MultiCash®

Schnelleinstieg für Administratoren

Benutzerhandbuch

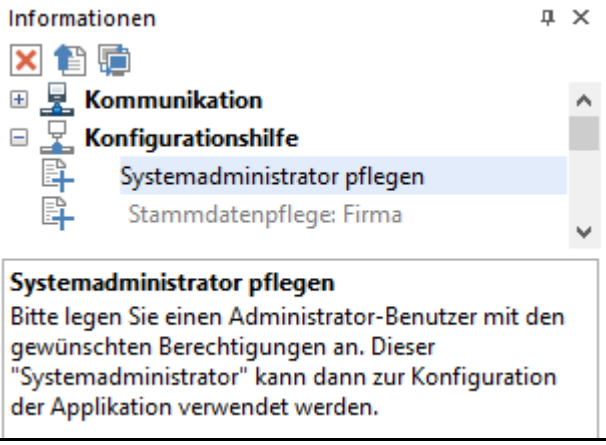
Omikron Systemhaus GmbH & Co. KG
Von-Hünefeld-Str. 55
D-50829 Köln

Tel.: +49 (0)221 -59 56 99 -0
Fax: +49 (0)221 -59 56 99 -7

info@omikron.de
www.omikron.de

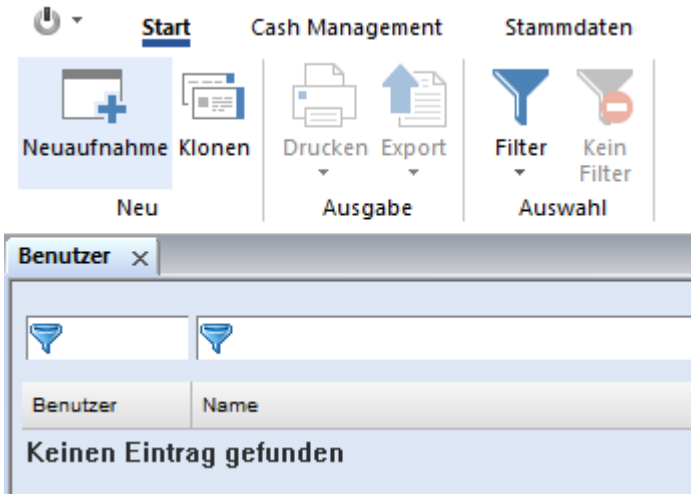
1 Systemeinrichtung mittels Konfigurationshilfe:

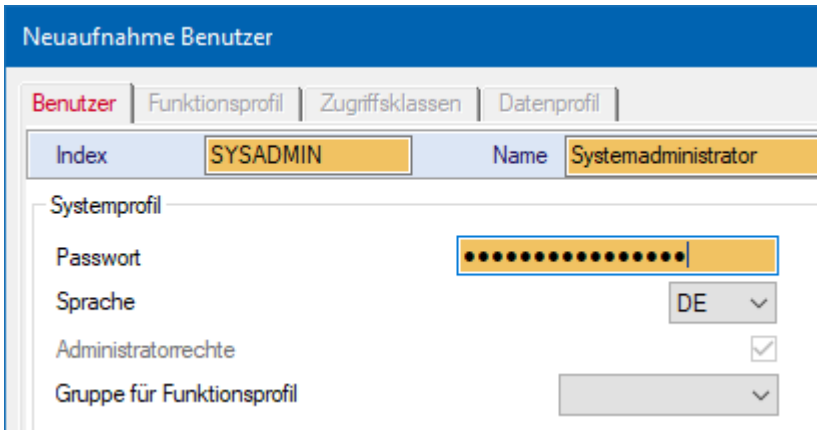
Nach einer Installation der gewünschten Programmvariante (vgl. Benutzerhandbuch-Kapitel 1.1) wird im Informationen-Fenster eine Konfigurationshilfe mit mehreren Unterpunkten eingeblendet.
Ein **Doppelklick** auf den jeweiligen Funktions-Eintrag öffnet den zugehörigen Ziel-Dialog für die Durchführung der beschriebenen Aktion. Anschließend verschwindet der Eintrag.

Nr.	**Funktion** (geforderte Aktion)	**Beschreibung** (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	**Ziel-Dialog**	**Kapitel im Benutzer-handbuch**
Anmeldung als Benutzer ADMIN2				
1	System-administrator pflegen (obligatorisch)		Verwaltung/ Benutzer	1.2.1

Beim ersten Programmzugang zu einer neuen Umgebung wird die bei der Installation erstellte Masterpasswortdatei benötigt, mit der Sie automatisch als Sonderadministrator ADMIN2 angemeldet werden. Aus Sicherheitsgründen ist dieser ADMIN2-Benutzer lediglich zur Anlage von administrativen Benutzergruppen und Administrator-Benutzern berechtigt.

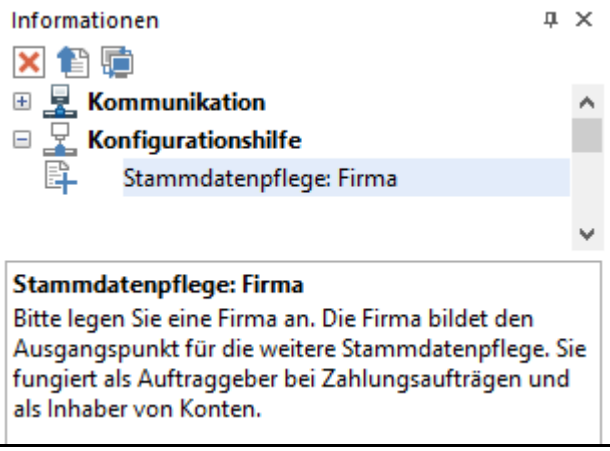
Nehmen Sie als ADMIN2-Benutzer einen **Systemadministrator** (Administrator-Benutzer) auf.



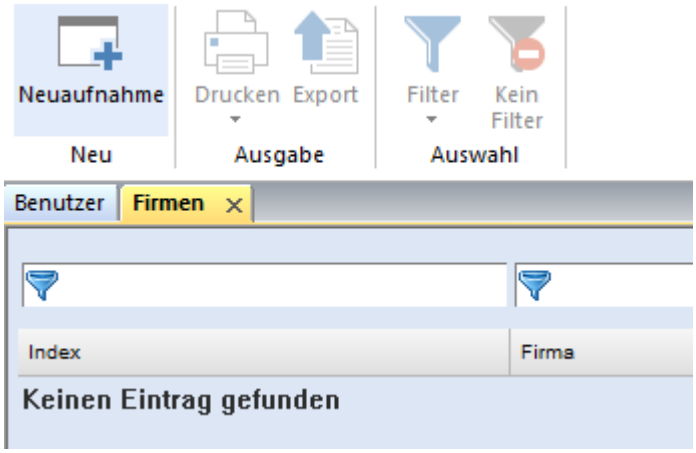


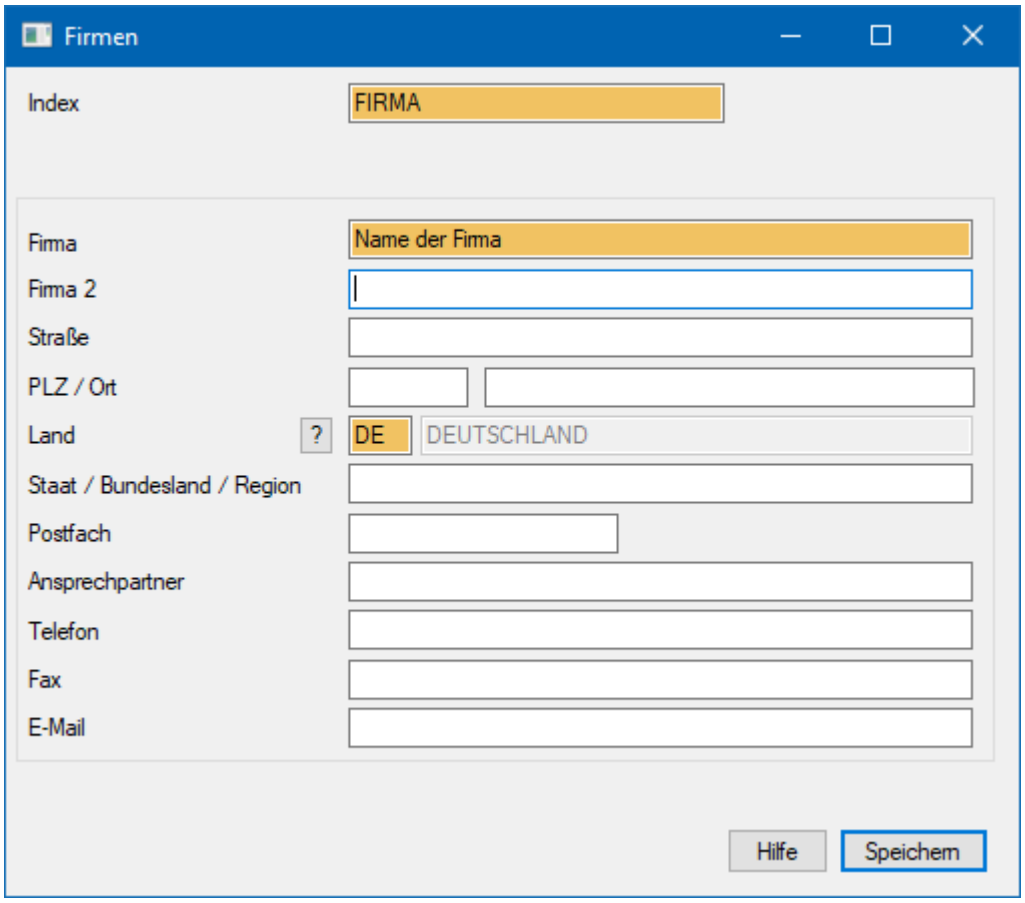
Dieser "Systemadministrator" muss sich nach Schritt 2 anmelden und die weitere Konfiguration vornehmen.

In einem weiteren Schritt legen Sie als ADMIN2 die Stammdaten der **Firma** an.

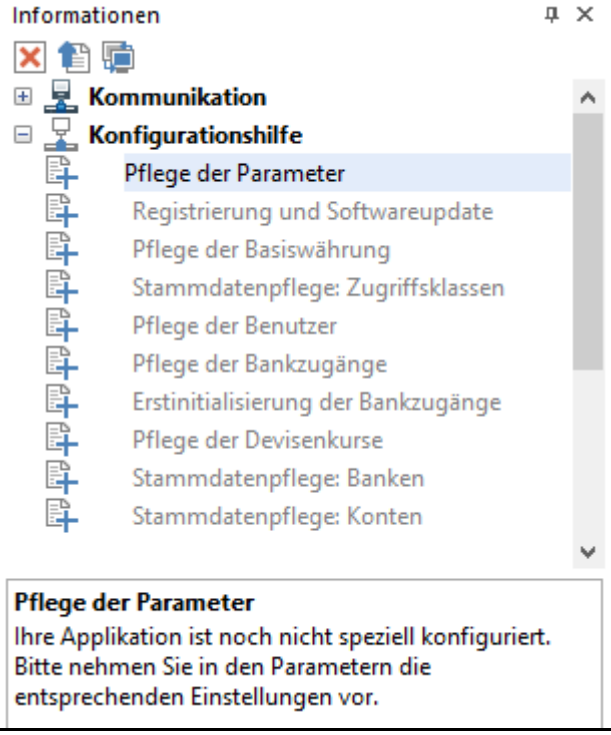
Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Benutzer ADMIN2				
2	Stammdaten-pflege: Firma (obligatorisch)		Stammdaten/ Firma	3.1

Pflegen Sie anschließend die Daten der Firma ein.




Firmen
Index
FIRMA
Firma
Name der Firma
Firma 2
Straße
PLZ / Ort
Land
?
DE
DEUTSCHLAND
Staat / Bundesland / Region
Postfach
Ansprechpartner
Telefon
Fax
E-Mail
Hilfe
Speichern

Melden Sie sich nun als ADMIN2-Benutzer ab und melden Sie sich mit dem angelegten "Systemadministrator" wieder an (vgl. Benutzerhandbuch-Kapitel 1.2.3). Dabei erfolgt zunächst ein Passwortwechsel für den neu angemeldeten Benutzer. Als Administrator beginnen Sie mit der Pflege der **Parameter**.

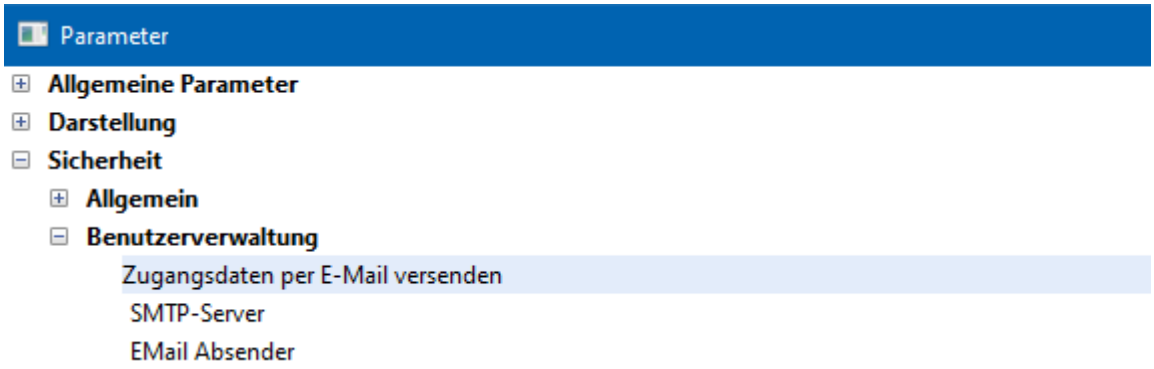
Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Systemadministrator (=Administratorrechte gesetzt)				
1	Pflege der Parameter (optional)		Verwaltung/ Parameter	2.1

Nach der Anmeldung als Systemadministrator können Sie die Parameter des Systems pflegen, z. B.

