Dokumentation

Datensatzberechtigungen in orgAnice und Benutzerverwaltung mit Active Directory

Datensatzberechtigungen in orgAnice

Allgemeines

Ein Feature von orgAnice CRM sind die Datensatzberechtigungen. Die Datensatzberechtigungen sind als Lese- und Schreibberechtigungen realisiert, sie können sich auf Benutzer- und Berechtigungslisten (Benutzergruppen) beziehen.

Dieses Kapitel richtet sich an Entwickler und Datenbankadministratoren; es gibt Ihnen eine Einführung in die Datensatzberechtigungen in orgAnice. So finden Sie Antworten auf die folgenden Fragen:

- Wie funktionieren die Datensatzberechtigungen?
- Wie richte ich Datensatzberechtigungen benutzerbezogen ein?
- Wie richte ich Datensatzberechtigungen gruppenbezogen ein?
- Wie kann ich die Datensatzberechtigungen über die COM-Schnittstelle nutzen?
- Welche Funktionalitäten gibt es in orgAnice Data?

Voraussetzungen

Die Datensatzberechtigungen stehen ausschließlich in den orgAnice-Editionen Professional und Enterprise zur Verfügung (in der Lizenznummer muss der FeatureCode „*DBS*“ enthalten sein).

Unterschiede MS SQL / internes Datenbankformat

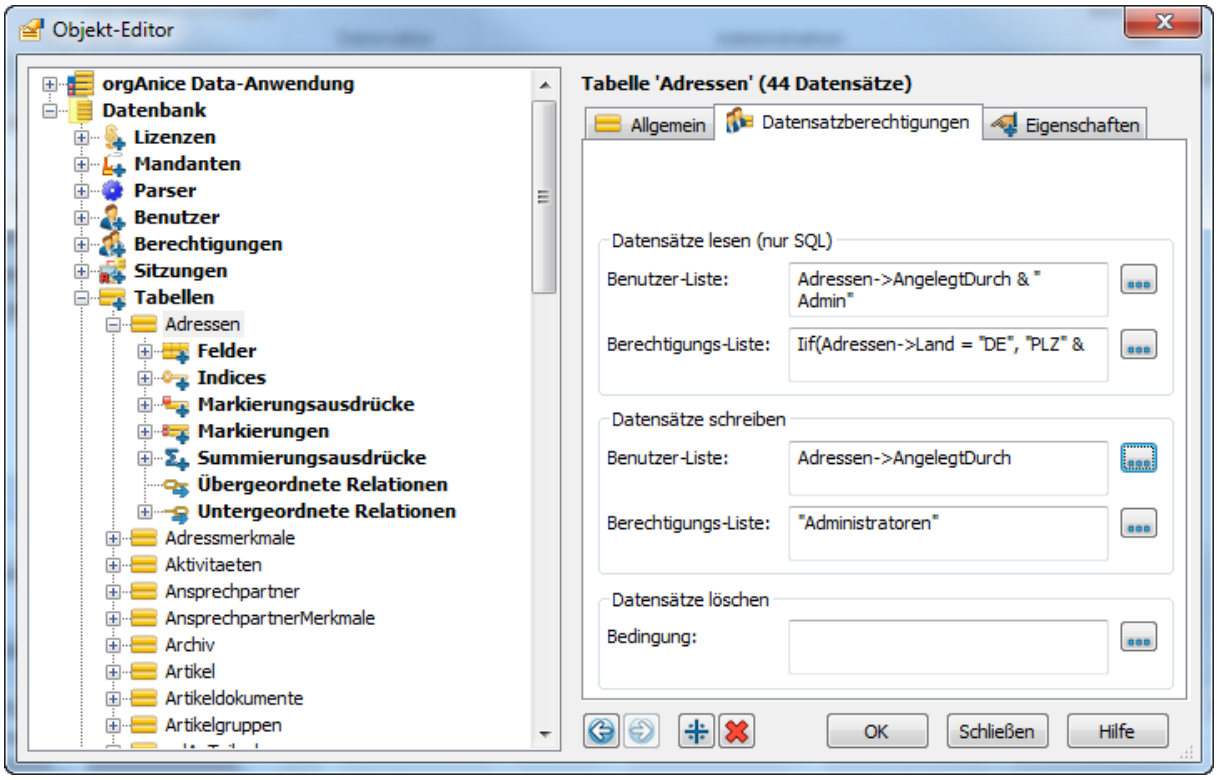
Die Leseberechtigungen stehen ausschließlich unter bei Verwendung des MS SQL Servers zur Verfügung. Die Schreibberechtigungen stehen sowohl bei Verwendung des MS SQL Servers als auch des internen Datenbankformats zur Verfügung (Betrifft nur orgAnice CRM 2008 und 2010, in orgAnice CRM 7 steht das interne DB-Format nicht mehr zur Verfügung).

Datensatzberechtigungen

Jeder Tabelle können vier Berechtigungsausdrücke zugewiesen werden:

- Leseberechtigung auf Benutzerebene
- Leseberechtigung auf Benutzergruppenebene
- Schreibberechtigung auf Benutzerebene
- Schreibberechtigung auf Benutzergruppenebene

Die Funktionalität der bereits vorhandenen Löschbedingung bleibt unverändert.



Die Berechtigungsausdrücke müssen so konstruiert werden, dass sie eine Zeichenkette mit Namen von Benutzern bzw. Benutzergruppen (Berechtigungen) zurückgeben. Die einzelnen Namen müssen durch Leerzeichen getrennt sein.

Die Ausdrücke werden für jeden Datensatz ausgewertet - die Benutzer bzw. Benutzergruppen, deren Namen in der zurückgegebenen Zeichenkette enthalten sind, besitzen die erforderliche Berechtigung. Allen anderen Benutzer wird die Berechtigung verwehrt (Sie sehen den Datensatz nicht oder können ihn nicht beschreiben).

Dem Benutzer wird die Berechtigung gewährt, wenn sein Name in der zurückgegebenen Benutzerliste enthalten oder wenn er Mitglied mindestens einer der Benutzergruppen in der zurückgegebenen Berechtigungsliste ist. Die Erfüllung beider Kriterien gleichzeitig ist nicht notwendig.

