SAP PRESS

SAP® System Security

- Configure and maintain application, database, platform, and infrastructure security
- Set up identity and access management with user accounts, authorizations, and authentication
- Secure SAP S/4HANA, SAP Fiori, and cloud solutions

Pradeep Kumar Mishra

Rheinwerk Publishing

Contents

PART IV Infrastructure-Level Security

Chapter 1
User Management

You may have heard the saying: Identity is the new perimeter. This chapter explores how SAP user management defines that perimeter and protects the integrity of your business operations.

The primary objective of security for an organization using SAP is to protect its data and business processes from unauthorized access and use. That, in turn, makes the processes for securing user accounts, roles, and authorizations critical business processes. *User management* encompasses the processes and controls that ensure the security of SAP user accounts throughout their entire lifecycle, from creation to suspension, and ultimately to deletion or termination.

To use SAP functionalities, a user needs a user account or a user ID with the appropriate authorization to perform the intended tasks within the SAP environment. Managing these user accounts is one of the critical activities carried out by SAP security professionals. When SAP is installed in an organization, some user accounts are automatically created. Such user accounts are referred to as *standard accounts*, and they typically use well-known passwords. The installation team logs in with these IDs and changes their passwords to secure them. These IDs are then used to create user accounts for other users, such as the SAP security team, who take the onus of managing user accounts.

The three pillars of user management are identity lifecycle management, authentication, and authorization. *Identity lifecycle management* governs user IDs from their creation to termination. *Authentication* verifies user identity to ensure that the user account is used by the individual for whom it is intended. *Authorization* determines the actions a user of an SAP account can perform based on their assigned business functions. This chapter deals with user account lifecycle management, and we'll dive into authorization in Chapter 3.

The persistent set of user account data, such as logon data, user type, roles/profiles, parameters, and validity, is called *user master data*. The runtime authorization data loaded into an application server session derived from all the profiles assigned to the user is called the *user buffer*. The user buffer can be viewed using Transaction SU56. The SAP authorization concept requires that each authorization be explicitly mentioned in the user master to allow respective users to utilize the functionality referred to by the authorization. SAP accounts are *client-dependent*, meaning that a user account created in a client exists only within that client. SAP system clients and their security are dealt with in Chapter 5. User accounts are stored in table `USR02` and other `USR` tables, which can be viewed using a table viewing transaction code, such as Transactions SE16 or SM30.

In this chapter, we'll dive into these concepts in detail, starting with SAP user IDs and managing accounts before moving through password security, user information management, and more.

1.1 Types of SAP User IDs

The purpose of all user accounts is not the same. Some are designed for dialog use; some work in the background to perform routine system maintenance tasks; and some are used for communication among SAP systems. SAP has five different types of user accounts, each with various attributes to suit the class of tasks for which they are created: dialog, service, system, communication, and reference. This section covers the various types of user accounts and their associated attributes.

User accounts vary in many different aspects and have been created to meet specific requirements. When creating a user account in SAP, it is essential to understand its purpose and choose the user type that best suits that purpose.

A user's user type can be seen in Transactions SU01 or SU01D. After executing the transaction, enter the user ID of the account in the **User** field. In the following screen, click the **Logon Data** tab, as shown in Figure 1.1. The **User Type** field defines the type of user.

Figure 1.1: Viewing User Type in Transaction SU01

The user type can also be viewed in the user tables, like `USR02`, via a data browser transaction like Transactions SE16, SE16N, or SM30.

Let's take a closer look at all five user types:

- **Dialog user: Type A**
  This is the user account used by individual users. Dialog accounts are *interactive*, meaning they can be logged into. Users have a unique dialog account to set up accountability and maintain licensing compliance. SAP transactions can be executed using SAP GUI or other interfaces, such as SAP Fiori tiles or SAP Business Client. Dialog accounts don't allow multiple logons. If a dialog account is set for password login, the system checks

each time it logs in whether the password has expired or is invalid. If so, it asks the user to set up a new password with appropriate complexity. Dialog accounts can also be logged into using single sign-on (SSO) mechanisms (see Chapter 2).

- **System user: Type B**
  System user accounts are created for system-related background activities, such as running background processes and workflows. Dialog login to the SAP interfaces is not possible. Although their passwords are subject to defined complexity, these accounts do not expire. The initial password created for a system account remains valid throughout its entire lifecycle and can only be changed by the administrator. They allow multiple logons.
- **Communication user: Type C**
  The communication user accounts are used for communication among SAP systems and non-SAP systems integrated into the SAP environment. Protocols like remote function call (RFC) or Common Programming Interface for Communications (CPIC) are used in these communications. Passwords are subject to password rules and expire, so they need to be changed periodically. Dialog login in SAP GUI is not possible, but it does allow multiple logins.
- **Service user: Type S**
  Service-type user IDs are used for generic accounts, which a group of users share. The system does not check if the password has expired for a service-type account. Dialog logon and even multiple logins are possible. However, limited authorizations are assigned to service accounts due to their shared nature. Some organizations use service-type users as firefighter accounts in SAP Access Control.
- **Reference user: Type L**
  Reference users are used to assign additional authorizations to dialog-type accounts. Reference accounts are assigned to dialog accounts. When a reference ID is assigned to a dialog ID, all the authorizations assigned to the reference user are added to the user master of the dialog user. SAP limits the number of authorization profiles that can be assigned to a dialog user to 312. One use case for reference accounts is to overcome that limitation. Some organizations use reference accounts to assign additional access to nonproduction systems. Each user inherits their production access in a nonproduction environment when systems are refreshed. If a user requires additional access in a nonproduction environment, it is assigned through reference accounts. When a dialog ID with a reference user assigned attempts to run an SAP transaction code, the SAP kernel performs an authorization check on the reference user first. If this check fails, it then checks the dialog user ID.

From a security governance standpoint, each user type maps to specific control objectives. Dialog users are mostly human; they should be subject to strong authentication requirements, least-privilege authorization, and periodic access reviews. System and communication user types are primarily for intersystem communication and automated system maintenance. Their credentials should be vaulted. Service users are mostly shared

across shared accounts, so nonrepudiation risk exists and should be mitigated through controls.

1.2 SAP Standard Accounts

As mentioned at the beginning of this chapter, a few user accounts are automatically created in the system when SAP is installed. These accounts are referred to as *standard* or *default accounts* and are used for specific purposes. They have widely known passwords, which are changed immediately to secure them.

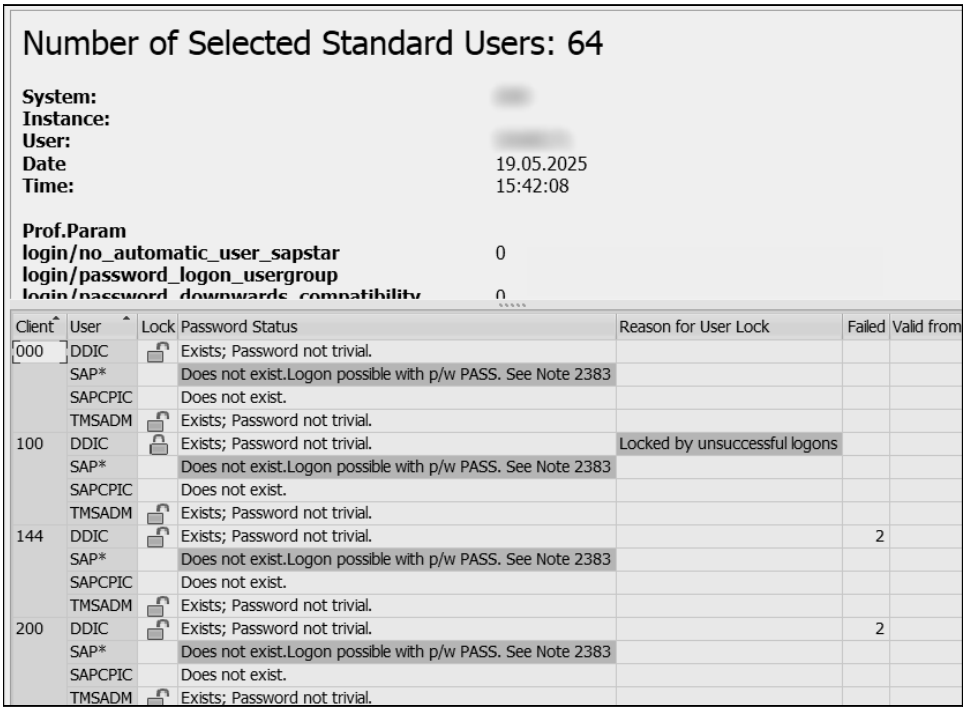
To understand the specific purpose of some default IDs, it is essential to understand SAP clients. *SAP clients* are self-contained, independent units within the system that has their master records. For example, different clients can be used for development, quality, and production environments; or within the same environment, multiple clients can be created for various business purposes. Clients have unique three-digit identities. For example, master client 000 serves as a reference, containing the standard customization settings and default configurations. We'll discuss clients in more detail in Chapter 5.

Let's walk through the SAP standard IDs:

- **`SAP*`: The SAP system super user**
  The `SAP*` ID is automatically created when a new client is created, so it exists in all clients, including 000 and 066. Its default password is `PASS`. Security best practice is to change the password immediately and lock the ID. There is a system parameter, `login/no_automatic_user_sapstar`, that has possible values of `0` and `1`. When the `SAP*` ID is deleted, the system automatically regenerates the ID if this parameter is set to a value of `0`. Hence, to secure the ID, this parameter is set to `1`.
- **`DDIC`: ABAP Dictionary and software logistics super user**
  The `DDIC` user is a privileged, default user automatically created in clients 000 and 001 after the SAP installation. Set its master password after installation. As it has vast privileges, its default password should be changed immediately, and the ID should be locked. It has authorization to maintain data dictionary objects. It is the only user allowed to log in during system upgrades.
- **`EARLYWATCH`: User for SAP EarlyWatch services**
  `EARLYWATCH` is a default user created in client 066, and its default password is `SUPPORT`. It is used for SAP EarlyWatch Alert, which analyzes system performance, security, and stability. The user should use this account for SAP EarlyWatch functions only, and the password should be changed after installation.
- **`SAPCPIC`: Default RFC user**
  `SAPCPIC` is another default user created in client 000 and in any new client. The default password is `ADMIN`, which should be changed immediately. It is used as a communication tool for RFC connections and system integration, and it plays a critical role in legacy system integration. SAP recommends deleting the `SAPCPIC` ID if it is no longer required in the client.

- **TMSADM: User for transport management system**
  The default user ID TMSADM is a system user created automatically in client 000. It plays a critical role in transport requests and system communication. TMSADM's default password should be changed using the procedure described in SAP Note 1414256. The ID should also be deleted in all other clients.

In the description of each standard ID, it has been emphasized that the default password for these IDs should be changed immediately, and the ID should be locked. If the IDs are not required for any specific client, they should be deleted in that client. SAP provides a standard report named RSUSR003, which highlights the status of standard IDs across all system clients (see Figure 1.2). It indicates whether they exist in a specific client, whether they are locked, and whether the default password has been changed.



Number of Selected Standard Users: 64

System: [redacted]
Instance:
User: [redacted]
Date 19.05.2025
Time: 15:42:08

Prof.Param
login/no_automatic_user_sapstar 0
login/password_logon_usergroup
login/password_downwards_compatibility 0

Client	User	Lock	Password Status	Reason for User Lock	Failed	Valid from
000	DDIC		Exists; Password not trivial.			
	SAP*		Does not exist.Logon possible with p/w PASS. See Note 2383			
	SAPCPIC		Does not exist.			
	TMSADM		Exists; Password not trivial.			
100	DDIC		Exists; Password not trivial.	Locked by unsuccessful logons		
	SAP*		Does not exist.Logon possible with p/w PASS. See Note 2383			
	SAPCPIC		Does not exist.			
	TMSADM		Exists; Password not trivial.			
144	DDIC		Exists; Password not trivial.		2	
	SAP*		Does not exist.Logon possible with p/w PASS. See Note 2383			
	SAPCPIC		Does not exist.			
	TMSADM		Exists; Password not trivial.			
200	DDIC		Exists; Password not trivial.		2	
	SAP*		Does not exist.Logon possible with p/w PASS. See Note 2383			
	SAPCPIC		Does not exist.			
	TMSADM		Exists; Password not trivial.			

Figure 1.2: Standard Report RSUSR003

1.3 Transaction SU01: Managing User Account Lifecycle

Transaction SU01 is used to create, delete, lock, and assign roles/profiles to user IDs. A display version, Transaction SU01D, is also available. While Transaction SU01 should only be restricted to security administrators, the display version can be assigned to any user in the organization to view the status of user accounts.

Transaction SU01 includes several tabs, and data can be entered in the fields displayed on these tabs when creating a user. Although there are several fields in these tabs, the only fields that are mandatory while creating a user are **User ID**, **Last Name**, and **Password**. All other fields can be entered as needed according to the organization's policies.

Let's create the following user in the system using Transaction SU01:

- First name: ALICE
- Last name: SAPLAND
- User name: `ASAPLAND`

Log into the SAP system and start Transaction SU01 by entering "SU01" in the field in the upper-left corner (see Figure 1.3) and pressing the Enter key.

The Transaction SU01 window opens, displaying two empty fields (see Figure 1.4): one named **User** and the other called **Alias**. In the **User** field, enter the user ID name. The **Alias** field is not mandatory and can be left blank. Some organizations use this field to enter another unique user attribute, like the user's personnel number.

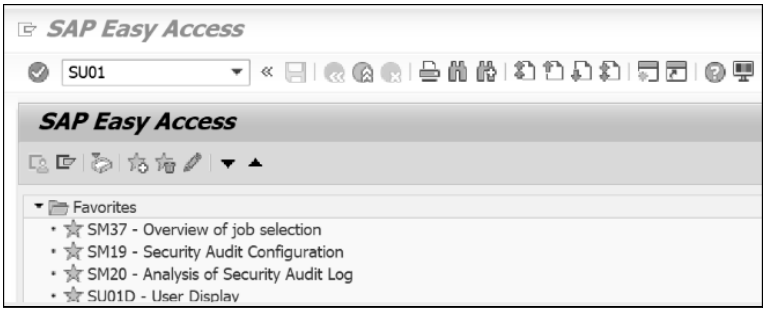


Figure 1.3: Entering Transaction SU01 in SAP GUI

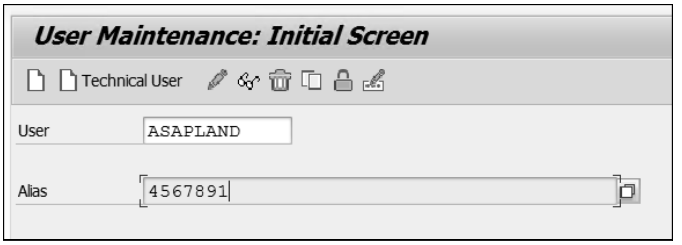


Figure 1.4: Initial Screen of Transaction SU01

On the menu bar of the initial Transaction SU01 screen, there are icons to create a new user, create a new technical user, change a user, display a user, delete a user, copy a user, lock a user, and reset a user's password. For users who prefer using the keyboard over a mouse, the functionalities of these icons also can be invoked using keyboard shortcuts. Table 1.1 summarizes the keyboard shortcuts. These keyboard shortcuts are shown as tooltip texts when you hover your mouse cursor over the corresponding icon.

Functionality	Keyboard Shortcut
New user	F8
Change user	Shift + F6
Delete user	Shift + F2
Lock user	Ctrl + F5
New technical user	Ctrl + F8
Display user	F7
Copy user	Shift + F5
Reset password	Shift + F8

Table 1.1: Keyboard Shortcuts for Icons in Menu Bar of Transaction SU01

The first two icons, **Create a User** and **Create a Technical User**, require further clarification. Every user in the company has personal data, including their first name, last name, job function, department, and other relevant details. All these values can be entered in Transaction SU01 in a special **Address** tab. If an account is not intended exclusively for an end user, then this data does not need to be entered. For example, system accounts, which are designed for system-to-system communication, running background jobs, or even generic IDs like firefighter IDs used in SAP GRC, do not contain personal data. Such IDs can be created using the new **Technical User** icon in the menubar. When creating a new user, the Transaction SU01 screen displays 11 tabs for data entry. However, when creating a technical user, the **Address** tab does not appear, resulting in only 10 tabs.

