KomMonitor
Kommunales Monitoring zur Raumentwicklung

52°North

Dokumentation Mandantenfähigkeit KomMonitor

Stand: 16.10.2024

Inhalt

1 Einleitung

Kreise und deren kreisangehörige Städte stellen besondere Anforderungen an die gemeinsame Nutzung einer KomMonitor Instanz. Insbesondere der Wunsch nach kommunaler Autonomie in der Verwaltung von Datensätzen, Benutzern, Rollen und Zugriffsrechten erforderte die Erweiterung des bestehenden Rechte-Managements in KomMonitor. Dieses Dokument beschreibt das neue Konzept der Mandantenfähigkeit von KomMonitor, das Kreise und kreisfreie Städte in die Lage versetzt, eine gemeinsame KomMonitor Instanz sowohl selbst- als auch fremdverwaltet zu nutzen. In einigen Abschnitten werden Unterschiede zum alten Rollen- und Rechtemodell aufgezeigt. Der Begriff „altes Rollen- und Rechtemodell“ bezieht sich dabei auf folgende KomMonitor Versionen:

- Data Management API < 5.0.0
- Web Client < 4.0.0

Das Dokument beschreibt außerdem das Konzept des Rollen- und Rechtemodells zum Stand der Umsetzung von Milestone 6, der Teil einer umfassenden Roadmap ist(siehe Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.**), die darauf abzielt weitere Aspekte einer Mandantenfähigkeit von KomMonitor umzusetzen.

2 Konzept

2.1 Mandanten- und Gruppenkonzept

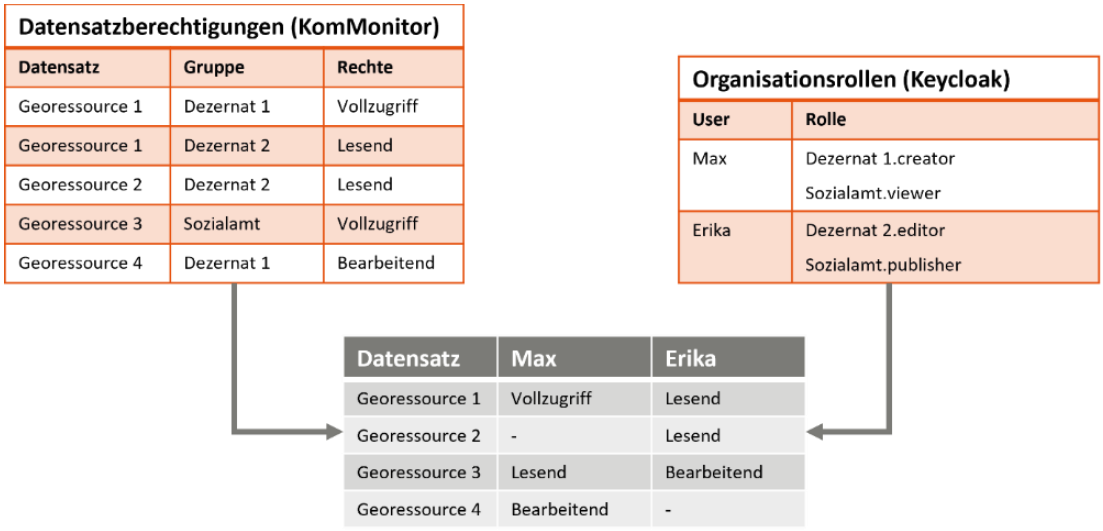
2.1.1 Altes Rollen- und Rechtemodell

Das alte Rollen- und Rechtemodell sah eine implizite Gruppenmitgliedschaft von Usern vor. Für jede Organisationseinheit in KomMonitor existierte ein Satz von vier verschiedenen Organisationsrollen innerhalb von Keycloak:

- ***<orga>.viewer***: Darf Datensätze für eine Organisation lesen
- ***<orga>.editor***: Darf Datensätze für eine Organisation bearbeiten
- ***<orga>.publisher***: Darf Datensätze für eine Organisation veröffentlichen
- ***<orga>.creator***: Vollzugriff auf Datensätze für eine Organisation

Durch die Zuweisung einer Organisationsrolle an einen User wurde die Rechtestufe eines Users innerhalb einer Organisation festgelegt. Gleichzeitig konnte für Datensätze in KomMonitor festgelegt werden, welche Gruppe welche Rechte für einen Datensatz besitzt. Welche Rechte ein bestimmter User für einen Datensatz besitzt, bestimmte zum einen die Organisationsrolle eines Users und zum anderen die Datensatzfreigaben für die Organisation, die der User angehört. Durch das vierstufige Rechtekonzept konnten unterschiedliche User unterschiedliche Rechte für eine Organisation besitzen.

Beispiel:



Datensatzberechtigungen (KomMonitor)

Datensatz	Gruppe	Rechte
Georessource 1	Dezernat 1	Vollzugriff
Georessource 1	Dezernat 2	Lesend
Georessource 2	Dezernat 2	Lesend
Georessource 3	Sozialamt	Vollzugriff
Georessource 4	Dezernat 1	Bearbeitend

Organisationsrollen (Keycloak)

User	Rolle
Max	Dezernat 1.creator Sozialamt.viewer
Erika	Dezernat 2.editor Sozialamt.publisher

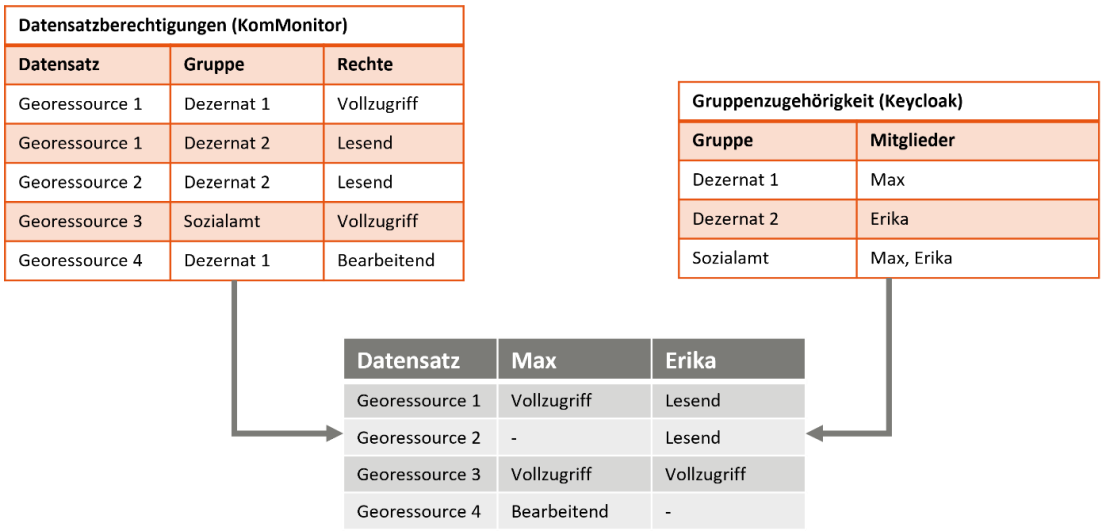
Datensatz	Max	Erika
Georessource 1	Vollzugriff	Lesend
Georessource 2	-	Lesend
Georessource 3	Lesend	Bearbeitend
Georessource 4	Bearbeitend	-

Abbildung 1: Altes Rollen und Rechtemodell. Die Zugriffsrechte eines Users setzen sich aus den Datensatzberechtigungen und der Organisationsrollen eines Users zusammen.

2.1.2 Neues Gruppen- und Rechtekonzept

Das neue Gruppen- und Rechtekonzept sieht zum einen eine explizite Gruppenmitgliedschaft von Usern und zum anderen eine Vergabe von Datensatzberechtigungen an Gruppen vor. Eine Rechtevergabe an User erfolgt daher nun über Keycloak Gruppen und nicht über die Zuweisung von Organisationsrollen. Zu diesem Zweck besteht eine 1:1 Zuordnung zwischen Organisationseinheiten, die in KomMonitor existieren und Gruppen in Keycloak. Diese Verknüpfung ist technisch so implementiert, dass für jede Organisationseinheit, die in KomMonitor angelegt wurde, gleichzeitig auch eine Keycloak Gruppe mit demselben Namen erzeugt wird. Es fällt die Möglichkeit der unterschiedlichen Rechtestufen innerhalb einer Organisation weg. Alle User innerhalb einer Gruppe besitzen dieselben Rechte in Bezug auf Datensätze sowie dieselben administrativen Berechtigungen (siehe Abschnitt 2.3).

Beispiel:



Datensatzberechtigungen (KomMonitor)

Datensatz	Gruppe	Rechte
Georessource 1	Dezernat 1	Vollzugriff
Georessource 1	Dezernat 2	Lesend
Georessource 2	Dezernat 2	Lesend
Georessource 3	Sozialamt	Vollzugriff
Georessource 4	Dezernat 1	Bearbeitend

Gruppenzugehörigkeit (Keycloak)

Gruppe	Mitglieder
Dezernat 1	Max
Dezernat 2	Erika
Sozialamt	Max, Erika

Datensatz	Max	Erika
Georessource 1	Vollzugriff	Lesend
Georessource 2	-	Lesend
Georessource 3	Vollzugriff	Vollzugriff
Georessource 4	Bearbeitend	-

Abbildung 2: Neues Rollen- und Rechtemodell. Die Zugriffsrechte eines Users richten sich ausschließlich nach den Datensatzberechtigungen und der Gruppenzugehörigkeit eines Users. Es gibt keine Rechteabstufungen innerhalb einer Gruppe.

Registrierte User können Mitglied von 1 - n Gruppen in Keycloak sein. Die Rechte, die ein registrierter Benutzer hat, werden einzig über die Benutzergruppen definiert, denen er angehört.

2.1.3 Gruppenhierarchien

Gruppen können hierarchisch angelegt sein. Eine neu angelegte Gruppe besitzt entweder eine bereits vorhandene Gruppe als Obergruppe und ist damit Teil eines Mandanten oder bildet selber einen Wurzelknoten für weitere Untergruppen.

2.1.4 Mandanteneigenschaft

Gruppen, die selber keine Obergruppe besitzen und einen Wurzelknoten bilden, fungieren als Mandant. Jeder Mandant besitzt jeweils eine eigene Gruppenhierarchie. Es gibt keine Mandantenübergreifenden Gruppen, also keine Gruppen, die mehreren Mandanten angehören. Jeder Mandant besitzt seine eigene unabhängige Gruppenstruktur. Ebenso sind Benutzer und Datensätzen von KomMonitor nur einem einzigen Mandanten angehörig. Ein Mandant, bzw. eine Gruppe, die für den Mandanten die Verwaltung übernimmt, ist verantwortlich für die Verwaltung von Benutzern und Datensätzen die dem gleichen Mandanten angehören.

2.1.5 Anonyme Benutzer

Anonyme Benutzer gehören dagegen keiner Benutzergruppe an. Anonyme Benutzer sind nicht in Keycloak registriert und können KomMonitor lediglich ohne Anmeldemöglichkeit benutzen. In der Kartenoberfläche stehen anonymen Benutzern daher lediglich Datensätze zur Verfügung, die explizit in der KomMonitor Admin UI der Öffentlichkeit freigegeben wurden.

2.2 Eigentümerschaft an Datensätzen

Für jeden KomMonitor Datensatz (Indikatoren, Raumeinheiten und Georessourcen) muss eine Eigentümerschaft hinterlegt sein. Eigentümer eines Datensatzes kann nur eine bestimmte Organisationseinheit/Gruppe sein und kein individueller Benutzer. Benutzer, die das Recht zur Datenverwaltung für eine Gruppe, die Eigentümer eines Datensatzes ist, besitzen, können ebenfalls als Eigentümer für die eigentliche Eigentümer-Gruppe handeln.

2.3 Feingranulare administrative Berechtigungen

Das alte Rollen- und Rechtemodell von KomMonitor sah lediglich eine einzige globale Administratorrolle vor, nämlich den „kommonitor-creator“. User, die diese Rolle besaßen, hatten vollumfängliche Rechte um

- neue Organisationen und die dazugehörigen Rollen *-viewer, *-editor, *-publisher, *-creator über die KomMonitor Admin-UI anzulegen,
- Nutzer in Keycloak anzulegen und zu verwalten sowie Rollen zuzuweisen,
- technische Konfigurationen in der KomMonitor Admin-UI vorzunehmen,
- Themen anzulegen und zu verwalten sowie
- Vollzugriff auf alle Datensätze in KomMonitor zu erhalten.