Wir empfehlen, insbesondere bei größeren Benutzeranzahlen, vorrangig mit Benutzergruppen zu arbeiten. Bei einer höheren Benutzerfluktuation wird dadurch die Administration erleichtert, da die Ausdrücke bei neuen oder weggefallenen Benutzer nicht angepasst werden müssen. Für die benutzergruppenbezogene Zuordnung von einzelnen Datensätzen in orgAnice Data steht der Steuerelementtyp „*Berechtigungs-Lookup-Liste*“ zur Verfügung.

Soll allen Benutzern Zugang gewährt werden, sollte der Benutzerlisten-Ausdruck eine leere Zeichenkette zurückgeben. Vorsicht: eine aus einem Leerzeichen bestehende Zeichenkette verbietet allen Benutzern den Schreibzugriff (eine solche Zeichenkette beinhaltet keine gültigen Benutzernamen, sondern ausschließlich das Trennzeichen).

Die Ausdrücke können und sollten sich auf Feldinhalte beziehen, denn nur so erreicht man wirkliche Datensatz-Berechtigungen. Selbstverständlich sind auch konstante Ausdrücke zulässig - sie bewirken

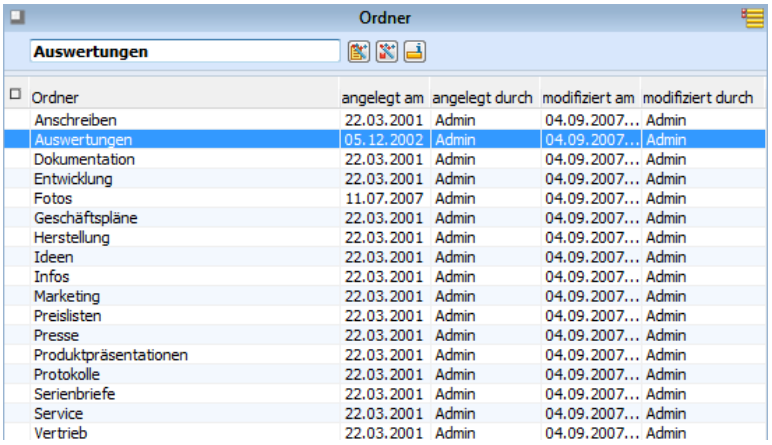
allerdings nichts anderes als die bereits vorhandenen Tabellenberechtigungen, da sie für jeden Datensatz identische Rückgabewerte liefern.

Die Leseberechtigungen sind den Schreibberechtigungen übergeordnet - *„wer nicht lesen kann, der kann auch nicht schreiben*“. Dies bedeutet: Ein Datensatz, für den der Benutzer keine Leseberechtigung besitzt, wird auch dann nicht angezeigt, wenn aufgrund des Schreibberechtigungsausdrucks der Benutzer den Datensatz eigentlich beschreiben könnte.

Bei der Anmeldung mit Datenbankverwaltungsrechten sind die Lese- und Schreibberechtigungen außer Kraft gesetzt - der Administrator darf alle Datensätze einsehen und beschreiben.

Berechtigungs-Lookup-Liste als Steuerelement

Der Steuerelementtyp *„Berechtigungs-Lookup-Liste*“ stellt alle definierten Berechtigungen in einer Auswahlliste zur Verfügung (analog zur Benutzer-Lookup-Liste). Dieses Steuerelement eignet sich besonders für die Zuweisung von Datensatzberechtigungen.



Ordner	angelegt am	angelegt durch	modifiziert am	modifiziert durch
Anschreiben	22.03.2001	Admin	04.09.2007...	Admin
Auswertungen	05.12.2002	Admin	04.09.2007...	Admin
Dokumentation	22.03.2001	Admin	04.09.2007...	Admin
Entwicklung	22.03.2001	Admin	04.09.2007...	Admin
Fotos	11.07.2007	Admin	04.09.2007...	Admin
Geschäftspläne	22.03.2001	Admin	04.09.2007...	Admin
Herstellung	22.03.2001	Admin	04.09.2007...	Admin
Ideen	22.03.2001	Admin	04.09.2007...	Admin
Infos	22.03.2001	Admin	04.09.2007...	Admin
Marketing	22.03.2001	Admin	04.09.2007...	Admin
Preislisten	22.03.2001	Admin	04.09.2007...	Admin
Presse	22.03.2001	Admin	04.09.2007...	Admin
Produktpräsentationen	22.03.2001	Admin	04.09.2007...	Admin
Protokolle	22.03.2001	Admin	04.09.2007...	Admin
Serienbriefe	22.03.2001	Admin	04.09.2007...	Admin
Service	22.03.2001	Admin	04.09.2007...	Admin
Vertrieb	22.03.2001	Admin	04.09.2007...	Admin

