NUTZEN SIE DIE DYNAMIK.

Microsoft Dynamics Lösung für das Immobilienmanagement.

Seminar
RELion Administration

mse
Immobiliensoftware GmbH

RELion®

Microsoft Dynamics

Inhaltsverzeichnis

1 RELion Datenbanken und Mandanten

1.1 Datenbank

Alle Daten und auch die Anwendungsprogramme werden bei RELion jeweils in einer einzigen Datenbank im MS SQL Server gespeichert.

In der Regel werden von mse auf dem Kundensystem zwei Datenbanken installiert:

Für die Echtmandanten die Datenbank „FirmaName_RELion“.
Für Test- und Schulungszwecke die Datenbank „RELion_Schulung“ mit den Demo-Mandanten.

Jede der Datenbanken enthält eigenständige Tabellen und den kompletten Programmcode der Anwendung. Änderungen an Programmobjekten und Daten in einer Datenbank wirken sich also nicht auf die andere Datenbank aus. Daher kann auch ohne Weiteres eine gesonderte Datenbank (TEST...) für Testzwecke erstellt werden. Beachten Sie, dass jede Änderung an einem Objekt immer für alle Mandaten einer Datenbank wirksam wird.

1.2 Mandant

In RELion können quasi beliebig viele Mandanten eingerichtet werden. Die Anzahl der Mandanten ist nur durch die Performance des Systems und den Plattenplatz begrenzt.

Ein Mandant ist in der Regel eine rechtlich selbständige Gesellschaft oder einfach ein Buchungskreis für die Fremdverwaltung. Innerhalb eines Mandanten können bei der Fremdverwaltung beliebig viele Zinshäuser und WEG’s von beliebig vielen Eigentümern zusammen verwaltet werden. Innerhalb eines Mandanten können nur Objekte mit Sollversteuerung (Bilanzierung) oder nur mit unrealisierter MwSt (Ist-Versteuerung USt) verwaltet werden. Soll bei der Fremd- oder WEG-Verwaltung neben der Objektbuchhaltung der fremden Objekte auch die der Verwaltungsgesellschaft in RELion erfolgen, so sollen dafür zwei getrennte Mandanten geführt werden, um eigenes und fremdes Vermögen voneinander klar zu trennen.

Alle Verarbeitungsroutinen beziehen sich immer auf einen Mandanten, das trifft auch auf Reports zu. Für Konsolidierungszwecke und Konzernbilanzen kann aber ein Konzernmandant angelegt werden, der die Umsätze der Sachkonten seiner Konzerngesellschaften aufnimmt.
Tipp: Verwenden zur Vorbereitung der Konsolidierung in allen Mandanten die Dimension MANDANT.

Um sich die Anlage neuer Mandanten zu vereinfachen, empfiehlt es sich, in der Echt-DB auch einen Mandanten „_Vorlage“ als Kopiervorlage für die neuen Mandanten zu führen. Alle zukünftigen Änderungen an der Grundeinrichtung und Kontenplänen müssen dann aber immer auch im Vorlagemandanten erfolgen

1.3 Globale Daten

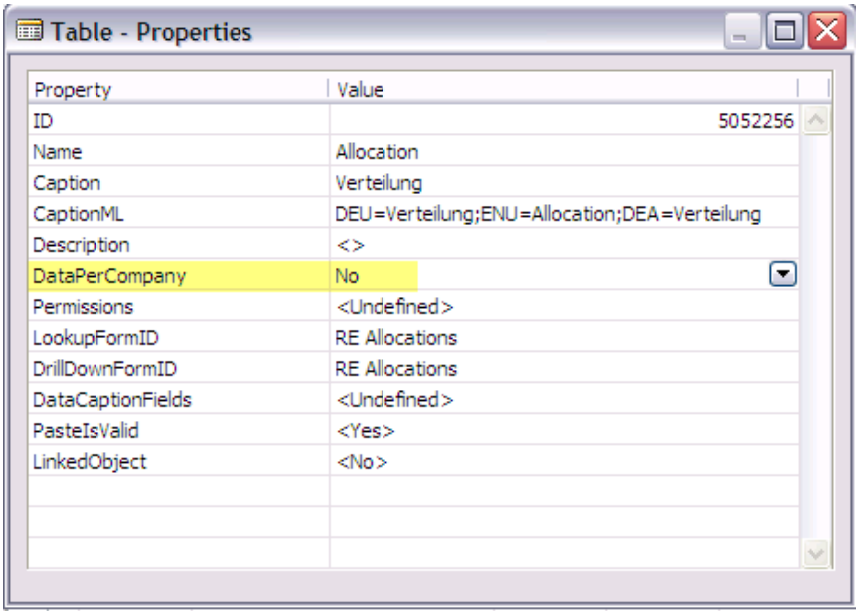
In RELion werden die meisten Daten standardmäßig je Mandant verwaltet.
Mit RELion R4.3. SP5 bzw. R.5.0 wurden ca. 50 Tabellen global gestellt, um die Verwaltung grundlegender Einrichtungen bei mehreren Mandaten zu vereinfachen.

Die globalen Tabellen sind unter anderem:

BLZ
PLZ
Anrede
Anredeformel
Zahlungsbedingungen
Lieferbedingungen
Liefermethoden
Zahlungsform
Mahnmethode
Mahnstufe
Mahntext
Service Zone
Kündigungs. -Leerstandsgrund
Produktbuchungsgruppe
Geschäftsbuchungsgruppe
MwSt.-Geschäftsbuchungsgrp.
MwSt.-Produktbuchungsgrp
IM Konto
Abrechnungsart
Einzelwertber. Miete
Mängel - Schaden
Ausstattung Schaden Leistung
IM Branche
Verteilung

Fläche für Einheit
Raum & Fläche
Lage / Stockwerk
IM Tabelle Überschrift
Beschreibung Zahlungsdatei
Nutzungsart
Mietspiegel Code
Mietspiegel
Index Code
Indexverwaltung
Geschäftsbeziehungsklasse
IM Bearbeiter Rolle
IM Bearbeiter Rollen Tab
IM Vorlage Einr. Word
IM Anhang Word
IM Vorlage Word
IM Vorl. Sprache Word
Word Vorlage Tabelle
Word Vorlage Feld
Word Vorlage Tab. Filter
Word Vorl Laufzeitfilter
Darlehen Variabler Zins
Darlehen Var. Zinszeilen
Ausstattung u. Schlüssel

Im Object Designer wird diese Eigenschaft zur Tabelle verwaltet:



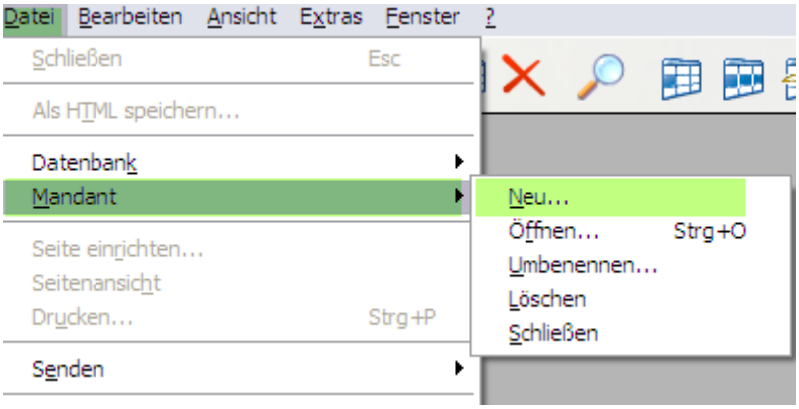
1.4 Neuen Mandanten anlegen / Mandant kopieren

Sie können einen neuen Mandanten erstellen, in dem Sie dafür einen neuen leeren Mandanten anlegen und anschließend gegebenenfalls die Daten aus einem anderen Mandanten kopieren.

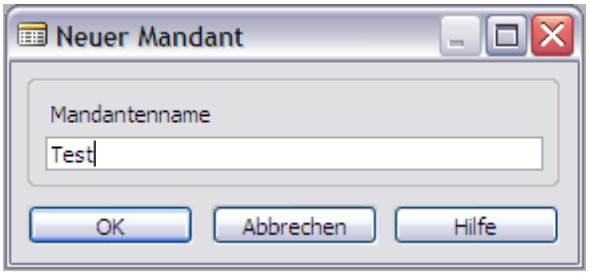
1.4.1 Leeren Mandanten anlegen

Das Anlegen eines neuen Mandanten dauert in der Regel nur einige Sekunden. Ein solcher neuer Mandant enthält keinerlei Daten. Die für die Grundeinrichtung benötigten Daten können aber per „copy and paste“ aus einem anderen Mandanten übertragen werden. Sie öffnen dafür RELion zweimal, öffnen in den beiden Anwendungen den neuen Mandanten und den, von dem sie kopieren wollen. Als nächstes rufen Sie nacheinander die einzelnen Einrichtungsfunktionen auf und kopieren die Daten von dem einen Mandaten in den anderen.

Mandant erstellen:



Im nächsten Fenster geben Sie den Namen des neuen Mandanten (hier Test) ein:



Bestätigen Sie mit OK.

In einer Statusanzeige wird dann der Vorgang angezeigt. Der Prozess ist nach Erstellung aller Tabellen abgeschlossen. Sie können den Mandanten sofort benutzen.

Bitte sprechen Sie gegebenenfalls mit unserem Consulting, damit wir Sie bei der Grundeinrichtung unterstützen können.

1.4.2 Daten kopieren

Zum Kopieren von Daten nutzen Sie die Einrichtungscheckliste (Modul Verwaltung) oder kopieren die Daten per „copy and paste“, indem Sie RELion zweimal starten.

2 Object Designer

Der Object Designer kann bei entsprechender Berechtigung per Menü oder per Shift + F12 aufgerufen werden. „Normale“ Anwender können diese Funktion nicht aufrufen. Achten Sie bei der Einrichtung Ihrer Zugriffsrechte darauf, dieses Zugriffsrecht entsprechend zu vergeben.

Im Object Designer können prinzipiell alle Daten und Programmobjekte der RELion-Anwendung und des Basis- Systems MS Dynamics NAV bearbeitet werden.
Die Möglichkeiten sind dabei von der erworbenen Entwicklungsumgebung abhängig.

Die im Rahmen eines Updates ausgelieferten FOB-Dateien werden hier importiert.

Beachten Sie, dass der Import von neuen Programmobjekten im ObjectDesigner (s.u.) immer für alle Mandanten wirksam ist, egal in welchem Mandanten Sie den Object Designer geöffnet haben!

Bei entsprechender Lizenzierung steht eine umfassende Programmentwicklungsumgebung zur Verfügung. Der Anwender kann aber aus Sicherheitsgründen nur bestimmte Objekte verändern oder neu erstellen, so dass der Systemkern und Datenbanktabellen von RELion nicht verändert werden können.

Endkunden können aus Sicherheitsgründen nur das Design der Tabellen im Bereich 50.000 bis 50.999 ändern und auch nur dort eigene Tabelle anlegen. Alle anderen Bereiche können nur durch Microsoft selber und die Microsoft Partner (z.B. mse) bearbeitet werden.

Für Forms und Reports gilt diese Einschränkung nicht. Der Kunde muss aber berücksichtigen, dass jedes Update, welches das geänderte Objekt betrifft, diese Änderungen wieder überschreiben wird.

