

SAP Authorizations Handbook

SAP Security Beginner's Guide

ERP  **ecurity Training**

Title: SAP Authorizations Handbook,
SAP Security Beginner's Guide

© erpsecurity.training, 2020

All rights are reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of the author.

www.erpsecurity.training

Content

1. Introduction to SAP authorization concept	7
1.1. Security principles.....	7
1.2. Authorization structure	8
2. User Maintenance (SU01)	12
2.1. Access control	12
2.2. User types	13
2.3. User login	14
2.3.1. Errors during login.....	15
2.3.2. Login parameters	16
2.3.3. Forbidden passwords	17
2.4. User creation and maintenance.....	17
2.5. User master setting.....	28
2.6. Change documents	28
2.7. Mass user maintenance (SU10).....	30
3. Role Maintenance (PFCG)	34
3.1. Create and modify roles	34
3.1.1. Subtleties of role maintenance	44
3.1.2. Default values (SU24)	46
3.1.3. Expert mode	50
3.1.4. Mass role maintenance (PFCGMASVAL).....	51
3.2. Special roles	53
3.2.1. Composite roles	54
3.2.2. Derived roles.....	55
3.2.3. Customizing roles.....	60
4. Tools for authorization analysis	67
4.1. Authorization error analysis (SU53)	67
4.2. System Trace (ST01 or STAUTHTRACE)	70
4.3. Load monitor (ST03N)	75
4.4. Audit log (SM20 or RSAU_READ_LOG)	76
5. User information system (SUIM)	80
6. Special authorization profiles.....	82
6.1. SAP_ALL authorization profile.....	82
6.2. SAP_NEW authorization profile	82
6.3. SAP_APP authorization profile.....	83
6.4. Other profiles.....	83
7. Relevant tables.....	84
7.1. User tables.....	84
7.2. Roles and authorization tables.....	85

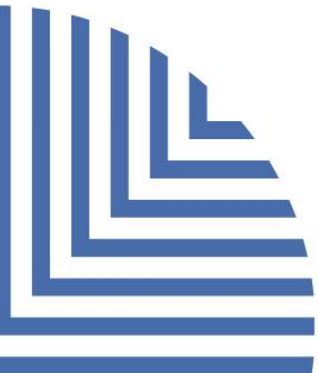
SAP SECURITY

FROM SCRATCH

Powered by


Acquire the skills and knowledge necessary to design, implement, and manage robust security solutions for SAP systems. Whether you are new to SAP security or seeking to enhance your expertise, this course will empower you with the tools and techniques needed to safeguard your organization's SAP environment effectively.

REGISTER NOW



1. Introduction to SAP authorization concept

The SAP authorization concept protects SAP systems against unauthorized access to **transactions**, programs, and services. Based on a set of security principles and the concept of authorizations, administrators assign to users the permissions that determine what actions they can perform in the system, after they have logged in to the system and have authenticated.

1.1. Security principles

In general terms, information security is defined as the set of preventive, corrective and detective measures to protect the confidentiality, integrity and availability of information in a system. The objectives to be achieved from the point of view of the security of SAP systems are:

- **Availability:** Availability ensures that users can access to their resources whenever they need them. When determining the requirements regarding the availability of resources, costs resulting from unplanned downtime, lost customers, costs of unproductive employees and overtime should be considered. Some damages cannot be fully quantified in terms of money, for example loss of reputation.
- **Authentication:** Authentication determines the actual identity of the user. The following authentication mechanisms can be used in a system environment:
 - User ID and password authentication.
 - Smart card authentication.
 - Smart card and PIN authentication.
- **Authorization:** Authorization defines the rights and privileges of the identified user. It also determines the functions that a user can access. The application must be programmed to verify whether a user is authorized or not, before the user accesses a particular function.
- **Confidentiality:** Confidentiality ensures that user history and communication are kept confidential. Information and services must be protected from unauthorized access. Authorizations to read, change or add information or services must be explicitly granted only to a few users and must be denied to all other users.
- **Integrity:** Integrity guarantees that the user information that has been transmitted or stored has not been modified. Programs and services

must run successfully and provide accurate information. As a result, people, programs, or hardware components must not modify programs and services.

- **Non-repudiation:** In the context of information security, repudiation is the denial of an act, while non-repudiation ensures that people cannot deny their actions.
- **Segregation of duties:** Segregation of duties defines and implements an effective separation of the functions and responsibilities of the organizations personnel to avoid conflicts of interest and minimize the risks of information security derived from the accumulation of privileges and knowledge in people.

1.2. Authorization structure

To access business elements (orders, invoices, financial reports, etc.) or execute SAP transactions, a user requires the corresponding authorizations, as business elements and transactions are protected with **authorization objects**. Authorizations represent generic authorization object **instances** and are defined based on the activity and responsibilities of the employee.

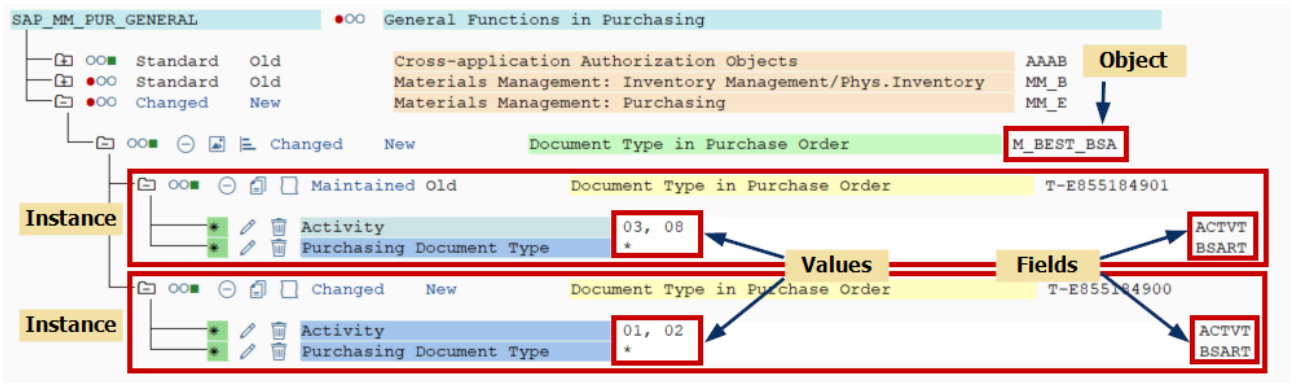


Figure 1.1. Authorization object instances.

Authorizations are combined into an **authorization profile**, which is associated to a **role**. User administrators assign the corresponding roles using the **user master** so that users can use the appropriate transactions for their tasks.

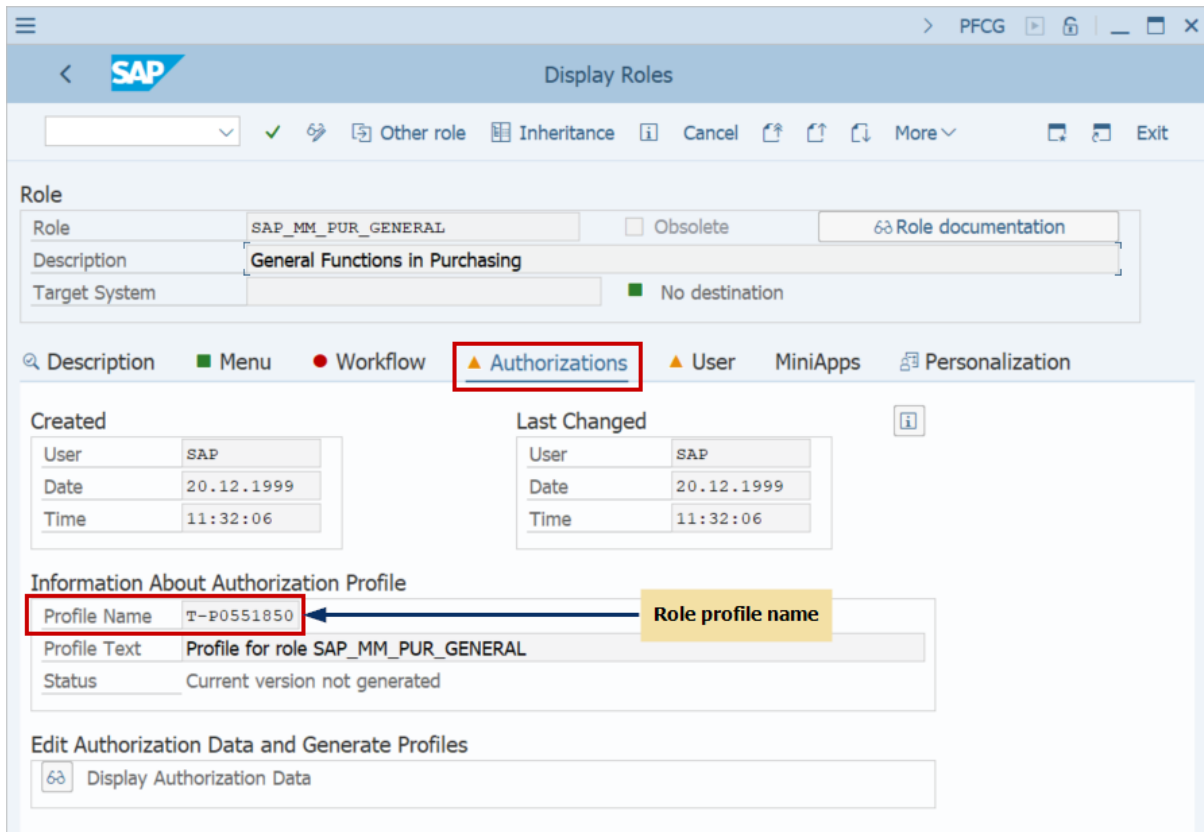


Figure 1.2. Authorization profile associated to the role.

To ensure that a user has the appropriate authorizations when they perform an action, the system performs **authorization checks**.

The following actions are subject to authorization checks that are performed **before** the start of a program or table maintenance, and SAP applications cannot avoid nor disable:

- Start SAP transactions (authorization object S_TCODE)
- Start programs (authorization object S_PROGRAM)
- Call RFC function modules (authorization object S_RFC)
- Maintain tables with generic tools (authorization object S_TABU_DIS or S_TABU_NAM)

A **transaction** is a code consisting of letters, numbers, or both. Transactions are used to run a specific SAP program. Users can directly enter the transaction code in the toolbar command field, or find it in the SAP menu.

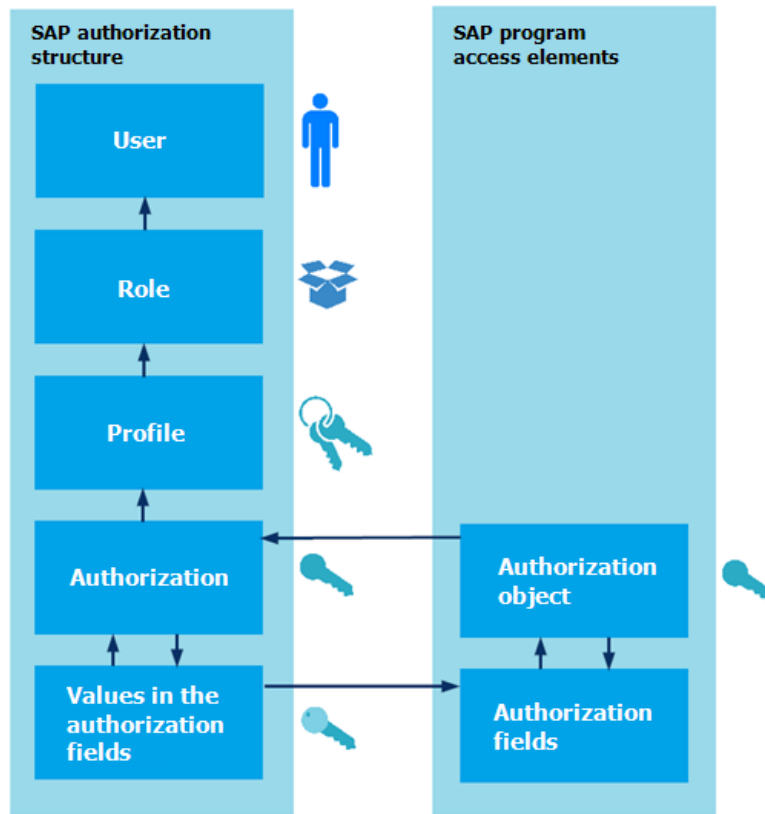


Figure 1.3. Authorization check diagram.

Authorizations allow to use certain functions within the SAP systems. Each authorization is related to an **authorization object** and defines a value or values for each **authorization field** contained in the authorization object. Authorizations are grouped into **authorization profiles** that are included in the user master record.

Authorization objects have authorization **fields**, which represent the **values** that will be validated during authorization checks. In addition, there is a special type of field, known as **organizational level**, which is associated with certain organizational areas of the structure of a company, such as, Company Code, Plant, Sales Organization, etc. Organizational levels have the particularity that they are maintained differently from fields that are not organizational level (see Chapter 3, Section 3.1.1).

Authorization profiles are the elements that group authorizations, which are identified by the name of an authorization object, the names of the authorization fields and the values that each field contains.

The way in which authorization profiles are assigned to users is generally through the roles that contain those profiles. There are also certain profiles

that can be granted directly, without the need to assign an associated role (see Chapter 6).

The set of authorization profiles assigned to a user, and therefore the set of authorizations assigned to the user, make up the user's **authorization buffer**.

2. User Maintenance (SU01)

In order for a user to be able to access SAP and be able to work within the system, they must have a registered ID, with authorization to access, that is, they must have a **user master record**. The assignment of these authorizations can be managed individually, but also, to a certain extent, massively. The individual management of the user master is carried out through **transaction SU01**.

2.1. Access control

Each user must have a unique ID (user master record) to access the system, in order to guarantee the principle of non-repudiation. Likewise, all IDs must have a password to access the system.

When creating a **dialog user**, the system requires an initial password to be assigned to it. The password must meet all the internal requirements established (parameterized) in the system, such as, for example, that it is not a trivial password, or that it has a minimum length. When the new user signs in for the first time, they must specify a new password. The following table shows the password requirements and if they are determined by the system or if they are parameterized:

Password requirements	Type
Minimum length: 3 characters	It can be defined by the Administrator. It can (must) be increased.
Expiration	It can be defined by the Administrator. The number of days after which a password must be changed when set.
The password cannot be a value that is contained in a reserved list	It can be defined by the Administrator. Rule: only passwords PASS and SAP * are excluded from the application.
The first character cannot be "!" or "?"	Established by SAP.
The first 3 characters do not have to appear in the same sequence as in the "user ID".	Established by SAP.
The first 3 characters cannot be identical	Established by SAP.
The space character is not allowed within the first 3 characters	Established by SAP.
The password cannot be PASS or SAP *	Established by SAP.
Any character that can be typed from the keyboard is allowed in a password.	Established by SAP.
The last 5 passwords cannot be repeated.	Established by SAP.

A user cannot change their password more than once per day. This restriction does not apply to administrator users. Established by SAP.

Table 2.1. Password requirements.

2.2. User types

The following are the different types of users that can be created within an SAP system depending on their purpose:

Dialog (A): User type for exactly one person who interacts with the system.

- During a dialog login, the system checks if the password is initial or if it has expired. Dialog users can change their passwords themselves.
- Multiple simultaneous sessions can be avoided.

System (B): Type of user suitable for background processing and communication within the same system (internal RFCs).

- It is not possible to initiate dialogue sessions with these types of users.
- The system does not check if the password is initial or if it has expired.
- Only administrators can change the password.
- Multiple sessions are allowed.

Communication (C): User type suitable for communication between systems, such as RFC users for ALE, Workflow or TMS.

- It is not possible to initiate dialogue sessions with these types of users.
- The system does not verify if the password is initial, but in this case the password expiration policies do apply. In either case, whether the system requests the password change will depend on whether the login mechanism is interactive (DIAG) or non-interactive (RFC or HTTP).

Service (S): User type suitable for anonymous multi-person access. Very restricted authorizations must be assigned to these types of users.

- During login, the system does not check if the password is initial or if it has expired. Only administrator users can change the password.
- Multiple sessions are allowed.

Reference (L): Similar to the Service user, this type of user is not associated with a person. With a reference user it is not possible to access the system, but it is used for additional assignment of authorizations. Reference users are used for the purpose of providing users with identical authorizations.

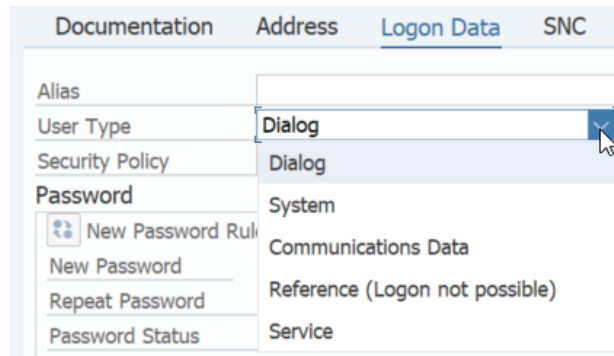


Figure 2.1. User type list.

2.3. User login

To access the system, the user must first identify himself with a user ID and password, since it is not possible to have an empty password.

Before allowing access, the system verifies:

- If the user is locked, either due to too many failed access attempts, or because the administrator wants to prevent access to users while maintenance tasks are carried out.
- If the password entered is valid. If it is the first time that the user accesses, they must enter a new password before accessing, in which case the system will request to be entered twice. In the system parameters it is possible to set for how long the initial passwords are valid.

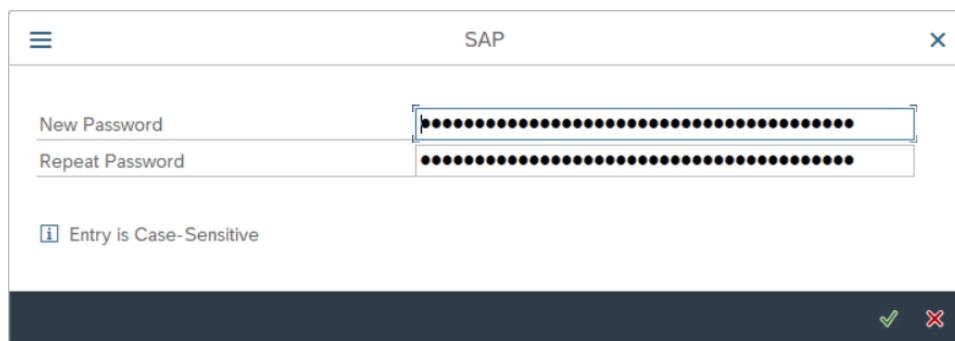


Figure 2.2. New password confirmation window.

- If the current date is between the start and end validity dates, both inclusive.

If the user ID and password are correct, the system displays the date and time of the user's last access. With this data users can verify that no one else has accessed with their ID. The date and time of the login cannot be modified

in a standard SAP environment, however the system does not save the date and time of the moment the last session was closed.

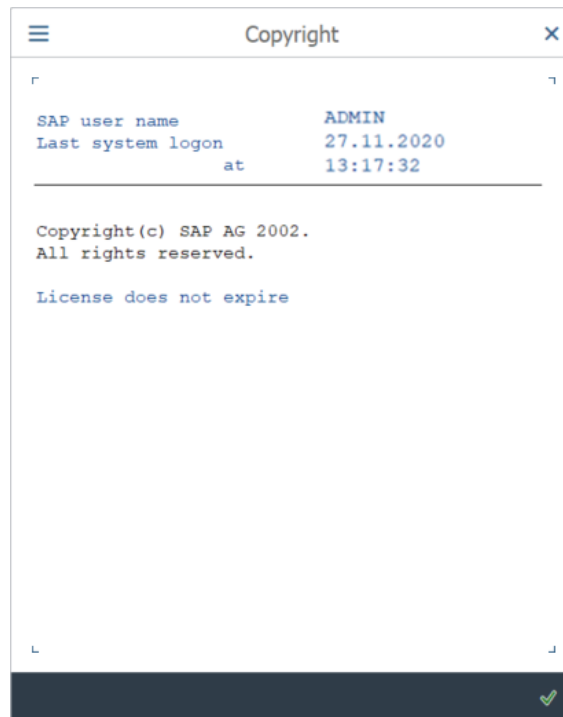


Figure 2.3. Last system logon message.

2.3.1. Errors during login

If a user did not use a valid ID, the system allows them to continue trying until they log in with a valid ID.

If a user enters an incorrect password, then the system allows four additional attempts before locking the user ID. The maximum number of failed attempts allowed is 5 by default, although this value can be modified with the system parameter `login/fails_to_user_lock`.

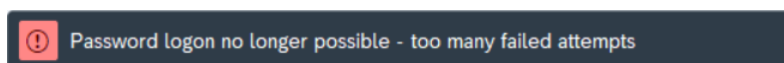


Figure 2.4. Too many failed attempts error message.

An ID that has been blocked due to failed attempts will be automatically unlocked at midnight of the day it was blocked if the `login/failed_user_auto_unlock` parameter has value 1. By default, this parameter has the value 0. The administrator can unlock users locked by too many failed attempts at any time.

An ID that has been locked by the administrator will not be able to access the system.

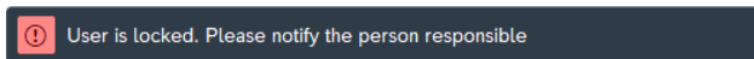


Figure 2.5. Admin lock error message.

An ID that has an expiration date earlier than the current date will not be able to access the system. This value can be maintained from transaction SU01, in the Logon Data tab.



Figure 2.6. User account not in validity date error message.

2.3.2. Login parameters

One way to control user passwords is through system parameters:

Parameter	Description
login/disable_multi_gui_login	Deactivation of multiple dialog logons
login/disable_password_logon	Controls the deactivation of password-based logon
login/failed_user_auto_unlock	Defines whether user locks due to unsuccessful logon attempts are automatically removed at midnight
login/fails_to_session_end	Defines the number of unsuccessful logon attempts before the system does not allow any more logon attempts
login/fails_to_user_lock	Defines the number of unsuccessful logon attempts before the system locks the user
login/min_password_diff	Defines the minimum number of characters that must be different in the new password compared to the old password
login/min_password_digits	Defines the minimum number of digits (0-9) in passwords
login/min_password_letters	Defines the minimum number of letters (A-Z) in passwords
login/min_password_lng	Defines the minimum length of the password
login/min_password_lowercase	Specifies how many characters in lowercase letters a password must contain
login/min_password_specials	Defines the minimum number of special characters in the password
login/min_password_uppercase	Specifies how many characters in uppercase letters a password must contain
login/multi_login_users	List of users, who are permitted to log on to the system more than once
login/password_expiration_time	Defines the validity period of passwords in days.
login/password_history_size	Specifies the number of passwords (chosen by the user, not the administrator) that the system stores and that the user is not permitted to use again
login/password_logon_usergroup	Controls the deactivation of password-based logon for user groups
login/password_max_idle_initial	Specifies the maximum period for which an unused initial password (a password set by the user administrator) remains valid
login/password_max_idle_productive	Specifies the maximum period for which an unused productive password (a password set by the user) remains valid

login/system_client	Specifies the default client that the system automatically enters on the logon screen
---------------------	---

Table 2.2. Login parameters.

2.3.3. Forbidden passwords

In addition to the system parameters, it is also possible to control user passwords using the illegal password table USR40, which is maintained through transaction SM30. Entries in this table can be created generically using the following two characters:

- "?" for a single character.
- "*" for any character string.

For instance:

- When entering "123 *" in the USR40 table, passwords cannot start with the character string "123".
- When entering "*ABC*", passwords cannot contain the string "ABC" in any position.

Additionally, there are a series of predefined rules for passwords, which cannot be deactivated.:

- They must contain at least 6 characters (by default).
- They should not start with "?" or "!".
- They cannot be "pass".
- The new password must be different from the previous one by at least one character.

2.4. User creation and maintenance

A user will be able to log into an SAP system if there is a record in the user master with the corresponding password. The scope of each user's activities in an SAP system is defined within the user master record by one or more roles, and is limited by the assignment of the appropriate authorizations.

Within each SAP system there may be different clients, and the user master is specific to each client.

In order to create and maintain users, it is necessary to have the following authorizations assigned:

- Authorization to create or maintain a user master record and assign a user group to it (object S_USER_GRP).

- Authorization to assign authorization profiles to users (object S_USER_PRO).
- Authorization to create and maintain authorizations (object S_USER_AUTH)
- Authorization to protect roles. With this authorization object, it is possible to specify which roles can be processed and with what type of activity (create, modify, display, etc.) (object S_USER_AGR).
- Authorization to specify which transactions can be added to the role menu and for which execution authorization can be assigned in the Profile Generator (object S_USER_TCD).
- Authorization to restrict the values that an administrator can insert or modify in a role within the Profile Generator (object S_USER_VAL).

The transaction used for user management is SU01:

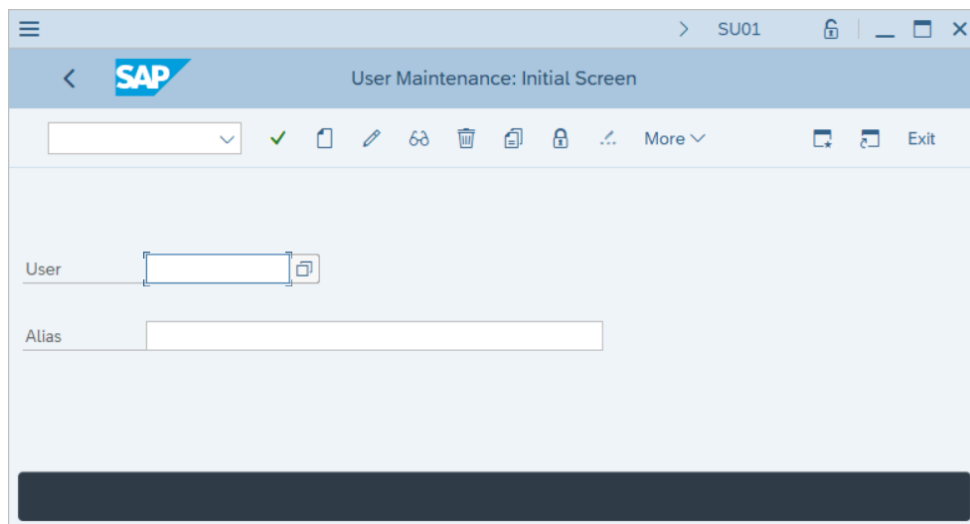








Figure 2.7. Transaction SU01 main screen.

The following options are found in the main window of transaction SU01:

- Create new users, by clicking on the button .
- Modify existing users. Clicking on the button  will open the user record in edit mode.
- In the same way, clicking on the button  will open the user's record in display mode.
- There is also the option of creating new users as a copy of another, for which you have to click on the button .
- Pressing on the button  locks the user, or unlocks it, depending on whether it was previously locked or not.

- By clicking on the button  the system offers the option to change the user's password.