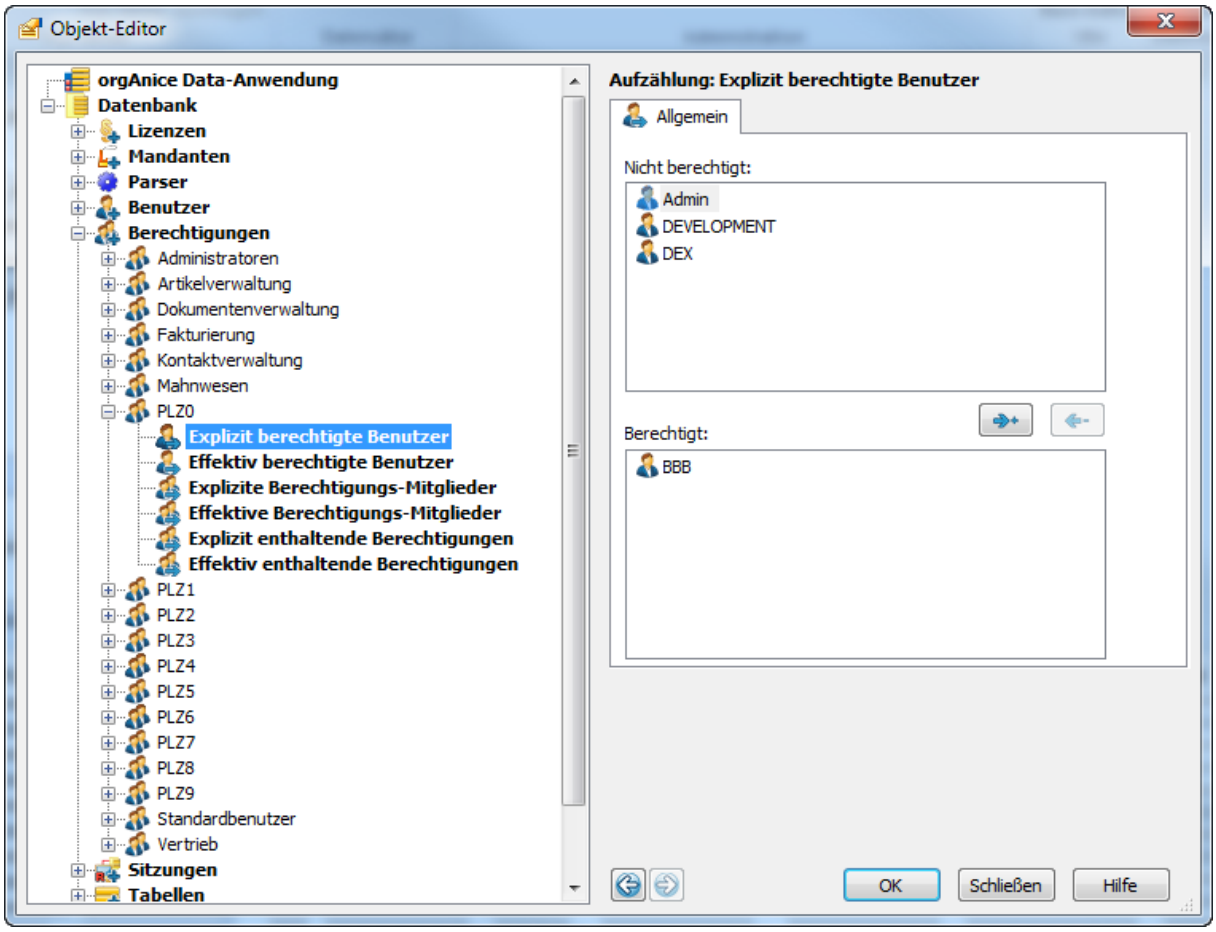
Beispiele für die Verwendung der Datensatzberechtigungen

Anforderung: Jeder Benutzer darf nur die Datensätze sehen, die er angelegt hat. Benutzer ADMIN darf alle Datensätze sehen.
Lösung: Ausdruck für die Benutzerliste: `Adressen->AngelegtDurch & " ADMIN"`

Anforderung: Jeder Benutzer darf nur die Datensätze beschreiben, die er angelegt hat.
Lösung: Ausdruck für die Benutzerliste: `Adressen->AngelegtDurch`

Anforderung: Die Vertriebsmitarbeiter dürfen nur die Adressen aus ihnen zugeordneten PLZ-Gebieten sehen.
Lösung:

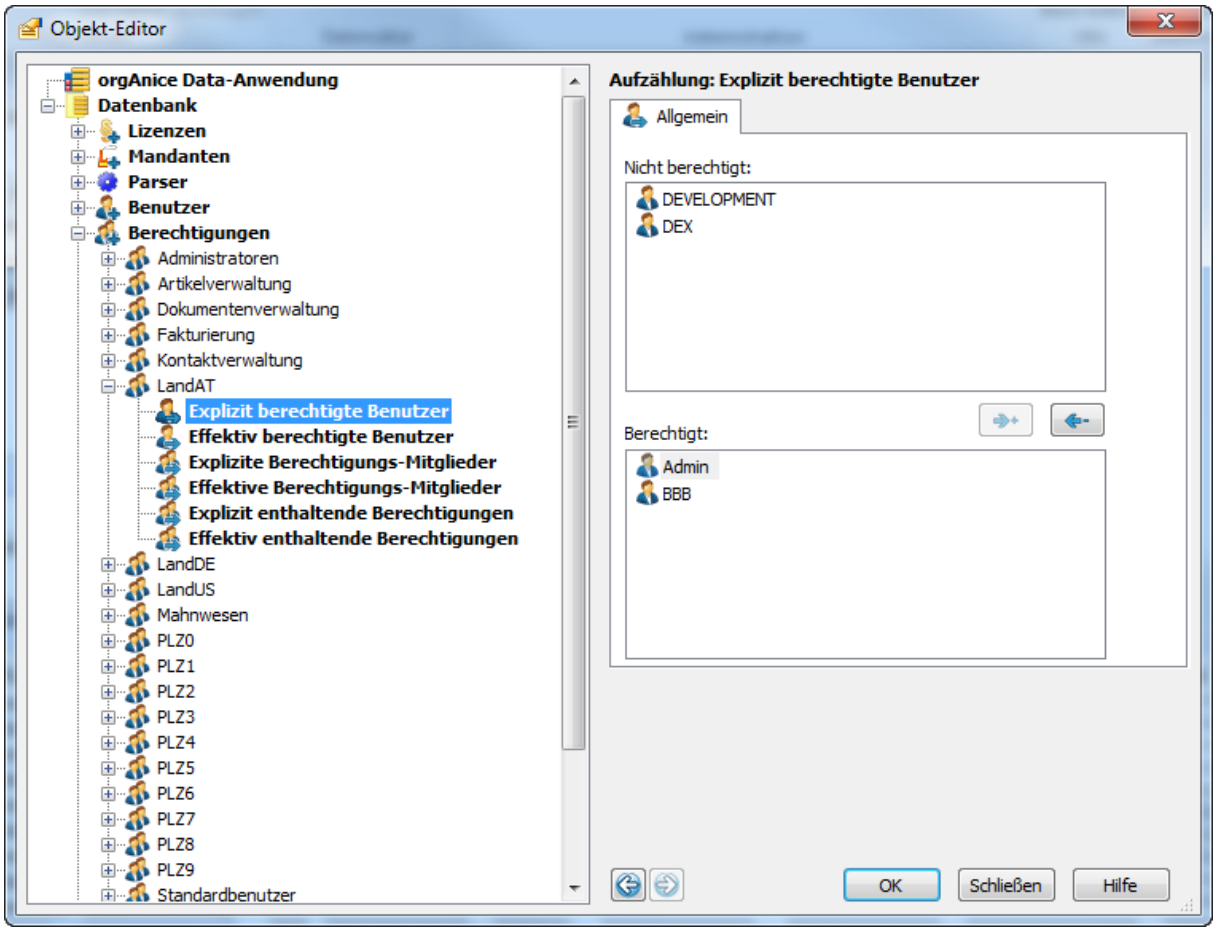
1) Erstellen Sie 10 Berechtigungen mit den Namen PLZ0, PLZ1, PLZ2, …, PLZ9 und ordnen Sie den Berechtigungen die gewünschten Benutzer zu.



