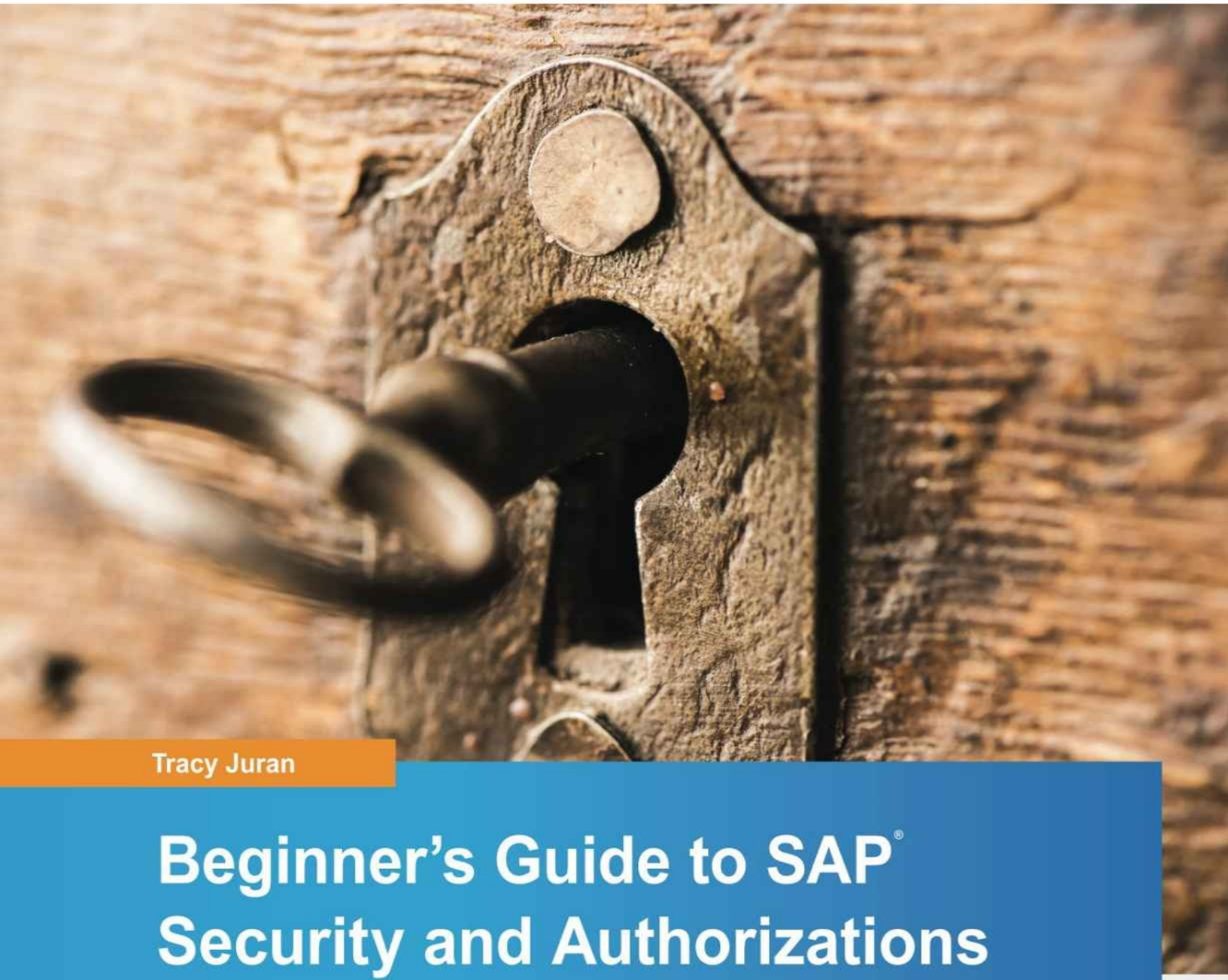
espresso tutorials



Tracy Juran

Beginner's Guide to SAP® Security and Authorizations

- Basic architecture of SAP Security and Authorizations
- GRC Access Control introduction
- User profile creation and role assignments
- Common security and authorization pain point troubleshooting

Tracy Juran

Beginner's Guide to SAP® Security and Authorizations

ISBN:	978-3-9451-7087-8 (ePUB)
Editor:	Lisa Jackson
Cover Design:	Philip Esch, Martin Munzel
Cover Photo:	Fotolia #51570006 © larshallstrom
Interior Design:	Johann-Christian Hanke

1st Edition 2016, Gleichen

URL: www.espresso-tutorials.com

Feedback:

We greatly appreciate any kind of feedback you have concerning this book. Please mail us at info@espresso-tutorials.com.

Thank you for purchasing this book from Espresso Tutorials!

Like a cup of espresso coffee, Espresso Tutorials SAP books are concise and effective. We know that your time is valuable and we deliver information in a succinct and straightforward manner. It only takes our readers a short amount of time to consume SAP concepts. Our books are well recognized in the industry for leveraging tutorial-style instruction and videos to show you step by step how to successfully work with SAP.

Check out our YouTube channel to watch our videos at https://www.youtube.com/user/EspressoTutorials.

If you are interested in SAP Finance and Controlling, join us at http://www.fico-forum.com/forum2/ to get your SAP questions answered and contribute to discussions.

Related titles from Espresso Tutorials:

- Boris Rubarth: First Steps in ABAP®
  http://5015.espresso-tutorials.com
- Sydnie McConnell, Martin Munzel: First Steps in SAP®, 2nd edition
  http://5045.espresso-tutorials.com
- Antje Kunz: SAP® Legacy System Migration Workbench (LSMW)
  http://5051.espresso-tutorials.com
- Darren Hague: Universal Worklist with SAP® NetWeaver Portal
  http://5076.espresso-tutorials.com
- Michał Krawczyk: SAP® SOA Integration—Enterprise Service Monitoring
  http://5077.espresso-tutorials.com

- Ann Cacciottolli: First Steps in SAP® Financial Accounting (FI)
  http://5095.espresso-tutorials.com

- Kathi Kones: SAP List Viewer (ALV)—A Practical Guide for ABAP Developers
  http://5112.espresso-tutorials.com

- Jelena Perfiljeva: What on Earth is an SAP IDoc?
  http://5130.espresso-tutorials.com

Table of Contents

For Alex and Tamara, whose enthusiasm is contagious, and for Merkel, who also caught the bug.

Preface: Introduction to SAP Security and Authorizations concept

SAP has a wide range of built-in functionality to meet various security requirements, including network protection, data protection, and SAP authorizations. This book will focus on the application of SAP authorizations and how user access can be limited by transaction codes, organizational levels, field values, *etc.* SAP Security and Authorizations is designed so that the system must explicitly indicate what each user can do. This is done by assigning authorization roles, which are groupings of profiles comprised of authorizations.

The basic architecture of SAP Security and Authorizations is a 6-tiered approach:

1. User Master Record: Accounts for users to enable access to the SAP system; primarily used for user administration purposes.
2. Role: Compilation of transactions and permissions that are assigned to one or more user master records; usually includes commonality amongst a job role or job task.
3. Profile: Assigned when a role is generated and added to its corresponding user master record.
4. Authorization Object Class: Logical grouping of authorization objects by business area.
5. Authorization Object: Groupings of 1-10 authorization fields; configuration is performed against authority check statements written in the SAP code.
6. Authorization Field: Least-granular element in which values can be maintained to secure data and information.

Authorizations can be useful in limiting access to items such as: billing and vendor information, personnel and payroll information, key financial data, and critical system areas such as basis, configuration, development, and security. Users obtain their authorizations by being assigned to roles and users cannot start a transaction or complete a transaction without the proper authorization role assignment. In order to perform an action, a user may need several authorizations. For example, in order to create a sales order, the user will need access to the transaction, the “create” authorization, general authorization for the sales org, and the authorization for the specific sales document type. Therefore, the relationships required in order to meet user access requirements can become very complex.

The SAP authorization concept was created on the basis of authorization objects. Each authorization object is comprised of multiple authorization fields. A user’s permissions always refer to authorization objects, which can contain a single value or a range of values for each field. Both report and dialog transactions in SAP have predefined “authorization checks” imbedded in the program logic which protects the functions and information within them.

The basis of an organization’s role design should always be the *rule of least privilege*, which is the SAP Security best practice of giving users exactly what they need to perform their job responsibilities, not much more, and not much less. *Access creep* is the adversary of this privilege as users may retain unnecessary access after a job function change or may receive unnecessary access as a result of the application of permissions or transactions to roles which are shared between users who have similar, but not identical, responsibilities. Ultimately, security is the gateway to the SAP system, but it can often be difficult to manage and understand. Information stored in SAP is a valued business asset, and SAP Security can aid an organization by increasing flexibility and customization at the user level and protecting critical information from unauthorized use.

This book includes SAP best practices for user and role maintenance and how to create an SAP Security design that is both low maintenance and scalable. You will learn how to use and interpret SAP authorizations and troubleshoot security and authorization issues. Lastly, you will discover some advanced topics surrounding SAP authorizations, including an overview on upgrading your SAP Security environment and reducing avoidable segregation of duties conflicts.

We have added a few icons to highlight important information. These include:

Tips

Tips highlight information concerning more details about the subject being described and/or additional background information.

Examples

Examples help illustrate a topic better by relating it to real world scenarios.

Attention

Attention notices draw attention to information that you should be aware of when you go through the examples from this book on your own.

Finally, a note concerning the copyright: all screenshots printed in this book are the copyright of SAP SE. All rights are reserved by SAP SE. Copyright pertains to all SAP images in this publication. For simplification, we will not mention this specifically underneath every screenshot.

1 User maintenance overview

This chapter covers creating users in the system and assigning roles to their corresponding user master records. This section also provides information on assigning personal attributes to each user, password rules in SAP, and creating and assigning user groups. Additionally, the chapter includes the method for performing a mass change to user master records.

A person must have an SAP user ID and password in order to log into an SAP system. This information is stored in the *user master record*. User master records are client-specific. It is important to establish a naming convention for the user ID, which allows the user to be easily identifiable after taking into account any pre-existing identification systems within the organization. Often times, an existing e-mail or network naming convention is ideal. Some compilation of a user's name is also a viable option, for example:

First letter of the first name, last name

- TLEVINE (Tracy Levine)

Last name, first letter of the first name, first letter of middle name

- LEVINETM (Tracy M Levine)

Last name, country of origin

- LEVINEMX (Tracy Levine, Mexico)

User IDs are limited to a minimum length of 3 characters and a maximum length of 12 characters. However, user IDs that are both required and predelivered by SAP in the system: SAP* and DDIC. SAP* is a super user in SAP and does not need a user master record. This ID is hard-

coded in the system and provides the ID with unlimited access. The SAP* default password should be changed, but it cannot be deleted. DDIC is the maintenance user in SAP and has special privileges surrounding the ABAP dictionary and installations. DDIC is the only user ID that can log on during a system upgrade.

1.1 User master record

The user master record maintenance transaction, SU01, is primarily used to create and modify user master records in the SAP system. As previously mentioned, user master records are intended as a repository to store user information and assign necessary authorizations to a user to perform necessary job responsibilities. In the initial SU01 screen (see Figure 1.1), the SAP Security administrator can carry out the following activities:

- Create user master record (**PAPER** button)
- Change user master record (**PENCIL** button)
- Display user master record (**GLASSES** button)
- Delete user master record (**TRASH CAN** button)
- Copy user master record (**DUAL PAPER** button)
- Lock/Unlock user master record (**LOCK** button)
- Change password of user master record (**WRITING PENCIL** button)

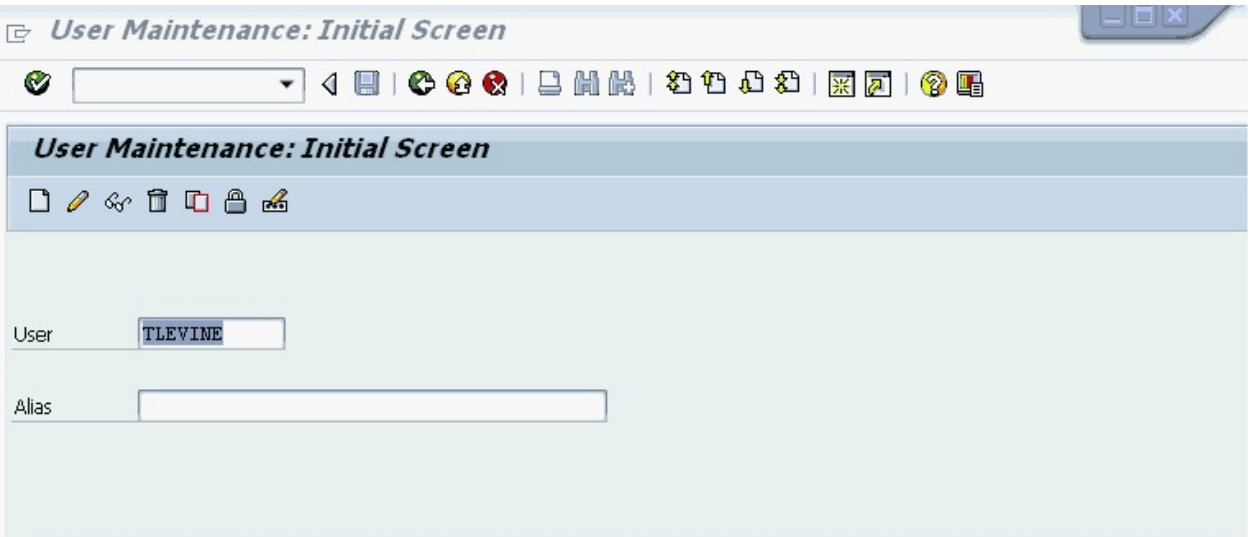


Figure 1.1: User master maintenance initial screen (transaction SU01)

In order to execute any of the above functions, a user ID must be defined in the **USER** field, as shown in Figure 1.1. An *alias* is used to perform activities that interact with SAP via the Internet. When a user registers an alias on the Internet (such as a customer or vendor name) a corresponding SAP user ID is automatically generated at random. The **ALIAS** field on the **USER MAINTENANCE** initial screen is used to uncover the unknown SAP user IDs of Internet users.

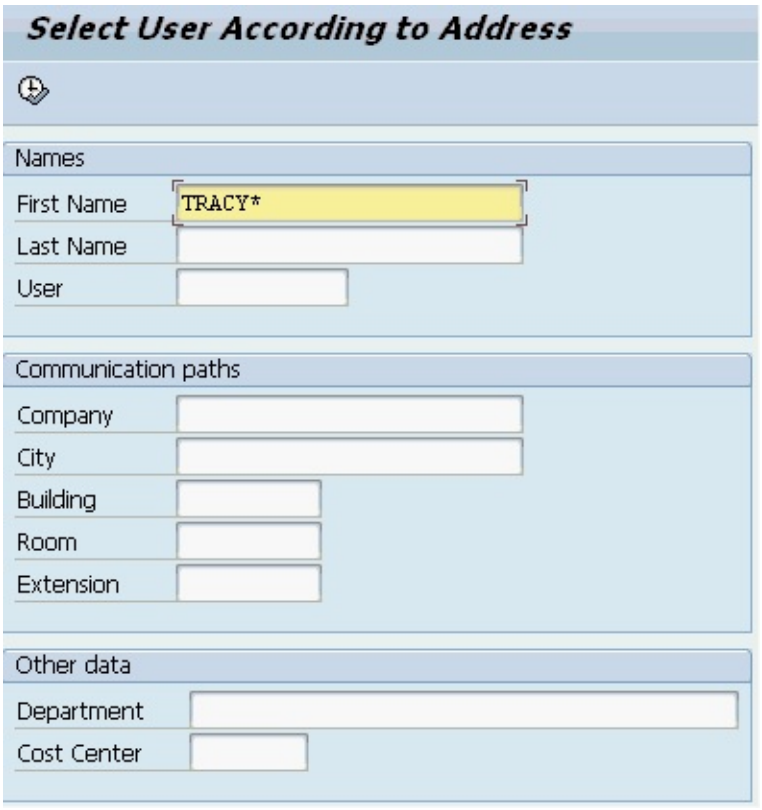


Figure 1.2: User master maintenance address tab (transaction SU01)

The **ADDRESS** tab in SU01 (see Figure 1.2) is used to more completely identify the users and to supply contact information. The **ADDRESS** tab should be filled out as completely as possible. The button for **OTHER COMMUNICATION** allows for additional entries of various communication methods that are more atypical, and therefore, not on the main screen (such as **PAGER** and **URL HOMEPAGE**). The **COMM. METH** drop-down allows you to identify the user's preferred communication method.

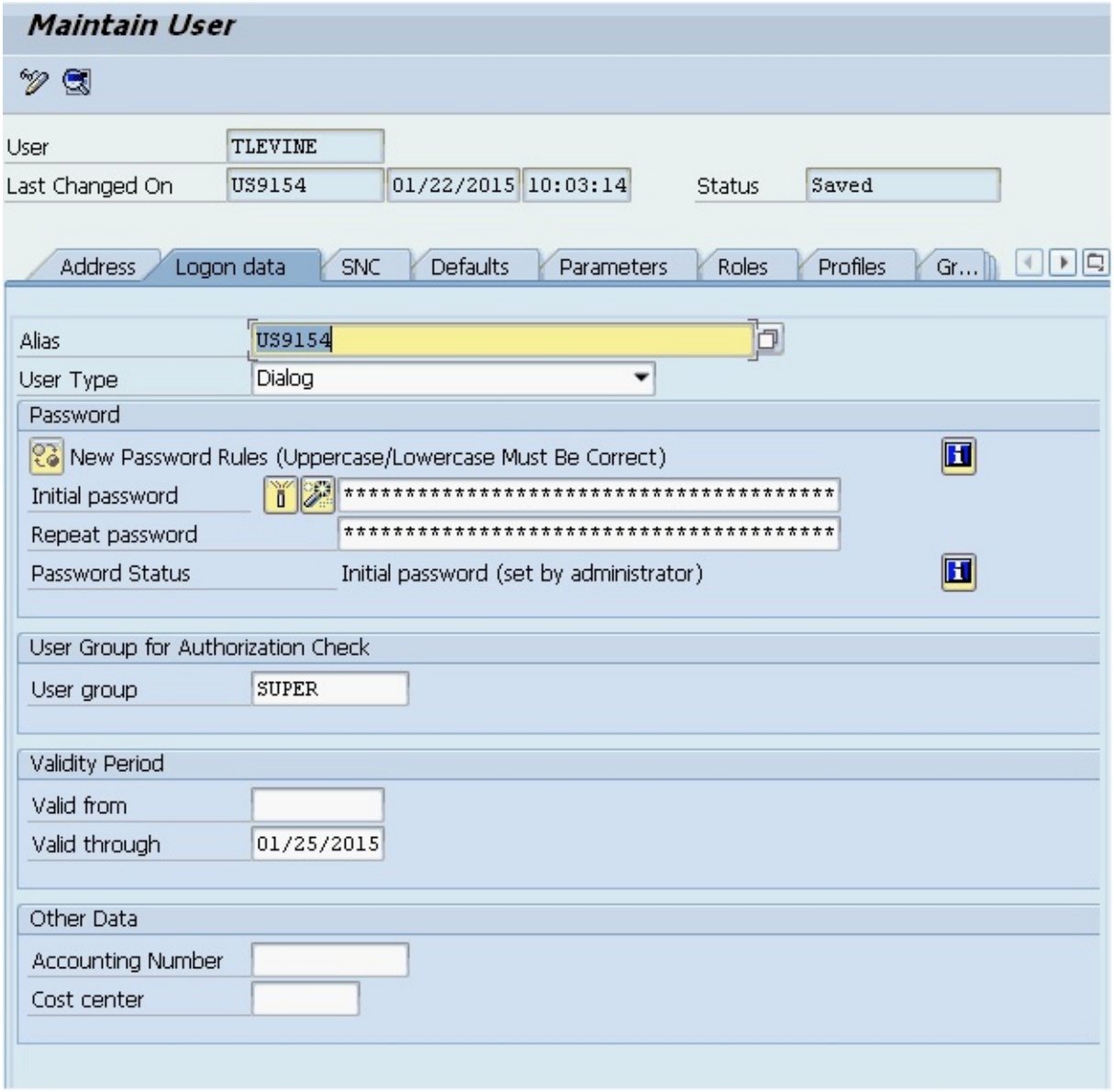


Figure 1.3: User master maintenance logon data tab (transaction SU01)

The **LOGON DATA** tab in SU01 (see Figure 1.3) is primarily focused on user validation upon logon. The **ALIAS** field allows the SAP Security administrator to assign a recognizable 40-digit ID to the user, which can be used to search for the user ID on the initial SU01 screen as shown in Figure 1.1. The two mandatory sections on the **LOGON DATA** tab are **USER TYPE** field and the **PASSWORD** area. The purpose of the **USER TYPE** field is to identify the type of user who will be transacting in the system. Section 1.2 outlines the different user types and their primary purposes. When a new user is created, the SAP Security administrator must enter an **INITIAL**

PASSWORD.

The **USER GROUP** field is valuable when multiple security administrators are responsible for maintaining user master records, but for different groups of users. If no user group is defined, any administrator has the ability to modify the user master record.

Maintaining different user groups: Example

If an organization has five SAP Security administrators and each is responsible for one geographical region, five different user groups should be maintained: 1. NORTH
2. SOUTH
3. EAST
4. WEST
5. CENTRAL

Other organizations can segregate user maintenance by company code or functional area.

The validity period section is beneficial for multiple reasons. Many organizations like to keep a record of all user master records even if an account or a user has been terminated. The **VALID THROUGH** field can be used in this instance to prohibit anyone from logging in with a particular ID. The user master record can also be locked by the administrator on the initial screen. **VALID FROM** and **VALID THROUGH** are often used as a means of assigning access to a temp or seasonal employee.

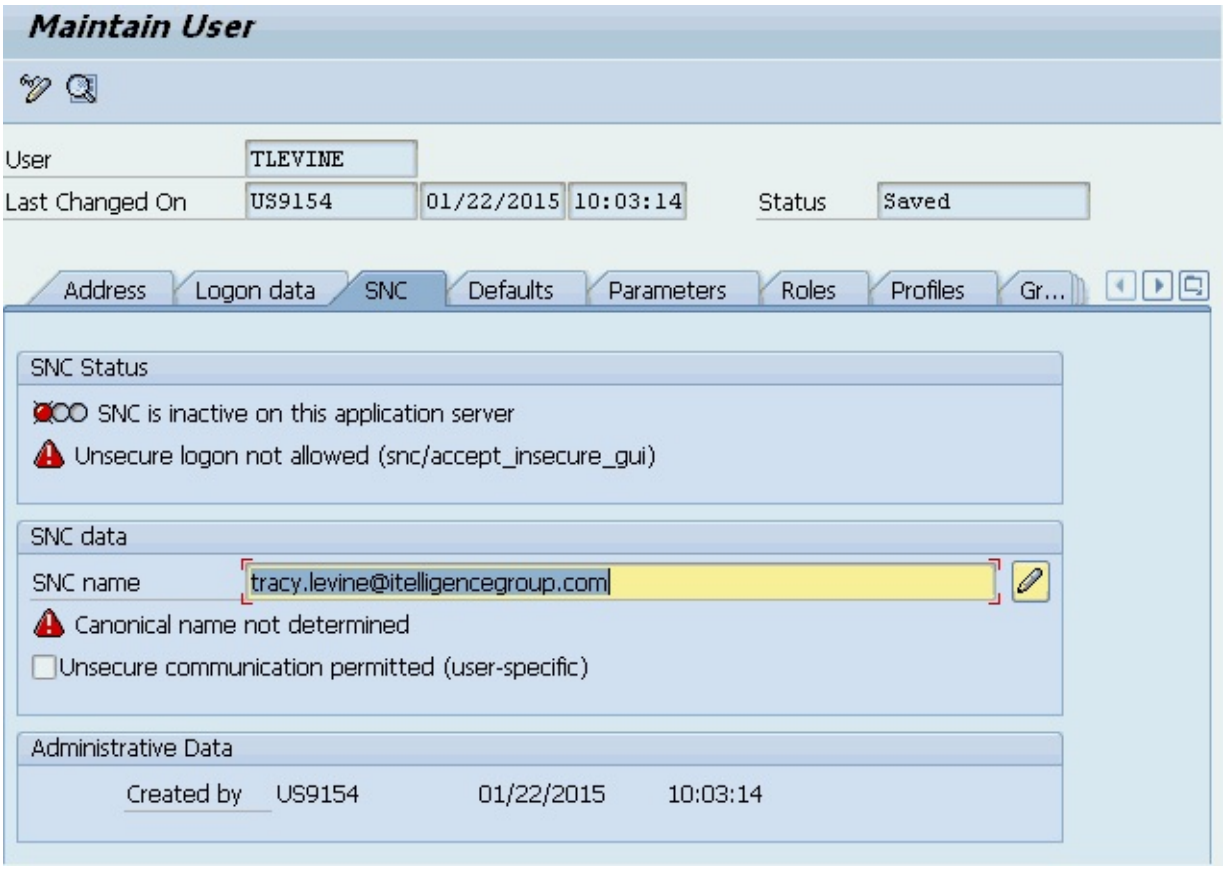


Figure 1.4: User master maintenance, SNC tab (transaction SU01)

On the **SNC** tab of SU01 (see Figure 1.4) the field for **SNC NAME** is used when the user will access the SAP system via a secure network connection rather than logging in with a user ID and password. The SAP system is limited in that only a single SNC name can be assigned to each user in the system for auditing purposes.

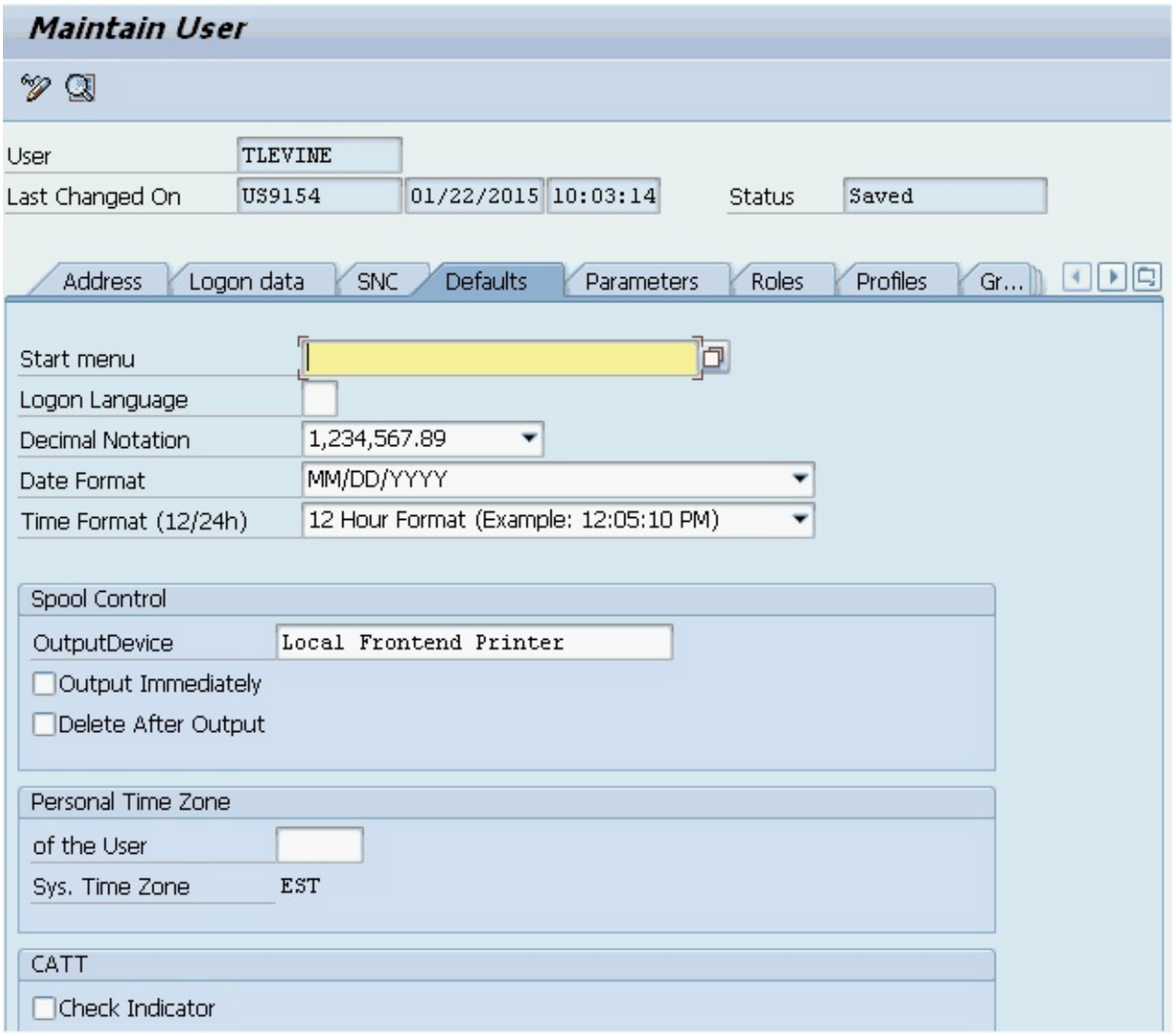


Figure 1.5: User master maintenance, defaults tab (transaction SU01)

The **DEFAULTS** tab in SU01 (see Figure 1.5) is used as it is described to establish default settings for maintaining the user ID, such as the date and time format that will be appear throughout the system. The **OUTPUTDEVICE** field is used to define a default printer to the user. If multiple languages have been configured in the system the **LOGON LANGUAGE** field can be set for each user. Likewise, if all users are not transacting at the same time, the **PERSONAL TIME ZONE OF THE USER** field can be set. The **START MENU** field is maintained if there is a user who wants a particular default menu upon logon.

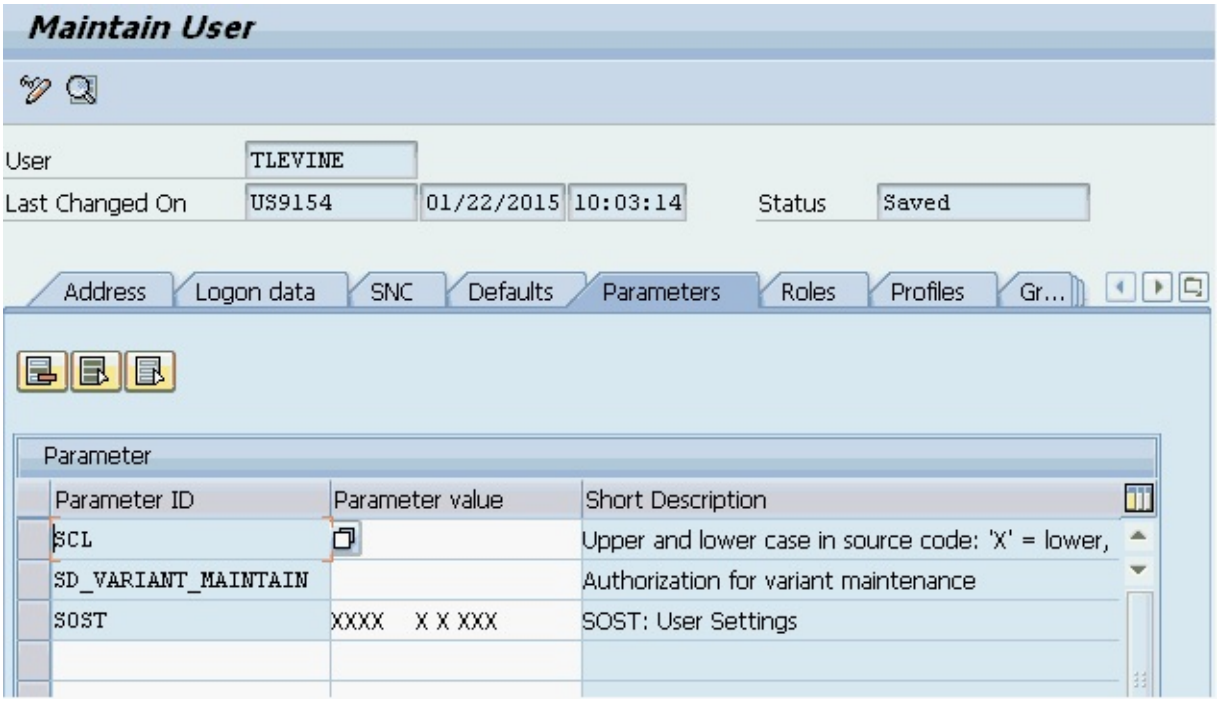


Figure 1.6: User master maintenance, parameters tab (transaction SU01)

The **PARAMETERS** tab in SU01 is often maintained as a means of identifying additional user defaults and settings, which increase system convenience (see Figure 1.6). Additionally, some user authorizations can be maintained via the **PARAMETERS** tab.