Es gibt folgende Objektarten

Objektart	Bedeutung	Funktion
Table	Tabelle	Alle Daten von RELion sind in Tabellen gespeichert. Die Daten können hier direkt bearbeitet werden. Achtung: Da es hier keine Eingabemasken gibt, werden die Daten hier in vielen Fällen ohne weitere Prüfung verarbeitet.
Form	Bildschirmmaske	Beschreibt die Eingabe-/Anzeigemaske
Report	Report	Auswertung der Daten als Liste zum Drucken oder als Excel-Tabelle. Es gibt auch spezielle Reports (s.g. Stapel), die Daten korrigieren.
Dataport	Daten Import/Export	Daten werden gelesen, aufbereitet, für andere Anwendungen aufbereitet (z.B. HK-DTA L/M-Satz) und als Datei exportiert.
XML-Port	Daten Import/Export per XML	Wie beim Dataport, die Daten werden aber im XML-Format verarbeitet.
Codeunit	Programm	Codeunits stellen spezielle Funktionen zentral für alle Objekte des RELion-Systems zur Verfügung. Beispielsweise die Berechnung einer Miete für einen Stichtag.
MenuSuite	Menü	Programm für die Darstellung der Menüs

3 Neue Programmversionen testen und Testumgebung erstellen

Beachten Sie, dass der Import von neuen Programmobjekten und Änderungen an Programmobjekten im ObjectDesigner (s.u.) immer für alle Mandanten innerhalb der Datenbank wirksam ist.

Bezüglich der genauen Arbeitsschritte im MS SQL Server konsultieren bitte zusätzlich auch die Online-Hilfe und die einschlägige Literatur.

Wenn Sie neue Programmversionen ohne Beeinträchtigung Ihres Echtsystems testen wollen, erstellen Sie eine Kopie der kompletten Echt-Datenbank. In diese Test-Datenbank importieren Sie dann die neuen Objekte.

Eine Datenbank können Sie (bzw. Ihr Administrator) direkt im MS SQL Server sichern und dann unter einem anderen Namen wiederherstellen. Vergeben Sie als neuen DB-Namen unbedingt einen Namen der mit TEST... anfängt. Damit vermeiden Sie Verwechselungen mit der Echt-DB und außerdem wird beim Öffnen ein entsprechender Warnhinweis angezeigt. Beim Kopieren der Datenbank werden alle Tabellen, also auch die Anwender-Anmeldungen mit Ihren Rollen und Zugriffsrechten übertragen.

Falls nicht alle Anwender mit der Test-Datenbank arbeiten dürfen, entfernen Sie diese Anwender aus den Anmeldungen (Extras > Zugriffsrechte > Datenbank/Windows Anmeldungen)

Nach der Wiederherstellung der neuen Datenbank, müssen die Zugriffsrechte dieser Datenbank dann noch einmalig mit dem MS SQL Server synchronisiert werden.

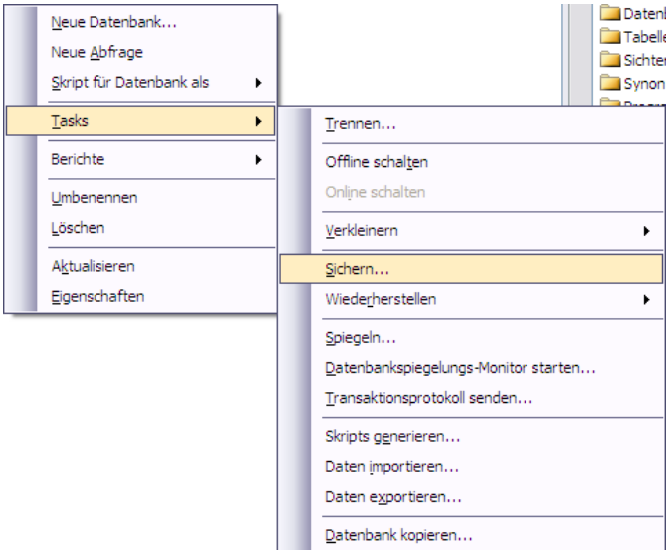
Anschließend kann jeder berechtigte Anwender sofort mit der neuen Test-Datenbank arbeiten, indem er die neue DB unter „Datei > Datenbank > Öffnen“ auswählt.

Die wichtigsten Schritte:

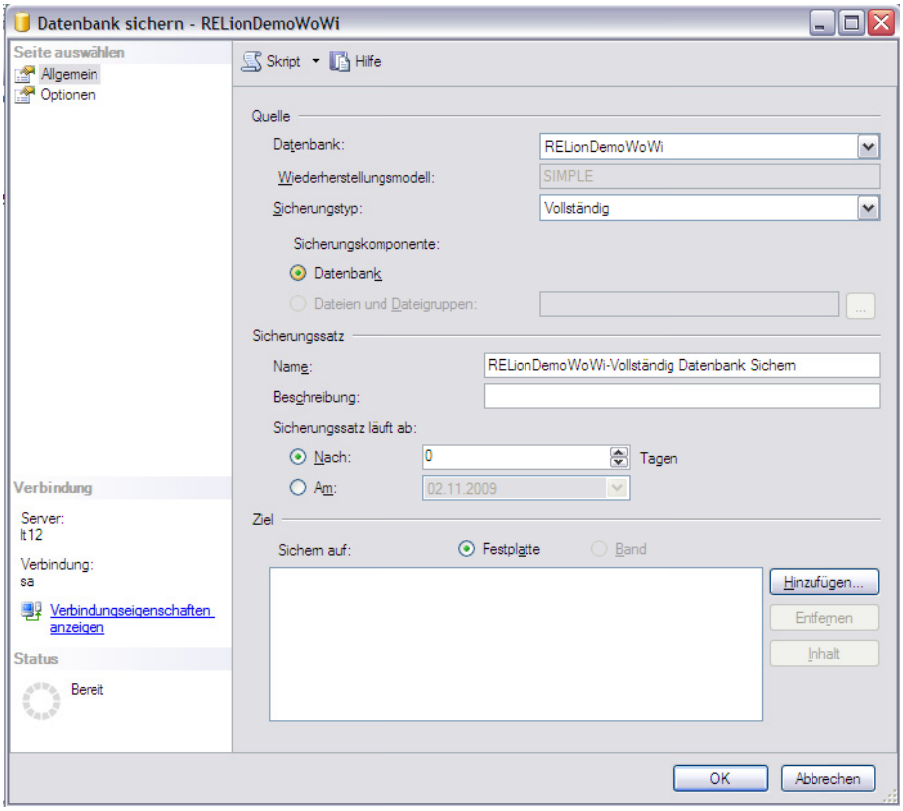
Sichern der Echt-Datenbank:

rechter Mausklick auf die zu sichernde Datenbank

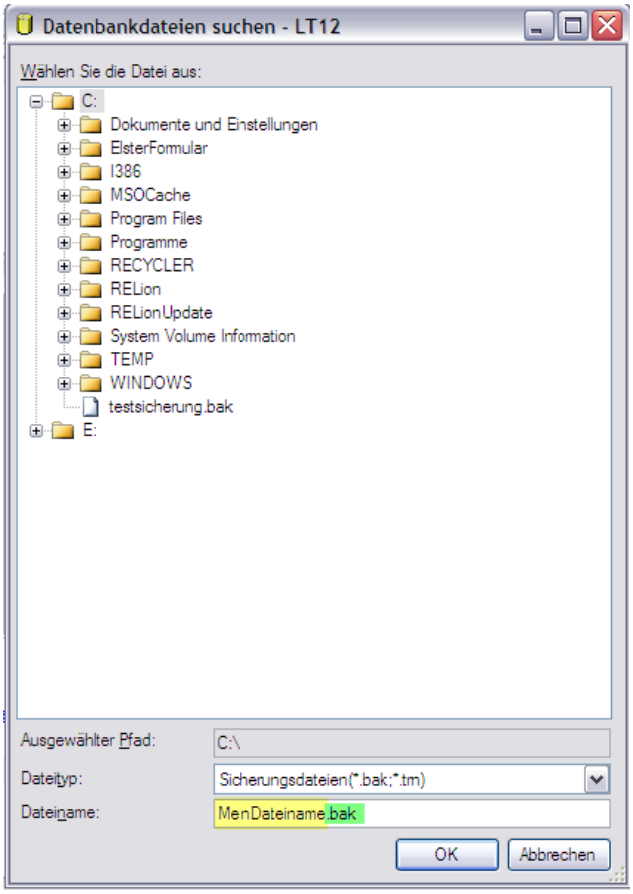
Auswählen Task > Sichern



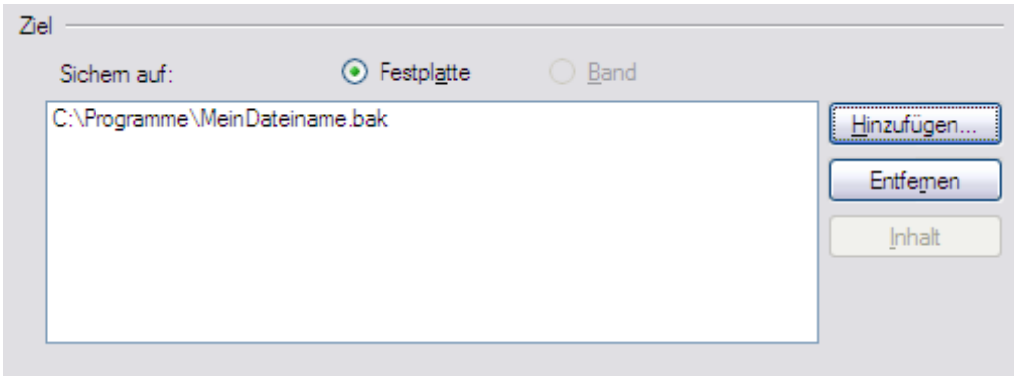
Wählen Sie als Ziel „Festplatte“.
Per Button „Hinzufügen“ wählen Sie den Pfad für die Speicherung der Sicherungsdatei.



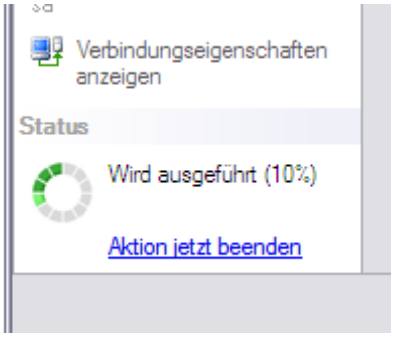
Geben Sie im nächsten Fenster den Pfad und einen Namen für die Sicherungsdatei an.
Die Dateiendung sollte .bak lauten.