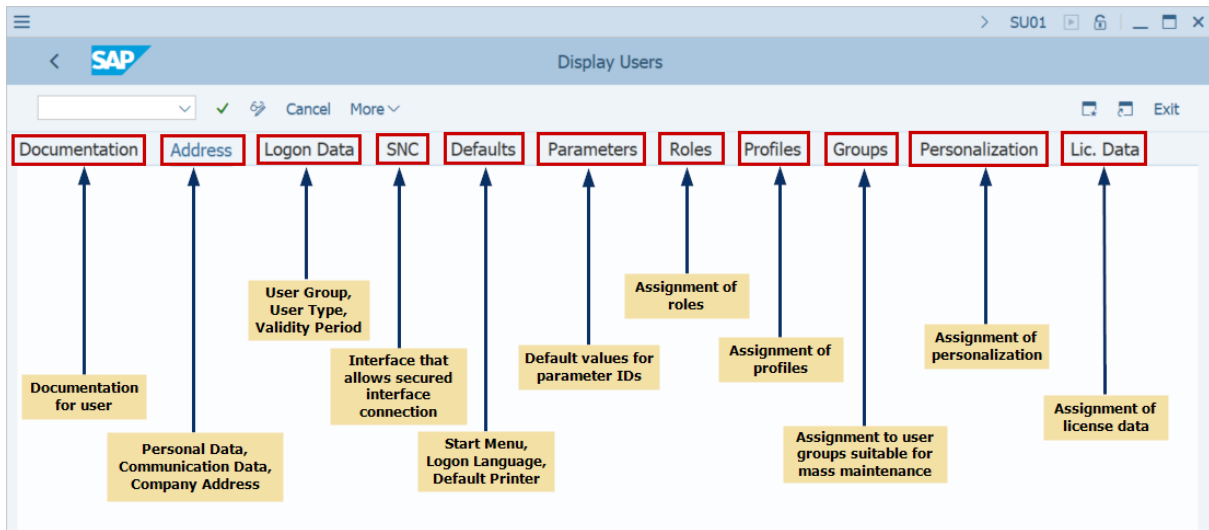


Figure 2.8. Transaction SU01 tabs.

Documentation tab:

The documentation tab can be used to document users.

Short description: This field contains a brief description of the user.

Person Responsible: This field can be used to indicate a user who is technically and effectively responsible for this ID. This can be useful for traceability within the system, especially for anonymous technical users.

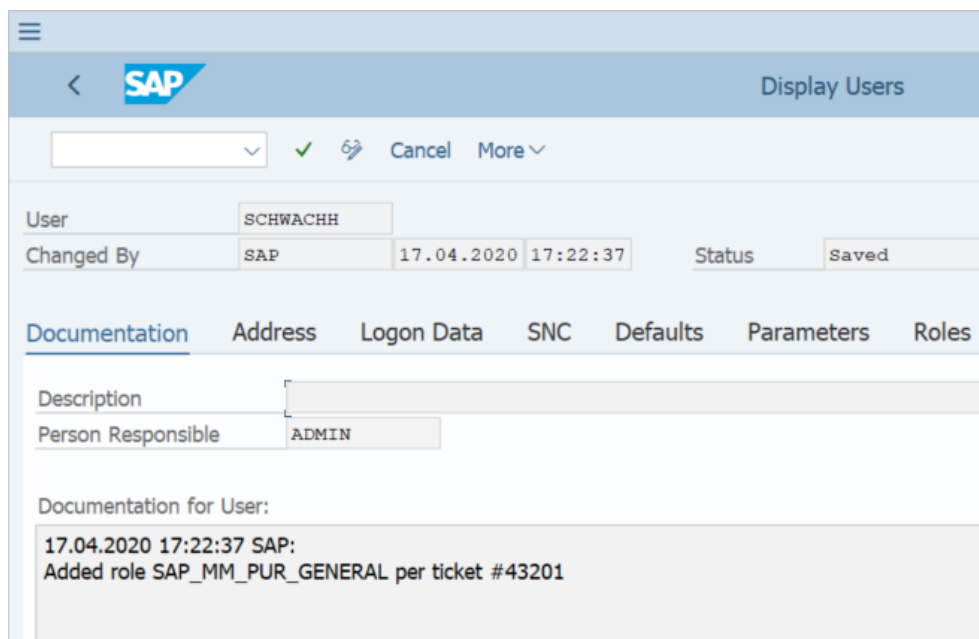


Figure 2.9. Documentation tab.

Documentation: This field contains user documentation. For each entry entered, the date and ID of the user who made the change are automatically recorded. It is only possible to create new entries, and it is not possible to change or delete old entries.

There is the possibility to use the report RSUSR_DELETE_USERDOCU to completely remove the documentation for the selected users. This report is intended to clean up after a client copy, for example. Selective deletion of individual entries is not intended, as it is necessary to ensure a consistent history.

Address tab:

The fields in the address tab are self-explanatory, just keep in mind that to create a user, at least the following information must be specified:

- In the Address tab, it is mandatory to maintain the Last name field.
- In the Logon Data tab, it is mandatory to enter an initial Password, or deactivate it.

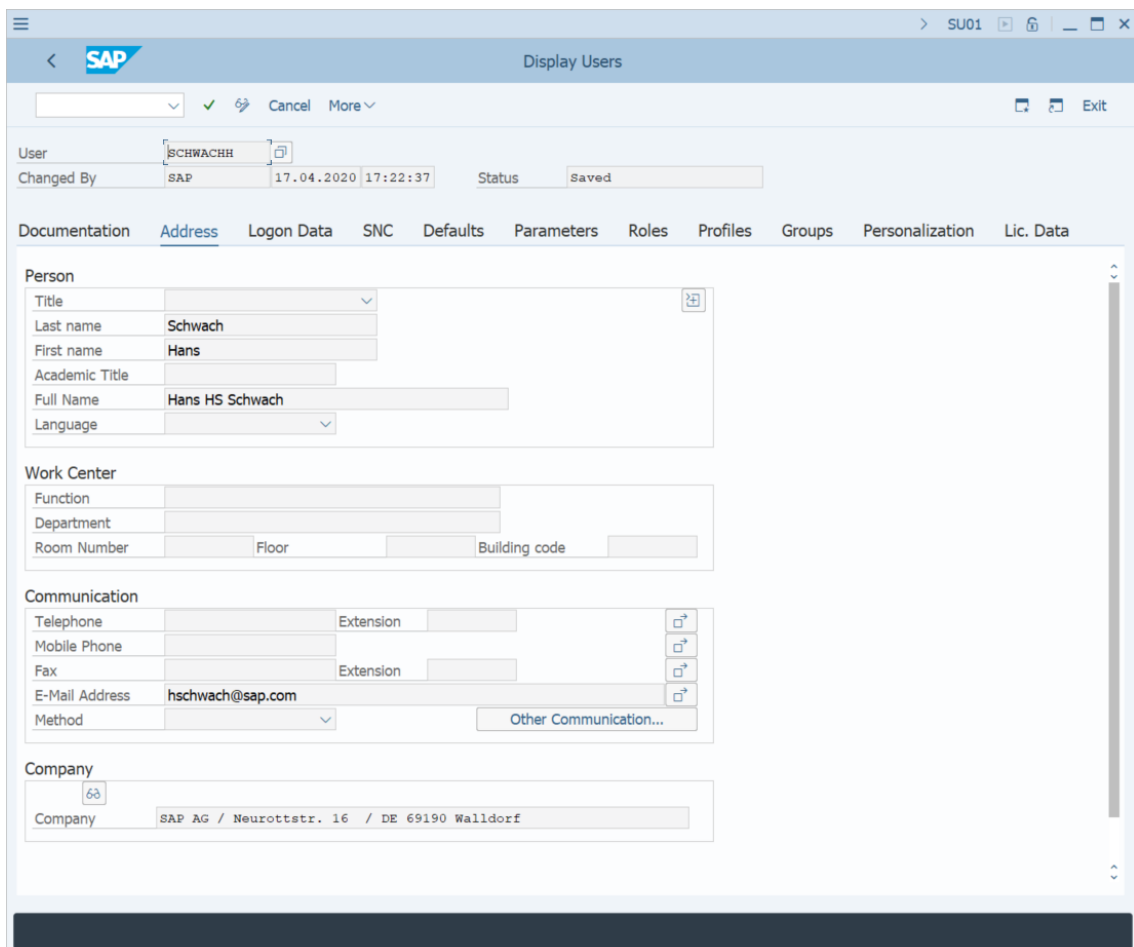


Figure 2.10. Address tab.

Logon Data Tab:

Alias is an alternate ID which can be assigned to users. This means that 40 characters are available to assign longer and more descriptive names to users. Therefore, the user can be identified by the user ID (12 characters) or by the alias. The alias is used primarily when users are created in a self-service scenario from the Internet. In this situation, only the alias is specified and used.

The screenshot shows the SAP SU01 'Display Users' transaction. The user 'SCHWACHH' is selected, and the 'Logon Data' tab is active. The form displays the following information:

- User: SCHWACHH
- Changed By: SAP
- Changed On: 17.04.2020 17:22:37
- Status: Saved
- Alias: (empty field)
- User Type: Dialog
- Security Policy: (empty field)
- Password Status: Production Password
- User Group for Authorization Check: User group ESSUSER, User Group for ESS Users
- Validity Period: Valid from 16.06.2010, Valid To 29.12.2022
- Other Data: Account no. (empty field), Cost center (empty field)

Figure 2.11. Logon Data tab.

Security policy: sometimes users require a security policy for login and passwords different than the default one. For example, users with elevated privileges, such as administrators, should have passwords with a higher level of protection than standard business users. These users should be forced to change their passwords more frequently or have more complex rules for their passwords. However, such requirements, if widely enforced for all users, it can result in increased incidents of users requesting password recovery.

This field can be used to choose a specific security policy for the user, if not, the user uses the standard security policy.

Initial password: To assign initial passwords, you can enter the password manually, generate a random password, or disable the password. Deactivating it would imply that the user could no longer log in with a password, and could only with variants of Single Sign-On (X.509 certificate, logon ticket). Disabling the password can be useful when a password login is not required because it is done exclusively in a different way. In this case, disabling the password would increase security, since passwords that are not used tend to remain initial.

User group for authorization checks: To assign the user to a user group, simply enter the group ID. This is necessary if you want to divide user maintenance among multiple administrators. Only the administrator who has authorization for the group will be able to maintain users from that group. If the field is left empty, the user will not be assigned to any group, which means that any administrator can maintain the user.

User Type: the default value proposed by the system is Dialog (normal dialog user). The other types of users can be assigned when special processing is needed.

Validity period: With these fields it is possible to specify the validity period of the user's master record. In case of not needing to restrict the validity, simply leave the fields empty.

Other data: For each user or group of users, it is possible to assign an accounting number, depending on the business needs. Useful accounting numbers can be for example the user's cost center or company code.

SNC Tab:

SNC (Secure Network Communications) functions allow you to use an external security product to protect communications between SAP system components (for example, between application servers and clients). Encryption can be used in three areas:

- Application level end-to-end security.
- Protection of integrity and privacy in data transfer.
- Secure user authentication.

The screenshot shows the SAP 'Display Users' interface for user 'SCHWACHH'. The 'SNC' tab is selected. The 'SNC Status' section shows a warning icon and the text 'SNC is not active on this application server' and 'Unsecured logon is permitted for specific users'. The 'SNC Data' section shows a text field for 'SNC name' with a search icon, a warning icon and the text 'Canonical name not defined', and a checkbox for 'Allow password logon for SAP GUI (user-specific)' which is currently unchecked. The top navigation bar includes 'Documentation', 'Address', 'Logon Data', 'SNC', 'Defaults', 'Parameters', 'Roles', 'Profiles', 'Groups', 'Personalization', and 'Lic. Data'. The top status bar shows 'User: SCHWACHH', 'Changed By: SAP', '17.04.2020 17:22:37', and 'Status: saved'.

Figure 2.12. SNC tab.

Default Values Tab:

Start menu: An area menu can be specified in this field, which can be chosen using the search help. In this way, the SAP menu will only contain the components of this area menu.

For a user who needs for example credit management transactions to carry out their daily work, if FRMN is entered as the start menu in that user's data, the SAP menu will show only credit management transactions.

The screenshot shows the SAP 'Maintain Users' interface for user 'SCHWACHH'. The 'Defaults' tab is selected. The 'Start menu' field is empty. The 'Logon Language' field is empty. The 'Decimal Notation' field is set to '1.234.567,89'. The 'Date Format' field is set to 'DD.MM.YYYY'. The 'Time Format (12/24h)' field is set to '24 Hour Format (Example: 12:05:10)'. The 'Spool Control' section includes an 'Output Device' field, a 'Print Now' checkbox, and a 'Delete After Output' checkbox. The 'Personal Time Zone' section includes a 'Time Zone' field and a 'System Zone' field set to 'CET'. The 'CATT' section includes a 'Test Status' checkbox. The top navigation bar includes 'Documentation', 'Address', 'Logon Data', 'SNC', 'Defaults', 'Parameters', 'Roles', 'Profiles', 'Groups', 'Personalization', and 'Lic. Data'. The top status bar shows 'User: SCHWACHH', 'Changed By: SAP', '17.04.2020 17:22:37', and 'Status: saved'.

Figure 2.13. Defaults tab.

In transaction SSM2 the initial menu can be specified globally for the entire system.

Logon language: the language the system is in when the user logs in. On the login screen, the user can choose any other language if necessary.

Output device: short name of a printer in the SAP system, specified in the device definition. Users must use this name (or the long name) to select the output device.

Time zone: The time zone describes the location of an object in relation to its local time. The underlying rule set describes the difference between the time zone and UTC in hours and minutes, and the start and end of daylight saving time.

Date format and decimal notation: Countries use different formats for numbers and dates. The usual format for the user's country must be entered.

Parameters Tab:

By using parameters, fields can be populated with default values from the SAP system memory.

Example: A user who only has authorization for company code 1000. When executing a transaction, the value of this company code is stored in memory associating it with the ID of the corresponding parameter. In all subsequent screens, all the fields that refer to the company code data element will be automatically filled with the value 1000.

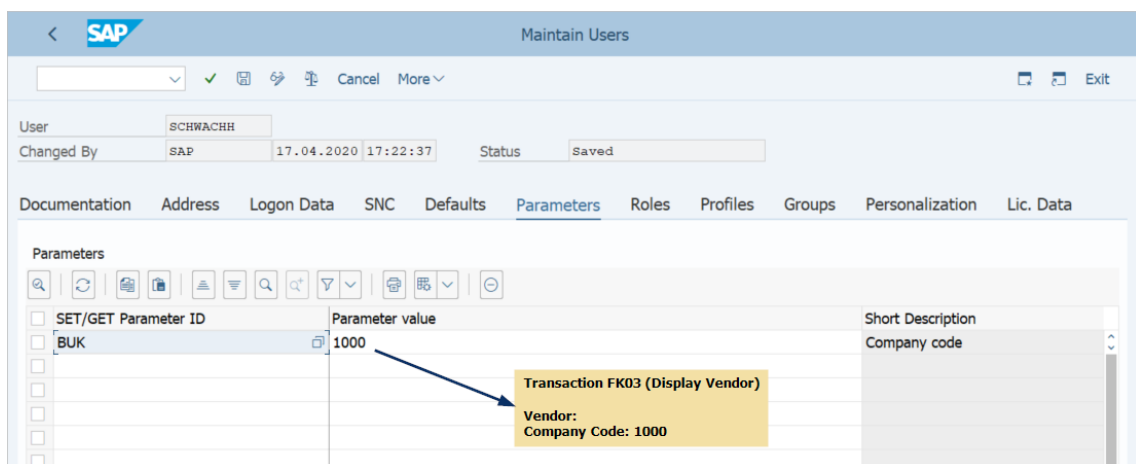


Figure 2.14. Parameters tab.

Roles Tab:

In the Roles tab, you can use the search help (by pressing F4) to display a list of all available roles, and then select the desired entries.

It is possible to assign any number of roles and then restrict their validity using the validity columns. If the search help is used in these columns, the system displays a calendar from which the date can be selected.

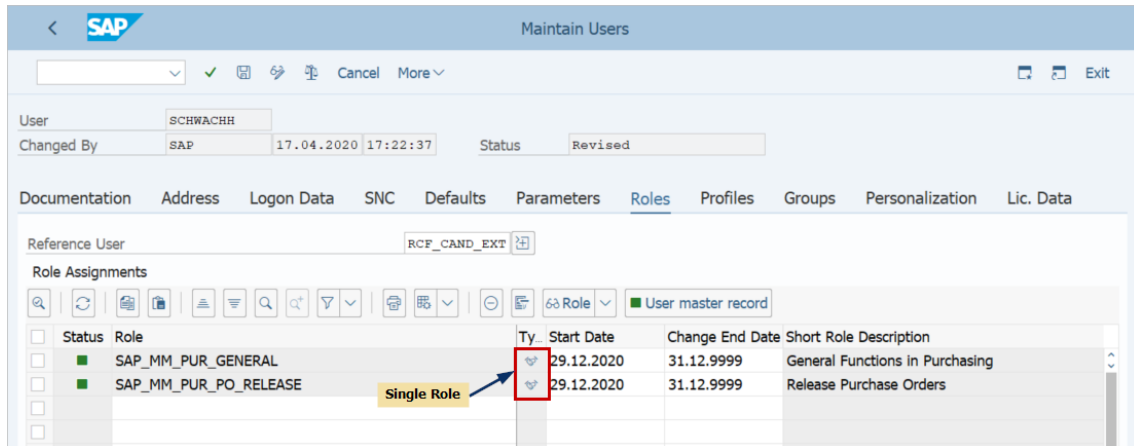


Figure 2.15. Roles tab.

Profiles Tab:

In the Profiles tab, authorization profiles, and therefore authorizations, can be assigned to a user. The profiles associated with the roles assigned to the user are also shown here, which will appear shaded in gray.

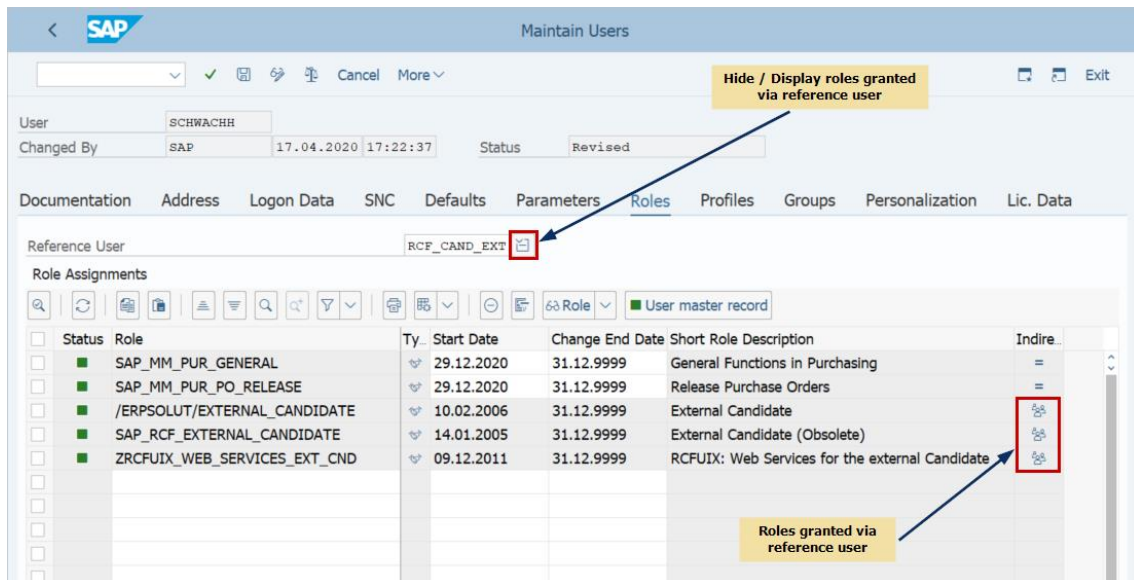


Figure 2.16. Roles assigned via reference user.

Additionally, there is the possibility of assigning additional authorizations via a reference user. In this case, in addition to the roles assigned to the user himself, he also receives the roles and profiles assigned to the reference user.

Each profile grants the user a series of authorizations. It is advisable to structure the content of the authorizations using the PFCG transaction and not using "manually created profiles".

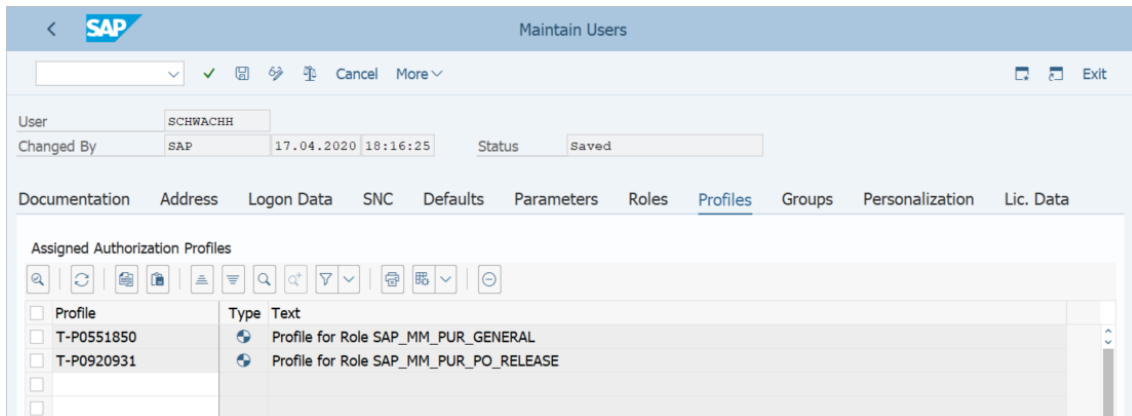


Figure 2.17. Profiles tab.

Caution: The profiles generated by the PFCG transaction should not be entered directly in the Profiles tab, since if there is no corresponding entry in the Roles tab, the PFUD transaction will remove these assignments. When a role is assigned to a user in the Roles tab, the profile generated for this role is automatically assigned in the Profiles tab and the profiles in the user's master record. PFUD is a transaction used in SAP for user master data reconciliation. SAP systems usually have a daily background job scheduled that runs this program.

The SAP system contains a number of predefined profiles, for example:

- **SAP_ALL:** To assign all authorizations that exist in the SAP system to users, this profile is assigned.
- **SAP_NEW:** composite profile to compensate for differences between updates in the event that new authorization checks are changed or added for existing functions, so that users can continue working normally.

It is strongly recommended not to assign these profiles in Productive environments.

Groups Tab:

Groups tab is currently not used. The main use of this tab is the Global User Manager, which has been officially disabled. For this reason, this tab is not discussed in detail.

Personalization Tab:

In the Personalization tab, user-related settings can be made using personalization objects. Customization is available in both role maintenance and user maintenance. Here, you can define values that control the results that are displayed when running programs (for example, display periods: Last 3 months, Number of entries: Max. 50, etc.).

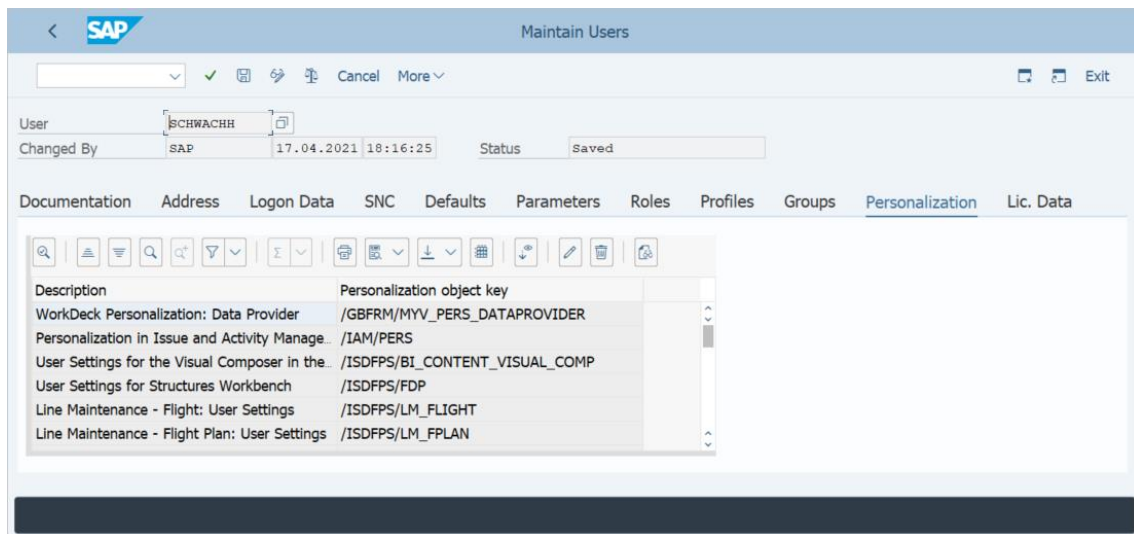


Figure 2.18. Personalization tab.

License Data Tab:

The SAP software contains a measurement program with which each system produces the information necessary to determine the cost of the user licenses for the installation. The measurement program is used exclusively to determine the number of users and the units of the SAP products used. The results are evaluated according to the conditions agreed in the contract with SAP.

The data entered in the License field is merely informative, and do not entail any economic cost. However, the license data must be maintained according to the conditions agreed with SAP, so that when the measurement is made, the data obtained is accurate.

2.5. User master setting

There is the possibility of assigning roles to users for a limited period of time. This may make sense, for example, during the close of the financial year: activities related to physical inventory should only be allowed for a limited time. For the changes in the user master to be effective, the comparison must be executed before the user accesses the system.

There are two procedures to perform this function:

- As a background job that runs the PFCG_TIME_DEPENDENCY report before the shift starts, but after midnight, so that the authorization profiles in the user master record are always up-to-date in the morning. It is highly recommended to schedule this job periodically to run on a daily basis.
- Alternatively, by executing the PFUD transaction. Administrators should regularly run this transaction as a check. This way, it is possible to manually process errors that may have arisen and that have been reported during the execution of the background job.

2.6. Change documents

To access the modification documents for users, you can use report RSUSR100N (through transaction SA38). The RSUSR100N report has been introduced in newer versions of SAP, and replaces the outdated RSUSR100 report.

Alternatively, it can be accessed from transaction SU01 itself, through the More → Information → Change Documents for Users menu path, or in SUIM transaction using the menu node of the Change Documents → For users area.

Figure 2.19. Change documents for users report.

In the selection window you can choose between different filters to suit your needs: ID of the user for whom you want to make the query, who made the modification, between what dates, etc.

On the other hand, at the bottom you can choose which results you want the report to show, if any. For example, within user attributes, you have the option of choosing the changes made at the level of locks, validity dates, password changes, or when the user was created:

Figure 2.20. Selection criteria bottom part of change documents for users report.

2.7. Mass user maintenance (SU10)

There are situations where you may need to create or modify multiple user master records. The easiest and fastest way to maintain users in bulk is provided by transaction SU10.