Example

If a user only requires authorization for company code 2000, this information can be stored under the corresponding parameter ID. Any transactional fields that refer to that organization unit will be automatically populated with 2000.

Another example refers to user authorization rather than user defaults. You will learn more about authorization objects later, but currently, standard SAP authorization objects only exist for maintaining global layouts (all reports and transactions) or finance-only related reports and transactions. As demonstrated in Figure 1.6,

the parameter SD_VARIANT_MAINTAIN controls a user's authorization to maintain variants for sales-and distribution-related reports and transactions. The following parameter values each equate to a different level of variant maintenance:

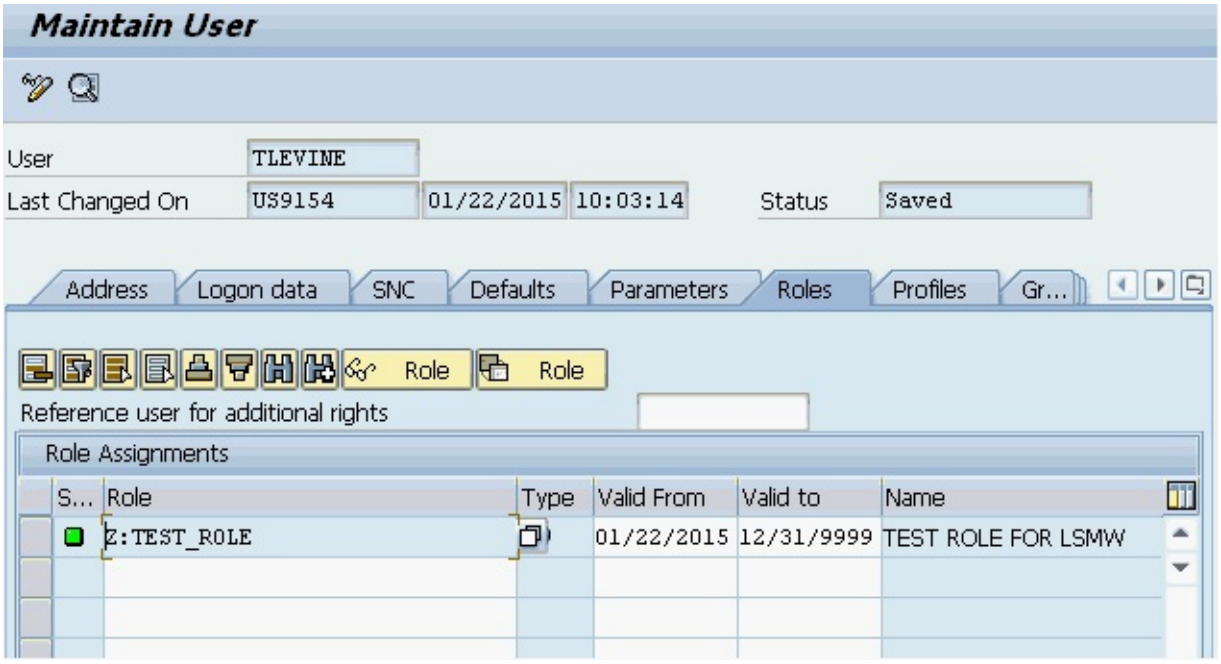


Figure 1.7: User master maintenance (transaction SU01, roles tab (transaction SU01)

An *SAP role* is a compilation of transactions and permissions that are assigned within the user master record. The **ROLES** tab in SU01 is where the SAP Security administrator can display or modify all role assignments for the user (see Figure 1.7). A user can be assigned to more than one role. More on role types later on, but the **TYPE** column in the **ROLES** tab indicates whether the role is a *composite role* (a compilation of single roles that are assigned as a group) or a *single role*. The **VALID FROM** and **VALID TO** fields indicate when the assignment will become or became active and when the role assignment will expire. The **VALID TO** field automatically defaults to "12/31/9999."

If a single role is assigned as a result of the assignment of a corresponding composite role, the role name will appear in blue, rather than black. In this instance, the assignment of these single roles cannot

be maintained individually; assignments can only be removed and the validity dates modified at the composite role level.

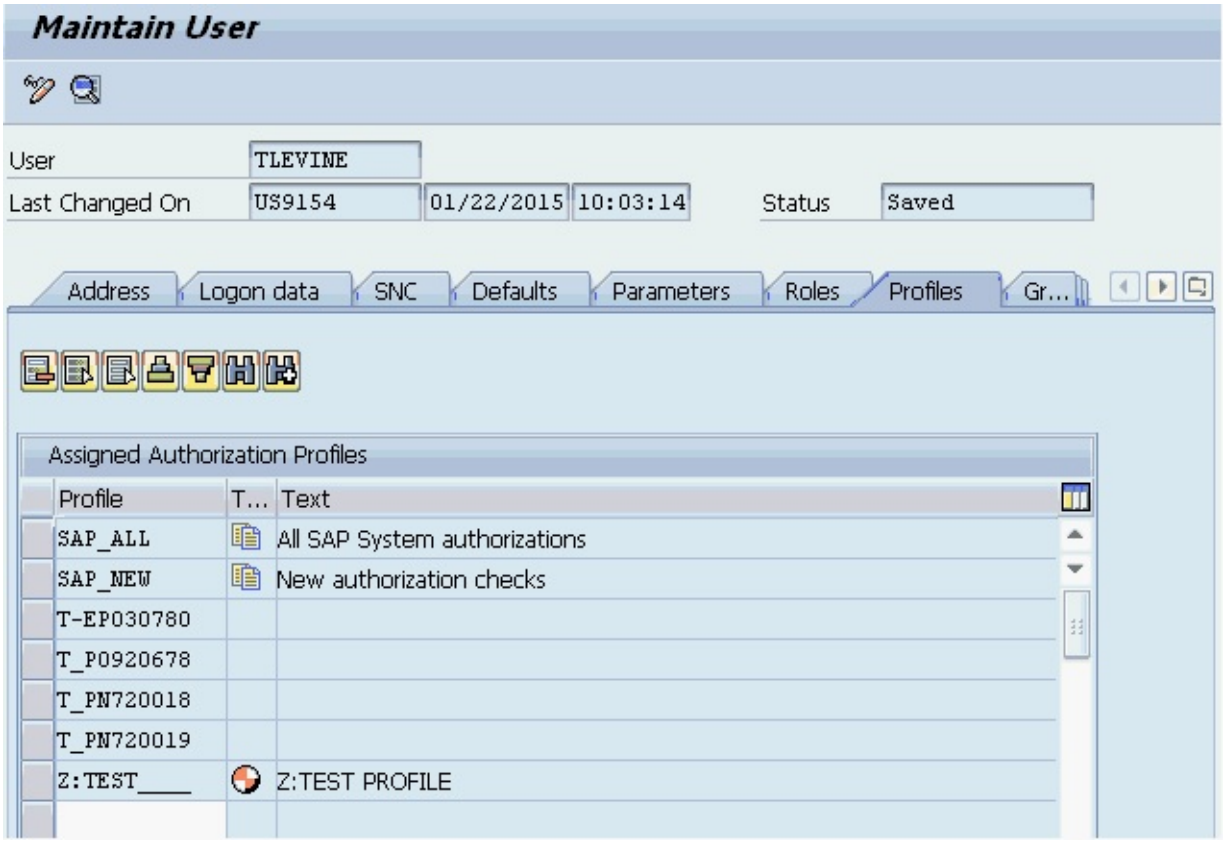


Figure 1.8: User master maintenance, profiles tab (transaction SU01)

Authorization profiles are created when roles are generated. When roles are added to the user master record, the corresponding profile(s) also get assigned via the **PROFILES** tab (see Figure 1.8). With the exception of a few preconfigured SAP profiles for super-user access, profiles should not be directly assigned to users. The maximum number of profiles that can be assigned to a user is 312. The relationship of roles:profiles is typically 1:1, unless a role contains a significant amount of transactions and permissions (i.e. a 'display all' or super-user role). As mentioned, SAP has two primary preconfigured profiles that can be assigned only to system administrators and SAP support users.

1. SAP_ALL is a compilation of all standard authorizations that exist in the SAP system.

2. SAP_NEW is a compilation of all new standard authorizations that exist in the SAP system (includes authorization objects brought in from new releases).

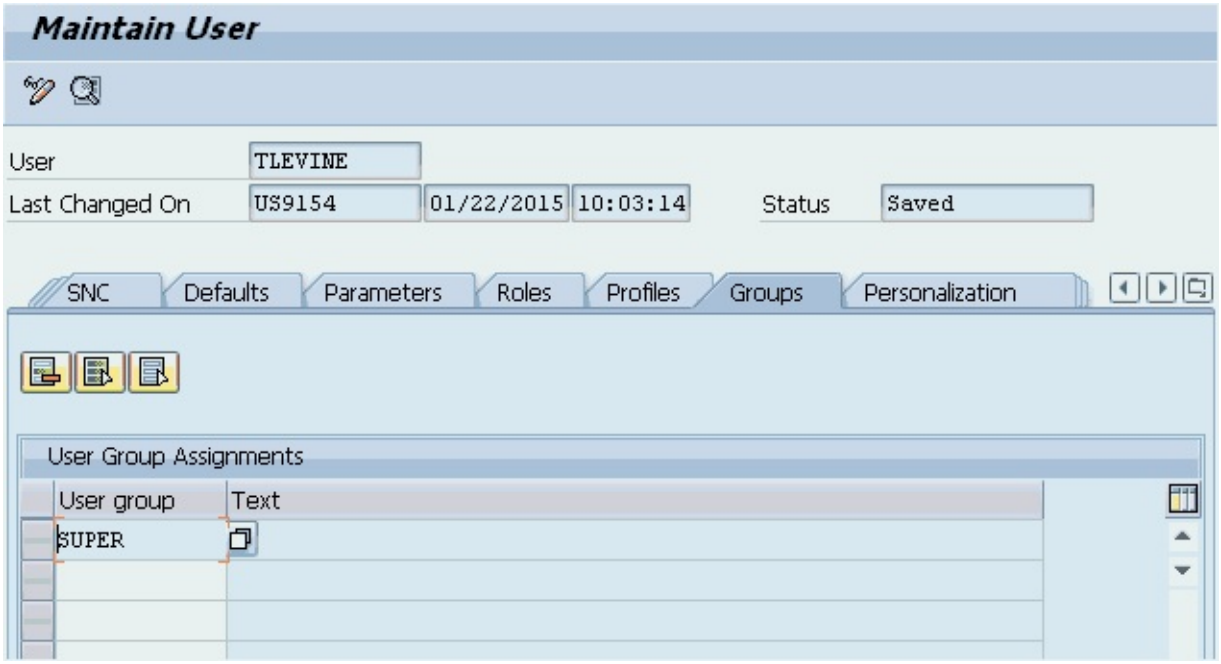


Figure 1.9: User master maintenance, groups tab (transaction SU01)

Multiple user groups can be assigned to the user master record in the **GROUPS** tab (see Figure 1.9). If there are multiple user administrators, groups can be set up and assigned to specific users. SAP Security administrators are then assigned user master record maintenance based on user group and, therefore, mass changes can be easily made to users in groups. See Section 1.3 for more information on user groups.

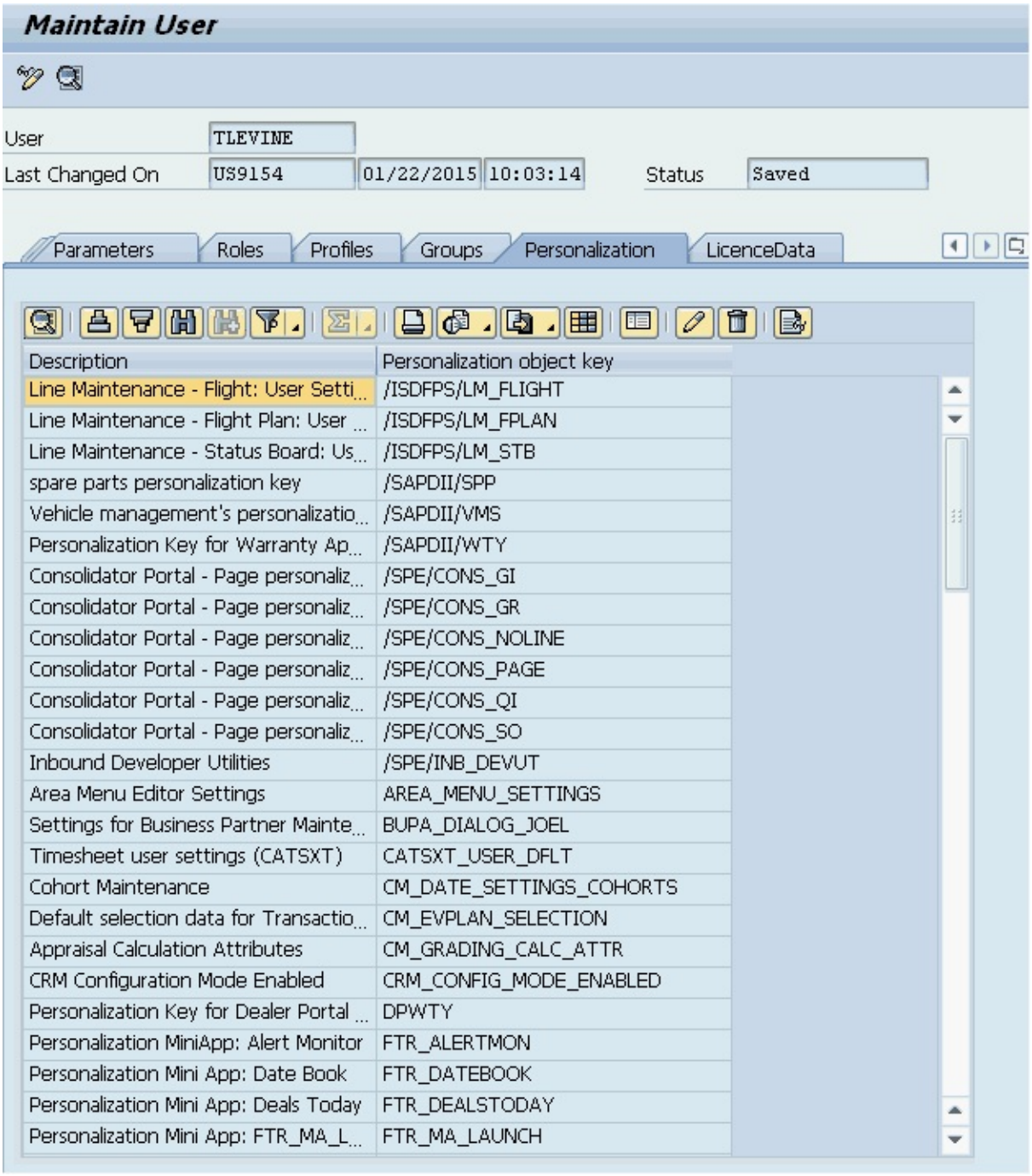


Figure 1.10: User master maintenance, personalization tab (transaction SU01)

The **PERSONALIZATION** tab in SU01 is just that; the location where personalized objects are stored, such as workflows, user layouts, time sheet settings, approvals, *etc.* (see Figure 1.10). Personalization objects can also be assigned to a specific role in the role maintenance transaction (PFCG) in the **PERSONALIZATION** tab.

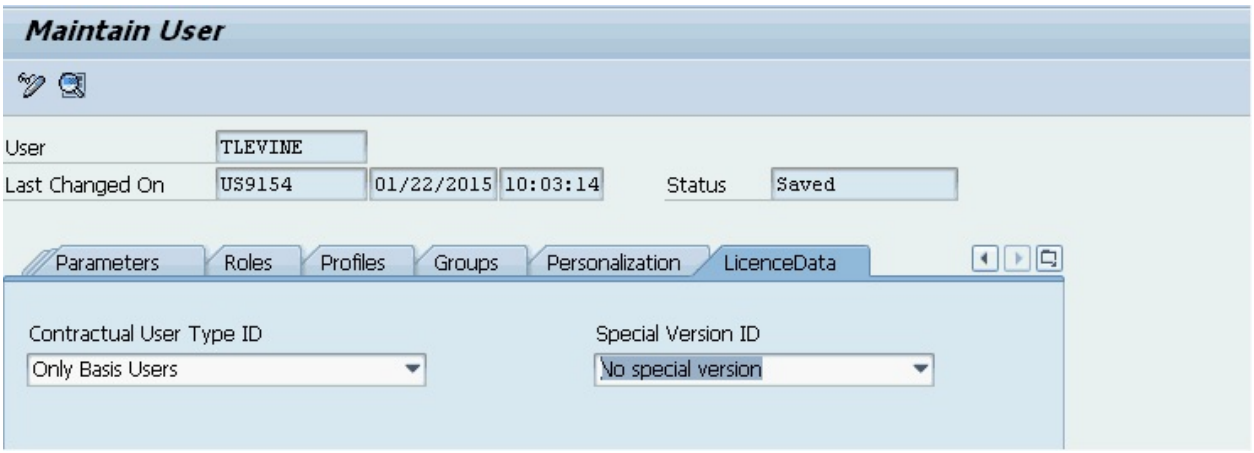


Figure 1.11: User master maintenance, license data tab (transaction SU01

The **LICENSE DATA** tab (see Figure 1.11) is used to track information that is processed for licensing purposes by SAP. SAP charges different rates based on contractual user types, which are determined based on the amount of transacting the user does in the system.

1.2 User types

In the SU01 **LOGON DATA** tab, users must be classified as one of the following user types (see Figure 1.3):

- *Dialog*: **Dialog users are the most common user type assigned to end users who will be transacting in the system.** Dialog users are checked at logon for initial passwords, user ID, password validity, and the allowance of multiple logons. The password for the dialog user can be changed by the user.
- *Communication:* Communication users are assigned to CPIC (common programming interface for communications) and RFC (remote function call) users that do not require dialog logon. Communication users are commonly used **between SAP and external systems and applications** for ALE, TMS, and workflow.
- *System:* System users are similar to communication users in the sense that they are assigned to CPIC and RFC users that do not require dialog logon. However, system users are used for ALE, background processing, TMS, and workflow within **one system.**

System users have no password validity and multiple logons are allowed. System user passwords can only be changed by SAP Security administrators. Multiple logons are allowed via a system user ID.

- *Service:* **Service user IDs are used by transacting-anonymous dialog users** through an ITS (information technology service), often a Web application. Multiple logons are allowed, but there is no check for initial or obsolete passwords. Multiple logons are allowed via a service user ID.
- *Reference:* Reference IDs are used for groups of users who require identical authorization. Reference users simplify the assignment of authorizations Web users. Dialog logon is not possible for a reference user.

1.3 User groups

User group assignment is not a required field when creating users. However, in order to delegate user maintenance authorization to different SAP Security administrators, this is a necessary step.

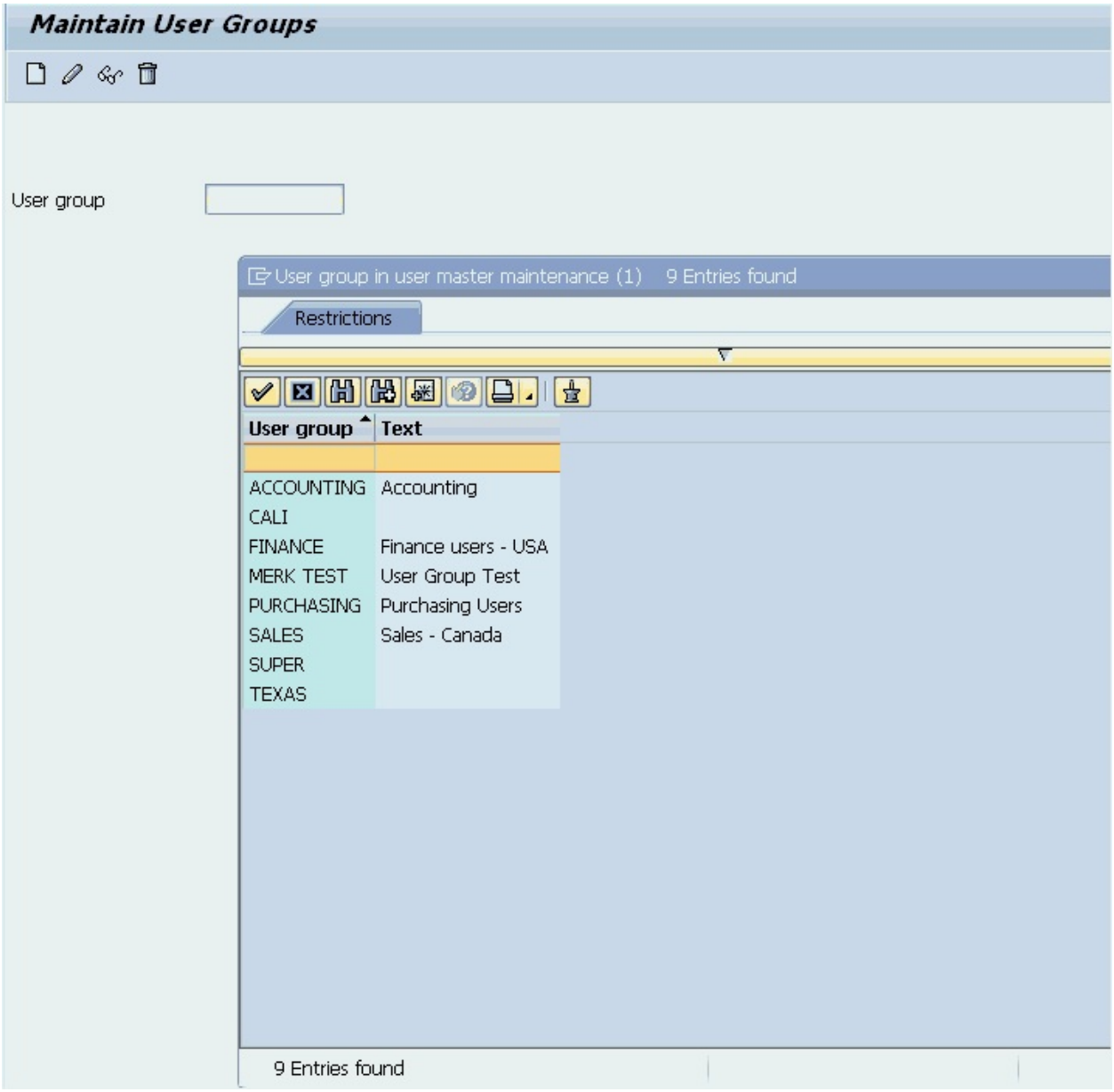


Figure 1.12: Maintain user groups (transaction SUGR)

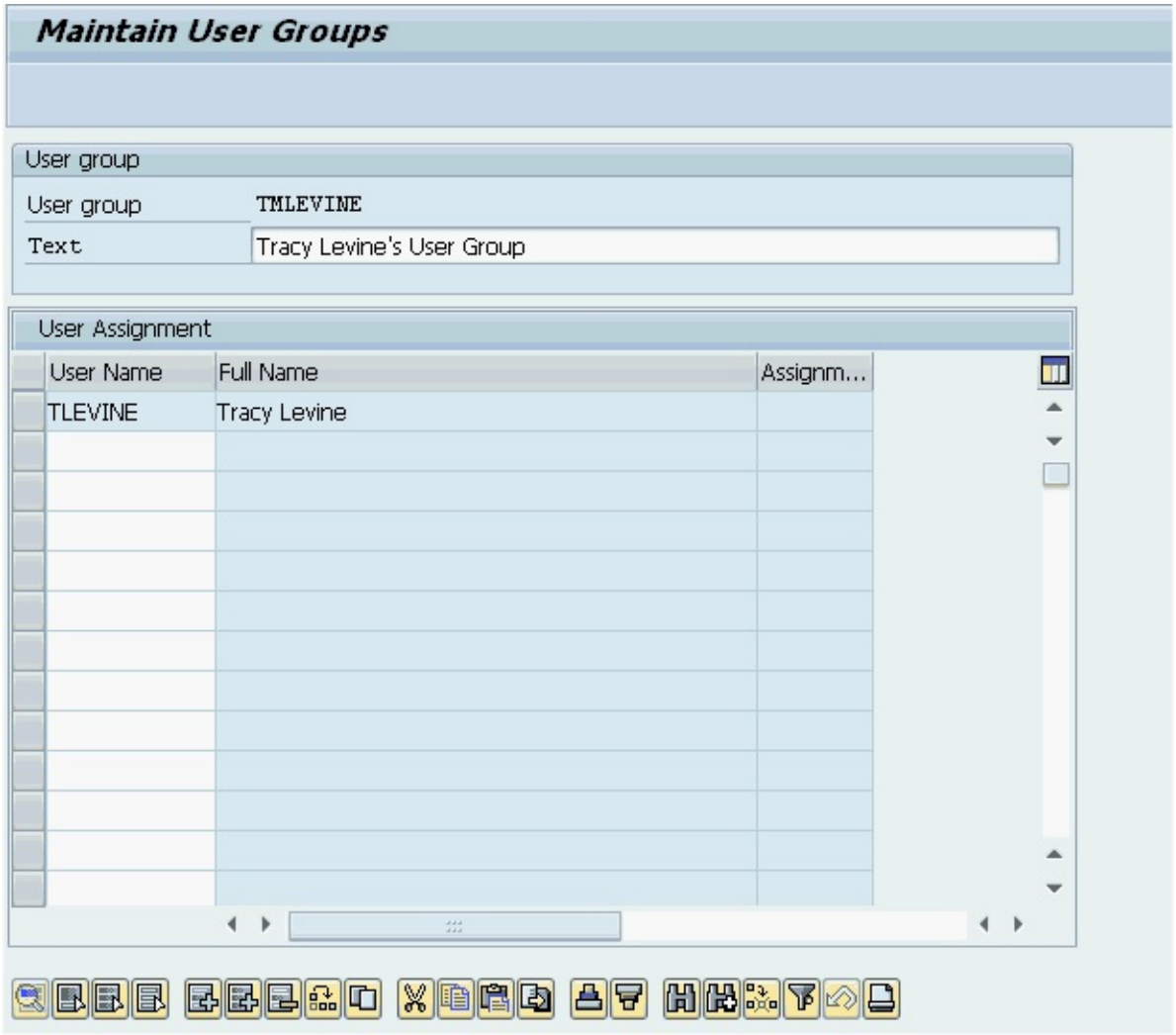


Figure 1.13: Assigning users to user groups (transaction SUGR)

User groups can be created, displayed, deleted, and modified via transaction SUGR as demonstrated in Figure 1.12. Users can also be assigned to a user group in transaction SUGR, as they can in the **USER GROUP** tab in SU01 (see Figure 1.13).

1.4 Mass user maintenance (SU10)

Transaction SU10 allows for mass maintenance of user master records. Using SU10, a user can perform most of the changes made on individual users in the user maintenance transaction (SU01), but for many users at one time.

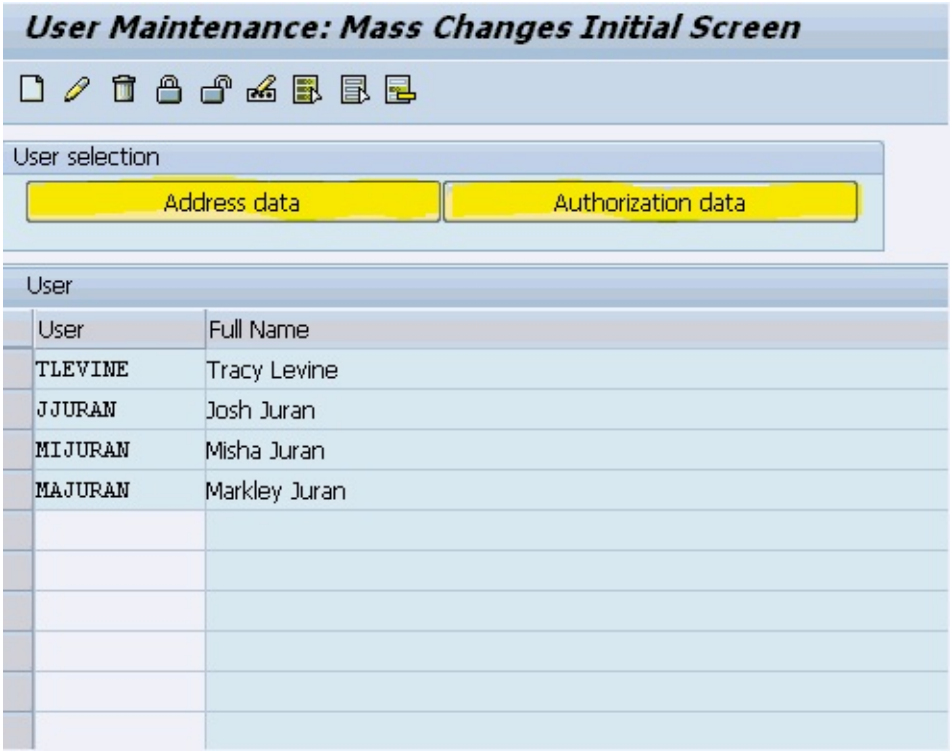


Figure 1.14: User maintenance: Mass changes initial screen (transaction SU10)

As demonstrated in Figure 1.14, on the initial SU10 screen a maximum of 25 SAP user IDs can be copied from the clipboard for user mass maintenance. If mass changes are required for more than 25 users, a wider selection of users can be chosen by clicking on the **ADDRESS DATA** button or **AUTHORIZATION DATA** button, as highlighted. In each of these tabs, a greater list of user IDs can be copied from a clipboard or selected based on various attributes.