Diese weitgefassten administrativen Rechte sind insbesondere in Situationen kritisch zu sehen, in denen mehrere Kommunen sich innerhalb derselben KomMonitor-Instanz vollkommen autonom verwalten möchten oder lediglich einen Teil der administrativen Aufgaben an den Kreis delegieren möchten. Denkbar ist etwa, dass ein Kreis (oder jede beliebige andere Organisationseinheit) die

Gruppen- und Nutzerverwaltung für eine Kommune übernimmt, während die Kommune weiterhin für die Administration von Themen und Datensätzen verantwortlich ist. Aus diesem Grund wurde die global Administratorrolle (die weiterhin existieren wird) um zusätzliche fein-granulare administrative Rollen ergänzt:

- ***.client-user-creator***
  Kann Nutzer für eine Gruppen und alle untergeordneten Gruppen in Keycloak administrieren
- ***.client-resources-creator***
  Kann Ressourcen für eine Gruppe und alle untergeordneten Gruppen administrieren
- ***.client-themes-creator***
  Kann Themen für eine Gruppen und alle untergeordneten Gruppen in KomMonitor administrieren
- ***. unit-user-creator***
  Kann Nutzer für eine Gruppe, aber nicht die untergeordneten Gruppen administrieren
- ***. unit-resources-creator***
  Kann Ressourcen für einen Gruppe, nicht jedoch für die untergeordneten Gruppe administrieren
- ***. unit-themes-creator***
  Kann Themen für eine Gruppe, nicht jedoch für die untergeordneten Gruppen in KomMonitor administrieren

Beispiel:
Nutzer Max besitzt folgende Rollen aus bestimmten Gruppenmitgliedschaften:

- *Demo Kreis.client-user-creator:*
  Das Recht, für die Gruppe „Demo Kreis“ sowie für all derer Untergruppen die User und Gruppen zu verwalten
- *Team 42.unit-resources-creator*
  Das Recht, nur für “Team 42” Datensätze zu verwalten
- *Team 42.unit-themes-creator*
  Das Recht, nur für „Team 42“ Themen zu verwalten

Diese Rollen werden Gruppen zugewiesen, sodass die Mitglieder solcher Gruppen mit entsprechenden Rechten ausgestattet werden. Es findet keine direkte Rollenzuweisung an Usern statt, sodass alle User, die Mitglied derselben Gruppe sind, dieselben administrativen Berechtigungen besitzen. Außerdem wurde für die Rechtevergabe eine Oberfläche in der KomMonitor Admin UI geschaffen (siehe Abbildung 3), sodass eine Vergabe von Rollen an Gruppen nicht mehr über die Keycloak Oberfläche erfolgen muss.

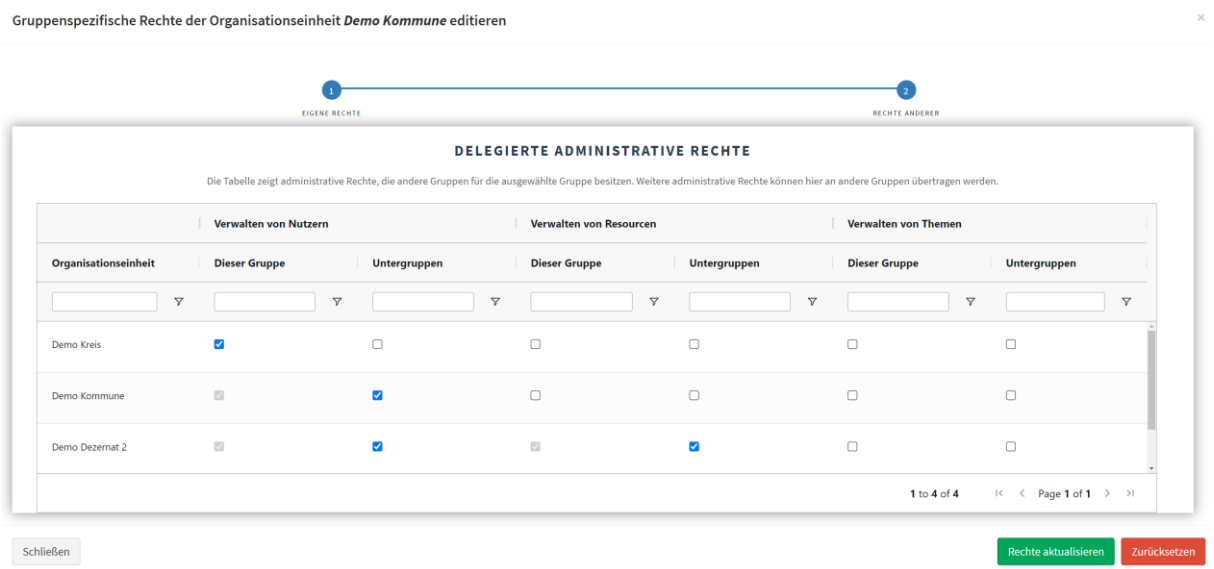


Abbildung 3: Vergabe administrativer Berechtigungen über die KomMonitor Admin UI

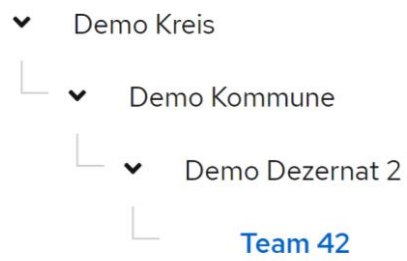
3 Erste Schritte

3.1 Use Case

Zur Einrichtung eines selbstverwalteten Mandanten in KomMonitor werden in den folgenden Abschnitten alle notwendigen Schritte samt Screenshots beschrieben. Dabei folgen die einzelnen Schritte durchgängig einem gängigen Use Case beim Umgang mit Mandanten in KomMonitor:

- Ein globaler KomMonitor Admin richtet für alle Mandanten eine Gruppe ein
- Dem Mandanten wird das Recht übertragen sich selber vollständig zu verwalten
- Für jede Mandanten-Gruppe wird ein User in Keycloak angelegt. Durch die Mitgliedschaft in der Mandanten-Gruppe wird er zum Mandanten-Admin.
- Jede weitere Strukturierung des Mandanten obliegt dem Mandanten-Admin

Die Mandantenstruktur gliedert sich dabei wie folgt:



Wir haben es in unserem Demo Use-Case also mit einer sehr einfachen hierarchischen Struktur für einen einzigen Mandanten, dem „Demo Kreis“ zu tun. Generell sind auch durchaus komplexere Hierarchien mit mehreren Mandanten und mehreren Untergruppen auf einer Ebene möglich.

3.2 Use Case Ablauf

Zur Umsetzung des Use Case ist die Durchführung folgender Schritte notwendig, die in den folgenden Abschnitten detailliert beschrieben werden:

1. Anmelden als User mit der Rolle *kommonitor-creator* beim KomMonitor Web Client
2. Anlegen eines Mandanten im Bereich Gruppenverwaltung
3. Vergabe der Rechte zur Selbstverwaltung für User, Ressourcen und Themen an den Mandanten (Rechte für Mandanten selber und dessen Untergruppen)
4. Anlegen eines neuen Users, der Administrator für den Mandanten sein soll
    a. Anmelden als User mit der Rolle *kommonitor-creator* bei Keycloak
    b. Neuen User anlegen und Zuweisung des Users in Gruppe, die dem Mandanten entspricht
5. Anmeldung als Mandanten-Admin beim KomMonitor Web Client und bei Keycloak
6. Aufbau der Mandantenstruktur
    a. Aufbau der Gruppenhierarchie innerhalb des Mandanten durch Erstellen von Untergruppen des Mandanten
    b. Vergabe von administrativen Rechten für Untergruppen des Mandanten sowie Vergabe von Rechten für Datensätze
    c. Erstellen von weiteren Usern in Keycloak und Einteilung in Gruppen

3.3 Einzelschritte

3.3.1 Anmeldung als globaler Admin

Globale Administratoren sind wie gehabt User, die die *kommonitor-creator* Rolle besitzen. Administratoren haben vollumfängliche Rechte in allen Programmbereichen von KomMonitor und Keycloak sowie in Bezug auf Organisationseinheiten und Datensätze (Themen, Georessourcen, Indikatoren, Raumeinheiten). Nur Administratoren können eigenständige Mandanten anlegen. Während sich Mandanten untereinander nicht verwalten können, haben globale Administratoren Vollzugriff auf alle Mandanten einer KomMonitor Instanz.

Damit das Anlegen von Mandanten über die KomMonitor Admin UI möglich ist, müssen sich globale Administratoren daher zunächst in KomMonitor anmelden. Nach erfolgter Anmeldung führt das überarbeitete Login-Fenster die *kommonitor-creator*-Rolle als effektive Rolle des angemeldeten Users auf (siehe Abbildung 4).

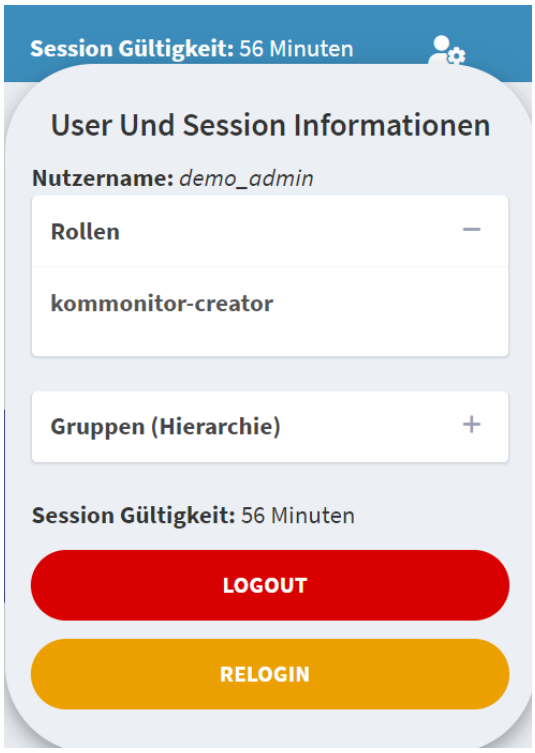


Abbildung 4: Anmeldung als kommonitor-creator im Login-Bereich von KomMonitor

3.3.2 Anlegen eines Mandanten

Das Anlegen eines Mandanten ist im Bereich zur Verwaltung von Organisationseinheiten der KomMonitor Admin UI möglich. Nach erfolgter Anmeldung als globaler Administrator steht dieser Programmbereich zur Verfügung und kann aufgerufen werden. Zum Anlegen eines Mandanten muss eine neue Organisationseinheit registriert werden (siehe Abbildung 5).

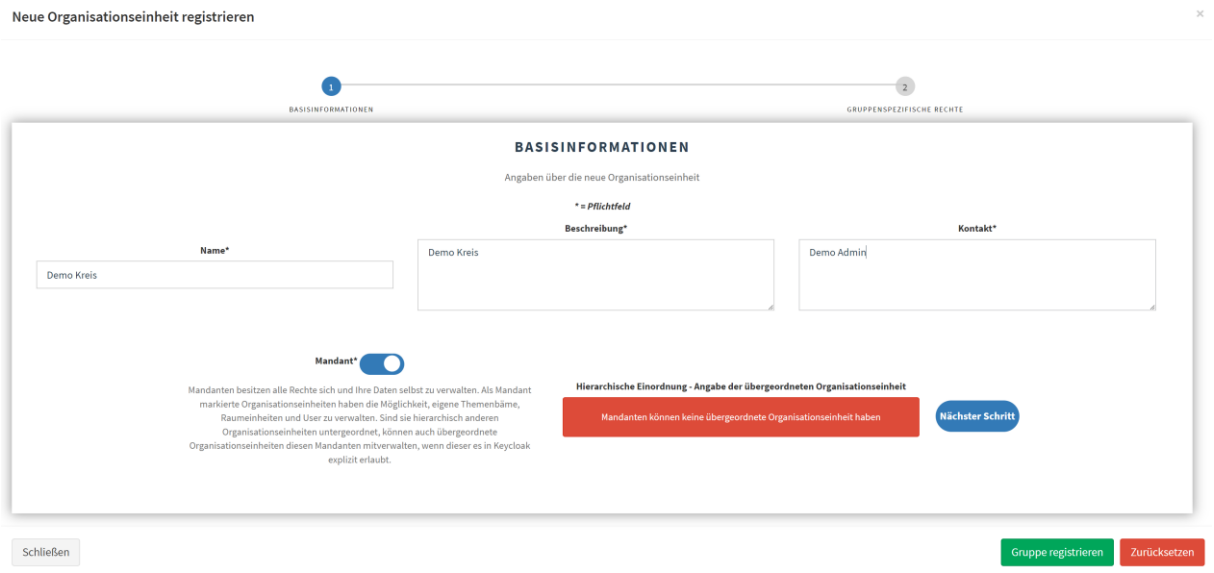


Abbildung 5: Registrierung einer neuer Organisationseinheit als Mandant

Standardmäßig werden Organisationseinheiten nicht als eigener Mandant sondern als Bestandteil (Untergruppe) eines bestehenden Mandanten angelegt. Die Kennzeichnung einer Gruppe als Mandant erfolgt explizit durch die Aktivierung des entsprechenden Toggle-Buttons (siehe Abbildung 6).

