Creatio Academy

Access management

Version 8.0

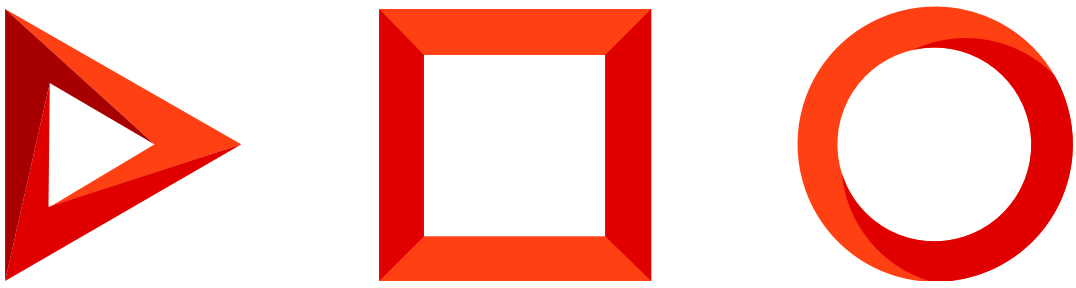


Table of Contents

Object operation permissions

PRODUCTS: ALL CREATIO PRODUCTS

This article covers the setup of **business data access permissions**. Access to business data involves CRUD data operations: create, read, update, and delete. To grant access to business data, configure access permissions to corresponding Creatio objects.

If you are just getting started with Creatio, we recommend familiarizing yourself with the principles of Creatio object permissions in the e-learning course: User and role management, Access permissions.

Configure object permissions on several levels:

- **Operation permissions**. This article covers the setup of data operation permissions for different Creatio objects: section and detail.
- **Record permissions**. Learn more in a separate article: Record permissions.
- **Column permissions**. Learn more in a separate article: Column permissions.

Access to functions can be granted through system operations. Object operations are different from system operations. Set up system operation permissions in the [*Operation permissions*] section of the System Designer. Learn more in a separate article: System operation permissions.

> **Note.** Certain system operations cancel any other object permission settings, namely: “View any data” (“CanSelectEverything” code), “Add any data” (“CanInsertEverything” code), “Edit any data” (“CanUpdateEverything” code), and “Delete any data” (“CanDeleteEverything” code). The user that has access to these operations receives permissions regardless of the settings in the [*Object permissions*] section.

Creatio includes the following object permissions out-of-the-box:

- “All employees” organizational role has permissions to create, read, update and delete any record in any object. Creatio also grants these permissions to All employees role for objects with “Use operation permissions” switch disabled.
- “All portal users” organizational role has no operation permissions for Creatio records. To enable the users with this role to see their records and their organization's data in the portal, set up operation permissions for each section available in the portal.
- “System administrators” organizational role has system operation permissions to add, view, edit and delete any data. These permissions have higher priority than object operation permissions.