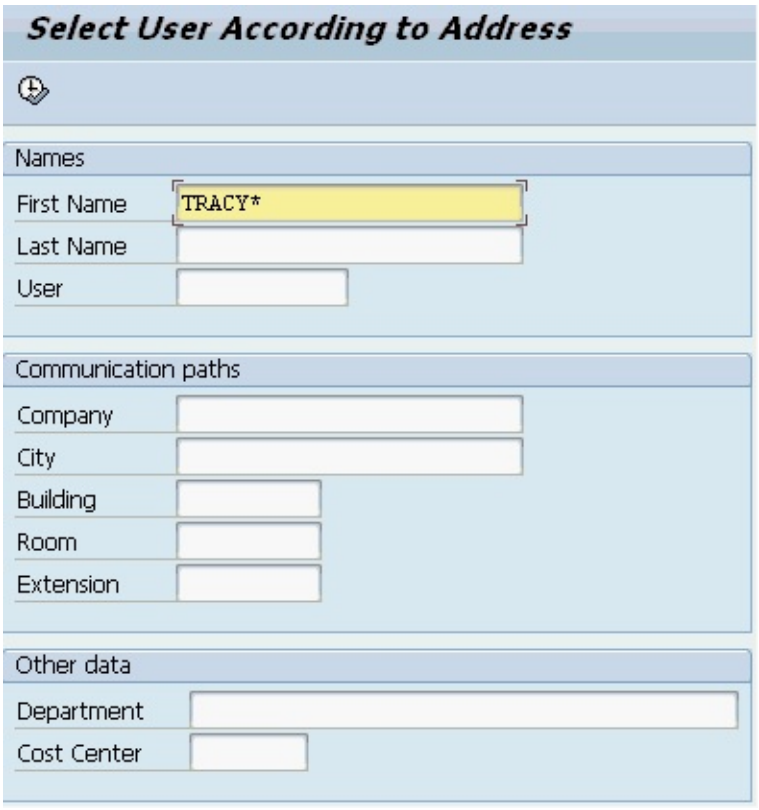


Figure 1.15: SU10 address data button

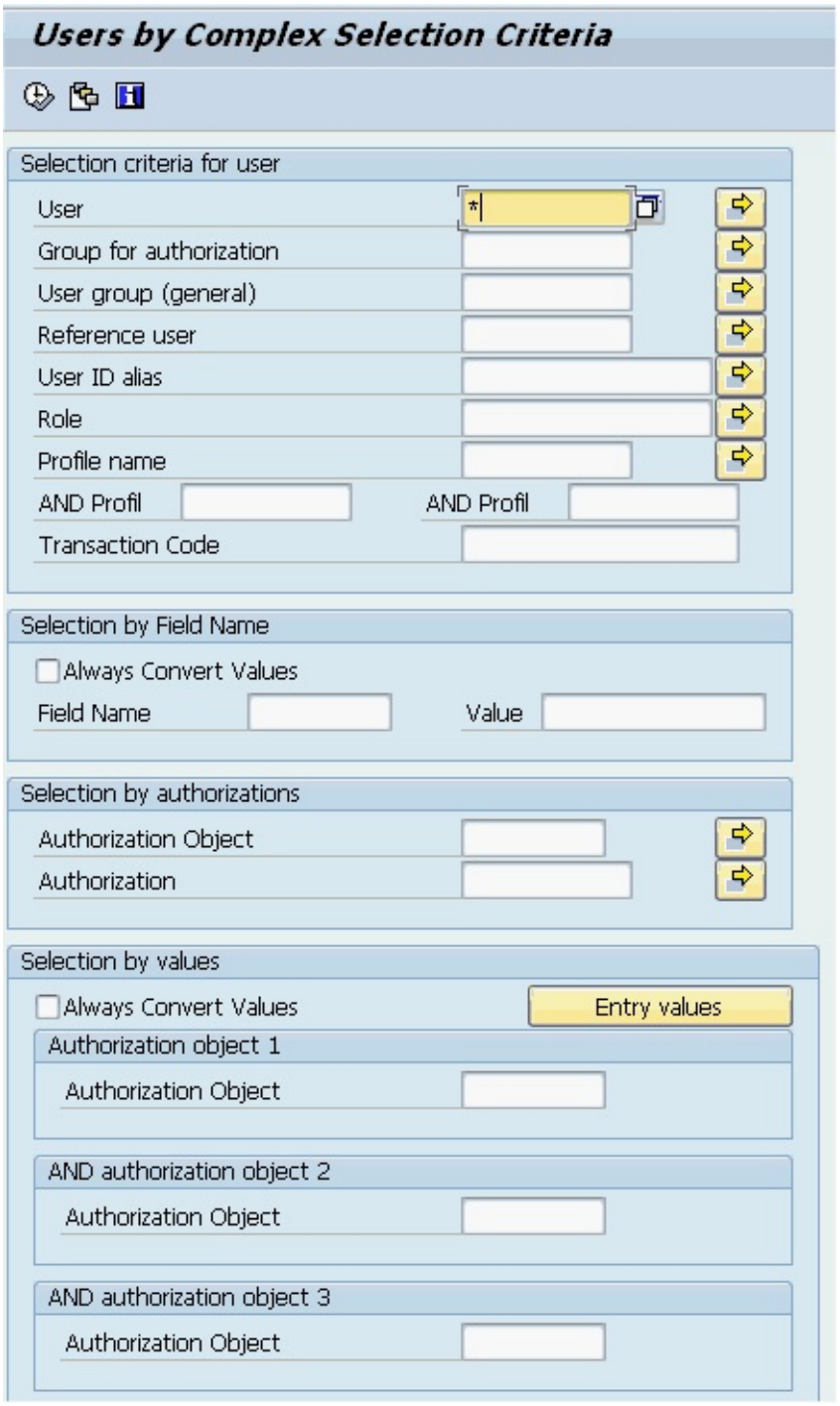


Figure 1.16: Selection criteria page from SU10 authorization data button

Figure 1.15 and Figure 1.16 show the selection criteria that can be used to search for groups of users that are desired to mass maintain. If the user IDs for these individuals are already known, they can be copied from an Excel spreadsheet and pasted from the clipboard by clicking the arrow

button next to the **User** field on the **Selection Criteria** page from the SU10 **Authorization Data** button. Furthermore, if a mass change is required for all users in the system, a value of * can be set in the **User** field.

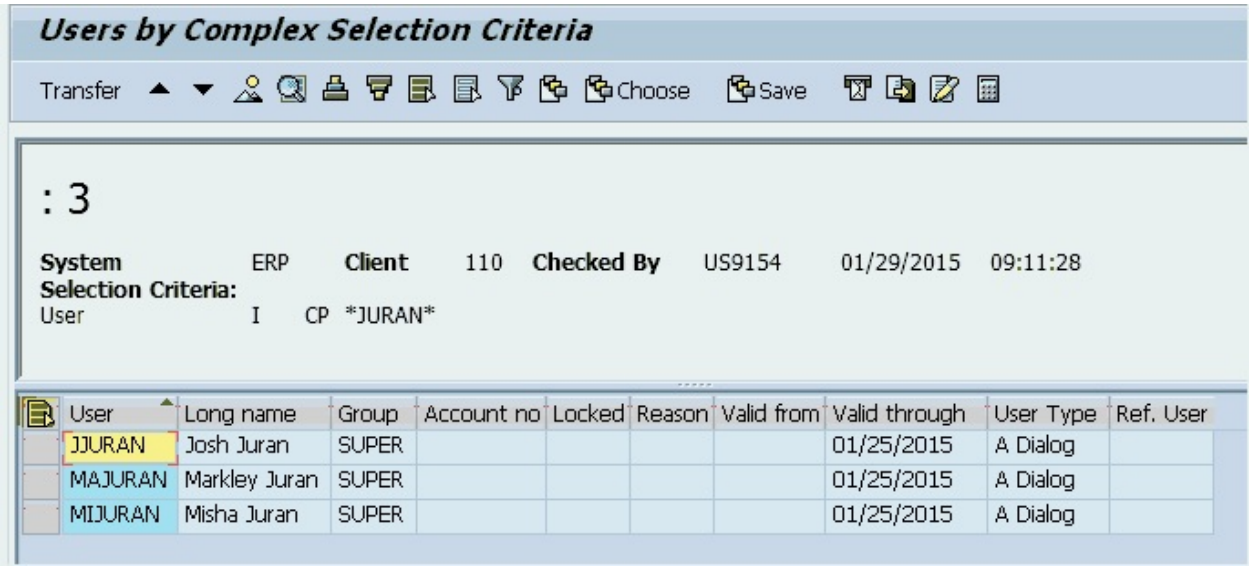


Figure 1.17: Users to be changed resulting from user selection criteria (transaction SU10)

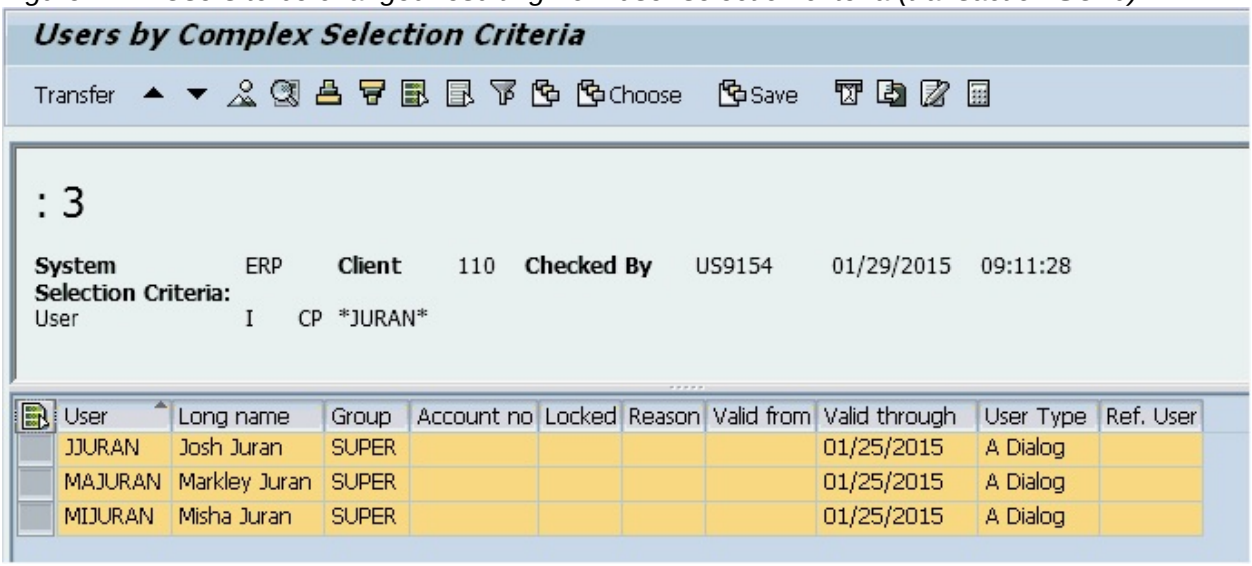


Figure 1.18: Selected users to be changed (transaction SU10)

After executing the selection criteria, a list of all applicable users appears (see Figure 1.17). In order for the shown users to be mass changed, all desired user names must be highlighted and the **Transfer** button clicked (see Figure 1.18).

After defining the users to be changed, the user IDs and names appear in the initial screen of transaction SU10 (as previously shown in Figure 1.14). Possible user changes in the SU10 initial screen reflect those on the SU01 initial screen with one caveat, passwords cannot be defined and changed en masse. The **GENERATE PASSWORD** button, as seen in Figure 1.14, will generate a unique password for each user. Generated passwords for each user can be viewed in the log display after changes are complete. In order to change user attributes, such as logon data, user defaults, and roles assigned, select the pencil (change) button on the initial screen.

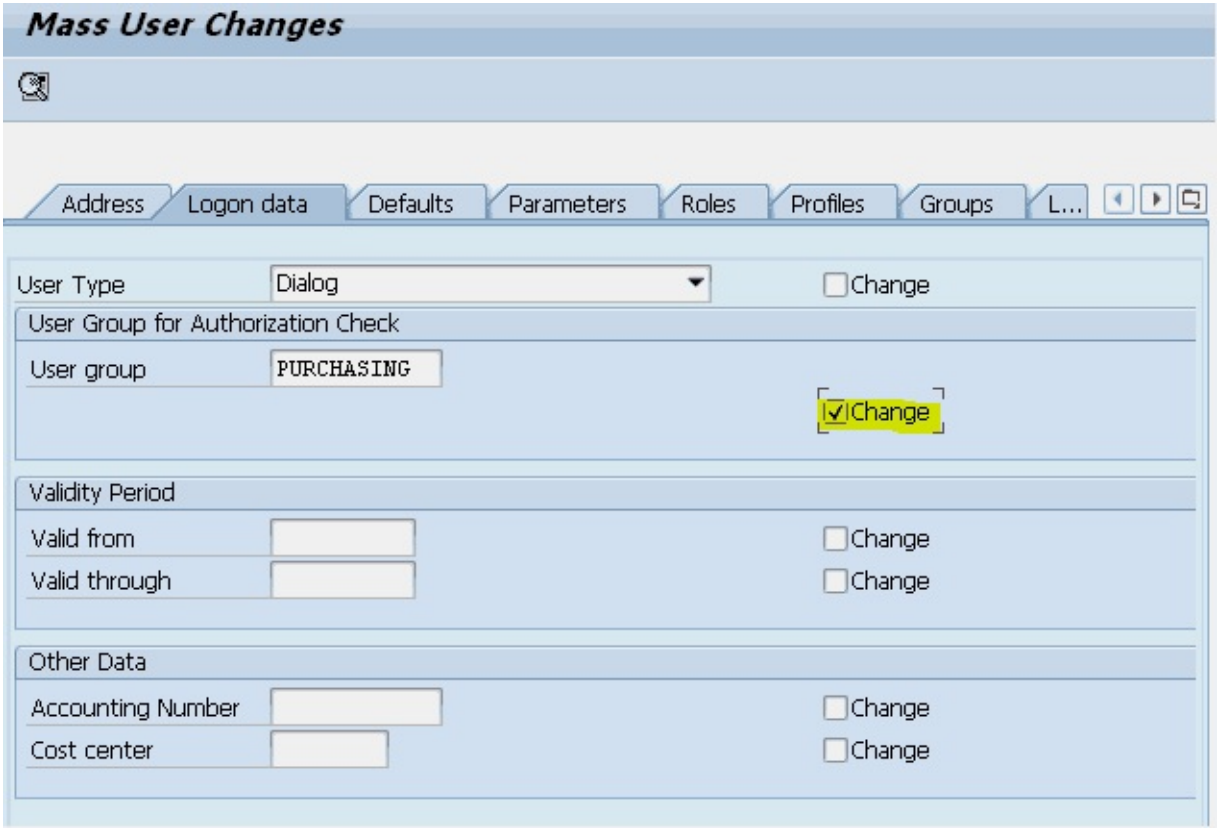


Figure 1.19: Mass user changes to logon data (transaction SU10)

Adding and removing roles

Make sure to select the **CHANGE** indicator (see Figure 1.19) prior to saving changes.

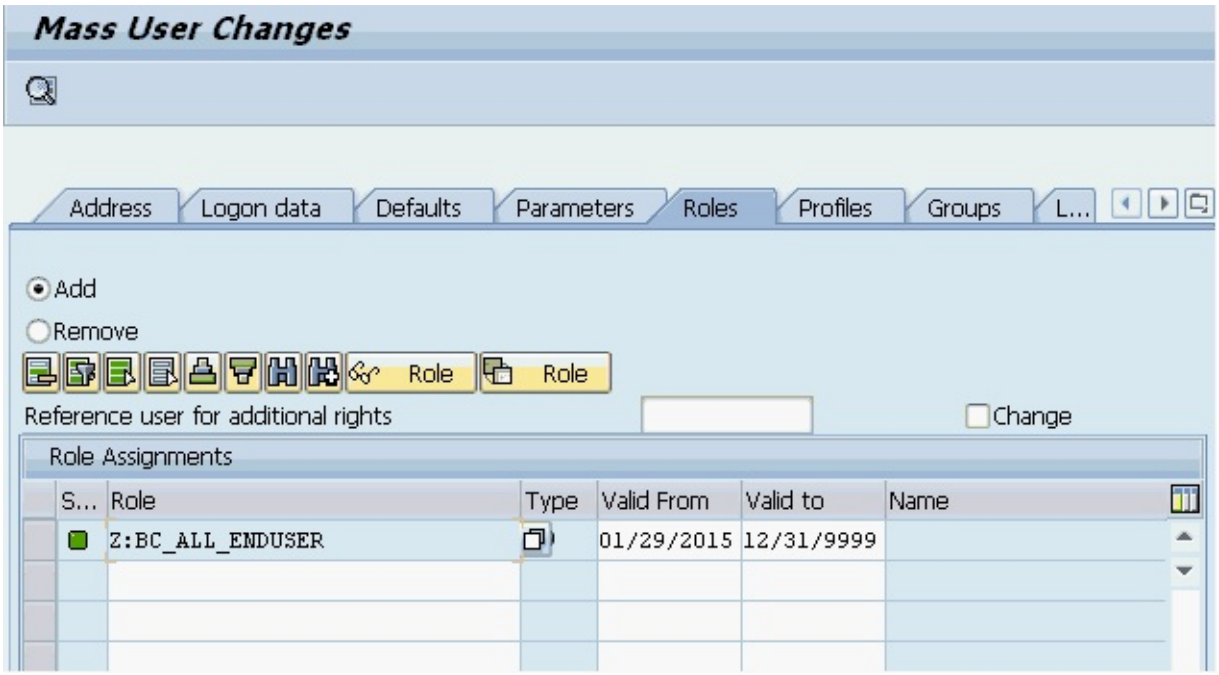


Figure 1.20: Mass user changes to role assignment (transaction SU10)

Role and profile changes differ slightly from other changes in SU10. Roles and profiles can be added or removed during a single instance of SU10, but not both.

Mass assignment of a role example

Figure 1.20 is an example of adding a role to a group of users. The role that is being assigned is a general end-user role in that it has the transactions and permissions needed for all users transacting in the SAP system. If a new role is created in an organization and needs to be assigned to all or many users, transaction SU10 is the most efficient method. The **ADD** indicator must be selected as noted in Figure 1.20.

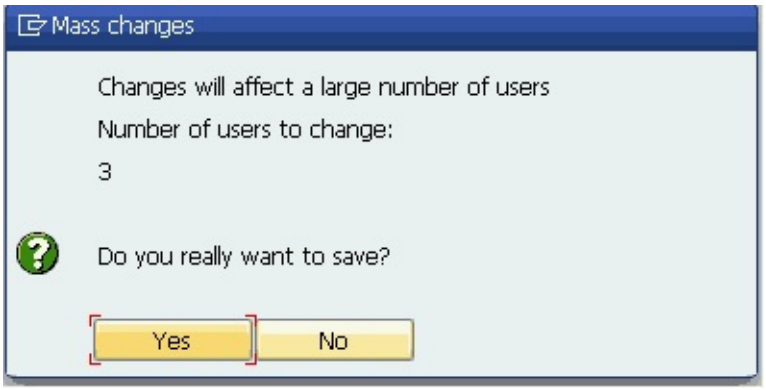


Figure 1.21: Warning message after saving (transaction SU10)

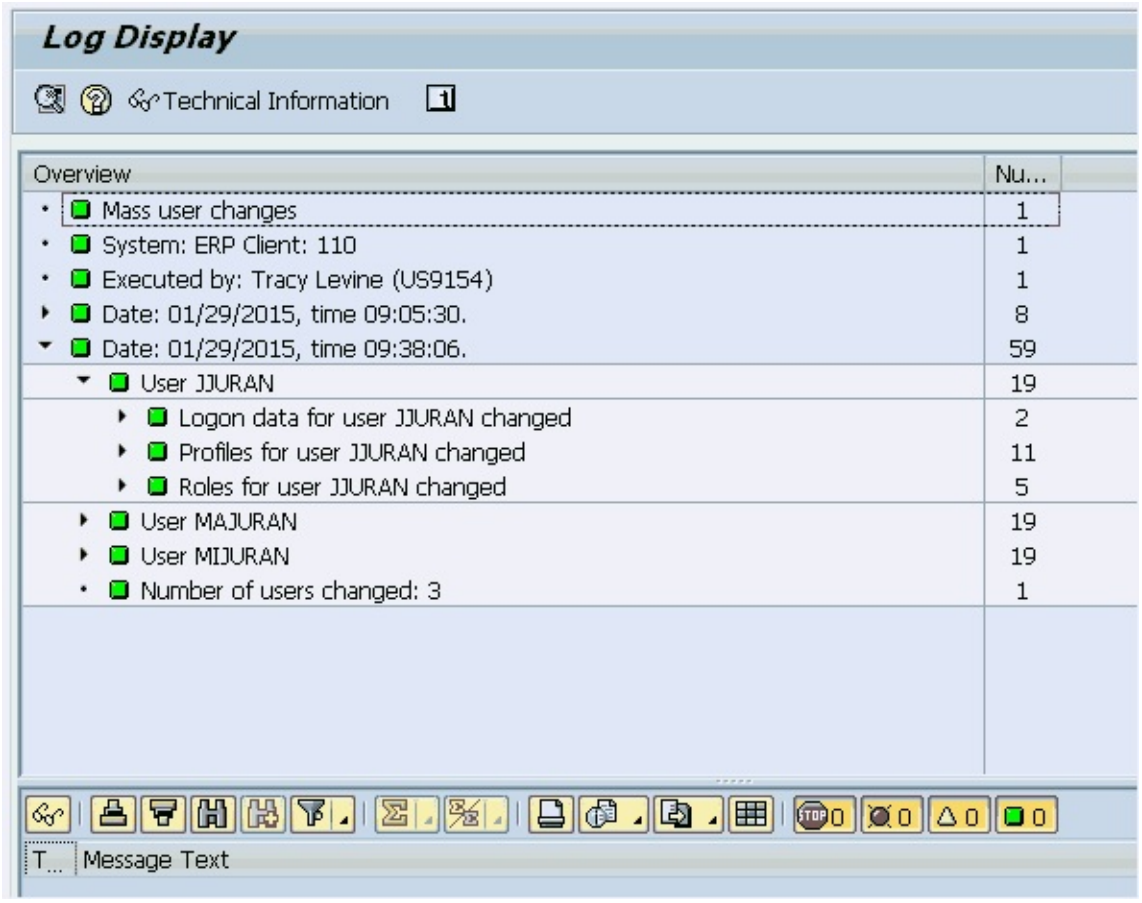


Figure 1.22: Log display after mass changes (transaction SU10)

Once saved, a warning message advises you as to the number of users that the changes will affect (see Figure 1.21). Click the **CHECK** button to indicate that these changes are desired. After confirmation, a log display appears (see Figure 1.22). Green traffic lights indicate successful changes, as shown in Figure 1.22; yellow traffic lights indicate warning messages (although not necessarily unsuccessful); and red traffic lights

indicate all or some of the changes were unsuccessful.

1.5 Passwords

SAP has password setting parameters that include:

- A minimum length of three characters
- No expiration date
- Preconfigured blocked passwords
- Case sensitivity
- Any character, but cannot start with a “?” or “!”
- Not allowing 3 sequential characters from the user’s SAP user ID

However, there are also additional suggested password settings that can be configured, such as:

- A minimum of six characters
- Passwords that expire at regular intervals (4-6 weeks)
- Utilization of the password blocking list
- Requirement of special characters

Recently, SAP introduced a new password protection feature called *Security Policies*. With this new addition, different password rules and logon restrictions can be applied to different groups of users within the same client. Security policy configuration is done in DEV and transported to production via transaction SECPOL. Users are assigned a security policy via the **Logon Data** tab in transaction SU01 or SU10. If the security policy field on the user master record is left blank, the system profile parameters are applied as a default.

1.6 Central user administration (CUA)

An SAP landscape consists of several SAP systems with potentially several clients each. Most SAP ERP landscapes have at least one

development (configuration), one quality (testing), and one production (live) client. These clients are used to maintain system stability by transporting and testing changes prior to introduction into the live system. Individual user master records must be created and maintained in each client within each system.

Utilizing central user administration (CUA) allows the SAP Security administrator to create and maintain all users in one system. All information stored in the user master record is distributed to the dependent systems.

2 Role overview

This chapter provides an overview of user roles in SAP and introduces the profile generator transaction (PFCG). A *role* in SAP can be thought of as a person's job in SAP, or a subset of a person's job responsibilities in SAP.

Example of a user role in SAP

For example, if Tracy Levine is a sales clerk at company XYZ, her SAP user roles reflect sales clerk access. Tracy can have one role assigned to her that will be a compilation of all transactions and authorizations required. However, Tracy can also have many roles assigned, which in totality will provide her the permissions necessary to complete her job tasks.

A role in SAP is created by the profile generator (transaction PFCG). Roles provide access to transactions, reports, Web applications, *etc.* Within each role, you can also view and maintain user assignments. The *rule of least privilege* is a fundamental principle in SAP Security. The rule can be summarized by the notion that a user should be given exactly what is needed to perform the job; not much more and not much less.

2.1 Role types

There are two types of SAP roles: *single* and *composite*. Furthermore, single roles can be set up as *reference-derived roles* or *enabler roles*. This section provides a brief overview of each type of role and what each type is used for. Chapter 3 shows how to create each role and maintain it using the profile generator transaction (PFCG).

Single roles provide access to actions and permissions that make up a user's job or a subset of job responsibilities. Actions can be thought of as transactions and permissions thought of as authorization objects and associated field values. Single roles are the most common type of SAP role.

Actions and permissions example

Sales clerk Todd Levine needs to be able to create and maintain sales orders in SAP. This translates to transaction codes VA01 and VA02. However, Todd can only maintain certain sales doc types (he is not allowed to create return orders) and is only authorized to do so using company code 1000. These limitations are controlled by his explicit access to various authorization objects within his user roles.

Referenced-derived roles are roles that inherit the menu structure, authorization objects, and authorization values from an existing role. Derived roles are often called *child roles*, whereas the imparting role may be called the *parent or master role*. A derived role is useful when you want to mirror the exact same functionality as the master role, but want to manipulate the organizational levels. When creating derived roles, organization levels and user assignments are not passed from the parent to the child. In fact, these are the only role attributes that should be maintained directly in the derived role, all other changes should be maintained in the master role and inherited by the children.

Reference-derived role example

As noted above, Todd Levine is a sales clerk for company XYZ. However, Todd only needs access to maintain and create sales orders for company code

1000. Marla Levine, however, needs access to maintain and create sales orders for company code 2000. Otherwise, their access should be identical. In this case, a master role, Z_MAINT_SALES_ORDERS_ALL would be created as the parent or imparting role. Two derived roles, Z_MAINT_SALES_ORDERS_1000 and Z_MAINT_SALES_ORDERS_2000 would be maintained as referenced-derived roles.

Many companies use a reference-derived role as a tactical tool to reduce the time and resources necessary for ongoing role maintenance. Reference-derived roles are also used as a case for scalability because they can easily be mixed and matched to fit a business user's job responsibilities and organizational assignments.

An enabler role can be thought of as a bolt-on role. Unlike derived roles, enabler roles are created without any link to an already existing role. Enabler roles have manually added authorization objects added to them with only desired field values maintained.

Enabler role example

Release strategies are a common example of when enabler roles are useful. An example is when a company wants all purchasing administrators to have access to all purchasing-related activities, but wants to limit the team's access to specific release strategies based on levels. Release strategy authorization is controlled by a single SAP authorization object: M_EINK_FRG which has two fields, Release Code and Release Group. This authorization object can be inactivated within the purchasing admin role and bolt-on enabler roles can be created, one for each Release Code and Release Group combination and assigned ad hoc to each purchasing admin.

A *composite role*, also known as a collective role, is a grouping of two or more single roles. Composite roles are used for the purpose of simplifying the assignment of roles to users. Composite roles do not contain any authorization data, only other roles. Furthermore, composite roles can only be groupings of single roles, not other collective roles.

3 Profile generator and role maintenance overview

This chapter introduces the profile generator transaction, PFCG. The profile generator tool is responsible for enabling the SAP Security administrator to create specific user roles, which contain authorizations to various system functions. Chapter 4 identifies the relationship between profiles, roles, and authorizations and the basic maintenance features within the transaction.

3.1 What is a profile?

The *profile generator* is a tool that creates SAP user roles, which correspond to profiles. Access to the profile generator is via transaction code PFCG. A *profile* is a collection or grouping of SAP authorizations.

Role definitions

Best-in-class SAP Security role designs take into account some critical success factors, considering sustainability and scalability are absolutely essential when designing SAP Security roles. Furthermore, involving the business in role content and governance is imperative.

3.2 What is an authorization?

The following information is stored in a profile:

Authorization object classes

- Logical grouping of authorization objects

- Contain one or more authorization objects

Authorization objects

- Fields linked to various database tables
- Can contain up to 10 fields (see Figure 3.1)

Authorization

- An instance of a specific authorization object
- Allowing several authorizations for an authorization object with combinations of different field values
- An instance can be tracked by unique two-digit number

Authorization object example

Authorization object V_VBAK_AAT is contained in the below role twice, hence, two authorizations (T-I855600400 and T-I855600401). The authorization object class is SD (Sales and Distribution). This authorization object controls the assigned users' ability to maintain various sales document types. The two authorizations combined dictate authorization for the business process in totality. The user can display all sales document types, but only maintain and create standard sales orders.

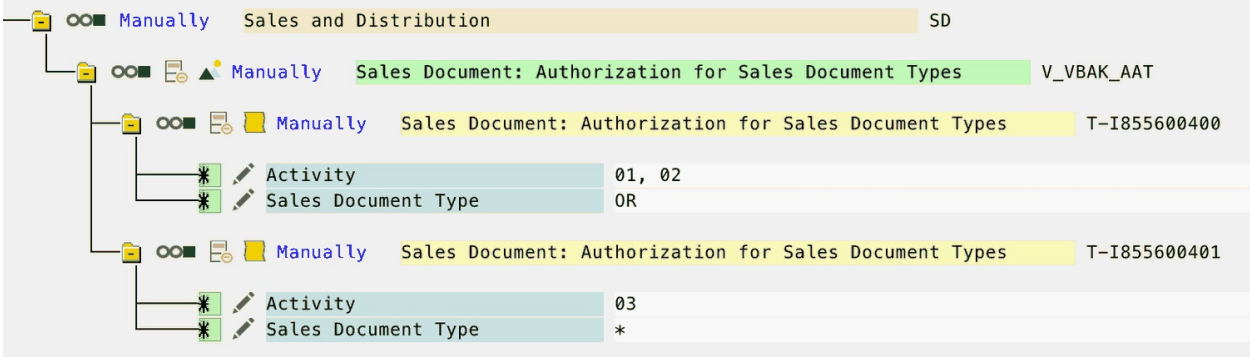


Figure 3.1: Authorization object as seen in transaction PFCG

There are over 20,000 standard SAP authorization objects.

3.3 Profiles and roles

Although a role and a profile may seem similar, there are a few distinct differences. Roles are the actual containers for storing authorization objects and their values. Once the user roles are generated in PFCG, the profiles are generated. Typically, the ratio of roles:profiles is 1:1, however, only 150 authorizations can fit into a profile. If the number of authorizations within a role exceeds 150, a new profile is automatically created within the profile generator.

Roles are added to user master records via transaction SU01. When roles are added with a proper validity date, the corresponding authorization profiles are assigned to the user. As a reminder, a role can be thought of as a user's role or a subset of job responsibilities.

Figure 3.2 is a simple graphical depiction provided by SAP of the SAP Authorization Concept.

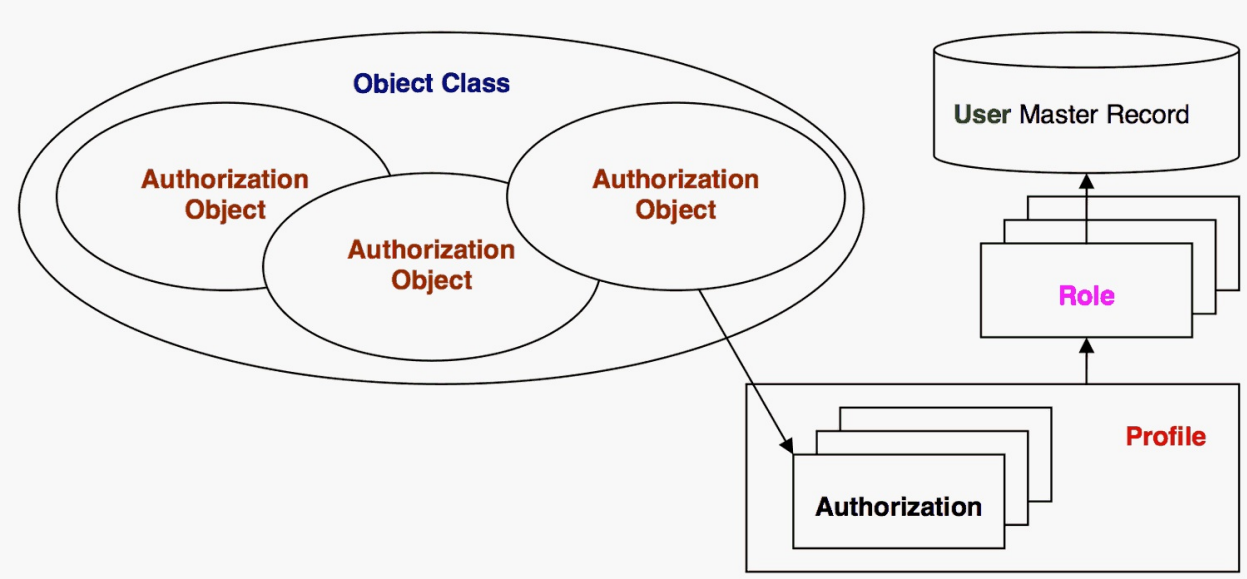


Figure 3.2: SAP Authorization Concept "(Authorization Objects-A Simple Guide," SAP)

4 Advanced topics for role maintenance

The profile generator is an SAP tool in which roles are created and then generated to create profiles. As a reminder, a profile is a collection of authorizations.

4.1 Profile generator deep dive

The following section provides an overview into the profile generator tool and how the PFCG transaction can be used. Role/profile maintenance is always performed in the development client, transported to the quality environment for testing, and finally moved to the production environment for use.

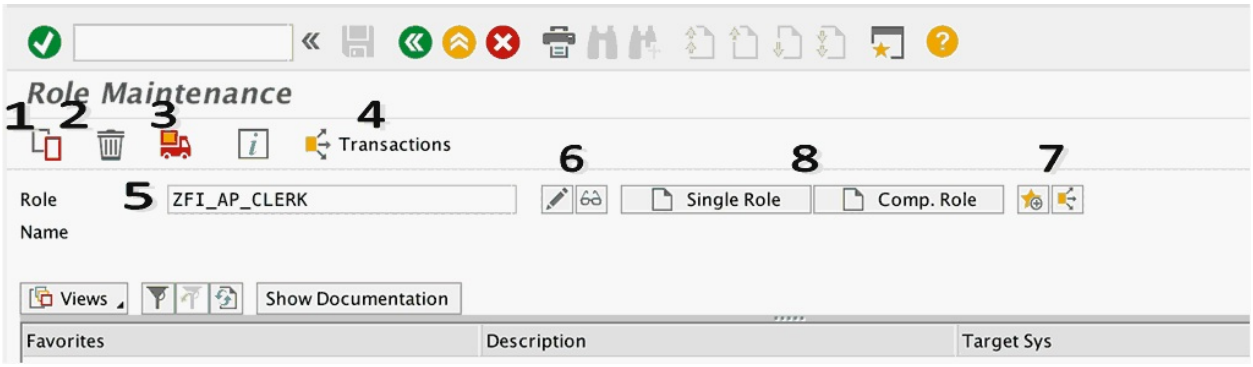


Figure 4.1: PFCG transaction home screen

As shown in Figure 4.1, the home screen of PFCG has an abundance of buttons in order to create and manipulate roles. The following is an explanation of the most important screen elements, beginning at the top of the screen and moving from left to right:

❶ The **DOUBLE PAPER** button is used to copy an existing role or elements of one role to another.