Bestätigen Sie die Eingabe bis Pfad und Dateiname im vorherigen Fenster angezeigt werden:



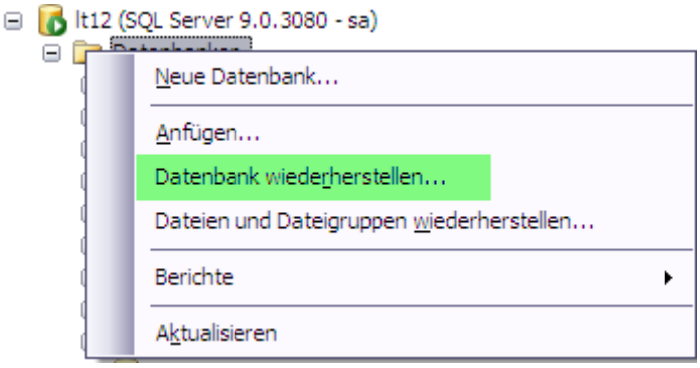
Bestätigen Sie mit OK, die Datenbank wird gesichert.
Eine Statusanzeige informiert sie über den Verlauf:



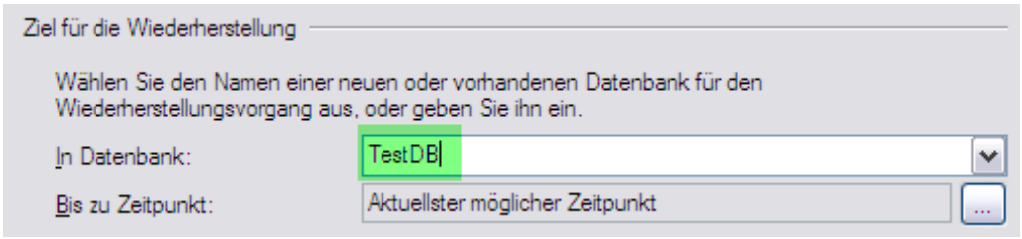
Erfolgsmeldung:

Wiederherstellen der Datenbank unter einem anderen Datenbanknamen:

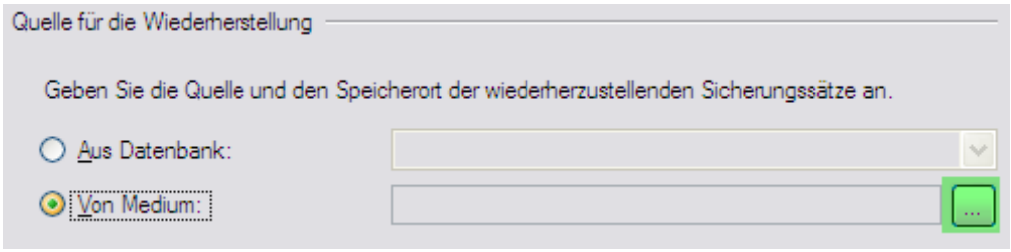
rechter Mausklick auf Datenbanken
Auswählen Task > Datenbank wiederherstellen



Geben Sie den neuen Datenbanknamen an:

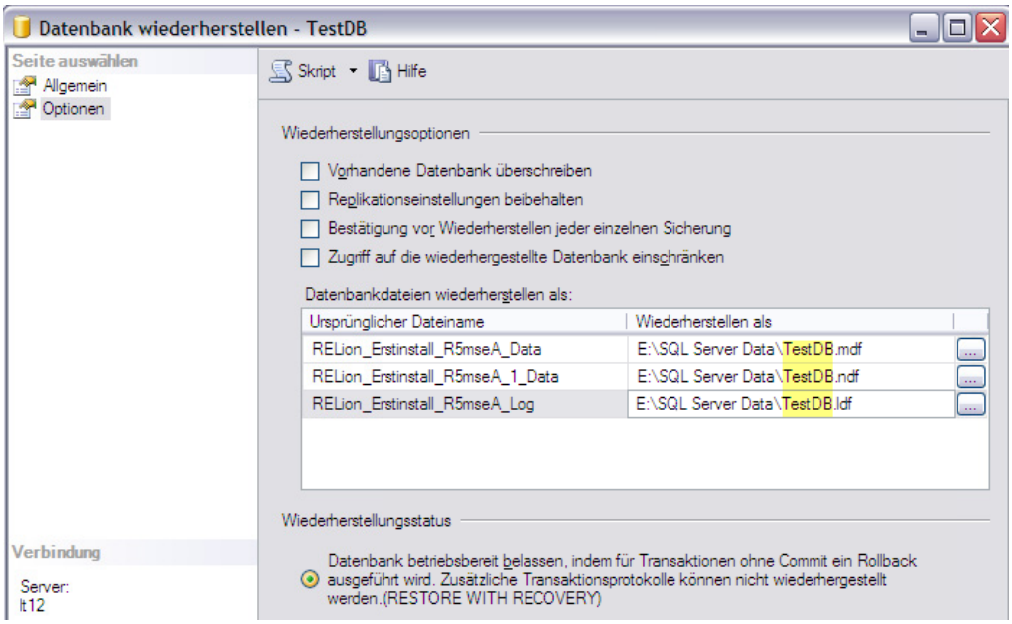


Wählen Sie unter „Quelle für die Wiederherstellung“ die Option „Von Medium“.



Suchen Sie Ihre Sicherungsdatei.

Wählen Sie das Register „Optionen“ und geben Sie den neuen Datenbankdateinamen (TEST...) an. Die drei Dateien haben die Dateiendungen .mdf und .ndf und .lfd.



4 Anwenderverwaltung

Für jeden Anwender, der mit RELion arbeiten soll, wird in MS Dynamics NAV eine Anmeldung angelegt.

Bei der Installation der RELion-Datenbank auf dem Kundensystem wird im SQL-Server die Authentifizierungsmethode Windows-Authentifizierung und SQL Server-Authentifizierung eingestellt.

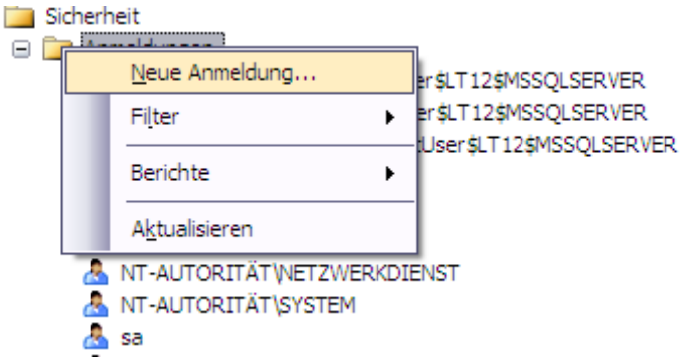
Für Datenbankanmeldungen müssen Sie den Anwender zuerst im SQL Server anlegen.

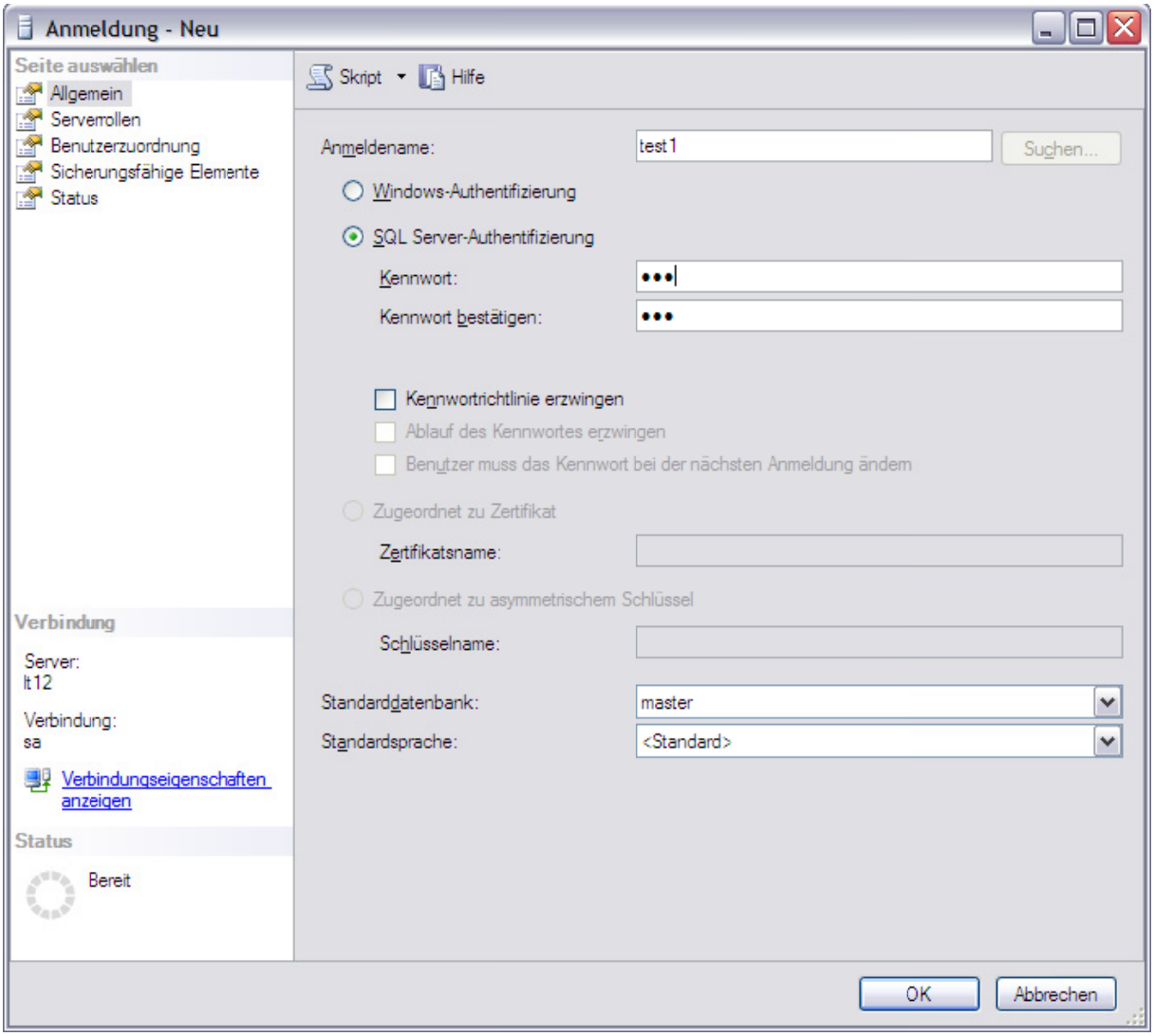
Für Windowsanmeldungen muss der Anwender zuerst im Active Directory angelegt werden.

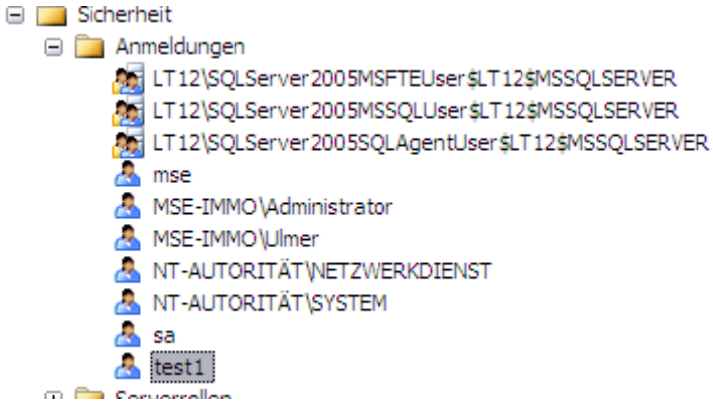
Bei der Erstinstallation erstellen wir bei Bedarf alle Anmeldungen des Kunden in RELion.

Für die Anwender des Kunden wird in der Regel die Windows-Authentifizierung genutzt. Bei diesem Verfahren reicht die Anmeldung unter Windows aus, um RELion zu starten; es ist also keine weitere Anmeldung in RELion notwendig. Was der Anwender dann darf, regeln die ihm zugeordneten Rollen in RELion.

Zusätzlich wird für die Arbeit vor Ort und für Wartungszwecke die Datenbank-Anmeldung „mse“ von uns erstellt.

