Berechtigungskonzept auf Datensatzebene in Meffert Recruiter/Meffert WebRecruiter

Dokumentation und Bedienungsanleitung

Stand: März 2019

1 Das Konzept

Das Berechtigungskonzept auf Datensatzeben basiert auf dem Prinzip von "Einschränkungen des Datenzugriffs". Sie können den Zugriff auf bestimmte Datensätze in Meffert Recruiter auf konkret aufgeführte Benutzer oder Benutzergruppen einschränken. Sind weder Benutzer noch Gruppen zugeordnet (= Standardeinstellung), dann ist der Datensatz nicht eingeschränkt und für alle sichtbar. Bestehen für einen Datensatz Einschränkungen, dann ist dieser nur dann sichtbar, wenn der aktuell angemeldete Benutzer Mitglied wenigstens einer der zugeordneten Benutzergruppen ist oder wenn sein Benutzername direkt zugeordnet wurde.

Wenn Datensätze für bestimmte Benutzer unsichtbar sind, bedenken Sie bitte, dass dadurch Dubletten entstehen können. Wenn beispielsweise ein Researcher eine Person identifiziert, die zwar schon in der Datenbank existiert, für ihn aber unsichtbar ist, wird er ihn neu anlegen. Die User mit uneingeschränktem Datenzugriff sehen dann zwei Personendatensätze.

In der Benutzerverwaltung können Sie über Berechtigungen festlegen, wer überhaupt solche Datenzugriffs-Einschränkungen definieren kann.
Ferner können Sie in der Benutzerverwaltung standardmäßige Berechtigungen pro User oder pro Gruppe festlegen, die bei Neuanlage einer Person, einer Firma und eines Projekts automatisch gesetzt werden. So muss z.B. ein Researcher, der nur seine Daten sehen soll, nicht selbst die Berechtigungen festlegen, sondern dieser werden vom System automatisch gesetzt.

Eingeschränkte Datensätze vererben ihren Zugriffsschutz standardmäßig auf abhängige Datensätze weiter.
Ist z.B. der Zugriff auf einen Personendatensatz auf bestimmte User und Gruppen eingeschränkt, wirkt sich dieselbe Einschränkung auch auf die zugeordneten Aktivitäten und Dokumente aus, ohne dass bei diesen Datensätzen eine explizite Einschränkung festgelegt wurde. Eine explizite Einschränkung bei Aktivitäten und Dokumenten kann den Zugriff weiter einschränken, aber den vererbten Zugriffsschutz nicht aufheben.

Projekte vererben ihre Einschränkungen ebenfalls auf zugeordnete Aktivitäten und Dokumente.

Die größte Wirkung haben Einschränkungen bei Firmendatensätzen.
Diese wirken sich auf die als aktuellen Job zugeordneten Personen aus, auf die beauftragten Projektdatensätze (Verlinkung des Projekts mit der Firma über beide Firmenfelder Kunde und Arbeitsort), auf Aktivitäten mit Verlinkung zur Firma, und auf Firmendokumente.

Rechtsform: Kommanditgesellschaft
Sitz: Wiesbaden
Umsatzsteuer Identnummer: DE 260058742
Amtsgericht Wiesbaden, HRA 9010

Persönlich haftende Gesellschafterin:
CM Verwaltung GmbH, Sitz: Wiesbaden
Geschäftsführer: Patricia Meffert und Christoph Meffert
Amtsgericht Wiesbaden, HRB 23590

Microsoft Partner
Silver Volume Licensing
Silver Application Development

Übersicht der Berechtigungs-Vererbungen:

Berechtigungen für:	Wirken sich direkt aus auf:
Projekte	Aktivitäten Projektdokumente
Personen	Aktivitäten Personendokumente
Firmen	Personen, Projekte mit Bezug auf diese Firma bei Auftraggeber oder Arbeitsort, Aktivitäten, Firmendokumente

Beispiel:

Ein „Projekt X“ wurde beschränkt auf „Gruppe B“. Somit können nur noch die User, die der „Gruppe B“ zugeordnet sind, das „Projekt X“ sehen.