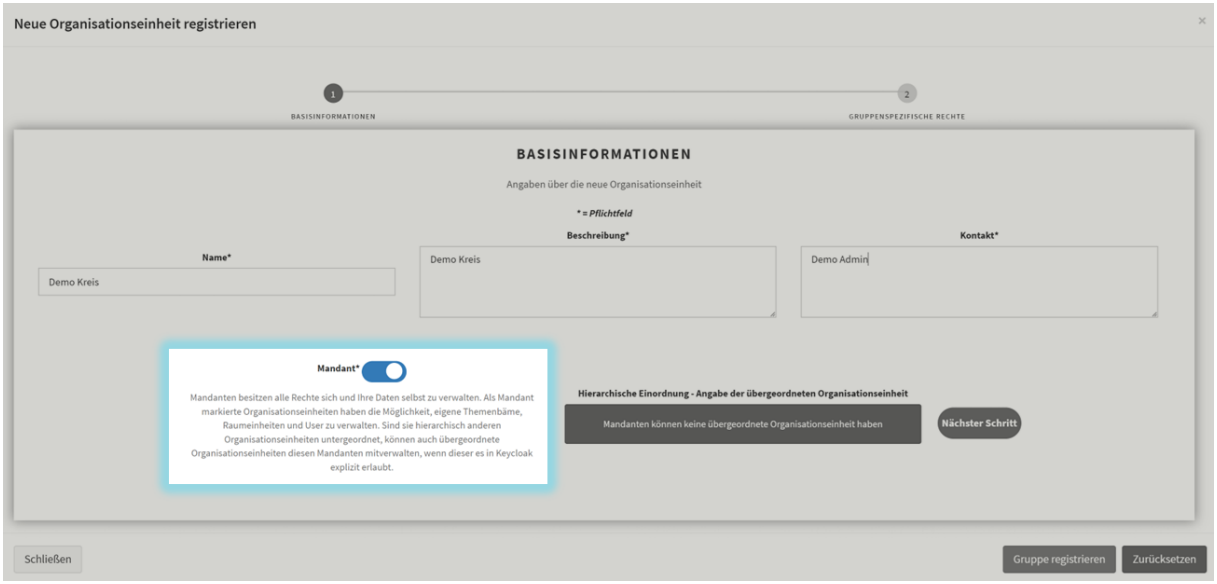


Abbildung 6: Kennzeichnung einer neuen Organisationsienheit als Mandant

Mandanten können außerdem kein Bestandteil eines anderen Mandanten sein. Sie stehen in der Gruppenhierarchie also am oberen Ende als Wurzelknoten und besitzen keine Obergruppen. Eine hierarchische Einordnung kann daher nicht für Organisationseinheiten vorgenommen werden, die als Mandant gekennzeichnet wurden (siehe Abbildung 7).

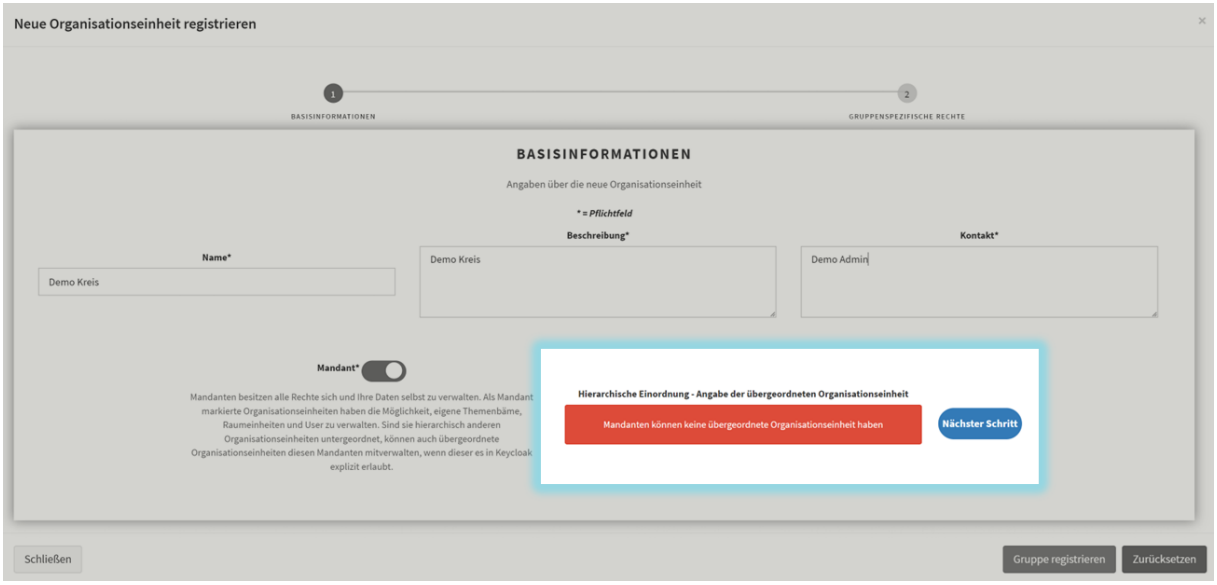


Abbildung 7: Eine hierarchische Einordnung als Untergruppe ist für Mandanten nicht möglich

Nachdem eine Organisationseinheit als Mandant registriert wurde, ist diese in der Übersichtstabelle der Admin UI aufgelistet. In einer separaten Spalte der Übersichtstabelle wird die Mandanteneigenschaft ausgewiesen.

3.3.3 Vergabe der Rechte zur Selbstverwaltung

Damit sich ein Mandant selbstverantwortlich verwalten kann, müssen diesem durch den globalen Administrator zunächst noch alle notwendigen Rechte zugewiesen werden. Unterschieden werden administrative Berechtigungen zur Verwaltung von Themen, Ressourcen und Nutzern (siehe Abschnitt 2.3). Diese Rechte können sich jeweils nur auf eine einzelne Organisationseinheiten/Gruppe beziehen

oder aber auch alle Untergruppen mit einbeziehen. Die Zuweisung von administrativen Berechtigungen an Organisationseinheiten ist im Programmbereich „Gruppenverwaltung“ über den „Rechte verwalten“ Button möglich (siehe Abbildung 8).

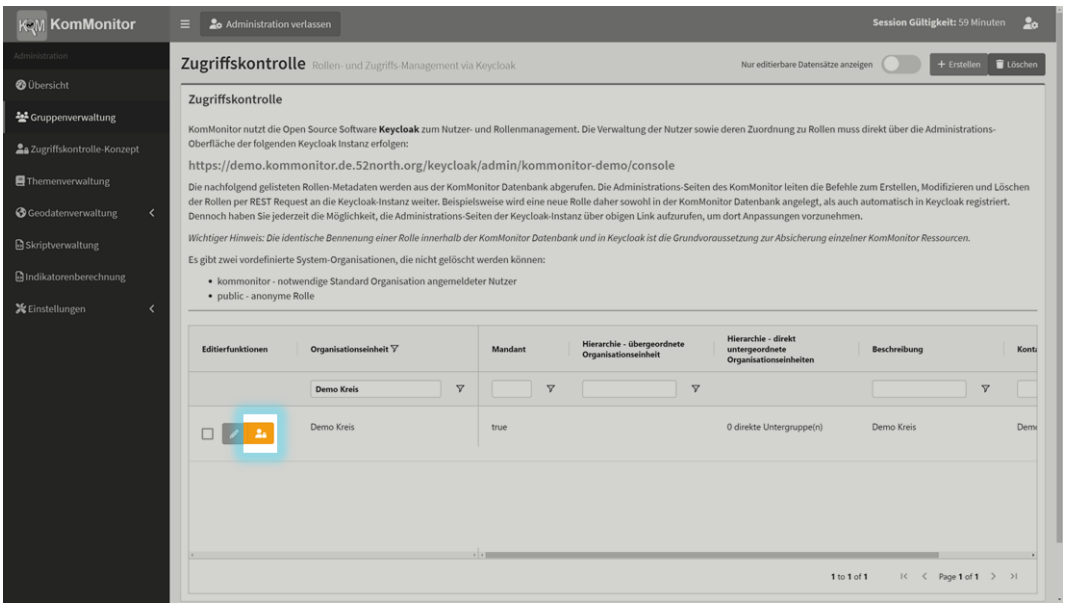


Abbildung 8: Verwaltung administrative Berechtigungen über den "Rechte verwalten" Button

Im sich öffnenden Fenster zur Rechteverwaltung gibt es zwei verschiedene Seiten. Die Seite „Eigene Rechte“ bietet eine Übersicht über alle administrativen Rechte der ausgewählten Gruppe (siehe Abbildung 9). Eine Gruppe kann sich jedoch nicht selber Rechte für andere Gruppen geben. Daher ist diese Tabelle nicht editierbar.

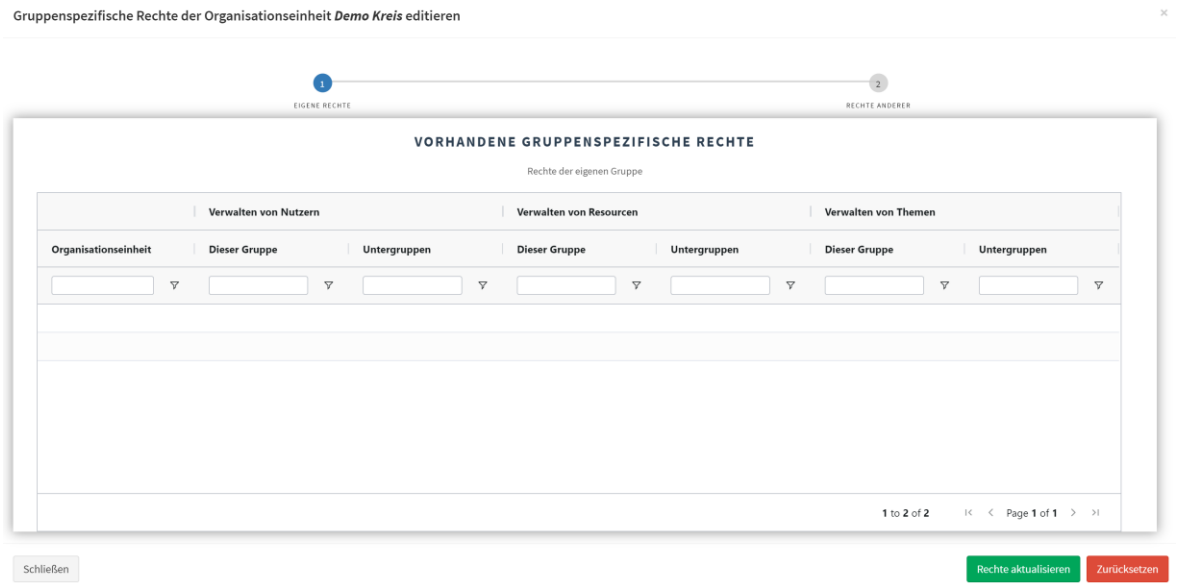


Abbildung 9: Übersicht aller bestehenden administrativen Rechte einer Gruppe

Auf der Seite „Rechte Anderer“ können dagegen anderen Gruppen administrative Rechte für die ausgewählte Gruppe zugewiesen werden. Um dem Mandanten „Demo Kreis“ das Recht zu Selbstverwaltung zu geben wird für dieselbe Gruppe in allen drei administrativen Bereichen (Nutzer, Ressourcen, Themen) jeweils das Recht zur eigenen Verwaltung und zur Verwaltung aller (bestehenden und zukünftigen) Untergruppen gegeben (siehe Abbildung 10). Demnach sind alle Checkboxes aktiviert.

In Fällen, in denen ein Mandant die Verwaltung nur eines administrativen Bereichs für seine Untergruppen vornehmen soll (z.B., wenn ein Mandant nur die Nutzerverwaltung für seine Gruppen übernimmt), können natürlich auch nur die dafür vorgesehenen Checkboxes aktiviert.

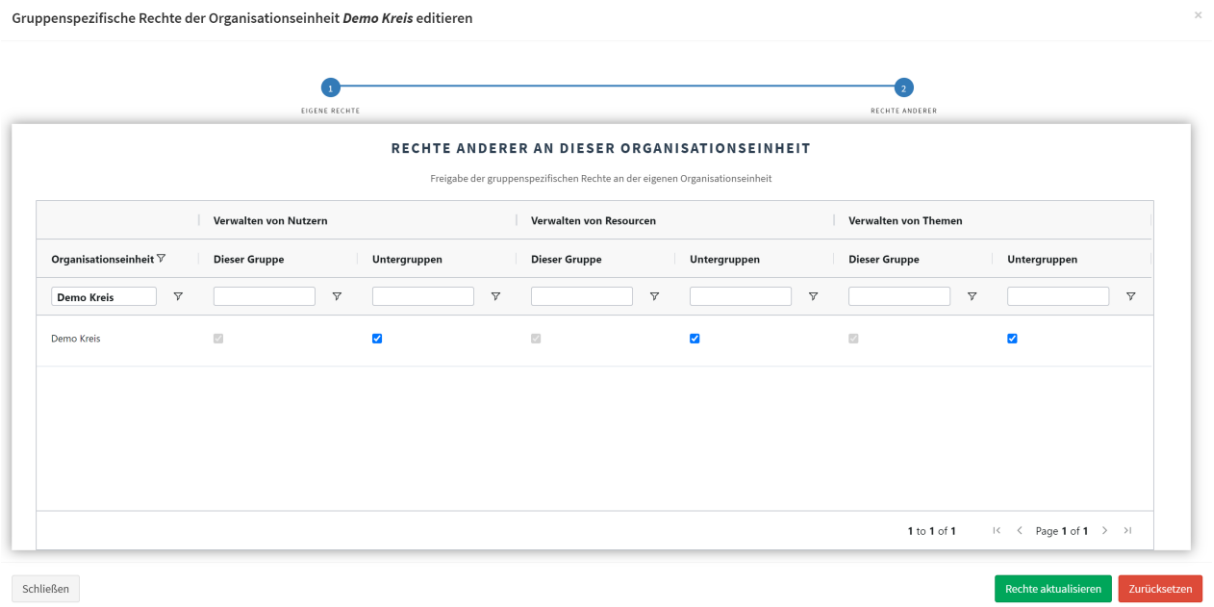


Abbildung 10: Übersicht der administrativen Rechte anderer Gruppen an der ausgewählten Gruppe

Nachdem über den „Rechte aktualisieren“ Button die administrativen Rechte übertragen wurden, werde diese für diejenigen Gruppen, die die neuen Rechte erhalten haben, auf der Seite „Eigene Rechte“ gelistet (siehe .Abbildung 11).