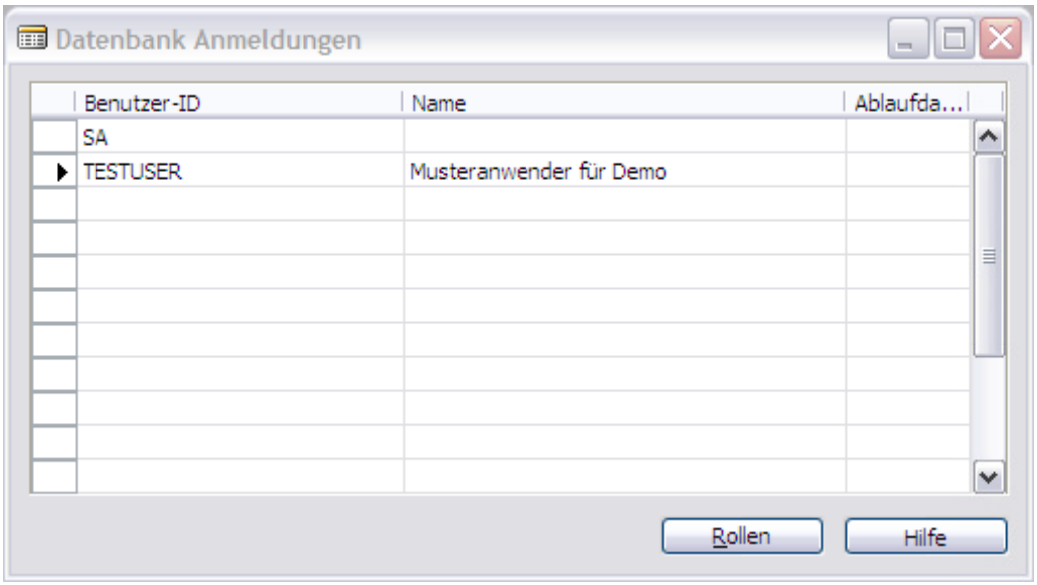

Sicherheit
Neue Anmeldung...
Filter
Berichte
Aktualisieren
er$LT12$MSSQLSERVER
er$LT12$MSSQLSERVER
User$LT12$MSSQLSERVER
NT-AUTORITÄT\NETZWERKDIENST
NT-AUTORITÄT\SYSTEM
sa


Anmeldung - Neu
Seite auswählen
Allgemein
Serverrollen
Benutzerzuordnung
Sicherungsfähige Elemente
Status
Skript
Hilfe
Anmeldename:
test1
Suchen...
Windows-Authentifizierung
SQL Server-Authentifizierung
Kennwort:
Kennwort bestätigen:
Kennwortrichtlinie erzwingen
Ablauf des Kennwortes erzwingen
Benutzer muss das Kennwort bei der nächsten Anmeldung ändern
Zugeordnet zu Zertifikat
Zertifikatsname:
Zugeordnet zu asymmetrischem Schlüssel
Schlüsselname:
Standarddatenbank:
master
Standardsprache:
<Standard>
Verbindung
Server:
lt12
Verbindung:
sa
Verbindungseigenschaften anzeigen
Status
Bereit
OK
Abbrechen



Sie rufen dafür in RELion folgende Funktionen auf:

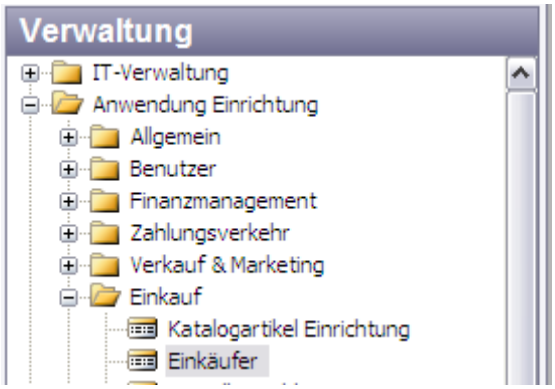
Extras > Zugriffsrechte > Datenbank Anmeldungen
bzw.
Extras > Zugriffsrechte > Windows Anmeldungen

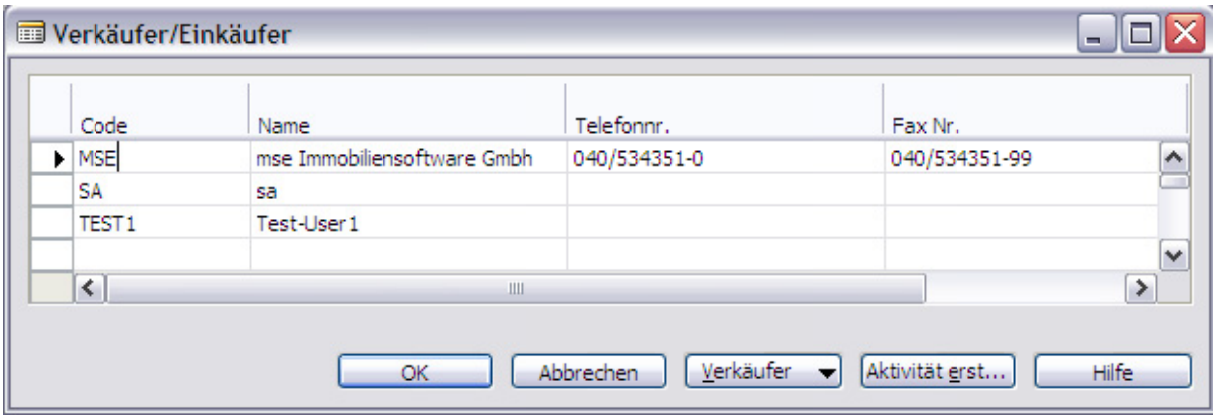


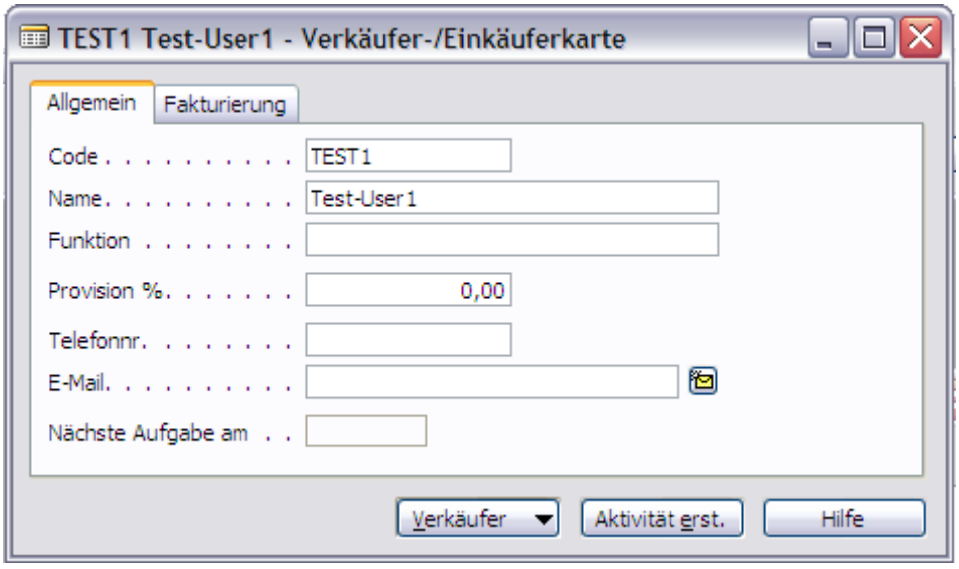
Als nächstes legen Sie den Anwender als Einkäufer/Verkäufer an und ordnen ihn in der Benutzereinrichtung zu. Als letztes wird der RELion-Bearbeiter angelegt.

Einkäufer/Verkäufer anlegen

Hier können auch die Kontaktdaten Telefon, Fax-Nr. und E-Mail hinterlegt werden.

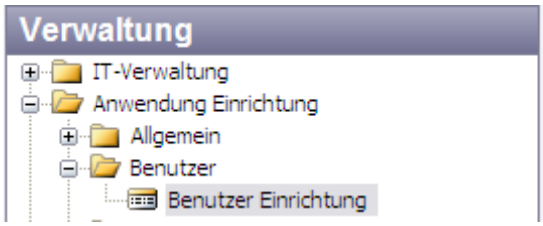




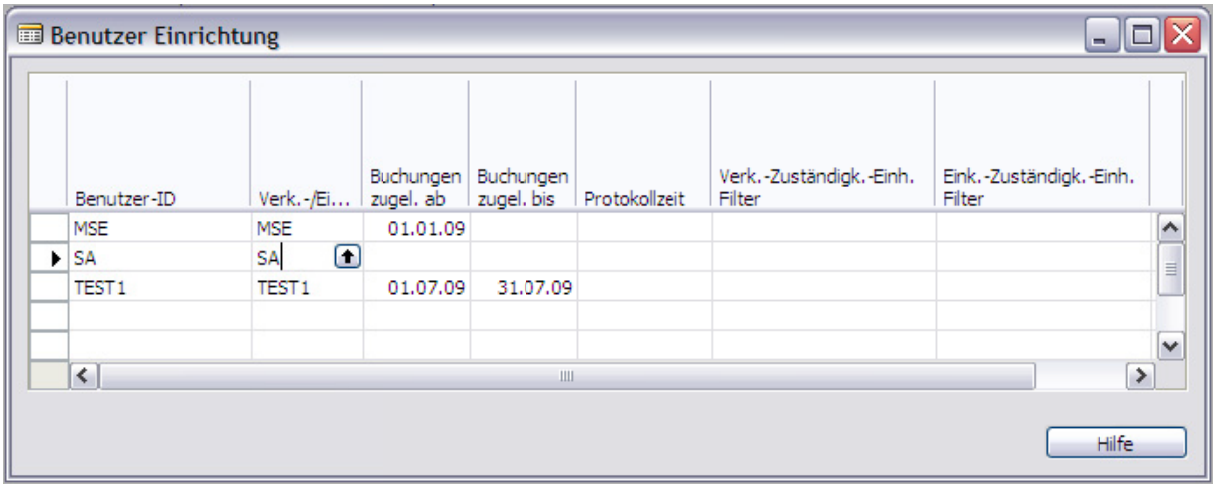


Als Basis für Freigaberegeln können Sie den Einkäufer/Verkäufer hier auch Teams zuordnen.

Benutzereinrichtung:



Hier können Sie bei Bedarf den zulässigen Buchungszeitraum des Anwenders einschränken.



Wenn Sie neue Anwender in RELion hinzugefügt haben, müssen Sie als letztes die gewünschten Rollen zuordnen und zuletzt die Zugriffsrechte synchronisieren.

Näheres dazu finden Sie im nächsten Kapitel.

5 Rollen und Zugriffsrechte

Ausführliche Erläuterungen zur Sicherheit finden Sie auch in der Online-Hilfe, wenn Sie beispielsweise nach den Begriffen Rollen, Sicherheit und Sicherheitsfilter suchen.

Sicherheit

Eine Enterprise Business Solution muss über ein integriertes Sicherheitssystem verfügen, das gewährleistet, dass nur autorisierte Personen Zugriff auf die jeweiligen Unternehmensdaten haben. Ein Mindestmaß an Sicherheit erfordert, dass den Benutzern Benutzer-IDs und Kennwörter zugewiesen werden und damit der Zugriff auf die Anwendung beschränkt wird. Microsoft Dynamics NAVerfüllt diese Anforderungen durch die Integration des eigenen Sicherheitssystems mit dem Active Directory-Sicherheitssystem von Windows und dem von Windows unterstützten Anmeldesystem.

Hiermit ermöglicht Ihnen Microsoft Dynamics NAV die vollständige Kontrolle darüber, welche Informationen für den Benutzer zugänglich sind. Sie können aus Microsoft Dynamics NAV heraus Benutzer erstellen, ihnen Rollen zuweisen und ihre Berechtigungen ändern. Zusätzlich können Sie in der SQL Server Option für Microsoft Dynamics NAV auch Sicherheitsfilter verwenden, um die Berechtigungen zu begrenzen, die Sie einem Benutzer oder einer Rolle gewähren. Damit ist die Möglichkeit gegeben, den Zugriff auf bestimmte Debitoren, Kreditoren, Dimensionen oder Ähnliches zu beschränken.

Um Benutzer in Microsoft Dynamics NAV zu erstellen, müssen Sie ihnen eine ID in der Datenbank zuweisen, die es ihnen erlaubt, sich am System anzumelden. Wenn sich die Benutzer an der Datenbank angemeldet haben, sind sie in der Lage, die Aufgaben, die ihren Berechtigungen entsprechen, durchzuführen.

