VALSIGHT

# Valsight – Berechtigungen vergeben (T09)

03/2020

Bei Fragen wenden Sie sich gerne an:
support@valsight.com

Valsight-Team

# 1. Allgemeine Informationen

## 1.1. Berechtigungen

Es gibt verschiedene Arten von Berechtigungen. Diese lassen sich unterscheiden auf die Befugnisse, die ein Nutzer hat und die Ebene innerhalb des Projekts. Die Berechtigungen können für die Nutzer individuell angepasst werden. So kann beispielsweise ein Nutzer für das Projekt nur Leserechte besitzen und Benutzerrechte für ausgewählte Modelle und Workspaces. Die folgenden Berechtigungen innerhalb eines Projektes gibt es:

### Projekt

- Can use – Diese Benutzer können auf das Projekt zugreifen. Sie haben jedoch noch keine Einsicht in die verschiedenen Modelle und Workspaces und können diese auch nicht bearbeiten.
- Project Admin – Diese Benutzer haben uneingeschränkten Zugriff auf das Projekt. Sie können neue Modelle und Workspaces anlegen und haben vollständigen Zugang zu allen Datenquellen, Dimensionen und Levels.

### Modell

- Can view – Diese Benutzer können die gewählten Modelle sehen, sie können jedoch nicht das Modell öffnen.
- Can edit – Diese Benutzer können das Modell sehen, öffnen und bearbeiten.

### Workspace

- Limited access – Diese Benutzer können Workspaces öffnen und neue Annahmen und Charts anlegen. Sie können keine Veränderungen bezüglich der Workspace-Filter vornehmen.
- Full access – Diese Benutzer haben zusätzlich die Berechtigung den Workspace-Filter zu verändern und können Benutzerberechtigungen für den Workspace bearbeiten.

### Datenberechtigung

- Read access – Diese Benutzer können Daten als Teil von Charts oder Analysen einsehen.
- Write access – Diese Benutzer können Daten einsehen und zusätzlich Annahmen auf Basis dieser Daten erstellen und bearbeiten.

Datenberechtigungen definieren welche Daten ein Benutzer im Workspace einsehen und bearbeiten kann. Die Datenberechtigungen haben keine Auswirkungen auf den Modell-Editor.

## 1.2 Benutzertypen

Neben den eingangs beschriebenen Berechtigungen innerhalb eines Projektes gibt es auch noch die Möglichkeit fünf vorgefertigte Benutzergruppen auszuwählen. Diese unterscheiden sich in den Rechten, die der jeweilige Benutzer hat und werden im Folgenden beschrieben.

1. Reader: Dieser Benutzertyp kann lediglich Präsentationen einsehen.
2. Analyst: Diese Benutzer können den Szenario Manager nur in einem Arbeitsbereich anzeigen, den Rest des Arbeitsbereichs bearbeiten und sowohl Präsentationen einsehen als auch erstellen.
3. Simulation User: Diese Benutzer haben die gleichen Rechte wie die zuvor erläuterte Gruppe „Analyst" und können zudem den Szenario Manager bearbeiten, neue Arbeitsbereiche erstellen und an Workflows teilnehmen.
4. Model User: Dieser Benutzertyp hat abgesehen von den Rechten, die ein „Simulation User" hat das Recht Modelle, Dimensionen, und Datenquellen zu erstellen und zu bearbeiten.
5. Unrestricted User: Ist berechtigt alles zu tun was ein „Model User" kann und zudem Projekte erstellen und bearbeiten. Außerdem kann diesen Nutzern die Rolle des globalen Admins zugewiesen werden.

## Hinweis:

Die Benutzertypen schränken nur die Zugriffsrechte ein, die Benutzer müssen trotzdem für jedes Projekt, Modell, Arbeitsbereich, Präsentation und Workflow, auf das sie zugreifen möchten, spezifische Rechte erhalten. Zusätzlich bedeutet dies auch, dass Benutzer mit einem eingeschränkten Benutzertyp (z.B. als Reader) ein Projekt nicht öffnen können, obwohl ihnen der Zugriff darauf gewährt wurde.

Um die Berechtigungen eines Projektes einzusehen und neue Berechtigungen zu erteilen, gehen Sie in das Konfigurationsmenü (siehe Abb. 1) und wählen bei „Projekte" dort das entsprechende Projekt aus. Anschließend wählen Sie die Schaltfläche „Security" (siehe Abb. 2) und „Access Report" (siehe Abb. 3), dort erhalten Sie eine Liste der Benutzer und die jeweiligen Berechtigungen für das Projekt.

