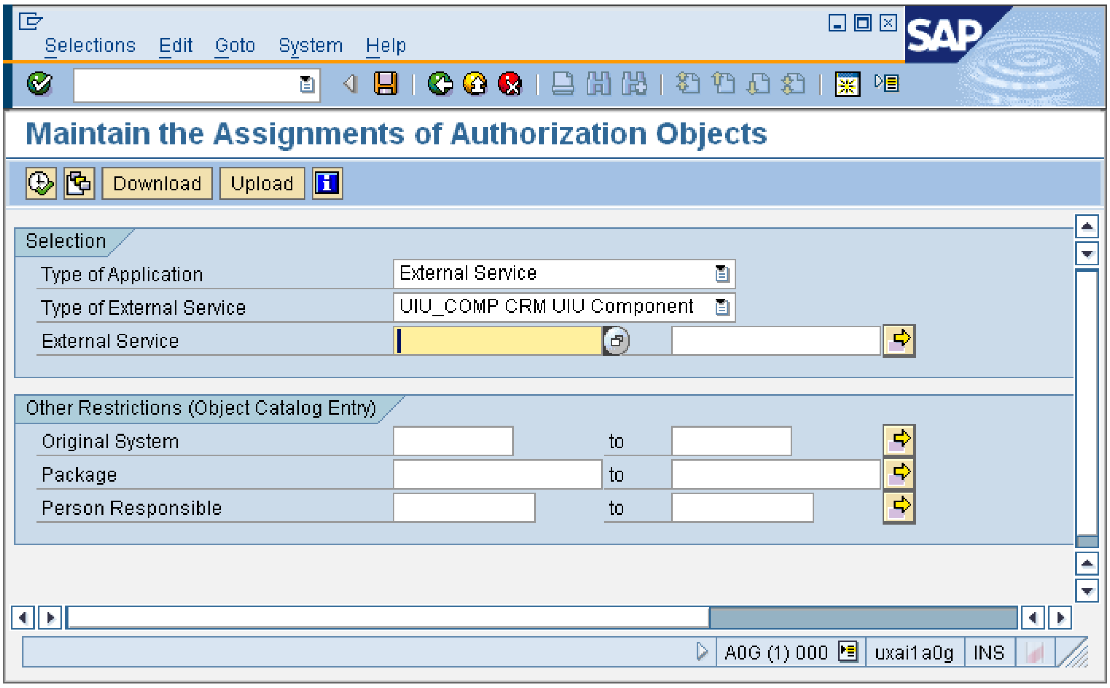
- Transaction: RZ11
  - `auth/authorization_trace = Y: active`
  - `auth/authorization_trace = N: inactive`

Step 3: Maintaining Authorizations

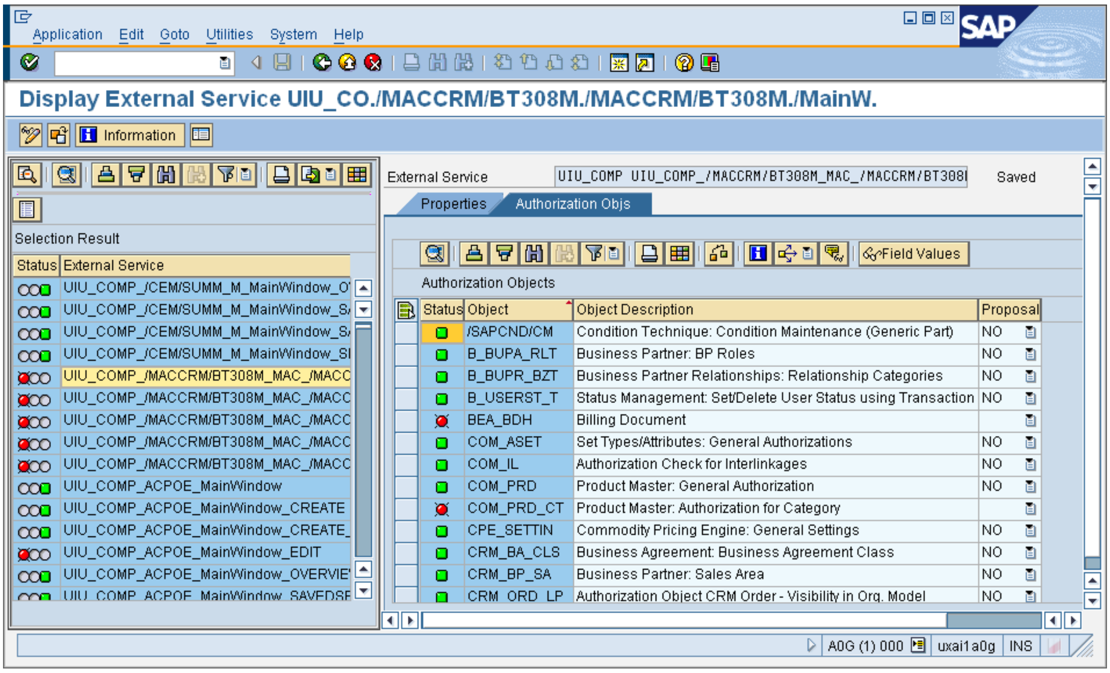
Authorization Trace (SU24)

Maintaining authorization proposals in SU24 is the preferred approach if you are dealing with many business roles and therefore need to maintain your authorizations centrally. If you just have few business roles and prefer maintaining authorizations directly in the PFCG profile continue with chapter **Authorization Profile (PFCG).**

- Check whether new SU24 traces have been written for your business role:
  - Execute transaction SU24 and select the UIU_COMP as external service. You can find there all authorization checks performed when running the CRM Web Client.



  - Incomplete or new traces are marked with a red status indicator



- Maintain authorization proposals for traces written by your modified UI component(s). You may also maintain proposals for traces delivered by SAP if the authorization proposals are not complete. Some proposals have intentionally have been left empty since they highly depend on your customizing settings and can therefore only be maintained on customer site.
- Set the check indicator to 'YS' for those authorization objects you are explicitly testing in your application.
- Set the check indicator to 'NO' for authorizations like S_DEVELOP which are still checked but which should usually not get into a user's authorization profile by authorization proposals (unless you really know what you are doing). The fact that these authorizations are checked does not mean that they should be assigned to a business user under normal circumstances. The following table gives an overview on some of those authorization objects

Authorization Object	Description
S_BTCH_ADM	Background Processing: Background Administrator
S_CTS_ADMI	Administration Functions in Change and Transport System
S_CTS_SADM	System-Specific Administration (Transport)
S_DEVELOP	ABAP Workbench. In some scenarios (Interaction Center) this authorization with activity = 03 may be required.
S_ESH_ADM	Administration Enterprise Search Appliance
S_GUI	Authorization for GUI activities
S_LOG_COM	Authorization to Execute Logical Operating System Commands.
S_RFC	Authorization check for RFC access.
S_RZL_ADM	Control Station: System Administration

S_SYS_RWBO	System-Specific Authorization Object for WBO Proxy Functions
S_TABU_DIS	Table Maintenance (via standard tools such as SM30)
S_TCODE	Transaction Code Check at Transaction Start. The Business Partner component may need the following authorization assigned: TCT = /SAPAPO/LRP_ACCESS
S_USER_AGR	Authorizations: Role Check
S_USER_GRP	User Master Maintenance: User Groups
S_USER_PRO	User Master Maintenance: Authorization Profile

Hint:

- You can get online documentation on an authorization object by clicking on the 'i' button.
- SU24 traces are maintained in the development client.

