

User Administration :-

SAP has provided some standard user ID's

1. DDIC - will able to login with admin password.
(Basis team set the password)

2. SAP* - "pass" (New created client).

3. Early Watch Alert - will be logged to "066" client. for with password = support.

- When we install the system for every client there are user id's available by default.

⇒ Due to audit requirement there standard user ID's will be "LOCKED" Always.

⇒ At the implementation these ID's will be used by Basis team.

⇒ End user / Business never use these ID's.

⇒ These user ID's having full access in the SAP system. They are super users.

⇒ We have some standard profiles.

SAP-ALL

SAP-NBW

S-A. System

S-A. Admin

S-A. ABAP.

⇒ SAP-ALL - It's standard composite profile provided by SAP. need for Basis team

- Basis team is required to perform all tasks in the SAP system objects / T-codes.
- It contains all system objects and t-codes.
- It should not assign to any user.
- SAP-ALL is very critical and SAP* user is have this profile.
- No other dialog user have SAP-ALL profile

SAP-NEW:-

- It's also composite profiles which is usually assigned temporarily during an upgrade.
- It's contain all the necessary objects and T-codes for the users to complete their work during the upgrade.
- we need to remove once the activity has been completed.
- ⇒ These profile we can give Non-production system for temporary basis.
- ⇒ Why we are not using profiles creation / assignment to users?
- * After ECC 4.6C version onwards the Role Concept came.
- * Before this version we used to create profile & assign to users.

1. Single User Creation :- If any user who are joined the organization (or) project. they need SAP Access.

SPOC list given to us.

AC -> Authorization Controller.

SPOC -> point of Contact. (PMO Team)

in our security with out approval we never give access to any one for any activity.

→ The approval process there in any organization & the approval context list (Role sheet matrix) will provide to us at the time of KT.

- Some projects will have approval process like based on Country (or) models. etc. -

- | | |
|--------|--------|
| US | SD |
| UK | MM |
| India | RICO |
| etc. - | PP. |
| | etc. - |

12.1) For every request we should required the Ticket. (Remedy / Service Now)
with out ticket we will not work any request.

→ Some org. will drop a mail for any request.

13. URF (User Request Form) Contain all the user related information.

like:

User First Name, Country,
Last Name, Decimal Notation
Email ID, Validity, User Groups,
Department
Reference user ID / Clone ID / Mirror ID.

* ~~It may have GRC no need~~

* AD - Active Directory? - It contains all the user related information. (Reporting manager/line).
- When we joined any organization, our/user ID will be created in AD.

Ex: ITIM: Identity Tivoli management.

IDS: Internal Directory services.

(SAP tool) ← LDAP: Light weight Directory Active protocol

⇒ Generally AD will be connected to SAP system (or) GRC system when we give user ID's

The user details by default come.

* SU01 - User maintenance? -

It is used to create, change, lock/unlock, Delete, password, copy, user ID's.

→ It contains below tabs available.

Documentation, Address, Logon Data, SNC,

Default, Roles, profiles, parameters, Groups,

personalization, Licence type,

Interview:

- What are the mandatory fields to create user ID?

1. User ID.
2. user Last Name.
3. pass word.

with out give above details ~~user~~ user ID will not be create.

⇒ Based on the project to project the user ID Naming Conventional will be follow.

- They might go with user first Name Last Name.

Example: -

FirstName: Ramesh
LastName: - Mekala.

The user ID will be depends.
→ First Name of first word.

1. RMEKALA

→ 1st Name → Last Name.

2. RXMEKAL

→ Some common letter → Last Name.

→ Last Name of 1st letter.

3. MRAMESH

→ 1st Name

* The user ID contain maximum 12 letters.
length -

we will not give more than '12' letters.

⇒ How to create New user in SAP?

Execute TCode: SU01

* give the user ID as per the New user ID Naming Convention. (Depends project policy).

* and fill the required details based on details provided in the Form (URM) (or) Mirror user ID (Reference user ID).

* Logon Data: -

User type: update the user type that you want to update user - like

1. Dialog
2. System
3. Service
4. Communication
5. Reference.

password: update the Initial password (Sap@123)

later user can change the password.

- It is mandatory to follow the password parameters.

Validity period: as per the request

update the "Validity From & Validity through."

* Default Tab: - we need to of Logon Language,
Date format,
Time format,
Start Menu,

* Spool Control: Specifying the output device
like printer.

* personal Time Zone: - we can update the
time zone based on location.

* parameters: - It's help to open some trade
autofilled values when create a Trade.

- This field can be filled with proposed
values from SAP memory using a parameter.

* Simply say ~~free~~ pre-defined field in SAP.

Ex: Trade MB21 there are field for "site"

* Roles: - user Role is one of important
step to be assign to user.

- Security team/people will assign the role
to user to perform activities based his position.

* profiles: - we have discussed in earlier page.

personalization: This is rarely used tab in SU01

- I am sure that no security consultant will use.

& doesn't know the purpose of

⇒ It is used to assign the personalized object which has some default settings such as.

Ex: workflow/Approval.

User Layouts.

Table ~~SP~~ SPERS_OBJ hold the information

⇒ Groups: - "SUGR" is used to create user groups.

- It is used to identify/classify the users in the organization.

- It is also used to give administrative rights to users.

- User groups are client dependent, so have to create groups in each client/system manually.

