Passwortkriterien und Systemparameter

Passwort-Qualitäts-Kriterien

Die Qualitätskriterien für die Passwörter können über die Systemparameter (Spring Beans Konfiguration) eingestellt werden. Folgende Qualitäts-Kriterien existieren (siehe Klasse *PoPasswordQuality*):

- **validityDays -** die Anzahl Tage, nach der das Passwort geändert werden muss.
- **minimalLength -** die gesamte minimale Länge
- **requiresUpperAndLowerCharacters -** wenn **true** müssen sowohl klein- wie auch grossgeschriebene Zeichen vorkommen
- **minimalDigitsCount -** minimale Anzahl Ziffern "0-9"
- **minimalSpecialCharactersCount -** minimale Anzahl spezieller Zeichen wie "@" oder "!"
- **numberOfDifferingLatestPasswords -** minimale Anzahl von verschiedenen Passwörtern, bis eines wiederholt werden darf
- **resetPasswordTokenValidityInHours -** Gültigkeit (in Stunden) des Links, den der Benutzer per E-Mail zum Setzen eines neuen Passworts erhält

Für einzelne Mandanten können die minimale Länge, Groß- und Kleinbuchstaben, die Mindestanzahl von Ziffern und Sonderzeichen, die Anzahl unterschiedlicher Passwörter und die Gültigkeit des Reset-Links in den Passwort-Einstellungen des Mandanten abweichend festgelegt werden. Ein dort gesetzter Wert hat Vorrang vor dem Systemparameter. Dort kann außerdem die 2-Faktor-Authentifizierung für alle Benutzer des Mandanten erzwungen werden ("2-Faktor Authentifizierung erzwingen").

NOTIZ

Will man den Ablauf von Passwörtern generell deaktivieren, so stellt man die **validityDays** auf den Wert **-1**

Für die Passwortverwaltung relevante Systemparameter:

Modul	Bean	Eigenschaft	Erklärung	Wert(e)
po	PoPasswordQuality	**minimalDigitsCount**	notwendige Anzahl der Ziffern im neuen Passwort	Zahl einzugeben (z.B. 4; Standard: 0)
po	PoPasswordQuality	**minimalLength**	die minimale Länge (Zeichen) des neuen Passworts	Zahl einzugeben (z.B. 6; Standard: 0)
po	PoPasswordQuality	**minimalSpecialCharactersCount**	notwendige Anzahl spezieller Zeichen wie "@" oder "!" im neuen Passwort	Zahl einzugeben (z.B. 2; Standard: 0)
po	PoPasswordQuality	**numberOfDifferingLatestPasswords**	minimale Anzahl von verschiedenen Passwörtern, bis ein vorheriges Passwort wiederverwendet werden darf	Zahl einzugeben (z.B. 3; Standard: 0)
po	PoPasswordQuality	**requiresUpperAndLowerCharacters**	wenn **true**, müssen sowohl klein- wie auch	"true" oder "false" (Standard: false)

			großgeschriebene Zeichen im neuen Passwort vorkommen	
po	PoPasswordQuality	**validityDays**	die Anzahl Tage, nach der das Passwort geändert werden muss. Nach Ablauf wird der Benutzer bei der Anmeldung aufgefordert, ein neues Passwort zu setzen. Ist diese Zahl -1, so müsssen die Passwörter **NIE** geändert werden. Der Wert 0 ist nicht vorgesehen (kleinster sinnvoller Wert: 1).	Tagesanzahl einzugeben (z.B. 30; Standard: 30)
po	PoPasswordQuality	**resetPasswordTokenValidityInHours**	Stunden des Links, den der Benutzer per E-Mail zum Setzen eines neuen Passworts erhält ("Passwort vergessen?", Ersteinrichtung des Passworts für neue Personen)	Zahl einzugeben (Standard: 24)
po	AuthenticationOptions	**allowPasswordResetByUser**	Wahl, ob auf der Anmeldeseite der Link "Passwort vergessen?" angeboten wird. Der Benutzer erhält dann eine Mail (PoPasswordResetMail) mit einem Link, über den er selbst ein neues Passwort setzt.	"true" oder "false" (Standard: true)
po	AuthenticationOptions	**maxNumberOfFailedLoginAttempts**	Anzahl fehlgeschlagener Anmeldeversuche innerhalb von maxNumberOfSecondsBetweenFailedLoginAttempts Sekunden, nach	Zahl einzugeben (z.B. 5; Standard: 0)

			der der Benutzer gesperrt wird; er erhält darüber eine Mail (Bean PoLockUserMail). Über "Passwort vergessen?" kann er ein neues Passwort setzen und wird damit wieder entsperrt. 0 = keine Sperre.	
po	AuthenticationOptions	**maxNumberOfSecondsBetweenFailedLoginAttempts**	Zeitraum in Sekunden, in dem die fehlgeschlagenen Anmeldeversuche gezählt werden	Zahl eingeben (Standard: 60)
po	AuthenticationOptions	**allow2ndFactorPerUser**	Auswahl, ob Benutzer in ihren Sicherheitseinstellungen die 2-Faktor-Authentifizierung selbst aktivieren bzw. deaktivieren können. Ist beim Mandanten "2-Faktor Authentifizierung erzwingen" aktiviert, gilt sie für alle Benutzer des Mandanten.	"true" oder "false" (Standard: false)
po	PoPasswordNewPerson	**explicitRecipient**	Empfänger der Mail für die Ersteinrichtung des Passworts, falls nicht die für die Person gepeicherte E-Mail verwendet werden soll	E-Mail Adresse (z.B. empfänger@workflow.at)
po	PoPasswordNewPerson	**senderMailAddress**	die als Absender für die Willkommens-Mail einzusetzende Mail-Adresse	E-Mail Adresse (z.B. welcome@workflow.at; Standard: office@workflow.at)
po	PoPasswordNewPerson	**subject**	Betreff-Zeile der E-Mail zur Ersteinrichtung des Passworts	Freitext (z.B. "You need to setup your Webdesk password")

