Mitarbeiter, Rollen und Berechtigung

ADITO Software GmbH

Ab Version xRM 2026.4.0 | April 2026

Screenshots

Das UX-Design von ADITO wird kontinuierlich für Sie optimiert. Es kann daher zu Abweichungen bei den Screenshots kommen.

Gendergerechte Sprache

Aus Gründen der besseren Lesbarkeit wird in der Dokumentation das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen beziehen sich gleichermaßen auf alle Geschlechter.

Agenda

Mitarbeiterverwaltung

Rollen- & Berechtigungsverwaltung

Klicken Sie im Dokument auf das ADITO A, um zur Agenda zurück zu kommen.

Mitarbeiter

Mitarbeiter

Ein Mitarbeiter ist ein Nutzer des CRM-Systems.

Der Context „Mitarbeiter“ enthält Verwaltungsfunktionen:

- Mitarbeiter Anlage
- Passwortvergabe
- Rollenvergabe
- Eigenschaften/Dokumente
- Kalenderberechtigung
- User Token

Mitarbeiter

Überblick – Filteransicht

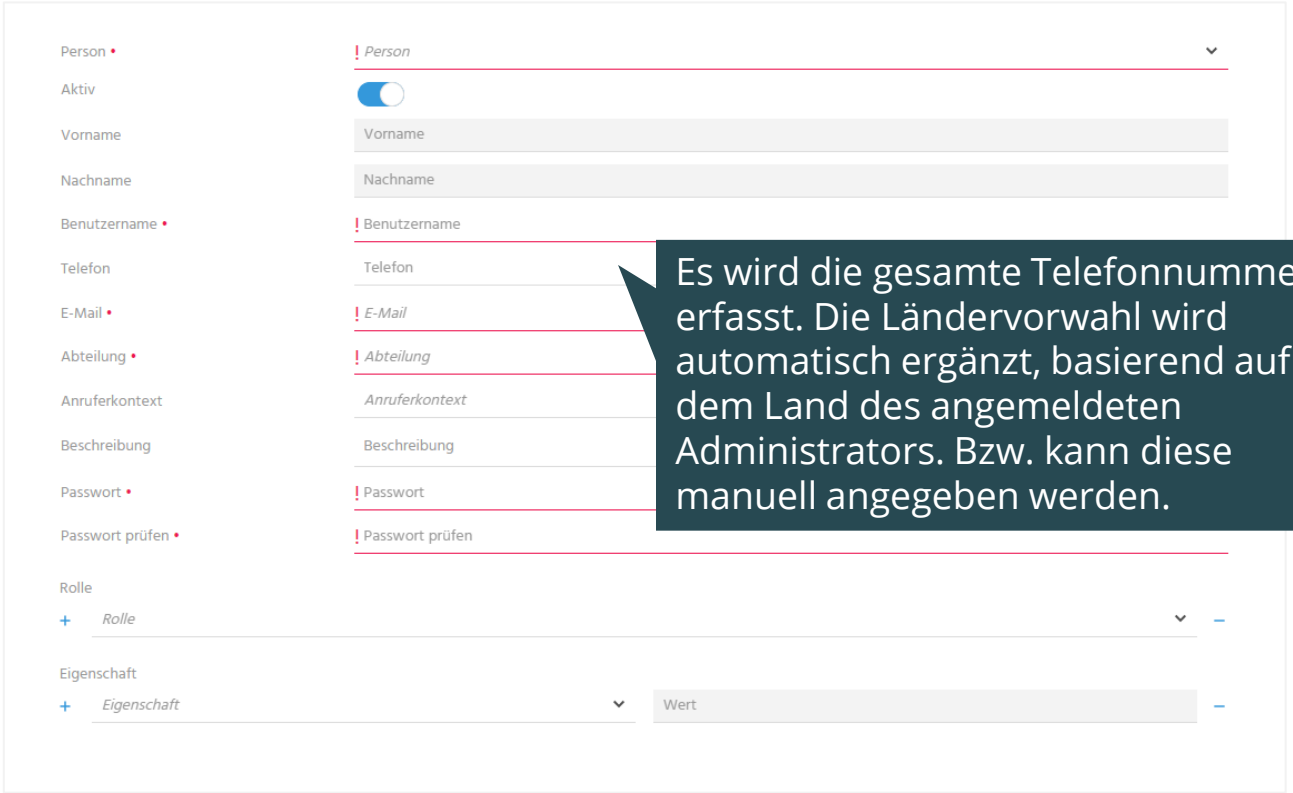
Aktiv				
Ja	Linda	Reiter	Geschäftsleitung	lreiter@meinefirma.adito.de
	Susanne	Lustig	Vertrieb / Innendienst	slustig@meinefirma.adito.de
	Melanie	Hueber	Vertrieb / Aussendienst	mhueber@meinefirma.adito.de
			Service / Aussendienst	snagel@meinefirma.adito.de
			Geschäftsleitung	hobermeier@meinefirma.adito.de
			Vertrieb / Innendienst	hstorbeck@meinefirma.adito.de
Ja	Peter	Pfiffig	Marketing	ppfiffig@meinefirma.adito.de
Ja	Jan	Frohberg	Service / Innendienst	jfrohberg@meinefirma.adito.de
Ja	Tim	Admin	IT	tadmin@meinefirma.adito.de
Ja	Paula	Strauss	Geschäftsleitung	pstrauss@meinefirma.adito.de
Ja	Christian	Pabst	Vertrieb / Aussendienst	cpabst@meinefirma.adito.de
Ja	Harold	Smith	Service	hsmith@meinefirma.adito.de
Ja	Birgit	Leicht	Vertrieb	bleicht@meinefirma.adito.de
Ja	Max	Mustermann	Geschäftsleitung	mmustermann@meinefirma.adito.de
Ja	Lisa	Sommer	Marketing	lsommer@meinefirma.adito.de

Mitarbeiter

Anlage

Voraussetzung:
Der Mitarbeiter ist als Kontakt im CRM angelegt.

Dies ist notwendig, weil die Daten an dem Kontakt z. B. für Platzhalter in E-Mails, Briefen, Serienmail usw. verwendet werden.



Mitarbeiter

Anbindung an Telefonanlage

Telefon: Telefonnummer der Telefonieanlage

Beispiel:

Ein Mitarbeiter verlässt das Unternehmen und die Telefonnummer wird neu vergeben.

1. Der ehemalige User wird inaktiv gesetzt.
2. Der neue aktive User erhält die Durchwahl des ehemaligen Users.

Anbindung an Exchange

Employee-E-Mail-Adresse wird für die Anbindung des Kalenders verwendet. Ändert sich diese, wird auch die Kalender-ID geändert, d.h. der zugeordnete Kalender ändert sich.

Beispiel:

Mitarbeiter ändert seinen Namen.

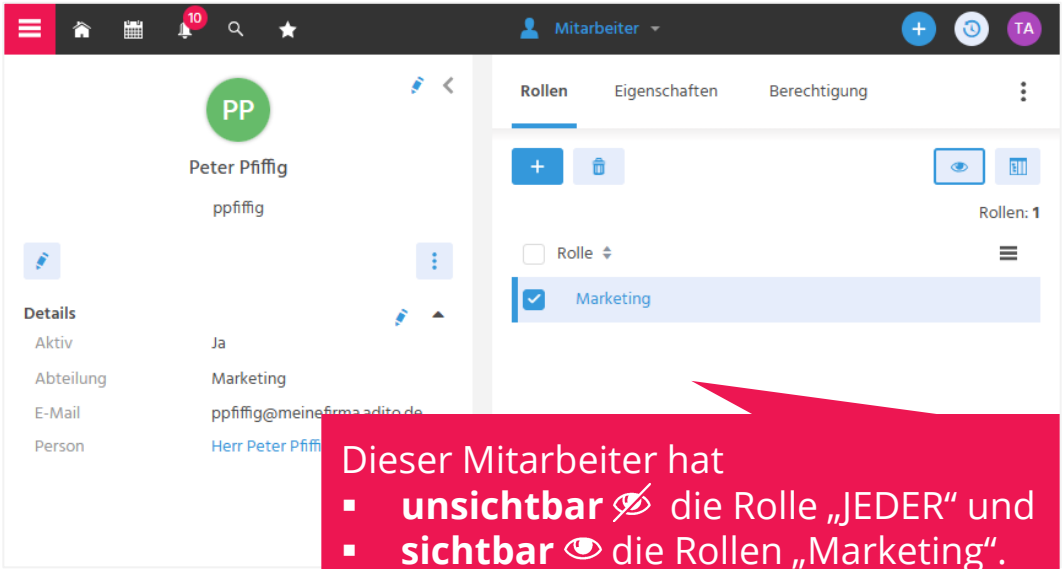
1. Context Kontakt: Namen und Kontakt-E-Mail-Adresse ändern.
2. Context Mitarbeiter: Benutzername und Employee-E-Mail-Adresse ändern.
3. User muss sich neu anmelden.

Hier ist letztlich immer das individuell angepasste Projekt zu betrachten.

Mitarbeiter

Tab „Rollen“

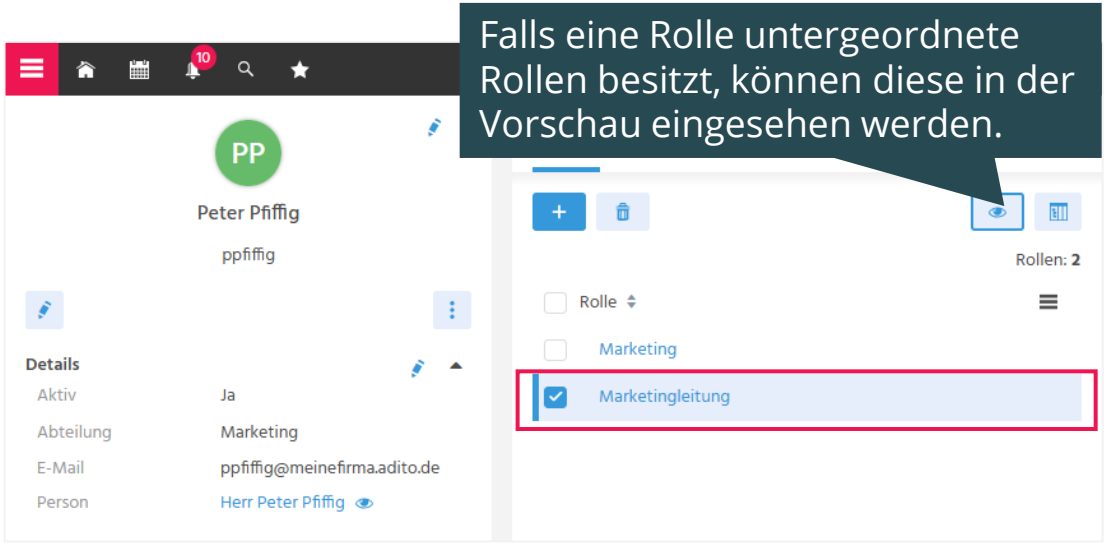
- **Jeder Mitarbeiter erhält die Rolle JEDER,** diese wird **nicht** in der Übersicht angezeigt.
- Die zusätzlich zugewiesenen Rollen werden im **Tab „Rollen“** angezeigt.



Mitarbeiter

Tab „Rollen“

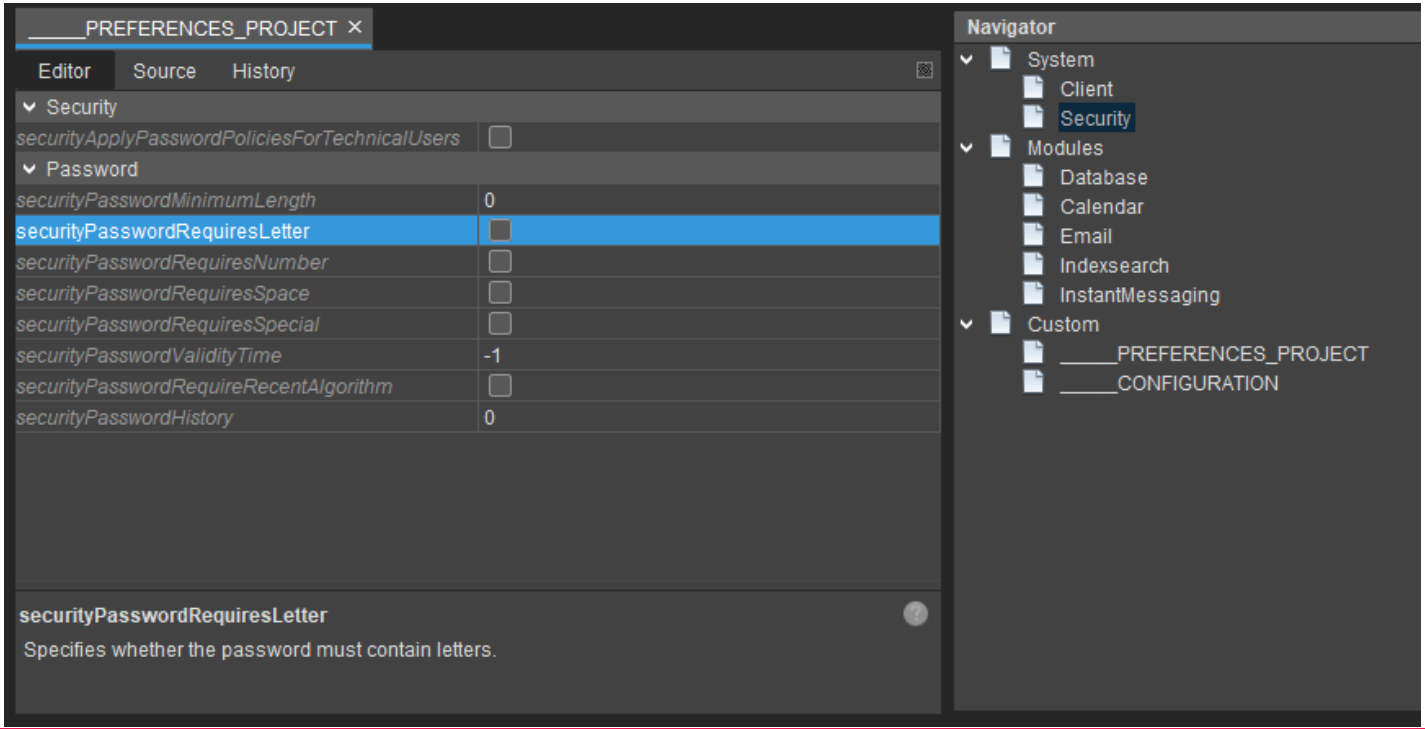
- Weitere Rollen können angelegt werden, um den Mitarbeiter weitere Rollen zuzuweisen.
- Rollen können gelöscht werden, um die Rollen zu entziehen.
- Die Rollen werden mit ODER verknüpft.



Nach einer Änderung der Rollenzuweisung ist ein Client-Neustart bzw. ein erneutes Anmelden des Mitarbeiters erforderlich.

Mitarbeiter

Passwort-Richtlinien im ADITO Designer definieren

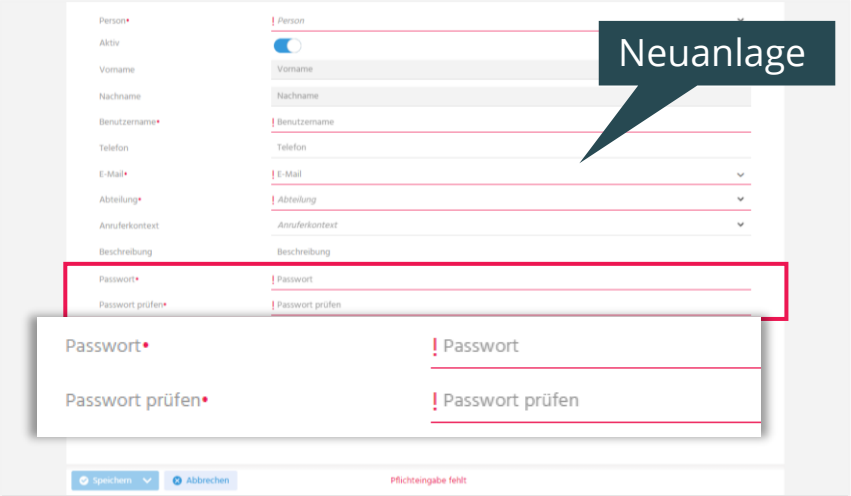


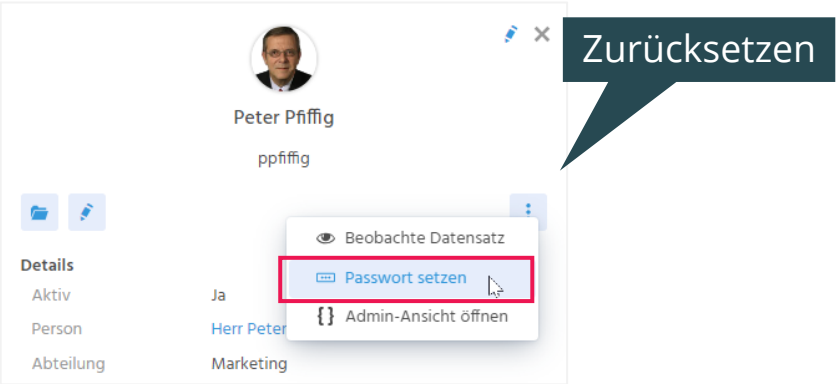
Mitarbeiter | Passwort

Passwort setzen als Administrator

- bei **Neuanlage** eines Mitarbeiters
- **Zurücksetzen**

Bei Mitarbeitern, die über den AD Prozess neu angelegt werden, wird ein zufälliges Passwort gesetzt. **Der Admin muss im Anschluss manuell ein neues Passwort für die Anwender setzen.**



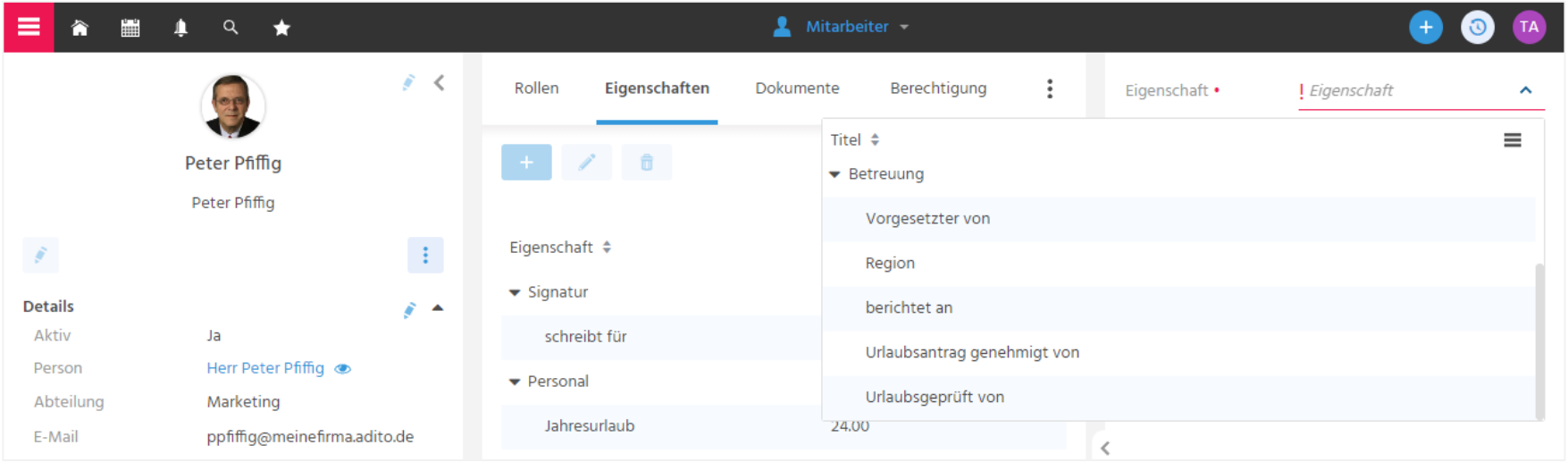


Mitarbeiter | Passwort

Passwort ändern als Mitarbeiter

Mitarbeiter

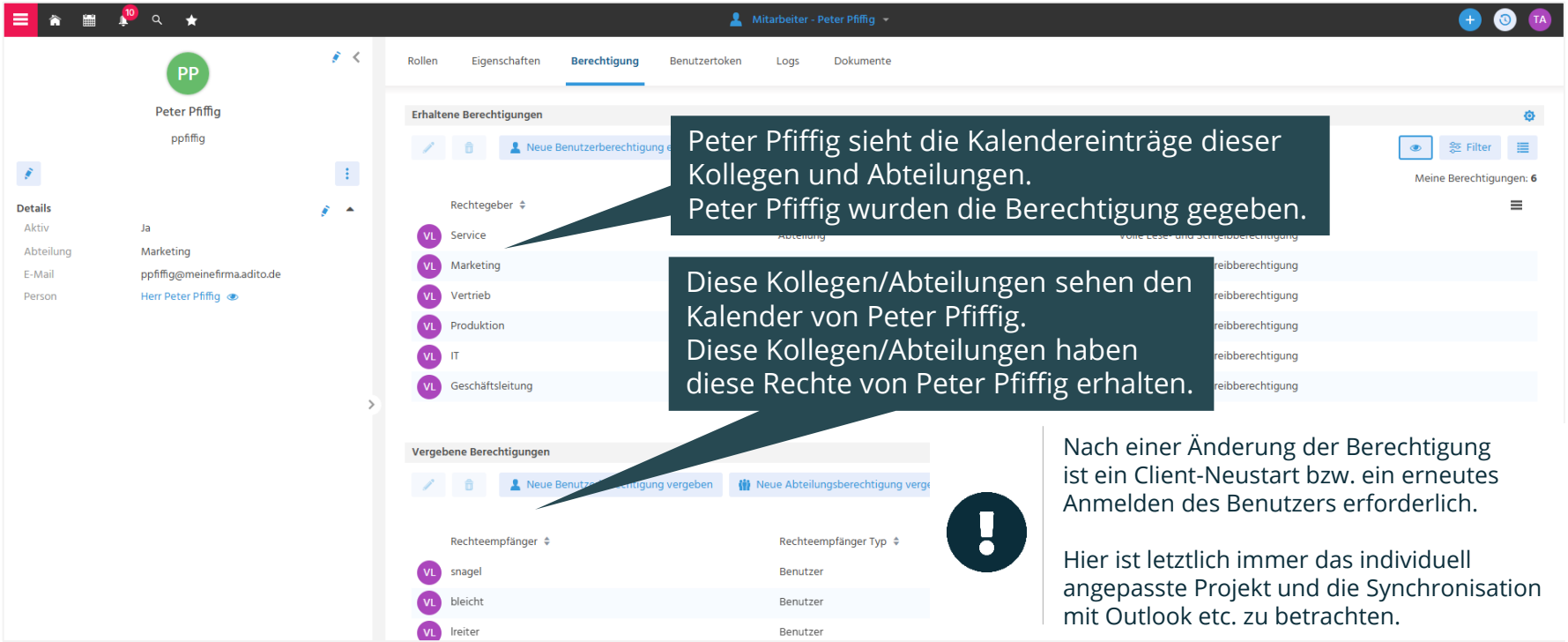
Tab „Eigenschaften“



Hier ist letztlich immer das individuell angepasste Projekt zu betrachten.

