# Employees, Roles and permissions

ADITO Software GmbH

From version xRM 2026.4.0 | April 2026

## Screenshots

The UX design of ADITO is continuously optimized for you. There may therefore be deviations in the screenshots.

# Agenda

## Employee administration

- Adding employees
- Assigning roles
- Password
- Employee Attributes
- Calendar permission
- User Tokens

## Roles & permission administration

- Role-dependent possibilities
- Overview of roles
- Role-dependent menu structure
- Adding roles
- "Passing on" roles
- Configuring permission for Entitys, Fields and Actions
- Deleting roles
- Deactivating permissions

Click on the ADITO A in this document to return to the agenda.

# Employee

# Employee

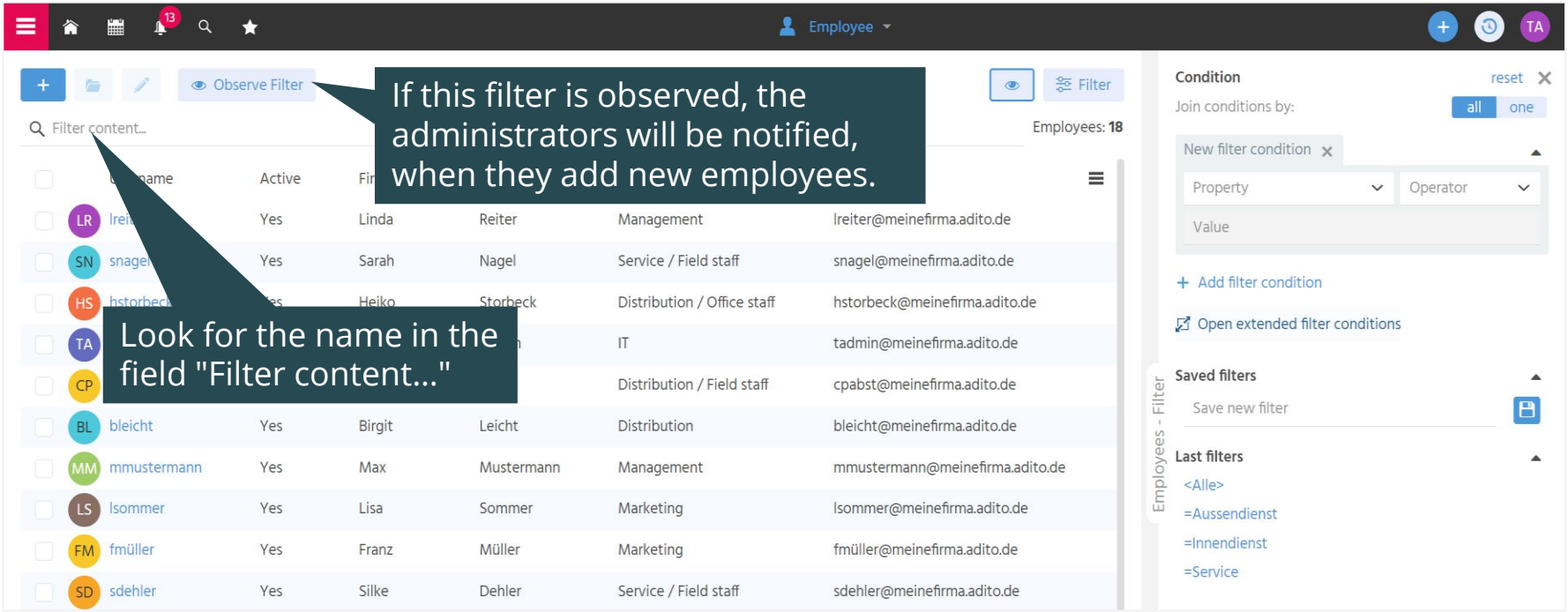
**An employee is a user of the CRM system.**

The Context "Employee" consists of administration functions:

- Adding an employee
- Password assignment
- Role assignment
- Attributes/documents
- Calendar permission
- User Token

# Employee

## Overview – FilterView

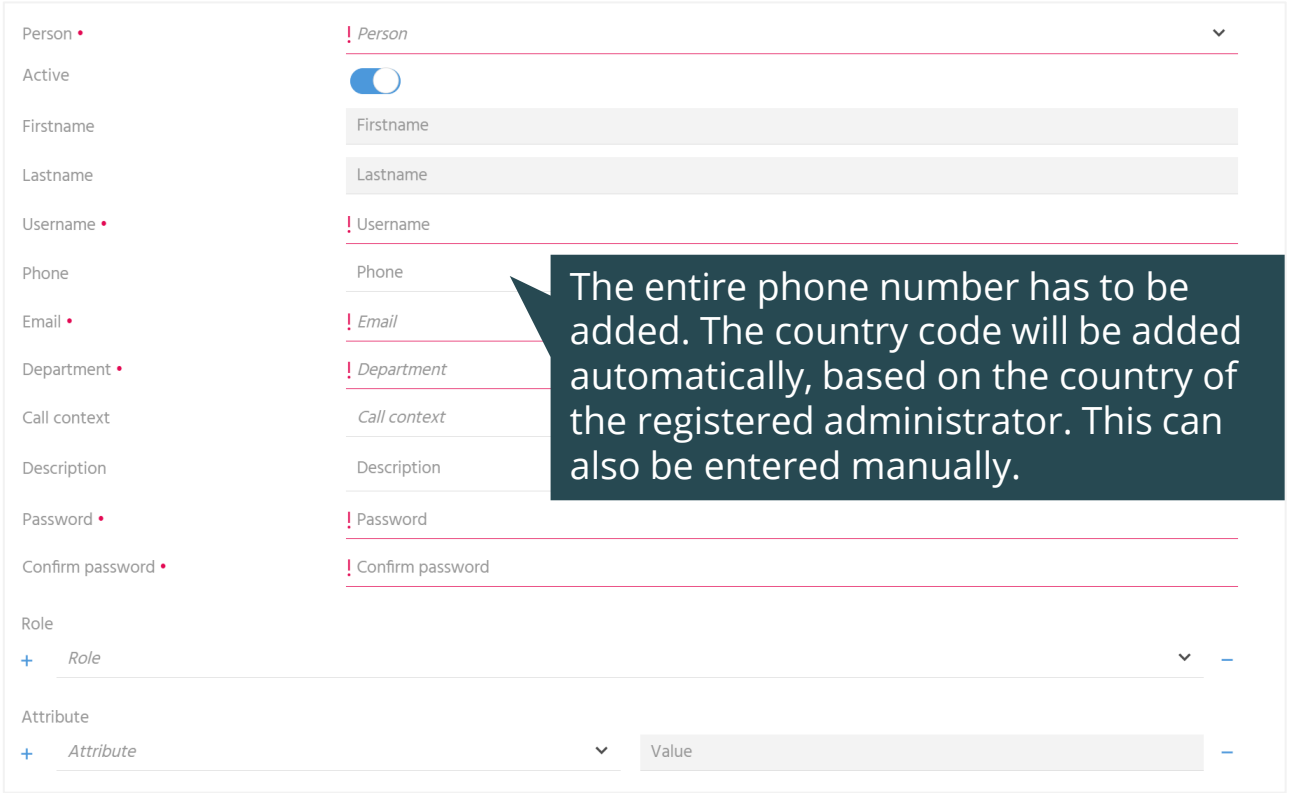


# Employee

## Adding employee

**Requirement:**
The employee is added as Contact in CRM.

This is necessary, since the data within the contact will be used for, e.g. placeholders in emails, letters, serial mails, etc.



# Employee

## Connection to telephone system

Telephone: Phone number of telephone system

**Example:**

An employee leaves the company and the phone number will be assigned again.

1. The former user will be set as inactive.
2. The new active user receives the extension of the previous user.

## Connection to Exchange

Employee email address will be used for the connection to the calendar. If this changes, the calendar ID will also change, i.e. the assigned calendar changes.

**Example:**

Employee changes their name.

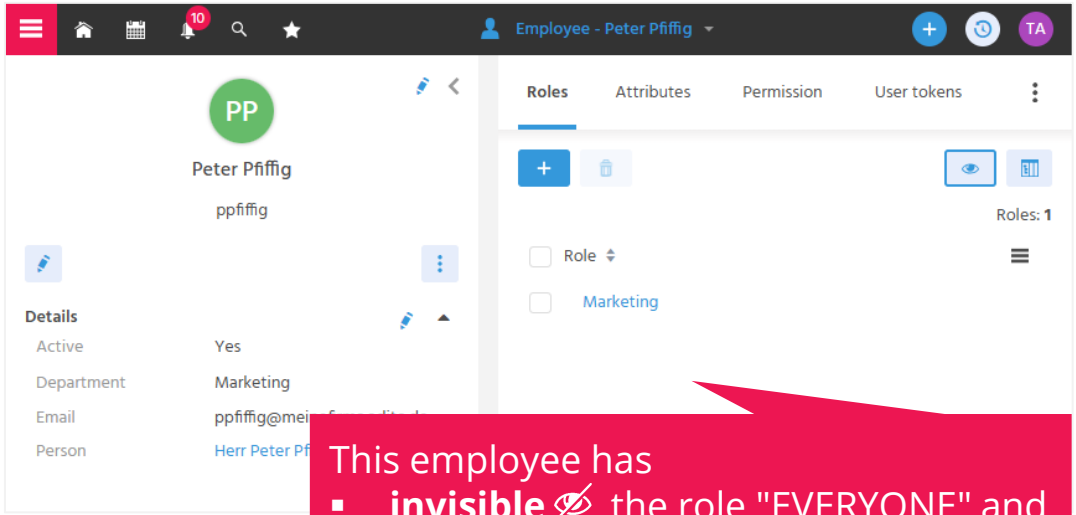
1. Context Contact: Change name and contact email address.
2. Context Employee: Change user name and Employee email address.
3. User has to sign in again.

Ultimately, the individually customized project must always be considered here.

# Employee

## Tab "Roles"

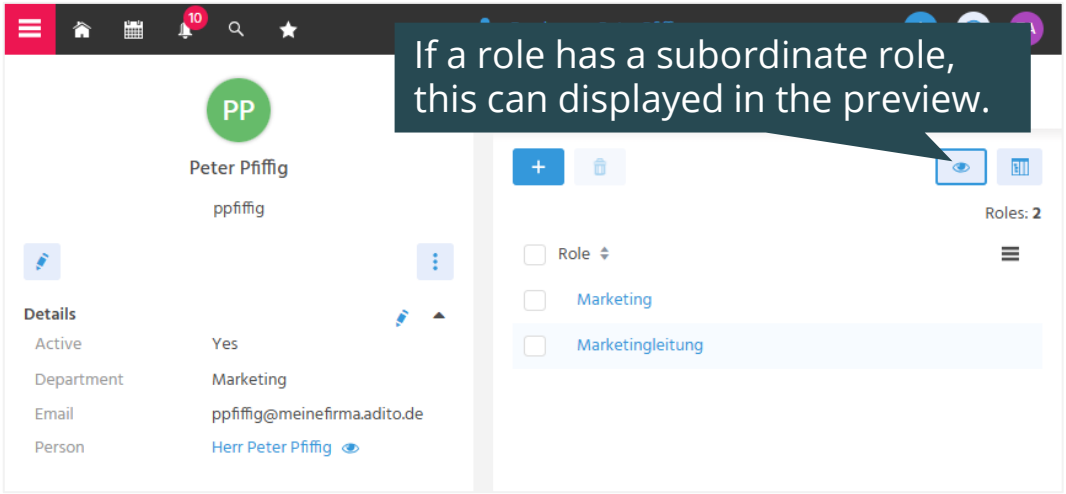
- **Every employee has the role "EVERYONE",** this will **not** be shown in the overview.
- The additional assigned roles will be displayed in the **tab "Roles"**.



# Employee

## Tab "Roles"

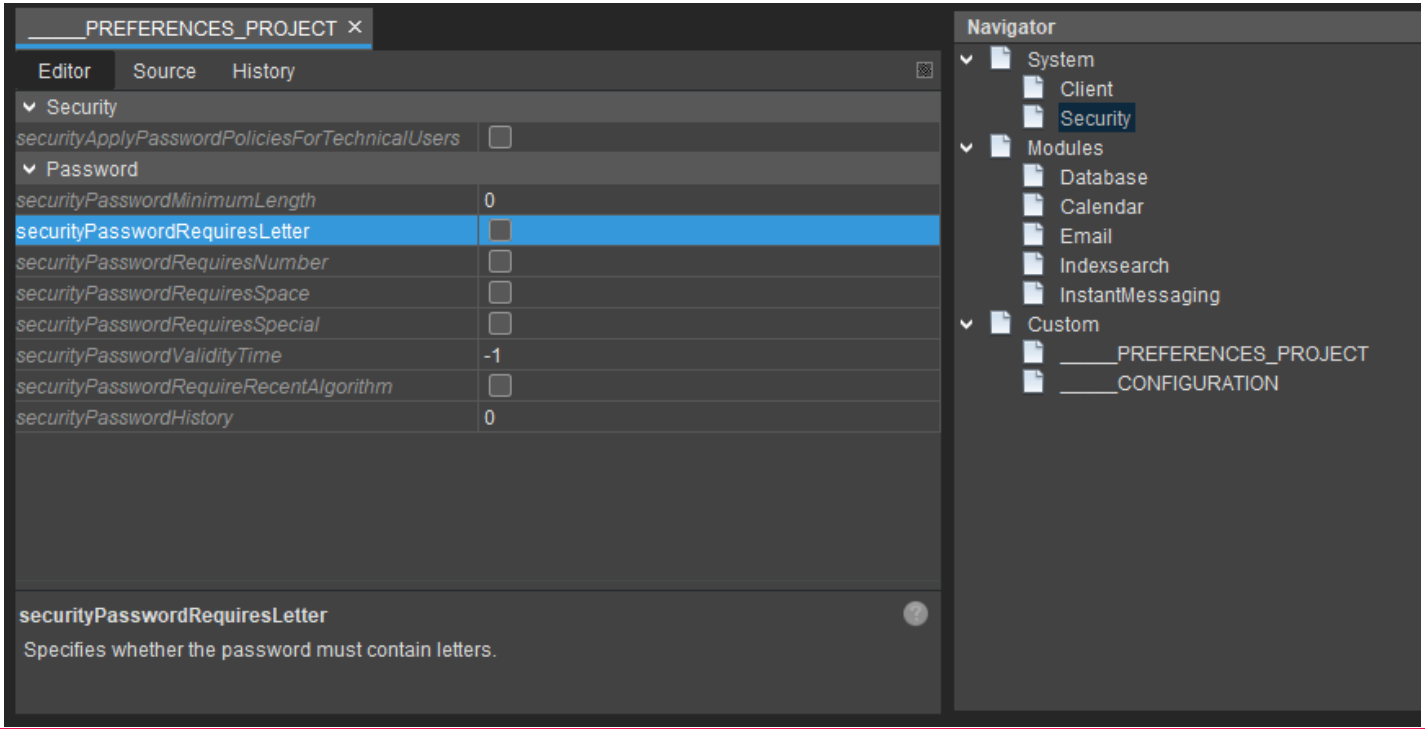
- Additional roles can be added in order to assign further roles to the employee.
- Roles can be deleted in order to remove them.
- The roles are connected with OR.




After changing the role assignement, the Client must be restarted, or the employee must login again.

# Employee

## Defining password guidelines in ADITO Designer

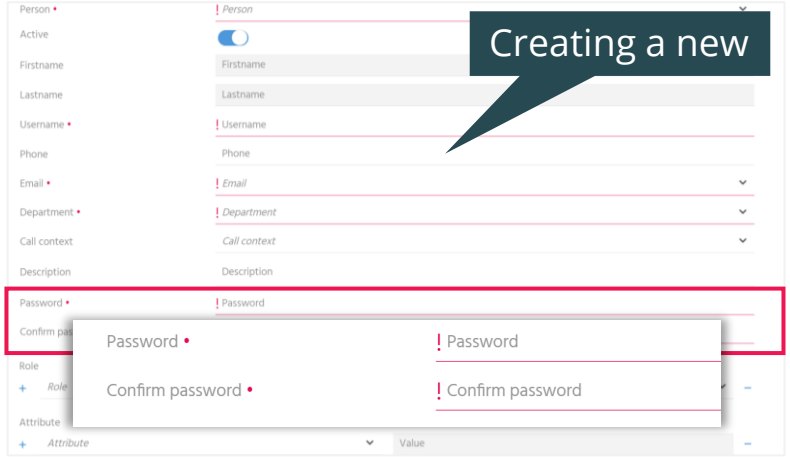


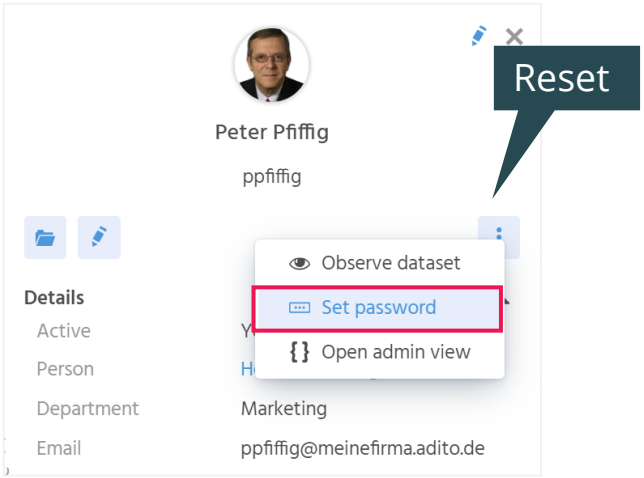
# Employee | password

## Set password as administrator

- When **creating a new** employee
- **Reset**

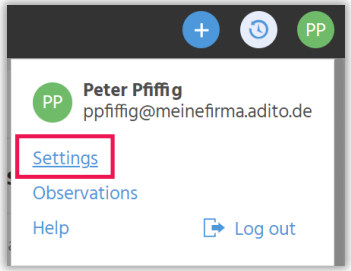
A random password is set for employees who are newly created via the AD process. **The administrator must then manually set a new password for the users.**

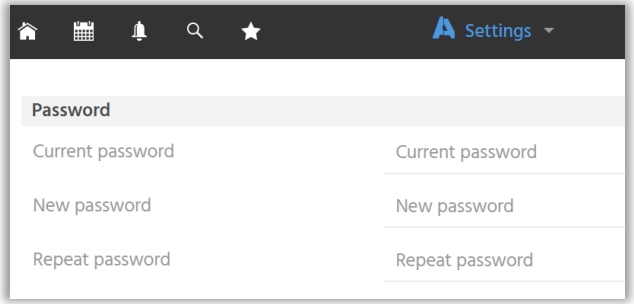


# Employee | password

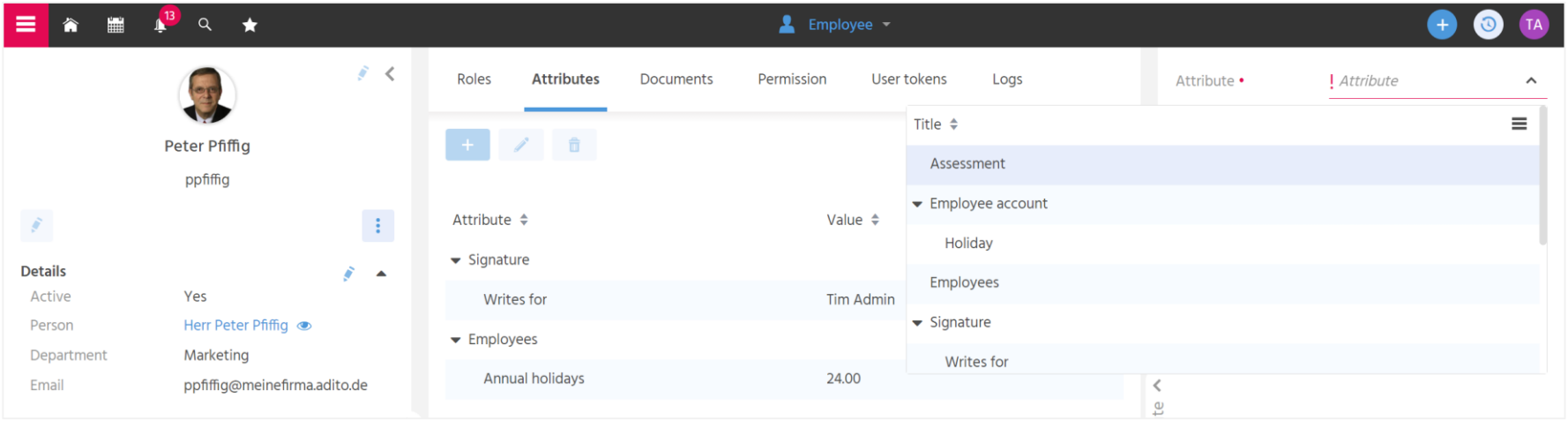
## Change password as employee



# Employee

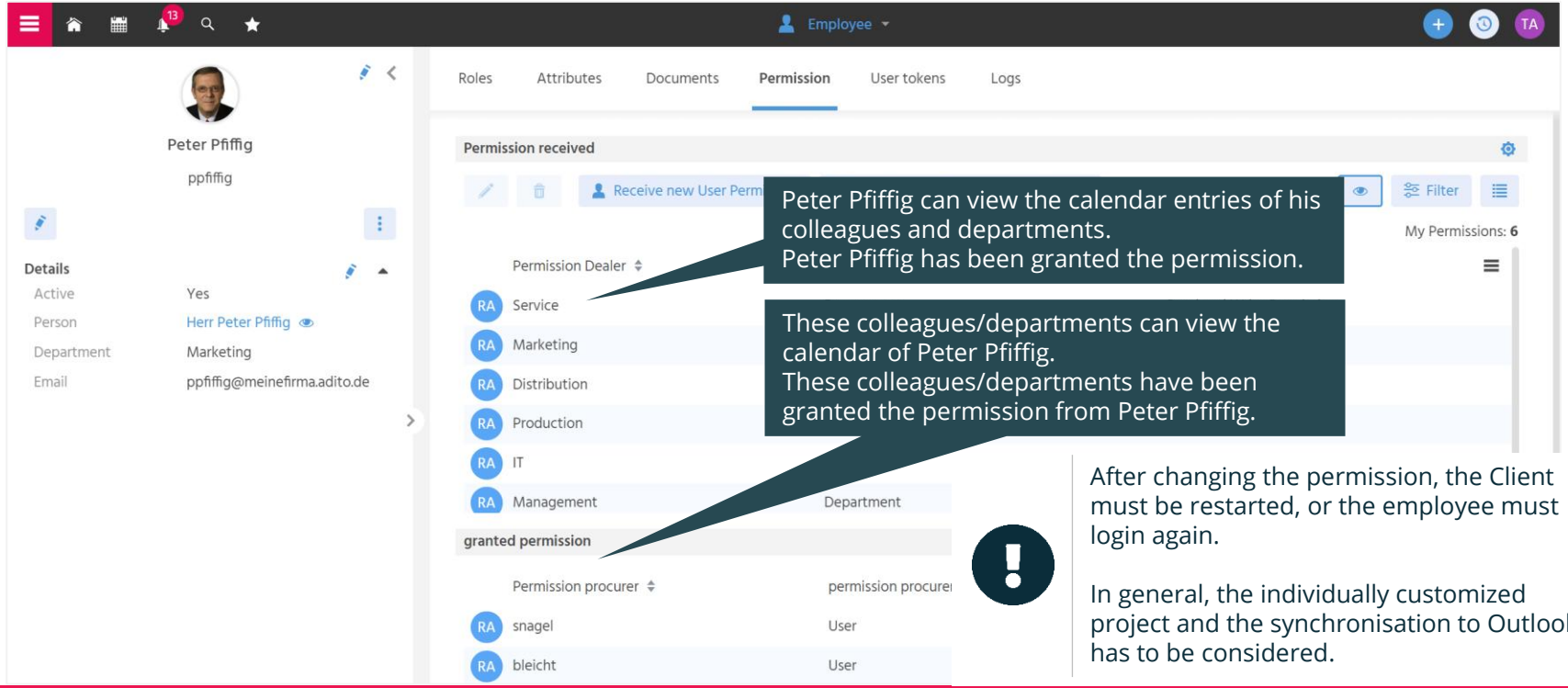
## Tab "Attributes"




Ultimately, the individually customized project must always be considered here.

