White Paper

WinLine - Änderungen Passwörter



mesonic
mit sicherheit ein gewinn

Inhaltsverzeichnis

1. White Paper - Änderungen im Bereich Passwörter 3
1.1. Erweiterung der Passwort-Länge und Änderung der Passwort-Verschlüsselung 3
1.1.1. Folgen der Umstellung 3
1.1.1.1. Was passiert? 3
1.1.1.2. Die Folge daraus 4
1.1.1.3. Wie kann diese Fehlermeldung verhindert werden? 4
1.1.1.4. Was tun, wenn die Workstations nicht upgedatet werden können? 4
1.1.1.5. Update vom Client aus 5
1.2. Anbindung ActivDirectory 8
1.2.1. Windows Benutzer übernehmen 9
1.2.1.1. Ablauf bzw. Möglichkeiten im Fenster 12

1. White Paper - Änderungen im Bereich Passwörter

Mit der WinLine Edition 2027 - Version 12.35 wurden tiefgreifende Änderungen im Bereich der Passwörter durchgeführt, die dafür sorgen, dass das Arbeiten mit der WinLine noch sicherer ist. Die Änderungen betreffen:

- ✓ Erweiterung der Passwort-Länge auf 64 Stellen
- ✓ Umstellung der Passwort-Verschlüsselung
- ✓ Anbindung an Windows-ActiveDirectory

Nachfolgend werden die einzelnen Detailbereiche beschrieben.

1.1. Erweiterung der Passwort-Länge und Änderung der Passwort-Verschlüsselung

Bisher war die Passwort-Länge auf 15 Stellen beschränkt. Um den aktuellen Passwortrichtlinien zu entsprechen, wurde nun die Passwortlänge innerhalb der WinLine / MWL auf 64 Stellen erweitert. D.h. alle Eingabefelder, wo ein Passwort eingegeben werden kann, wurden auf die 64 Stellen erweitert.

Im Zuge dessen wurde auch die Passwort-Verschlüsselung geändert, d.h. mit dem Patch 12.35 werden alle Passwörter auf eine AES-256-GCM-Verschlüsselung umgestellt.

Diese Umstellung passiert im Zuge des Updates auf die WinLine Edition 2027 - Version 12.35 aufwärts. Dabei wird zuerst ein zentraler Schlüssel (mesonic.pfx) erstellt, mit dem dann alle gespeicherten Passwörter umgestellt werden. Die mesonic.pfx ist immer mit der mesoserverconnect.meso (die im Zuge dessen auch aktualisiert wird) und mit der System-Datenbank "verknüpft" und demnach müssen auch alle gemeinsam gesichert werden. Ein "Verlust" der mesonic.pfx führt dazu, dass das Programm nicht mehr gestartet werden kann.

1.1.1. Folgen der Umstellung

Die erste Auswirkung zeigt sich während des Updates, wenn eine Netzwerkinstallation mit Clients des Typs "Client/Server verwendet wird. Dabei kann es sich sowohl um lokal installierte Clients als auch um Terminalserver handeln, die als Basis für Terminalserver-Benutzer dienen. Voraussetzung ist, dass die Clients nicht automatisch aktualisiert werden, was dem Standardverhalten entspricht.

1.1.1.1. Was passiert?

Mit dem Update, das am Server eingespielt wird, werden die Passwörter umgestellt, d.h. in der T002SRV, wo die Benutzer gespeichert werden, wird das Passwort "neu" geschrieben. Dazu wird auch die mesoserverconnect.meso mit dem neu verschlüsselten Passwort aktualisiert.

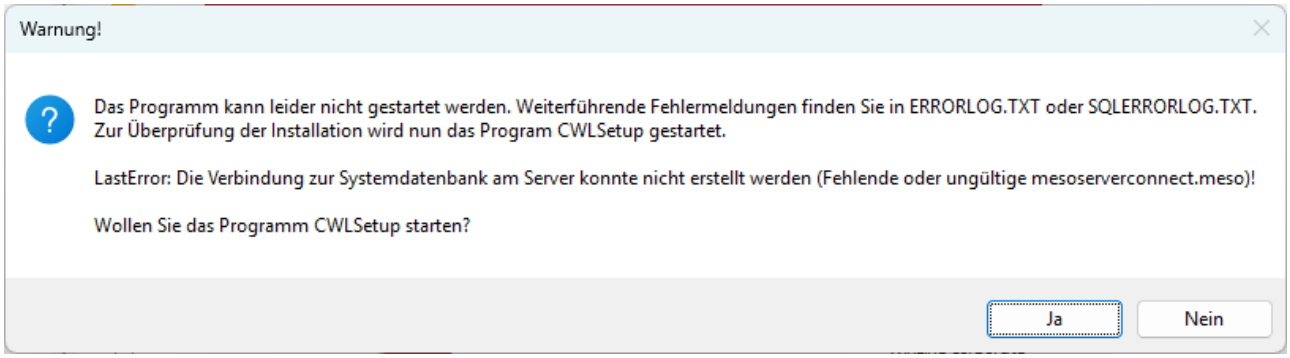
Beispiel:

