



## Neuerungen bei den Kennwortregeln in SAP (ab WebAS ABAP 7.0/ NetWeaver 2004s)

© IT AUDIT

Mit dem vorliegenden Dokument möchten wir einen Überblick über die Neuerungen und Änderungen im Bereich Kennwortregeln bzw. Anmeldeverfahren in SAP geben, die mit WebAS ABAP 7.0/NetWeaver 2004s ausgeliefert werden.

### **Kennwörter: Unterscheidung zwischen Groß- und Kleinschreibung; maximale Kennwortlänge**

[1] Die Kennwörter für das SAP-System waren bisher auf eine Länge von maximal 8 Zeichen beschränkt. Zudem wurde die Groß- und Kleinschreibung nicht berücksichtigt. Dieses wird sich mit WebAS ABAP 7.0/NetWeaver 2004s ändern.

[2] Bei neu vergebenen Kennwörtern wird ab WebAS ABAP 7.0/NetWeaver 2004s zwischen Groß- und Kleinbuchstaben unterschieden; zudem dürfen Kennwörter nun aus bis zu 40 Zeichen bestehen; bisher galt eine maximale Länge von 8 Zeichen. Bei neu installierten Systemen trifft dies sogleich auf alle Benutzer zu; bei Systemen, welche durch Upgrade von einem älteren Releasestand auf WebAS ABAP 7.00/NetWeaver 2004s entstanden sind, ist sichergestellt, dass sich alle Benutzer weiterhin mit ihrem alten Kennwort anmelden können. Im Benutzerstammsatz ist gespeichert, ob der Benutzer über ein neuartiges Kennwort oder über ein Kennwort alter Bauart verfügt; diese Information wird bei einer Kennwortprüfung ausgewertet: besitzt der Benutzer ein Kennwort alter Bauart, so werden die ersten 8 Zeichen des Kennworts in Großbuchstaben konvertiert; die restlichen 32 Zeichen müssen Leerzeichen sein. Andernfalls wird das Kennwort in voller Länge und ohne Konvertierung in Großbuchstaben ausgewertet. In Unicode-Systemen dürfen Unicode-Zeichen in Kennwörtern verwendet werden.

[3] Zur weiteren Steuerung der Kennwortzusammensetzung werden (ab SAP NetWeaver 6.40) neue Profilparameter eingeführt:

- 'login/min\_password\_lowercase'  
Dieser Parameter gibt an, wie viele Zeichen in Kleinbuchstaben in einem Kennwort enthalten sein müssen. Der Defaultwert beträgt '0', so dass Kleinbuchstaben nicht zwingend gefordert sind.
- 'login/min\_password\_uppercase'  
Dieser Parameter gibt die minimale Anzahl von Zeichen in Großbuchstaben in einem Kennwort an. Der Defaultwert beträgt '0'.
- 'login/password\_downwards\_compatibility'  
Hierdurch wird der Grad der zu erreichenden Abwärtskompatibilität (der Hash-Werte der Kennwörter) festgelegt.

### **Kennworthistorie**

[4] In der Kennworthistorie werden die Kennwörter gespeichert, die der Benutzer im Zuge einer Kennwortänderung vergeben hat. Wobei zu beachten ist, dass vom Benutzeradministrator gesetzte Kennwörter nicht gespeichert werden. Das System hindert den Benutzer daran, die zuletzt verwendeten und in der Kennworthistorie gespeicherten Kennwörter erneut zu verwenden. Bisher war die Kennworthistorie auf 5 Einträge begrenzt; nun kann die Größe der Kennworthistorie per Profilparameter ('login/password\_history\_size') festgelegt werden. Die Kennworthistorie kann maximal 100 Einträge umfassen (Maximalwert).

### **Sperrfrist für Kennwortänderung**

[5] Um ein Aushebeln der Kennworthistorie zu verhindern, darf ein Benutzer sein Kennwort erst nach Ablauf einer Sperrfrist, die über den Profilparameter 'login/password\_change\_waittime' vorgegeben werden kann, erneut ändern. Ausgenommen hiervon sind Kennwortänderungen, bei denen der Benutzer vom System zur Änderung des Kennworts aufgefordert wird. Der Parameter kann auf maximal 1.000 Tage eingestellt werden (Maximalwert).

### **(Vorzeitige) Kennwortänderung bei verschärften Kennwortregeln**

[6] Es ist jetzt möglich, gezielt nur diejenigen Benutzer zur (vorzeitigen) Änderung des Kennworts aufzufordern, deren aktuelles Kennwort nicht mehr den aktuellen (verschärften)



## Neuerungen bei den Kennwortregeln in SAP (ab WebAS ABAP 7.0/ NetWeaver 2004s)

© IT AUDIT

Kennwortregeln genügt. Hierzu muss der Profilparameter 'login/password\_compliance\_to\_current\_policy' auf den Wert '1' gesetzt werden.