Nun erhält der Auftraggeber des „Projekt X“, die „Firma F“, eine Beschränkung auf „Gruppe A“. Diese Beschränkung vererbt sich zusätzlich auf das zugeordnete „Projekt X“ und vermischt sich dort zu einer neuen Gesamtberechtigung: nun kann das „Projekt X“ von den Usern der „Gruppe A“ und den Usern der „Gruppe B“ gesehen werden.

2 Voraussetzungen

Das aktuelle Berechtigungskonzept auf Datensatzebene ist verfügbar ab Meffert Recruiter Version 7.2.

Da bei jeder Speicherung eines Datensatzes (Person, Firma, Projekt, Aktivität, Dokument) errechnet wird, welche User aufgrund direkter Berechtigungszuordnung(en) oder über Gruppenzuordnung(en) diesen Datensatz sehen dürfen, sind bei größerer Benutzeranzahl und vielen Datensätzen eventuell leicht spürbare Verzögerungen beim Speichern festzustellen.

Dürfen z.B. 10 User alle Personen sehen und haben Sie 100.000 Personen gespeichert, dann entstehen bereits 1 Million Berechtigungsdatensätze für alle Personen (10 User x 100.000 Personen).

Ändert sich die Zuordnung von Benutzern zu Gruppen in der Benutzerverwaltung, müssen alle Berechtigungen neu berechnet werden, um sicherzustellen, dass Wechselwirkungen und gegenseitige Ausschlüsse berücksichtigt werden. Diese Neuberechnung kann, je nach Leistungsfähigkeit des Servers, mehrere Minuten dauern.

Vor dem Hintergrund der höheren Schreiblast und der Anzahl der Datensätze in den Berechtigungstabellen empfehlen wir folgendes:

- Ein sehr leistungsfähiger, dedizierter (=eigenständiger) Datenbankserver mit mehr Arbeitsspeicher, als von Microsoft empfohlen
- Keine Verwendung der Replikation (zumindest nicht über langsame Verbindungen wie z.B. das Internet)

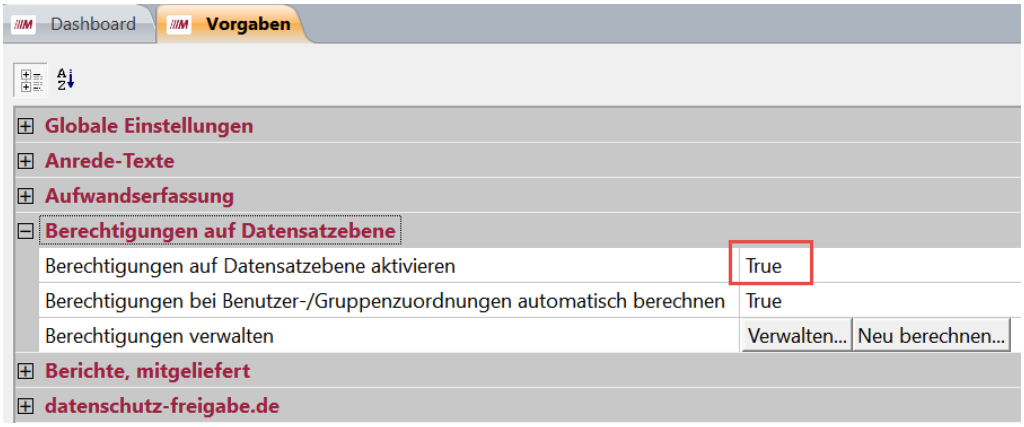
Bitte fragen Sie uns vor Aktivierung der Datensatzberechtigungen. Wir beraten Sie gerne.

3 Anleitung

3.1 Aktivieren und Verwalten von Datensatzberechtigungen

Standardmäßig ist das Berechtigungskonzepts auf Datensatzebene nicht aktiviert, folglich kann jeder Benutzer, der sich an Meffert Recruiter anmelden kann, alle Datensätze (gemeint sind hier die Personen, Firmen, Projekte, Aktivitäten und Dokumente) sehen.

Wünschen Sie, dass Benutzer nur bestimmte Datensätze sehen, können Sie die Berechtigungen auf Datensatzebene in den globalen Einstellungen/Vorgaben aktivieren.