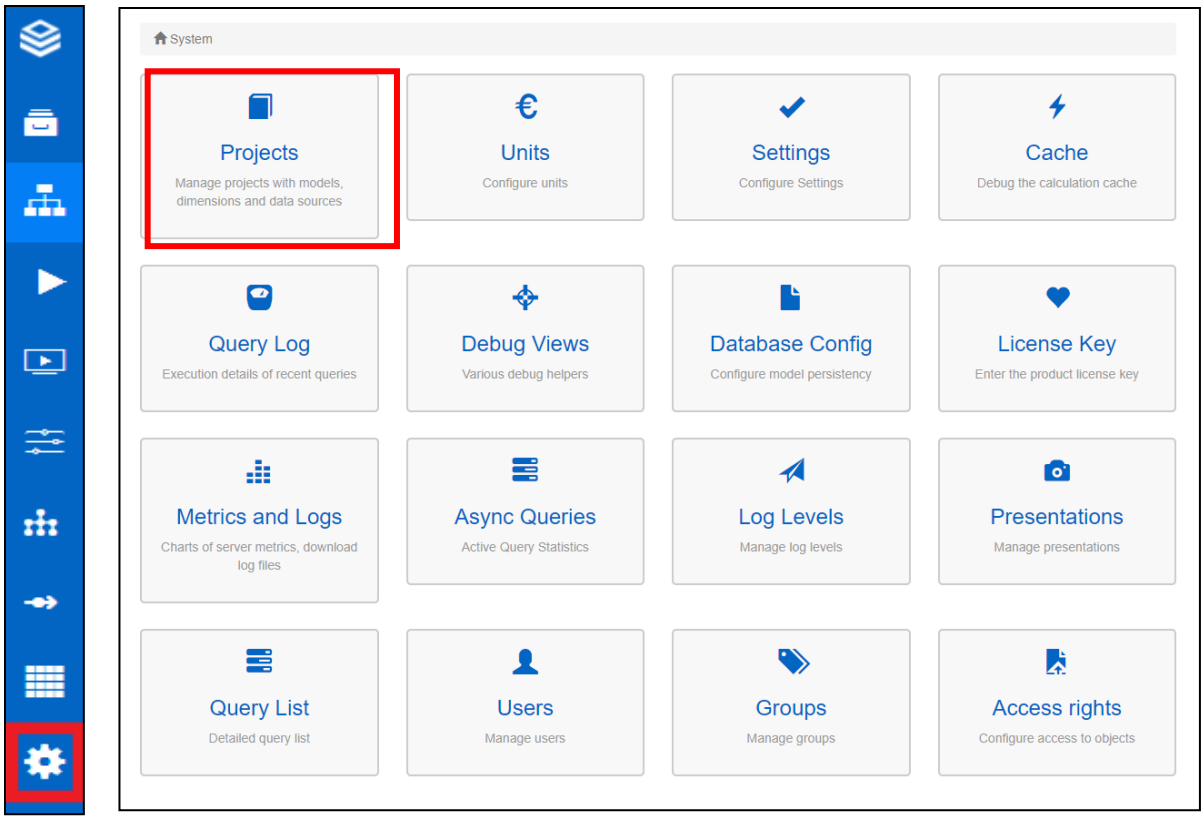


Abbildung 1: Konfigurationsmenü

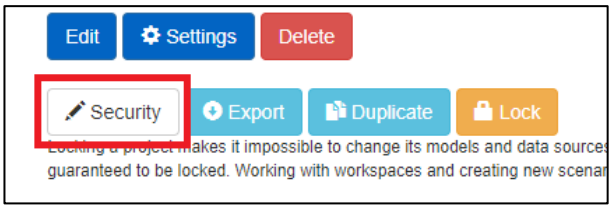


Abbildung 2: Projekt-Sicherheit

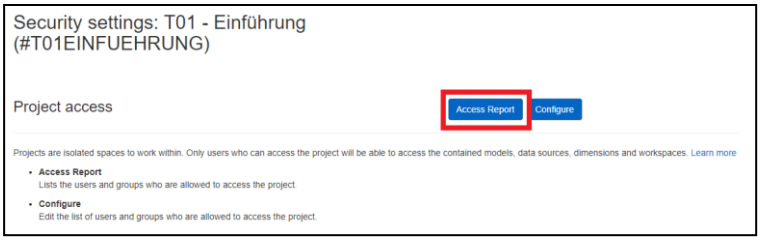


Abbildung 3: Access Report

Anhand dieser Liste können Sie die Berechtigungen der jeweiligen Benutzer einsehen und anpassen. Für die Anpassung der Berechtigungen gibt es zwei Möglichkeiten:

1. Über „Edit" können Sie die Liste der Benutzer anpassen, welche Zugriff auf das Projekt hat.
2. Indem Sie einen Benutzer auswählen und auf den Namen klicken, können Sie die einzelnen Berechtigungen des Nutzers individuell anpassen.

Um die Berechtigungen nicht nur für das gesamte Projekt einzustellen, sondern auch bezüglich der Modelle, Workspaces, Präsentationen und Datenquellen anzupassen, gehen Sie zurück in das Konfigurationsmenü (siehe Abb. 1). Dort wählen Sie nicht „Projects", sondern „Access Rights" aus (siehe Abb. 4). Dann erhalten Sie eine Liste aller Benutzer sowie aller Projekte, Modelle, Workspaces, Präsentationen und Datenquellen.

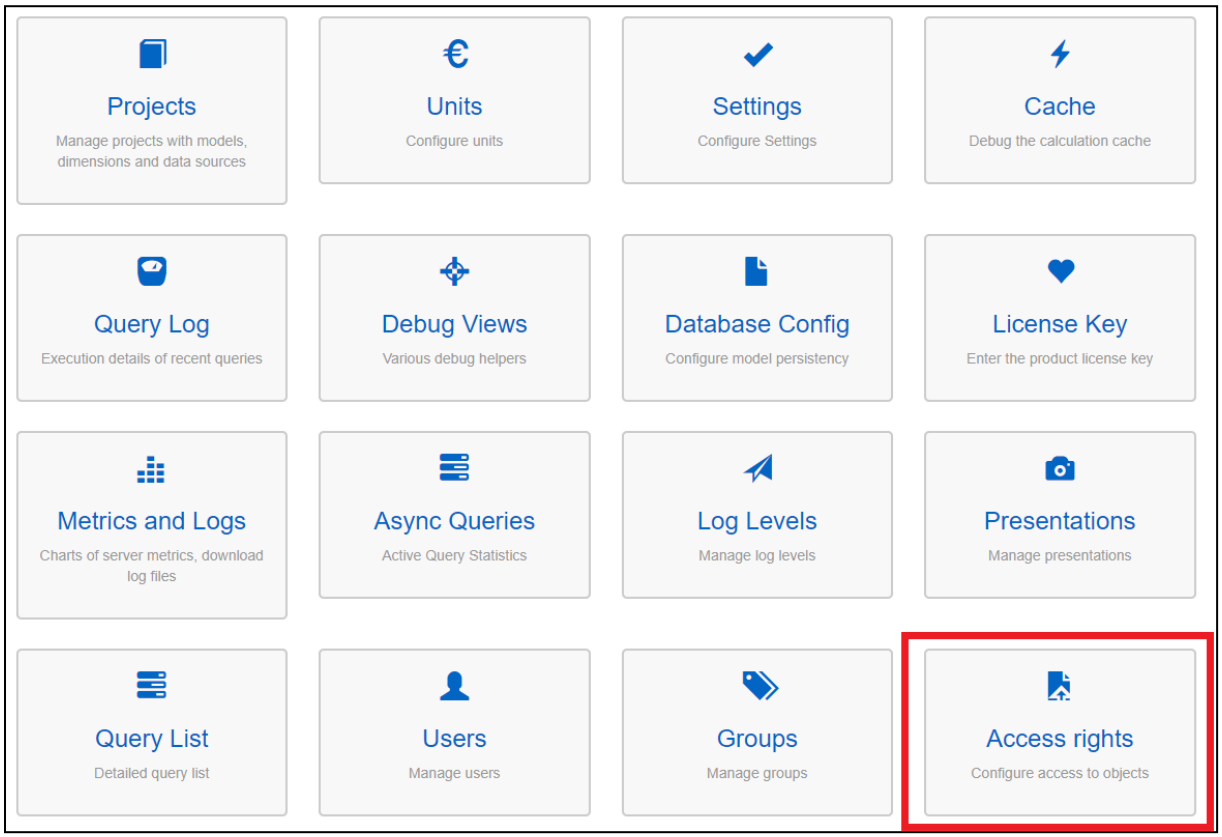



Abbildung 1: Access rights

Um das entsprechende Projekt auszuwählen, wählen Sie im Dropdown-Feld das Projekt aus und klicken auf „Show" (siehe Abb. 5). Es besteht ebenfalls die Möglichkeit, über das Setzen von Haken nach den Modellen oder Workspaces etc. zu filtern. Über „Show" aktualisiert sich die Ansicht.