Configure access to operations in section objects

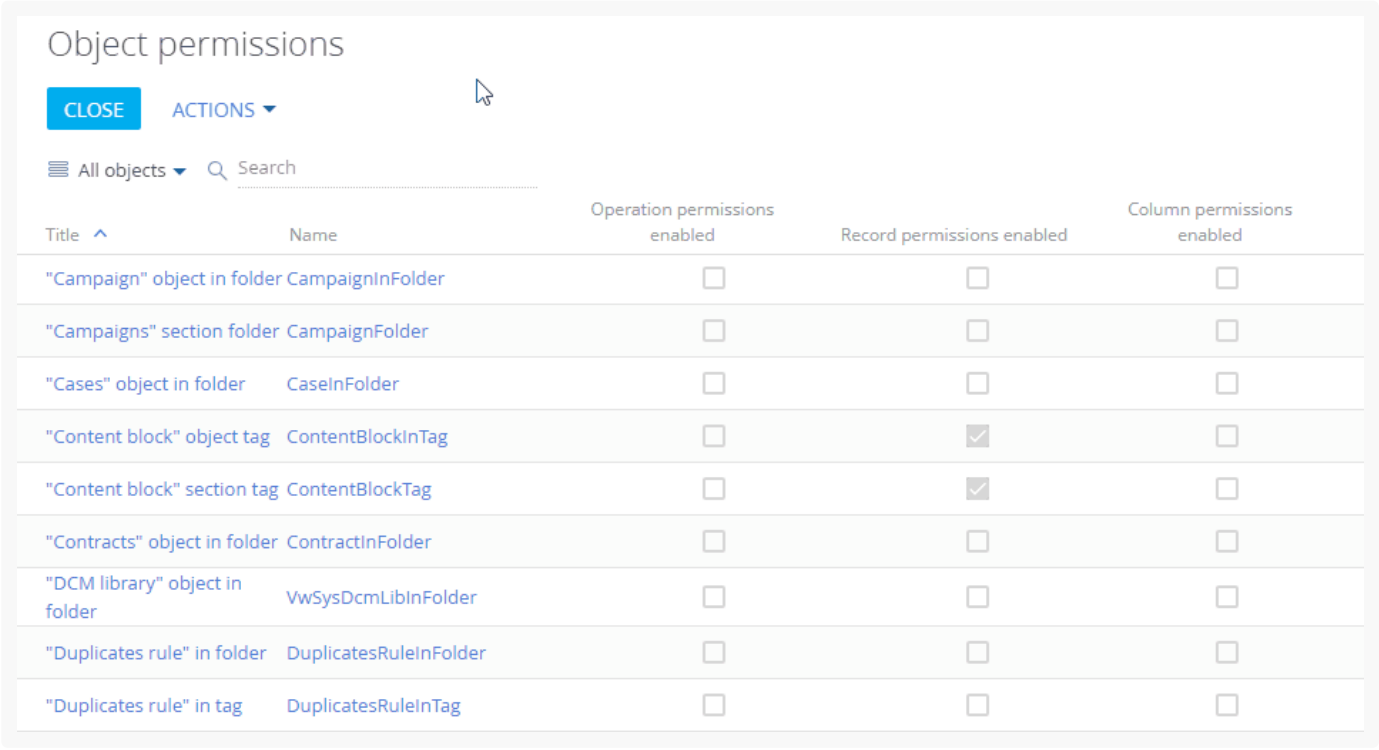
> **Case.** Set up the following permissions to the [*Opportunities*] section:
>
> Sales managers must have all permissions to section records except for the “Delete” permission.

Their managers must have full access to records.

One of the employees with the “Secretaries” role must have a permission to view the section records, while all other secretaries should not be able to view the [*Opportunities*] section at all.