In der Demo-Version hat der Benutzer "a" das Passwort "b". In der Datenbank wird das Passwort nicht als "b" sondern mit einem Hashwert z.B. "187jfklas" (vereinfacht dargestellt) gespeichert. Bei der Umstellung wird nun dieser Hashwert geändert und der ist dann z.B. "4xWQIOREUAFJW354665442lejwrelkjwre" (vereinfacht dargestellt).

1.1.1.2. Die Folge daraus

Wenn sich nun ein Client, der noch die "alte" Version installiert hat, mit dem Server verbindet, dann wird im ersten Schritt die mesoserverconnect.meso ausgelesen (inkl. meso-Benutzer und Passwort) und damit wird die Verbindung zum SQL-Server erstellt. Am SQL-Server wird dann in der T004SRV nachgeschaut, ob ein Update verfügbar ist oder nicht.

Genau dieser Schritt funktioniert nun aber nicht mehr, weil in der mesoserverconnect.meso das Passwort zwar immer noch das gleiche ist, die "alte" Version hat aber einen anderen Schlüssel für die "Übersetzung" des Passworts, was dazu führt, dass die Verbindung auf den SQL-Server und die T004SRV nicht mehr durchgeführt werden kann. Somit kann sich der Client nicht wie gewohnt das Update selbst kopieren. Die Fehlermeldung, die daraus resultiert, lautet:



D.h. wenn das Update wie gewohnt mit den Standardeinstellungen durchgeführt wird, kommt es zwangsläufig zu der Fehlermeldung.

1.1.1.3. Wie kann diese Fehlermeldung verhindert werden?

Die Fehlermeldung kann verhindert werden, indem man vor dem Update prüft, ob Clients nicht gleich im Zuge des Updates mit der neuen Version versorgt werden können.

Voraussetzung dafür ist, dass die Clients in der Datei "zipupdateclients.txt" am Server eingetragen sind (siehe auch Anleitung Patchupdate). Dazu müssen die Clients über eine funktionelle Freigabe des WinLine-Verzeichnisses (für den Windows-Benutzer, der das Update am Server durchführt) verfügen und die Clients müssen zum Zeitpunkt des Updates online sein.

Sind diese Voraussetzungen erfüllt, dann werden die Clients im Zuge des Updates mit der neuen Version versorgt und nachdem die neuen EXE am Client vorhanden sind, funktioniert auch die Verbindung zum Server und die Workstation kann "normal" starten.

1.1.1.4. Was tun, wenn die Workstations nicht upgedatet werden können?

Es gibt Szenarien, wo die Workstation nicht upgedatet werden kann, z.B. weil die Workstation nicht online ist, oder dergleichen. In diesem Fall gibt es zwei Möglichkeiten, wie man die Workstation mit der neuen Version versorgen kann.

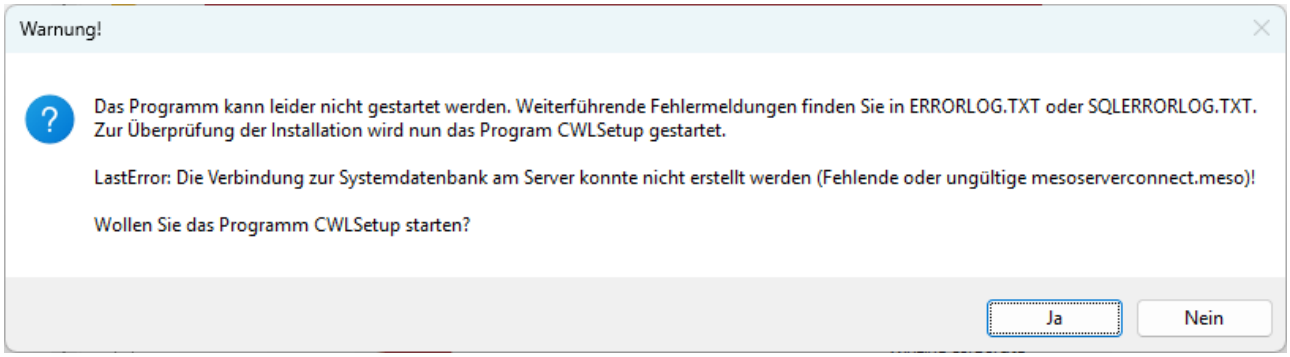
- ✓ Update Wizard im MSM
  Über den Update Wizard im Menüpunkt MSM im WinLine ADMIN können nachträglich Clients mit einer aktuellen Version beschickt werden. Auch hier gilt wieder die Voraussetzung, dass der Client eine funktionelle Freigabe des WinLine-Verzeichnisses haben muss, und der Client online ist.