Naming Convention for User IDs

Organizations follow certain naming conventions to create user IDs as a security best practice. Such a convention can be as simple as the user's first initial followed by their last name, or more complex. Note that user IDs are limited to a maximum of 12 characters. Hence, if an organization uses a naming convention that incorporates parts of a user's name, sometimes it may need to be truncated to limit it to 12 characters. If such a naming convention results in duplicate IDs for two different users, then numerals can be used to distinguish them—for example, `JDOE`, `JDOE1`, and so on. Some companies use the uniqueness of users' personnel numbers (`PERNR`) to create their user IDs. According to the organization's needs, a specific value may be entered for the **Alias** field. Enter the **User** field with the user ID name and, if applicable, the **Alias** field and press the **New User** icon, the first icon on the menu bar.

Now, let's walk through each of the 11 tabs in Transaction SU01:

- **Documentation**
  The **Documentation** tab, shown in Figure 1.5, features a large text field, labeled **Documentation for User**, in which any information about the user can be stored.

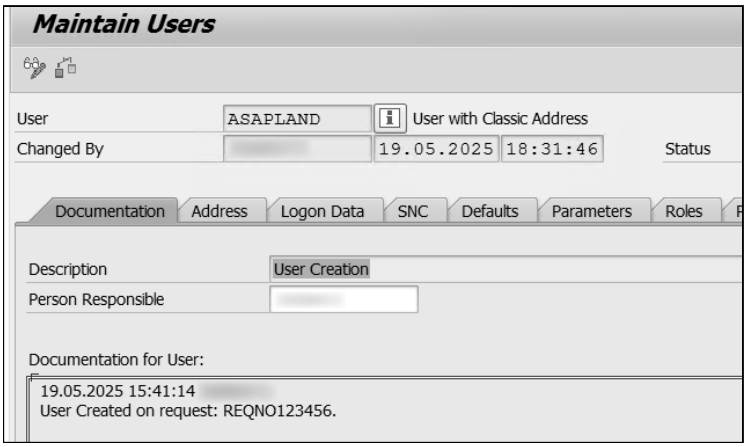


Figure 1.5: Documentation Tab

  It may contain the IT Service Management (ITSM) ticket number or any suitable information that the organization needs to maintain about a new user. It may also include the history of changes the user ID has gone through during its lifecycle. Although user changes can be obtained through the change document, the data maintained in the change document is very restricted and does not contain information about the reasons for changes. The **Documentation for User** field is not mandatory, so it can be left blank. The data in the **Documentation** field can be deleted using report RSUSR_DELETE_ USERDOCU.

- **Address**
  The **Address** tab, shown in Figure 1.6, contains user details about the new user.

  The tab includes several fields under various sections: **Person** contains information about the person; **Work Center** provides information about the user's position, department, and physical location; **Communication** contains information like the user's phone number and email address; and **Company** includes the user's company information. The only mandatory field in this tab is the **Last name** field. All other fields in this tab can be left blank. It can be good practice to enter as much data as possible here so the company has detailed information about its users.

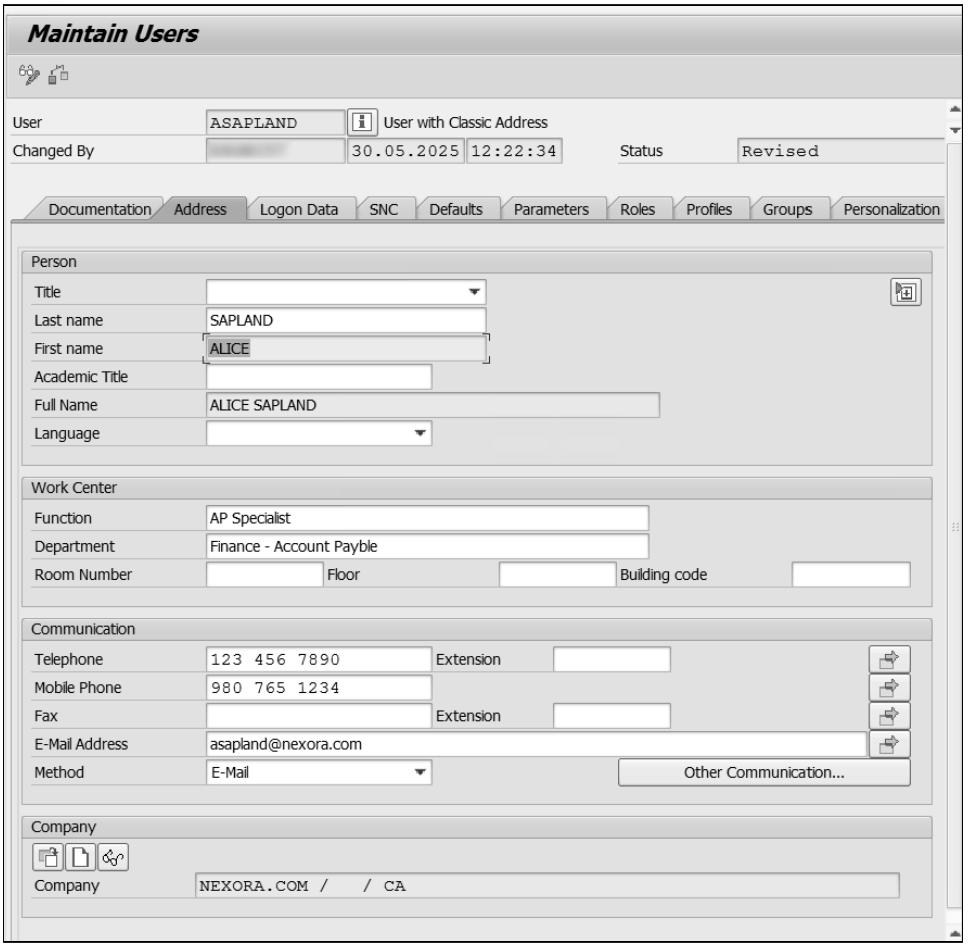


Figure 1.6: Address Tab

- **Logon Data**
  The **Logon Data** tab, shown in Figure 1.7, has several fields to maintain information about the user. One of the most crucial fields in this tab is the **Password** field, contained in the **Password** section of the screen. Other sections under this tab include **User Group** for authentication checks, **Validity Period**, and **Other Data**, as well as fields for **Alias**, **User Type**, and **Security Policy**. In the **User Type** field, a dropdown list holds all five user types described in Section 1.1, allowing the appropriate one to be chosen. A security policy can be entered in the **Security Policy** field if one is available for the user. Security policies are addressed in more detail in Section 1.10.

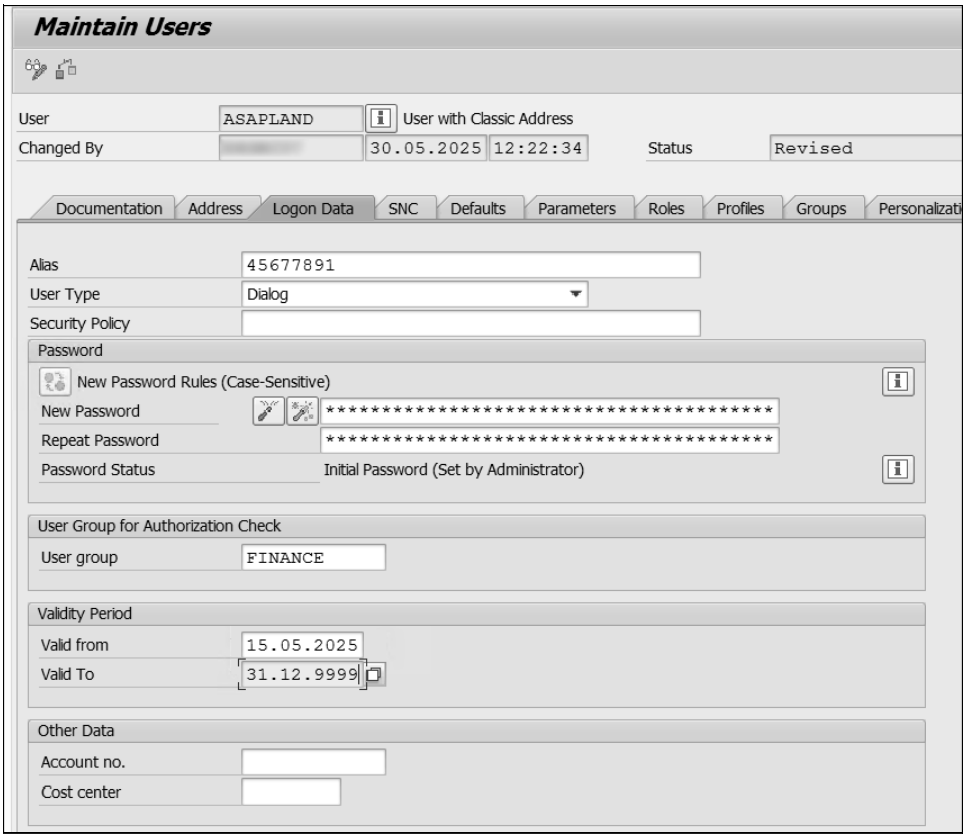


Figure 1.7: Logon Data Tab

The **New Password** field is mandatory in this tab. In this field, the security administrator can enter a new password that satisfies the organization's password policy. The same password has to be confirmed by reentering it in the **Repeat Password** field. A complex password can also be generated by clicking the **Generate** button (the second icon after the **New Password** label), as shown in Figure 1.8. The initial password can be shared with the new user using a secure channel. The initial password needs to be changed the first time the user logs into the account. If the company uses SSO for user authentication, the password can be deactivated by clicking the **Deactivate** button (the first icon after the **New Password** field).

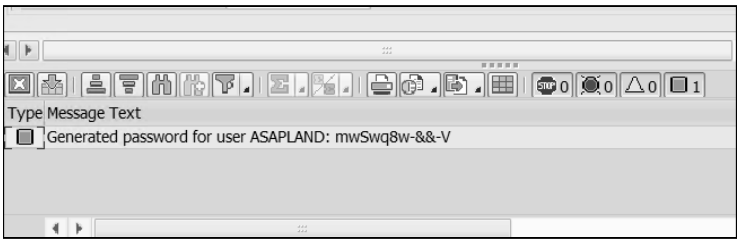


Figure 1.8: Generated Password for User

The **User Group** field enables you to assign a unique user group to the user. Section 1.5 provides an in-depth examination of the user group concept. The **Valid From** and **Valid To** fields in the **Validity Period** section allow you to maintain the user's validity dates. If a new user is to be onboarded on a future date, that date can be entered in the **Valid From** field. Users cannot log into the system if they attempt to do so outside their validity period. The **Account no** and **Cost Center** fields can be entered in the last section of this tab. These fields are not mandatory.

- **SNC**

  SNC stands for Secure Network Communications. The **SNC** tab, shown in Figure 1.9, can mention an organization's use of another application to secure communication between SAP GUI and the application server in the backend. SSO is one frequently used application. Such applications assign a unique SNC ID to each user, which can be used in the **SNC name** field.

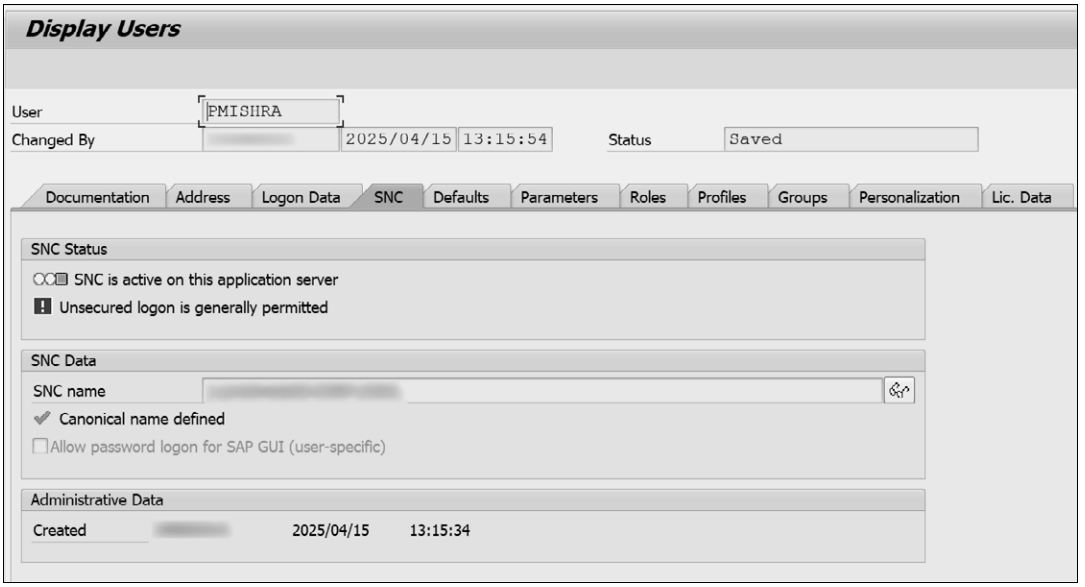


Figure 1.9: SNC Tab

If a user is configured for SSO, they still can log in using a password if the **Allow password log on for SAP GUI** checkbox is checked. For more information on SNC and SSO, see Chapter 2.

- **Defaults**

  The **Defaults** tab (see Figure 1.10) defines several default values, including **Decimal Notation**, **Date and Time** format, default spool information, **Time Zone**, and **CATT** information. Most fields in this tab are generic and maintained centrally for the entire organization; therefore, these fields are autopopulated when Transaction SU01 is run.

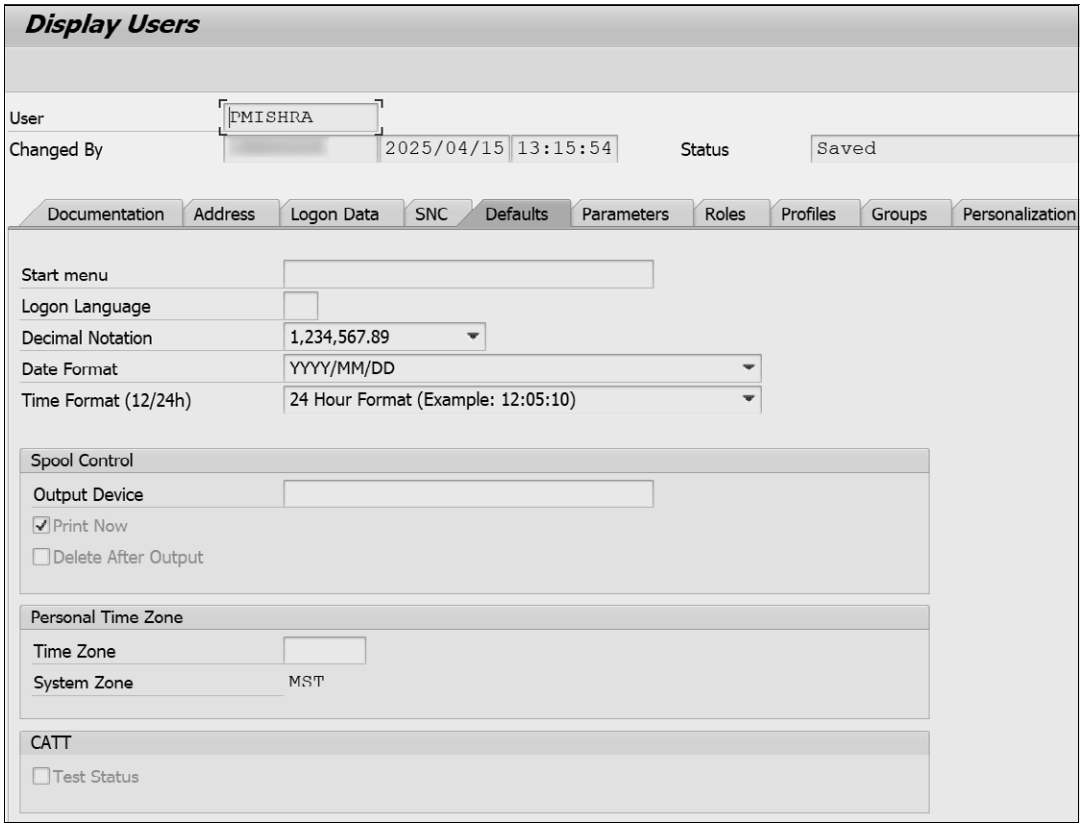


Figure 1.10: Defaults Tab

- **Parameters**
  Some default values for a user can be entered in the **Parameters** tab, shown in Figure 1.11. The user can also enter these values using Transaction SU3. Some standard parameters that can be defined in the **Parameters** tab are as follows:
  - **WRK**: Work site purchasing transactions; for example, ME21
  - **BUK**: Company code for financial transactions
  - **CAC**: Controlling area for cost management
  - **SWK**: Maintenance plant in plant maintenance transactions
  - **XUS**: User ID for authentication-related processes
  - **IHK**: Planner group in maintenance orders
  - **AAR**: Work center category for production planning

  If a user specifies the value of a specific parameter—say, **BUK** = **2000**—then whenever a financial transaction is run, the value of the **Company Code** (**2000**) will appear by default.