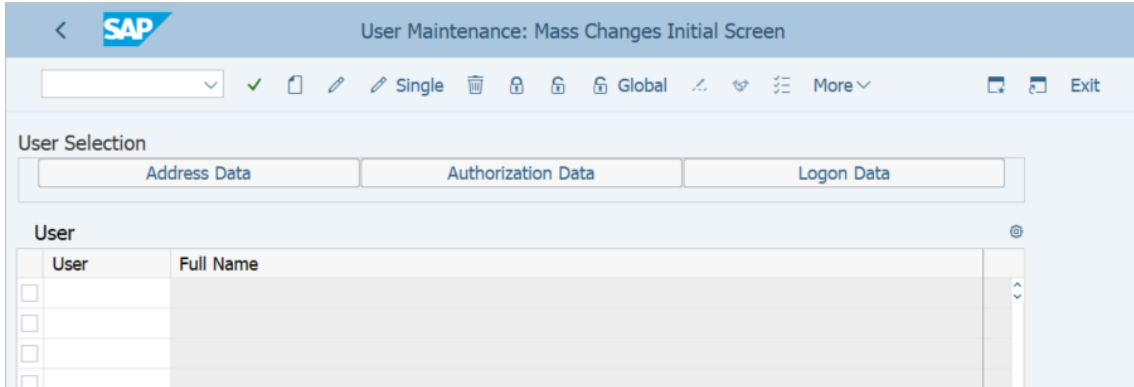


Figure 2.21. Transaction SU10.

The biggest limitation of transaction SU10 is that in a single run, the same settings will be applied to the entire set of users. Any operation with transaction SU10 has two basic steps, selecting users and modifying the selected users. The user selection area on the SU10 home screen allows user selection based on their existing address or authorization data. Users can also be added manually to the list on the initial screen.

The following example searches for users that begin with the string "test". The query returns a list of users that satisfy the criteria and passes the list of users for further processing:

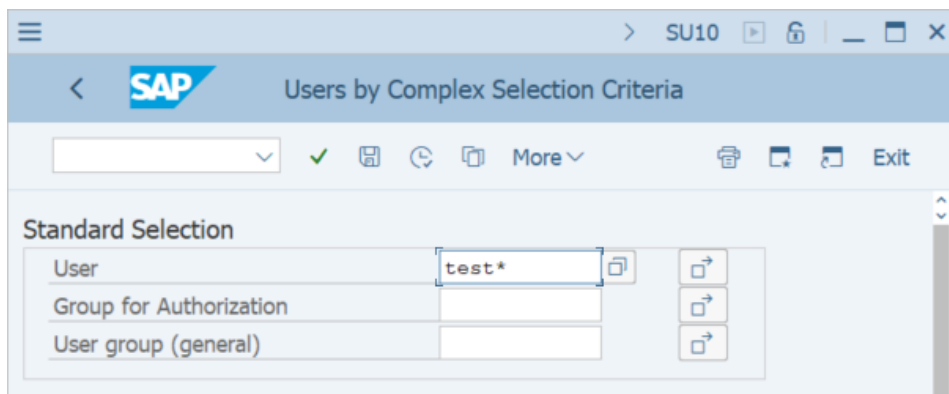
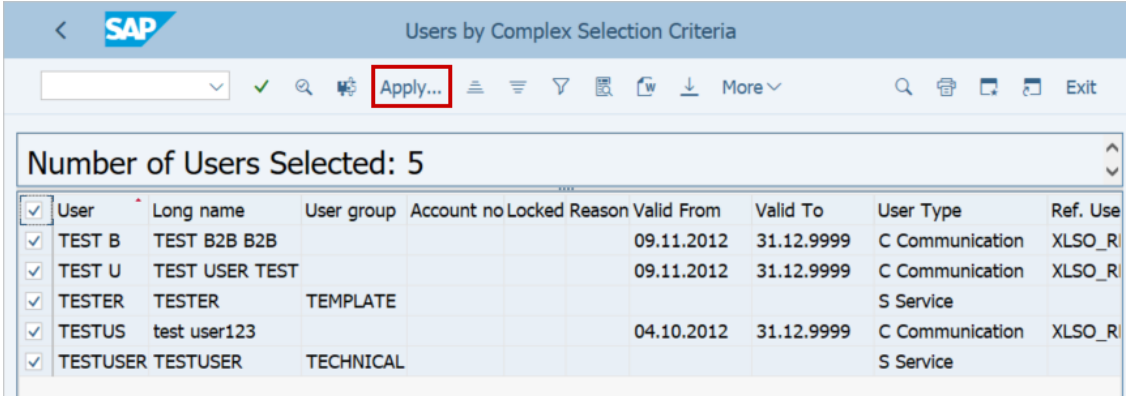


Figure 2.22. Users by complex selection criteria window.

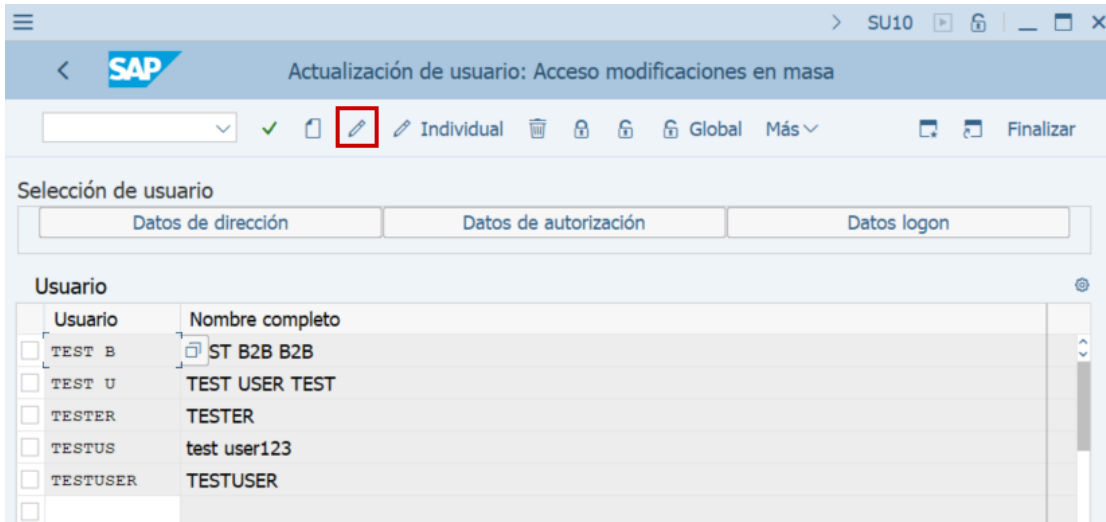


Number of Users Selected: 5

<input checked="" type="checkbox"/>	User	Long name	User group	Account no	Locked	Reason	Valid From	Valid To	User Type	Ref. Use
<input checked="" type="checkbox"/>	TEST B	TEST B2B B2B					09.11.2012	31.12.9999	C Communication	XLSO_R
<input checked="" type="checkbox"/>	TEST U	TEST USER TEST					09.11.2012	31.12.9999	C Communication	XLSO_R
<input checked="" type="checkbox"/>	TESTER	TESTER	TEMPLATE						S Service	
<input checked="" type="checkbox"/>	TESTUS	test user123					04.10.2012	31.12.9999	C Communication	XLSO_R
<input checked="" type="checkbox"/>	TESTUSER	TESTUSER	TECHNICAL						S Service	

Figure 2.23. List of users selected.

Once the list of users has been transferred, to make the changes in bulk, you must click on the edit button:



Actualización de usuario: Acceso modificaciones en masa

Selección de usuario

Datos de dirección Datos de autorización Datos logon

Usuario	Nombre completo
<input type="checkbox"/> TEST B	ST B2B B2B
<input type="checkbox"/> TEST U	TEST USER TEST
<input type="checkbox"/> TESTER	TESTER
<input type="checkbox"/> TESTUS	test user123
<input type="checkbox"/> TESTUSER	TESTUSER

Figure 2.24. Transaction SU10 with selected users.

The SU10 transaction allows the massive modification of addresses, login data, parameters, roles, profiles, etc.:

2 User Maintenance (SU01)

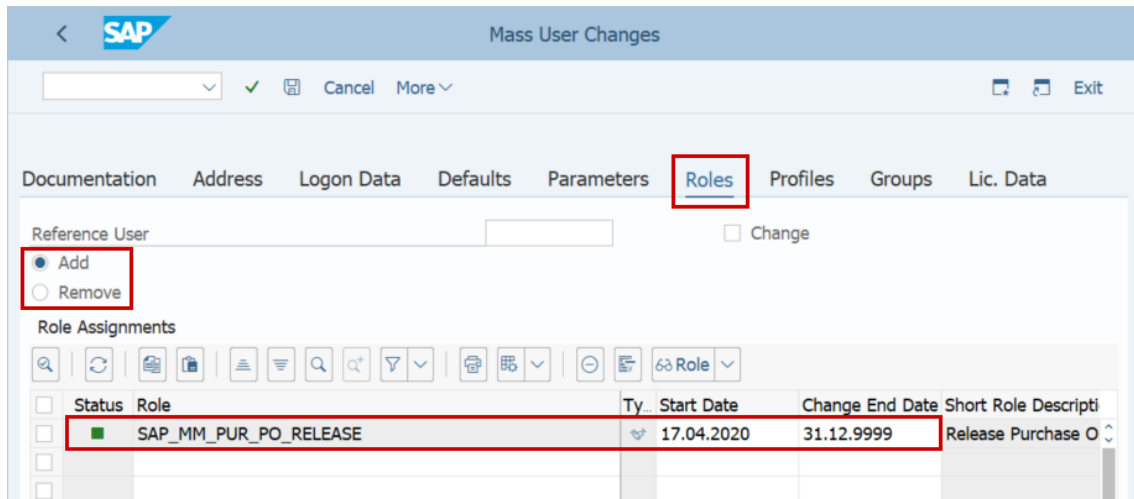


Figure 2.25. Roles selected to add.

Once the data to be modified has been entered, click on the save button to make the changes effective. Transaction SU10 executes the specified actions and generates a log with the entries that it has modified during execution:

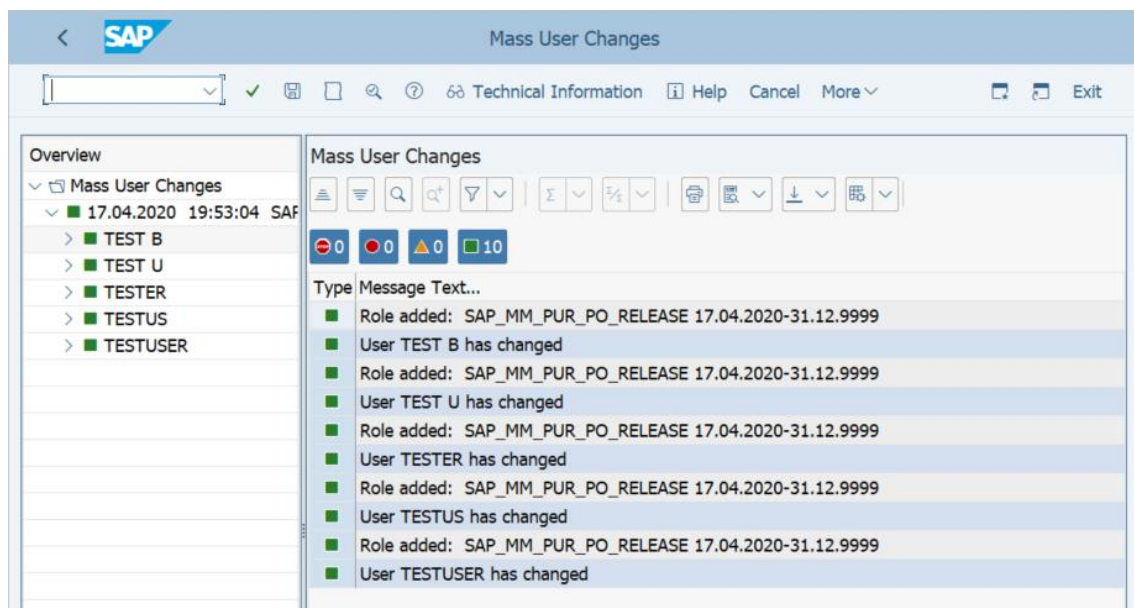


Figure 2.26. Log of modifications made by transaction SU10.

Another interesting use that can be given to the SU10 transaction is to block and unblock users in bulk. Users can be locked out by selecting the lock button:

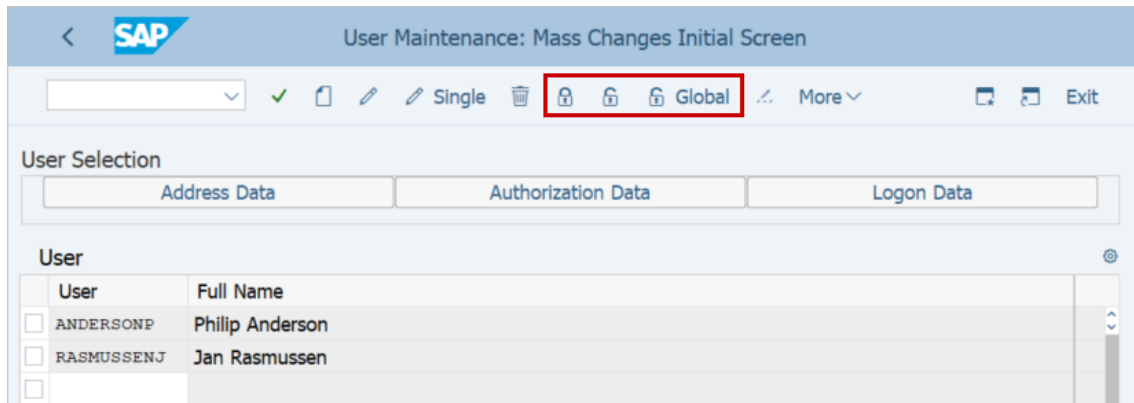


Figure 2.27. Lock and unlock buttons in transaction SU10.

3. Role Maintenance (PFCG)

The Profile Generator is the central tool to generate authorizations, authorization profiles, and assign them to users. To access this tool, execute **transaction PFCG**.

Within the PFCG transaction, administrators can add to the role: transactions, reports, web addresses, parts of the SAP menu or area menus. The functions chosen correspond to activities related to the business area of the user or group of users.

Therefore, a role is a set of functions that describe a specific work area. The "Account Receivable Accountant" role, for example, will contain transactions, reports, and/or internet/intranet links that account receivable accountants need for their daily tasks.

Roles can be used to implement the menus that users can work with when logging into the SAP system. There is the possibility of using predefined roles delivered by SAP and also roles created by the system administrators themselves. To display a list with all the roles predefined by SAP, report RSUSR070 can be used. Generally, these roles are used as a template to create your own roles to suit your needs.

3.1. Create and modify roles

It is possible to access the Profile Generator (PFCG) through the SAP menu, navigating to Tools → Administration → User maintenance → Role Administration → Roles.

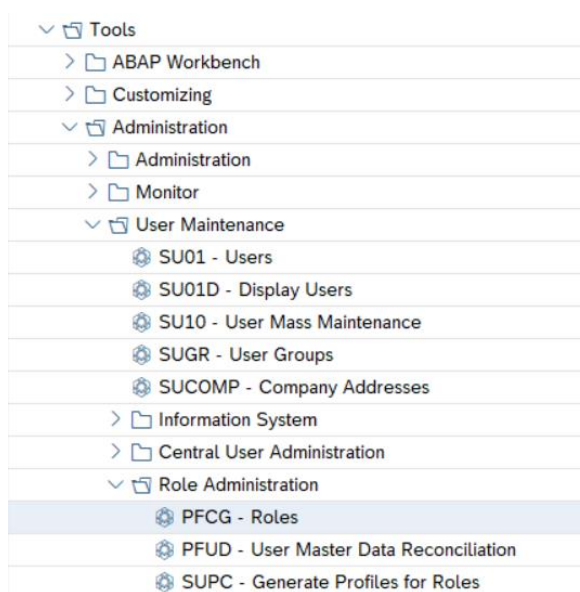


Figure 3.1. PFCG transaction path in the standard menu.

At a general level, the steps to create a role, including assigning the role to the user, are:

- The first step is to define the role and enter a short description of its content.
- In the second step, the activities of the role are defined. The result of this definition process is a technical role within SAP that collects all the activities of the business role that is being defined, consisting of a series of transactions, reports, and web links.
- At the same time, the menu tree for the new role is defined.
- Subsequently, the authorizations for the selected activities are created and the profiles are generated. This step is the one that usually takes the most time.
- The roles are then assigned to the users.
- Finally (depending on the configuration of the PFCG), the comparison is made with the user master records of the users to whom the role has been assigned.

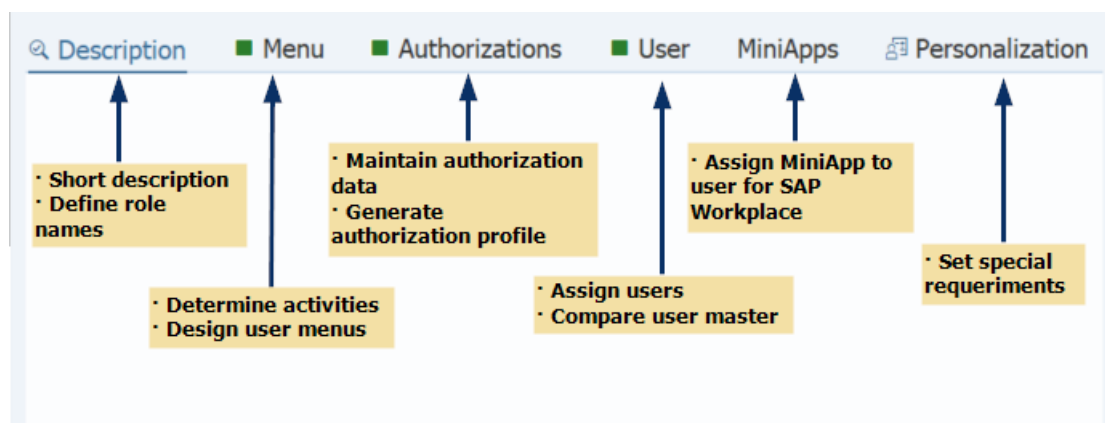


Figure 3.2. PFCG transaction tabs.

The steps to follow and the available functions that can be found within the PFCG transaction when creating/managing roles are described below:

1. Execute PFCG transaction.
2. If you want to create a new role from scratch, you must enter the name of the role to create and press the button .
 - a. All standard SAP roles have the prefix 'SAP_', therefore it is not possible to use this prefix for non-standard roles. Instead, a naming convention with its own prefix must be agreed. The most common are 'Z', 'Y' or 'G'.
 - b. SAP does not distinguish between the names of single, derived or composite roles (see Section 3.2), so it is also interesting to

include the type of role within the naming convention, for example using the letter 'S' to identify single roles.

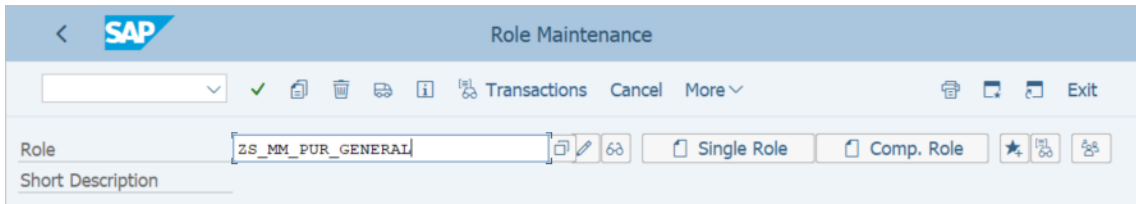



Figure 3.2. Single role creation example.

3. If you want to create a role as a copy of an existing one, enter the name of the source role and click on the button  .

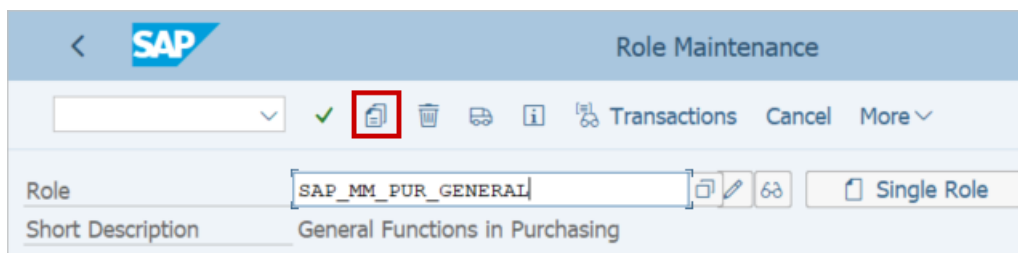


Figure 3.3. Example of creating a role as a copy of another.

In the next window, in the 'to role' field, enter the name of the new role.

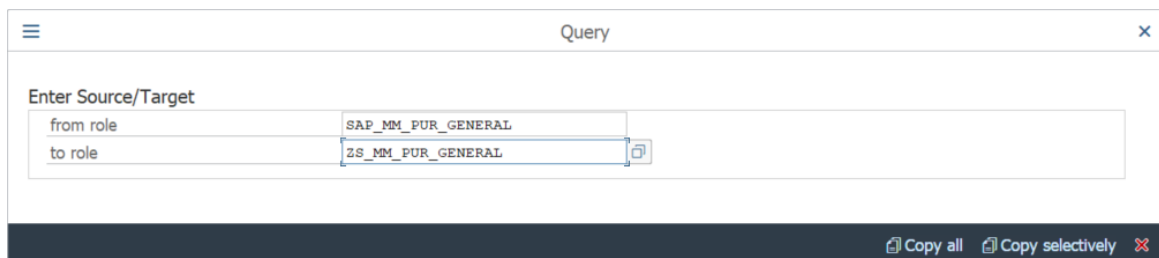


Figure 3.4. Selection window for copying a role.

4. Click on the 'Copy all' or 'Copy Selectively' button, as appropriate.
5. Once the role is created, click on the button  to modify it.

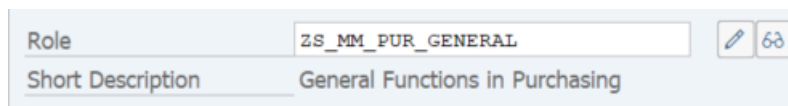


Figure 3.5. Role name.

The fields and tabs that can be found within the PFCG transaction are described below, once you have accessed to modify or view a role:

Role

Role	ZS_MM_PUR_GENERAL	<input type="checkbox"/> Obsolete	Role documentation
Description	General Functions in Purchasing		
Target System		<input checked="" type="checkbox"/> No destination	

Administration Information

	Created	Changed
User	SAP	SAP
Date	17.04.2020	17.04.2020
Time	17:41:31	17:41:32

Transaction Inheritance

Derive from Role

Long Text

Li 1, Co 1 Ln 1 - Ln 1 of 1 lines

Figure 3.6. Initial window of PFCG transaction.

First, if it has not been done yet, the 'Short description' field must be filled in with details of the role's functionality.

In the **Description tab**, there is a text field which can be used to expand the documentation of the role with information that is relevant. In addition, it is common practice to use this field to document the changes that occur in the role over time.

Long Text

14.03.2012 - This role was created to grant access to Purchasing General Functions.
08.06.2012 - Transaction ME61 has been added.

* Li 3, Co 46 Ln 1 - Ln 3 of 3 lines

Figure 3.7. Change history documentation example.

In the **Menu tab**, you enter all the transactions, programs and links that you want the role to contain, as well as the custom menus.

When creating the role menu there are several possibilities, which are displayed by clicking on the button  :

- From the standard SAP Menu:

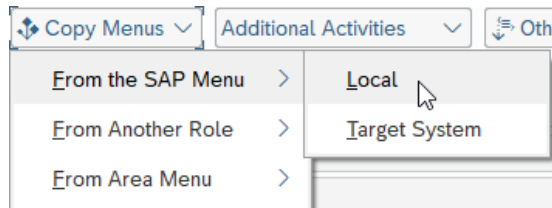


Figure 3.8. Path to create the role menu from the SAP Menu.

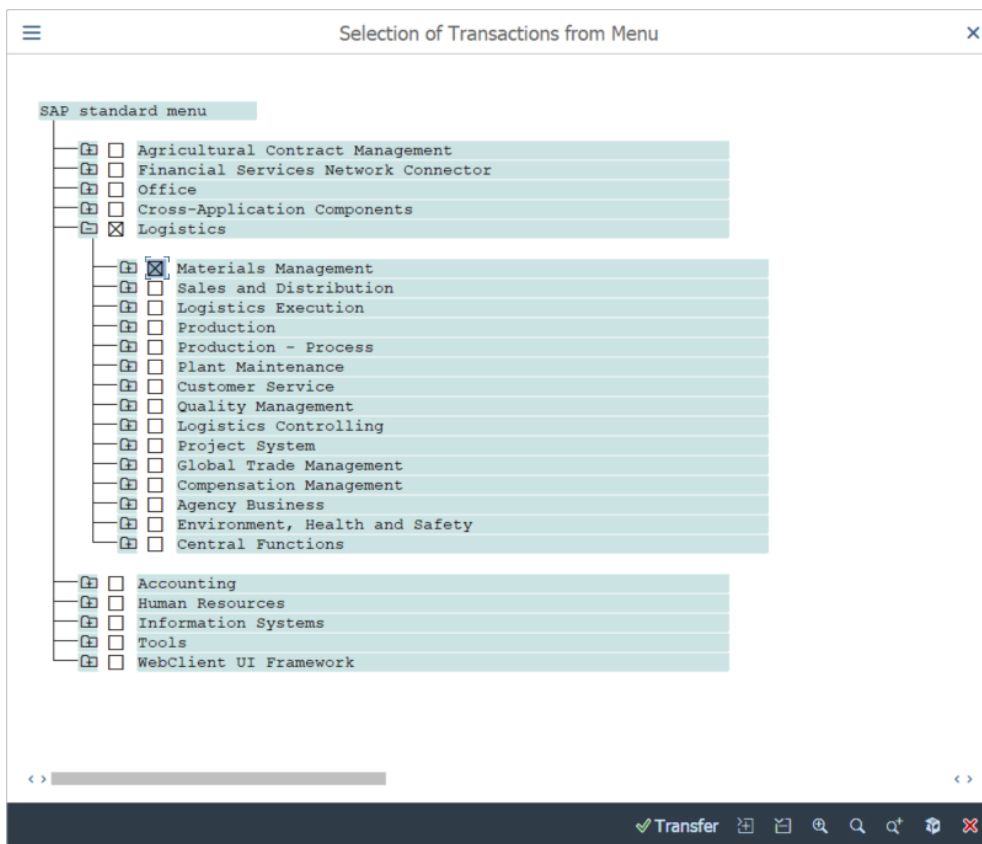


Figure 3.9. Transaction selection window from the SAP menu.