Authorization Profile (PFCG)

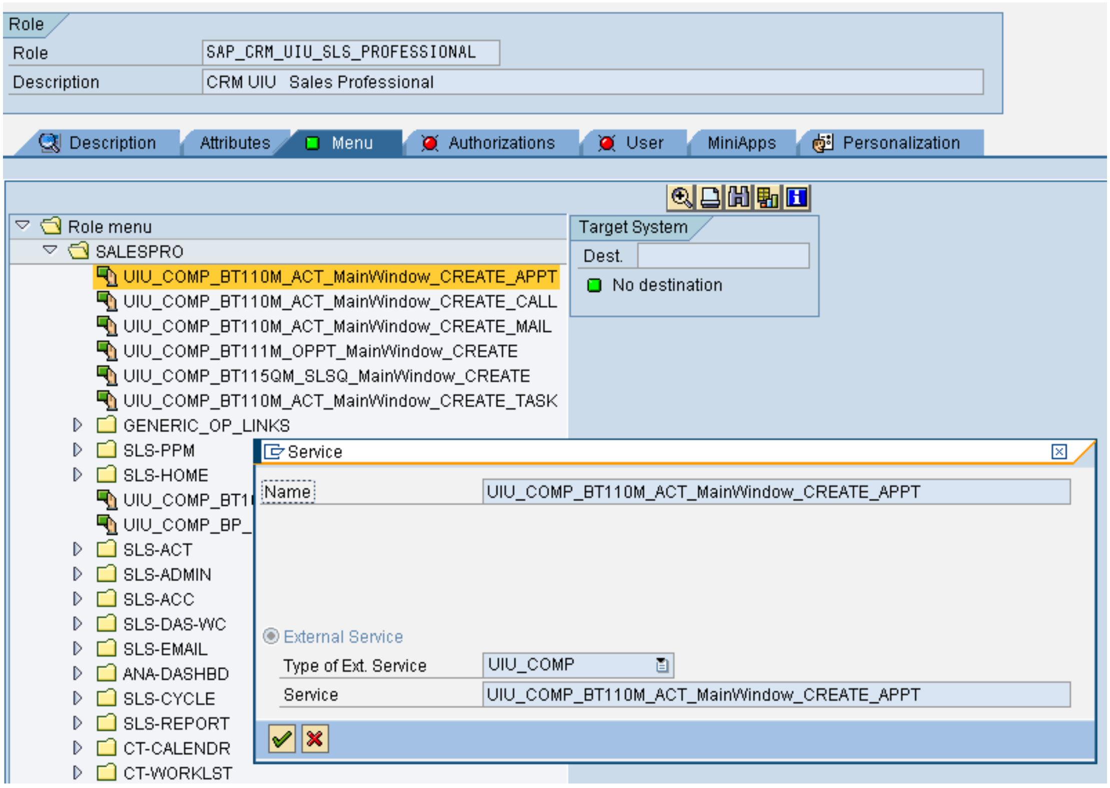
Instead of using SU24 you can also maintain your authorization settings directly in the PFCG profile. This is useful if you are just dealing with few Business/PFCG and there is no need to re-use authorization settings.

Step 4: Updating the Role Menu

All activities described in this step are performed in transaction PFCG.

The PFCG role menu is needed to link the PFCG authorization role with the SU24 authorization traces. The authorization profile generator uses this information to collect all need authorization objects.

You can display the SU24 trace linked to a role menu entry by selecting ‘Display Details’ from the context menu of a particular menu entry.



The entries in the role menu must match to the UI components which are part of the business role in order to get best possible coverage of the authorizations. In fact, there is not only one entry per UI component but one entry for each combination of UI component/window/inbound plug used in the business role. This leads to a large number of entries in the role menu tree.

It is recommended to update the role menu tree after you have made changes in the business role customizing. A correct role menu is the prerequisite for the profile generator to get those authorizations needed by your business role. Since it would be very cumbersome to create the role menu manually there is the report CRMD_UI_ROLE_PREPARE. The next paragraph describes how to use it.

Execute the Report CRMD_UI_ROLE_PREPARE

This report determines the SU24 traces relevant for a business role by analyzing the business role´s logical links. Since the report cannot directly write the role menu into the PFCG role it creates a text file containing the menu information. This file will be imported in PFCG in the next step.

- SE38: Execute Report CRMD_UI_ROLE_PREPARE
- Select your business role (for scenarios that don't assign users in the organizational model—like Channel Management—select a PFCG role) and language EN.
- A file is created and saved locally (e.g. on Windows: C:\Documents and Settings\<your user ID>\SapWorkDir)

Assign Business Role Data to the PFCG Role

In this step you assign the role menu data created in the previous step to the PFCG role. Perform this step in the same system/client as the CRMD_UI_ROLE_PREPARE report.

- Go to transaction PFCG.

- Select your PFCG role (e.g. SAP_CRM_UIU_SRV_PROFESSIONAL) and go to the change mode.
- Import the file to your PFCG Profile via Menu → Import from file.
- If you just want to update the role menu you have to delete the already exiting role menu first. Select the menu (e.g. SALESPRO) and press the delete button.

