Manual User Rights
Compano Online Software

Version 4.1

File	COS_Manual_User_Rights.docx
Date	23/05/2024

Content

1 Introduction

This manual describes how to manage User Rights in Compano Online Software, version L03. User rights determine which activities a user may perform within the Compano application.

User rights in COS are set on the User Group level, with users added to groups inheriting the group rights. To further ease management of users and groups, **Active Directory Provisioning**[1] has been implemented. This way users and groups can be synced with the clients Active Directory.

*The main user of the application (Admin, Beheerder) always has **all rights***

1.1 Concepts

COS
Compano Online Software.

User
A user has access to the Compano application with a user account, which includes a login name, password, license type and user interface access rights.

User group
A user group contains one or more users. Access rights to the COS user interface are handled at the group level; any users in the group will inherit the access rights of the group.

User rights
A 'user' rights reflects the type of access a user has to view, edit (including import) or export information in COS.

Single Sign-on
Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. True single sign-on allows the user to log in once and access services, including COS, without re-entering authentication credentials.

Azure Active Directory (Azure AD)
Azure Active Directory is Microsoft's enterprise cloud-based identity and access management (IAM) solution. Azure AD is the backbone of the Office 365 system, and it can sync with on-premise Active Directory and provide authentication to other cloud-based systems via OAuth.

Provisioning
Provisioning is the processes of creating an identity in a target system based on certain conditions. *De-provisioning* is the process of removing the identity from the target system when conditions are no longer met. *Synchronization* is the process of keeping the provisioned object, up to date, so that the source object and target object are similar. Azure can provide all three mentioned services.

---

[1] For further details, see the Technical Documentation Azure Authentication And Provisioning.

2 Manage user rights

In COS, user rights are **always** managed through **Group rights** and are **never** set or changed for individual users. *Detailed View, Edit* and *Export* rights can be set for each user group. These rights can be set for:

- **Overviews**: Overview of data of a single entity
- **Functions**: Functions which will effect data in Compano
- **Field groups**: Certain fields groups, e.g. that only certain users are allowed to see that you still get a 2% bonus; or that they are not allowed to see the purchase price.

Users and user rights in Compano are managed through the following procedure:

1. **Add user group(s)**, either manually or through AD provisioning
2. **Add user(s)**, either manually or through AD provisioning
3. **Assign user(s)** to group(s), either manually or through AD provisioning
4. **Set group rights**, per user group

2.1 Add user groups

Important: To set User Rights, even for a single user, a **User Group** needs to be created first.

To add a User Group:

1. Through the Menu, go to *System > User Groups*:

2. Under Edit, click on *+Add*:

4
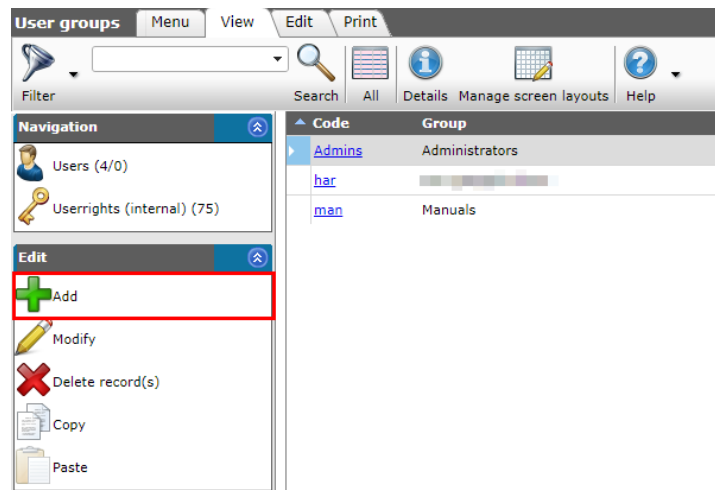
3. In the pop-up window:

    a. **Group name**: Type a name for the group.

4. Click on *Save record* to save the new group.

2.1.1 Add groups through AD provisioning

User groups (and Users) can also be added through synchronisation with a clients **Active Directory** (Microsoft Azure), through *Authorisation* and *Provisioning*. Please contact your Compano consultant, should you wish to set-up synchronisation with your Active Directory.

2.2 Add users

Next, **individual user accounts** can be added to the system[2]:

To add a user:

1. Through the Menu, go to *System > Users*:

---
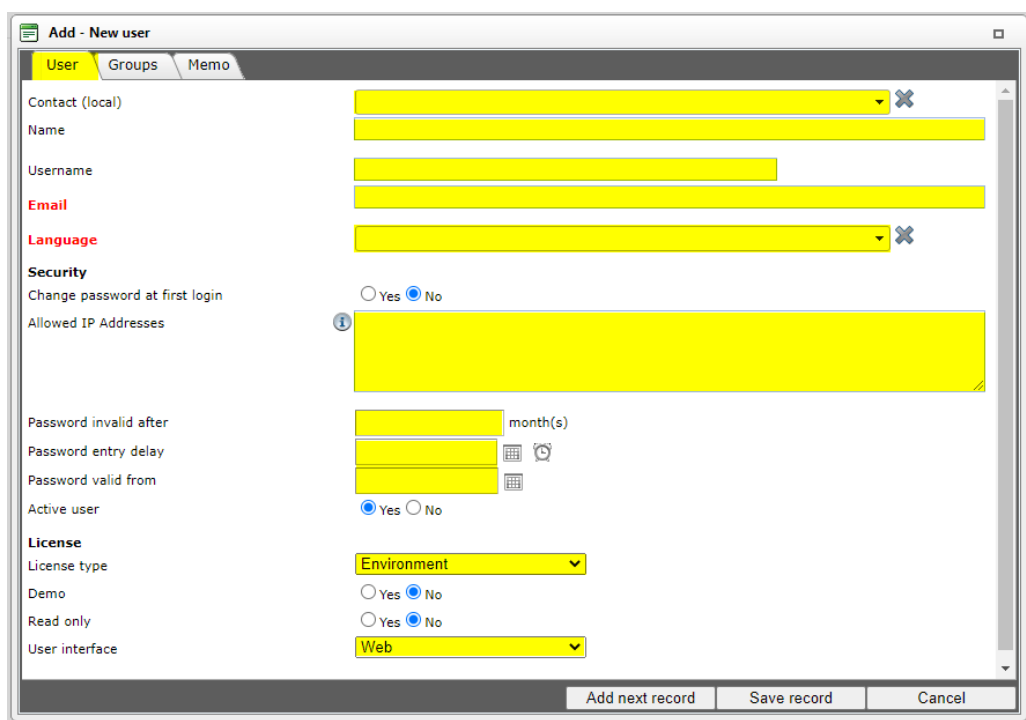
[2] Individual user accounts can always be added to COS to allow access to the application, however **only** through User Groups can detailed user rights be set.
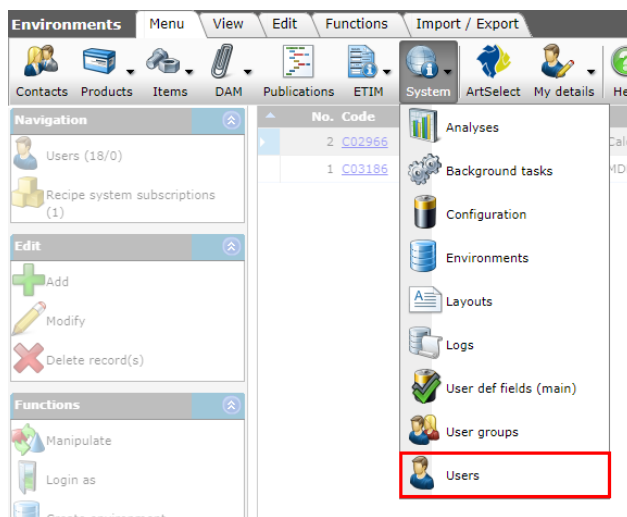
2. Under Edit, click on *+Add*:
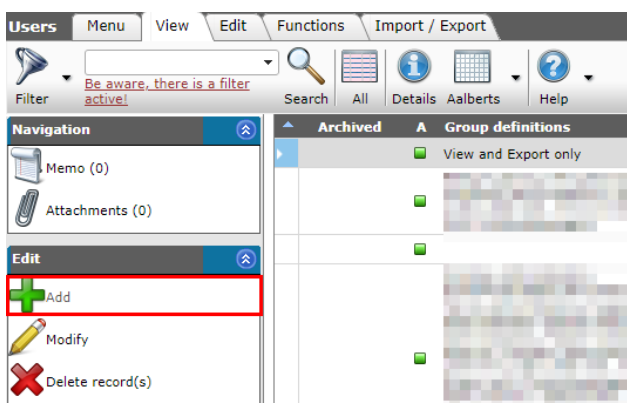
3. In the pop-up window:

User tab

a. **Contact** (optional): Select a pre-existing contact (from Relations) to promote them to User.
b. **Name**: Enter the name of the user.
c. **Username**: Enter the username of the user.
d. **Email**: Enter the e-mail address of the user.
e. **Language**: Select the language for the user interface; the COS-application UI is available in Dutch, English or German.
f. **Change password at first login**: Set to *Yes*, to force the user to change his/her password on first login.
g. **Allowed IP Addresses**: Access to the user interface can be restricted based on IP-address. Note: Multiple IP-addresses can be entered, separated by a semi-colon.
h. **Password invalid after**: This setting can be used to grant temporary access for a user. Enter the number of month(s) after which the current password will become invalid.
i. **Password entry delay**: Set the duration (in minutes) for which to block login after [NUMBER] failed attempts.
j. **Password valid from**: Set the date from which the password is valid; the user cannot login before this date.
k. **Active user**: Set to *No* to de-active this user; this user will then no longer have access to the application.
l. **License type**: Options are *Guest* and *Environment*.
m. **Demo**: Set to *Yes* if the environment is meant as a demo only. Any changes to the data or settings will rolled back during the nightly server recycle action.
n. **Read only**: Set to *Yes* if the user should have read-only access. Records can be viewed and exported, but not added or edited.
o. **User interface**: Set the type of user interface for the user:
   - i. **Web**: User has access to the full COS web interface.
   - ii. **Mobile**: User has access to the COS mobile interface for smartphones and tablets.
   - iii. **FTP**: Not a real user. Used for (automated) FTP-tasks
   - iv. **Feed**: Not a real user. Used for (automated) JSON- and XML-feeds in combination with an API-key. User credentials for this type can no longer be used to login to the User Interface. Furthermore, the API-key associated with the 'feed user' account will only be visible to the Admin user of the system.
   - v. **OData**: Not a real user. Used for (automated) OData-feeds in combination with an API-key. User credentials for this type can no longer be used to login to the User Interface. Furthermore, the API-key associated with the 'feed user' account will only be visible to the Admin user of the system.
   - vi. **ArtConnect**: Not a real user. Used for connecting to ArtConnect.
   - vii. **ArtSelect**: Not a real user. Used for connecting to ArtSelect.

Groups tab

Use the **Group tab** to assign users to one or more groups. Note: Remember that user rights are set group level (!)
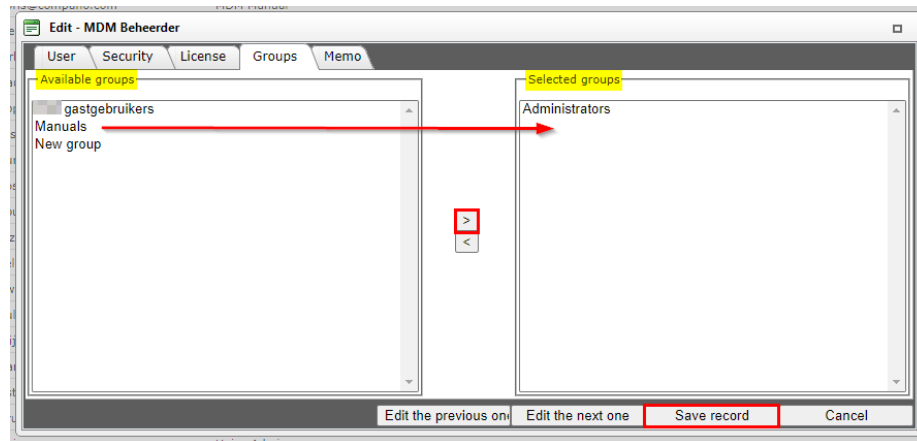
      a. **Available groups**: Select a group and use the `>` arrow to assign the user to this group.

      b. **Selected groups**: Lists the groups to which the user has been assigned.

4. Now, save the record; the user account has been created and added to one or more user groups.

2.2.1   Add users through AD provisioning

User groups can also be added through synchronisation with a clients **Active Directory**. This way users and groups can be managed through **Microsoft Azure**. Please contact your Compano consultant, should you wish to set-up synchronisation with your Active Directory.