- From another role:

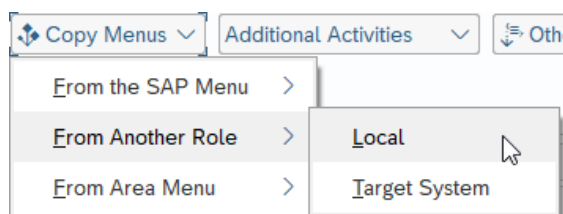


Figure 3.10. Path to create the role menu from another role.

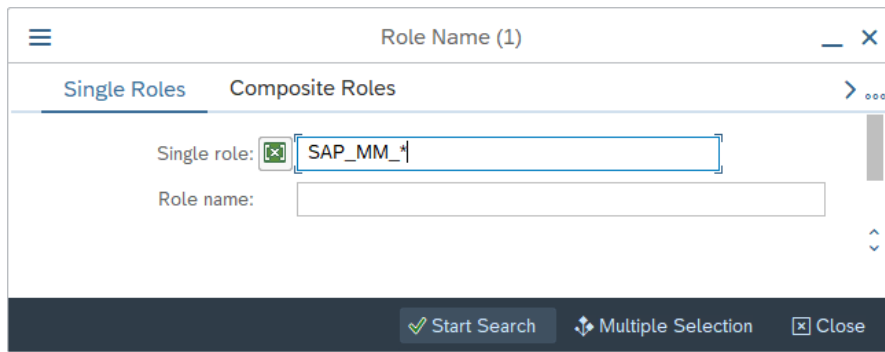


Figure 3.11. Role selection window to copy the menu.

- From an area menu:

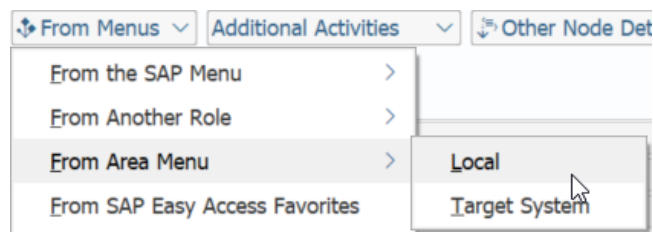


Figure 3.12. Path to create role menu from scope menu.

- From the favorites of a specific user:

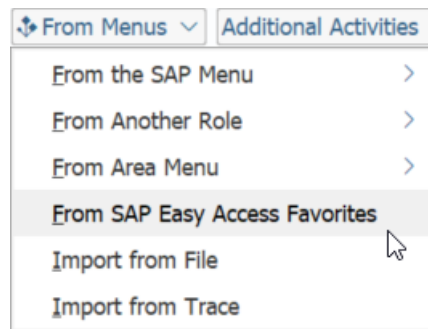
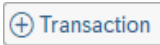



Figure 3.13. Path to create role menu from favorites.

- Import the data from a file or from a system trace.

It is also possible to create a Menu from scratch:

By clicking on the button  Transaction you can select one or more transactions to add to the role. By clicking on the button  you can create the folders and subfolders necessary to build the menu tree.

To change the text of the node or folder, double click on the node, and on the right side a field will appear a field in which it is possible to edit the text of the node:

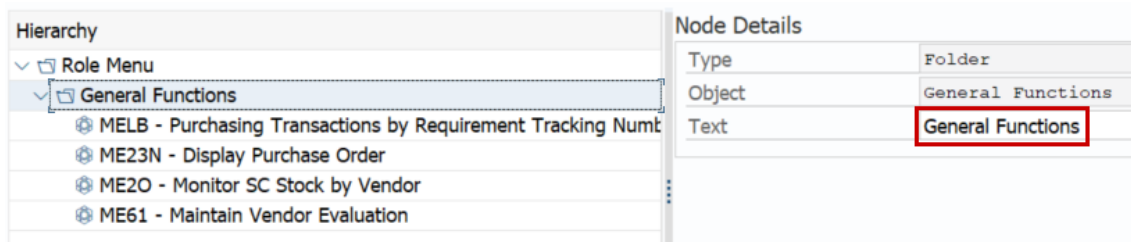


Figure 3.14. Change folder text.

To move a node up or down you can click on buttons respectively. If you want to delete the node, you can click on the button or, if you want to delete all the entries, you can click on the button shown in Figure 3.15.

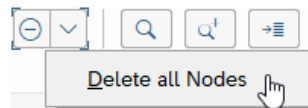


Figure 3.15. Button to delete all nodes.

The menu status traffic light will appear red if no menu is assigned. At least one node must be assigned to appear green.

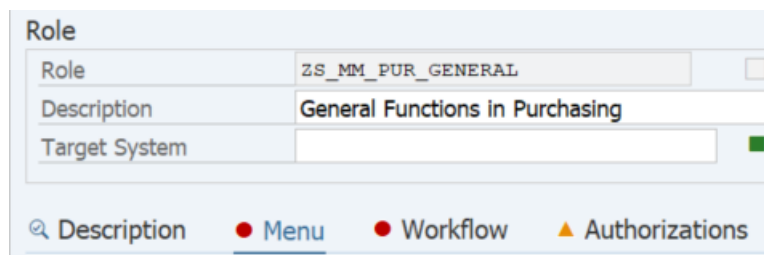


Figure 3.16. Menu status in red.


If you want to see the codes of the transactions or reports of each node, you can activate them by clicking on the button .

Click on the button to save the changes.

In the **Authorizations tab**, if it is the first time that authorizations are maintained, you must click on the button to carry out maintenance of authorization objects, authorization fields and their values.

The screenshot shows the SAP Role Maintenance (PFCG) interface. At the top, there are tabs for Description, Menu, Workflow, Authorizations (selected), User, MiniApps, and Personalization. Below the tabs, there are two tables: 'Created' and 'Last Changed', both showing User: SAP, Date: 17.04.2020, and Time: 17:41:32. Below these tables is the 'Information About Authorization Profile' section, which includes fields for Profile Name, Profile Text, and Status (Current version not generated). At the bottom, there is a section titled 'Edit Authorization Data and Generate Profiles' with two buttons: 'Change Authorization Data' and 'Expert Mode for Profile Generation'. The 'Change Authorization Data' button is highlighted with a red box.

Figure 3.17. Options for modifying authorizations.

If it is an update of the role, such as adding a transaction to the menu, click on the button  and then choose the option "Read old version and adjust with new data".

If a window appears asking if you want to save the modifications made so far, choose the 'Yes' option:

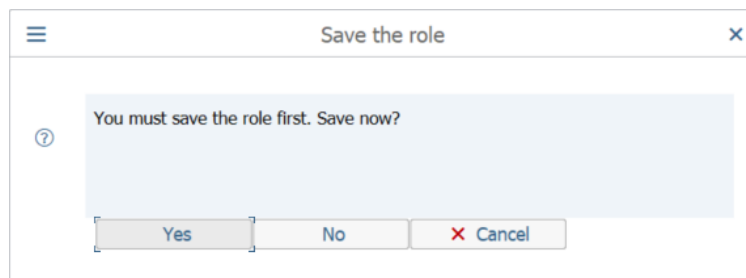


Figure 3.18. Notice window to save the role.

In the next window, the authorizations that the role contains will appear in the form of a tree. As explained in Chapter 1, authorizations are structured in the form of authorization object instances.

As can be seen in Figure 3.19, the parent node is the role itself, and a series of object classes hang from it, which is the way in which objects are grouped in SAP. Within each class the authorization objects can be found, and within these, the instances of each object, each one with certain values in the authorization fields.

3 Role Maintenance (PFCG)

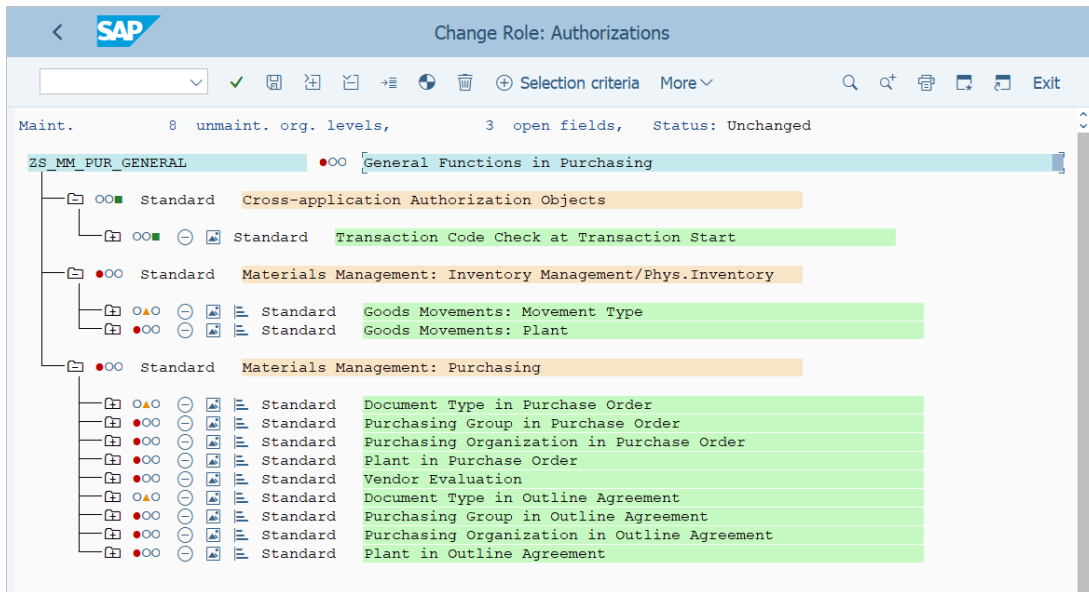


Figure 3.19. Role authorization window.

Depending on the configuration, the technical names of the authorization objects may not appear. If you want them to appear, they must be activated from the top menu path More → Utilities → Technical names on

In more recent SAP versions, a new view can be found, which can be activated or deactivated from the user options, in the 'Display' section.

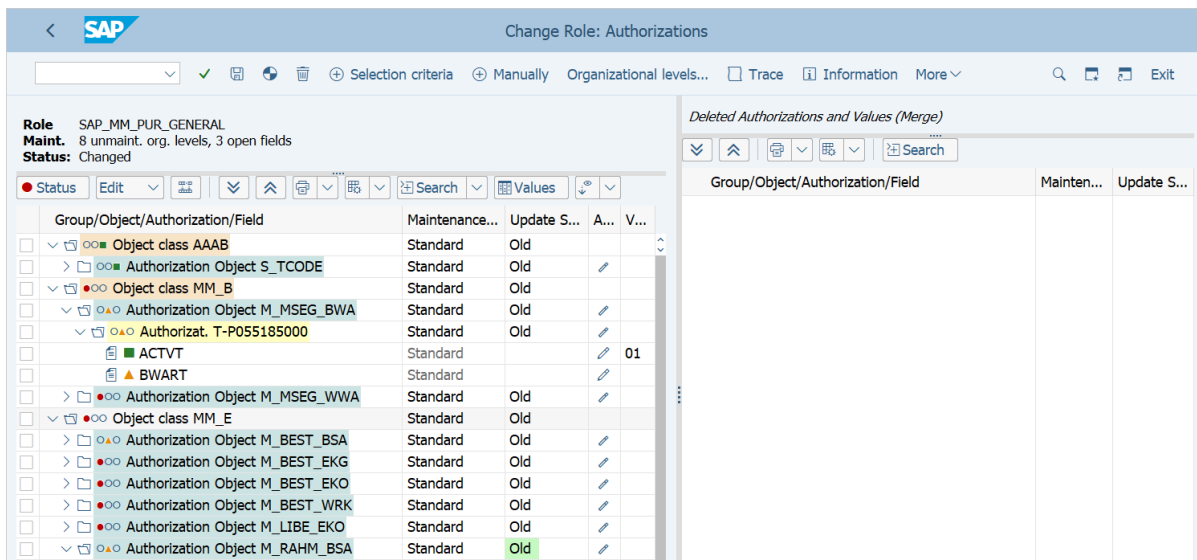


Figure 3.20. New tree look for role authorizations.

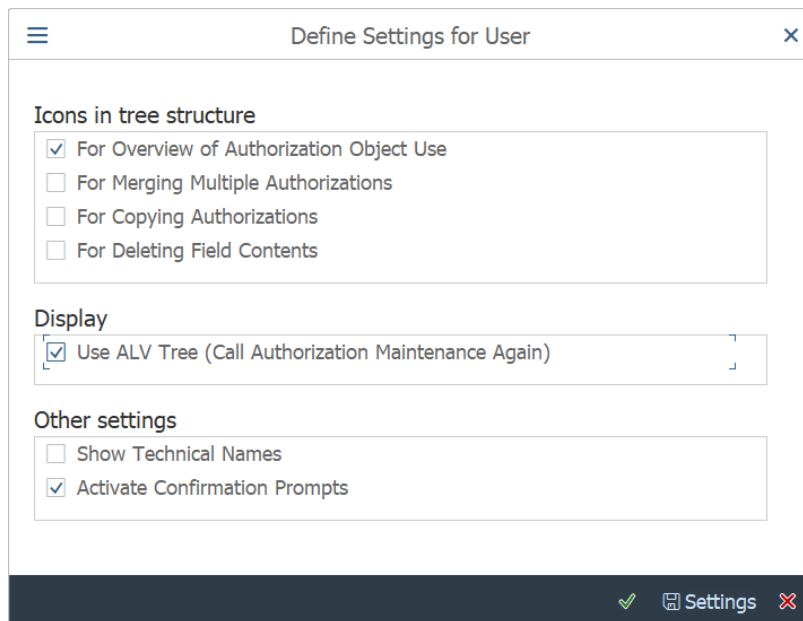



Figure 3.21. Window for defining user settings in PFCG.

In the authorization window you must make the appropriate changes, save and then press the button  to generate the profile. Always in that order, **first save and then generate.**

There will be times when a warning window appears, indicating that not all the expected tasks have been performed.

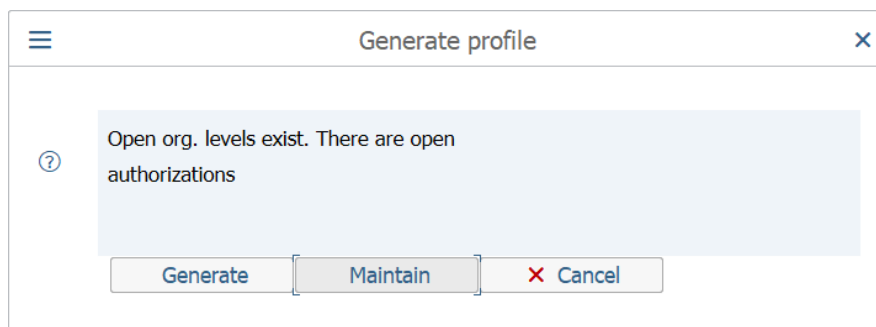
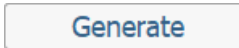



Figure 3.22. Notice message with pending tasks.

When pressing the button  , the window shown in Figure 3.23 will appear, where it is possible to modify the name of the profile associated with the role, and its description. Once these values have been chosen, press the button  .

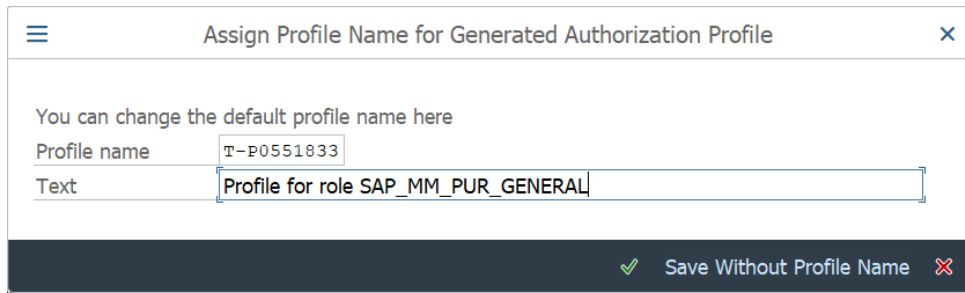



Figure 3.23. Window for naming the generated profile.

Once the profile has been generated, press the back  button. When going back, the profile field that was previously empty (see Figure 3.17) will now appear filled, along with the description of the profile and its status.

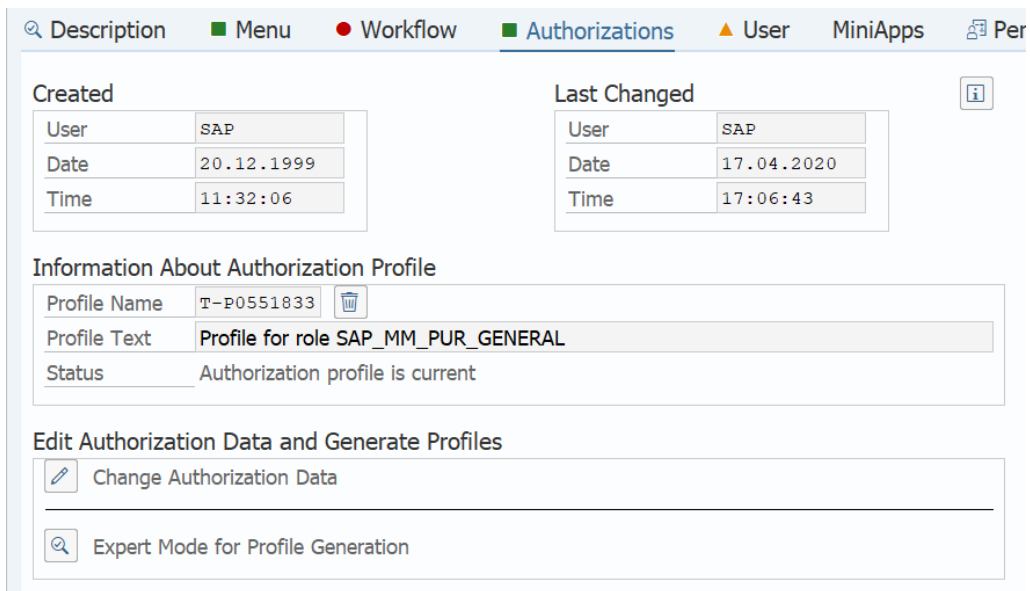





Figure 3.24. PFCG transaction authorizations tab.

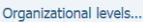
3.1.1. Subtleties of role maintenance

When maintaining and editing authorizations in PFCG, different **terms and icons** appear that are not always interpreted correctly.







On the one hand, for each instance of a certain object there is a **traffic light**, which is one of the most important elements for the administration of authorizations. This indicator can be used to quickly get an overview, showing the current maintenance status of authorizations at various levels. The different values that this icon can take are green, yellow and red:

-  All the fields of the instance are filled with any value. It is important to emphasize that, regardless of the traffic light, all entries should always be reviewed. The green traffic light does not mean that the content should be accepted without being reviewed.



-  There is at least one field (but no organizational level) in the instance for which there are no default values and no values entered.
-  There is at least one organizational level in the instance for which no value has been maintained.

Caution: Organizational levels should never be assigned directly in the field. This would cause the object to change to the "Modified" state (see the status section in this section). The button  should always be used or the key combination "Control + F8" to assign the values.

The following symbols can be found next to the traffic light:

-   Deactivate/Activate the authorization object. Inactive authorizations are ignored when profiles are generated.
-  Delete the instances or the values of the fields.
-  Shows which transactions are associated with this object.
-  Group multiple authorizations.
-  Copy authorization objects.

The following symbols or functions appear next to the authorization fields:

-  Click on this button to make the appropriate changes in the authorization field.
-  Click on this button to assign all possible permissions.

On the other hand, the status text shows the maintenance status. The statuses of the different authorization elements can be:

- **Standard:** All the fields in the lower levels have the default values, that is, they have the values maintained in transaction SU24 for the relevant transaction (see section 3.1.2). If the relevant transaction is removed from the role menu, the corresponding authorization objects will be removed.
- **Updated:** In cases where the object has been maintained in transaction SU24, but the values are not fully defined, the object will appear in the role with one or more empty fields. When these fields are updated with some value, then the status of the object becomes "Updated".

- **Modified:** When any of the authorization object values proposed in transaction SU24 are modified, the status of the object becomes "Modified". This removes the link between the object and the related transactions. If the transaction for which the objects are in the "Modified" state is removed from the role menu, these objects will remain in the role. For this reason, it is recommended to configure the SU24 correctly, to eliminate the need to have authorization objects in the "Modified" state.
- **Manual:** There is the possibility to add authorization objects manually to provide additional and different authorizations to the values configured in the SU24 of the relevant transaction. As with the "Modified" status, there is no link between any transaction in the menu. Used correctly, manually added objects can be effective in situations where updating the SU24 transaction is undesirable, but if not properly documented and managed, it can result in the assignment of unwanted authorizations.

Additionally, after a comparison (such as the one performed after adding a transaction to the menu) the following statuses can be found:

- **Old:** No new authorizations have been added.
- **New:** At least one new authorization has been added.

3.1.2. Default values (SU24)

When a transaction is added to a role menu and the authorization data is accessed to be maintained, the system automatically adds a series of authorization objects. These objects are those found as proposed in transaction SU24 for the transaction in question.

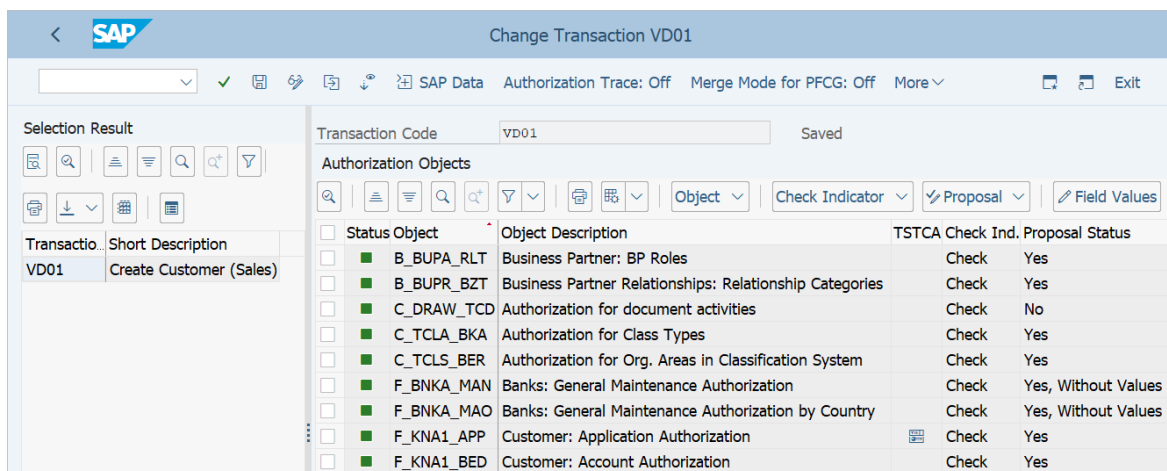
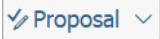


Figure 3.25. SU24 transaction main window.

Setting the default values

Authorization objects for which authorization values have not been maintained by default have the value "No" in the "Proposal" column. To change this status, you must select one or more lines in the section "Authorization objects" and click on the button  to choose one of the following values:

- **No:** This state indicates that the object is not necessary to be able to execute the main functionality of the transaction, which does not mean that it is not necessary in functionalities other than the main one. If the transaction is added to a role, the Profiler does not add an authorization for this object in the role. Not to be confused with the verification flag, which disables verification of the object at run time. For more information on verification indicators, see "Editing check indicators for objects" in this section.
- **Yes:** This state indicates that the object is required in order to run the **main functionality** of this application. Consequently, when the transaction is added to the menu of a role, the Profile Generator will add an instance for this object in the role with the values in the authorization fields that have been indicated as default values. If no value needs to be specified, option 'Yes, Without Values' can be used. Normally, if the values that the program checks are known, they will be included as default values in the fields of the authorization object. However, the fields should be left empty if the values are not defined, or if they depend on the roles.
- **Yes, Without Values:** This status indicates that the object is required to be able to run the main functionality of this application, but the object contains fields that can only be filled when defining the role. When adding the transaction to the menu of a role, the Profile Generator will add an empty instance for this object in the authorizations of the role.

Tips for setting Proposal status

- Generally, authorization objects that are explicitly checked in the program code by AUTHORITY-CHECK receive the default status **Yes** or **Yes, without values**.

- If users cannot use the main functionality of an application without a particular authorization, the default status **Yes** or **Yes, Without Values** for this authorization object.
- If in transaction SE93¹, in the definition of a transaction code, an authorization object is specified as an additional start authorization check, the status **Yes** must be assigned to this authorization object in transaction SU24. As default values for the fields, set at least the values entered in transaction SE93.

Display Dialog Transaction	
Transaction code	FK01
Package	WLIF
Transaction text	Create Vendor (Accounting)
Program	SAPMF02K
Screen number	105
Authorization Object	F_LFA1_APP Values
<input checked="" type="checkbox"/> Editing of standard transaction variant allowed	

Figure 3.26. Transaction SE93.

- Generally, authorization objects from Basis and Human Resources area that are verified in applications that do not belong to the Basis and Human Resources area receive the authorization status by default **No**.
- The start authorization check is a special case and affects to S_TCODE, S_START, S_RFC, and S_SERVICE authorization objects. In these cases, it is not necessary to set the default authorization state Yes for these authorization objects. Since the Profile Generator automatically adds to the role a start authorization for the application in question, it is not necessary to add the application name as the default authorization value in the SU24 transaction for these objects. Therefore, the default status should be set to No.

Tips for setting the default values

¹ Transaction SE93 is used to generate the transaction codes that SAP programs run.

- For fields that describe activities or other fixed values, enter the values that the system checks during the authorization check for the transaction.
- For authorization objects that contain the ACTVT activity field, enter only the activities that the developer has configured as allowed activities in the authorization object definition.
- The fields that describe Organizational Units are automatically populated with the corresponding variable, \$VARIABLENAME, which the system will fill in later when the role is created. This variable name should not be modified.
- Leave the fields empty if you want to complete them when defining the role.
- In the case of authorization object fields that are not used by the transaction, and that the system verifies with the DUMMY value, enter two single quotation marks (' '), and for fields with a length of 1 character, a single quotation mark (').
- If you cannot specify default authorization values for any field in an authorization object (for example, because the authorization object only has Customizing fields), set the default status to **Yes, Without Values** instead of **Yes**.

Editing check indicators for objects

In the case of transactions, it is also possible to control the authorization check with check flags that are set for each authorization object.

Status	Object	Object Description	Check Indicator	CA Check Ind. P
<input type="checkbox"/>	B_BUPA_RLT	Business Partner: BP Roles	Check	Y
<input type="checkbox"/>	B_BUPR_BZT	Business Partner Relationships: Relationship Categories	Check	Y

Figure 3.27. Check indicators.