❷ The **TRASH CAN** button is used to delete an existing role.

Tip for transporting role deletions

If a to-be-deleted role already exists in clients other than development (quality and production) then it must be placed in a transport request first. The process to delete a role from multiple clients is to place it in a transport request in the development client, delete the role in the profile generator, and then release the transport request and move it to quality and production. This process will transport the deletion to the other clients as well.

❸ The TRUCK button is used to transport a role from the development environment to quality and production.

❹ The first BOX WITH ARROWS button that displays the word *transaction* is used to search for roles that contain a specific transaction.

❺ In the **ROLE** text field**,** the role that is to be created, changed, deleted, or copied must be entered.

❻ The next two buttons, the PENCIL button and GLASSES button are repetitive in their meaning throughout the SAP system. The former is for role maintenance and the latter is to display roles.

❼ The second BOX WITH ARROWS button on the same plane as the role name will display a *where-used list* for the role. The where-used list appears if the identified role is contained in any composite roles.

❽ The final two important buttons, the SINGLE PAPER and COMPOSITE PAPER buttons, indicate the role type to be created. In Section 4.3 you will learn more about the differences between single and composite roles.

In order to create a role, first identify the role name in the ROLE text field of the PFCG landing screen and click the SINGLE PAPER button to create.

Role name tip

Prior to role creation, an explicit naming convention should be determined for all roles. Role names can be up to 40 characters in length and should accurately reflect the role content, including transactions, authorizations, and organizational entities that it provides access to. Role names must be unique and cannot start with “SAP.” The roles which do begin with “SAP” are predelivered templates and should be copied and re-named prior to being maintained.

The following screens provide a walk-through of the role creation and profile generation processes. Role maintenance works in the same manner. Throughout the different tabs and screens within PFCG, you will notice an abundance of **TRAFFIC LIGHTS**. The traffic lights are red, yellow, or green indicators that indicate how far along you are in the role creation process.

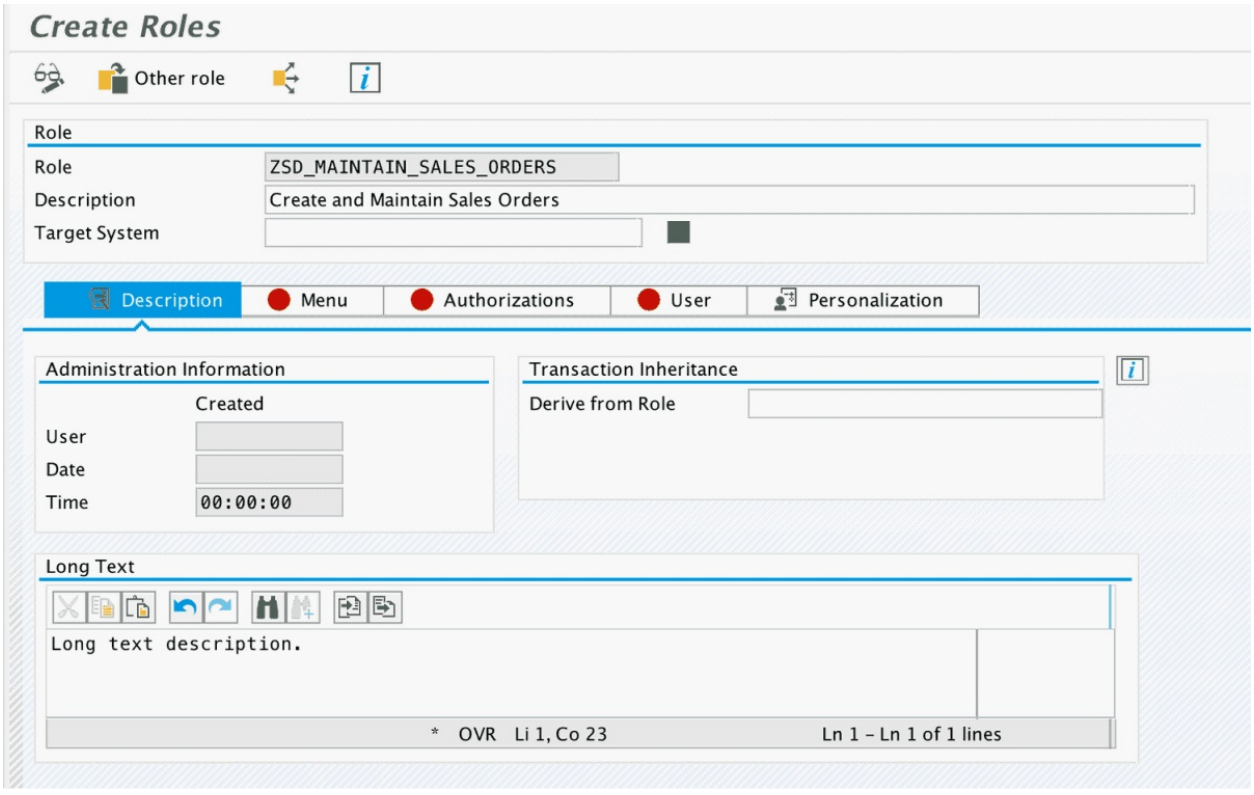


Figure 4.2: PFCG description tab

The description tab, as seen in Figure 4.2, is used to provide a description of the role and its contents. The **LONG TEXT** box enables the security administrator to note additional information that may be useful for future role maintenance and also to leave a log of all changes that have been made to the role over time. The **DESCRIPTION** tab identifies the user name, date, and time that the role was created and the last time it was changed. This can be very useful information if there is more than one security administrator creating or changing roles.

Transaction inheritance allows the role to derive authorizations from an existing role. If the role is derived, the parent or master role appears in the **DERIVE FROM ROLE** text box (more on derived roles in Section 4.3).

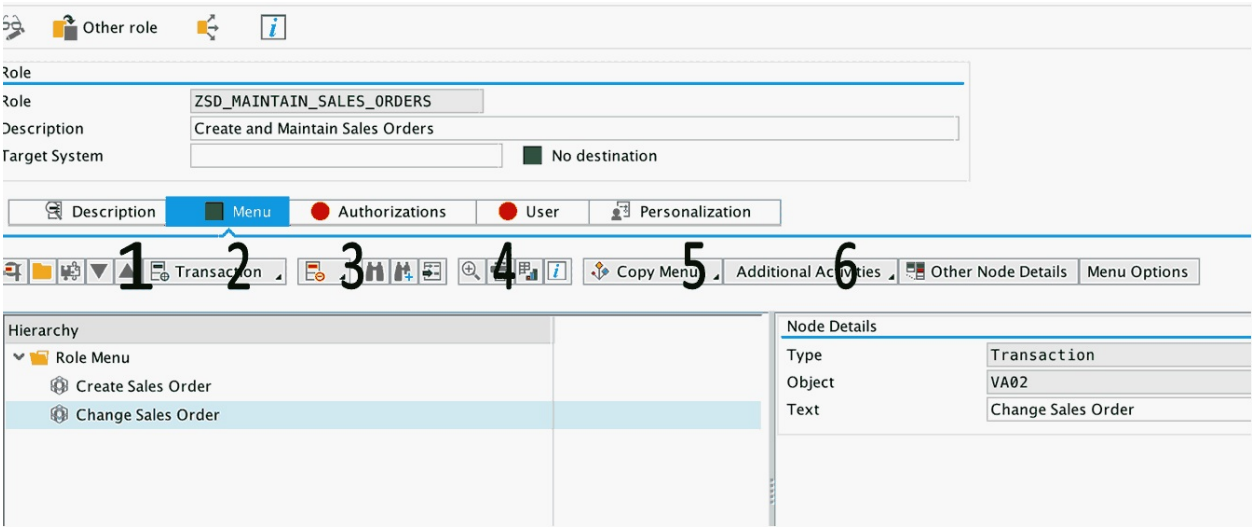


Figure 4.3: PFCG menu tab

The **MENU** tab is primarily used to build the role at the transaction level. This is the first step in supplying the role with authorizations that allow users to complete one or more tasks in the system. Aside from transactions, other objects can also be added to the role via the **MENU** tab such as Web applications and reports. Additionally, folders may be added to the menu (**FOLDER** button) and transactions can be arranged using these folders, which will translate to how they appear on the user's home screen upon logging into SAP.

The following list provides an explanation of all the important screen

elements in Figure 4.3.

❶ The ARROW buttons allow the security administrator to navigate the menu.

❷ The TRANSACTION button is used to add a transaction to a role or other objects that can be selected from the drop-down list.

❸ Deletes a transaction, report, or other object from the menu.

❹ Toggles technical names on and off in the menu.

Technical names in menu

If technical names are enabled, transaction VA01 will appear in the MENU tab as "VA01 – Create Sales Order," if they are disabled, the transaction will appear simply in the menu as "Create Sales Order."

❺ COPY MENUS button can be used to call role menus from a template or within another role .

❻ ADDITIONAL ACTIVITIEs button allows the administrator the ability to:

- Translate a node from one language to another
- Display any documentation for transactions, programs, *etc.*
- Search in Report Documentation

Menu tab example

A user needs access to transaction code VA01 (Create a Sales Order). The security administrator then gives the user access to this transaction by adding VA01 to the menu in the role to which they are already assigned.

Ultimately, the **Menu** tab is used to manage role content at the highest level, which typically equates to transaction codes, reports, and Web services.

The heart of the role/profile maintenance process lies within the authorization tab of PFCG because this is where all the authorization data is configured. As you can see in Figure 4.4, no authorization currently exists for the role.

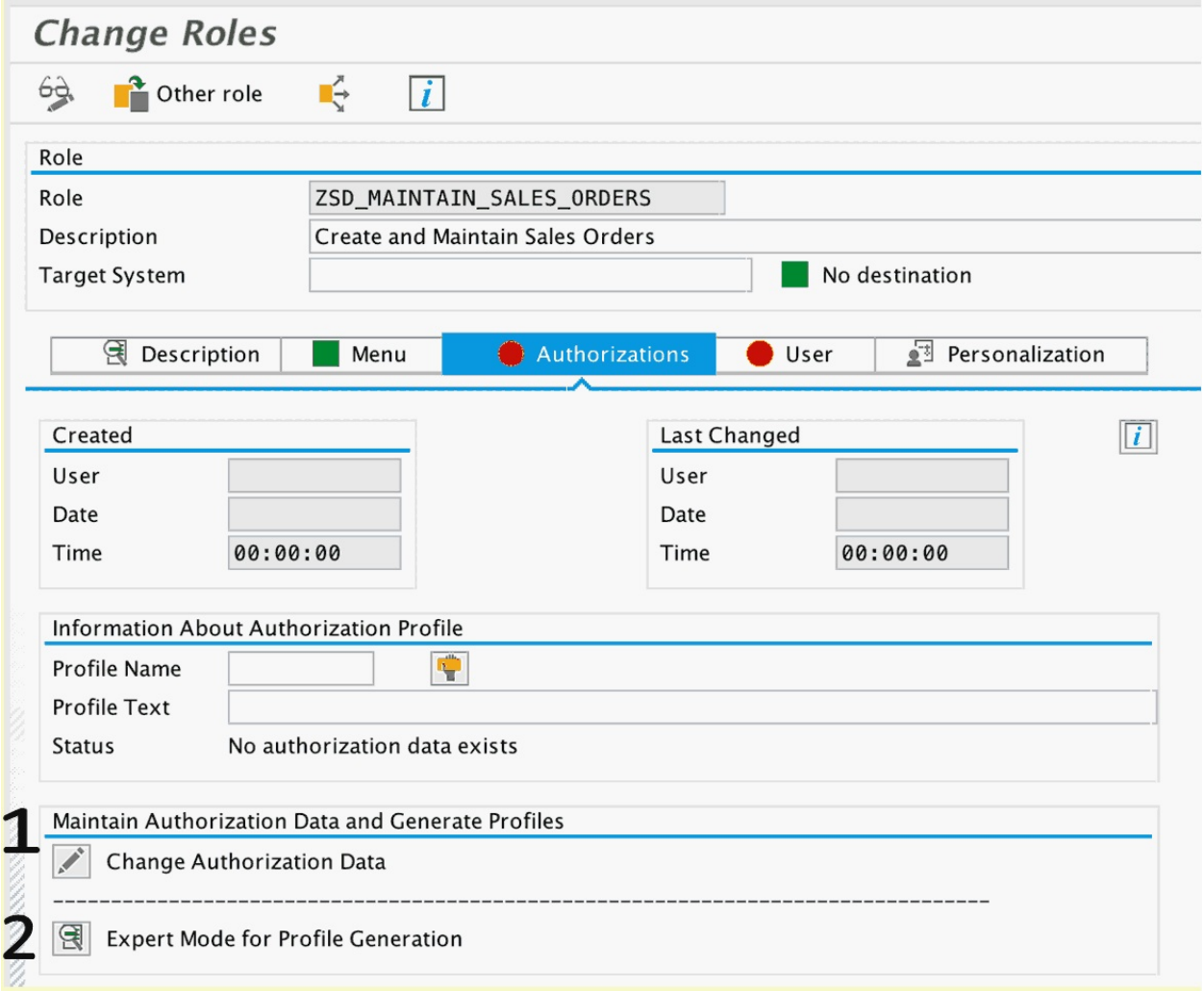


Figure 4.4: PFCG authorization tab

In order to configure authorization data for the role, one of two buttons needs to be pressed:

❶ The **CHANGE AUTHORIZATION DATA** button enables you to manipulate authorization data that already exists in the role.

❷ The **EXPERT MODE FOR PROFILE GENERATION** button allows the role administrator to choose the mechanism for populating and changing role authorization data.

Manipulating role authorization data

The best practice for manipulating role authorization data is to select the button **Expert Mode for Profile Generation**. When no authorization data currently exists for the role, no options for authorization maintenance appear. **Expert Mode** will only display options if the authorization data was previously configured and saved. When role data has previously been configured, the role administrator should always select the option for "Read Old Status and Merge with New Data." This will add or remove any default authorization objects and values that SAP associates with changes that have been made in the **Menu** tab. The data repository that stores the relationships between transactions, authorization objects, and values (and can be manipulated to meet the needs of the specific SAP client) is in transaction SU24 (see Section 5.4).

The first screen within the authorization tab is the **Define Organizational Levels** window as seen in Figure 4.5. The screen appears if any of the authorization objects associated with the transactions in the **Menu** tab check for an organizational field. Such fields include company code, sales organization, plant, account type, *etc.* A role can have access to one or more organizational values for each field in the **Organizational Levels** window or open-wide access.

Field values with open-wide access

If the desired value for an authorization field is open access to all possible field values, the "" *indictor may be used. For example, a role may have access to all sales organizations within a single company code. In this instance, the company code field will be populated with "1000" and the sales org field will be marked as "*" within the **Organizational Levels** window.

The SAP best practice is to populate organization field values only in this window. Any fields populated in this window will automatically distribute to any authorization objects in which they reside. This practice is essential in order to ensure role integrity. The **ORGANIZATIONAL LEVELS** windows distribute the entered values in all authorization objects in which each field is present, so that the role has consistent access to the same organizational entities, which should be reflected in the role name.

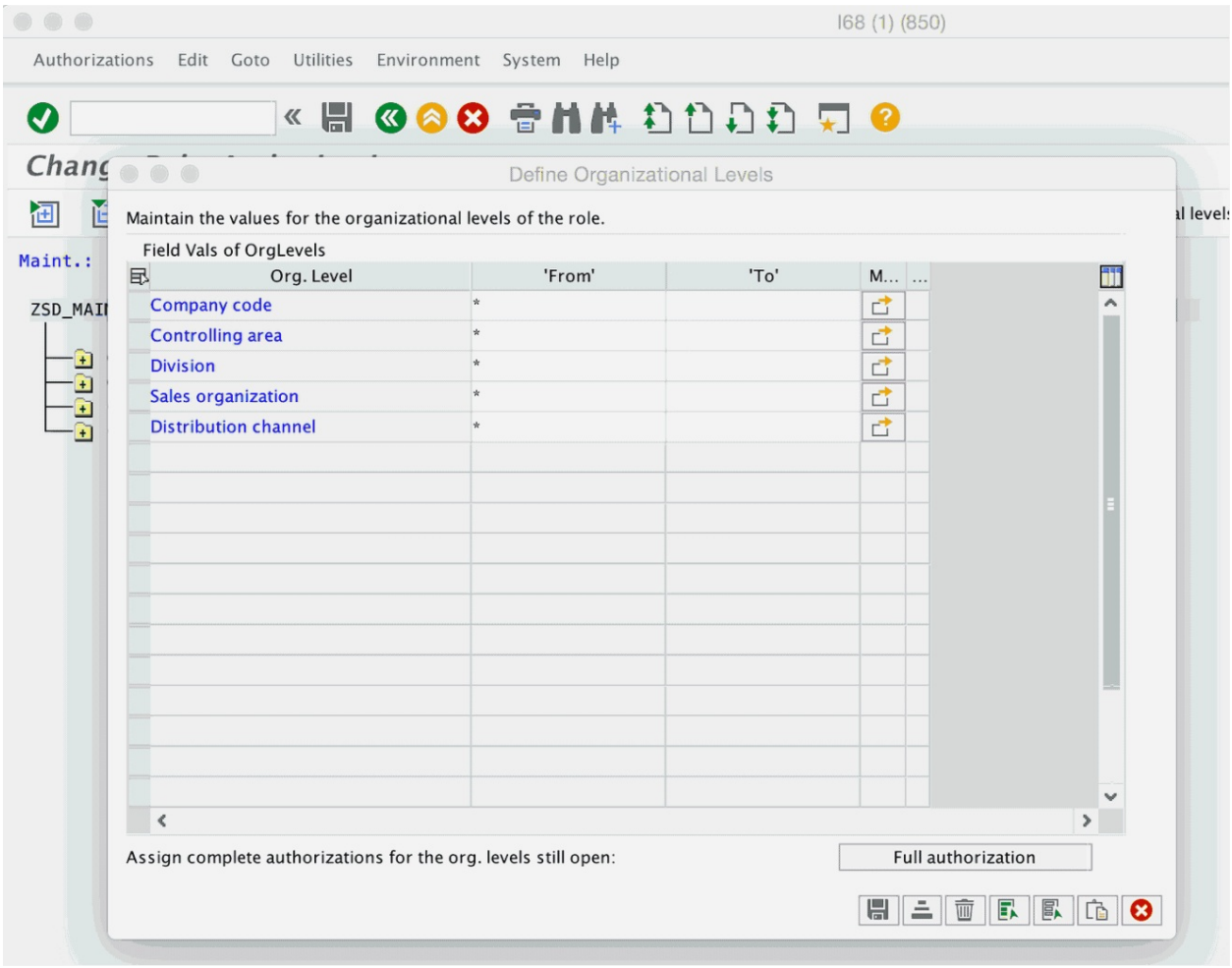


Figure 4.5: The role organization levels window

After the **Organizational Levels** window is populated and the values have been saved, all authorization objects associated with the role appear, as shown in Figure 4.6. You may now be asking yourself, what really just happened? What exactly am I looking at? Here's a recap:

1. Transactions were added to the **Menu** tab for the role.
2. The necessary authorization objects were automatically pulled into the role based on the transaction/authorization relationship data stored in SU24.
3. A screen appeared, which required that all organizational data for the role be defined. This organizational data is contained in one or more authorization objects within the role.
4. A screen appears with traffic light indicators (see Figure 4.6) when

authorization data for the role is maintained.

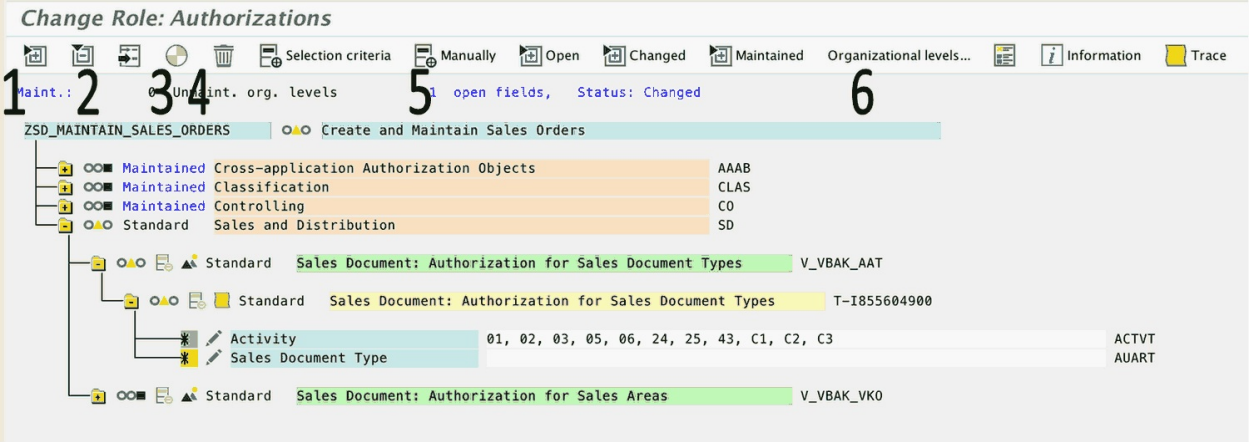


Figure 4.6: Role authorization data screen

Before continuing on with authorization maintenance, here is a recap of a few key definitions:

Authorization object classes

- Logical grouping of authorization objects
- Contain one or more authorization objects
- Sales and Distribution is an example of an authorization object class as seen in Figure 4.6

Authorization objects

- Fields linked to various database tables
- Can contain up to 10 fields
- V_VBAK_AAT is an example of an authorization object as seen in Figure 4.6

Authorization

- An instance of a specific authorization object
- Enabling several authorizations for an authorization object with combinations of different field values

- An instance can be tracked by unique two-digit number
- T-I855604900 is an example of an authorization as seen in Figure 4.6

The following screen elements on the role authorization screen are important:

❶ Expand all role authorization data
❷ Collapse all role authorization data
❸ Generate authorization data. This button will create or update the role's associated profile(s) upon completion of authorization maintenance.
❹ Delete authorization from the role
❺ Manually add authorization object to the role
❻ Specify organizational levels for the role

What do the "traffic lights" indicate?

- **Green**: Fully maintained authorization fields
- **Yellow**: Partially maintained authorization fields
- **Red**: Unmaintained organizational levels. As previously stated, returning to the **ORGANIZATIONAL LEVELS** window and maintaining the org values in the single location will rectify this.

Possible field entries for an unmaintained authorization field can be found by clicking on the **PENCIL** button. Various pop-up windows may be visible upon this action to aid the administrator in populating authorization fields. Figure 4.7 displays possible field values for **SALES DOCUMENT TYPE** for authorization object V_VBAK_AAT. Upon clicking the **PENCIL** button, a pop-up appears in which field values can be manually entered or the administrator can further select from a drop-down menu. An additional option for the security administrator is to populate a range of field values for the given authorization.

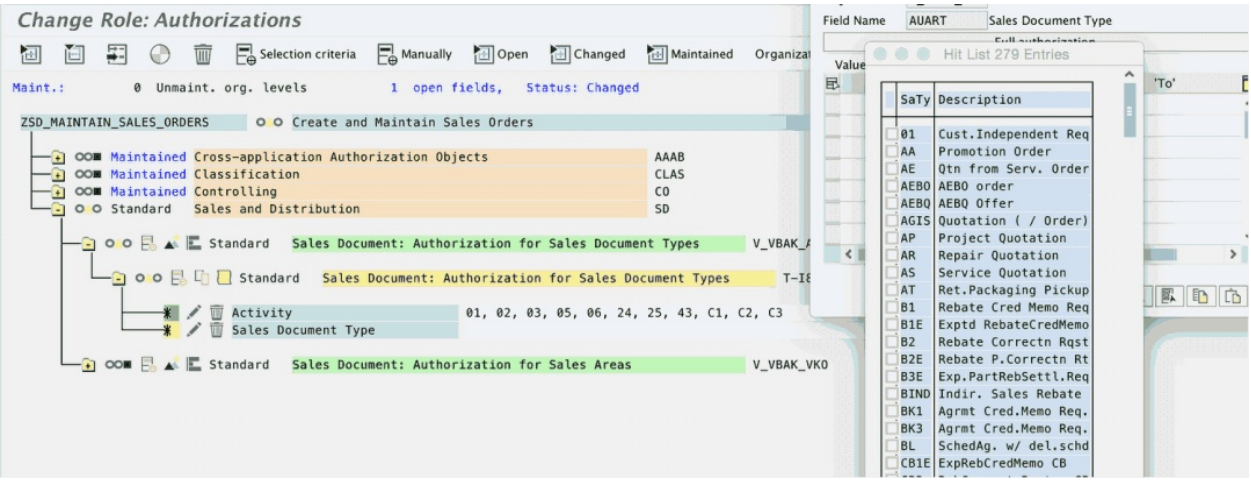


Figure 4.7: Authorization object and potential field values

Once all fields have been maintained for an authorization, the associated traffic light turns green. All traffic lights appear green when all authorization fields within the role have been maintained. Once all authorization fields have been maintained, the final step is to generate the profile(s) associated with the role. This step is essential! If the profile is not generated, the assigned users will not receive access to the transactions and authorizations within the system. In order to generate the profile(s), click the beach ball button on the authorization screen (❸). A pop-up screen appears to allow the administrator to manually change the name of the authorization profile or keep it as the SAP standard. Once this step has been completed, a message appears stating successful generation of the authorization profile(s).

Recap

The SAP Security administrator just finished configuring all the authorization data for the role. Field-level authorizations were defined for all authorization objects automatically brought in by the transaction codes in the **MENU** tab. The profile was then generated and any user assigned to this role is able to access the identified transaction codes and field-level authorizations within the SAP system.

A profile can only contain 150 individual authorizations. Therefore, if a role contains more than 150 authorizations, a separate profile will be generated for each set.

A user master record can only be assigned to 312 profiles.

After generating the profile, it is best to back out of the authorization window and go to the **User** tab (see Figure 4.8). Within this tab, a user or group of users can be assigned to the role in the same manner an individual user can be assigned to multiple roles within the user master record. The **User Compare** button reconciles the user master records of the users entered onto this tab. A user comparison must be completed after users have been entered on this tab of PFCG in order for these users to receive the authorizations within the roles. The **From** and **To** fields can be utilized to specify users' access to a role by date, which can be useful if the user is substituting responsibilities for another or testing a particular functionality.

User comparison

A user comparison must be completed after users have been selected in order for these users to receive the role and its authorizations. Not unlike the rest of the role maintenance process, the **User** tab will continue to have a red traffic light until a user comparison has been completed.

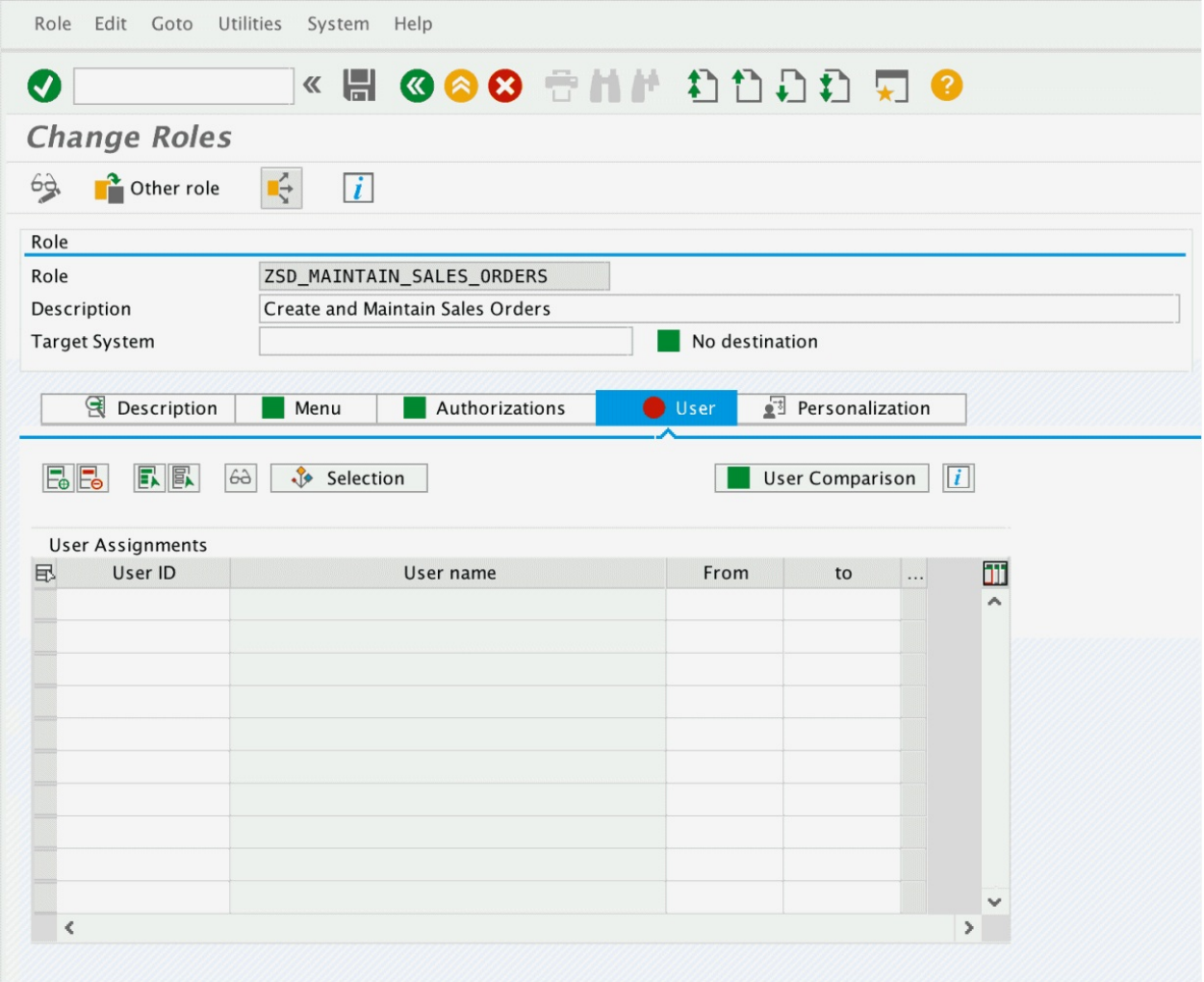


Figure 4.8: PFCG User tab

As previously stated, SAP comes with hundreds of role templates that begin with “SAP” and can be used as templates for role creation.

4.2 Authorization-object level security

Now that you have reviewed all the required steps in the role creation and maintenance process, it is time to dig a little deeper. At this point you may be asking yourself, “Ok, so I know all the technical steps, but how do I know exactly what field values to include for a given authorization in PFCG?” There are many tips and tricks that will aid the SAP Security administrator in filling out the correct information.

The first and most simplistic way to maintain the field values for an

authorization is to ask a functional person who is within the department that is requesting the role to be created or changed. Continue to use authorization object V_VBAK_AAT, Authorization for Sales Document Types, with this example. V_VBAK_AAT contains two authorization fields: **Activity** and **Sales Document Type (**see Figure 4.9). The functional department should be privy to the sales document types (i.e. standard orders, return orders, and quotations) and activity types (i.e. create, change, and delete) included in this role.

If the functional department cannot provide the required information, the next step would be to use all of the relevant information on the screen and do further research within the SAP system.