Microsoft Dynamics NAV bietet Ihnen zwei unterschiedliche Methoden, sich anzumelden:

Datenbankanmeldungen
Windows Anmeldungen

Um die Datenbankanmeldung zu nutzen, muss Ihnen eine Datenbankanmeldung in Microsoft Dynamics NAV zugewiesen worden sein. Wenn Sie die Windows Anmeldung verwenden möchten, müssen Sie ein gültiges Benutzerkonto in der aktuellen Domäne haben und muss Ihnen eine Windows Anmeldung in Microsoft Dynamics NAV zugewiesen worden sein.

Alle Active Directory-Sicherheitsgruppen werden in Microsoft Dynamics NAV angezeigt. Es ist möglich, diesen Active Directory-Gruppen eine Windows Anmeldung und Rollen innerhalb von Microsoft Dynamics NAV zuzuweisen.

Das Microsoft Dynamics NAV-Sicherheitssystem ist mandantenspezifisch und enthält Informationen über die Zugriffsrechte, die jedem einzelnen Benutzer mit Zugriff auf die jeweiligen Mandanten gewährt werden. Dies schließt Informationen über die Rollen der Benutzer und deren zusätzliche Rechte ein, die Ihnen als individuelle Benutzer gewährt wurden. Wenn Sie festlegen, dass die Zugriffsrechte eines Benutzers nur in einem bestimmten Mandaten innerhalb der Datenbank gelten, dann wird der Benutzer nur auf diesen Mandanten zugreifen können.

In RELion werden die Zugriffsrechte je Anwender oder Anwendergruppe definiert. Definierte Zugriffsrechte werden dabei zuvor in Rollen zusammengefasst.

Der Kunde kann im System unbegrenzt viele Rollen für unterschiedliche Aufgaben anlegen.

Einem Anwender können Sie beliebig viele Rollen zuordnen.

RELion wird mit allen Standardrollen von Microsoft Dynamics NAV und zusätzlich einer Vielzahl von speziellen musterhaften RELion-Rollen ausgeliefert. Diese Rollen kann der Kunde nach Belieben verändern. Da die mit der Installation ausgelieferten Rollen nur als Muster verstanden werden können, sind die Rollen vom Kunden auf seine speziellen Anforderungen und seine Organisationsstruktur anzupassen.

mse unterstützt den Kunden dabei bei Bedarf.

Wichtige Hinweise zur Rolle SUPER:

Das Microsoft Dynamics NAV-Sicherheitssystem wird in dem Moment gestartet, wenn Sie das erste Datenbanklogin erstellen. Daher sollte das erste Login für einen Superbenutzer eingerichtet werden, dem die Rolle SUPER in Microsoft Dynamics NAV zugeteilt wird. Der Superbenutzer verfügt dann über alle Zugriffsrechte auf die Datenbank und verwaltet diese innerhalb von Navision. Bitte beachten Sie, dass sich die Design-Funktionalität in einem Produktionssystem für Mitglieder der Gruppe "Super" nicht sperren lässt. Bis Sie einen Superbenutzer erstellen, kann jeder Benutzer mit Zugang zu der Anwendung beliebige Transaktionen in der Microsoft Dynamics NAV-Datenbank durchführen.

Einer der ersten Vorgänge, die der Superbenutzer dann durchführt, sollte die Einrichtung von Benutzer-IDs und deren Rollen für die anderen Benutzer der Datenbank sein.

Da zum Zeitpunkt der Erstinstallation das Rollenkonzept meistens noch nicht erarbeitet und implementiert ist, erhalten alle Anwender häufig zuerst die Rolle SUPER, mit der alle Daten bearbeitet und alle Funktionen verwendet werden können. Diese uneingeschränkte Berechtigungsvergabe kann in der Projektphase sinnvoll sein, damit die Anwender während dieser Zeit alle Daten ohne Einschränkung prüfen und auch korrigieren können. Dabei ist natürlich zu bedenken, dass in dieser Zeit jeder Anwender auch alle Einrichtungsparameter verändern kann.

Wir empfehlen aus Sicherheitsgründen dringend, die Berechtigungen spätestens ab dem Echtbetrieb auf die tatsächlichen Arbeitsgebiete einzuschränken. Der Kunde muss hierfür die notwendigen Rollen und Zugriffrechte einrichten und allen Anwendern die notwendigen Anwenderrollen zuordnen.

5.1 Rollen zuordnen

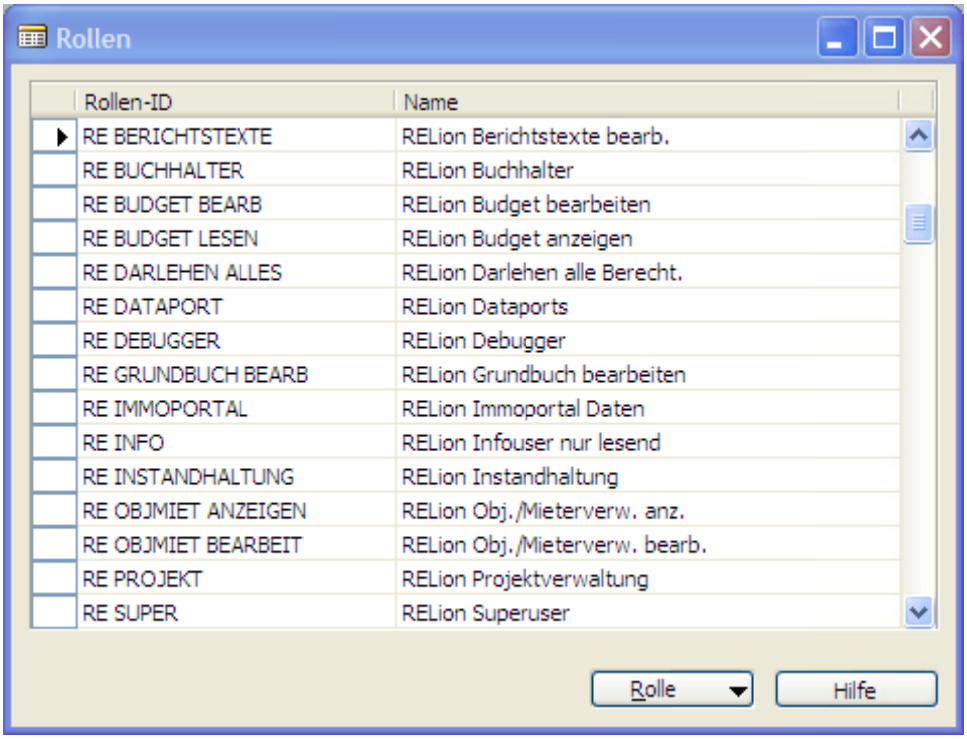
Einem Anwender können Sie beliebig viele Rollen zuordnen.

Grundsätzlich benötigt jeder Anwender zuerst die Rollen RE ALLE USER und RE GLOBAL. Diese Rollen enthalten alle Zugriffsrechte, die nötig sind, um überhaupt mit dem System zu arbeiten.

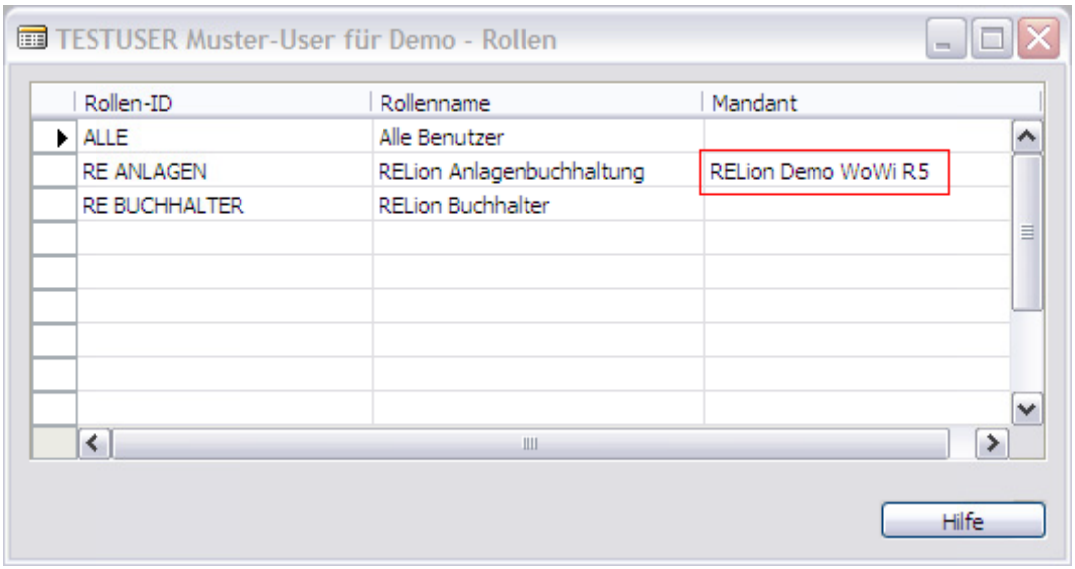
Anschließend ordnen Sie dem Anwender alle speziellen Rollen zu, die Sie für RELion erstellt haben.

Als Muster liefert mse beispielsweise Rollen für Buchhalter und Rollen für die Objekt- und Mieterverwaltung aus.

Beispiel:

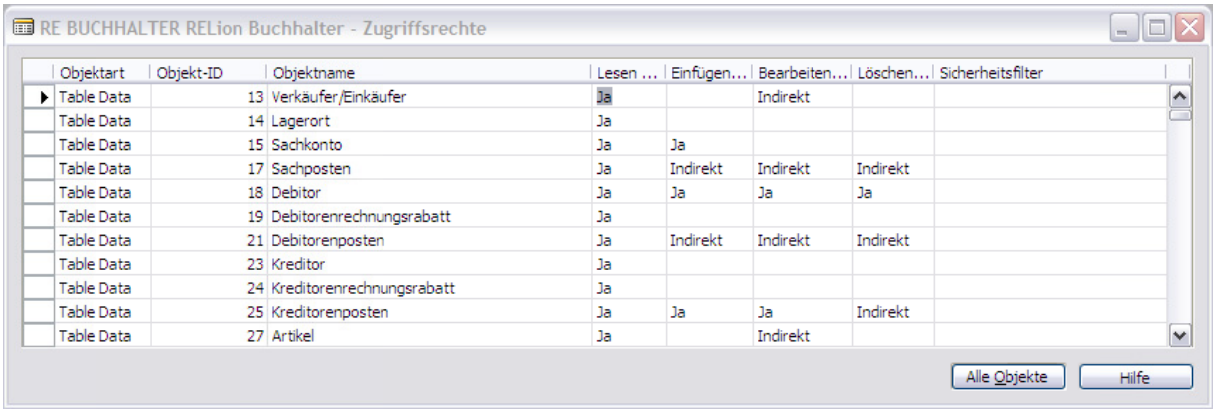


Bei der Zuordnung von Rollen auf den Anwender können die Zugriffsrechte generell auf bestimmte Mandanten begrenzt werden.



Hinweis:
Jeder Anwender muss für die globalen Tabellen zumindest Leseberechtigung haben. Wenn Sie die Zugriffsrechte auf einzelne Mandanten einschränken wollen, dann müssen Sie dafür eine zusätzliche Rolle einrichten, die nur die globalen Tabellen enthält. Diese Rolle müssen Sie ohne Mandantenbeschränkung zuordnen.

Einer Rolle werden Zugriffsrechte für unterschiedliche Objektarten zugeordnet (siehe Object Designer)
Dazu gehören Tabellendaten (lesen, anlegen, bearbeiten, löschen) und Ausführungsrechte für u.a. Reports, Forms (Masken) und Dataports (Daten Import/Export).