Zusätzlich können Sie über das Suchfeld nach einzelnen Gruppen oder Benutzern suchen. Nun haben Sie erneut die Möglichkeiten die Berechtigungen der Benutzer anzupassen über „Edit" oder einen Klick auf den Namen der Nutzer.

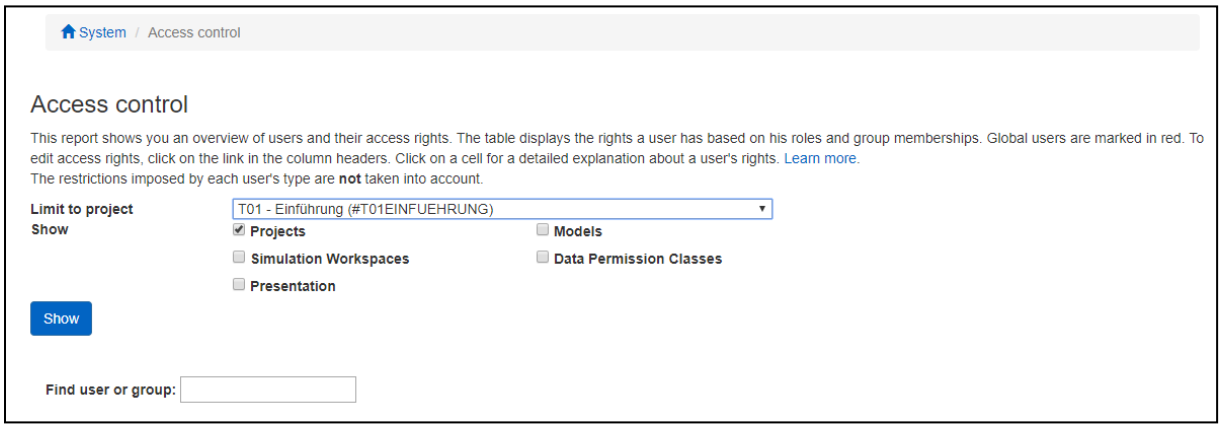



Abbildung 2: Show Project

## Hinweis:

Es empfiehlt sich für die einzelnen Planungseinheiten, die Benutzer in Gruppen anzulegen und den Gruppen die Berechtigungen zu vergeben. Für einzelne Personen, die auch projektübergreifend Zugriffe erhalten sollen, ist die Vergabe über „Access Rights" sinnvoll.

Weitere Informationen finden Sie unter wiki.valsight.com/doc/user-guide/projects .

# 2. Anwendungsbeispiel

Im folgenden Beispiel werden neue Nutzer angelegt, verschiedene Berechtigungen vergeben und der eingangs erläuterte Vorgang durchlaufen. In unserem Beispiel verwenden wir nun das Trainingsmodell „T08-PLANNING“. Dieses Trainingsmodell kennen Sie bereits und finden Sie hier:

https://wiki.valsight.com/doc/user-guide/other/de-training-modelle

In unserem Beispiel gehen wir von folgender Ausgangssituation aus:

| Name | Position |
|---|---|
| Anna Müller | Projektleitung |
| Peter Schmidt | Controlling LE 1 |
| Heike Schneider | Controlling LE 1 |
| Jens Fischer | Controlling LE 2 |
| Eva Weber | Konzern |

Die Projektleitung soll sämtliche Berechtigungen für das Projekte und für alle Inhalte besitzen.

Die Abteilungen Controlling soll Bearbeitungsrechte für die relevanten Modelle und entsprechenden Workspaces haben (BM1 + BM2 | LE1 bzw. LE2).

Der Konzern soll alle Modelle und alle Workspaces einsehen und bearbeiten können.

Die Abteilung Controlling LE 1 soll nur die Daten für die Legal Entity 1 einsehen und bearbeiten können.

Die Abteilung Controlling LE 2 soll nur die Daten für die Legal Entity 2 einsehen und bearbeiten können.

## 2.1. Benutzer anlegen

### 2.1.1. Einzelne Nutzer anlegen

Als erstes müssen die Benutzer angelegt werden. Dafür öffnen Sie das Konfigurationsmenü und wählen anschließend das Feld „Users“ (siehe Abb. 6). Anschließend legen Sie über „+ Add User“ einen neuen Benutzer an (siehe Abb. 7). Dabei legen Sie den Namen des Benutzers fest, geben Ihr eigenes Passwort ein und legen zusätzlich ein erstes Passwort für den Benutzer an (siehe Abb. 8). Das Passwort kann der Benutzer später noch ändern. An dieser Stelle können sie außerdem den Benutzertyp bestimmen, dies entscheidet darüber über welche Rechte der Nutzer verfügt. Die verschiedenen Benutzertypen sind in Kapitel 1.2 erläutert. Danach klicken Sie auf das Feld „Create User“. Dieser Vorgang wiederholt sich für die anderen Benutzer.