# Employee

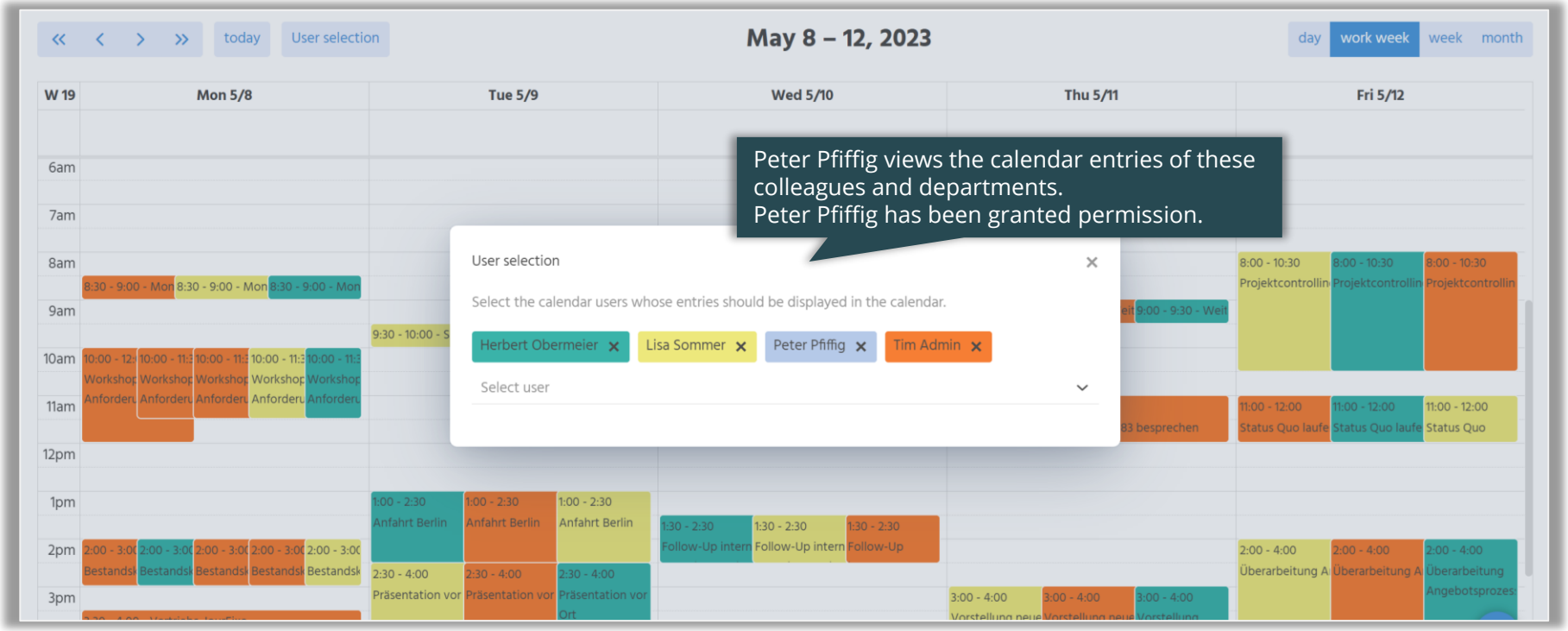
## Calendar permission – Tab "Permission"




After changing the permission, the Client must be restarted, or the employee must login again.

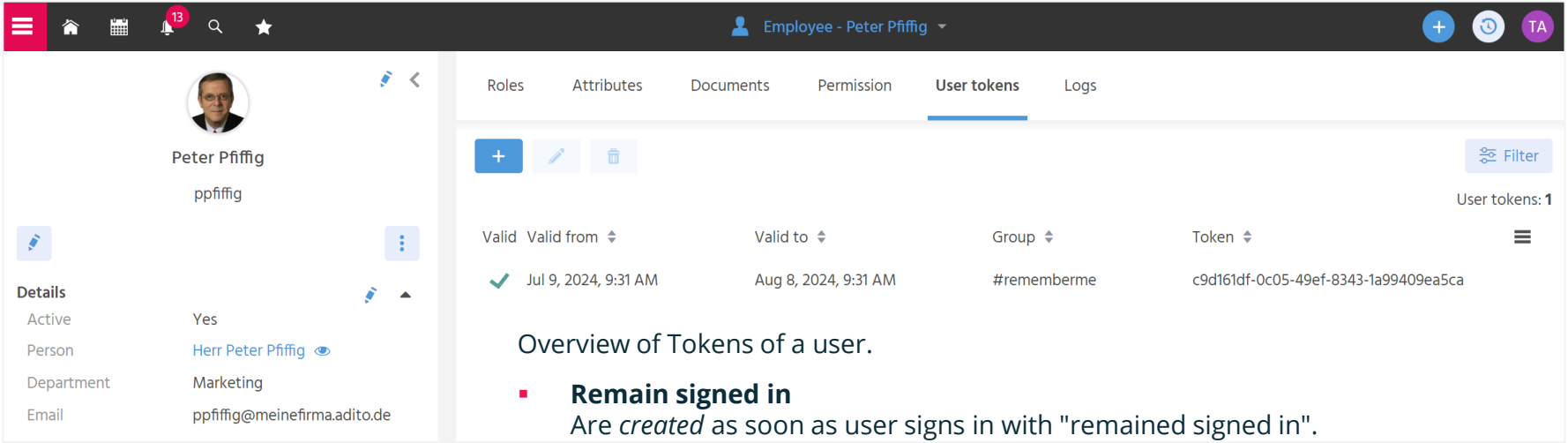
In general, the individually customized project and the synchronisation to Outlook has to be considered.

# Calendar permission



# Employee

## User Tokens

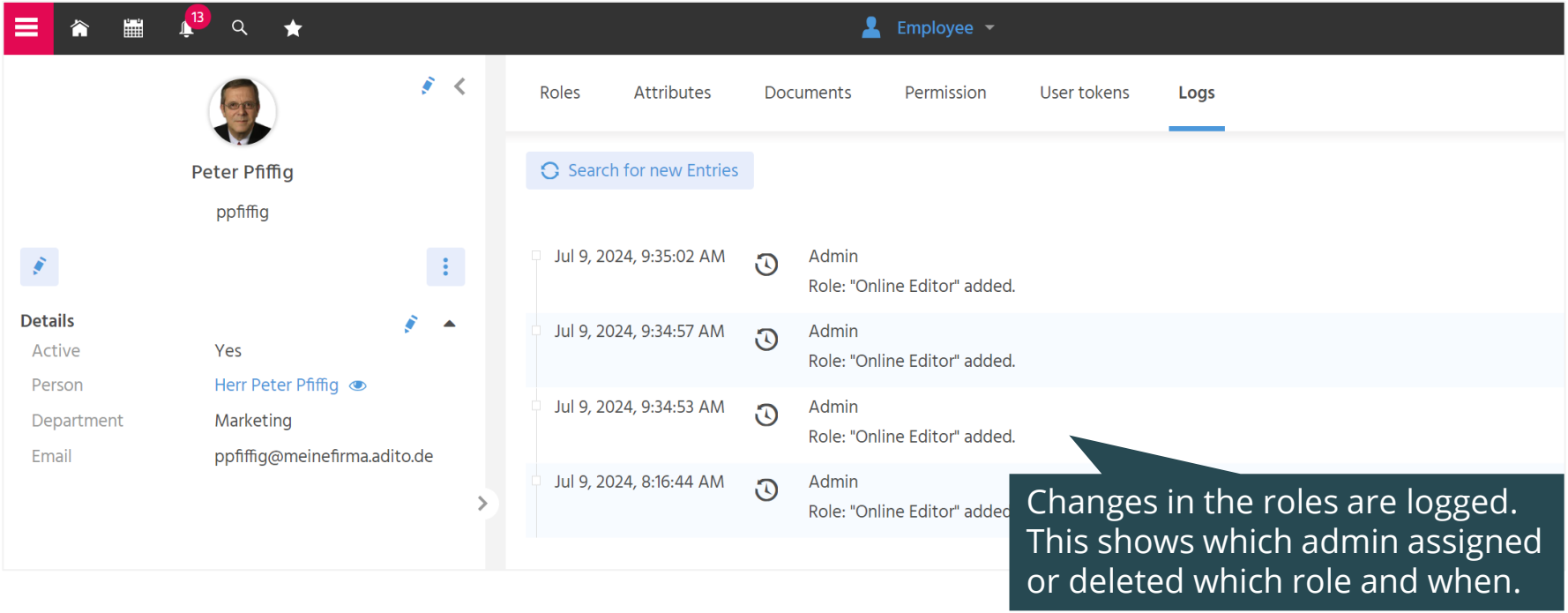



Overview of Tokens of a user.

- **Remain signed in**
  Are *created* as soon as user signs in with "remained signed in".
  Are *deleted*, as soon as user signs out.
- **Login Token**
  Are created by the admin with new creation. Access through Token is no longer possible, if **invalid** or **timeframe expired**. Access Web-Client through Token:
  *https://localhost:8443/client/?tokenId=*
  *Functionality has to be activated in Client Configurations.*

# Employee

## Tab "Logs"




Changes in the roles are logged. This shows which admin assigned or deleted which role and when.

# Employee

## Set to inactive

- Administrator sets the indicator "Active" to inactive in the employee data record.
- The employee receives the message "LoginFailed: Account expired" the next time they try to sign in

# Roles & Permissions

# Role-dependent possibilites in ADITO

## What can be mapped with roles?

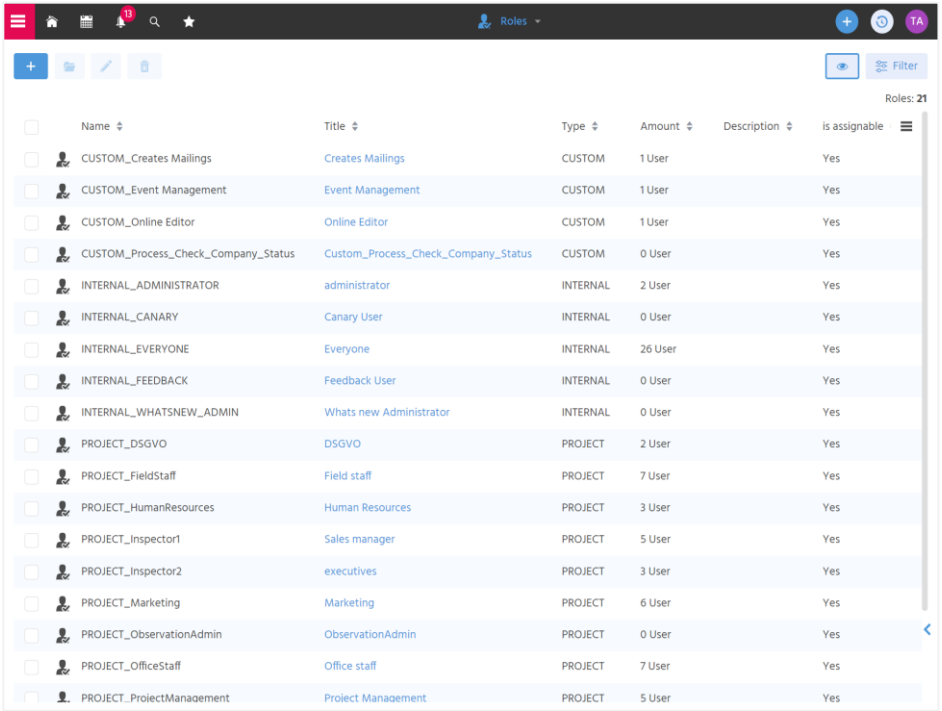
The **structure of the Global Menu** can be mapped depending on the role.

Role

**Permissions** can be mapped depending on the role. I.e. the display of Entitys, fields or buttons, as well as the editing, etc. of data records.

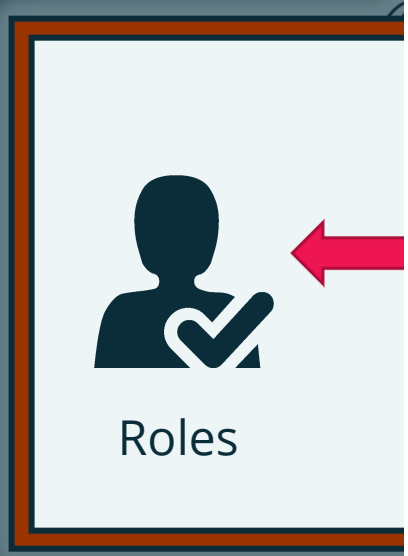
# "Overview" of Roles

## Context "Roles" – FilterView




- In the FilterView you receive an overview over all roles, which are available in the system and can be assigned to the employees.
- With the **"Create new" button** you create new roles of the type CUSTOM.
- Delete roles of the type CUSTOM.
- Open the main view of a role to configure the permissions.
- Further information to the type.
- Further information to the tag "Can be assigned", for the configuration of role groups.

# Role types




**CUSTOM_Roles**

- Are created in the ADITO Web-Client.

**INTERNAL_Roles**

- Are supplied by the ADITO core.
- INTERNAL_EVERYONE, INTERNAL_ADMINISTRATOR
- Can be used for the structuring of the menu.

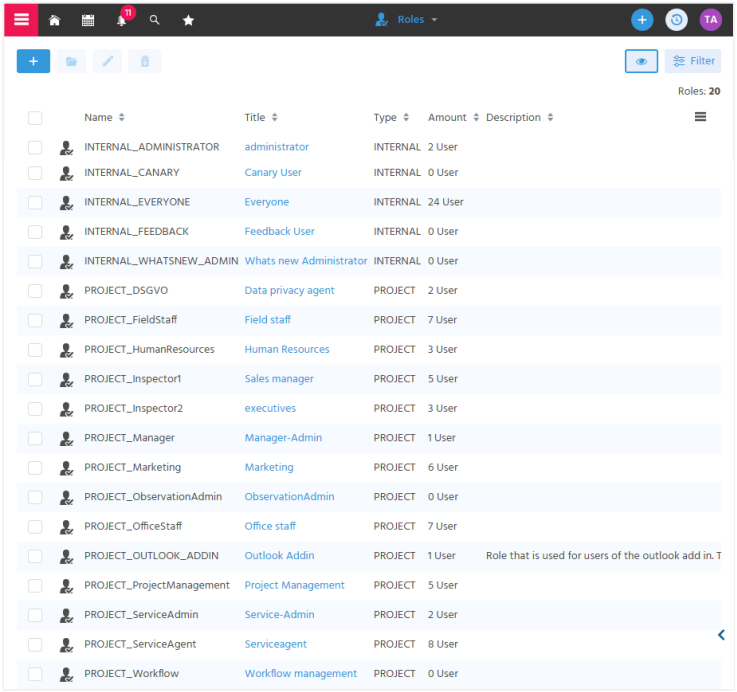
**PROJECT_Roles**

- Are created in the ADITO Designer.
- Can be used for the structuring of the menu.

The **authorization configuration** for **all role types** takes place in the Web Client.

# Roles in the xRM

## Roles that are available with the xRM: Type "Internal"

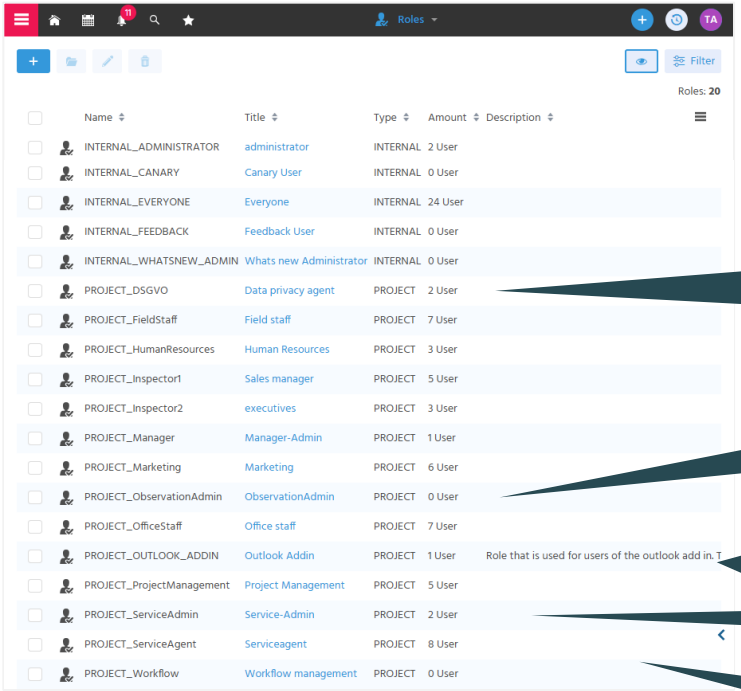



Roles of the type INTERNAL are set by ADITO and cannot be changed. They are used to map various basic rights/functions in the system.

- **INTERNAL_EVERYONE:** Roles that every user has in general (these are **not shown** in the tab "Roles" in the employee data record).
- **INTERNAL_ADMINISTRATOR:** Role with permission to access Entitys of Roles & Permission, Manager, sensitive attributes and the activity
- INTERNAL_CANARY: Role to test a new ADITO version, which is presented in a specific Canary area.
- INTERNAL_FEEDBACK, INTERNAL_WHATSNEW_ADMIN: (optional) Roles for the authorization of corresponding Contexts, if these are integrated in the system.

# Roles in the xRM

## Roles that are available with the xRM: Type "Project"




The roles "Field staff", "Human Resources", "executives" etc. are to be considered as examples and are partly assigned to different menu groups in the Designer.

Regarding the roles of the type "Project", ultimately, the individual implementation in the project must always be considered.

Users with the role of “Data privacy agent” can manage deletion indicators and define data protection-related attributes in the “Data protection administration” Context.

Users with the role "ObservationAdmin" can set Observations for others and activate email notifications for them.

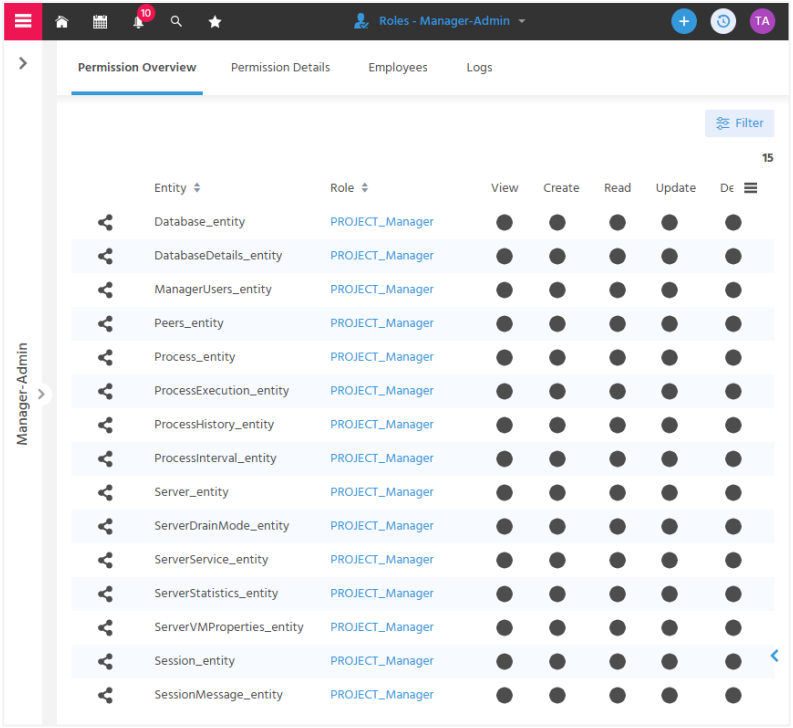
To use the Outlook add-in, users need the “Outlook Addin” role, together with the “INTERNAL_Webservice” role.

Role that is assigned to the Contexts of the Service Administration

Role in relation to access to the Workflow Modeler

# Roles in the xRM

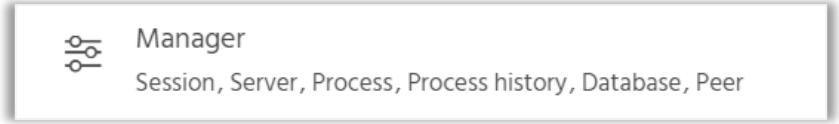
## Roles that are available with the xRM: PORJECT_Manager




The authorizations for the “Manager” menu group are mapped in the PROJECT_Manager role.

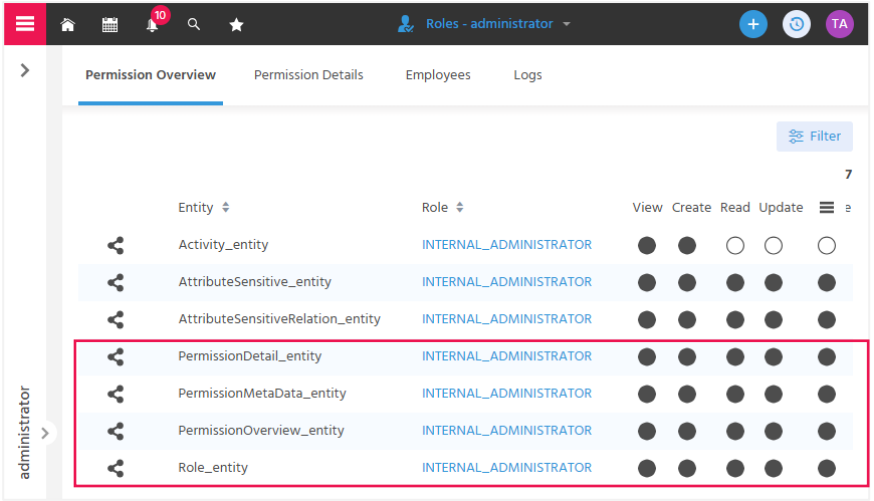
**This role must be assigned to the users who are to have access to the manager.**

In the xRM demo data, Tim Admin was assigned this role, so he can see the menu group.



# Roles in the xRM

## Special role of administrator: Pre-defined basic setting for permissions




The administrator (INTERNAL_Administrator) has the permission to the **Permission Entitys** in the Client. Those are:

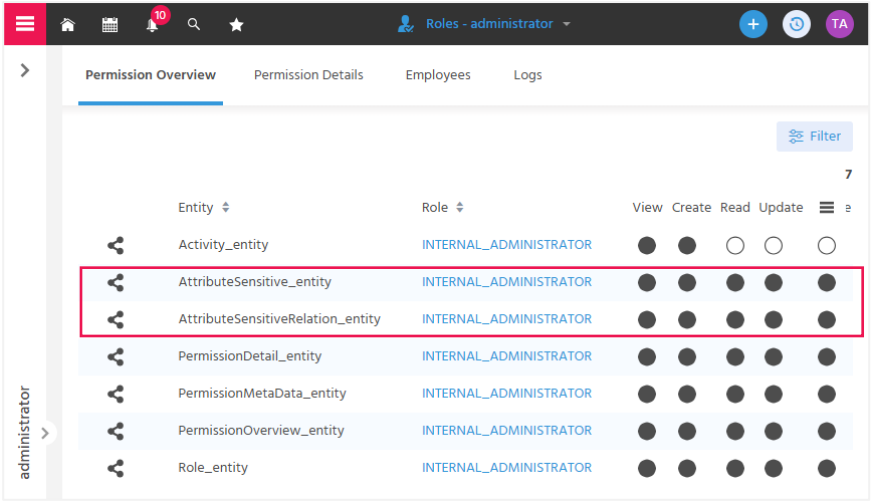
- Roles & Permission (Access to the Contexts through the Global Menu)
- Permission overview & Permission Detail (Tabs in the Contexts Roles & Permission)

This ensures that only the administrator has access to it in the project and can assign permissions accordingly.