Objektart	Objekt-ID	Objektname	Lesen ...	Einfügen...	Bearbeiten...	Löschen...	Sicherheitsfilter
Table Data	13	Verkäufer/Einkäufer	Ja		Indirekt		
Table Data	14	Lagerort	Ja				
Table Data	15	Sachkonto	Ja	Ja			
Table Data	17	Sachposten	Ja	Indirekt	Indirekt	Indirekt	
Table Data	18	Debitor	Ja	Ja	Ja	Ja	
Table Data	19	Debitorenrechnungsrabatt	Ja				
Table Data	21	Debitorenposten	Ja	Indirekt	Indirekt	Indirekt	
Table Data	23	Kreditor	Ja				
Table Data	24	Kreditorenrechnungsrabatt	Ja				
Table Data	25	Kreditorenposten	Ja	Ja	Ja	Indirekt	
Table Data	27	Artikel	Ja		Indirekt		

Wenn Sie wollen, dass eine Rolle alle Tabellen lesen darf, dann vergeben Sie das Recht für „Table Data“ Objekt-ID 0 und Lesen = Ja.

5.2 Sicherheitsfilter

Allgemeine Erläuterung

Die SQL Server Option für Microsoft Dynamics NAV ermöglicht es Ihnen, den Zugriff von einzelnen Benutzern auf die Daten in der Datenbank zu begrenzen. Dies können Sie vornehmen, indem Sie jedem Benutzer eine oder mehrere Rollen zuweisen. Diese Rollen legen fest, dass der Benutzer nur Zugriff auf bestimmte Objekte in der Datenbank hat. Auf diese Weise können Sie festlegen, dass der Benutzer nur Zugriff auf die Daten in bestimmten Tabellen hat und ob der Benutzer für diese Tabellen berechtigt ist, Daten zu lesen, zu ändern oder einzugeben.

Wenn Ihnen diese Sicherheitsfunktionen nicht ausreichen, besteht die Möglichkeit, das Sicherheitssystem weiter zu verfeinern. Microsoft Dynamics NAV bietet Ihnen die Möglichkeit, die Rollen weiter zu verfeinern, indem Sie Sicherheitsfilter anwenden, in denen für den Benutzer festgelegt wird, auf welche Datensätze er in der Tabelle zugreifen darf.

Sicherheitsfilter können verwendet werden, um nicht autorisierte Benutzer vom Zugriff auf sensitive Daten auszuschließen. Sie können den Zugriff des Benutzers z. B. auf bestimmte Konten, bestimmte Buchhaltungsperioden oder auf die Informationen zu bestimmten Debitoren und Kreditoren begrenzen.

Die Einrichtung eines Sicherheitsfilters stellt noch nicht sicher, dass der Benutzer nur die in dem Filter festgelegten Datensätze in der Tabelle sehen kann. Jeder Benutzer hat normalerweise mehr als eine

Rolle in der aktuellen Datenbank und erhält die Berechtigungen von jeder dieser Rollen. Die Gesamtzahl der Berechtigungen, über die der Benutzer verfügt, ist die Summe der Berechtigungen aller Rollen, die dem Benutzer zugewiesen worden sind.

Wenn ein Benutzer zwei Rollen hat, die über Berechtigungen für die gleiche Tabelle verfügen und auf beide Rollen Sicherheitsfilter angewendet werden, wird die Summe dieser Sicherheitsfilter angewendet. D. h. wenn der eine Filter festlegt, dass der Benutzer nur die Posten 1-10 lesen kann und der andere Filter festlegt, dass der Benutzer die Posten 5-20 ändern kann, kann der Benutzer nur die Posten 5-20 verändern, aber die Posten 1-20 lesen.

Beachten Sie, das wenn kein Sicherheitsfilter auf eine Tabelle angewendet wird, der Benutzer alle Datensätze in der Tabelle z. B. lesen lann. Dies bedeutet, wenn mehr als eine Rolle dem Benutzer Berechtigungen für den Zugriff auf Daten einer Tabelle gibt, der Sicherheitsfilter der einen Rolle keine Anwendung findet, wenn die andere Rolle dem Benutzer die Berechtigung gibt, die gleichen Operationen in der Tabelle auszuführen, ohne dass ein Sicherheitsfilter angewendet wird.

Sicherheitsfilter können nur auf den Objekttyp "Tabellendaten" angewendet werden.

Weiterhin werden die Berechtigungen aller Benutzer mit der Rolle in der Datenbank beeinflusst, wenn Sie einen Sicherheitsfilter anwenden. Es kann daher erforderlich sein, neue Rollen zu erstellen, bevor Sicherheitsfilter angewendet werden. Falls Sie die vordefinierten Rollen nicht verändern wollen, müssen Sie neue Rollen mit den gleichen Zugriffsrechten erstellen und die Sicherheitsfilter darauf anwenden.

Wichtig:
Sicherheitsfilter auf Datensatzebene unterstützen keine Platzhalterzeichen. Das heißt, in diesen Filtern können * und ? nicht verwendet werden. Die anderen Symbole und Operatoren, wie etwa <, >, |, & und =, können verwendet werden.

Ein Sicherheitsfilter kann aus bis zu 250 Zeichen bestehen, wobei alle Ausschlusszeichen, Symbole und Operatoren (z. B. <, >, |, &, .. und =) ebenfalls als Zeichen zählen. Die Länge des Sicherheitsfilters, den Sie eingeben, kann dadurch merklich kleiner werden.

Außerdem werden Sicherheitsfilter verkettet, sodass die Summe aller Sicherheitsfilter, die auf einen Benutzer oder eine Rolle angewendet werden, 250 Zeichen nicht überschreiten darf

5.3 Einrichtungsbeispiele für Sicherheitsfilter in RELion

Bei Bedarf können die Datenberechtigungen innerhalb einer Tabelle anhand von Sicherheitsfiltern zusätzlich auch auf bestimmte Daten eingeschränkt werden. Beispielsweise können so Berechtigungen auf bestimmte Sachkonten oder bestimmte Objekte begrenzt werden.

Zur Verdeutlichung geben wir jetzt ein Beispiel.

Der Anwender soll nur die Konten und Umsätze aus dem Mietebereich und Betriebskosten sehen können. Bankkonten, Kapital- und Eigentümerkonten sollen nicht sichtbar sein.

Damit die Funktionen, die Salden aus Sachposten berechnen, wie die Einheitenübersicht, korrekt funktionieren, müssen dafür alle beteiligten Sachkonten berechtigt werden.

Für Mieter und Eigentümer sollen es diese Sachkonten sein.

2000 Mietforderungen

4401 und 4402 VZ BK/HK

6000 bis 6094 Mieterlöse

9995 SaVo

Die Konten 8000 bis 8049 sind Betriebskosten.

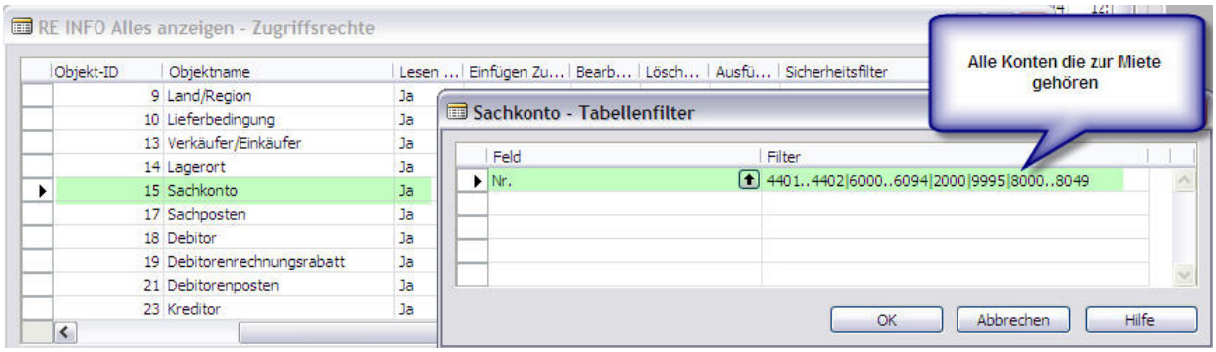
Beachten Sie dabei, dass Sie für weitere Funktionen, wie die Erstellung der BK-Abrechnung möglicherweise weitere Konten berechtigen müssen. Für die Abrechnung können dies bspw. Konten wie VSt, MwSt, Gegenkonto Abrechnung usw. sein.

Einrichtung:

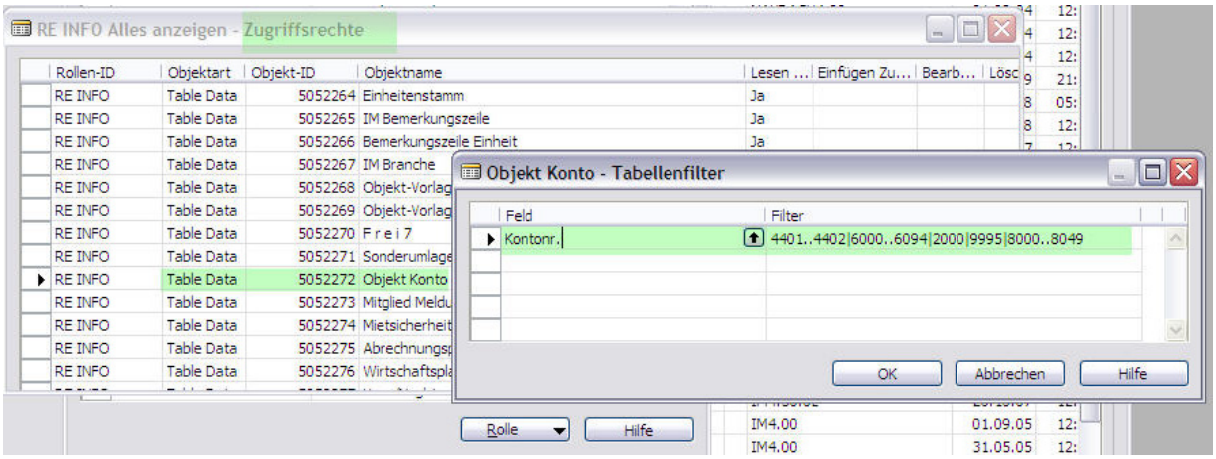
In den bei dem Anwender vorhandenen Rollen müssen Sie prüfen, ob dort uneingeschränkte Rechte für die Tabellen 15 Sachkonto und 5052272 Objektkonto vorhanden sind und diese löschen

Sie legen dann eine neue Rolle an, die nur diese Tabellen mit den entsprechenden Sicherheitsfiltern hat.

