NOTE NOVEMBER 2007

SAP® standard / special users

With the installation of a SAP® system, some standard users are created in the individual clients or system environments. Some of these users have already high authorizations from the beginning, and of course most of them have standard passwords assigned that are generally known.
These special users need special treatment and special protection.

1. SAP*

The user SAP* exists right after the installation in **all** clients. He has the composite profile SAP_ALL assigned and with that all relevant authorizations for the system set up.

SAP® has implemented a backdoor [coding] for this user. If someone deletes the user SAP*, a login is possible with the standard password **PASS** including the corresponding SAP_ALL authorizations.

To prevent a login of the SAP* after a deletion, the parameter *login/no_automatic_user_sapstar* can be utilized.

With a parameter setting to 0 the login is possible. Any value higher than 0, prevents a login after the deletion.

The standard password for this user directly after the installation is **06071992.**
The standard password after deletion is **PASS.**

The preferable method to protect this user is the deactivation of SAP* :

- Remove all authorizations from this user.
- Lock the user account.
- Set the parameter login/no_automatic_user_sapstar to 1.
- Activate the audit log for this user.

You can also consider to assign this user to a user administration group that is protected by a dual control principle.

This report **RSDELSAP** deletes the user SAP*in the client 066. The corresponding source code is not active but available.

2. DDIC

The user DDIC is established in the client 000 and 001 with the installation [and copies of these].
This standard user is uitilized to cover installation and release updates including changes to the data dictionary. The use of the transport management system is restricted to *Display only*.
This is the protection against direct developments.
As the technical steps related to this process are initiated in the client 000, the DDIC only needs to be a dialog user in this client.

In all other clients he can be set to the user type “system”.
The standard password for this user directly after the installation is **19920706.**

The report **RDDPWCHK** allows to check the password that is assigned to the user DDIC. In case the password matches, the dialog window will be closed. For mismatches the message *False* is displayed.
The counter for falso login does not count these password attempts.

3. TMSADM

The user TMSADM is automatically created at the set up the change and transport management system in the client 000.
His user type is “Communication”, and he is utilized for transports by the CTS.

He has the profile S_A.TMSADM assigned that authorizes the use of RFC with display of the development environment e.g. as well as writing to the file system.

The standard password for this user directly after the installation is **PASSWORD**.

4. SAPCPIC

The user SAPCPIC is created as a “communication” user at the installation and is utilized especially for EDI. The standard profile S_A.CPIC restricts the access to the use of RFC.

This user is coded into the function module INIT_START_OF_EXTERNAL_PROGRAM together with his standard password. This needs to be considered in case of password changes for this user.

The standard password for this user directly after the installation is **ADMIN**.

5. EARLYWATCH

The user EARLYWATCH is created in the client 066 at the installtion. He can be utilized for remote control by SAP® and is only set up with some standard authorizations S_TOOLS_EX_A for performance monitoring. The user is to be locked in general, and can be unlocked upon request.

Evaluation

For the evaluation of the passwords you may use the report **RSUSR003**.

6. SAP* in J2EE

The user is established with full authorizations for the administration. With regard to security, the user has no standard password assigned.

To utilize this user as emergency user the properties in the UME need to be maintained.

Setting the *ume.superadmin.activated* property to *true* will activate the use of this user for emergency cases.

Setting a password in *ume.superadmin.password* will then activate the user finally after the restart of the engine.

While the user SAP* is in use, all other users will be inactivated during this time.

When the system is fixed, the deactivation can be achieved by setting the *ume.superadmin.activated* property to *false*.

7. J2EE_ADMIN_<SID>

This user is the Java standard user with full administration authorization in this environment. The password is to be assigned during the set up. High complexity is recommended for this password.

8. J2EE_GUEST

This user is a Java standard user who can be utilized for anonymous access. The user is locked per default. The password is assigned during the installation.

9. SAPJSF_<SID>

This user is a standard communication user for LDAP [Lightweight Directory Access Protocol] data sources.

10. ADSuser

This standard user is utilized for the communication between Java and ADS [Adobe Document Service].

11. caf_mp_scvuser

This standard user is utilized in the context of the Composite Application Framework (CAF) core transport system and communication with other Java services.

Special user	Client 000	Client 001	Client 066	Initial pass	Xtra
SAP*	X	X	X	06071992	PASS Lock and deactivate
DDIC	X	X		19920706	SYSTEM user in prod.
TMSADM	X			PASSWORD	
SAPCPIC	X	X		ADMIN	Cave! PW coded
EARLY WATCH			x	SUPPORT	Lock
SAP* in J2EE				Assigned at activation	
J2EE_ADMIN				Assigned during installation	
J2EE_GUEST				Assigned during installation	
ADSuser				Assigned during installation	
caf_mp_scvuser				Assigned during installation	

Any changes to the passwords of the J2EE users after installation can be performed with the help of the UME and the AS Java administration toolset.