2) Verwenden Sie den folgenden Ausdruck für die Berechtigungs-Liste: `"PLZ" & Left(Adressen->PLZ, 1)`

Um das Beispiel einfach zu halten, findet bisher keine Prüfung des Landes statt. Angenommen, die Mitarbeiter sind auch den Ländern zugeordnet, so könnte die Lösung beispielsweise so aussehen:

3) Erstellen Sie weitere Berechtigungen mit den Namen „*LandXXX*“. XXX steht hier für die in orgAnice verwendeten Länderkürzel, also bspw. „*LandDE*“, „*LandAT*“, „*LandUS*“. Ordnen Sie den Berechtigungen die gewünschten Benutzer zu.



4) Verwenden Sie den folgenden Ausdruck für die Berechtigungs-Liste:

```
Iif(Adressen->Land = "DE", "PLZ" & Left(Adressen->PLZ, 1),
"Land" & Adressen->Land)
```

Beachten Sie, dass Adressen aus Ländern, für die es keine Berechtigungsgruppen gibt, von keinem Benutzer gesehen werden.

COM-Schnittstelle

- Eigenschaften *Table.ReadUserListPrq*, *Table.ReadPermissionListPrq*, *Table.WriteUserListPrq*, *Table.WritePermissionListPrq*: Der WriteUserListPrq muss so formuliert sein, dass er eine mit Leerzeichen getrennte Liste von Benutzern zurückgibt, die den Datensatz schreiben dürfen. Wird trotzdem versucht, den Datensatz zu speichern, kommt der Fehlercode ORGDB_E_NORECORDWRITEPERMISSION.
- Eigenschaften *Table.CanWriteRecord* und *Table.CanDeleteRecord*: Im Unterschied zu *CanWrite* und *CanDelete* werden hier nur datensatzabhängige Schreib- und Löschberechtigungen geprüft. Ein Datensatz darf also gelöscht werden, wenn sowohl *Table.CanDelete* als auch *Table.CanDeleteRecord* `True` zurückgeben.
- Methode *Document.Clone*: Erzeugt eine Kopie des gegebenen Dokuments.
- Fehlercodes *ORGDB_E_NODOCREADPERMISSION, ORGDB_E_NODOCWRITEPERMISSION, ORGDB_E_NORECORDWRITEPERMISSION, ORGDB_E_NORECORDDELETEPERMISSION, ORGDB_E_DEVELOPMENTUSER*: Die eigenständigen Fehlercodes dienen der besseren Abgrenzung zwischen Objekt-, Dokument- und Datensatzberechtigungen bzw. zur Kennzeichnung der Sonderstellung des DEVELOPMENT-Benutzers.

- Fehlercode *ORGDB_E_NORECORDWRITEPERMISSION* - kommt der Benutzer kein Schreibrecht auf den aktueller Datensatz besitzt. Um den Fehler zu vermeiden, sollte vor dem Speichern die Eigenschaft *Table.CanWriteRecord* abgeprüft werden.

Besonderheiten

- Das Löschen aller Datensätze einer Tabelle per *Table.ClearRecords* benötigt Verwaltungsrechte, da Löschberechtigungsausdrücke bzw. schreibgeschützte Dokumente vorhanden sein könnten, die nur bei Anmeldung mit Verwaltungsrechten "*ausgehebelt*" werden. Im Dialog "*Datensätze löschen*" ist also der Radio-Button "*Alle Datensätze*" nur beim Anmelden mit Verwaltungsrechten aktiv.
- *Table.DeleteRecords* nimmt Rücksicht auf Datensatz-Löschberechtigungen. Datensätze, die aufgrund eines Löschausdrucks nicht gelöscht werden dürfen, werden ignoriert und nicht mitgezählt. Das gilt auch für Datensätze in untergeordneten Tabellen. In diesem Fall wird, falls ein DS in einer untergeordneten Tabelle nicht gelöscht werden konnte, der übergeordnete DS auch nicht gelöscht. Insofern kann es auch beim Löschen aller sichtbaren Datensätze dazu kommen, dass eben nicht alle sichtbaren Datensätze gelöscht werden.
- Das Löschen eines Master-Datensatzes ist nicht mehr möglich, wenn der aktuelle Benutzer für einen der Detail-Tabellen keine Löschberechtigung aufgrund des Löschausdrucks hat.
- Das Löschen eines Master-Datensatzes ist nicht mehr möglich, wenn der aktuelle Benutzer in einer der Detail-Tabellen keine statische Löschberechtigung hat.
- Beim Löschen eines Datensatzes wird geprüft, ob Schreibberechtigung auf alle enthaltenen Dokumente besteht.
- Löschberechtigungen auf untergeordnete Tabellen greifen nur dann, wenn in der untergeordneten Tabelle mindestens ein verknüpfter Datensatz vorhanden ist. Ist also eine Löschberechtigung auf die Tabelle "*Kundennummern*", aber nicht auf "*Adressen*" gesetzt, darf die Adresse nicht mehr gelöscht werden, sobald eine Kundennummer zugeordnet wurde. Das gilt auch für das Löschen mehrerer Datensätze per *Table.DeleteRecords*.

Benutzerverwaltung mit Active Directory

Benutzerverwaltung mit Active Directory

Allgemeines

orgAnice CRM 7 unterstützt Active Directory (AD) für die Benutzerverwaltung. Für die Anmeldung an Ihre orgAnice Datenbank kann statt der orgAnice-Anmeldung, die Windows-Authentifizierung verwendet werden. Die Benutzer werden in dem von Windows bereitgestellten Verzeichnisdienst Active Directory verwaltet. orgAnice übernimmt die zentral verwalteten Benutzerdaten, so dass kein weiterer Konfigurationsaufwand entsteht.

Für optimale Abwärtskompatibilität gibt es einen nativen Modus und einen AD-verwalteten Modus. Der Datenbankadministrator kann zwischen den Modi in der Benutzerverwaltung umschalten.

Nach der Einschaltung der AD-Unterstützung kann ein Benutzer mit einfachem Doppelklick die Datenbank öffnen. Schlägt die Authentifizierung über Active Directory fehl, erscheint der Anmeldedialog. Alternativ kann der Anmeldedialog durch einen Kommandozeilen-Schalter erzwungen werden. Je nach Datenbankeinstellung wird das Kennwort gegen die Windows-Authentifizierung oder gegen das orgAnice-Passwort geprüft.