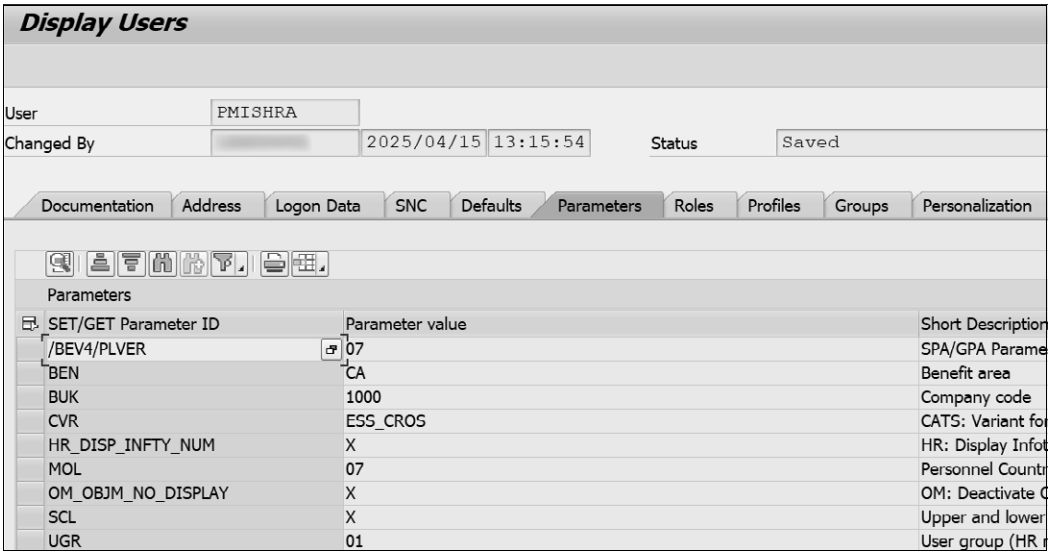


Figure 1.11: Parameters Tab

- **Roles**

  Roles are assigned to a user in the **Roles** tab, as shown in Figure 1.12. This tab can also be used to display the roles assigned to a user.

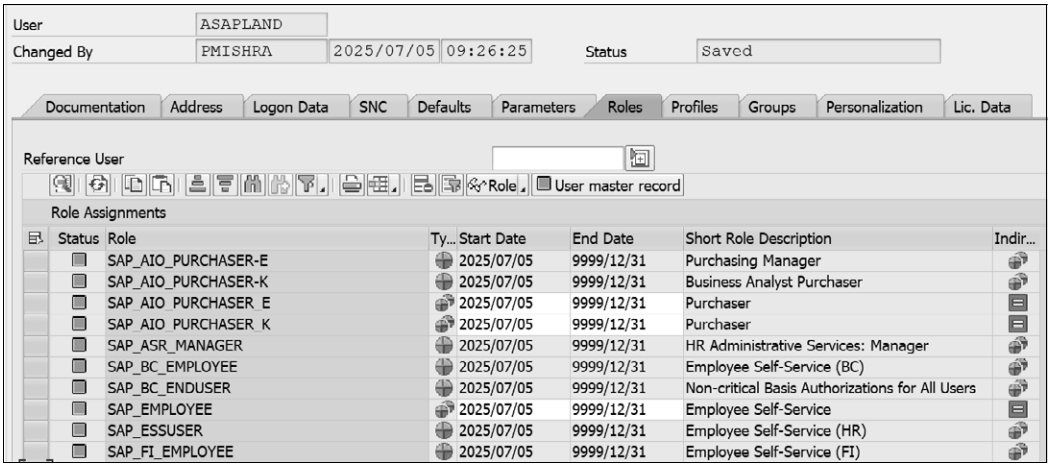


Figure 1.12: Roles Tab

In the **Role Assignments** grid, the **Role** column contains the name of the roles assigned to the user. The next column shows whether it is a single or composite role. The **Start Date** and **End Date** indicate the validity dates of the role assignment. The last column indicates whether a role is assigned to the user directly or indirectly through an HR org object, such as a position.

To assign a new role to a user, enter the role name in a new line in the **Role** column, and enter a **Start Date** and an **End Date**. If no **Start Date** and **End Date** are entered, then the default values for these are the current date and 9999/12/31, respectively.

SAP Note 2110144 describes how to display the role assignment that comes from the reference user (if any) assigned to the user.

- **Profiles**

  The **Profiles** tab, shown in Figure 1.13, can be used to assign profiles to a user directly. Also, it displays the profiles of the roles and profiles assigned to a user. To assign a new profile to a user, enter the profile name in the **Profile** column of the **Assigned Authorization Profiles** grid.

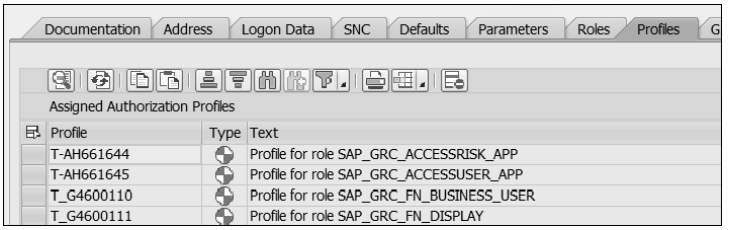


Figure 1.13: Profiles Tab

- **Groups**

  In the **Groups** tab, shown in Figure 1.14, you can enter user groups to which a user belongs. The groups entered here differ from the **User Group** value entered in the **Logon Data** tab. Suppose a company decides that user administrators cannot make any changes to users in the employee and contractor user groups of the **Logon Data** tab. That restriction can be controlled through a suitable entry in the `S_USR_GRP` authorization object. When a user administrator opens a user ID in Transaction SU01 to make changes, the kernel checks the `S_USR_GRP` object during the authorization check to ensure the administrator has the required authorization. However, the group entered in the **Groups** tab is not checked for authorization. It is intended solely for categorizing users for mass changes in Transaction SU01 or SUIM reports.

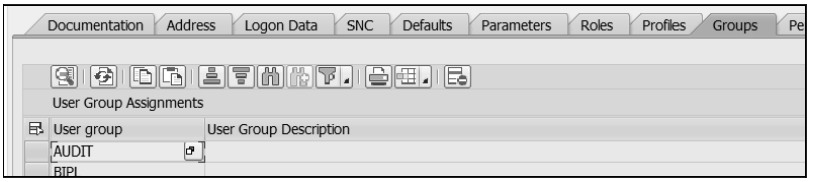


Figure 1.14: Groups Tab

A user can belong to multiple groups in the **Groups** tab. However, in the **Logon Data** tab, the **User Group** field can contain only one value; hence, a user can belong to only one user group linked to an authorization.

- **Personalization**
  User-specific settings can be entered for a user in the **Personalization** tab (see Figure 1.15), allowing SAP transactions and programs to run and provide output in a specific manner (such as the number of rows or columns). It can also be used to specify preferences for output devices, printer types, workflow approvals, and layouts. The **Personalization** tab in Transaction PFCG (Profile Generator; see Chapter 3) contains the same values, and they work in sync.

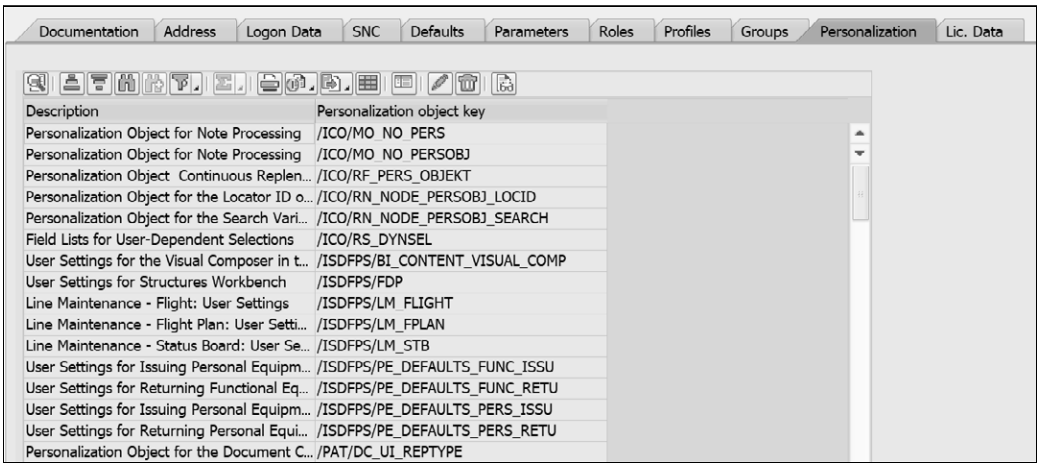


Figure 1.15: Personalization Tab

Personalization data is saved in table `SPERS_OBJ` in the SAP database.

- **License Data**
  The **License Data** tab, shown in Figure 1.16, maintains licensing information for each user. It has only one dropdown field, **Contractual User Type ID**. There are four options available by default in the dropdown. While creating a user, the security administrator can choose the appropriate option. For the technical teams (Basis, security, and ABAP development), **SAP Platform User** is the most appropriate choice in SAP S/4HANA. For business users, **SAP NetWeaver Gateway User for Productivity Apps** may be the most suitable option.

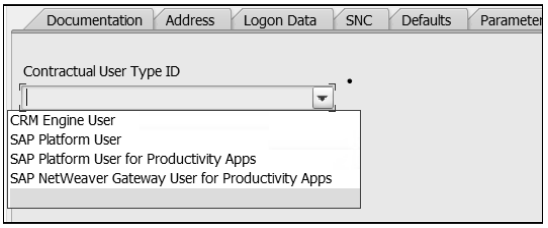


Figure 1.16: License Data Tab in Transaction SU01

Transaction SU01 is used for all identity-related operations. You can create a new user, modify an existing user, copy a user to create a new user, lock or unlock a user, or even

delete an existing user. Let's discuss how these operations are carried out using Transaction SU01:

- **Copying a user**
  If a new user is to be created that is very similar to an existing user, the existing user can be copied to create the new user, thus saving some obvious data entry work (see Figure 1.17).

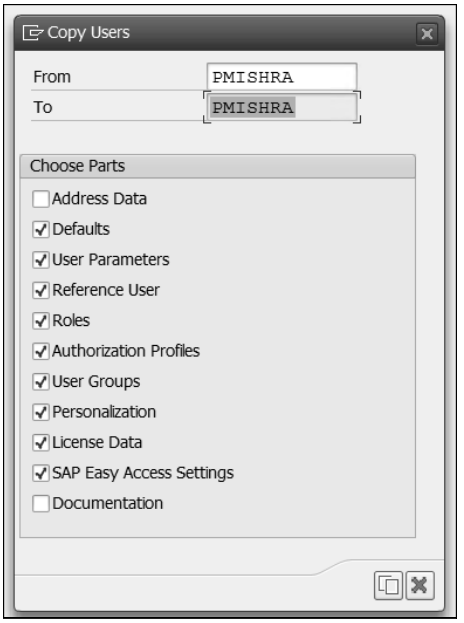


Figure 1.17: Initial Screen of Copying User in Transaction SU01

To copy an existing user, click the **Copy** icon in the menu bar. A new popup screen shows two fields at the top, **From** and **To**. Enter the name of the existing user ID and the new user ID in these fields. In the panel named **Choose Parts**, the names of all the tabs in Transaction SU01 appear, with a checkbox next to each one. All the checkboxes are already checked, except for the **Address Data** and **Documentation** tabs. This means that all of the existing user's data will be copied to the new user, except for the data in the **Address Data** and **Documentation** tabs. This is logical because the data in these tabs is specific to each user. The security administrator can uncheck any other tab as needed. Data from those tabs won't be copied and will need to be entered manually. Click the **Copy** icon at the bottom of the popup screen; the Transaction SU01 screen will reappear, with the **User** field populated with the new user ID. As you can check, all the data is copied from the existing user to the new user except for the fields in the unchecked tabs on the previous screen. Enter the data for those tabs manually and save the new user.

When many users are to be created with very similar data, the **Copy User** feature in Transaction SU01 can be convenient for efficiently accomplishing this task.

- **Deleting a user**
  Transaction SU01 allows you to easily delete a user ID. Run Transaction SU01 and open the user that needs to be deleted. Click the **Delete** icon on the menu bar. The popup screen shown in Figure 1.18 appears. Clicking the **Yes** button will delete the user.

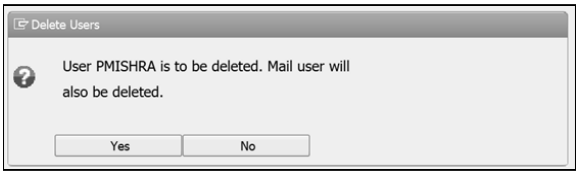


Figure 1.18: Confirmation Screen for Deleting User

  However, deleting users in the SAP environment is not recommended as a best practice. Deleting a user can impact historical transactional records and workflows involving the user, potentially causing system issues. It is recommended that the user be deactivated by locking it, adjusting the validity dates, removing roles from it, and moving the it to the user group of deactivated users.

- **Locking/unlocking a user**
  The **Lock** icon on the menu bar of Transaction SU01 is used to lock/unlock a user. To lock a user, run Transaction SU01, enter the user ID in the **User** field, and click the **Lock** icon. A popup screen appears that specifies the user's current lock status, as shown in Figure 1.19.

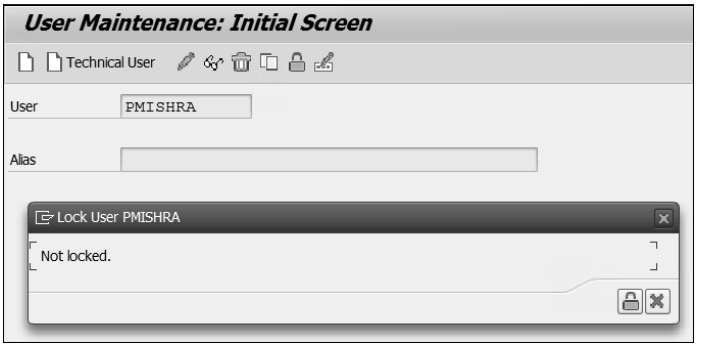


Figure 1.19: Lock Status of Current User, Displaying Lock Button to Lock User

  Click the **Lock** icon on the popup screen and the kernel will lock the user and give a confirmation message. A locked user can be unlocked in a very similar fashion.

Lock Status of a User in SAP

In SAP, there are four lock statuses, each indicating a user's lock status. When a user is not locked, their lock status is 0. If a user is locked across the landscape using some central user management system like Central User Administration (CUA), the lock status of the user is 32. When a user is locked by the administrator using Transaction SU01,

their lock status is 64. When a user is locked out because of entering the wrong passwords multiple times, their lock status is 128. The number of times a user must try to log in with the wrong passwords to get locked out is specified in a system parameter, `login/fails_to_user_lock`. The parameter's default value is 5; administrators can choose any value between 1 and 99. In table `USR02`, users lock statuses are displayed in a column showing these numbers. When a user is locked for multiple reasons, you can see the sum of the respective numbers in the **Lock** column.

