NOTE MARCH 2008

SAP® NetWeaver security parameter

The SAP® NetWeaver is a comprehensive application and integration platform that consists of several components and tools. Important components are e.g. the NetWeaver Application Server, NW[1] Business Intelligence, NW Exchange Infrastructure, NW Master Data Management, NW Mobile, NW Portal, Auto-ID infrastructure, NW Identity management. Relevant tools are e.g. Adaptive Computing Controller, NetWeaver Composition Environment, NW Developer Studio, NW Visual Composer, SAP® Solution Manager.

Just like for the former basis kernel the security of this platform is controlled by corresponding system security parameters. The following overview provides a short introduction in the relevant aspects of selected parameters.

You can review the current settings with the help of the report RSPFPAR or RSPARAM [via transaction SE38 e.g]. The parameter change history is available through transaction TU02.

The system profile parameters are stored in files on the operation system level [an instance, a start and default.pfl] and are supposed to configure the different instances.

Dynamic parameters can be changed on the fly, while for static parameters a restart of the corresponding instance is necessary to activate the setting.

[1] NW = SAP® NetWeaver

Parameter	Default	Recom.	Description
login/min_password_lng	6	6-8	Controls the minimum length of a password. Possible entries: 3-40 [until NW 6.4 up to 8]
login/min_password_digits	0	1-2	Controls the minimum number of digits [0-9] in a password. Possible entries: 0-40 [until NW 6.4 up to 8]
login/min_password_letters	0	1-2	Controls the minimum number of letters [A-Z] in a password. Possible entries: 0-40 [until NW 6.4 up to 8]
login/min_password_specials	0	1-2	Controls the minimum number of special characters in a password, such as !"@ $%&/()=?'`*+~#-_.,;:{[]}\<>|] and space Possible entries: 0-40 [until NW 6.4 up to 8]
login/min_password_lowercase	0	1-2	Controls the minimum number of lower-case letters in a password. Possible entries: 0-40 [after NW 6.4]
login/min_password_uppercase	0	1-2	Controls the minimum number of upper-case letters in a password. Possible entries: 0-40 [after NW 6.4]

Parameter	Default	Recom.	Description
login/password_charset	1		**0** –restrictive. Only letters, digits and the following special characters are allowed !"@ $%&/()=?'`*+~#-_.,;:{[]}\<>|] and space in a password. **1** – downwards compatible. The password may consist of various characters [incl. national specialties, such as e.g. ä, ö] All characters aside from the above listed will then be stored as one special character, and can therefore not be differentiated. **2** – not downwards compatible. The password may consist of any character and will be stored in UTF-8 format [Unicode]. If the system does not support unicode, not every character can be entered during login. This parameter should only be set to 2, if the systems support the code.[with rel. 6.4]
login/min_password_diff	1	2-3	Controls the number of characters that have to be different form the previous password. Possible entries: 1-40 [until NW 6.4 up to 8]
login/password_expiration_time	0	30-90	Controls the number of days, after which a password change is required. Possible entries: 0-1000

Parameter	Default	Recom.	Description
login/password_history_size	5	12	Controls the number of passwords that are stored as history and cannot be used
login/password_change_waittime	1	<30-90	Controls the number of days a user has to wait to be allowed to change his password again. Possible entries: 1-1000 [after NW 6.4]
login/disable_multi_gui_login	0	1	Controls whether multiple logins are enabled or disabled. 0 = enable 1 = disable
login/multi_login_users		No entry	Here a list [user ID]can be deposited that would allow users a multiple login even though the multi login is generally disabled. The multiple login information are stored in the table URSR41_MLD
login/system_client		Productive client [comm.-on client]	Controls the suggested client number for login. The common client for each system should be entered here.
login/fails_to_session_end	3	< = login/fails_to_user_lock	Controls the number of false login attempts after which the session is ended. The session can be restarted, with continuous login attempt until the user is locked by the corresponding setting in login/fails_to_user_lock.

Parameter	Default	Recom.	Description
login/fails_to_user_lock	5	3-5	Controls the number of false login attempts until the user is locked. Possible entries: 1-99
login/failed_user_auto_unlock	0	0	Controls if the user ID stays locked after false login attempts or not. 0- the ID will stay locked until manually unlocked 1 – the ID will automatically be unlocked after midnight.
login/no_automatic_user_sapstar	1	1	Controls the activation of the ID SAP* after deletion. [OSS note 2383 and 68048]. If the parameter is set to 1, no one can logon with SAP* and the password PASS in case the ID was for example accidentally deleted. SAP* is not recommended to be used as an emergency user. It is recommended to establish a separate, especially protected emergency user ID as part of an emergency user concept [please also see SAP Security Guide II].
rdisp/gui_auto_logout	0	900-1800 [maybe in combination with network security]	Number of seconds, after which an inactive user is automatically disconnected from the GUI. Possible entries: any numeric value

Parameter	Default	Recom.	Description
login/password_downwards_compatibility	1	0-2	Controls the downwards compatibility of password security. **0** – no downwards compatibility. The system only generates only new hash values that cannot be interpreted by older kernel versions. **1** – the system internally generates downwards compatible hash values, but does not evaluate them upon logon. This setting is required in a CUA controlled landscape with systems that have older kernel releases. **2**- the system generates downwards compatible hash values and checks them -logged in system log- upon failed login attempts to detect compatibility issues. The login fails. **3** – as 2, but with successful login **4** – as 3, but without system log entry. 5 – completely downwards compatible. [after NW 6.4]

Parameter	Default	Recom.	Description
login/password_compliance_to_current_policy	0	1	1 - The system check during login if the password is compliant with the password security settings. If not, a password change will be enforced. 0 – no check Users of type Service and system are generally excluded from password change requirements. [after NW 6.4]
login/disable_password_logon	0		Controls the deactivation of password logon, in case of Single Sign On integration e.g. 0- password enabled 1 – password logon only enabled for users that are listed in login/password_logon_usergroup 2 – password no longer possible
login/password_logon_usergroup			Here a list [user ID]can be deposited that would allow users a password login even though the password login is generally disabled.
login/password_max_idle_productive	0		Controls the number of days that may pass from the last password change of a user to his next logon. After that period of time, the password is rejected. 0 – unlimited validity 1- only valid for same day >1 – number of days before rejection

Parameter	Default	Recom.	Description
login/password_max_idle_productive	0	< 30	Controls the number of days an initial password is valid after creation. 0 – unlimited Possible entries: 0-24.000 [after NW 6.4]

The definition of illegal passwords is set up by maintaining entries for the table **USR40**.

There you can enter passwords that you want to exclude from usage in your company, as they might be easy guessed – for example the company name, address etc..

Wild cards can be used like *01, *02, or Quarter* etc.

! Please never enter a ***** as single entry.

Please be aware that a communication of the corresponding entries will help to reduce confusion; an additional short introduction into the risks of low level passwords security may also help to increase the level of user security compliance.