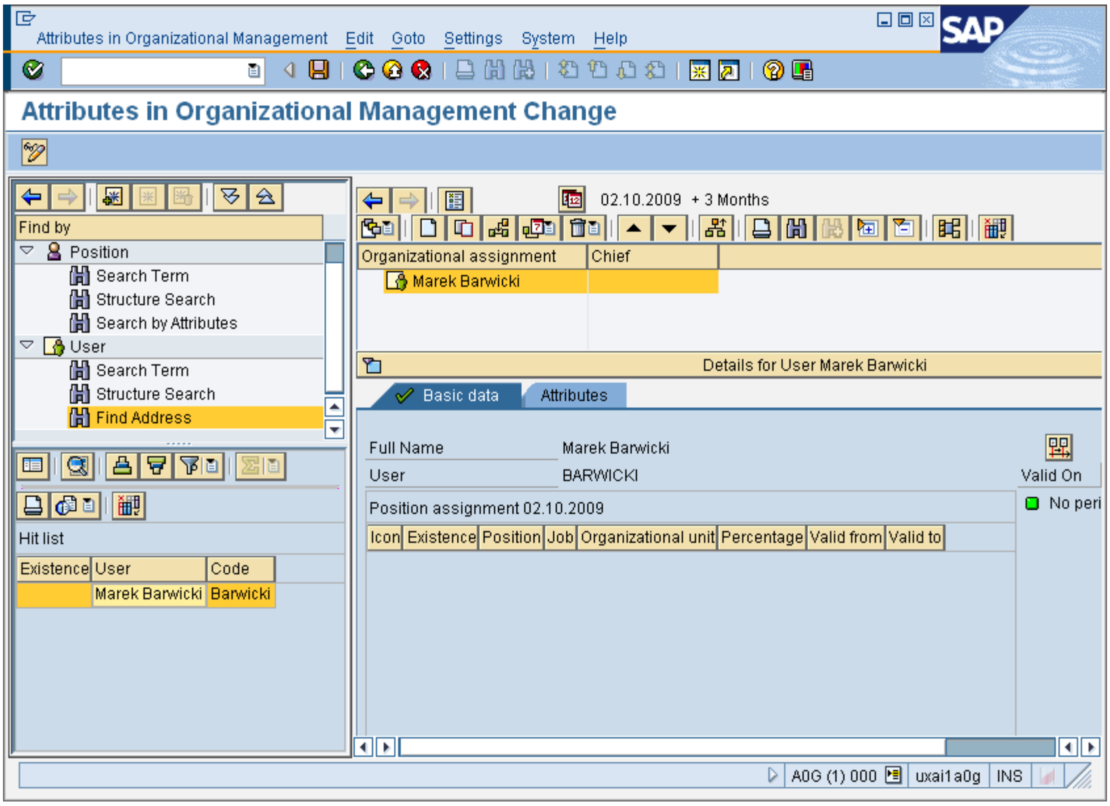
Step 5: Setting up the PFCG Profile

In this final step, after creating the business role and their corresponding PFCG role, you will assign restricted authorization to the user and check whether he still can run the business role.

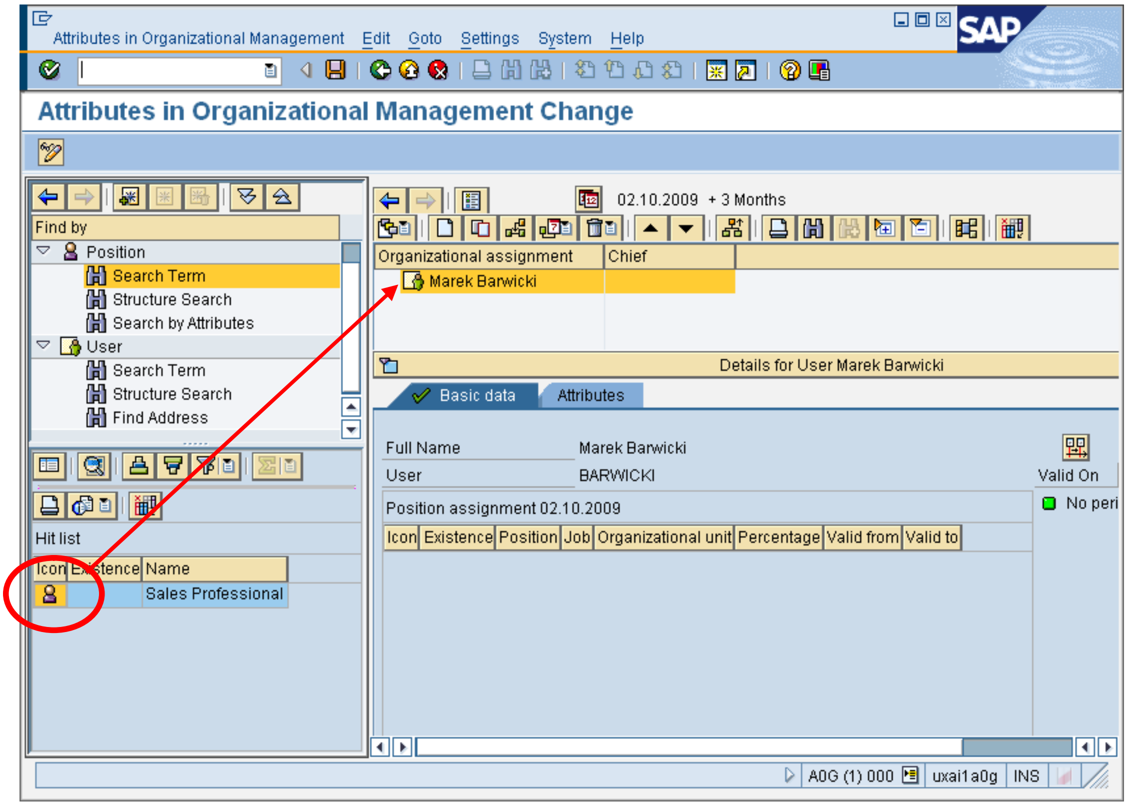
You have to perform the following steps:

Assign User to Right Position in the Organization

- Call the transaction PPOMA_CRM.
- Search for your user and click on it.



- Search the position you want to assign the user to.
- You can assign the position to the user by dragging the icon of the position to the user name (right hand side).



This chapter assumes that you are testing existing Business Roles which are already assigned to the organizational position. If you have created a new business role you have to assign it to the position like this:

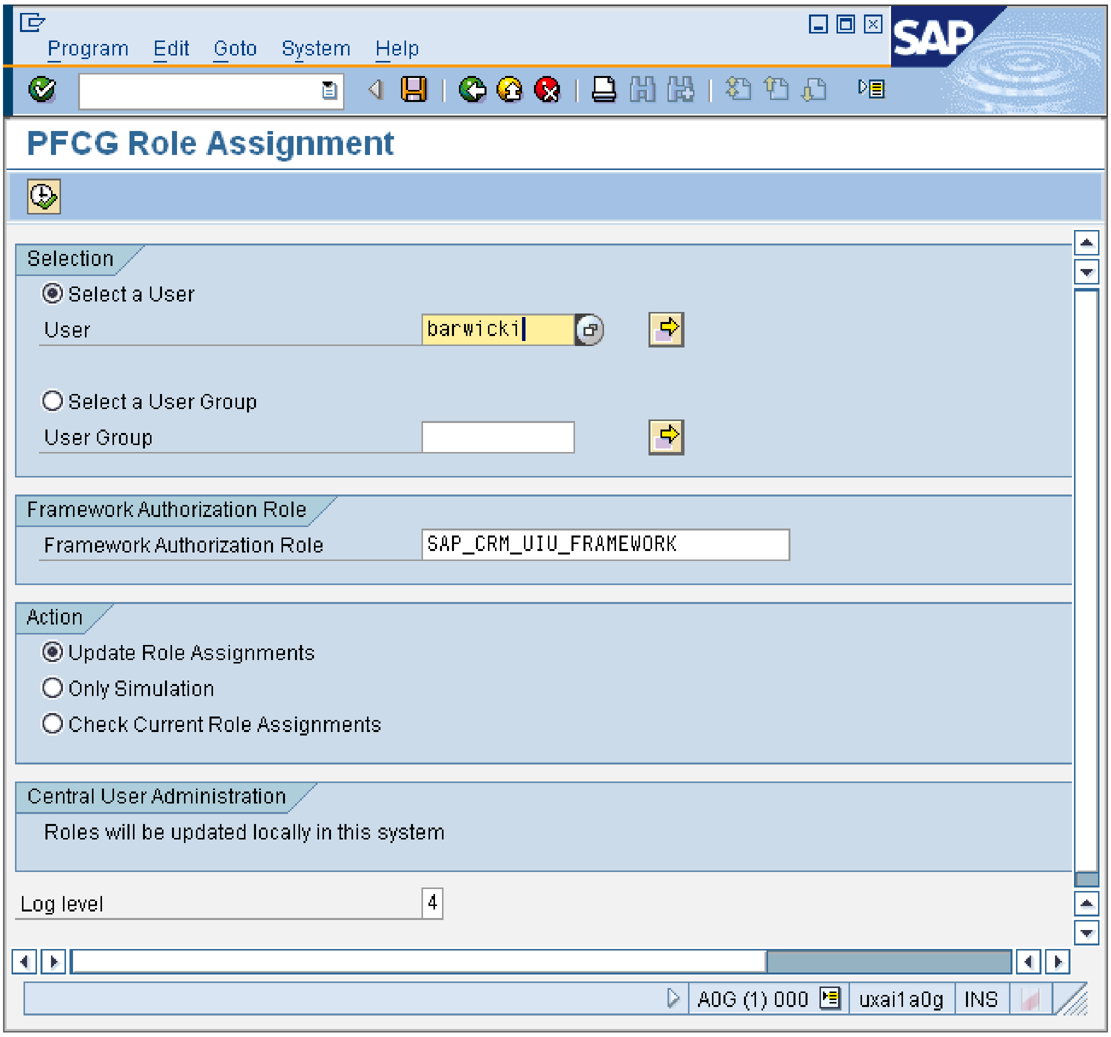
- Search for the Organizational Unit
    - Search for the organizational unit to which you want to assign the business role.
    - In the hit list on the left select the organizational unit.
    - Double-click the organizational unit or the position on the right.
- Assign Business Role to Organizational Unit or Position
    - Choose Goto → Detail object → Enhanced object description.
    - Select Business Role in the Active tab page.
    - Click Create infotype.
    - Enter the business role.

Assign User to PFCG Role

The user will be assigned to the right PFCG according to his position in the organization.

This is done using the report CRMD_UI_ROLE_ASSIGN. This report determines the business roles a user is assigned to. Based on the business role the PFCG profiles are determined and assigned.

- SE 38: CRMD_UI_ROLE_ASSIGN
- Select a business role.

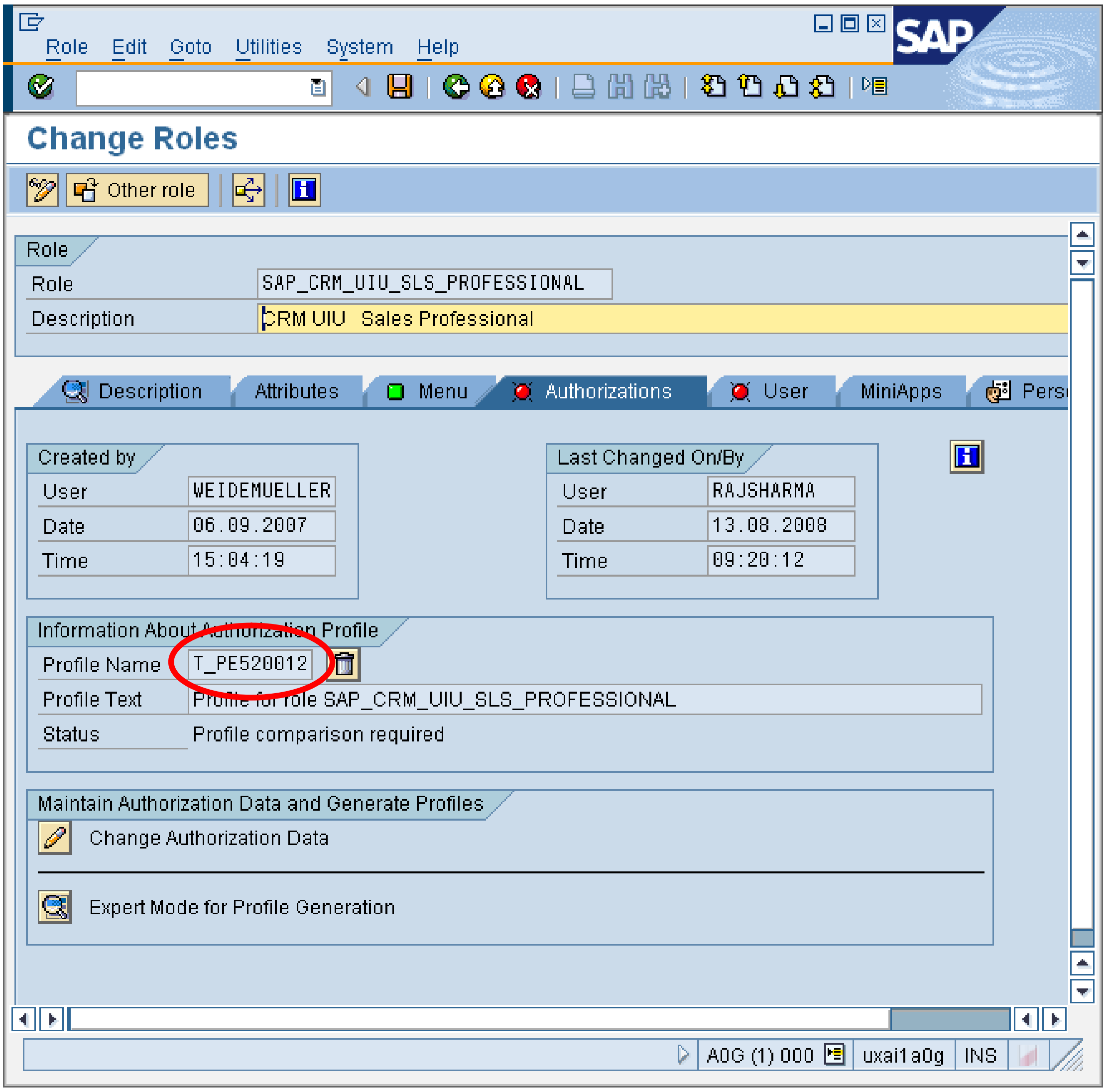


- Start first in simulation mode. After checking start the update of assignments.

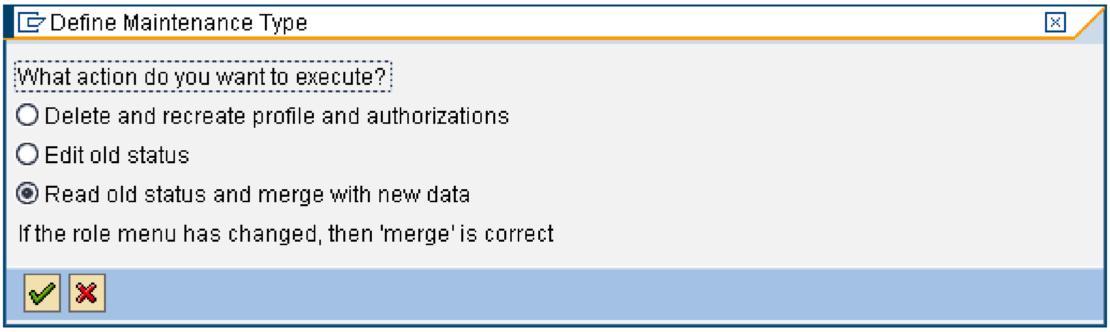
Setup the PFCG Authorization Profile

The user has been assigned to the PFCG role in the previous step. You have to update the PFCG authorization profile before start testing.