1.4 Transaction SU10: Managing User Accounts in Bulk

Transaction SU01 deals with one user account at a time. If multiple user accounts need to be processed simultaneously, the transaction to be used is Transaction SU10. You can create, lock, unlock, assign roles/profiles, assign user groups, and simultaneously enter licensing information for all selected users. The transaction works in two stages: user selection and action. In the *user selection stage*, users can be selected based on various criteria. In the *action stage*, actions such as creating, assigning roles/profiles, locking, unlocking, and so on can be carried out. One limitation of Transaction SU10 is that the action must be the same; for example, if you want to assign one role to a group of users and another role to another group of users, it must be done in two passes only. In the first pass, assign the first role to the first group of users, and in the second pass, repeat the same process with the second role and the second group of users.

In the following sections, we'll dive into the options for selecting users with Transaction SU10 and the different actions available.

1.4.1 Selecting Users

The initial screen of Transaction SU10 is shown in Figure 1.20.

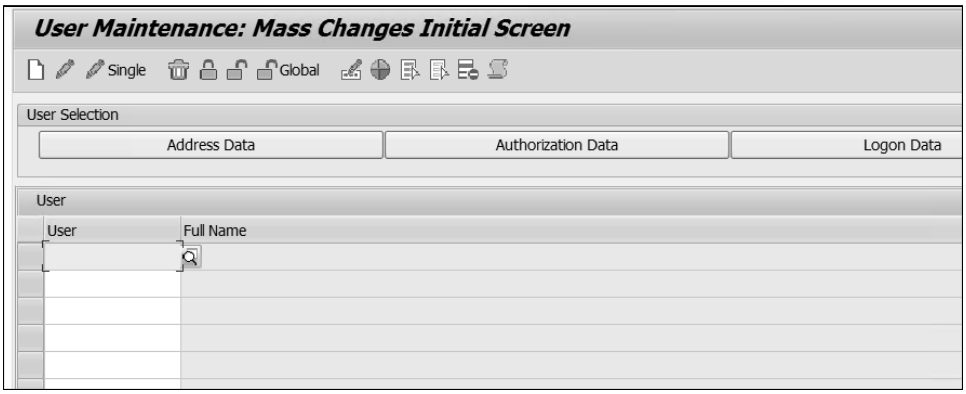


Figure 1.20: Initial Screen of Transaction SU10

If already chosen, users can be pasted from your clipboard into the grid shown in the **User** panel. Transaction SU10 also provides ample scope for the admin to select users using various complex criteria. The **User Selection** panel has three buttons: **Address Data**, **Authorization Data**, and **Logon Data**. Pressing these buttons opens popup screens for user selection; we'll walk through each one in the following sections.

Selecting Users Based on Address Data

Users can be selected from their address data by clicking the **Address Data** button. A popup screen similar to the **Address Data** tab of Transaction SU01 opens (see Figure 1.21), but each field now has an option to choose multiple values. You can click the multiple selection button at the end of each field to enter your selection criteria. For example, suppose a test system has numerous users created with user names that start with TEST for some testing work, and now you want to delete or lock them. You can click the multiple selection button at the end of the **Users** field, and your selection criteria will be **TEST***. Now, all users with user names starting with TEST will appear in the user grid of Transaction SU10, from which they can be locked, unlocked, or deleted with a single click.

If you want to add a role to all users belonging to one or more specific departments, you can select the departments from the **Department** field on this screen.

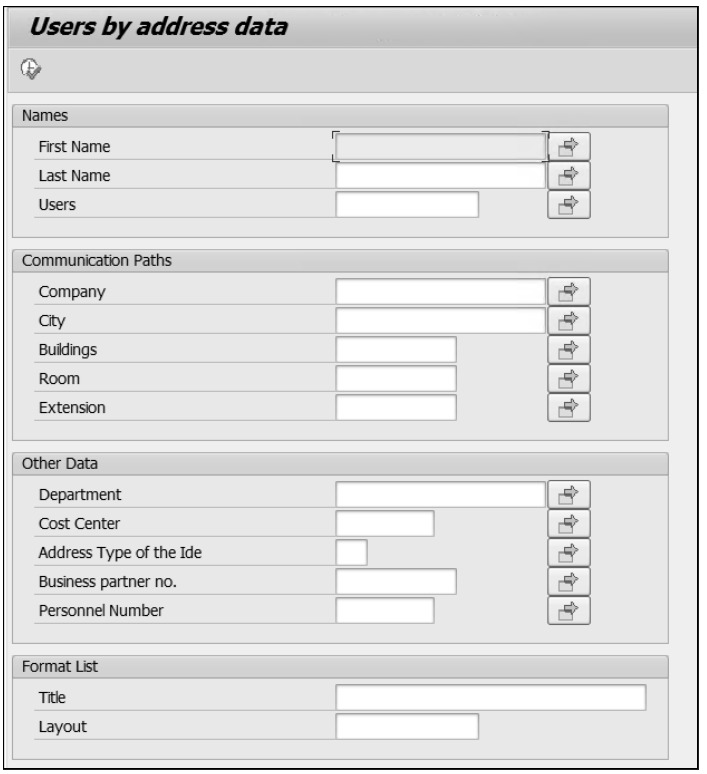


Figure 1.21: Enter User Data to Select Users Based on Address Data

Extreme care must be taken when selecting users to ensure that all users within the scope of your current work are diligently included, none are missed, and no user is unintentionally added.

Selecting Users Based on Authorization Data

If you press the **Authorization Data** button in the user selection panel of Transaction SU10, a screen appears with multiple tabs (see Figure 1.22). At the top of these tabs is a **Standard Selection** panel with three fields: **User**, **Group for Authorization**, and **User group (general)**. Using these fields, you can select based on user IDs; multiple selection is possible, or you can select all users belonging to one or more authorization groups (determined by the **Group** field in the **Logon Data** tab of Transaction SU01) or one or more user groups. Also, you can open one of the tabs in the **Selection Criteria** section, each of which has multiple fields representing various attributes in the user master. All users that satisfy some specific attribute chosen from the existing field can be selected.

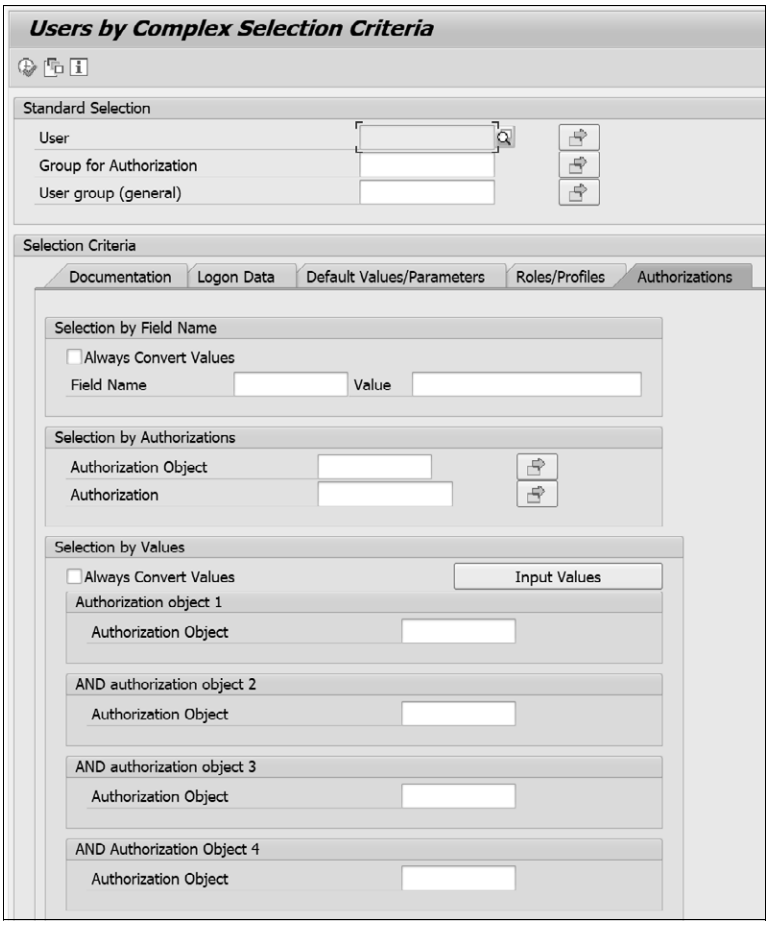


Figure 1.22: Enter User Data to Select Users Based on Authorization

You can select all users with one or more specific authorizations by selecting those authorizations in the **Selection by Authorization** section of this screen. Click the multiple selection button beside the **Authorization Object** field, then select a few objects in the field beneath it. You can also choose users with multiple authorization objects and specific field values by adding up to four authorization objects and their respective field values in the selection screen. Thus, there are numerous ways to select users based on the authorizations they have.

User Selection by Logon Data

This is the third option to select users based on the fields available in the **Logon** tab of Transaction SU01. As for the previous options, this screen also offers a considerable number of ways to select users to act upon. There are several sections on this screen, as shown in Figure 1.23.

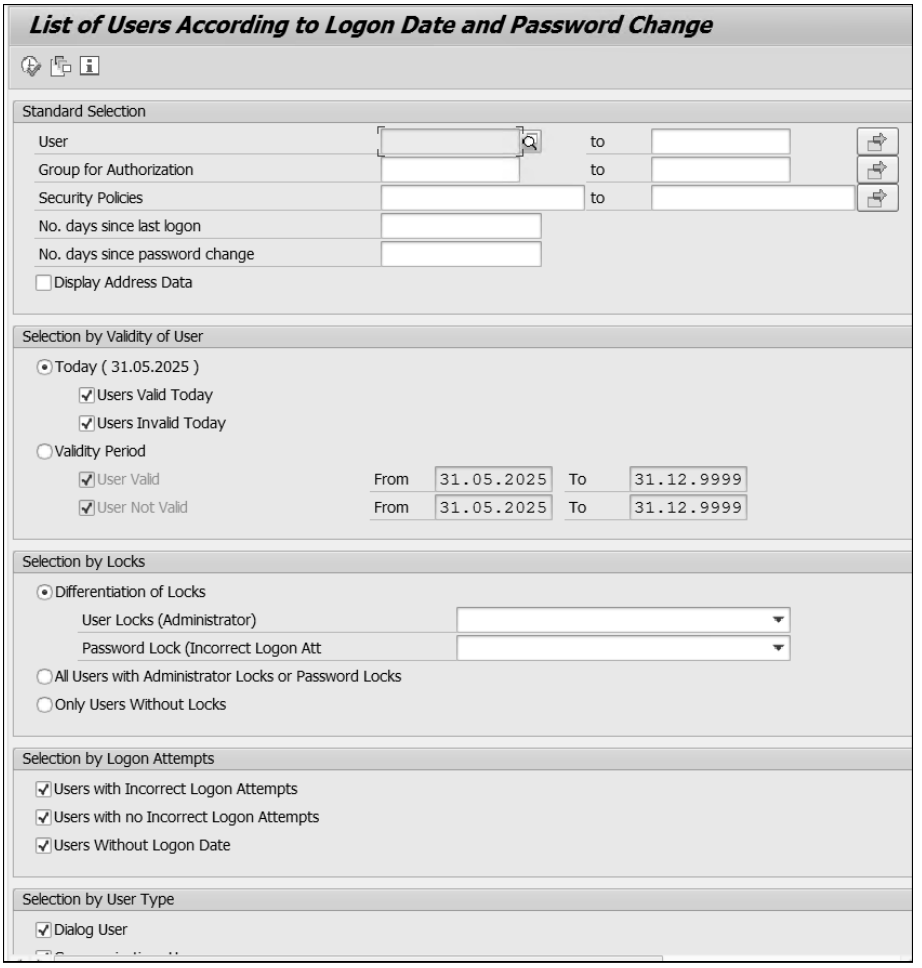


Figure 1.23: Enter User Data to Select Users Based on Authorization

Figure 1.23 illustrates a portion of the user selection screen, based on logon date and password change. The **Standard Selection** section of the screen contains standard fields such as **User** and **Group for Authorization**, as well as **Security Policies**. You can select users based on these attributes, and each offers the option to make multiple selections. The following section is titled **Selection by Validity of User**. This section has several date options to choose users based on their validity dates. Other sections on this screen offer options to select users based on the type of locks they have, their user types, and the number of logon attempts. You also can create a mix-and-match selection including options from across the various sections of this screen.

1.4.2 Actions for the Selected Users

After selecting the users in the first stage of Transaction SU10, various actions can be taken on these users. Figure 1.24 shows the menu bar of Transaction SU10. Actions can be initiated for the selected users by clicking the respective icons.

Figure 1.24: Actions Available in Transaction SU10 for Selected Users

Let's discuss each of these icons and the actions they support:

- **Create new users**
  The first icon in the menu bar lets you create new user accounts in bulk. In the selection screen, enter the user name for all the new accounts that need to be created, then click the **Create** icon. This opens a new screen with all the tabs of Transaction SU01. The **Documentation** and **Address** tabs are grayed out, indicating that data cannot be entered in these tabs. Also, the password fields are missing in the **Logon Data** tab as the password cannot be the same for multiple users. All other fields in the **Logon Data** tab and all other tabs are available for data entry. For example, all these users may belong to the same authorization group, and the same roles and profiles may be added. Enter all the common data for all these users, then click the **Save** button to save all these users. All users will be created in the system. The next screen will provide a unique password generated for each user, which can be shared with them.
- **Change users**
  The second icon lets you make mass changes. After selecting the users, click the **Change** icon. Again, a screen appears with all the tabs of the Transaction SU01 screen, and the **Documentation** and **Address** tabs are grayed out. The password fields are missing in the **Logon Data** field. All other fields are available with their current values. Changes can be made to the data as required and saved. Transaction SU10 completes the transaction and displays a screen that shows all the changes made to the users.

- **Change users (single)**

  The next icon on the menu bar lets you change users. You can choose multiple users using the selection scopes described in the previous subsections. However, you can then act on them individually. As shown in Figure 1.25, the users are first selected. When you click the **Change User (Single)** button, the users are displayed in the left panel, and all the Transaction SU01 tabs are shown in the right panel (see Figure 1.26). One user can be selected in the left panel; the right panel will then display all the Transaction SU01 data available for that user, which can be modified. After modifying each user, Transaction SU10 asks you to save the data. The transaction can be closed after the data for all users has been changed and saved.

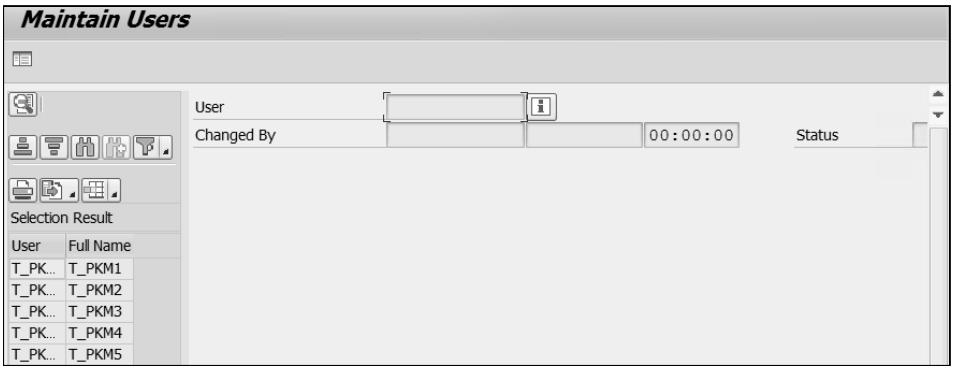


Figure 1.25: Transaction SU10 Screen Showing All Selected Users

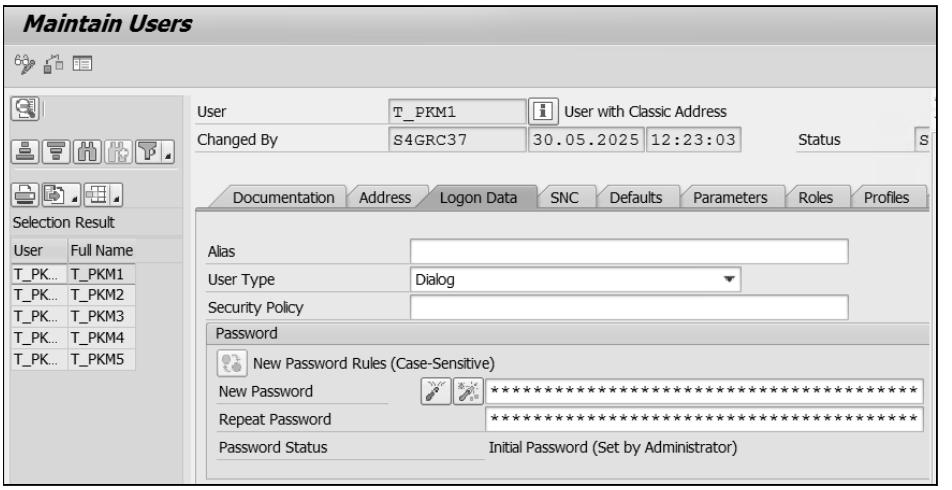


Figure 1.26: Transaction SU10 Screen to Select Specific User to Modify

- **Delete users**

  The next icon in the menu bar is the well-known trashcan icon, which can be used to delete users. After selecting the users in the first step of the transaction, they can all be deleted with a single click of this icon. However, deleting users is not a best practice for

security in a production environment, and even in any other environment, you should be very cautious about using this button. If many users are selected and this button is pressed by mistake, all the users will be deleted. Transaction SU10 requests confirmation before deleting users. If confirmed, there is no way to undo this action, and recreating many users one by one can be a very time-consuming process.