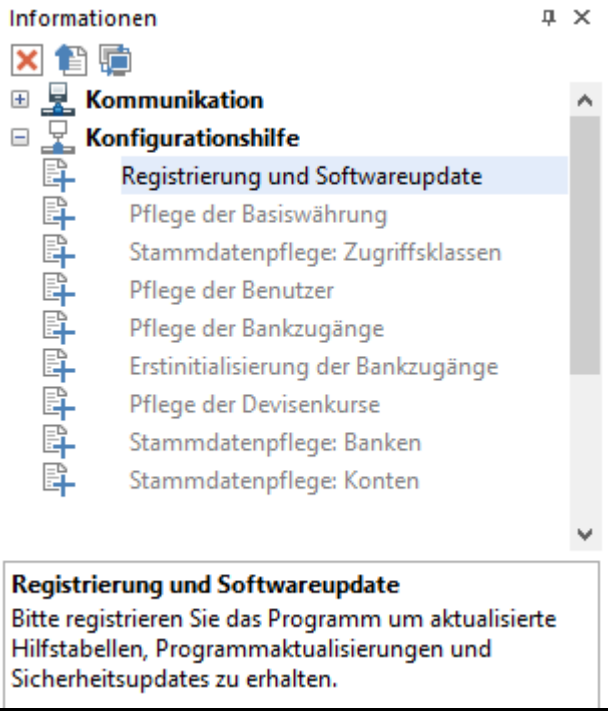
- Übertragungsparameter/ Proxy-Einstellungen
- Kommunikationsmanager/ Automatischer Export empfangener Dateien und Datenpfad automatischer Export
- Elektronische Unterschrift/ Speichermedium / USB-Stick



Wenn Sie den Versand der Zugangsdaten per E-Mail wünschen, sollte der entsprechende Parameter unter Sicherheit/Benutzerverwaltung aktiviert werden.



Anschließend erfolgt die **Registrierung** des Programms und die Konfiguration von **Softwareupdates**.

Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Systemadministrator (=Administratorrechte gesetzt)				
2	Registierung und Softwareupdate (obligatorisch)		Verwaltung/ Software-Update	2.9

Hier können Sie Ihre Software für automatischen Aktualisierungen oder Software-Updates (Zusatz-Service) registrieren.

Wenn Sie die Software registrieren, bietet Ihnen Ihr Software-Hersteller eine **kostenlose Basisaktualisierung** als Service zur Aktualisierung von wichtigen Standardtabellen und Verarbeitungsregeln an:

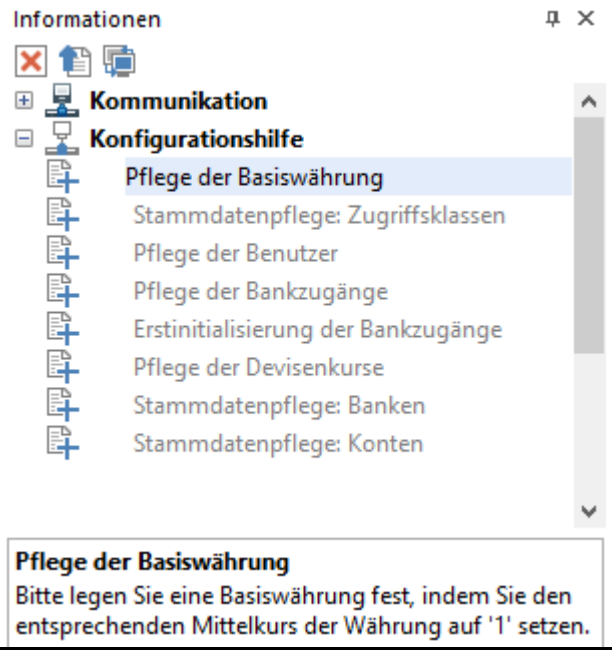
- Regelwerke für IBAN- und Euro-Verarbeitung
- Bankleitzahlentabellen für Deutschland, Österreich und die Schweiz
- Register der SEPA unterstützenden Banken in Europa (SCL-Directory)
- Zugangsdaten vieler EBICS-Bankrechner

© 2024 Omikron Systemhaus GmbH & Co. KG

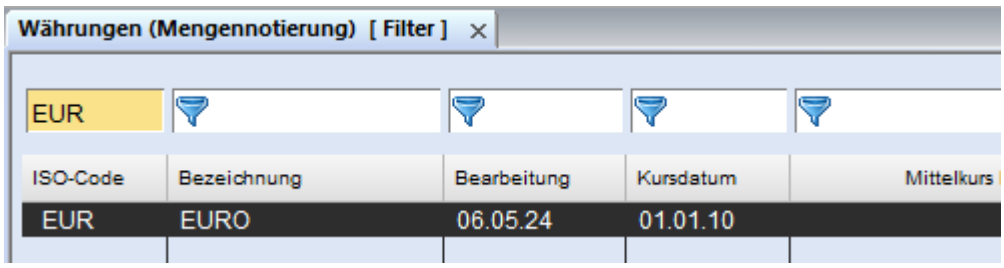
Optional bietet Ihnen Ihr Software-Lizenzgeber einen Service für **vollständige Softwareaktualisierungen** für die von ihm bezogenen Softwaremodule an (Direktkunden von Omikron sollten immer diese Variante wählen). Wenn diese Option aktiv ist und ausgewählt wird, erhalten Sie zusätzlich zur Basisaktualisierung neue Software-Versionen, die Sie nach Ihren organisatorischen Regeln zum von Ihnen definierten Zeitpunkt installieren können. Es ist kein Problem ein Update zu überspringen. Sie erhalten dann später ein neues, erweitertes Update-Paket, wenn weitere Komponenten aktualisiert werden sollten.



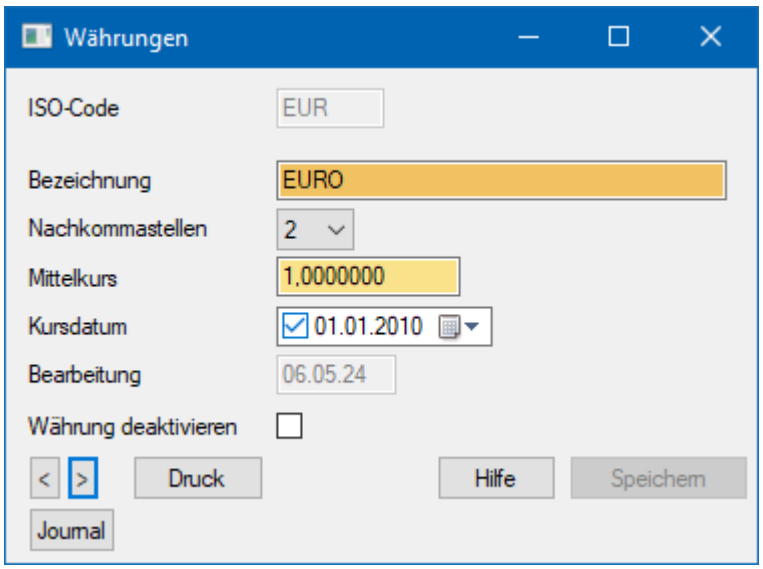
Anschließend muss eine **Basiswährung** für das System festgelegt werden.

Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Systemadministrator (=Administratorrechte gesetzt)				
3	Pflege der Basiswährung (obligatorisch)		Stammdaten/ Währungen	3.6

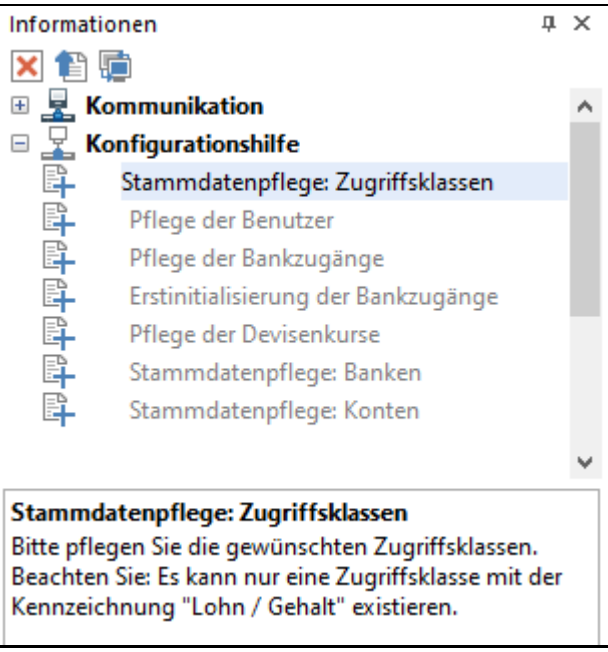
Wählen Sie zunächst eine Währung aus.



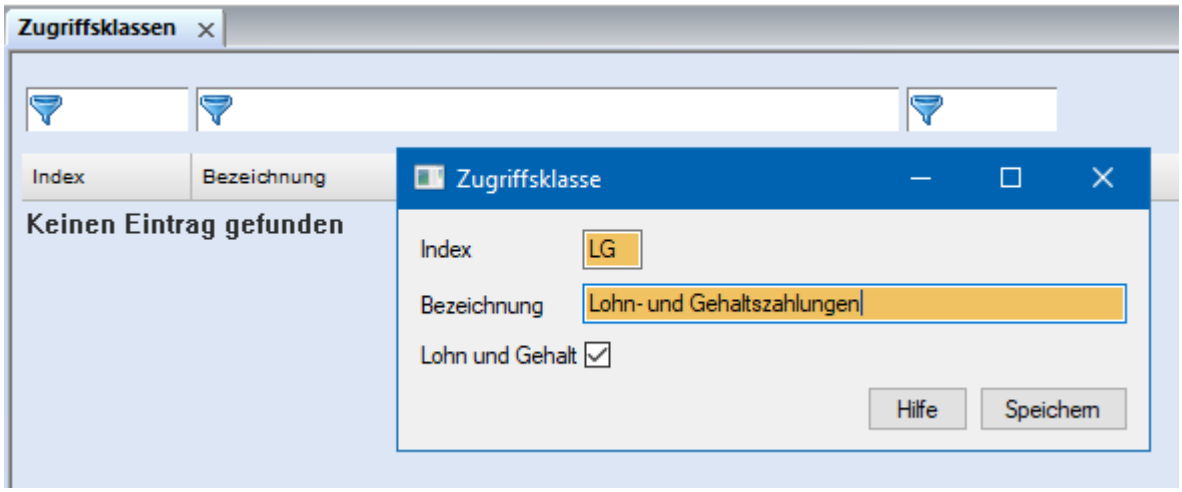
Durch Setzen des Mittelkurses der Währung =1 definieren Sie diese als Basiswährung des Systems.



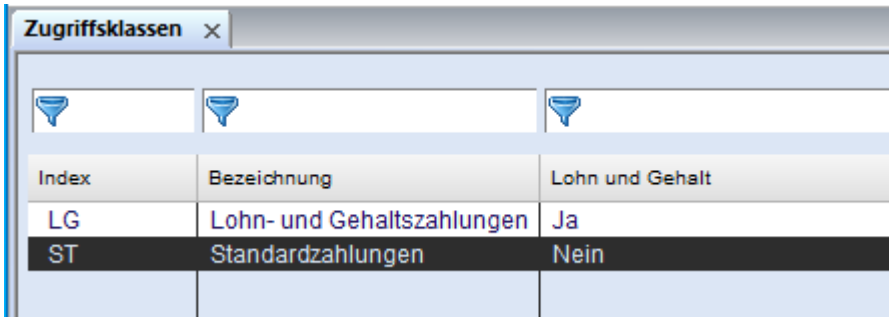
Falls Sie die Zugriffssteuerung für vertrauliche Zahlungen verwenden möchten, legen Sie danach die benötigten **Zugriffsklassen** an.

Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Systemadministrator (=Administratorrechte gesetzt)				
4A	Stammdaten-pflege: Zugriffsklassen (optional)		Verwaltung/ Zugriffs-klassen	2.6

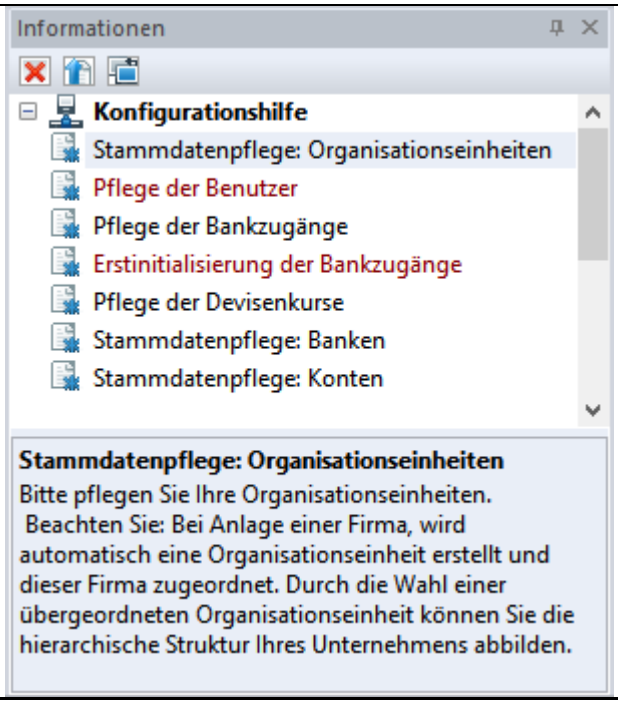
Legen Sie die Zugriffsklassen für das System fest.