Ist diese Option aktiviert, erscheint in den Masken für Personen, Firmen, Projekte, Aktivitäten und Dokumente ein Button mit einem Schloss.

Über diesen Button kann die Berechtigung für den betreffenden Datensatz eingestellt werden.

Der Button zeigt ein graues, geöffnetes Schloss als Symbol an, wenn keine Einschränkungen am Datensatz existieren. Bestehen Einschränkungen, wird ein rotes, geschlossenes Schloss angezeigt.

Zuvor müssen Sie jedoch in der Benutzerverwaltung Berechtigungen vergeben, diese Funktion nutzen zu dürfen, denn andernfalls erhalten die User beim Klicken auf das Schloss eine Fehlermeldung.

Alle Datensätze, die vor Aktivierung dieser Funktion erfasst wurden, besitzen keine Einschränkungen. Wenn Sie wünschen, dass auch bestehende Datensätze mit bestimmten einheitlichen Einschränkungen versehen werden, wenden Sie sich bitte an unseren Support. Wir können Datenbank-seitig Skripte ausführen, mit denen die Berechtigungen aller Datensätze einmalig gesetzt werden können.

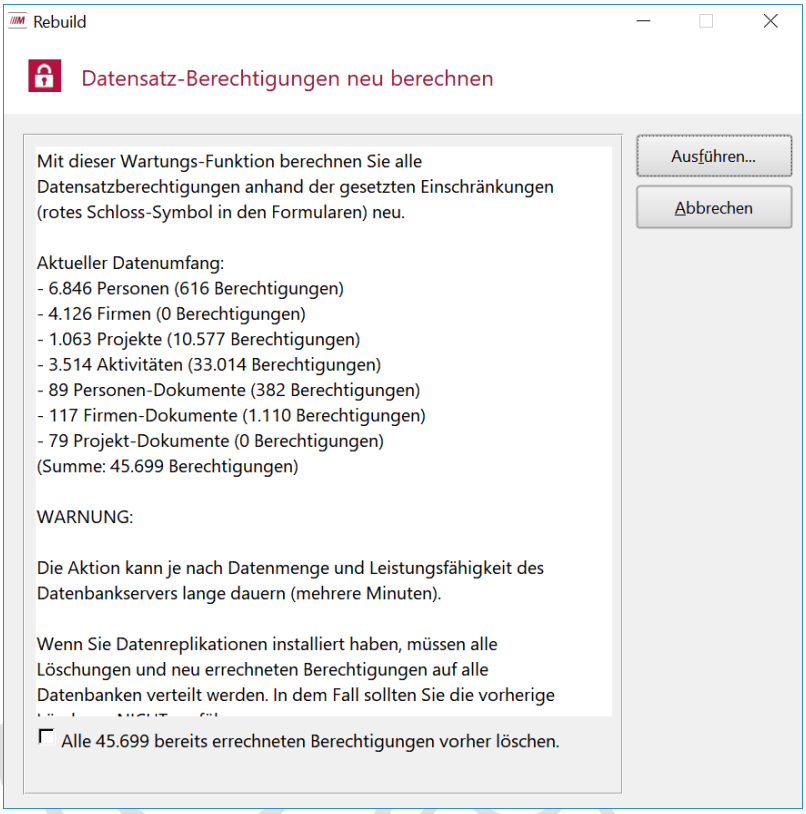
Berechtigungen bei Benutzer-/Gruppenzuordnungen automatisch berechnen
Standardmäßig ist diese Option aktiviert, d.h. die Datenbank berechnet die Datensatzberechnungen im Hintergrund automatisch neu, wenn Sie Benutzer- und Gruppenzuordnungen verändern.
Bei großen Datenmengen kann dies sehr zeitaufwendig sein und möglicherweise kann die Benutzer- und Gruppenzuordnung nicht gespeichert werden. Ist dies der Fall, deaktivieren Sie diese Option und starten die Neuberechnung der Berechtigungen manuell, nachdem Sie die Benutzer-/Gruppenzuordnung abgeschlossen haben.