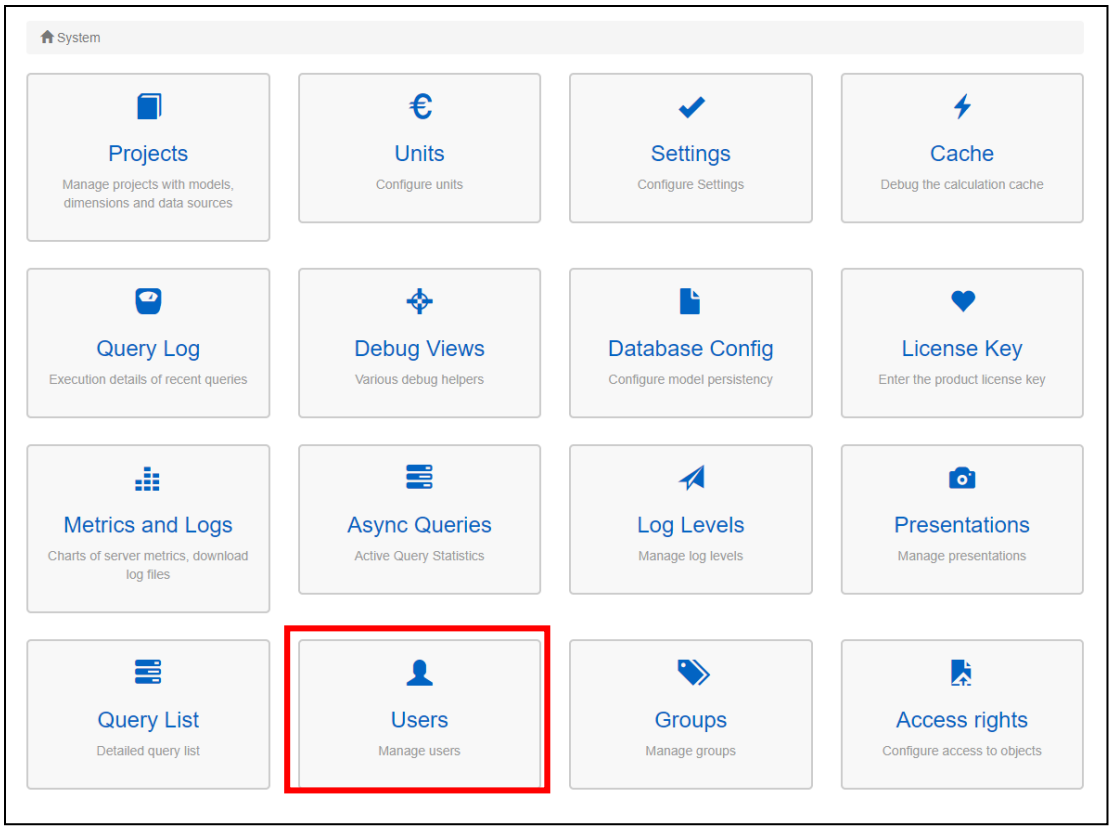



Abbildung 3: Konfigurationsmenü

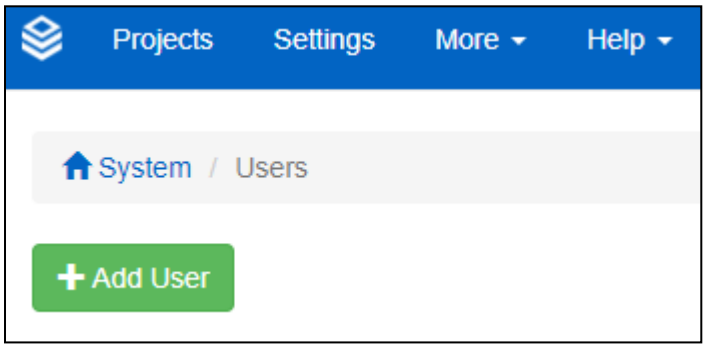



Abbildung 4: Benutzer hinzufügen

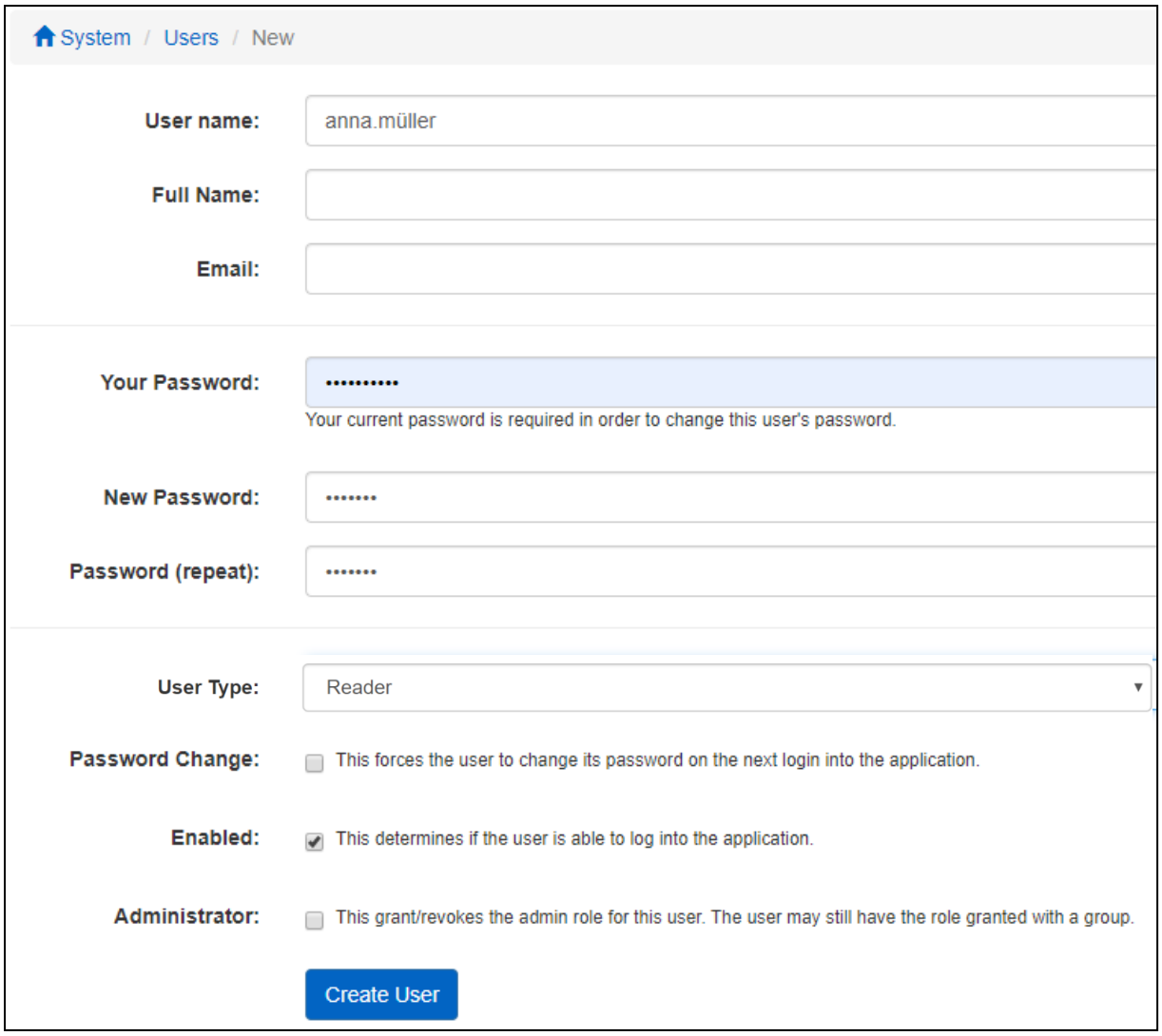



Abbildung 5: Neuen Benutzer definieren

### 2.1.2. Gruppen anlegen

Sie können mehrere Nutzer einer Gruppe zuordnen und damit den Vorgang für die Vergabe der Berechtigungen vereinfachen. Dies ist sinnvoll, wenn mehrere Benutzer dieselben Berechtigungen haben sollen.