To change a verification indicator, select one or more lines in the Authorization Objects section and use the Check Indicator button to choose one of the following states:

- **Check:** default check indicator. The system will perform the check, as long as it is explicitly checked in the program code with the `AUTHORITY-CHECK` statement. If verification does not exist in the code, activating verification in transaction SU24 has no effect.
- **Do not check:** Authorization verification for this authorization object is disabled, so the system does not check if the user has this object. This means that the ABAP `AUTHORITY-CHECK` statement always returns `sy-subrc = 0`, which means that the authorization check has no effect. **Therefore, this value should be used only in exceptional cases, and it is not allowed for Basis and Human Resources authorization objects.** If a transaction cannot be used without specific authorization, it is usually incorrect to assign the check flag **Do not check** for this authorization object. Instead, you should leave the verification flag set to **Check**, set the default status to **Yes**, and assign the appropriate default authorization values. If no default value can be specified, the status must be set to **Yes, Without Values**.

3.1.3. Expert mode

In the Authorizations tab of the PFCG transaction, you can find two different buttons when updating authorizations.

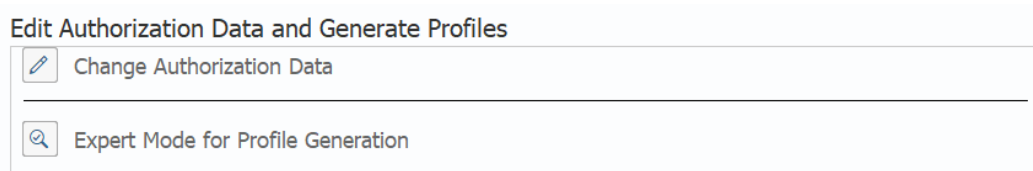


Figure 3.28. Options to update authorization data in transaction PFCG.

By clicking on the "Expert mode" button, the following three options will appear:

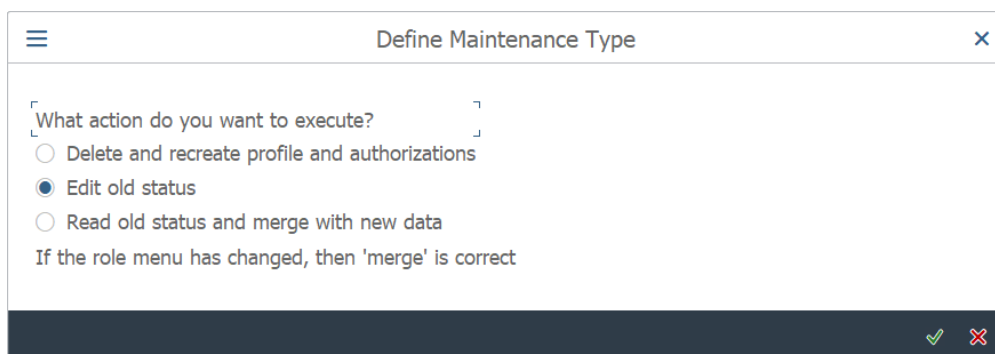


Figure 3.29. Maintenance types.

If the profile is being generated for the first time, there is no difference between “Modify authorization data” and any of the three options that appear when clicking on “Expert mode to generate profiles”. But if you are modifying a role, which already had the profile generated, you must select the option that best suits your needs.

- **Delete and recreate profile and authorizations:** All authorizations are recreated. Values that had previously been maintained, modified, or added manually are lost. Only the values held for organizational levels remain.
- **Edit old status:** The latest version of the stored data is displayed. This option is not useful when the role menu has been modified.
- **Read old status and merge with new data:** If transactions are added or removed from the role menu, this is the default option. The Profile Generator compares the existing authorizations with the default values of the menu transactions. If new authorizations are added automatically during this process, they will receive the status “New”. Authorizations that already existed will receive the status "Old".

The following aspects should be considered during the comparison:

- Organizational level values that are no longer required are removed, all others are preserved. If new organizational levels are added, they should be maintained.
- The values for the standard instance of the S_TCODE object are always auto-populated with the current transactions from the role menu. This instance cannot be copied or modified manually, only deactivated.

3.1.4. [Mass role maintenance \(PFCGMASSVAL\)](#)

PFCGMASSVAL transaction allows you to change authorization values for multiple roles at the same time.

With this transaction it is possible to maintain values of organizational levels, values of authorization fields for a selected object and values of the same field in different authorization objects.

3 Role Maintenance (PFCG)

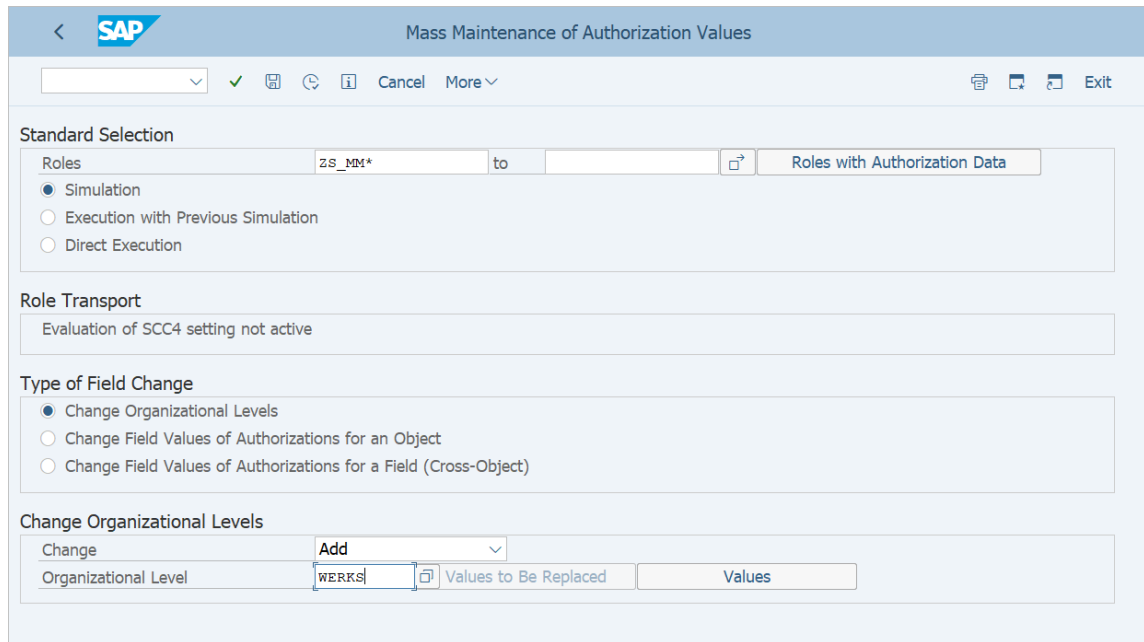


Figure 3.30. Transaction PFCGMASVAL.

By clicking on the 'Information' button on the initial screen of the transaction you can find additional documentation.

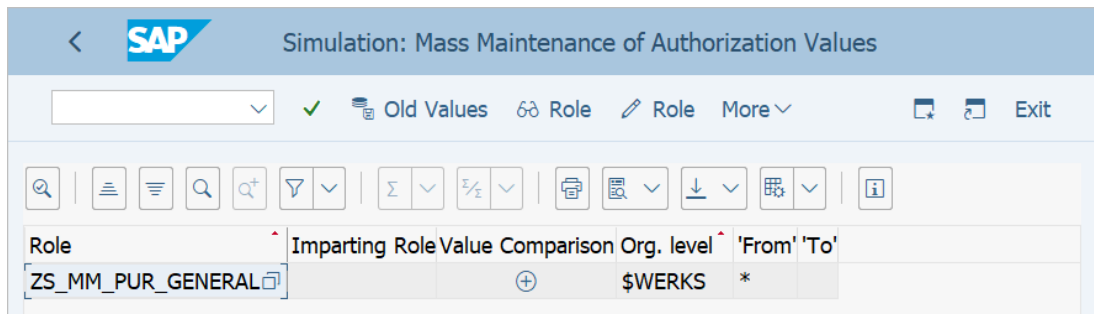


Figure 3.31. Result of a simulation with transaction PFCGMASVAL.

In general, it is recommended to:

- Always use a selection of roles, it is never desirable to make a modification on all roles of the system.
- Run the simulation first. This mode simulates the changes you want to make and displays them in a list of results.

Type of Field Change

Change Organizational Levels
 Change Field Values of Authorizations for an Object
 Change Field Values of Authorizations for a Field (Cross-Object)

Change Field Values of Authorizations for a Field (Cross-Object)

Change: Add

Object for Input Help:

Field Name: * Values to Be Replaced Values

Figure 3.32. Options for the change type.

- Use the selection options with care; you most likely do not want to convert the status of the "Standard" and "Updated" authorizations to "Modified". Therefore, the corresponding checkboxes for "Standard" and "Updated" should not be selected, and the checkbox "do not change to Modified state" should be kept active (see Figure 3.33).

Old Authorization Status (Irrelevant for Organizational Levels)

Standard
 Maintained
 Changed
 Manual

Options

No Switch to Status 'Changed' (Irrelevant for Organizational Levels)
 Exclude Derived Roles

Figure 3.33. Options for changing the previous authorization status.

- After changing the authorization data of the master roles, the derived roles must be adjusted for each master role, choosing the option Menu → Adjust derived roles, from the PFCG transaction. Alternatively, the SUPRN_REGENERATE_DEPENDENT report can be launched. To avoid modifying derived roles by accident, it is possible to activate the "Exclude derived roles" check box.

3.2. Special roles

Within role maintenance certain types of advanced roles can be found, which extend to standard roles in a useful way with special properties. A typical requirement in a company might be, for example, to create a role that has as clear menu as possible, but also fully describes a position or workplace. These attributes can be implemented in a Composite role.

The Reference, Derived and Customizing roles complete these possible requirements, and it is possible to create them using the Profile Generator.

3.2.1. Composite roles

A Composite role contains one or more single roles, which can help simplify role maintenance and optimize their use. When users are assigned a composite role, all the single roles that the composite contains will be assigned automatically, with all the permissions they grant.

Composite roles are very useful if several users in the same department need the same authorizations, that is, the same roles. By creating a composite role and assigning it to users, only one role is assigned to each user, avoiding having to assign many roles to each user.

The complete menu structure, which is the sum of all the menus of the single roles included in the composite role, can also be edited.

The procedure to create a composite role is:

1. Enter the name of the role in the Role field in the PFCG transaction. It is important to remember that SAP does not distinguish between simple and compound role names, so it is convenient to include some character that identifies the role as composite:

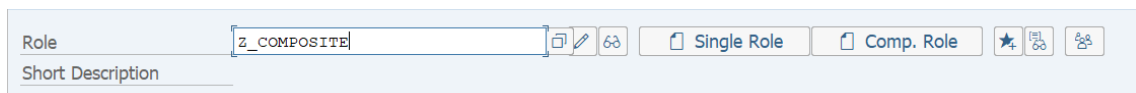
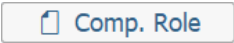


Figure 3.34. Composite role creation.

2. Press button  .
3. Define the single roles that will be part of the composite role.
4. Enter the name of the users in the User tab.
5. Save.

Description Roles Menu User Personalization				
Role	Name	Target Sys	Activ	
<input type="checkbox"/> SAP_MM_PUR_GENERAL			<input checked="" type="checkbox"/>	
<input type="checkbox"/> SAP_MM_PUR_PO_RELEASE			<input checked="" type="checkbox"/>	
<input type="checkbox"/> SAP_MM_PUR_PR_RELEASE			<input checked="" type="checkbox"/>	
<input type="checkbox"/>			<input type="checkbox"/>	

Figure 3.35. Single roles included in a composite role.

Composite roles cannot contain other composite roles.

3.2.2. Derived roles

Sometimes you may encounter situations where you need to create roles whose content differs only in authorizations and not in transactions. For example: two employees in the sales area with the same work center, but different plants (1100, 1200). Derived roles can be helpful in these situations, and using them can simplify future tasks. Examples of using derived roles are:

1. The menu of the roles must be identical, but the authorizations for the actions contained in the menu are assigned in the derived role.
2. The derived role menu and authorizations must be identical, but the organizational levels are assigned in the derived role.

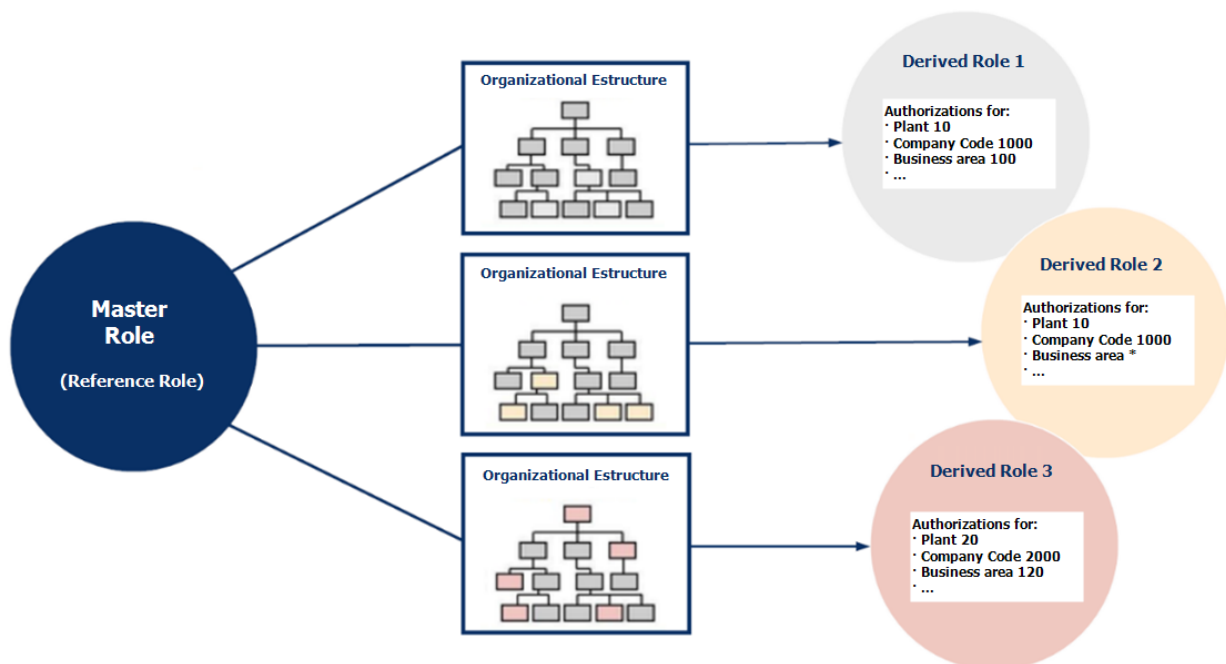


Figure 3.36. Derived roles diagram.

Therefore, derived roles refer to roles that already exist. Derived roles inherit the menu and included functions (transactions, reports, web links, etc.) within the reference roles (also called master roles, or template roles). In other words, roles derived from another role cannot have additional menu entries, that is, they cannot have additional transactions or reports. User mapping is not inherited by the derived role.

The procedure to create a derived role is:

1. First, you need to create a single role, or use an existing one, which will serve as the master role:

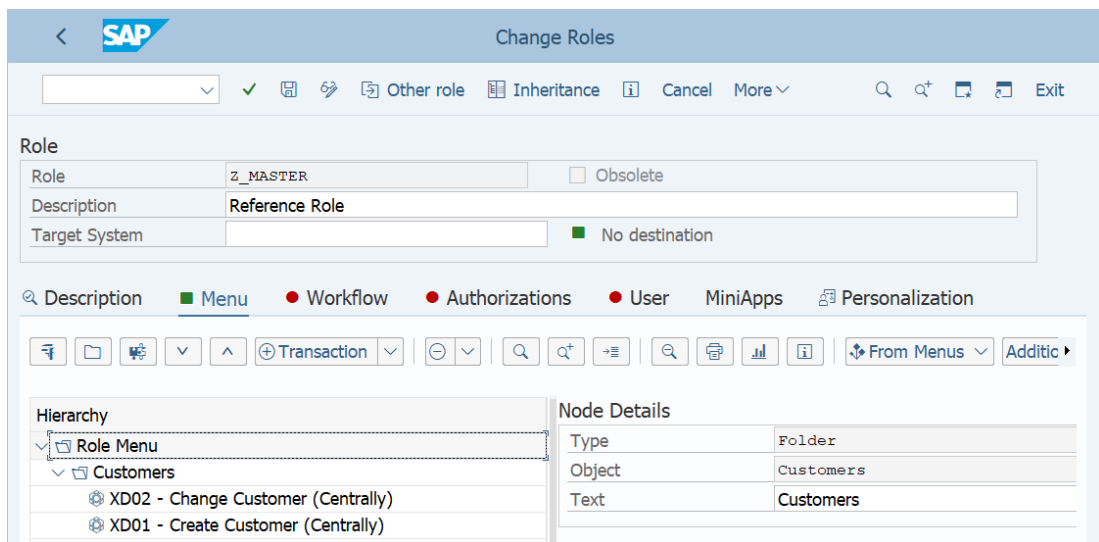


Figure 3.37. Master role creation.

2. Afterwards, you must create another single role, in the same way that has been done so far, and enter a descriptive text.
3. In the description tab, there is a section for 'Transaction Inheritance'. In the field 'Derive from role' you must enter the name of the master role, that is, the role of which all transactions and the menu structure will be included.

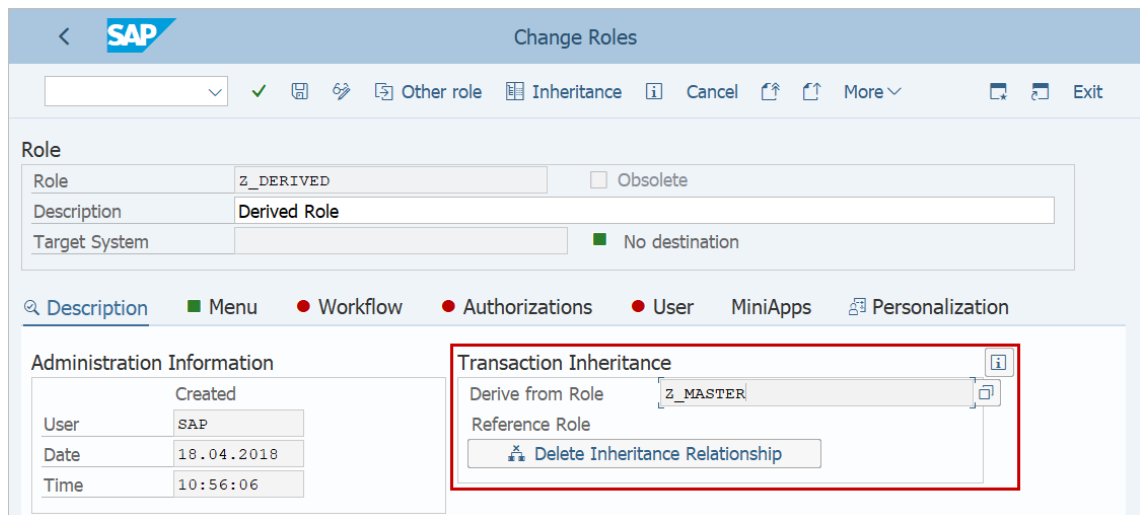




Figure 3.38. Derived role creation.

When saving the role, a role (derived) will have been created whose menu is “inherited” from another role (master).

The next step is to propagate the authorizations from the master role to the derived role:

1. From the PFCG transaction, edit the role from which the authorizations are to be propagated, that is, the master role. To do this, you must press the button  on the Authorizations tab.
2. To propagate authorizations to derived roles, select Authorizations → Adjust derived → Generate Derived Roles. You can also click on .

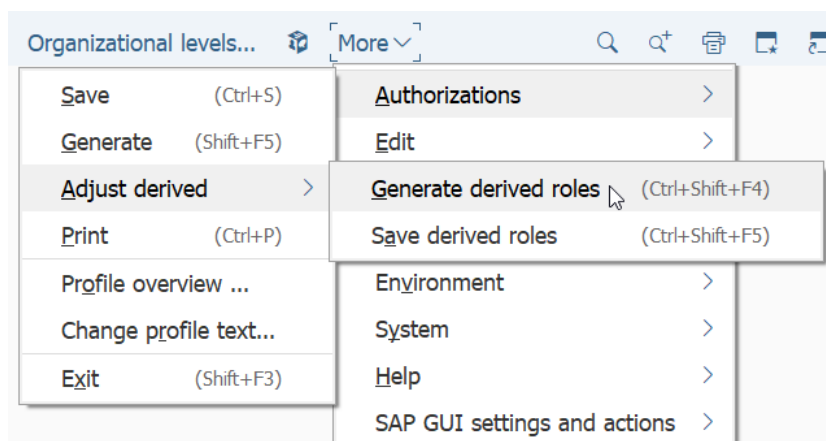



Figure 3.39. Generate derived roles.

In this way the authorization data is copied to the derived roles. When performing this action, the system will display an information message describing the procedure to generate derived roles. Click on the button  to continue.

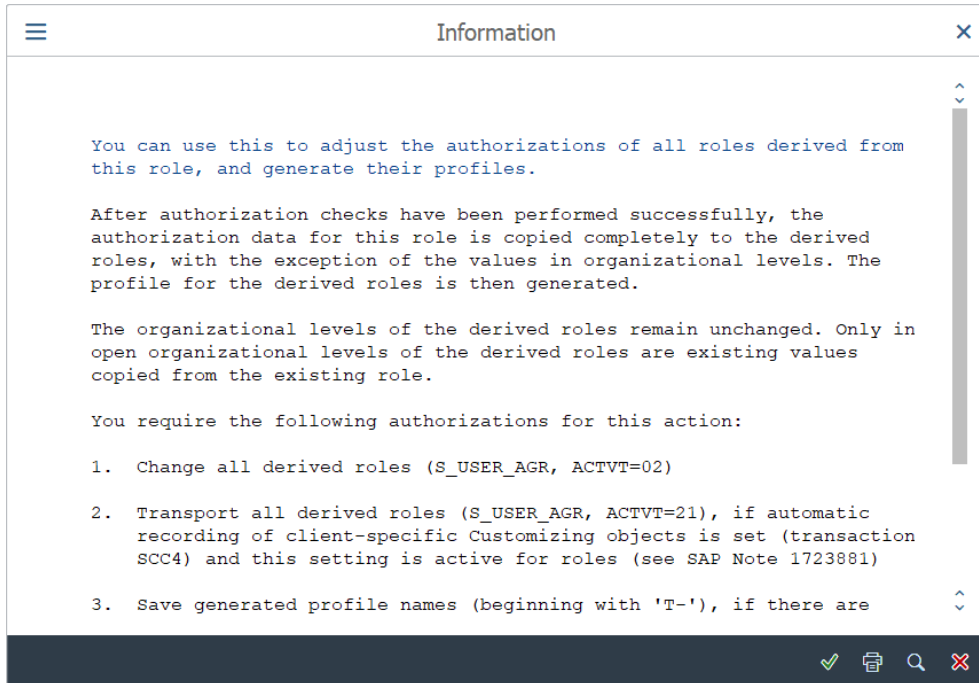


Figure 3.40. Information message when generating derived roles.

If there are authorizations with the yellow or red traffic light (see section 3.1.1) the system will display a message indicating that there are authorizations pending to be maintained:

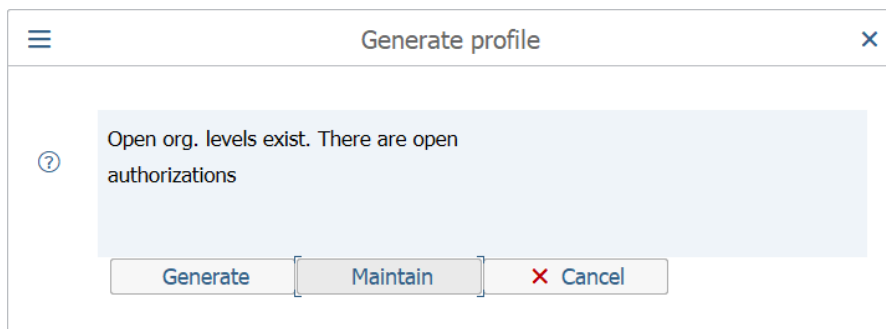


Figure 3.41. Notice message with pending tasks.

Before continuing, authorizations must be properly maintained, and propagated to derived roles. In the case of organizational levels, they should be maintained in the usual way.

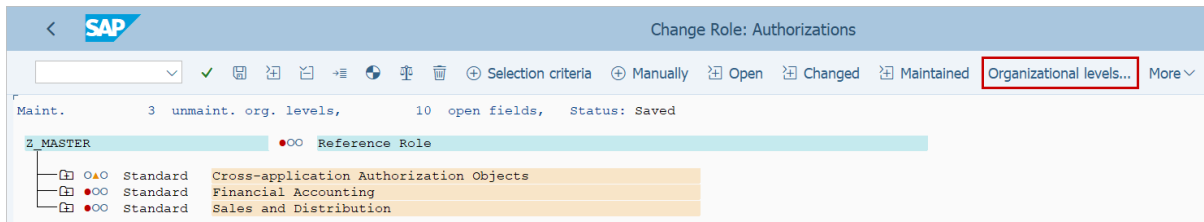


Figure 3.42. Maintenance of organizational levels.

In the case of master roles, it is a common practice to maintain the organizational levels with neutral values, such as single quotation marks (' '), and then maintain them properly in the derived roles.

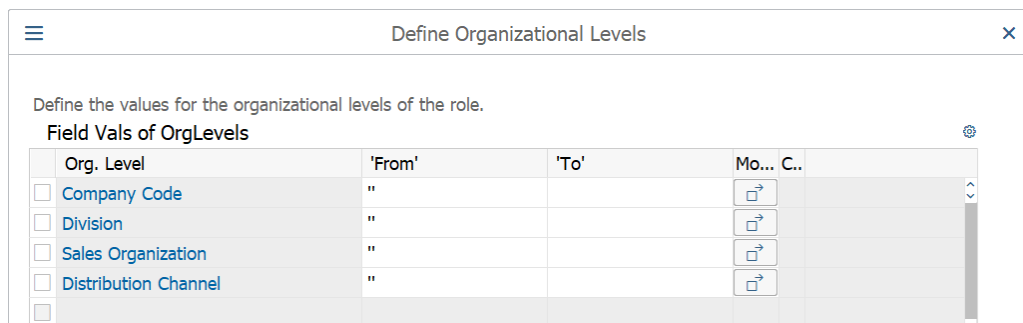


Figure 3.43. Organizational levels of a master role.

3. Finally, the derived roles must be edited and the Organizational Levels must be maintained according to the requirements. Derived roles are identical to the master role, except for the values of the fields that are organizational levels, which are maintained in the derived roles:

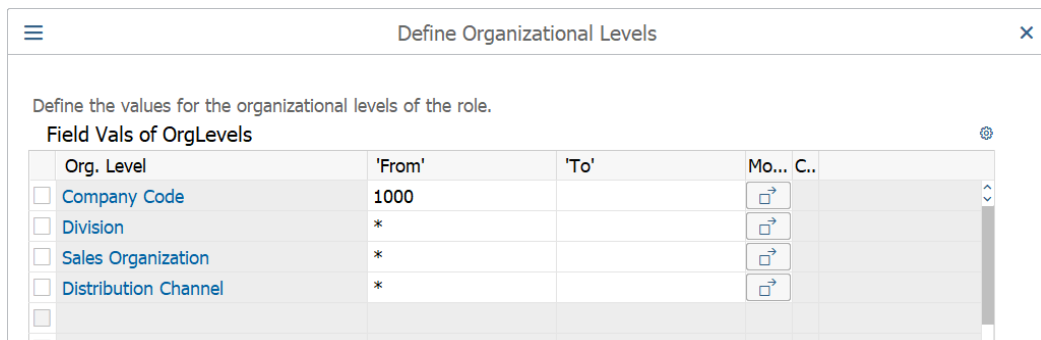


Figure 3.44. Organizational levels of a derived role.