2.3   Group access

Once the user groups have been created, **access rights** for the different groups can be set. Group access is set **per Overview,** and allows users in that group access to that Overview.

Note: *Access* allows users to navigate to that Overview through the main menu, however to be able to actually see records of that Overview, detailed access rights need to be set; see paragraph 2.4 Detailed group rights.

Group access can be set manually per Overview:

1. Through the Menu, go to *System > Configuration*:
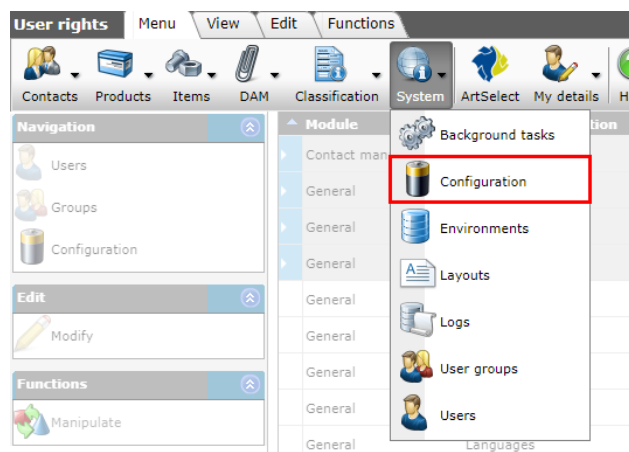
2. In the list, click on *User Rights*:
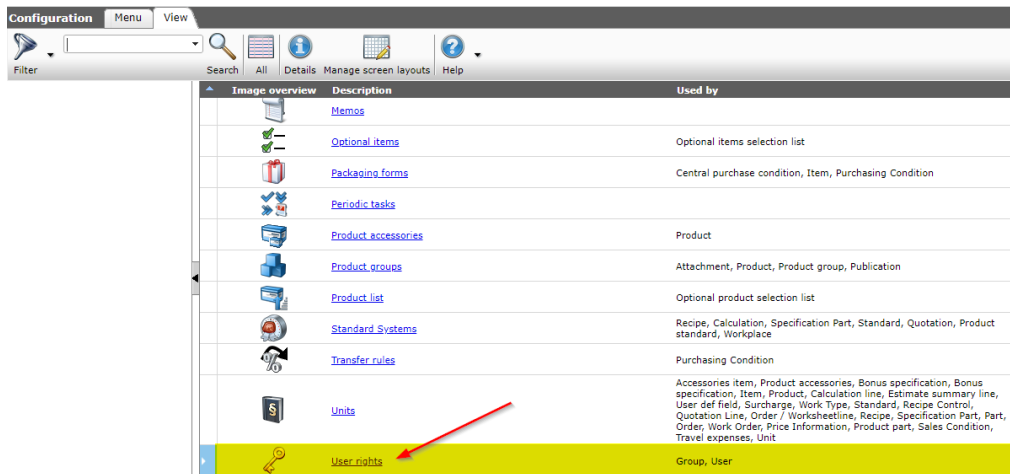
3. On the next screen, you will see a list of *Overviews*. To set access for a Group, select an Overview and, under Edit, click on *Modify*:
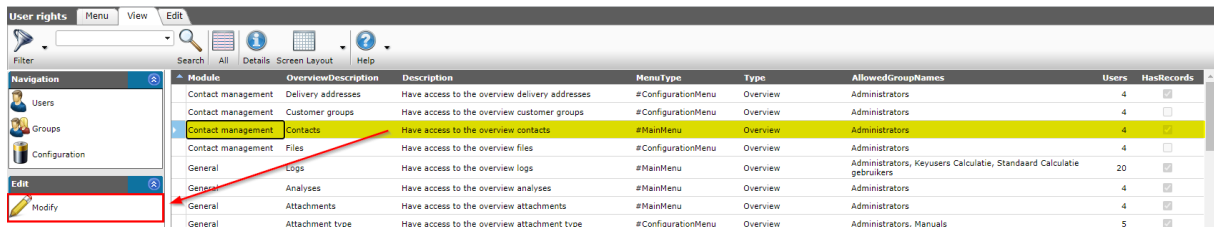
4. In the Edit window:
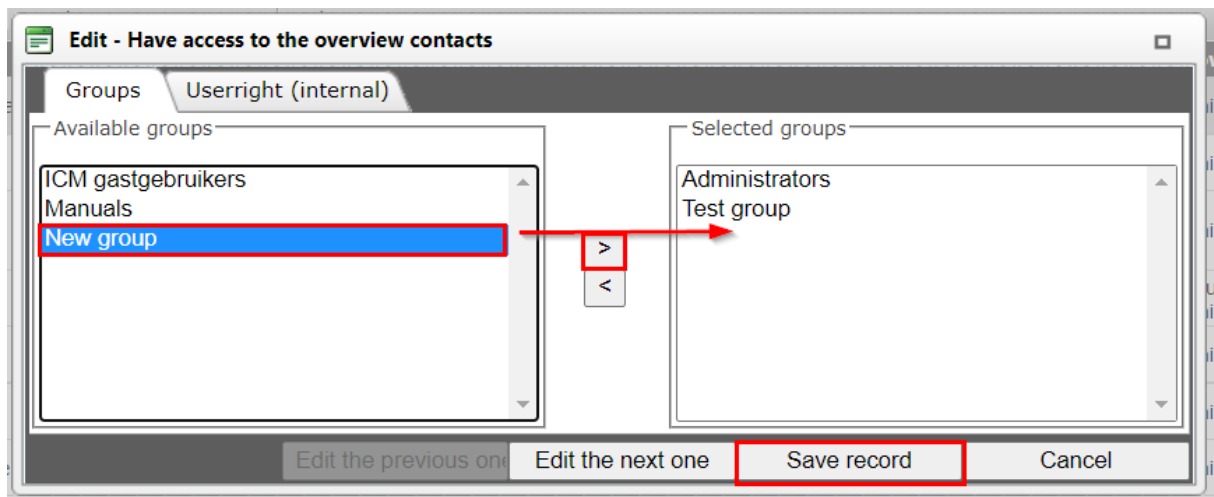
a. **Available groups**: Select any available group and use the ❯ arrow to assign this group to the overview Note: Double-clicking the group will also move it to the Selected groups.

b. **Selected groups**: Selected groups have access to overview.