Sicherheitsfilter für Tabelle 15 Sachkonto:

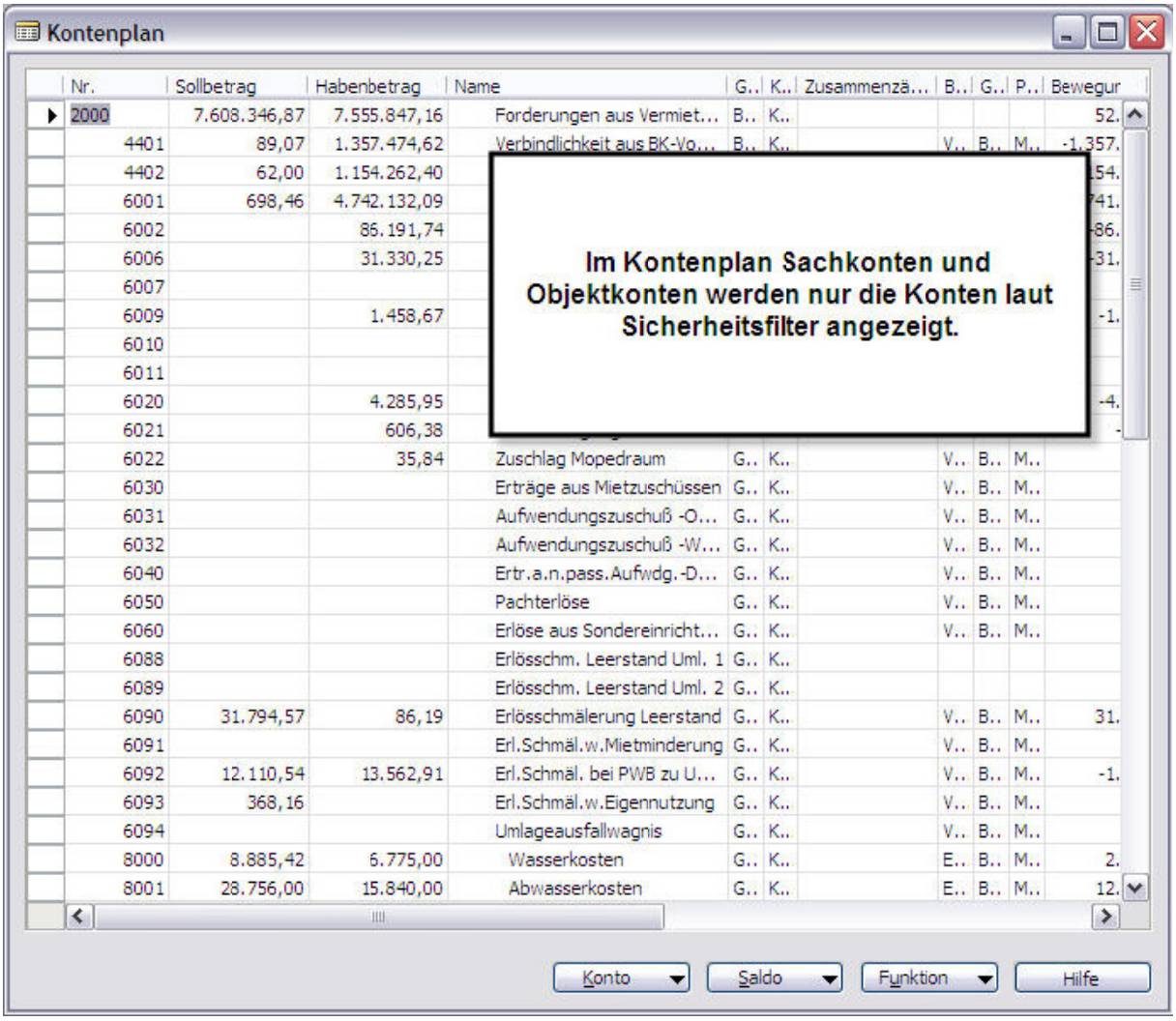


Sicherheitsfilter für Tabelle 5052272 Objektkonto:

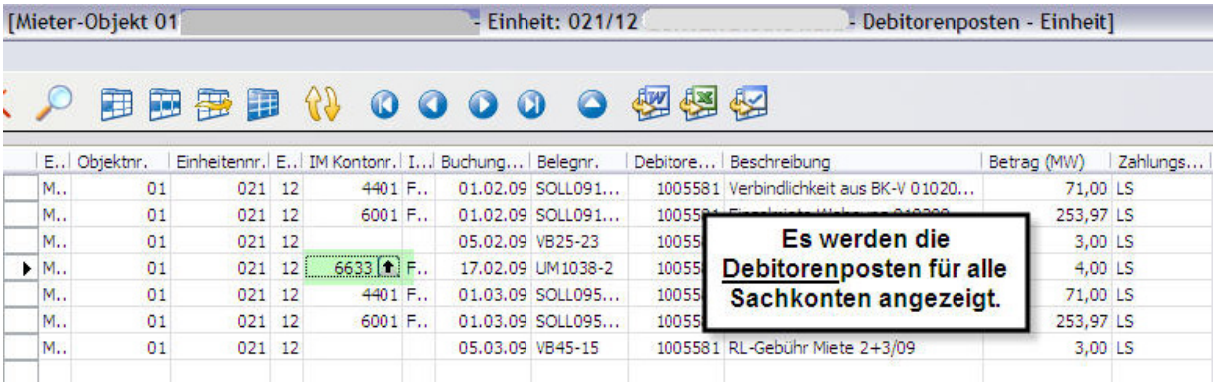


Ergebnis:

Im Kontenplan (Sachkonten, Objektkonten) werden die Konten aufgelistet, für die Berechtigung erteilt wurde. Gleiches gilt für alle Reports.

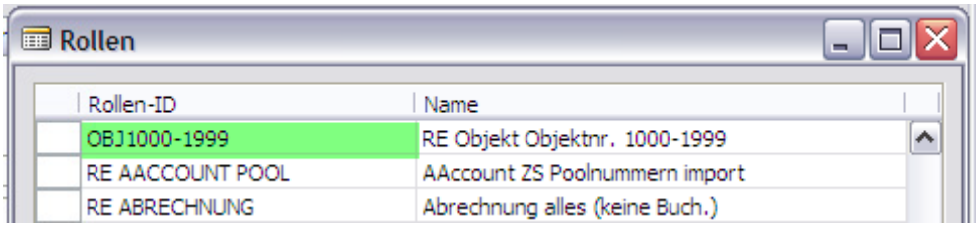


Die Debitorenposten werden uneingeschränkt angezeigt. Bei einem Aufruf von Konten (z.B. per IM Kontonr.) werden dann nur die berechtigten Konten angezeigt.

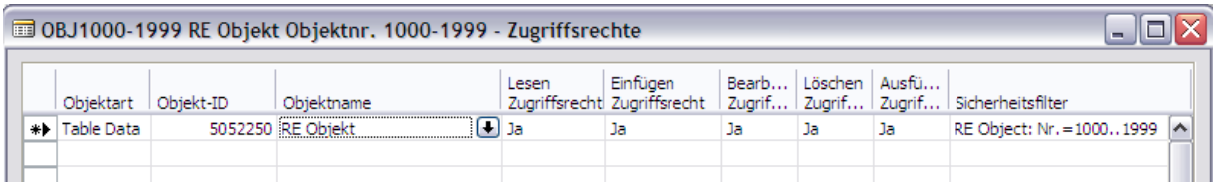


Beispiel für Zugriffsrechte auf Objekte mit bestimmten Objektnummern:

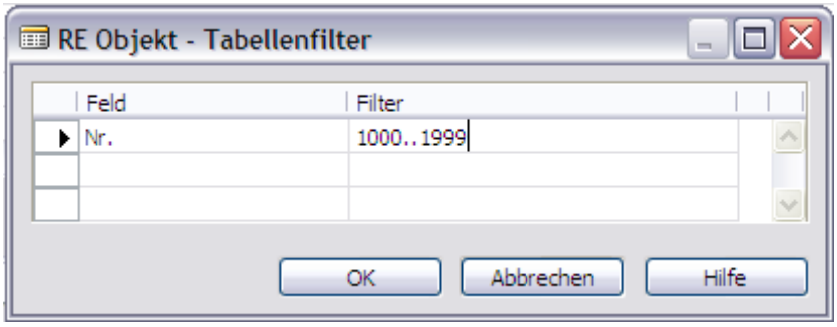
Entfernen Sie ggf. aus allen Rollen das Zugriffsrecht für die Table Data Objekt-ID 5052250.
Dann erstellen Sie eine Rolle für diese Tabelle und einen Sicherheitsfilter auf die entsprechenden Objektnummern.



Zugriffsrecht für Table Data Objekt-ID 5052250:

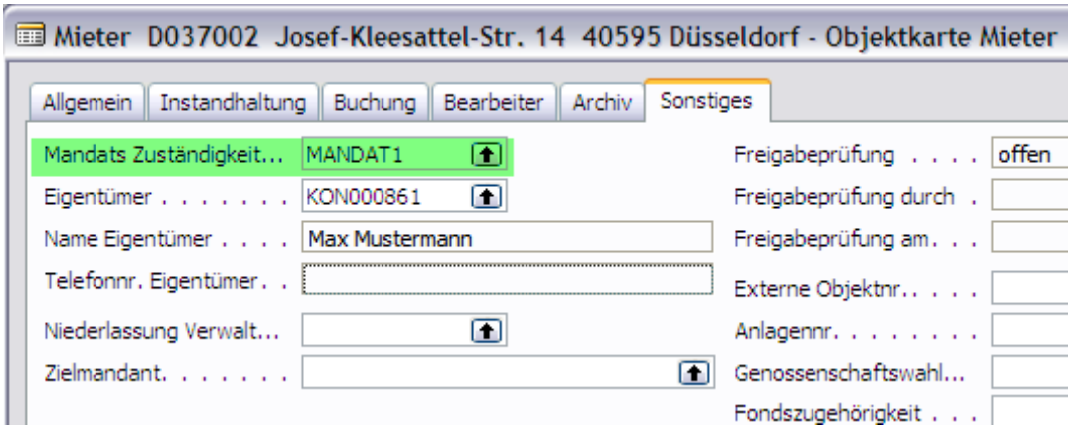


Sicherheitsfilter:



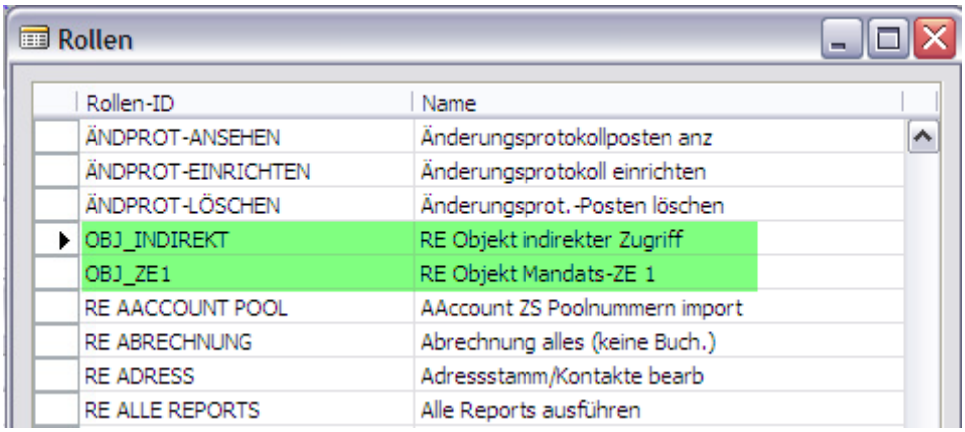
Beispiel für Zugriffsrechte auf Objekte bestimmter Mandats-Zuständigkeitseinheiten

Alle Objekte sind einer Mandats-Zuständigkeitseinheit zugeordnet

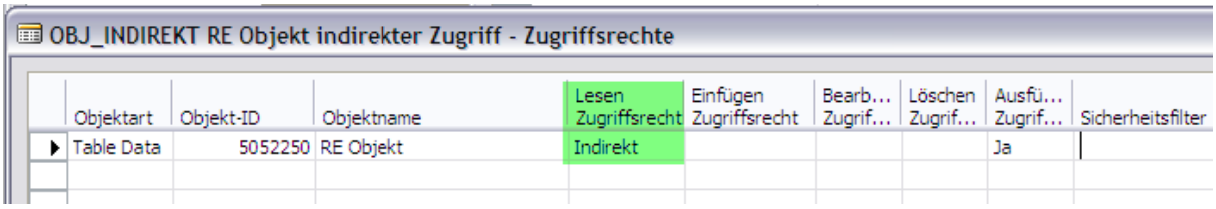


Da es sich bei dem gewünschten Sicherheitsfilter nicht um das Schlüsselfeld handelt, muss eine zusätzliche Rolle für den indirekten Zugriff auf die Tabelle RE Objekt erstellt werden. Die beiden Rollen werden dann dem Anwender zugeordnet.