The relationship between master and derived roles can be undone. To do this, you must edit the derived role, and press the button located in the main window.

3 Role Maintenance (PFCG)

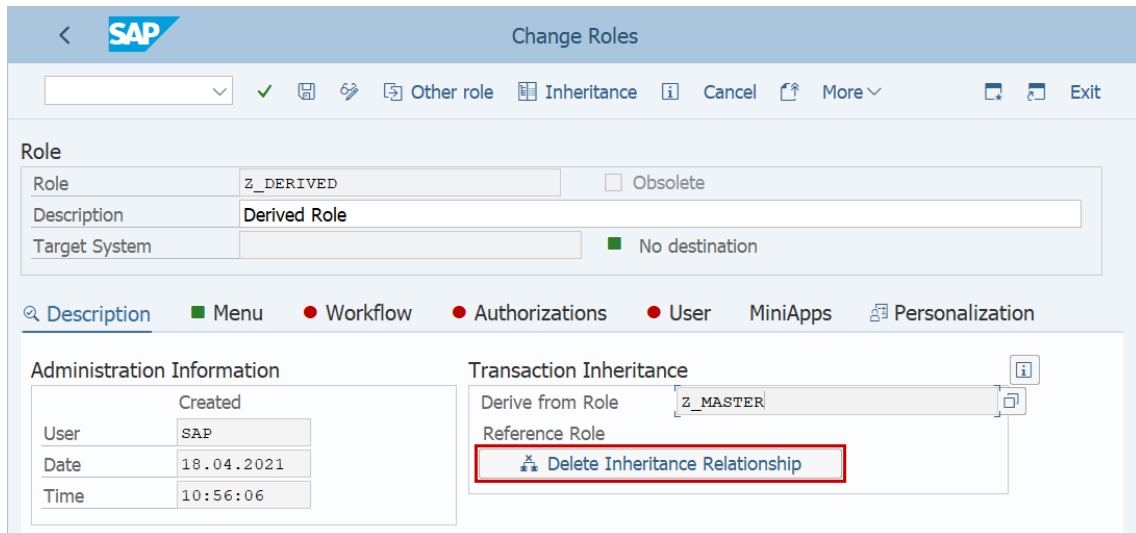


Figure 3.45. Delete relationship between master and derived role.



Figure 3.46. Inheritance deletion confirmation message.

3.2.3. Customizing roles

Customizing roles, also called parameterization roles, provide the ability to assign projects, or project views, from the Implementation Guide (IMG) to a Customizing role. The purpose of this assignment is to generate authorizations for certain IMG activities and assign them to users, or in other words, give authorizations to specific nodes of the SPRO transaction, which is the transaction with which the Implementation Guide is accessed.

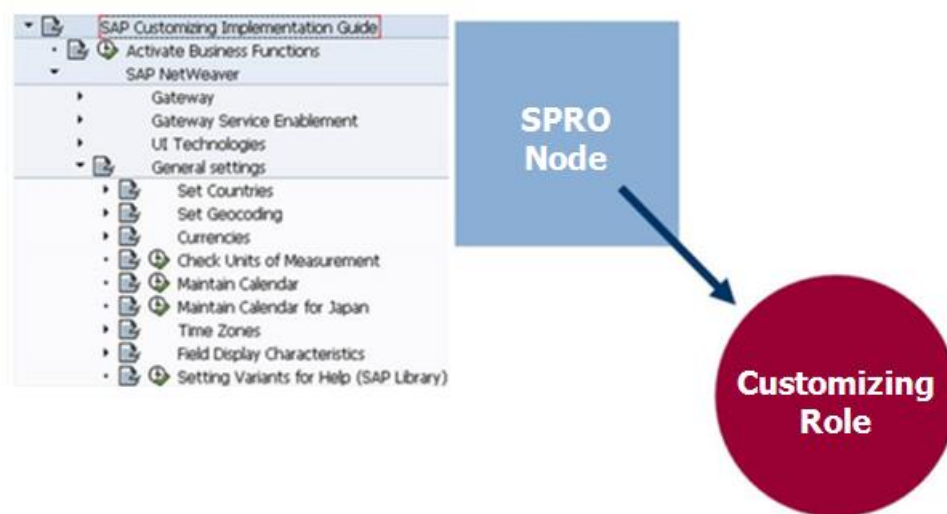


Figure 3.47. Customizing roles diagram.

Suggestion: Since Customizing activities are carried out on a project basis and for a limited period of time, it is good practice to maintain the end of validity date for users assigned to these roles. This ensures that users assigned to the role lose authorization for the assigned projects/project views after the project is finished.

To create this type of role, you must first create a SPRO project, then add it to the role. To do this, you must access the SPRO transaction and select the option Goto → Project Management. SPRO_ADMIN transaction can also be executed.

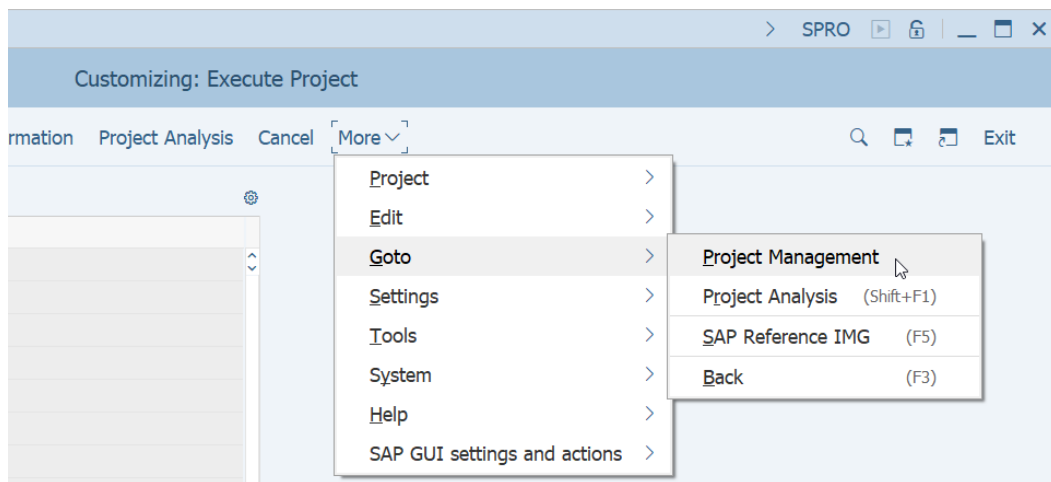


Figure 3.48. Path to the creation of Customizing projects.

In the next window, click on the button to create a new project:

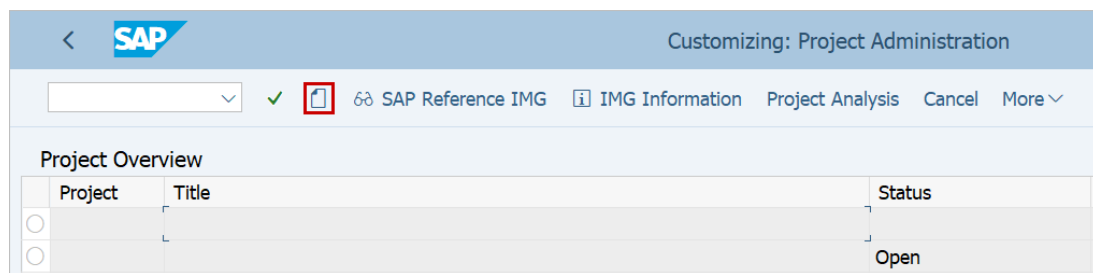


Figure 3.49. Customizing project creation.

Then enter a Title for the project, and save:

3 Role Maintenance (PFCG)

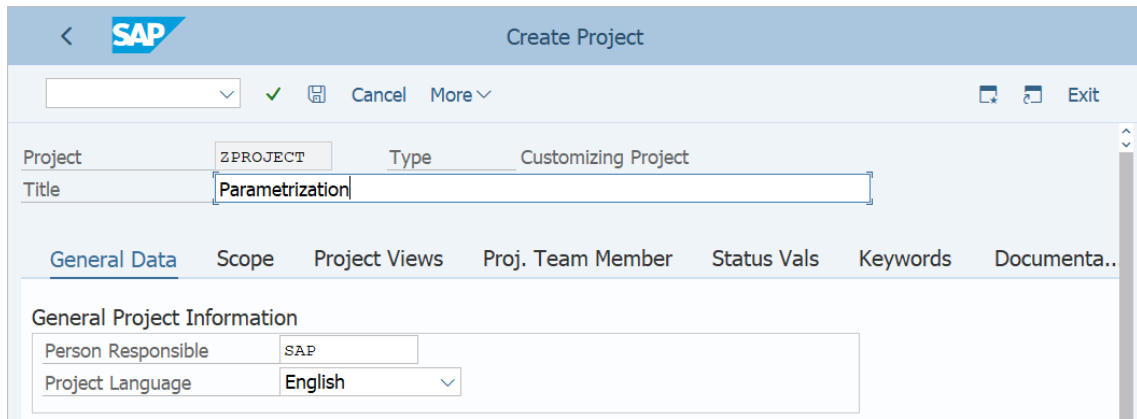


Figure 3.50. Customizing project general data.

Then, in the Scope tab, click on 'Specify scope'. If you have not saved yet, the system will warn you that the project must be saved first:

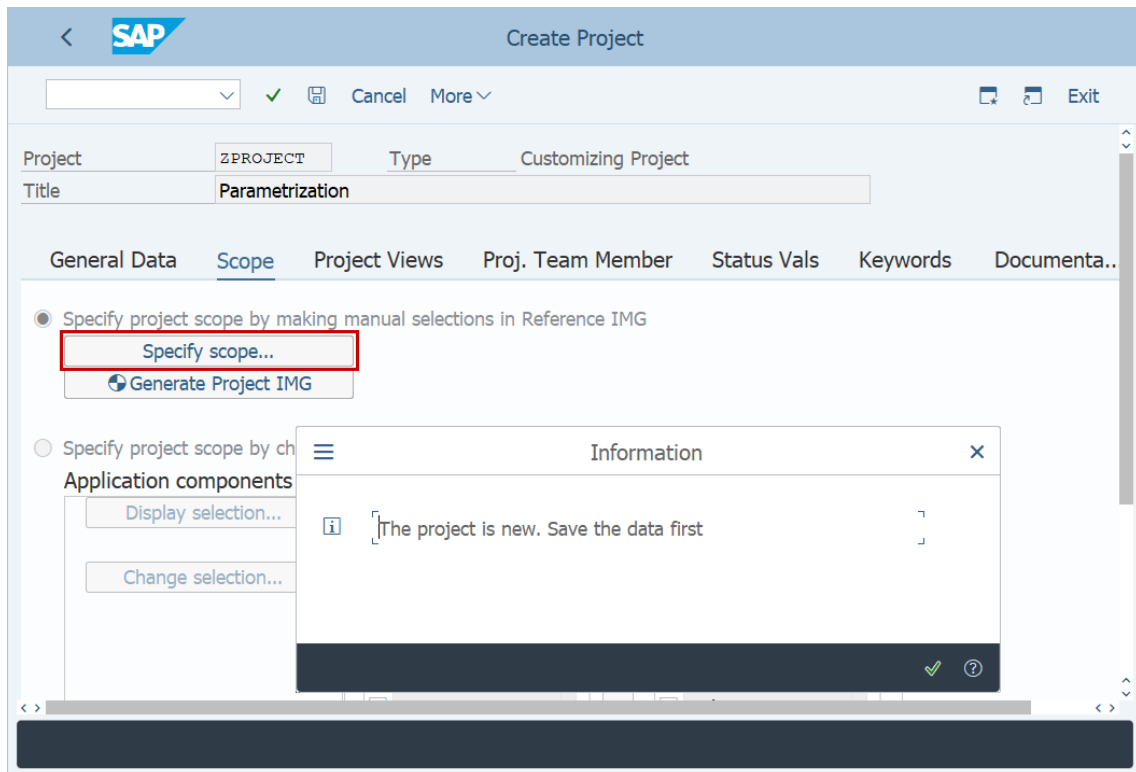


Figure 3.51. Customizing project scope.

Next, select the nodes that you want to include in the project, which will be the ones that will later be added to the role:

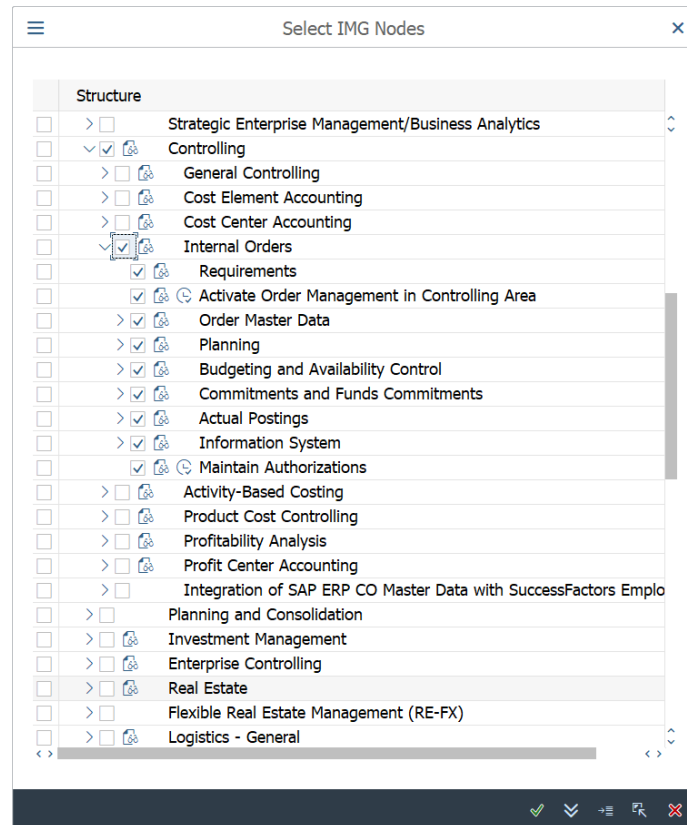


Figure 3.52. IMG node selection window.

At the end of this step, if everything has gone correctly, the system will display the following message:

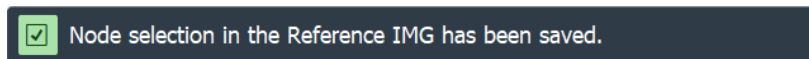


Figure 3.53. Node selection saving confirmation message.

Finally, click on the button [Generate Project IMG](#) in the Scope tab, and accept the following dialog box:

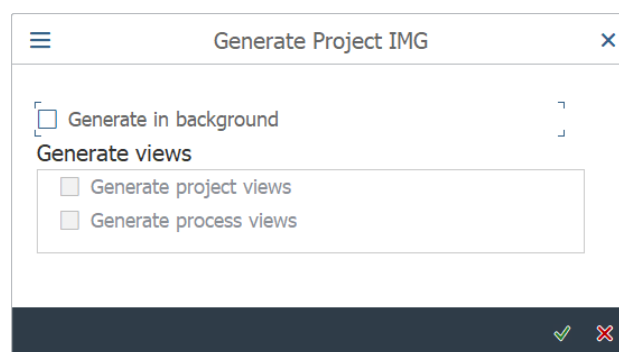


Figure 3.54. Generate Project IMG.

If everything went okay, the system will display the following message:

3 Role Maintenance (PFCG)



Figure 3.55. Project IMG creation confirmation message.

Once the project is generated, it is now possible to add it to a role. To do this, the PFCG transaction must be executed, and a new role must be created. From the top menu, select Utilities → Customizing Authorization:

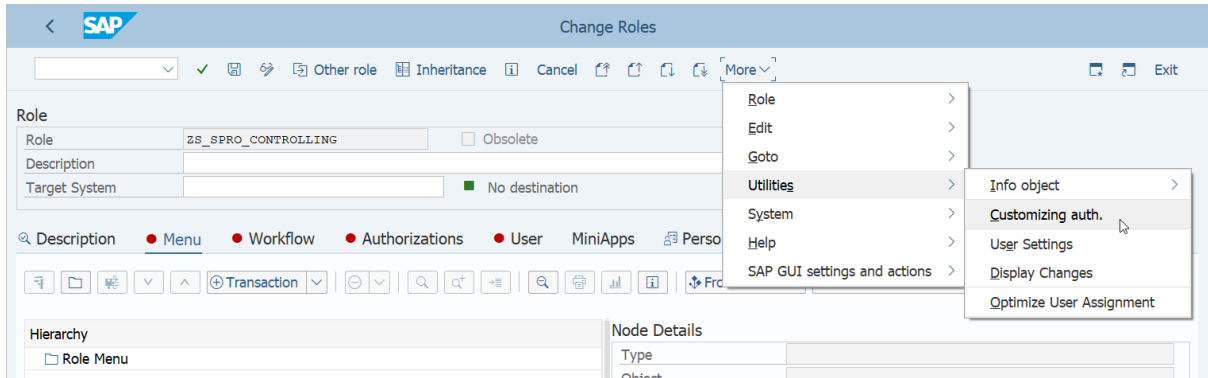


Figure 3.56. Path to add customizing authorizations to a role from PFCG transaction.

In the next window, click on the Add button:

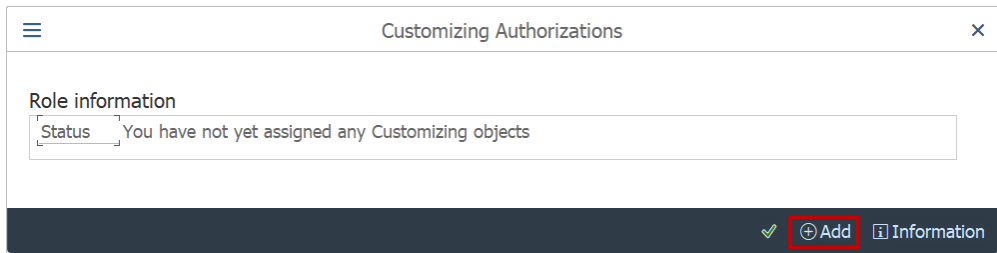


Figure 3.57. Add customizing authorizations.

Next, select the source for the IMG activities, which in the case of the example is an 'IMG Project':

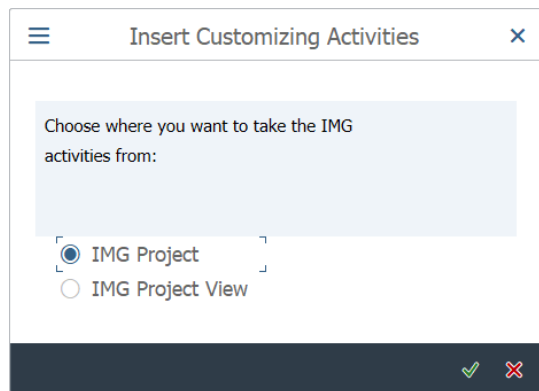


Figure 3.58. Available options to insert customizing activities.

Select the previously created project:

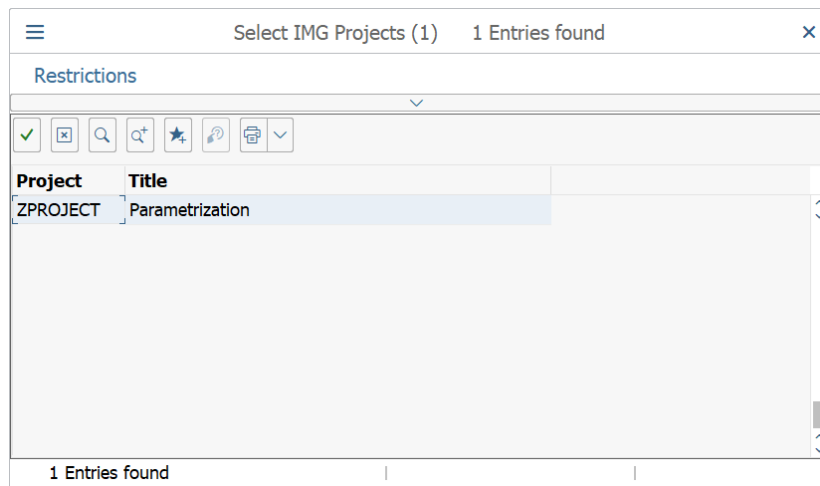


Figure 3.59. IMG Projects selection window.

By performing this action, the transactions contained in the previously selected nodes are automatically added to the role:

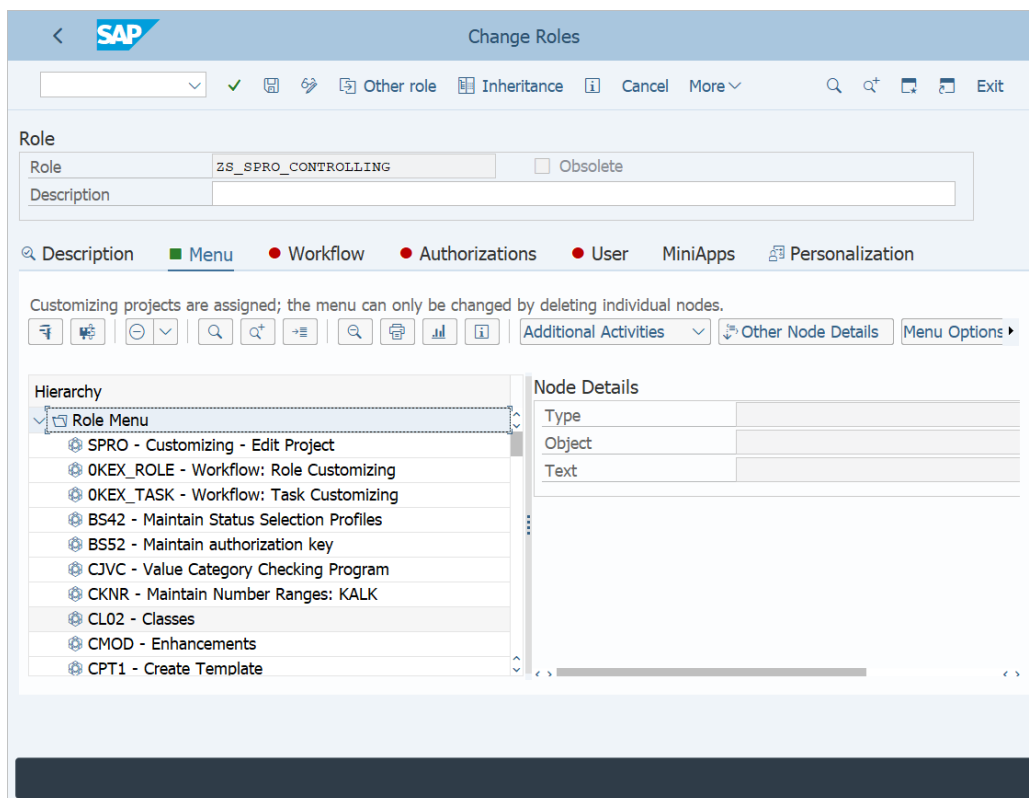


Figure 3.60. Transaction added to a customizing role.

Finally, the authorizations must be maintained, and the role profile generated in the usual way.

3 Role Maintenance (PFCG)

Caution: If a project or project view has been assigned to a role, it will no longer be possible to manually add transactions to this role. This means that the role can only be used to generate and assign Customizing authorizations. Similarly, a role to which transactions have been manually assigned cannot be used for Customizing authorizations.

4. Tools for authorization analysis

In the day-to-day life of an SAP system administrator, there may be situations in which a user receives authorization error messages when trying to execute a transaction, or during the execution of it. For these cases, there are mechanisms to determine the necessary authorizations:

1. Authorization error analysis, transaction SU53.
2. System trace, transaction ST01 or STAUTHTRACE.

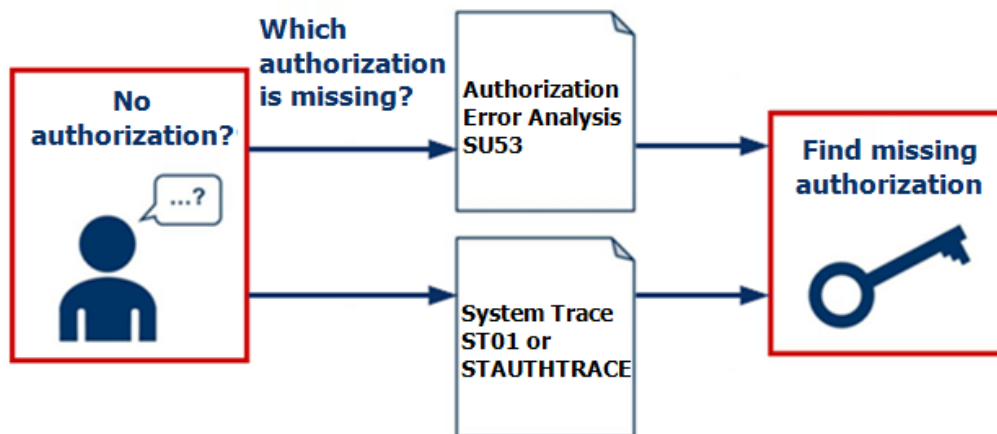


Figure 4.1. Authorization error analysis diagram.

There is also the possibility that it is necessary to analyze the transactions that a user has executed during a certain period of time, or the failures in the initiation of transactions or access to the system. In this case, you can use:

1. Workload monitor, transaction ST03N.
2. Audit log, transaction SM20.

4.1. Authorization error analysis (SU53)

Transaction SU53 can be used to analyze an unauthorized access error that just occurred in the system. This transaction shows the last **failed** authorization check and the authorizations the user has in their authorization buffer.

To execute transaction SU53, you can access the menu path System → Utilities → View authorization verification, or enter the transaction code SU53 in the command field.

Imagine that a user receives the following message when executing transaction FD02 (Change Customer):

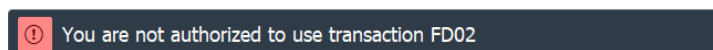


Figure 4.2. Authorization error message.