- **Lock/unlock/global lock**
  The three lock icons on the menu bar (shown in Figure 1.24) are related to locking users. With a single click of the **Lock** or **Unlock** icon, all the users selected in Transaction SU10 can be locked or unlocked. If the organization uses CUA, all the selected users can be locked across the environment using the **Lock (global)** icon.
- **Password change**
  Using the **Password Change** icon, the passwords of all users can be deactivated, or each user can be assigned a unique initial password generated automatically. In the second scenario, Transaction SU10 displays each user's password in the right-hand side panel. These passwords can be copied and shared with each user individually.
- **Change role assignment**
  The next icon on the menu bar allows you to change role assignments. Clicking this icon opens a screen with two radio buttons that show the **Add** and **Remove** labels at the top, and a grid to enter roles below that. Click one of the radio buttons to choose the **Add** or **Remove** action. Enter the roles to be added or removed in the grid below, then click the **Save** button. The action will be carried out and saved. The only limitation of this approach is that the roles that can be added or removed from all the users must be the same.
- **Select all/deselect all/remove**
  The next two icons in the menu bar allow you to select or deselect all users, and the button after those removes users from the selected user list.
- **Display application logs**
  The menu bar's last icon displays application logs from the database. On clicking the icon, a selection screen appears for the administrator to choose parameters for the log they intend to display. Clicking the **Execute** button extracts the logs from the backend database and displays them.

Transaction SU01 is a powerful tool for managing account lifecycle events, especially the joiner, mover, and leaver scenarios. However, each action must have controls in place to manage compliance requirements. For example, when a new hire joins the organization, the creation of a user ID, passwords, and role assignment should be based on approvals and proper documentation. When someone moves within the organization, access assignment should be based on defined processes. In both situations, a step to manage segregation-of-duties (SoD) risk should be part of the process. Finally, when someone leaves the company, their access should be removed immediately, and the user account locked. This is a part of many compliance requirements.

1.5 User Groups

In Transaction SU01, two types of user groups exist: one in the **Logon Data** tab, which is related to authorization object S_USER_GRP, and the other in the **Groups** tab. Using the first one, you can control who will be allowed to maintain users belonging to certain user groups. The second one is for logical grouping of the users for reporting, searching, and sorting. For authorization purposes, a user can only belong to one user group in the **Logon Data** tab. However, a user can be assigned to multiple groups in the **Groups** tab.

Transaction SUGR is used for creating, modifying, deleting, or displaying user groups. On the initial transaction screen, as shown in Figure 1.27, there is only one field for entering the **User group** name. If it is an existing group, the **Change** icon can be used to modify the group, the **Display** icon can be used to display the group and its members, and the **Delete** icon can be used to delete the group.

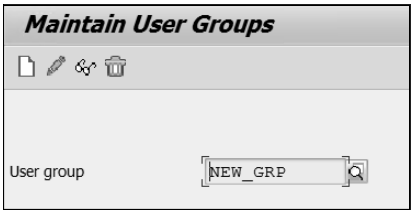


Figure 1.27: Initial Screen of Transaction SUGR

To create a new group, enter a group name and click the **Create** icon in the menu bar. A new screen appears to enter a user group description and add users to the group (see Figure 1.28).

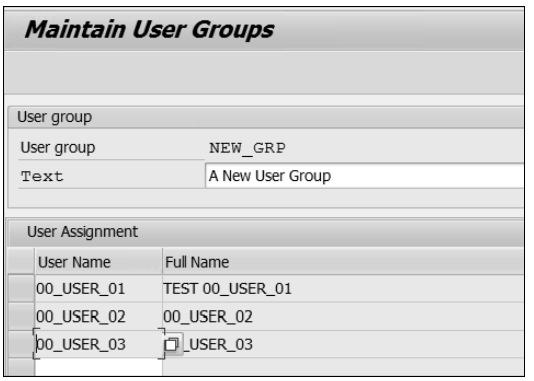


Figure 1.28: Creating New User Group

If you open one of these users in Transactions SU01 or SU10, you can see that the user has been added to the new user group in the **Groups** tab. However, the user group in the **Logon** tab remains unchanged; it is the same as before adding this user to the new group. Even if the **User Group** field in the **Logon** tab is blank, it won't be populated by adding users to a **Group** in Transaction SUGR.

Existing user groups in a client can be viewed in table USGRP. Every user should be assigned to a user group in the **Logon Data** tab. If no user group is assigned, then there is a risk that the user can be modified by any user via Transaction SU01 or SU10. User maintenance operations should be segregated through the **User Group** field to control the user maintenance process, at least in the production environment.

1.6 Tables Related to User Management

SAP runs on a relational database management system (RDBMS). Hence, all SAP data is stored in tables, and these tables are grouped into authorization groups. Security-related tables belong to authorization classes SC and SS. Table 1.2 lists some of the frequently used tables by security admins. These tables can be accessed through any table browsing transaction, such as Transaction SE16, SE16N, SM30, or SM31.

Table	Description
User Master Tables	
USR01	User master data: General user information.
USR02	User logon information, password status, lock status, and user type.
USR03	User address data.
USR04	Assigned authorization per user.
USR05	User master data, ID parameters.
USR06	Additional data for users (e.g., license data).
USR21	Assignment of user master to address data.
Address Tables	
ADRP	Personal address information (e.g., first name, last name).
ADRC	General address information.
ADR6	User email addresses.
BUT000	Business partner general data. Users can be linked to business partner type person.
BUT021_FS	Business partner address information.
Role and Authorization Tables	
AGR_DEFINE	General information about roles. It pulls data from the **Long Text** field in Transaction PFCG.

Table 1.2: SAP Tables Related to User Management

Table	Description
AGR_USERS	Roles assigned to users.
AGR_1251	Authorization data for roles
AGR_AGRS	Mapping of composite roles to single roles
AGR_TCODES	Transaction codes in roles.
USR10	Definition of authorization profiles.
USR11	User master texts for profiles.
USR12	User master authorization values.
UST04	Mapping of users to profiles.
TSTCA	Transaction to authorization object assignment.
Other Related Tables	
USGRP	User groups.
USR40	Table of forbidden passwords.
USRACL	Mapping of users to SNC names.
HRP1001	HR objects: Relationship. Useful table for organizations using SAP HCM.

Table 1.2: SAP Tables Related to User Management (Cont.)

1.7 Securing Passwords

For most SAP customers, SAP is a business-critical system because it stores critical business data, including financial information, supply chain details, confidential trade data, and personal data of users and business partners. A compromised password is the simplest way to hack a computer system. Hence, the first step an organization can take to bolster its security is to secure user passwords. Gone are the days when user passwords were stored in plain text format. Now, most software will store the hashed values of passwords.

Cryptographic hash functions are used to compute hash values. A cryptographic hash function is a mathematical algorithm that takes an input, such as a password, and returns a fixed-length string, known as a hash value or digest, that is cryptographically secure. It is designed to be a *one-way* function, meaning that it is simple to compute the hash value of any given string, but it is computationally infeasible to reverse engineer the original input from the hash, even if thousands of known hash values are available.

Since the invention of public key cryptosystems in 1970, several hash functions have been proposed, and cryptanalysts have analyzed their strengths. With advancements in

computational technologies and intensive cryptographic research, numerous hash functions have been proposed through the years, only to be broken from time to time, and the search for newer and stronger hash functions continues. Some of the popular hash functions used by many software systems to generate hash values of passwords include MD5, SHA-1, and SHA-2. MD5 was proposed in 1991, but it was proven to be vulnerable against so-called collision attacks in 1995. NIST proposed SHA-1 in the same year, but by 2000, it was proven to be susceptible to newer collision attacks. Multiple versions of SHA-2 have been invented and used. In 2007, NIST initiated a competition for a newer hash function, SHA-3, and Keccak was selected as SHA-3 in 2012. However, most software systems, including SAP, still use MD5 and SHA-1. To strengthen the hash value, they use a *triple hash value*; that is, they apply one or two hash algorithms three times, consecutively, to the input in order to derive a provably stronger hash value.

In the rest of this section, we will discuss SAP tables related to passwords, password-related profile parameters, and some recommendations to maintain the security of passwords.

1.7.1 Password-Related SAP Hash Tables

SAP stores hash values in tables and views. These tables are critical from a security perspective and must be protected adequately. Only administrators should have access to these tables, and only on a need-to-know basis. The tables storing passwords and related information are `USR02`, `USH02`, `USH02_ARC_TMP`, and `USRPWDHISTORY`. The two most frequently used views are `VUSER001` and `VUSR02_PWD`.

In the SAP world, algorithms computing the hash values of user passwords have also gone through an evolution process, and improved hash algorithms have replaced weaker ones to enhance password security. In table `USR02`, you can see a column named **Code Version**, with a single-character value like A, B, and so on. This is the algorithm used to compute the hash value of passwords. The algorithm related to code version A was the initial one, which is obsolete now. Code version B used MD5, with a password of eight characters in length. Code version F uses SHA-1 and accepts passwords of up to 40 characters. The most recent code version is I, which uses the triple-hash technique. It computes the MD5 value of the user's password and then the SHA-1 value of the MD5 output, then it applies a generic version of SHA-1 again.

An organization can choose the code version it wants to use by setting the `login/password_hash_algorithm` system parameter to the appropriate value. This is a system-wide parameter, not a client-specific one.

1.7.2 The Logon Process

When a user attempts to log into an SAP system using a user name and password, the system undergoes multiple steps to facilitate the login process. The following series of challenges and answers can summarize these steps:

1. Does the user possess a valid password (password not deactivated)?
2. Is the user permitted to use password login?
3. Is the user's lock status 0 (not locked by the administrator or by multiple failed login attempts)?
4. Is the password correct (hash value of the entered password = stored hash value in table `USR02`)?
5. Does the user need to change their password (initial or expired)?

The user can only log in if all the answers are favorable. If the answer to the last question is yes, then the kernel will provide a dialog box to change the user's password.

After logging in, if you click **System • Status** in the menu bar, the screen shows data about the logged-on user, as shown in Figure 1.29. It displays the previous and current logins, as well as the number of failed password login attempts.

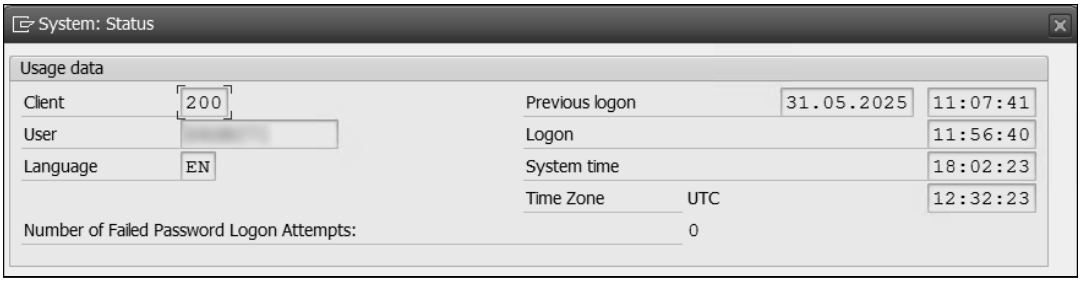


Figure 1.29: System Status Screen Showing Data of Current User

1.7.3 Password-Related System Parameters

SAP passwords can be secured by setting appropriate values in some system `Logon` parameters. Users can be required to use a combination of uppercase and lowercase letters, numeric characters, and special characters to create complex passwords. Security researchers have demonstrated that password strength is more dependent on the password length than on its complexity. Hence, users can also be required to use passwords of a secure length through system parameter `login/min_password_lng`. Another essential characteristic of a secure password is its validity period; after a specific time, users may be required to change their existing password, and the new password should be different from the last *n* passwords. Logon parameter `login/password_expiration_time` lets the admin choose a time period in days after which a user must change their password. The parameter lets the system administrators choose the value of *n* (4 or 5 is good enough). Table 1.3 summarizes the system parameters related to passwords and recommended values.

Parameter	Description	Recommended Value
login/min_password_lng	Minimum password length	12 to 16
login/min_password_letters	Minimum number of letters in the password	1
login/min_password_uppercase	Minimum number of lowercase letters	1
login/min_password_lowercase	Minimum number of uppercase letters	1
login/min_password_digits	Minimum number of numeric characters	1
login/min_password_specials	Minimum number of special characters	1
login/password_history_size	Number of password changes before the same password can be set again	12
login/password_expiration_time	The number of days after which a user must change their password	90
login/min_password_diff	Minimum number of characters that must be different between subsequent passwords	4
login/password_change_waittime	Number of days to wait to change one's own password	1
login/password_max_idle_productive	Number of days for an unused productive password to expire	30
login/password_max_idle_initial	Number of days for an unused initial password to expire	15
login/password_compliance_to_current_policy	Forces users to comply with the password policy and requires a password change if noncompliant (value 1 or 0)	1
login/password_downwards_compatibility	Allow old MD5 password hash values (value 0 or 1)	0

Table 1.3: Password-Related Profile Parameters

Parameter	Description	Recommended Value
login/fails_to_user_lock	Number of failed attempts before locking the user	5
login/fails_to_session_end	Ends the session after a certain number of failed attempts	3
login/failed_user_auto_unlock	Determines if locked users are automatically unlocked after a set time (1 or 0)	0

Table 1.3: Password-Related Profile Parameters (Cont.)

1.7.4 Table USR40: Obviating Obvious Passwords

Table USR40 can be used to blacklist obvious passwords. Users tend to set obvious and easy-to-remember passwords to access systems quickly. Such obvious passwords pose a considerable risk of being compromised and thus pulling the entire organization into a security incident.

Table USR40 can be populated with such obvious passwords. The table allows simple passwords and also regular expressions containing wildcard characters like * and ?. The ? character stands for a single character, and * stands for a sequence of any combination of characters of any length. For example, the entry ?elcome can be entered in table USR40 to forbid both welcome and Welcome or any other seven-character string ending in elcome as passwords. The expression *123* can be entered to forbid any password that contains the string 123 within it, at any location, including at the beginning, end, or anywhere in between (see Figure 1.30).

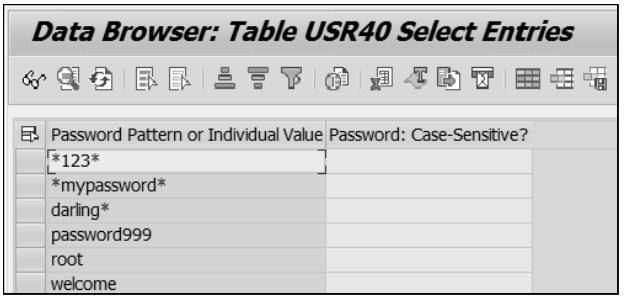


Figure 1.30: Table USR40

1.7.5 Some Recommendations to Secure Passwords

Securing passwords in an SAP environment is crucial for protecting your organization from unauthorized access to the system. Here are some essential considerations for a secure password policy:

- **System configuration and policies**
  The first line of defense against a password compromise is to force users to use strong passwords through system configurations. In the previous section, we discussed password-related profile parameters that can technically enforce a strong password—for example: Encourage users to use long passwords that include a mix of uppercase, lowercase, numeric, and special characters. Disallow obvious passwords via table `USR40`. Lock users who attempt to use the wrong password multiple times, and don't automatically unlock them.
- **Other technical measures**
  SAP S/4HANA and SAP ERP use secure hashing algorithms to store the hashed value of passwords. Ensure that the algorithms used are always the most recent. If they are upgraded, you upgrade too, and run report CLEANUP_PASSWORD_HASH_VALUES to clean up the older hash values. Ensure that both the operating system (OS) and the SAP environment are regularly patched. Integrate the SAP environment with the company's Security Information and Event Monitoring (SIEM) system, or acquire a monitoring system like SAP Enterprise Threat Detection to monitor suspicious login attempts, brute force attacks, and unusual user behavior. Implementing a multifactor authentication (MFA) method also can be very useful for password-based security. Although primarily RFC-based connections are nondialog, securing RFC connections with strong authentication mechanisms and securing system interfaces are critical.
- **User education and awareness**
  Educate users on password best practices and explain how they are crucial for both their digital security and that of the organization. Discourage the sharing of passwords and encourage the use of a password manager so that users don't have to remember complex passwords. Raise awareness about phishing attempts and other digital social engineering attacks. Use the *principle of least privilege*, meaning that user accounts should have just enough authorization to carry out the user's day-to-day work; this way, a compromised account does not have wider privileges.
- **Organizational policies**
  It cannot be overstated how important it is to create enterprise-wide password security awareness. Implement a robust password policy and communicate it effectively. A periodic security email can be effective. Review the password policy regularly and update it if necessary. In addition, follow a sound account lifecycle management policy to ensure the timely creation, locking, unlocking, and deactivation of user accounts.
- **Monitoring**
  To optimize the benefits of adopting a sound password policy, a monitoring strategy should be implemented. The strategy can include monitoring events such as repeated failed logons, spikes in user lockouts and password resets, or changes to high-risk accounts. Regular monitoring would also be beneficial if real-time alerts cannot be implemented. In suspicious cases, a procedure should be developed to follow up and investigate factors such as timing, source client system, destination app server, IP

address, location, and so on. High-risk events should be monitored through the enterprise's Security Information and Event Monitoring (SIEM) system.

Implementing the tips suggested here can significantly enhance an organization's security posture from the password perspective. The most effective way to secure your system is to take a multilayered approach that combines technical controls, user education, and strong organizational policies.

1.8 Transaction SUIM: The SAP User Information Management Reports

For SAP security professionals, running reports on users, roles, transactions, and authorizations is a critical daily activity. From that perspective, Transaction SUIM is a practical resource. If you run Transaction SUIM, you will see a **User Information System** root node on the initial screen, along with several subnodes below it named **User**, **Roles**, **Profiles**, **Authorizations**, and more (see Figure 1.31). Each of these subnodes can be expanded to reveal several reports.

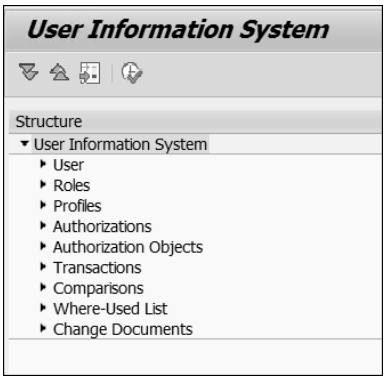


Figure 1.31: Initial Screen of Transaction SUIM

Let's walk through these nodes in more detail:

- **User**
  If you expand the **User** node, you will see several executable items under it, as shown in Figure 1.32. These items are reports. In addition, you will see two subnodes: **Cross-System Information** and **Users by Complex Selection Criteria**. The first node can be used if you have CUA configured in your environment. CUA is not being used by many organizations, but a brief note about it is in order. CUA is an SAP application that allows companies to manage users across multiple SAP systems from a single, centralized client. From CUA, you can centrally create, modify, lock, unlock, and assign roles to users in each connected child system. If CUA is configured in your environment, you can run reports to find users by **System**, **Roles**, **Profiles**, or **License Data**. The data in these reports can be further analyzed by entering appropriate values in the selection screens.

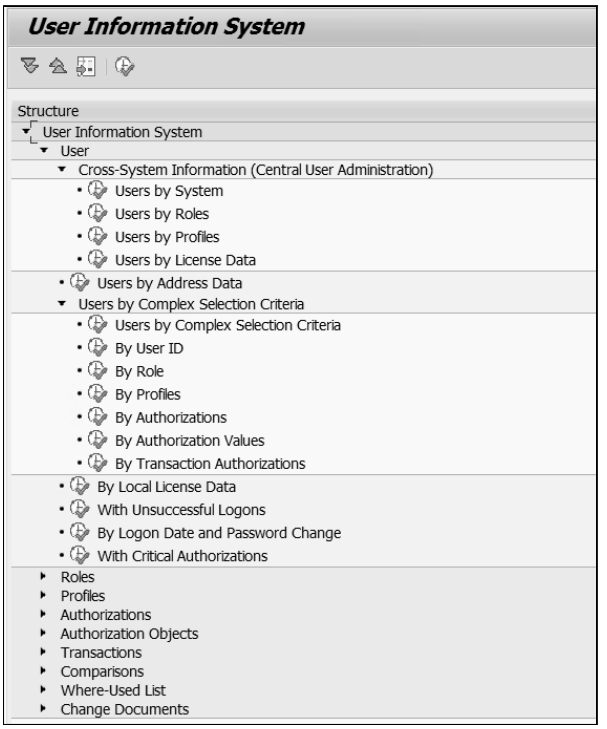


Figure 1.32: Expanded User Node of Transaction SUIM

Note

Each report in Transaction SUIM has multiple fields in which values can be entered to filter the data. All reports available in Transaction SUIM are accessible individually, each with a separate name. For example, report RSUSR002 is the Users by Complex Selection Criteria report. It isn't easy to remember all the report names, so SAP has consolidated all the standard user reports into a single transaction code, which can be executed in a user-friendly graphical user interface (GUI) environment.

The first report is **Users By Address Data**. If you click the **Execute** icon next to the report name, you will see a screen in which you can enter values to filter the data according to your requirements, as shown in Figure 1.33. You can filter the data using fields such as **First Name**, **Last Name**, **User ID**, **Company**, and others.

The most useful report among those under the **User** node is the one called **Users by Complex Selection Criteria**, which offers a wide range of interesting fields to filter on. As shown in Figure 1.34, the selection features multiple tabs, each of which contains numerous fields to enter values for filtering. For example, in the **Authorizations** tab, there are four fields to select authorization objects and report users who have those authorization objects with specific field values. We'll discuss authorization objects and fields in detail in Chapter 3.

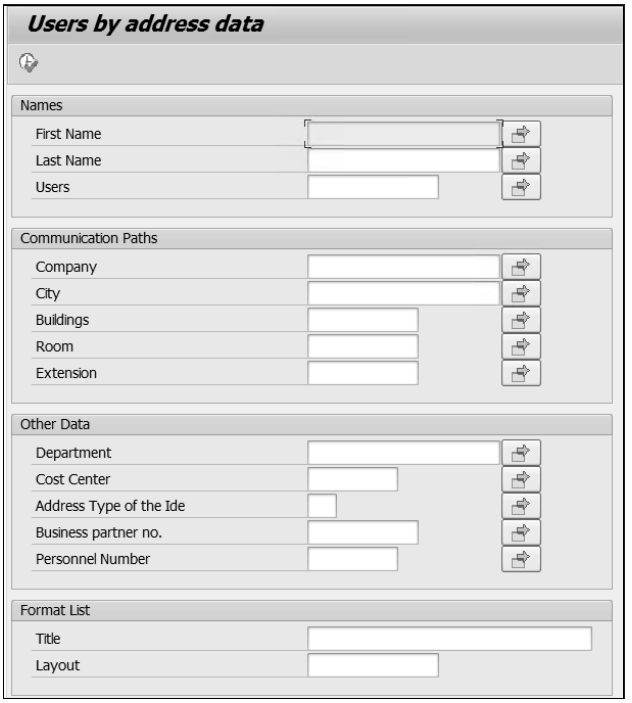


Figure 1.33: Selection Screen for Running User Report Based on Address Data

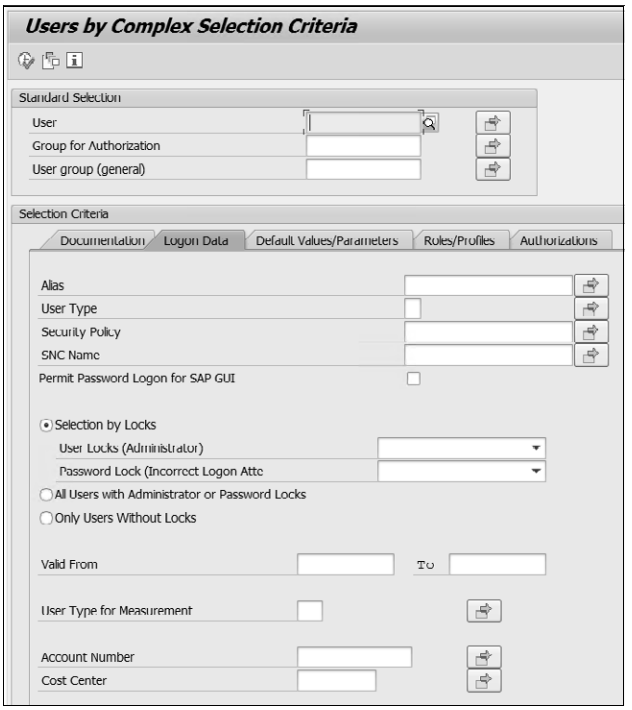


Figure 1.34: Selection Screen for Running User Report Based on Complex Selection Criteria

- **Roles**

  Under the **Roles** node (see Figure 1.35), several reports are available to retrieve roles based on role name, user assignment, transaction assignment, profile assignment, and other criteria. Again, the most interesting of these reports is the one called **Roles by Complex Selection Criteria**, which offers the maximum number of fields to slice and dice your data based on complex selection criteria. For example, you can select **Single** or **Composite** roles, or both, based on whether they are assigned to specific users, as determined by the authorization objects and the values they contain. In Chapter 3, this book covers roles and all the related concepts.

  There are two reports in the **Roles** node that can be very useful in the SAP S/4HANA environment: **Applications in Role Menu** and **Startable Applications in Roles**. You can use these reports to identify roles containing SAP Fiori apps. Also, if you have the role name, then you can see which SAP Fiori apps are included in these roles. You can also get the same functionality by directly running Transactions RSUSR_ROLE_MENU and RSUSR_START_APPL. For more details, refer to SAP Notes 2341600 and 2356418.

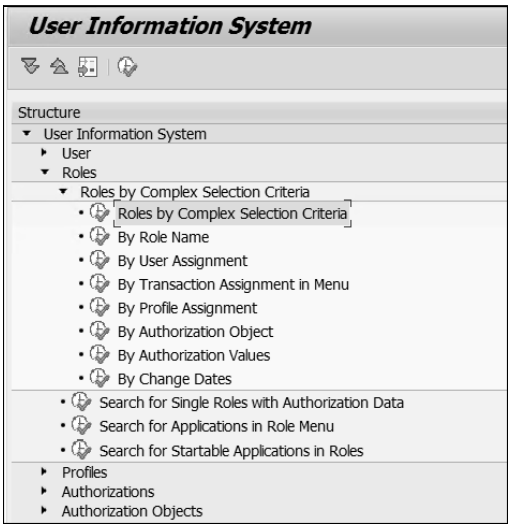


Figure 1.35: Fully Expanded Roles Node in Transaction SUIM

- **Profiles**

  Profiles are containers for authorization objects. SAP introduced the role-based authorization concept with the Profile Generator in SAP R/3 version 4.6 in 2000. Previously, users were authorized using authorization profiles created in Transaction SU02. Currently, when a role is created in Transaction PFCG, profiles are automatically created and linked to the role. Some standard profiles, such as `SAP_ALL` and `SAP_NEW`, are still in use. However, these standard profiles have extremely high privileges and are not assigned to end users under ordinary circumstances. Reports related to profiles are listed under the **Profiles** node in Transaction SUIM, as shown in Figure 1.36.

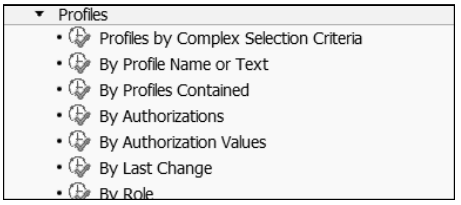


Figure 1.36: Expanded Profile Node in Transaction SUIM

In SAP, users are authorized to execute transactions through authorization objects. Authorization objects contain several fields. For example, one field commonly found in many authorization objects is `ACTVT` (activity), which has several possible values: `1`, `2`, `3`, and so on, where `1` represents create, `2` represents change, `3` represents display, and so on. Suppose a user is assigned an authorization object with `ACTVT = 3`. In that case, the user cannot create or modify objects of the type referred to in the authorization object; they can only display them. By an *authorization object*, we mean the object itself with a few fields and possible values for each field. When you choose specific values for each field, it becomes an *authorization*. The next two nodes in Transaction SUIM are related to authorizations and authorization objects.

- **Authorizations**

  Under the **Authorizations** node in Transaction SUIM, reports related to authorization objects and authorizations are available. These can be run to discover authorizations and authorization objects available in your SAP environment. There are four reports under the node, as shown in Figure 1.37. The top option is **Authorizations by Complex Selection Criteria**, and the others allow searching for authorizations by specific objects, specific values of the authorization fields, or by a specific field and text.

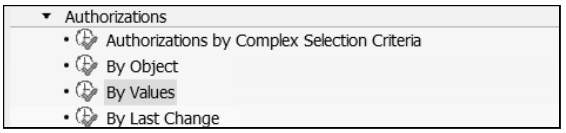


Figure 1.37: Expanded Authorization Tab in Transaction SUIM

- **Authorization Objects**

  This node in Transaction SUIM enables the user to query authorization objects (see Figure 1.38). Using the **Authorization Objects by Complex Criteria** report option, reports can be run to obtain authorization objects by object name, text, object class, field, or any combination. There are reports with just one of these attributes, too.

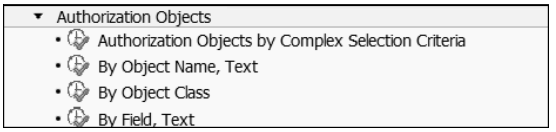


Figure 1.38: Authorizations Objects Node in Transaction SUIM

- **Transactions**
  This node is for querying the transactions available in the system, filtered by various conditions, as shown in Figure 1.39. For example, to find the transactions available inside a role, you can run the **Executable for Role** report. Or to know what transactions are available for a user, you can run the **Executable for User** report.

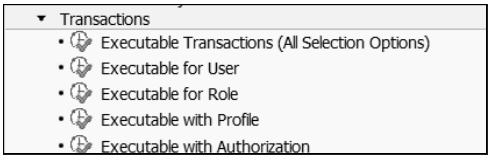


Figure 1.39: Transactions Node in Transaction SUIM

- **Comparisons**
  Using the reports in the **Comparisons** node, you can compare users, roles, profiles, or authorizations. For example, you can compare two users to see what authorization objects they have. To do so, execute the **Of Users** report in the **Comparisons** node of Transaction SUIM (see Figure 1.40).

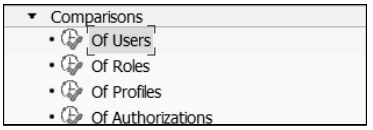


Figure 1.40: Comparisons Node in Transaction SUIM

A new screen appears with two input boxes, one for each user, as shown in Figure 1.41. Enter the user IDs of the two users and click the **Execute** button.