Mitarbeiter

Kalenderberechtigung – Tab „Berechtigung“



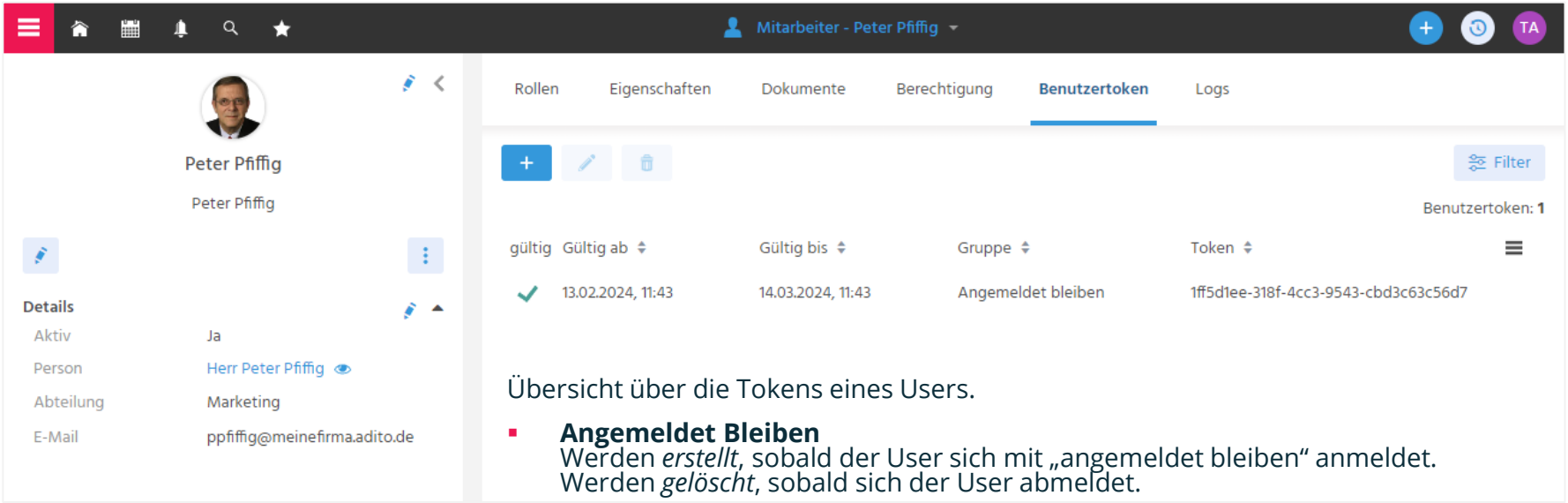
Nach einer Änderung der Berechtigung ist ein Client-Neustart bzw. ein erneutes Anmelden des Benutzers erforderlich.

Hier ist letztlich immer das individuell angepasste Projekt und die Synchronisation mit Outlook etc. zu betrachten.

Kalenderberechtigung

Mitarbeiter

User Tokens

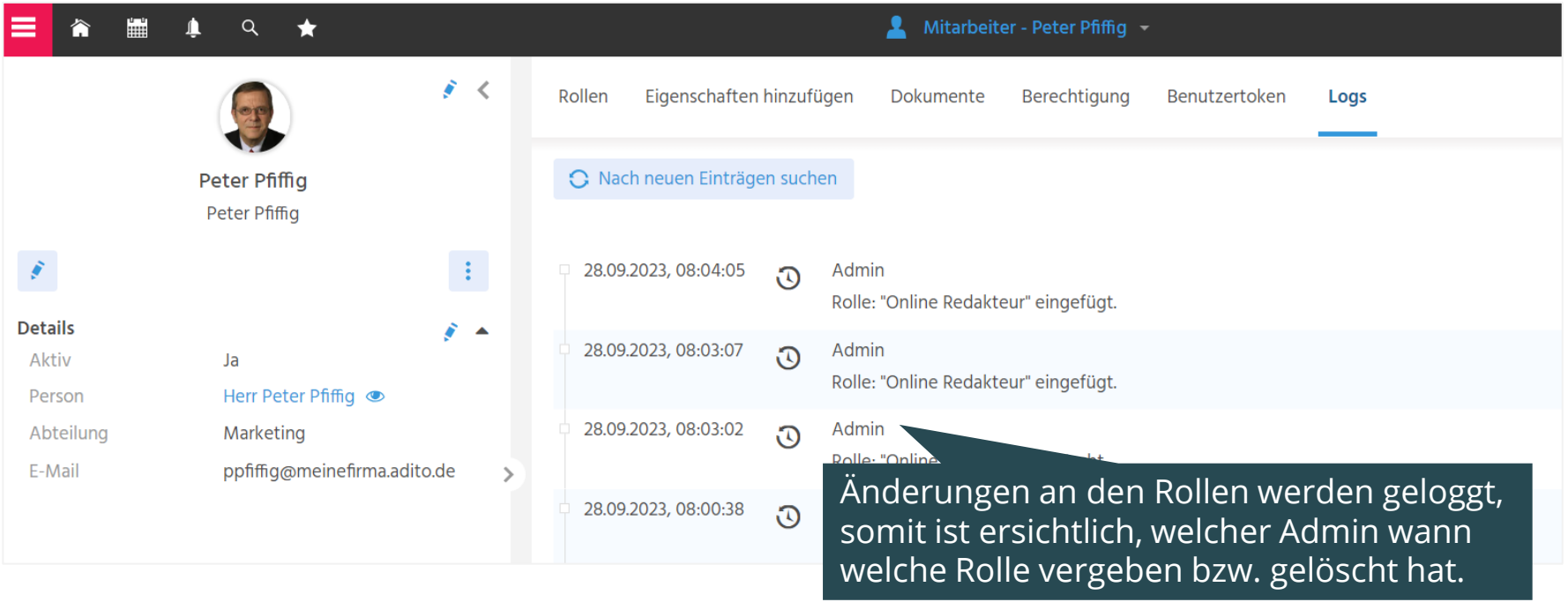


Übersicht über die Tokens eines Users.

- **Angemeldet Bleiben**
  Werden *erstellt*, sobald der User sich mit „angemeldet bleiben“ anmeldet.
  Werden *gelöscht*, sobald sich der User abmeldet.
- **Login Token**
  Werden vom Admin mit Neuanlage erstellt. Zugang über Token nicht mehr möglich, wenn **invalid** oder **Zeitraum abgelaufen**. Aufruf des Web-Clients mit Token: *https://localhost:8443/client/?tokenId=*
  Funktionalität muss in den Client Configurations aktiv sein.

Mitarbeiter

Tab „Logs“



Änderungen an den Rollen werden geloggt, somit ist ersichtlich, welcher Admin wann welche Rolle vergeben bzw. gelöscht hat.

Mitarbeiter

Inaktiv setzten

- Administrator setzt im Mitarbeiterdatensatz das Kennzeichen „Aktiv“ auf inaktiv.
- Bei der nächsten Anmeldung erhält der Mitarbeiter den Hinweis „LoginFailed: Account abgelaufen“

Rollen & Berechtigung

Rollenabhängige Möglichkeiten in ADITO

Was kann mit Rollen abgebildet werden?

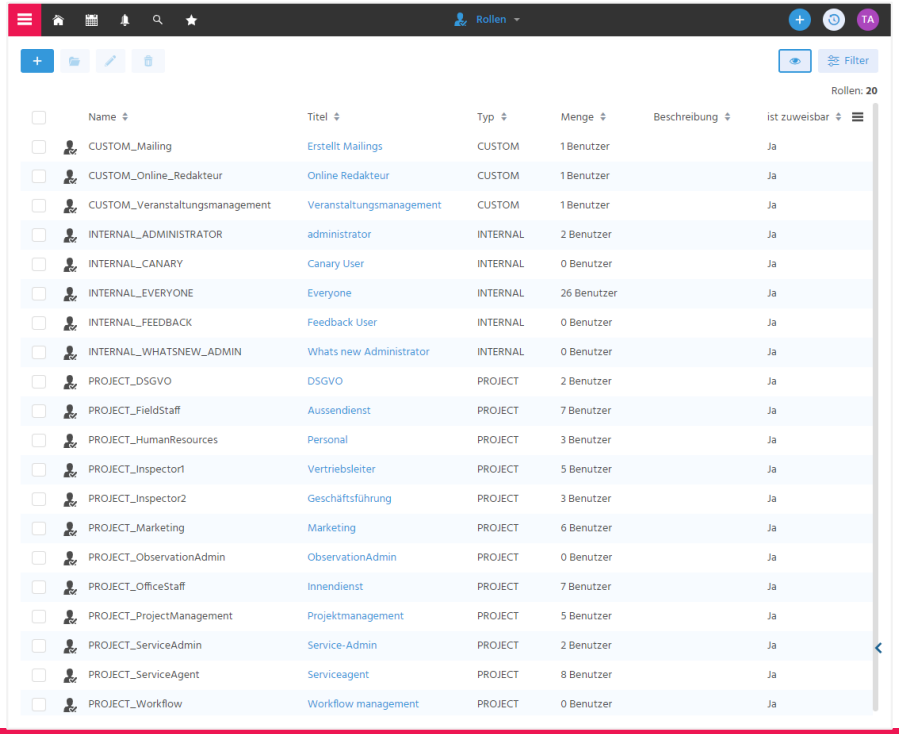
Rollenabhängig kann die **Struktur des Globalen Menüs** abgebildet werden.

Rollenabhängig kann die **Berechtigung** abgebildet werden. D.h. die Anzeige von Entitys, Feldern oder Buttons, sowie die Bearbeitung etc. von Datensätzen.

Rolle

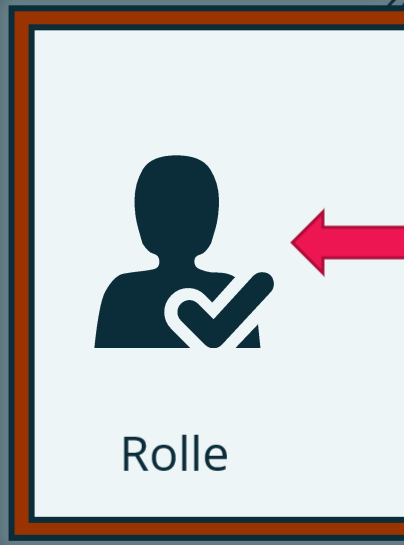
Rollen im „Überblick“

Context „Rollen“ – Filteransicht



- In der Filteransicht erhalten Sie einen Überblick, über alle Rollen, die im System verfügbar sind und die den Mitarbeitern zugewiesen werden können.
- Mit dem **Neuanlage-Button** legen Sie neue Rollen vom Typ CUSTOM an.
- Löschen von CUSTOM Rollen.
- Öffnen Sie die Hauptansicht einer Rolle, um die Berechtigung zu konfigurieren.
- Weitere Informationen zum Typ.
- Weitere Informationen zum Kennzeichen "ist zuweisbar", zur Konfiguration von Rollengruppen.

Rollentypen



CUSTOM_Rollen

- Werden im ADITO Web-Client angelegt.

INTERNAL_Rollen

- Werden vom ADITO Kern ausgeliefert.
- INTERNAL_EVERYONE, INTERNAL_ADMINISTRATOR
- Können für die Menüstrukturierung verwendet werden.

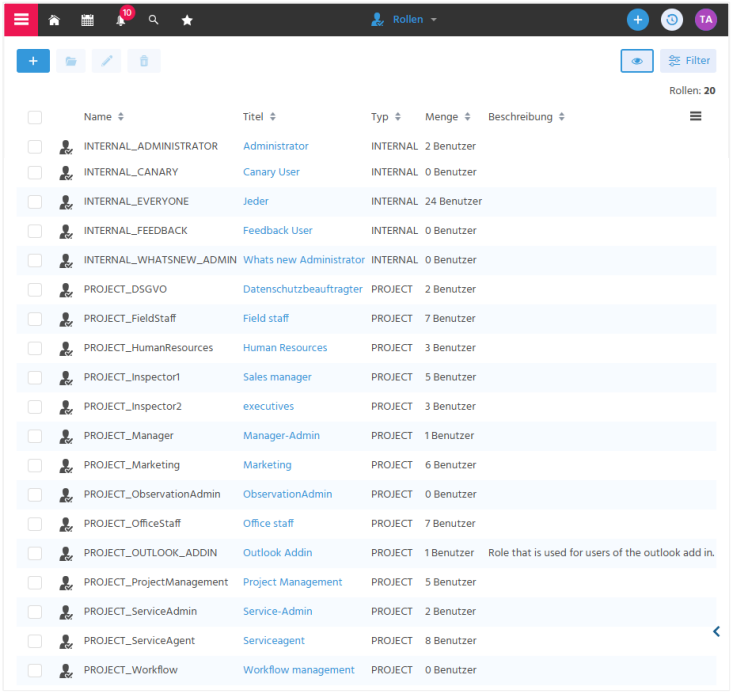
PROJECT_Rollen

- Werden im ADITO Designer angelegt.
- Können für die Menüstrukturierung verwendet werden.

Die **Berechtigungskonfiguration** findet für **alle Rollentypen** im Web-Client statt.

Rollen im xRM

Rollen, die mit dem xRM ausgeliefert werden: Typ „Internal“

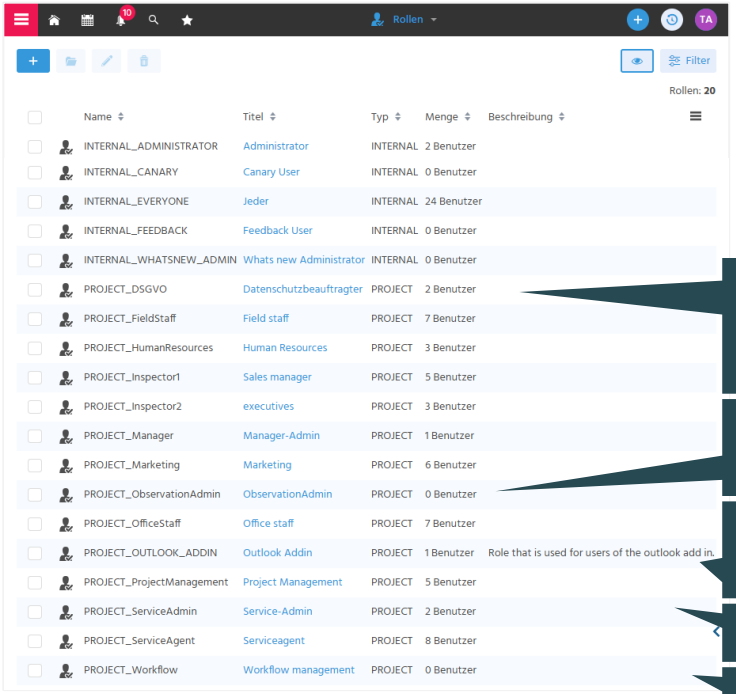


Rollen vom Typ INTERNAL werden von ADITO festgelegt und können nicht verändert werden. Damit werden verschiedene grundlegende Rechte/Funktionen im System abgebildet.

- **INTERNAL_EVERYONE:** Rolle, die grundsätzlich jeder Benutzer hat (diese wird im Mitarbeiterdatensatz im Tab „Rollen“ **nicht angezeigt**).
- **INTERNAL_ADMINISTRATOR:** Rolle mit Berechtigung auf die Entitys zu Rollen & Berechtigung, den Manager, die sensiblen Eigenschaften und die Aktivität.
- INTERNAL_CANARY: Rolle zum Test einer neuen ADITO Version, die in einem speziellen Canary-Bereich bereitgestellt wird.
- INTERNAL_FEEDBACK, INTERNAL_WHATSNEW_ADMIN: (optional) Rollen für die Berechtigung von entsprechenden Contexten, falls diese im System integriert werden.

Rollen im xRM

Rollen, die mit dem xRM ausgeliefert werden: Typ „Project“



Die Rollen „Aussendienst“, „Personal“, „Geschäftsführung“ etc. sind beispielhaft zu betrachten und werden z.T. im Designer verschiedenen Menügruppen zugeordnet.

Bzgl. der Rollen vom Typ „Project“ ist letztlich immer die individuelle Umsetzung im Projekt zur beachten.

User mit der Rolle „Datenschutzbeauftrager“ können im Context „Datenschutzadministration“ Löschkennzeichen verwalten und datenschutzrelevante Eigenschaften definieren.

User mit der Rolle „ObservationAdmin“ können Beobachtungen für andere einstellen und E-Mail Benachrichtigungen für sie aktivieren.

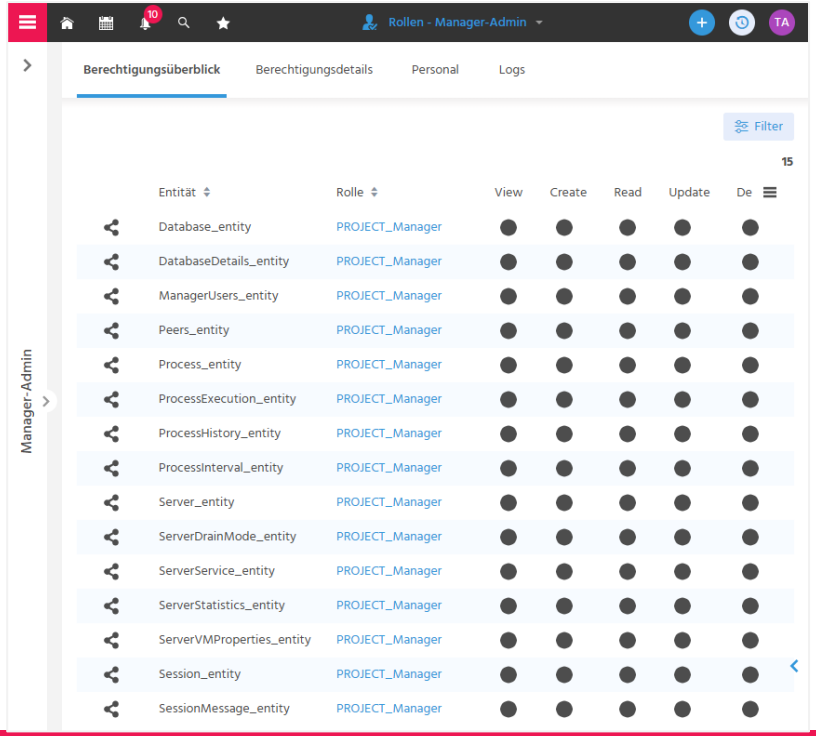
Um das Outlook Add-In nutzen zu können, benötigen User die Rolle „Outlook Addin“, zusammen mit der Rolle „INTERNAL_Webservice“.

Rolle, die den Contexten zur Service Administration zugewiesen ist

Rolle bzgl. Zugang zum Workflow Modeler

Rollen im xRM

Rollen, die mit dem xRM ausgeliefert werden: PROJECT_Manager



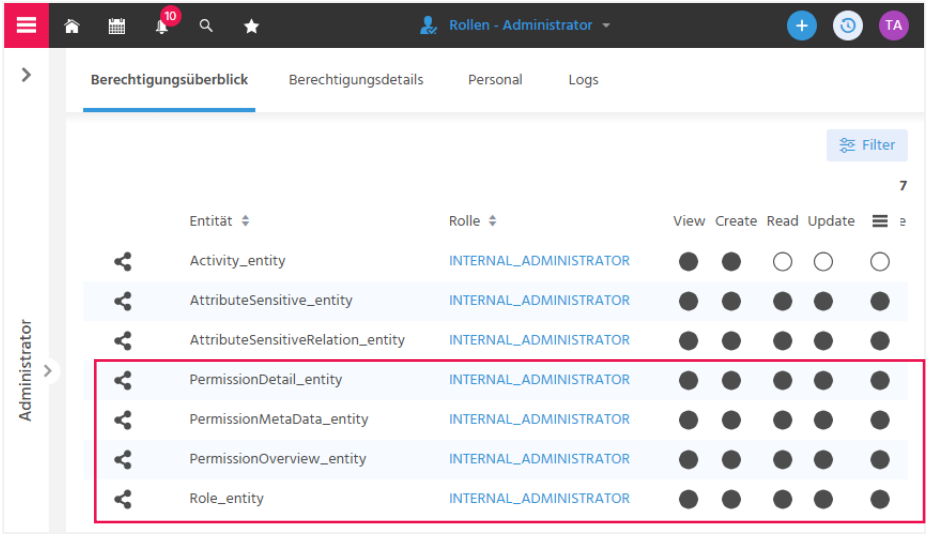
Die Berechtigungen für die Menügruppe „Manager“ sind in der Rolle PROJECT_Manager abgebildet.

Diese muss den Usern zugewiesen werden, die auf den Manager Zugriff haben sollen.

In den Demodaten des xRM wurde Tim Admin diese Rolle zugewiesen, somit kann er die Menügruppe sehen.

Rollen im xRM

Sonderstellung Administrator: Vordefinierte Grundeinstellung der Berechtigung



Der Administrator (INTERNAL_Administrator) hat die **Berechtigung auf die Berechtigungsentitys** im Client. Diese sind:

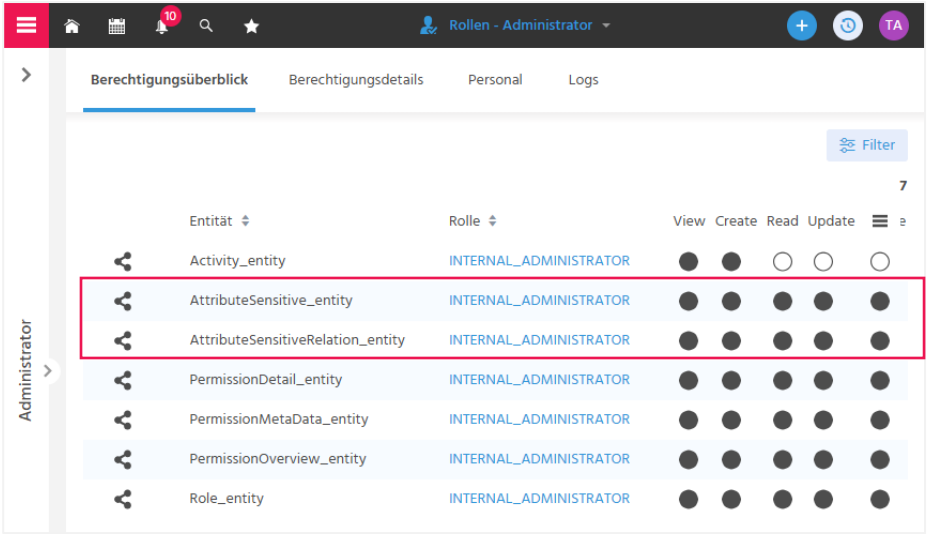
- Rollen & Berechtigung (Zugang zu den Contexten über das Globale Menü)
- Berechtigungsüberblick & Berechtigungsdetail (Tabs in den Contexten Rollen & Berechtigung)

Somit ist sichergestellt, dass im Projekt ausschließlich er darauf Zugriff hat und entsprechend Berechtigungen vergeben kann.

ACHTUNG: Als Administrator müssen Sie darauf achten, dass Sie das Property "usePermission" bei den Berechtigungsentitys nicht entfernen, da sonst alle Benutzer darauf berechtigt wären.

Rollen im xRM

Sonderstellung Administrator: Vordefinierte Berechtigung bzgl. sensibler Eigenschaften



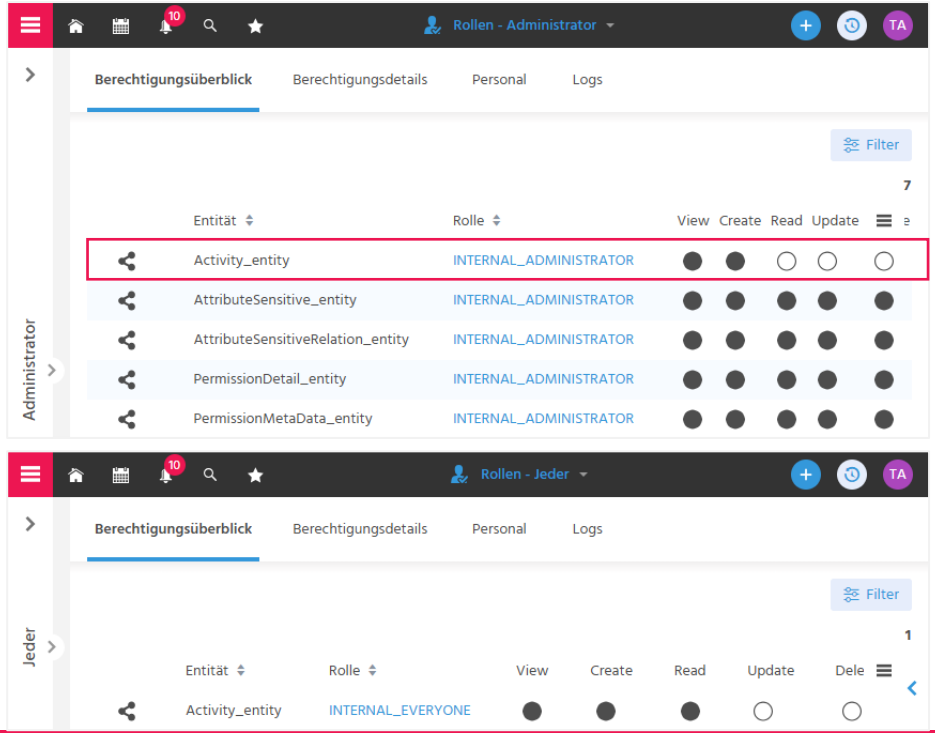
Der Administrator (INTERNAL_Administrator) hat die Berechtigung auf die Entitys, um **sensible Eigenschaften im Client zu erfassen**. Diese sind:

- Die Tabelle „sensible Eigenschaften“ (Tab „Eigenschaften“ in Firma) AttributeSensitiveRelation_entity)
- Das Dropdown für sensible Eigenschaften (AttributeSensitive_entity)

Somit ist im Projekt definiert, das zunächst der Admin darauf Zugriff hat und ggf. weitere Rollen bzgl. sensibler Eigenschaften anlegen und berechtigen kann.