Es sind also zwei Rollen einzurichten:

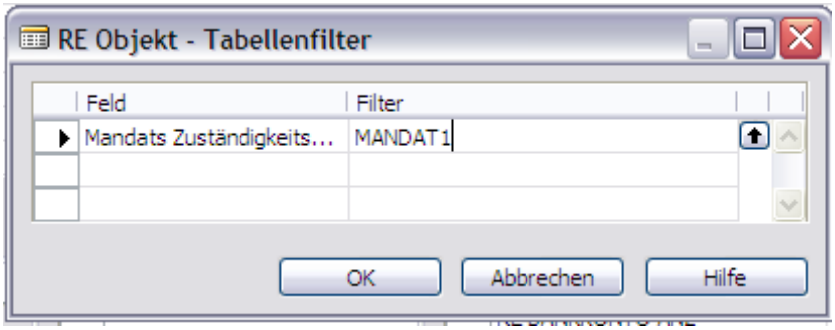


Rollen für das indirekte Lesezugriffsrecht:

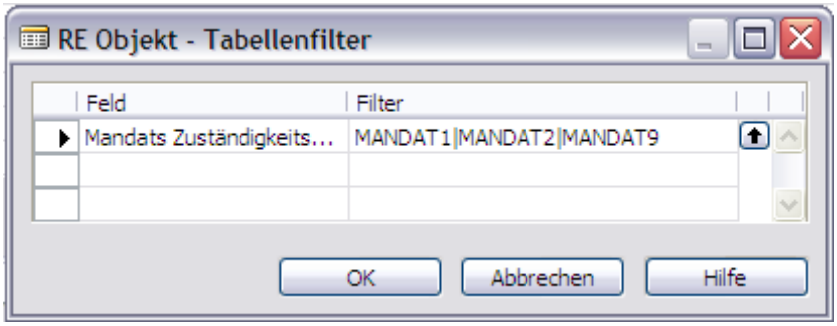


Rolle für die Bearbeitung mit Sicherheitsfilter:

Sicherheitsfilter:



Wenn Sie mehrere ZE in einem Filter zuordnen wollen, so können Sie auch eine Auflistung von Werten angeben, wobei die Einzelwerte durch das Pipezeichen | zu trennen sind.
Beispiel:



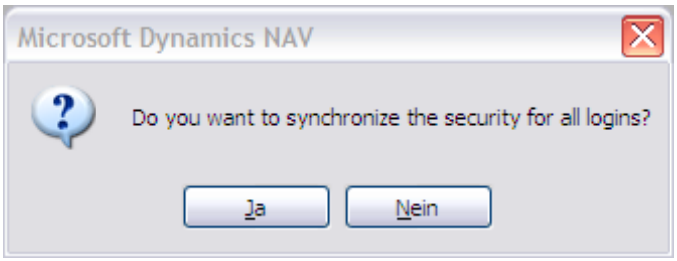
5.4 Synchronisation der Zugriffsrechte

Nach jeder Änderung von Zugriffsrechten innerhalb einer Rolle und auch der Zuordnung von Rollen bei Anwendern müssen die Zugriffsrechte mit dem MS SQL Server synchronisiert werden.

Damit die neuen Zugriffsrechte bei dem/den Anwender/n wirksam werden, müssen die betreffenden Anwender einmal die Datenbank schließen und wieder öffnen. Alternativ kann RELion auch komplett geschlossen und neu gestartet werden.

Extras > Zugriffsrechte > Synchronisieren

Es kommt folgende Frage, die Sie mit Ja beantworten.



Die Synchronisation dauert in der Regel nur ein paar Sekunden.

6 Protokoll Datenänderung

In RELion steht für alle durch Anwendungsfunktionen ausgeführten Datenänderungen eine äußerst flexibel konfigurierbare Protokollfunktion zur Verfügung.

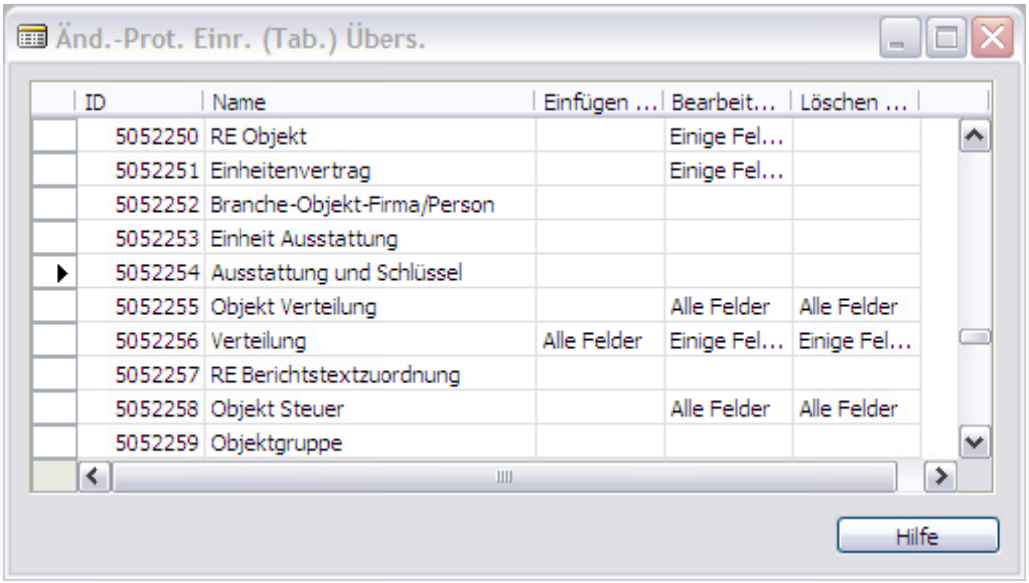
Die Einrichtung erfolgt in der Funktion

Verwaltung > Anwendung Einrichtung > Allgemein > Änderungsprotokoll Einrichtung.

In der Einrichtung wird für jede Tabelle angegeben, ob und in welchem Umfang Datenänderungen automatisch protokolliert werden. Es kann dabei nach den Funktionen Einfügen, Bearbeiten und Löschen unterschieden werden. Außerdem ob alle oder nur bestimmte Felder protokolliert werden sollen.

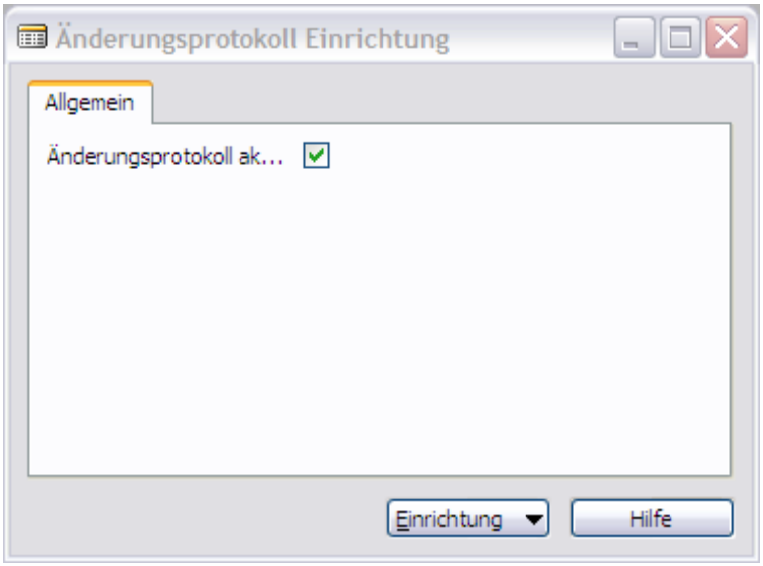
Zu jeder definierten Tabelle werden dann automatisch zu jedem Datensatz die Informationen alter/neuer Wert, Zeitpunkt der Änderung und Anwender gespeichert. Die protokollierten Änderungen können (bei entsprechender Berechtigung) nach diversen Kriterien ausgewertet werden. Unter anderem je Tabelle, je Anwender und dem Zeitpunkt der Änderung.

Beispiel für Tabellen im Bereich RELion (5052xxx):



Das Änderungsprotokoll kann jederzeit aktiviert und deaktiviert werden, was ebenfalls im Änderungsprotokoll festgehalten wird.

Es empfiehlt sich unbedingt, diese Protokollfunktion spätestens ab dem Echtbetrieb zu aktivieren. Bei einer manuellen Datenübernahme sollte sie bereits ab Beginn der Datenübernahme aktiviert sein.

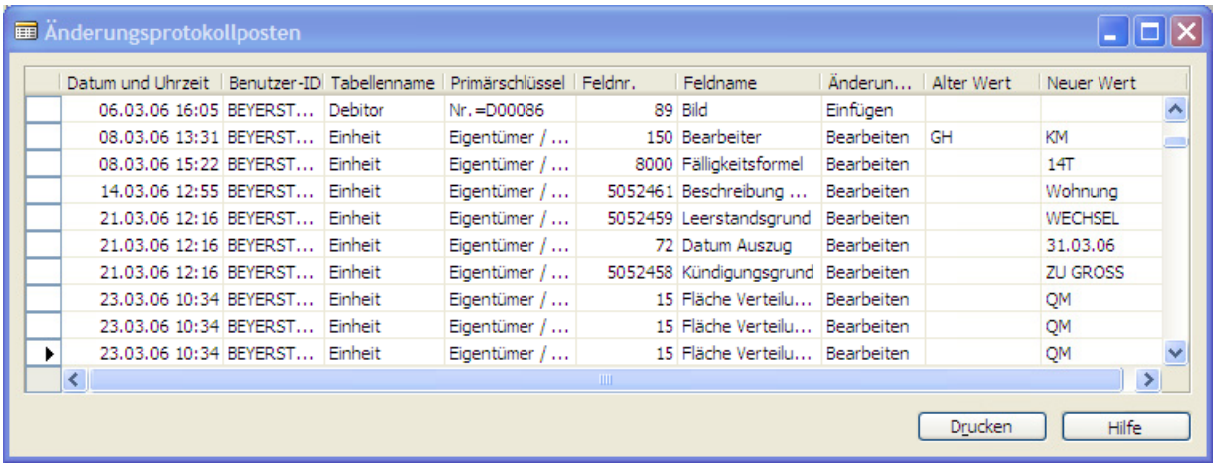


Hinweis:

Es ist wichtig, dass die Einrichtung des Änderungsprotokolls durch eine gesonderte Rolle geschützt wird und nur wenigen Anwendern zugänglich ist. Anwender mit der Rolle SUPER können die Einrichtung nach Belieben verändern!

Auswertung der Änderungsprotokollposten:
Die Auswertung erfolgt in der Funktion
Verwaltung > Anwendung Einrichtung > Allgemein > Änderungsprotokoll.

Beispiel:



Bestimmte Tabellen sollten wegen der großen Masse an Änderungen und wegen ihrer geringen Relevanz nicht protokolliert werden. Dazu gehört z.B. das Löschen von Buchblattzeilen.

7 Datensicherung

Ab dem Installationszeitpunkt ist eine mindestens tägliche Datensicherung des MS SQL Servers und aller Datenbanken auf geeigneten Medien (z.B. Bandlaufwerk) zwingend erforderlich.

Aus Sicherheitsgründen ist es dringend angeraten, periodisch auf mehrere Medien zu sichern, also beispielsweise jeweils ein Band je Tag.

Wir weisen ausdrücklich darauf hin, dass der Kunde ein geeignetes Sicherungsverfahren eigenverantwortlich realisieren muss.
Für die Einrichtung und die Durchführung der Datensicherung ist der Kunde verantwortlich.

Insofern mse die Hardware und das Server-Betriebssystem liefert und betreut, sind wir bei der Einrichtung gern behilflich oder führen die Einrichtung bei Beauftragung gern durch.