Wichtiger Hinweis:
In der aktuellen Version zum Zeitpunkt der Erstellung dieses Handbuchs ist es noch notwendig, KomMonitor neu zu laden, z.B. über „F5“, damit die neu vergebenen Rechte abgerufen und gelistet werden.

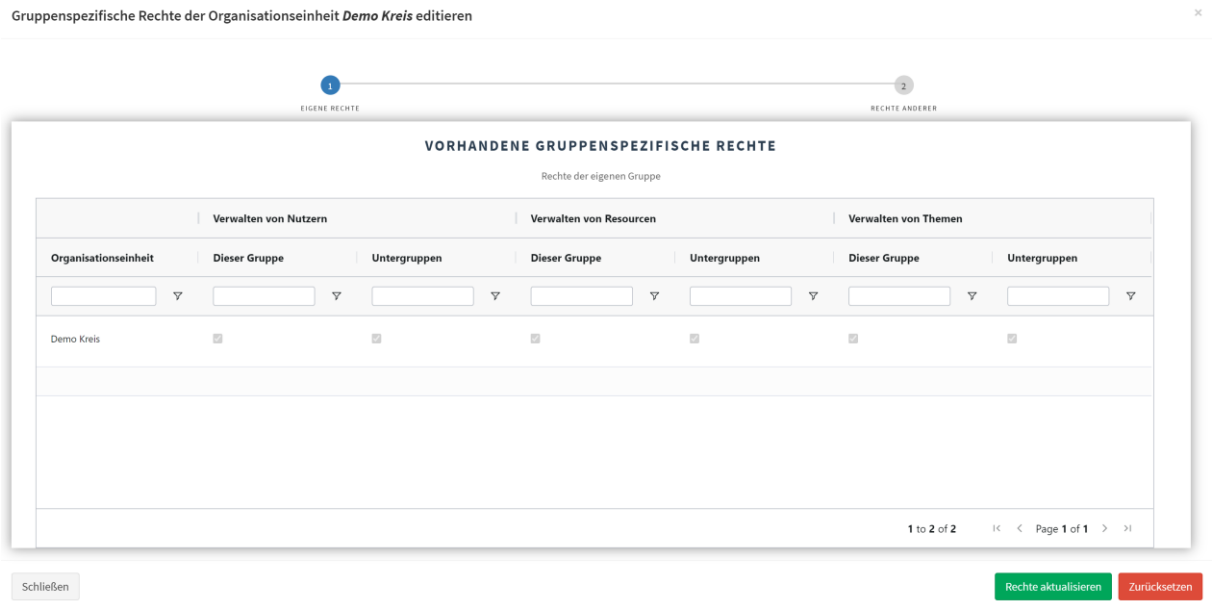


Abbildung 11: Neu vergebene Rechte werden unter "Eigene Rechte" gelistet

3.3.4 Anlegen eines Users als Mandanten-Administrators

Nun kann der globale Administrator dazu übergehen, einen Administrator für den soeben angelegten Mandanten anzulegen. Hierzu ist das Registrieren eines Users in Keycloak notwendig. Im Bereich „Gruppenverwaltung“ der KomMonitor Admin UI ist der Link zur jeweilig zuständigen Keycloak-Instanz aufgeführt (siehe Abbildung 12). Durch Klick auf diesen Link, öffnet sich Keycloak im Browser und der globale Administrator kann sich dort anmelden.

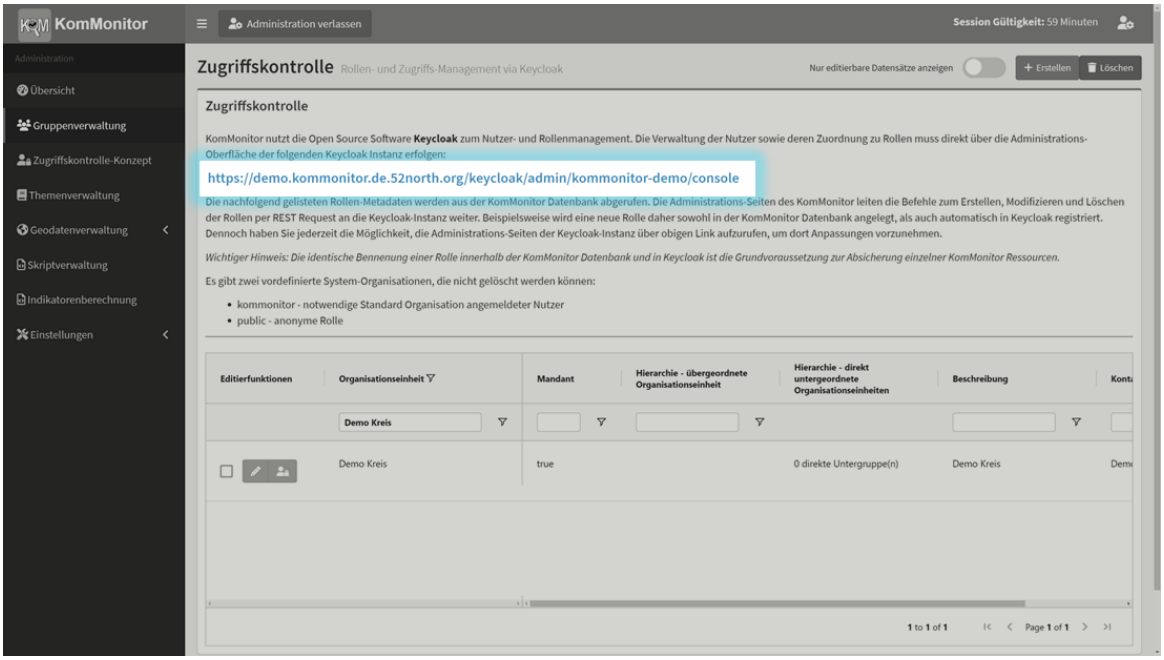


Abbildung 12: Link zur Keycloak-Instanz im Bereich "Gruppenverwaltung"

Natürlich kann jeder beliebige vorhandene User in Keycloak zum Administrator für den Mandanten bestimmt werden. In unserem Use Case gehen wir jedoch von einer leeren Instanz aus, bei der lediglich der globale Administrator in Keycloak registriert wurde. Somit muss der globale Administrator nun einen neuen User in Keycloak anlegen (siehe Abbildung 13).

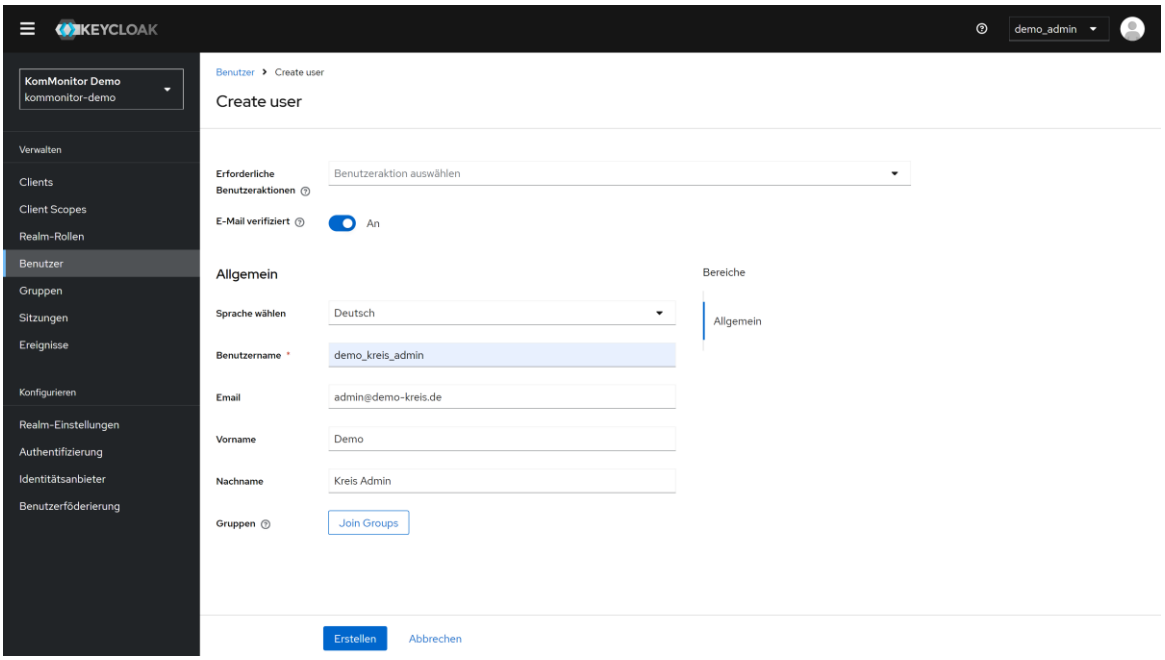


Abbildung 13: Registrierung eines Users in Keycloak

Wie gehabt werden alle Informationen zum User eingetragen sowie ein Passwort für den User hinterlegt. Nachdem der User registriert wurde, muss dieser nun zum Administrator für den Mandanten gemacht werden. Dies erfolgt allerdings nicht wie beim alten Nutzer- und Rollenkonzept durch die direkte Zuweisung von Rollen, sondern durch die Zuweisung des Users in eine Gruppe, der zuvor über die KomMonitor Admin UI administrative Berechtigungen zur Verwaltung des Mandanten zugewiesen wurden (siehe Abschnitt 3.3.3). Dies ist über den Gruppen-Tab in der Keycloak-Oberfläche möglich. Im sich nun öffnenden Fenster werden alle zuvor angelegten Gruppen aufgelistet (siehe Abbildung 14). Hier ist auch die zuvor registrierte Mandanten-Gruppe zu finden. Bei einer Vielzahl von Gruppen, ist es ratsam, die Suchfunktion innerhalb des Fensters zu verwenden. Soll nun eine Gruppe ausgewählt werden, der der User zugewiesen werden soll, muss die entsprechende Checkbox der Gruppe aktiviert werden.

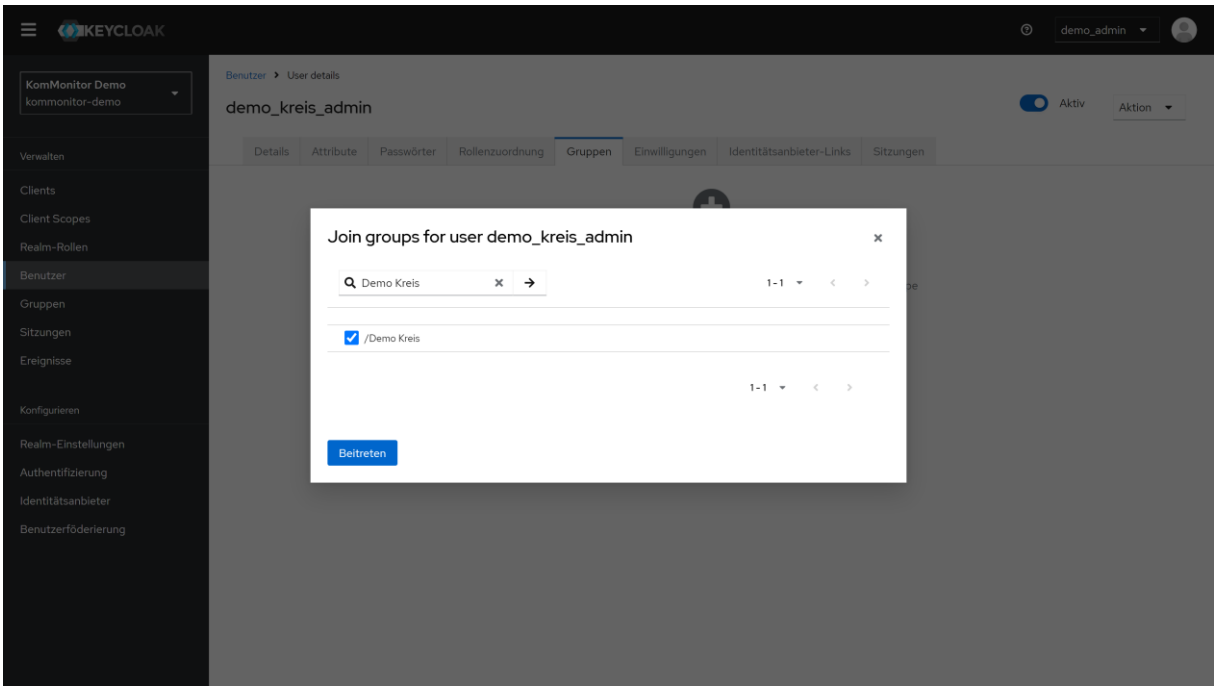


Abbildung 14: Zuweisung eines Users zu einer Keycloak-Gruppe

Für unseren Use Case wird der User lediglich der Mandanten-Gruppe zugewiesen. Mit Klick auf den „Betreten“ Button, wird der User Mitglied in der Mandanten-Gruppe. Da wir der Mandanten-Gruppe zuvor alle Rechte zur Selbstverwaltung zugewiesen hatten, wird der User somit de-facto zum Administrator des Mandanten. Der globale Administrator kann sich nun zurücklehnen und die gesamte weitere Verwaltung des Mandanten dem neu angelegten User überlassen.