Rollen im xRM

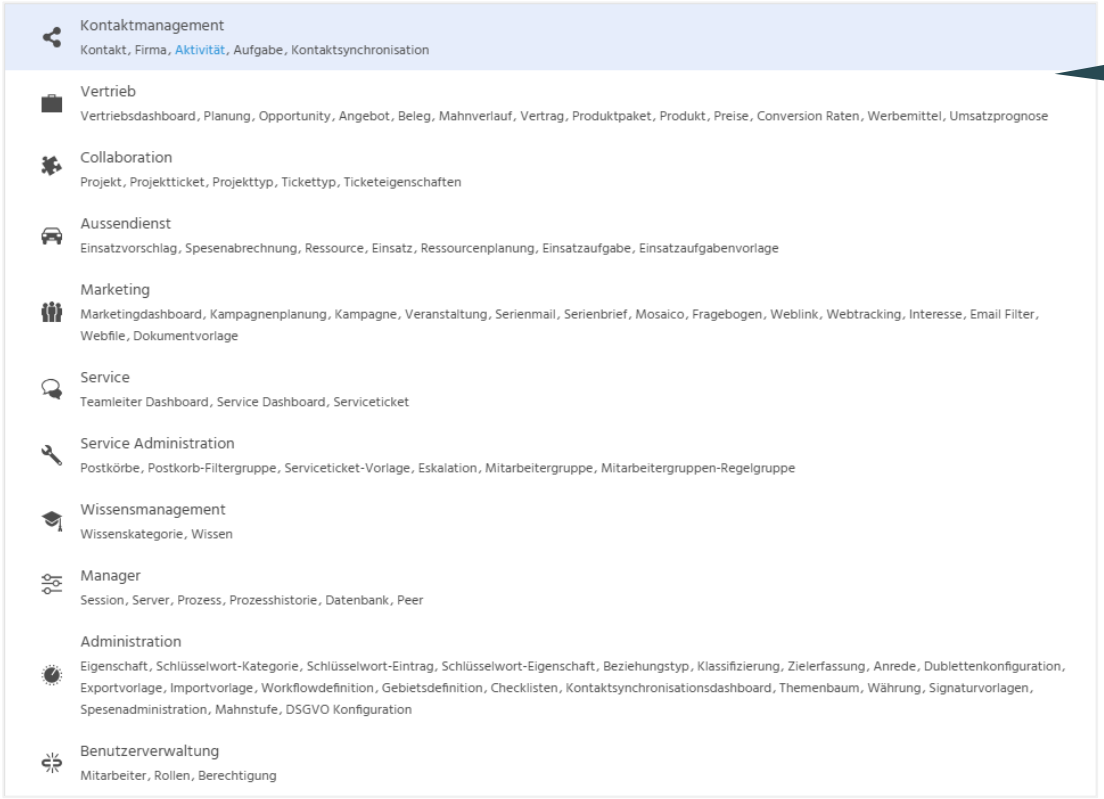
Sonderstellung Administrator: Vordefinierte Berechtigung bzgl. Aktivitäten



Der Administrator (INTERNAL_Administrator) hat die Berechtigung auf das Activity-Entity, um **Aktivitäten der Kategorie „System“** zu bearbeiten oder zu löschen.

Diese Aktivitäten werden vom System erstellt und können von jemandem mit der Rolle „Jeder“ (INTERNAL_Everyone) nicht bearbeitet werden. Dies ist jeweils in der Berechtigung dieser beiden Rollen als Bedingung an den Rechten erfasst.

Struktur des Globalen Menüs

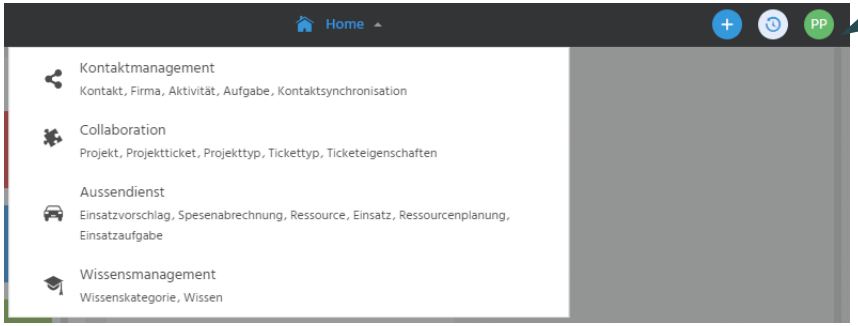


Beispiel: Aufteilung/Gruppierung aller möglichen Contexte im Globalen Menü

- Was muss JEDER sehen können?
- Was benötigt nur der Administrator?
- Was benötigt man innerhalb von Abteilungen?
- Was benötigt man für spezielle Prozesse?

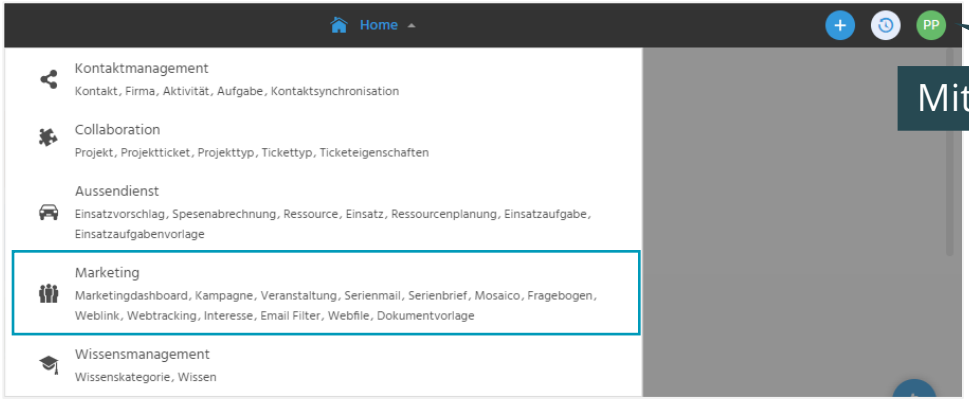
Struktur des Globalen Menüs

Beispiel



Mitarbeiter hat die Rollen JEDER.

In ADITO xRM sind diese Menügruppen der Rolle JEDER zugeordnet.



Mitarbeiter hat die Rollen JEDER und Marketing.

In ADITO xRM ist die Menügruppe Marketing mit ihren Contexten der Rolle Marketing zugeordnet.

Struktur des Globalen Menüs

Vorgehen

Im Applicationmodell legen Sie fest, wie die Menüstruktur des Globalen Menüs aussieht, die ein Benutzer anhand seiner Rollen sieht. Dazu können Sie Rollen vom Typ INTERNAL oder PROJECT verwenden.

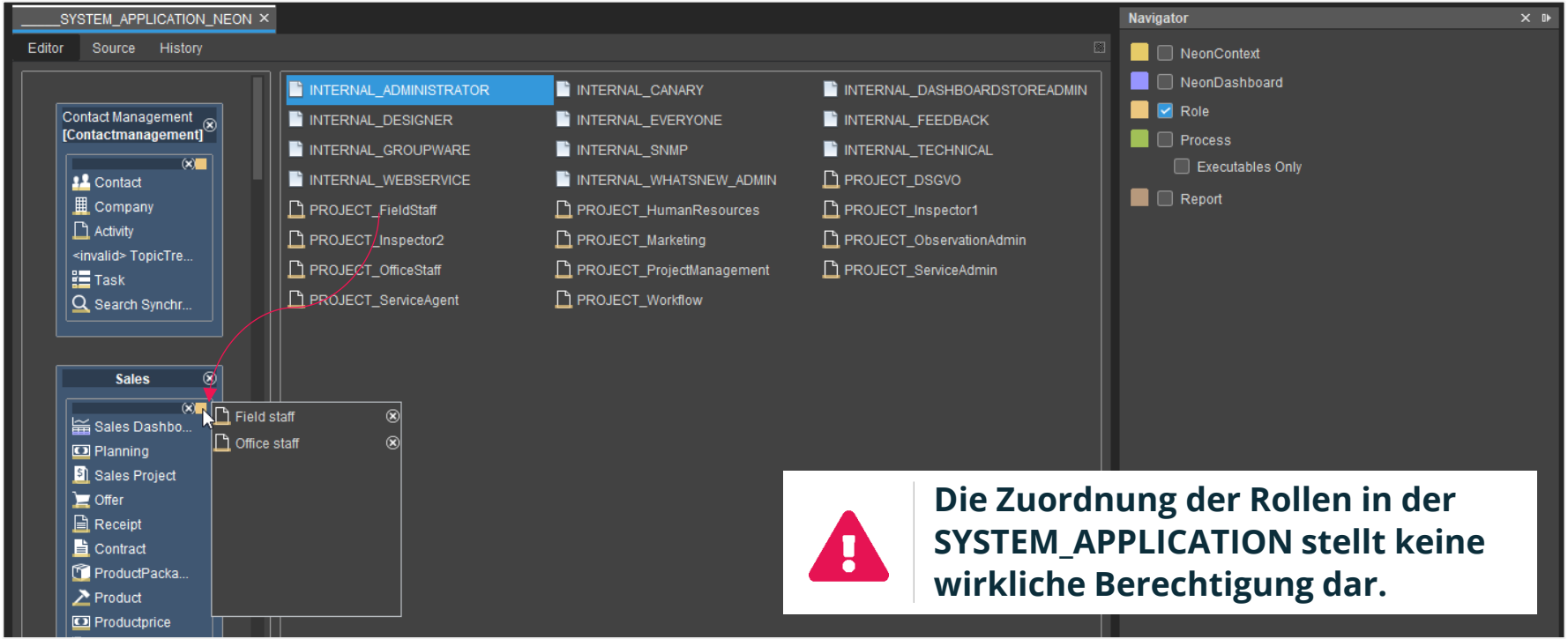
Die Rollen werden den Menügruppen zugeordnet. Dabei kann eine Menügruppe auch nur einzelne Contexte beinhalten (siehe nächste Folie).

Die allg. Vorgehensweise zur Erstellung und Zuordnung der Rollen im Designer finden Sie im Customizing Manual.

Es ist aber auch möglich, dass Sie im Applicationmodell nur die Rolle "Jeder" verwenden und allen Menügruppen zuordnen. Somit können Sie die Menüstruktur des Globalen Menüs über die CUSTOM-Rollen in der Berechtigungsverwaltung im Web-Client .

Struktur des Globalen Menüs

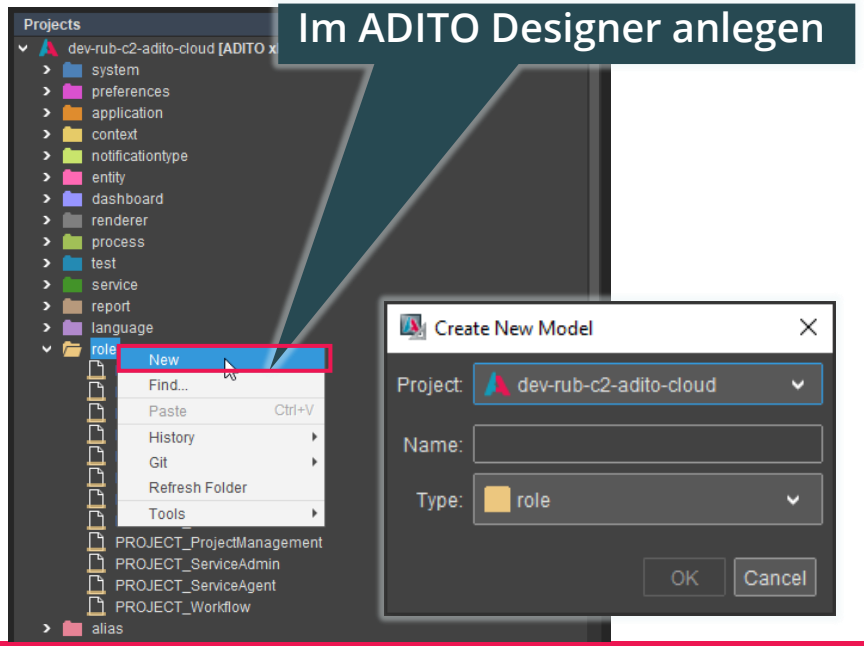
Per Drag&Drop können den Menügruppen Rollen zugeordnet werden

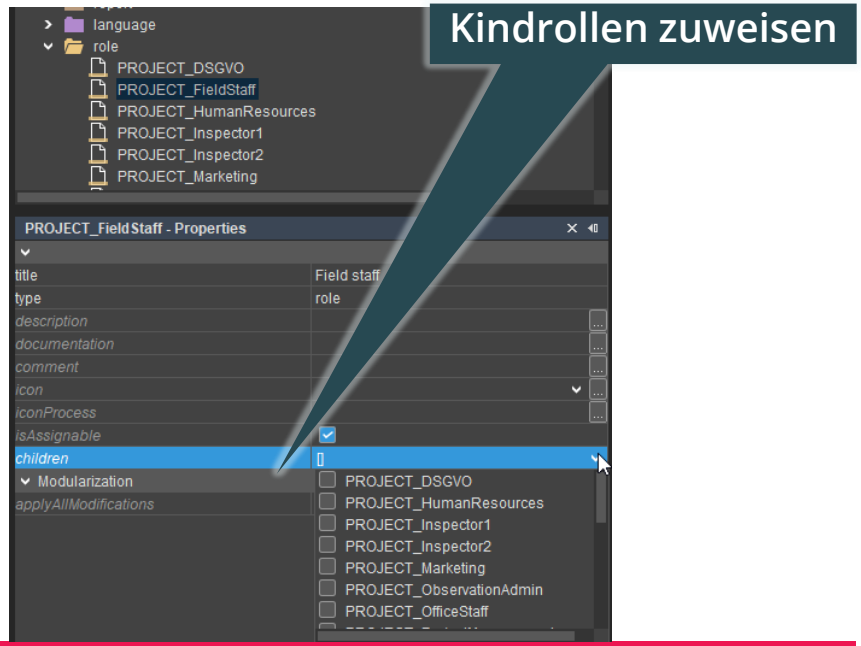


Die Zuordnung der Rollen in der SYSTEM_APPLICATION stellt keine wirkliche Berechtigung dar.

PROJECT_Rollen

Dieser Typ kann von Ihnen **im Designer** innerhalb des Projekts angelegt werden und ist somit auch im Git-Projekt gespeichert. Diese Rollen können im Designer den jeweiligen Menügruppen (Kontaktmanagement, Vertrieb, Marketing, etc.) im Applicationmodell zugeordnet und für die Definition der Menüstruktur verwendet werden. Zudem wäre wenn notwendig eine Verwendung im JDito-Code möglich.





Was können Rollen abbilden?

Rollen können...

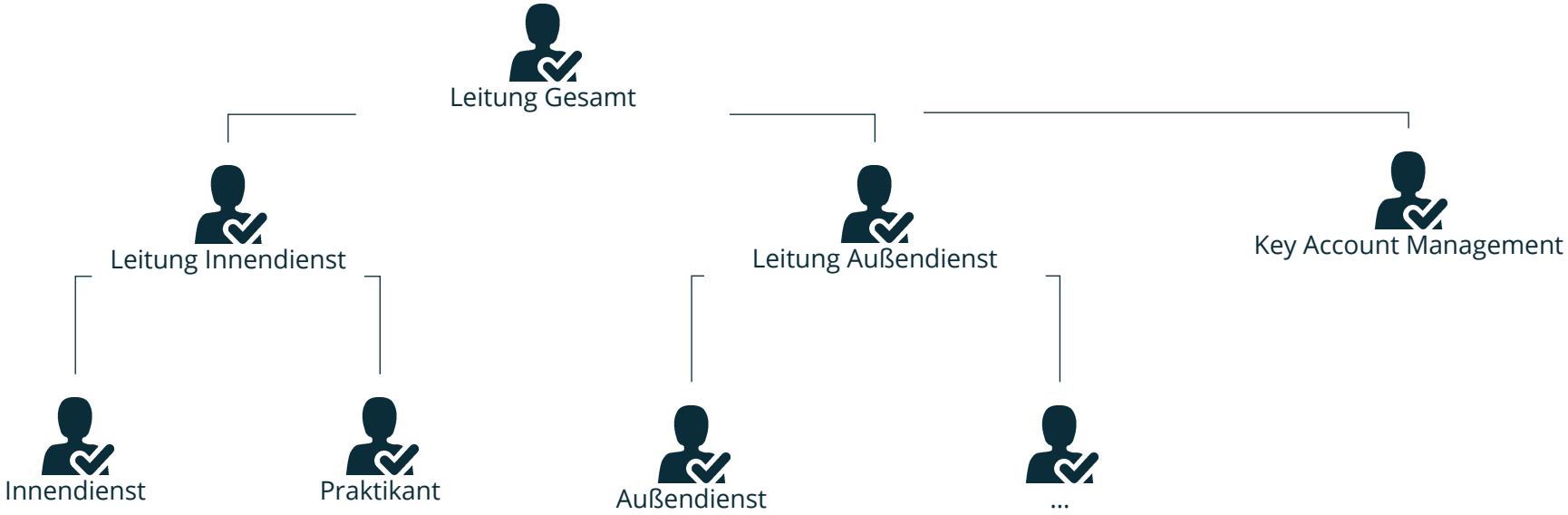
- **Personas** abbilden, die die Rollen der Mitarbeiter darstellen (Rollengruppen*).
- **Prozesse** abbilden, die die Personas durchführen können (Rollengruppen*).
- **Funktionen** und **Filter** abbilden, die zur Durchführung dieser Prozesse benötigt werden.

*Wieso spricht man von Rollengruppen?

Personas und Prozessrollen werden auch als Rollengruppen bezeichnet, da bei ihnen die Berechtigungen nicht direkt verlinkt werden, sondern sie ihre Rechte über eine Gruppe von Kindrollen erhalten. Es ist aber auch möglich, die Funktions- oder Filterrollen in der Personarolle zu gruppieren, ohne Prozessrollen zu verwenden.

Was können Rollen abbilden?

Personas in Organigrammen z.B. Abteilung Vertrieb



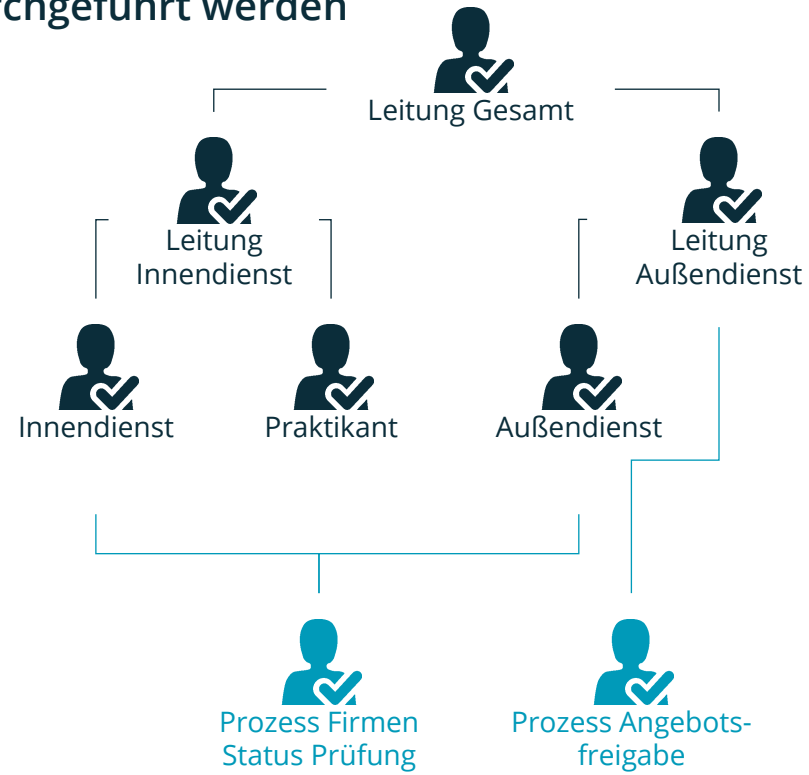
Was können Rollen abbilden?

Prozesse (Arbeitsabläufe), die von Personas durchgeführt werden

Beispiele:

- Prozess Firmen Status Prüfung
- Prozess Urlaubsgenehmigung
- Prozess Umsatzauswertung
- Prozess Umsatzplanung
- Prozess Angebots Prüfung
- Prozess Produktanlage
- ...

Die Prozess-Rollen werden an die Personas vererbt, die den jeweiligen Prozess durchführen können sollen.



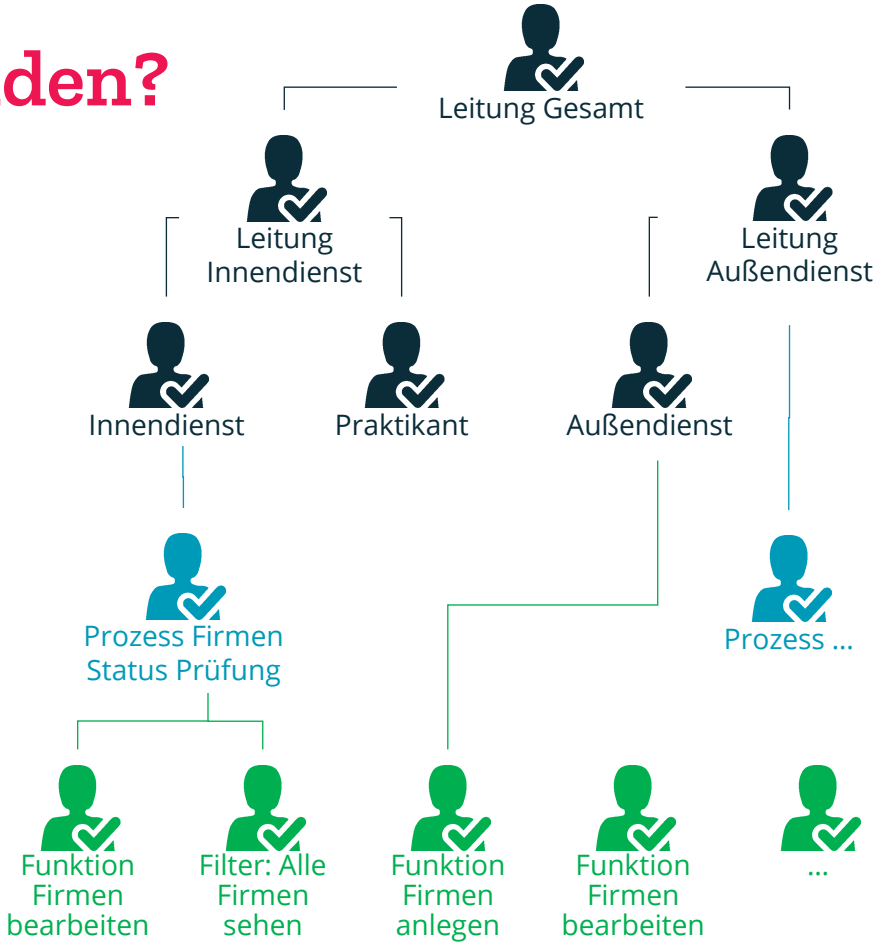
Was können Rollen abbilden?

Funktionen und Filter

Beispiele:

- Filter: Alle Firmen sehen
- Filter: Firmen meiner Gebiete sehen
- Funktion Firmen anlegen
- Funktion Firmen bearbeiten
- Funktion Firmen löschen
- Funktion Status sehen
- Funktion Status bearbeiten
- …

Die Funktions- bzw. Filter-Rollen werden an die Prozess-Rollen oder Personas vererbt.