Berechtigungen verwalten
Klicken Sie auf den Button „Verwalten, um die Datensatzberechtigungen zu löschen und neu zu berechnen. Normalerweise ist das Löschen von Berechtigungen nicht erforderlich und Sie sollten die Löschung auch sehr gut überlegen, weil dadurch große Mengen an Datenänderungen produziert werden, die ggfs. bei Verwendung der Datenbank-Replikation auf alle Abonnenten übertragen werden müssen.

Das Löschen von Berechtigungen ist erforderlich, wenn die Datensatzberechtigungen deaktiviert und nicht mehr verwendet werden soll. Das Deaktivieren alleine löscht nicht die bisher gespeicherten Datensatzberechtigungen.

Neuberechnung der Berechtigungen nach Gruppenzuordnungen
Wenn Sie in der Benutzerverwaltung die Zuordnungen von Benutzern zu Gruppen verändern, dann müssen alle Datensatzberechtigungen neu berechnet werden, da die alle abgeleiteten Berechtigungen von diesen Änderungen betroffen sein können.

Klicken Sie hierzu in der Benutzerverwaltung auf den Button „Recalc Restrictions“. Dieser Button ist nur sichtbar, wenn die Benutzerrechte auf Datensatzebene aktiviert sind. Führen Sie die Neuberechnung bitte erst dann aus, wenn Sie alle Änderungen an den Benutzer- und Gruppenzuordnungen abgeschlossen haben, damit diese Routine, die im Hintergrund auf dem Datenbankserver läuft und viele interne Änderungen erzeugt, nur einmal laufen muss.

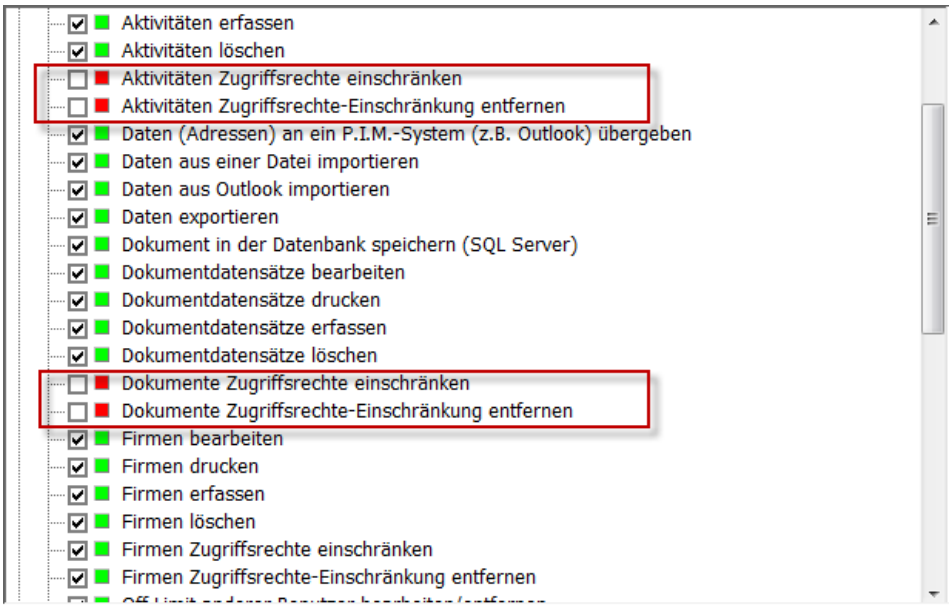


Die Benutzerverwaltung wird Sie auch daran erinnern, die Berechnung neu durchzuführen, wenn Sie Änderungen an den Zuordnungen von Benutzern und Gruppen vorgenommen haben.

Solange keine Änderungen bei den Benutzer- und Gruppenzuordnungen durchgeführt wurden sondern lediglich Berechtigungen bei den Benutzern oder Gruppen geändert wurden, ist keine Neuberechnung der Datensatzberechtigungen erforderlich.