Die Benutzer, die sich an orgAnice anmelden dürfen, werden in einer Benutzergruppe im Active Directory angelegt. In der orgAnice-Datenbank ist der Name dieser Benutzergruppe abgelegt, zusammen mit den Verbindungsdaten zum AD-Server.

Das Konzept unterstützt auch AddOn-Lizenzen: jeder AddOn-Lizenz kann eine AD-Benutzergruppe zugeordnet werden.

Die konkurrierenden Benutzer bekommen eine eigene AD-Benutzergruppe zugeordnet. Ist ein Benutzer sowohl in der permanenten als auch als in der konkurrierenden AD-Benutzergruppe enthalten, ist er permanent.

Genügt die orgAnice-Lizenz nicht, um allen Benutzern in der Benutzergruppe permanenten Zugang zur Datenbank zu gestatten, wird nach dem Prinzip „*first come, first serve*“ gearbeitet: Ein neuer Benutzer wird dann im Zweifelsfall auf „*passiv*“ oder „*konkurrierend*“ gesetzt.

Auch jede orgAnice-Berechtigung kann an eine AD-Benutzergruppe gekoppelt sein.

Voraussetzungen

- orgAnice CRM 2008, 2010, 2012 oder CRM 7, mindestens in der Professional-Edition
- In Ihrer Lizenz muss der Feature-Code „*ACL*“ enthalten sein

Lizenzvergabe

Wenn bei der automatischen orgAnice-Lizenzvergabe anhand von Windows-Berechtigungen auf einer orgAnice-Lizenz die Anzahl permanenter Benutzer nicht ausreicht, um den Benutzer zu aktivieren, wird für alle orgAnice-Benutzer, denen ein Windows-Benutzer zugeordnet ist, geprüft, ob sie laut Windows-Berechtigung für die Datenbanklizenz immer noch für permanenten Zugriff freigeschaltet sind. Wenn nicht, wird deren Aktivitätsstatus geändert, also auf „*passiv*“ bzw. „*konkurrierend*“ gesetzt. Wenn der Aktivitätsstatus eines permanenten Benutzers geändert wurde, kann der aktuelle orgAnice-Benutzer aktiviert werden, ohne die Lizenz-Einschränkungen zu verletzen.

Beispiel: Der neue Mitarbeiter Klaus Schuster ist Mitglied der Windows-Berechtigungsgruppe „*orgAnice-Benutzer*“. Außerdem enthält diese Windows-Berechtigungsgruppe noch zwei weitere Benutzer. Die Datenbanklizenz erlaubt aber nur drei permanente Benutzer und die orgAnice-Datenbank enthält neben den zwei Kollegen von Herrn Schuster auch Herrn Meyer, der inzwischen aus der Firma ausgeschieden ist und nicht mehr Mitglied der Windows-Berechtigungsgruppe „*orgAnice-Benutzer*“ ist. Beim ersten Anmeldeversuch von Herrn Schuster wird der orgAnice-Benutzer „*KlausSchuster*“ automatisch angelegt und zunächst auf „*passiv*“ gesetzt. Der anschließende Versuch, den Aktivitätsstatus dieses Benutzers auf „*permanent*“ zu setzen, schlägt fehl, da die Datenbanklizenz keine weiteren permanent aktiven Benutzer zulässt. Daraufhin prüft orgAnice alle orgAnice-Benutzer mit zugeordnetem Windows-Benutzer, auch „*HansMeyer1*“, ob sie immer noch permanenten Zugriff auf die Datenbanklizenz laut Windows-Zugriffskontrollliste der Datenbanklizenz haben. Da der Windows-Benutzer „*Hans Meyer*“ nicht mehr berechtigt ist, wird sein Aktivitätsstatus in der orgAnice-Datenbank auf „*passiv*“ gesetzt. Anschließend kann die Aktivierung des orgAnice-Benutzers „*KlausSchuster*“ erfolgreich abgeschlossen werden.

Die Zuordnung eines Windows-Benutzers zu mehr als einem orgAnice-Benutzer ist nicht möglich. Der Versuch wird mit dem neuen Fehlercode „*ORGDB_E_DUPSID“* zurückgewiesen.

Änderungen bei der Anmeldung

orgAnice Data

Beim Doppelklick einer .odb-Datei im Windows-Explorer versucht orgData zunächst die automatische Anmeldung mit dem aktuellen Windows-Konto. Schlägt diese fehl, wird der herkömmliche Anmeldedialog gezeigt. (Intern wird beim Doppelklick einer Datei im Explorer die OrgData.exe mit der .odb-Datei und dem Schalter „*/DIALOG*“ als Kommandozeilenparameter gestartet. Der Kommandozeilenparameter „*/LOGIN*“ beeinflusst dieses Verhalten, ebenso wie die Angabe eines Benutzers mit dem Schalter „*/USER*“. In diesem Fall erscheint der herkömmliche Anmeldedialog in jedem Fall.)

orgAnice Datenbank-Server

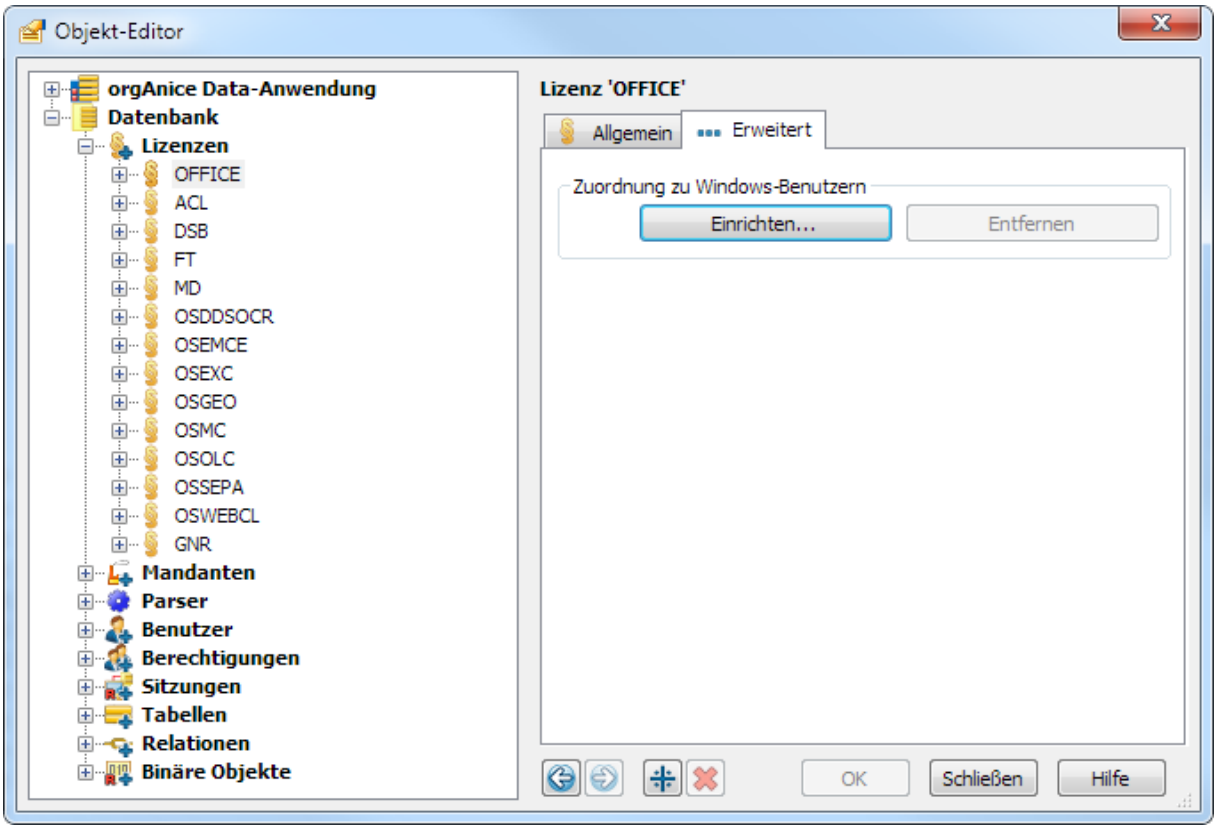
Bei der Anmeldung an orgAnice brauchen nicht mehr zwingend ein Benutzername und ein Kennwort angegeben zu werden. Wenn der aktuell an Windows angemeldete Benutzer einem orgAnice-Benutzer zugeordnet ist, wird dieser orgAnice-Benutzer für die Anmeldung an orgAnice verwendet. Wenn eine Anwendung zunächst die automatische Anmeldung probieren möchte, kann sie die Methode „*Server.Open*“ oder „*Database.Open*“ mit leerem Benutzernamen und Kennwort ausführen. Kommt der Fehler „*ORGDB_E_INVALIDUSERNAME*“ zurück, heißt das in diesem Fall, dass die automatische Anmeldung nicht funktioniert hat und die Anwendung auf die bisherige Anmeldung mit orgAnice-Benutzernamen und -Passwort zurückgreifen muss.

Wenn für einen orgAnice-Benutzer eine Zuordnung zu einem Windows-Konto besteht, kann die Anmeldung mit diesem orgAnice-Benutzer nicht mehr durch Angabe von orgAnice-Benutzername und -Kennwort erfolgen. Beim Versuch kommt der Fehlercode „*ORGDB_E_WINLOGON*“.

Änderungen im Objekt-Editor

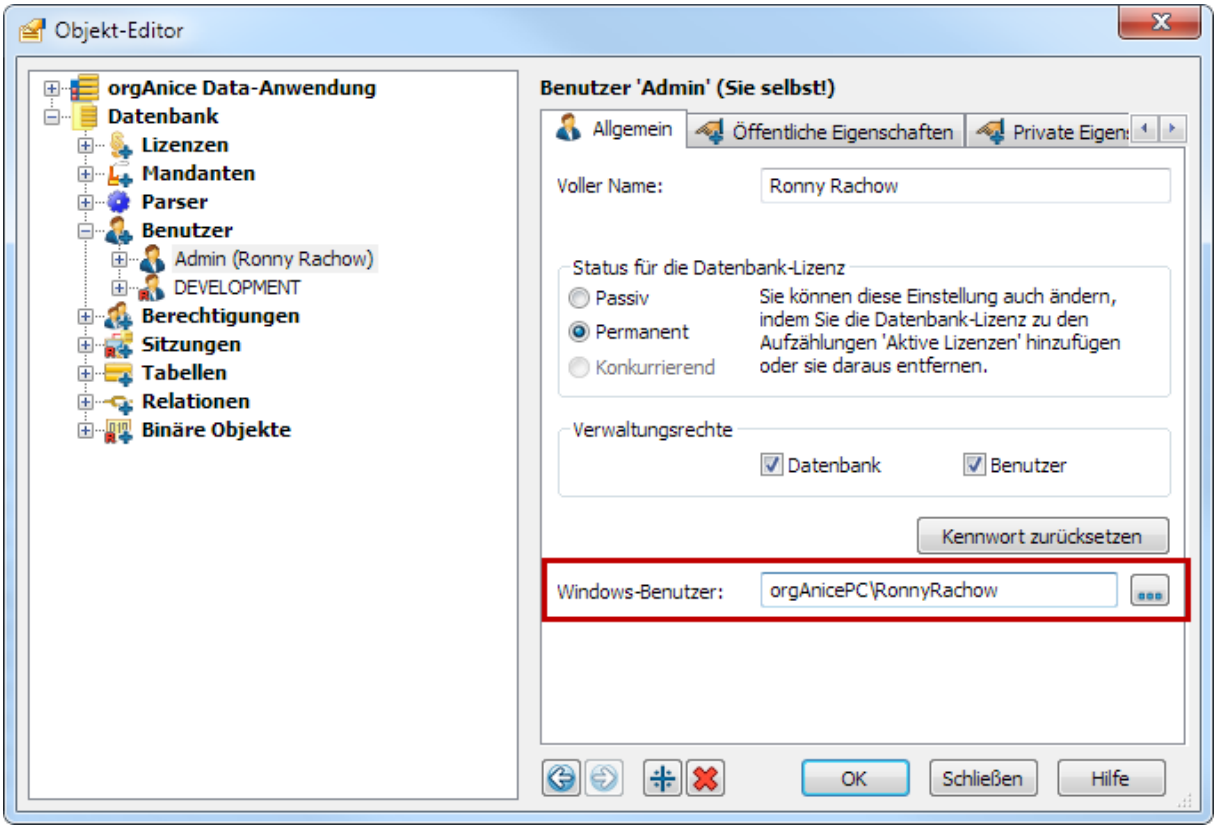
Lizenz

Neue Registerkarte „Erweitert“ für die Definition von Sicherheitsbeschreibungen zu einer Lizenz (Eigenschaft: „*WindowsSD*“). Die Zuordnung ist sowohl für Datenbank- als auch AddOn-Lizenzen möglich.