✓ Update vom Client aus
Mit dem Update wird am WinLine Server (dort, wo sich auch die mesoserverconnect.meso und jetzt neu auch die mesonic.pfx befindet) eine neue Datei "mesoClientCopy.exe" zur Verfügung gestellt. Wenn diese vom Client aufgerufen wird, kann damit die CWLStart.exe auf den Client kopiert werden, womit dann zumindest das Programm gestartet werden kann (mit der Verbindung auf den SQL-Server), um in weiterer Folge das Update auf den Client durchführen zu können.

1.1.1.5. Update vom Client aus

Damit das Update vom Client aus durchgeführt werden kann, sind folgende Schritte notwendig - das könnte auch so als Info (z.B. als Mail) an die WinLine-Benutzer weitergegeben werden:

Wenn beim Starten der WinLine eine Fehlermeldung erscheint, die so aussieht

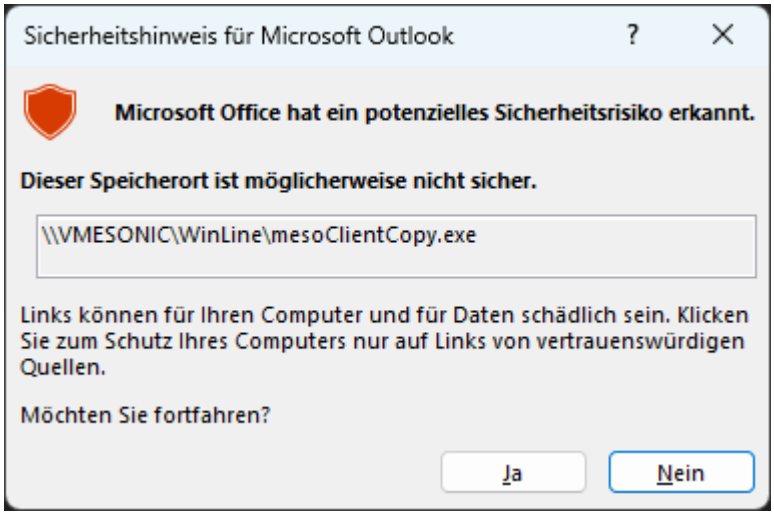


dann sind bitte folgende Schritte durchzuführen:

Zuerst ist die Meldung/Warnung mit "NEIN" zu bestätigen!

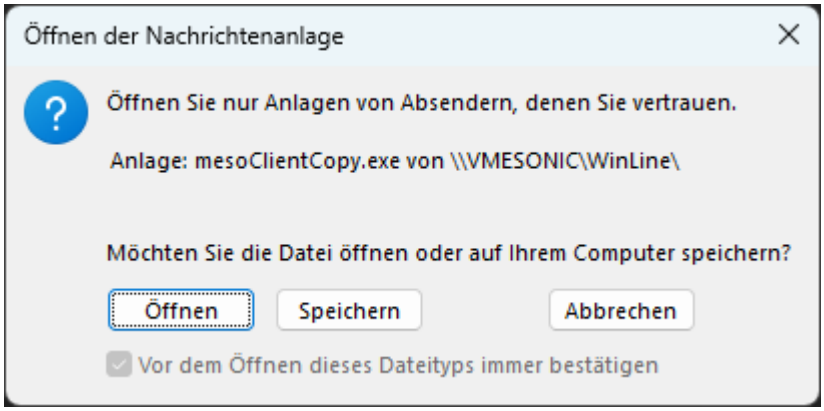
Dann muss der Link \\<SERVER>\<FreigabeWinLine>\mesoClientCopy.exe angeklickt werden