c. **Edit previous/next**: Use the *Edit previous* and *Edit next buttons* to quickly set group access for the next Overview in the list. <u>Note</u>: Group settings for the current overview will be saved when switching to the next (or previous) record.
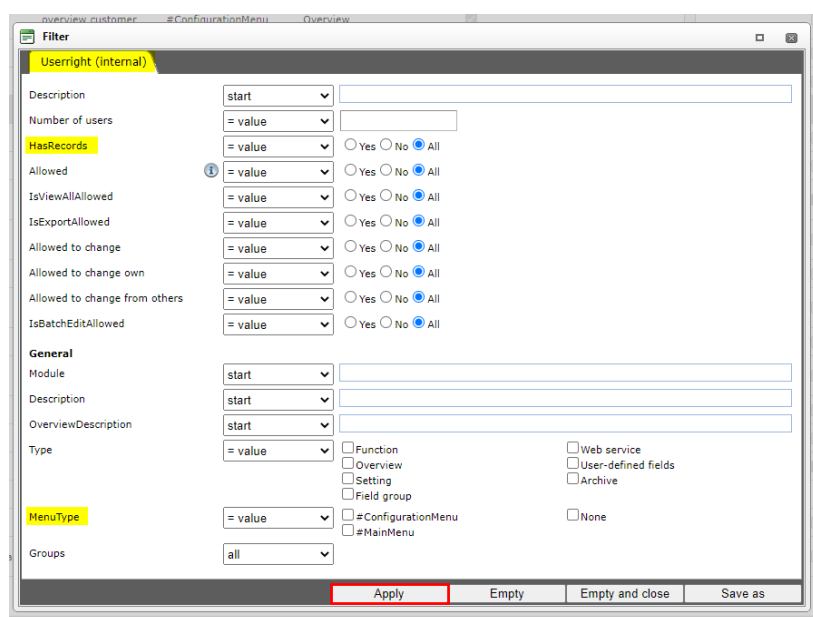
d. **Save record** (optional): Use the *Save record* button to save the access settings for the current overview.

2.3.1 Filtering overviews

To facilitate setting group access, overviews can be filtered on several parameters. Either use the *Comprehensive Filter* or the *Quick Filter* to select types of Overviews.
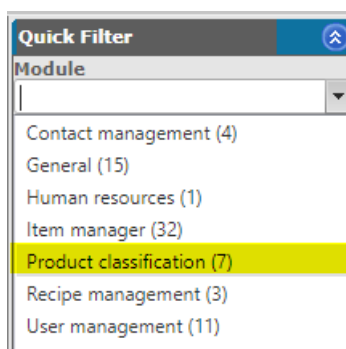
Comprehensive Filter
The comprehensive filter offers multiple options for filtering Overviews. For instance, you could filter on only Overviews that actually have records, or Overviews that belong to a certain menu type:
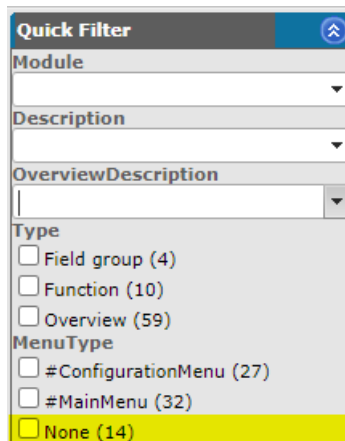
Quick Filter
The quick filter offers a quick selection of Overviews that already have rights set. For example, rights that have been set for the *Product classification* overview:

Also, there is an option to filter out all overviews for which **no rights** have been set:

2.4 Detailed group rights

Now that a group has been assigned to each of the Overviews, **detailed group rights for each Overview** can be set.

For each of the groups, the following rights can be set:

Access to overview (**Allowed**)	User has access to this overview (through the main menu)
View all records (**IsViewAllAllowed)**	User can view *all* records
View own records (**IsViewOwnAllowed**)	User can only view records which he has added himself (only available on certain overviews)
Export allowed (**IsExportAllowed**)	User can export records[3]
Edit own records (**Allowed to change own**)	User can only edit records which he has added himself
Edit all records (**Allowed to change from others**)	User can also edit records which have been added by others
Batch edit allowed (I**sBatchEditAllowed**)	User can edit multiple records; this includes **Manipulation**, all **Import** functions, auto-fill tables and add **User-specific fields** (for that specific overview only)
Edit layouts from a parent environment (**Is edit environment layouts allowed**)	Edit layouts which have been defined in a 'parent' environment

Important: By omitting certain permissions, function buttons might be missing from the interface.

Note: Edit rights include: *Modify, Copy/Paste, Remove, Line Edit.*

2.4.1 Set group rights for a single overview (Edit)

To set group rights for a single overview:

1. Through the menu, go to *System > User groups*:

---

[3] This includes export of attachments and images, export of classification data, export to 2BA, Artikelbeheer, ARGE, Fesah, export of conditions (ICC), CUE, GAEB, UGL, IGM, VGH, Magento and export of publications.

11

2. In the Overview select a group and, under Navigation, click on *User rights (internal)*:

3. On the next screen a list of all Overviews to which the group has access is presented. For each Overview, checkmarks indicate which group rights have been set:

4. To set (or change) a group right, select the Overview and, under Edit, click on *Modify*:

5. Next, set the user rights by selecting **Yes/No** options in the pop-up window:

Note: Setting some rights, such as *Batch edit allowed*, will trigger the setting of other rights, such as *Allowed to change own records*.