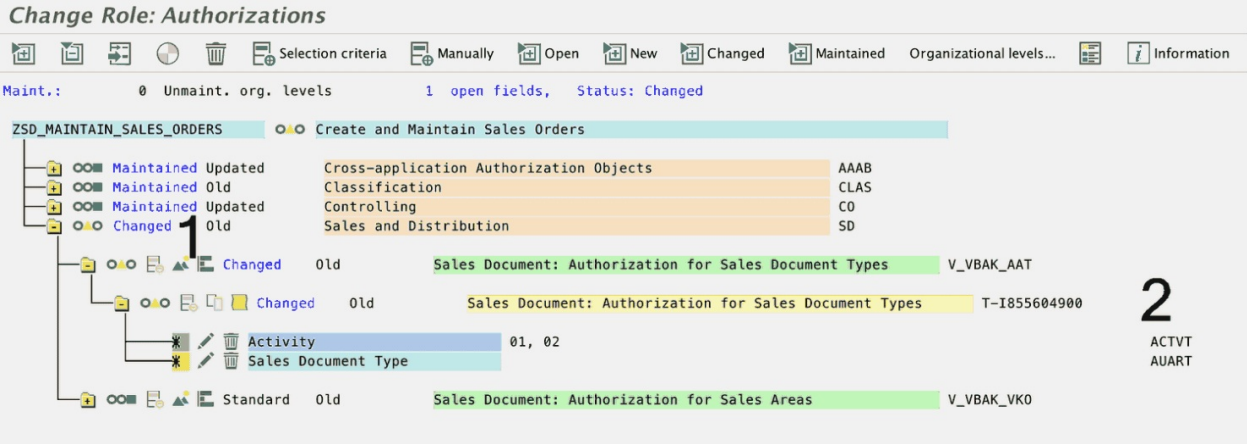


Figure 4.9: Role authorization screen

❶ Notice the button that looks like a mountain range. Once clicked, a pop-up window appears and displays the transactions in this role that are associated with the authorization object (see Figure 4.10). The pop-up window also displays the field values that are automatically brought into the role for that object when the transaction is added. As a reminder, this relationship information is stored and can be manipulated in transaction SU24.

❷ Other relevant information provided on the authorization window is the technical name for each field value. If the functional department doesn't know the information you are asking them to provide, you can make note of the technical field name (in this case AUART) and go to the corresponding transaction code (VA01). Look for the field (**SALES**

DOCUMENT TYPE) on the screen (see Figure 4.11) and show it to the functional team.

Role ZSD_MAINTAIN_SALES_ORDERS
Transactions, RFC functions, and services that require authorization object V_VBAK_AAT:

Type of Application	Application	Short Description	Authorization fld	Value range
Transaction	VA01	Create Sales Order	ACTVT	01
				02
				03
				05
				06
				24
				25
				43
				C1
				C2
				C3
			AUART	
	VA02	Change Sales Order	ACTVT	02
				03
				05

Figure 4.10: Authorization object and transaction relationship

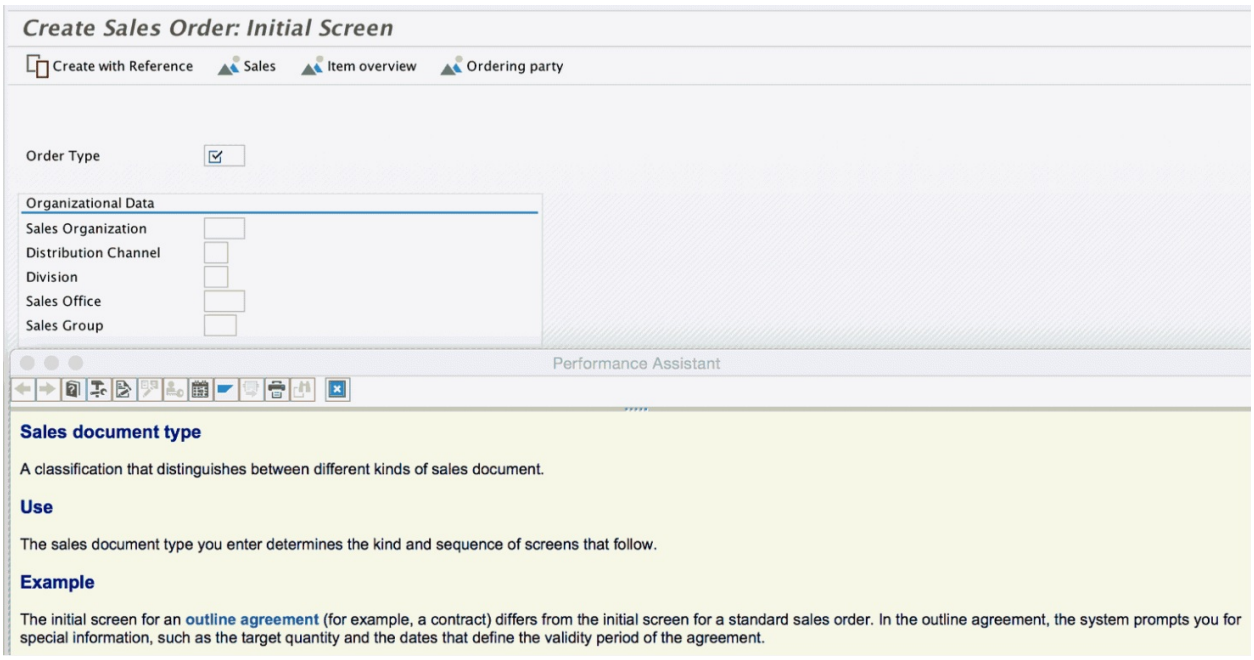


Figure 4.11: Sales document type as it appears in functional transaction

If you cannot find the field explicitly labeled on the screen, you can use the **"F1"** key (help) on each field until you find the correct one (as in Figure 4.11). This pop-up window will display valuable information about the field and its use, as well as a functional business example of its application. The pop-up window will also have a **TOOLS** (technical information) button that when clicked will provide other information that may prove relevant (see Figure 4.12).

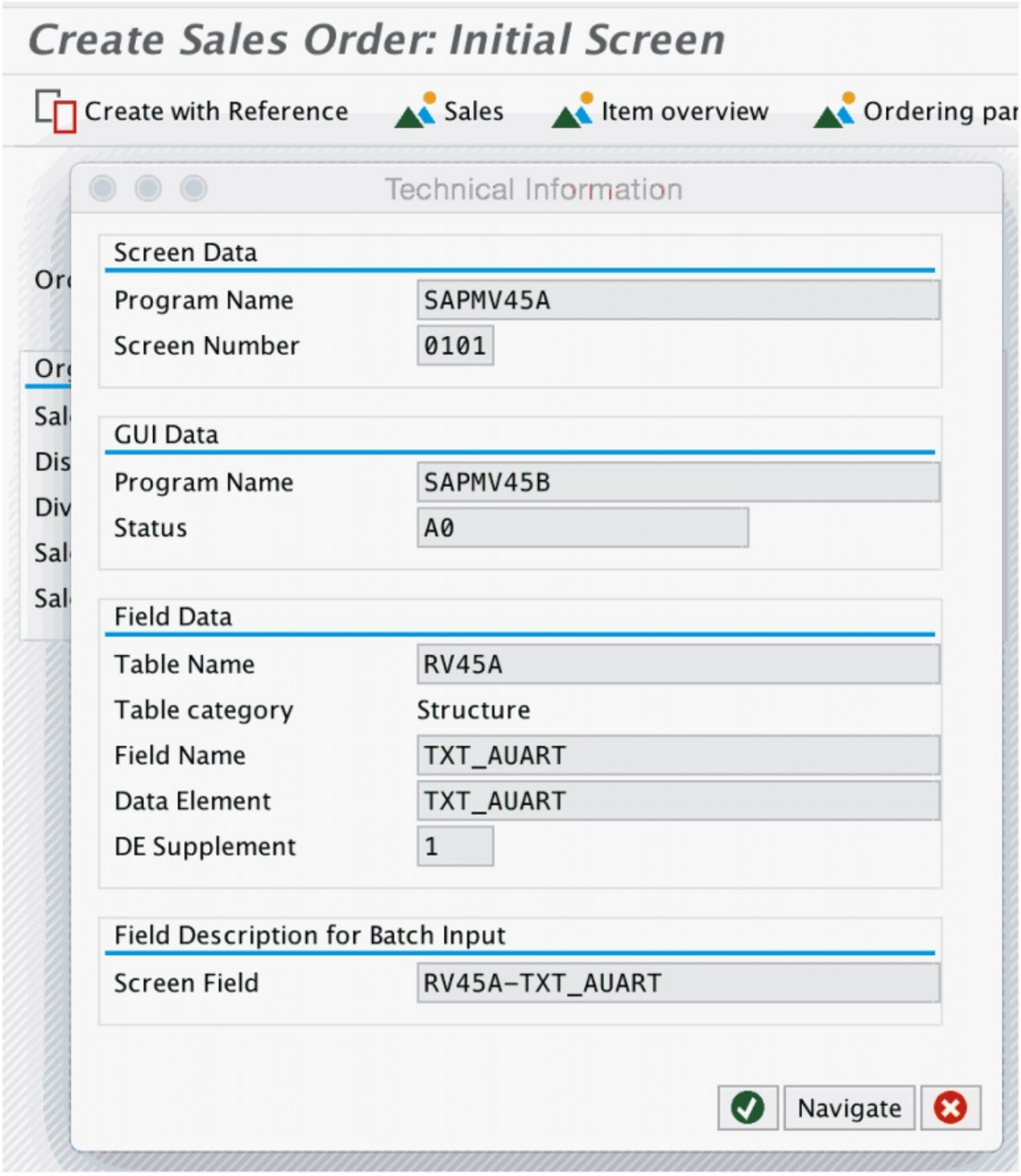


Figure 4.12: Field technical information

In Figure 4.12, you can see that the technical field name (AUART) matches the technical name in the authorization role. At this point, the SAP Security administrator can show the functional team the field name in the transaction they are attempting to define.

If an organizational field is unmaintained, it appears red in the authorization window (see Figure 4.13). Notice how the field name has the word $VKORG in the line where field values would ordinarily be maintained, this is often how they appear when an organizational level has not been determined. Once the field level has been assigned in the **ORGANIZATIONAL LEVELS** window, $VKORG disappears and the field values appear as maintained.

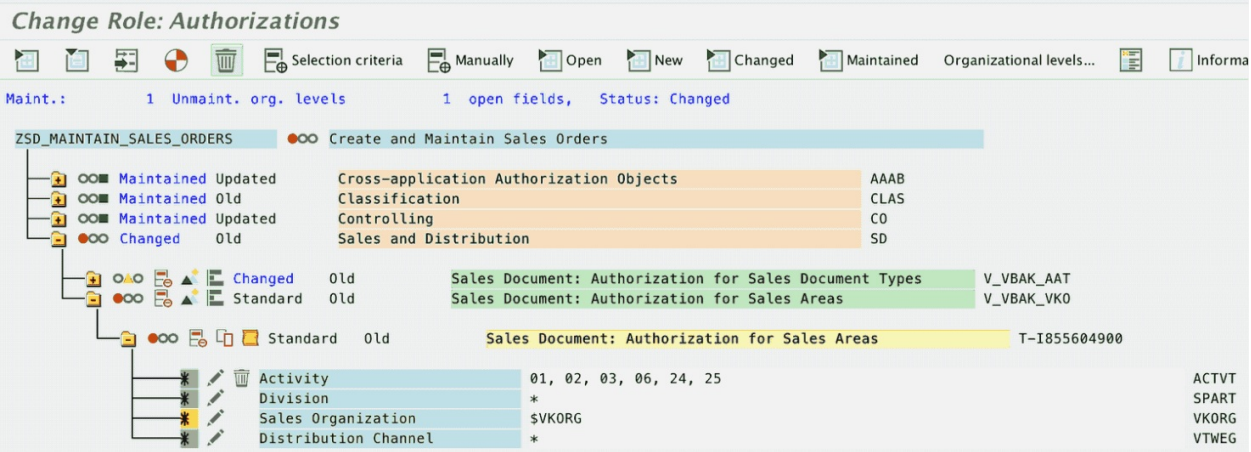


Figure 4.13: Authorization object with unmaintained org level

Pressing **"F1"** on authorization objects and fields within the PFCG authorization window will also produce a list of helpful information. Such information may include a description of the authorization object and potential field values.

Transaction SU21 can also aid the security administrator in finding similar useful information. As seen in Figure 4.14, clicking on the respective module (in this case SD) and the authorization object (V_VBAK_AAT) will show additional information.

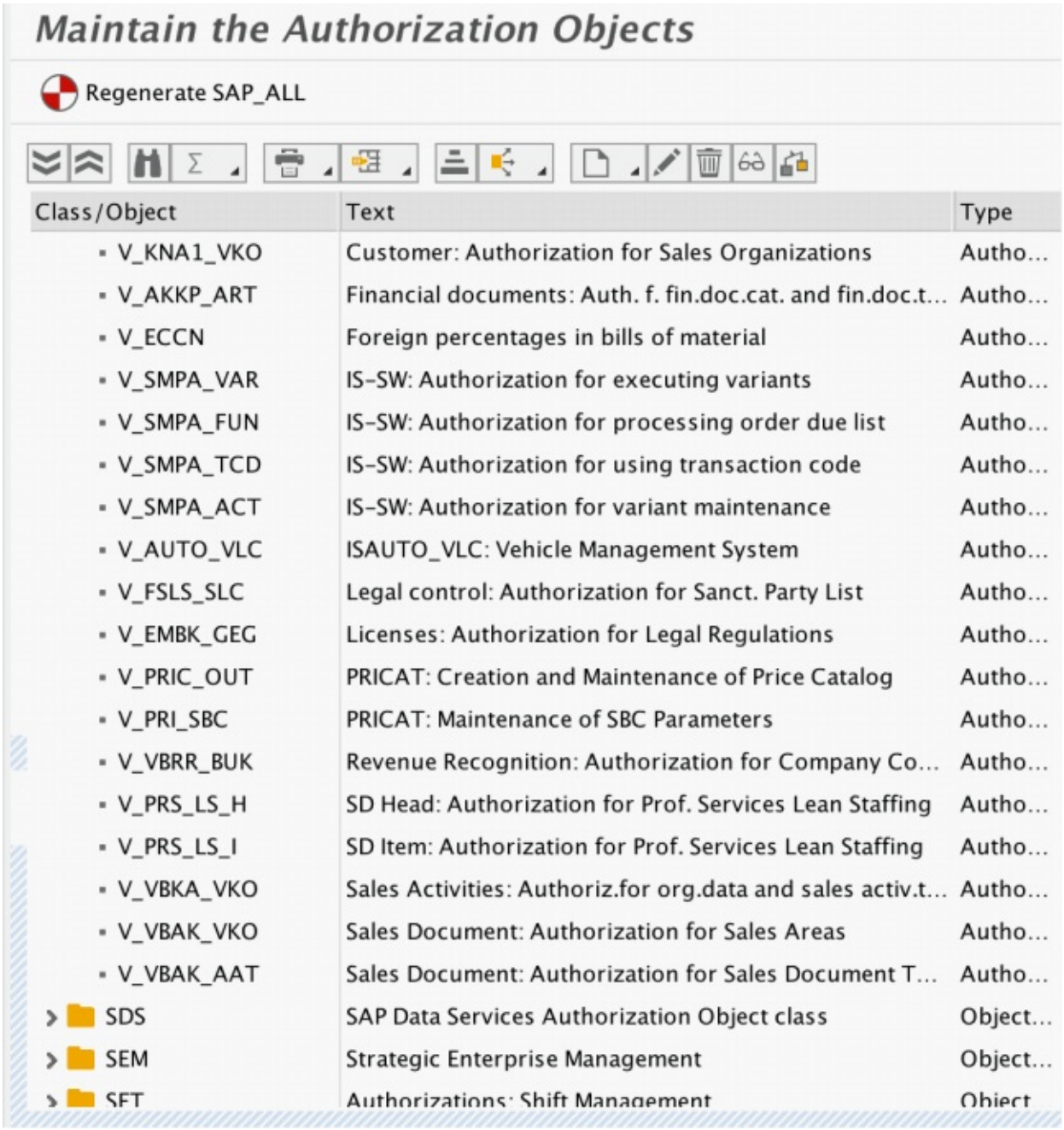


Figure 4.14: SU21 landing screen

Clicking the **DISPLAY OBJECT DOCUMENTATION** button in Figure 4.14 produces a pop-up window with the authorization object definition, field-level information, and possible field values (see Figure 4.15).

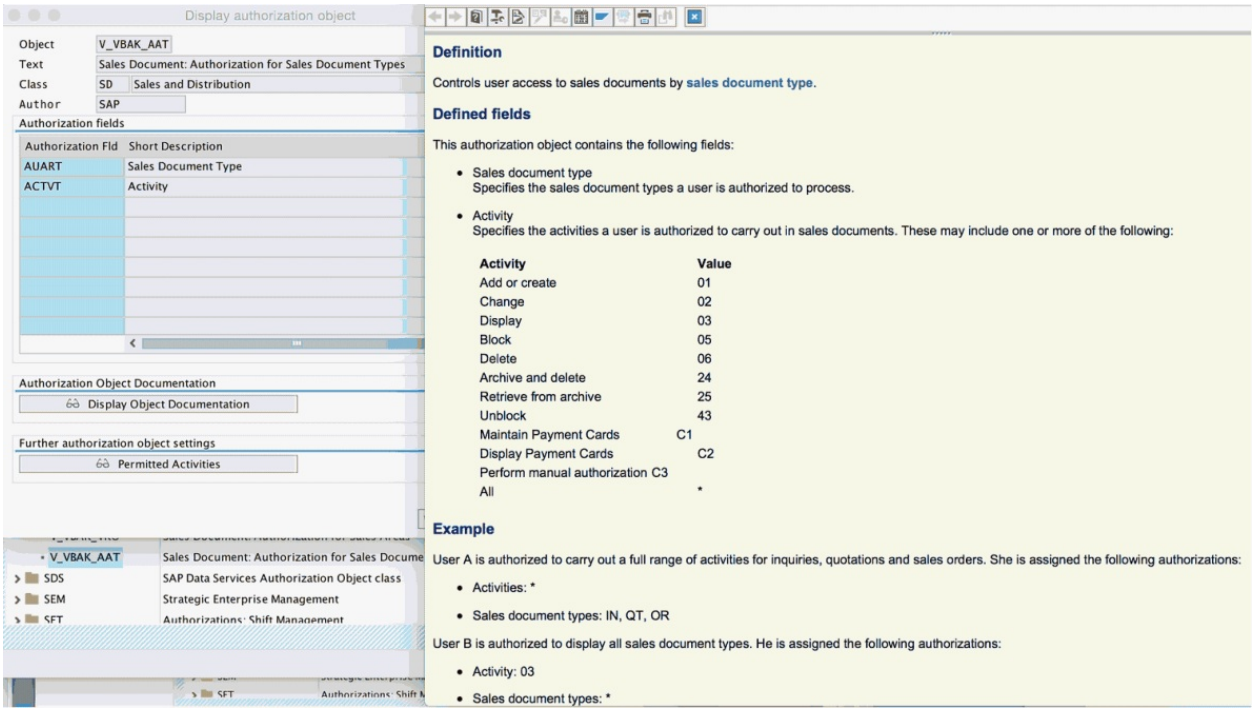


Figure 4.15: Object documentation

Once a role has been tested, it may be necessary to inactivate or delete an instance of an authorization object or the authorization object itself if user access is not required. Remember: a single authorization object can have more than one set (instance) of defined field values.

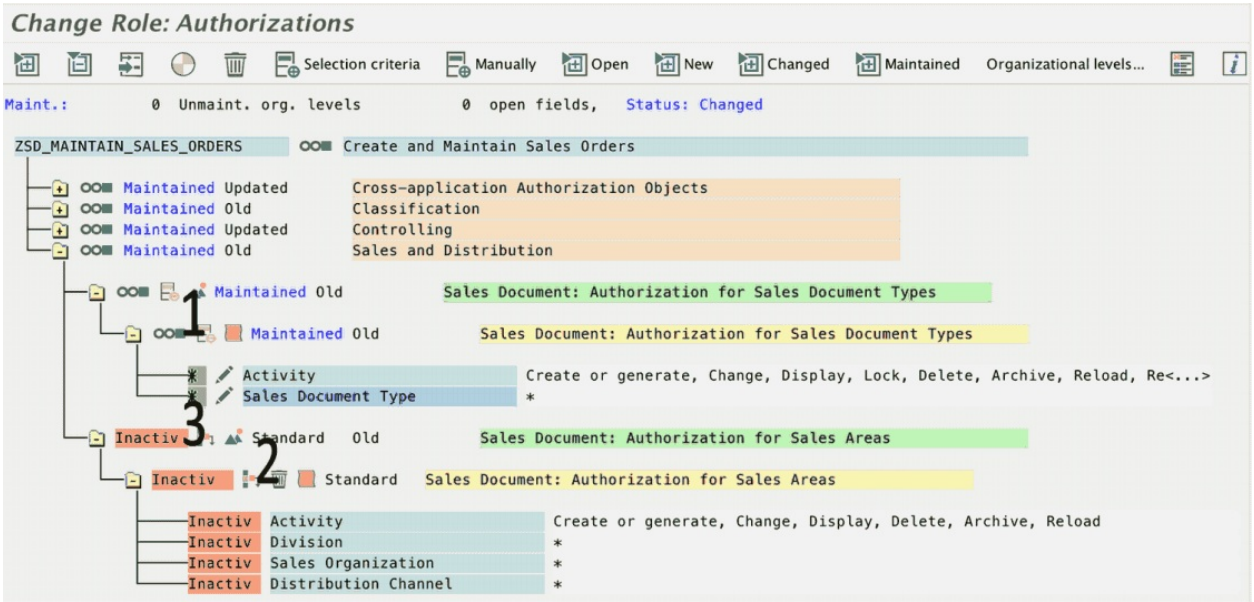


Figure 4.16: Inactivated authorization

❶ To inactivate an instance of an authorization object, click on the

MINUS button for the instance, as seen in Figure 4.16.

❷ Notice that once an instance has been inactivated a TRASH CAN appears, so that the instance can be deleted. If more than one instance of an authorization object exists, the same method is used, but click the INACTIVATE button at the object level.

❸ The button that replaces the inactivate button allows you to re-activate the instance or object that was previously inactivated.

Always inactivate

Personal experience dictates that it is always better to inactivate an instance of an authorization, but not to delete it. If the SAP Security administrator ever needs to refer back to the original state of the role, they are able to if this practice is followed.

If the administrator wishes to copy an instance of an authorization object, they only need to click on the authorization, select EDIT from the menu path, and choose COPY AUTHORIZATION. This will produce an identical instance of the authorization that was selected.

Once all the authorization data for the role has been configured, the administrator can clean up the authorization window by merging identical authorizations. This can be done by selecting UTILITIES from the menu path and choosing MERGE AUTHORIZATIONS. This task will combine authorizations and may reduce the number of profiles created for the role (remember only 150 authorizations can fit within a profile). To view all the profiles for a single role, select AUTHORIZATIONS from the menu path and choose PROFILE OVERVIEW. Only the first profile will be displayed on the role's authorization tab.

4.3 Role type review

There are three different types of SAP standard roles: single, derived, and composite (collective) roles.

4.3.1 Single roles

A single role contains authorization data. Section 4.1 discussed how to create single roles using the profile generator transaction (PFCG).

4.3.2 Composite roles

A *composite role*, also known as a *collective role*, is a grouping of single roles. When a composite role is assigned to a user, all the single roles associated with that composite role appear in the user master record. The user will have access to all the authorization data contained in those single roles and if the authorizations in a single role change, the composite role will automatically be updated as well. Creating a composite role also begins in the profile generator transaction (PFCG landing screen). First, enter the role name as desired, in this case Z_AP_CLERK (as seen in Figure 4.17) and then click the **COMP. ROLE** button.

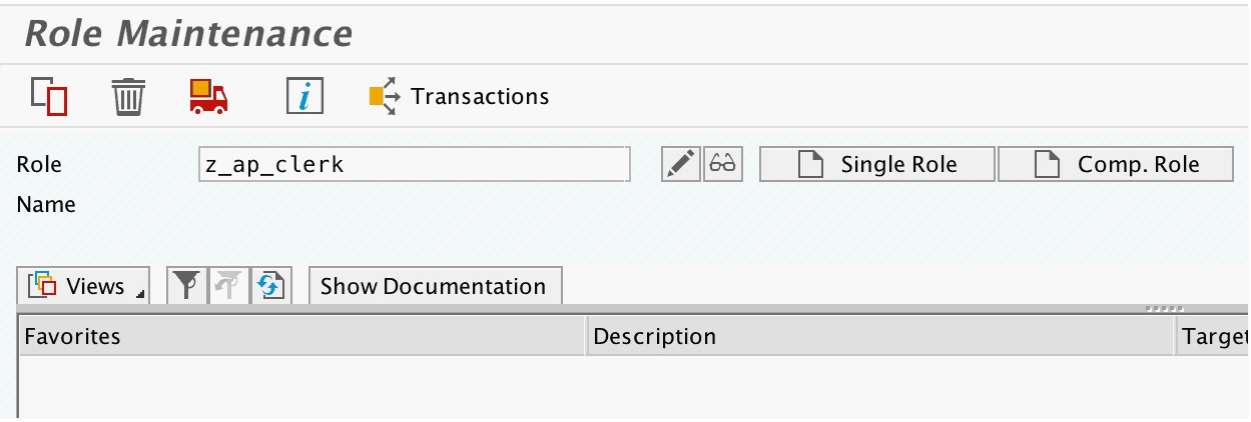


Figure 4.17: Creating a composite role

As with a single role, make sure to enter a role description on the description tab. The long text box can also be used to record additional information about the role and its contents. It is in the roles tab that the single roles contained in the composite are identified, as seen in Figure 4.18.

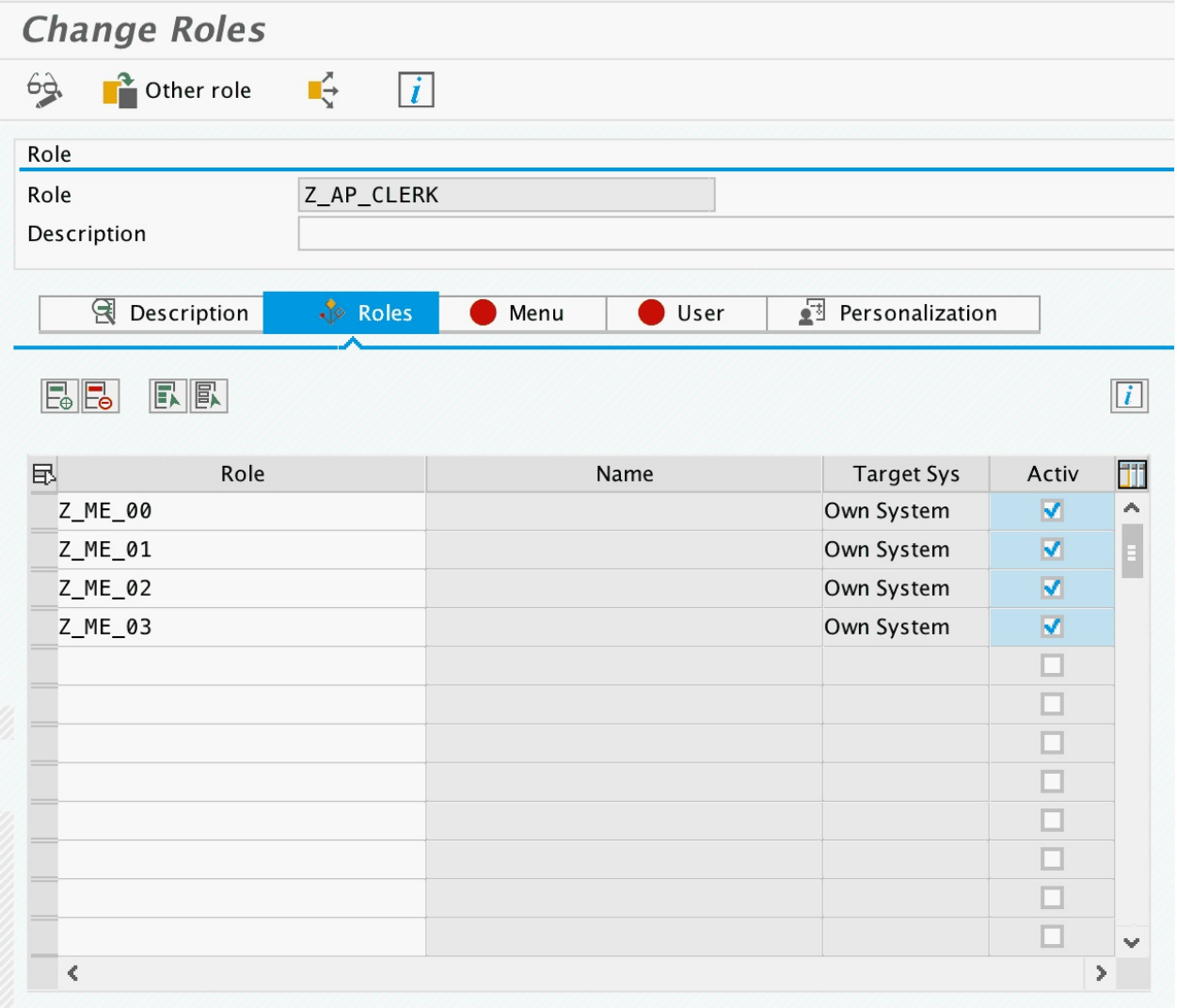


Figure 4.18: Roles tab in composite role

Roles can be manually entered or selected from the drop-down box and searched for by a role. Any user assigned to a composite role can see a composite role menu upon logging into SAP. On the menu tab of the role, all menus from the single roles can be imported into the composite to create a collective menu. As with a single role, users can be assigned to a composite role within the role's user tab or from transaction SU01 (user master record) or SU10.

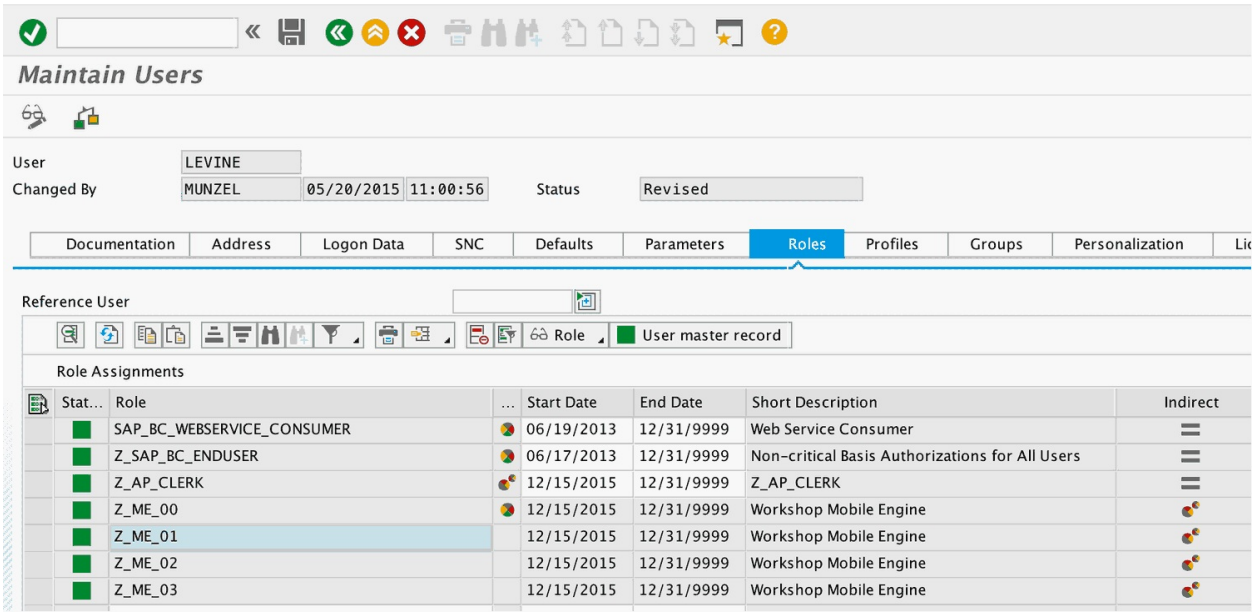


Figure 4.19: Composite role assignment in SU01

You will notice in Figure 4.19 that the composite role assignment appears differently in the user master record than previously assigned single roles. The colored circles next to the role name indicate the type of role that has been assigned, one circle indicates a single role and two circles indicate a composite role. The type column also shows whether the role has been directly or indirectly (from a composite role) assigned. The single roles that are assigned as a result of the composite role assignment cannot be removed from the user's master record without removing the entire composite role.

4.3.3 Derived roles

A *reference-derived role* is a type of single role that inherits the menu structure, transactions, reports, and any other objects from an existing role. A derived role is useful when a need exists to mimic a role's functionality, but provide access to different organizational levels. In a derived role, the only elements not inherited are user assignments and organizational levels. A derived role is also referred to as a *child role*, and the role from which it inherits its authorizations is often referred to as a *parent role* or *master role*.

Derived role examples

Jen and Allyson are both sales clerks and need access to the same transaction codes and authorizations, however, Allyson works in sales organization 2000, whereas Jen works in sales organizations 2000 and 3000. Their boss, Tracy, works across all sales organizations. Derived roles can be created based on the all-inclusive role that Tracy has and limited to company codes 2000 and 3000. Jen will receive both derived roles and Allyson will receive only the one for 2000.

Now, you may argue that in the example above, Tracy's role could be copied and the **ORGANIZATIONAL LEVELS** window could merely be manipulated to account for the deviations in sales org access. This is possible; however, if a new transaction is made to Tracy's role, the corresponding derived roles would be updated, decreasing redundancy and man-hours to maintain the role design. If the role is copied and changed, the transaction needs to be added to the copied roles.

To create a derived role, begin with the same steps as for any single role. Go to the profile generator transaction (PFCG) and enter the derived role name in the **ROLE** text box and click the **SINGLE ROLE** button, as seen in Figure 4.20.

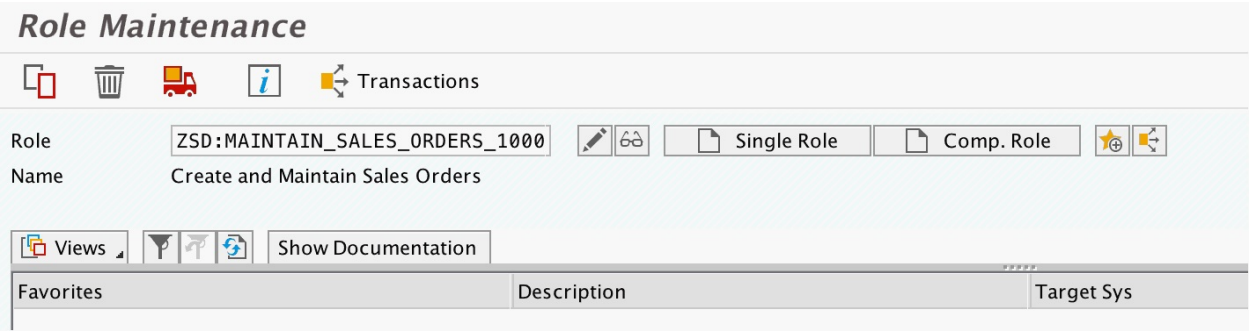


Figure 4.20: Creating a derived role

The next step is to enter the parent or master role in the **DERIVE FROM**

ROLE text box. The system prompts you to confirm that you desire to enter the specified imparting role in a pop-up window (see Figure 4.21).

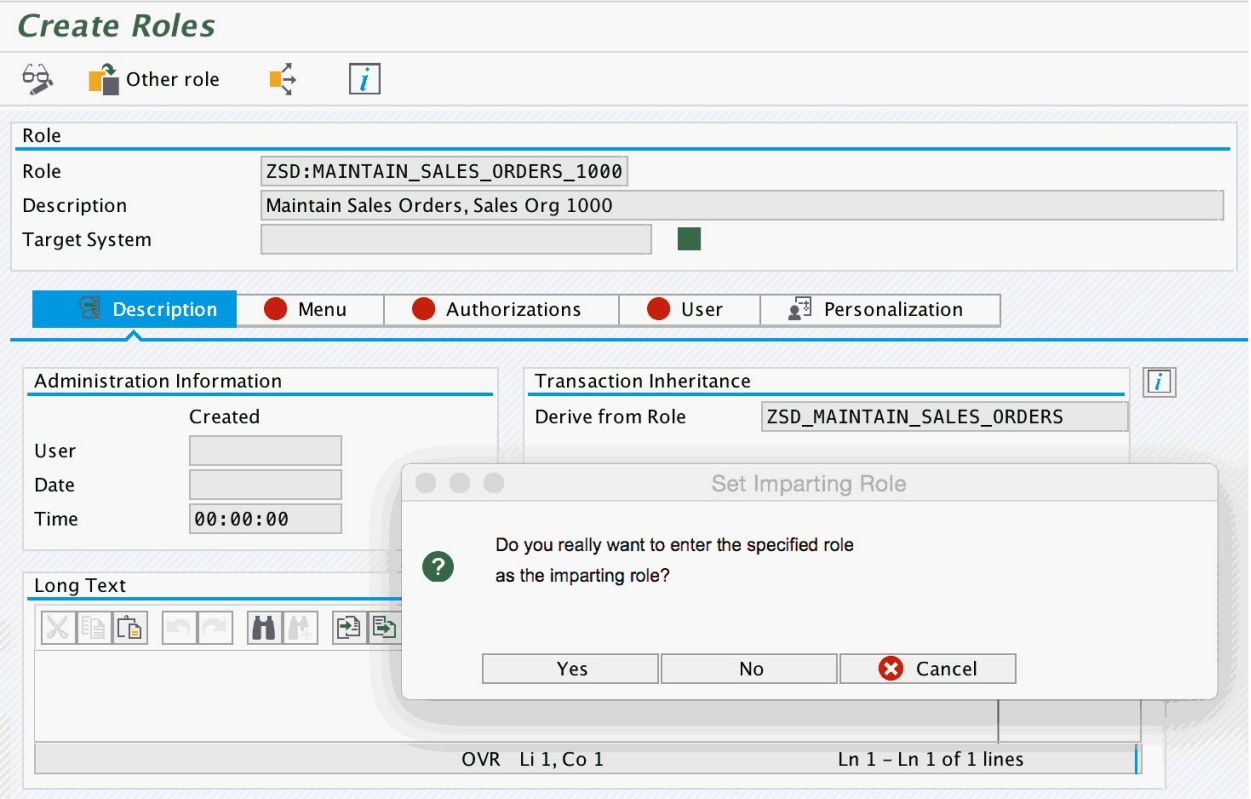


Figure 4.21: Identifying the parent (master) role

After saving, the menu tab traffic light turns green. This is because the menu has been brought over from the parent role. Alternatively, the traffic light on the authorization tab is still red. The authorizations and their field values still need to be retrieved. To do this, back out of the derived role to the PFCG landing page, enter the parent role in change mode, and go to the authorization window from the authorization tab. When a single role becomes a master role, a new button appears in the authorization window. This button has **TWO BOXES AND TWO ARROWS** on it and appears next to the **PROFILE GENERATION** button (see Figure 4.22).

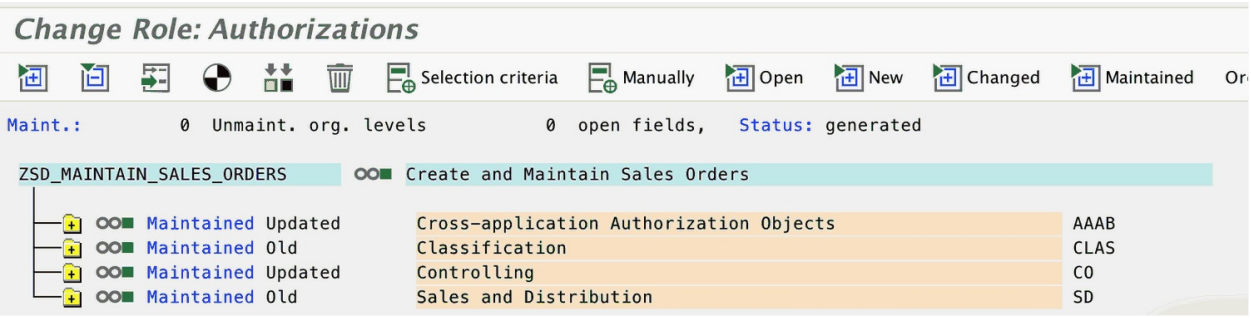


Figure 4.22: Pushing authorizations to child (derived) roles

The new button that appears is used to generate the associated derived role(s). There can be numerous derived roles associated with one parent role if there are many organizational levels for which access needs to be differentiated amongst the user population. Upon clicking this button, a pop-up window appears to confirm your action and once this is complete, the profiles for the derived roles are generated and the authorization objects and field values are populated in their respective authorization windows.

The last step is to update the derived role's organizational window with the correct values to differentiate it from the master role. Such is the case with the role, as shown in Figure 4.23, which is specific to sales organization 1000. As always, the role must be saved and the profile generated.

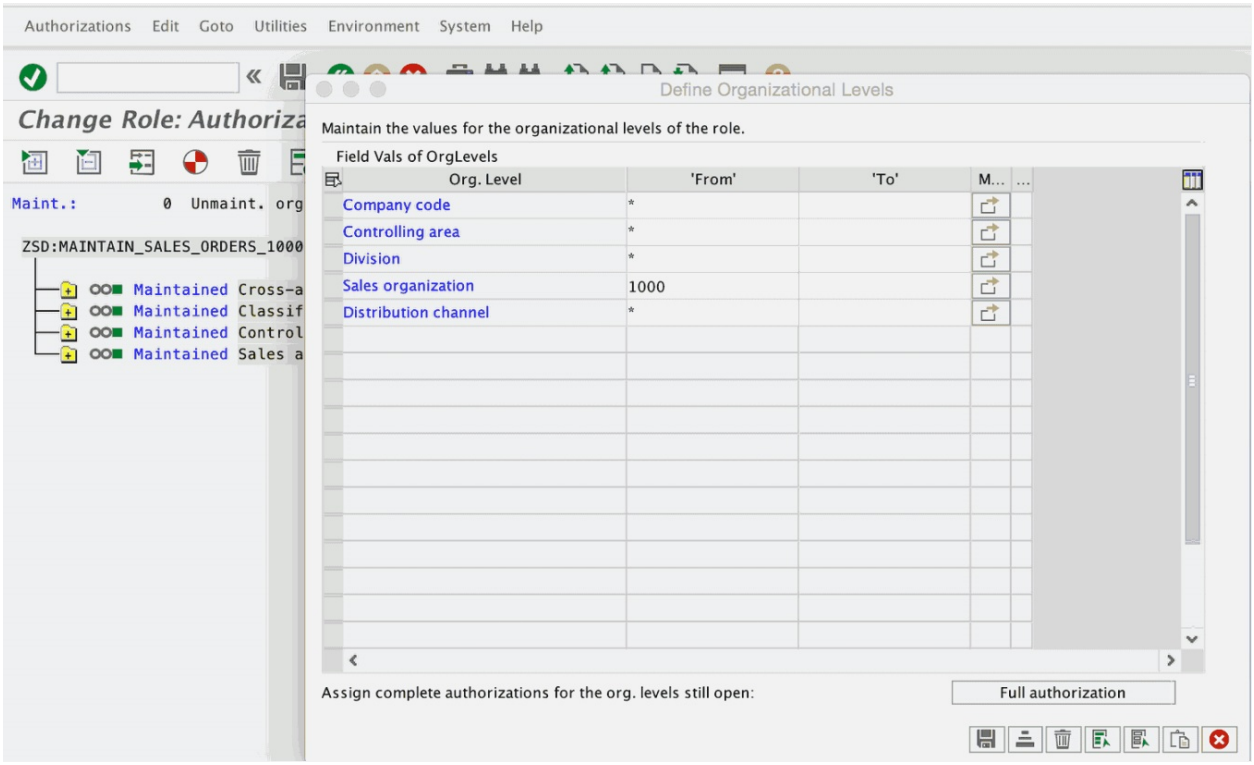


Figure 4.23: Updating org levels in derived role

4.3.4 Best practices for SAP role designs

The single most important rule to live by as an SAP Security

administrator is the *rule of least privilege*. The rule of least privilege dictates that users should have exactly what they need to do their daily jobs and very little else. Most SAP Security experts will promote a task-based role design in which each single role corresponds to a specific task in the system, such as maintain purchase orders. By utilizing a task-based role design, single roles can be more easily mixed and matched to account for differentiation between users who may have the exact same job title, such as AP clerk, but may not need authorization to perform identical tasks. As previously stated, all role names should be as explicit as possible and be an accurate representation of the authorizations contained in the role. Position-based composite or collective roles (i.e. Role for AP Clerk) can be created, but the best practice is to create these based on the lowest-level common denominator between the users who share this title.

Position-based composite roles

There are 3 AP clerks in company XYZ. XYZ utilizes a task-based role design with position-based composite roles. AP Clerk 1 needs task roles A, B, C, D, and E. AP Clerk 2 needs task roles A, B, C, D, and F. AP Clerk 3 needs task roles A,B, and C. The composite role for AP Clerk should include task-based single roles A, B, and C. Clerk 1 should also receive task roles D and E, and Clerk 2 should receive task role D and F.

User access reviews should be performed on a periodic basis to certify the assignment of roles and authorizations and to reduce *access creep*. Access creep occurs when users gain access to roles and authorizations that they do not require.

Access creep scenarios

Access creep may be difficult to detect and can occur for a variety of reasons. The most common access creep scenarios include:

1. One user fills in for another temporarily and their access is not removed upon the original user's return to work.

2. A user requires access to an additional task in the system. This access is then added to one of the user's roles and others who do not require the access inadvertently receive it through the role.

3. A user performs a task on a cyclical basis and retains the access when they no longer require it.

Now that you understand the rule of least privilege and access creep, you are ready for segregation of duties (SoD) risks. The only segregation of duties risks that should occur within an SAP system are those that are unavoidable and not merely a result of access creep. SoD risks are unavoidable when there simply are not enough individuals in a functional department to split up all of the job tasks in the manner necessary so that no risks occur. Security administrators can work in conjunction with a company's internal audit team and external auditor to better understand their specific risk and controls matrix and how to prevent avoidable SoD violations.

4.4 Transporting authorizations

Role changes are always done in the development environment and transported to the quality environment for testing and to the production system for live use. User master record changes are conducted directly in production, as it is a best practice not to move user role assignments when transporting roles. The transport management process includes three distinct steps.

1. Create transport request

1. Create transport request

- Roles can be transported individually or in large groups. In order to transport a single role, click on the **TRUCK** button on the PFCG landing page (see Figure 4.1) and follow the prompts. To transport groups of roles, click on **UTILITIES** in the menu bar on the PFCG home screen and choose **MASS TRANSPORT**. Role lists can be selected from the drop-down box or lists can also be copied from the clipboard prior to executing, as seen in Figure 4.24.

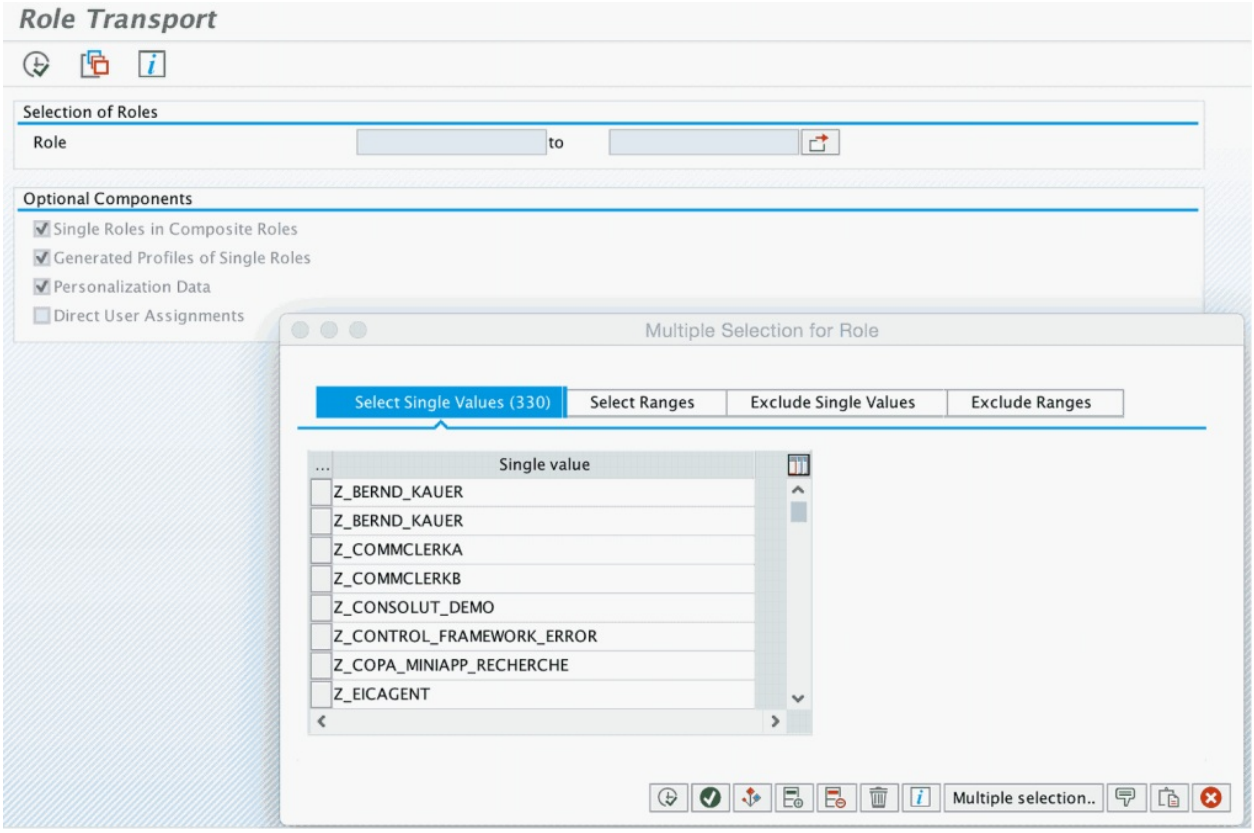


Figure 4.24: Mass transport of roles

- The following steps will be the same regardless of whether a single role or a group of roles are being transported. A prompt will appear for a customizing request (transport). To create a new transport request, click the **PAPER** button on the pop-up box (see Figure 4.25). Enter a short description and click the **FLOPPY DISK** button to save.

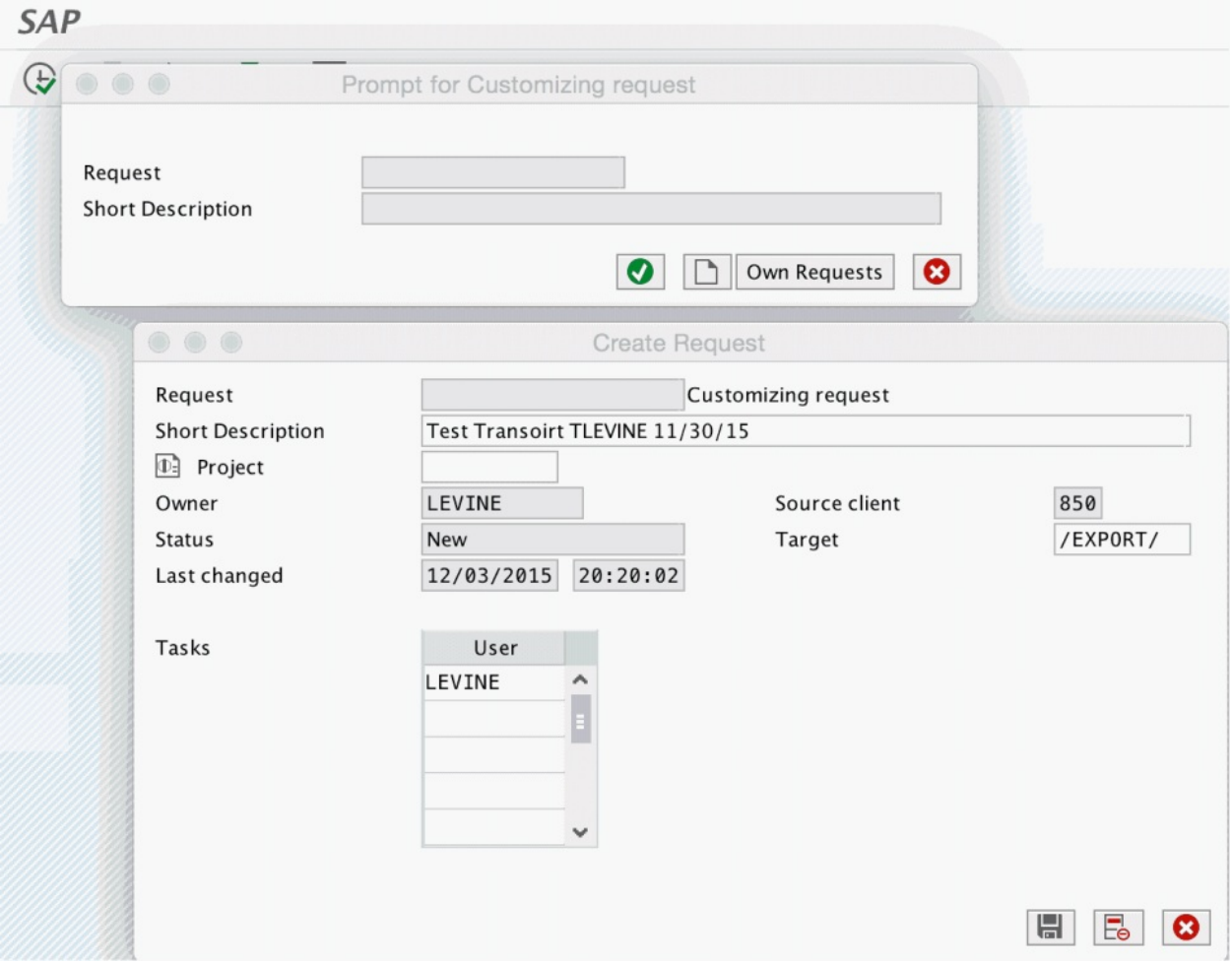


Figure 4.25: Creation of customizing request

- After the transport has been created, make sure to jot down the transport number because you will need it in the next step. Once you enter through the prompt for CUSTOMIZING REQUEST screen, the roles included in the transport will appear. As always, success is indicated by green traffic lights, whereas red traffic lights indicate an error with the inclusion of a specified role within the transport.
- Roles can also be added to an existing transport by searching for the existing request number instead of creating a new request.

2. Release transport request

- Go to transaction SE10 (transport organizer) to release the transport request (see Figure 4.26).

- Click the **DISPLAY** button and a list of transport requests will appear.

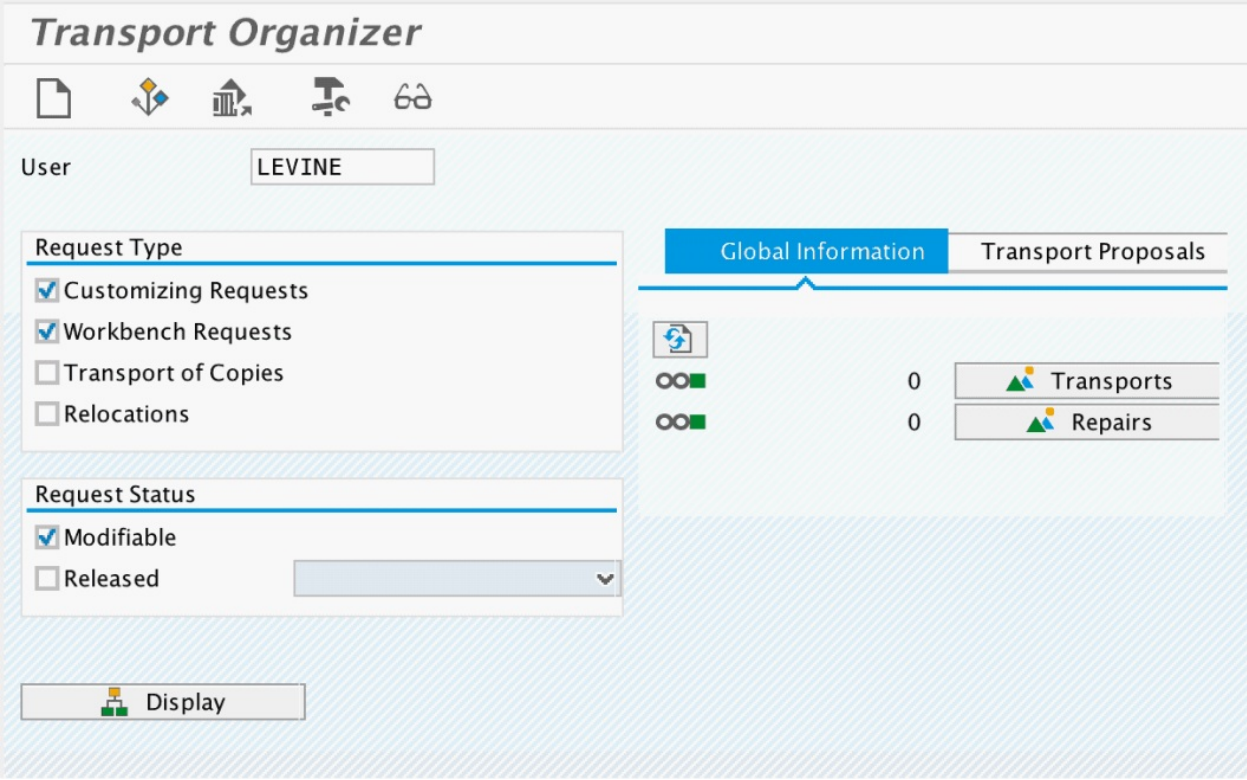


Figure 4.26: Transport organizer

- Select the request number from the list and expand the selection, as seen in Figure 4.27.
- Highlight the line in the request that is labeled as task. Click the **SINGLE TRUCK** button.
- Highlight the top line item in the request. Click the **SINGLE TRUCK** button.

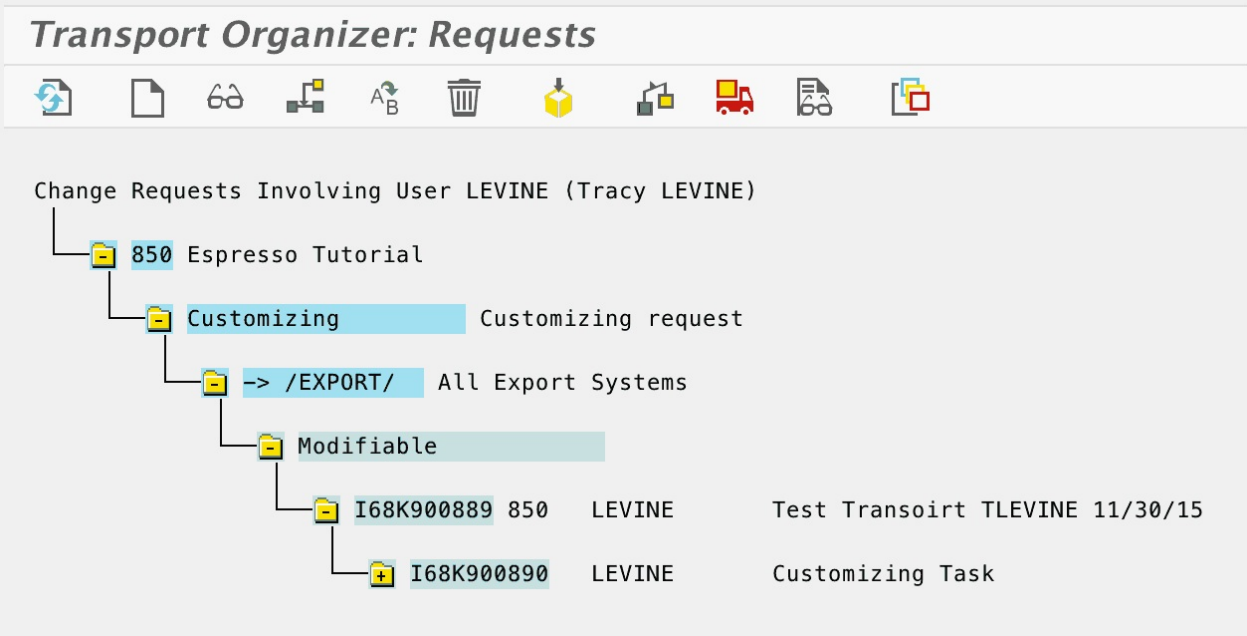


Figure 4.27: Transport request release screen

- A message will appear once the request has been successfully released.

3. Move transport to quality and/or production

- Most organizations will have a dedicated change management process, which will include the procedure behind transporting and testing security role changes.
- The responsibility of moving transport requests usually falls on the SAP Basis resource.

5 SAP Security and Authorizations trouble-shooting

This chapter covers some more advanced topics, including security and authorization trouble-shooting techniques. It also touches on some valuable tools and tables for identifying user master records and role and authorization information.

5.1 Reading an SU53

Transaction SU53 is useful if a user is a receiving an error message because of missing authorizations. To diagnose authorization errors using transaction SU53, follow these steps: 1. Have the user recreate the error and IMMEDIATELY go to transaction /nsu53 and send a screenshot of that page.

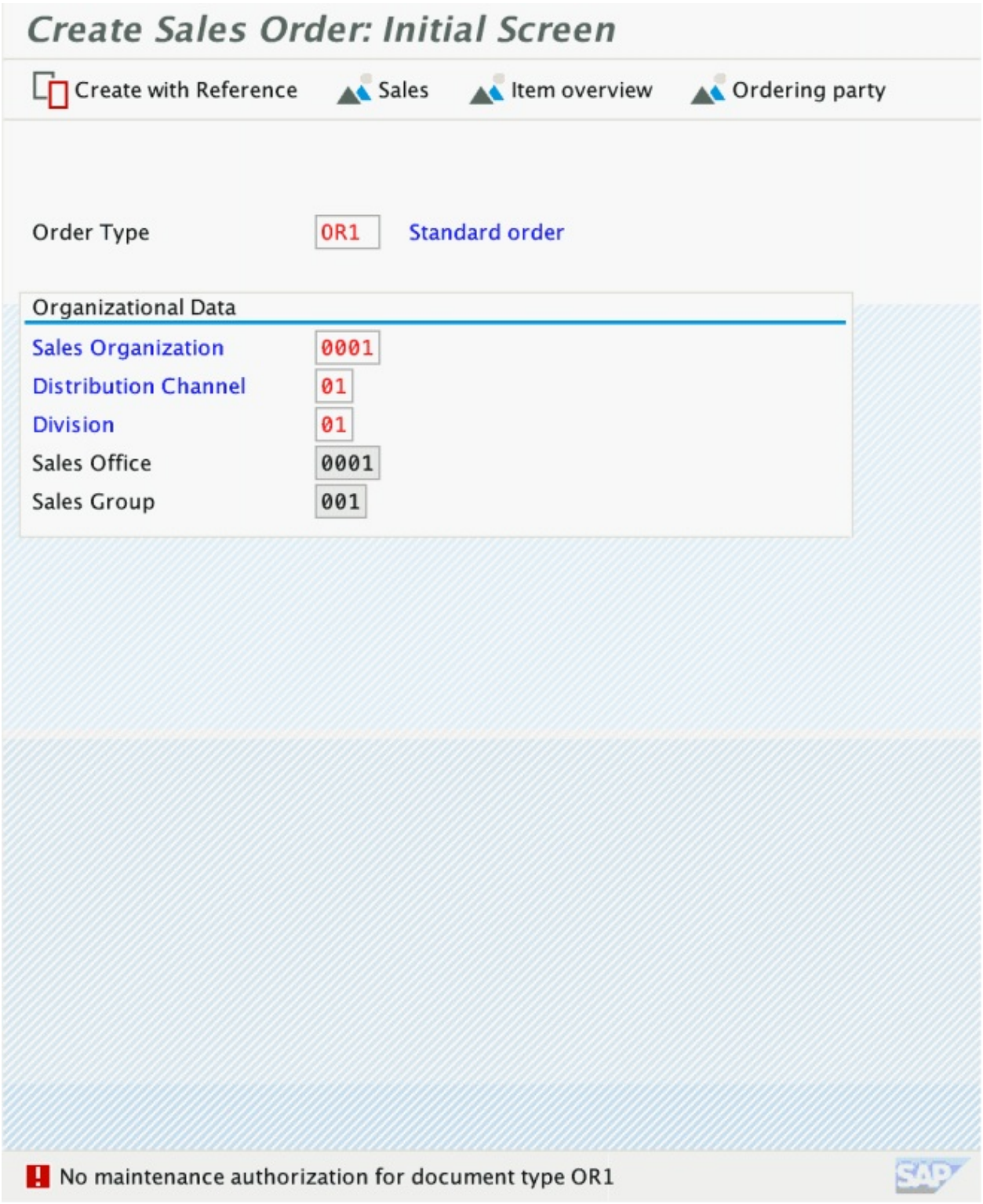


Figure 5.1: Error Message: "No authorization for document type OR1"

2. The page will show authorization object ''_''_'' and values that are needed.

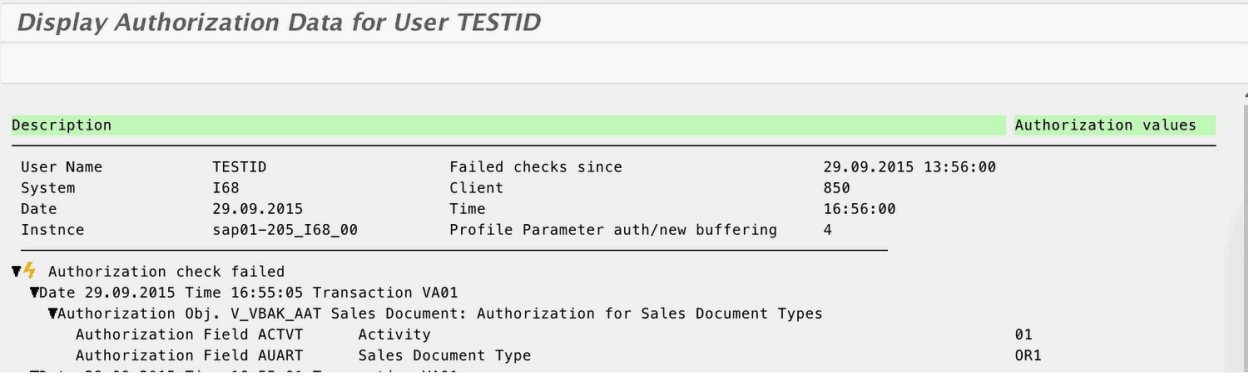


Figure 5.2: Transaction SU53 displays last authorization object error and missing field values

SU53 example

In the above screen shots, user “TESTID” is aiming to create a standard sales order (sales document type OR1) in Sales Organization 1000 via transaction VA01 (create sales order). The user is able to execute the transaction, but upon sales order creation receives the error message “no authorization for document type OR1” (Figure 5.1). The user executed transaction SU53 to diagnose the authorization error (Figure 5.2). As the authorization error indicates, the user failed on authorization object V_VBAK_AAT (authorization for sales doc types). The field values required are also indicated; Activity 01 (create) and Sales Document Type OR1 (standard order). Currently, the role that the user is assigned to only has authorization to display standard orders.