Dadurch erscheint die Meldung



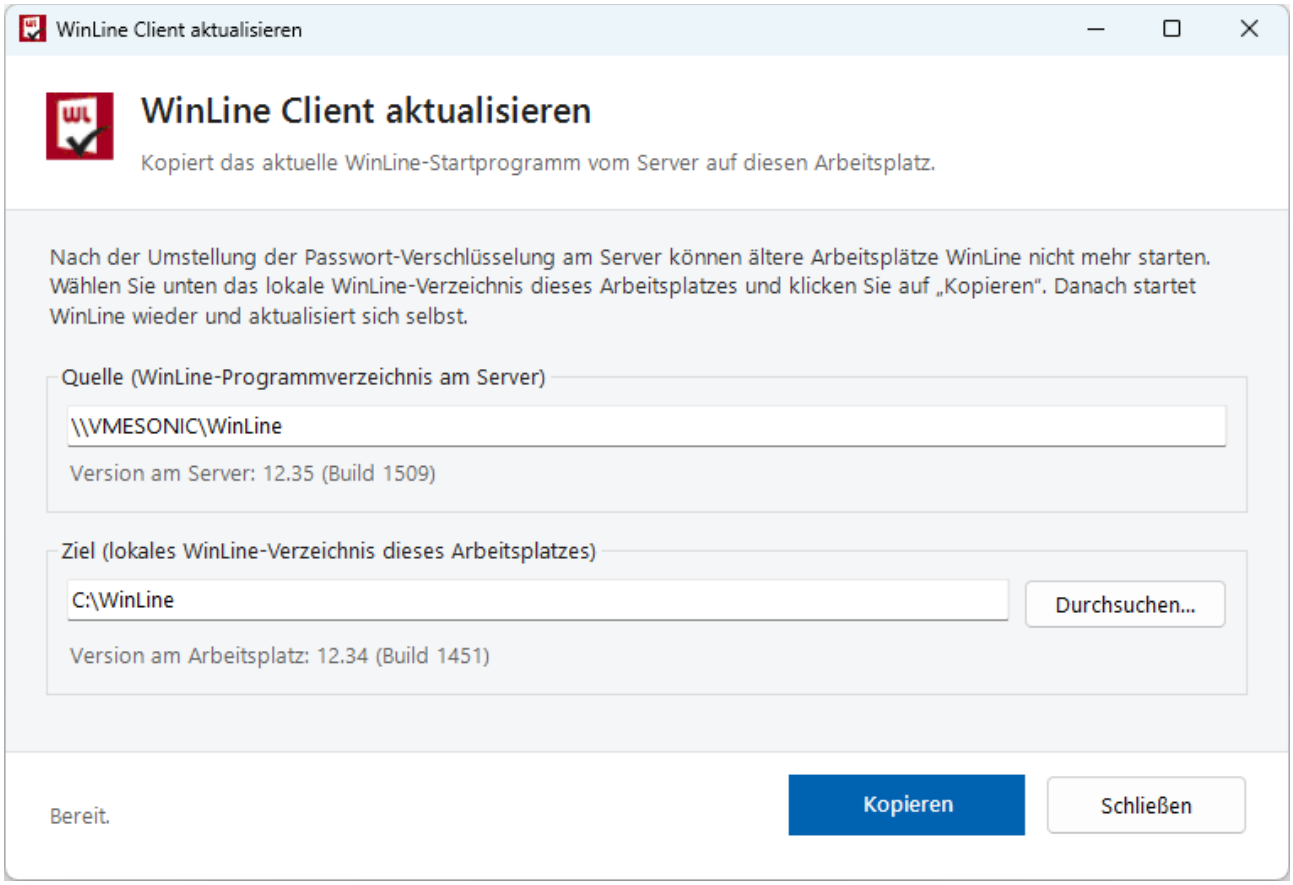
(die Meldung kommt ggf. nicht, wenn die EXE signiert ist?)

die mit "Ja" bestätigt werden muss. Ggf. kommt dann noch eine zweite Meldung:



die durch Anklicken des "Öffnen"-Buttons bestätigt wird.

Dadurch wird ein neues Fenster geöffnet



Hier wird eine Quelle angezeigt, die nicht verändert werden darf!

Das Feld "Ziel" ist zuerst leer - daneben gibt es einen Durchsuchen - Button, der angeklickt werden muss.

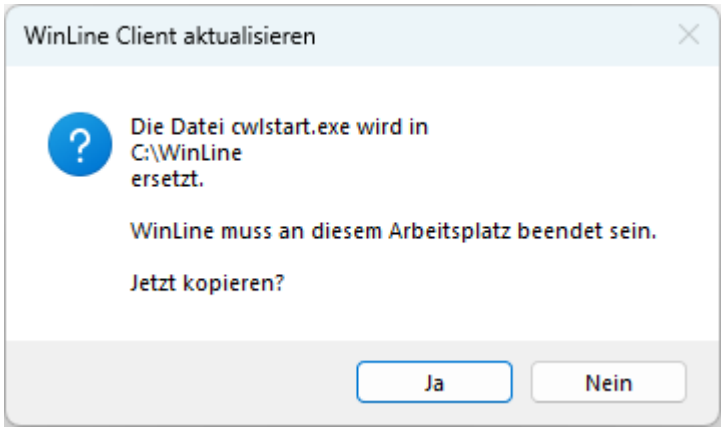
Es wird ein weiteres Fenster geöffnet, aus dem das Zielverzeichnis - in dem die WinLine installiert ist - ausgewählt werden muss.