Wählen Sie dafür im Konfigurationsmenü das Feld „Groups". Anschließend können Sie einen Namen vergeben und die Mitglieder der Gruppe auswählen. Wenn Sie einen Haken im Kästchen „Administrator" setzen haben alle Mitglieder der Gruppe automatisch die Berechtigung als „Project Admin" (siehe Abb. 9).

Die Vergabe der Berechtigungen für eine Gruppe durchläuft denselben Prozess wie für einen einzelnen Benutzer.

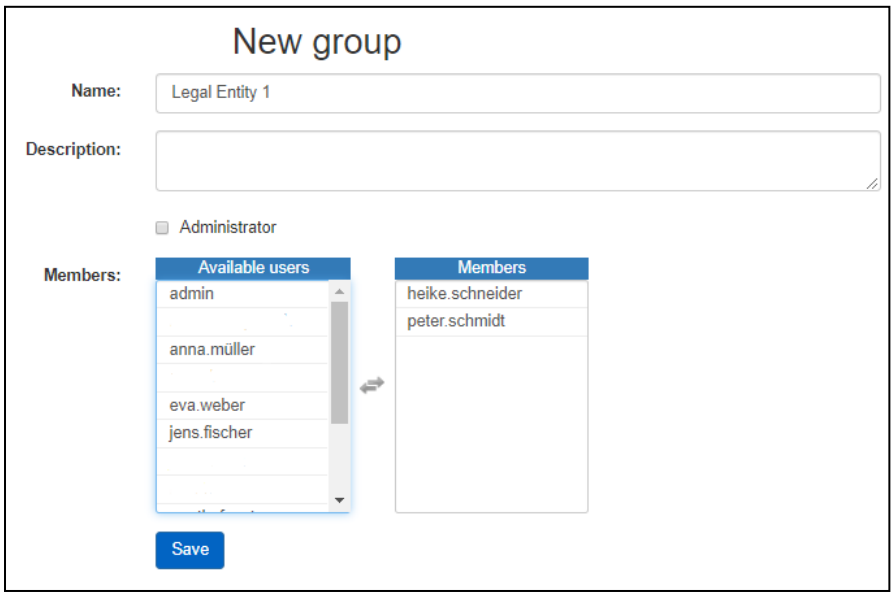



Abbildung 6: Neue Gruppe anlegen

## 2.2. Berechtigungen

### 2.2.1. Berechtigungsübersicht anzeigen

Nun können Sie für die Benutzer die Berechtigungen vergeben. Klicken Sie dafür im Konfigurationsmenü auf das Feld „Access Report" unten rechts.

Anschließend wählen Sie über „Switch Project" das Projekt aus (siehe Abb. 9). Achten Sie darauf, dass die gewünschten Projekte und Modelle angezeigt werden. Dies ist möglich zu filtern über die grünen Schalter (siehe Abb. 10).

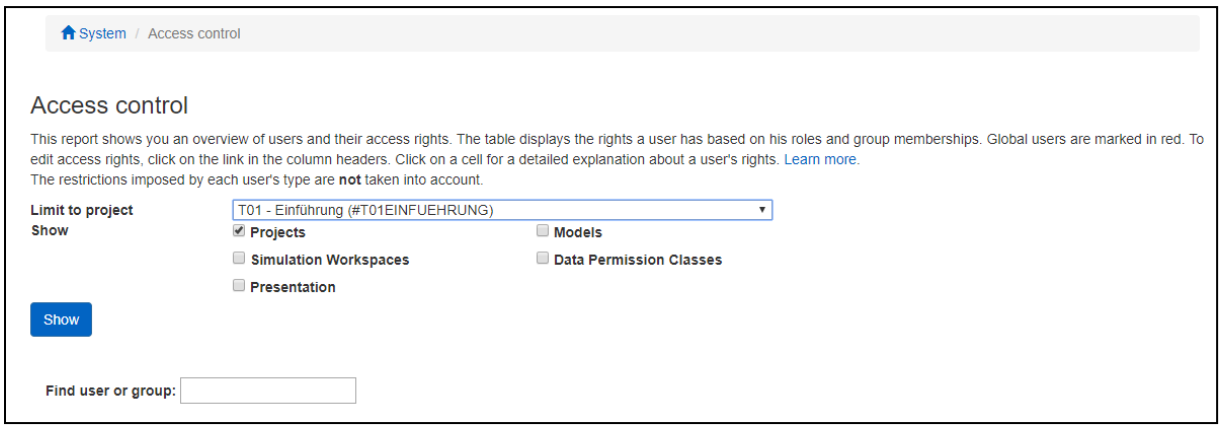
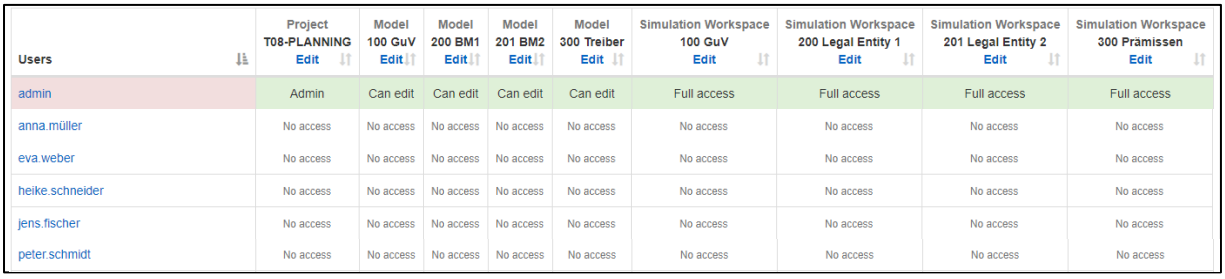



Abbildung 7: Projekt auswählen

Danach erscheint eine Liste mit allen Benutzern als Übersicht mit den jeweiligen Berechtigungen für das Projekt (siehe Abb. 11).



| Users | Project T08-PLANNING Edit | Model 100 GuV Edit | Model 200 BM1 Edit | Model 201 BM2 Edit | Model 300 Treiber Edit | Simulation Workspace 100 GuV Edit | Simulation Workspace 200 Legal Entity 1 Edit | Simulation Workspace 201 Legal Entity 2 Edit | Simulation Workspace 300 Prämissen Edit |
|---|---|---|---|---|---|---|---|---|---|
| admin | Admin | Can edit | Can edit | Can edit | Can edit | Full access | Full access | Full access | Full access |
| anna.müller | No access | No access | No access | No access | No access | No access | No access | No access | No access |
| eva.weber | No access | No access | No access | No access | No access | No access | No access | No access | No access |
| heike.schneider | No access | No access | No access | No access | No access | No access | No access | No access | No access |
| jens.fischer | No access | No access | No access | No access | No access | No access | No access | No access | No access |
| peter.schmidt | No access | No access | No access | No access | No access | No access | No access | No access | No access |

Abbildung 8: Benutzerliste

Aus dieser Liste lässt sich erkennen, dass die angelegten Benutzer noch keine Berechtigungen haben, bis auf den Admin. Sie können die Berechtigungen nun bearbeiten.

### 2.2.2. Berechtigungen vergeben

Für die Vergabe der Berechtigungen gibt es zwei Ansätze:

a) Das Projekt, Modell oder Workspace auswählen und die berechtigen Benutzer hinzufügen. Hier werden die Berechtigungen für das Projekt vergeben. Dafür klicken Sie in der jeweiligen Spalte auf „Edit" für das Projekt. Dadurch erscheint die Auswahl der Berechtigung „Can use" und „Project Admin". In der linken Spalte befinden sich zunächst alle Nutzer, die noch keine Berechtigung für das Projekt haben. Durch einen Klick auf den Namen erscheint der Benutzer in der rechten Spalte und erhält die Berechtigung (siehe Abb. 12).

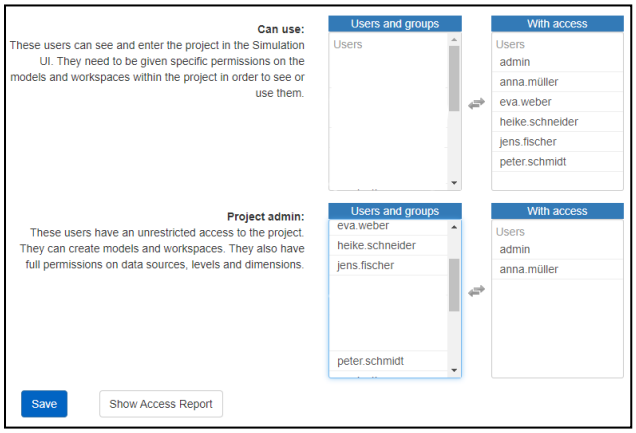



Abbildung 9: Berechtigungen vergeben

b) Sie können die Benutzer auswählen und die Berechtigungen einzeln je Benutzer vergeben. Dafür klicken Sie in der Berechtigungsübersicht auf den Namen eines Benutzers. Damit können Sie für diesen Benutzer individuell die Berechtigungen vergeben. Dafür aktivieren Sie für die entsprechende Modelle und Workspaces die Kästchen (siehe Abb. 13).

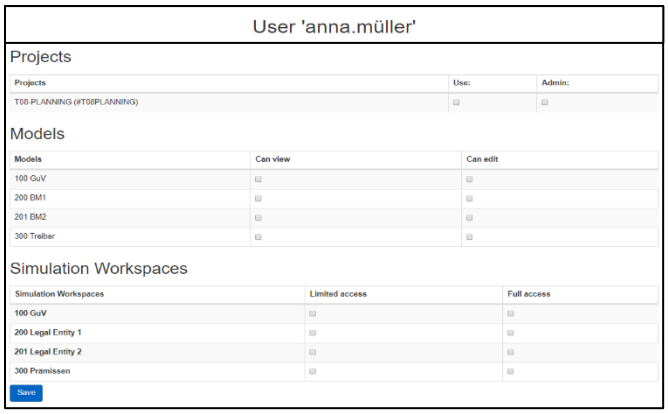



Abbildung 10: User-Übersicht

Nun werden im Beispiel für die Personen die Berechtigungen wie folgt vergeben:

Die Projektleitung soll sämtliche Berechtigungen für das Projekte und für alle Inhalte besitzen.

Die Abteilungen Controlling sollen Bearbeitungsrechte für die relevanten Modelle und entsprechenden Workspaces haben (BM1 + BM2 | LE1 bzw. LE2).

Das Management soll alle Modelle und alle Workspaces einsehen und bearbeiten können.

Als Ergebnis sollte die Berechtigungsübersicht aussehen wie in Abbildung 14:

| Users | Project T08-PLANNING Edit | Model 100 GuV Edit | Model 200 BM1 Edit | Model 201 BM2 Edit | Model 300 Treiber Edit | Simulation Workspace 100 GuV Edit | Simulation Workspace 200 Legal Entity 1 Edit | Simulation Workspace 201 Legal Entity 2 Edit | Simulation Workspace 300 Prämissen Edit |
|---|---|---|---|---|---|---|---|---|---|
| admin | Admin | Can edit | Can edit | Can edit | Can edit | Full access | Full access | Full access | Full access |
| anna.müller | Admin | Can edit | Can edit | Can edit | Can edit | Full access | Full access | Full access | Full access |
| eva.weber | Use | Can edit | Can edit | Can edit | Can edit | Full access | Limited access | Limited access | Full access |
| heike.schneider | Use | Can view | Can edit | Can edit | Can view | No access | Full access | No access | No access |
| jens.fischer | Use | Can view | Can edit | Can edit | Can view | No access | No access | Full access | No access |
| peter.schmidt | Use | Can view | Can edit | Can edit | Can view | No access | Full access | No access | No access |

Abbildung 11: Berechtigungsübersicht

### 2.2.3. Datenberechtigungen

Nun werden im nächsten Schritt die Berechtigungen so eingestellt, dass die Legal Entities im Workspace nur ihre eigenen Daten einsehen können und nicht die Daten der jeweils anderen Legal Entity.

Dabei werden sogenannte Datenklassen verwendet, um die Zuordnung von Daten zu Benutzern zu ermöglichen. Die Zuordnung der Datenklassen erfolgt nach einer Dimension im Projekt.

#### Definition des Sicherheitskonzepts

Die Daten können nach verschiedenen Dimensionen gesichert werden. Analog zu diesen Dimensionen lassen sich dann die Berechtigungen vergeben. Das Ziel ist, anhand der gewählten Dimensionen, die Benutzer unterscheiden und zuordnen zu können.

In unserem Beispiel wird die Dimension „Legal Entity" hierfür benutzt. Die Benutzer werden unterschieden in „LE 1" und „LE 2".