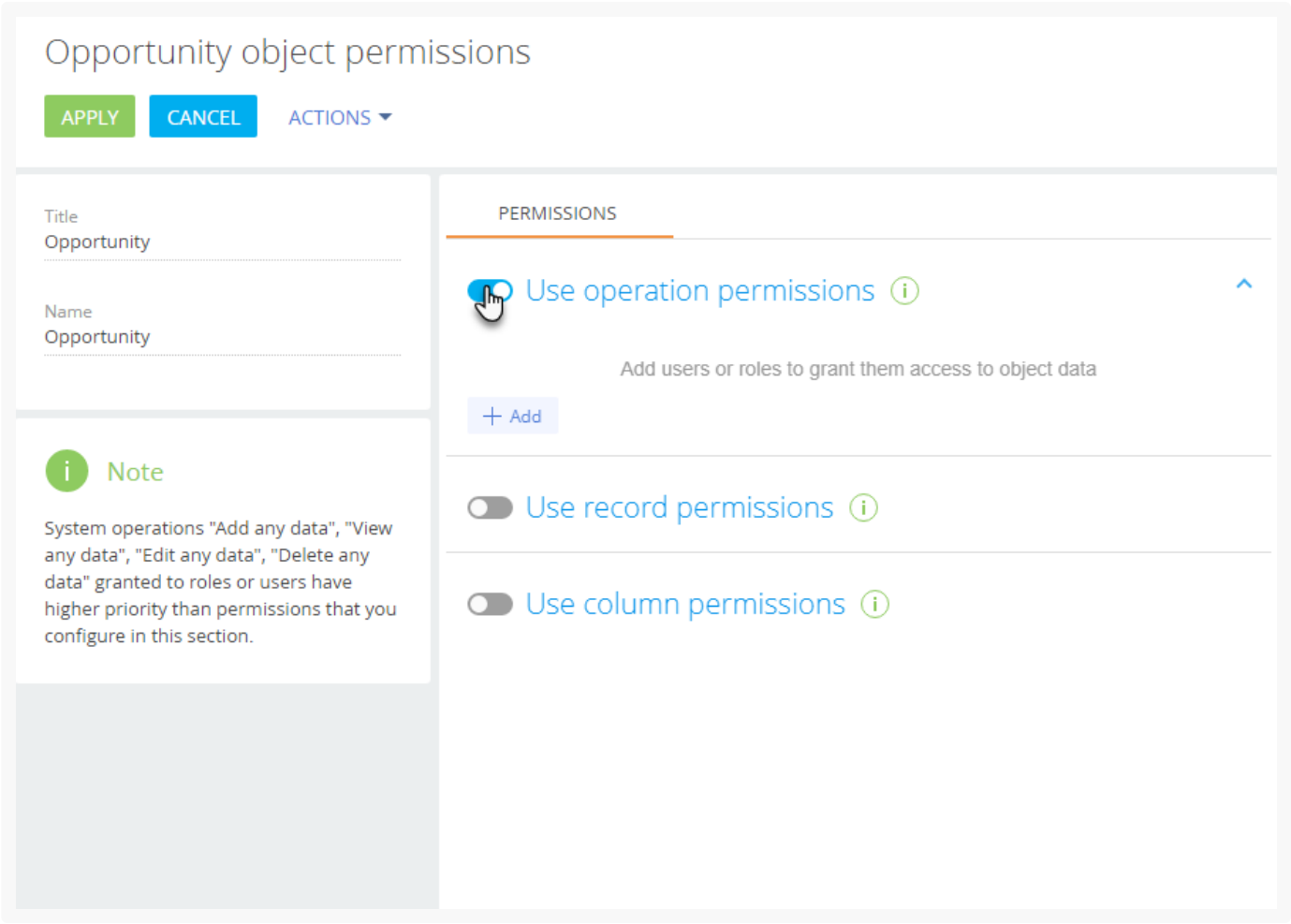
1. Go to the System Designer (button) and open the [*Object permissions*] section.
2. Select the necessary object in the list or use the search box. For example, to configure access permissions to the [*Opportunities*] section, select the “Sections” filter and choose the “Opportunity” object. Click the name (or title) of the object to open the object permission settings window (Fig. 1).

Fig. 1 Choosing the section object and opening the permissions settings window



3. Enable the “Use operation permissions” switch (Fig. 2).

Fig. 2 Enable the “Use operation permissions” switch



Attention. If you remove the “All employees” role from the settings area, and then disable the “Use operation permissions” switch and apply the changes, users will not be able to see the object records.

4. Click [*Add*] and select the necessary users and roles. You can use the search box or the [*Organizational roles*], [*Functional roles*] and [*Users*] tabs to quickly find users and roles. In this case:

   a. The “All employees” role (added automatically).