ATTENTION: As an administrator, you must make sure that you do not remove the “usePermission” property from the permission entities, as otherwise all users would be authorized to do so.

# Roles in the xRM

## Special role of administrator: Pre-defined permissions with regard to sensitive attributes



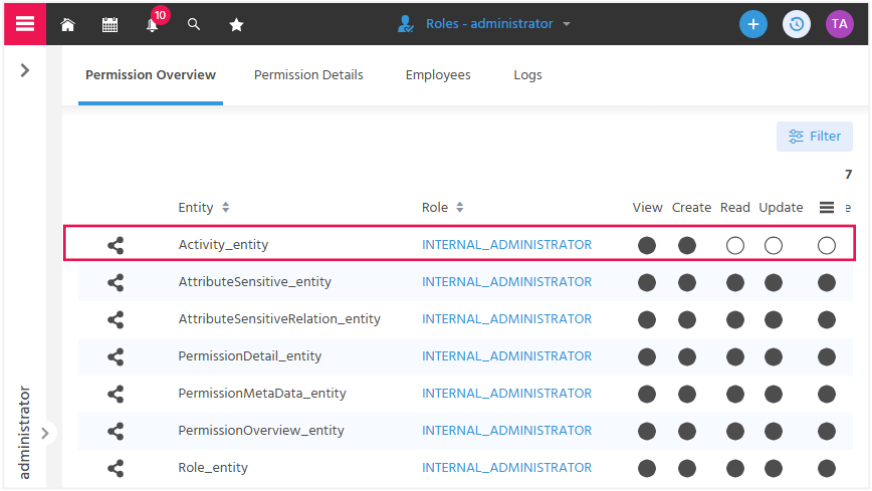

The administrator (INTERNAL_Administrator) has permission to access the Entitys in order to **record sensitive attributes in the Client**. These are:

- The table "sensitive Attributes" (Tab "Attributes" in Company) AttributeSensitiveRelation_entity)
- The dropdown for sensitive attributes (Attribute for sensitive attributes) (AttributeSensitive_entity)

This defines in the project that first the admin has access to it and can, if necessary, create and permit further roles for sensitive attributes.

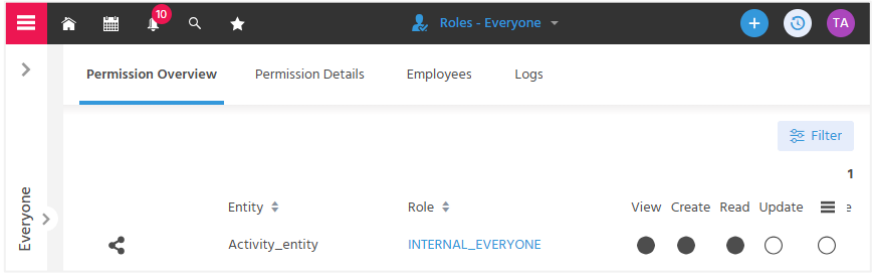
# Roles in the xRM

## Special role of administrator: Pre-defined permissions with regard to activities

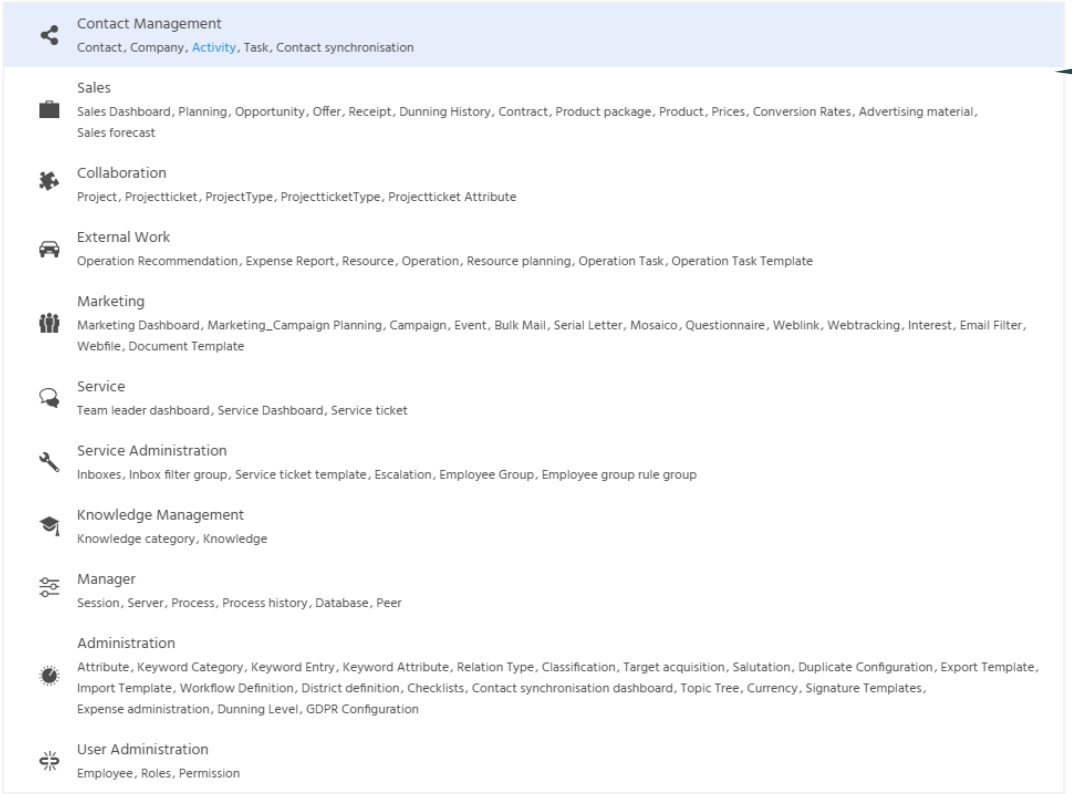



The administrator (INTERNAL_Administrator) has permission to the Activity-Entity, in order to edit or delete **Activities in the category "System"**.

These activities are created by the System and cannot be edited by somebody with the role "EVERYONE" (INTERNAL_Everyone). This is set in the permissions of both roles as a condition of the rights.



# Structure of the Global Menu

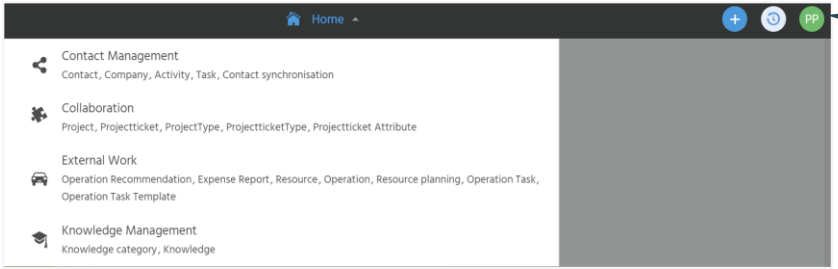



Example: Division/Grouping of all possible Contexts in the Global Menu

- What does EVERYONE have to view?
- What does only the Administrator need?
- What is required within the departments?
- What is required for special processes?

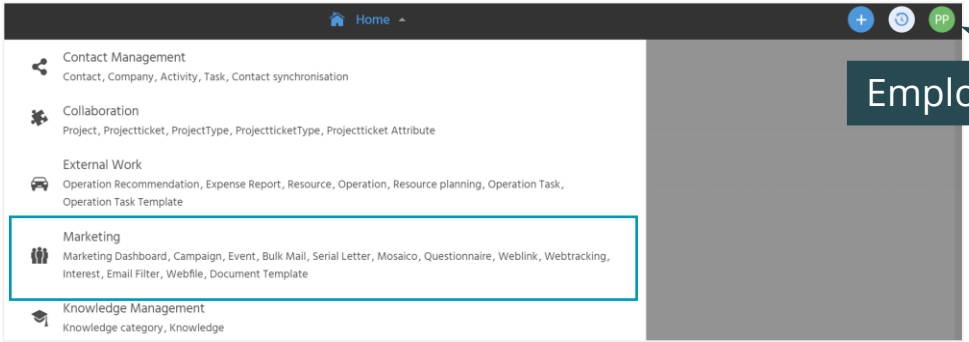
# Structure of the Global Menu

## Example




Employee has the role EVERYONE.

These menu groups are assigned to the role EVERYONE in the ADITO xRM.




Employee has the roles EVERYONE and Marketing.

The menu group "Marketing" and its Contexts in ADITO xRM are assigned to the role Marketing.

# Structure of the Global Menu

## Procedure

In the application model, you define the menu structure of the global menu that a user sees based on their roles. You can use roles of the type INTERNAL or PROJECT for this.

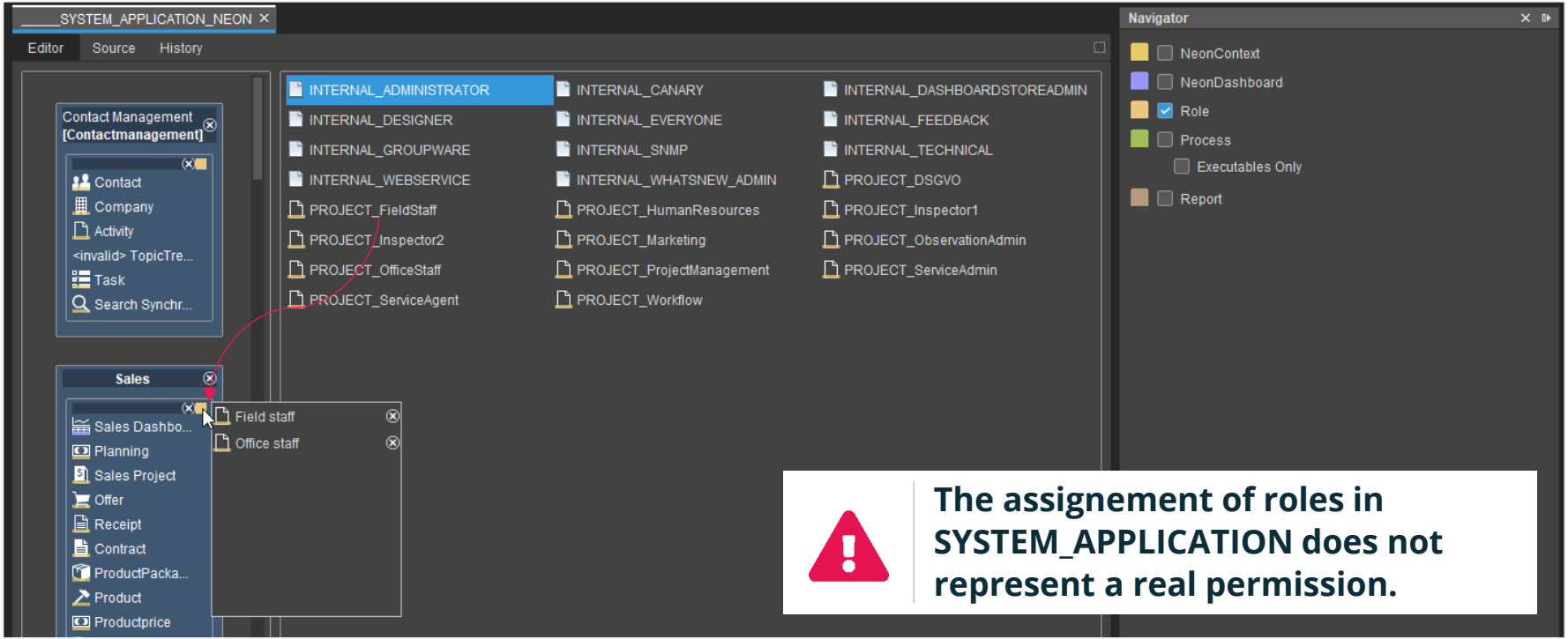
The roles are assigned to the menu groups. A menu group can also contain only individual contexts (see next slide).

The general procedure for creating and assigning roles in the Designer can be found in the Customizing Manual.

However, it is also possible to use only the “Everyone” role in the application model and assign it to all menu groups. This allows you to customize the global menu structure using the CUSTOM roles in the authorization management in the web client.

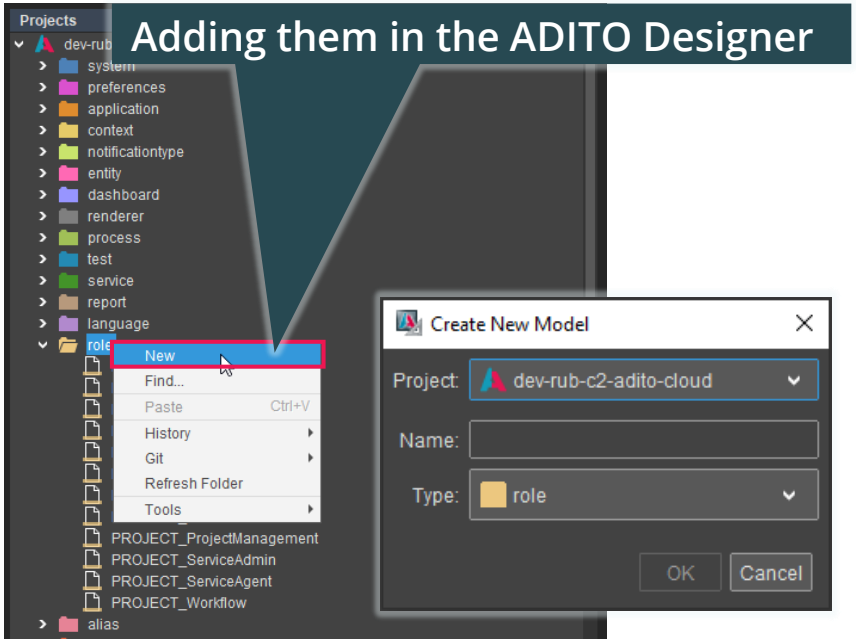
# Structure of the Global Menu

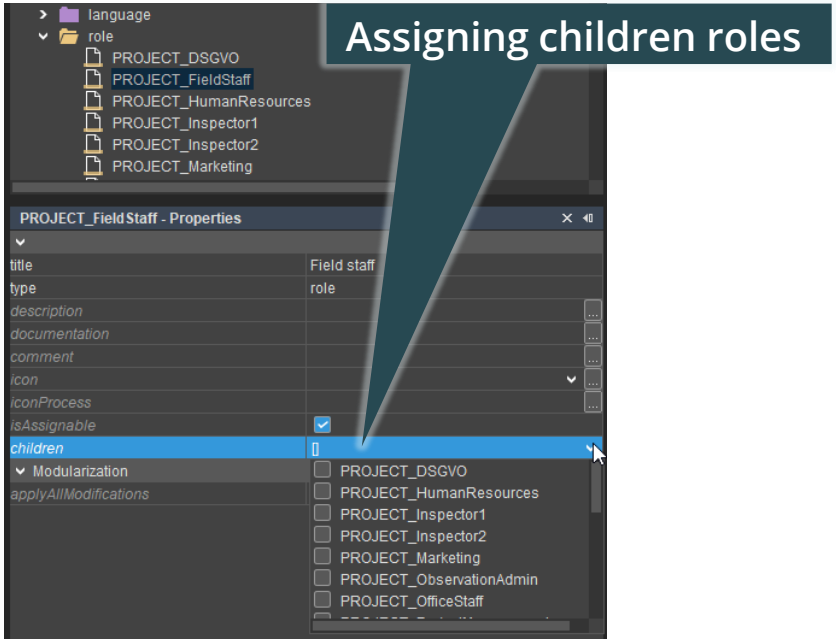
## Roles can be assigned to menu groups using Drag&Drop



# PROJECT_Roles

You can create this type **in the designer** within the project, and it is thus also saved in the Git project. These roles can be assigned to the respective menu groups (contact management, sales, marketing, etc.) in the application model in the designer and used to define the menu structure. In addition, it would be possible to use them in the JDito code if necessary.



# What can roles represent?

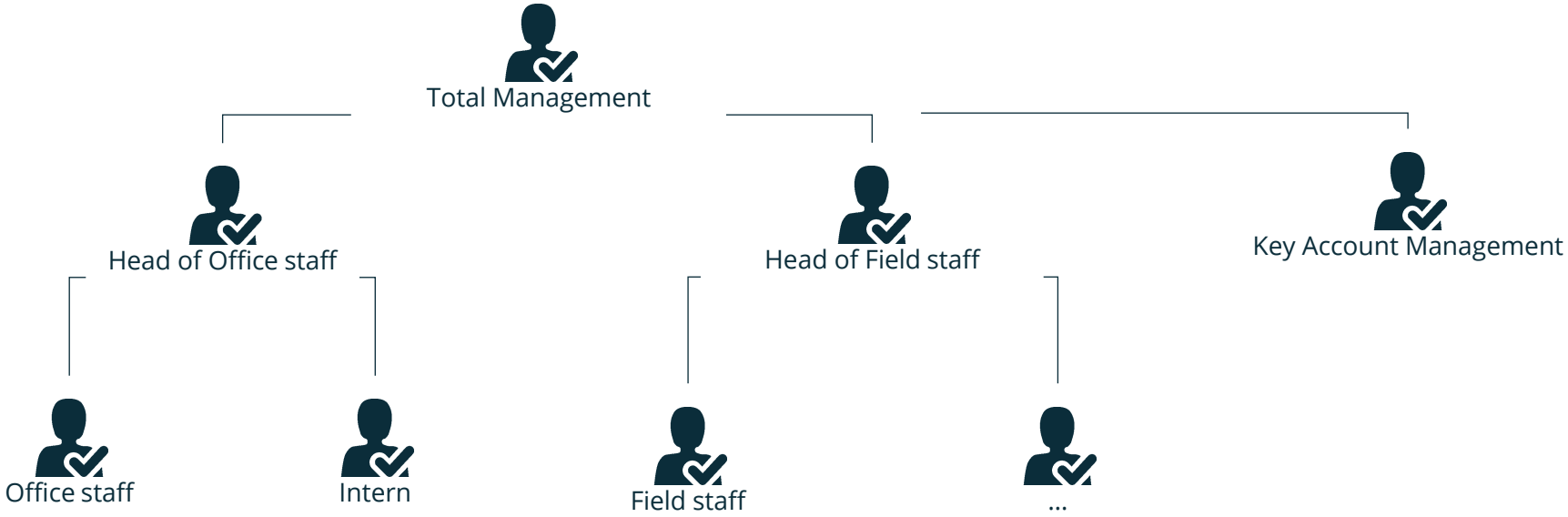
**Roles can…**

- Represent **personas,** which present the roles of the employees (Role groups*).
- Represent **processes,** which Personas can perform (Role groups*).
- Represent **functions** and **filter,** which are required for the performance of these processes.

*Why are we talking about role groups?
Personas and process roles are also referred to as role groups because their permissions are not directly linked, but they only receive their rights through a group of child roles. However, it is also possible to group the function or filter roles in the persona role without using process roles.

# What can roles represent?

## Personas in Organizational charts, e.g. Sales department



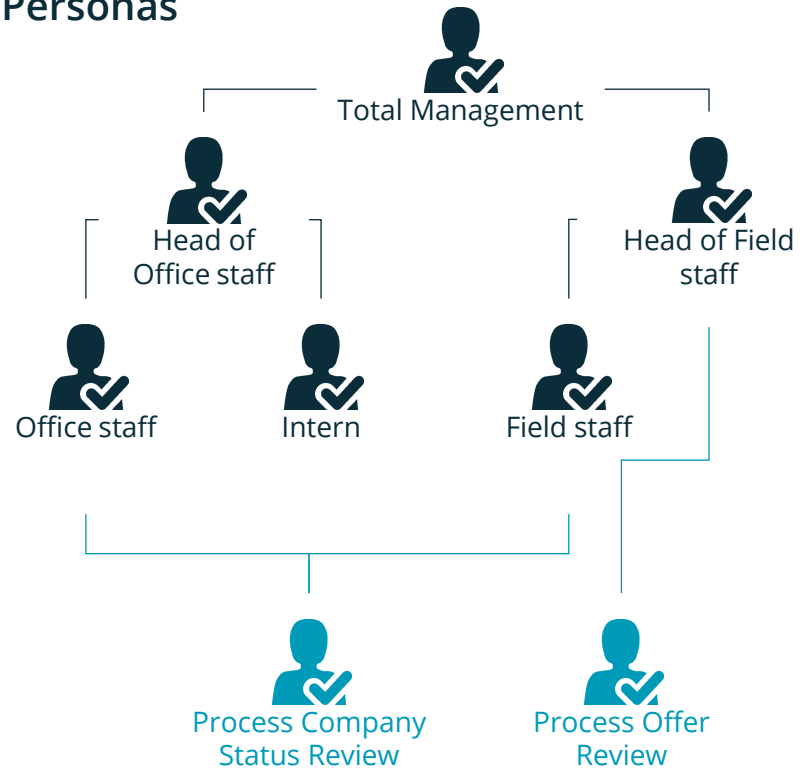
# What can roles represent?

**Processes (workflows), which are carried out by Personas**

Examples:

- Process Company Status Review
- Process Vacation approval
- Process Sales evaluation
- Process Sales planning
- Process Offer Review
- Process Product creation
- ...

The process roles are passed onto those Peronas that should carry out the respective process.



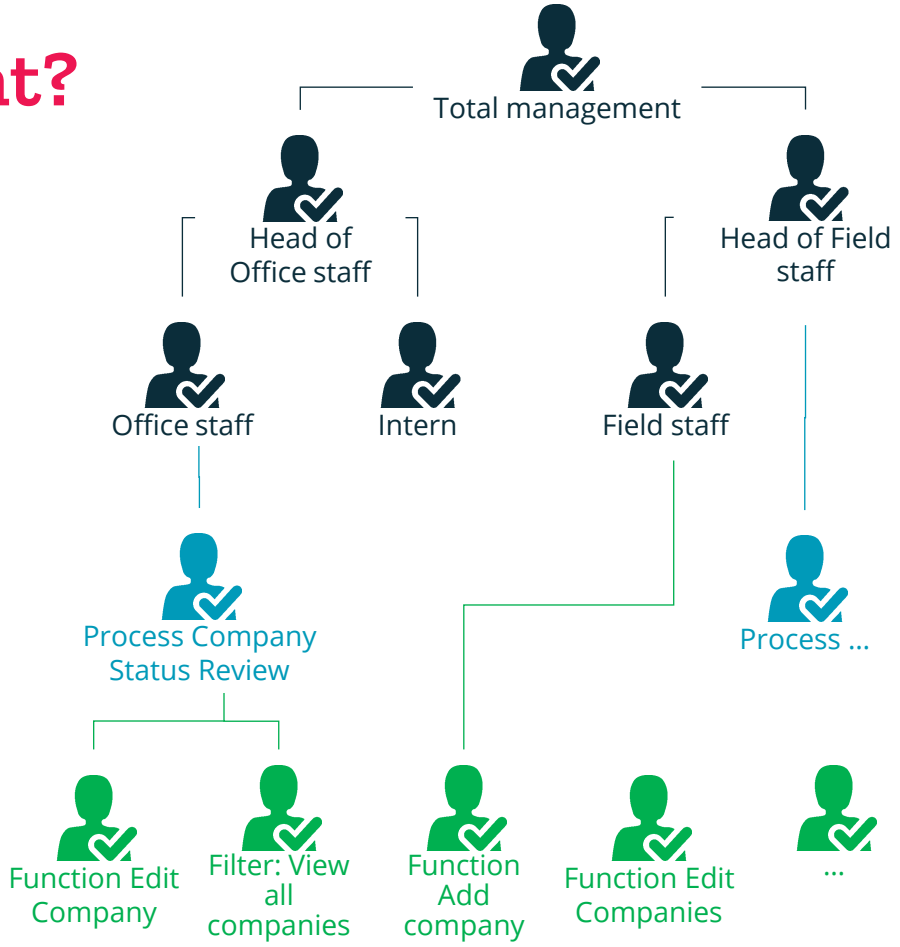
# What can roles represent?

## Functions and Filter

Example:

- Filter: view all companies
- Filter: view all companies from my region
- Function Add companies
- Function Edit companies
- Function Deleting companies
- Function view status
- Function Edit status
- …

The function or filter roles are inherited by the process roles or personas.



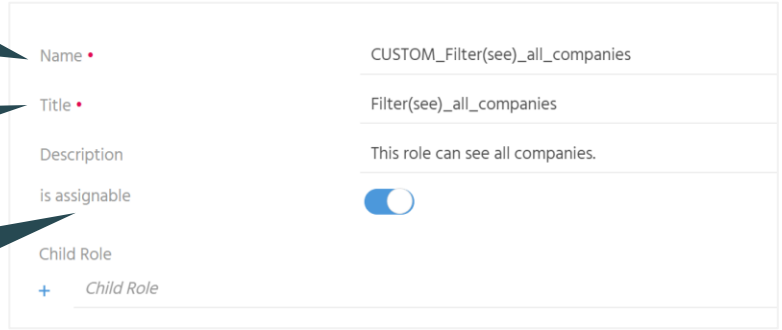
# CUSTOM_Roles

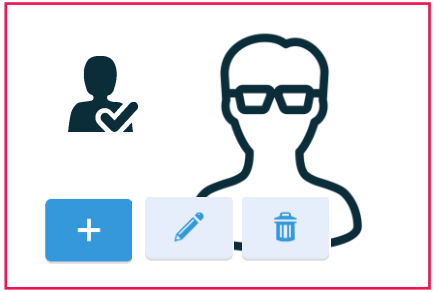
## Add in ADITO Web-Client

The name is the unique key for the role and can therefore only be assigned once. It is automatically supplemented by the designation of the type.

The title is the name of the role that is displayed, for example, when the employee is assigned.

The indication "is assignable" must be activated, in order to assign this role to a different role as child role.



# How can roles be "passed on"?

## Parent / child roles

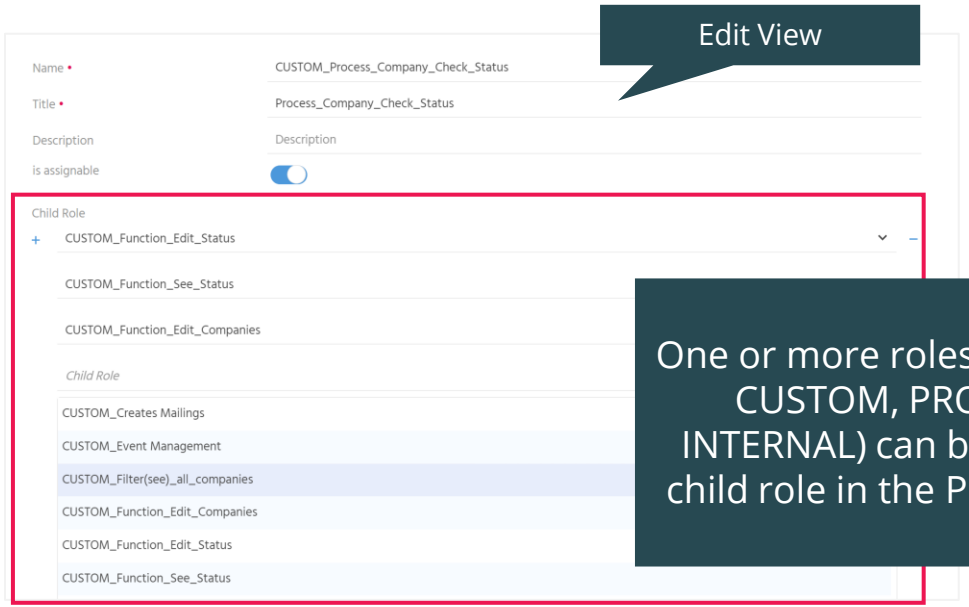
**Conditions:**

- With the **Is assignable** indicator, a role is made available to others as a child role and can transfer its authorizations to the parent role.
- CUSTOM roles can be used in the client as child roles and can be assigned CUSTOM, PROJECT or INTERNAL roles can be assigned.
- PROJECT roles can be used as child roles in the Designer and assigned to them.

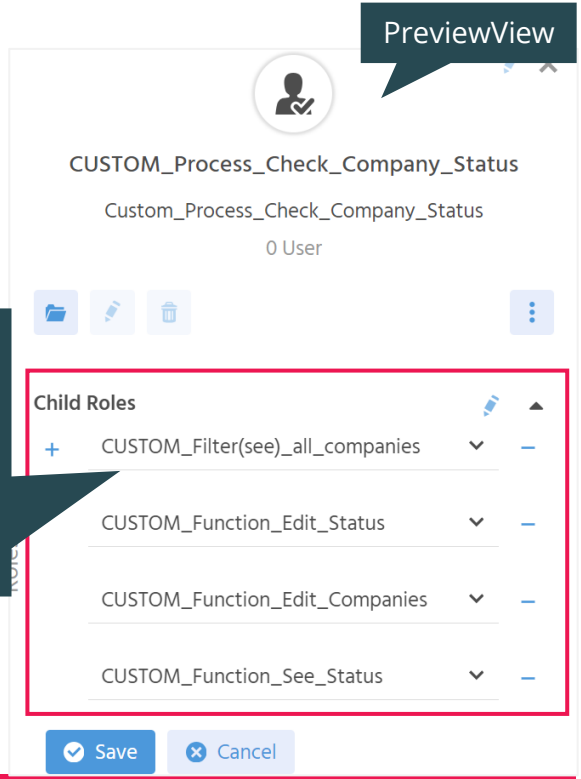
- The roles are linked with OR. **This means that they are not "inherited" but "stapled".**
- This means that someone receives "virtually the maximum" of all authorizations that they receive via the roles.

# Parent and subordinate roles

## Assigning Child Roles in the Web-Client for CUSTOM roles

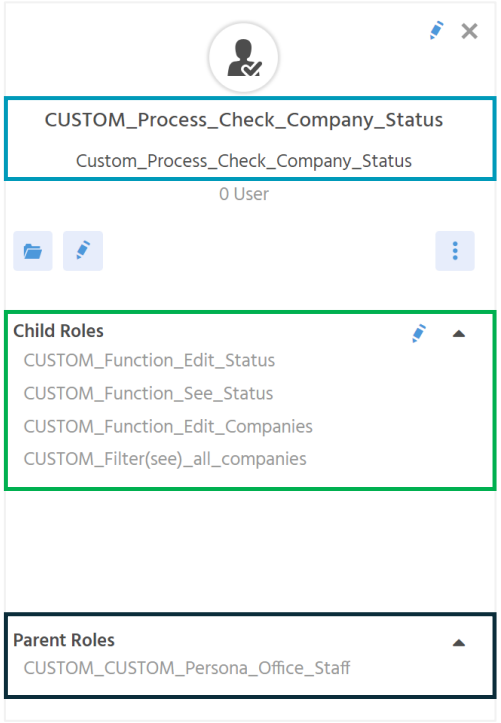



One or more roles (of the type CUSTOM, PROJECT or INTERNAL) can be added as child role in the PreviewView.

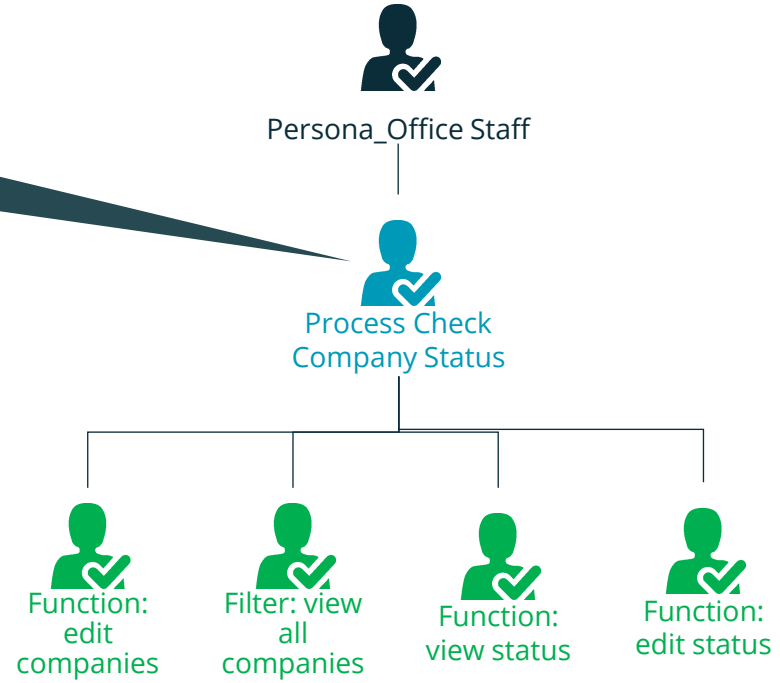


# Parent and subordinate roles

## Overview in the PreviewView

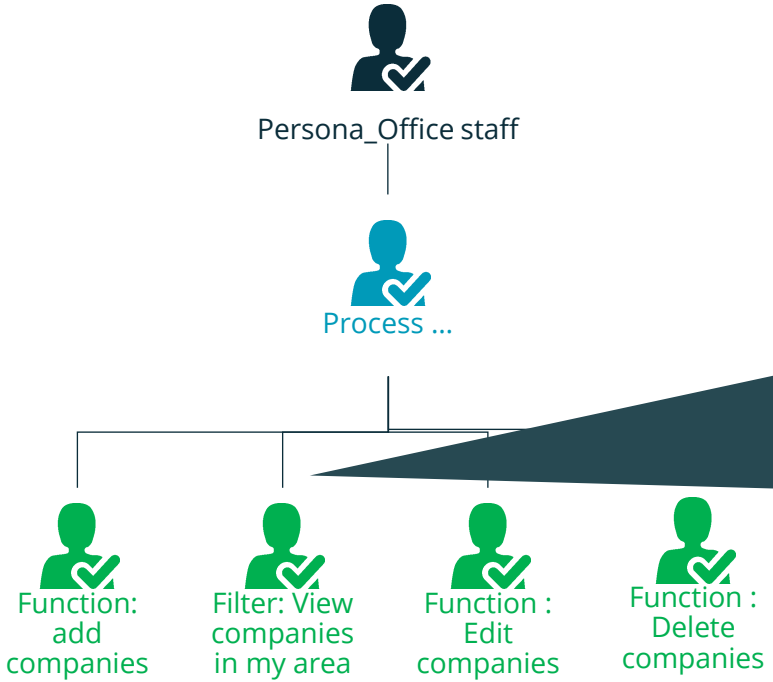



Perspective from the view of the "middle" role.



# Parent and subordinate roles

## Grouping of the roles

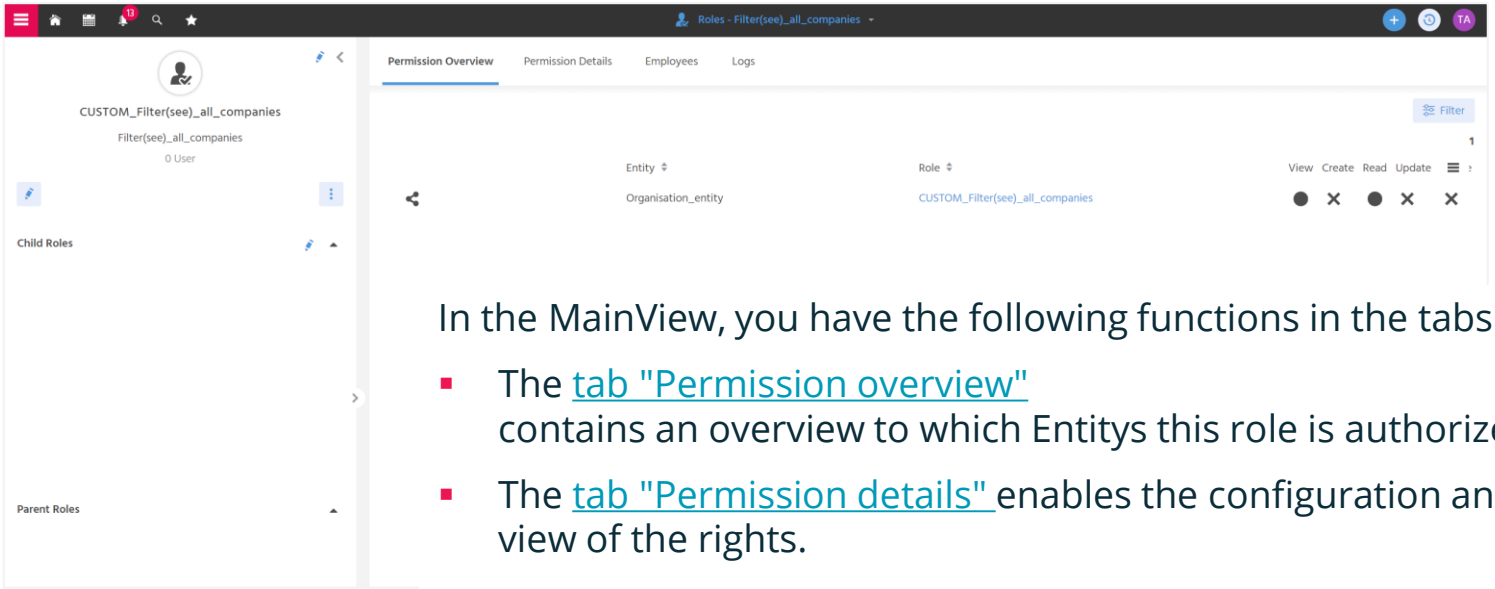



If a role group uses the restricted view of data records, the restriction can be waived for the Edit and Delete rights, unless other restriction conditions are required for these rights.

Example:
The role only views (READ) companies from the area assigned to it. This means that the UPDATE and DELETE rights do not need to be restricted by the condition, as the role can only edit or delete what it views

# Context "Roles"

## MainView



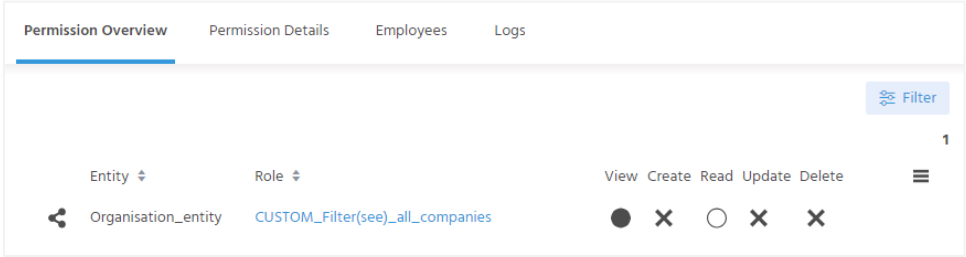

In the MainView, you have the following functions in the tabs:

- The tab "Permission overview" contains an overview to which Entitys this role is authorized to.
- The tab "Permission details" enables the configuration and the detailed view of the rights.
- The tab "Employees" offers an overview of all users assigned to this role.

# Context "Roles"

## Tab "Permission overview"

- In the columns VIEW and CREATE, the rights to the **Entity level** are displayed. Therefore, the display of views of the Entity are controlled, as well as the creation of new data records.
- The columns READ, UPDATE and DELETE concern the **data record level**. This controls which data records can be viewed, edited or deleted.
- By looking at the **icon**, you can check which **Permission status** has been assigned:
  - ● Circle (filled): is always allowed
  - ○ Kreis (empty): is limited allowed, i.e. a filter condition has been added
  - ✕ Cross: is never allowed

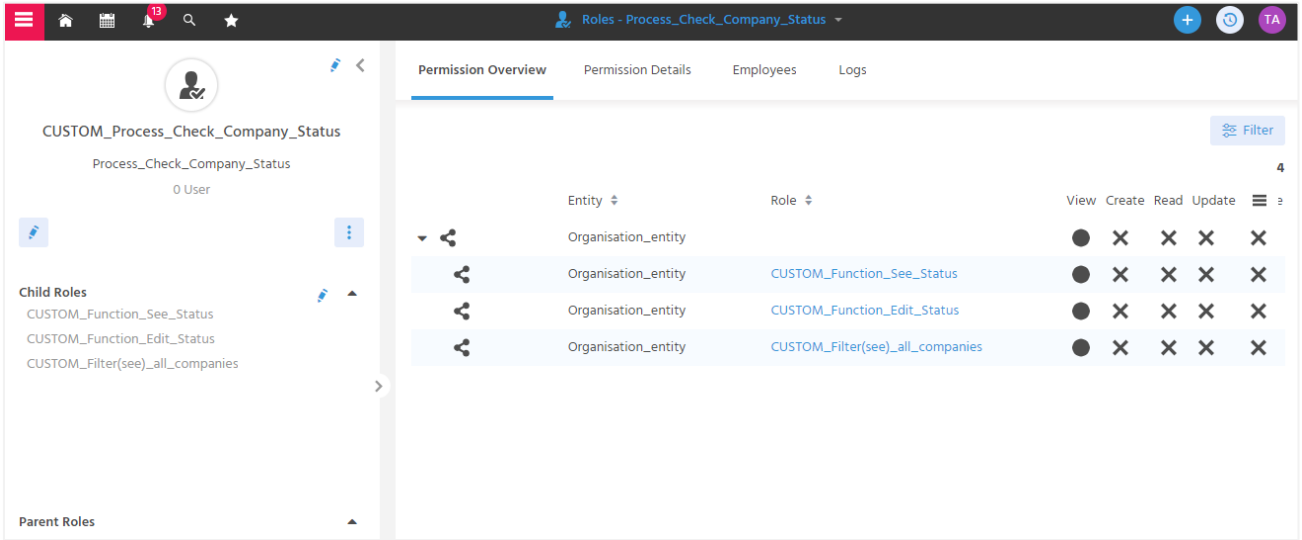


# Context "Roles"

## Tab "Permission overview"

In the MainView of a role with child roles,the individual roles and its permissions are displayed in the tab "Permission overview" in the form of a treetable.

The sum of the authorizations for the parental role can therefore be viewn in the first line.



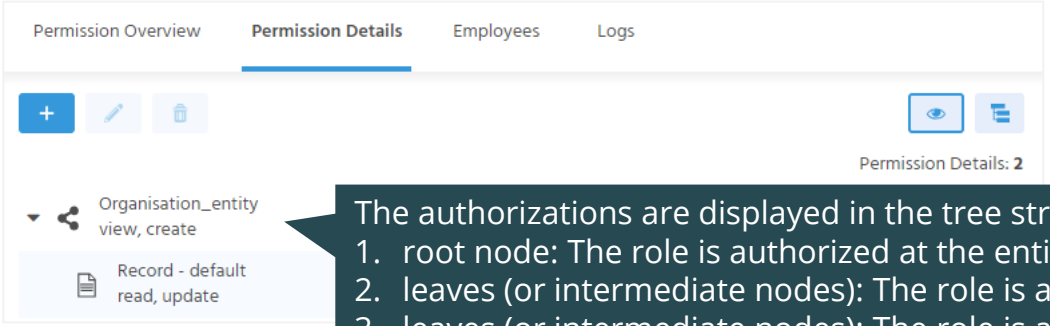

Child roles of child roles are not shown in the overview. This view only shows the direct connections of roles from the next level.

# Context "Roles"

## Tab "Permission Details"

The tab enables the **creation/editing** and the **detailed overview** of rights

- You can assign all rights at once by activating the “Complete Authorizations” checkbox.
- Or you can authorize step by step, first at the entity level, then at the data record level (possibly with filter conditions) and, if necessary, at individual fields or actions.



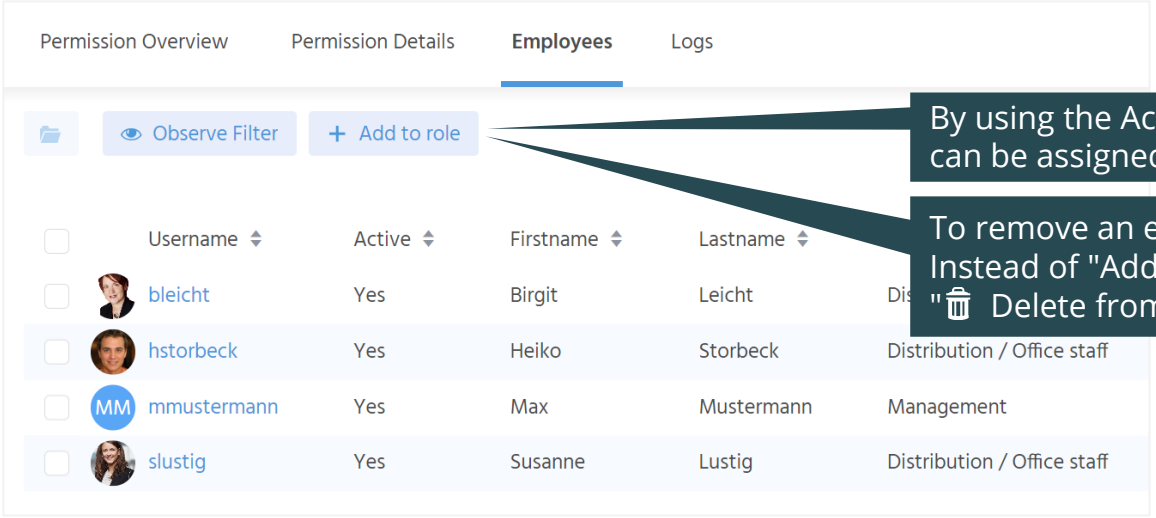

The authorizations are displayed in the tree structure:
1. root node: The role is authorized at the entity level.
2. leaves (or intermediate nodes): The role is authorized at the data record level.
3. leaves (or intermediate nodes): The role is authorized at the individual field or action level.

Further examples for the configuration of rights in the tab "Permission details"
From the perspective of the Context "Permission" can be found on the next pages.

# Context "Roles"

## Tab "Employees"

In this tab, all employees, who were assigned this role, are listed.

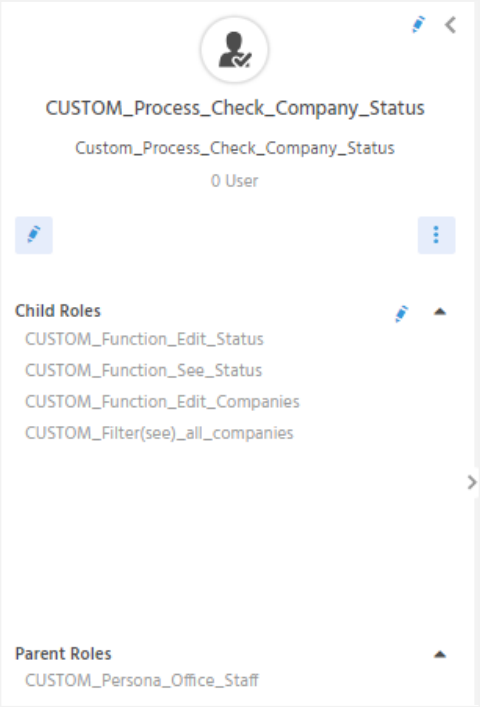



By using the Action "Add to role", an employee can be assigned to this role in this specific tab.

To remove an employee of a role, select the employee. Instead of "Add to role", there is now the Action "Delete from role" available.

# Context "Roles"

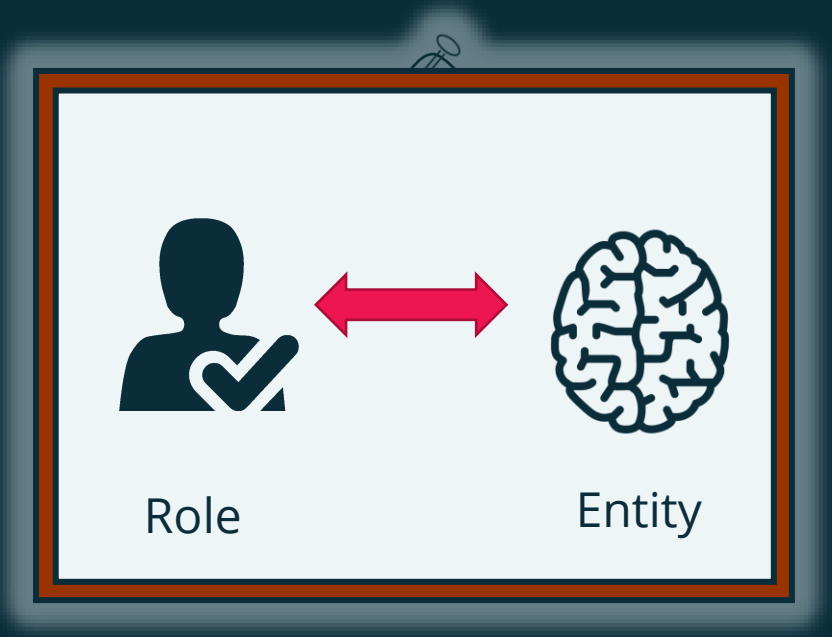
## Preview




Here you can view:

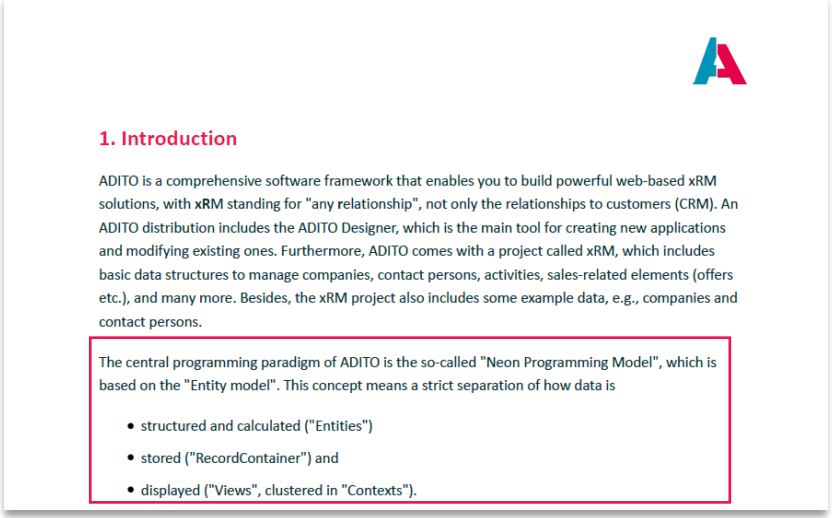
- Name of the role
- Title of the role
- Number of users, who are assigned to it
- Description (if available)
- Overview of subordinate child roles
- Overview of parental roles

# "Permission"



# What is permitted/authorized?

## Entitys, Fields, Actions are authorized.



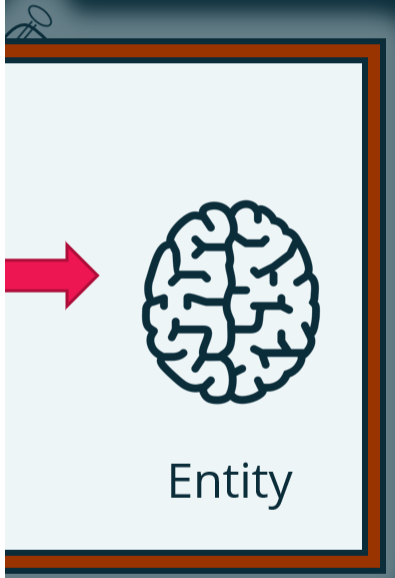
### 1. Introduction

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").

Excerpt from the Customizing Manual




The permission of an Entity controls if a role can view the Context in the Global Menu and which Data, Fields and Actions they can view and edit.

# Permission

## Activate

In the intitial condition of ADITO xRM, **no permissions** are granted (with the exception of Admin Permissions).

**Only when the property "usePermissions" is activated, all permissions are withdrawn and have to be assigned to the required roles.**

This means, **everything – Entitys, Fields, Actions** – that is not marked with usePermissions in the Designer, is visible, modifiable and executable for every role.

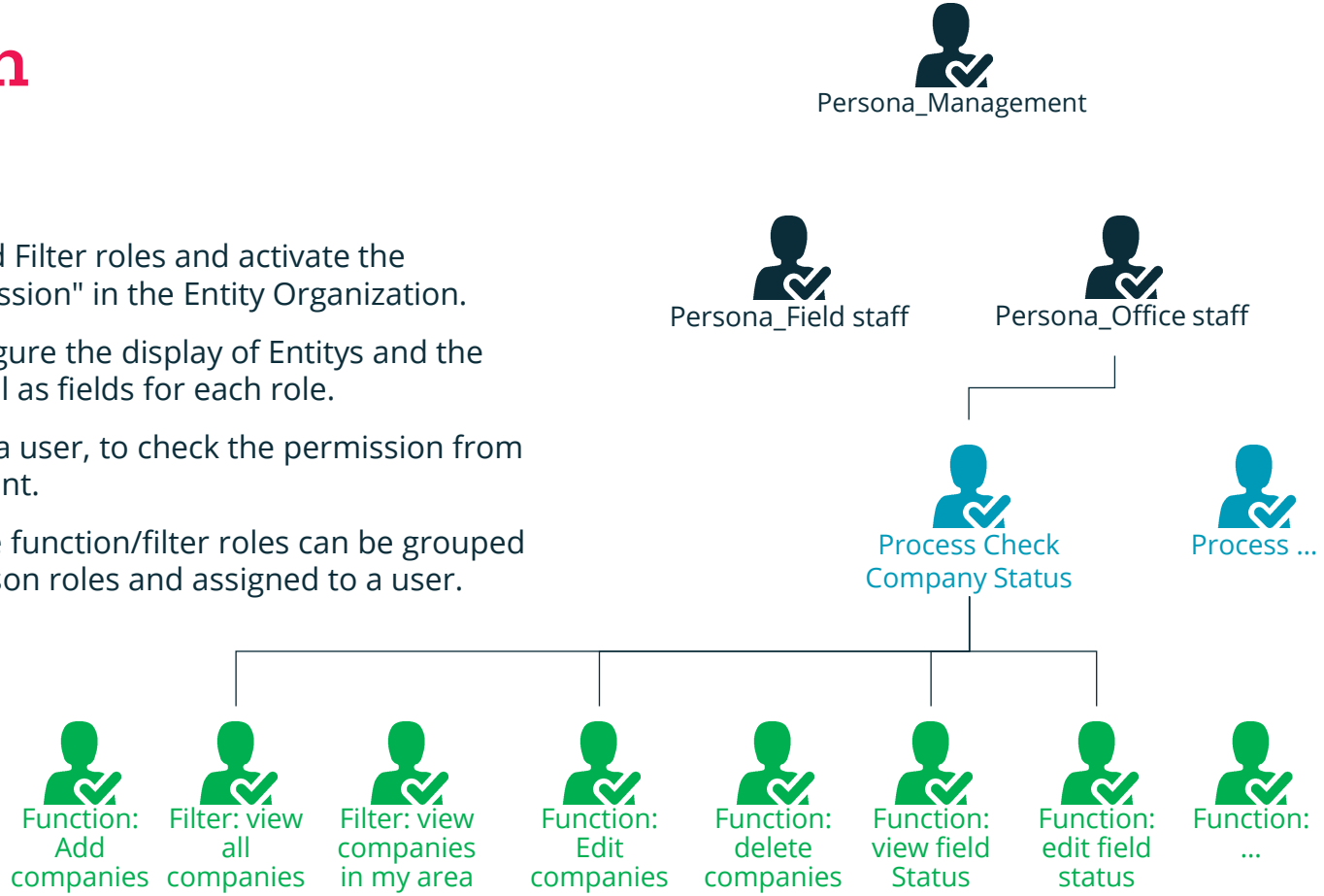
Please note that

- the activation of the property “usePermissions” is only possible in the ADITO Designer and
- the assignment of role-specific rights (role ←→ entity) only takes place in the ADITO web client.

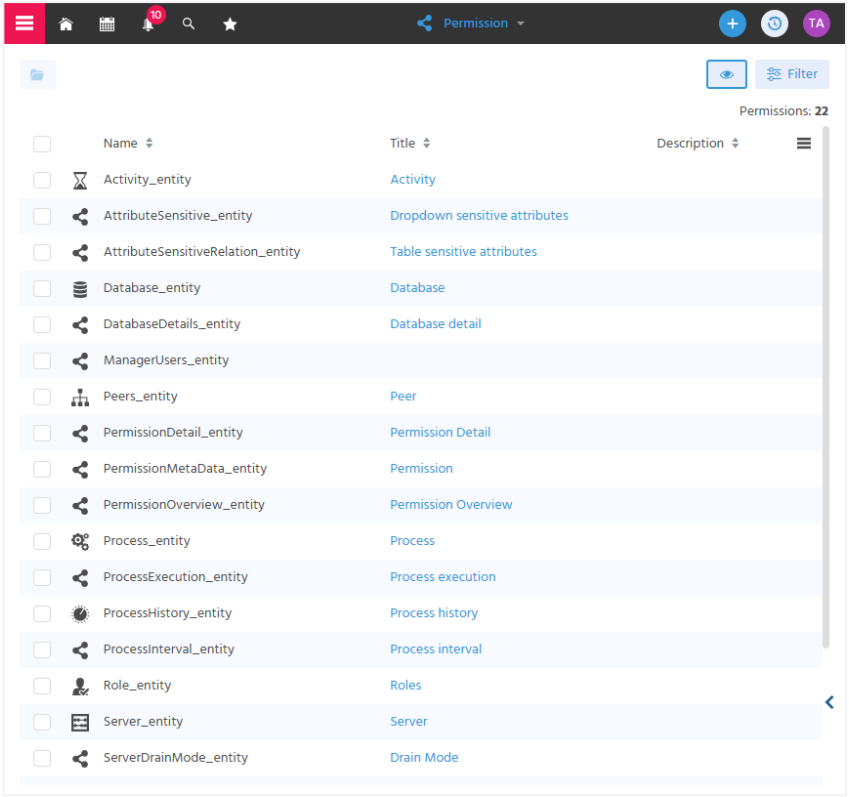
# Permission

## Example

1. Create Function and Filter roles and activate the property "usePermission" in the Entity Organization.
2. Permission to configure the display of Entitys and the data records, as well as fields for each role.
3. Assign each role to a user, to check the permission from the user view in Client.
4. In the next step, the function/filter roles can be grouped into process or person roles and assigned to a user.



# Authorizing Entitys




The Context "Permission" provides an overview of all Entitys, whose permissions were activated.

For every Entity, which is listed here, the Property "usePermission" has been activated. Only after a role has been authorized, it can view the Context and work depending on the authorization.

The "Administrator" role has been authorized in xRM for the entities shown in the screenshot (check "Special position of Adminstrator").

To display more Entitys in this list, the following steps are required in the Designer:

# Authorizing Entitys

**Possibility 1:**

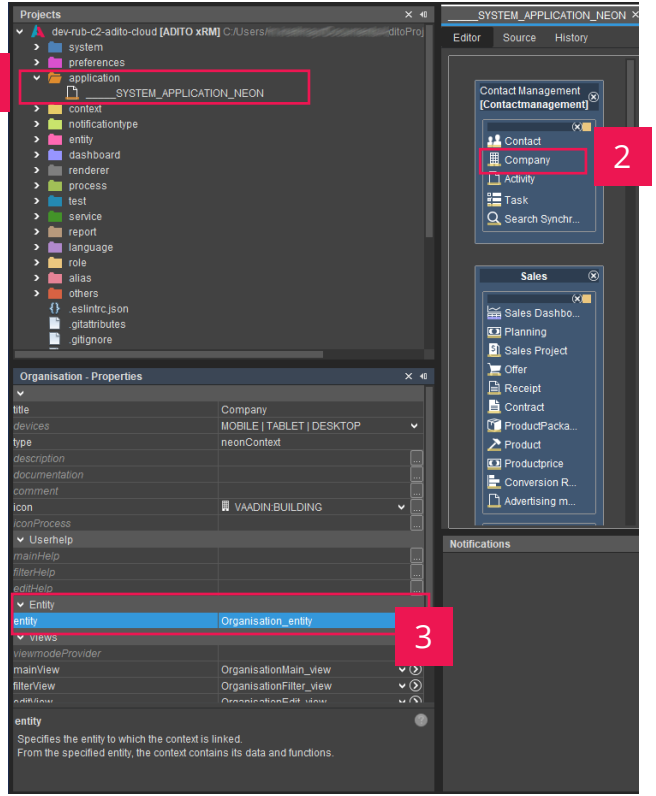
1. Access via _____SYSTEM_APPLICATION.
2. Search for Context Company
3. Open the connected Organisation_entitys
4. Open the Properties of the Entity
5. Activate usePermissions

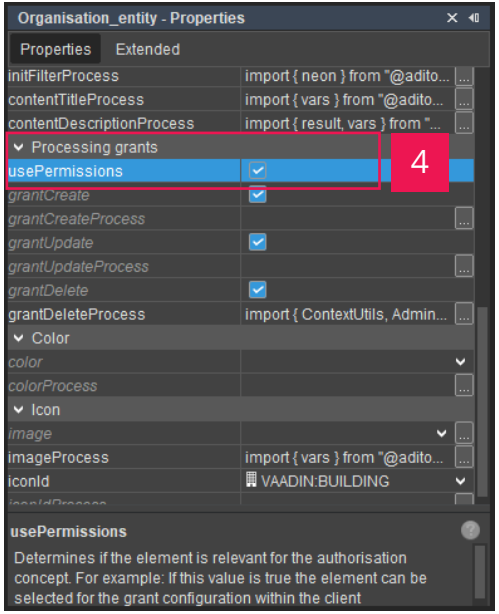
**Possibility 2:**

Access through complete selection "context" in area Projects.
(Follow steps 3. – 5.)

**Possibility 3:**

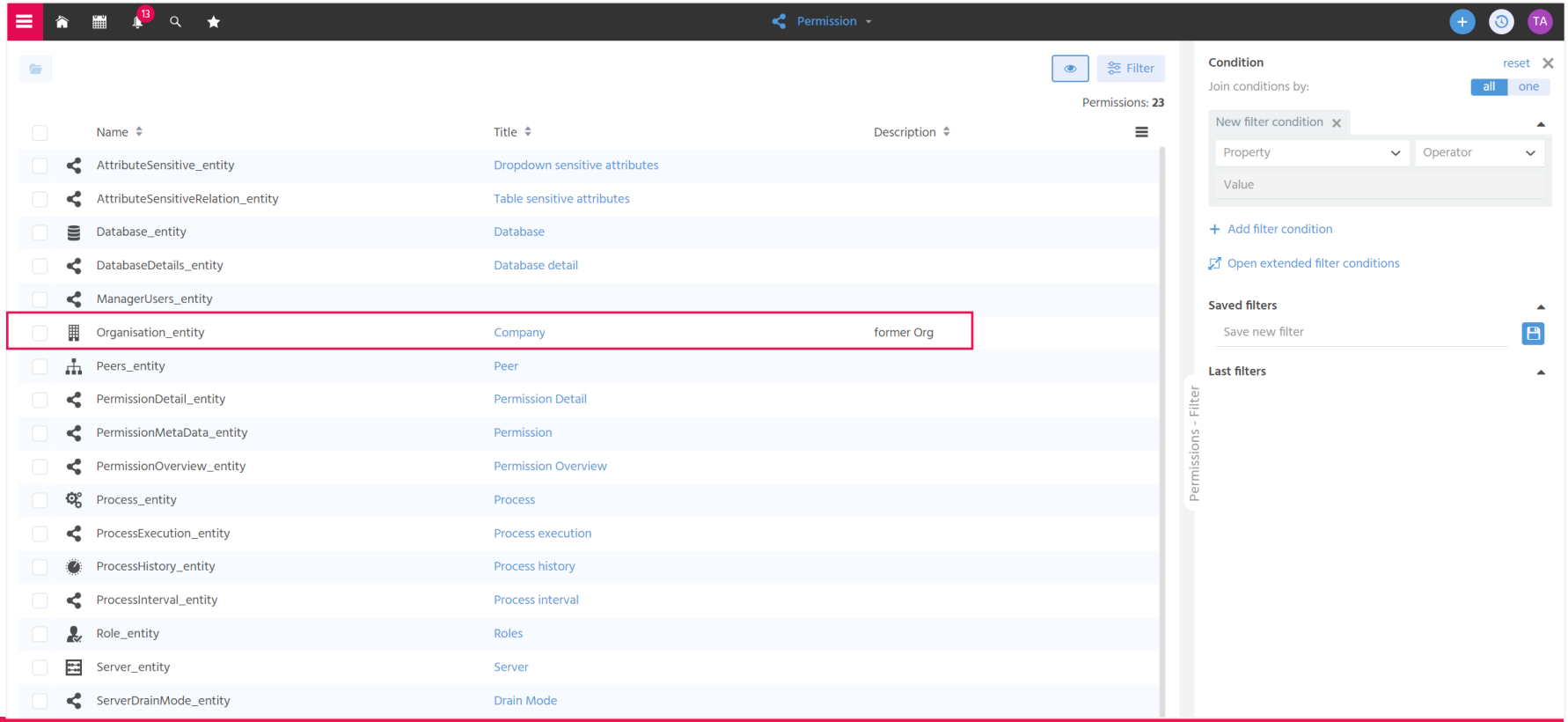
Access through complete selection "entity" in the area Projects.
(Follow steps 4. und 5.)



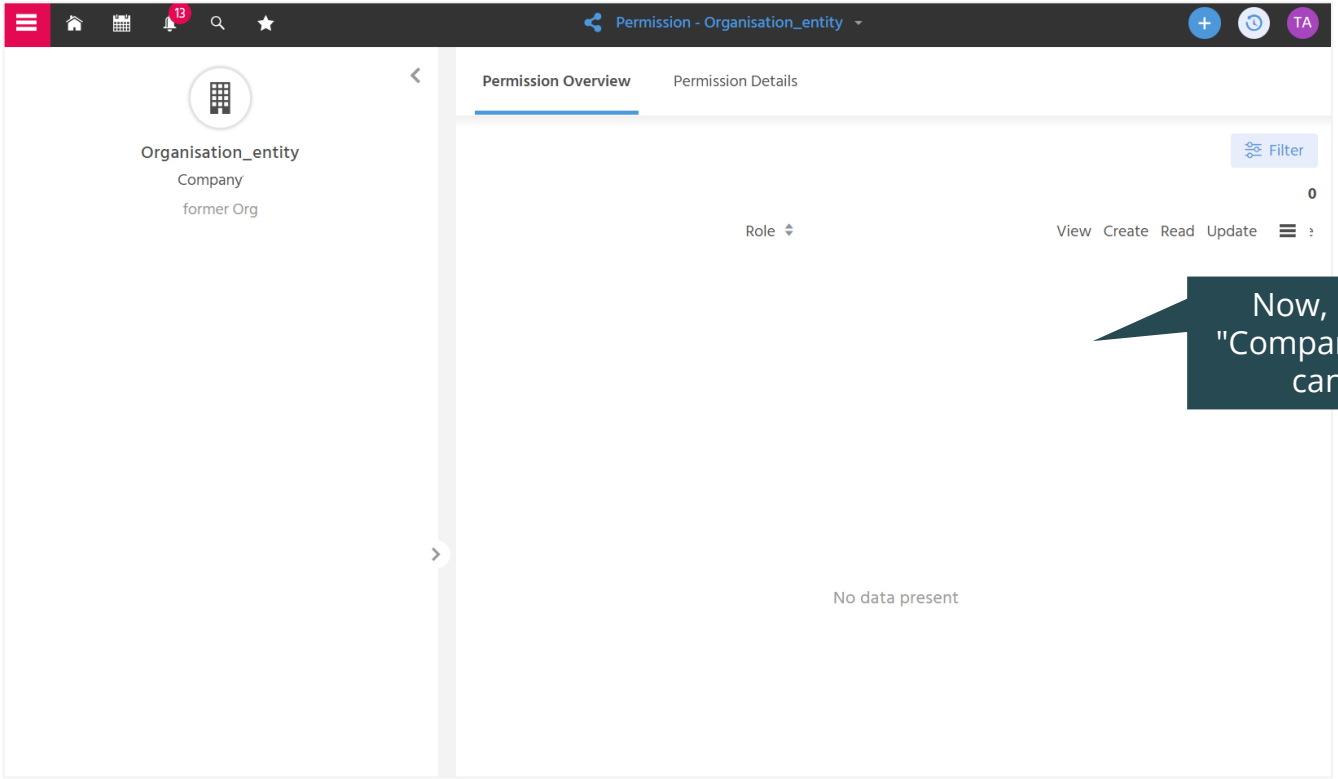




5 Deploy

# Authorizing Entitys



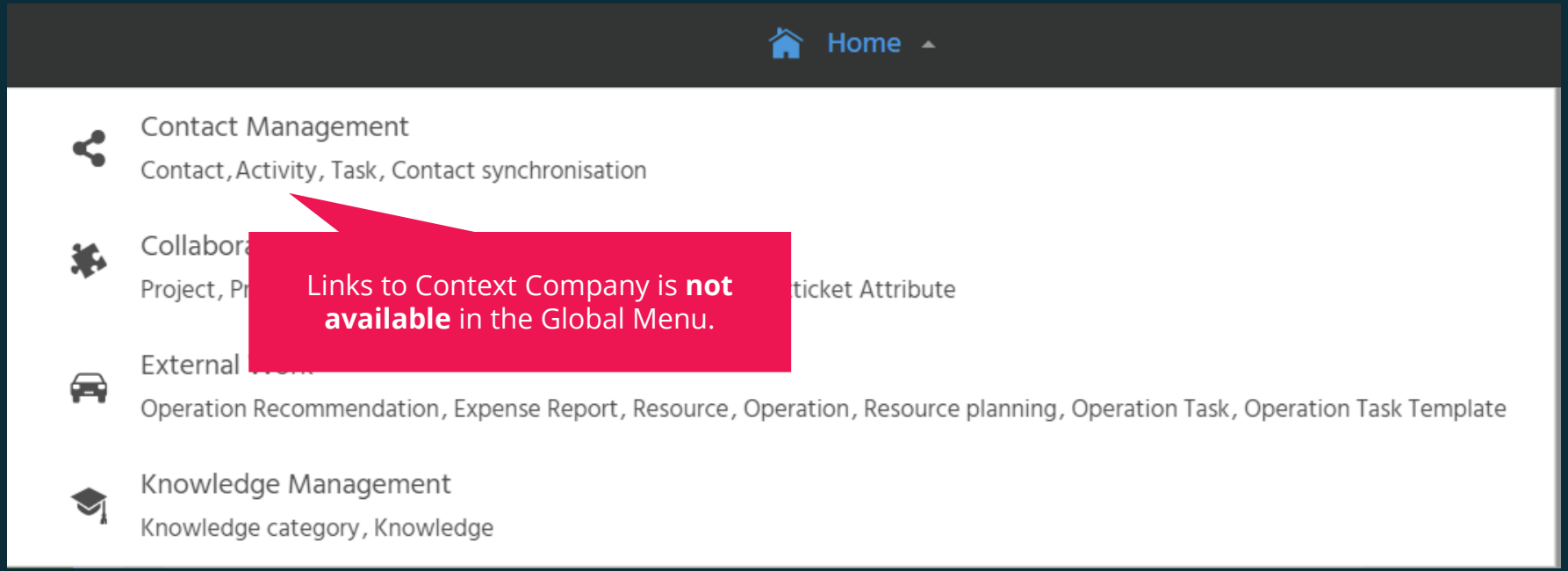
# Authorizing Entitys




Now, no role can view the Link "Company" in the Global Menu and cannot edit data records.