Grundsätzlich kann mehr als eine Dimension für die Datenberechtigung verwendet werden. Dadurch sind Kombinationen der Datenklassen und -berechtigungen möglich. Für ein anderes Beispiel wäre eventuell eine Dimension „Product" und eine Dimension „Country" sinnvoll.

#### Erstellen der Datenklassen

Es werden nun zwei Datenklassen erstellt. Dafür wählen Sie im Konfigurationsmenü „Projekte" und wählen dann Ihr Projekt aus. Anschließend klicken Sie auf „Security" (siehe Abb. 15).

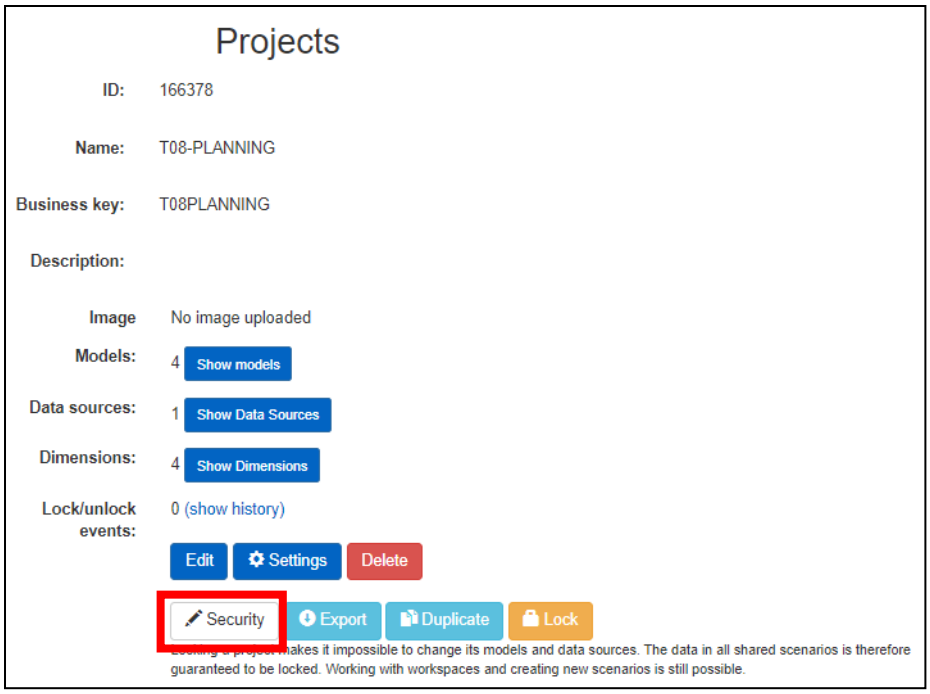



Abbildung 12: Projekt-Sicherheit

Danach wählen Sie das blaue Feld „Manage" (siehe Abb. 16).

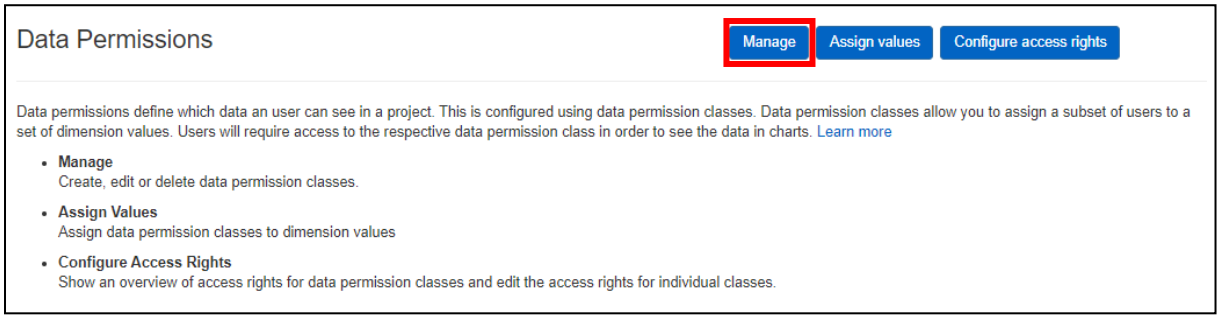



Abbildung 13: Manage Datenberechtigungen

Anschließend klicken Sie auf das grüne Feld „create new data permission class", um eine Datenklasse anzulegen. Dort geben Sie als Namen #LE 1 an. Der Vorgang wiederholt sich für #LE 2. (siehe Abb. 17).

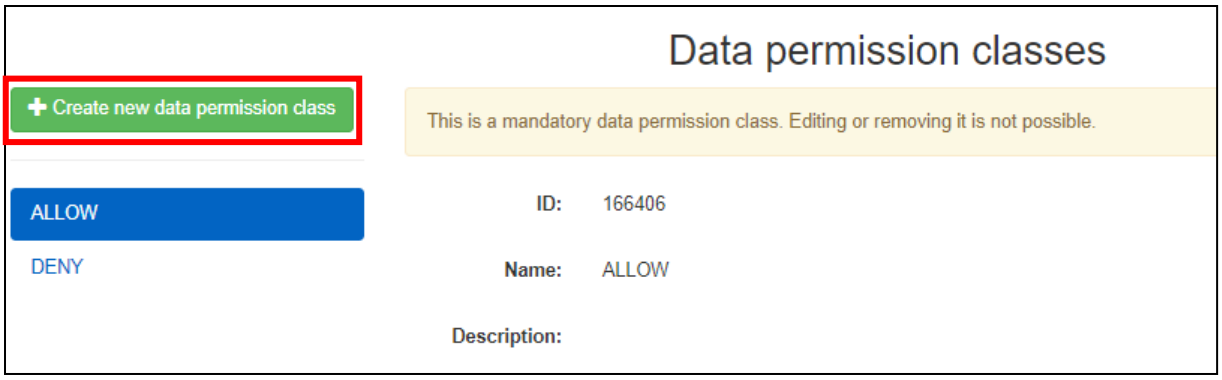



Abbildung 14: Datenklasse erstellen

Wenn die beiden Datenklassen erstellt wurden können im nächsten Schritt die Daten zu den Datenklassen zugeordnet werden.

## Daten zu den Datenklassen zuordnen

Gehen Sie wieder in die Security-Einstellungen ihres Projekts und wählen Sie „Assign Values“ (siehe Abb. 18).