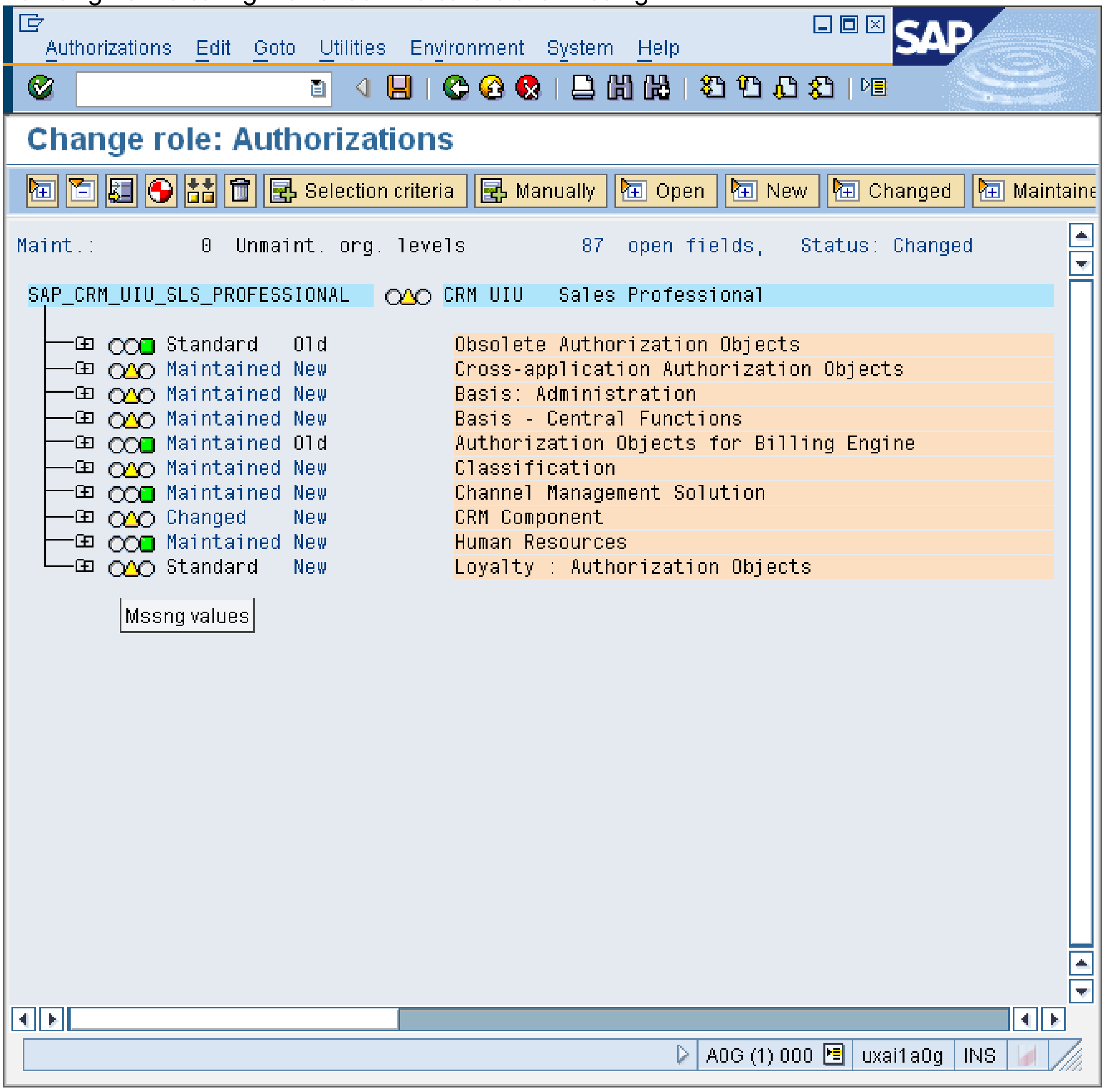
- If you have already maintained some authorization setting you should merge new authorizations (coming from SU24) with the existing ones.



- Click 'Expert Mode for Profile Generation' and merge existing setting with the new one.



- The PFCG profile has now already been created out of the PFCG role menu and the SU24 entries. As you can see, it's not yet completely maintained—there are yellow traffic lights indicating that check indicators are missing:



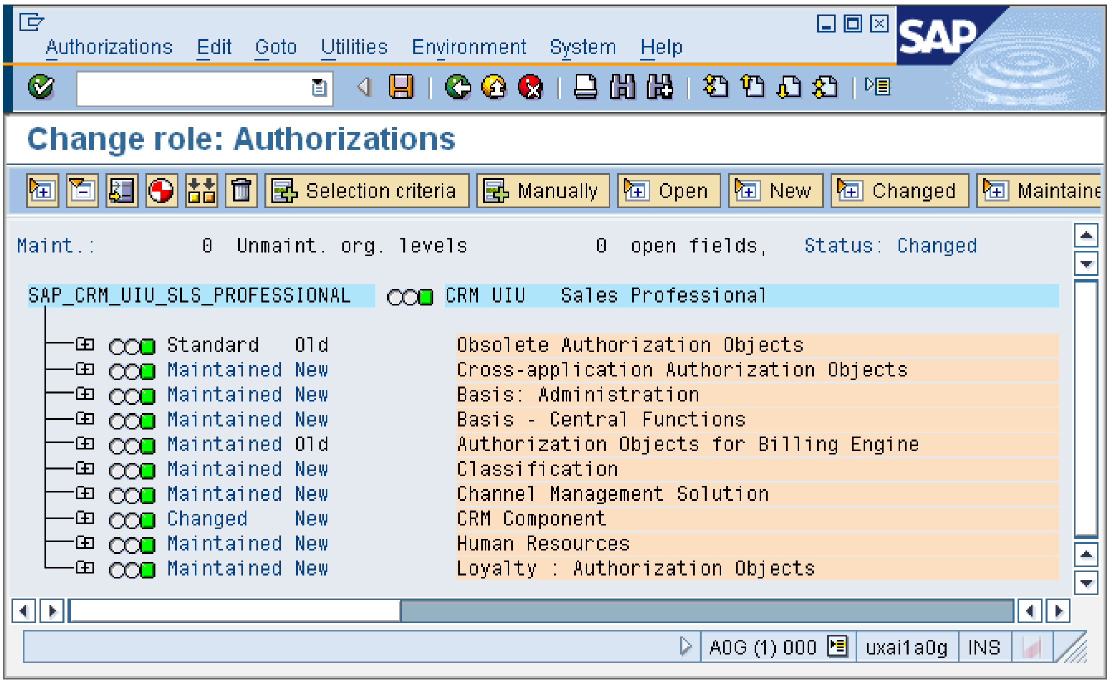
What is the meaning of the yellow traffic lights?

As described above, the PFCG profile is generated by "multiplying" the PFCG role menu entries with the SU24 authorization suggestion values to the the PFCG authorization profile. So only authorization objects which are directly needed for the business role are generated into the PFCG profile.

In the SU24 (or SU22 at SAP) the developers made suggestions for authorization object entries where possible—but not for all authorization object attributes for all authorization object suggestions can be made. E.g., there are authorization checks against customizing entries—as the developer does not know how the customizing of the customer will look like, nothing can be entered in the authorization object attribute value as suggestion.