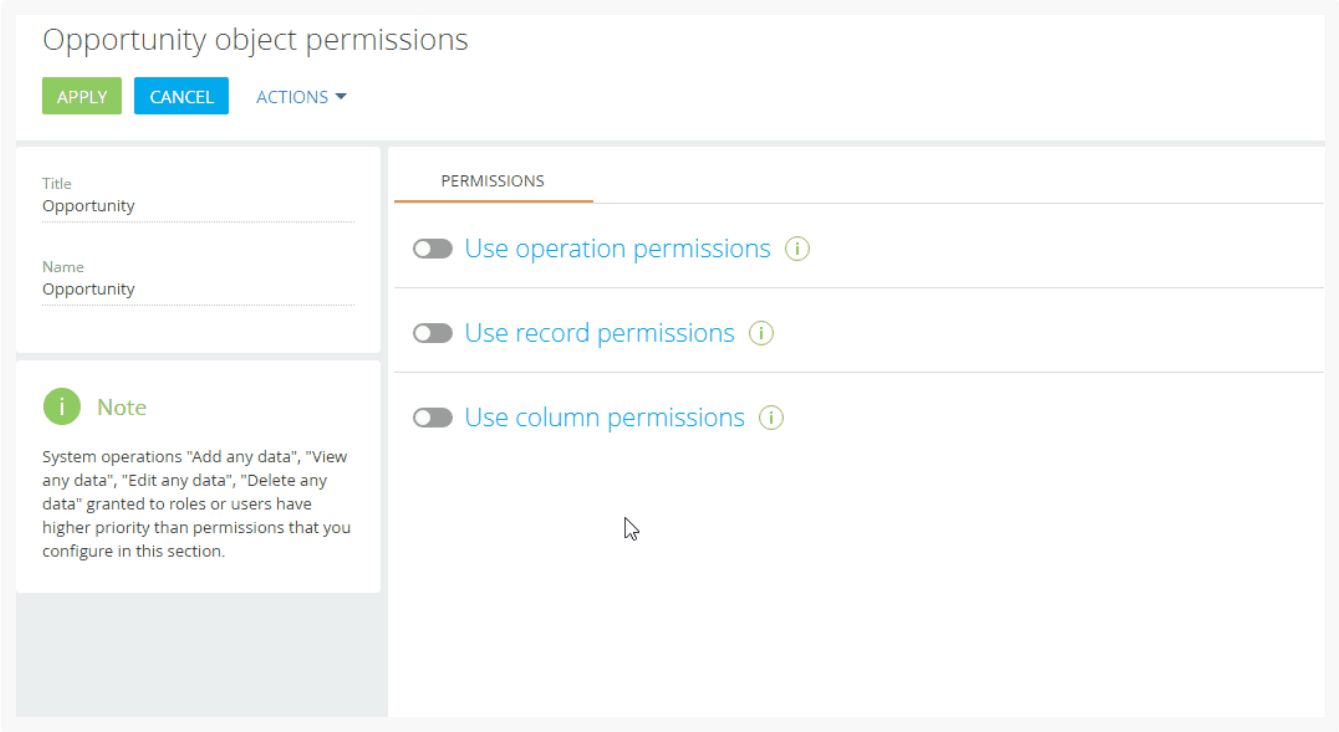
   b. The “Sales managers” organizational role.

   c. The “Sales managers. Managers group” organizational role.

   d. The “Secretaries” organizational role.

   e. An individual user from the “Secretaries” organizational role (Fig. 3), e. g., V. Murphy.

Fig. 3 Adding users and roles to grant access permissions to the section



5. By default, each user or role that you add is granted access to read, create, update and delete object data. Edit these permissions according to your requirements, for example:

   a. Leave the [*Read*] checkbox selected and clear the [*Create*], [*Edit*] and [*Delete*] checkboxes for the "**All employees**" role. As a result, all company employees can read section records but cannot create, edit or delete them.

   b. Leave the [*Read*], [*Create*], [*Edit*] checkboxes selected and clear the [*Delete*] checkbox for the "**Sales managers**" role. As a result, sales managers will be able to read, create and edit section records without the ability to delete them.

   c. Leave the [*Read*], [*Create*], [*Edit*] and [*Delete*] checkboxes selected for the "**Sales managers. Managers group**" role. As a result, sales department managers will have permission to read, create, edit or delete records in the [*Opportunities*] section.

   d. Clear the [*Read*], [*Create*], [*Edit*] and [*Delete*] checkboxes for the "**Secretaries**" role. As a result, the [*Opportunities*] section will be hidden from the company's secretaries.

   e. Leave the [*Read*] checkbox selected for the **specific user in the "Secretaries" role**. As a result, the user can read records in the [*Opportunities*] section.