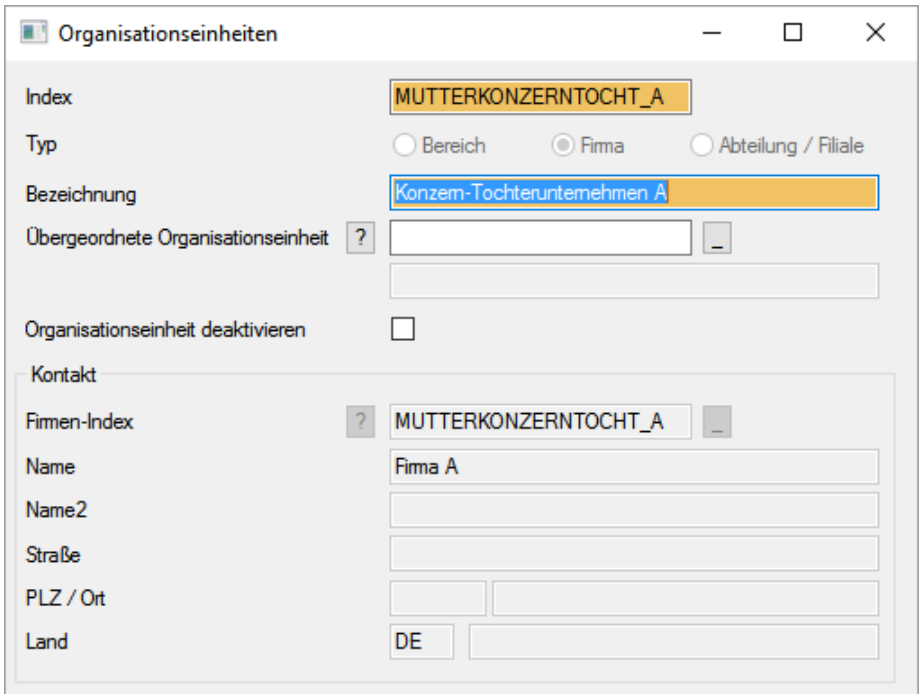
Beachten Sie bitte, dass es nur eine Zugriffsklasse mit der Kennzeichnung "Lohn und Gehalt" geben kann.



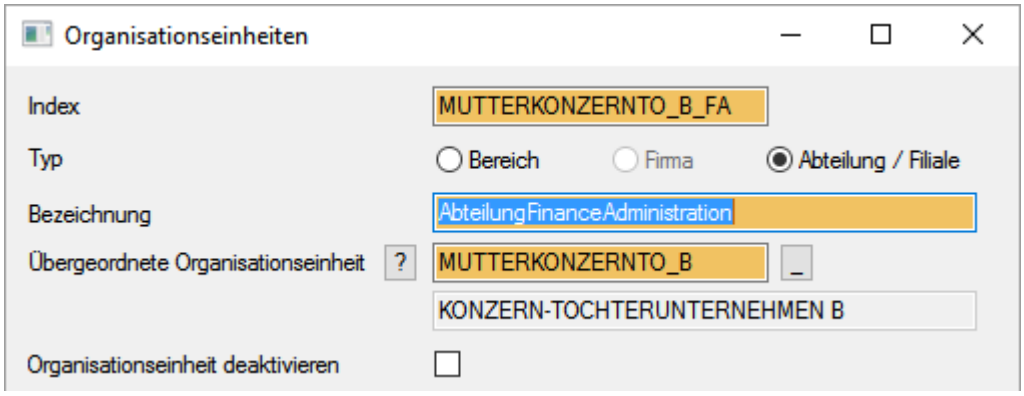
Falls zur Verwaltung einer Konzernhierarchie das **Zusatzmodul "Konzernverwaltung"** installiert ist, pflegen Sie jetzt die **Organisationseinheiten** ein.

Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Systemadministrator (=Administratorrechte gesetzt)				
4B	Stammdaten-pflege: Organisations-einheiten (optional) **nur, wenn das Zusatzmodul "Konzern-verwaltung" installiert wurde**		Verwaltung/ Organisations einheiten	2.7

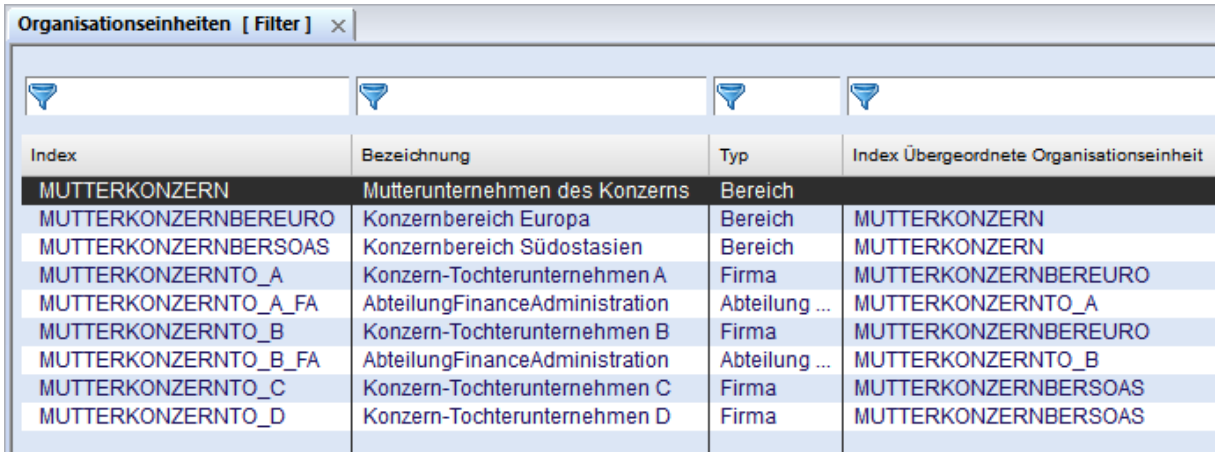
Pflegen Sie Ihre Konzernstruktur über die Funktion "Organisationseinheiten" ein.



Durch entsprechende Zuordnung "Übergeordneter Organisationseinheiten" bilden Sie die unternehmenseigenen Hierarchieebenen ab.



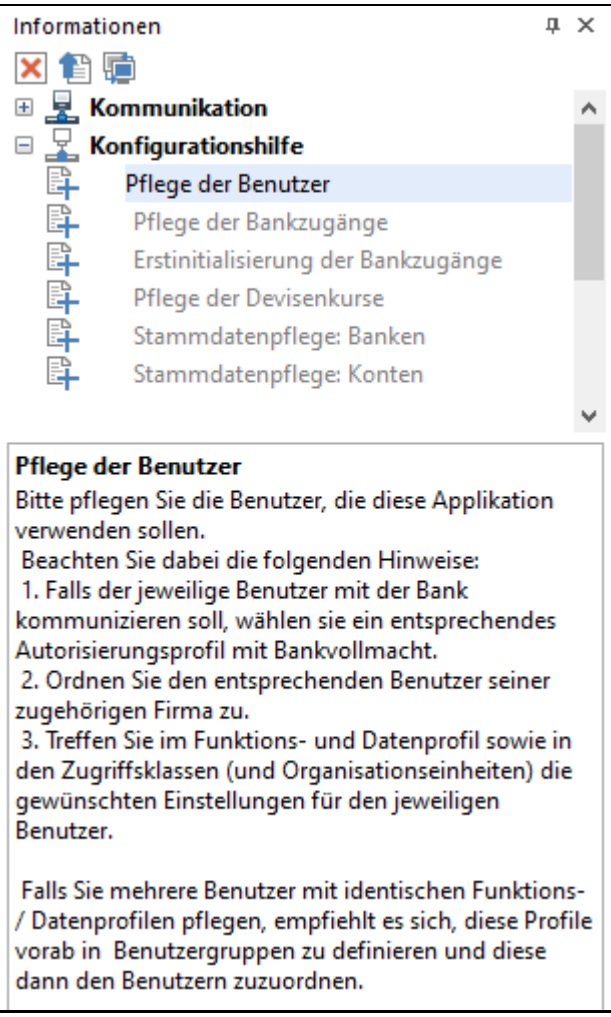
Erfassen Sie so die vollständige Organisationstruktur Ihres Unternehmens.



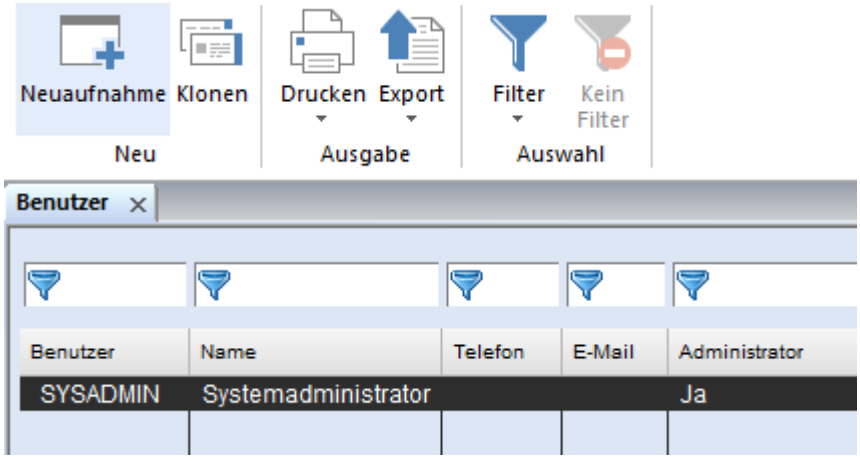
Index	Bezeichnung	Typ	Index Übergeordnete Organisationseinheit
MUTTERKONZERN	Mutterunternehmen des Konzerns	Bereich	
MUTTERKONZERNBEREURO	Konzernbereich Europa	Bereich	MUTTERKONZERN
MUTTERKONZERNBERSOAS	Konzernbereich Südostasien	Bereich	MUTTERKONZERN
MUTTERKONZERNTO_A	Konzern-Tochterunternehmen A	Firma	MUTTERKONZERNBEREURO
MUTTERKONZERNTO_A_FA	AbteilungFinanceAdministration	Abteilung ...	MUTTERKONZERNTO_A
MUTTERKONZERNTO_B	Konzern-Tochterunternehmen B	Firma	MUTTERKONZERNBEREURO
MUTTERKONZERNTO_B_FA	AbteilungFinanceAdministration	Abteilung ...	MUTTERKONZERNTO_B
MUTTERKONZERNTO_C	Konzern-Tochterunternehmen C	Firma	MUTTERKONZERNBERSOAS
MUTTERKONZERNTO_D	Konzern-Tochterunternehmen D	Firma	MUTTERKONZERNBERSOAS

© 2024 Omikron Systemhaus GmbH & Co. KG

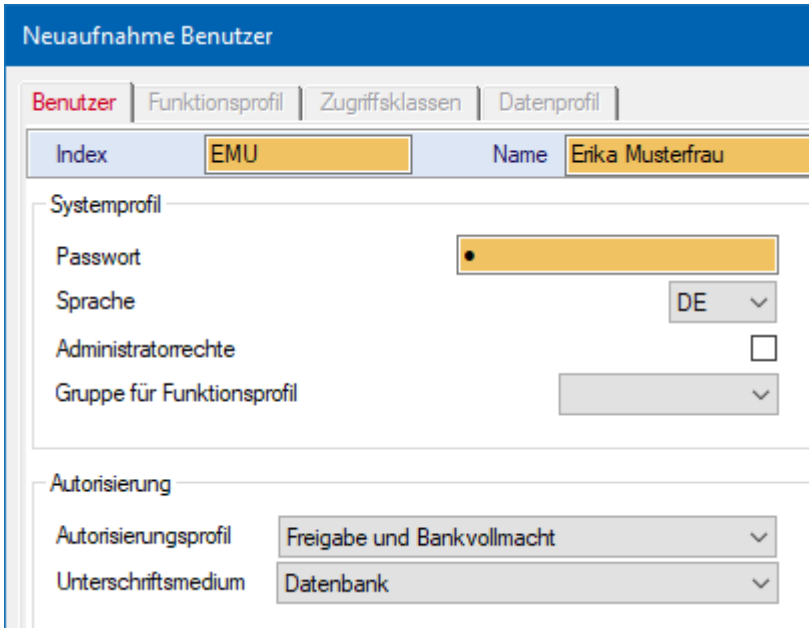
Legen Sie nun die **Benutzer** an, die mit dem System arbeiten sollen.

Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Systemadministrator (=Administratorrechte gesetzt)				
5	Pflege der Benutzer (obligatorisch)		Verwaltung/ Benutzer	2.4

Legen Sie weitere Benutzer an.



1. Falls der jeweilige Benutzer mit der Bank kommunizieren soll, wählen Sie ein entsprechendes Autorisierungsprofil mit **Bankvollmacht**.

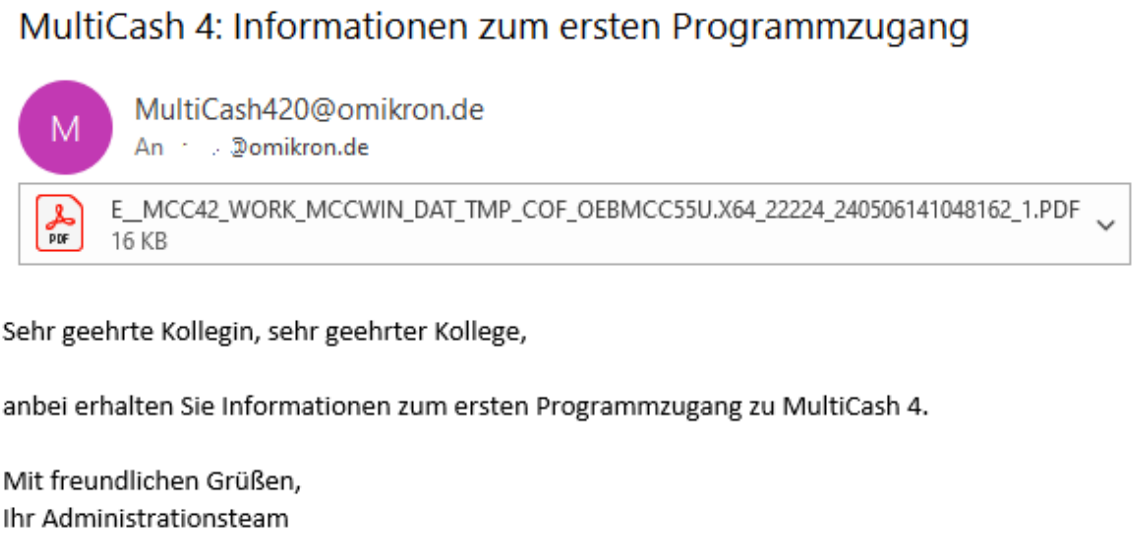


2.a Ordnen Sie jedem Benutzer die Firma zu.