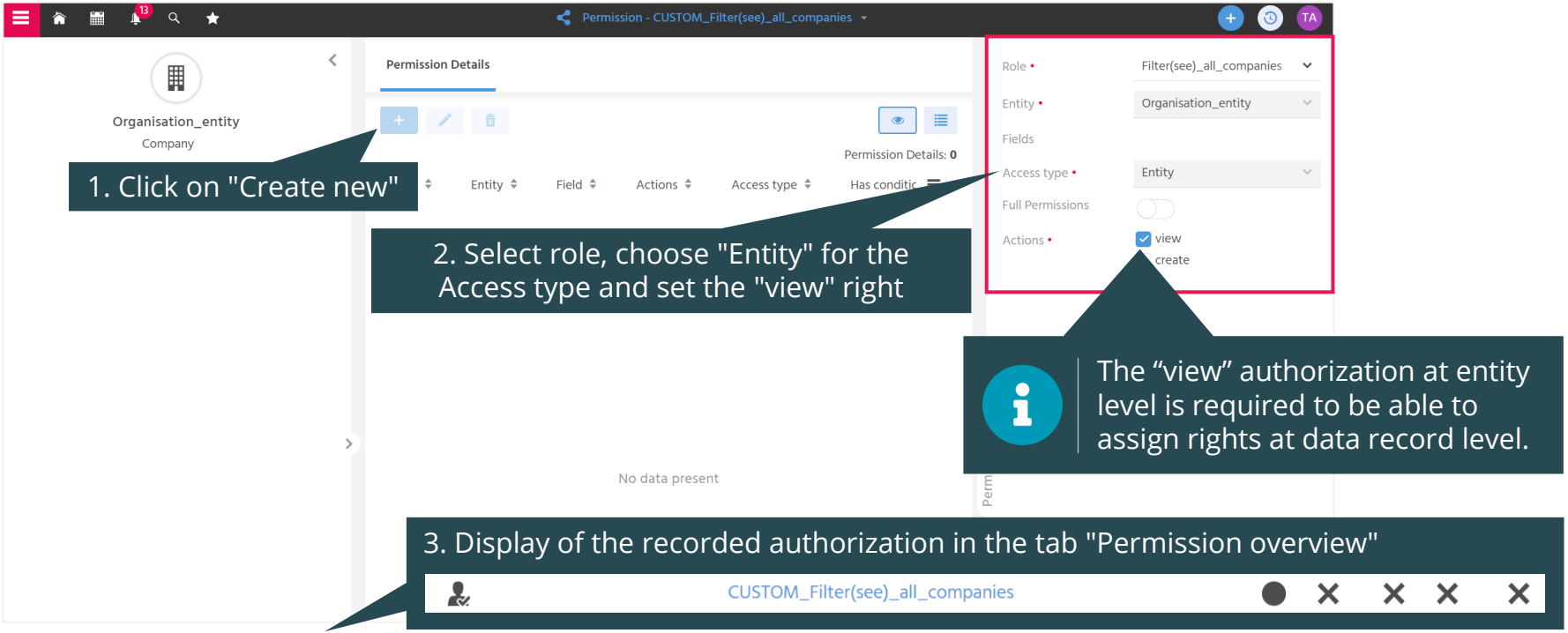
# Authorizing Entitys

View of the user



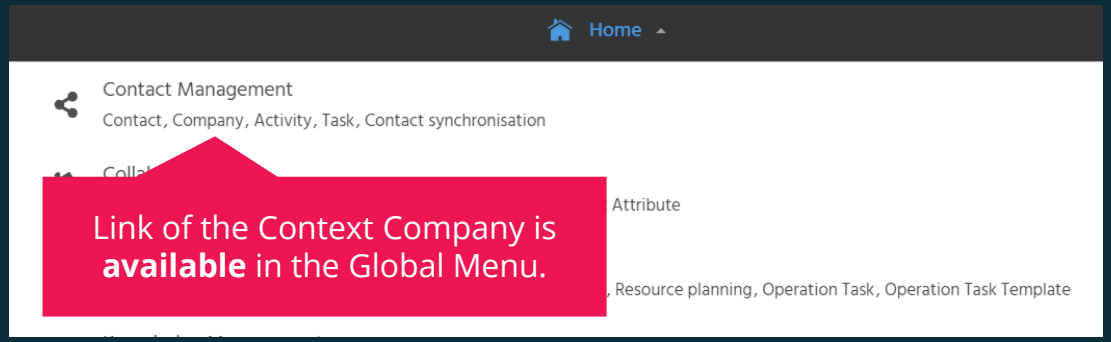
# Authorizing Entitys

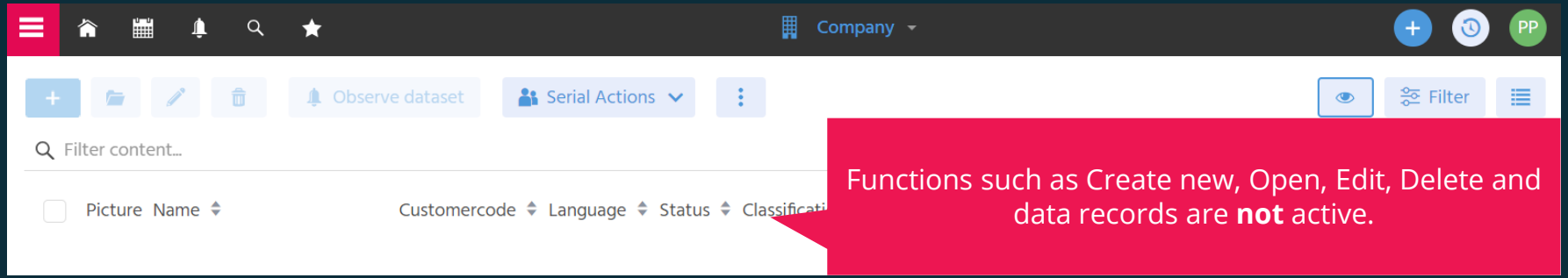
## Control the display of the links in the Global Menu: grant VIEW-authorization



# Authorizing Entitys

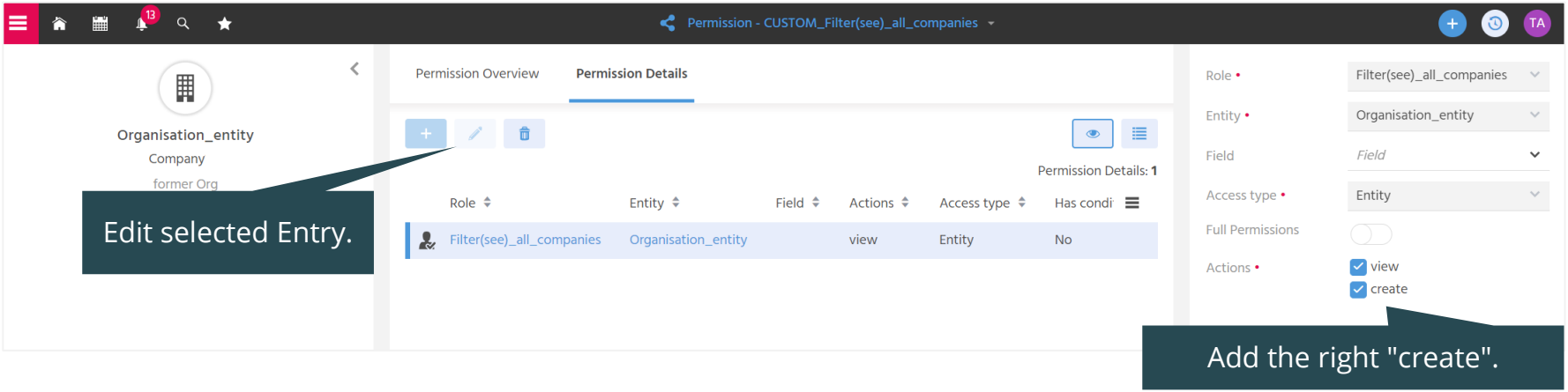
## View of the user



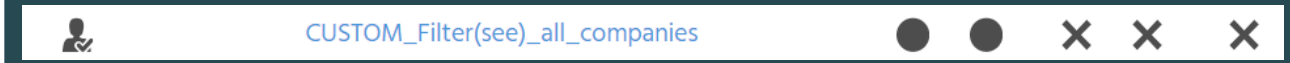



# Authorizing Entitys

## Create new data records: grant CREATE permission

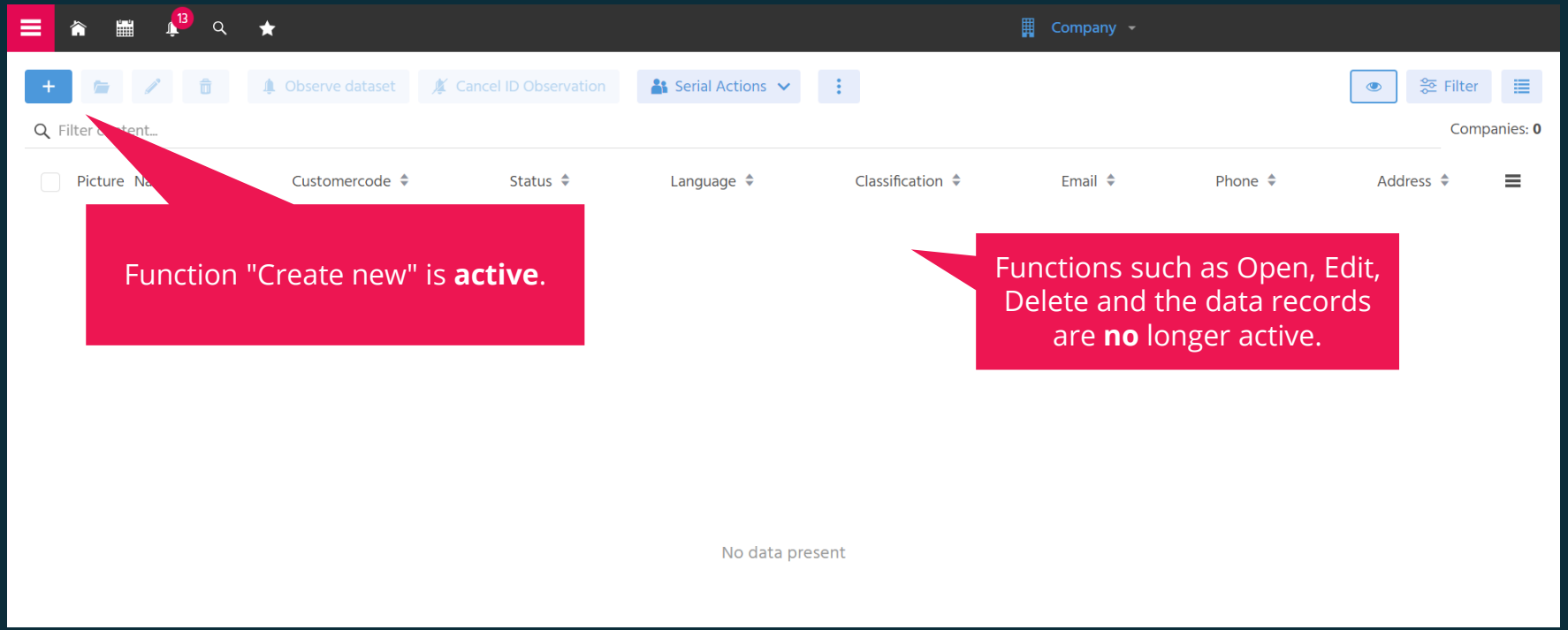



Display of recorded permissions in tab "Permission overview"



# Authorizing Entitys

## View of user

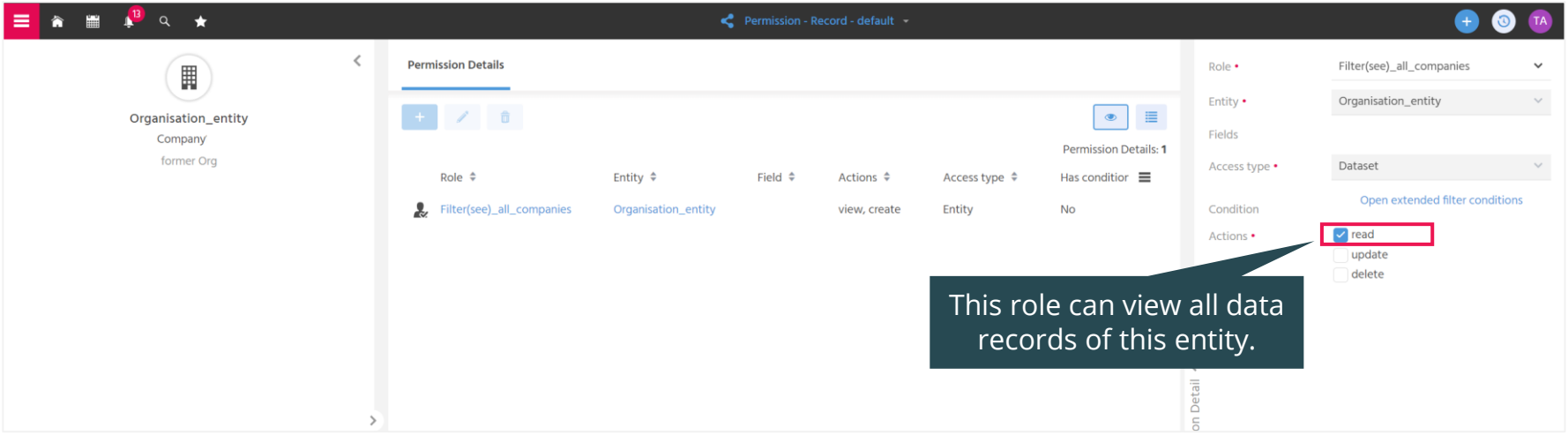


# Authorizing Entitys

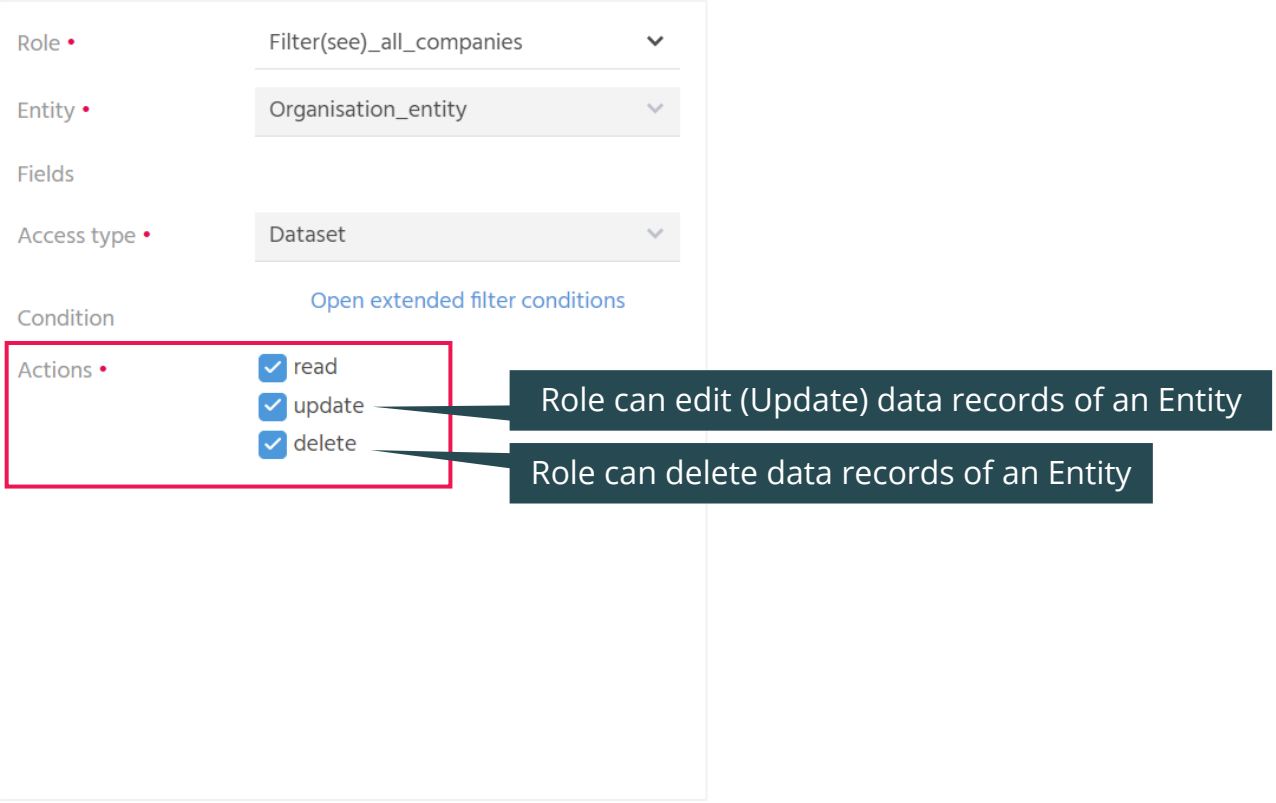
## Configurate all rights for an Entity and its data records.

The rights **Open** (**Read**), **Edit** (**Update**) or **delete (Delete)** can be assigned for the selected Entity at data record level.

These rights can, for example, be assigned to a role or individual function/filter roles.
**However, the condition is that every one of these roles has the right to VIEW at Entity level.**



# Authorizing data records



# Authorizing data records

## Configurating all rights for an Entity and its data records.


The rights READ, UPDATE and DELETE were split among three roles.

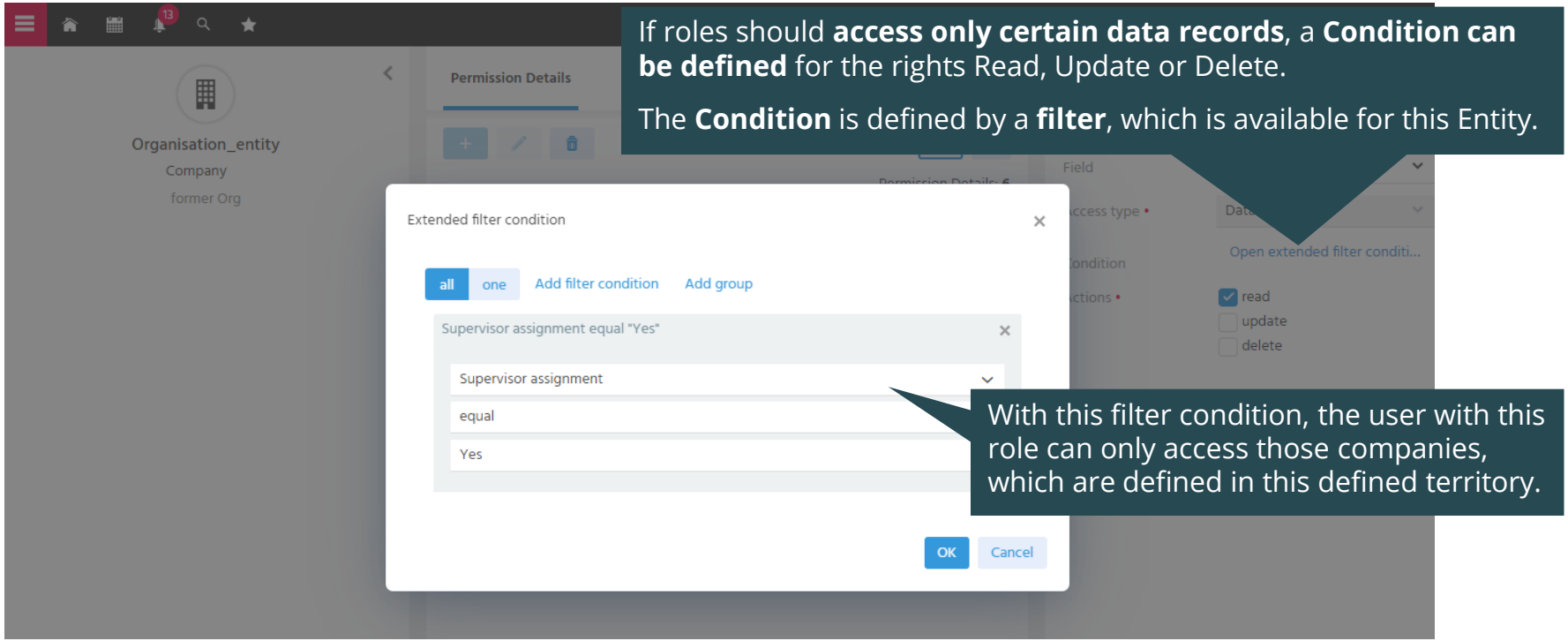
# Authorizing data records

## View of user


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

# Authorizing data records

## Authorize only certain data records



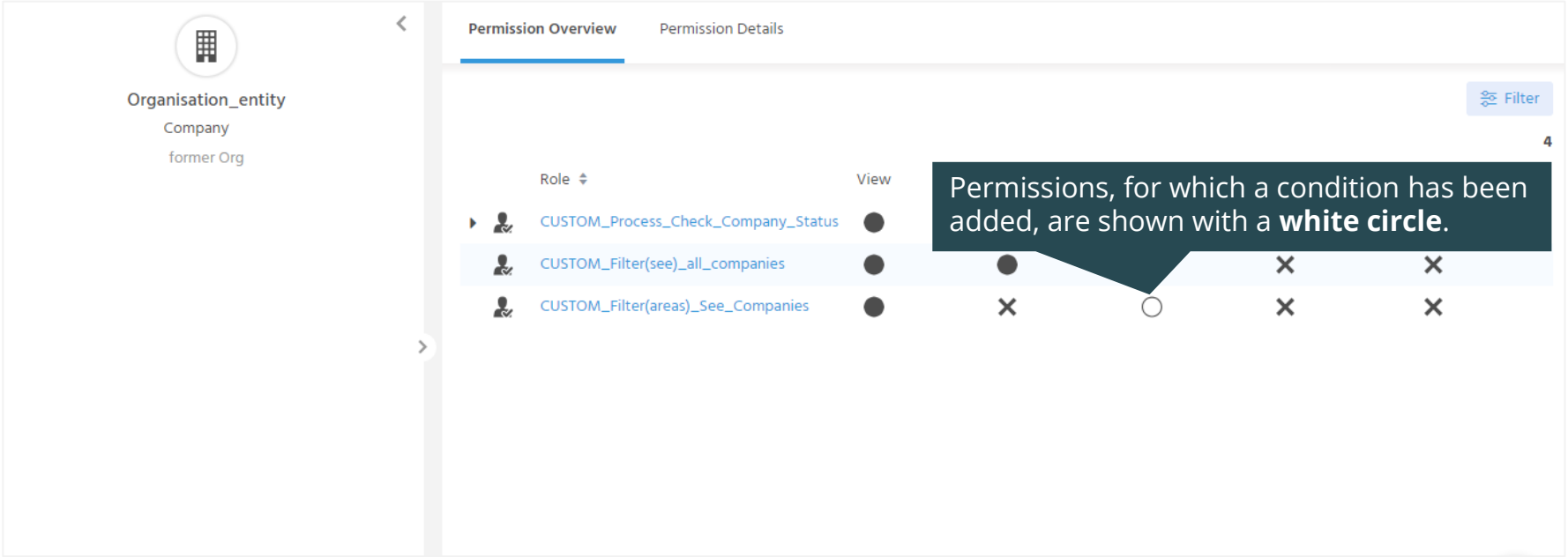

If roles should **access only certain data records**, a **Condition can be defined** for the rights Read, Update or Delete.