* There are 3 ways to assign users to user groups

1. using SUGR T-code

2. Group tab in SU01

3. Logon data tab in SU01.

* User Group for Authorization check:

- Only one group can be assigned.

- It is relevant for the object S-USER-GRP

⇒ General user Groups: Here we can assign multiple user group to the user.

— But it is not relevant for object.

S - USER - GRP.

— User group all protecting administration activities on user master record itself.

Ex: password reset.

user validity change. etc.

⇒ Licence Type: - It's used to specify the type of users.

— Licence will be used in production system only.

— Based licence type 'SAP' will charge the client -

— For solution manager system there is no charges as it is provided SAP.

→ When we scroll down Licence Page.

we will find out

CAT-I professional licence (SAP Application professional) like developer, & Administrator.

— user can perform functional operation & administration activities. It is full charged.

— We can use Create, Change, / Display no meta

— It's who perform system admin tasks.

like: managing performance.

Application support latest version, packages etc.

2. SAP Application Limited professional :- CAT-2

This type of user can perform only operational activity only. & ~~not~~ not system admin activities

- It's only changeable access & rest of all Display access.

3. CAT-III SAP Application Employee :-

* Only Display Access.

- user who is authorized to access the licensed software, the purpose of executing t-codes.

like ; Desktop procurement self service,

Travel planning, Expenses reporting.

Talent management self services. etc -

4. CAT-IV SAP application ; For end users.

User Types :- Based on the user ID usage will set the user types in SUCO.

1) Dialog : (A)

⇒ Users who are communicating/interactive SAP system (GUI) directly.

- These users are possible with SAP GUI

⇒ Dialog user can login in to the system using interface called SAP GUI (Network version of GUI) & it can be download from SAP marketplace

⇒ Multiple login is possible with SAP GUI. But it can be restricted by the parameters.

* login/Disable - multi-GUI - login.

⇒ password will be expired.

= During the first login, the user has to change the ^{initial} password

Ex: End users, Support users. etc.

2) System Type : (B)

⇒ Users who are not communication with SAP system interactively.

⇒ All system types are nothing but Background users, (Are used for background processing & communication with in SAP)

⇒ System users can not login by using SAP GUI.

- ⇒ password will not expired.
- ⇒ System type user ID's will be used with the system.
- ⇒ No Logon is possible.

Ex: RFC, CUA, Remote client copy
(such as RFC users for ALE, Workflows, TMS, and CUA).

3. Communication Type: - (C)

- ⇒ These type of users also background users.
- ⇒ Communication type users will be used between the system.
- ⇒ They are not connect by using SAP GUI.
- ⇒ password will not be expired.
- ⇒ No Logon is possible.

Ex: CUA, RFC. etc. - -

4. Service user Type: (S) :-

- ⇒ These users are like enormous group of users. (they are not technically sound)
- ⇒ The password will not check for expired / Initial passwords during 1st logon.
- ⇒ Service users same like dialog users.
- ⇒ Service users can login by using SAP GUI.

⇒ password is not required to change initially.

Ex:- Test, Demo, Training etc.

5, Fire Fighter ID (used to give wide range of access to user in emergency situation with limited period of time)

Reference users (L) :- Is used to give extra privileges to user when some other user goes on vacation.

* used to give extra privileges if user exceed more than 312 profiles.

User-A \leftarrow User-B Example.

#> Chang Documents For the User :-

- Is used to identify the changes happend to users master record.

1. Go-to - SU01 → Information → change document for users / roles.

2. Go-to - SU1M (T-code)
↳ chang document.

#> User Lock Statuses :-

1. 0 → user is NOT locked. Globally.

2. 32 → user is locked by system admin (CUA)

3. 64 → user is locked by system admin locally.

4. 128 → user is locked due to incorrect logons and system

5. 192 → user is locked due to incorrect logon & system admin.

→ We can see these lock code in

Go-to - SE16 → USR02 → Table →

User Termination / Deletion / Rollout :-

→ When ever its user will rollout from the project (or) Contract is over we need to terminated (or) delete the user as per the process.

→ Manager will raise a Ticket (Request) to terminate the "SAP user ID" for all the environment (PROD-NONPROD) system.

→ Then once the security receive the request. they will follow the below process in Generally. (project to project)

1. Go-to-^{SU01} Locks the user ID.
2. Change the user type to Reference.
3. Move the user to Terminated / deleted / Expired user Groups. (Based on Company policy)
4. Change the user validity Date to yesterday
5. Remove the Roles & profiles also Licence type.

Mass user administration :-

- T-Code → SUIO
- It is used to create, modify, lock/unlock, delete and assign roles/profiles massively.
 - To ~~us~~ create single user we can use SUO.
 - To setup number of users (or) update users access we cannot do by SUO1. As it's time consuming.
 - We can do it by using SUIO, LIMW, SECAT.

⇒ Disadvantages of SUIO :-

- 1) Address data cannot be maintained for every user separately.
 2. password cannot be initiated.
 3. Single values can be assigned to multiple users but different values cannot be maintained for different users.
- ⇒ To avoid 18 number user in Initial screen in SUP we can go with Authorization data opt there we can give 'N' number of user ID's to perform one activity.

#> Mass Lock/Unlock Activity: - SUP/EW25 T-codes

In real time basis team will perform some System refresh/Downtime/Release activities during that they will ask us to lock/unlock ID's.

- Except some user ID's like Basis & Security & people who are going to perform that activity.