3.2 Funktionsberechtigungen in der Benutzerverwaltung

In der Benutzerverwaltung von Meffert Recruiter können Sie für Benutzer und Gruppen festlegen, wer Zugriffsrechte auf Datensätze einschränken darf, und wer bestehende Einschränkungen auch wieder entfernen darf. Diese Einstellungen werden für Firmen-, Personen-, Projekte-, Aktivitäten- und Dokumentdatensätze getrennt vorgenommen.

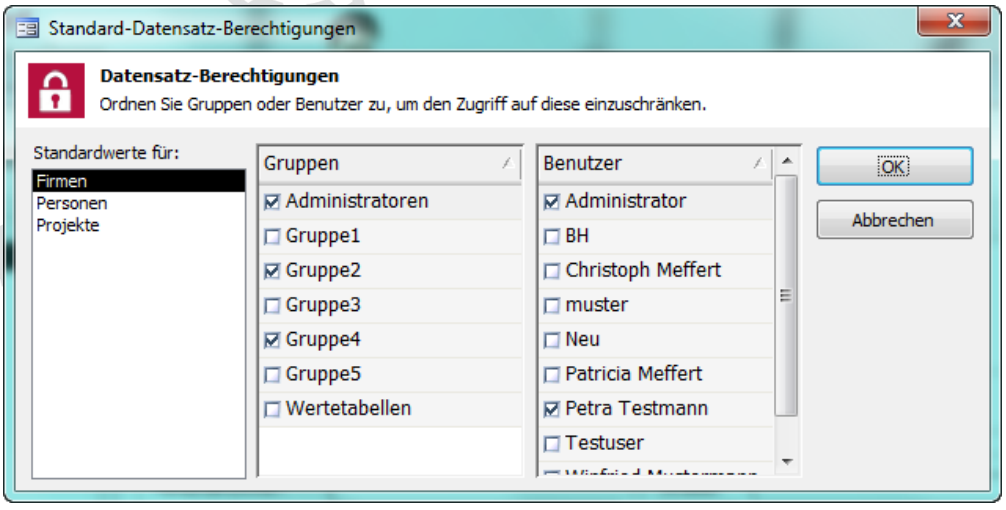


Ist für einen Benutzer keine dieser Berechtigungen zugeordnet, erhält der Benutzer eine Meldung, dass er keine Berechtigung für diese Funktion hat.

3.3 Festlegen von Standardberechtigungen in der Benutzerverwaltung

Das Schloss-Symbol steht nach Aktivierung der Berechtigungen auf Datensatzebene auch in der Benutzerverwaltung zur Verfügung, und zwar auf der Stammdaten-Seite der Benutzer und der Gruppen.

Klicken Sie auf das Schloss, um Standard-Datensatz-Berechtigungen festzulegen.



Die Standard-Einschränkungen werden für Firmen, Personen und Projekte getrennt eingestellt. Wählen Sie in der linken Liste das Wort Firmen, Personen oder Projekte aus und ordnen Sie dann in den beiden rechten Listen die gewünschten Gruppen und/oder Benutzer durch Ankreuzen aus.

Ihre Änderungen werden erst durch Klicken auf OK in der Datenbank gespeichert.

Für Aktivitäten und Dokumente steht keine Standard-Definition zur Verfügung, da diese abhängigen Datensätze ohnehin schon durch die vererbten Einschränkungen ihrer übergeordneten Datensätze (Personen, Firmen und Projekte) beeinflusst werden.

Ist keine Standard-Berechtigung festgelegt, ist das Schlosssymbol grau und offen, ansonsten rot und geschlossen.

Standard-Einschränkungen für Gruppen und/oder Benutzer wirken sich aus, wenn der betreffende Benutzer einen neuen Datensatz in der Datenbank erfasst. Beim Erstmaligen Speichern eines neuen Datensatzes werden automatisch die Einschränkungen auf Benutzer und Gruppen zugeordnet, die sich aufgrund seiner Benutzergruppenzugehörigkeit und seines Benutzernamens in Summe ergeben.
Gehört der Benutzer mehreren Gruppen an, die unterschiedliche Standard-Einschränkungen besitzen, dann erhalten neue Datensätze automatisch alle Einschränkungen aus den zugeordneten Benutzergruppen.

