Password criteria and system parameters

Password quality criteria

The quality criteria for passwords can be set via the system parameters (Spring beans configuration). The following quality criteria exist (see class *PoPasswordQuality*):

- **validityDays -** the number of days after which the password must be changed.
- **minimalLength -** the total minimum length
- **requiresUpperAndLowerCharacters -** if **true**, both lowercase and uppercase characters must occur
- **minimalDigitsCount -** minimum number of digits "0-9"
- **minimalSpecialCharactersCount -** minimum number of special characters such as "@" or "!"
- **numberOfDifferingLatestPasswords -** minimum number of different passwords before one may be reused
- **resetPasswordTokenValidityInHours -** validity (in hours) of the link that the user receives by e-mail for setting a new password

For individual clients, the minimum length, uppercase and lowercase letters, the minimum number of digits and special characters, the number of different passwords and the validity of the reset link can be set differently in the client's password settings. A value set there takes precedence over the system parameter. There, two-factor authentication can also be enforced for all users of the client ("Enforce two-factor authentication").

NOTIZ

If you want to deactivate password expiry in general, set **validityDays** to the value **-1**

System parameters relevant to password management:

Module	Bean	Property	Explanation	Value(s)
po	PoPasswordQuality	**minimalDigitsCount**	required number of digits in the new password	Enter a number (e.g. 4; default: 0)
po	PoPasswordQuality	**minimalLength**	the minimum length (characters) of the new password	Enter a number (e.g. 6; default: 0)
po	PoPasswordQuality	**minimalSpecialCharactersCount**	required number of special characters such as "@" or "!" in the new password	Enter a number (e.g. 2; default: 0)
po	PoPasswordQuality	**numberOfDifferingLatestPasswords**	minimum number of different passwords before a previous password may be reused	Enter a number (e.g. 3; default: 0)
po	PoPasswordQuality	**requiresUpperAndLowerCharacters**	if true, both lowercase and uppercase characters must occur in the new password	"true" or "false" (default: false)

po	PoPasswordQuality	**validityDays**	the number of days after which the password must be changed. After expiry, the user is asked at login to set a new password. If this number is -1, passwords must **NEVER** be changed. The value 0 is not intended (smallest sensible value: 1).	Enter the number of days (e.g. 30; default: 30)
po	PoPasswordQuality	**resetPasswordTokenValidityInHours**	**Validity in hours** of the link that the user receives by e-mail for setting a new password ("Forgot password?", initial setup of the password for new persons)	Enter a number (default: 24)
po	AuthenticationOptions	**allowPasswordResetByUser**	Decision of whether the "Forgot password?" link is offered on the login page. The user then receives a mail (PoPasswordResetMail) with a link through which they set a new password themselves.	"true" or "false" (default: true)
po	AuthenticationOptions	**maxNumberOfFailedLoginAttempts**	**Number of** failed login attempts within maxNumberOfSecondsBetweenFailedLoginAttempts seconds after which the user is locked; the user receives a mail about this (bean PoLockUserMail). Via "Forgot password?" the user can set a new password and is thereby unlocked again. 0 = no lockout.	Enter a number (e.g. 5; default: 0)

po	AuthenticationOptions	**maxNumberOfSecondsBetweenFailedLoginAttempts**	Relevant time in which the failed login attempts are counted	Integer number (default: 60)
po	AuthenticationOptions	**allow2ndFactorPerUser**	Selection of whether users can activate or deactivate two-factor authentication themselves in their security settings. If "Enforce two-factor authentication" is activated for the client, it applies to all users of the client.	"true" or "false" (default: false)
po	PoPasswordNewPersonMail	**explicitRecipient**	Recipient of the mail for the initial setup of the password, if the e-mail stored for the person is not to be used	E-mail address (e.g. recipient@workflow.at)
po	PoPasswordNewPersonMail	**senderMailAddress**	the mail address to be used as sender for the welcome mail	E-mail address (e.g. welcome@workflow.at; default: office@workflow.at)
po	PoPasswordNewPersonMail	**subject**	Subject line of the e-mail for the initial setup of the password	Free text (e.g. "You need to setup your Webdesk password")
po	PoPasswordNewPersonMail	**templateBody**	Mail text for new persons in Webdesk for the initial setup of the password. Can contain the variables $person.firstName and $person.lastName. The text must contain the link for setting the password with the variable $resetId (e.g. <Webdesk-URL>/ changepassword?resetId=$resetId).	Free mail text (the default text does not yet contain a link and must be adapted)

po	PoPasswordResetMail	**explicitRecipient**	Recipient of the password change mail, if the e-mail stored for the person is not to be used	E-mail address (e.g. recipient@workflow.at)
po	PoPasswordResetMail	**senderMailAddress**	the mail address to be used as sender	E-mail address (e.g. password-service@workflow.at; default: office@workflow.at)
po	PoPasswordResetMail	**subject**	Subject line of the mail	Free text (e.g.: "Your Webdesk password has been reset")
po	PoPasswordResetMail	**templateBody**	Mail text; the mail contains no password, but a link through which the user sets a new password. The text must contain the link with the variable *$resetId* and can contain *$person.xxx* (person data).	Free mail text, e.g.: Dear $person.firstName $person.lastName, please click this link to set a new password: <Webdesk-URL>/changepassword?resetId=$resetId (the default text does not yet contain a link and must be adapted)
po	PoPasswordResetPolicy	**forcePasswordChangeAfterReset**	Setting of whether a password change is mandatory after the administrator has reset the password (true = yes)	"true" or "false" (default: true)
po	PoPasswordResetPolicy	**forcePasswordChangeAfterResetToRandomPass**	When resetting via e-mail link ("Forgot password?"), a random password is no longer assigned; the user sets a new password themselves via the link.	"true" or "false" (default: false)
po	PoPasswordResetPolicy	**standardResetPassword**	Default password to which the password is reset if	Free text, entry of a default password (e.g. "webdesk"; default: webdesk)

			"useUsernameAsStandardPassword" is set to false	
po	PoPasswordResetPolicy	**useUsernameAsStandardPassword**	**Boolean** whether the user name is to be used as the default password when the password is reset	"true" or "false" (default: true)

In *"**Advanced functions**"* there are two new actions in the select box under *"Module-specific actions"*:

- **Reset all passwords**
  all passwords are reset to the value specified by the password reset policy
- **Reset all passwords to random values and send mails**
  despite the name, random passwords are no longer assigned: Each user receives a mail (PoPasswordResetMail) with a link through which they can set a new password (valid according to resetPasswordTokenValidityInHours); the previous password remains valid until then. A valid e-mail address for the person is required.

"Stay logged in" function

The "stay logged in" function is intended as an aid for those system installations where no single sign-on with the operating system is provided. So that the user does not have to re-enter their password every time, the option "stay logged in" can be selected when logging in, and the user is then automatically logged in the next time they access Webdesk from the same browser within a period of 14 days.
Neither the user name nor the password is stored in the browser; instead a login token stored in the Webdesk database is used. After each use it is replaced by a new one, and on logout it becomes invalid. How should the security risk be assessed? If someone has access to the user's computer and can log in with their Windows user, they can also open their Webdesk (analogous to the classic SSO scenario).

NOTIZ

For this function to be used, the system parameter **po->AuthenticationOptions->allowRememberMe** must be set to **true** (default: true).

Felder

Name	Wert
Modul	Portal & Organisation (po)
Webdesk Actionname	po_changePassword
Artefakt-Typ	Action