Hinweis:
Das Zielverzeichnis ist standardmäßig das Verzeichnis <lokale Festplatte:\WinLine-Verzeichnis>, z.B.

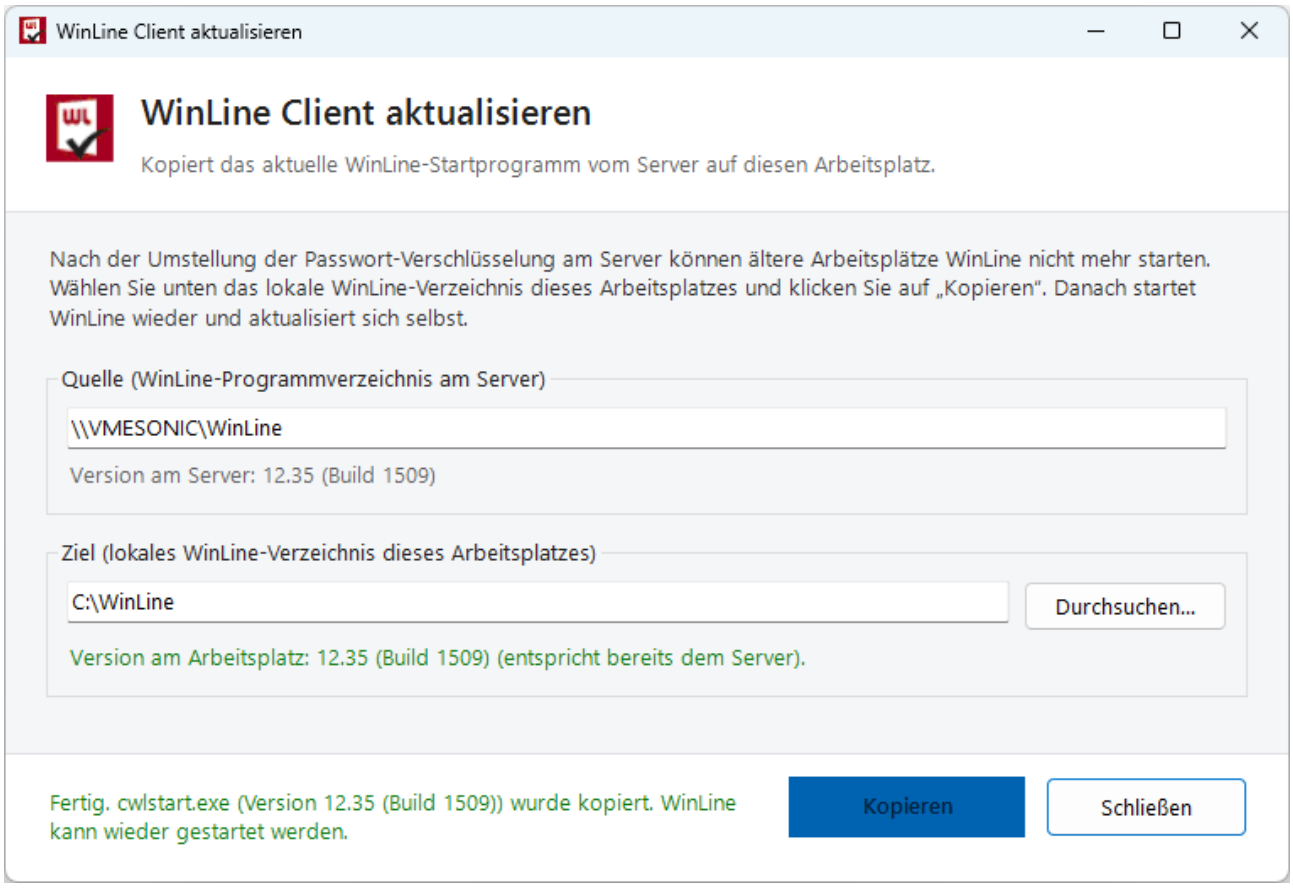
- **C:\WinLine**

Das Verzeichnis wird durch den Button "Ordner auswählen" übernommen - das Verzeichnis wird dann auch in das Feld "Ziel" eingetragen.
Dabei wird geprüft, ob sich im Zielverzeichnis eine cwlstart.exe befindet und es wird davon auch die Version ausgelesen und unter dem Verzeichnis angezeigt.