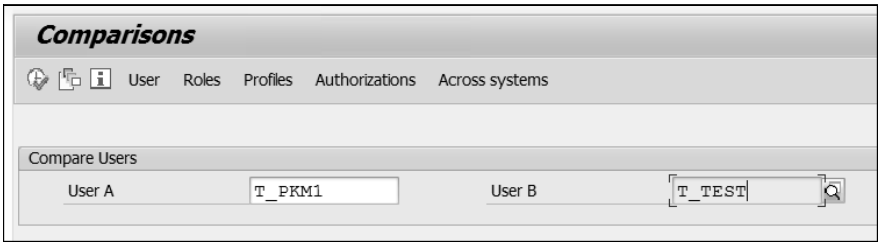


Figure 1.41: Comparing Two Users

The system returns a table with all the authorization objects the two users have in one column and the names of the users in two other columns (see Figure 1.42). When a user has an authorization object, there is a green traffic light for that user for that object; otherwise, there is a red traffic light. Thus, the report shows the similarities or discrepancies in assigned authorization objects for the two users.

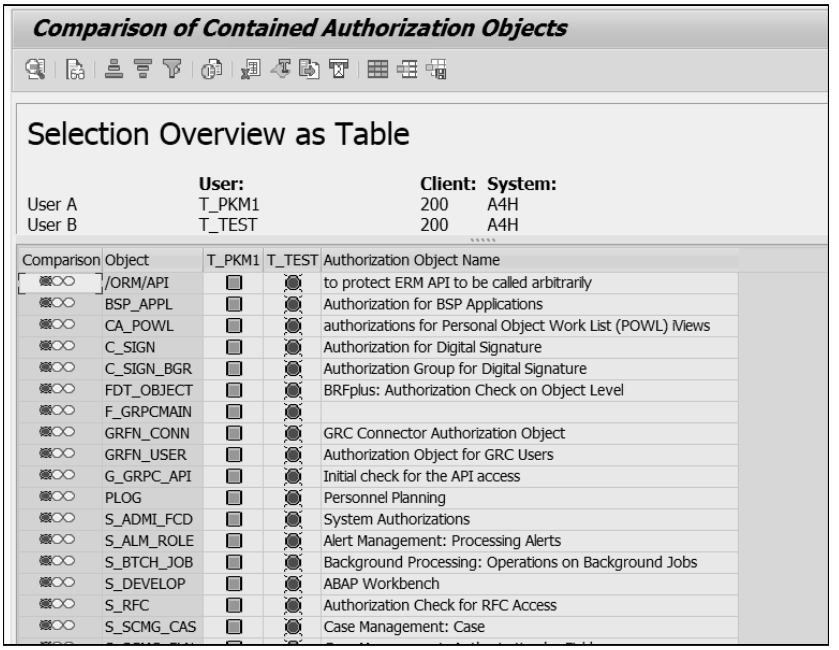


Figure 1.42: Comparison of Two Users

- **Where-Used List**

  Under this node, as shown in Figure 1.43, you will find reports for roles, profiles, authorizations, authorization objects, and security policies. On execution, these reports will provide information on where the objects they cover are being used in the system; that is, by running a where-used report for one or more roles, you can find all the users to whom those roles are assigned. If you run the where-used report called **In Programs**, under **Authorization Objects**, and select a program, the output will be all the authorization objects called by the program. Where-used reports work almost identically for all other items.

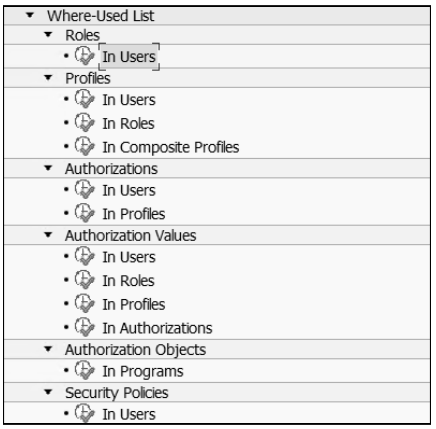


Figure 1.43: Where-Used Reports of Transaction SUIM

- **Change Documents**
  The **Change Documents** node in Transaction SUIM, shown in Figure 1.44, contains fascinating and helpful reports for security professionals and auditors. These reports display when and who made changes to users, roles, profiles, and other objects. For example, auditors may be interested in knowing who was assigned the SAP_ALL profile and when, which SAP logs. Using the reports in the **Change Documents** node, you can query logs and uncover valuable information about the changes. For example, auditors execute these reports to ensure that all changes made to users, roles, or other objects within the scope of the audit are authorized.

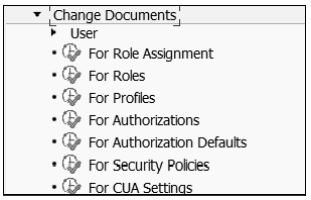


Figure 1.44: Change Document Reports in Transaction SUIM

Let's briefly discuss the change documents for roles; we'll defer the discussion of change documents for users to Section 1.9. As shown in Figure 1.44, there are two reports for roles: one for role assignments and another for roles. The first one queries role assignments that have happened in a specific period, initiated by a particular user, and initiated for specific users. All these parameters can be chosen as per the administrator's requirement. The second one, the change document for roles, has several options to query how a role or a group of roles has been modified over a specific period. In both, wildcard characters can be used freely. Let's take a closer look at both reports:

- **Change documents for role assignment**
  Figure 1.45 displays the initial screen of the change document for the **For Role Assignment** report.

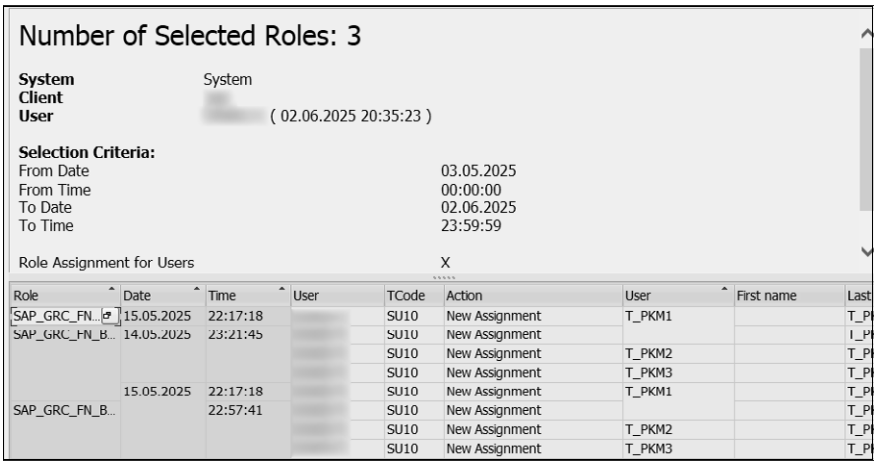


Figure 1.45: Selection Screen for Change Document for Role Assignment

The **User** input field does not allow multiple inputs, but wildcards can be used to select multiple users. Alternatively, a wildcard (*) in that field can represent all users in the system. The **Role Name** field allows for multiple inputs, and wildcards also can be used. A blank in that field means any role will be matched. You can enter a user name in the **Changed By** field to query the role assignments made by a specific user, choose multiple users, or leave the field blank to indicate any user. The **From Date** and **To Date** fields can be entered to specify the query period. Pressing the **Week, Month**, or **Year** button sets the period as the last week, month, or year, respectively. For an example, we have run the report by entering just "T_PKM*" in the **User** field and querying for the last month by pressing the **Month** button. The output is shown in Figure 1.46.

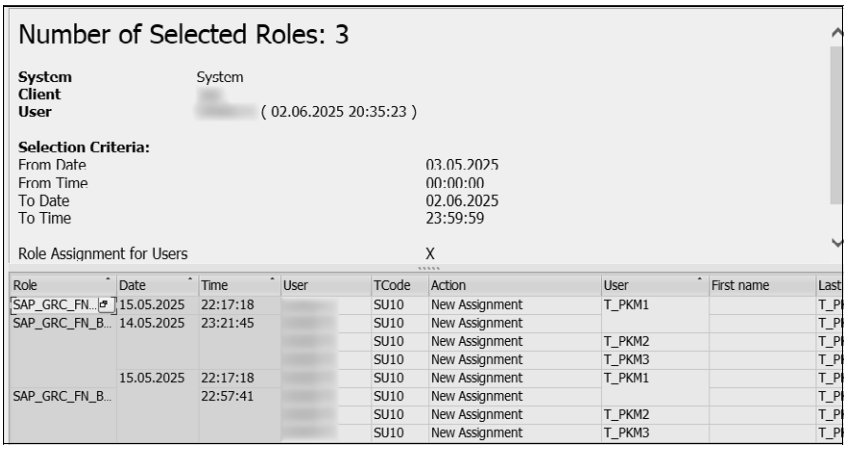


Figure 1.46: Change Document for Role Assignments Sample Output

- **Change document for roles**
  The selection screen for the **For Roles** report is shown in Figure 1.47.

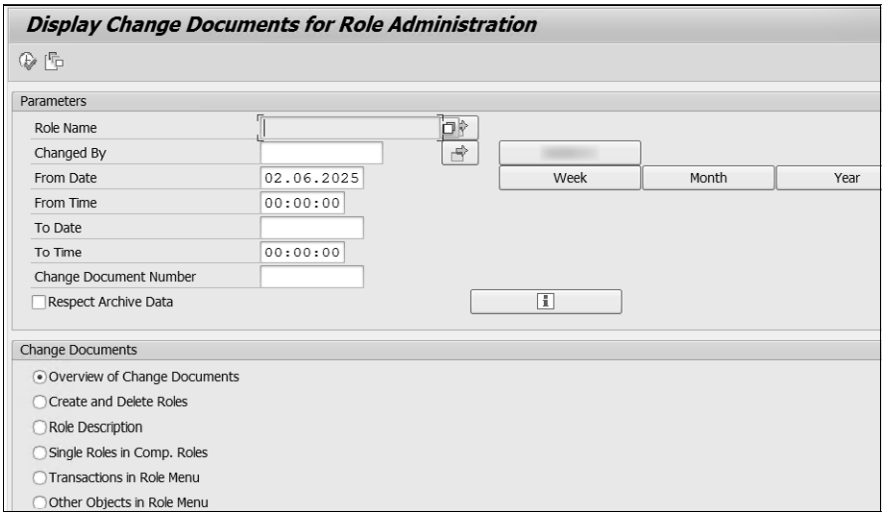


Figure 1.47: Selection Screen for Change Document for Roles

Most fields in the **Parameters** panel are similar to the previous report. The **Role Name** field offers the option for multiple selection, allowing you to choose one or more roles or even select all roles (with *) if desired. The period can be determined explicitly by entering date values in the **From Date** and **To Date** fields, or you can press the **Week, Month**, or **Year** button. Several options exist in the **Change Documents** panel to query changes related to a specific role attribute. For example, you can query modifications related to the creation or deletion of roles, single roles within composite roles, transactions in the role menu, and so on during the specified period. A reasonable limitation is that only one attribute can be selected at a time.

These examples make it evident that Transaction SUIM's change document reports are handy tools for investigations, audits, or regular monitoring activities.

1.9 Change Documents for Users

Change documents for a user can be retrieved in at least two ways: one is through Transaction SU01, and the other is via Transaction SUIM.

Let's execute Transaction SU01. Select the **Information • Change Documents for Users** menu option. The resulting selection screen is shown in Figure 1.48.

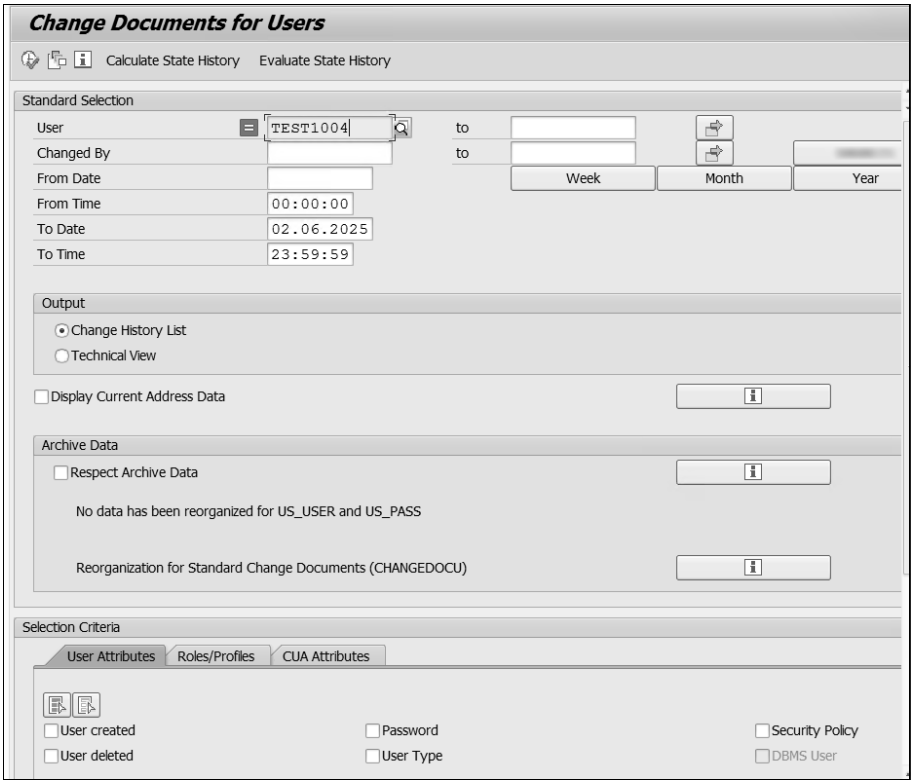


Figure 1.48: Selection Screen for Change Document for Users

In the **Standard Selection** section, there are some standard fields that we have also encountered in other reports. The **Output** section provides two options for the output format. The **Selection Criteria** section provides three panels. The first panel, **User Attributes**, offers several attributes to choose from, including **User Created**, **User Deleted**, **Password**, **User Type**, **Security Policy**, and others. The **Roles**/**Profiles** tab, shown in Figure 1.49, provides the option of choosing role or profile names to query role assignments for the selected users. The fields are enabled for multiple choice, and wildcards also can be used. The third tab is enabled if CUA is configured in your environment.

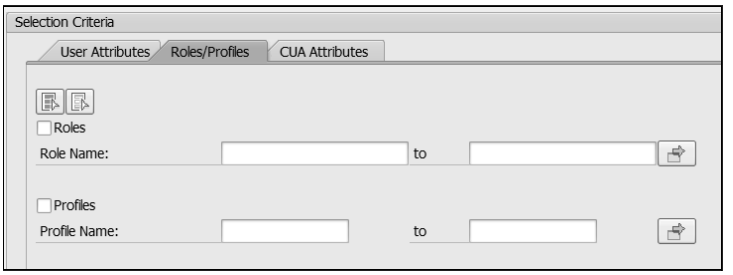


Figure 1.49: Roles Tab of Input Screen for Change Documents for Users

For example, we will run the report for the users **T_PKM*** for the last month, with all attributes selected in the **User Attributes** tab and * entered for the roles in the **Roles**/**Profiles** tab. The output is displayed in Figure 1.50.

Number of Selected Change Documents: 7

System [redacted] **Client** [redacted] **User** [redacted] 02.06.2025 21:09:43

Selection Criteria:

User	I	CP	T_PKM*
From Date			03.05.2025
To Date			02.06.2025

User	Date	Time	Changed By	Action	Old value	Text	New value	Text for the New Value
T_PKM1	14.05.2025	23:21:45	[redacted]	Role added			SAP_GRC_FN_BASE	GRC - Base role to run GRC applic
	15.05.2025	22:17:18		Role added			SAP_GRC_FN_ALL	GRC - Power User
				Role added			SAP_GRC_FN_BASE	GRC - Base role to run GRC applic
		22:57:41		Role added			SAP_GRC_FN_BUSINESS_USER	GRC - Business User
T_PKM2	14.05.2025	23:21:45		Role added			SAP_GRC_FN_BASE	GRC - Base role to run GRC applic
	15.05.2025	22:57:41		Role added			SAP_GRC_FN_BUSINESS_USER	GRC - Business User
T_PKM3	14.05.2025	23:21:45		Role added			SAP_GRC_FN_BASE	GRC - Base role to run GRC applic
	15.05.2025	22:57:41		Role added			SAP_GRC_FN_BUSINESS_USER	GRC - Business User

Figure 1.50: Sample Output of Change Document for Users

1.10 Security Policies

For operational reasons, it may be necessary to implement stricter security measures for some users and more liberal measures for others. For example, user accounts with broader access to administrative tasks may be subject to a more stringent security policy to provide

more security to such accounts. The company may require such users to have longer passwords with higher complexity and fewer days to expiration than everyday users, so their passwords are changed more frequently. On the other hand, communication and system accounts that cannot be used interactively may be subjected to a liberal security policy. The communication accounts (type C) are subject to password rules such as a password expiration rule. Hence, their passwords expire after the number of days mentioned in the `login/password_expiration_time` parameter has elapsed. However, if these accounts are used to communicate regularly between two systems, the communication may fail after the account's password expires. To avoid such a situation, an organization may exempt communication accounts from the password expiry rule.