The **Condition** is defined by a **filter**, which is available for this Entity.

With this filter condition, the user with this role can only access those companies, which are defined in this defined territory.

# Authorizing data records

## Authorize only certain data records

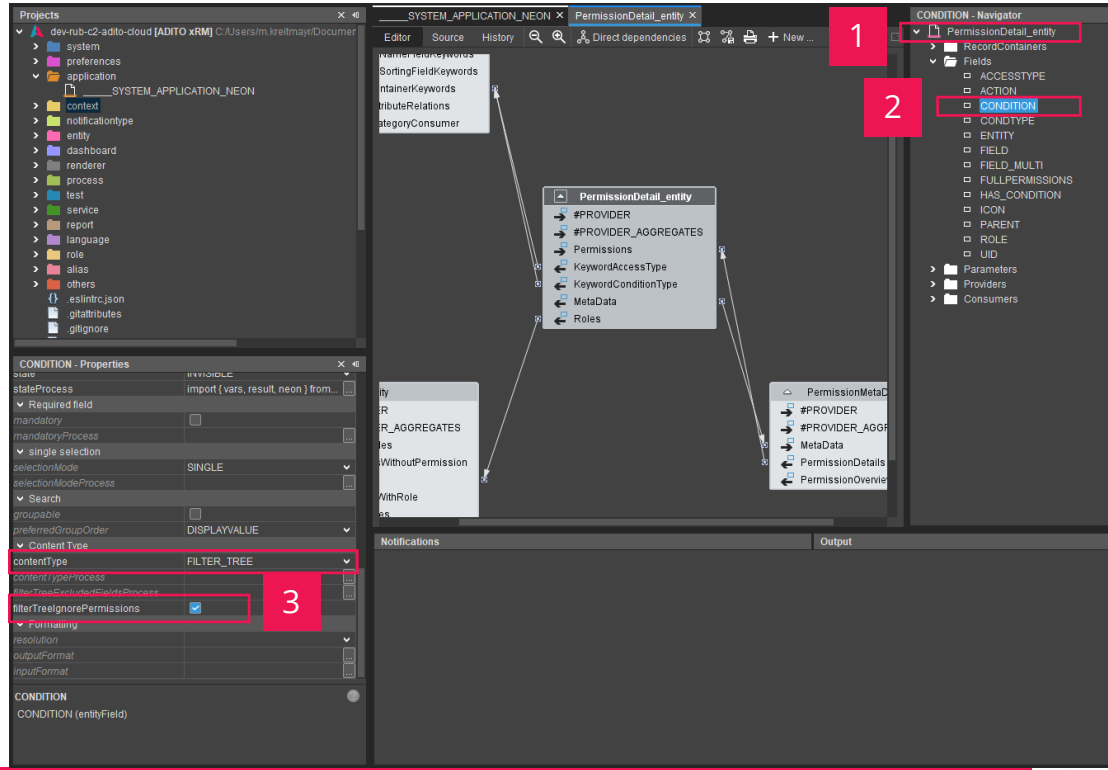


# Condition

## Display of filter properties

To be able to access the filter for recording the condition, without the administrator having rights to the entity, the property "filterTreeIgnorePermission" must be activated for the field "Condition" in the Entity "PermissionDetail".

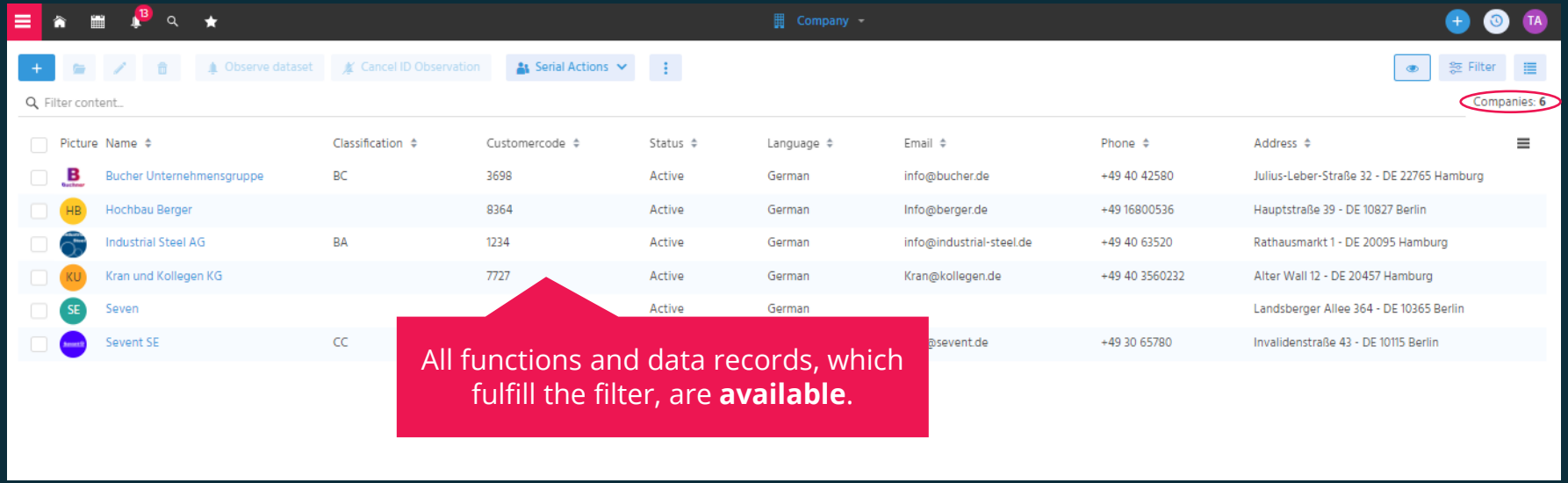
If this checkbox is ticked, the permission (VIEW permission on the respective entity) is ignored when the filter tree component is opened.




This setting is deactivated by default.

# Authorizing data records

## View of user



# Authorizing fields

**Possibility 1:**

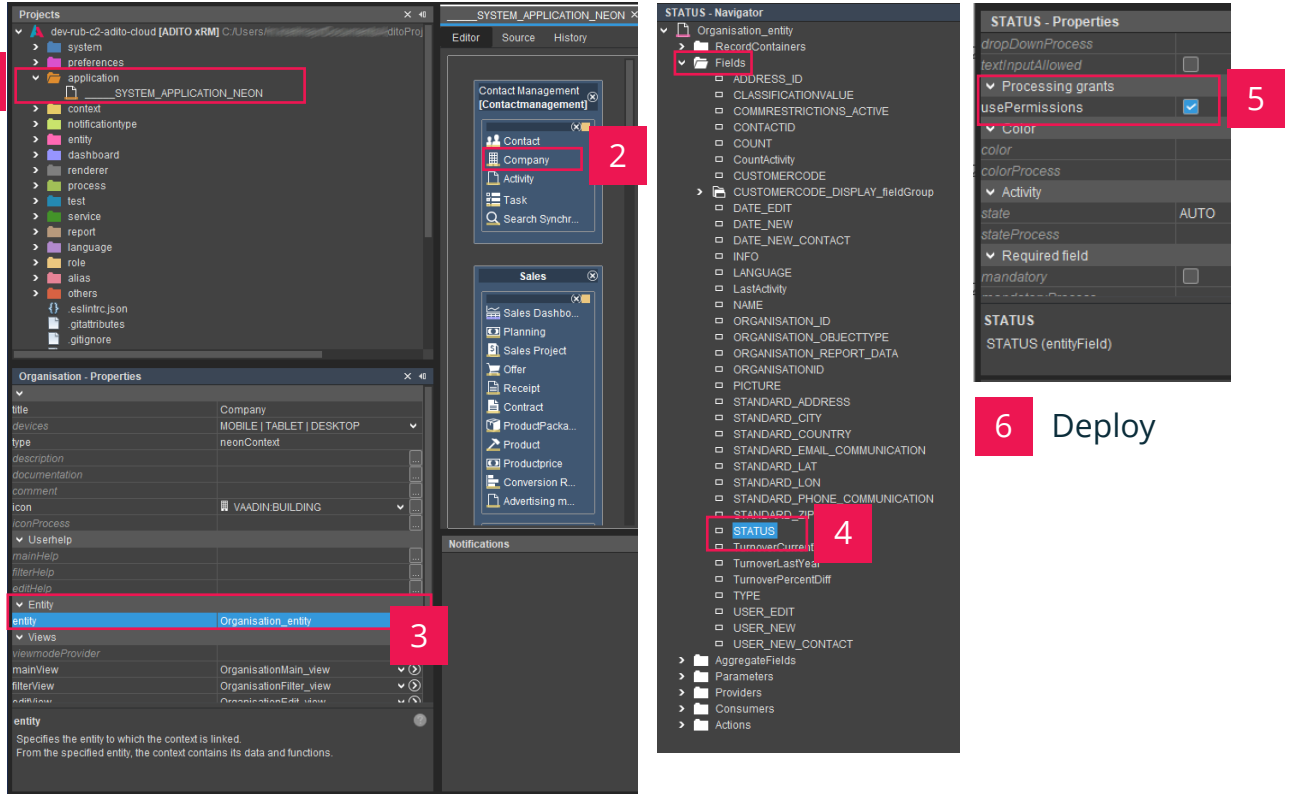
1. Access through the SYSTEM_APPLICATION.
2. Search the Context Company
3. Open the associated Organisation_entitys
4. Open properties of this field
5. Activate usePermissions

**Possibility 2:**

Access through complete selection "context" in Projects.
(Follow steps 3. – 5.)

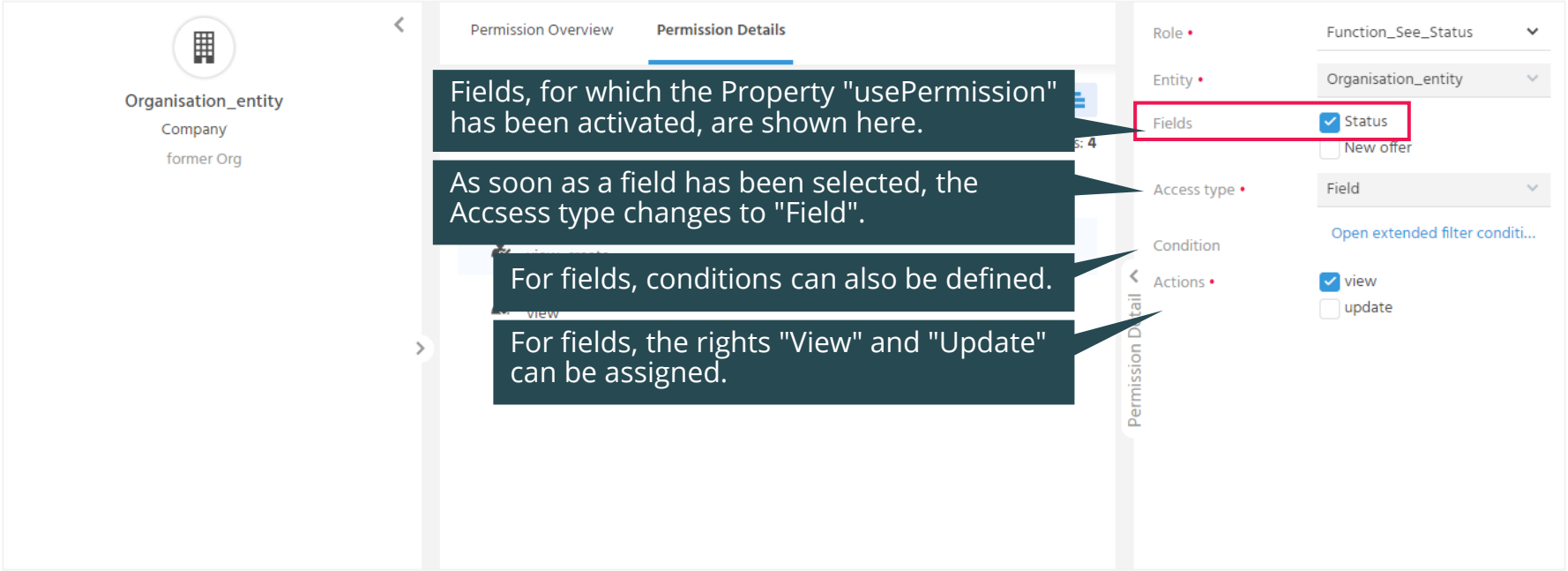
**Possibility 3:**

Access through complete selection "entity" in Projects.
(Follow steps 4. und 5.)

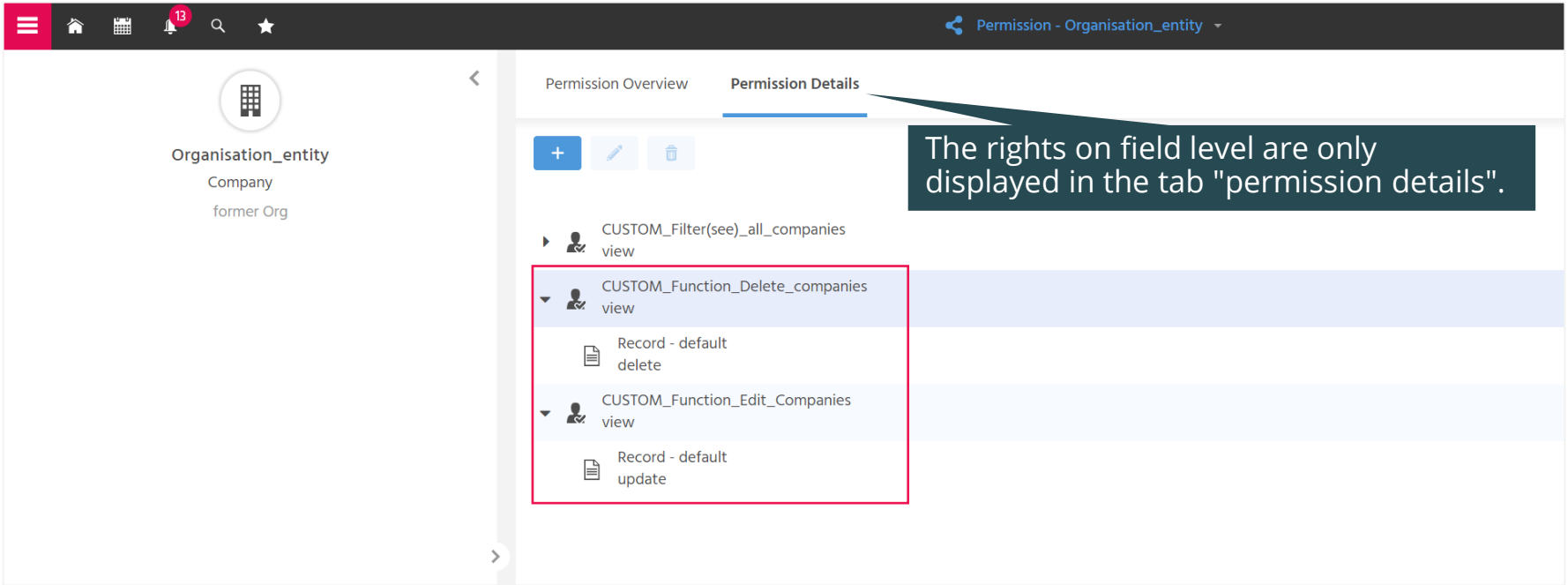


# Authorizing fields

## Show fields

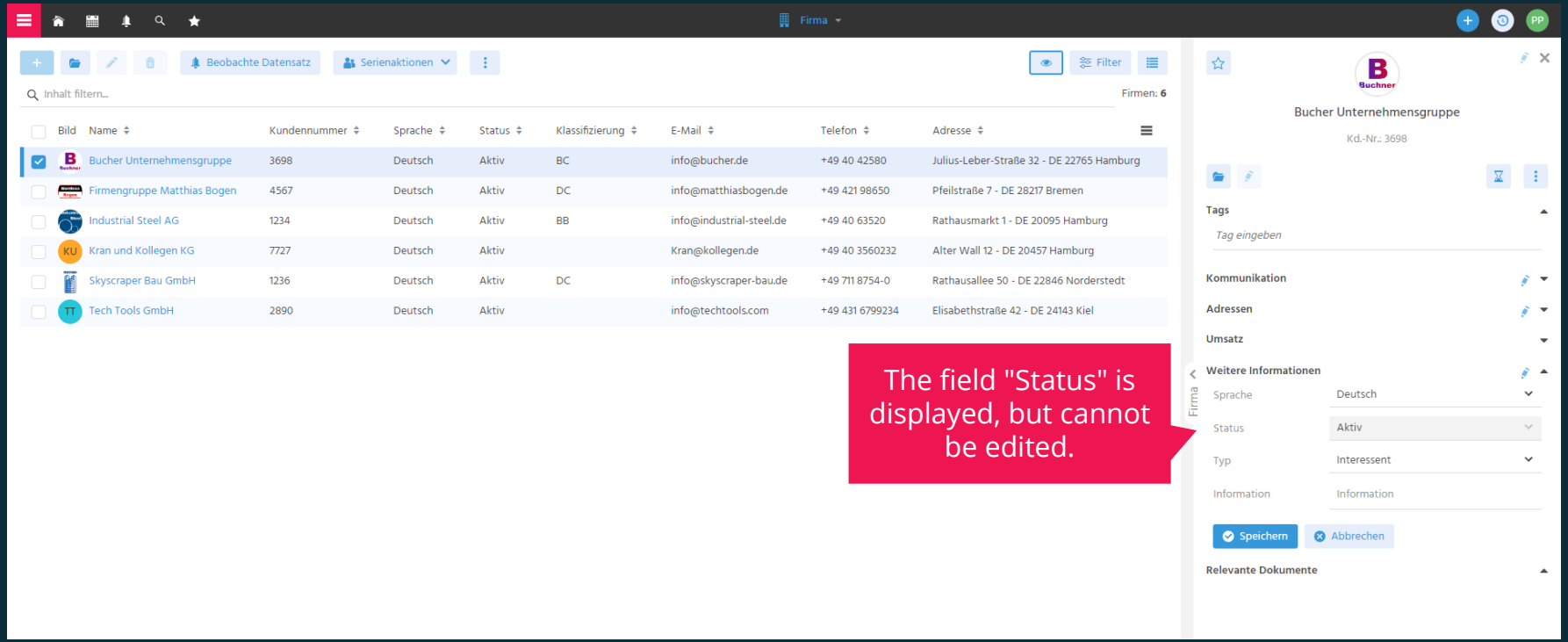


# Authorizing fields



# Authorizing fields

## View of the user with the role "Function_View_Company_Status"



# Authorizing Actions

**Possibility 1:**

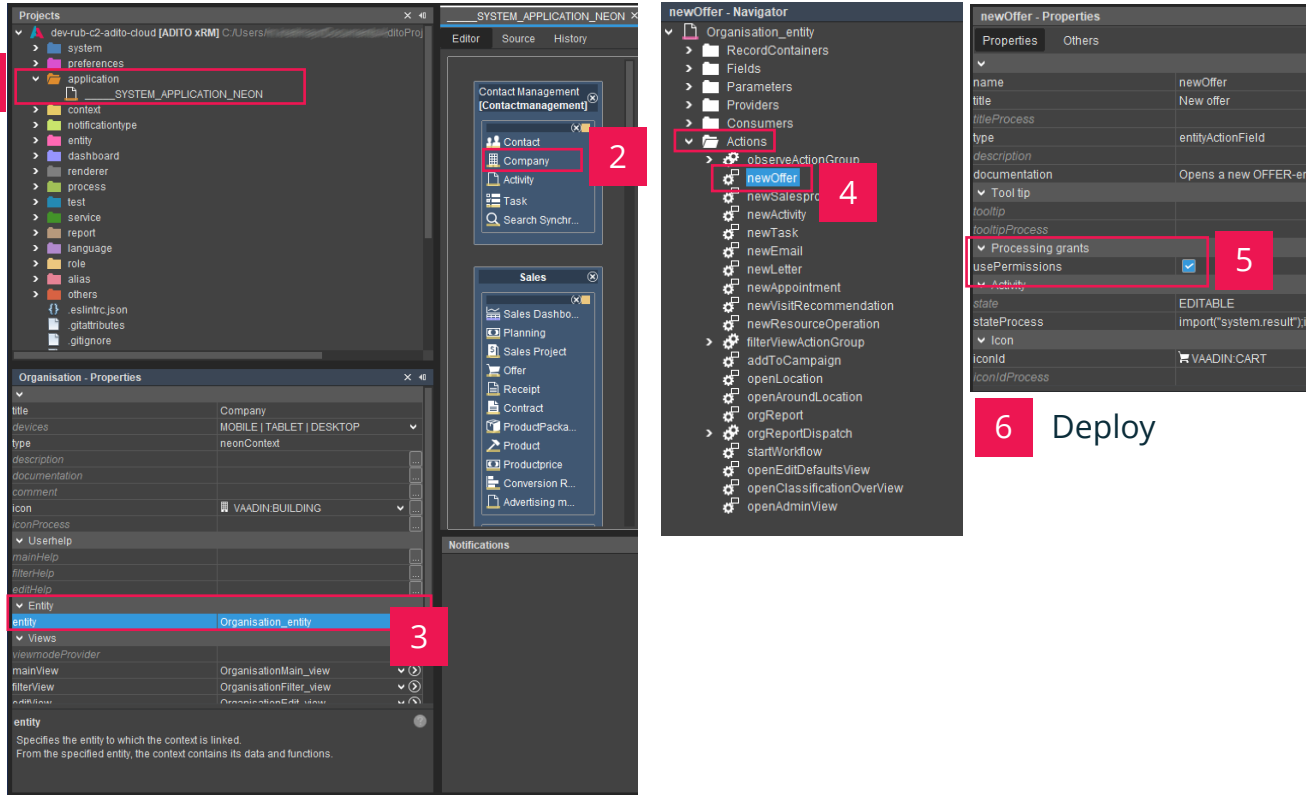
1. Access through the SYSTEM_APPLICATION.
2. Search the Context Company
3. Open the associated Organisation_entitys
4. Öffnen der Properties der Aktion
5. Aktivieren von usePermissions

**Possibility 2:**

Access through the complete selection "context" in Projects.
(Follow steps 3. – 5.)