The user then enters the transaction code /NSU53 in the command field, and executes it. The system displays the failed authorization checks, the most recent being the one that likely caused the error:

Description		Authorization values
User Name	JOHNDOE	Failed checks since 18.04.2020 09:06:15
System	SAP	Client 100
Date	18.04.2020	Time 18:06:15
Instance	SAP_00	Profile Parameter auth/new buffering 4

⚠ Authorization check failed		
Date 18.04.2020 Time 12:06:13 Transaction SESSION_MANAGER		
Authorization Obj. F_KNAP_APP Customer: Application Authorization		
Authorization Field ACTVT	Activity	02
Authorization Field APPKZ	Customer and Vendor Master Data Application Authorization	F
Authorization Obj. S_TCODE Transaction Code Check at Transaction Start		
Authorization Field TCD	Transaction Code	PFCG
User's Authorization Data JOHNDOE		
Authorization Object S_TCODE Transaction Code Check at Transaction Start		
Authorization Object F_KNAP_APP Customer: Application Authorization		
Authorization. T-E855185500		
Prof. T-E8551855 Profile for role Z_CUSTOMERS		
Role Z_CUSTOMERS		
Authorization Field ACTVT	Activity	03
Authorization Field APPKZ	Customer and Vendor Master Data Application Authorization	F

Figure 4.3. Transaction SU53.

It is important to always keep in mind that the SAP system is constantly performing authorization checks, and not everything that transaction SU53 shows may be related to the error being dealt with. For this reason, it must be considered whether the **context** of the error and the context of the authorization objects that appear in SU53 match. In the example, and as can be seen in Figure 4.3, there have been two failed authorization checks. The first refers to the authorization object S_TCODE with the value PFCG, does this mean that the user needs to have access to PFCG transaction in order to execute FD02 transaction? Obviously not. In this case, the system has verified whether the user has access to the PFCG transaction because in the initial SAP screen, in the top menu there is a direct access to the PFCG transaction, which will appear or not depending on whether the user has access to transaction PFCG:

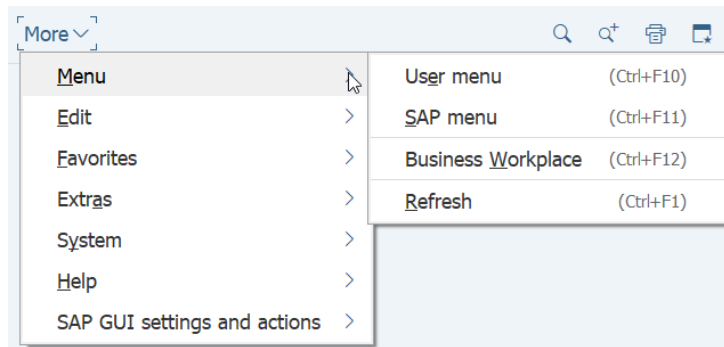


Figure 4.4. Menu displayed when user does not have access to PFCG transaction.

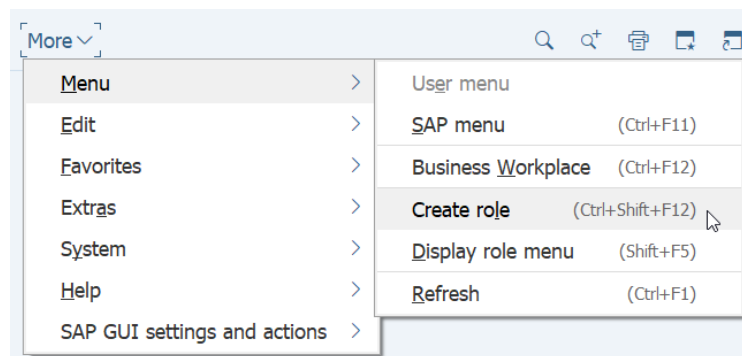


Figure 4.5. Menu displayed when user does have access to PFCG transaction.

Because the user tried to execute transaction FD02 just after logging in, the two authorization checks appear with very little time spacing between them. If the context is not taken into account, authorizations that the user does not need could be granted, resulting in unnecessary over-access.

Continuing with the example, transaction SU53 shows in the upper part of the screen the value of the object that the program required and, in case of having the object in its user master record, in the lower part of the screen it shows the value that has and through what profile and what role. In this case, the authorization object that the system is verifying when executing transaction FD02 is F_KNA1_APP, which the user does have in his buffer, but instead of the required activity "02" (Change), the user only is authorized for activity "03" (Display), and that authorization is being granted through role Z_CUSTOMERS.

Transaction SU53 shows a maximum of 100 failed authorization checks for each user, for the last three hours at most. If there are many active users and many failed authorization checks, the number of checks and the period covered may also be less for each user. In addition, it also shows the context in which the verification was performed (that is, the transaction, the RFC

function module, or the service). In the lower area, user authorizations are displayed for all authorization objects displayed at the top.

When executing transaction SU53, the system shows your own authorization data and failed verifications, but it is also possible to access the data of other users, as long as one has permissions to do so. To change user, click on the following button:



Figure 4.6. How to select different user in SU53 transaction.

Additionally, an important aspect at the system architecture level must also be considered, and that is that systems can be made up of one or more server application instances, and authorization verifications occur in the application server in which the user is currently logged in. For this reason, you must take into account how many servers the system you are on has, and always confirm if the analysis is being carried out on the same server where the user was connected at the time of the failure. To view how many servers the system has, and to access any of them, transaction SM51 can be used:

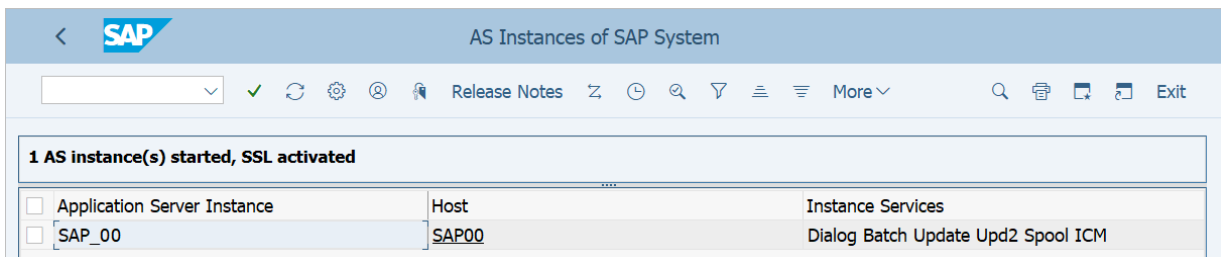


Figure 4.7. Transaction SM51.

4.2. System Trace (ST01 or STAUTHTRACE)

If you want to record the internal activities of SAP, you must use the system trace, which can be accessed through transaction ST01.

Through the system trace, the following components can be monitored:

- Authorizations.
- Kernel functions.
- Kernel modules.
- Access to Databases (SQL trace).
- Table buffers.
- RFCs, HTTP, APC or AMC calls.

- Lock operations.

To make use of the trace, it must first be activated, selecting the components to be monitored. The steps are the following:

1. Mark the components of the trace that are of interest, which in general will only be the authorization checks:

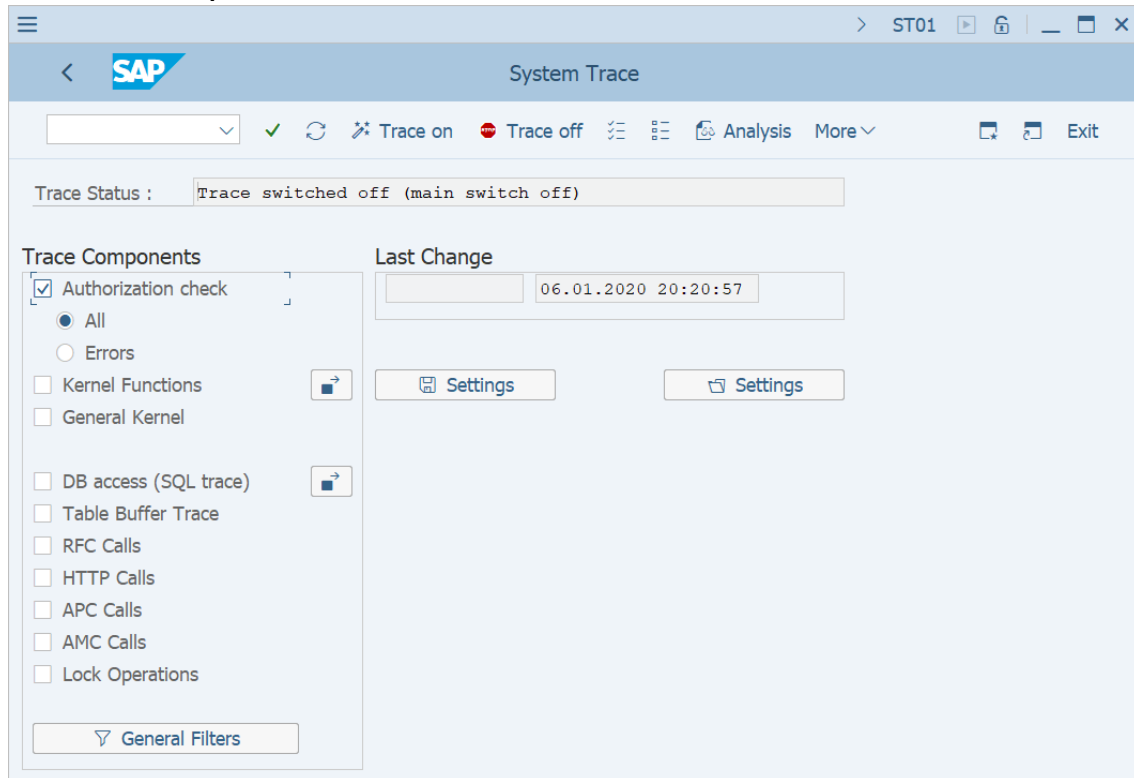


Figure 4.8. Transaction ST01.

Additionally, a filter can be added to the trace so that it only monitors a particular process, user, transaction or program. To do this, you must click on the button .

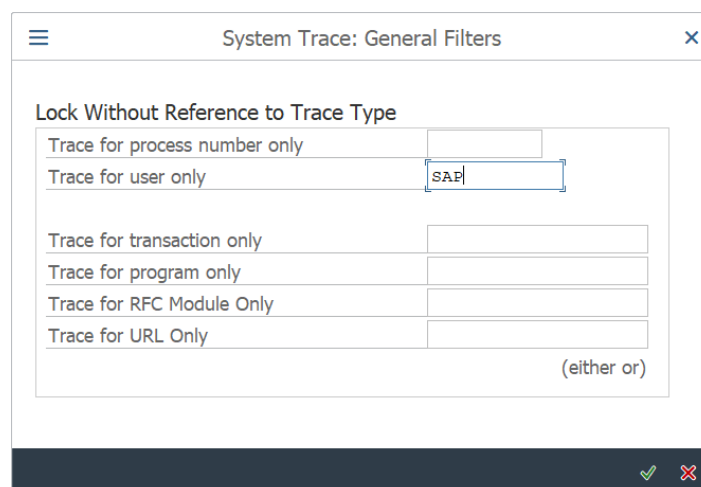

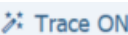
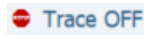


Figure 4.9. General filters in transaction ST01.

2. Once the desired filters have been established, click on the button .
3. From the main window, click on the button  to activate the trace. If you need to disable it, click on the button . Once the trace is activated, it will monitor all the components that have been selected, taking into account the configured filters.

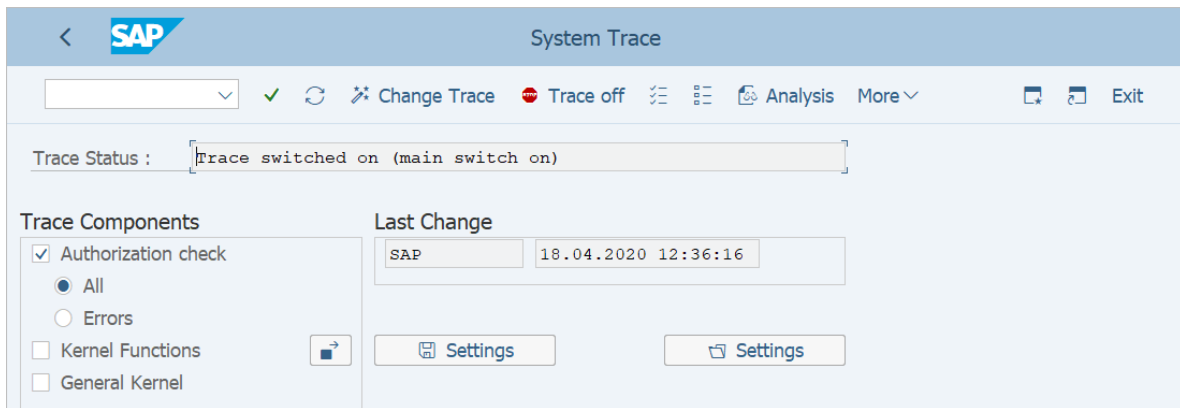


Figure 4.10. System Trace switched on.

4. To see the results of the trace, click on the button .

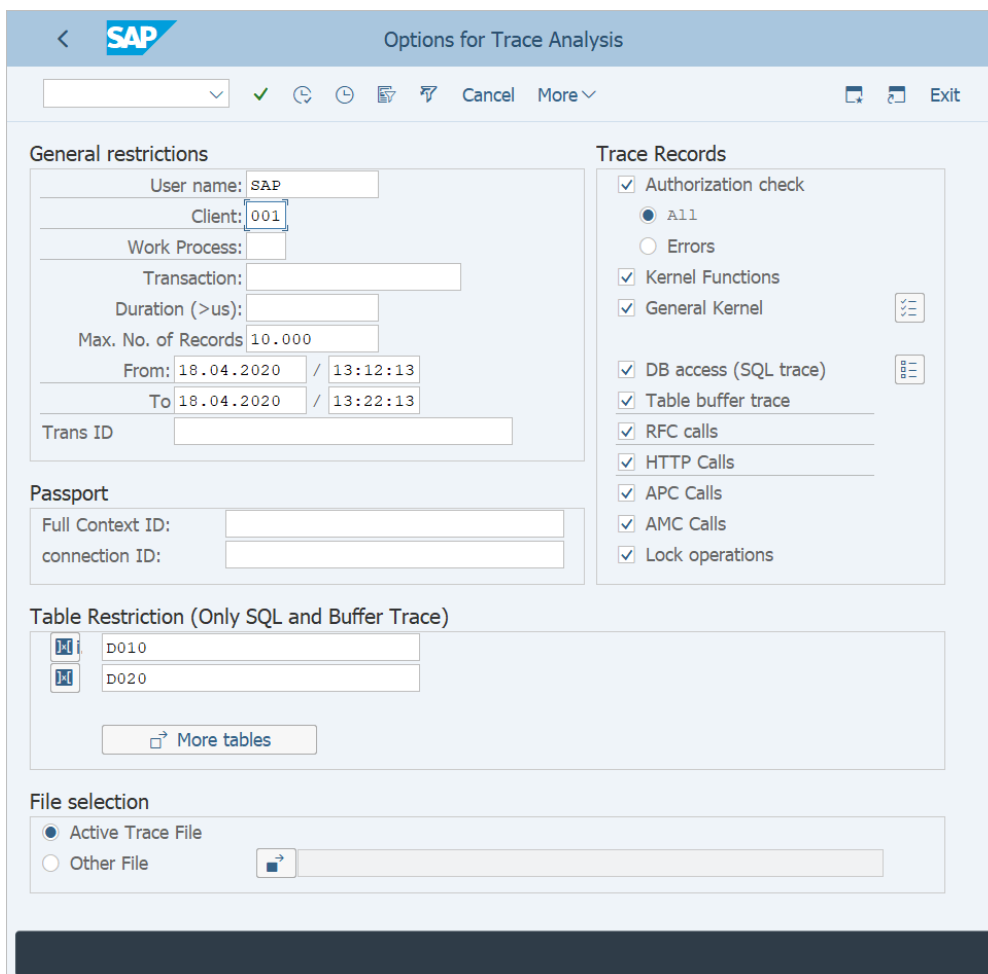

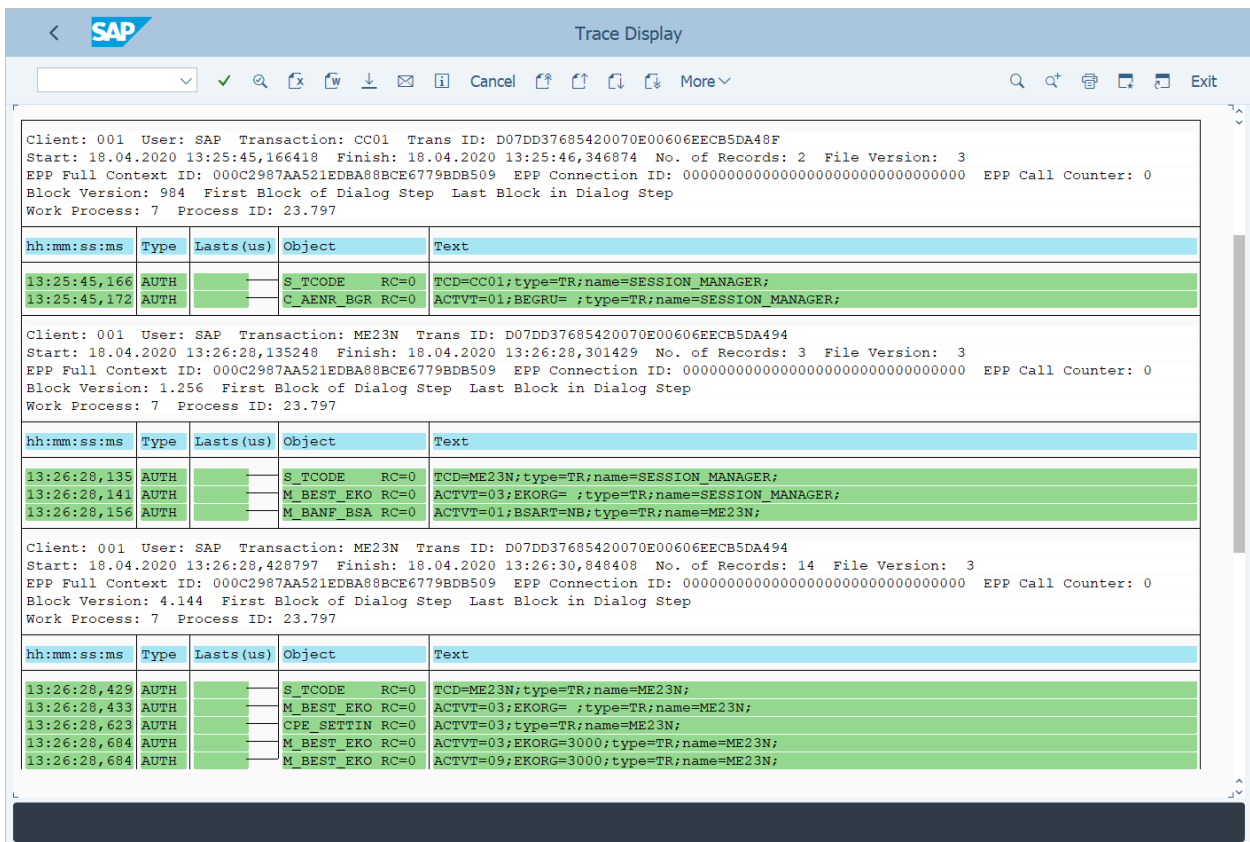


Figure 4.11. Options available for trace analysis.

5. In the next window (see Figure 4.11), you can configure a filter for the results, choosing for example the user for whom you want to see the results, or the transaction in question. If you need to perform the evaluation for all users, you can write a * in the 'User name' field, or leave the field empty, taking into account the filter that was established when activating the trace. Once the filter has been chosen, click on the button .
6. Next, a window with the results is displayed.



The screenshot shows the SAP Trace Display window with three distinct trace entries. Each entry includes client, user, transaction, and process information, followed by a table of authorization events. The events are categorized by time (hh:mm:ss.ms), type (AUTH), duration (Lasts(us)), object, and text (containing TCD, ACTVT, and EKORG values).

hh:mm:ss.ms	Type	Lasts(us)	Object	Text
13:25:45,166	AUTH		S_TCODE RC=0	TCD=CC01;type=TR;name=SESSION_MANAGER;
13:25:45,172	AUTH		C_AENR_BGR RC=0	ACTVT=01;BEGRU= ;type=TR;name=SESSION_MANAGER;
13:26:28,135	AUTH		S_TCODE RC=0	TCD=ME23N;type=TR;name=SESSION_MANAGER;
13:26:28,141	AUTH		M_BEST_EKO RC=0	ACTVT=03;EKORG= ;type=TR;name=SESSION_MANAGER;
13:26:28,156	AUTH		M_BANF_BSA RC=0	ACTVT=01;BSART=NB;type=TR;name=ME23N;
13:26:28,429	AUTH		S_TCODE RC=0	TCD=ME23N;type=TR;name=ME23N;
13:26:28,433	AUTH		M_BEST_EKO RC=0	ACTVT=03;EKORG= ;type=TR;name=ME23N;
13:26:28,623	AUTH		CPE_SETTIN RC=0	ACTVT=03;type=TR;name=ME23N;
13:26:28,684	AUTH		M_BEST_EKO RC=0	ACTVT=03;EKORG=3000;type=TR;name=ME23N;
13:26:28,684	AUTH		M_BEST_EKO RC=0	ACTVT=09;EKORG=3000;type=TR;name=ME23N;

Figure 4.12. Trace display window.

The Type column indicates the component, which in this case is authorization verification (AUTH). The object column shows the object that has been verified by the system, and in the text field you can see which values have been verified for the authorization fields. One of the most important elements of the trace is the Return Code, which can be found in the Object field, and can take the following values:

- RC = 0: The authorization check is successful. The user has the authorization object in his buffer, with the set of values checked.

4 Tools for authorization analysis

- RC = 4: Authorization verification failed. The user has the authorization object in their buffer, but with a different set of values than the verified ones.
- RC = 12: Authorization verification failed. The user does not have the authorization object in their buffer.
- RC = 40: The specified user does not exist.

Authorization fields that do not appear, or that have the specified DUMMY value, are not checked.

As in transaction SU53, the system trace only evaluates authorization checks on the application server where we are, so it must be taken into account when performing the analysis.

In newer versions of SAP (as of SAP_BASIS 7.00 SP26) a new transaction for authorization verification has been introduced: STAUTHTRACE. This transaction provides an optimized interface for the analysis of authorization checks. It works in the same way as the system trace (transaction ST01), however, it only evaluates authorization checks. The main advantage that this transaction introduces is that it allows activating and evaluating the trace for all the application servers of the system in a centralized way.

In a similar way as with transaction ST01, to make use of the trace for authorization verification, it must first be activated, but in this case it is not necessary to select any component, since by default only authorization data can be analyzed with this transaction.





The screenshot shows the SAP System Trace for Authorization Checks interface. The title bar reads "System Trace for Authorization Checks". Below the title bar, there is a navigation bar with buttons for "Evaluate", "Activate Trace", "Deactivate Trace", "System-Wide Trace", and "More". There are also icons for "Exit" and "Print".

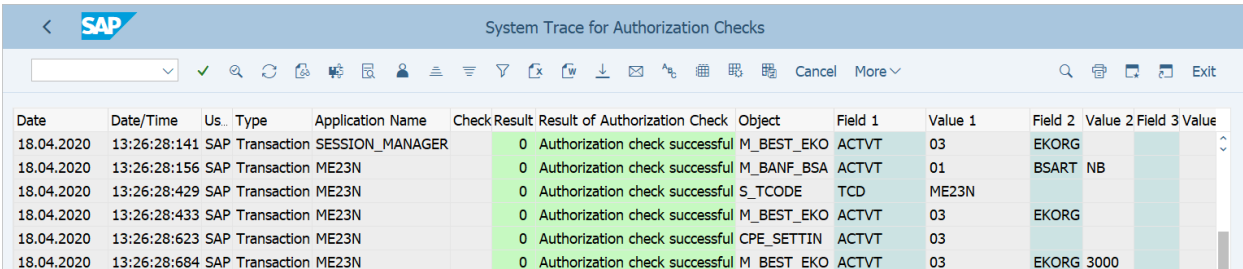
The main content area is divided into three sections:

- Trace Information:** A table showing the current trace status. The "Trace Status" is "Trace is switched off". The "Last Changed" is "SAP" on "18.04.2020" at "13:32:06". The "Server" is "SAP_00".
- Trace Options:** A section with two checkboxes: "Trace for user only" (checked) and "Trace for errors only" (unchecked).
- Restrictions for the Evaluation:** A section with several input fields and checkboxes. The "User" field is empty. The "From" field is "18.04.2020 12:31:19" and the "To" field is "18.04.2020 13:32:11". The "Type of Application" is a dropdown menu. The "Application Name" field is empty. The "Authorization Object" field is empty. The "Result" field is empty. The "Maximum Number of Records" is "10.000". There are two checkboxes: "Filter Duplicate Entries" (unchecked) and "Evaluate Extended Passport" (unchecked).

Figure 4.13. Transaction STAUTHTRACE.

In general, the steps to make use of the trace for authorizations checks are:

1. If necessary, configure the 'Trace for user only'.
2. To access the global trace for all application servers, click on the button .
3. To activate the trace, click on , and to deactivate it, click on .
4. As with transaction ST01, in the lower part of the main window you can configure a filter for the results, choosing, for example, the user for whom you want to see the results. To evaluate the trace, click on .



Date	Date/Time	Us.	Type	Application Name	Check Result	Result of Authorization Check	Object	Field 1	Value 1	Field 2	Value 2	Field 3	Value 3
18.04.2020	13:26:28:141	SAP	Transaction	SESSION_MANAGER	0	Authorization check successful	M_BEST_EKO	ACTVT	03	EKORG			
18.04.2020	13:26:28:156	SAP	Transaction	ME23N	0	Authorization check successful	M_BANF_BSA	ACTVT	01	BSART	NB		
18.04.2020	13:26:28:429	SAP	Transaction	ME23N	0	Authorization check successful	S_TCODE	TCD	ME23N				
18.04.2020	13:26:28:433	SAP	Transaction	ME23N	0	Authorization check successful	M_BEST_EKO	ACTVT	03	EKORG			
18.04.2020	13:26:28:623	SAP	Transaction	ME23N	0	Authorization check successful	CPE_SETTIN	ACTVT	03				
18.04.2020	13:26:28:684	SAP	Transaction	ME23N	0	Authorization check successful	M_BEST_EKO	ACTVT	03	EKORG	3000		

Figure 4.14. System Trace for authorization checks display window.

4.3. Workload monitor (ST03N)

This transaction can help you find out what transactions a user has executed in the last few months. To do this, the following steps must be followed:

1. From the command line enter the transaction code ST03 or ST03N².
2. In the left panel, within the 'Workload' section, select the required date range: Day, Week, Month. Statistics will appear in the right panel.
3. 'Analysis views' will appear in the lower left pane. Select 'User and settlement statistics', and then 'User profile'.
4. A screen like the following will be displayed:

² Transactions ending in N are known as *enjoy* transactions, which generally have a much more user-friendly appearance than their counterpart without the N, can support custom controls, and have improved structures.