6. Save the record.

To speed up the process of setting group rights, you can make use of either the **Edit the next one** *option or use the* **Manipulate** *or* **Line edit** *functions.*

2.4.2 Set group rights for multiple overviews (Manipulate)

To set group rights for multiple overviews:

1. Through the menu, go to *System > User groups*:

2. In the Overview select a group and, under Navigation, click on *User rights (internal)*:

3. On the next screen a list of all Overviews to which the group has access is presented. For each Overview, checkmarks indicate which group rights have been set:

4. To set (or change) the group rights for multiple overviews, select two or more Overviews and, under Functions, click on *Manipulate*:

14
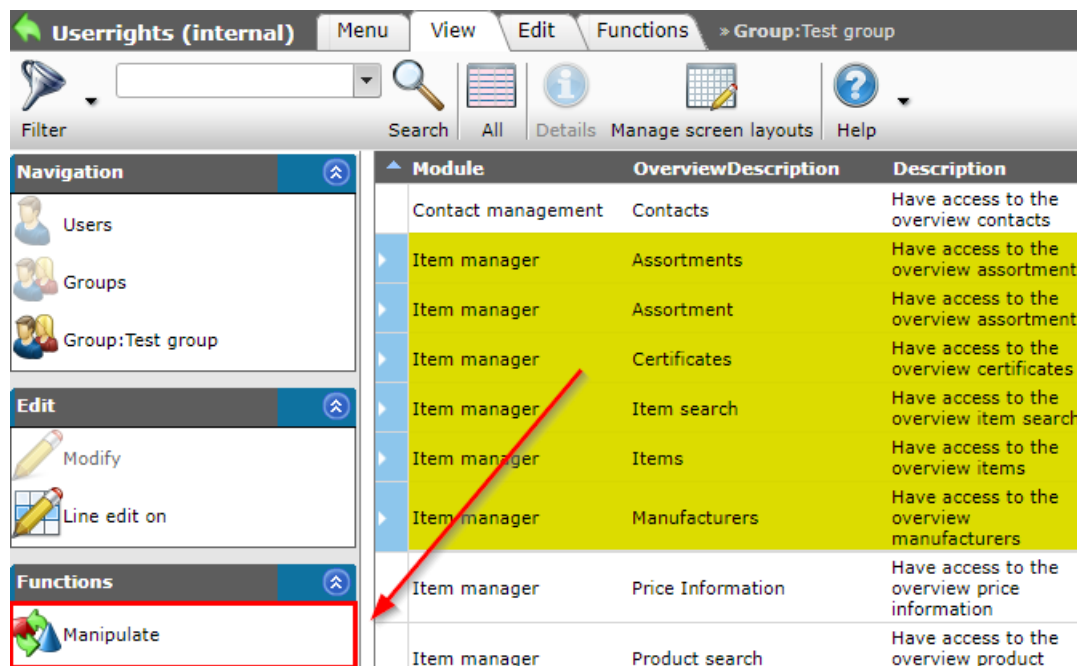
5. Next, set the user rights by selecting `Grant` and setting the `Yes/No` options in the pop-up window:
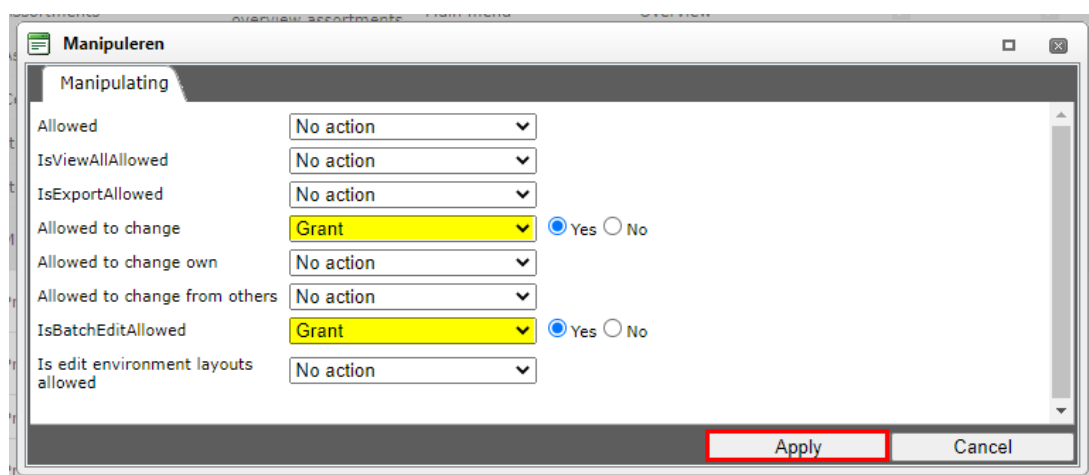
6. Click on *Apply* and in the next pop-up window, confirm by clicking *OK*:
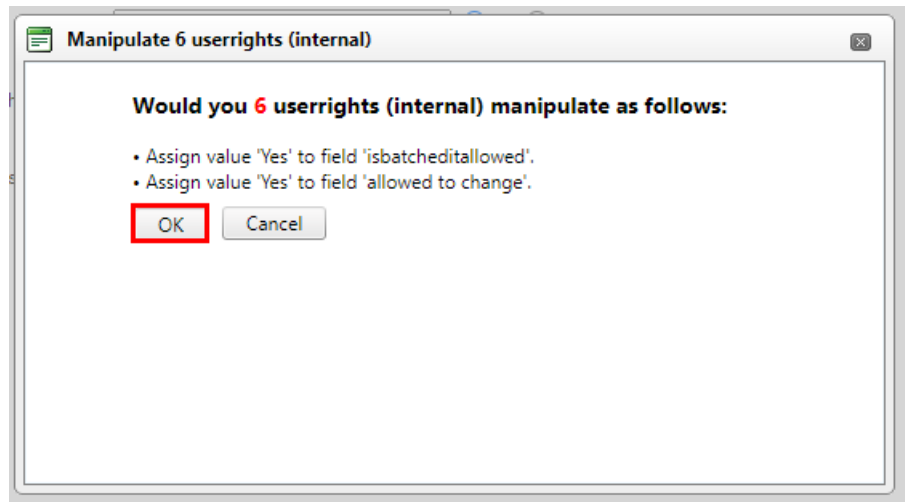
2.4.3 Set group rights (Line edit)

Alternatively, group rights can be set by using the *Line edit* function:

1. Through the menu, go to *System > User groups*:

2. In the Overview select a group and, under Navigation, click on *User rights (internal)*:

3. On the next screen a list of all Overviews to which the group has access is presented. For each Overview, checkmarks indicate which group rights have been set:

4. To set (or change) the group rights, under Edit, first click on *Line edit on*:

5. Next, in the list, click on any of the checkboxes to add or remove group rights of one or more Overviews:

6. Once you have applied all the changes, make sure to click on *Line edit off*:
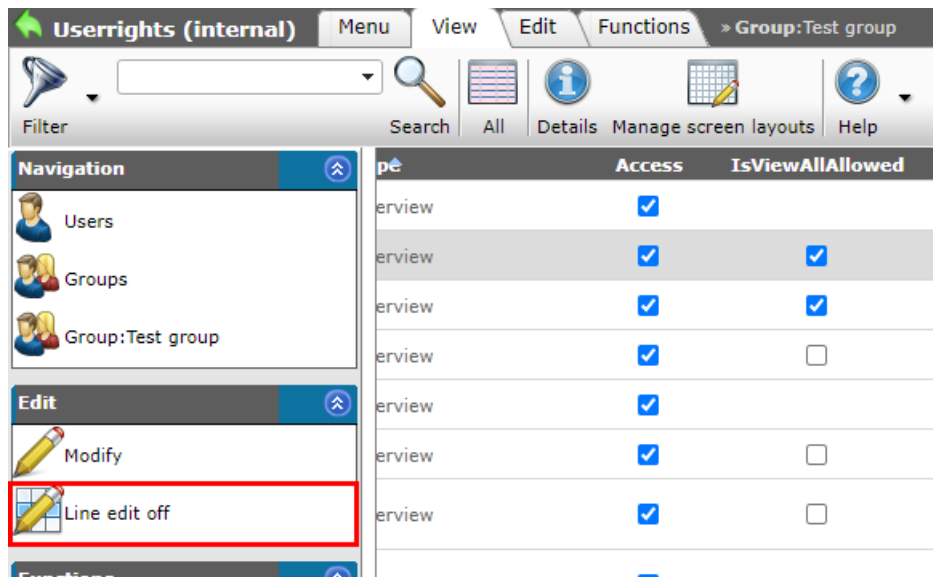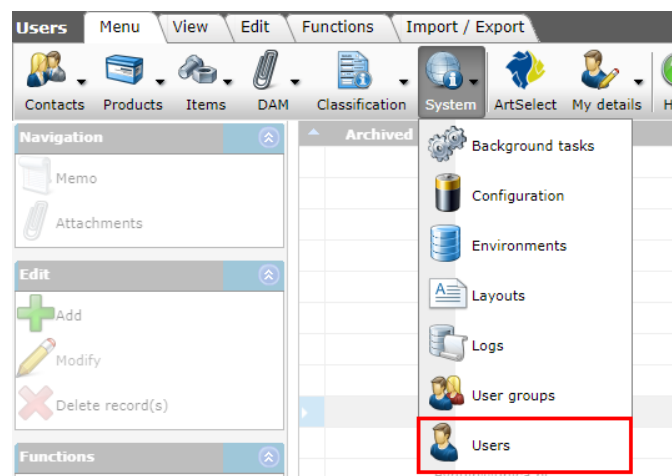

3 Check user rights

To check which rights a user has or which rights might be missing:

- First, check the user license settings;
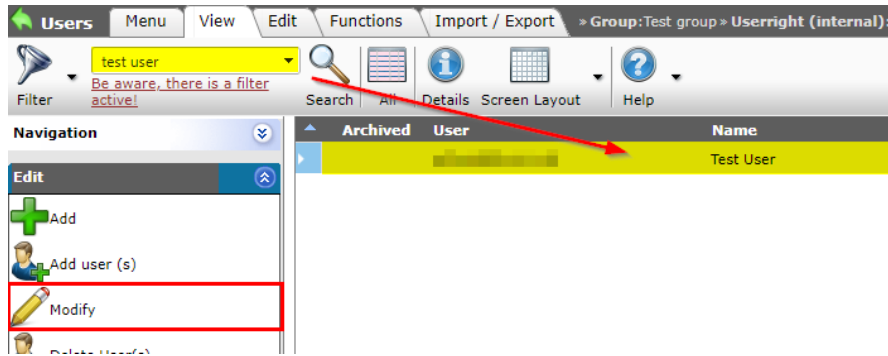- Next, check user group assignment;
- Next, check the group rights.

3.1 Check user license settings
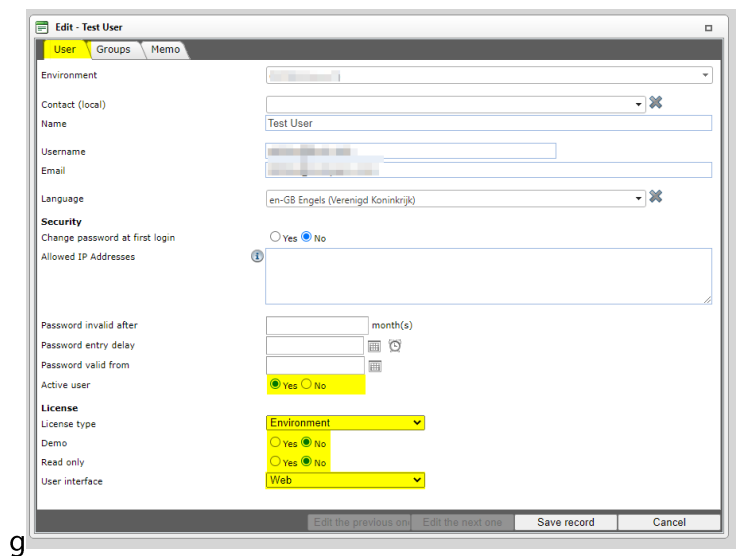
To check the user license settings:

1. Through the menu, go to *System > Users*:

2. Optionally, use the Filter or Search box to find and select the user and, under Edit, click on *Modify*:

18

3. In the pop-up window, check the following settings and make any adjustment where necessary:

g

User tab

a. **Active user**: Set to Yes. When set to No, the user no longer has access to the COS application.

b. **License type**: Commonly set to `Environment`

c. **Demo**: Set to No. When set to Yes, the user has full access to the application however any changes to the data or settings will be rolled back during the nightly recycle action. Note that only an Admin user can change this setting.

d. **Read only**: Set to No. When set to Yes, the user can only view data.

e. **User interface**: Commonly set to Web. Other options are:

| User interface setting	Access to User interface	Other access
Web	Web and mobile	-
Mobile	Mobile only	-
SFTP	No	SFTP locations on Compano server
Feed	No	Request XML or JSON feed
Odata	No	Request Odata feed
Art Connect		
Art Select		

3.2 Check user group assignments

To check to which groups the user has been assigned:

1. Through the menu, go to *System > Users*:
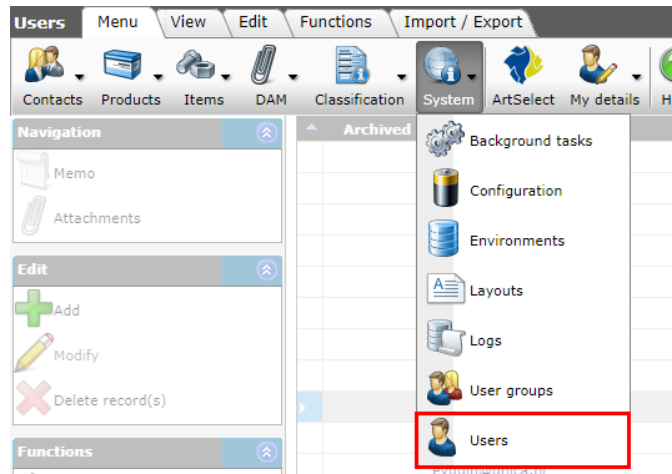
2. Optionally, use the Filter or Search box to find and select the user and, under Edit, click on *Modify*:
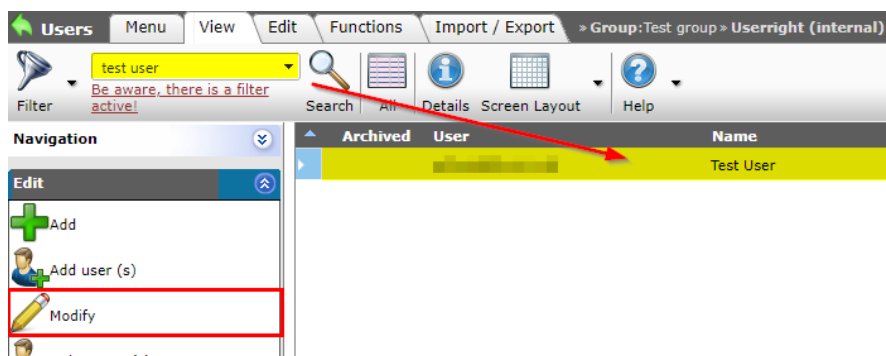
3. In the pop-up window, check the following settings and make any adjustment where necessary:
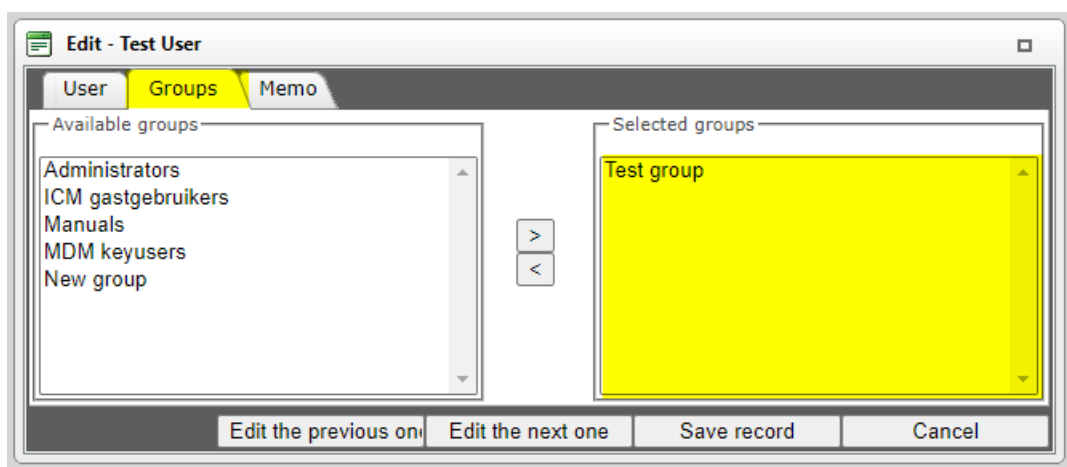
   Groups tab

a. **Available groups**: Groups to which the user currently has *no* access.
b. **Selected groups**: Groups to which the user currently has access.

Note: These general user settings are in addition to any detailed group rights, thus for example a user which has 'read only' rights AND has no access to the Products overview, will not be able to view any products.

3.3   Check group rights

Now that has been established to which groups a user has been assigned, the group rights can be checked:

1. Through the menu, go to *System > User groups*:
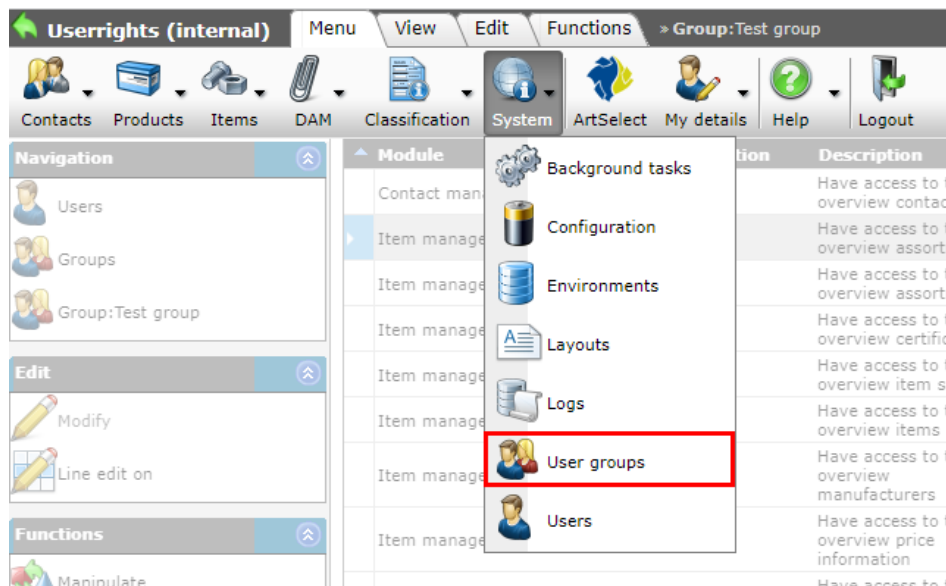
2. In the Overview select a relevant user group and, under Navigation, click on *User rights (internal)*:
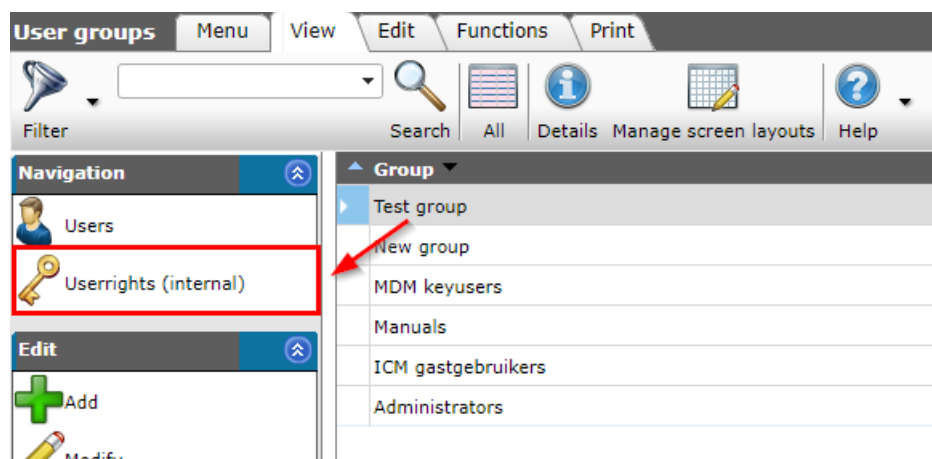
3. On the next screen a list of all Overviews to which the group has access is presented. For each Overview, checkmarks indicate which group rights have been set:

4. Make any adjustments where necessary; see 2.4 Detailed group rights.

4 Print user rights

For a convenient overview of user rights, these can be printed.

4.1 Print group rights

User rights are tied to group rights, thus to get an overview of a user's rights, the detailed group rights need to be printed.
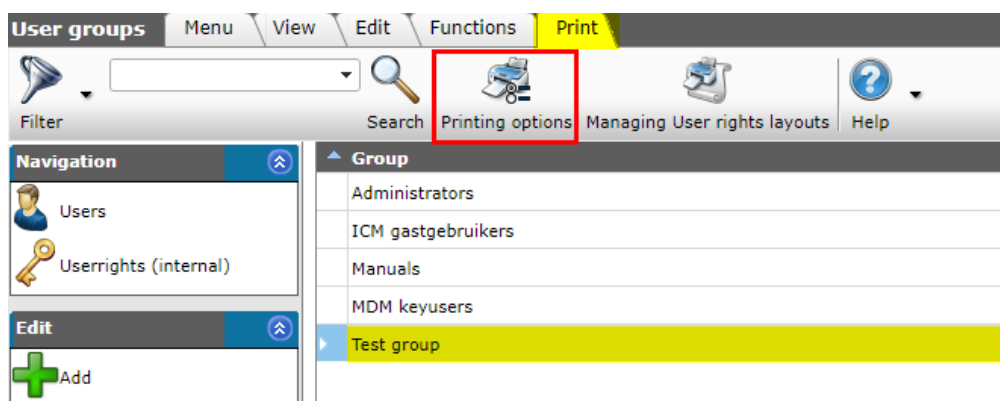
Note: Should a user have access to multiple groups, then the group rights of all groups should be printed .

To print the detailed group rights:

1. Through the menu, go to *System > User groups*:
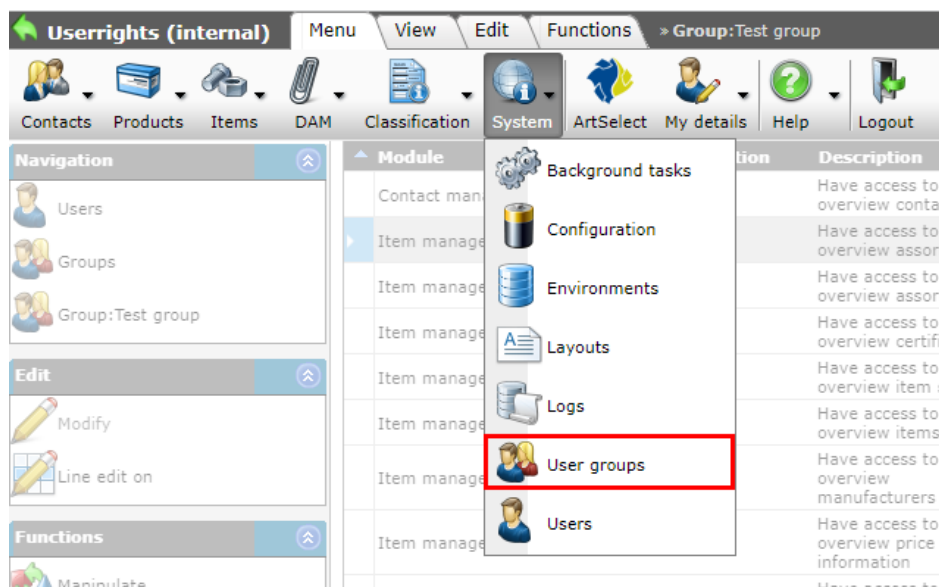
2. In the Overview select a group and, on the Print tab, click on *Printing options*:

3. In the pop-up windows, click on *Print*:

Group Name Test group

Full name

Description	IsViewAllAllowed	IsExportAllowed	Allowed to change	Allowed to change from others
Have access to the overview contacts		No	No	
Have access to the overview assortments	Yes	Yes		No
Have access to the overview	Yes	No		No

5 Appendix A – Examples

Some examples of how to set user rights.

5.1 User rights per Assortment

When only *one* user should be able to edit (items) in an Assortment, user rights can be set as follows:

1. Create a User Group, for instance `Local Assortment responsible`.
2. Set the rights for this group for: `Have access to the overview assortment`:

    a. **Edit all records**: Set to No, as the users in this group should only be allowed to edit the assortment to which they are assigned as *Data Manager*.
    b. **Other rights**: Set to Yes.
3. Set the rights for this group for: `Have access to the overview items`:

    a. **Edit all records**: Set to No, as the users in this group should only be allowed to edit the items in the assortment to which they are assigned as *Data manager*.
    b. **Other rights**: Set to Yes.
4. Add a user to the group.

24

5. Modify the Assortment and set the same user as the *Data manager* of that Assortment:

5.2 User rights per Manufacturer

When only *one* user should be able to edit (products of an Manufacturer, user rights can be set as follows:

1. Create a User Group, for instance `Local Manufacturer responsible`.
2. Set the rights for this group for: `Have access to the overview manufacturer`:

a. **Edit all records**: Set to No, as the users in this group should only be allowed to edit the manufacturer to which they are assigned as *Data Manager*.

b. **Other rights**: Set to Yes.

3. Set the rights for this group for: `Have access to the overview products`:

a. **Edit all records**: Set to No, as the users in this group should only be allowed to edit the items in the assortment to which they are assigned as *Data manager*.

b. **Other rights**: Set to Yes.

4. Add a user to the group.

5. Modify the Manufacturer and set the same user as the ***Data manager*** of that Manufacturer: