Basis-Konfiguration & Passwortrichtlinie

In der Datei "ApplicationConfig.properties" können diverse Einstellungen für das GlobalTaxCenter vorgenommen werden. Die Datei befindet sich im GTC-Deployment im Verzeichnis "<gtc-root>/WEB-INF/classes/com/pwc/login/authentification".

Sollte das Deployment als ".war"-Datei vorliegen, muss die Datei vorher mit 7-zip entpackt werden. Alternativ benennen Sie die Datei *gtc.war* in *gtc.zip* um, dann können Sie den Windows-Explorer dafür verwenden.

Die nachfolgende Tabelle fasst die Möglichkeiten dieser Konfiguration zusammen. Die grün hinterlegten Felder markieren Einstellungen, die seit der letzten Hauptversion angepasst wurden.

Parameter	Default-Wert	Wertebereich	Beschreibung
DictFile	common-passwords.txt	-	Name der Datei (relativ zum classes-Verzeichnis), welche "triviale" Passwörter enthält, die nicht benutzt werden dürfen. Typische Beispiele sind "test", "1234" oder "asdf".
LoginLength	8	0 - 2157583648	Mindestlänge des Loginnamens
PWLength	8	1 - 255	Mindestlänge des Passworts
PWLivetimeMax	180	1 - 180	Maximale Lebensdauer des Passworts in Tagen; nach dieser Zeit muss das Passwort geändert werden
PWLivetimeMin	1	1 - 10	Minimale Lebensdauer des Passworts in Tagen; das Passwort kann nicht eher geändert werden
PWGraceLogin	5	1 - 10	Anzahl der erlaubten Logins, nachdem das Passwort abgelaufen ist (Gnaden-Login).
PWUniqueness	10	1 - 255	Eindeutigkeit des Passworts; Es müssen mindestens … verschiedene Passwörter verwendet werden, bevor ein Altes erneut verwendet werden kann.
PWTrivialityChar	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, muss das Passwort mindestens einen Groß- und einen Kleinbuchstaben enthalten.
PWTrivialityDigit	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, muss das Passwort mindestens eine Ziffer enthalten.
PWTrivialitySpecial	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, muss das Passwort mindestens ein Sonderzeichen enthalten.
PWUnsuccessfulAttemps	3	3 - 5	Anzahl der Fehlversuche bei Eingabe eines Passworts, bevor der Login gesperrt wird.
checkLoginLength	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, wird die minimale Länge des Loginnamens (Parameter "LoginLength") überprüft.
checkPWLength	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, wird die minimale Länge eines Passworts (Parameter "PWLength") überprüft.
checkPWLivetimeMax	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, wird die maximale Gültigkeitsdauer eines Passworts (Parameter "PWLivetimeMax") überprüft.
checkPWLivetimeMin	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, wird die minimale Gültigkeitsdauer eines Passworts (Parameter "PWLivetimeMin") überprüft.
checkPWGraceLogin	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, wird die Anzahl der Gnaden-Logins (Parameter "PWGraceLogin") überprüft.
checkPWDict	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, werden die Passwörter auf Trivialität geprüft, d.h. sie dürfen nicht in der Passwort-Datei (Parameter "DictFile") vorkommen.
checkPWUnsuccessfulLogin	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, wird die Anzahl der Fehlversuche (Parameter "PWUnsuccessfulAttemps") überprüft.
checkHistory	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, wird die Passworteindeutigkeit (Parameter "PWUniqueness") überprüft.
checkUserExpired	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, wird das Ablaufdatum des Logins überprüft.
archiveExpiredInitialPassword	false	true / false	Wenn dieser Parameter auf "true" gesetzt und die maximale Zeit für die initiale Anmeldung (Parameter "initialPasswordTimespan") verstrichen ist, wird der Login archiviert.
initialPasswordTimespan	15		Maximale Zeit in Tagen, die ein Anwender Zeit hat, sich initial im GTC einzuloggen, bevor der Login gesperrt wird.
useEncryption	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, sollen Passwörter verschlüsselt (MD5) in der Datenspeicher abgelegt werden.
usePassPhrase	true	true / false	Wenn dieser Parameter auf "true" gesetzt ist, soll die MD5-Verschlüsselung zusätzlich den Wert aus dem Parameter "passPhrase" verwenden.
passPhrase	pass	<Text>	Der Wert des Parameters wird zusätzlich für die MD5-Verschlüsselung der Passwörter verwendet. Ob und wie Passwörter verschlüsselt werden, steuern die Parameter "useEncryption" und "usePassPhrase".
blockUser	120		Maximale Zeit in Tagen, die ein Anwender sich nicht einloggen muss, bevor der Login automatisch gesperrt wird.

checkBlockUser	false	true / false	Wenn dieser Parameter auf "true" gesetzt ist, soll das Sperren von Anwendern (Parameter "blockUser") überprüft werden.
TimeOut	3600	0 - 2157583648	Ablaufzeit einer Session (Sitzung, wenn ein Anwender angemeldet ist) in Sekunden; wenn ein Anwender …. Sekunden keine Aktion im GTC durchführt, wird der Anwender automatisch ausgeloggt.
ELSTER_TIMEOUT	60000	0 - ?	Definiert die Zeitüberschreitung in Millisekunden für den Aufbau einer Verbindung zur Finanzverwaltung (Elster-Web-Service)
CaseSensitiveLoginNames	true	true / false	Wenn dieser Parameter auf „true“ gesetzt ist, sind die Loginnamen „case-sensitiv“
familyOfficePermissionNeeded	false	true / false	Wenn dieser Parameter auf „true“ gesetzt ist, können sich nur Benutzer anmelden, die dem FamilyOffice angehören