Wenn Standard-Beschränkungen existieren, dann ist das Schlosssymbol schon bei Neueingabe rot und geschlossen.

Empfehlungen / Best Practice:
Wir empfehlen, Standardberechtigungen und auch einzelne Datensatz-Einschränkungen grundsätzlich über Gruppen zu organisieren. So können die Zugriffe bei Bedarf umorganisiert werden. Wechselt ein Mitarbeiter z.B. die Abteilung, hat er durch Zuordnung zu einer anderen Benutzergruppe automatisch Zugriff auf andere Datensätze.

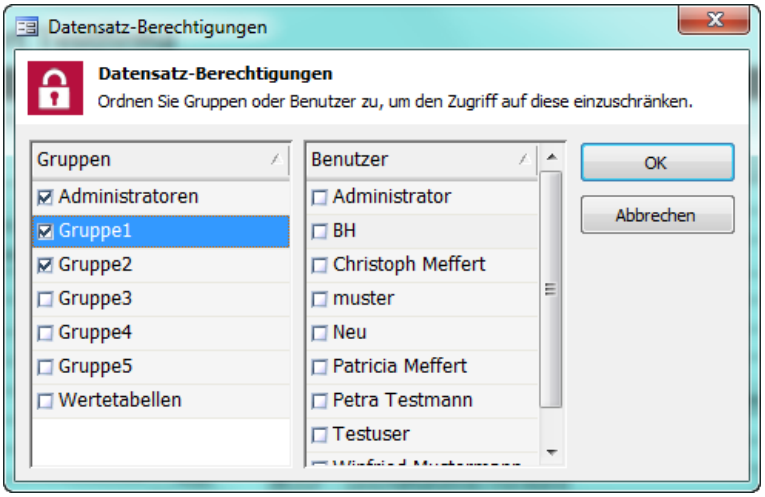
Wir empfehlen auch von Anfang an, eine administrative Gruppe als Standard-Einschränkung festzulegen, z.B. die Gruppe „Administratoren“. So ist sichergestellt, dass es immer eine Gruppe gibt, die Zugriff auf alle Datensätze hat. Andernfalls hätte nicht einmal mehr der Administrator Zugriff auf geschützte Datensätze.

3.4 Festlegen einer Datensatz-Zugriffsbeschränkung

Um einem Datensatz eine Einschränkung hinsichtlich des Datenzugriffs auf bestimmte Benutzer zu definieren, klicken Sie auf den Button mit dem Schloss.

Ein graues, geöffnetes Schloss zeigt an, dass noch keine Einschränkungen definiert sind und der Datensatz folglich für alle Benutzer sichtbar ist. Ein rotes, geschlossenes Symbol zeigt an, dass Zugriffsbeschränkungen definiert sind. Wenn Sie das rote Schloss bei einem existierenden Datensatz sehen, dann gehören Sie zu den erlaubten Benutzern für diesen Datensatz.

Klicken Sie auf das Schloss, um die Berechtigung zu verändern.



Wählen Sie durch Ankreuzen von Gruppen und Benutzernamen aus, wer auf den Datensatz künftig nur noch zugreifen darf. Für alle anderen bleibt der Datensatz unsichtbar.

Klicken Sie auf OK, um die Änderungen in der Datenbank zu speichern.

Haben Sie keine Berechtigung, bestehende Einschränkungen zu entfernen, dann sind die bereits angekreuzten Namen deaktiviert (ausgegraut) und können nicht verändert werden. Haben Sie keine Berechtigung, neue Einschränkungen zu definieren, dann können Sie keine Einträge ankreuzen.

Wenn Standard-Beschränkungen in der Benutzerverwaltung angelegt worden sind, dann ist das Schlosssymbol schon bei Neueingabe eines jeden Datensatzes rot und geschlossen. Eine Veränderung der Vorgabe ist möglich, sofern der Benutzer die Berechtigung dazu hat. Erst nach dem Speichern des Datensatzes kann die Berechtigung geändert werden.

4 Kontakt

Meffert Software GmbH & Co. KG
Daimlerring 4
D-65205 Wiesbaden
www.meffert.de
Email: support@meffert.de