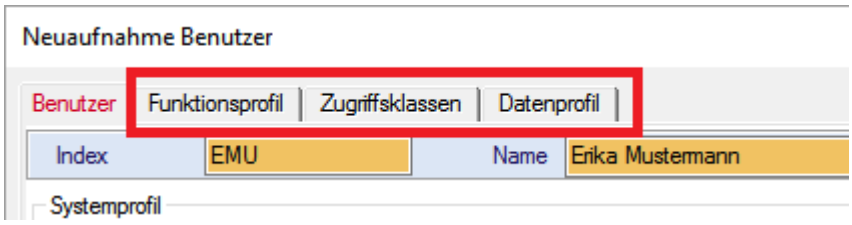
2.b Tragen Sie die E-Mail-Adresse des jeweiligen Benutzers unter den Kontaktdaten ein, damit dieser beim Klick auf [***Speichern***] automatisch eine E-Mail mit dem von Ihnen initial vergebenen Passwort erhält.



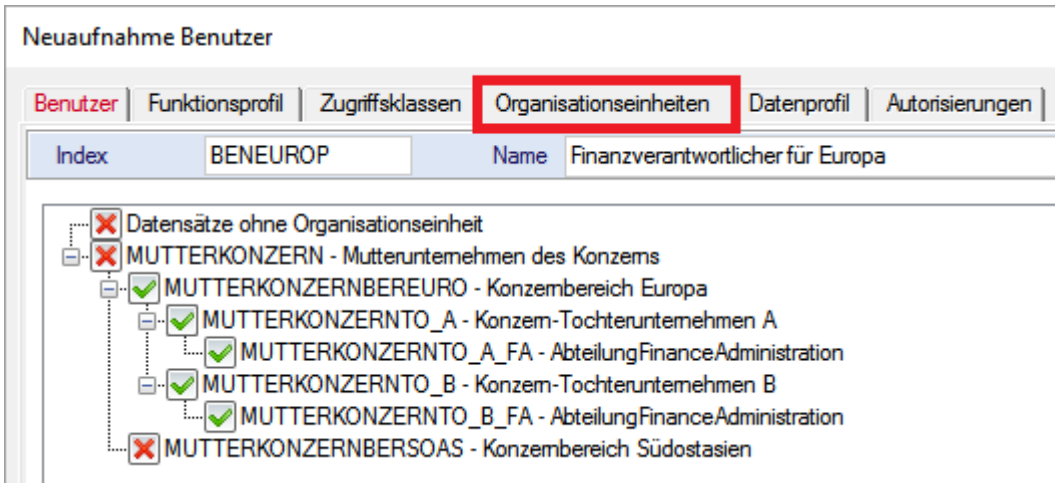
Beispiel für eine entsprechende E-Mail:



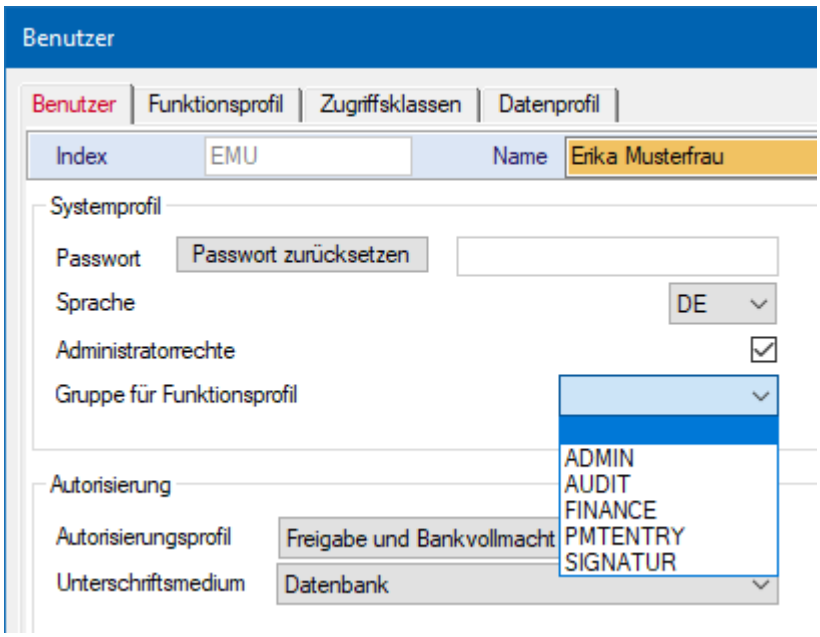
3.a Treffen Sie im Funktions- und Datenprofil sowie in den Zugriffsklassen (und ggf. Organisationseinheiten) die gewünschten Einstellungen für den jeweiligen Benutzer, sofern dies nicht bereits über eine Gruppenzuordnung erfolgt ist.



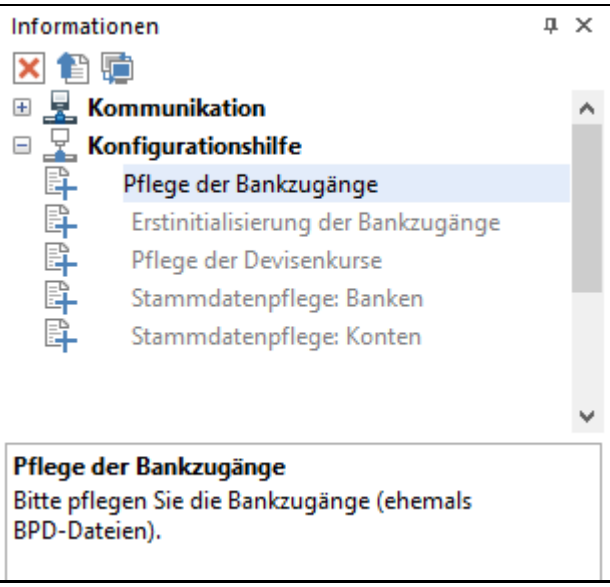
Ist das Zusatzmodul Konzernverwaltung installiert, sind auch auf der Registerkarte Organisationseinheiten entsprechende Einstellungen vorzunehmen.



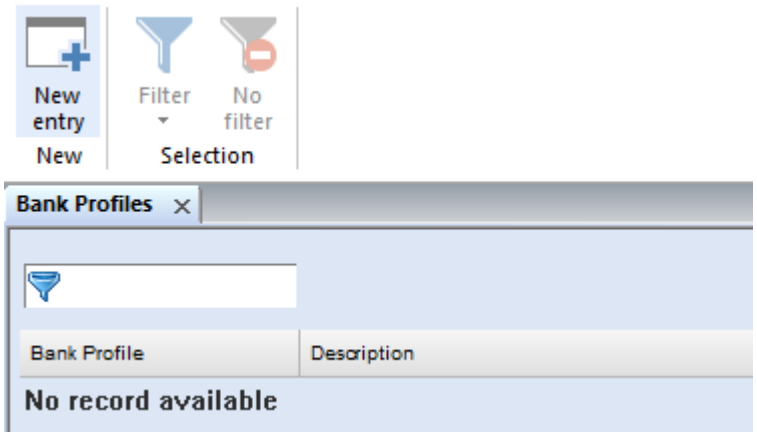
3.b [optional] Falls Sie mehrere Benutzer mit identischen Funktions- / Datenprofilen pflegen, empfiehlt es sich, diese Profile vorab in den **Benutzergruppen** (Kapitel 2.5) zu definieren und diese dann den Benutzern zuzuordnen.



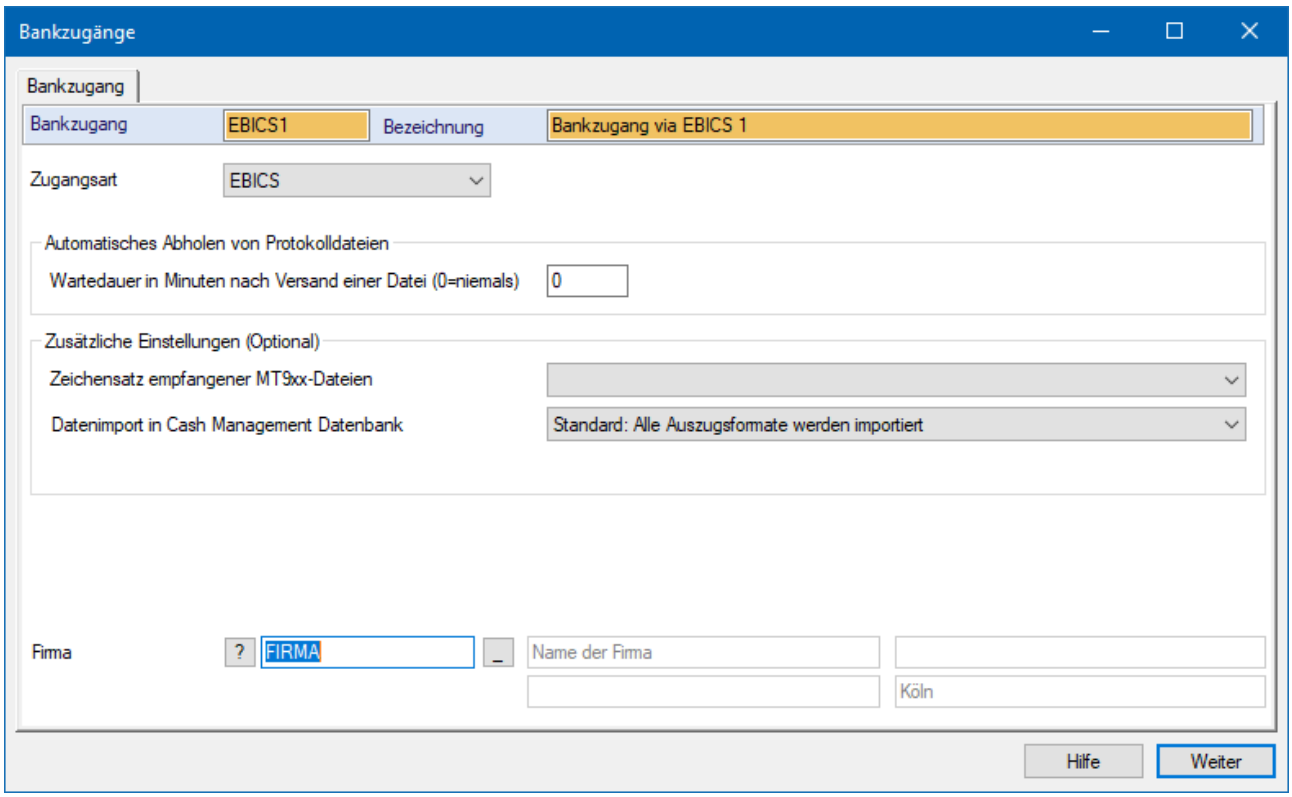
Legen Sie dann die **Bankzugänge** im System an.

Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Systemadministrator (=Administratorrechte gesetzt)				
6	Pflege der Bankzugänge (optional)		Kommuni-kation/ Bankzugänge	4.1

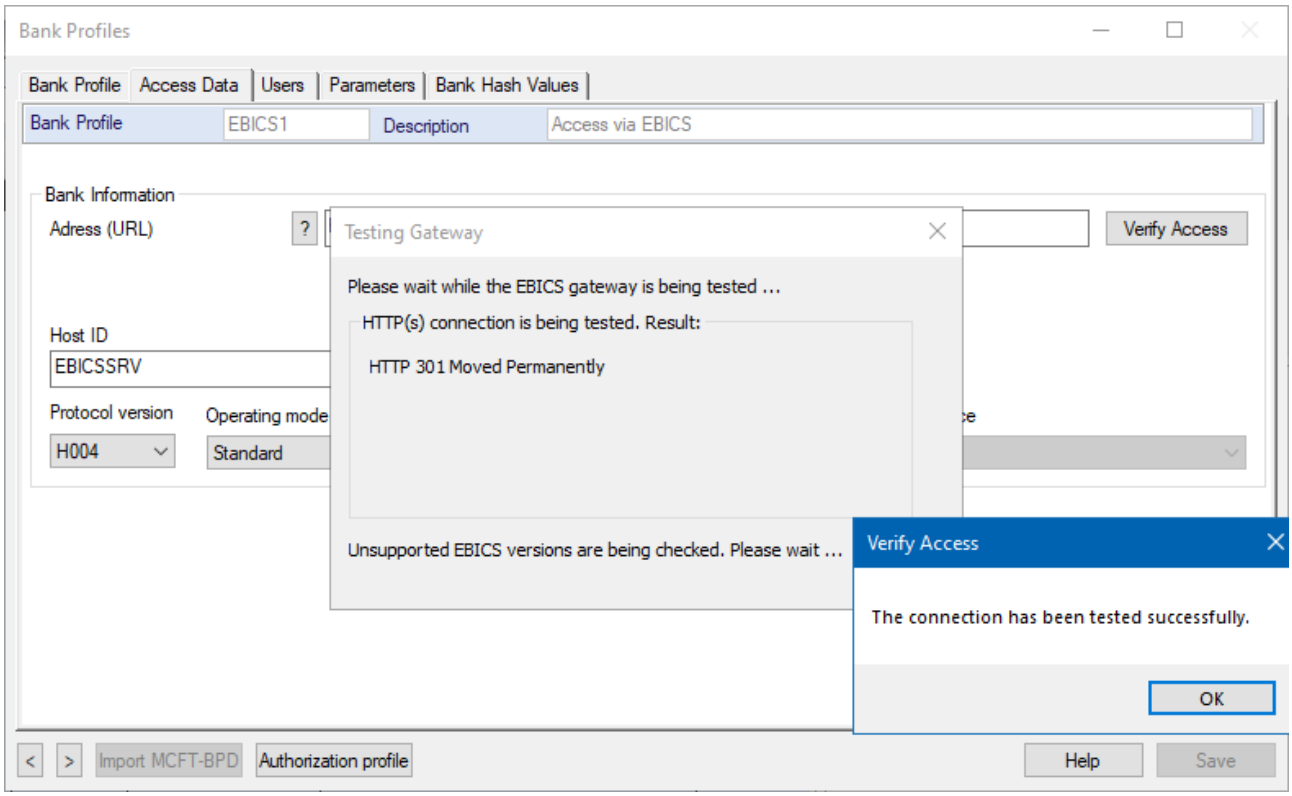
Legen Sie einen Bankzugang an (hier z. B. für die Zugangsart EBICS).



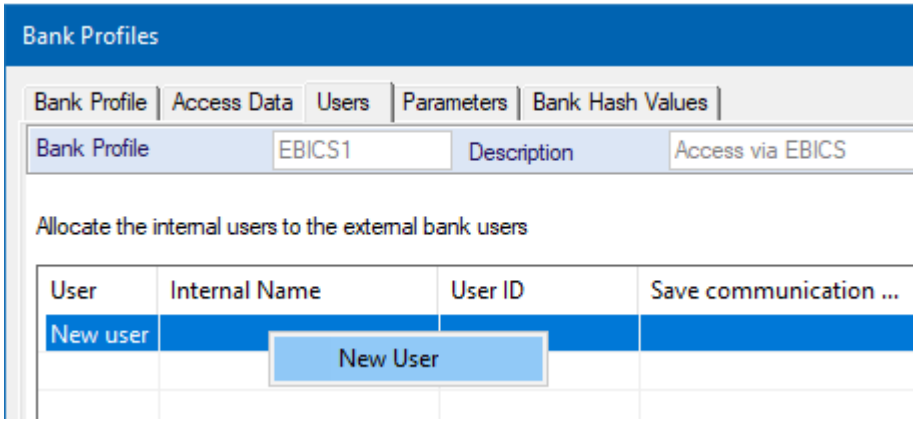
Tragen Sie auch hier die Firma ein.

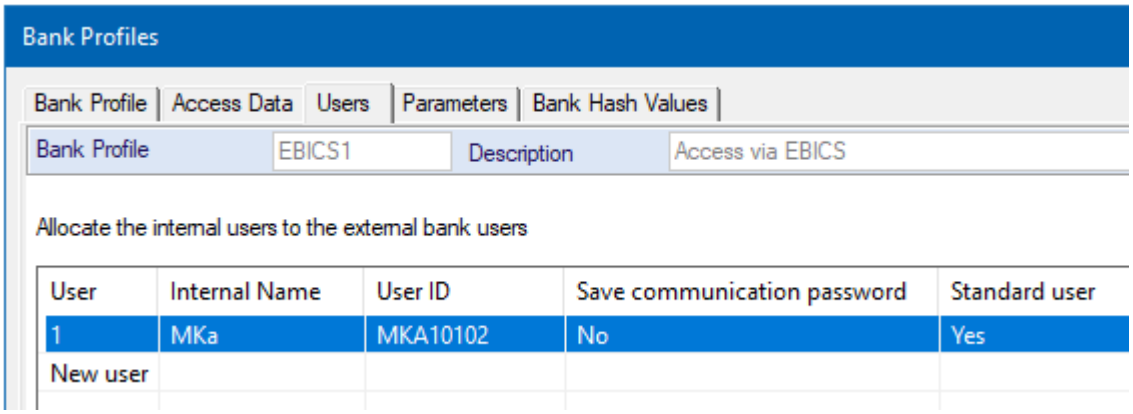


Erfassen Sie die Zugangsdaten zur Bank. Bei Bedarf können Sie den Zugang über eine entsprechende Schaltfläche direkt prüfen.

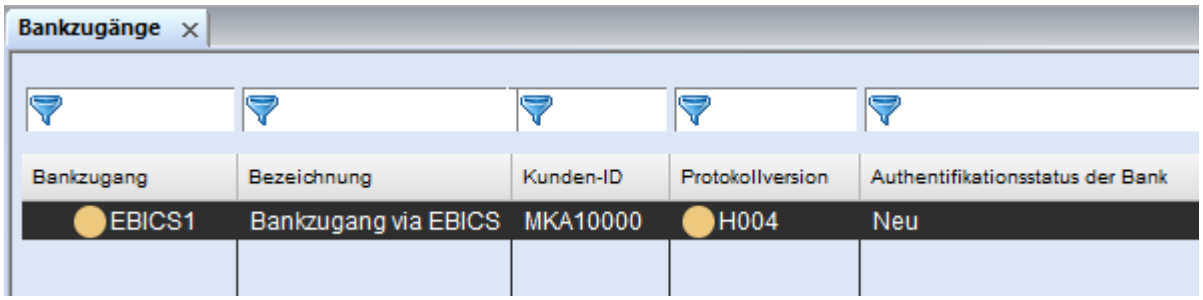


Erfassen Sie auf der Registerkarte Teilnehmer über den Eintrag "**Neuaufnahme Benutzer**“ die jeweiligen Benutzer (interne Namen) und ihre zugehörigen externen Namen (aus den Zugangsdaten der Bank).

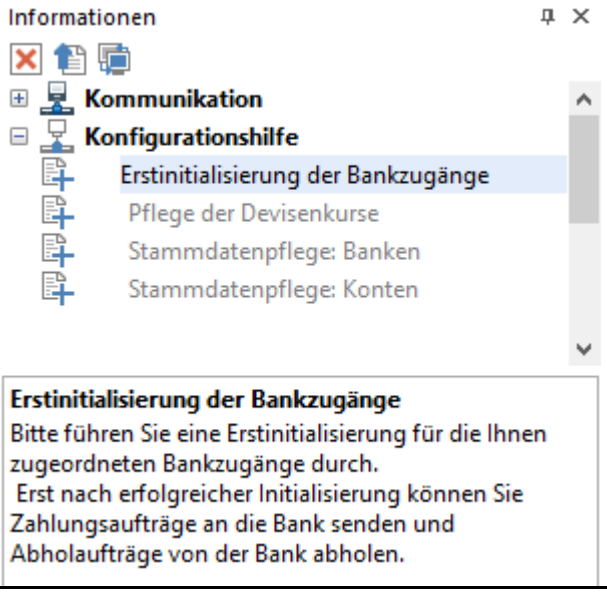




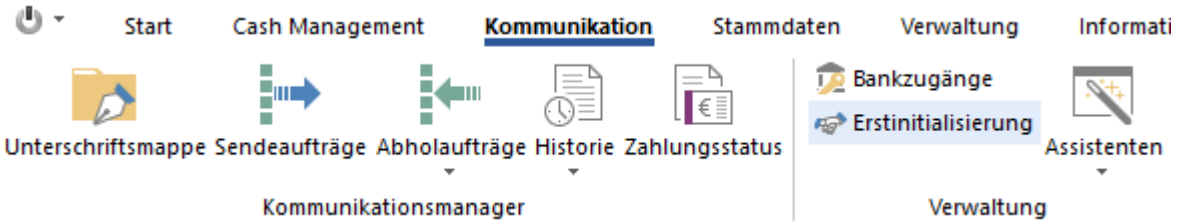
Anschließend befindet sich der Bankzugang im Status "**Neu**“ (gelbes Ampelsymbol).



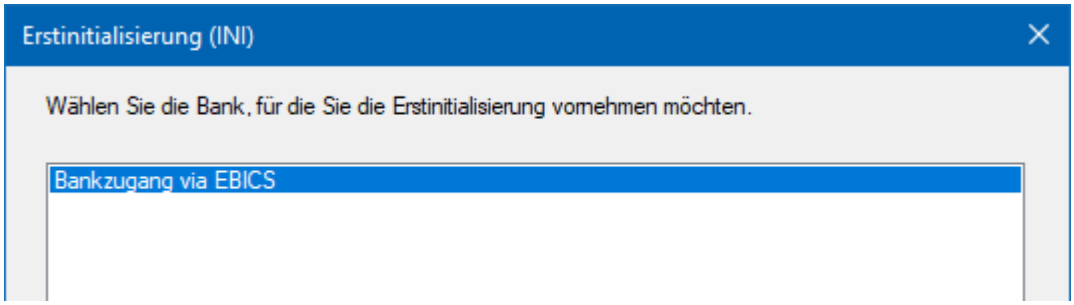
Anschließend müssen Sie eine Neuanmeldung und **Erstinitialisierung** mit jedem bankbevollmächtigtem Benutzer durchführen, mindestens aber mit dem Standardbenutzer.

Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Benutzer				
7	Erstinitialisierung der Bankzugänge (obligatorisch)		Kommuni-kation/ Erst-initialisierung	4.2

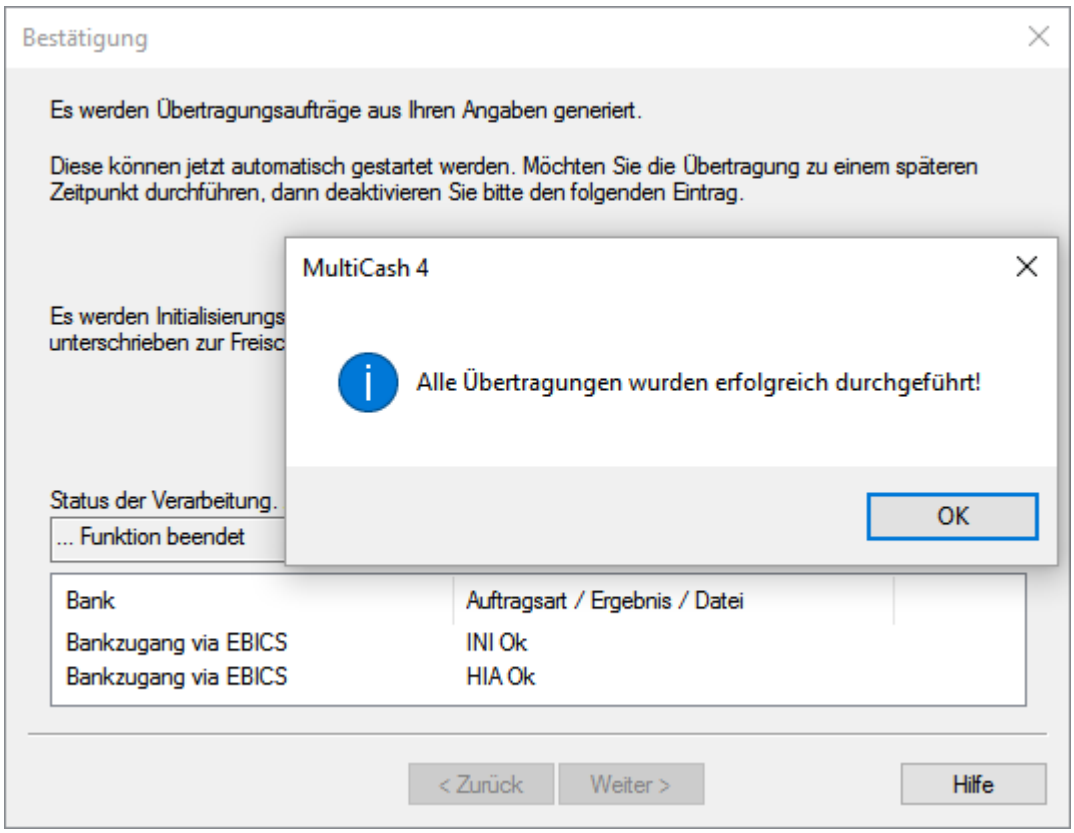
Wählen Sie unter **Kommunikation** / **Erstinitialisierung** den zu initialisierenden Bankzugang aus.



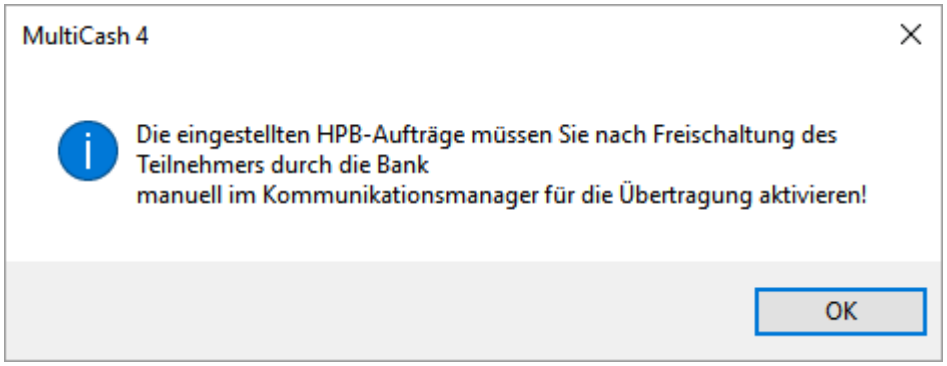
Folgen Sie den Anweisungen und starten Sie die Initialisierung.



Bestätigen Sie abschließend die erfolgreich übertragenen Initialisierungsaufträge mit [***OK***].



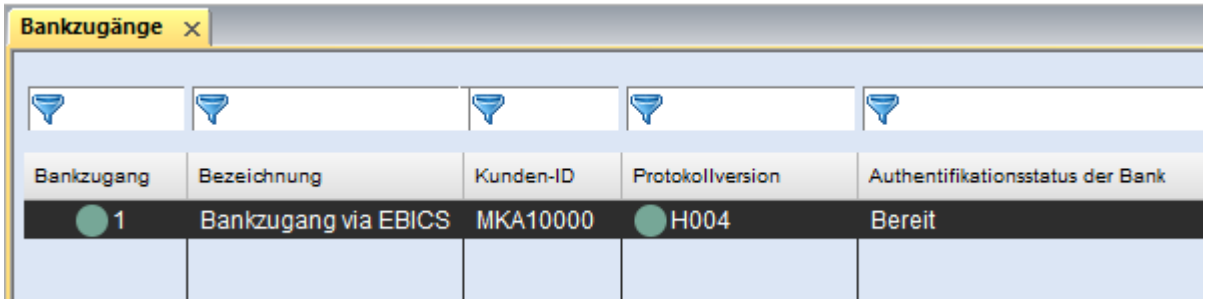
Bestätigen Sie auch den Hinweis auf die angelegten HPB-Aufträge mit [***OK***]. Warten Sie dann zunächst die Freischaltung Ihrer Teilnehmer durch die Bank ab.



