NOTE JUNE 2009

Report RSUSR003

The report **RSUSR003** allows the cross client password review of the SAP® standard users SAP*, DDIC, SAPCPIC and EARLY WATCH as well as a check of the respective system login parameters.

In the past when the report was selected for execution it was required to have matching authorization to change the user group SUPER and to perform client maintenance.

S_TABU_DIS with ACTVT=02 for DICBERCLS= SS
S_TABU_CLI with CLIDMAINT=X

[via *VIEW_AUTHORITY_CHECK*] and

S_USER_GRP with CLASS=SUPER and ACTVT=02

This concept was revised.
The above critical authorization did not allow auditors to actually run the reports by themselves.

Therefore the new authorization object **S_USER_ADM** was created and implemented. It is similar to the object S_ADMI_FCD.

This object is already available with the support packages:

SAP_BASIS	46C	SAPKB46C48
SAP_BASIS	46D	SAPKB46D36
SAP_BASIS	610	SAPKB61039
SAP_BASIS	620	SAPKB62039
SAP_BASIS	640	SAPKB64002

The authorization object **S_USER_ADM** consists of the one field **S_ADM_AREA** and can obtain up to three different field values:

CHKSTDPWD:
Display of SAP® standard users (e.g. SAP*) with a check on standard passwords

PRGN_CUST:
Maintenance of the customizing table PRGN_CUST (Customizing table for user and authorization administration)

SSM_CUST:
Maintenance of customizing table SSM_CUST (Set up for Session Manager / profile generator)

The successful execution of the Report **RSUSR003** requires the authorization: authorization object

S_USER_ADM with value **CHKSTDPWD** for field **S_ADM_AREA**.

The above set up only allows Display access.

In case the authorization is not available in the user master, the report still checks for the prior mentioned authorization to maintain clients and the group SUPER.

Please also see OSS notes 704307 and 717123.

The execution of this report is logged in the SysLog [transaction **SM21**] with high priority in the group *E0* with sub-name *3* and the following text:

Program RSUSR003 Reports Security violation

This entry results from the following source code section in **RSUSR003**:

```
*write syslog-entry about this report
        ls_syslog-program = SY-REPID
        ls_syslog-text = ‘Security violation‘

CALL FUNCTION ‘RSLG_WRITE_SYSLOG_ENTRY‘
        EXPORTING SL_MESSAGE_AREA = ‘E0‘
                        SL_MESSAGE_SUBID = ‘3‘
                        DATA_AREA = ls_syslog.
```

The report is executable e.g. via transaction **RSUSR003** or **S_ALR_87101194**.