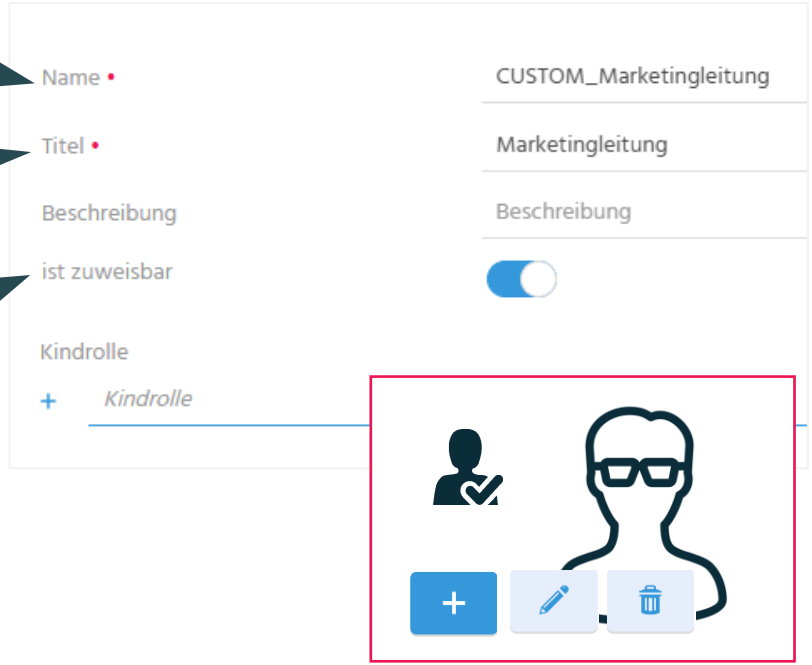
CUSTOM_Rollen

Im ADITO Web-Client anlegen

Der Name ist der eindeutige Schlüssel der Rolle und kann somit nur einmalig vergeben werden. Er wird automatisch um die Bezeichnung des Typs ergänzt.

Der Titel ist die Bezeichnung der Rolle, die bspw. bei der Vergabe für den Mitarbeiter angezeigt wird.

Das Kennzeichen „ist zuweisbar“ muss aktiv sein, um diese Rolle einer anderen Rolle als Kindrolle zuweisen zu können.



Wie lassen sich Rollen „vererben“?

Eltern- / Kind-Rollen

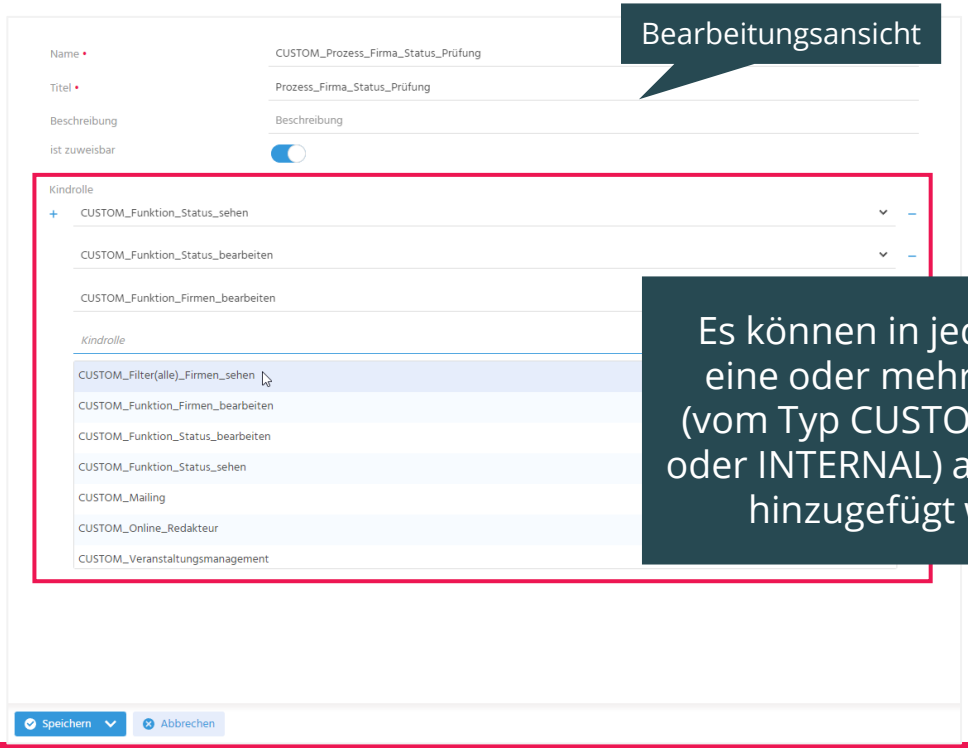
Bedingungen:

- Mit dem Kennzeichen **Is assignable (ist zuweisbar)** wird eine Rolle als Kinderrolle für andere zur Verfügung gestellt und kann ihre Berechtigungen an die übergeordnete Rolle übergeben.
- CUSTOM-Rollen können im Client als Kind-Rollen verwendet werden und CUSTOM-, PROJECT- oder INTERNAL-Rollen zugewiesen bekommen.
- PROJECT-Rollen können im Designer als Kind-Rollen verwendet werden und diese zugewiesen bekommen.

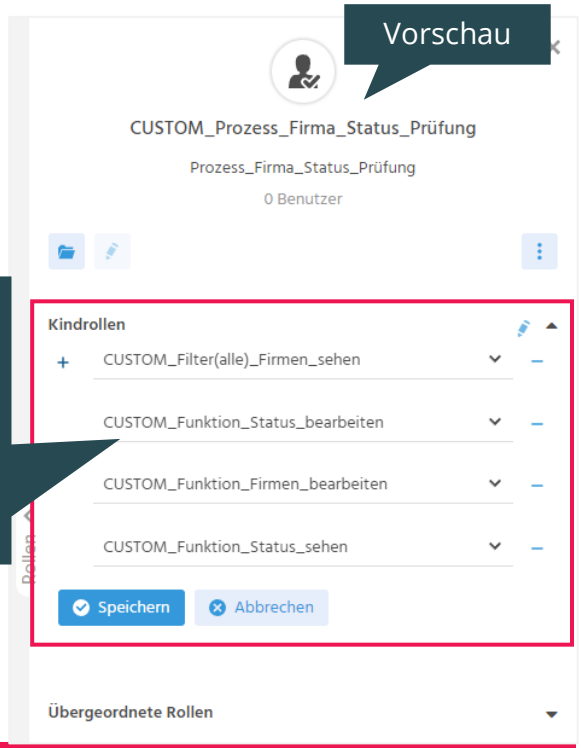
- Die Rollen werden mit ODER verknüpft. **D.h. es wird nicht „vererbt“ sondern „geklammert“.**
- Somit erhält jemand "quasi das Maximum" aller Berechtigungen, die er über die Rollen bekommt.

Über- u. untergeordnete Rollen

Kind-Rollen zuweisen im Web-Client für CUSTOM-Rollen

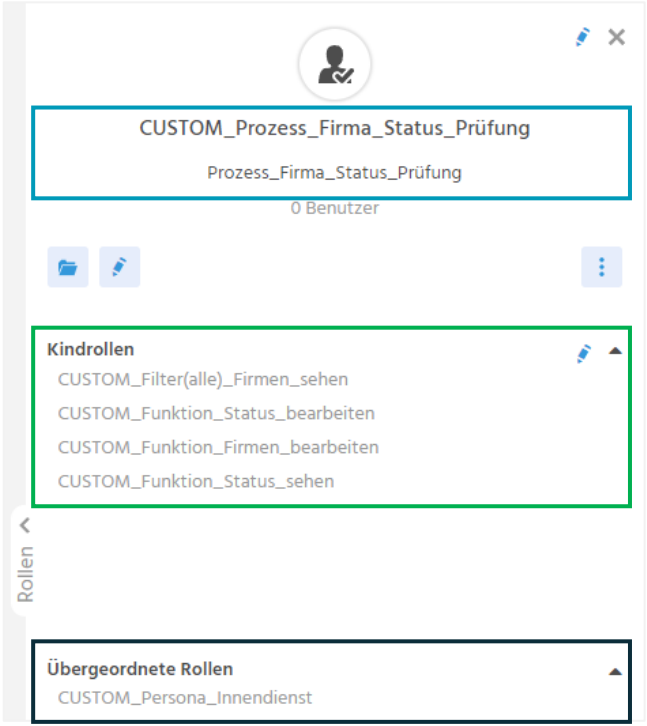


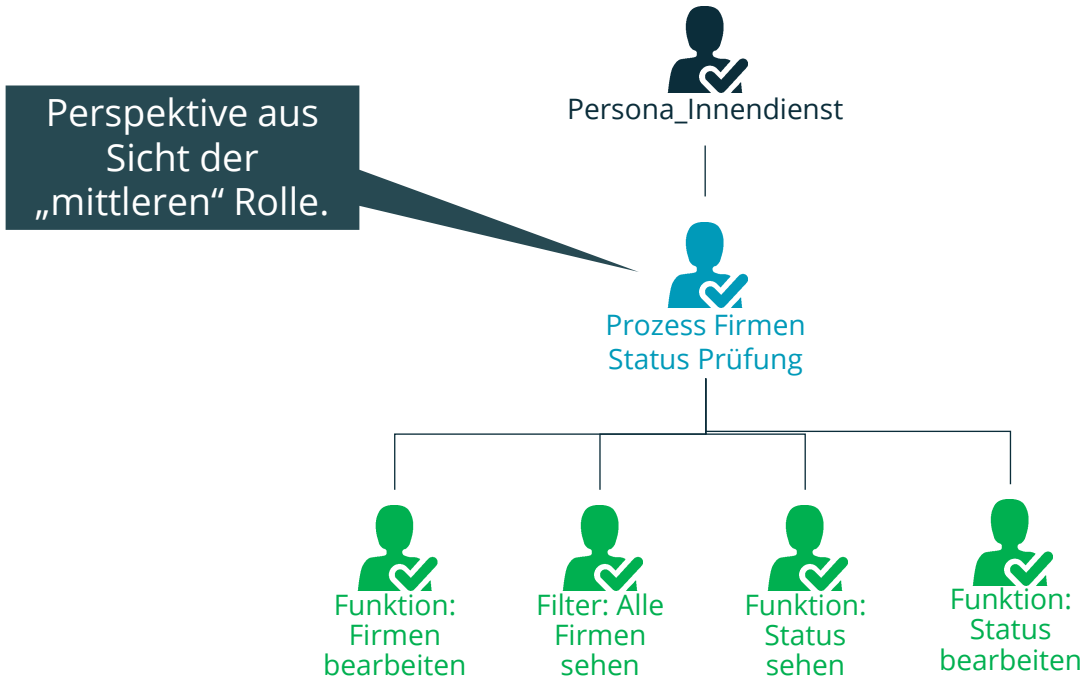
Es können in jeder Ansicht eine oder mehrere Rollen (vom Typ CUSTOM, PROJECT oder INTERNAL) als Kindrollen hinzugefügt werden.



Über- u. untergeordnete Rollen

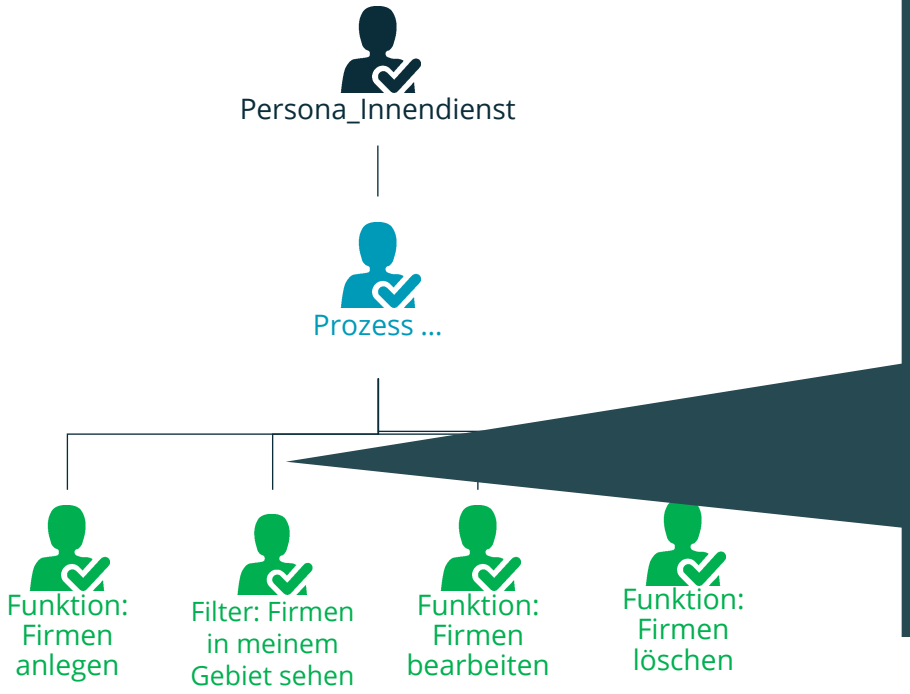
Übersicht in der Vorschau





Über- u. untergeordnete Rollen

Gruppierung der Rollen

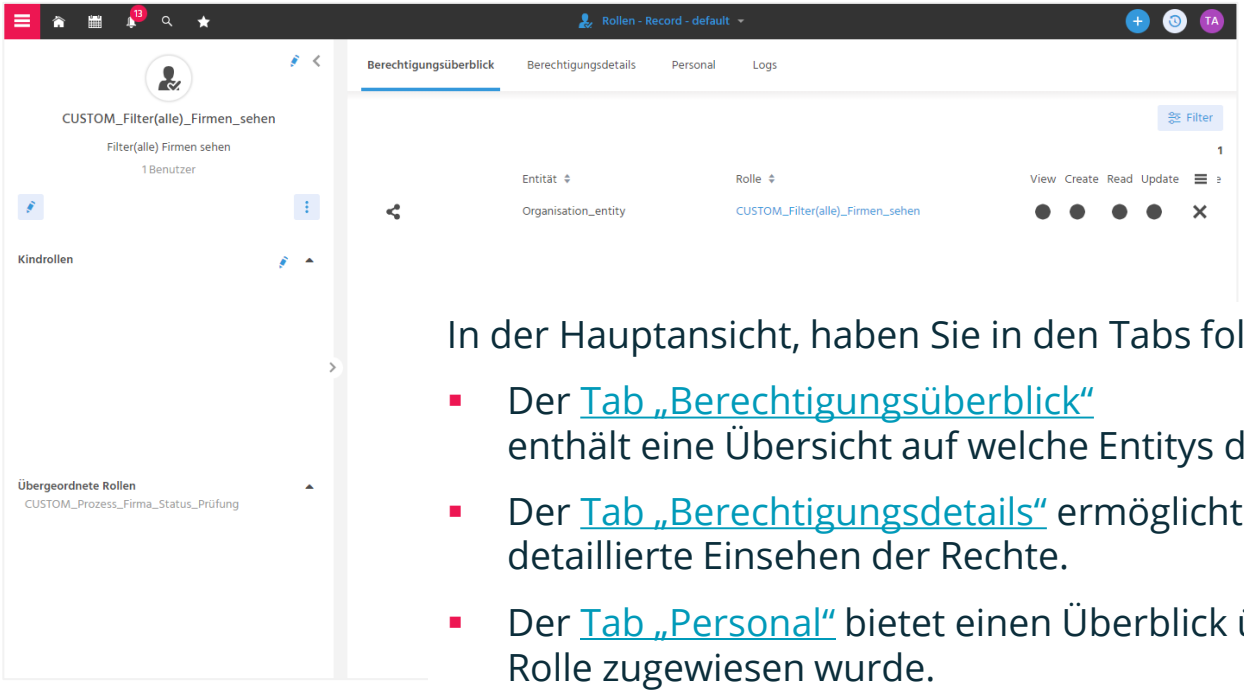


Nutzt eine Rollengruppe die eingeschränkte Sicht auf Datensätze, kann bei den Rechten Bearbeiten und Löschen auf die Einschränkung verzichtet werden, außer es werden für diese Rechte andere Einschränkungsbedingungen benötigt.

Beispiel:
Die Rolle sieht (READ) nur Firmen aus dem ihr zugeordnetem Gebiet. Somit kann bei den Rechten UPDATE und DELETE auf die Einschränkung durch die Kondition verzichtet werden, da die Rolle nur bearbeiten oder löschen kann, was sie sieht.

Context „Rollen“

Hauptansicht



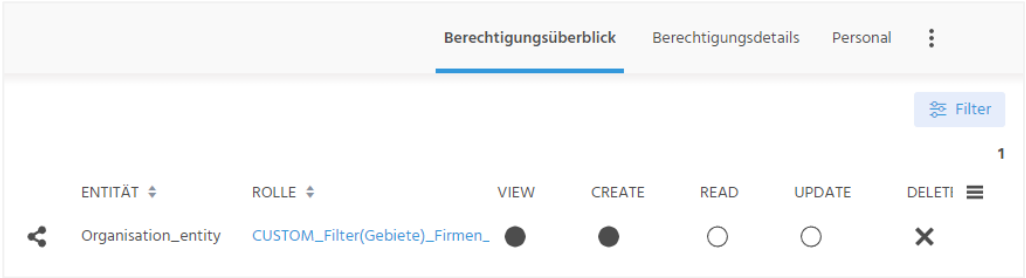
In der Hauptansicht, haben Sie in den Tabs folgende Funktionen:

- Der Tab „Berechtigungsüberblick“ enthält eine Übersicht auf welche Entitys diese Rolle berechtigt ist.
- Der Tab „Berechtigungsdetails“ ermöglicht die Konfiguration und das detaillierte Einsehen der Rechte.
- Der Tab „Personal“ bietet einen Überblick über die User, denen diese Rolle zugewiesen wurde.

Context „Rollen“

Tab „Berechtigungsüberblick“

- In den Spalten VIEW und CREATE werden die Rechte auf **Entityebene** angezeigt. Somit wird die Anzeige der Views des Entitys gesteuert und die Neuanlage von Datensätzen.
- Die Spalten READ, UPDATE und DELETE betreffen die **Datensatzebene**. Damit wird gesteuert, welche Datensätze gesehen, bearbeitet oder gelöscht werden dürfen.
- Mit Hilfe des **Icons** ist ersichtlich, welcher **Berechtigungsstatus** hinterlegt ist:
  - ● Kreis (voll): ist immer erlaubt
  - ○ Kreis (leer): ist bedingt erlaubt, d.h. hier ist eine Filterkondition hinterlegt
  - ✕ Kreuz: ist nie erlaubt

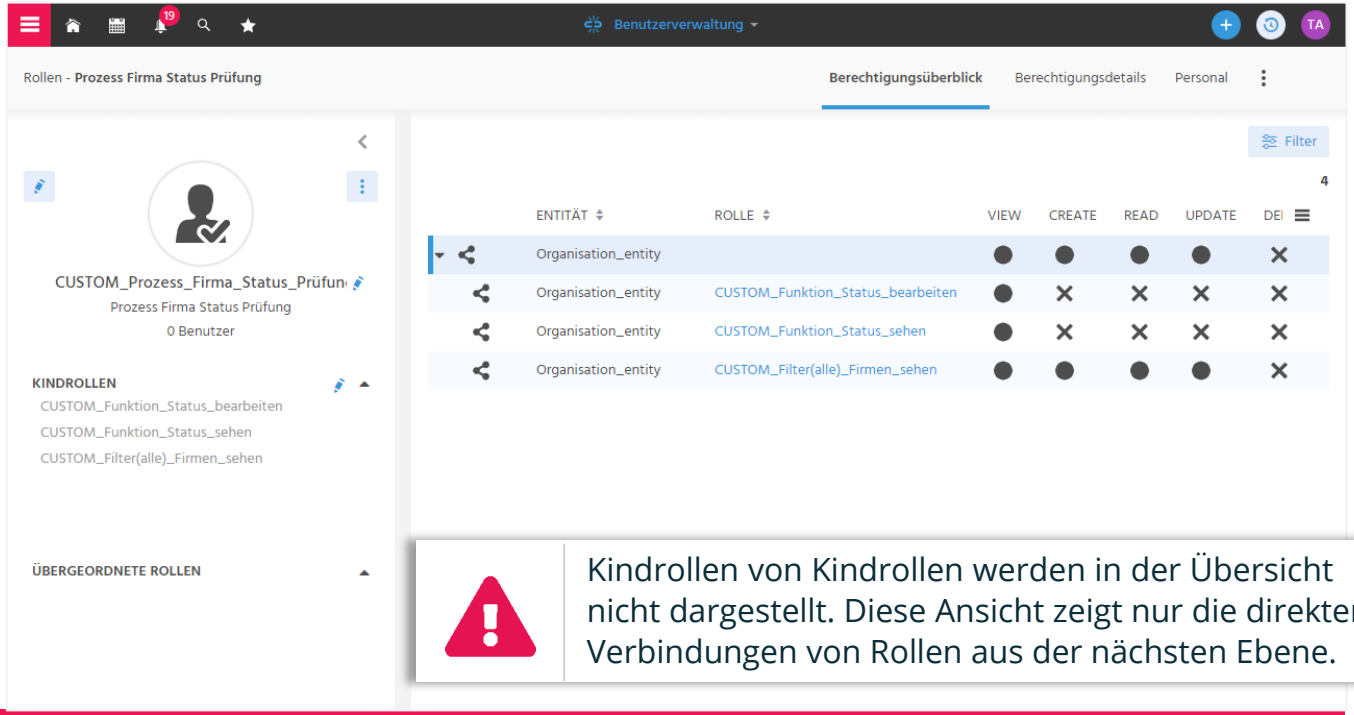


Context „Rollen“

Tab „Berechtigungsüberblick“

Handelt es sich um die Hauptansicht einer Rolle mit Kindrollen, werden im Tab „Berechtigungsüberblick“ in Form einer Baumtabelle die einzelnen Rollen und ihre Berechtigungen angezeigt.

Somit ist die Summe der Berechtigungen für die übergeordnete Rolle in der ersten Zeile ersichtlich.



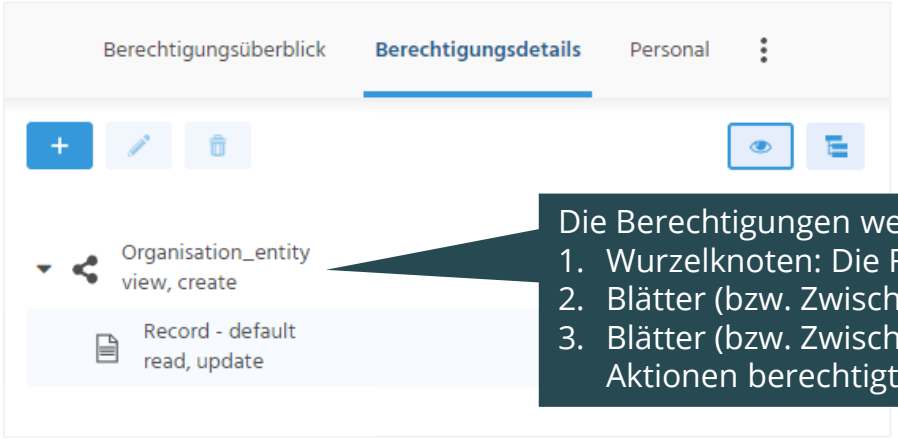
Kindrollen von Kindrollen werden in der Übersicht nicht dargestellt. Diese Ansicht zeigt nur die direkten Verbindungen von Rollen aus der nächsten Ebene.

Context „Rollen“

Tab „Berechtigungsdetails“

Der Tab ermöglicht die **Anlage/Bearbeitung** und das **detaillierte Einsehen** der Rechte.

- Sie können alle Rechte auf einmal vergeben, in dem Sie das Kennzeichen „Komplette Berechtigungen“ aktivieren.
- Oder Sie berechtigen Schritt für Schritt, zu erst auf Entityebene, dann auf Datensatzebene (evtl. mit Filterkonditionen) und ggf. auf einzelne Felder oder Aktionen.