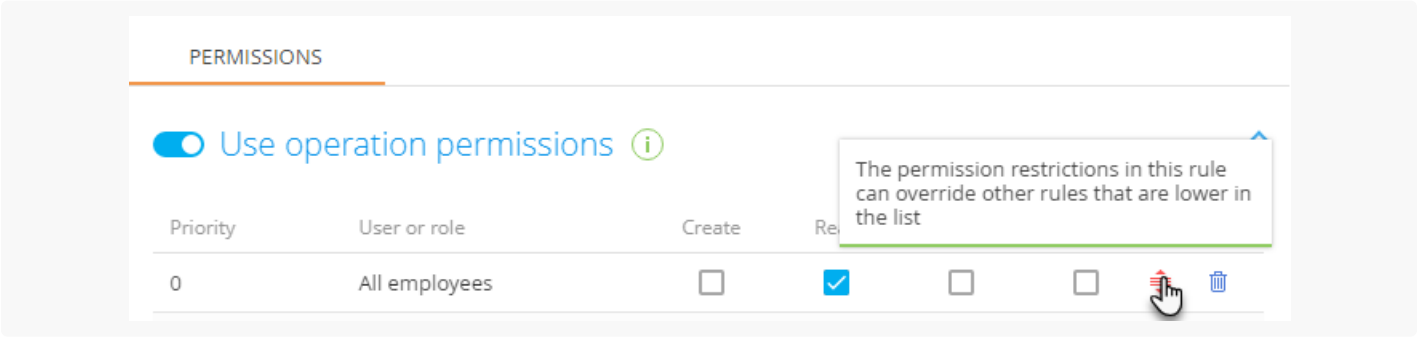
      icon might appear next to some permissions. This means that some settings contradict each other, and it is necessary to adjust their priorities.

Create the hierarchy of object operation permissions

Sometimes the access permissions that apply to the same user or role might contradict each other, since a user might be included in several roles. Also, organizational roles might inherit permissions from one another, for example, the "Sales managers," "Sales managers. Managers group," and "Secretaries" roles are a part of the "All employees" role. Additionally, permissions granted to an individual user might conflict with permissions that the user might have as a member of their role. These conflicts are indicated by the icon next to the conflicting access permission.

In case of a conflict, the permission that is the highest in the list will have a higher priority. The priority is shown in the [*Priority*] column and the highest possible priority is “0.” An icon next to an access permission rule indicates such a conflict. You can drag a rule to change its position in the list (Fig. 4).

Fig. 4 The need to adjust priorities in the list of permission rules



Please take the following into account while configuring access permission priorities:

- A user who is a part of several roles will get the access permissions of the **highest** role in the list.

  For example, all users should not access the [*Opportunities*] section records, but sales managers (who also belong to the “All users” role) should be given all permissions except those that enable them to delete records. To do this, place the “Sales managers” role higher than “All employees” in the list.

- To deny access permissions to an operation for a role while permitting the operation for some of its users, place this role **lower** in the list than the users who need to be granted access.

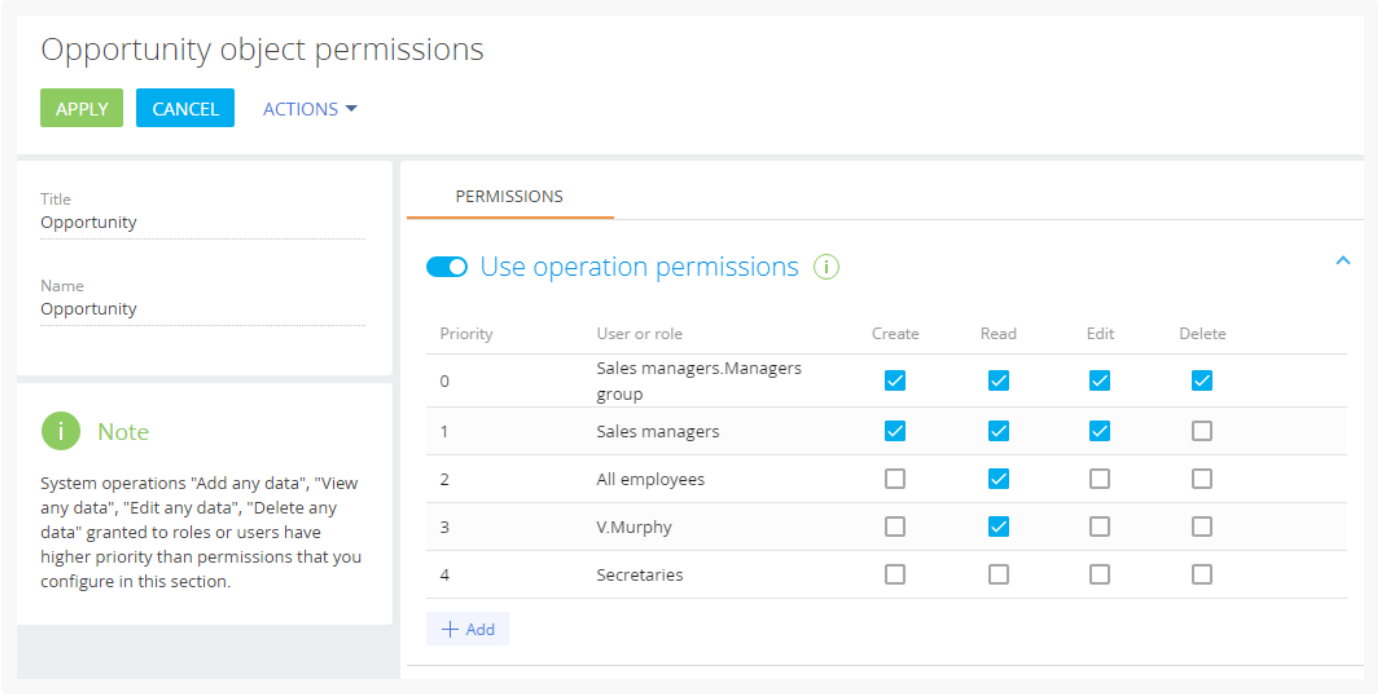
  Thus, if you deny access to the [*Opportunities*] section for the “Secretaries” role, but grant permission to read data to one of the secretaries, make sure that you move the “Secretaries” below the secretary employee who is supposed to access to the section.