Wichtiger Hinweis:
Die direkte Zuweisung von Rollen an User ist weiterhin über die Keycloak-Oberfläche möglich. Allerdings werden administrative Rechte, die in Verbindung mit bestimmten Rollen stehen, nur durch die direkte Mitgliedschaft in einer Gruppe, der administrative Berechtigungen zugewiesen wurden, wirksam. Direkt zugewiesene Rollen, die nicht in Verbindung mit einer Gruppenmitgliedschaft erworben wurden, sind nicht wirksam in KomMonitor.

3.3.5 Anmeldung als Mandanten-Admin

Der im vorigen Abschnitt registrierte User ist nun in der Lage als Administrator für den Mandanten zu handeln. Hierzu meldet er sich mit den ihm bekannten Credentials beim KomMonitor Web Client an. Das Info-Fenster im Login-Bereich listet nun alle mit administrativen Rechten verbundenen Rollen auf, die der User durch die Mitgliedschaft in der Mandanten-Gruppe erhalten hat sowie die Gruppenmitgliedschaft(en) auf (siehe Abbildung 15).

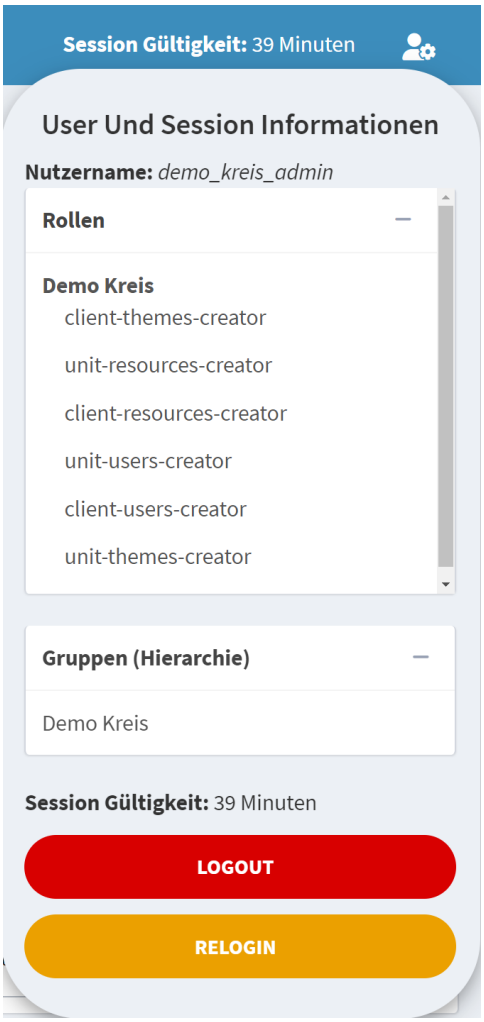


Abbildung 15: Anmeldung als Mandanten-Admin im Login-Bereich von KomMonitor

Im Bereich „Gruppenverwaltung“ stehen dem Mandanten-Admin nun alle Gruppen seines Mandanten zur Verwaltung zur Verfügung (siehe Abbildung 16). Es werden ausschließlich Gruppen des einzigen Mandanten, für den der User als Administrator handelt aufgeführt. Gruppen anderer Mandanten können nicht durch ihn verwaltet werden und werden daher auch nicht aufgeführt. Es besteht eine strenge Abgrenzung zwischen verschiedenen Mandanten.

In unserem Use Case wurde bisher lediglich die Mandanten-Gruppe angelegt, sodass dies auch die einzige aufgeführte Gruppe in der Übersichtstabelle ist.

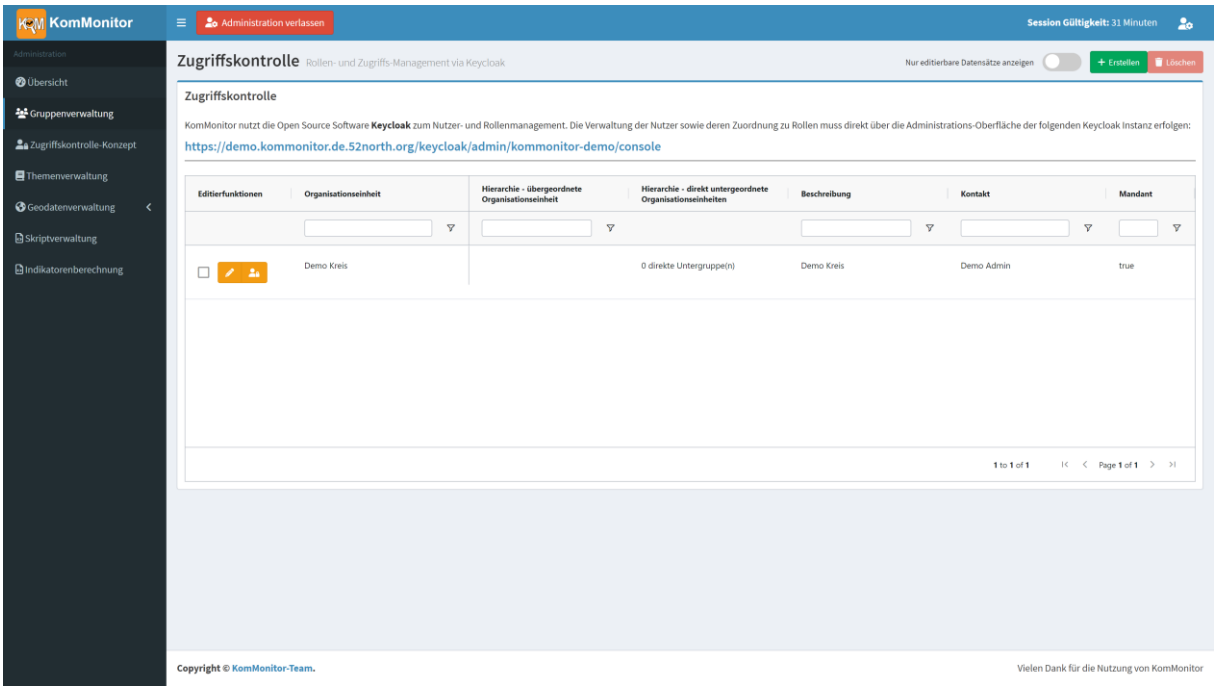


Abbildung 16: Übersichtstabelle zu allen Organisationseinheiten/Gruppen eines Mandanten

Als Mandanten-Admin können nun alle vorhandenen Gruppen, wie etwa auch die Mandanten-Gruppe editiert werden (siehe Abbildung 17). Es lassen sich jedoch lediglich Infos zur Gruppe anpassen. Ein Zurücksetzen der Mandanten-Eigenschaft oder eine Änderung der hierarchischen Einordnung sind mit Milestone 6 noch nicht möglich.

Abbildung 17: Änderung der Infos zu vorhandenen Gruppen

3.3.6 Aufbau der Mandantenstruktur

Der Mandanten-Admin kann nun für den Mandanten, den er verwaltet, die gesamte Mandantenstruktur aufbauen. Hierzu erstellt er im Bereich „Gruppenverwaltung“ neue Untergruppen innerhalb seines Mandanten. Jede neue Organisationseinheit/Gruppe, die angelegt wird, muss eine bereits vorhandene Gruppe als Obergruppe besitzen. Die erste Untergruppe, die erzeugt wird, hat zwangsläufig die Mandanten-Gruppe als Obergruppe, da dies bei einem gerade eingerichteten Mandanten die einzig existierende Gruppe ist (siehe Abbildung 18).

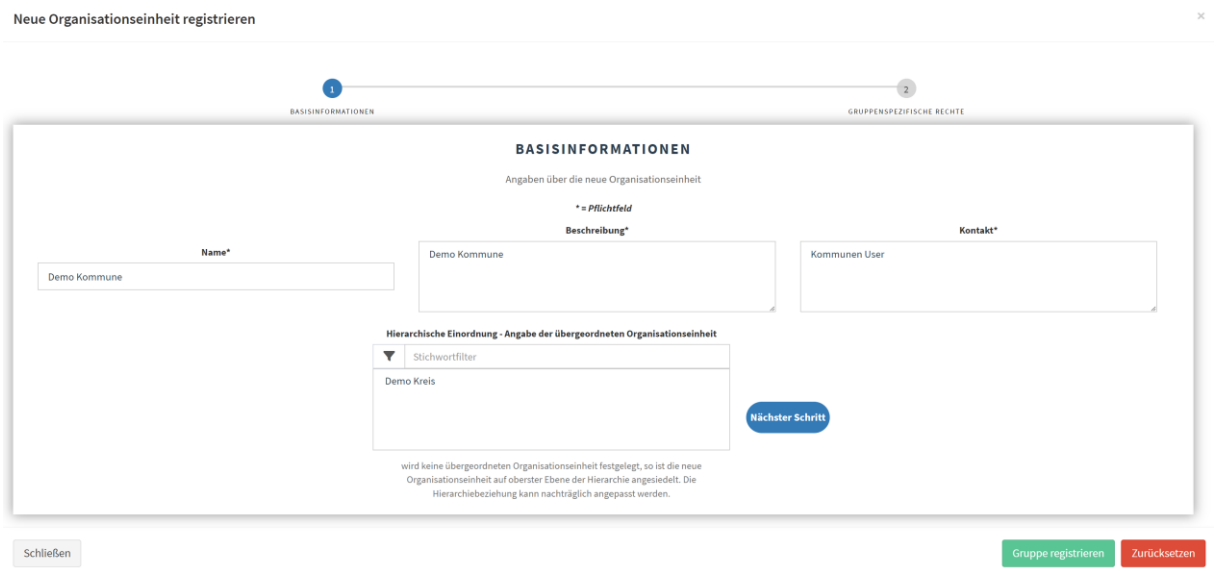


Abbildung 18: Anlegen der ersten Untergruppe eines Mandanten in der KomMonitor Admin UI

Im Auswahlbereich „Hierarchische Einordnung“ werden die für den gerade angemeldeten User verwaltbaren Gruppen eines Mandanten aufgelistet (siehe Abbildung 19). Mit der Auswahl einer Gruppe aus dieser Liste, wird die Obergruppe für die neu anzulegende Gruppe festgelegt. Nur mit einer ausgewählten Obergruppe kann die neue Gruppe registriert werden.

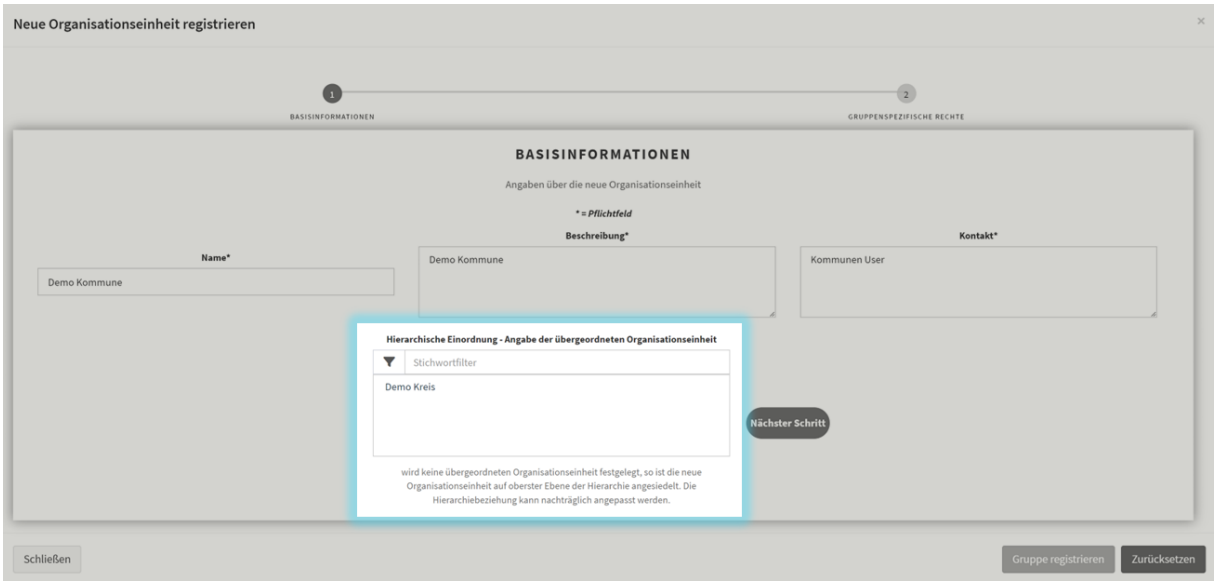


Abbildung 19: Auswahl einer Gruppe zur hierarchischen Einordnung

Der Mandanten-Admin kann beliebig viele Untergruppen erstellen, die beliebig hierarchisch verknüpft sein können. Als Ergebnis der Gruppenstrukturieren ergibt sich schließlich ein ähnliches Bild, wie in unserem Use Case (siehe Abbildung 20).