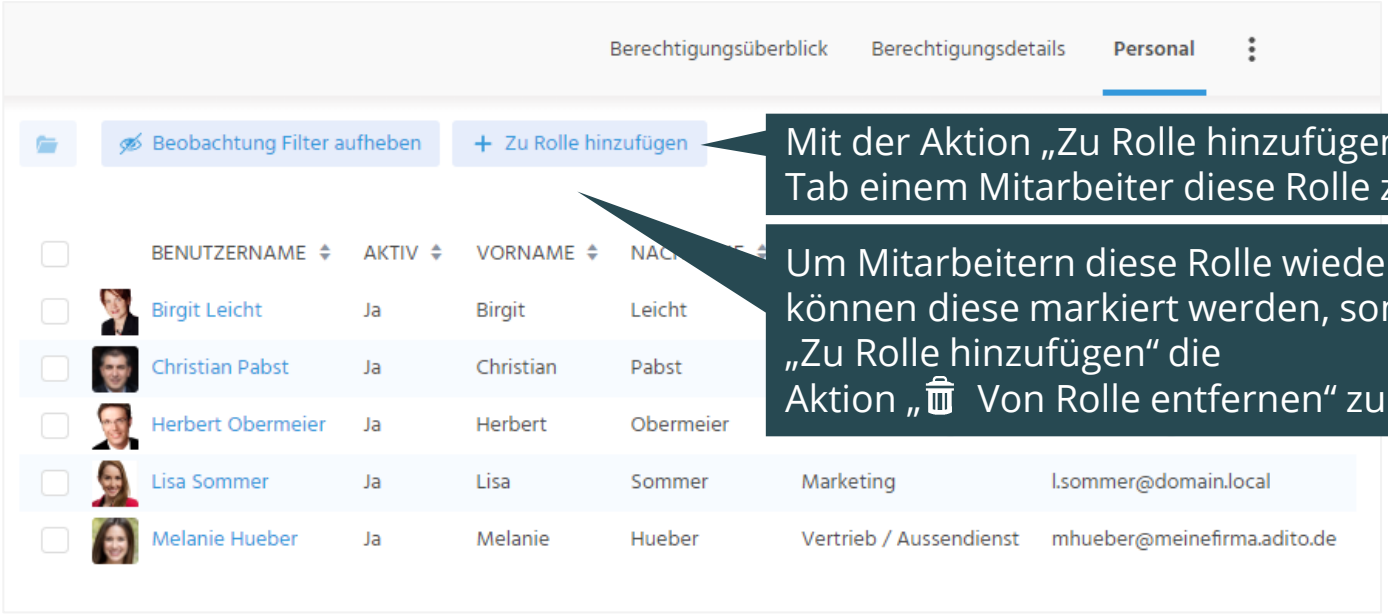
Die Berechtigungen werden in der Baumstruktur abgebildet:
1. Wurzelknoten: Die Rolle wird auf Entityebene berechtigt.
2. Blätter (bzw. Zwischenknoten): Die Rolle wird auf den Datensatz berechtigt.
3. Blätter (bzw. Zwischenknoten): Die Rolle wird auf einzelne Felder bzw. Aktionen berechtigt.

Weitere Beispiele zur Konfiguration der Rechte im Tab „Berechtigungsdetails“ aus Perspektive des Contexts „Berechtigung“ finden im Verlauf der Präsentation.

Context „Rollen“

Tab „Personal“

In diesem Tab werden alle Mitarbeiter aufgelistet, denen diese Rolle zugewiesen ist.

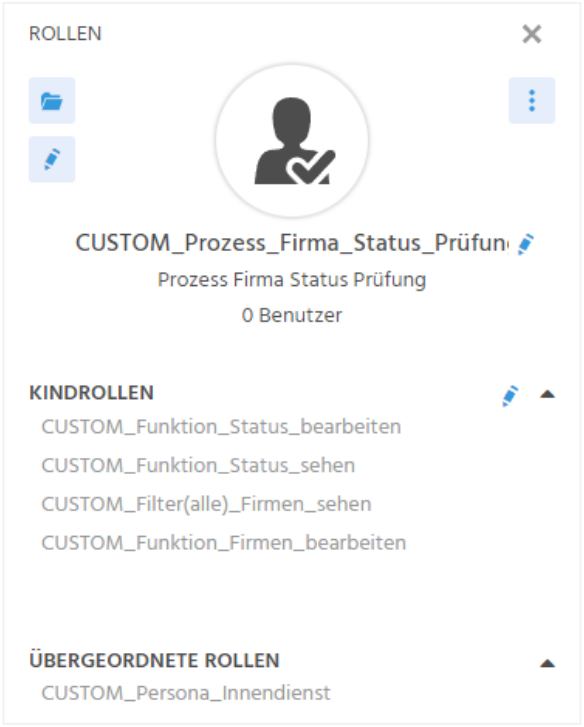


Mit der Aktion „Zu Rolle hinzufügen“, kann in diesem Tab einem Mitarbeiter diese Rolle zugewiesen werden.

Um Mitarbeitern diese Rolle wieder zu entziehen, können diese markiert werden, somit steht nun anstatt „Zu Rolle hinzufügen“ die Aktion „🗑 Von Rolle entfernen“ zur Verfügung.

Context „Rollen“

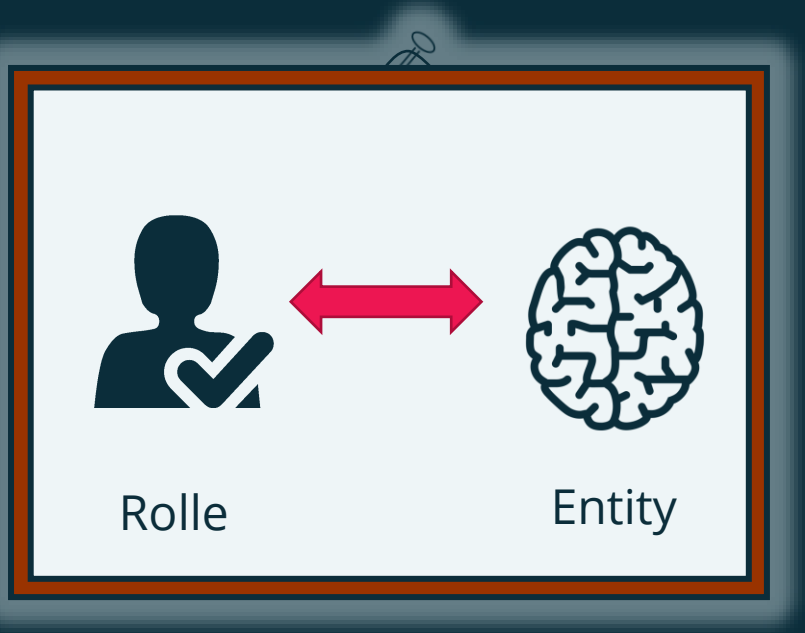
Vorschau



Hier ist ersichtlich:

- Name der Rolle
- Titel der Rolle
- Anzahl der Benutzer, denen sie zugewiesen ist
- Beschreibung (falls vorhanden)
- Übersicht über die untergeordneten Kindrollen
- Übersicht über die übergeordneten Rollen

„Berechtigung“



Was wird berechtigt?

Es werden Entitys, Fields, Actions berechtigt.

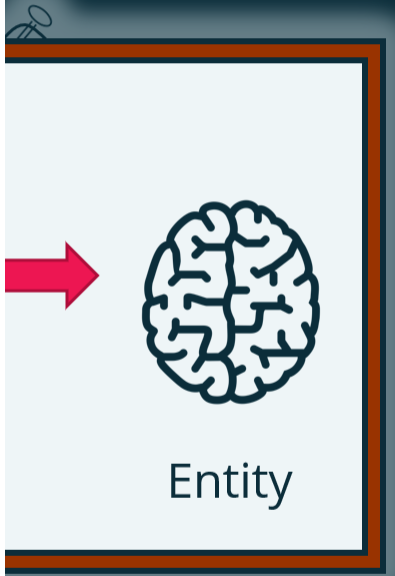
1. Introduction

ADITO is a comprehensive software framework that enables you to build powerful web-based xRM solutions, with **xRM** standing for "any relationship", not only the relationships to customers (CRM). An ADITO distribution includes the ADITO Designer, which is the main tool for creating new applications and modifying existing ones. Furthermore, ADITO comes with a project called xRM, which includes basic data structures to manage companies, contact persons, activities, sales-related elements (offers etc.), and many more. Besides, the xRM project also includes some example data, e.g., companies and contact persons.

The central programming paradigm of ADITO is the so-called "Neon Programming Model", which is based on the "Entity model". This concept means a strict separation of how data is

- structured and calculated ("Entities")
- stored ("RecordContainer") and
- displayed ("Views", clustered in "Contexts").

Auszug aus dem Customizing Manual



Über die Berechtigung des Entitys wird gesteuert, ob einer Rolle der Context im Globalen Menü angezeigt wird und welche Daten, Felder und Aktionen sie sehen und bearbeiten kann.

Berechtigung

Aktivieren

Im initial Zustand sind in ADITO xRM **keine Berechtigungen** vergeben (mit Ausnahme der Admin Berechtigungen).

Erst mit Aktivierung des Property "usePermissions" werden alle Berechtigungen entzogen und müssen den gewünschten Rollen zugewiesen werden.

D.h. **alles – Entitys, Fields, Actions –** was im Designer nicht mit usePermissions gekennzeichnet ist, ist für jede Rolle einsehbar, änderbar und ausführbar.

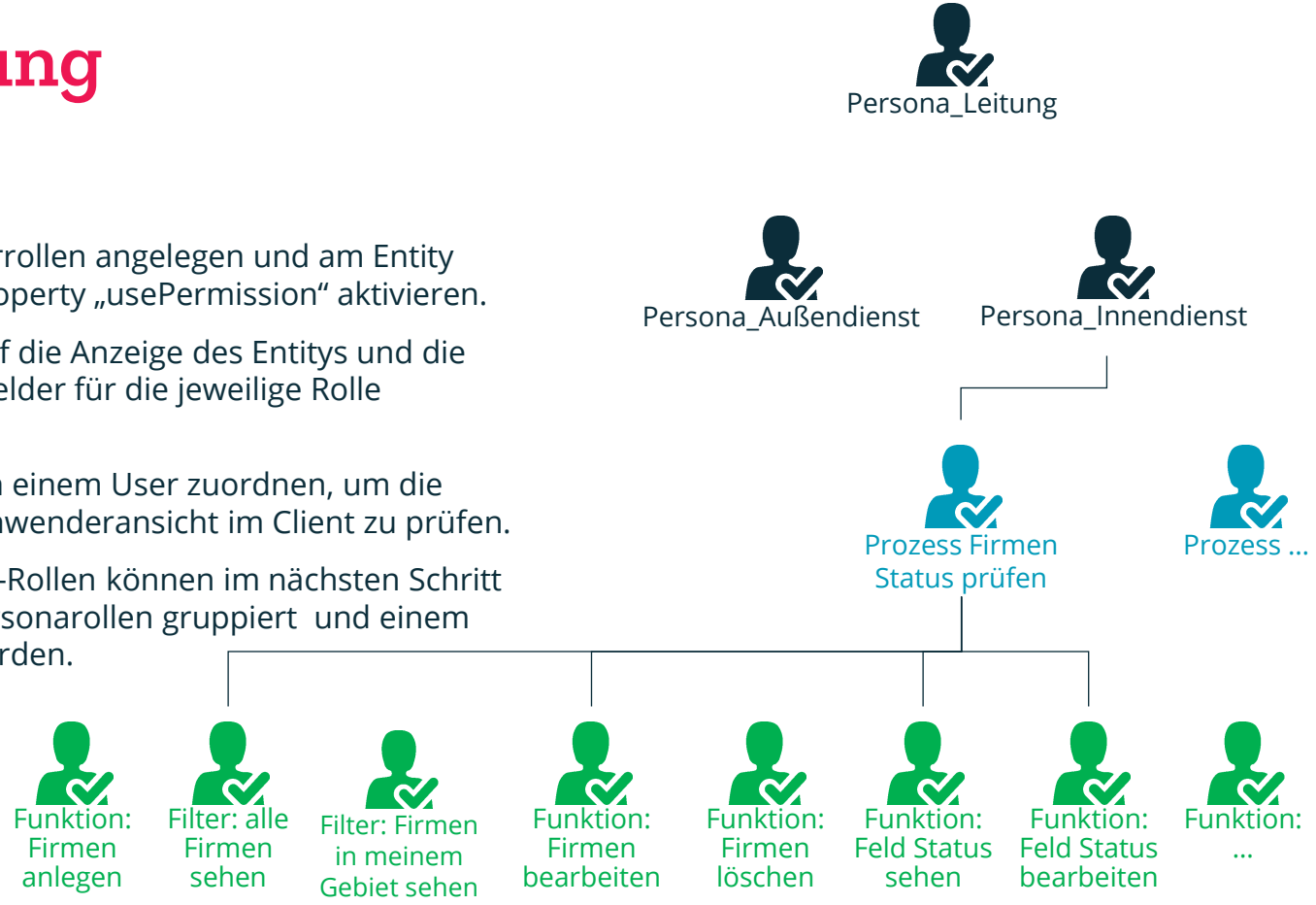
Hier ist zu beachten, dass

- die Aktivierung des Propertys "usePermissions" ausschließlich im ADITO Designer möglich ist und
- die Vergabe rollenspezifischer Rechte (Rolle ←→ Entity) ausschließlich im ADITO Web-Client stattfindet.

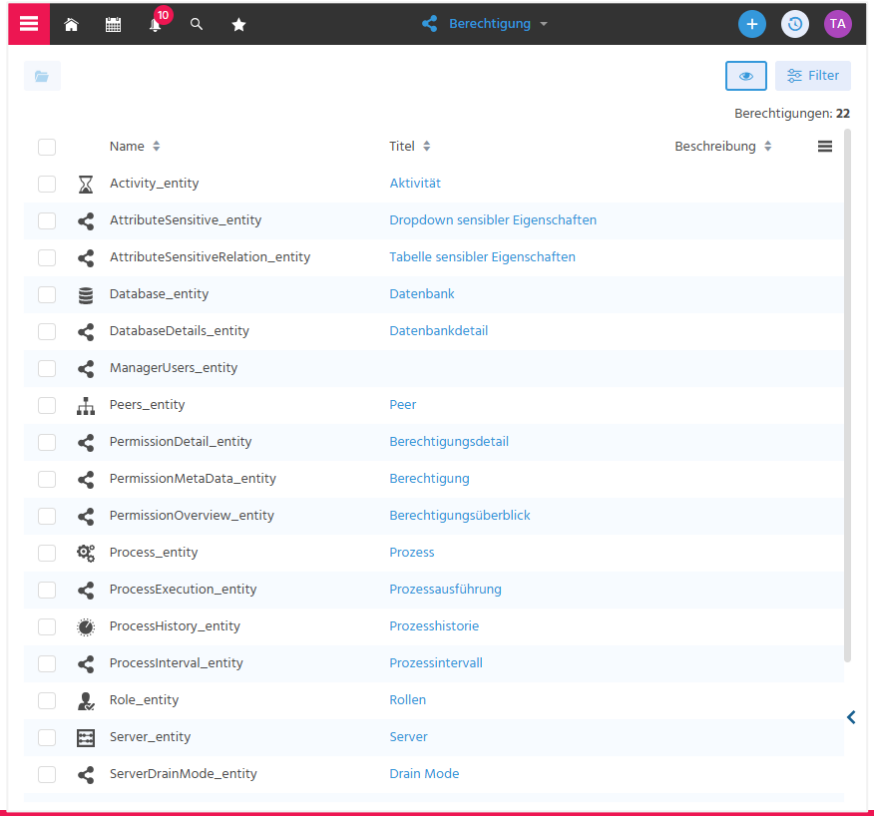
Berechtigung

Beispiel

1. Funktions- und Filterrollen angelegen und am Entity Organisation das Property „usePermission“ aktivieren.
2. Die Berechtigung auf die Anzeige des Entitys und die Datensätze, sowie Felder für die jeweilige Rolle konfigurieren.
3. Die jeweiligen Rollen einem User zuordnen, um die Berechtigung aus Anwenderansicht im Client zu prüfen.
4. Die Funktions-/Filter-Rollen können im nächsten Schritt zu Prozess- bzw. Personarollen gruppiert und einem User zugeordnet werden.



Entitys berechtigen



Der Context „Berechtigung“ gibt einen Überblick über alle Entitys, bei denen die Berechtigung aktiviert wurde.

Für jedes Entity, das hier aufgeführt ist, wurden das Property „usePermission“ aktiviert. Erst nach Berechtigung einer Rolle kann diese den Context wieder sehen und damit je nach Berechtigung arbeiten.

Auf die im Screenshot angezeigten Entitys wurde im xRM die Rolle „Administrator“ berechtigt (siehe „Sonderstellung Administrator“).

Damit weitere Entitys in dieser Liste angezeigt werden, sind im Designer folgende Schritte notwendig:

Entitys berechtigen

Möglichkeit 1:

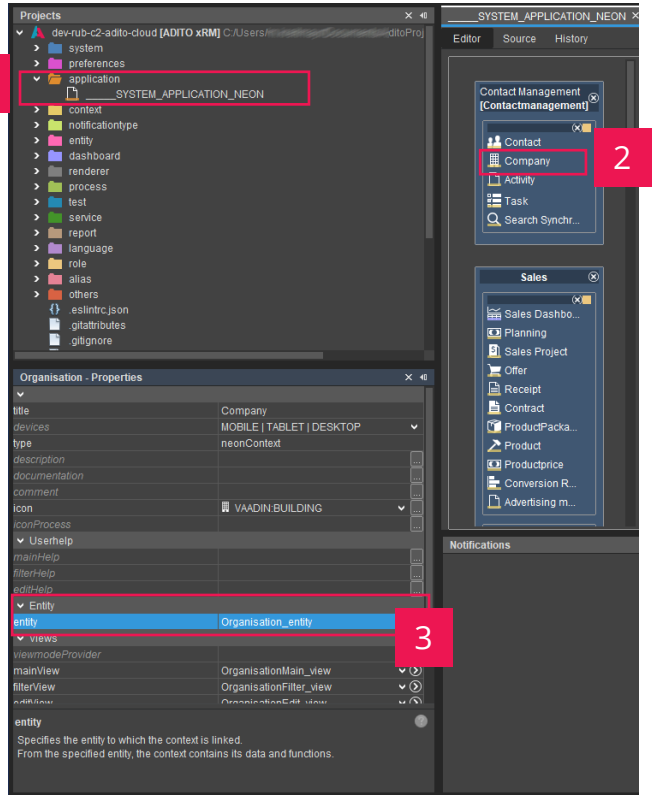
1. Einstieg über die _____SYSTEM_APPLICATION.
2. Suchen des Contextes Firma
3. Öffnen des damit verbundenen Organisation_entitys
4. Öffnen der Properties des Entitys
5. Aktivieren von usePermissions

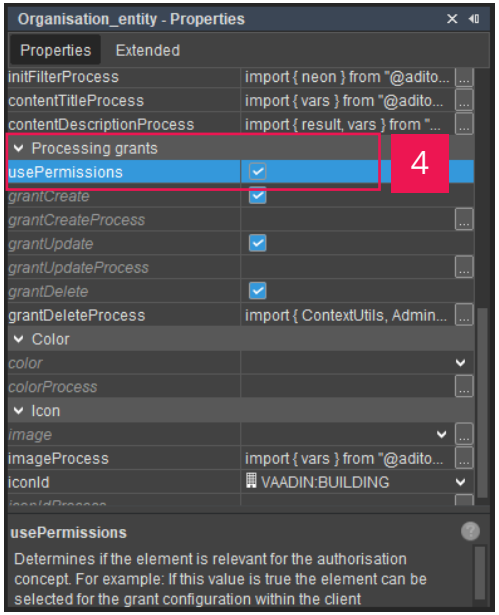
Möglichkeit 2:

Einstieg über die Gesamtauswahl „context“ im Bereich Projects.
(Es folgen die Schritte 3. – 5.)

Möglichkeit 3:

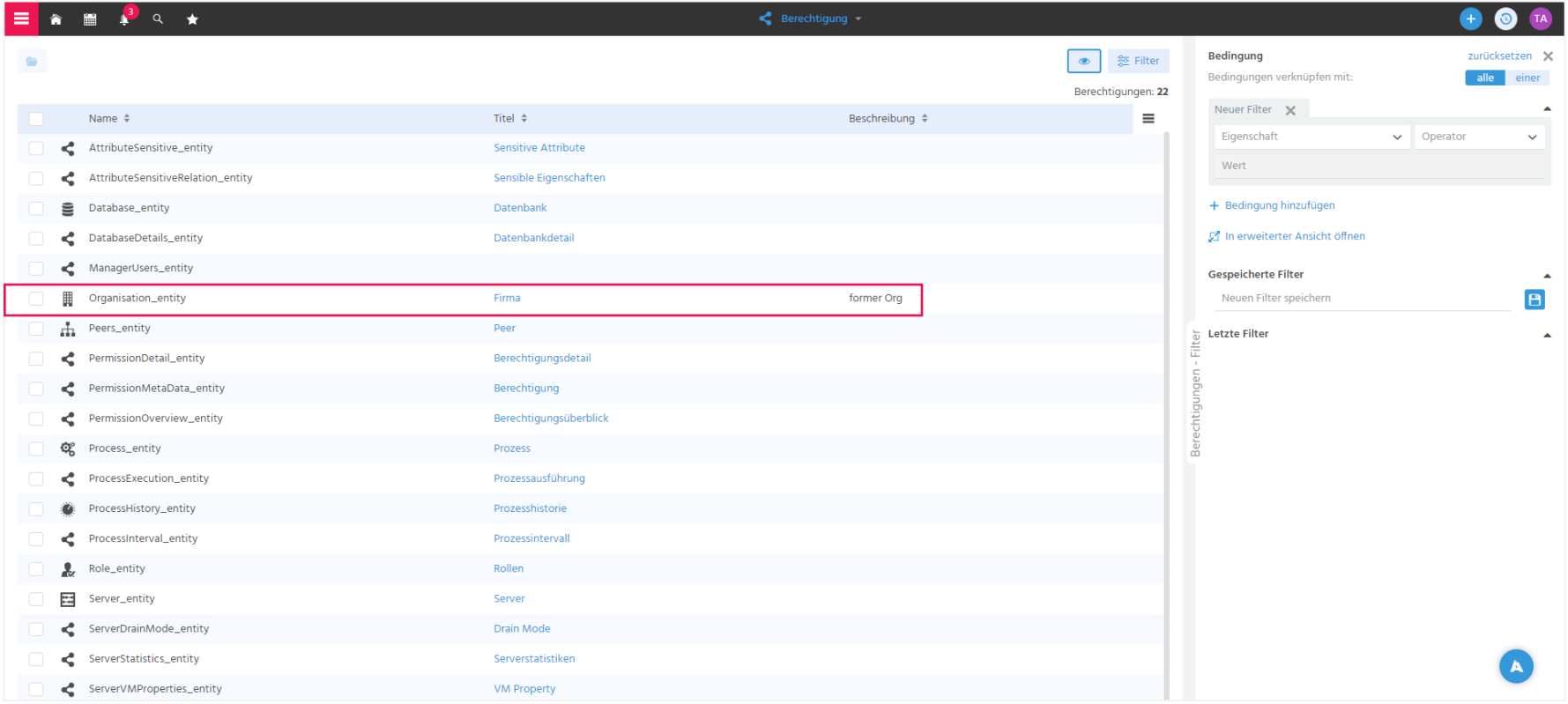
Einstieg über die Gesamtauswahl „entity“ im Bereich Projects.
(Es folgen die Schritte 4. und 5.)