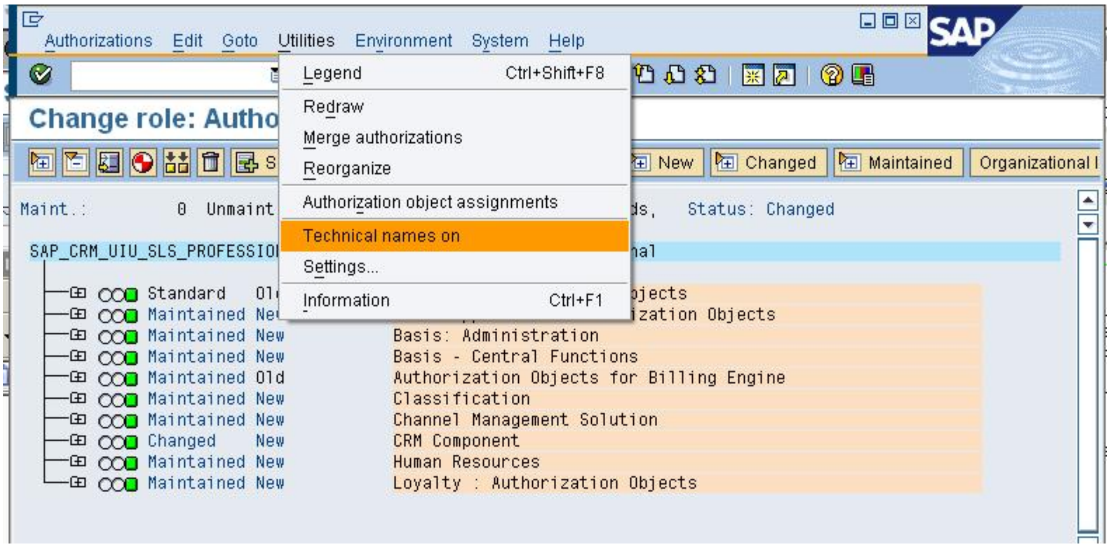
Such non-maintained authorization attributes in SU24 will now result in unmaintained fields in the PFCG profile—which is visualized via the yellow traffic lights.

- You have now to maintain all yellow entries until as the overall status is green.

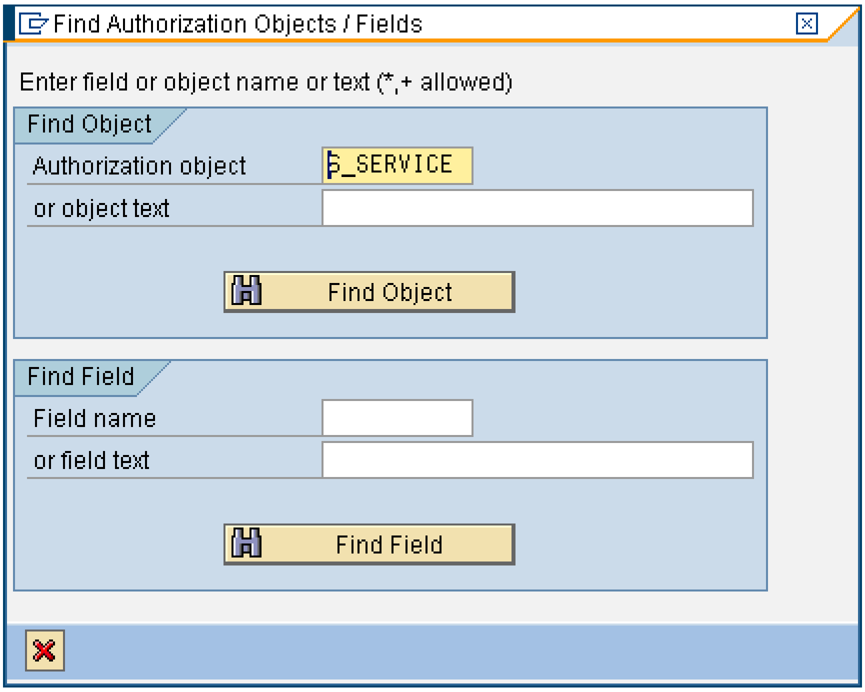


- Now you need to deactivate the authorization object S_SERVICE in the "Cross Application Authorization Objects".

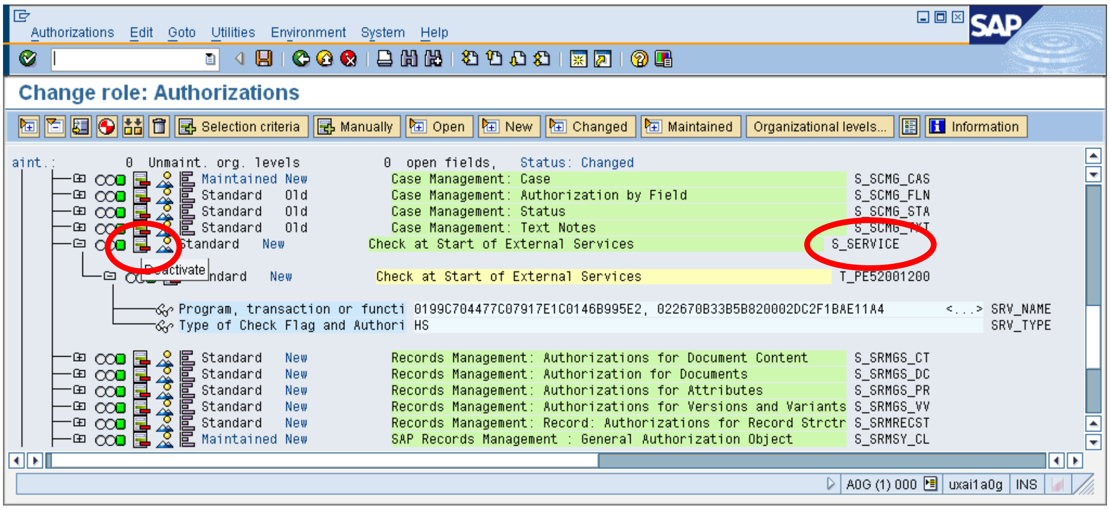
Hint: You can turn on the technical authorization object names via Utilities → Technical names on:



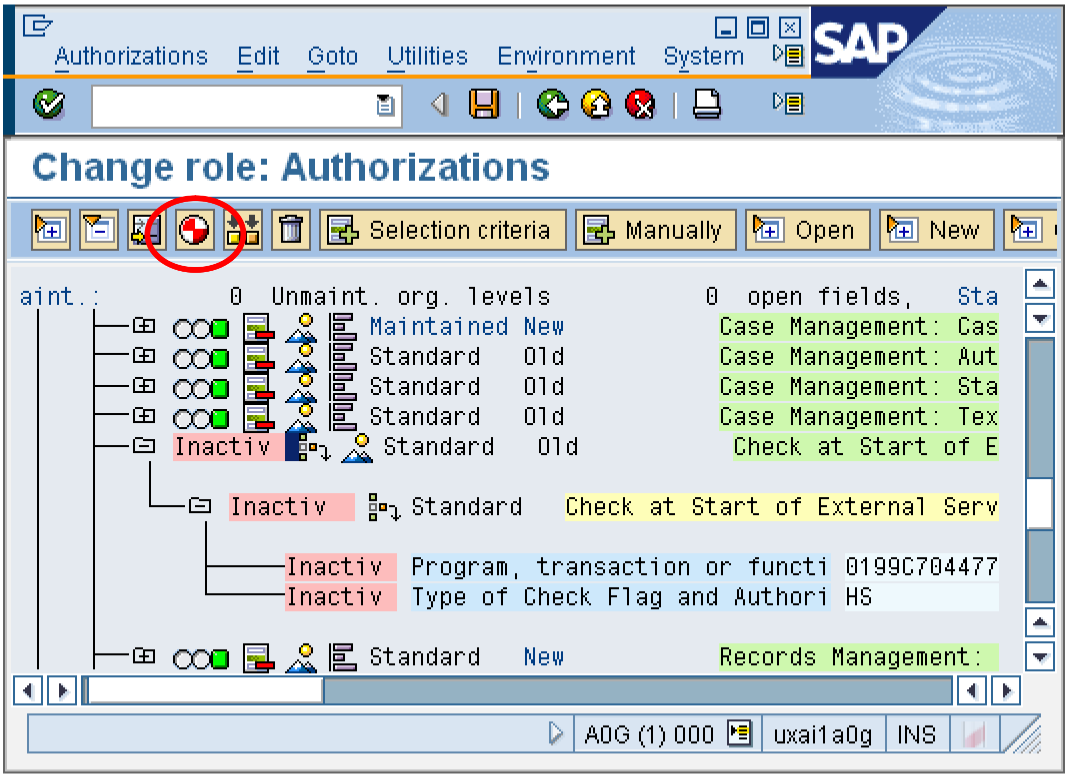
- Search for the S_SERVICE object.



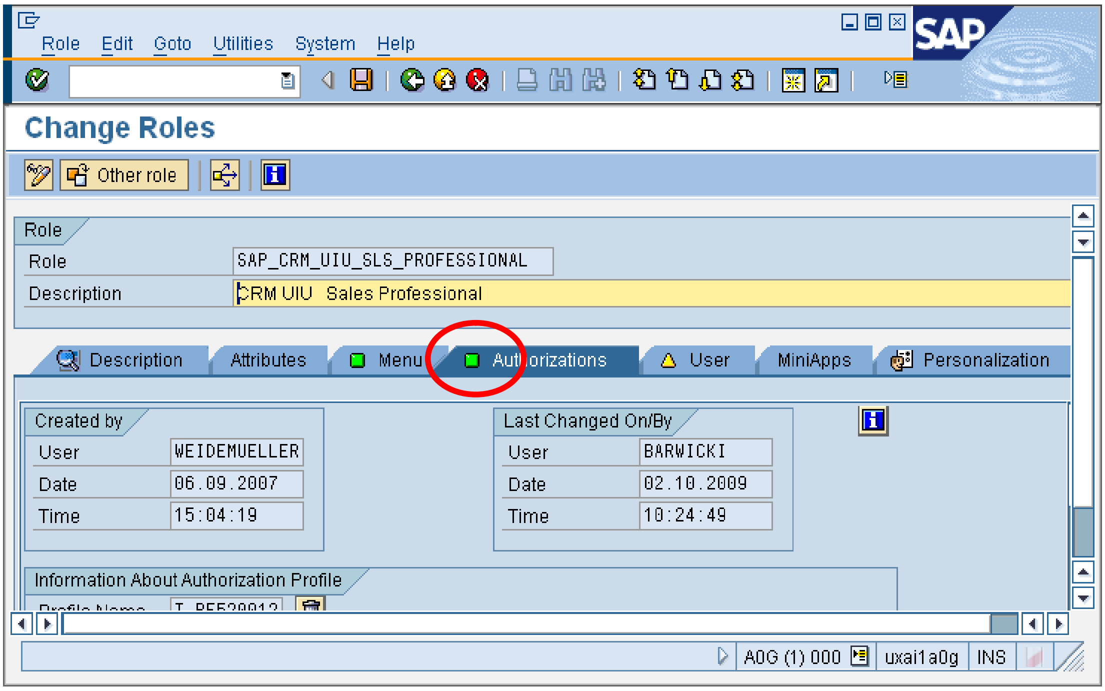
- Deactivate it.



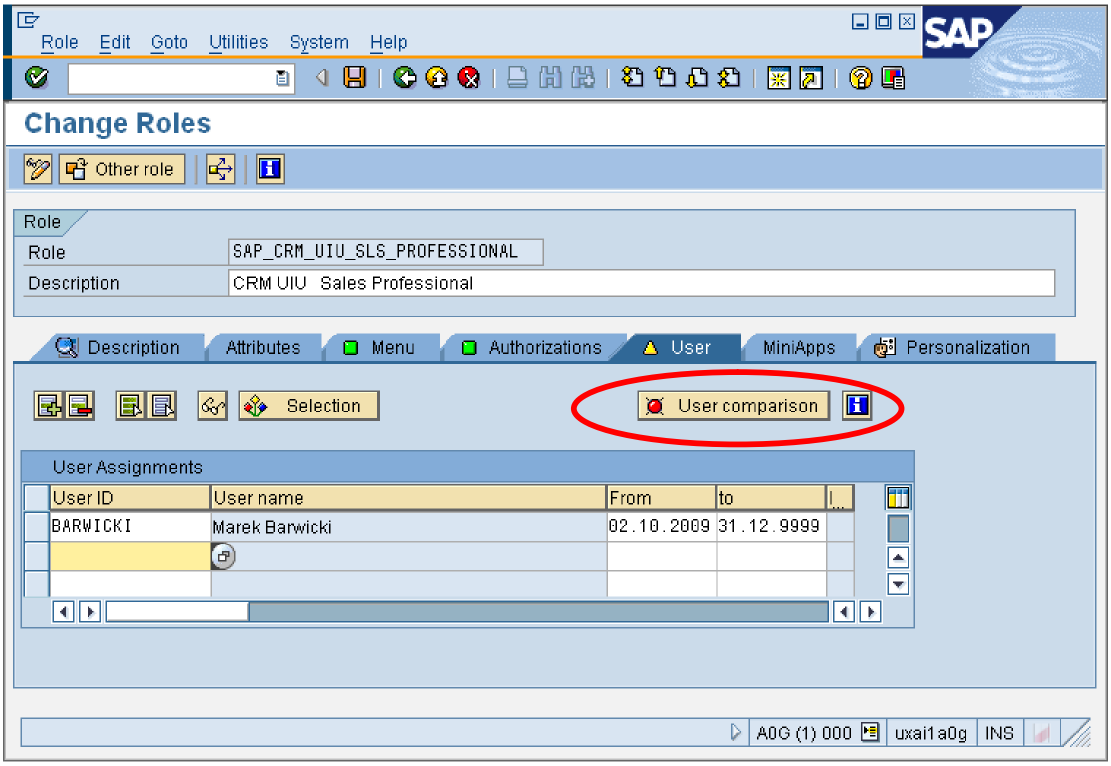
- Now save (and confirm the suggested PFCG profile name if asked).
- Generate the profile.