4 Tools for authorization analysis

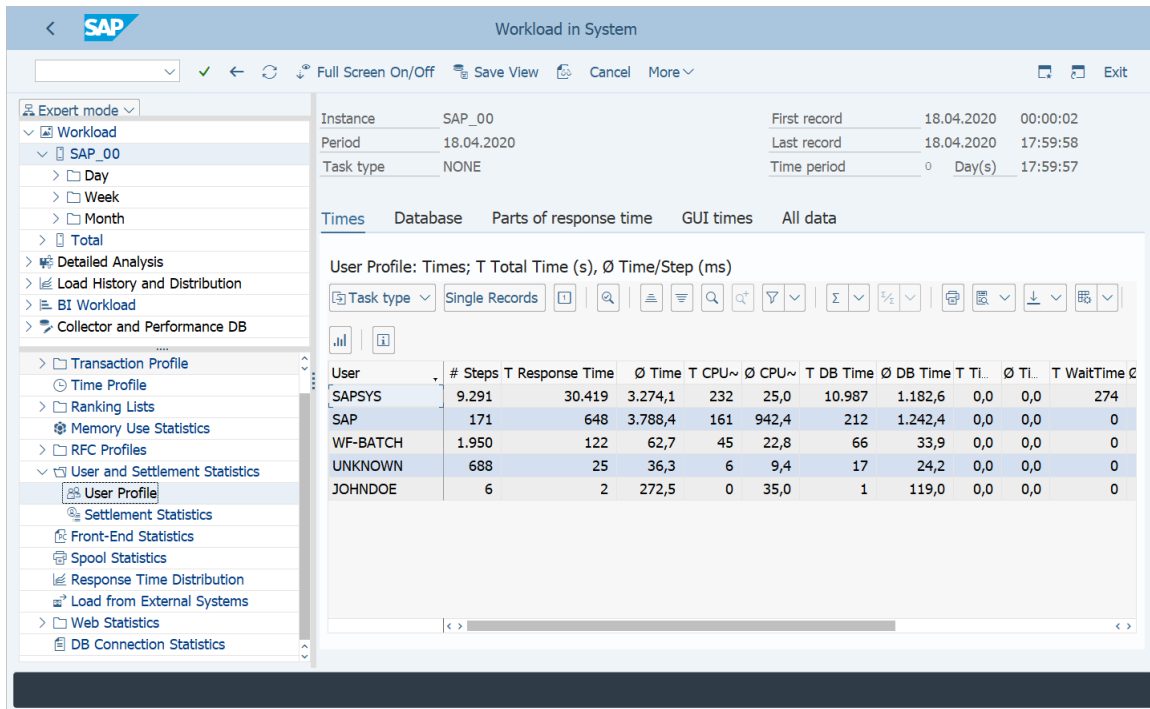


Figure 4.15. Transaction ST03N.

5. By clicking on any user, the transactions executed by the same appear.

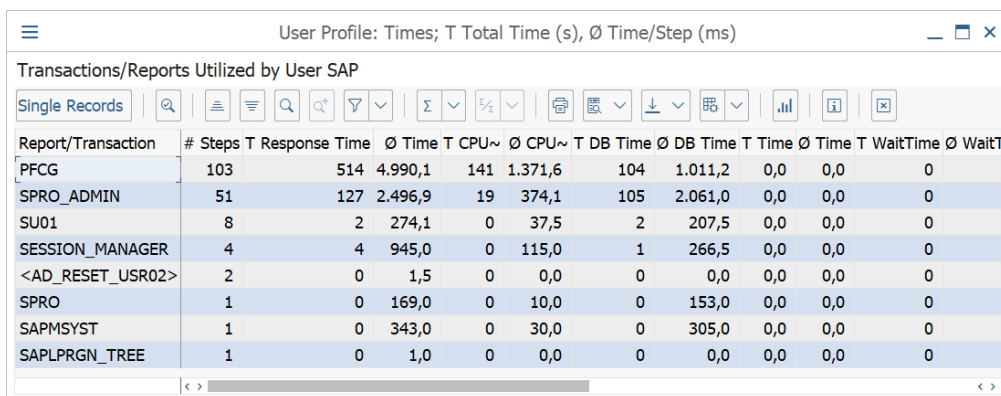


Figure 4.16. Transactions/reports executed by user.

4.4. Audit log (SM20 or RSAU_READ_LOG)

The audit log is a tool that can provide details of what happens in SAP systems. Similar to the system trace, the audit log must be activated and configured beforehand, before the results can be evaluated. Normally, the trace is activated in a timely manner, and the audit log is always activate.

To configure and activate the audit log, transaction SM19 or RSAU_CONFIG must be used:

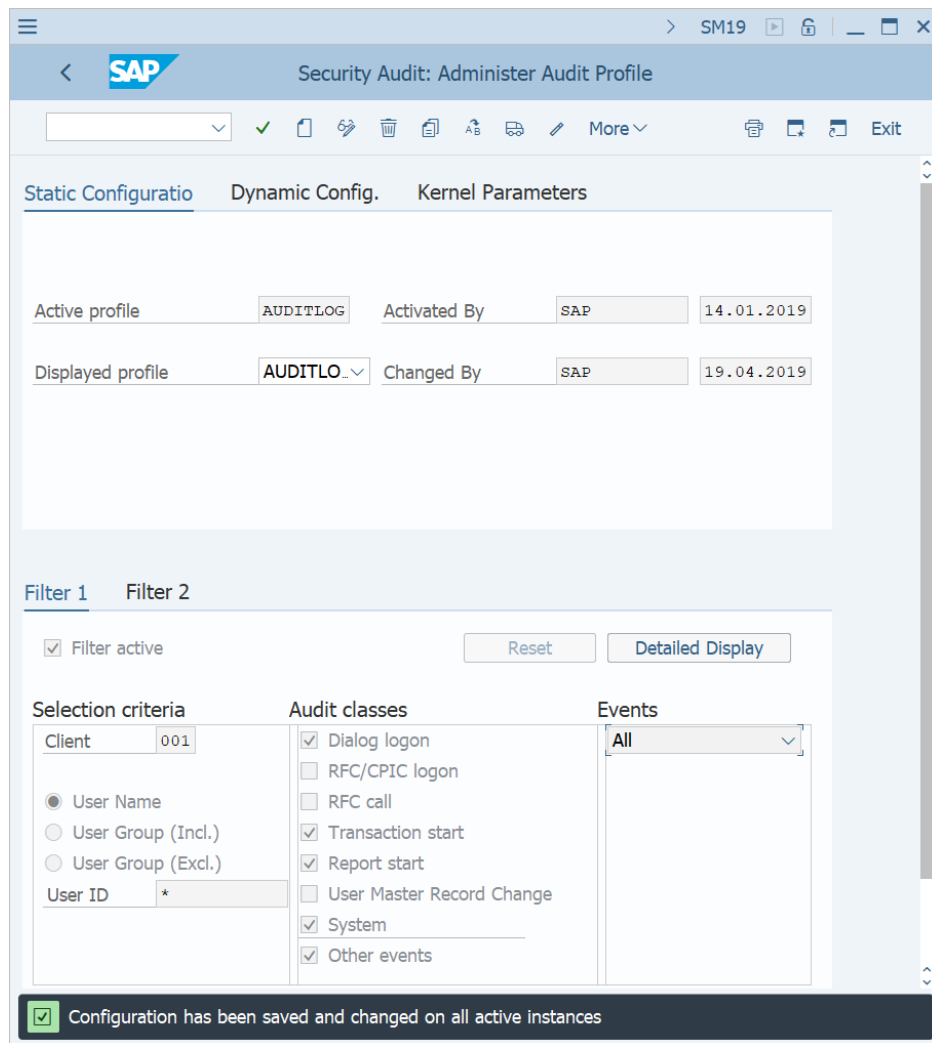



Figure 4.17. Transaction SM19.

An advantage of the audit log over the trace is that it allows you to monitor all the application servers in the system. To do this, the log must be configured from the tab **Dynamic Config.**

When this log is activated, the system records the activities that have been selected in the 'Audit classes' section. To edit the Filter, click on the button . The events that the audit log can collect are:

- Attempts to access the system, whether unsuccessful or successful.
- Access to the system through RFC connections.
- Calls to RFC functions.
- Failed or successful starts of transactions and reports.
- Modifications in the user master.
- Changes in system configuration.



Once you have finished configuring the filter, click on the button  to save it. In addition, you must make sure that the profile is active, and if it is not, you must click on the button  to activate it.

Figure 4.18. Audit log filter.

When an event occurs that corresponds to one of the active filter classes (the start of a transaction, for example), the audit log will generate the corresponding record and write it to the audit file. SAP does not delete or overwrite the audit files from previous days, but it is possible to delete them manually. These files are located on each application server, and their name and location can be defined with the "rsau/local/file" system parameter. The maximum size that this file can reach is defined with the parameter "rsau/ma_diskspace/local", which by default is 1000000 bytes (= 1 MB). If this limit is reached the audit process stops.

To view and evaluate the audit log, transaction SM20 or RSAU_READ_LOG must be used:

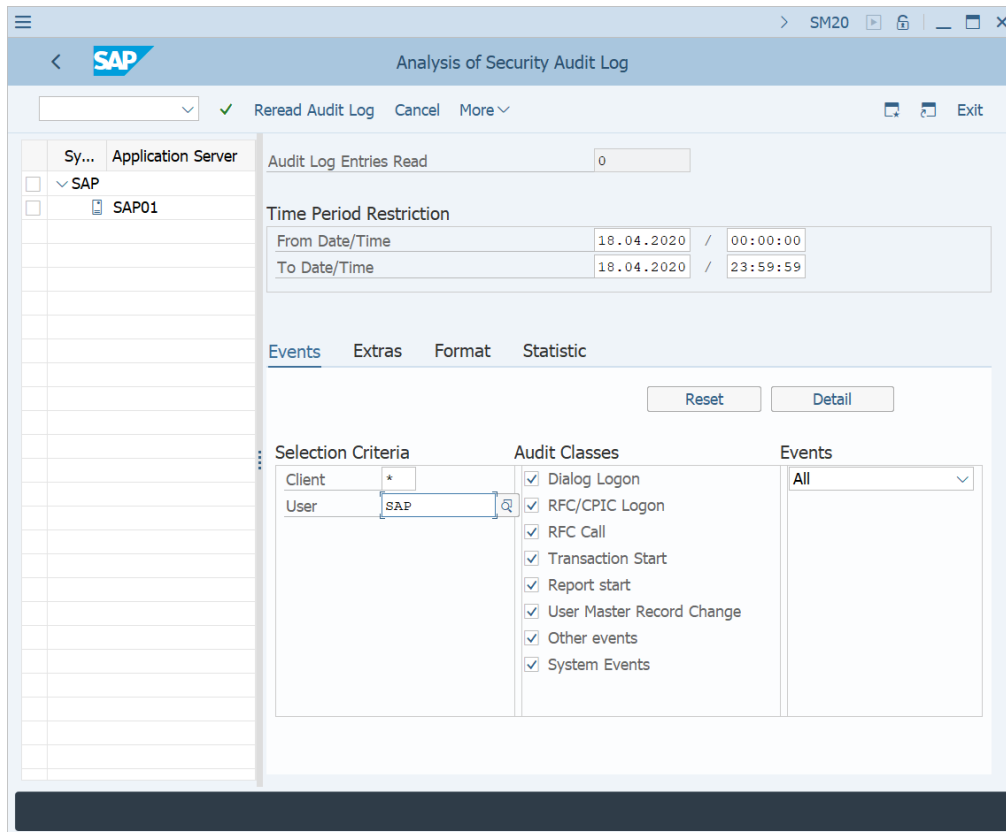


Figure 4.19. Transaction SM20.

Next, select the Classes needed, and if necessary, the client and the user. Once the filter data has been selected, click on the button **Reread Audit Log**, so that the system displays a window with the relevant data, together with the date, time and name of the terminal (see Figure 4.20):

Creation Date	Data/Time	Cl.	User	Terminal	Transaction Code	Program	Audit Log Msg. Text	Long Text Proc.	WP	variable data	Data	Data Data
01/06/2020	06:12:38	001	SAP	S0030910	SESSION_MANAGER	SAPMSYST	Logon successful (type=A, method=P)	D	016	A	0	P
01/06/2020	06:12:45	001	SAP	S0030910	SESSION_MANAGER	SAPMSYST	Password changed for user SAP in client 001	D	016	001		SAP
01/06/2020	06:12:47	001	SAP	S0030910	SESSION_MANAGER	RSRZLLG0	Report RSRZLLG0 started	D	016	RSRZLLG0		
01/06/2020	06:12:47	001	SAP	S0030910	SESSION_MANAGER	RSRZLLG0_ACTUAL	Report RSRZLLG0_ACTUAL started	D	016	RSRZLLG0_ACTUAL		
01/06/2020	06:12:48	001	SAP	S0030910	SESSION_MANAGER	SAPMSYST	Transaction SESSION_MANAGER started.	D	016	SESSION_MANAGER		
01/06/2020	06:13:06	001	SAP	S0030910	STAUTHTRACE	SAPLSMTR_NAVIGATION	Transaction STAUTHTRACE started.	D	017	STAUTHTRACE		
01/06/2020	06:13:56	001	SAP	S0030910	ME23N	SAPLSMTR_NAVIGATION	Transaction ME23N started.	D	016	ME23N		
01/06/2020	06:13:56	001	SAP	S0030910	ME23N	RM_MEPO_GUI	Report RM_MEPO_GUI started	D	016	RM_MEPO_GUI		
01/06/2020	06:25:37	001	SAP	S0030910	XK01	SAPLSMTR_NAVIGATION	Start of transaction XK01 failed (Reason=6)	D	015	XK01	6	

Figure 4.20. Audit log analysis.

5. User information system (SUIM)

Generally speaking, if you want to correct an authorization error, it is not recommended to create new roles immediately with the result obtained from evaluating the system trace or transaction SU53. It is much more interesting and efficient to first analyze the system in search of existing roles in which the necessary authorizations can be added. The information system can be used for this purpose.

You can use the user information system to obtain an overview of the authorizations and users of the SAP system at any time using the search criteria you want. For example, lists of users with authorizations classified as assigned critical can be obtained. You can also use the User Information System to:

- Compare roles and users.
- Show change documents for a user's authorization profile.
- Show the transactions contained in a role.
- Create usage lists.

It is advisable to regularly check the various lists that are considered relevant, and for this, monitoring and verification procedures must be defined to ensure that the authorization plan is continuously reviewed, and especially, determine which authorizations are considered critical and periodically review which users have these authorizations.

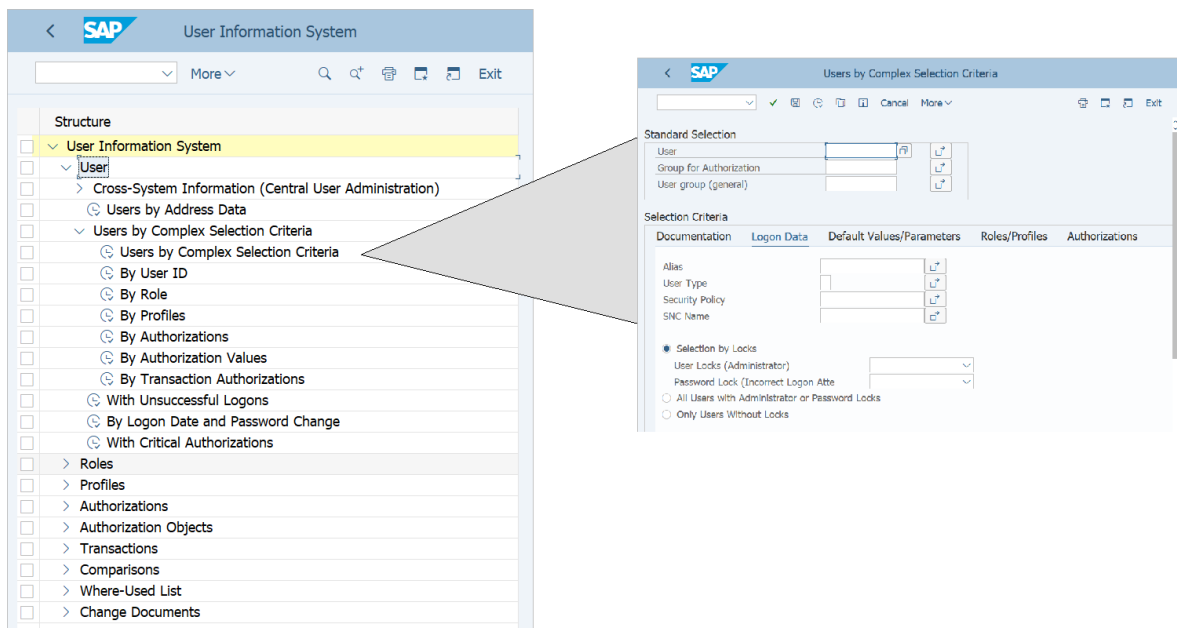


Figure 5.1. User Information System.

To start the Information System from the SAP menu, navigate to Tools → Administration → User Maintenance → Information System. The Information System can also be accessed from the User Maintenance transaction (SU01) by selecting the menu path Information → Information System. Another option is to run SUIM transaction directly. From here you can search for elements of the authorization system using different selection criteria.

The Information System and parts of the Information System can also be run as executable reports using transaction SA38. Here are some examples:

- RSUSR002: Users by complex selection criteria.
- RSUSR008_009_NEW: List of users with critical authorizations.
- RSUSR020: Profiles by complex selection criteria.
- RSUSR030: Authorizations by complex selection criteria.
- RSUSR040: Authorization objects by complex selection criteria.
- RSUSR070: Roles by complex selection criteria.
- RSUSR100N: Document of changes for users.
- RSUSR101: Document of changes for profiles.

More detailed analyzes can also be started using reports:

- RSUSR003: Standard user password verification in all clients.
- RSUSR200: List of users by password change and login data.

6. Special authorization profiles

There are a few special roles and profiles, which contain critical authorizations that must be protected.

6.1. SAP_ALL authorization profile

This composite profile contains almost all SAP authorizations, which means that a user with this profile can perform almost all tasks in the SAP system. There are certain very particular authorizations that are not included in this profile, such as the Trusted RFC authorizations (authorization object S_RFCACL).

Therefore, no user should be assigned this authorization profile. It is recommended to create only one user with this profile, keep this user's password secret and use it only in case of emergency.

Instead of using the SAP_ALL profile, the corresponding authorizations must be assigned to each position. For example, instead of assigning the system administrator (or superuser) the SAP_ALL profile, only the authorizations that apply to the administration of the system should be assigned, that is, those that grant him sufficient rights to administer the entire SAP system, without allow you to perform tasks in other areas such as Human Resources, for example.

It is possible to generate the SAP_ALL profile using report RSUSR406 or transaction SU21, which will generate the profile only in the client where the report is run. To generate the SAP_ALL profile in all the clients you can use the report AGR_REGENERATE_SAP_ALL.

6.2. SAP_NEW authorization profile

When an SAP system is updated, new authorization checks may appear on transactions that were already in use by users. These users will need the new authorizations to continue using the functions they have used up to now. The authorization profile SAP_NEW was created for this purpose, to bridge the differences in authorization checks between versions while preparing the upgrade and adjusting the roles. Therefore, SAP_NEW allows business processes to continue to function until the new authorization checks have been incorporated into the authorization concept.

The authorizations contained in the SAP_NEW profile are linked to the SAP_BASIS software component, so it only makes sense to use it if you are updating that component. Also, SAP_NEW should never be necessary in productive systems, and it is not necessary to assign SAP_NEW if the user already has SAP_ALL.

Starting with version 700 of the SAP_BASIS component, the authorization profile SAP_NEW has been replaced by a generated role called SAP_NEW. To generate this role, the REGENERATE_SAP_NEW report must be used. Basically, the old SAP_NEW authorization profile and the new SAP_NEW role serve the same purpose and are based on similar data.

Once the functionality of the SAP_NEW profile/role has been explained, it must be understood that, currently, the procedure to follow during a system update is to use transaction SU25 to add to the role model the new authorizations arising from the update itself. Normally, the SAP security team will be in charge of executing SU25 transaction and adjusting the roles including the necessary new authorizations, so it only makes sense to use the SAP_NEW role while the adjustment is being made; once the setting is complete, no user should have this role or profile assigned.

6.3. SAP_APP authorization profile

The SAP_APP profile contains all the authorizations for the applications. This profile is not created by default, but can be generated with the REGENERATE_SAP_APP report. When executing this report, you have the option of including authorizations from the Basis and Human Resources area, thus being able to exclude them. In addition, it is possible to generate it as a profile, or as a role. SAP_APP is intended for testing and development purposes, where the need to assign wide-ranging authorizations may arise. This role/profile should not be used in production environments.

6.4. Other profiles

Below are other profiles that are also interesting to know:

- S_A.DEVELOP - Authorizations for developers
- S_A.SYSTEM - Authorizations for system administrators
- S_USER_ALL - All authorizations for user maintenance and authorizations.

7. Relevant tables

Data stored in the system database tables can be viewed using transactions SE16 or SE16N:

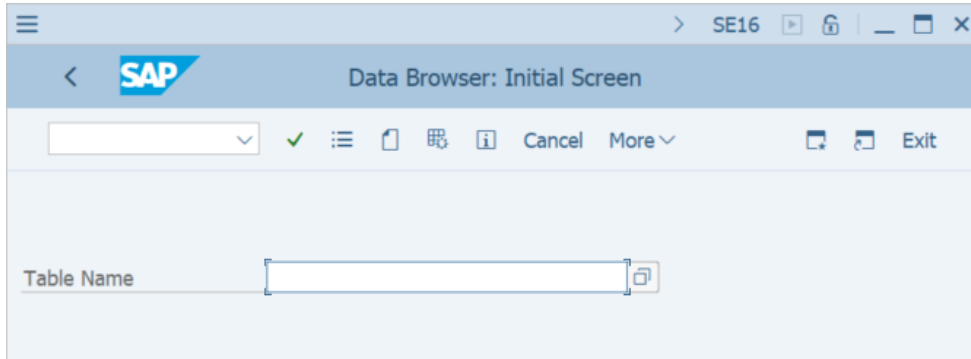


Figure 7.1. Transaction SE16.

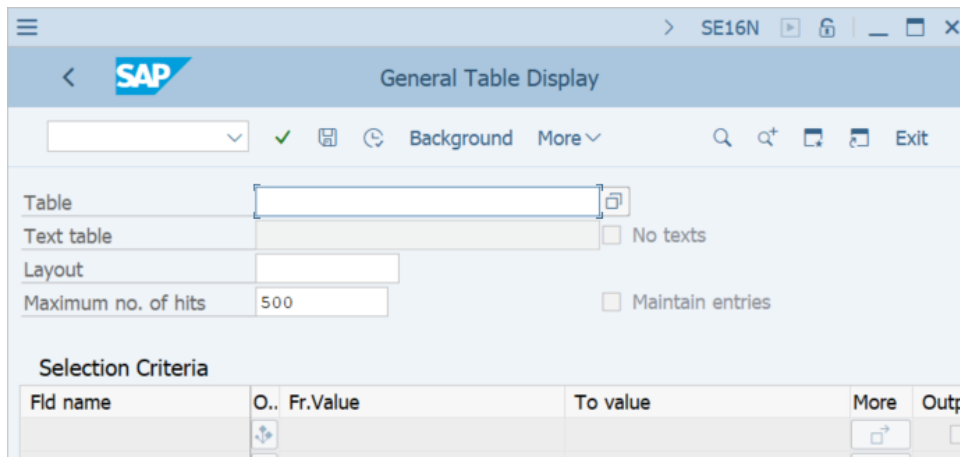


Figure 7.2. Transaction SE16N.

Some of the tables that may be interesting in the day-to-day maintenance of users and authorizations are described below.

7.1. User tables

These tables can be useful when you need to extract reports from system users.

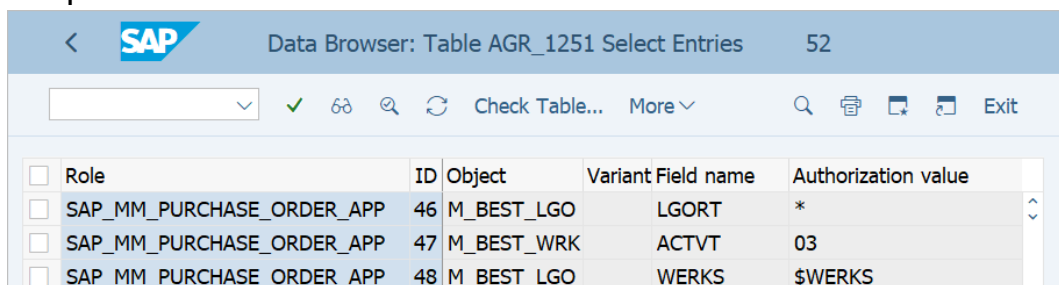
- **USR02 - Access data:** In this table you can find data related to access, such as the validity dates, the type of user, the user group, the last access date, or if the user is locked and the reason.

- **USER_ADDRS - Address data:** In this table you can find data related to the Address tab of the user master, such as the Name and Last Name fields.

7.2. Roles and authorization tables

These tables can be of help to carry out exhaustive analysis of roles, the authorizations they contain, and the users assigned to them.

- **AGR_1251 - Authorization data:** In this table you can find the relationship between roles and the values of the authorization objects they contain, with the exception of the values of the organizational levels, which will appear coded as a parameter, with the \$ symbol as a prefix.



Role	ID	Object	Variant Field name	Authorization value
SAP_MM_PURCHASE_ORDER_APP	46	M_BEST_LGO	LGORT	*
SAP_MM_PURCHASE_ORDER_APP	47	M_BEST_WRK	ACTVT	03
SAP_MM_PURCHASE_ORDER_APP	48	M_BEST_LGO	WERKS	\$WERKS

Figure 7.3. Table AGR_1251.

- **AGR_1252 - Organizational levels for authorizations:** In this table you can find the relationship between roles and the values of the organizational levels they contain, which can not be seen in the AGR_1251 table.
- **AGR_TCODES - Role Assignment for Transaction Codes:** It allows knowing the transactions that a role contains through the role menu.
- **AGR_AGRS - Roles in Composite Roles:** In this table you can find the relationship between single roles and composite roles, or what is the same, in which composite roles is a certain single role, or which single roles contains a composite role.
- **AGR_DEFINE - Roles definition:** This table allows you to see the short description of any role, and the relationship between master roles and derived roles in case of inheritance.
- **AGR_USERS - Assign roles to users:** In this table you can find the relationship between roles and users, that is, which roles are assigned

the users that are entered as input values, or vice versa, which users are assigned a certain role.

- **USVART - Possible Authorization Scopes as Variables:** In this table you can see the descriptions of the organizational levels.

SAP SECURITY

FROM SCRATCH

Powered by
udemy

Acquire the skills and knowledge necessary to design, implement, and manage robust security solutions for SAP systems. Whether you are new to SAP security or seeking to enhance your expertise, this course will empower you with the tools and techniques needed to safeguard your organization's SAP environment effectively.

REGISTER NOW



iThis is just the start,
you will find more in
[erpsecurity.training!](https://erpsecurity.training)

You can also find us in



ERP  **ecurity Training**