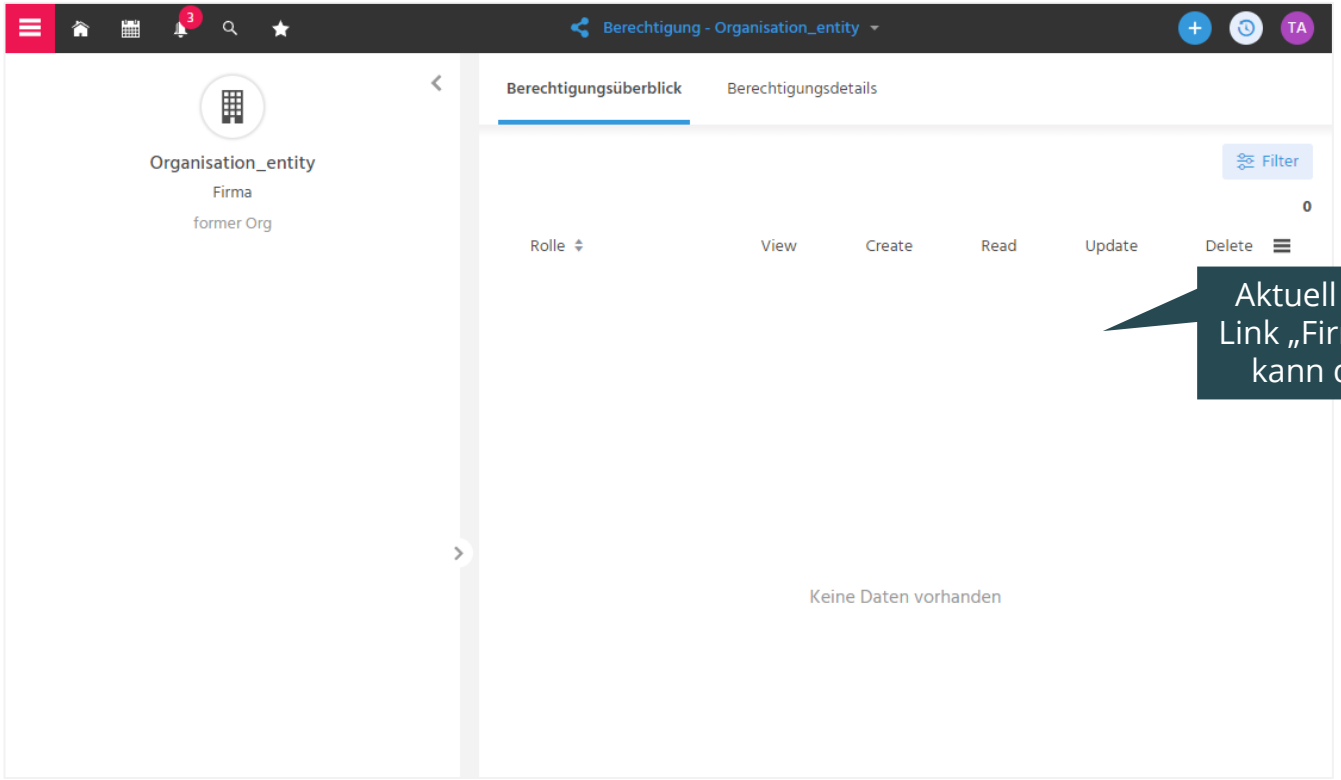


5 Deploy

Entitys berechtigen



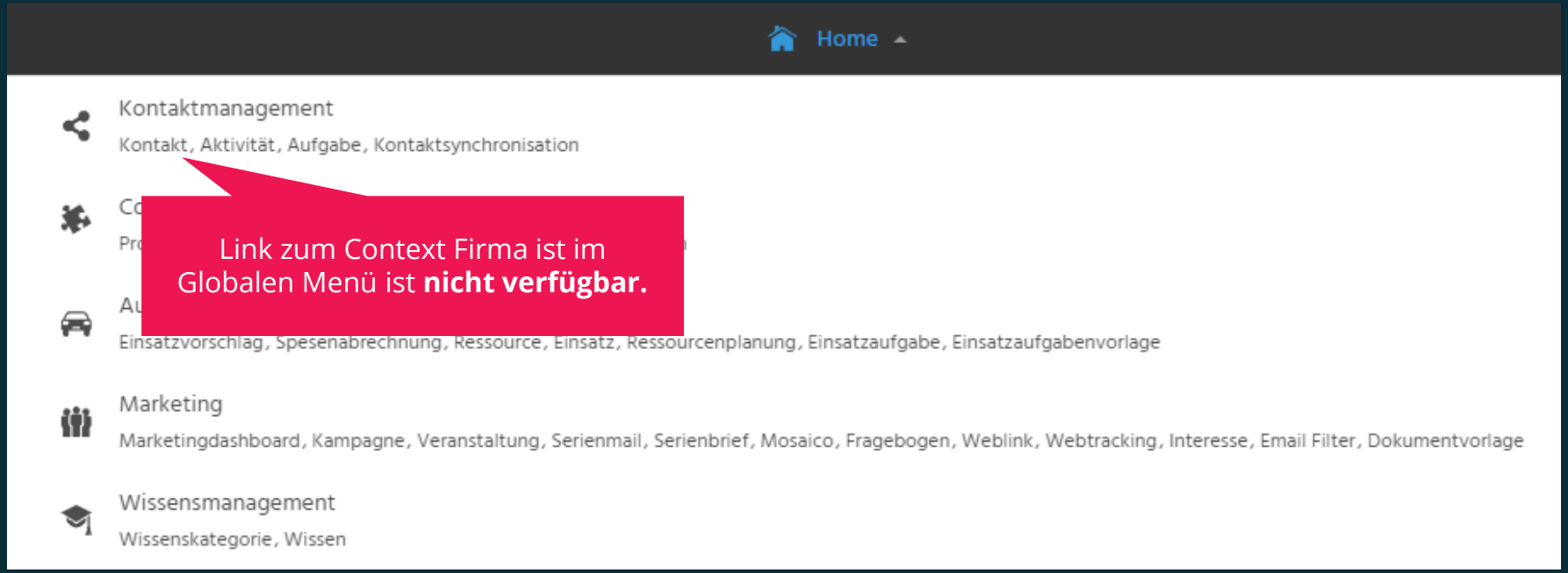
Entitys berechtigen



Aktuell sieht keine Rolle mehr den Link „Firma“ im Globalen Menü oder kann die Datensätze bearbeiten

Entitys berechtigen

Sicht des Anwenders

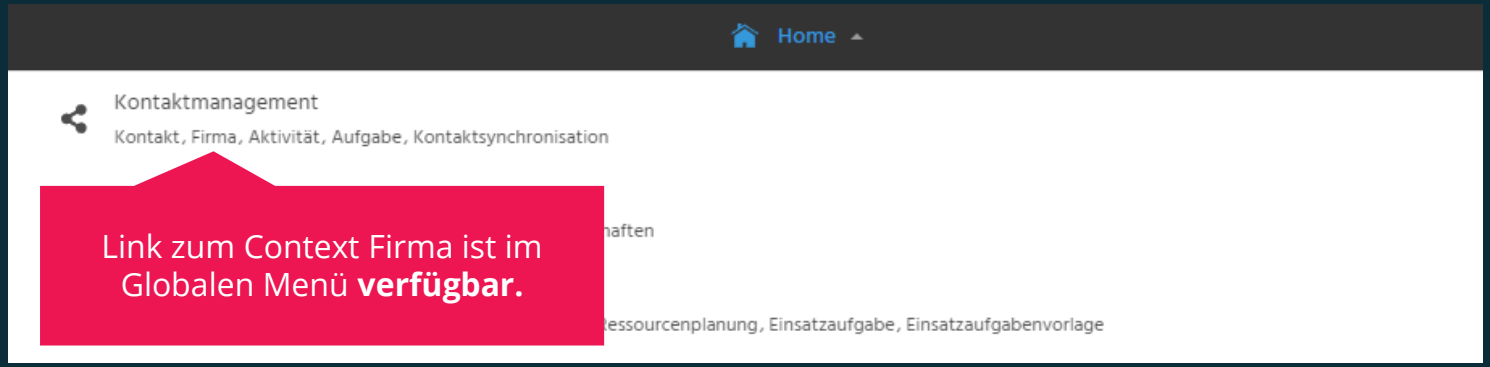


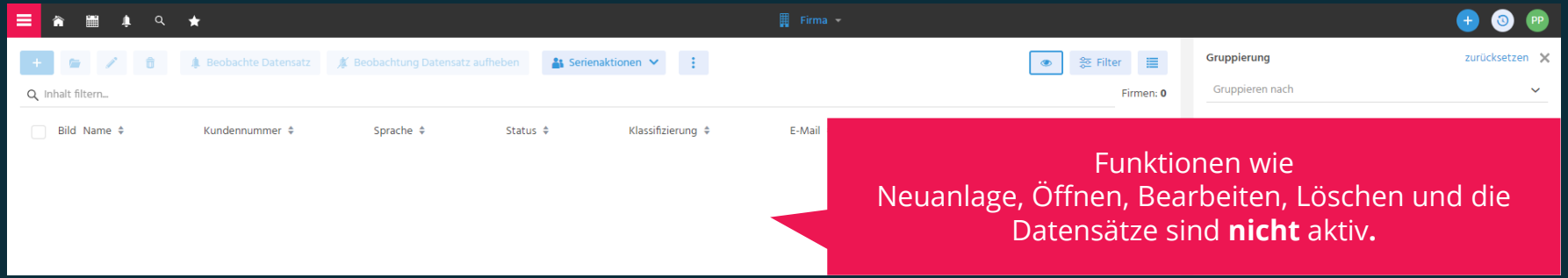
Entitys berechtigen

Anzeige des Links im Globalen Menü steuern: VIEW-Berechtigung erteilen

Entitys berechtigen

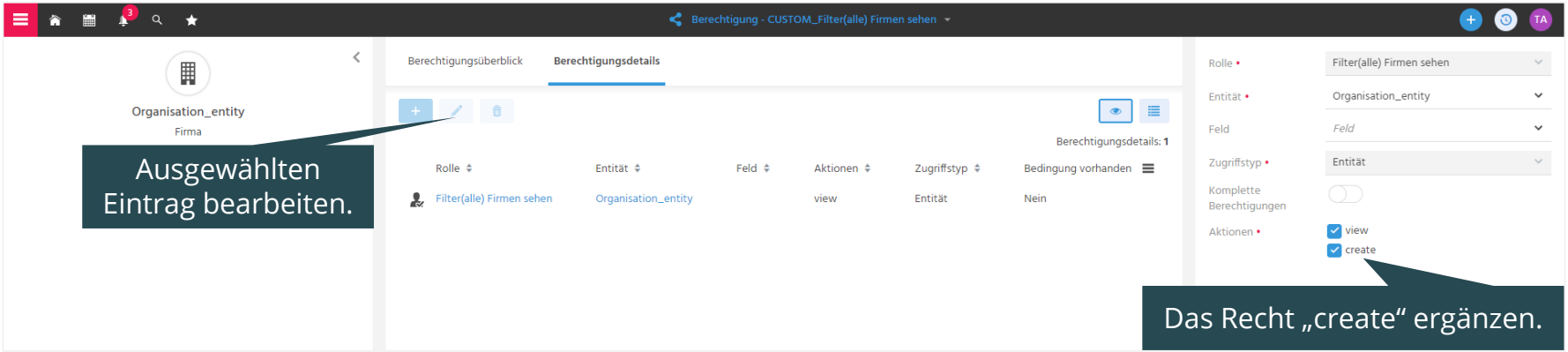
Sicht des Anwenders



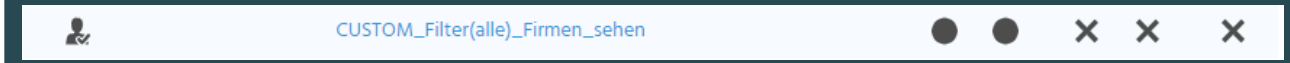


Entitys berechtigen

Neue Datensätze anlegen: CREATE-Berechtigung erteilen

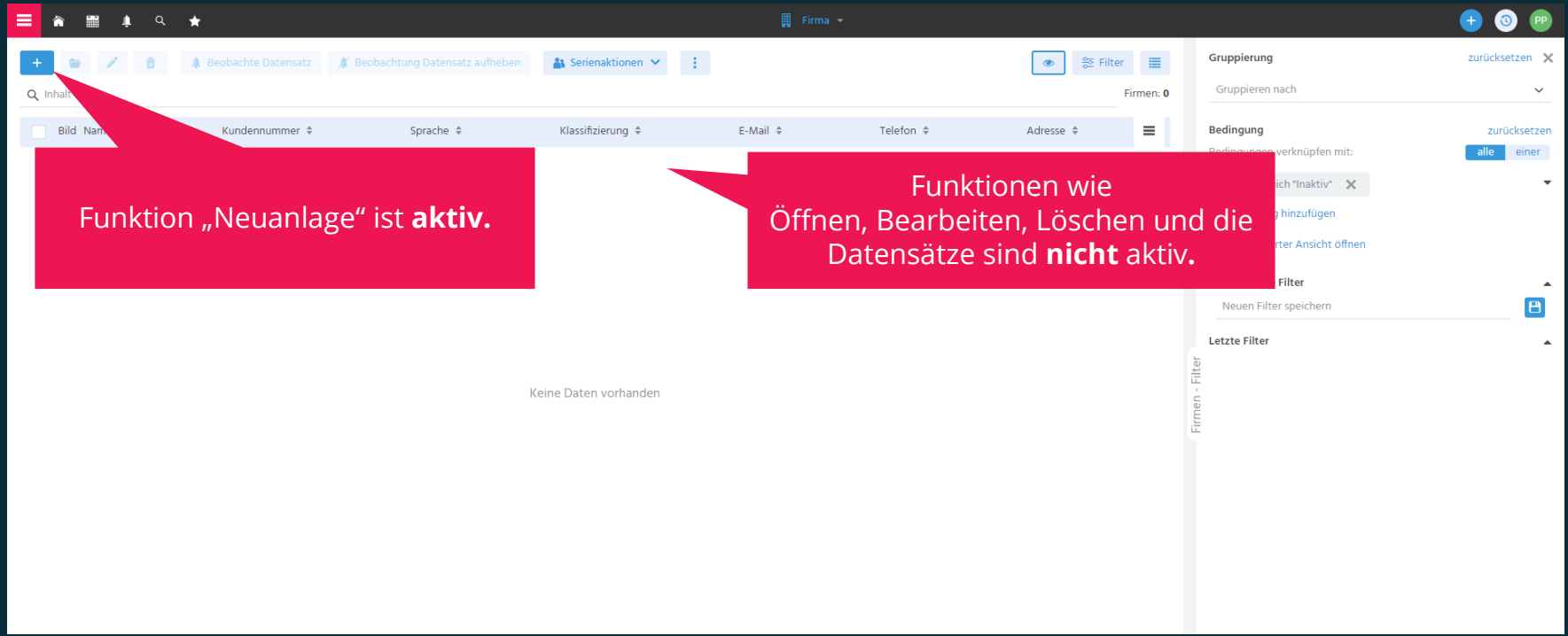


Darstellung der erfassten Berechtigung im Tab „Berechtigungsüberblick“



Entitys berechtigen

Sicht des Anwenders

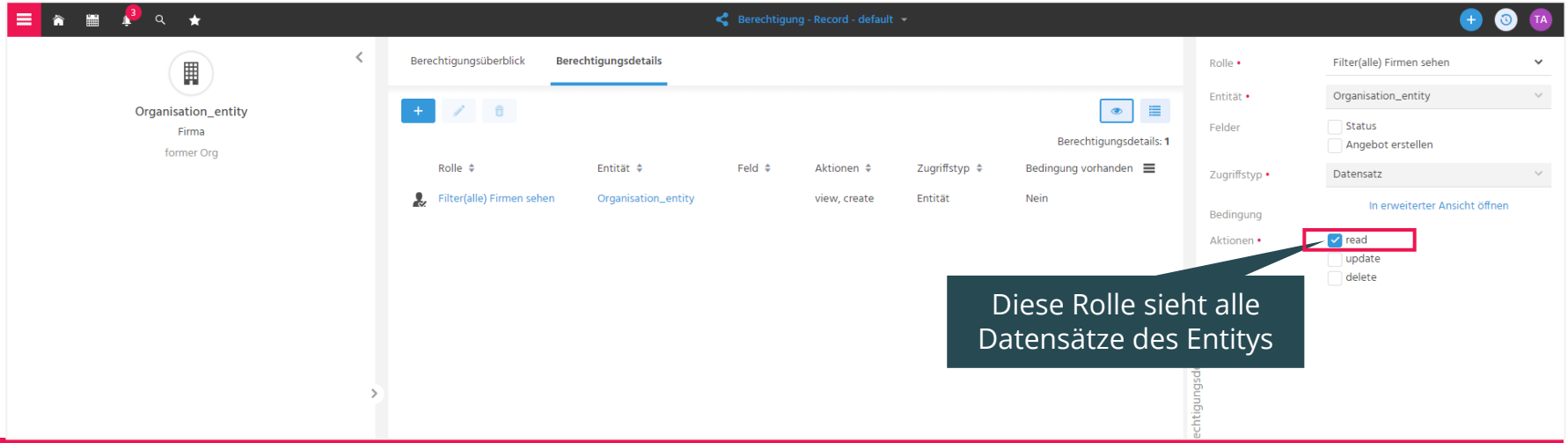


Datensätze berechtigen

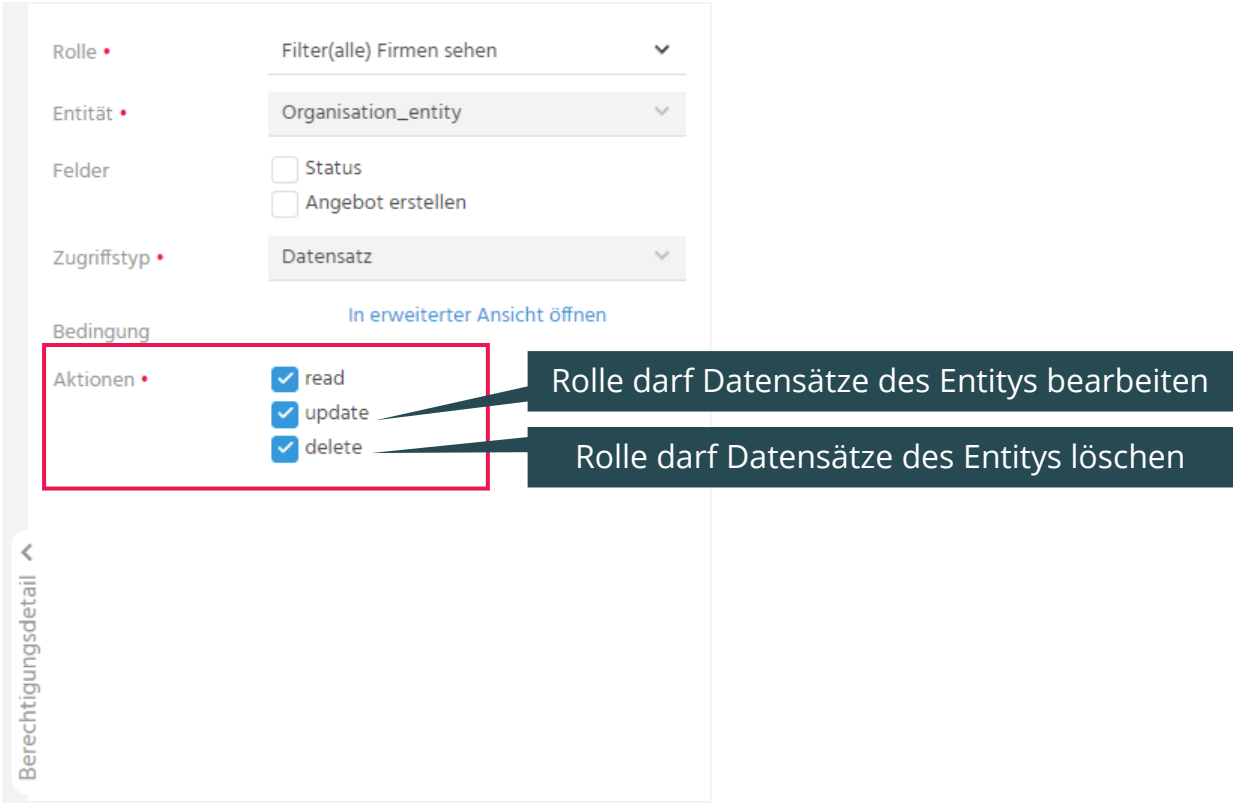
Alle Rechte für ein Entity und seine Datensätze konfigurieren

Die Rechte **Öffnen (Read)**, **Bearbeiten (Update)** oder **Löschen (Delete)** können für das gewählte Entity auf Datensatzebene (Record) vergeben werden.

Diese Rechte können bspw. an eine Rolle oder jeweils einzelne Funktions-/Filterrollen vergeben werden.
Bedingung ist dabei, dass jede dieser Rollen das Recht VIEW auf Entity Ebene hat.



Datensätze berechtigen



Datensätze berechtigen

Alle Rechte für ein Entity und seine Datensätze konfigurieren

ROLLE	VIEW	CREATE	READ	UPDATE	DELETE
CUSTOM_Filter(alle)_Firmen_sehen	●	✕	●	✕	✕
CUSTOM_Funktion_Firma_löschen	●	✕	✕	✕	●
CUSTOM_Funktion_Firmen_anlegen	●	●	✕	✕	✕
CUSTOM_Funktion_Firmen_bearbeiten	●	✕	✕	●	✕

Die Rechte READ, UPDATE und DELETE wurde auf drei Rollen aufgeteilt

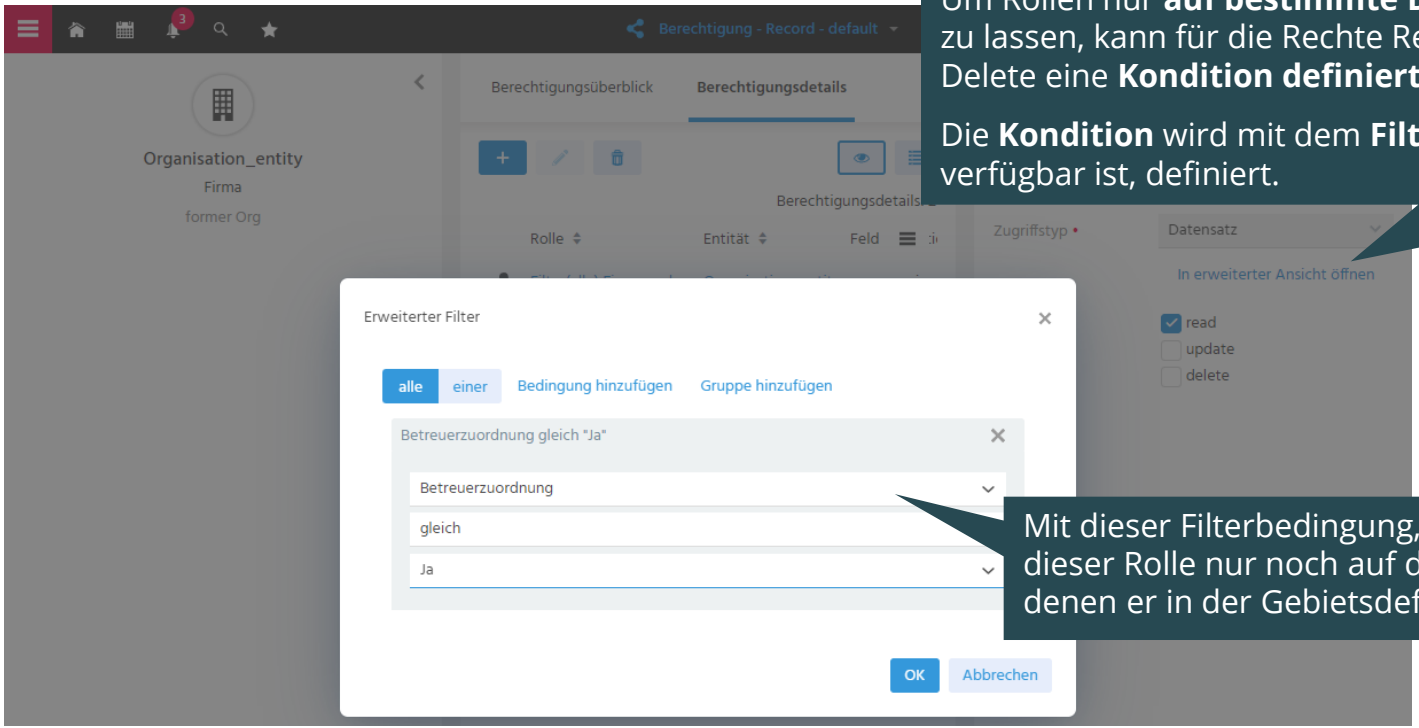
Datensätze berechtigen

Sicht des Anwenders

Bild	Name	Kundennummer	Sprache	Klassifizierung	E-Mail	Telefon	Adresse
	Aquire GmbH	3469	Englisch	--	info@aquire.de	+49 4321 78990	Friedenstraße 12 b - DE 93053 Regensburg
BG	Bohrmarkt GmbH	9612	Deutsch		info@bohrmarkt.de	+49 9246 552	Innstraße 11 - DE 93059 Regensburg
BM	Bornheimer Maschinenfabrik GmbH	4387	Deutsch		info@bornheimer.de	+49 2222 940210	Peter-Fryns-Platz - DE 53332 Bornheim
	Bucher Unternehmensgruppe	3698	Deutsch	BC	info@bucher.de	+49 40 42580	Julius-Leber-Straße 32 - DE 22765 Hamburg
EB	Emil Brandstätter AG	5609	Deutsch		kontakt@brandstaetter.de	+49 831 25359	Mühlhauserstr. 20 - DE 81379 München
EG	Ertl GmbH	7824	Deutsch	--	service@ertl.de	+49 335 12875	Belgische Straße 2 - DE 15234 Frankfurt (Oder)
FS	Fahey, Spencer and Armstrong	1793	Englisch	CD	greattohearfromyou@fsa.org	+44 20 3245 1844	69 New Street - GB B2 4DU Birmingham
	Firmengruppe Matthias Bogen	4567	Deutsch	DC	info@matthiasbogen.de	+49 421 98650	Pfeilstraße 7 - DE 28217 Bremen
FA	Fischer AG	1018	Deutsch	DC	info@fischer.tr	+49 6472 35000	Brenneckestraße 100 - DE 39116 Magdeburg
	Glob Group	1212	Englisch	BB	contact@globgroup.com	+44 20 1432 3000	32-40 Blackfriars Road - GB SE1 8NW London
	Grobbe-Werk GmbH	4758	Deutsch	CC	info@grobbe-werk.de	+49 841 32510	Regensburger Straße 65 - DE 85055 Ingolstadt

Datensätze berechtigen

Nur bestimmte Datensätze berechtigen



Um Rollen nur **auf bestimmte Datensätze zugreifen** zu lassen, kann für die Rechte Read, Update oder Delete eine **Kondition definiert** werden.