po	PoPasswordNewPersonTemplate	**templateBody**	Mail-Text für neue Personen in Webdesk zur Ersteinrichtung des Passworts. Kann die Variablen $person.firstName und $person.lastName enthalten. Der Text muss den Link zum Setzen des Passworts mit der Variable $resetId enthalten (z.B. <Webdesk-URL>/ changepassword? resetId=$resetId).	Freier Mailtext (der Standardtext enthält noch keinen Link und muss angepasst werden)
po	PoPasswordResetMail	**explicitRecipient**	Empfänger der Mail zur Passwortänderung, wenn nicht die für die Person gepeicherte E-Mail genommen werden soll	E-Mail Adresse (z.B. empfänger@workflow.at)
po	PoPasswordResetMail	**senderMailAddress**	die als Absender einzusetzende Mail-Adresse	E-Mail Adresse (z.B. password-service@workflow.at; Standard: office@workflow.at)
po	PoPasswordResetMail	**subject**	Betreff-Zeile der Mail	Freitext (z.B.: "Your Webdesk password has been reset")
po	PoPasswordResetMail	**templateBody**	Mail-Text; die Mail enthält kein Passwort, sondern einen Link, über den der Benutzer ein neues Passwort setzt. Der Text muss den Link mit der Variable *$resetId* enthalten und kann *$person.xxx* (Personen-Daten) enthalten.	Freier Mailtext, z.B.: Dear $person.firstName $person.lastName, please click this link to set a new password: <Webdesk-URL>/ changepassword? resetId=$resetId (der Standardtext enthält noch keinen Link und muss angepasst werden)

po	PoPasswordResetPolicy	**forcePasswordChangeAfterReset**	Ist hier eine Passwortänderung nach dem Zurücksetzen des Passworts durch den Administrator zwingend erforderlich ist (true = ja)	"true" oder "false" (Standard: true)
po	PoPasswordResetPolicy	**forcePasswordChangeAfterResetToRandomPassword**	Beim Zurücksetzen per E-Mail-Link ("Passwort vergessen?") wird kein Zufallspasswort mehr vergeben, der Benutzer setzt über den Link selbst ein neues Passwort.	"true" oder "false" (Standard: false)
po	PoPasswordResetPolicy	**standardResetPassword**	Standard-Passwort, auf das rückgesetzt wird, falls „useUsernameAsStandardPassword“ auf false gesetzt ist	Freitext, Eingabe eines Standard-Passworts (z.B. "webdesk", Standard: webdesk)
po	PoPasswordResetPolicy	**useUsernameAsStandardPassword**	Ist diese Option gesetzt, wird der UserName beim zurücksetzen des Passworts als Standardpasswort verwendet werden soll	"true" oder "false" (Standard: true)

In *"**Erweiterte Funktionen**"* befinden sich bei den *"Modul-spezifische Aktionen"* zwei neue Aktionen in der Select-Box:

- **Alle Passwörter zurücksetzen**
  alle Passwörter werden auf jenen Wert zurückgesetzt, den die Password-Reset-Policy angibt
- **Alle Passwörter zurücksetzen auf Zufallswerte und Mails senden**
  trotz der Bezeichnung werden keine Zufallspasswörter mehr vergeben: Jeder Benutzer erhält eine Mail (PoPasswordResetMail) mit einem Link, über den er ein neues Passwort setzen kann (gültig gemäß resetPasswordTokenValidityInHours); das bisherige Passwort bleibt bis dahin gültig. Voraussetzung ist eine gültige E-Mail-Adresse bei der Person.

Funktion "angemeldet bleiben"

Die Funktion "angemeldet bleiben" ist als Hilfe für jene System-Installationen gedacht, wo kein SingleSignOn mit dem Betriebssystem vorgesehen ist. Damit der Benutzer nicht jedes Mal sein Passwort neu eingeben muss, kann beim Einloggen die Option "angemeldet bleiben" gewählt werden und dadurch wird der Benutzer beim nächsten Aufruf von Webdesk von demselben Browser innerhalb eines Zeitraums von 14 Tagen automatisch angemeldet.
Dabei werden weder Benutzername noch Passwort im Browser gespeichert, sondern ein Anmelde-Token, das in der Webdesk-Datenbank hinterlegt ist. Nach jeder Verwendung wird es durch ein neues ersetzt,

beim Abmelden wird es ungültig. Wie ist das Sicherheitsrisiko einzuschätzen? Wenn jemand Zugang zum Computer des Benutzers hat und sich mit seinem Windows User einloggen kann, so kann er auch seinen Webdesk öffnen (analog zum klassischen SSO Szenario).

NOTIZ

Damit diese Funktion verwendet werden kann, muss der Systemparameter **po->AuthenticationOptions->allowRememberMe** auf **true** gesetzt sein (Standard: true).

Felder

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