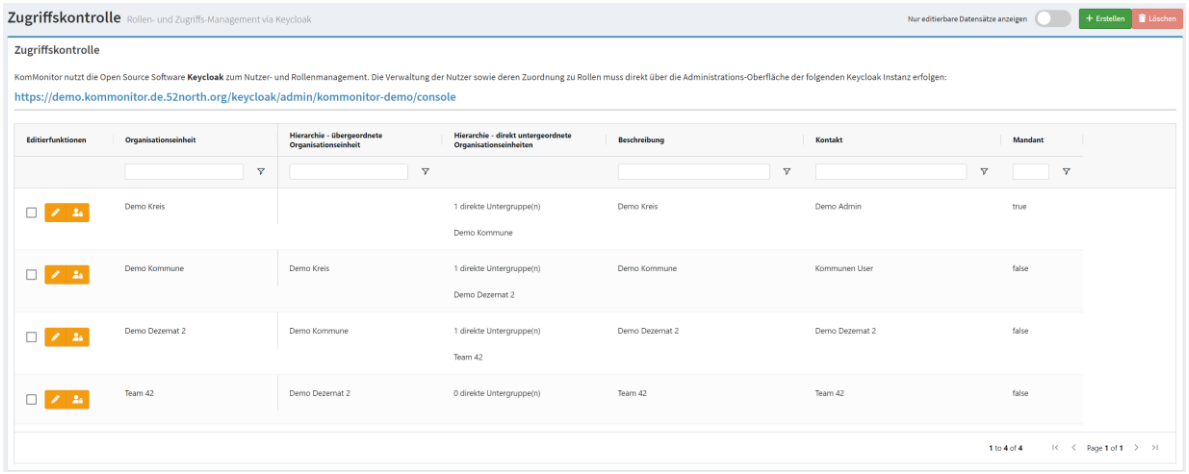


Abbildung 20. Übersichtstabelle zu einem beispielhaften Aufbau einer Mandantenstruktur

Wie in Abschnitt 2.1.2 bereits erwähnt, besteht zwischen Organisationseinheiten in KomMonitor und Gruppen in Keycloak eine 1:1 Beziehung. Die in KomMonitor vorgenommen Gruppenstrukturierung, wird daher 1:1 auf die Gruppenstrukturierung in Keycloak abgebildet. Meldet sich der Mandanten-Admin also bei Keycloak an, findet er im Bereich „Gruppen“ die bekannte Gruppenhierarchie vor (siehe Abbildung 21).

Wichtiger Hinweis:

Die Verknüpfung zwischen Organisationseinheiten in KomMonitor und Gruppen Keycloak erfolgt lediglich einseitig von KomMonitor aus. D.h. für Organisationseinheiten, die über die Admin UI in KomMonitor angelegt werden, wird automatisch auch eine entsprechende Gruppe in Keycloak mit der korrekten hierarchischen Einordnung registriert. Andersherum erfolgt jedoch keine Synchronisation von Keycloak nach KomMonitor. D.h. werden Gruppen in Keycloak neu erzeugt, vorhandene Gruppen gelöscht, umbenannt oder innerhalb des Gruppenbaums umgehängt, hat dies keine Auswirkungen auf die Organisationseinheiten in KomMonitor. Alle Änderungen an Gruppen, die direkt in Keycloak vorgenommen werden, bewirken somit einen inkonsistenten Zustand. In zukünftigen Versionen von KomMonitor, wird dies vrsl. anders sein.

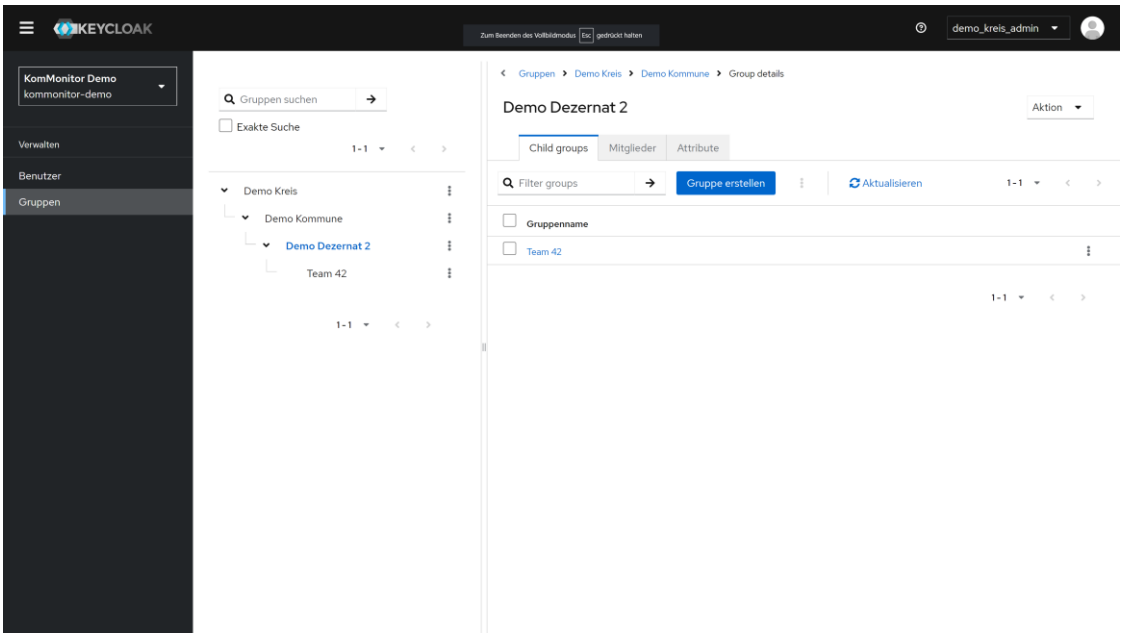


Abbildung 21: Abbildung der Gruppenhierarchie in Keycloak

3.3.7 Löschen von Gruppen

Zwar ist mit Umsetzungsstand von Milestone 6 noch nicht die Änderungen der hierarchischen Gruppenordnung möglich ist, jedoch lassen sich vorhandene Gruppen wieder löschen. Hierzu ist die entsprechende Organisationseinheit im Bereich „Gruppenverwaltung“ auszuwählen und anschließend der Button „Löschen“ zu drücken (siehe Abbildung 22).

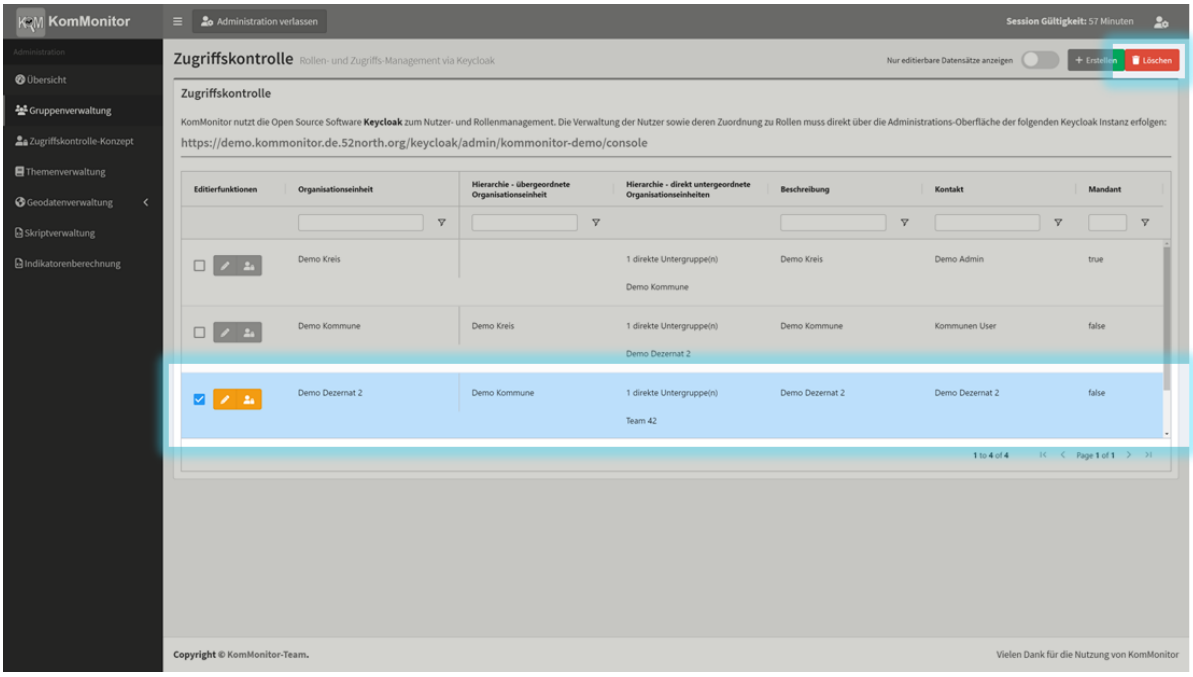


Abbildung 22: Auswahl einer Organisationseinheit zum Löschen

Im erscheinenden Infofenster für die zu löschende Organisationseinheit erscheinen nun zwei wichtige Hinweise:

Im oberen Bereich werden alle Untergruppen der zu löschenden Gruppe aufgelistet (siehe Abbildung 23). Bevor eine Obergruppe gelöscht werden kann, darf diese keine Untergruppen mehr besitzen. Es müssen daher zunächst alle Untergruppen gelöscht werden.

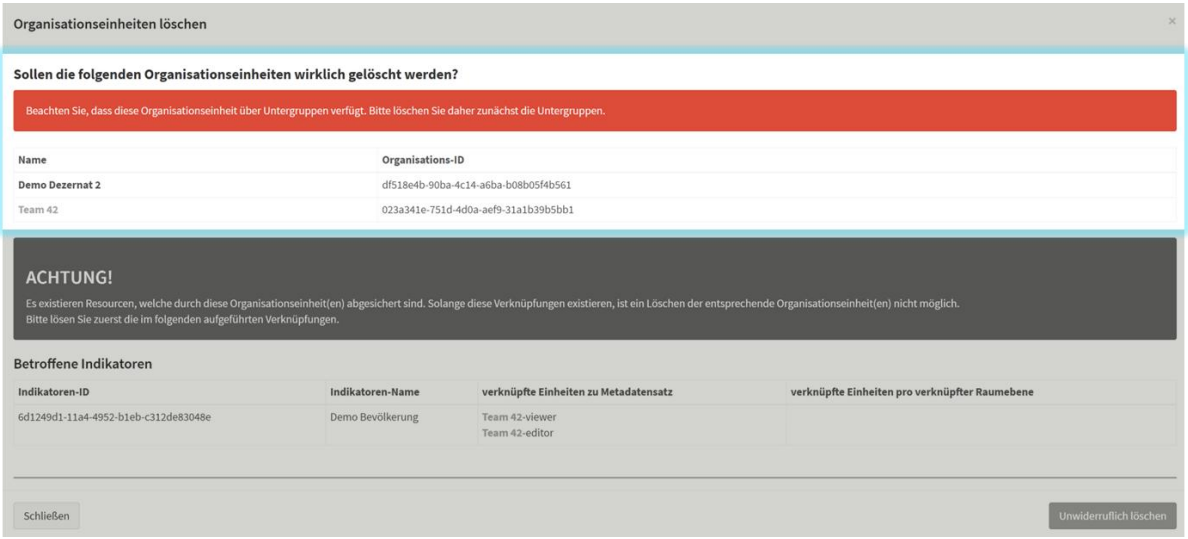


Abbildung 23: Hinweis über vorhandene Untergruppen einer zu löschenden Organisationseinheit

Im unteren Bereich werden dagegen alle Datensätze (Raumeinheiten, Indikatoren und Georessourcen) aufgeführt, die noch mit dieser Raumeinheit rechtemäßig verknüpft sind (siehe Abbildung 24). Eine zu löschende Raumeinheit darf keine Rechte mehr an Datensätzen aufweisen. Daher sind auch hier zunächst alle bestehenden Rechte an Datensätzen zu lösen, bevor das Löschen der Gruppe durchgeführt werden kann.

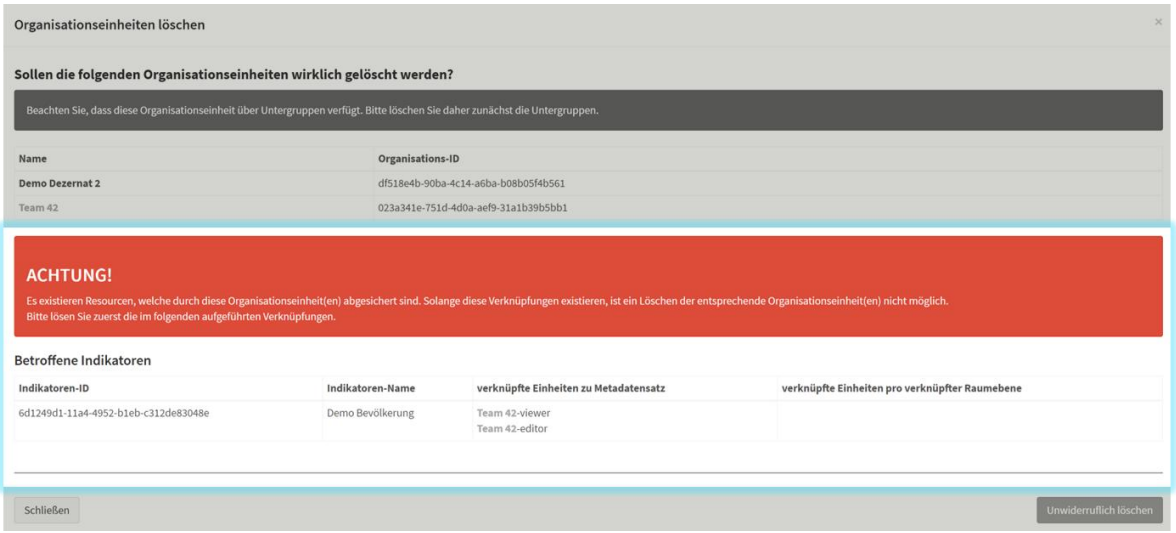


Abbildung 24: Hinweis über verknüpfte Datensätze einer zu löschenden Organisationseinheit

3.3.8 Anlegen von Themen

Um neue Themen anlegen zu können oder vorhandene Themen zu bearbeiten muss ein User Mitglied einer Gruppe sein, die das administrative Recht besitzt für sich oder andere Gruppen Themen zu verwalten. Je nachdem, ob sich dieses Recht nur auf eine bestimmte Gruppe bezieht oder auch alle Untergruppen, besitzt ein solcher User mindestens eine *.unit-themes-creator oder *.client-themes-creator-Rolle (siehe Abschnitt 2.3).