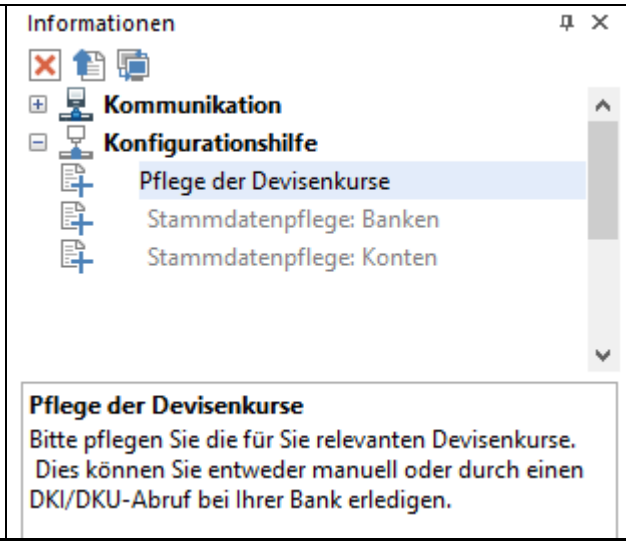
Nach Freischaltung durch die Bank müssen Sie den angelegten HPB-Sendeauftrag (zur Anforderung der Bankschlüssel) im Kommunikationsmanager ausführen.

© 2024 Omikron Systemhaus GmbH & Co. KG

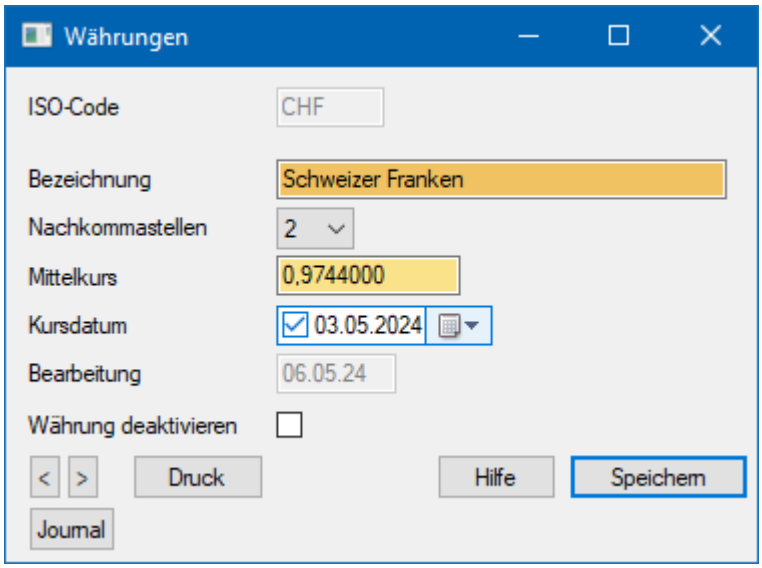
Nach erfolgreicher Abholung der Bankschlüssel befindet sich der Bankzugang im Status "**Bereit**" (grünes Ampelsymbol).



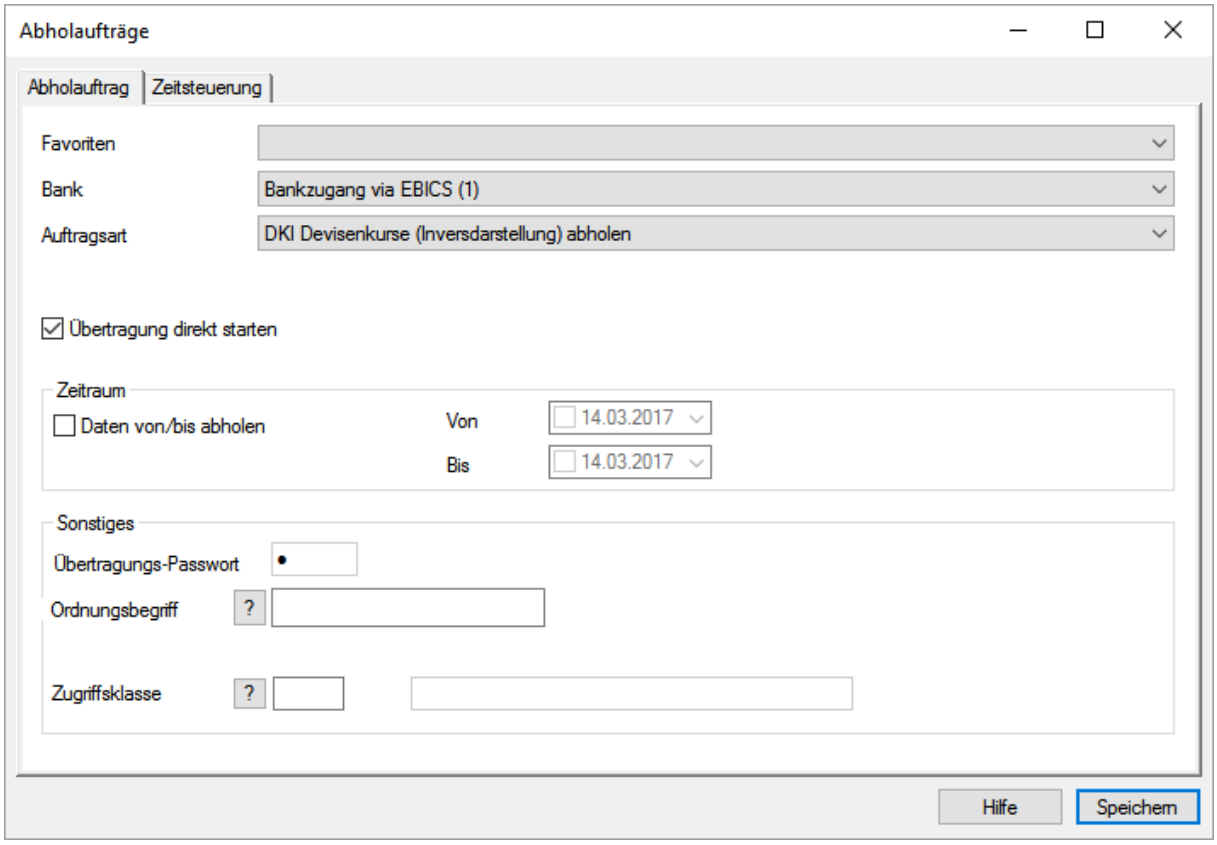
Anschließend pflegen Sie (wieder angemeldet als Systemadministrator) die benötigten **Devisenkurse**.

Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Systemadministrator (=Administratorrechte gesetzt)				
8	Pflege der Devisenkurse (optional)		Stammdaten/ Währungen	3.6

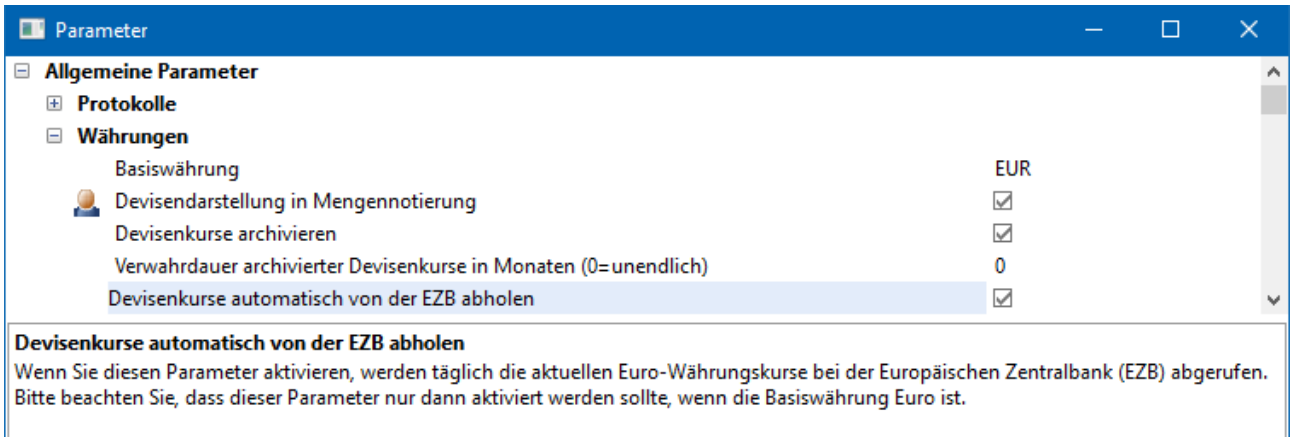
Die Pflege der Devisenkurse kann manuell erfolgen.



Die Devisenkursdaten können aber auch über einen DKI-(oder DKU-) Abholauftrag bei Ihrer Bank abgerufen werden (Kommunikationsmanager / Abholaufträge), sofern dies von Ihrer Bank unterstützt wird.

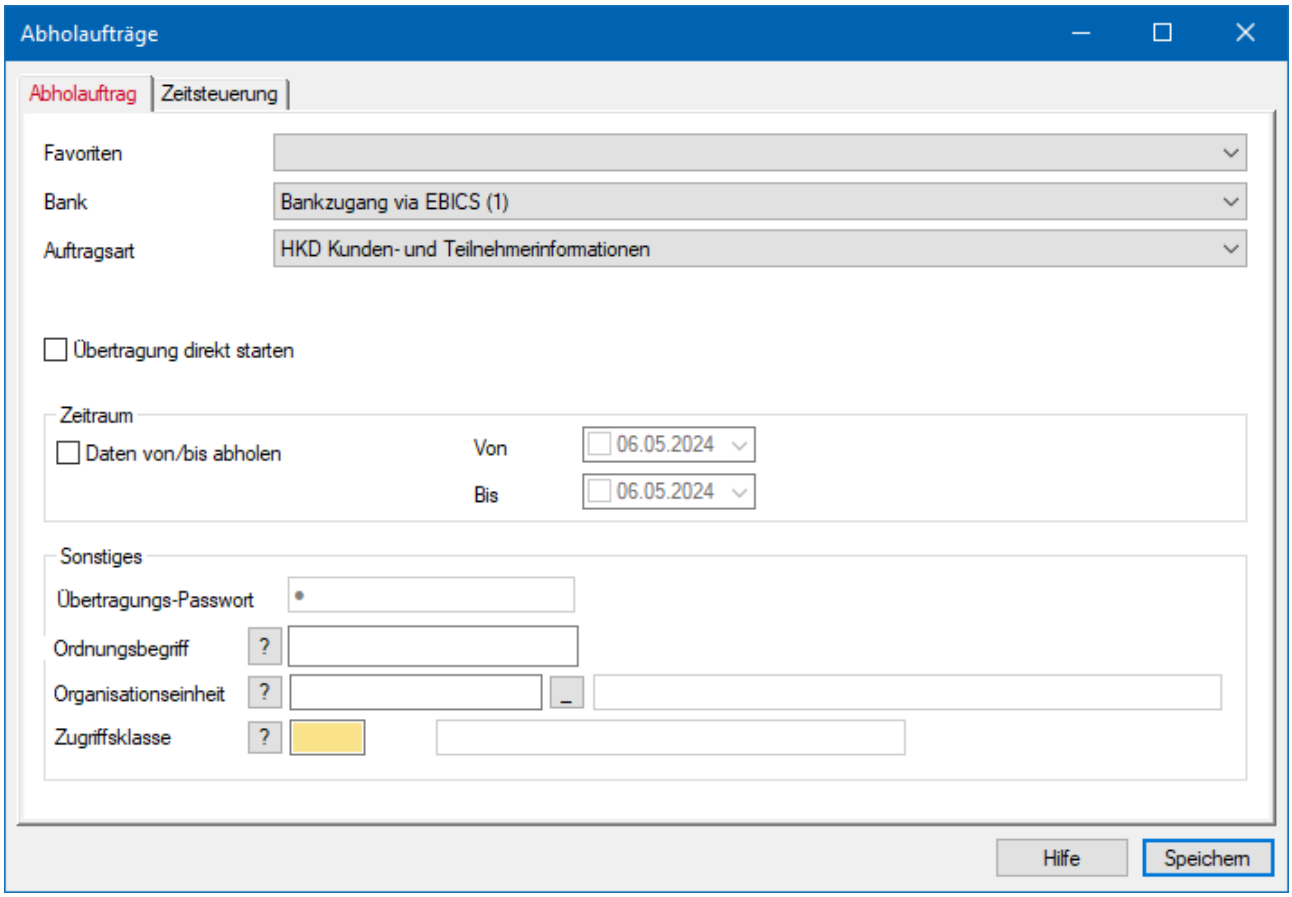


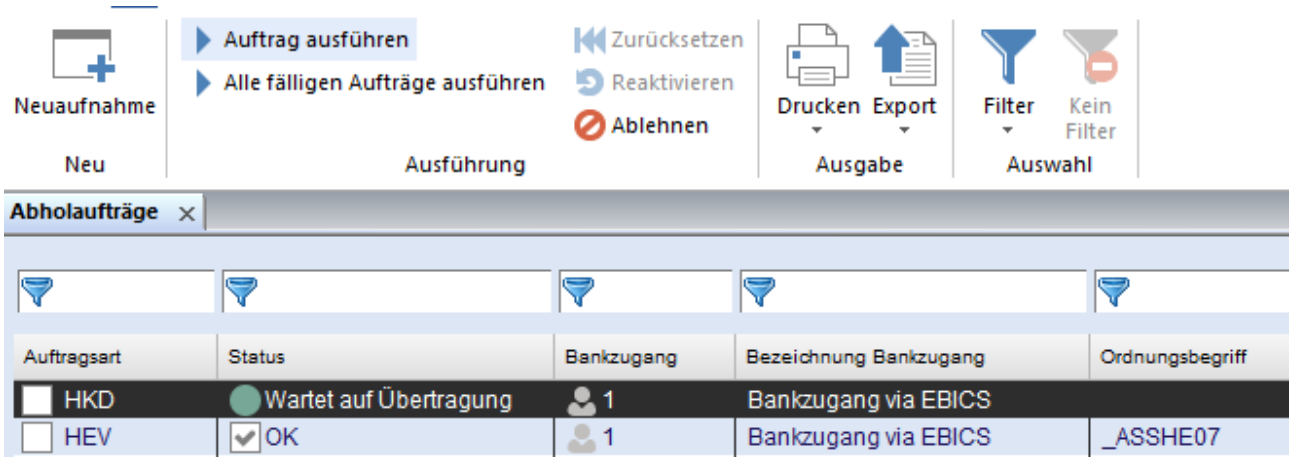
Die Abholung entsprechender Devisenkurse kann automatisch erfolgen, wenn folgender Parameter gesetzt wurde.