The good news is that security policies, such as stricter or more liberal ones, can be created and assigned to user account IDs to subject them to more rigorous or less stringent security requirements. The transaction code used to create security policies is Transaction SECPOL. A security policy developed by Transaction SECPOL is a set of attributes and their values. When a user assigned a security policy logs in, the values of the attributes mentioned in the security policy take precedence over the same attribute values stored in the system profile. Security policies are assigned to users via Transaction SU01, and only one security policy can be assigned to a user.

The rest of this section will walk you through how to create a security policy for communication accounts to exempt them from the password expiration requirement.

Start by executing Transaction SECPOL, which opens the initial screen shown in Figure 1.51.

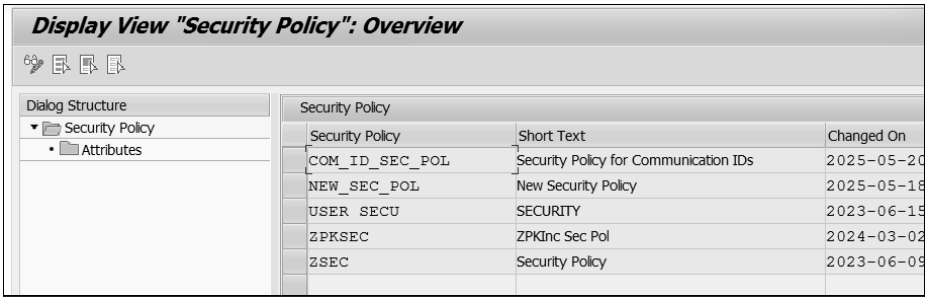


Figure 1.51: Initial Screen of Transaction SECPOL

Click the **Change/Display** icon so that the **New Entries** icon appears. Now click the **New Entries** icon. The input screen shown in Figure 1.52 appears. Enter the name of the **Security Policy** and a short description, then click **Save**. The system will now display all the security policies existing on the system, including the new one.

Click the newly created security policy to choose it, then click the **Attributes** icon. The following screen (see Figure 1.53) displays a table that shows attributes and their corresponding values. As this is a new security policy, the table is currently blank, with no attributes or values. Also, initially, it is grayed out, and new data can not be entered. Click the **New Entries** icon. The grid now becomes white, ready to accept your input.

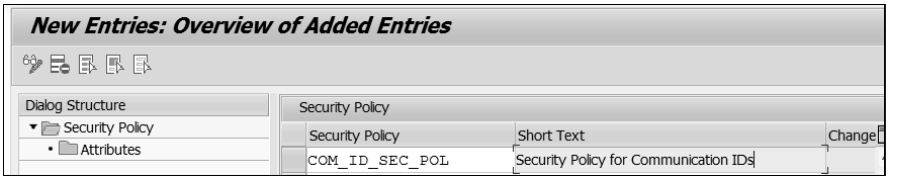


Figure 1.52: Input Screen to Create New Security Policy

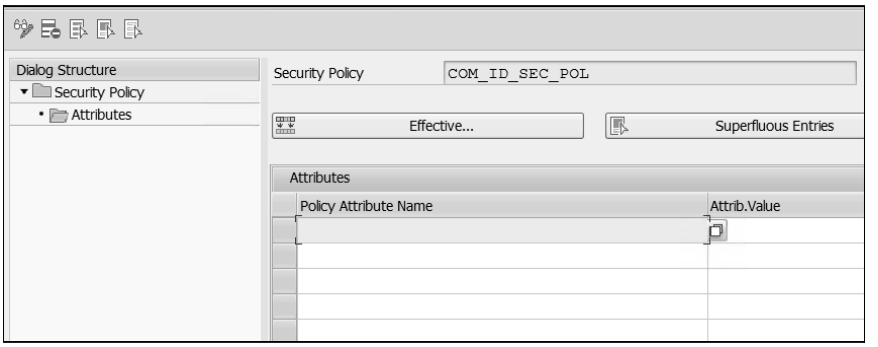


Figure 1.53: Enter the Attributes and Their Values

There is a match code search icon to the extreme right of the first cell in the **Policy Attribute Name** column. Click it. A new popup screen appears, as shown in Figure 1.54, displaying all the attributes available that can be added to the security policy.

Type	Policy Attribute Name	Long Field Label	Default
1	CHECK_PASSWORD_BLACKLIST	Check the Password Blacklist	1
1	MIN_PASSWORD_DIGITS	Minimum Number of Digits	0
1	MIN_PASSWORD_LENGTH	Minimum Password Length	6
1	MIN_PASSWORD_LETTERS	Minimum Number of Letters	0
1	MIN_PASSWORD_LOWERCASE	Minimum Number of Lowercase Letters	0
1	MIN_PASSWORD_SPECIALS	Minimum Number of Special Characters	0
1	MIN_PASSWORD_UPPERCASE	Minimum Number of Uppercase Letters	0
2	MIN_PASSWORD_CHANGE_WAITTIME	Minimum Wait Time for Password Change	1
2	MIN_PASSWORD_DIFFERENCE	No. of Different Chars When Changing	1
2	PASSWORD_CHANGE_FOR_SSO	Password Change Req. for SSO Logons	1
2	PASSWORD_CHANGE_INTERVAL	Interval for Regular Password Changes	0
2	PASSWORD_COMPLIANCE_TO_CURRENT_POLICY	Password Change After Rule Tightening	0
2	PASSWORD_HISTORY_SIZE	Size of the Password History	5
3	DISABLE_PASSWORD_LOGON	Disable Password Logon	0
3	DISABLE_TICKET_LOGON	Disable Ticket Logon	0
3	MAX_FAILED_PASSWORD_LOGON_ATTEMPTS	Maximum Number of Failed Attempts	5

Figure 1.54: All Available Attributes

The first column of the screen is **Type**, with three values, 1, 2, and 3, entered. This means there are three types of attributes to choose from:

- **1**: Attributes related to password rules (password length, lowercase, uppercase, etc.)
- **2**: Attributes related to password change policies (e.g., password expiry time)
- **3**: Attributes related to logon restrictions (maximum number of wrong logon attempts to lock the ID, etc.)

Under each of these types, many available attributes can be selected. As you are creating this security policy for communication accounts, the aim is to prevent password expiration for these accounts. To achieve this, select only one attribute for the security policy—**PASSWORD_CHANGE_INTERVAL**, as shown in Figure 1.55—and set its value to "0" in the **Attrib. Value** field. Note that the attributes available in Transaction SECPOL are not the same as the profile parameters.

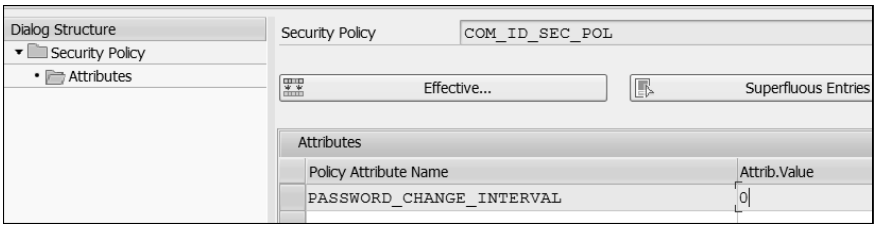


Figure 1.55: Entering Attributes for Security Policy

Save the security policy. Now it is ready to be assigned to users—specifically to the communication users in this case. This can be achieved through Transaction SU01.

Just as you liberalized one attribute for communication accounts through the security policy in this example, you can also enforce more stringent security for some users by creating a new security policy and adding appropriate parameters and their respective values.

1.11 Miscellaneous User Management Topics

In this section, we will briefly discuss some concepts related to user management. We'll cover naming conventions, buffers, and inactive users.

1.11.1 User Naming Conventions

Using a user naming convention to name users in the SAP environment may not sound very important, but it is one of the best practices for security. User management can become messy without a prudent naming convention. For dialog use, user organizations use numerous rules to create user IDs, such as the following:

- <First initial> + <Last Name>—for example, the user ID for John Doe is JDOE. If some users have similar names, you can append the user ID with one or two numeric characters—for example, JDOE1 for Jane Doe.

- <Name initials> + <Last three characters of personnel number>.
- <User type> + <A random, eight-digit number>. This is an example of a cryptic ID.

Many options are available for devising a user naming convention. However, you should choose one that avoids complexity in user management, identifies users via their user ID, complies to privacy laws (doesn't use personal information for a user ID), and honors legal requirements (sometimes, this means using a cryptic user ID).

User naming conventions should also be used for nondialog generic IDs, such as the communication IDs used for communication among systems, those used by systems for running workflow and background jobs, and even test users in test systems so that they can be easily distinguished from production users.

1.11.2 User Buffer

In SAP, individual permissions are assigned through authorization objects—for example, an authorization object that gives access to separate tables in `S_TABU_NAM`. This object has two fields, one for the **Table Name** and one for the **Activity**. You can add this authorization object to a role: Enter a table name for the **Table Name** field, such as "USR02", and a numeric value for the activity, such as **Activity = 3 (Display)**. This authorization is for display-only access to table `USR02` and thus the profile of this role contains this display authorization for table `USR02`. A user can have multiple roles, with several profiles assigned to them. When the user logs in to the system, a user buffer is created for the user, which contains all the authorizations from all the profiles assigned to the user (see the example in Figure 1.56). When the user attempts to run a transaction, the SAP kernel checks the buffer to verify if the user has sufficient permission to execute the transaction. If the user's buffer passes all the checks, then the user can run the transaction.

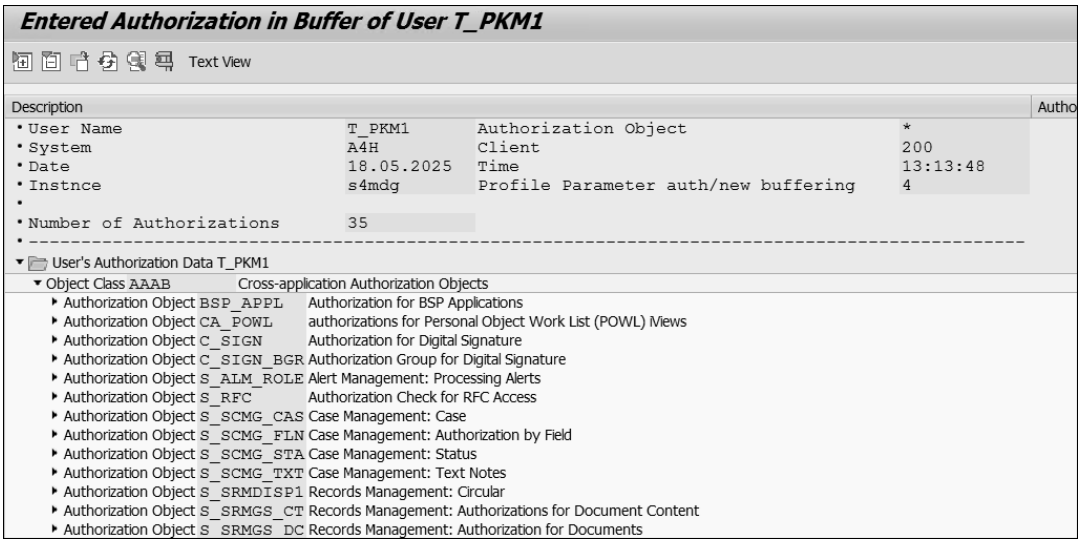


Figure 1.56: Sample Display of User Buffer in Transaction SM56

The user buffer can be displayed through Transaction SU56. If a user is logged on and a new role is assigned, the authorizations from the role are not immediately transferred to the user's buffer. The user must log out of SAP and then log in again to achieve this effect. However, if profile `SAP_ALL` is added to the user's profile, the log out/in process is not required, and the authorizations get assigned to the user buffer immediately.

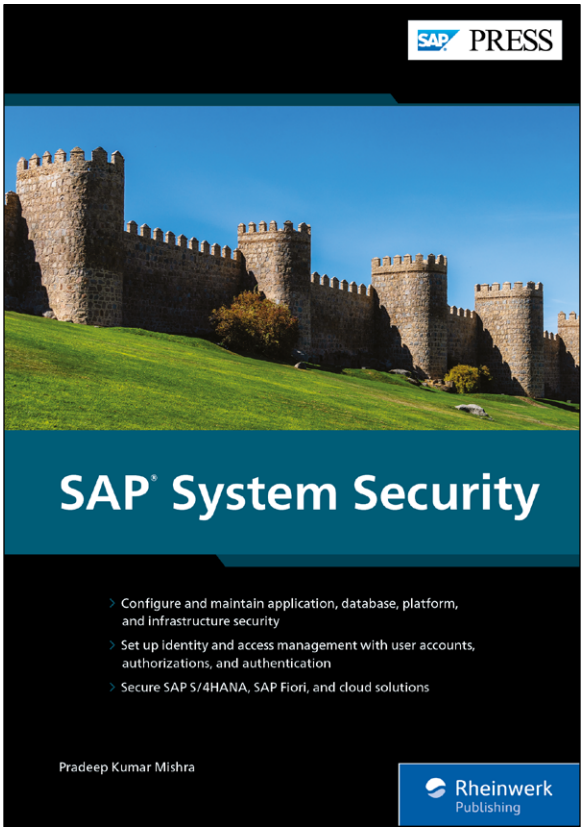
1.11.3 Inactive Users

When users retire or leave a company, their user IDs need to be deactivated. Many regulations (like the Sarbanes-Oxley Act [SOX]) require such user IDs to be deactivated within a reasonable time interval. Also, it is not uncommon in many organizations to have user IDs in the SAP environment that are never logged on. Some organizations run a periodic report to identify all the users who have not logged on for a specific period (say, one month) and lock those IDs. Such IDs can even be deleted if the users have not logged in for a significantly extended period (say, three to six months). The standard report RSUSR200 (which you can access via the **Users • By Logon Date and Password Change** option in Transaction SUIM) can be run to identify users who have not logged in to the system. Unused user IDs pose a security risk and should be removed (and deactivated if they have previously been active in the system). Removing such IDs will strengthen the system's security posture and help manage licensing costs.

1.12 Summary

User IDs are the objects users use to log in to SAP systems; hence, securing user IDs through appropriate system configuration, technical, or procedural policies is the first line of defense against unauthorized access to the system and preventing breaches. IDs can be created using a naming convention through transactions such as SU01 or SU10. Identity lifecycle management is an essential component of identity governance; IDs must be created and deactivated, and changes must be made promptly. Authentication and authorization are the other aspects of user ID maintenance, which will be covered in the following two chapters. Another critical aspect of security is regular auditing and monitoring of IDs. SAP provides several standard reports and transactions, such as Transaction SUIM, to audit and monitor user IDs. IDs can be subjected to stricter security measures by adding security policies.

In the next chapter, we'll discuss topics related to authentication techniques and protocols, the most important of which is SSO.



Pradeep Kumar Mishra

SAP System Security

- Configure and maintain application, database, platform, and infrastructure security
- Set up identity and access management with user accounts, authorizations, and authentication
- Secure SAP S/4HANA, SAP Fiori, and cloud solutions

www.sap-press.com/6189

The Author
Dr. Pradeep Kumar Mishra has more than 13 years of experience in SAP security and governance, risk, and compliance. He is certified in CISSP, CISA, and CRISC, and he specializes in securing complex enterprise SAP landscapes.

ISBN 978-1-4932-2774-7 • 622 pages • 04/2026
E-book: $94.99 • **Print book:** $99.95 • **Bundle:** $109.99

Rheinwerk Publishing