- Users or roles that are **not added** to the object operations settings area do not get access to operations and are not included in priority settings.

Configure access permission priorities. To change the rule display order, drag the rule to the necessary position in the list (Fig. 5).

1. Place the organizational role with the highest level of permissions (in our case, “Sales managers. Managers group”) at the top of the list.
2. Place the “Sales managers” role directly below.
3. The “All employees” role and the “V. Murphy” user (who belongs to the “Secretaries” role) have the same access permissions. Thus, you can place them directly below the “Sales managers” role in any order.
4. The “Secretaries” role should be placed at the very bottom of the list since they do not have access to the [*Opportunities*] section.
5. Save the changes by clicking “Apply” in the upper left corner of the page.

Fig. 5 Set up the access permission priorities



As a result:

- Users in the “**Sales managers**” role have access to the [*Opportunities*] section with the ability to create and edit section records. Sales managers do not have permission to delete records.
- Their **managers** should have full access to these records, including the permissions to delete them.
- **All company employees** can read section records but cannot create, edit or delete them.
- All **secretaries**, apart from V. Murphy, cannot view the [*Opportunities*] section records.
- **V. Murphy** can read the records in the section.

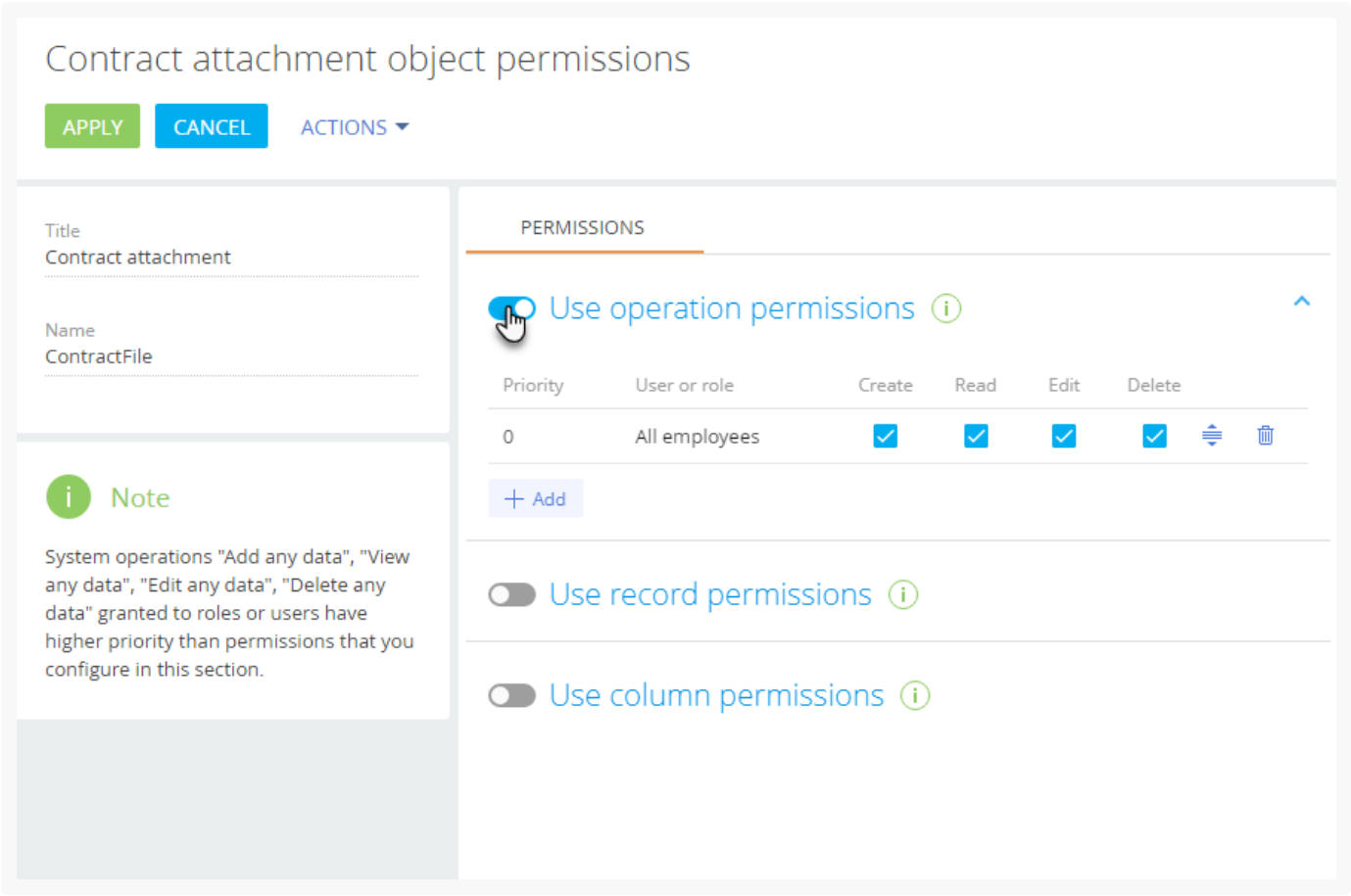
Configure access to operations in detail objects

Case. Configure access permissions to the [*Attachments*] detail in the [*Contracts*] section. Users in the “Sales managers” organizational role should have full access to detail records.