Die **Kondition** wird mit dem **Filter**, der für das Entity verfügbar ist, definiert.

Mit dieser Filterbedingung, kann der User mit dieser Rolle nur noch auf die Firmen zugreifen, denen er in der Gebietsdefinition zugeordnet ist.

Datensätze berechtigen

Nur bestimmte Datensätze berechtigen

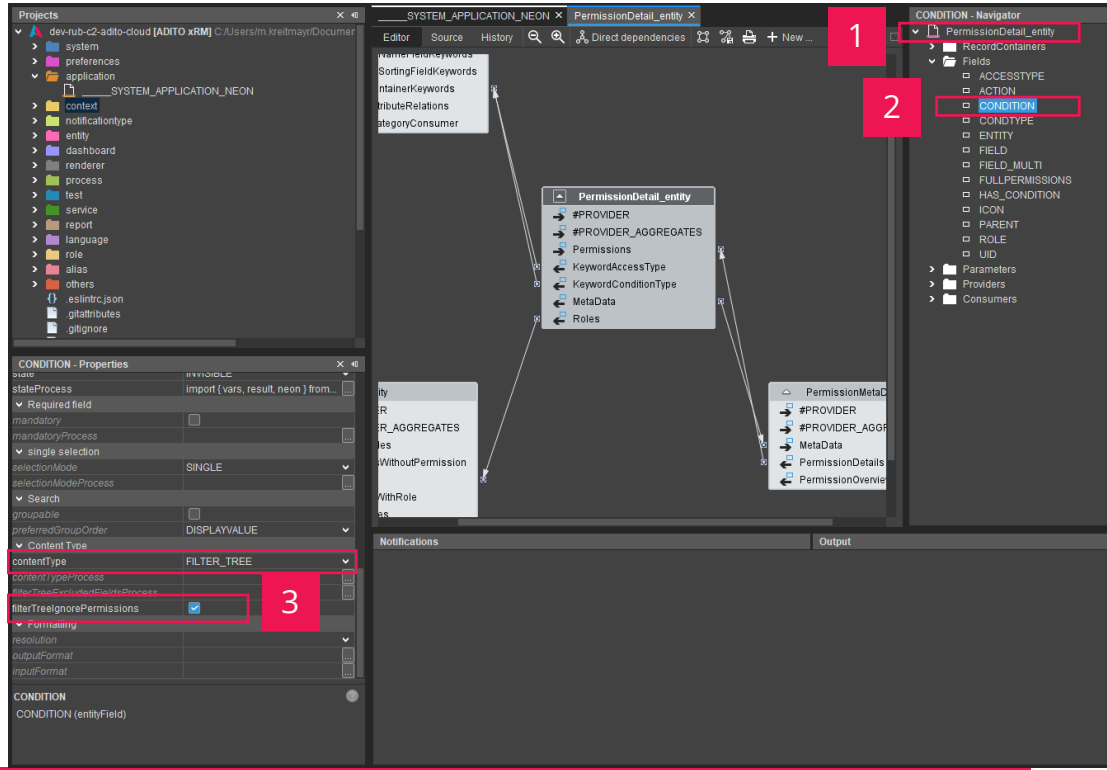
Kondition

Anzeige der Filtereigenschaften

Um auf den Filter zur Erfassung der Kondition zugreifen zu können, ohne das der Administrator selbst Rechte auf das Entity hat, ist für das Feld „Kondition“ des Entitys „PermissionDetail“ das Property „filterTreeIgnorePermission“ zu aktivieren.

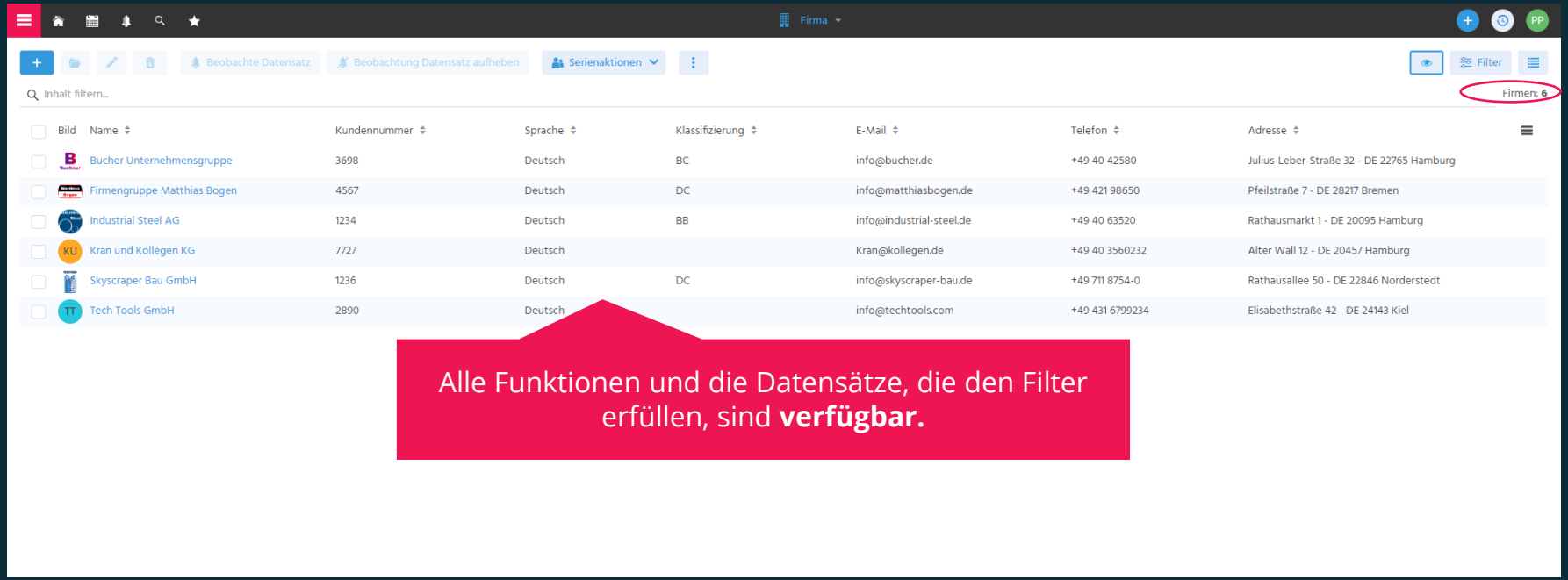
Ist diese Checkbox gesetzt, wird beim Öffnen der Filter Tree Komponente die Berechtigung (VIEW-Berechtigung auf dem jeweiligen Entity) ignoriert.

Diese Einstellung ist standardmäßig deaktiviert.



Datensätze berechtigen

Sicht des Anwenders



Felder berechtigen

Möglichkeit 1:

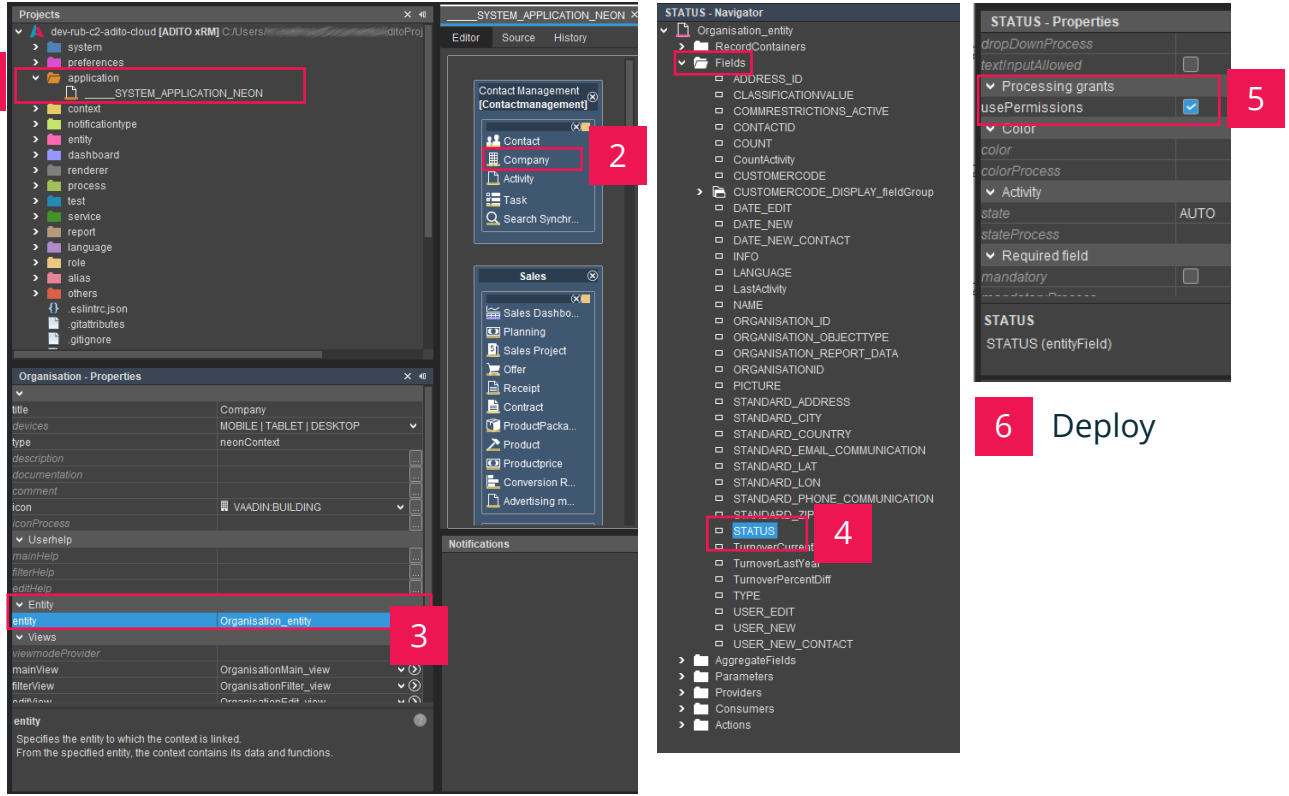
1. Einstieg über die SYSTEM_APPLICATION.
2. Suchen des Contextes Firma
3. Öffnen des damit verbundenen Organisation_entitys
4. Öffnen der Properties des Feldes
5. Aktivieren von usePermissions

Möglichkeit 2:

Einstieg über die Gesamtauswahl „context“ im Bereich Projects.
(Es folgen die Schritte 3. – 5.)

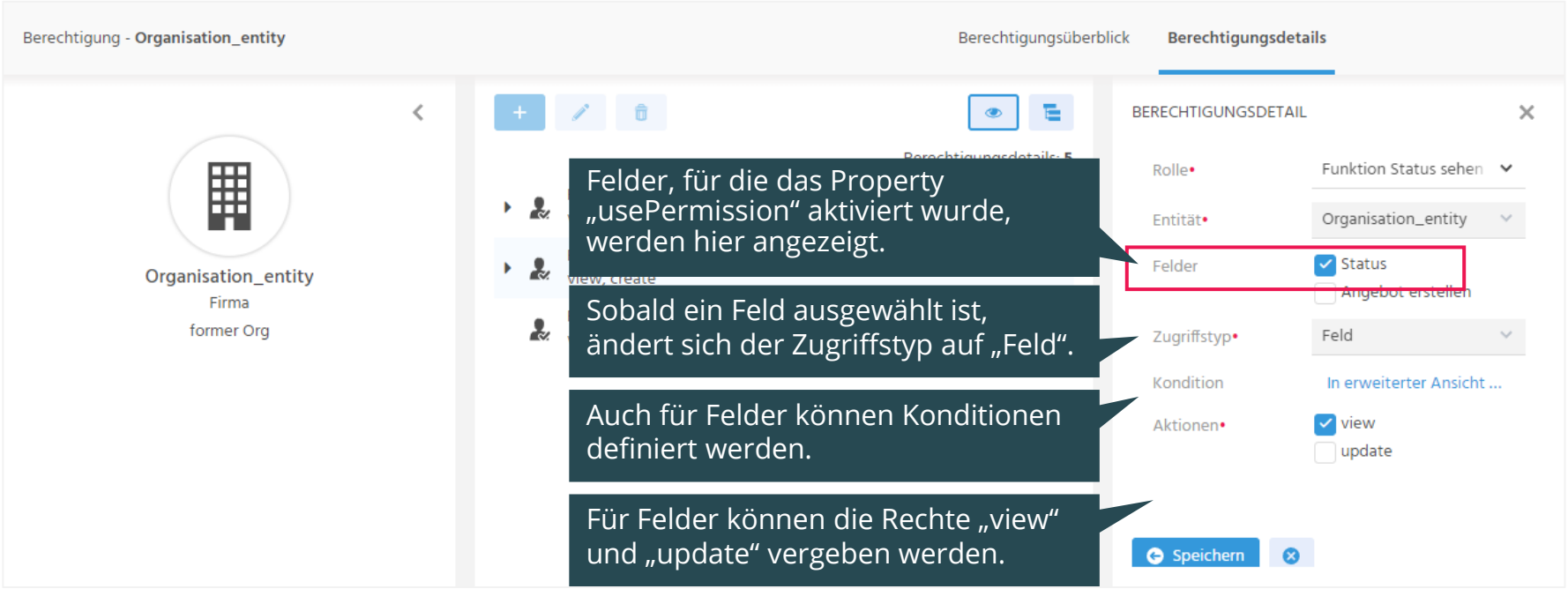
Möglichkeit 3:

Einstieg über die Gesamtauswahl „entity“ im Bereich Projects.
(Es folgen die Schritte 4. und 5.)

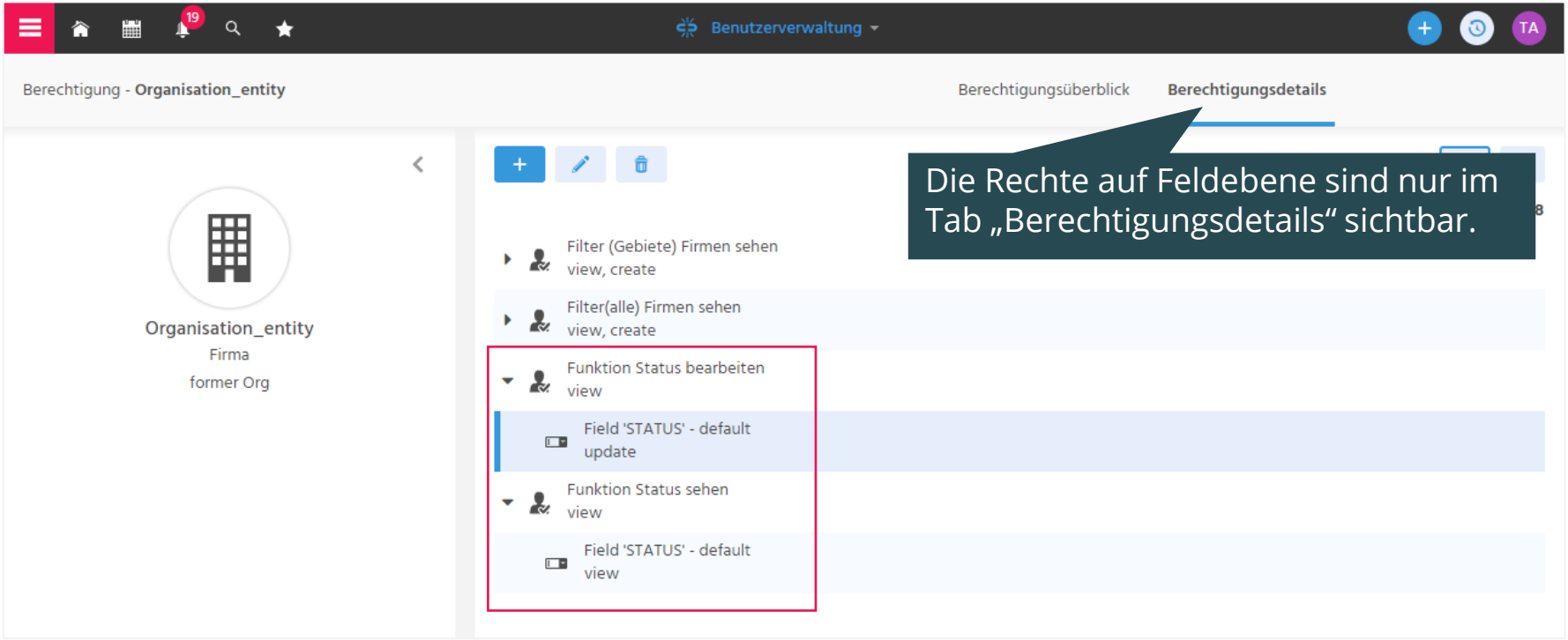


Felder berechtigen

Feld anzeigen

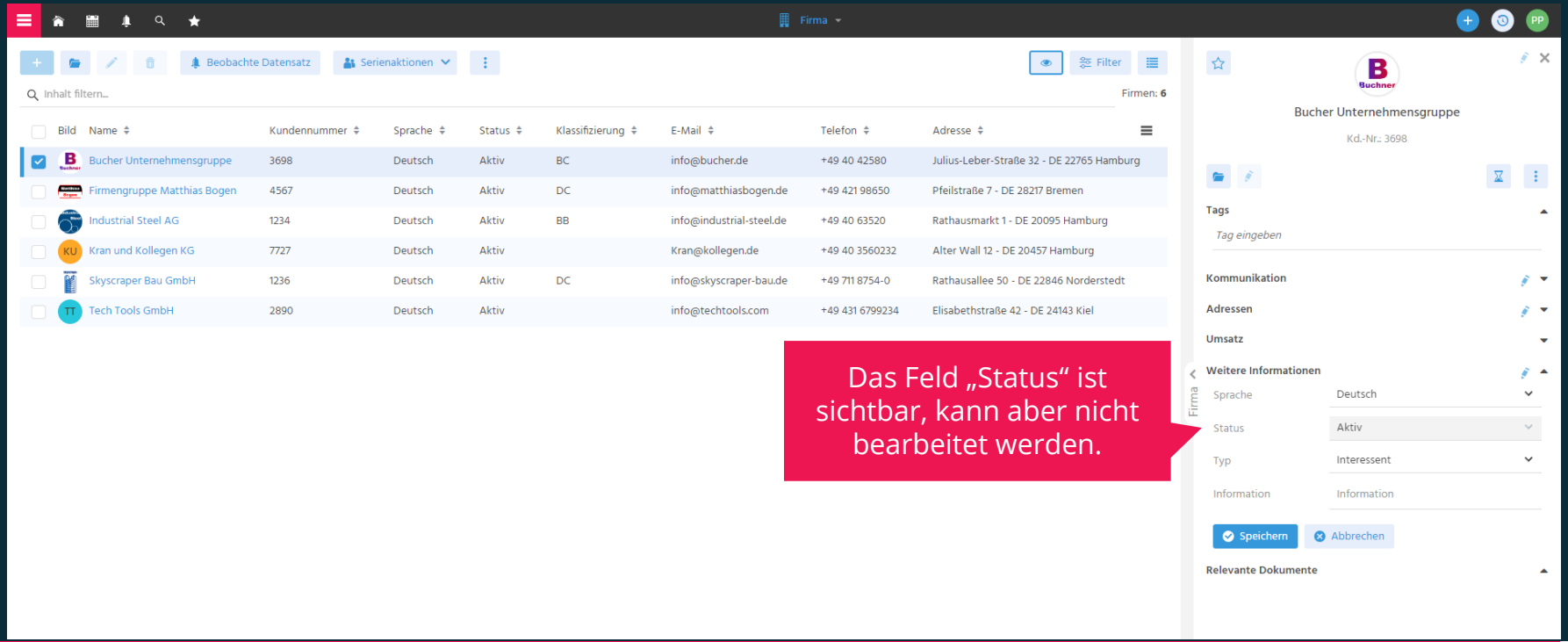


Felder berechtigen



Felder berechtigen

Sicht des Anwenders mit der Rolle „Funktion_Firmen_Status_sehen“



Aktionen berechtigen

Möglichkeit 1:

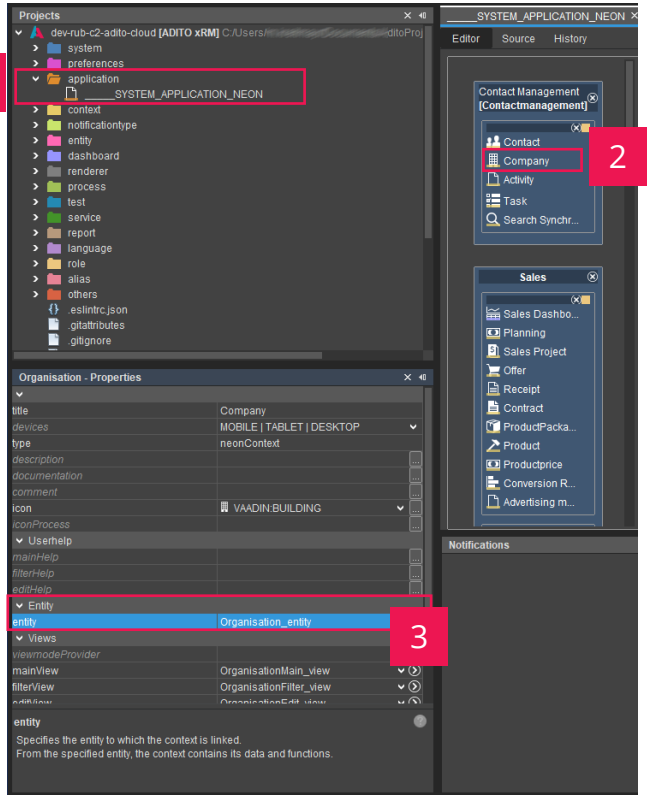
1. Einstieg über die SYSTEM_APPLICATION.
2. Suchen des Contextes Firma
3. Öffnen des damit verbundenen Organisation_entitys
4. Öffnen der Properties der Aktion
5. Aktivieren von usePermissions

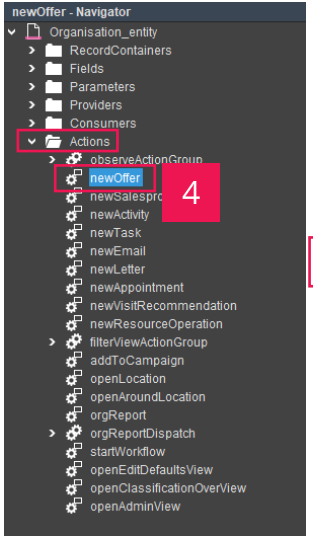
Möglichkeit 2:

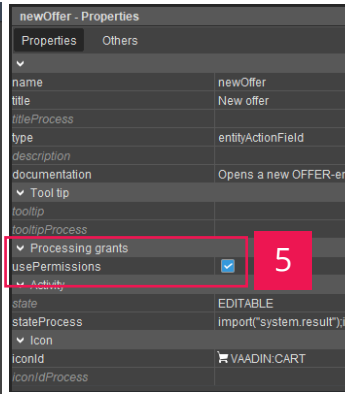
Einstieg über die Gesamtauswahl „context“ im Bereich Projects.
(Es folgen die Schritte 3. – 5.)