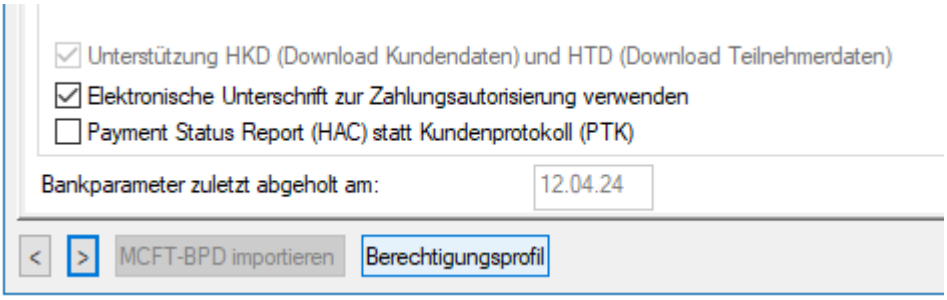
[optional] **Abrufen eines HKD** (=Kunden- und Teilnehmerinformationen) (Kommunikationsmanager / Abholaufträge).
Die Stammdaten der Banken und Konten werden dann automatisch angelegt und auch die Firma des Bankzugangs wird automatisch als Auftraggeber für die Banken übernommen.

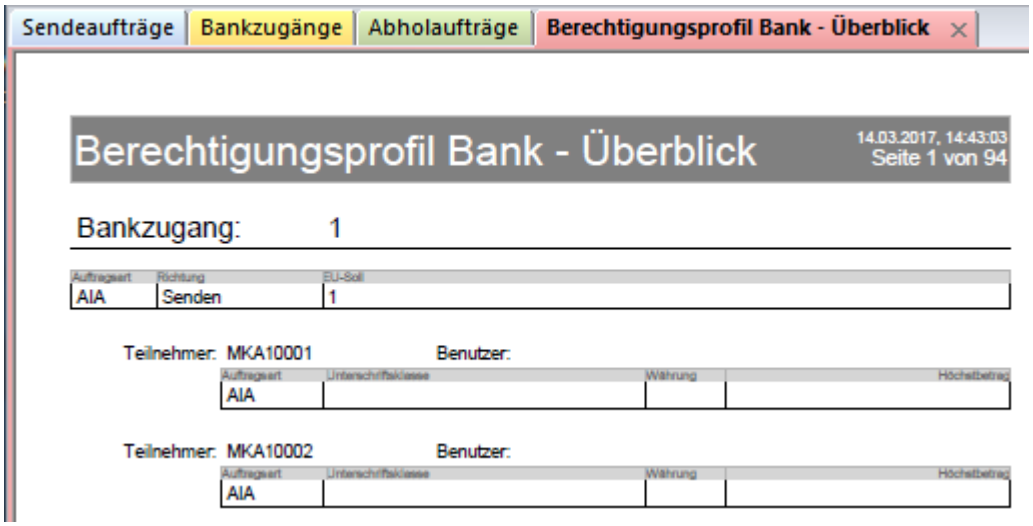
Richten Sie einen HKD-Abholauftrag (zur Abholung der Kunden- und Teilnehmerinformationen) ein und führen Sie den Auftrag aus.



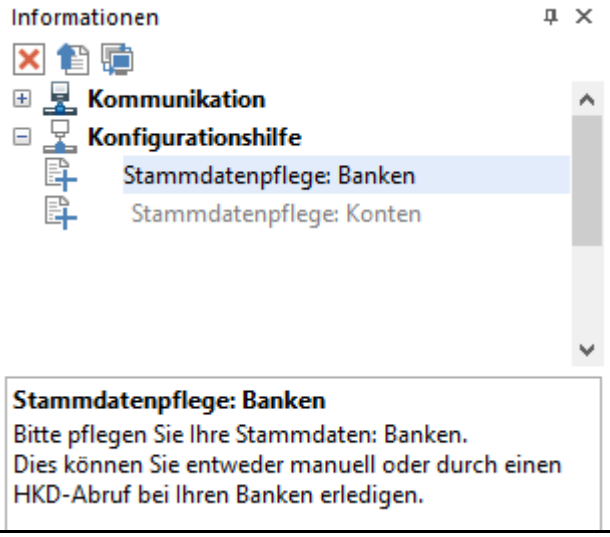


Die Berechtigungen bei der Bank können nun über entsprechende Schaltflächen abgerufen werden.

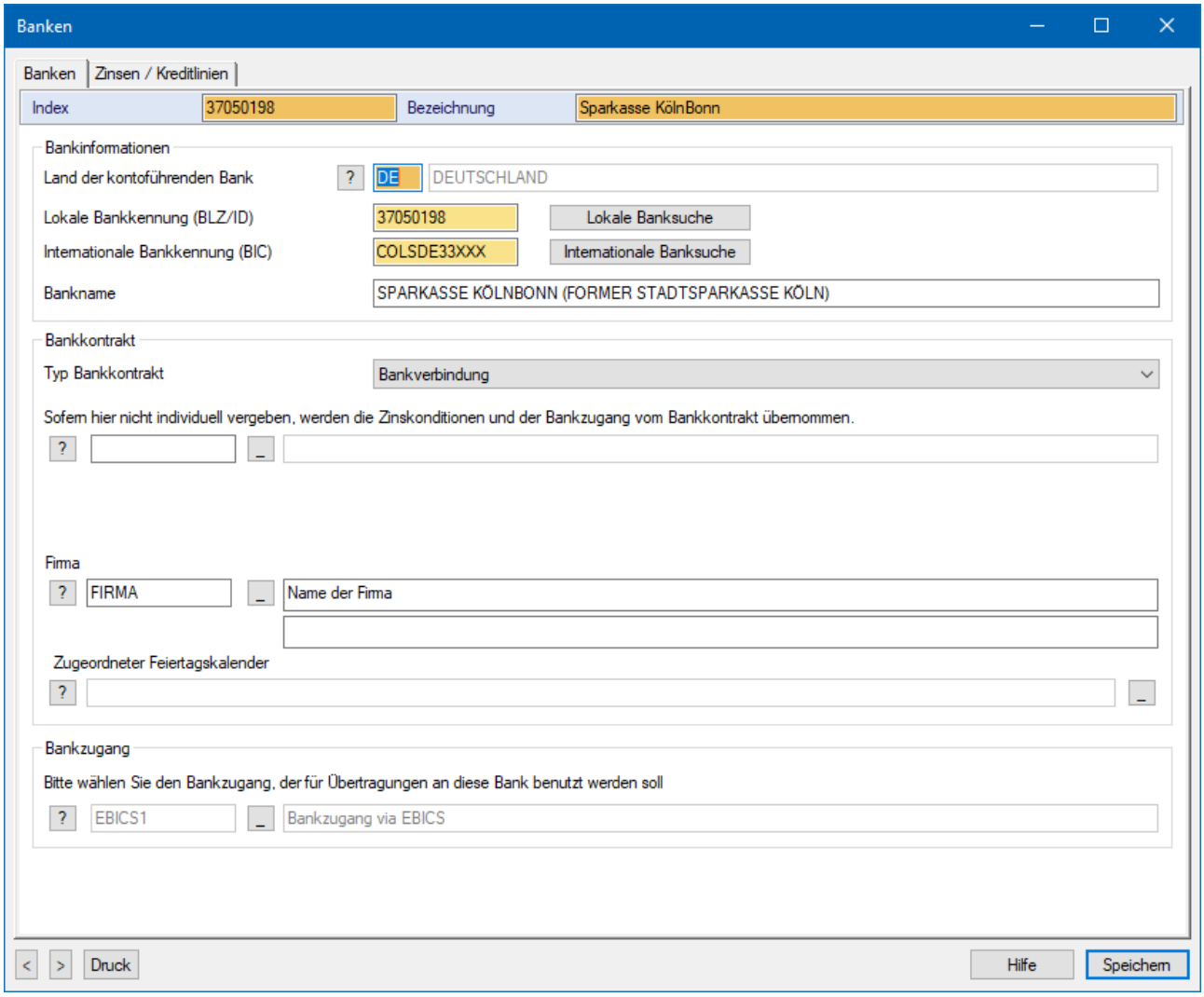




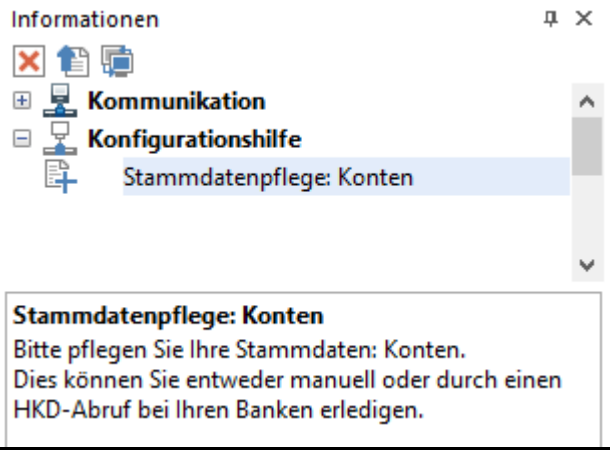
Statt per HKD-Abruf, können Sie die Stammdaten (**Banken** und Konten) auch manuell pflegen. Manchmal ist auch eine "Nachpflege" der per HKD abgeholten Daten notwendig.

Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Systemadministrator (=Administratorrechte gesetzt)				
9	Stammdaten-pflege: Banken (optional)		Stammdaten/ Banken	3.2

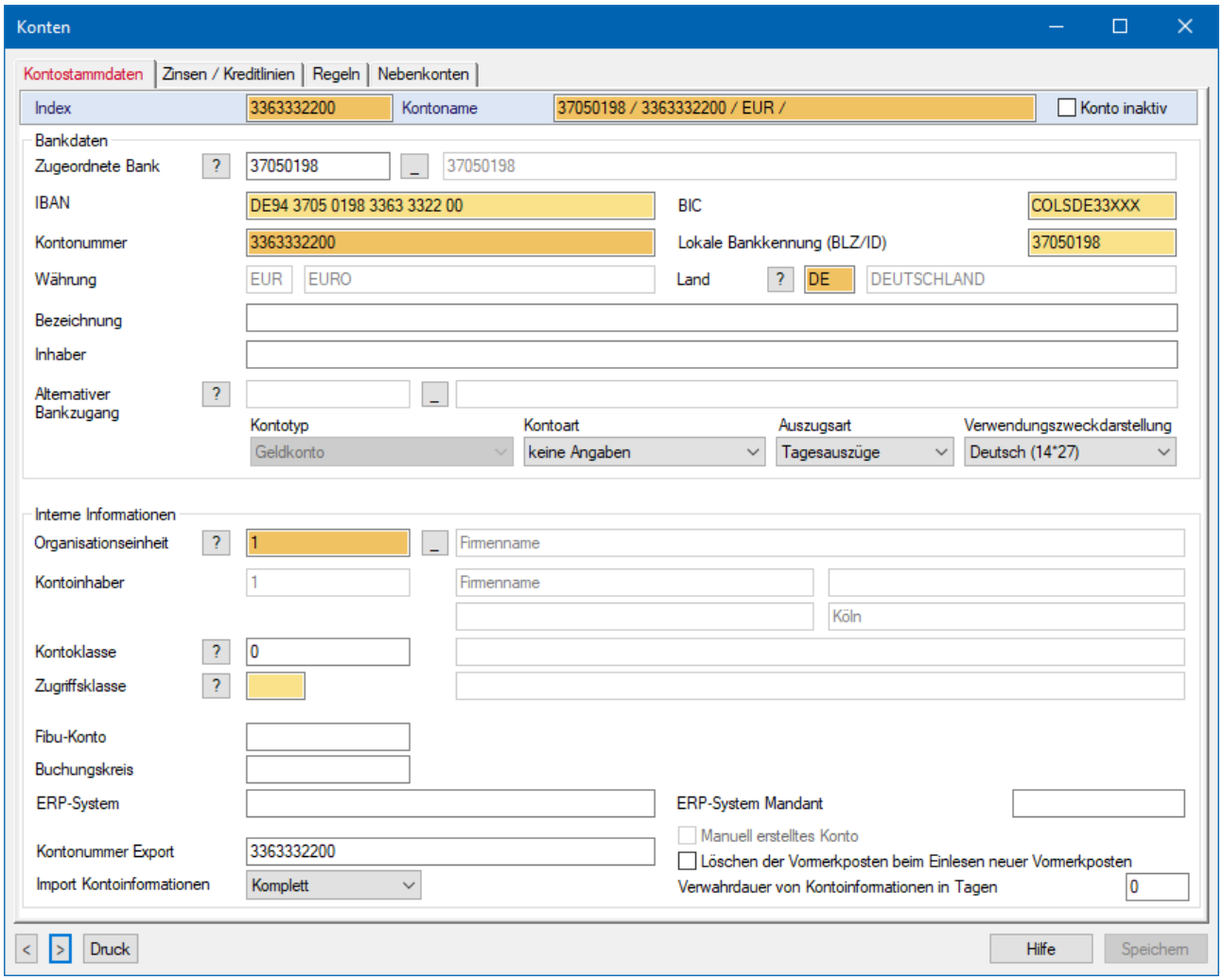
Prüfen und Nachpflegen fehlender Daten in den automatisch angelegten Stammdaten, insbesondere Zugriffsschlüssel (Feld Index), BIC, Länderkennzeichen.



Abschließend können noch die **Konten** (nach)bearbeitet werden.