All other users can only view the files in the detail and cannot edit or delete them.

1. Go to the System Designer (button) and open the [*Object permissions*] section.
2. Select the “All objects” filter.
3. Find the “Attachments” object via the search box.
4. Click the name or the title of the object to open the access permissions configuration window.
5. Enable the “Use operation permissions” switch (Fig. 6).

Fig. 6 Enable the “Use operation permissions” switch



6. Click [*Add*] and select the necessary users and roles. Use the search box to quickly find the necessary users and roles. In this case:

   a. The “All employees” role (added automatically).

   b. The “Sales managers” role.

7. By default, each user or role in the list is granted access to read, create, update and delete object data. Edit these permissions to fit the example requirements:

   a. Leave the [*Read*], [*Create*], [*Edit*] and [*Delete*] checkboxes selected for the “**Sales managers**” role. As a result, sales managers can read, create, edit and delete data in the [*Attachments*] detail.

   b. Leave the [*Read*] checkbox selected and clear the [*Create*], [*Edit*] and [*Delete*] checkboxes for the “**All employees**” role. As a result, all employee users can view the data on the [*Attachments*] detail without the ability to add, edit or delete anything.

8. If necessary, configure access priorities for the selected roles. Adjustments might be necessary if access levels conflict with each other (roles might overlap). For example, the “Sales Managers” role is included in the “All Employees” role. These conflicts are indicated by the icon next to the conflicting access permission. Learn more about priorities: Create the hierarchy of object operation permissions.