Möglichkeit 3:

Einstieg über die Gesamtauswahl „entity“ im Bereich Projects.
(Es folgen die Schritte 4. und 5.)



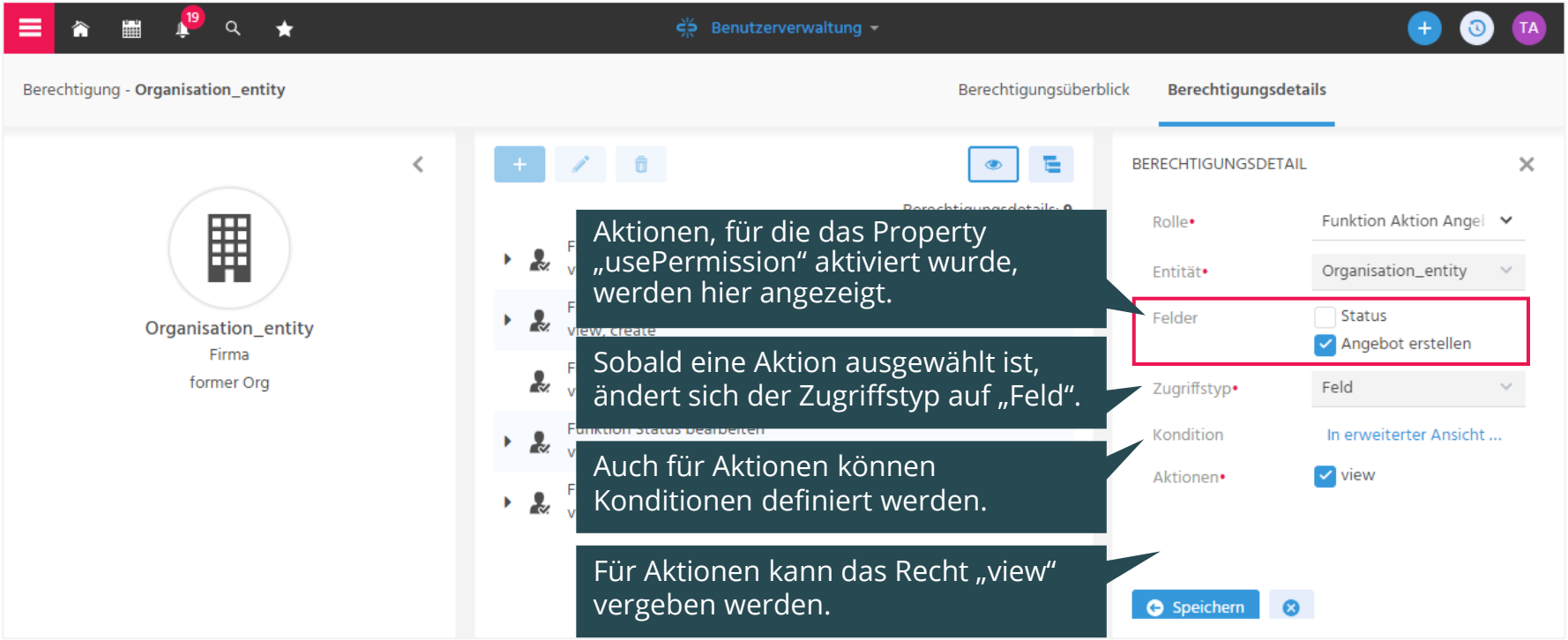




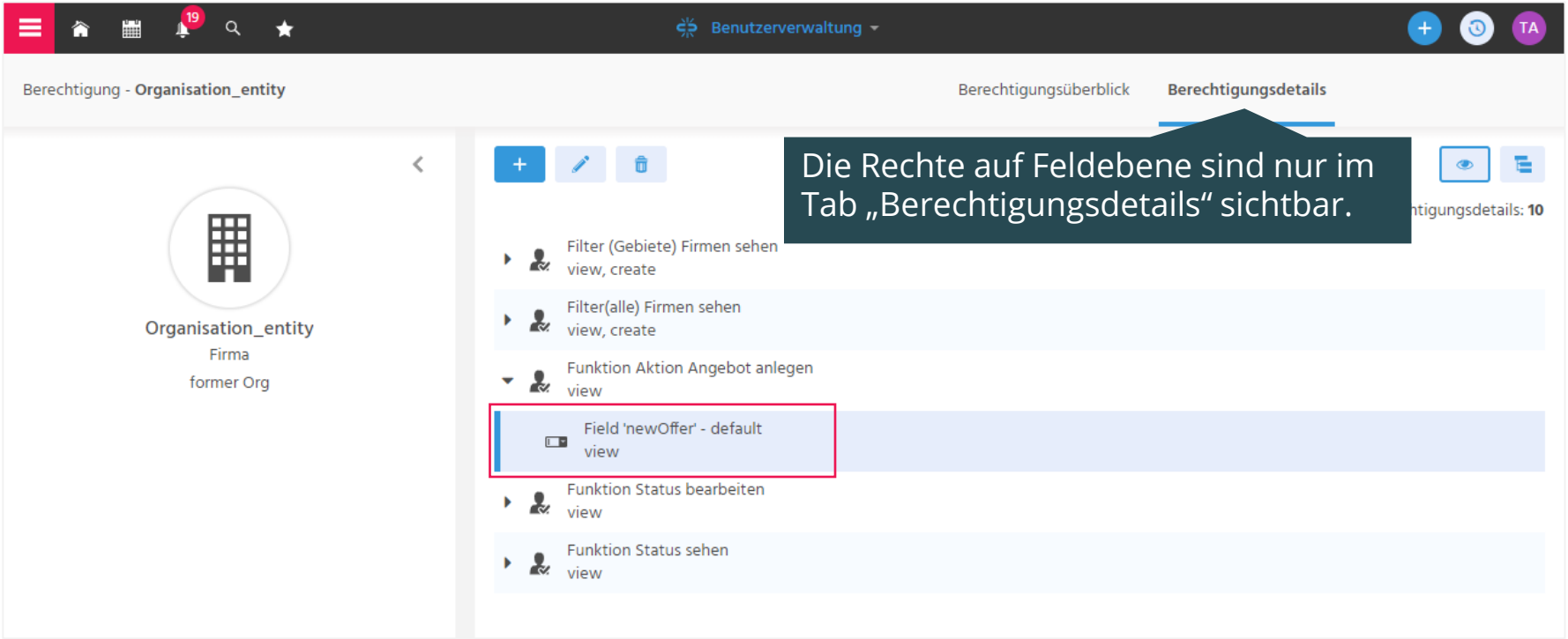
6 Deploy

Aktionen berechtigen

VIEW-Berechtigung

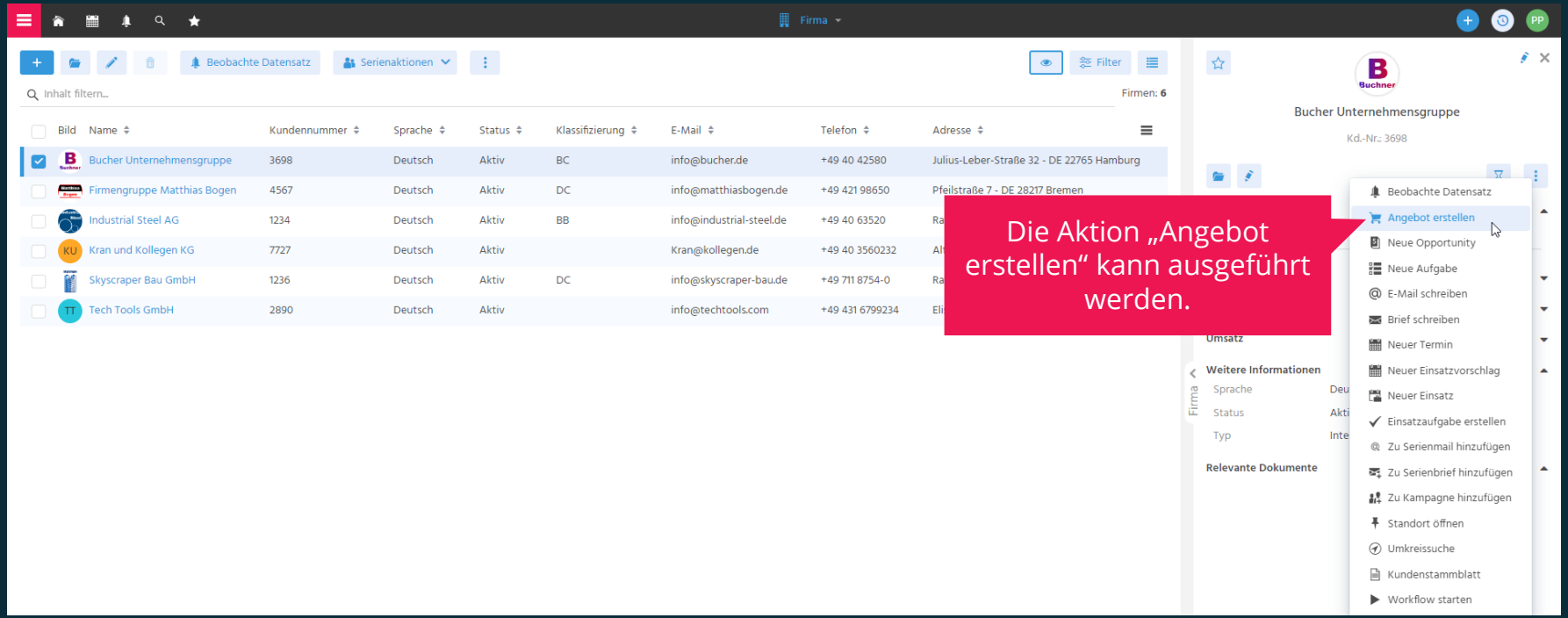


Aktionen berechtigen



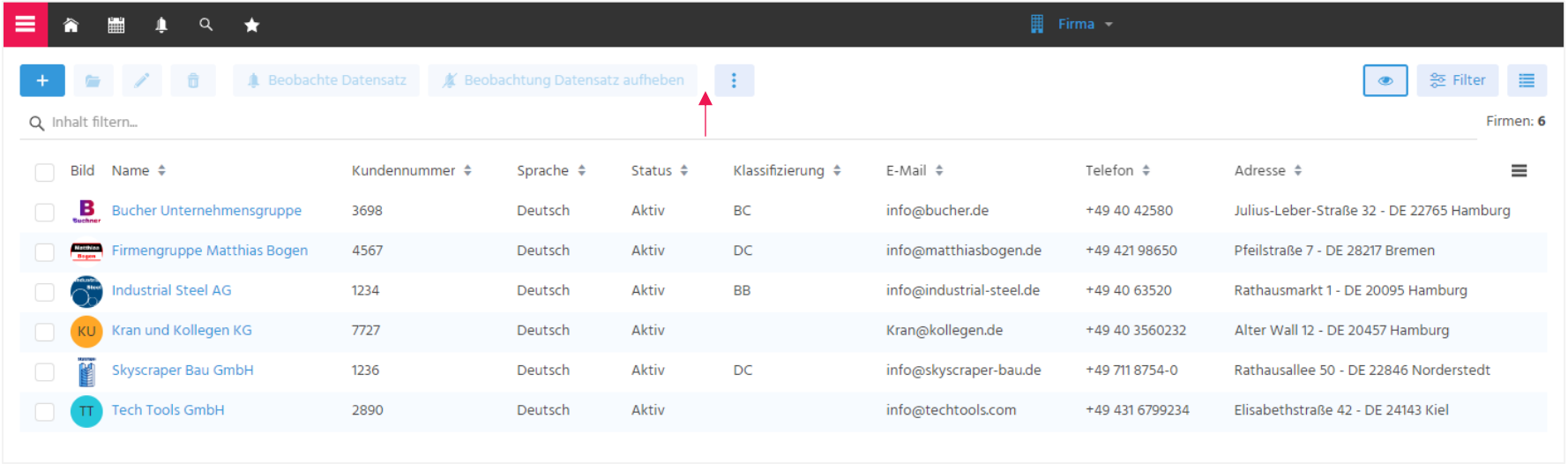
Aktionen berechtigen

Sicht des Anwenders

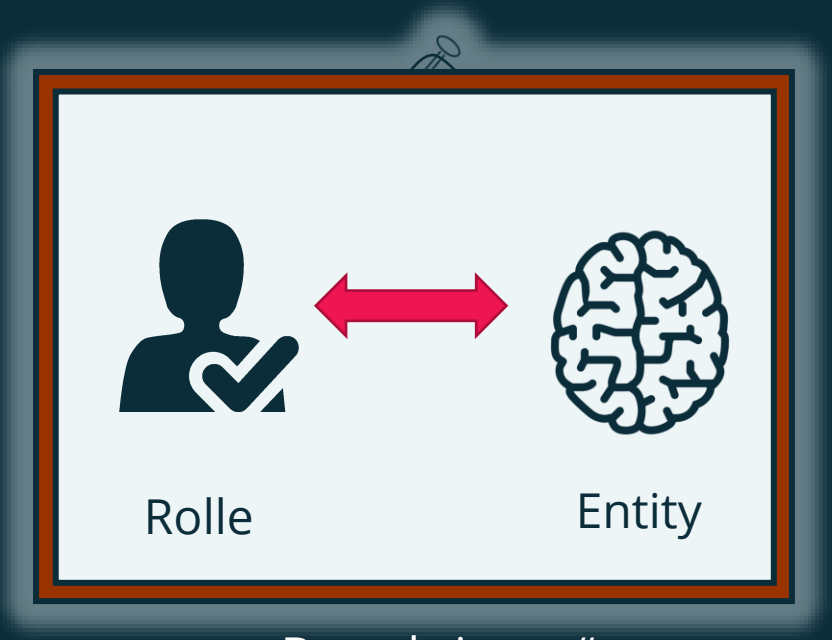


Button „Serienaktion“

Wenn an allen Aktionen, die einer Serienaktion untergeordnet sind, das Property „usePermission“ aktiv ist, und ein User keine Rolle erhält, die auf eine der Aktionen berechtigt, wird der Button „Serienaktion“ ausgeblendet.



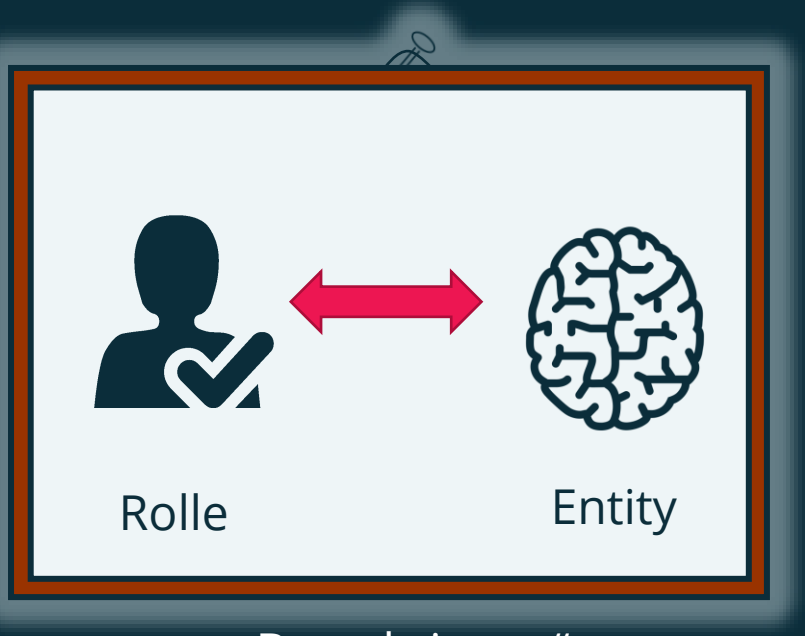
„Zwei Blick-Richtungen“



„Berechtigung“

„Zwei Blick-Richtungen“

Aus Perspektive des Entitys: „Welche Rollen sind auf mich berechtigt?“



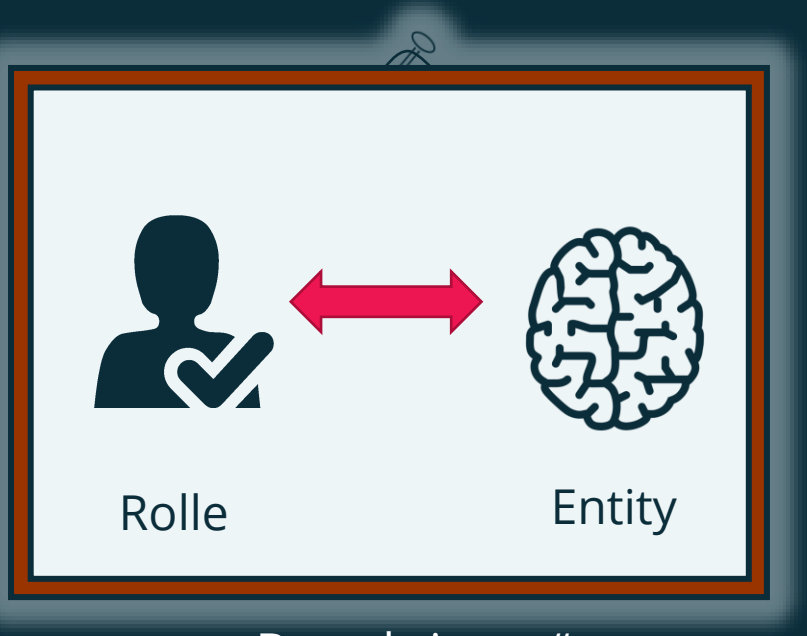
„Berechtigung“

Context
„Berechtigung“

„Zwei Blick-Richtungen“

Aus Perspektive der Rolle: „Auf welche Entitys bin ich berechtigt?“

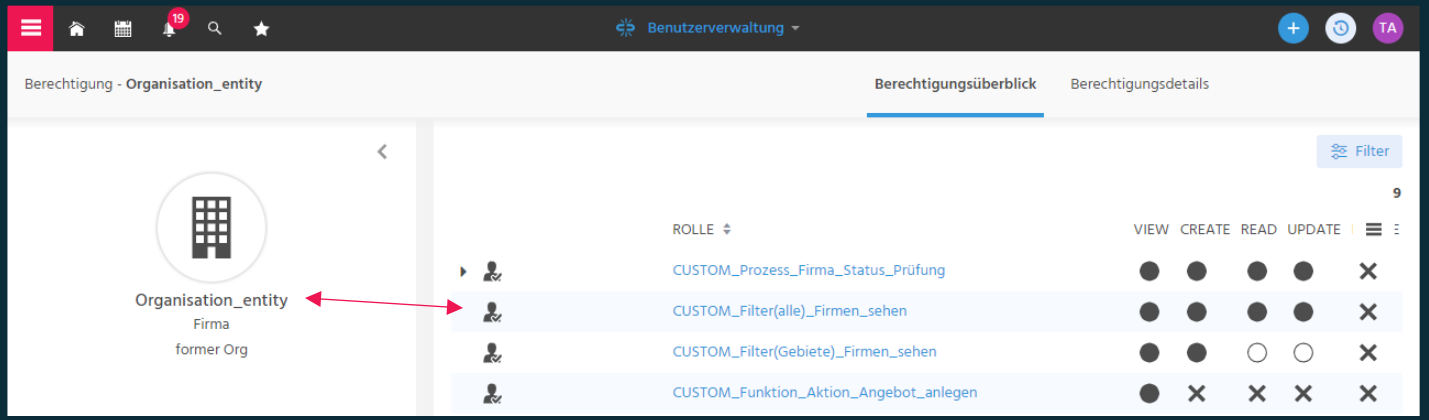
Context
„Rolle“



„Berechtigung“

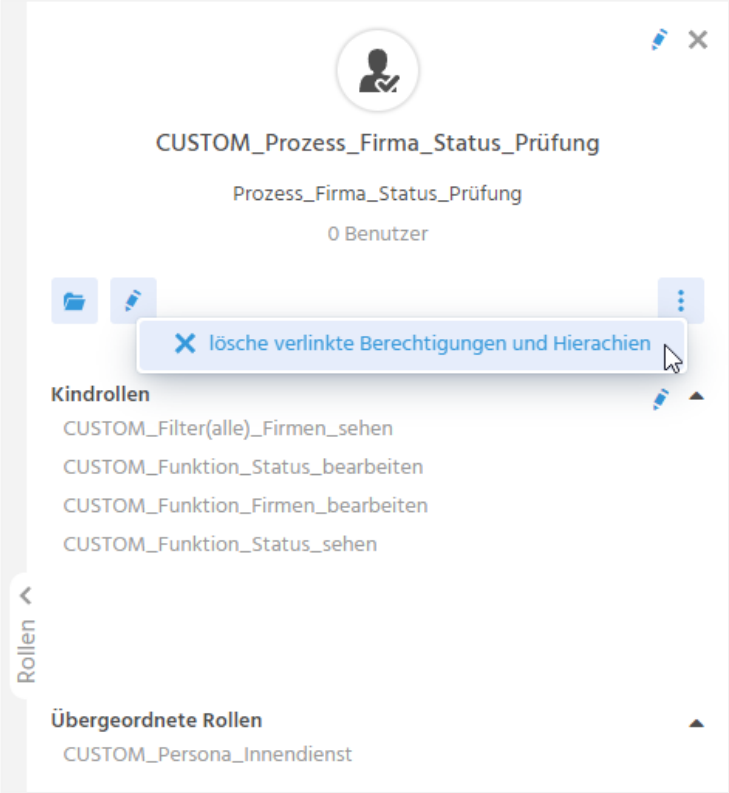
„Zwei Blick-Richtungen“

Context „Rolle“



Context „Berechtigung“

Rollen löschen

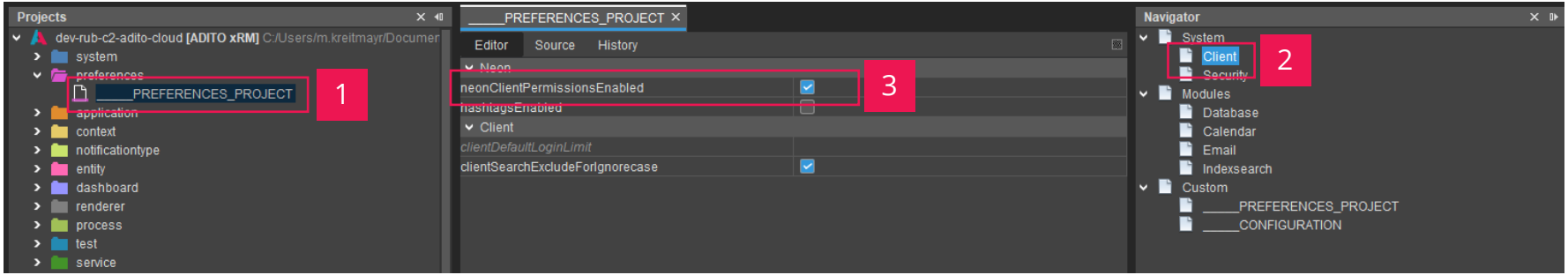


Sie können CUSTOM-Rollen im Client löschen, wenn diese keine Verlinkungen zu Berechtigungen oder nicht in Hierarchien (Rollengruppen) verwendet werden.

Vorgehen um eine Rolle zu löschen:

1. Aktion „Lösche verlinkte Berechtigungen und Hierarchien“ ausführen
2. Rolle in der Filteransicht auswählen oder Vorschau öffnen und Aktion „Löschen“ ausführen

Deaktivierung der Berechtigungen



4 Deploy

5 Server neu starten


ADITO®
Einzigartige Beziehungen