

Übersicht über Empfehlungen zu ausgewählten SAP-Sicherheitseinstellungen

Version 1.1

Inhaltsverzeichnis

1. Allgemein	3
2. Kennwortrichtlinien.....	3
3. Anmeldeverfahren	4

Tz.	Parameter	Erläuterung	Defaultwert	Empfehlung
1. Allgemein				
1.	rec/client	Parameter, der angibt für welche Mandanten (innerhalb eines Systems) eine Tabellenprotokollierung eingeschaltet werden soll. Der Wert 'OFF' bedeutet die generelle Deaktivierung der Protokollierung, der teilweise vorzufindende Wert 'ON' hat keine (technische) Bedeutung und wirkt wie 'OFF'. Bei Einrichtung von 'ALL' werden alle im System befindlichen Mandanten protokolliert. Hinweis: zusätzlich muß bei jeder Tabelle das sog. "Protokollflag" gesetzt sein, um die Änderungen zu protokollieren.	OFF	produktive Mandanten
2. Kennwortrichtlinien				
2.	login/min_password_lng	Mindestlänge des Passwortes (in Zeichen).	3	6 bis 8
3.	login/password_expiration_time	Gültigkeitsdauer von Passwörtern (in Tagen), danach wird ein Passwortwechsel systemseitig erzwungen (Wert '0' bedeutet unbegrenzte Gültigkeit).	0	30 bis 90
4.	login/min_password_diff (verfügbar ab Release 6.10)	Legt fest, in wie vielen Zeichen sich ein neues Kennwort vom alten Kennwort unterscheiden muss. Hierdurch kann die Nutzung von "Kennwortfolgen", wie 'HANSI01', HANSI02' usw. Dieser Parameter wirkt nicht beim Anlegen neuer Kennwörter (Initialkennwort) oder beim Zurücksetzen von Kennwörtern. Der Wert sollte mindestens die Hälfte der minimalen Kennwortlänge betragen (siehe Parameter 'login/min_password_lng').	1	3 bis 4
5.	login/min_password_digits (verfügbar ab Release 6.10)	Festlegung, wie viele Ziffern mindestens in einem Kennwort vorkommen sollen.	0	mind. 1
6.	login/min_password_letters (verfügbar ab Release 6.10)	Festlegung, wie viele Buchstaben mindestens in einem Kennwort vorkommen sollen.	0	mind. 1
7.	login/min_password_specials (verfügbar ab Release 6.10)	Festlegung, wie viele Sonderzeichen (!"\$%&/()=?@[{}]+*#...) mindestens in einem Kennwort vorkommen sollen.	0	mind. 1
8.	login/password_max_new_valid (verfügbar nur in SAP Web Application Server 6.20 und 6.40)	Festlegung, wie lange das vom Administrator vergebene Initialkennwort gültig ist. Erfolgt bis zu diesem Zeitpunkt keine Anmeldung, verliert dieses Kennwort seine Gültigkeit. Eine Anmeldung ist dann nur durch Einrichtung eines neuen Initialpasswortes durch den Administrator möglich (der Wert '0' bedeutet, dass die Initialkennwörter immer gültig sind). Hinweis: Dieser Parameter wirkt sich nicht auf Benutzer vom Typ 'Service' aus.	0	5 bis 10
9.	login/password_max_reset_valid (verfügbar nur in SAP Web Application Server 6.20 und 6.40)	Wirkt ähnlich wie der Parameter 'login/password_max_new_valid', gilt aber nicht bei der Vergabe von Initialkennwörtern sondern beim Zurücksetzen von Kennwörtern existierender Benutzer.	0	5 bis 10

Tz.	Parameter	Erläuterung	Defaultwert	Empfehlung
3. Anmeldeverfahren				
10.	rdisp/gui_auto_logout	Benutzer, die am System angemeldet und längere Zeit inaktiv sind, können durch diesen Parameter automatisch abgemeldet werden (der Wert '0' bedeutet, dass keine automatische Abmeldung erfolgt). Die Zeitangabe erfolgt in Sekunden.	0	1.800 (entspricht 30 Minuten)
11.	login/fails_to_session_end	Anzahl der fehlerhaften Anmeldeversuche bevor die Sitzung beendet wird (Schließen des SAPGUI, keine Sperrung des Benutzers). Der Parameter sollte auf einen niedrigeren Wert gesetzt werden, als der des Parameters 'login/fails_to_user_lock'.	3	3
12.	login/fails_to_user_lock	Anzahl der fehlerhaften Anmeldeversuche bevor der Benutzerstammsatz gesperrt wird (Sperrung läuft um 24:00 Uhr ab; siehe auch: 'login/failed_user_auto_unlock').	12	3 bis 6
13. x	login/failed_user_auto_unlock	Parameter, mit dem die automatische Freigabe der gesperrten Benutzerstämme um 24:00 Uhr abgeschaltet werden kann. Bei der Einstellung '0' erfolgt keine automatische Freischaltung (verfügbar ab Release 4.0).	1	0
14.	login/no_automatic_user_sapstar	Verhindert das Anmelden mit dem User 'SAP*', wenn dieser als Benutzer im System gelöscht wurde. Der Wert '1' bedeutet keine Anmeldung nach dem Löschen für 'SAP*' möglich (Siehe auch Hinweise '2383' und '68048').	0	1
15.	login/disable_multi_gui_login (verfügbar ab Release 4.6)	Festlegung, ob ein Benutzer sich mehrfach oder nur einmal an einem Mandanten anmelden kann. Dieser Parameter hat keine Auswirkungen auf RFC-Anmeldungen, die über den Parameter 'login/disable_multi_rfc_login' gesteuert werden. (Wert '1' bedeutet, dass Mehrfachanmeldungen möglich sind). Ausnahme: Mittels des Parameters 'login/multi_login_users' können bestimmte Benutzer ausdrücklich für Mehrfachanmeldungen zugelassen werden.	0	1
16.	login/multi_login_users (verfügbar ab Release 4.6)	Parameter zur Festlegung von bestimmten Usern, denen eine Mehrfachanmeldung trotz des Parameters 'login/disable_multi_gui_login' mit dem Wert '1' ermöglicht wird.	-	Administratoren, Super User und Notfallbenutzer

Disclaimer:

Trotz sorgfältiger Bearbeitung wird keine Gewähr für die Richtigkeit und Vollständigkeit der Inhalte und Darstellungen übernommen.