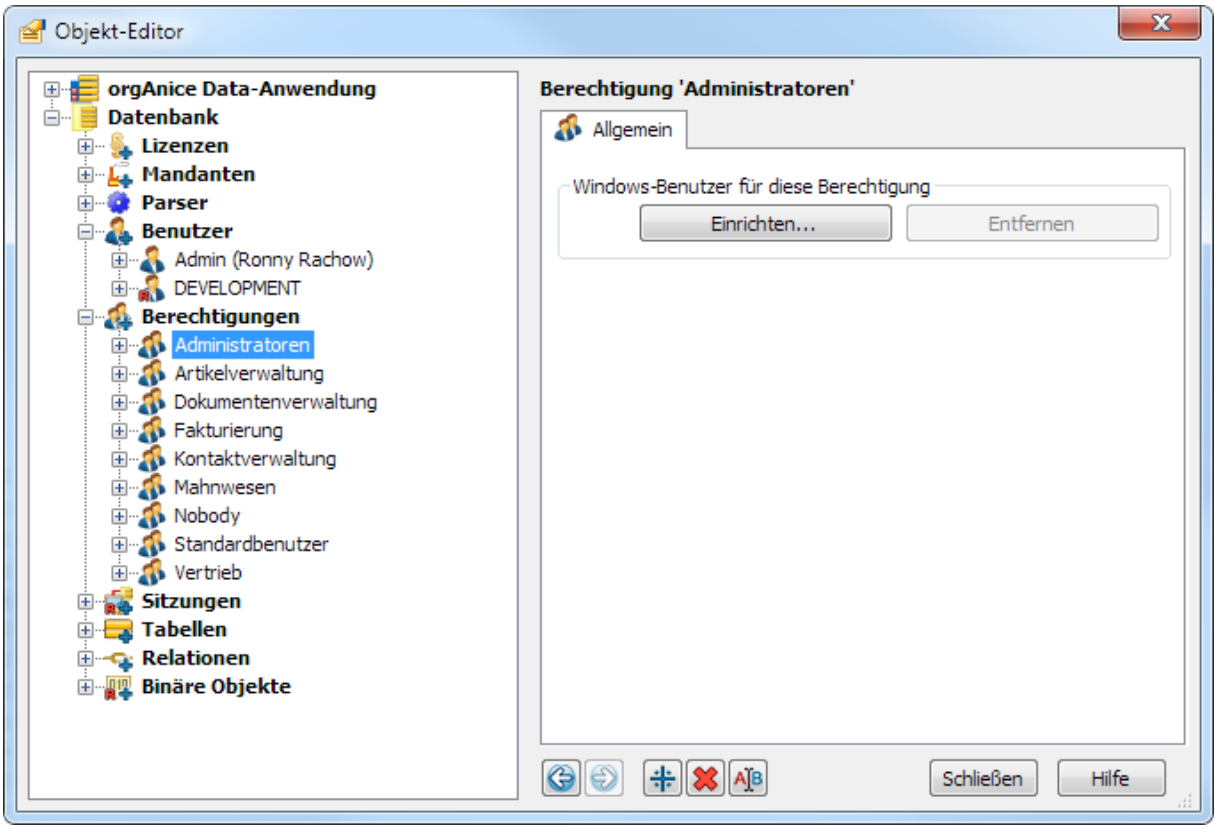
Benutzer

Neues Eingabefeld zur Definition einer Zuordnung eines Windows-Benutzers zu einem orgAnice-Benutzer. Bei Betätigung des Buttons „...“ erscheint der Windows-Standarddialog zur Objektsuche, allerdings wird vorher gegebenenfalls zum Speichern der Änderungen aufgefordert.



Berechtigung

Schaltflächen für die Definition von Sicherheitsbeschreibungen zu einer Berechtigung (Eigenschaft: „*WindowsSD*“).



Anwendung in der Praxis

Anmeldung eines bestehenden Benutzers

Der System-Administrator ordnet dem bestehenden orgAnice-Benutzer „*KlaraSchneider*“ den Windows-Benutzer „*DOMÄNE\Klara Schneider*“ zu. Jetzt öffnet sich die Datenbank bei Frau Schneider sofort ohne weiteren Anmeldedialog nach Doppelklick auf die Datenbankdatei. Durch die Zuordnung eines Windows-Benutzers zu dem orgAnice-Benutzer wird die automatische Anmeldung für diesen Benutzer aktiviert.

Wenn ein Windows-Benutzer eine Datenbank öffnet, in der er laut Windows-Zugriffskontrollliste der Datenbanklizenz Zugriff auf die Datenbank hat, werden der Aktivitätsstatus für die Datenbanklizenz (permanent bzw. konkurrierend) und die Verwaltungsrechte (Datenbank bzw. Benutzer) entsprechend der Zugriffskontrollliste für den orgAnice-Benutzer gesetzt. Das kann aus Lizenzgründen fehlschlagen, wobei in diesem Fall der von der Lizenzverwaltung festgestellte Fehler ausgelöst wird.

Zuordnung von Windows-Benutzergruppen zu orgAnice-Lizenzen

Der System-Administrator verwaltet im Active Directory eine Gruppe „*orgAnice-Benutzer*“ und eine Gruppe „*orgAnice-Administratoren*“. Im Objekt-Editor richtet er für die Datenbanklizenz (normalerweise von Typ OFFICE) eine Windows-Zugriffskontrollliste ein, die der Windows-Gruppe „*orgAnice-Benutzer*“ eine Berechtigung für die permanente Verwendung der Datenbanklizenz

einräumt, und der Benutzergruppe „*orgAnice-Administratoren*“ Datenbankverwaltungsrechte zuordnet.

Beispiel: Der System-Administrator fügt den Benutzer „*Klara Schneider*“ zur Windows-Benutzergruppe „*orgAnice-Administratoren*“ hinzu. Dadurch kann Frau Schneider schon bei ihrer nächsten Anmeldung die Datenbank verwalten, ohne dass der System-Administrator weitere Einstellungen in der orgAnice-Datenbank ändern muss. Ebenso kann ihr der Zugriff auf die Datenbankverwaltung und sogar auf die Datenbank durch Änderung der Windows-Benutzergruppe entzogen werden.