Durch Anklicken des Kopieren - Buttons wird die Meldung angezeigt, dass die cwlstart.exe kopiert wird.



Die Meldung muss mit "JA" bestätigt werden. Damit wird die Datei kopiert. Anschließend wird neben dem Kopieren - Button eine Erfolgsmeldung (in grün) angezeigt. Dies wird wie folgt dargestellt:



Damit kann das Fenster mit dem "Schließen"-Button beendet werden.

Im Anschluss daran kann die WinLine wie gewohnt gestartet werden. Dabei erscheint das bekannte Fenster "Client Update"



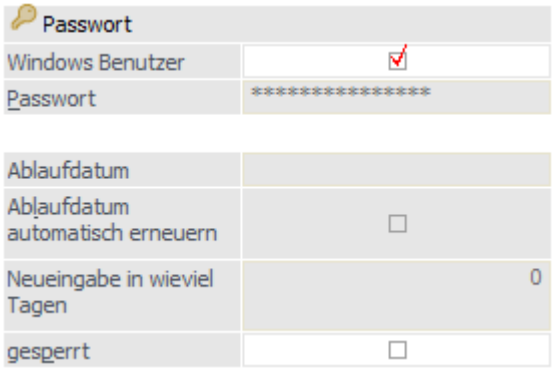
das mit "Update starten!" bestätigt werden kann. Damit ist die lokale WinLine dann auf dem aktuellen Stand.

1.2. Anbindung ActivDirectory

Mit der WinLine Edition 2027 - Version 12.35 haben wir die Möglichkeit geschaffen, WinLine Benutzer als "Windows-Benutzer" zu definieren. Ist das der Fall, wird das Passwort bei der Anmeldung nicht gegen die WinLine, sondern gegen Windows geprüft. Diese Funktion steht sowohl in der WinLine als auch in der MWL zur Verfügung.

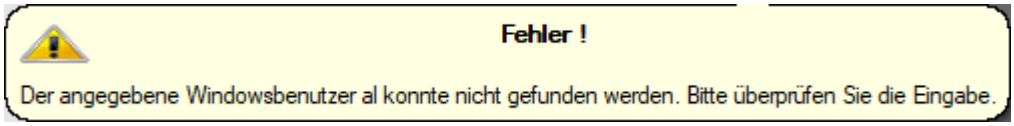
Dazu gibt es in der Benutzerverwaltung eine neue Option:

Bereich "Passwort"



- **Windows Benutzer**

Wird diese Checkbox aktiviert, wird geprüft, ob der aktuell ausgewählte Benutzername auch im AD vorhanden ist. Ist dies nicht der Fall, wird eine entsprechende Fehlermeldung ausgegeben:



Ist der Benutzer im AD vorhanden, dann werden die nachfolgenden Felder
- **Passwort**
- **Ablaufdatum**
- **Ablaufdatum automatisch erneuern**
- **Neuvergabe in wieviel Tagen**

automatisch gegrayed und können nicht mehr bearbeitet werden, weil das Passwort ab dem Zeitpunkt aus dem AD verwendet wird.

Für die Anlage von Benutzern aus dem AD wurde der Menüpunkt
- **Benutzer**
- **Automatische Benutzeranlage**

um ein Register erweitert.

1.2.1. Windows Benutzer übernehmen

In diesem Register können Windows-Benutzer als WinLine-Benutzer angelegt bzw. abgeglichen werden. Beim Aufruf des Fensters wird - sofern eine Domäne gefunden wird - die Tabelle mit allen gefundenen Windows Benutzern gefüllt und können in weiterer Folge bearbeitet werden. Dazu stehen folgende Funktionen zur Verfügung.

Domäne

- **Domänen-Controller**

In diesem Feld wird der Domänen-Controller vorgeschlagen, aus dem in weiterer Folge die Benutzer ausgelesen werden sollen. Standardmäßig wird der Domänen-Controller aus dem angemeldeten Netzwerk vorgeschlagen.

Berechtigungen von Benutzer übernehmen

- **Benutzer**

Hier kann ein Benutzer eingegeben bzw. auch über die Matchcode-Funktion gesucht werden, von dem die Berechtigungen in weiterer Folge auf neu angelegte Benutzer übertragen werden sollen. Dieser Benutzer wird dann auf alle Zeilen der Tabelle übertragen, wo ein neuer Benutzer angelegt werden könnte.