1. There are two options on how to proceed:
   a. Create a brand new authorization object (does not already exist in the role)
      i. Go to SU24 and maintain authorization object for specified transaction
         1. Anytime that transaction is added to a role from now on, that authorization object will be pulled in
      ii. Go to PFCG, AUTHORIZATION tab, Change Authorization
         1. Click the MANUALLY ADD button at top
         2. Manually add the authorization to the role
   b. Authorization object that exists in the role
      i. Get approval and update the role with the necessary values

5.2 Running a trace (ST01)

One of the drawbacks to using transaction SU53 is that it only shows the most recent authorization error. On occasion, SU53 will produce misinformation based on the last authorization failure.

SU53 warning

It is important to ask, “What is this user trying to do? Does SU53 make sense based on the job task being performed?” SU53 may sometimes give misinformation because it only reports the last failure, which may not be the authorization object required specific to the issue that is arising.

If SU53 is not a suitable option to diagnose an authorization, transaction ST01 (system trace) is a more all-encompassing option (see Figure 5.3). Trace files show all authorization passes and failures over a given period of time. Unlike SU53 however, transaction ST01 should be reserved for security administrators and other super-users, such as basis admins and developers. To run a security authorization trace using transaction ST01, follow these steps: 1. Select the **AUTHORIZATION CHECK** radio button 2.

Put a user ID in the **TRACE FOR USER ONLY** field in the **GENERAL FILTER** section 3. Click the button to **TURN TRACE ON**

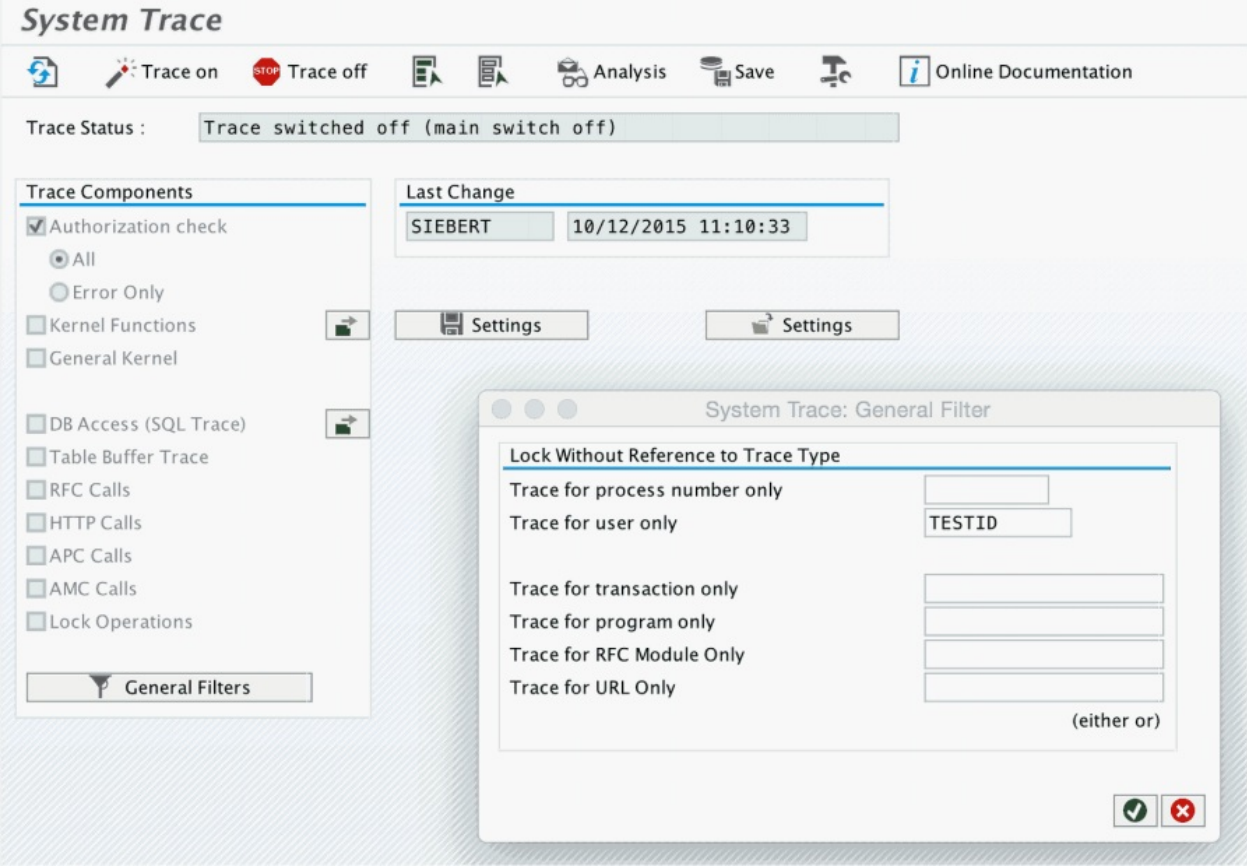


*Figure 5.3: Authorization trace home screen 4. Have the user recreate error 5. Click the button to **TURN TRACE OFF** 6. Click **ANALYSIS** 7. Fill in the credentials (make sure the user ID that you enter is the one you are running trace against) and execute (see Figure 5.4)*

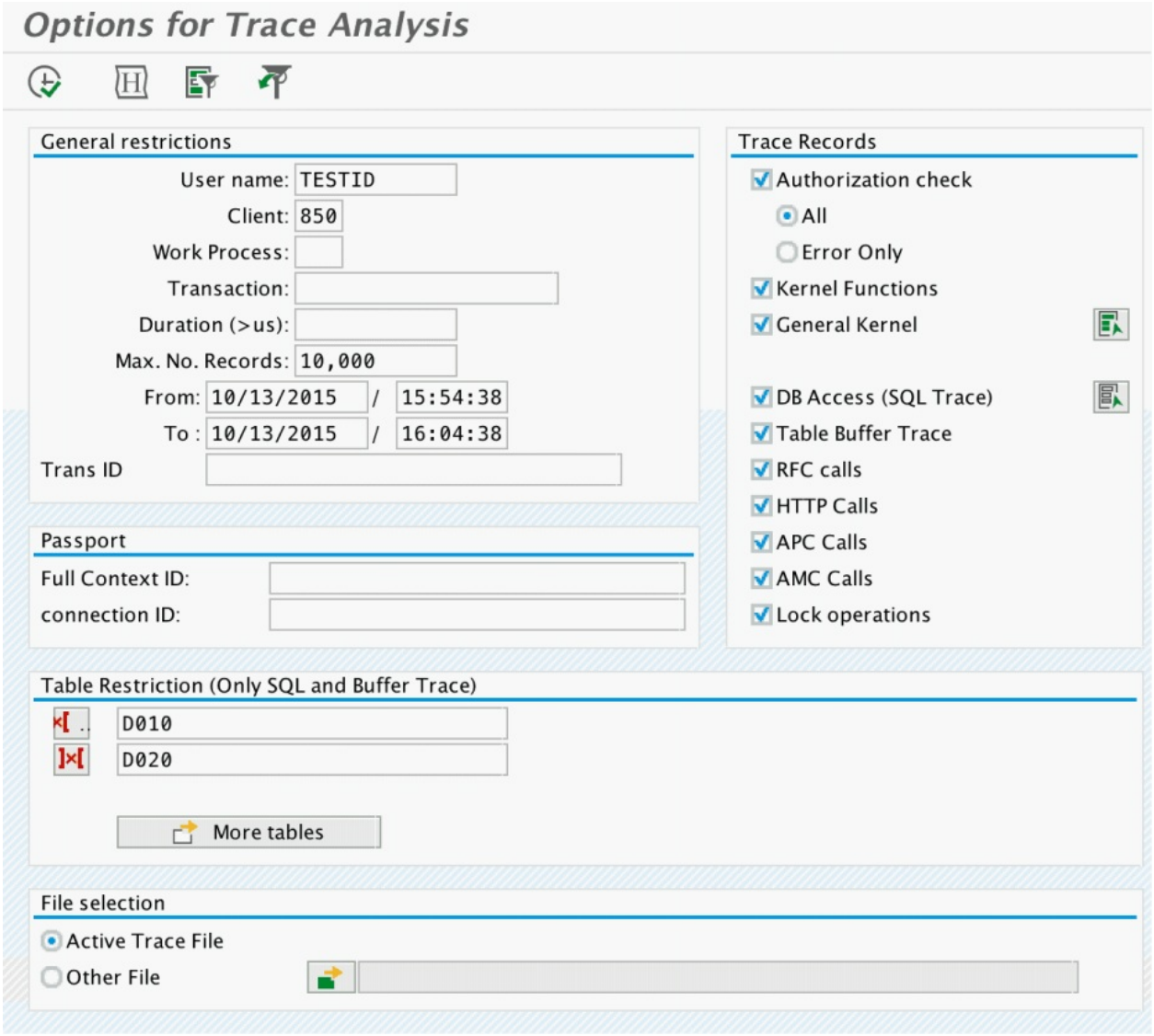


*Figure 5.4: Analysis credentials screen 8. Anytime **RC (RETURN CODE)** does not equal 0, it is a failure (as seen in Figure 5.5)*

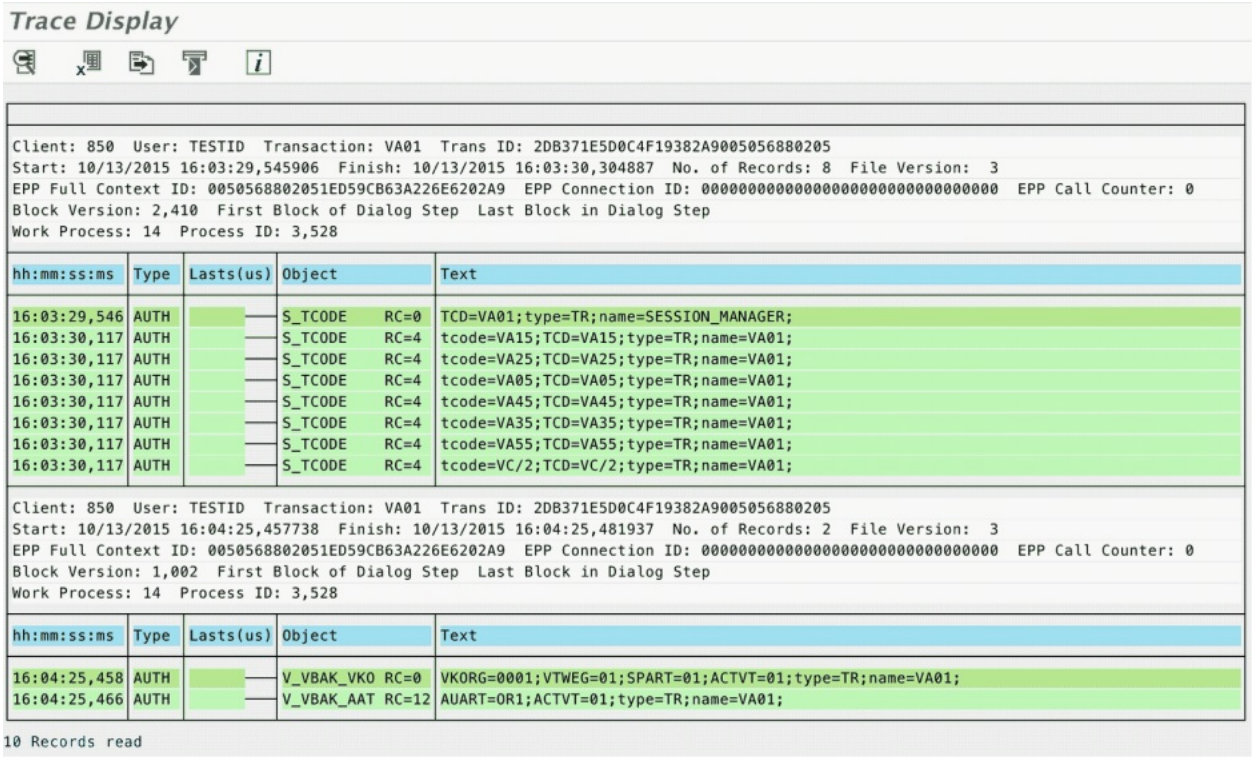


Figure 5.5: Authorization trace output for analysis Figure 5.5 reflects the identical authorization error to Figure 5.2 in that the user is unable to create a standard order (order type OR1) in transaction VA01. As previously mentioned, anytime a line item indicates that RC does not equal, an authorization failure is present. Such failures are also represented in a different color on the ST01 output screen.

Tip for running traces

On rare occasions, the information displayed in an ST01 trace file only shows authorizations that the user currently has and will not accurately depict authorization fails, which can make it difficult to diagnose issues. In this instance, compare the trace file of a user who can complete the task with one who cannot. The answer should lie in the differences.

5.3 Useful SAP Security tables and sensitive authorizations

SAP Security administrators and consultants will often need to utilize technical SAP tables to query large amounts of data as it relates to users

and roles. Many SAP transactions store field information that is housed in the table repository and such information can be viewed in transactions SE16 and SE16N, the data browsers (see Figure 5.6). The most commonly used SAP Security tables begin with “AGR” and “USR (see Section 5.3.1).”

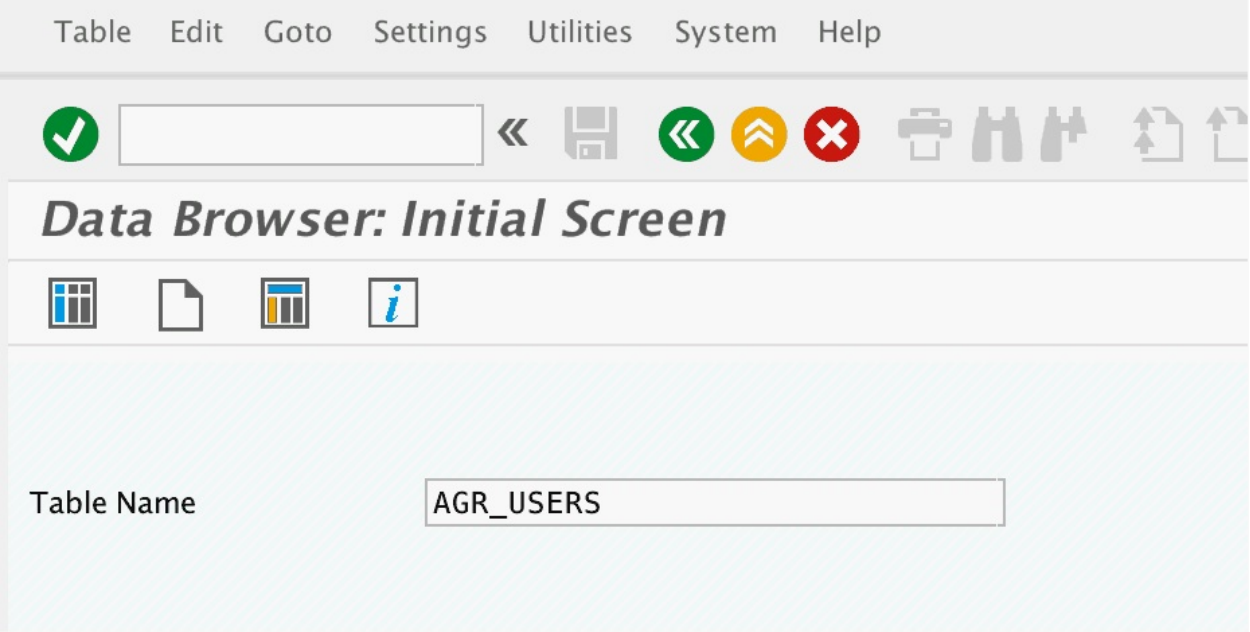


Figure 5.6: Home screen of transaction SE16 with table name “AGR_USERS” populated Table information is returned based on the selection criteria populated by the SAP security administrator, as seen in Figure 5.7.

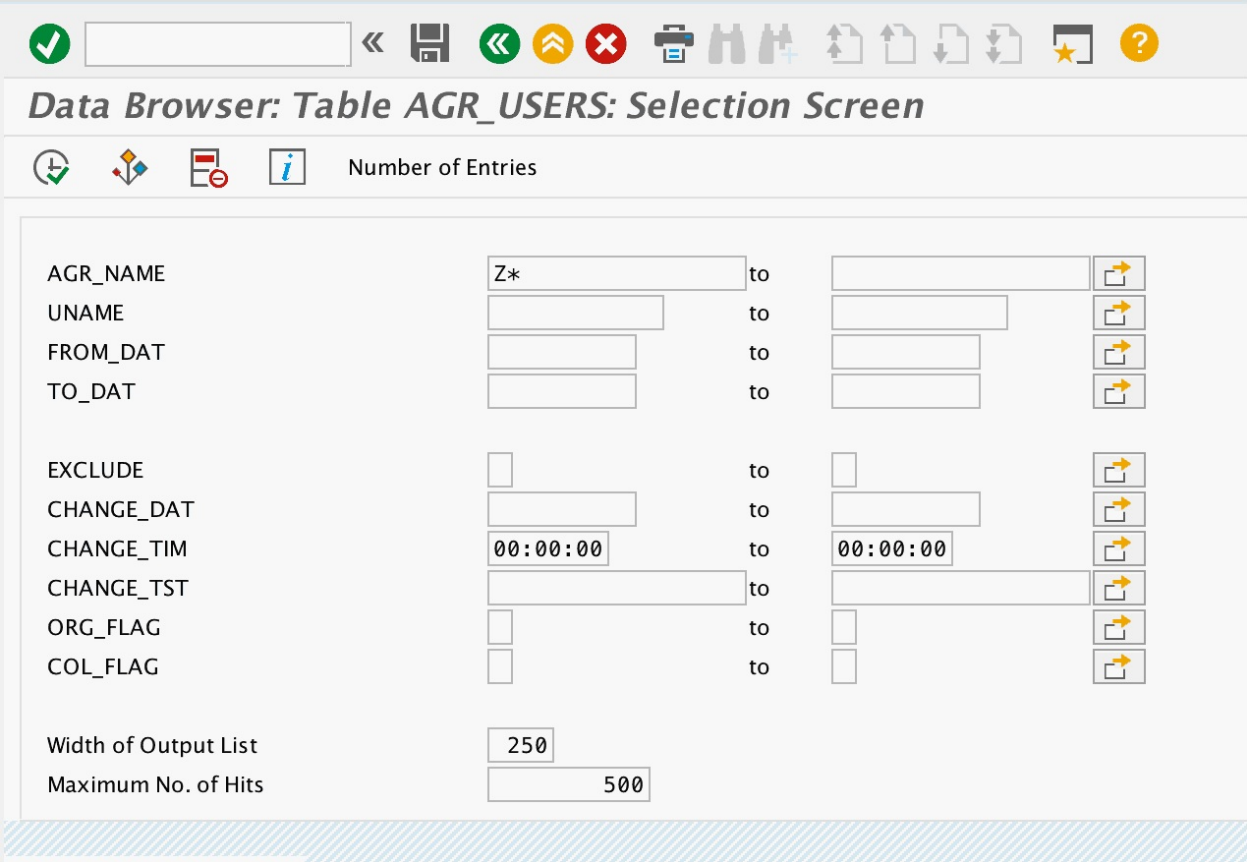


Figure 5.7: Selection criteria for table "AGR_USERS"

Figure 5.8 depicts the table data returned from the chosen selection criteria.

Data Browser: Table AGR_USERS Select Entries 57

Check Table...

Table: AGR_USERS
Displayed Fields: 11 of 11 Fixed Columns: 5 List Width 0250

MANDT	AGR_NAME	UNAME	FROM_DAT	TO_DAT	EXCLUDE	CHANGE_DAT	CHANGE_TIM	CHANGE_TST	O
850	ZSAP_MM_SSP_EMPLOYEE	VOLKER	08/20/2013	12/31/9999		08/20/2013	14:25:14	0	
850	ZUFCOPABUKRS	FAHRNSCHON	05/06/2015	12/31/9999		05/06/2015	09:26:50	0	
850	Z_GERHARD	CHRISTINE	10/07/2013	12/31/9999		11/10/2013	16:21:19	0	
850	Z_SAP_BC_BASIS_ADMIN	VOLKER	06/17/2013	12/31/9999		06/17/2013	15:04:36	0	
850	Z_SAP_BC_ENDUSER	ALICE	06/17/2013	12/31/9999		07/31/2015	17:49:29	0	
850	Z_SAP_BC_ENDUSER	ANJA	06/17/2013	12/31/9999		07/31/2015	17:48:56	0	
850	Z_SAP_BC_ENDUSER	BATCH	06/17/2013	12/31/9999		06/17/2013	15:27:01	0	
850	Z_SAP_BC_ENDUSER	BAUER	06/17/2013	12/31/9999		02/23/2014	17:40:35	0	
850	Z_SAP_BC_ENDUSER	CACCIOTTOLLI	06/17/2013	12/31/9999		07/31/2014	09:42:10	0	
850	Z_SAP_BC_ENDUSER	CUA_ALE	06/17/2013	12/31/9999		06/17/2013	15:27:01	0	
850	Z_SAP_BC_ENDUSER	DDIC	06/17/2013	12/31/9999		06/17/2013	15:27:01	0	
850	Z_SAP_BC_ENDUSER	DEPPE	06/17/2013	12/31/9999		07/28/2014	17:36:05	0	
850	Z_SAP_BC_ENDUSER	EIFLER	06/17/2013	12/31/9999		06/17/2013	15:27:01	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-00	06/17/2013	12/31/9999		07/30/2015	08:44:11	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-01	06/17/2013	12/31/9999		07/30/2015	08:44:13	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-02	06/17/2013	12/31/9999		07/30/2015	08:44:13	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-03	06/17/2013	12/31/9999		07/30/2015	08:44:13	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-04	06/17/2013	12/31/9999		07/30/2015	08:44:13	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-05	06/17/2013	12/31/9999		07/30/2015	08:44:13	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-06	06/17/2013	12/31/9999		07/30/2015	08:44:14	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-07	06/17/2013	12/31/9999		07/30/2015	08:44:14	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-08	06/17/2013	12/31/9999		07/30/2015	08:44:14	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-09	06/17/2013	12/31/9999		07/30/2015	08:44:14	0	
850	Z_SAP_BC_ENDUSER	ESPRESSO-10	06/17/2013	12/31/9999		07/30/2015	08:44:14	0	
850	Z_SAP_BC_ENDUSER	FONSECA	06/17/2013	12/31/9999		03/30/2015	19:59:46	0	
850	Z_SAP_BC_ENDUSER	FREIG	06/17/2013	12/31/9999		12/26/2013	11:00:56	0	

Figure 5.8: Data populated based on selection criteria

5.3.1 Useful SAP security tables

Table name:
Table description:

AGR_1251
Role object, authorization, field, and value AGR_1252
Organizational elements for authorizations AGR_AGRS
Roles in composite roles

AGR_DEFINE
To see all roles (Role definition) AGR_PROF
Profile name for role

AGR_TCODES
Assignment of roles to T-codes

AGR_TEXTS
Role and role description

AGR_USERS
Assignment of roles to users

TSTCT
Transaction code texts

USER_ADDR
Address data for users

USGRP
User groups

USR02
User data (logon data)

USR03
User address data

Authorization for the following SAP ECC (ERP Central Component) transaction codes (see Section 5.3.2) and authorization objects (see Section 5.3.3) are only to be assigned to roles, which indicate the inclusion of sensitive information or critical actions. Such roles are to be assigned to user master records with a fine toothcomb and access must be monitored on a periodic basis to ensure retention of such authorizations is required. The business processes of finance, human resources, basis, and security are commonly regarded as the most critical, regardless of industry, as reflected in the lists below.

5.3.2 Sensitive and critical SAP transactions

Transaction:
Transaction description:

CA87
Mass replace work center

CAT6
Human Resources

CL04
Delete class

F.34
Credit limit mass changes

F.80
Mass reversal of documents

F044
Vendor archiving

FI12
Change house banks or bank accounts IP30
Run-date monitoring

LN08
Number range maintenance: LVS_LENUM

MMPV
Close periods

MMRV
Allow posting to previous period

PA20
Display HR master data

PA30
Maintain HR master data

PA70
Fast entry

PA97
Compensation administration – matrix PFCG
Role maintenance – system integrity, stability at risk RZ04
Maintain SAP instances

SA38
ABAP reporting – can run programs not protected appropriately SARA
Archiving management – should be restricted to archive administrator SCC1
Client copy – special selections

SCC4
Client admin. – system stability and integrity at risk SCC5
Delete client – system stability at risk SCC6
Client import – system stability and integrity at risk SCC9
Remote client copy – system stability and integrity at risk SCCL
Local client copy – system stability and integrity at risk SE01
Transport organizer – system stability and integrity at risk SE11
Data dictionary maintenance – system stability and integrity at risk SE13
Maintain tech tables settings – system stability at risk SE16
Data browser – exposure to confidential information SE37
Function builder

SE38
ABAP editor – system stability and integrity at risk SM01
Lock transactions – system stability at risk SM02
System messages – should be restricted to system administrators only SM30
Table maintenance – system integrity and stability at risk SM49
Execute OS commands – system stability at risk SM50
Work process overview – system stability at risk SU01
User maintenance – should be restricted to user administrators only SU02
Profile maintenance – system stability and integrity at risk SU03
Maintain authorizations

SU05
Maintain Internet user

SU10
User mass maintenance – system stability at a very high risk SU20
Authorization object fields

SU21
Authorization objects

SU24

Maintain assignment of authorization objects SU25
Profile generator upgrade and first installation

5.3.3 Sensitive and critical SAP authorization objects and their values

Restricted object

Restricted field:

Authorization object description: S_DEVELOP

OBJTYPE
Prevent direct development access to production through DEBUG, FUGR, or PROG

S_ADMI_FCD
S_ADMI_FCD
System administrative functions

S_PROGRAM
P_GROUP
ABAP: Program flow checks

S_RFC
RFC_NAME
Authorization check for RFC access S_RFCACL
{Multiple}
Authorization check for RFC user (e.g. trusted system) S_TABU_DIS
DICBERCLS
Table authorization group restriction S_BDC_MONI
{Multiple}
Batch management authorization

S_BTCH_ADM
BTCADMIN
Restrict batch administrator access S_BTCH_JOB
{Multiple}
Background processing: Operations on background jobs S_BTCH_NAM
BTCUNAME
Background processing: Background user name S_ALV_LAYO
ACTVT
Sensitive object – S_ALV_LAYO for report maintenance S_SCRP_TXT
{Multiple}
SAP script: Standard text

S_IDOCMONI
EDI_MES
EDI message type restriction

S_USER_AGR
{Multiple}
Restrict the maintenance and assignment of roles S_USER_GRP
{Multiple}
Restrict the maintenance of user master records S_SPO_ACT
{Multiple}
Maintenance to spool requests which aren't your own S_SPO_DEV

Maintenance to spool requests which aren't your own S_SPO_DEV
SPODEVICE
Spool: Device authorizations

S_CTS_ADMI
CTS_ADMFCT
Control the flow of transports into production S_TRANSPRT
{Multiple}
Transport organizer

5.4 Maintain authorization object assignment to transaction codes (SU24)

Transaction SU24 is the transaction code that allows you to maintain the assignment of authorization objects to transaction codes. SU24 ties the SAP Security and Authorizations concept together at its core. When a transaction code is added to role, authorization objects, and all or some of their field values may be automatically brought into the role. How does SAP know what authorization objects and field values are tied to the transaction? Well, this information is stored in transaction SU24. SAP has developed standards for all transaction codes and associated authorization objects, but a company can also manually make changes to SU24 as required.

SU24 example

Anytime VA01 (created sales order) is added to a role, authorization object V_VBAK_AAT (authorization for sales document type) is also automatically brought in. V_VBAK_AAT has two fields: ACTVT (activity) and AUART (sales doc type). In the activity field, activity “01” (create) is also automatically populated, however no automatic entries are populated for sales doc type. At company XYZ, anytime a user has access to VA01, they should automatically be able to create sales document type “OR1” (standard order). In this instance, VA01 and V_VBAK_AAT can be updated manually via transaction SU24 to include authorization for standard orders.

In order to manually maintain the assignment of authorization objects and their values to transaction codes in SU24, follow these steps: 1. Go to transaction SU24 (see Figure 5.9).

2. As in the example above, you want to add sales doc type “OR1” anytime VA01 is added to a role. In this case, type “VA01” in the **TRANSACTION CODE** box**.** Click the **EXECUTE** button. If anytime the authorization object appeared in the role you want “OR1” to be added, switch to the **AUTHORIZATION OBJECT** tab and follow the same steps.