### Gültigkeitsdauer ungenutzter (Initial-)Kennwörter

[7] Kennwörter, die vom berechtigten Benutzer nicht genutzt werden, stellen ein grundsätzliches Sicherheitsrisiko dar. Daher sollte die Gültigkeitsdauer solcher Kennwörter begrenzt werden. Bei SAP wird hierbei zwischen initialen Kennwörtern, d.h. Kennwörtern, welche durch den Benutzeradministrator vergeben wurden und vom Benutzer bei der nächsten Gelegenheit zu ändern sind, und nicht-initialen Kennwörtern, d.h. Kennwörtern, welche vom Benutzer selbst gesetzt wurden, unterschieden. Von dieser Regelung ausgenommen sind (technische) Benutzer vom Typ 'SERVICE' und 'SYSTEM'.

[8] Zur Steuerung der Gültigkeitsdauer stehen zwei neue Profilparameter zur Verfügung (nach SAP NetWeaver 6.40):

- Parameter 'login/password\_max\_idle\_initial'  
Dieser Parameter gibt die maximale Frist (in Tagen) an, in der ein Initialkennwort (vom Benutzeradministrator eingerichtetes Kennwort) gültig bleibt, wenn es nicht benutzt wird. Nachdem diese Frist abgelaufen ist, kann das Kennwort nicht mehr zur Authentifizierung verwendet werden. Der Benutzeradministrator kann die Kennwortanmeldung durch Zuweisen eines neuen Initialkennworts reaktivieren.  
Der Defaultwert beträgt '0', so dass die Prüfung standardmäßig deaktiviert ist. Zulässige Werte sind '0' bis '24000'.  
Dieser Parameter ersetzt die beiden Profilparameter 'login/password\_max\_new\_valid' und 'login/password\_max\_reset\_valid' (siehe auch Anmerkungen zu den beiden Parametern in SAP-Hinweis '450452'), so dass nicht mehr zwischen dem ersten und dem nachfolgenden Setzen eines Kennwortes durch den Benutzeradministrator bzgl. der Begrenzung der Gültigkeit der resultierenden Initialkennwörter unterschieden wird.
- Parameter 'login/password\_max\_idle\_productive'  
Der Parameter gibt die maximale Frist (in Tagen) an, in der ein vom Benutzer gewähltes (produktives) Kennwort gültig bleibt, wenn es nicht benutzt wird. Nachdem

diese Frist abgelaufen ist, kann das Kennwort nicht mehr zur Authentifizierung verwendet werden. Eine Reaktivierung der Kennwortanmeldung ist nur durch das Zuweisen eines neuen Initialkennworts durch den Benutzeradministrator möglich.

Der Defaultwert beträgt '0', so dass die Prüfung im Standard deaktiviert ist. Zulässige Werte für diesen Parameter sind '0' bis '24000'.

### Überarbeitung von Vorgabewerten von Profilparametern

[9] Die Vorgabewerte (Defaultwerte) bestimmter sicherheitskritischer Profilparameter im SAP-System wurden geändert:

- Parameter 'login/failed\_user\_auto\_unlock'  
Die bisherige Standardeinstellung von '1', woraus eine automatische Freischaltung der aufgrund von fehlerhaften Kennworteingaben gesperrten Benutzer um 24:00 Uhr erfolgt, wird auf '0' umgestellt, so dass diese sog. "Fehlalarmesperren" unbegrenzt lange gültig bleiben.
- Parameter 'login/fails\_to\_user\_lock'  
Die maximale Anzahl fehlerhafter Kennworteingaben bevor ein Benutzer vom System gesperrt wird ("Fehlalarmesperre"), wird im Standard von 12 auf 5 reduziert.
- Parameter 'login/no\_automatic\_user\_sapstar'  
Der Defaultwert des Parameters wird von '0' auf '1' umgestellt, so dass bei gelöschtem Benutzerstamm 'SAP\*' eine Anmeldung am System mit dem allgemein bekannten (hart codierten) Initialkennwort dennoch nicht möglich ist.
- Parameter 'login/min\_password\_lng'  
Die Standardeinstellung der Kennwortlänge (in Zeichen) wird von 3 auf 6 Zeichen erhöht.
- Parameter 'login/ticket\_expiration\_time'  
Anmeldetickets sind nur noch 8 anstelle 60 Stunden lang gültig.

[10] Insbesondere die Änderungen der Defaultwerte der sicherheitskritischen Parameter entsprechen weitestgehend den Anforderungen der Revision.

Stand der Informationen: 03.07.2006