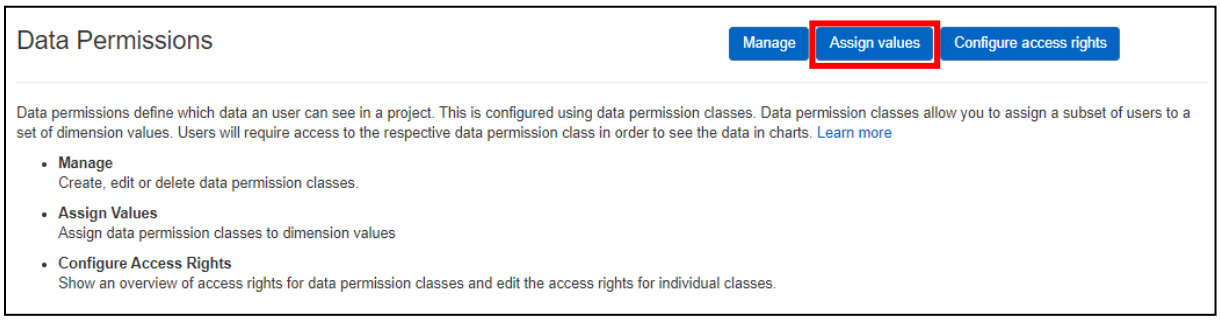



Abbildung 15: Datenklassen zuordnen

Dort erfolgt die Zuordnung der Daten der Dimension „Legal Entity“ zu den Datenklassen „#LE 1“ und „#LE 2“. In unserem Beispiel sollen die Daten grundsätzlich nur den jeweiligen Datenklassen zugänglich sein. Wählen Sie deshalb in dem Dropdownfeld für die Legal Entity 1 „#LE 1“ und für die Legal Entity 2 wählen Sie „#LE 2“ (siehe Abb. 19).

Für den Konzern kann noch eine Gesamteinsicht für alle Legal Entities gewährleistet werden. Es können auch Projektadmin-Berechtigungen vergeben werden, so dass die Admins alle Datenklassen einsehen können.

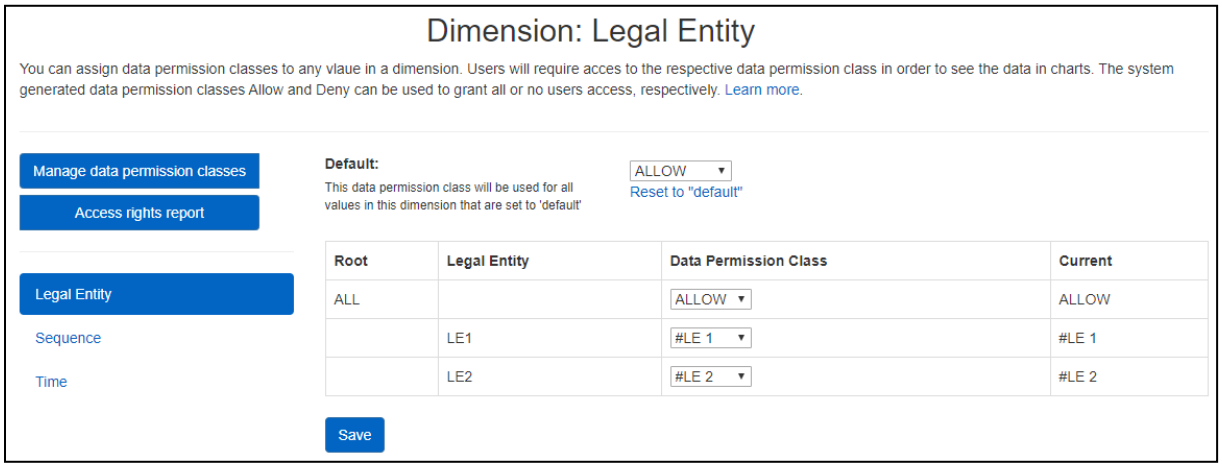



Abbildung 16: Datenklassen und Dimensionen zuordnen

Im nächsten Schritt werden für die Benutzer die Berechtigungen der Datenklassen vergeben.

## Berechtigung Datenklassen

Um die Berechtigungen für die Datenklassen an die Benutzer zu vergeben, gehen Sie wieder in die Security-Einstellungen ihres Projekts und wählen Sie „Configure access rights" (siehe Abb. 20).

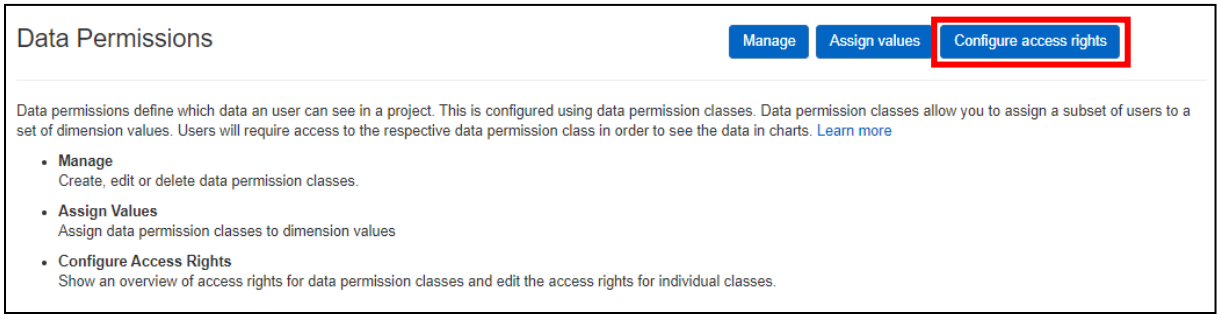



Abbildung 17: Berechtigung Datenklassen

Die Vergabe der Berechtigungen für die Datenklasse funktioniert nach demselben Vorgang wie bei den vorherigen Berechtigungen. Als Ergebnis sollen die Legal Entity 1 nur die #LE 1 und die Legal Entity 2 nur die #LE 2 sehen und bearbeiten können (siehe Abb. 21).

| Users | Data permission class #LE 1 Edit | Data permission class #LE 2 Edit |
|---|---|---|
| admin | Write access | Write access |
| anna.müller | Write access | Write access |
| eva.weber | Write access | Write access |
| heike.schneider | Write access | No access |
| jens.fischer | No access | Write access |
| peter.schmidt | Write access | No access |

Abbildung 18: Berechtigungsübersicht Datenklassen

Die Benutzer mit „Read Access" können Daten als Teil von Charts oder Analysen einsehen.

Die Benutzer mit „Write Access" können Daten einsehen und zusätzlich Annahmen auf Basis dieser Daten erstellen und bearbeiten.

Projektadmins haben automatisch „Write Access" für die Datenklassen.