

## Summary

### Symptom

Password-based logon attempts (to ABAP systems as of Release 7.00 / NetWeaver 2004s / SAP ERP 2005) fail, although the user has entered a supposedly correct password in a front end component or in a destination (of another system).

However, a (direct) SAPGUI logon with the same password is successful.

### More Terms

USR02, CODVN, BCODE, PASSCODE, hash password, logon password

### Cause and Prerequisites

As described in Note 862989, ABAP systems as of NetWeaver 2004s (7.00) support passwords of up to 40 characters, whereby they differentiate between uppercase and lowercase.

In earlier ABAP Releases (prior to 7.00), passwords could only be comprised of a maximum of 8 characters, whereby lowercase letters that were entered were automatically changed to uppercase letters.

If, in a newer ABAP system (as of Release 7.00), a downwardly incomplatible password is unknowingly granted (see below), and if the front end or middleware components are not able to process such passwords correctly, logon problems inevitably occur. This is usually due to the (invisible) automatic conversion from lowercase to uppercase letters.

**The problem is due to the fact that the password entered by the user does not arrive at the server in the same form, but is changed either during input or during the transmission (in which many components are involved).**

### Term definitions

- o **Password: downwardly compatible / downwardly incompatible**

A (plain text) password is downwardly compatible if it consists of a maximum of 8 characters and contains no lowercase letters.

A (plain text) password is downwardly incompatible if it consists of more than 8 characters or contains at least one lowercase letter.

Older ABAP systems support downwardly compatible passwords only. In newer ABAP systems (as of Release 7.00), downwardly incompatible as well as downwardly compatible passwords may be granted. **Since lowercase letters that you enter are now no longer changed to uppercase letters, the passwords granted in newer ABAP systems are normally downwardly incompatible.**

- o **Hash password procedure / Code versions**

ABAP systems do not save passwords in plain text, but instead calculate a hash value and save this together with the meta information using the hash password procedure ("code version").

This information is stored in the user master record and it is analyzed during the password check: A hash value is determined, using the code version specification (from the user master record), from the plain text password to be checked and it is compared with the reference hash value (from the user master record).

The quantity of the hash password procedure supported is release-dependent, whereby newer releases always support all procedures of preceding releases. This ensures that a password logon is also possible after a release upgrade.

Only the hash password procedures available as of Release 7.00 also support the processing of downwardly incompatible passwords. Older hash password procedures support downwardly compatible passwords only.

Whether downwardly compatible passwords are supported or expected during a password logon depends primarily on the specifications (code version) saved in the user master record.

## Solution

- o **When using the technical user (in RFC destinations):**

We strongly recommend that you use the SYSTEM user type on the server (or also SERVICE, provided a SAPGUI capability is required), since the password has unlimited validity only for these user types (see Note 622464).

If the password should be entered in an RFC destination of an older system (= RFC client), it must be granted as a downwardly compatible password on the server. For users of the SYSTEM or SERVICE type, this is always possible, even if the password rules of the system normally compel the use of downwardly incompatible passwords (for example, by login/min\_password\_lng > 8 or login/min\_password\_lowercase > 0).

- o **When using older front end or middleware components and password logon of "normal" user (DIALOG type):**

In this case, it is not practical to change the passwords of the (numerous) users affected (as in the above case with technical users). Instead you must replace the obsolete front end or middleware components.

Note 792850 describes as of which version level certain front end or middleware components support the interaction with downwardly incompatible passwords. In addition, you may need to update other software components (attached to these components), as well as those of external providers. This is particularly the case if these components lead their own password input dialog and are not able to support downwardly incompatible passwords (according to the above definition of the term).

For the moment, you can set the profile parameter login/password\_downwards\_compatibility on the server to the value 2 or 3 for test purposes. In this case, the server checks if the client has sent a matching downwardly compatible password for the expected downwardly incompatible password (that is, a password that is 8 characters long and converted to uppercase). If this is the case, it is logged in the sys log (for error analysis purposes), and the logon is assessed as successful (for value 3). Using

**SAP** Note 1023437 - **ABAP syst: Downwardly incompatible passwords (since NW2004s)**

---

transaction RZ11, you can change the profile parameter dynamically, that is, without restarting the system.

---

### Header Data

Release Status: Released for Customer  
Released on: 07.02.2007 13:35:08  
Priority: Recommendations/additional info  
Category: Consulting

Main Component BC-SEC-LGN Logon and SSO

### Valid Releases

Software Component	Release	From Release	To Release	and Following
SAP_BASIS	70	700	700	X
SAP_BASIS	710	710	710	

### Related Notes

Number	Short Text
1032402	EasyDMS Logon issue
862989	New password rules as of SAP NetWeaver 2004s (NW ABAP 7.0)
817925	Case sensitive, extended length passwords in SAPLogonControl
807895	Incorrect logon data after remote login with SM59
792850	Preparing ABAP systems to deal with incompatible passwords