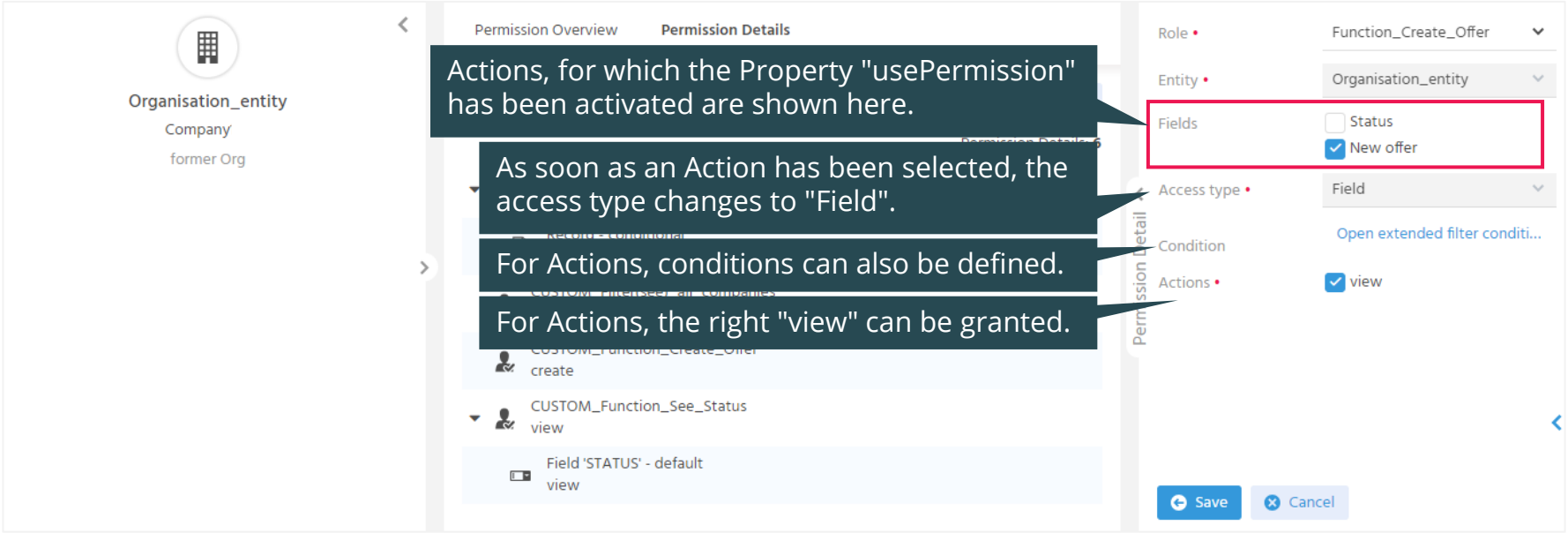
**Possibility 3:**

Access through the complete selection "entitys" in Projects
(Follow steps 4. und 5.)

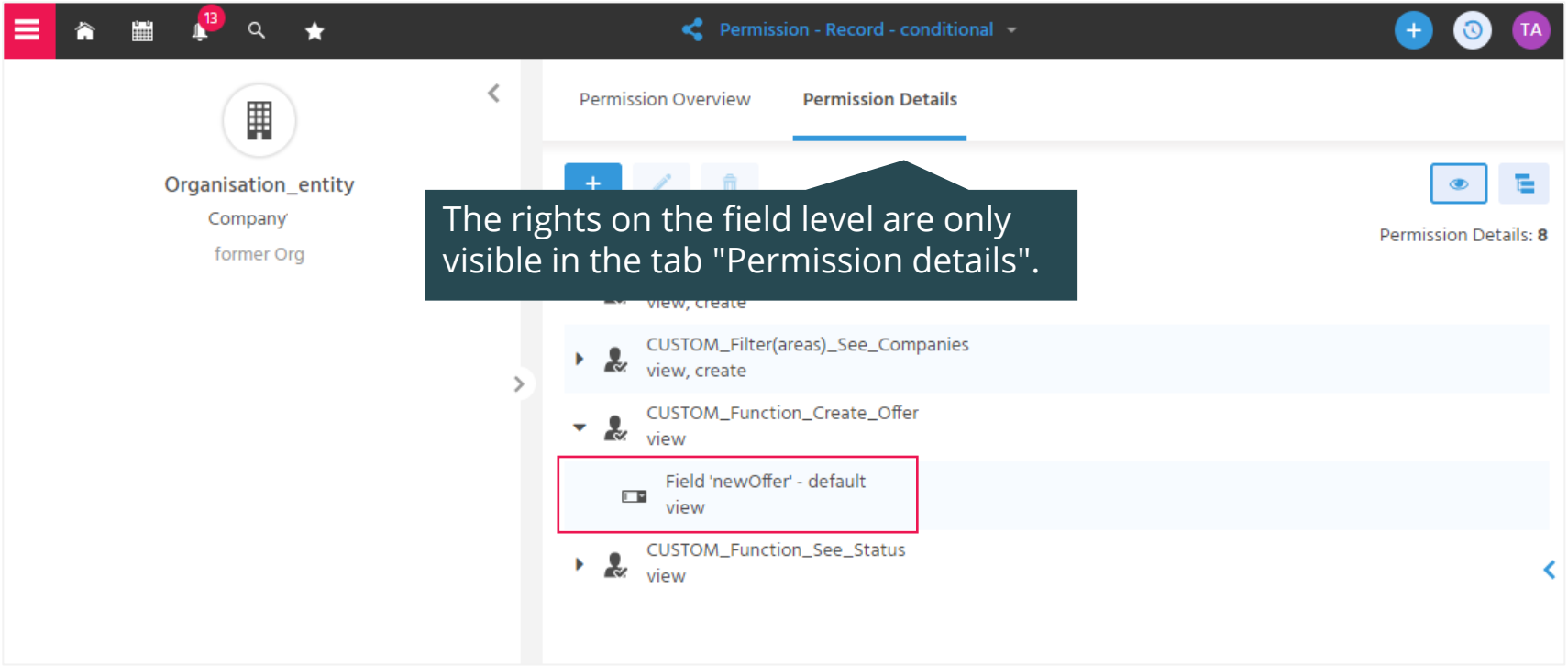


# Authorizing Actions

## VIEW permission

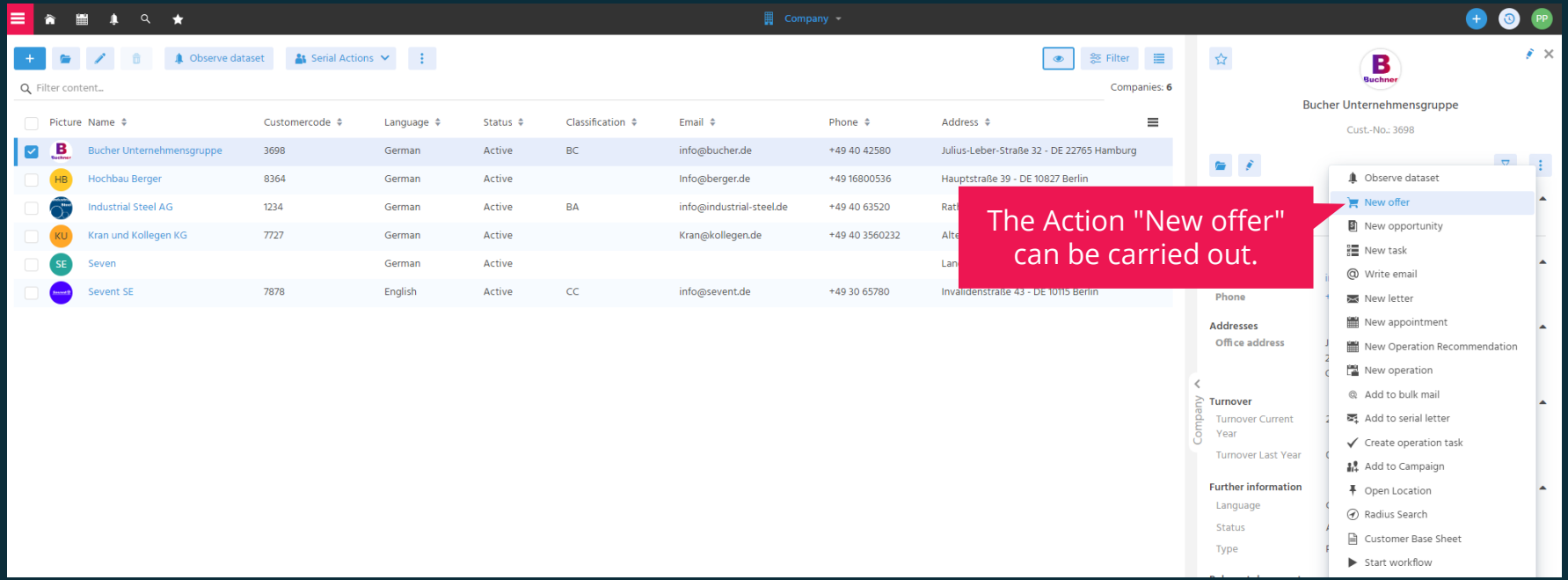


# Authorizing Actions



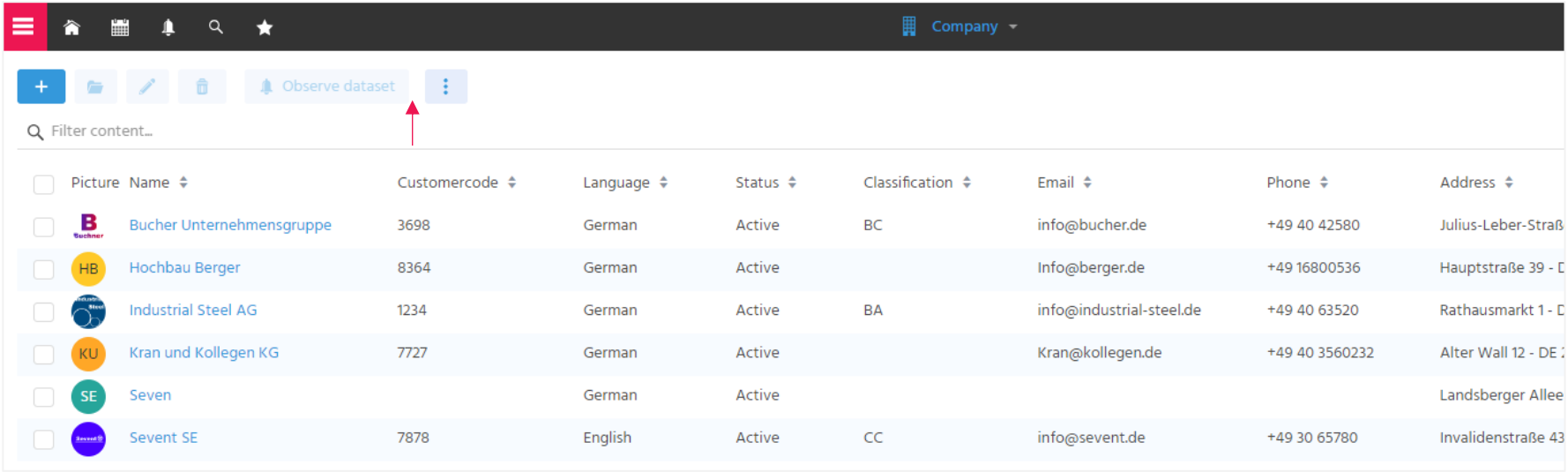
# Authorizing Actions

## View of user

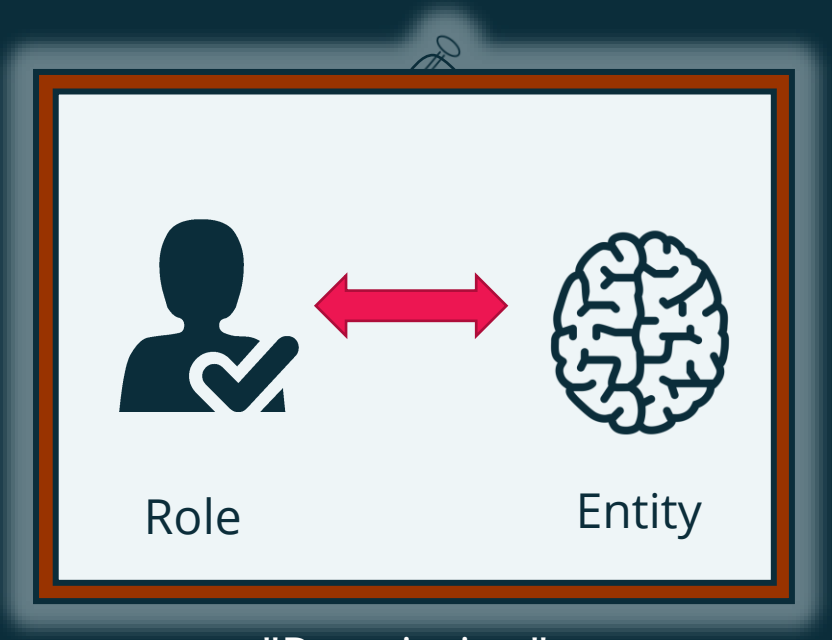


# Button "Serial actions"

If the Property "usePermission" is active on all Actions, which are subordinate to a Serial action and a user is not assigned a role that authorizes one of the actions, the button "Serial Actions" is hidden.



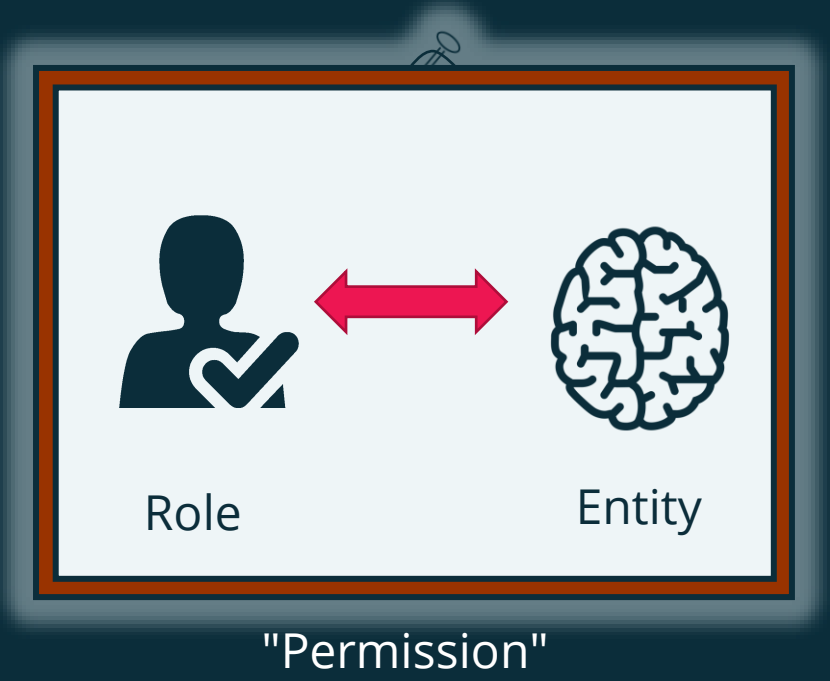
# "Two directions of view"




"Permission"

# "Two directions of view"

From the Entity‘s perspective: "Which roles am I entitled to?"

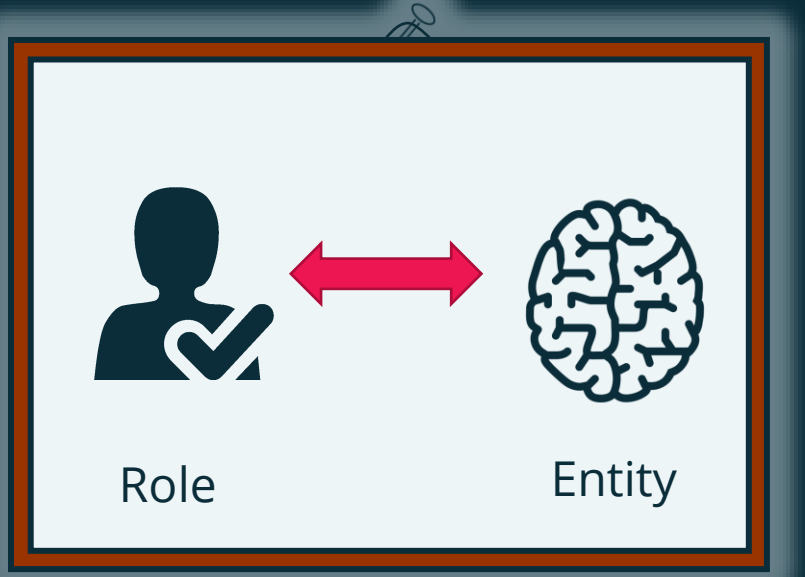



Context
"Permission"

# "Two directions of view"

From the role‘s perspective: "Which Entitys am I entitled to?"

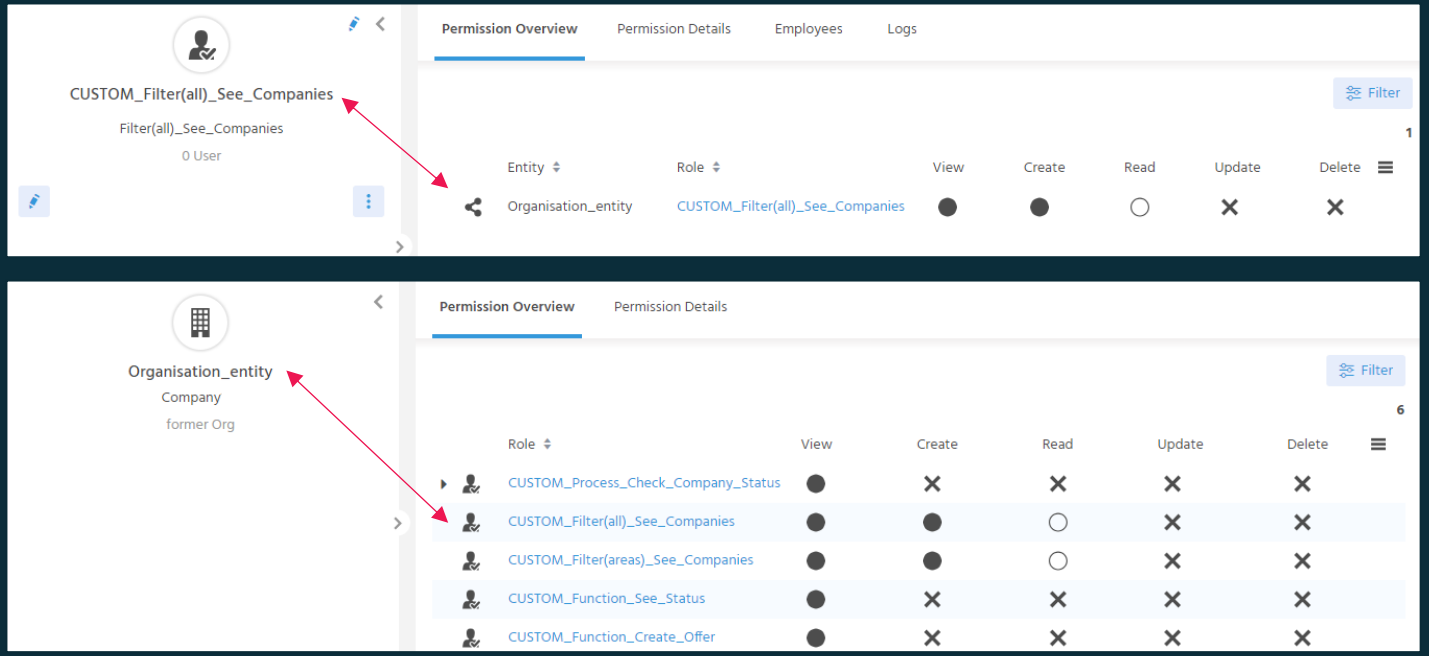
Context
"Role"




"Permission"

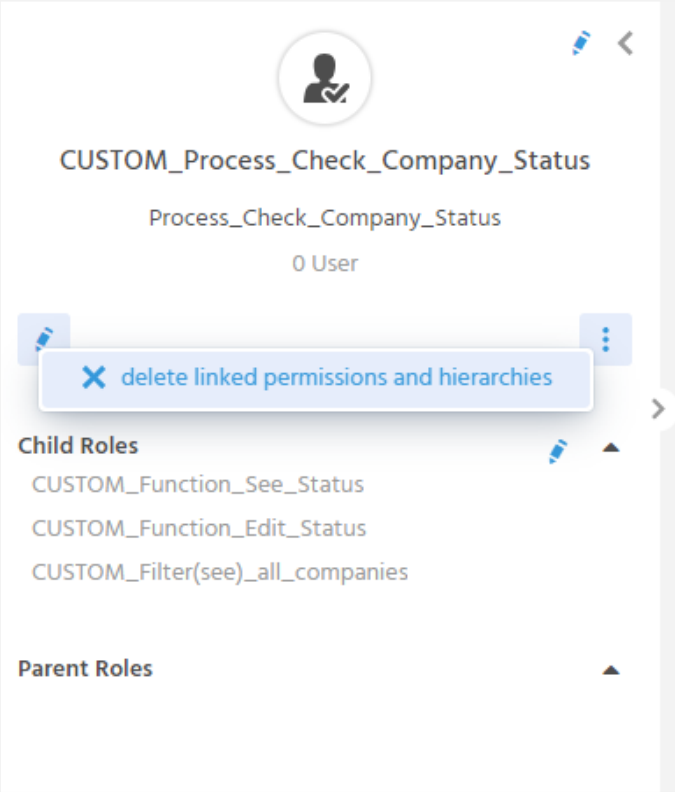
# "Two directions of view"

Context "Role"




Context "Permission"

# Delete roles

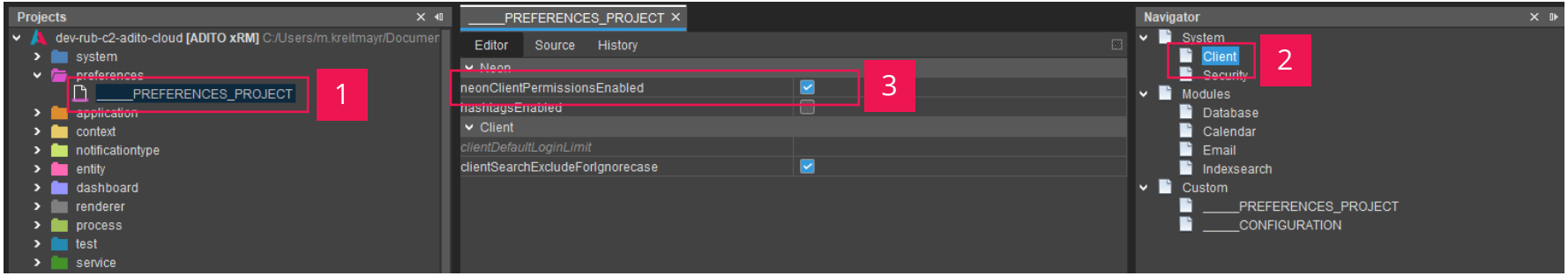



You can delete CUSTOM roles in the client if they are not linked to authorizations or are not used in hierarchies (role groups).

Procedure for deleting a role:

1. Execute Action "delete linked permissions and hierarchies"
2. Select role in FilterView or open the preview and execute Action "Delete"

# Deactivating permissions




4 Deploy

5 Restart server


ADITO®
Einzigartige Beziehungen