Passwortverwaltung

Webdesk unterstützt folgende Authentifizierungs-Varianten:

- **Datenbank basierte Authentifizierung**
  Webdesk Datenbank basierte Anmeldung; kann auch als Backup-Methode verwendet werden bei SSO / NTLM oder für nicht im Active Directory enthaltene Benutzer
- **Authentifizierung via LDAP**
  LDAP Server verwaltet Anmeldeinformationen
- **Authentifizierung mit SSO (NTLM)**
  Anmeldung per Microsoft Internet Information Server, Apache Server oder automatische Anmeldung anhand Windows Login-Info

Datenbankinterne Authentifizierung

Bei der **datenbankinternen Authentifizierung** werden **Username** und **Passwort** der Benutzer innerhalb der eigenen Datenbank gespeichert. Es besteht daher keine Abhängigkeit zu einem Drittsystem für die Authentifizierung.
Bei der DB-internen Authentifizierung muss der Benutzer beim Einstieg in den Webdesk in der **Login**-Maske seinen Usernamen und sein Passwort eingeben. Dieses Paar wird dann gegen die Datenbank geprüft und falls Gleichheit besteht, wird dann der Benutzer mit dem eingegebenen Usernamen am System angemeldet.

Die Passwortverwaltung ist als Unterpunkt der **Authentifizierung** zu sehen (DB basierte Authentifizierung)

Um die DB-interne Authentifizierung als primäre oder sekundäre Authentifizierungsart zu aktivieren, muss der entsprechende **Systemparamter** (BeanProperty) gesetzt werden.

- Modul PO > Bean Authentication
- als **primäre** Authentifizierungsmethode: Authentication**.authenticationMode** = **DB**
- als **sekundäre** (Backup) Authentifizierungsmethode:
  AuthenticaticationBackupForSSO.authenticationMode = DB

Die Passwörter werden in der Tabelle *PoPassword* gespeichert, zusammen mit ihrem Gültigkeitsdatum und einem Flag, das angibt, ob eine Änderung beim nächsten Einloggen erzwungen werden soll.

Änderung des Passwortes

Bei der DB-internen Authentifizierung muss der Benutzer beim Einstieg in den Webdesk in der **Login-Maske** seinen **Usernamen** und sein **Passwort** eingeben. Dieses Paar wird dann gegen die Datenbank geprüft und falls Gleichheit besteht, wird dann der Benutzer mit dem eingegebenen usernamen am System angemeldet.

Für die **Änderung des Passworts** bestehen im Webdesk 2 Möglichkeiten:

- Änderung des Passworts durch den **Benutzer** über die Aktion 'po_changePassword'
- Änderung des Passworts durch den **Administrator** über die Aktion 'po_editPerson'

Ist die **Gültigkeit** eines Passwortes abgelaufen, oder ist das "**Erzwinge-Passwort-Änderung**" Flag in den Systemparametern „PoPassword“ auf true gesetzt, so wird der Benutzer nach dem Einloggen aufgefordert, sein Passwort zu ändern. Der übliche Dialog mit nochmaliger Eingabe des alten Passwortes und doppelter Eingabe des neuen Passwortes folgt.
Nach erfolgreichem Ändern zeigt die Oberfläche eine Erfolgsmeldung und bietet einen Link zum Starten der Applikation.

Weiters befindet sich auf der Login-Maske nun ein **Hyperlink**, der die Änderung des Passwortes für jeden beliebigen *userNamen* ermöglicht. Mit Klick darauf kommt man nach Eingabe eines *userNamens* in oben beschriebenen Passwort-Änderungs-Ablauf.

Mit den Einstellungen betreffend ein **Passwort-Rücksetz-Mail** kann eine **Mailbenachrichtigung** konfiguriert werden, die beim Rücksetzen des Passwortes auf einen Zufallswert generiert wird. Diese werden über die Systemparameter vorgenommen.

In *"**Erweiterte Funktionen**"* befinden sich oben bei *"Modul-spezifische Aktionen"* zwei Aktionen in der Auswahlbox:

- **Alle Passwörter zurücksetzen**
  es werden alle Passwörter auf jenen Wert zurückgesetzt, den die PasswordResetPolica angibt
- **Alle Passwörter zurücksetzen auf Zufallswerte und Mails senden**
  alle Passwörter werden auf durch einen Zufalls-Generator erzeugte Werte gesetzt, und jedes dieser Passwörter wird in einer Mail an den entsprechenden Benutzer gesandt; dies wird nur durchgeführt, falls der Benutzer wirklich eine Mail-Adresse hat.

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

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	Mögliche Werte
po	PoPasswordQuality	minimalDigitsCount	notwendige Anzahl Ziffern im neuen Password	0-9
po	PoPasswordQuality	minimalLength	die minimale Länge des neuen Passworts	6
po	PoPasswordQuality	minimalSpecialCharactersCount	notwendige Anzahl spezieller Zeichen wie "@" oder "!" im neuen Passwort	1
po	PoPasswordQuality	numberOfDifferingLatestPasswords	minimale Anzahl von verschiedenen Passwörtern, bis eines wiederholt werden darf	3

po	PoPasswordQuality	requiresUpperAndLowerChars	wenn true müssen sowohl klein- wie auch großgeschriebene Zeichen im neuen Passwort vorkommen	true/false
po	PoPasswordQuality	validityDays	die Anzahl Tage, nach der das Passwort geändert werden muss	60
po	PoPasswordResetMail	explicitRecipient	Empfänger der Mail, wenn nicht PoPerson.email genommen werden soll. Ist diese Zahl 0 so müssen *ALLE* Passwörter sofort geändert werden. Ist diese Zahl -1, so müsssen die Passwörter *NIE* geändert werden.	
po	PoPasswordResetMail	senderMailAddress	die als Absender einzusetzende Mail-Adresse	office@workflow.at[1]
po	PoPasswordResetMail	subject	Betreff-Zeile der Mail	Your webdesk password has been reset
po	PoPasswordResetMail	templateBody	Mail-Text; muss die Variable $password (das neue Passwort) und kann $person.xxx (Personen-Daten) enthalten	<html><body>Your webdesk password has been reset, please change it as soon as possible! Current password: > $password Sincerly,Your Webdesk Administraton</body></html>
po	PoPasswordResetPolicy	forcePasswordChangeAfterResetToRandomPassword	"After Reset-Passwort-Änderung" Flag	true/false
po	PoPasswordResetPolicy	standardResetPassword	Standard-Passwort, auf das rückgesetzt wird, falls „useUsernameAsStandardPassword“ auf false gesetzt ist	webdesk

po	PoPasswordResetPolicy	useUsernameAsStandardPassword	Username als Passwort	true/false

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**
  alle Passwörter werden auf durch einen Zufalls-Generator erzeugte Werte gesetzt, und jedes dieser Passwörter wird in einer Mail an den entsprechenden Benutzer gesandt; Mailbenachtrichtigung erfolgt nur, wenn der Benutzer eine Mail-Adresse hat.

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 beim nächsten Aufruf von Webdesk von demselben Browser (im Kontext desselben Windows Benutzers!) innerhalb eines Zeitraums von 7 Tagen die letztgemerkte Benutzer/Passwort Kombination verwendet, um ein automatische Login zu versuchen.
Benutzername u. Passwort werden dabei verschlüsselt in Cookies am Browser gespeichert. 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). Darüberhinaus werden die Infos nirgendwo zusätzlich gespeichert.

NOTIZ

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

1. mailto:office@workflex.at