Benutzer

In der Tabelle werden im ersten Schritt alle angelegten Windows Benutzer ausgelesen und angezeigt. Zeilen, die farbig markiert sind, stellen Benutzer dar, die schon als Windows Benutzer definiert sind. Unter der Überschriftenzeile gibt es eine Filterzeile, in der eine Filterung der Tabelle nach allen Spalten durchgeführt werden kann, um z.B. auf einen bestimmten Benutzer einschränken zu können.

In der Tabelle stehen folgende Infos zur Verfügung bzw. können folgende Felder bearbeitet werden:

- **Importieren**

Mit dieser Option wird gekennzeichnet, dass der Benutzer übernommen werden soll. Die Option kann entweder manuell oder vom Programm automatisch gesetzt werden.

- **Nr.**

Wenn es mit dem gleichen Namen bereits einen WinLine Benutzer gibt, wird hier die WinLine Benutzernummer angezeigt. Gibt es für den Windows Benutzer noch keinen gleichnamigen WinLine Benutzer, wird hier 0 angezeigt.

- **Name**

Hier wird der Windows Benutzername angezeigt - dieser ist nicht veränderbar (in der Tabelle).

- **Berechtigung von Benutzer**

Hier kann entweder ein Benutzer direkt eingetragen (Vorschlag Autovervollständigung) oder über den Matchcode ausgewählt werden, von dem alle Berechtigungseinstellungen übernommen werden sollen. Wird ein Benutzer eingetragen, werden die nachfolgenden Felder (ab "Gruppe")

- **Anzeigename**

Wenn der Benutzer in der WinLine noch nicht angelegt ist, wird hier der komplette Name vom Windows Benutzer angezeigt. Für die Anlage des Benutzers in der WinLine kann der Name noch geändert werden. Ist der Benutzer in der WinLine bereits angelegt, wir der in der WinLine hinterlegte Anzeigenamen angezeigt.

- **SMTP Absender Adresse**

Wenn der Benutzer in der WinLine noch nicht angelegt ist, wird in diesem Feld die Mail-Adresse vom Windows Benutzer angezeigt, der auch in den WinLine Benutzer übernommen werden kann. Ist der Benutzer in der WinLine bereits angelegt, wir die in der WinLine hinterlegte Mail-Adresse angezeigt.

- **Gruppe**

Bei noch nicht zugeordneten Benutzern (Nr. 0) wird hier die "Default"-Gruppe angezeigt, bei bereits angelegten Benutzern ist die zugeordnete Gruppe ersichtlich.

- **Gesperrt**

Ist diese Checkbox aktiviert, dann kann sich dieser Benutzer nicht mehr in der WinLine bzw. der MWL anmelden.

- **Admin**

Diese Checkbox weist den Benutzer Administratorenrechte in der WinLine zu.

- **Demo**

Diese Checkbox weist den Benutzer als Demo-Benutzer der WinLine aus - d.h. der Benutzer kann alle Programme öffnen (auch die, für die keine Lizenz vorhanden ist).

- **CWL Benutzer**

Der Benutzer kann gemäß der vorhandenen Lizenz und der restlichen Einstellungen mit der WinLine arbeiten.

- **Digitalisierung/CRM Benutzer**

Der Benutzer kann den Programmbereich des CRMs innerhalb der WinLine (Desktop-Version) benutzen.

- **Konten einschränken**

Mit dieser Option wird gesteuert, ob der Benutzer alle Konten sehen darf, oder nur die, bei denen er als Vertreter hinterlegt ist. Eine weiterführende Einstellung ist nur in der Benutzeranlage selbst möglich.

- **Kassen Benutzer**

Wird diese Checkbox aktiviert, so können die Funktionen der WinLine KASSE (Desktop-Version) genutzt werden.

- **WinLine SMART Benutzer**

Mit dieser gesetzten Checkbox steht dem Benutzer über die MWL das SMART Cockpit zur Verfügung, welches alle Funktionen beinhaltet, die dem WinLine SMART Benutzer zur Verfügung stehen. Dafür muss auch eine entsprechende Lizenz vorhanden sein.

- **Mandant**

Aus der Auswahllistbox kann der Mandant gewählt werden, auf den der Benutzer in der MWL zugreifen soll.

- **Konto**

Hat derzeit keine Verwendung

- **Laufkunde**

Hat derzeit keine Verwendung

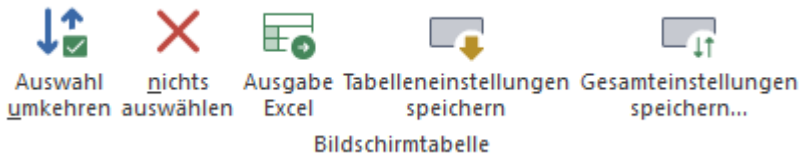
- **Arbeitnehmer**

Für die Verwendung von SMART Benutzern kann hier eine AN-/MA-Nummer eingetragen werden, unter welcher der Benutzer im WinLine LOHN/WinLine INFO angelegt ist.