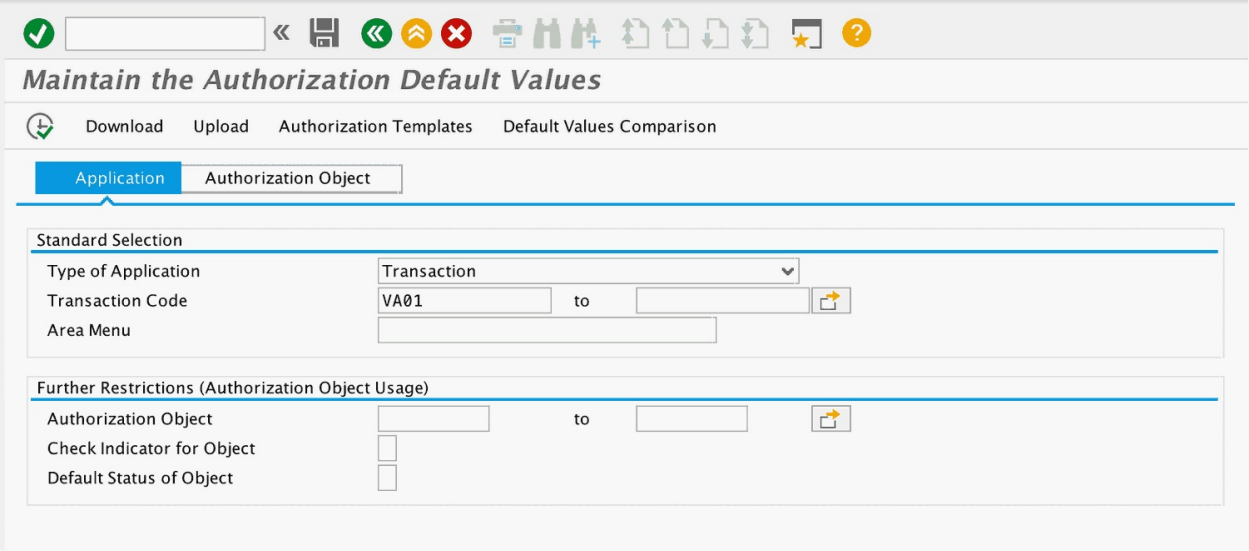


*Figure 5.9: Transaction SU24 landing page 3. All the authorization objects tied to that transaction code will be listed (see Figure 5.10). The **PROPOSAL STATUS** indicates whether or not the authorization is automatically brought into the role when the transaction is added to the role’s menu. Highlight the authorization object you desire to manipulate, in this case, V_VBAK_AAT and click the **GLASSES AND PENCIL** button to switch the page from display to change mode (see Figure 5.11).*

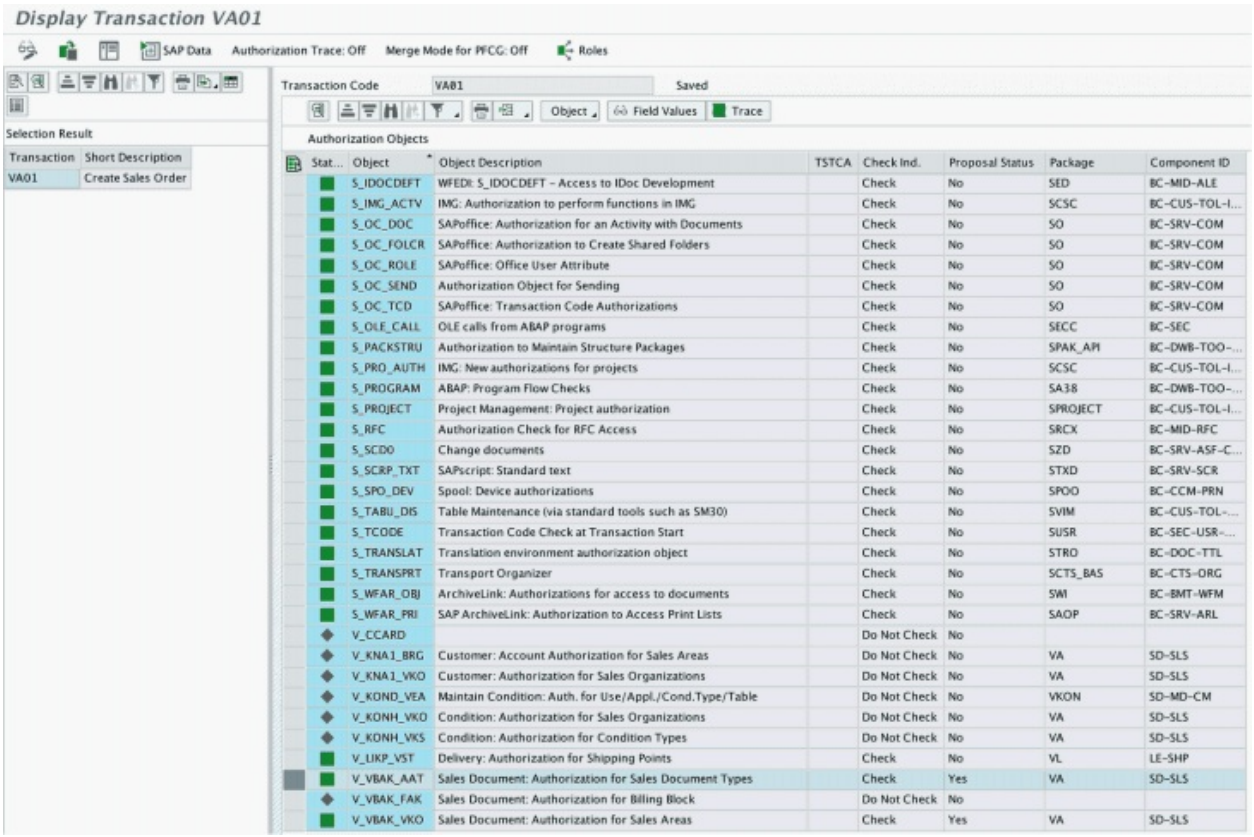


Figure 5.10: Display authorization objects associated 4. Once in change mode, you can click the ***CHANGE FIELD VALUES*** *button to manipulate the automatic assignments from V_VBAK_AAT. You can also change the proposal indicator for authorization objects, among other things.*

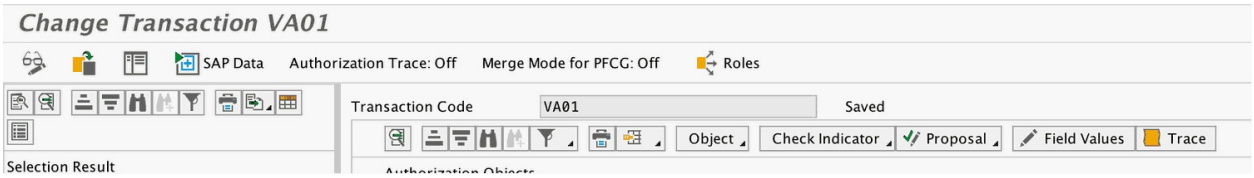


Figure 5.11: SU24 change mode 5. Change the default authorization values as desired and click the ***SAVE*** *button (see Figure 5.12).*

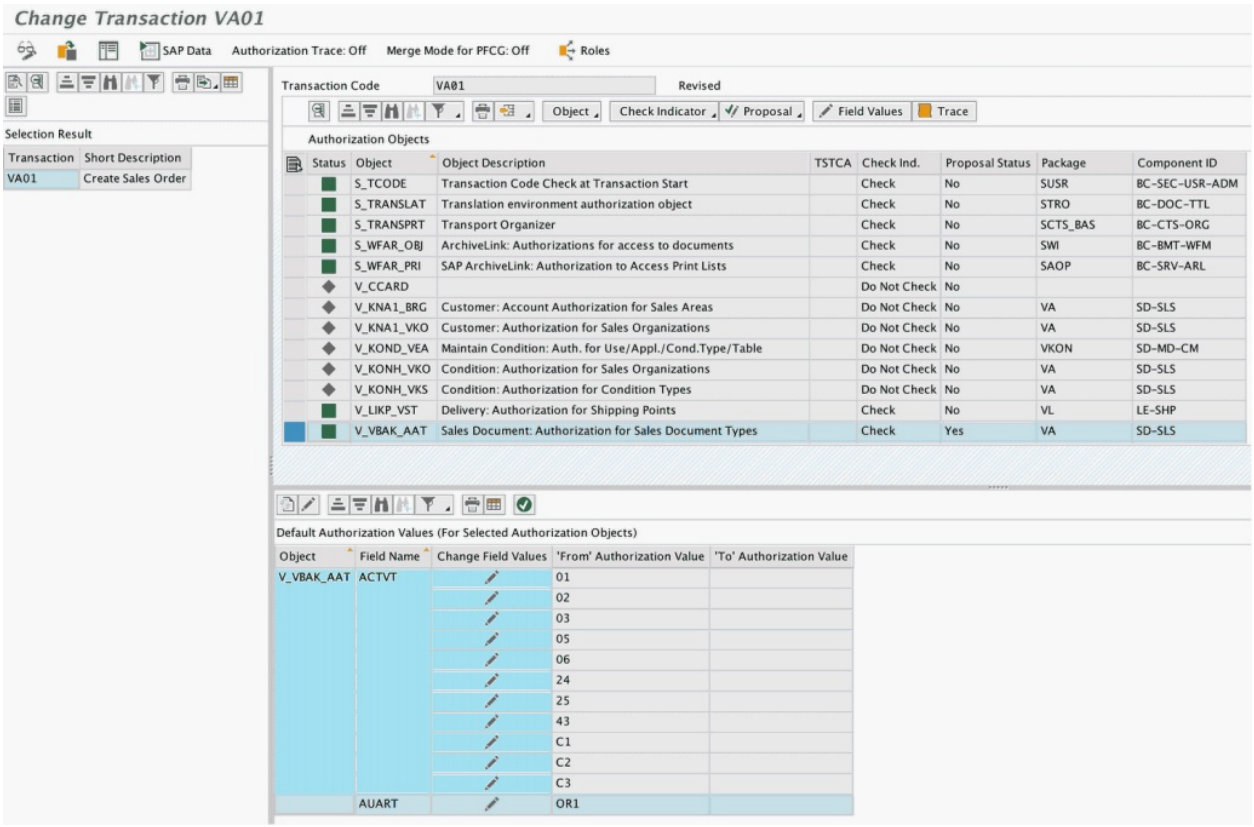


Figure 5.12: Authorization object V_VBAK_AAT with changes made to include default value OR1 for sales document type

5.5 User information system (SUIM)

The user information system, transaction SUIM, is another useful tool for reporting on user and authorization information based on a variety of criteria. SUIM is arranged in the manner of a reporting tree.

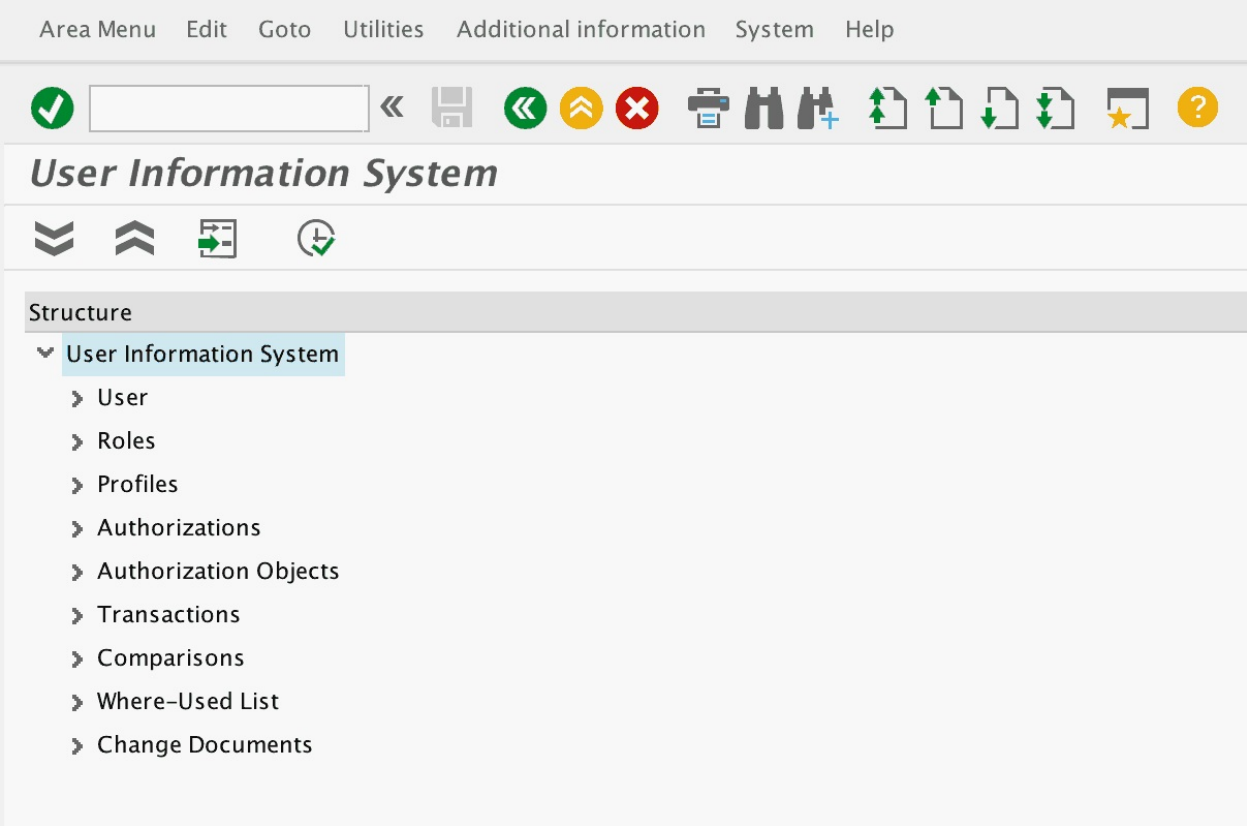


Figure 5.13: SUIM landing page Transaction SUIM, as seen in Figure 5.13, allows for reporting based on users, roles, and profiles. In addition, more detailed reports exist on the basis of transactions and change documents. Comparisons can also be made to roles and users across systems (see Figure 5.14).

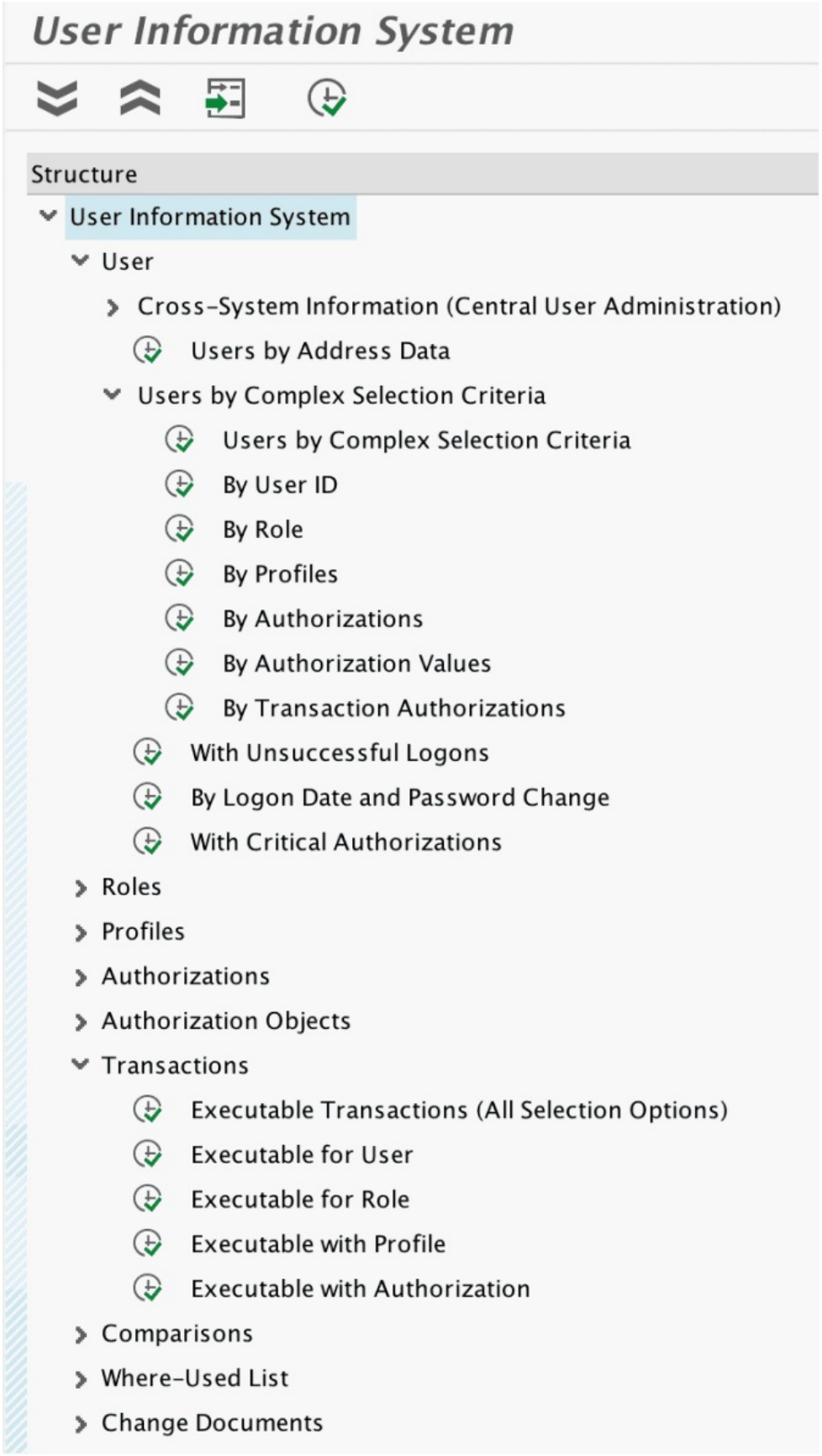

User Information System
Structure
User Information System
User
Cross-System Information (Central User Administration)
Users by Address Data
Users by Complex Selection Criteria
Users by Complex Selection Criteria
By User ID
By Role
By Profiles
By Authorizations
By Authorization Values
By Transaction Authorizations
With Unsuccessful Logons
By Logon Date and Password Change
With Critical Authorizations
Roles
Profiles
Authorizations
Authorization Objects
Transactions
Executable Transactions (All Selection Options)
Executable for User
Executable for Role
Executable with Profile
Executable with Authorization
Comparisons
Where-Used List
Change Documents

Figure 5.14: SUIM reporting tree

When using SUIM

When choosing which SUIM report to select, start with the idea “if this, then this.” For example, if you have a user’s SAP ID, then you want to know what roles are assigned to them or possibly what transactions the user can execute.

6 Advanced topics for SAP authorizations

This chapter covers advanced topics for SAP Security. It provides an overview of the security steps required when upgrading to a new release and introduces GRC Access Control. Finally, it gives a review the entire SAP authorization concept and ties everything together.

6.1 Upgrading to a new release (SU25)

At a given point in time, a service pack upgrade may be required as part of a larger SAP project. In conjunction with this upgrade, new applications may be introduced to the environment or SAP may have re-written code for existing SAP applications. Therefore, additional changes may be introduced within the code in the form of new security and authorization checks. These additions or changes must be accounted for within the existing SAP Security roles. SAP provides a tool, in the form of transaction SU25, for the purpose of managing an SAP Security upgrade. In order to complete the upgrade activities, steps 2A-2D must be completed (see Figure 6.1).

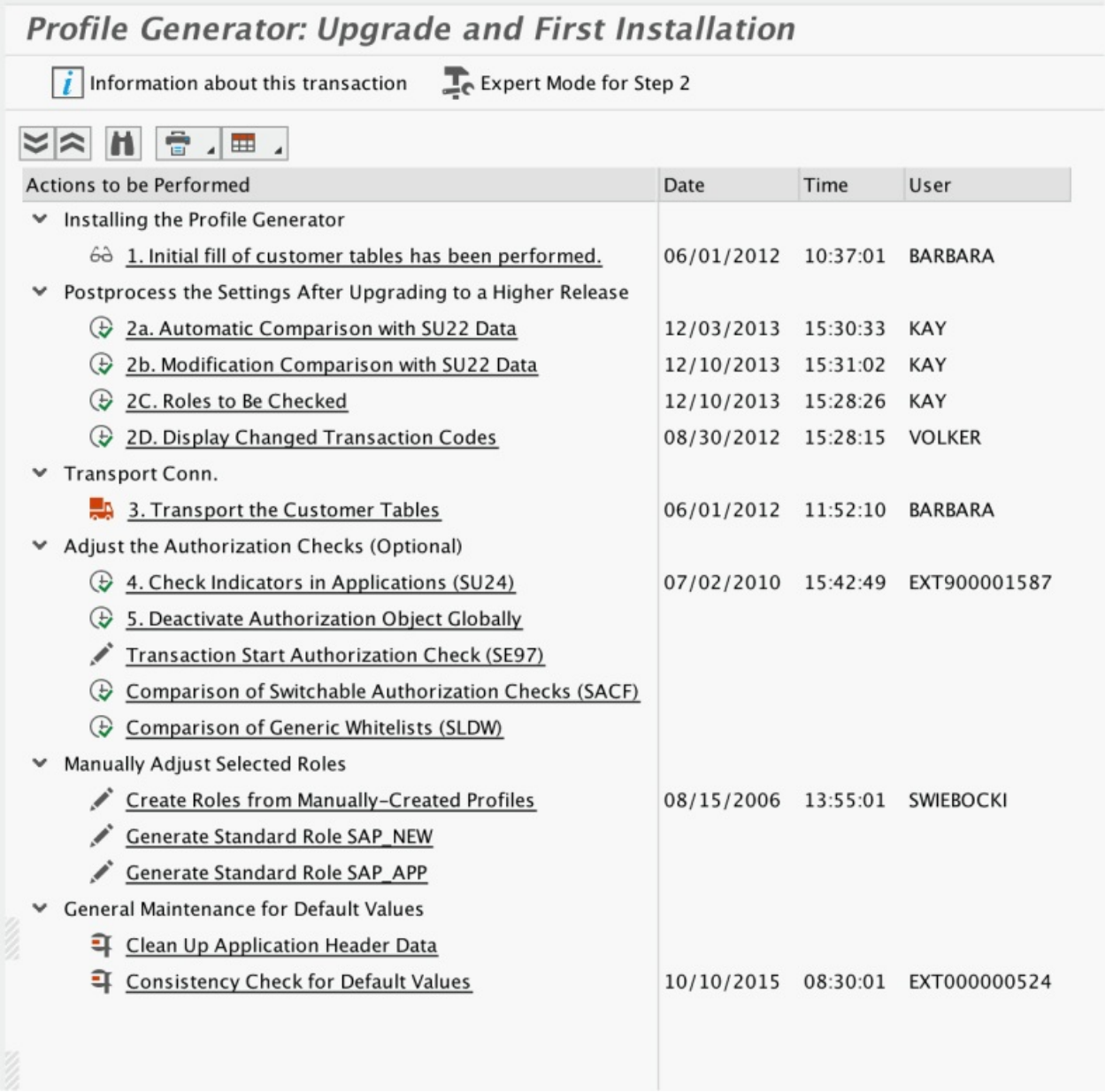


Figure 6.1: Home screen of transaction SU25

The following is a brief synopsis of the four SAP Security tasks, steps 2A-2D, to be completed in order:

- **Step 2A: Automatic Comparison with SU22 Data**
  Compares any authorization data manually maintained by the customer with values proposed by SAP.
- **Step 2B: Modification Comparison with SU22 Data**
  Information returned by step 2A is manually compared. One by one,

the customer reviews any conflict between the SAP proposed values and those manually modified in the past. One can choose to accept the proposed values or keep those that have been manually modified.

- **Step 2C: Roles to Be Checked**
  Roles affected by the upgrade are identified. These roles have transactions in their menu in which changes have been made to the proposed authorization values in SU24.
- **Step 2D: Display Changed Transaction Codes**
  This step is optional. It displays any new SAP transactions that have been introduced in place of those existing and the list of roles affected.

The final mandatory step in the SU25 upgrade process is to run Step 3: Transport the Customer Tables. The transport of the tables should be followed by a transport for all the roles that were modified and generated as part of Step 2C.

6.2 Introduction to GRC Access Control

SAP Governance Risk and Compliance (GRC) is part of SAP's analytics offerings. The use of such analytical tools can influence business outcomes by the changes an organization makes when using intelligent data. Figure 6.2 is the entire suite of SAP solutions for governance, risk, and compliance.

Figure 6.2: SAP solutions for governance, risk, and compliance

SAP GRC solutions provide a platform for organizations to gain visibility into all their risk and compliance activities, but furthermore, to more effectively and efficiently manage them. *GRC Access Control* is the primary solution to identify and mitigate access risks with real-time insight into segregation of duties (SoD) violations and critical access. GRC Access Control also provides the tools necessary for preventative user provisioning, through identification of conflicts prior to granting access. The GRC Access Control solution is comprised of four primary modules:

- Access risk analysis
- Emergency access management
- User access review
- Business role management

The solution enables organizations to achieve greater efficiency, agility, and effectiveness as it relates to governance, risk, and compliance.

- *GRC efficiency* provides savings in human and financial capital resources by reducing operating costs and automating processes.

- *GRC agility* is when an organization can respond rapidly to a change in the internal or external risk and control environments.
- *GRC effectiveness* is achieved when organizations have greater reliability of the information provided to internal and external auditors and when the organization is operating within the controls set forth.

6.2.1 Access risk analysis (ARA)

Access risk analysis (ARA) is the tool that automates the monitoring of segregation of duties (SoD), and critical access risks within SAP and non-SAP systems. ARA can leverage SAP's standard rule set or custom rule set(s) for identification of these conflicts. Key features include:

- Comprehensive and predefined SoD risk-rule set
- Ability to simulate changes to users and roles for the purpose of preventative action
- Real-time reporting

6.2.2 Emergency access management (EAM)

Emergency access management (EAM) provides the means to centrally manage the emergency and elevated access across SAP and non-SAP environments. Key features include:

- Reviewing user and role transaction usage upon completion of firefighter activities
- Notification upon use of critical or sensitive access

6.2.3 Access request management (ARM)

Access request management (ARM) automates the user access provisioning process by utilizing built-in workflow and approval functionality. ARM also automates the process of reviewing user access and SoD conflicts on a periodic basis. Key features include:

- Self-service access request and approval process using predefined workflows and e-mail-based notification templates
- Embedded risk analysis for preventative remediation of access risks and application of mitigating controls
- Integration with IdM (identity management) solutions
- Periodic review of role assignments to users, role content assignments, and mitigating control assignments

6.2.4 Business role management (BRM)

Business role management (BRM) is the tool that centralizes the creation and maintenance of user roles and automates the workflow process for role deployment. Key features include:

- Workflow-driven methodology for role definition and maintenance
- Definition of roles using business terms and alignment with business processes

GRC Access Control has also deployed a new role management concept to replace composite roles, called GRC *business roles*. Business roles work similarly to composite roles in that they are a grouping of many roles in a single entity, but business roles can contain roles across various SAP and non-SAP systems.

6.3 Wrap up: Putting a bow on it

User master records are created to house all applicable user information, including vital address data, logon credentials, password information, assigned roles, and profiles. When a user logs into the system, his or her authorizations are temporarily stored in memory, also known as the user buffer. When users try to execute a transaction code or complete a task in the system, they either have the authorization or not, which is based on the roles and profiles assigned to them in their user master records.

Roles contain authorizations and when generated, profiles are created.

Roles are designed in the profile generator transaction and the three most common role types are single, composite, and derived. If a user has authorization to complete a task in the system, all authorization checks the system performed are successful and the authorization objects and required field values are contained in one or more of the user's roles/profiles. If a user does not have authorization to complete a task, trouble-shooting techniques can be deployed, such as through SU53 or running a trace.

Ultimately, SAP has built-in functionality to meet the ever-growing needs to protect application data and reduce risk exposure in the system. When designing SAP Security roles, it is important to consider the rule of least privilege and alignment with business processes in conjunction with scalability and ease of maintenance.

7 Acknowledgements

I would like to express my sincere gratitude to the many people who saw me through this endeavor; to all those who provided support, talked things over, and offered comments. I would also like to thank Espresso Tutorials for enabling me to publish this book and especially Alice Adams, my editor, who encouraged me and pushed me throughout the duration of the journey.

Thanks to my two consulting families, both at IBM and itelligence. I became a consultant because I love working with people from all walks of life, because I bore easily, and because I love being a part of a team. None of this would be possible without any of you. And, of course, thank you to my clients who have made my career more exciting and rewarding than I ever thought possible.

Last and certainly not least, thanks to my family who I have confided in over the past 5 years – through first jobs, new positions, and challenging clients; you are simply the greatest. To my mom, who is the best mentor I could ask for – I promise to dedicate my first memoir to you, which is most likely never going to happen. And special thanks to my husband Josh, who is always supportive, always honest, and who always makes me feel better after a series of 80-hour weeks on the road when the end is still not in sight.

Thank you.

You have finished the book.

Sign up for our newsletter!

Want to learn more about new e-books?

Get exclusive free downloads and SAP tips.

Sign up for our newsletter!

Please visit us at newsletter.espresso-tutorials.com to find out more.

A About the author

Tracy Juran (Levine), CPIM, is a Managing Consultant at IBM as part of the Security Services Risk and Compliance practice. She has extensive experience in SAP Security and Authorizations; SAP Governance, Risk, and Compliance (GRC); and core cross-functional business processes. Tracy is a die-hard Ohio State Buckeyes fan and loves to plan parties with friends and travel the world; her favorite destinations include Thailand, Peru, and Israel. She resides in Cincinnati, Ohio with her husband, Josh, their dog, Markley, and cat, Misha. For more information please visit Tracy-Levine.com.

B Disclaimer

This publication contains references to the products of SAP SE.

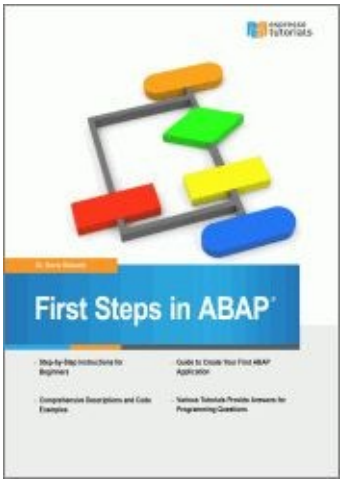
SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase, Inc. Sybase is an SAP company.

SAP SE is neither the author nor the publisher of this publication and is not responsible for its content. SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

More Espresso Tutorials eBooks



Boris Rubarth:
First Steps in ABAP®

- Step-by-Step instructions for beginners
- Comprehensive descriptions and code examples
- A guide to create your first ABAP application
- Tutorials that provide answers to the most commonly asked programming questions

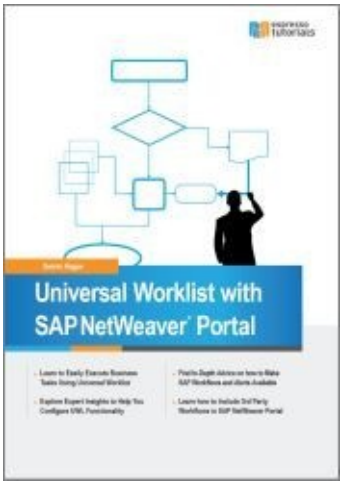
Sydnie McConnell, Martin Munzel:
First Steps in SAP®,2nd edition

- Learn how to navigate in SAP ERP
- Learn SAP basics including transactions, organizational units, and master data
- Watch instructional videos with simple, step-by-step examples
- Get an overview of SAP products and new development trends

Antje Kunz:
SAP® Legacy System Migration Workbench (LSMW)

- Data Migration (No Programming Required)
- SAP LSMW Explained in Depth

- Detailed Practical Examples
- Tips and Tricks for a Successful Data Migration



Darren Hague:
Universal Worklist with SAP® NetWeaver Portal

- Learn to Easily Execute Business Tasks Using Universal Worklist
- Explore Expert Insights to Help You Configure UWL Functionality
- Find In-Depth Advice on how to Make SAP Workflows and Alerts Available
- Learn how to Include 3rd Party Workflows in SAP NetWeaver Portal

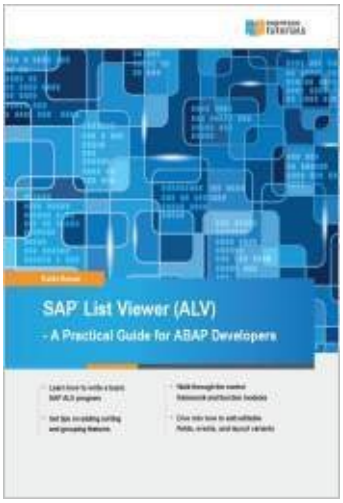
Michał Krawczyk:
SAP® SOA Integration—Enterprise Service Monitoring

- Tools for Monitoring SOA Scenarios
- Forward Error Handling (FEH) and Error Conflict Handler (ECH)
- Configuration Tips
- SAP Application Interface Framework (AIF) Customization Best Practices

- Detailed Message Monitoring and Reprocessing Examples

Ann Cacciottolli:
First Steps in SAP® Financial Accounting (FI)

- Overview of key SAP Financials functionality and SAP ERP integration
- Step-by-step guide to entering transactions
- SAP Financials reporting capabilities
- Hands-on instruction based on examples and screenshots

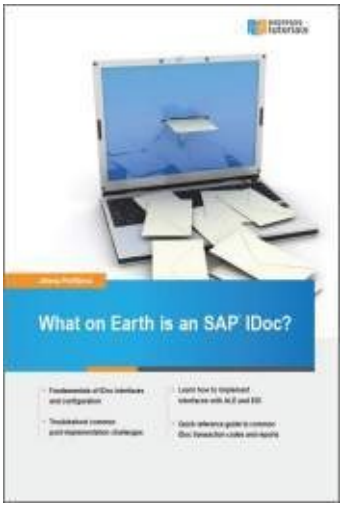


Kathi Kones:
SAP List Viewer (ALV) – A Practical Guide for ABAP Developers

- Learn how to write a basic SAP ALV program
- Walk through the object-oriented control framework and function modules
- Get tips on adding sorting and grouping features
- Dive into how to add editable fields, events, and layout variants

Jelena Perfiljeva:
What on Earth is an SAP IDoc?

- Fundamentals of inbound and outbound IDoc interfaces and configuration
- Learn how to implement interfaces with ALE and EDI
- Troubleshoot common post-implementation challenges



- Quick reference guide to common IDoc transaction codes and reports