Nr.	Funktion (geforderte Aktion)	Beschreibung (Funktion und angezeigter Text im Kommentarbereich des Informationen-Fensters)	Ziel-Dialog	Kapitel im Benutzer-handbuch
Anmeldung als Systemadministrator (=Administratorrechte gesetzt)				
10	Stammdaten-pflege: Konten (optional)		Stammdaten/ Konten	3.3

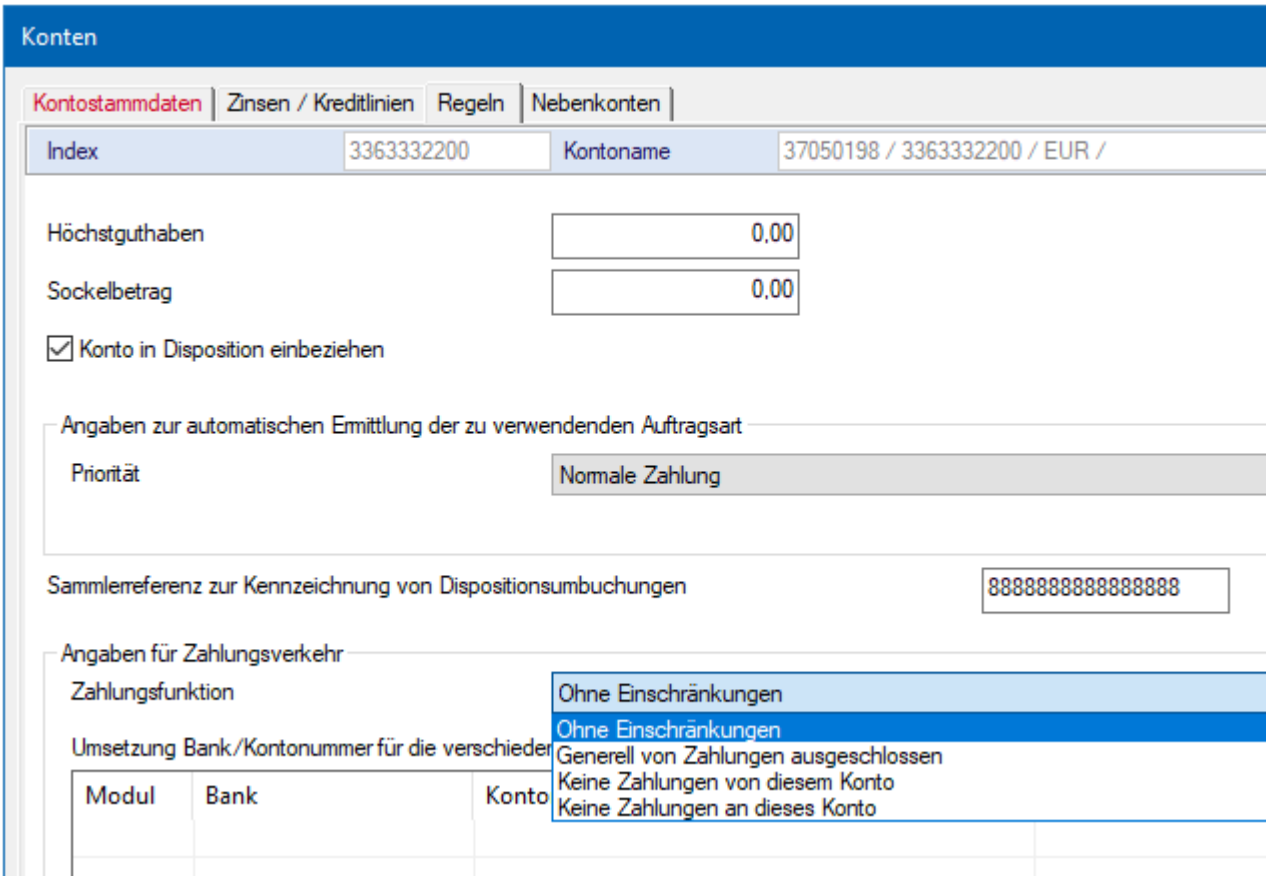
Prüfen und Nachpflegen fehlender Daten in den automatisch angelegten Stammdaten, insbesondere Zugriffsschlüssel (Feld Index), Kontoname, Länderkennzeichen, Kontonummer / ggf. abweichende Zahlungskontonummer (unter Regeln).



Die hier angelegten Konten stehen in den jeweiligen Zahlungsverkehrsmodulen nur zur Verfügung, wenn

a) die notwendigen Kriterien gefüllt sind (z. B. Land, BIC etc.) und

b) für das Konto auf der Registerkarte "**Regeln**" bei den "Angaben für Zahlungsverkehr" "**Ohne Einschränkungen**" (Standardeinstellung) konfiguriert wurde.



Danach ist die Konfigurationshilfe vollständig "abgearbeitet".



Die eingerichteten Benutzer können jetzt nach entsprechender Anmeldung mit dem System arbeiten.

© 2024 Omikron Systemhaus GmbH & Co. KG

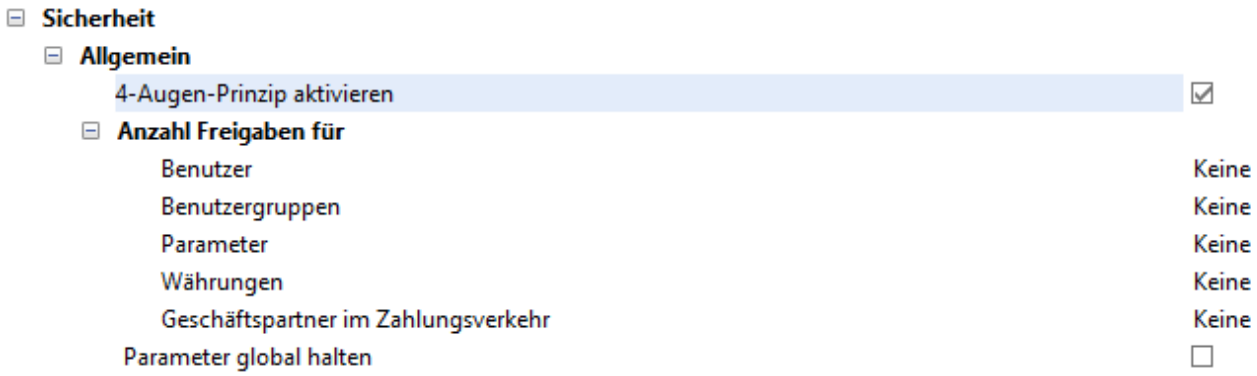
2 Anhang: Empfohlene Sicherheits-Einstellungen

MultiCash ist eine sehr flexible Anwendung, die durch eine Vielzahl von Parameter-Einstellungen an die Bedürfnisse des jeweiligen Kundenkontexts angepasst werden kann. Hierzu zählen auch diverse sicherheitsrelevante Parameter. Im Folgenden werden Empfehlungen für den sicheren Einsatz beschrieben. Die Evaluierung und Umsetzung (ggf. mit Abweichungen) obliegt dem jeweiligen Administratoren-Team des Kunden.

2.1 Systemparameter: Sicherheit

2.1.1 Allgemein

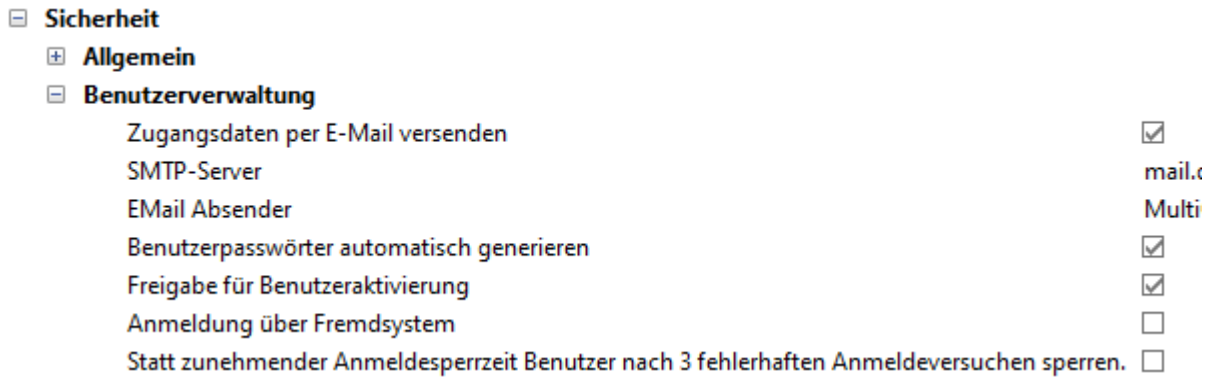
Wir empfehlen für die Pflege von Benutzerstammdaten und Parametern das generelle 4-Augen-Prinzip zu aktivieren. So ist sichergestellt, dass immer mindestens zwei Personen benötigt werden, um (ggf. sicherheitsrelevante) Einstellungen zu verändern.



2.1.2 Benutzerverwaltung

Sofern lokale Passwörter zur Anmeldung am System verwendet werden (also die Anmeldung nicht “über ein Fremdsystem” (LDAP) erfolgt, empfehlen wir:

1. Die Zugangsdaten automatisiert per Email an die Benutzer zu versenden.
2. Die automatische Generierung (sicherer) Initialpasswörter durch die Applikation.
3. Den Einsatz einer Freigabe für die Benutzeraktivierung, sodass ein Administrator einen Benutzer nach seiner initialen Anmeldung und dem damit verbundenen Passwortwechsel noch einmal freischaltet, bevor der Benutzer die Anwendung verwenden kann.



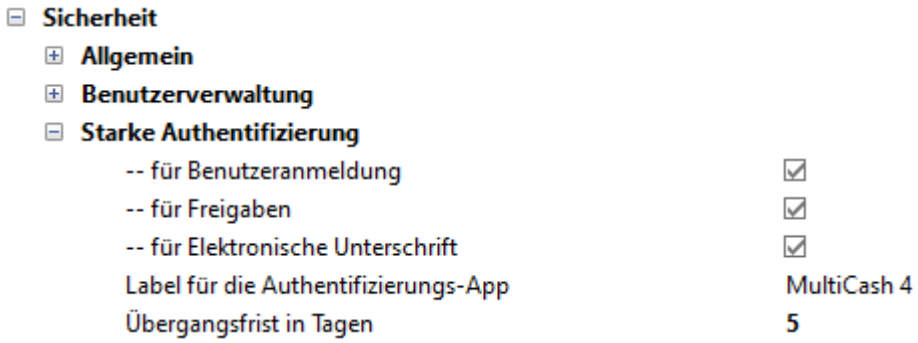
2.1.3 Starke Authentifizierung

Sofern das Zusatzmodul „Starke Authentifizierung“ lizenziert wurde (Empfehlung), so sollte diese für

1. Benutzeranmeldung
2. Zahlungsfreigaben
3. Elektronische Unterschriften

aktiviert werden.

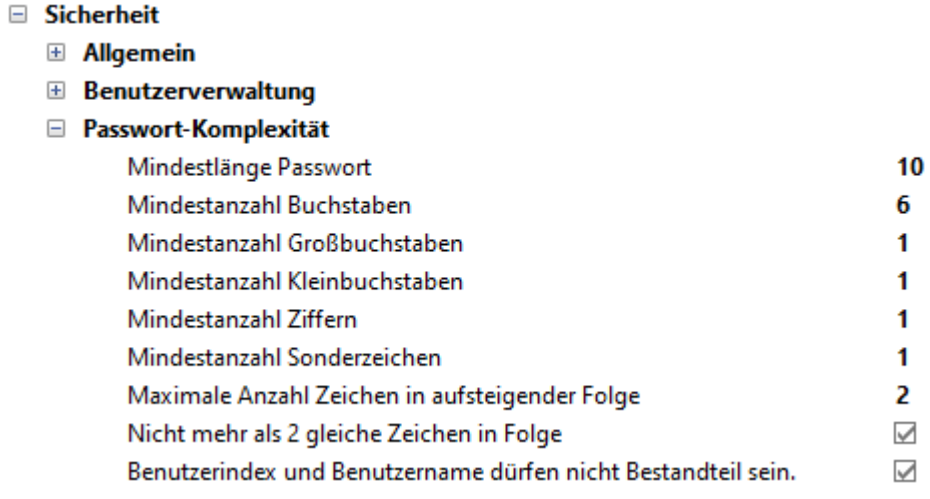
→Dadurch wird für die o.g. Vorgänge ein Zwei-Faktor-Verfahren (mittels Authenticator-App) obligatorisch.



2.1.4 Passwort-Komplexität

Sofern lokale Passwörter zur Anmeldung am System verwendet werden (also die Anmeldung nicht “über ein Fremdsystem” (LDAP) erfolgt, empfehlen wir die folgenden Mindestanforderungen für die Komplexität von Passwörtern einzurichten:

1. Mindestlänge des Passwortes: 10
2. Mindestanzahl von Buchstaben: 6
3. Mindestanzahl von Großbuchstaben: 1
4. Mindestanzahl von Kleinbuchstaben: 1
5. Mindestanzahl von Ziffern: 1
6. Mindestanzahl von Sonderzeichen: 1
7. Maximale Anzahl von Zeichen in aufsteigender Folge: 2
8. Nicht mehr als 2 gleiche Zeichen in Folge: Ja
9. Benutzerindex und Benutzername dürfen nicht Bestandteil sein: Ja



2.1.5 Passwort-Regeln

Zusätzlich zu den Komplexitäts-Kriterien, empfehlen wir die Anwendung der nachfolgenden Passwort-Regeln, um die Sicherheit zusätzlich zu erhöhen:

1. Passwortgültigkeit in Tagen: max. 90 Tage
2. Zeitraum bis zur Deaktivierung inaktiver Benutzer in Tagen: max. 30 Tage
3. Passwortänderung nur einmal täglich zulassen: Ja
4. Passwortwechsel erzwingen: Ja
5. Passwörter gegen Blacklist prüfen: Nicht zwingend erforderlich
6. Passwort-Historie pflegen (die letzten 10 Passwörter können nicht wieder verwendet werden): Ja
7. Letzten Zugriff beim Login anzeigen: Ja