- **Vertreter**

Hier kann dem Benutzer ein Vertreter zugewiesen werden. Über die Matchcode-Funktion kann nach allen angelegten Vertretern gesucht werden. Weiterführende Einstellungen dazu können in der Benutzeranlage durchgeführt werden.

Tabellenbuttons



- **Auswahl umkehren**

Durch Anklicken des Umkehren-Buttons kann die vorgenommene Einstellung in das Gegenteil gewandelt werden.

- **nichts auswählen**

Durch Anklicken des Buttons "nichts auswählen" werden alle getroffenen Selektionen gelöscht.

- **Ausgabe Excel**

Durch Anwahl des Buttons "Ausgabe Excel" wird der Inhalt der Tabelle an Microsoft Excel übergeben.

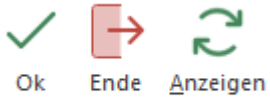
- **Tabelleneinstellungen speichern**

Die Spalten einer Tabelle können grundsätzlich an beliebige Positionen verschoben, bzw. in der Breite entsprechend angepasst werden. Durch Anwahl des Buttons "Tabelleneinstellungen speichern" werden die Einstellungen benutzerspezifisch gespeichert und bei dem nächsten Aufruf des Programmpunktes wieder vorgeschlagen.

- **Gesamteinstellungen speichern**

Im Gegensatz zu "Tabelleneinstellungen speichern" können mit "Gesamteinstellungen speichern" mehrere Tabellenaufbauten gespeichert und nach Wunsch geladen werden. Zusätzlich werden Sonderfunktionen der Tabelle (z.B. "Spalte gruppieren") ebenfalls bei der Speicherung bedacht.

Buttons



- **OK**

Durch Anklicken des OK-Buttons werden alle Benutzer gespeichert, wo die Option "Importieren" gesetzt ist. Anschließend wird die Tabelle neu geladen.

- **Ende**

Mit dem ENDE-Button bzw. durch Drücken der ESC-Taste wird das Fenster geschlossen, es werden keine weiteren Daten gespeichert.

- **Anzeigen**

Durch Anklicken des Anzeigen-Buttons wird die Tabelle neu geladen.

1.2.1.1. Ablauf bzw. Möglichkeiten im Fenster

Verknüpfte Benutzer

Wenn der Menüpunkt geöffnet wird, werden alle Windows Benutzer eingelesen. WinLine Benutzer, die bereits als Windows Benutzer angelegt sind, werden farbig dargestellt.

WinLine Benutzer bereits angelegt - Verknüpfung von Benutzern

Bei Benutzern, die bereits in der WinLine angelegt sind und die unter Windows den gleichen Namen aufweisen, wird die Benutzernummer angezeigt. Auch die restlichen Felder werden bereits aus der Benutzeranlage vorgeschlagen bzw. angezeigt.

Um hier eine Verknüpfung herzustellen, reicht es, die Option "Importieren" zu setzten. Damit wird dann beim Benutzer die Option "Windows Benutzer" gesetzt.

Neuanlage von Benutzern

Wenn in der Spalte "Nr." der Wert 0 angezeigt wird, dann gibt es in der WinLine noch keinen Benutzer für den Windows Benutzer. Durch Aktivieren der Option "Importieren" wird der Benutzer zur Anlage gekennzeichnet. In der Spalte "Berechtigung von Benutzer" kann nun ein Benutzer eingetragen oder über den Matchcode ausgewählt werden, von dem die Berechtigungen übernommen werden sollen. Mit Bestätigung des Benutzers werden die entsprechenden Einstellungen auch in den nachfolgenden Spalten angezeigt.

Wird kein Benutzer für die Übernahme der Berechtigungen eingegeben, muss die Benutzertypenzuordnung manuell erfolgen (CWL Benutzer, DIGI-Benutzer, etc.), ansonsten wird spätestens beim Speichern eine Meldung "Es muss ein Benutzertyp angegeben werden" angezeigt.

Der Anzeigename und die SMTP Absender Adresse werden vom AD ausgelesen und vorgeschlagen, können aber bei Bedarf noch verändert werden.

Durch Anklicken des OK-Buttons werden dann alle Benutzer, bei denen die Option "Importieren" gesetzt ist, entsprechend angelegt. Weiterführende Einstellungen können dann in der Benutzerverwaltung selbst durchgeführt werden.

Nach dem Speichern wird die Tabelle wieder aktualisiert, neu angelegte Benutzer werden dann auch gleich entsprechend markiert.