Wichtiger Hinweis:
Mit Umsetzungsstand von Milestone 6 sind alle Themen einer KomMonitor-Instanz Mandanten-übergreifend. D.h. Themen, die von einem Mandanten angelegt wurden, sind auch für andere Mandanten sicht- und zugreifbar. Mandanten-spezifische Gruppen sind aktuell noch nicht möglich, womit auch das Anlegen mehrerer Themen mit demselben Namen, aber für unterschiedliche Mandanten noch nicht möglich ist. Mandanten-spezifische Themen werden Bestandteil der Umsetzung in zukünftigen Milestones sein (siehe Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.**).

3.3.9 Vergabe von Rechten an Datensätzen

Initial werden in der Geodatenverwaltung nur öffentliche Datensätze aufgelistet, also Datensätze, die für die Öffentlichkeit freigegeben wurden (siehe Abbildung 25). Öffentliche Datensatzfreigaben sind Mandanten-übergreifend. D.h. ein Datensatz, der von Mandant A für die Öffentlichkeit freigegeben wurde, ist auch für Mandant B lesend verfügbar. An öffentlichen Datensätzen eines anderen Mandanten hat ein Mandanten-Admin keine Rechte zur Bearbeitung. Dementsprechend sind alle Buttons zur Bearbeitung eines Datensatzes deaktiviert.

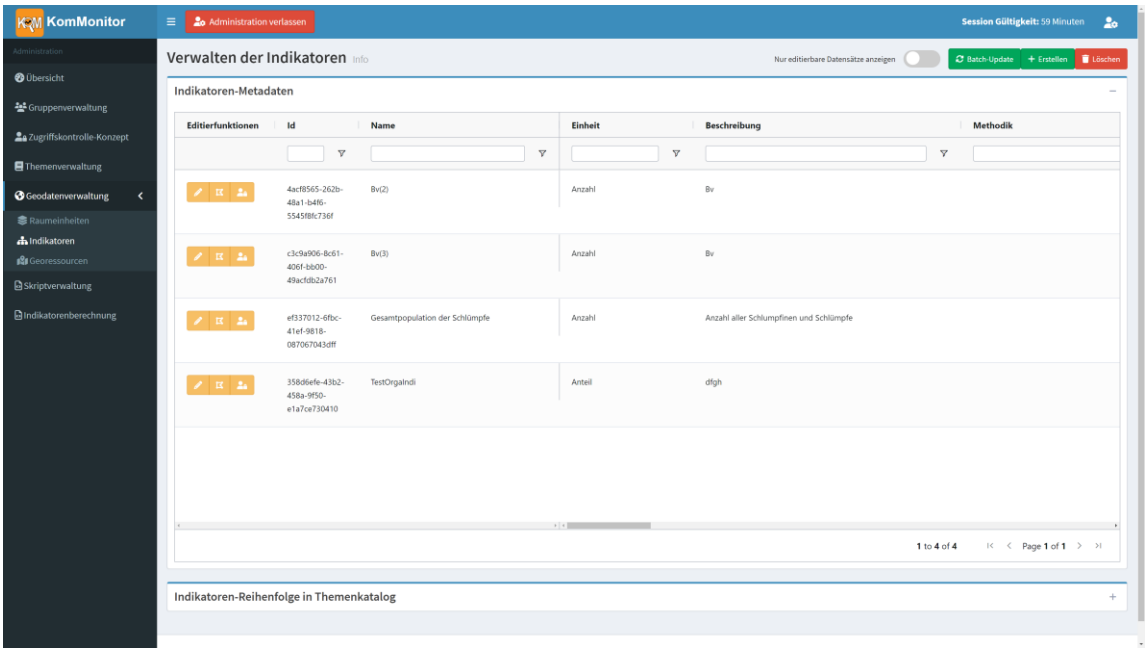


Abbildung 25: Übersicht zu Mandanten-übergreifenden öffentlichen Datensätzen ohne Rechte zur Bearbeitung

Der Mandanten-Admin kann nun für seinen Mandanten neue Datensätze (Indikatoren, Georessourcen, Raumeinheiten) anlegen. Generell ist das Anlegen von Datensätzen allen Usern möglich, die Mitglied in einer Gruppe sind, der das administrative Recht zum Anlegen von Datensätzen für sich oder eine fremde Gruppe eingeräumt wurde. Je nachdem, ob sich dieses Recht nur auf eine bestimmte Gruppe bezieht oder auch alle Untergruppen, besitzt ein solcher User mindestens eine **.unit-resources-creator* oder **.client-resources-creator*-Rolle (siehe Abschnitt 2.3).

Das Registrieren von neuen Datensätzen erfolgt in den ersten Schritten wie gehabt: es werden Metadaten sowie weitere Ressourcen-spezifische Informationen für einen neuen Datensatz in den entsprechenden Masken eingetragen. Neu ist jedoch, dass für den neu anzulegenden Datensatz ein Eigentümer hinterlegt werden muss (siehe Abbildung 26). Zur Auswahl stehen dabei alle Organisationseinheiten, für die der gerade anlegende User Rechte zur Ressourcenverwaltung hat. In

unserem Use Case sind für den Mandanten-Admin alle Organisationseinheiten/Gruppen des Mandanten zur Auswahl als Eigentümer an den Datensatz verfügbar. Durch die Eigentümerschaft einer Gruppe an einen Datensatz erhält diese Gruppe vollumfängliche Rechte an den Datensatz. Alle User einer Gruppe, die Eigentümer eines Datensatzes ist, können diesen dann beliebig ändern und löschen sowie Rechte an dem Datensatz vergeben. Diese Rechte besitzen ansonsten lediglich User anderer Gruppen, denen administrative Rechte zur Verwaltung von Datensätze für die Eigentümergruppe zugewiesen wurden.

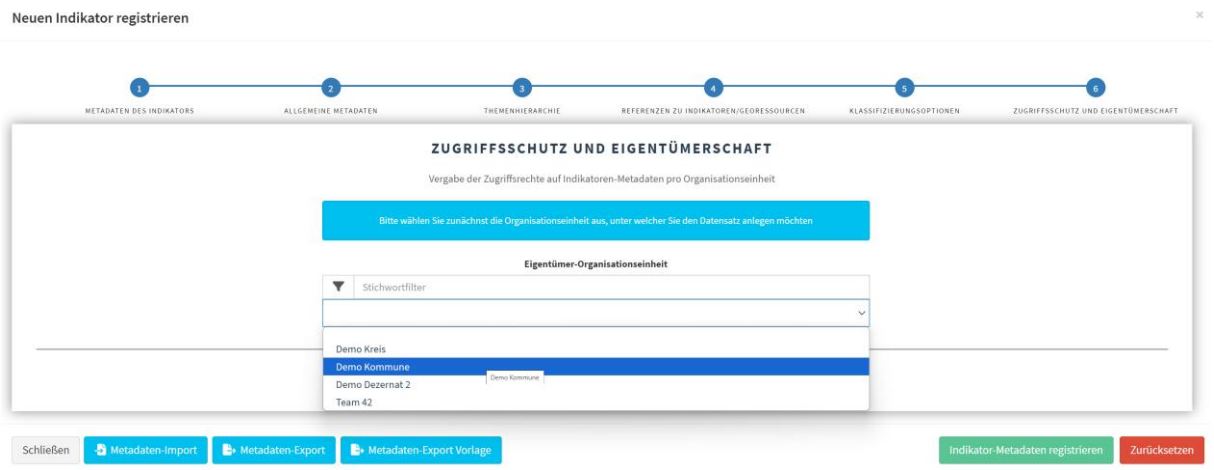


Abbildung 26: Angabe einer Eigentümerschaft beim Anlegen eines neuen Indikators

In einem zweiten Schritt können wie aus der alten KomMonitor Version bekannt, Rechte an dem anzulegenden Datensatz an andere Gruppen vergeben werden (siehe Abbildung 27). Zwei Änderungen gibt es jedoch für diesen Schritt: Erstens gibt es einen separaten Button zur Aktivierung der öffentliche Lesefreigabe des Datensatzes und zweitens können anderen Gruppen lediglich Lese- und Editierrechte an dem Datensatz vergeben werden, jedoch nicht mehr das Recht zum Löschen. Dieses Recht ist ausschließlich der Eigentümergruppe eines Datensatzes, bzw. den für die Eigentümergruppe mit administrativen Rechten belegten anderen Gruppen vorbehalten.

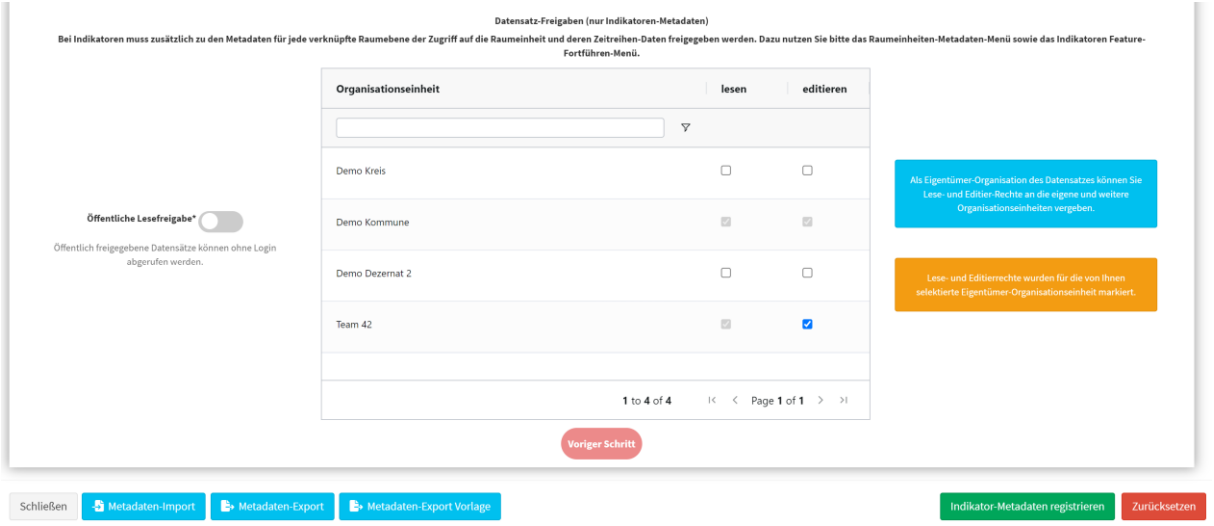


Abbildung 27: Vergabe von Gruppen-spezifischen Zugriffsrechten beim Anlegen eines neuen Indikators

3.3.10 Nutzerverwaltung

Neben der Gruppenverwaltung über die KomMonitor Admin UI ist der Mandanten-Admin nun auch berechtigt, die Userverwaltung in Keycloak zu übernehmen. Generell ist hierzu jeder User berechtigt, der Mitglied einer Gruppe ist, die das administrative Recht zur Verwaltung von Usern und Gruppen besitzt. Je nachdem, ob sich dieses Recht nur auf eine bestimmte Gruppe bezieht oder auch alle Untergruppen, besitzt ein solcher User mindestens eine *.unit-users-creator oder *.client-users-creator-Rolle (siehe Abschnitt 2.3). Innerhalb der Keycloak Oberfläche werden diesen Usern lediglich diejenigen Gruppen zur Verwaltung angezeigt, auf die sich das administrative Recht bezieht. Ebenso lassen sich auch nur diejenigen User verwalten, die in entsprechenden Gruppen Mitglied sind.

In unserem Use-Case wurde bis dato noch keine weiteren User außer unserem Mandanten-Admin angelegt. Daher wird initial dem Mandanten-Admin auch lediglich sein eigenes Benutzerkonto in der Keycloak Oberfläche angezeigt (siehe Abbildung 28). Über den Button „Benutzer hinzufügen“ kann der Mandanten-Admin aber nun weitere User anlegen und einer vorhandenen Gruppe zuweisen.