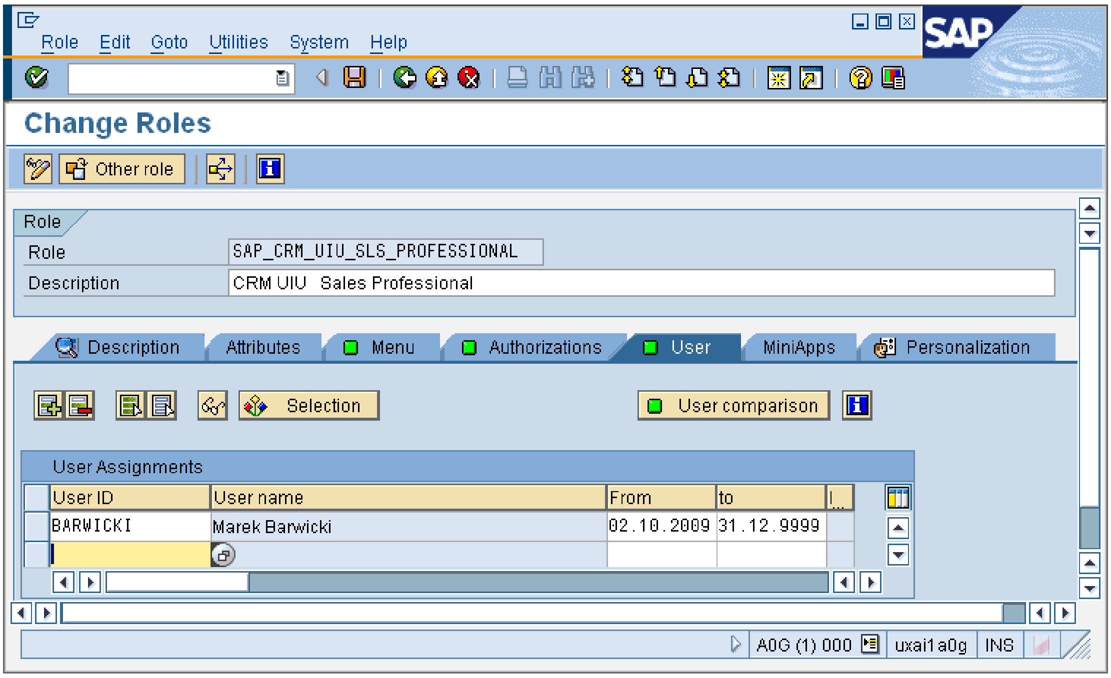
- Now the Authorizations tab has a green traffic light:



- Finally a user comparison has to be performed. Press the button "User Comparison" on the "User" tab and select "Complete Comparison":



- That's it! All traffic lights are green now:



Step 6: Testing with Restricted Authorizations

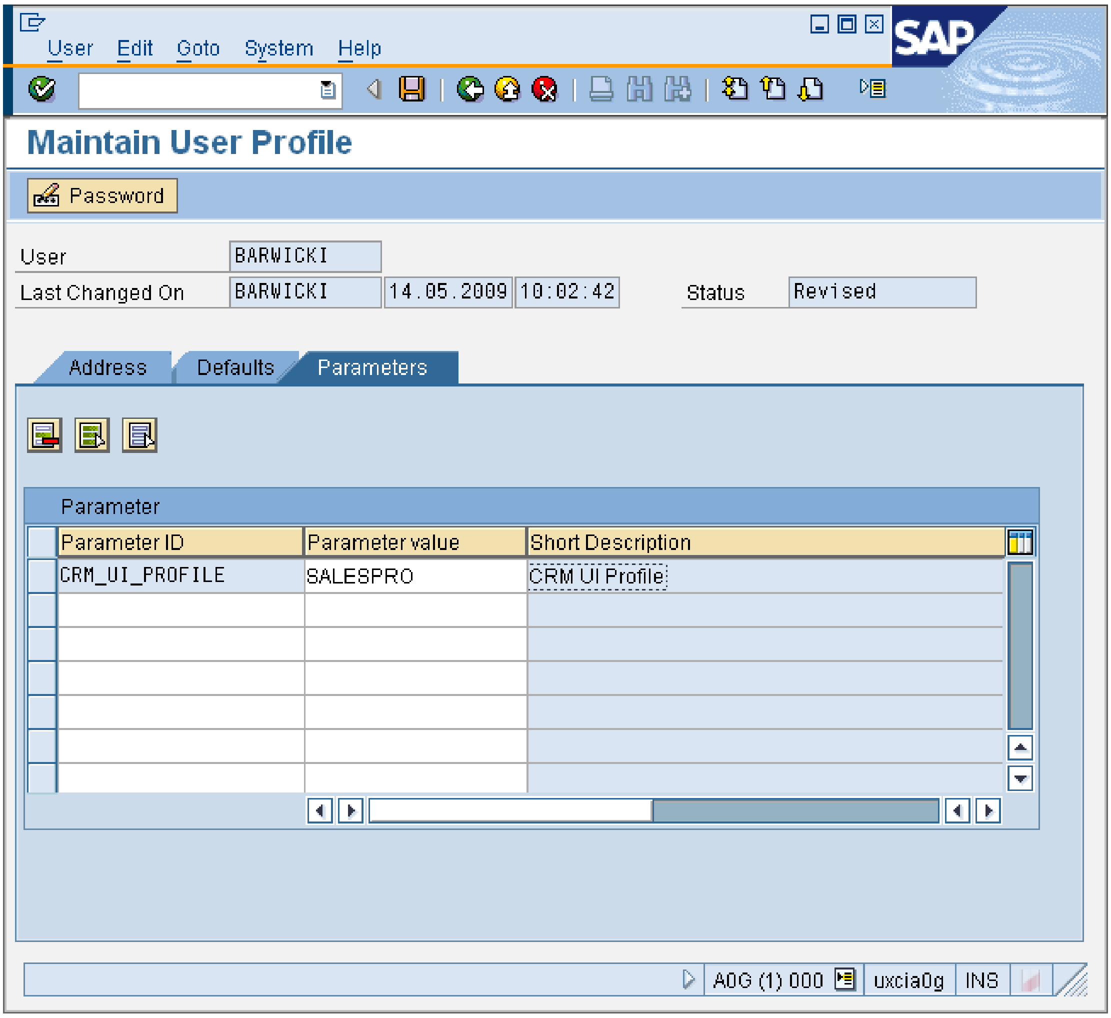
In this final step you have to run your application with restricted authorizations in order to find out whether the PFCG profile is set up correctly. This is the case if you do not encounter any errors due to missing authorization. Details on this topic are out of scope for this document but you can find details on how to analyze errors due missing authorization in the document 'CRM_Web_Client_Auth_Problems.pdf' attached to note 1244321.

3 Additional Useful Information

Determination of Business Roles

To use the CRM application a user needs to be assigned to a business role. The determination of the business roles is performed in the following order:

1. Check if a single business role is assigned using the user parameter `CRM_UI_PROFILE`. This setting overrules any other role assignments.



2. Check if there are business roles assigned via the organizational management.
3. If neither 1 nor 2 is the case, the system determines the PFCG roles assigned to the user and checks if they are linked to a business role. If this is the case, these business roles are used.

Documentation

You find detailed step-by-step descriptions on setting up authorizations for business roles in:

- Customizing for *Customer Relationship Management* under *UI Framework → Business Roles → Overview* and *UI Framework → Business Roles → Define Authorization Role*.
- SAP Help Portal (SAP CRM 7.0): Assigning Authorization Roles
- For information about assigning authorization roles, see also SAP Help Portal.
- SAP Note 1244321 provides information on how to analyze authorization issues. For more information, see SAP Note 1244321 - *Simplifying error analysis in CRM WebClient UI*.