Anmeldung an AddOns

Analog wird verfahren, wenn ein Add-On versucht, sich an „*seiner*“ Add-On-Lizenz anzumelden.

Anmeldung eines neuen Benutzers

Wenn es für den aktuellen Windows-Benutzer bei bestehender Berechtigung auf die Zugriffskontrollliste der Datenbanklizenz noch keinen orgAnice-Benutzer gibt, dem dieser Windows-Benutzer zugeordnet ist, wird ein neuer orgAnice-Benutzer angelegt, dem dieser Windows-Benutzer zugeordnet wird. Der Name des neuen orgAnice-Benutzers ergibt sich aus dem Windows-Benutzernamen (ohne Domäne), wobei ungültige Zeichen gefiltert werden und ggf. Eindeutigkeit durch Anhängen einer Ziffernkombination sichergestellt wird. Der Benutzer hat zunächst den Aktivitätsstatus „*passiv*“. Die anschließende Änderung des Aktivitätsstatus auf „*permanent*“ kann jedoch aus Lizenzgründen fehlschlagen.

Beispiel: Der neue Windows-Benutzer „*Hans Meyer*“ wird vom System-Administrator zur Windows-Benutzergruppe „*orgAnice-Benutzer*“ hinzugefügt. Herr Meyer kann sich sofort an der orgAnice-Datenbank anmelden, ohne dass der Administrator weitere Änderungen an der orgAnice-Datenbank durchführen muss. Da (in diesem Beispiel) die Datenbank bereits einen orgAnice-Benutzer „*HansMeyer*“ enthält, wird für den neuen orgAnice-Benutzer der Name „*HansMeyer1*“ gewählt.

Abgleich der orgAnice-Berechtigungen

Wenn sich ein Benutzer mit seinem Windows-Konto an einer Datenbank anmeldet, werden alle Berechtigungen, denen eine Windows-Sicherheitsbeschreibung zugeordnet ist, für diesen Benutzer abgeglichen.

Beispiel: Für die orgAnice-Berechtigung „*Vertrieb*“ hat der System-Administrator im Active Directory eine Benutzergruppe „*orgAnice-Vertrieb*“ angelegt. Die orgAnice-Benutzergruppe „*Vertrieb*“ ist so eingerichtet, dass alle Benutzer der Windows-Berechtigungsgruppe „*orgAnice-Vertrieb*“ Zugriff erhalten. Der Administrator fügt den Windows-Benutzer „*Klaus Schuster*“ zur Benutzergruppe „*orgAnice-Vertrieb*“ hinzu. Dadurch wird der orgAnice-Benutzer „*KlausSchuster*“ bei der nächsten Anmeldung an der orgAnice-Datenbank automatisch Mitglied in der orgAnice-Berechtigungsgruppe „*Vertrieb*“. Wird der Windows-Benutzer „*Klaus Schuster*“ aus der Benutzergruppe „*orgAnice-Vertrieb*“ entfernt, so wird auch der orgAnice-Benutzer „*KlausSchuster*“ bei der nächsten Anmeldung aus der orgAnice-Benutzergruppe „*Vertrieb*“ entfernt.

Anmeldung mit orgAnice-Benutzernamen

Ein orgAnice-Benutzer, dem ein Windows-Benutzer zugeordnet ist, darf sich mit orgAnice-Benutzernamen und -Kennwort anmelden, wenn er unter dem ihm zugeordneten Windows-Benutzer

agiert. Das sorgt dafür, dass alte Verknüpfungen, die orgAnice-Anmeldeinformationen enthalten, in vielen Fällen nach wie vor funktionieren.

COM-Schnittstelle

User.WindowsSID

Eigenschaft „User.WindowsSID“:
Speichert den Sicherheitsbezeichner (SID) des Windows-Benutzers, der diesem orgAnice-Benutzer zugeordnet wird. Wenn diese Eigenschaft einen Leerstring enthält, besteht keine Zuordnung. Die Eigenschaft steht nur zur Verfügung, wenn der Feature-Code ACL in der Datenbank vorhanden ist. Die Sicherheits-ID muss in einem gültigen Format vorliegen, sonst wird sie mit dem Fehler „*Ungültiger Parameter*“ abgewiesen. Beim Benutzer „*DEVELOPMENT*“ ist diese Eigenschaft nicht verfügbar.

User.WindowsName

Eigenschaft „User.WindowsName“:
Diese Eigenschaft liefert den Namen des Windows-Benutzers, der diesem orgAnice-Benutzer zugeordnet ist, im Format Domäne\Name zurück. Bei der Zuweisung eines Werts (im selben Format) wird versucht, diesen Namen in eine SID umzuwandeln, nur diese SID wird persistent gespeichert. Insofern genügt es für die Zuordnung eines Windows-Benutzers zu einem orgAnice-Benutzer, entweder die Eigenschaft WindowsSID oder die Eigenschaft WindowsName zu belegen. Wie auch WindowsSID steht diese Eigenschaft nur zur Verfügung, wenn der Feature-Code ACL in der Datenbank vorhanden ist. Analog ist beim Benutzer „*DEVELOPMENT*“ diese Eigenschaft nicht verfügbar.

License.WindowsSD

Eigenschaft „License.WindowsSD“:
Definiert eine Windows-Sicherheitsbeschreibung, die angibt, welchen Windows-Benutzern automatisch Zugang zu dieser Lizenz gewährt wird (permanent bzw. konkurrierend). Diese Eigenschaft benötigt den Feature-Code ACL und ist nicht verfügbar bei AddOn-Lizenzen, die einem Datenbank-Feature-Code entsprechen. Bei der Datenbanklizenz speichert die Sicherheits-beschreibung zusätzlich, welchen Benutzern automatisch Datenbank- bzw. Benutzer-Verwaltungsrechte zugewiesen werden.

Permission.WindowsSD

Eigenschaft „Permission.WindowsSD“:
Definiert eine Windows-Sicherheitsbeschreibung, die angibt, welchen Windows-Benutzern automatisch Zugang zu dieser orgAnice-Berechtigung gewährt wird. Diese Eigenschaft benötigt den Feature-Code ACL.