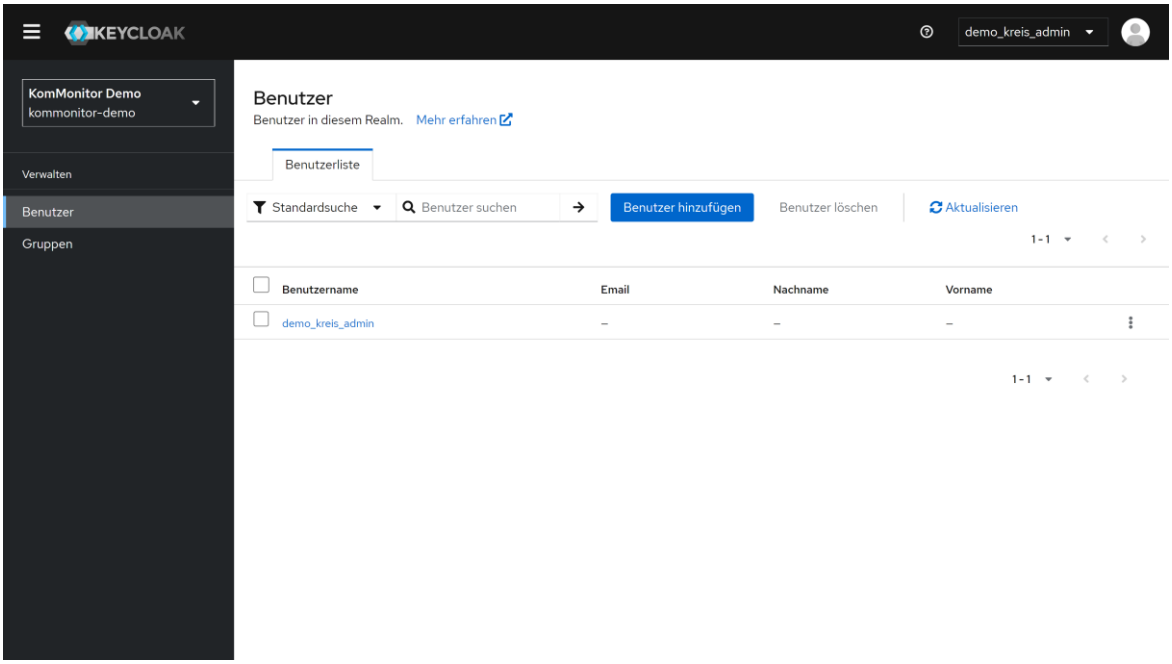


Abbildung 28: Sichtbarkeit von Usern in Keycloak für einen Mandanten-Admin

Wichtiger Hinweis:

Anders als beim globalen KomMonitor Administrator (vgl. Abschnitt 3.3.4), muss der Mandanten-Admin bereits beim Registriervorgang den neu anzulegenden User einer vorhandenen Gruppe zuweisen (siehe Abbildung 29). Andernfalls schlägt der Registriervorgang fehl. Hintergrund dieser Verhaltensweise ist, dass der Mandanten-Admin nur die Berechtigung zur Verwaltung bestimmter Gruppen und derer User besitzt. Ein neu angelegter User, der keiner Gruppe zugeordnet wird, fällt demnach nicht in den Zuständigkeitsbereich des Mandanten-Admins und kann lediglich durch den globalen Administrator angelegt werden.

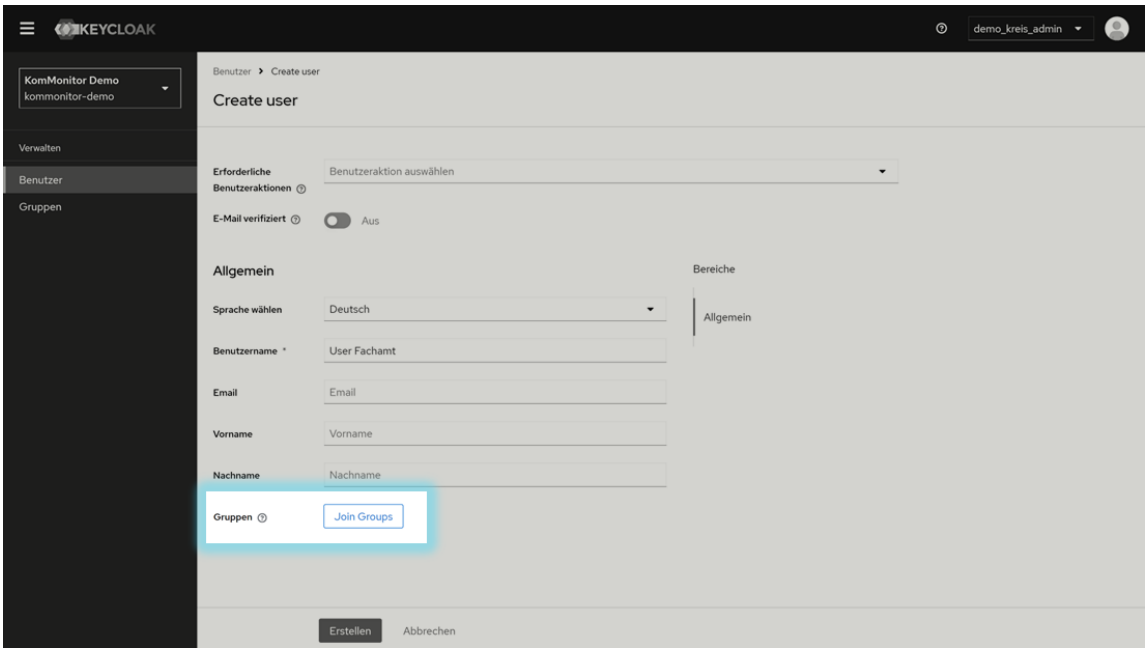


Abbildung 29: Zuweisung eines Users als Mitglied in eine Gruppe zum Zeitpunkt der Registrierung des Users in Keycloak

Mit Klick auf „Join Groups“ öffnet sich ein weiteres Fenster, über das die Zuweisung des neu anzulegenden Users in eine vorhandene und durch den Mandanten-Admin administrierbare Gruppe möglich ist.

Wichtiger Hinweis:
In manchen Fällen kann es sein, dass nicht direkt alle verwaltbaren Gruppen aufgelistet werden. In diesem Fall kann entweder über das Suchfeld direkt nach einer Gruppe gesucht werden oder die Anzahl der anzuzeigenden Gruppen wird mit Klick auf das Dropdownmenü rechts oben erhöht.

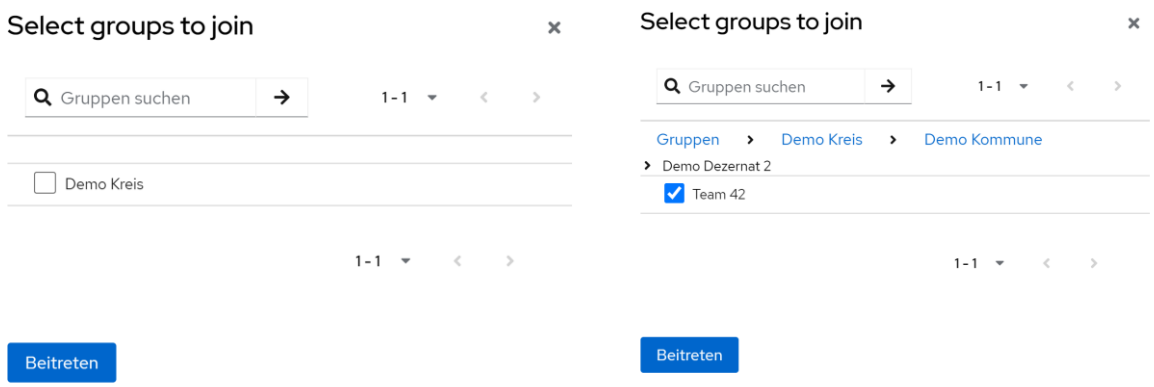


Abbildung 30: Auswahl der Gruppenmitgliedschaft eines neu zu registrierenden Users. Standardmäßig werden nur Obergruppen angezeigt (links). Untergruppen werden nach einem Klick auf eine Obergruppe gelistet (rechts)

In der Keycloak Oberfläche erhält der Mandanten-Admin auch einen Überblick über alle User, die Mitglied einer bestimmten Gruppe sind (siehe Abbildung 31) sowie umgekehrt auch einen Überblick über alle Gruppen, in denen ein User Mitglied ist (siehe Abbildung 32).

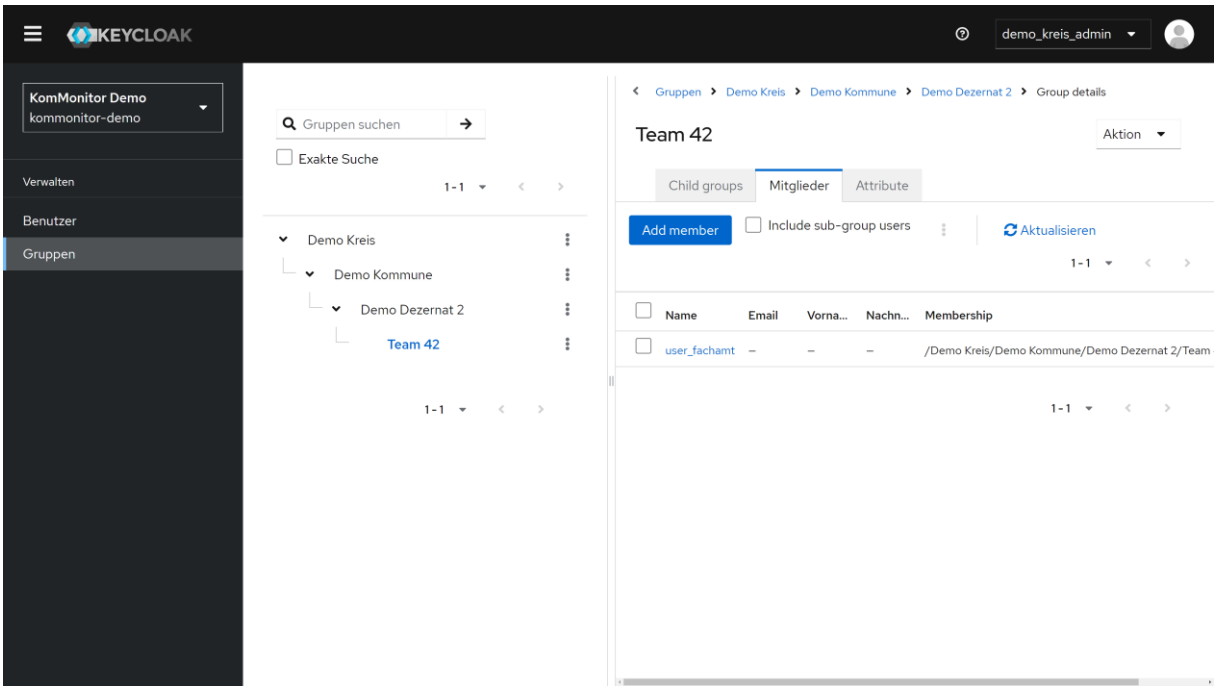


Abbildung 31: Übersicht aller Mitglieder einer Gruppe in Keycloak

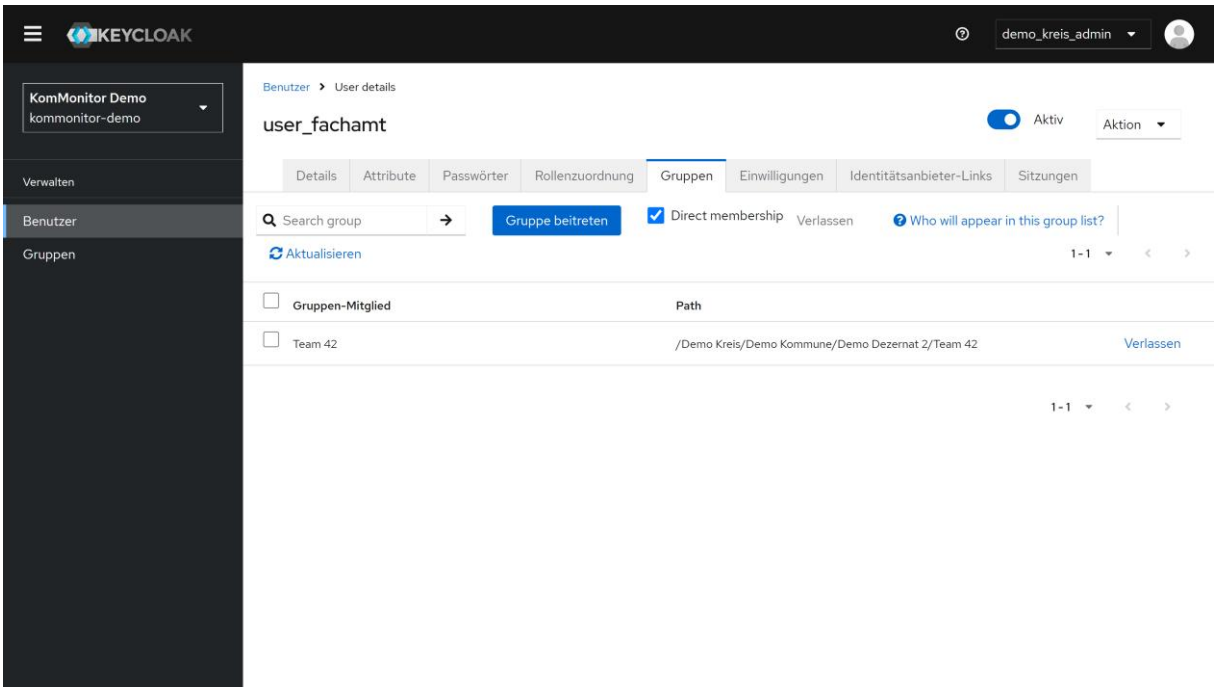


Abbildung 32: Übersicht aller Gruppenmitgliedschaften eines Users