As a result:

- Users in the “**Sales managers**” role have full access to the [*Attachments*] detail.
- **All company’s employees** can view the data on the [*Attachments*] detail without the ability to create, edit or delete anything.

Column permissions

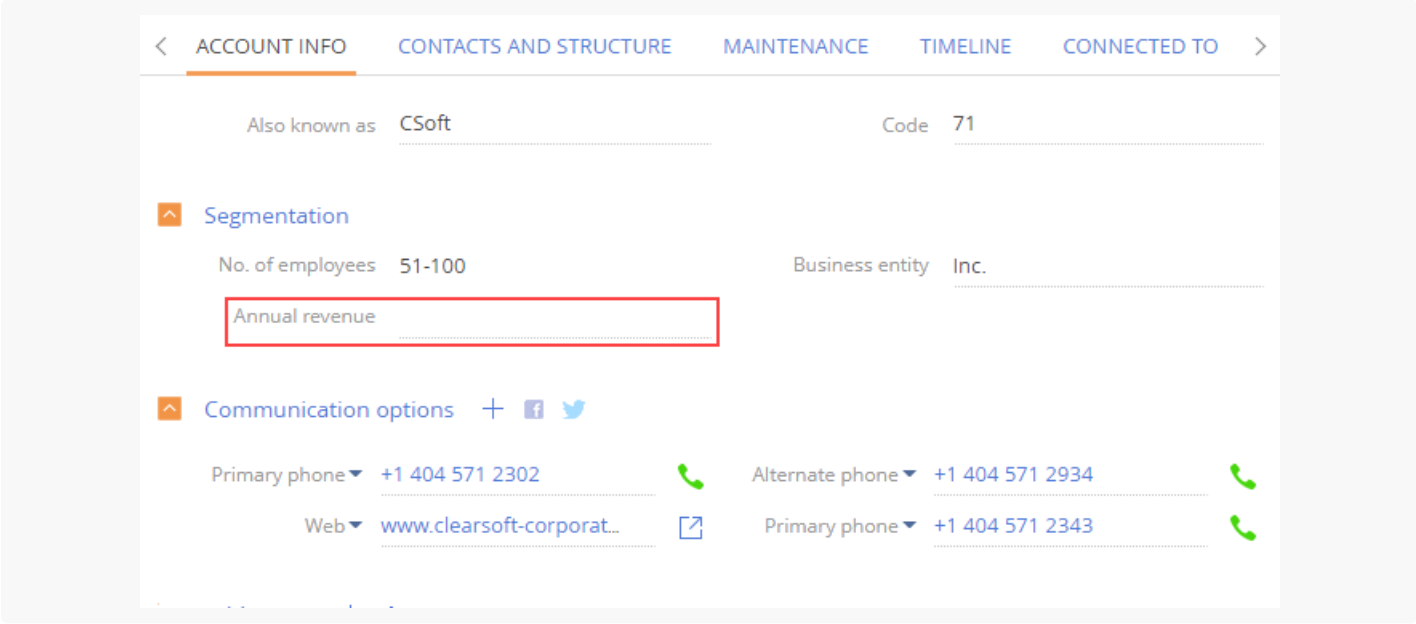
PRODUCTS: ALL CREATIO PRODUCTS

Configure object permissions on several levels:

- **Operation permissions**. Learn more in a separate article: Object operation permissions.
- **Record permissions**. Learn more in a separate article: Record permissions.
- **Column permissions**. This article explains how to configure permissions to read, edit, and delete **individual columns** of a particular object.

Object columns are displayed as fields on pages and section/detail lists. Column permissions let you limit access to read or edit individual object fields for individual users or roles. For example, you can limit permissions to read data in the [*Annual revenue*] field for the “Secretaries” organizational role and enable all other employees to read the data in that field. The users who do not have permission to read data in the [*Annual revenue*] field will see the field itself, but not its value (Fig. 1).

Fig. 1 The [*Annual revenue*] field with restricted access permissions



Operation permissions override column permissions for particular users or roles. For example, if the user lacks permission to read object data, Creatio does not display the object for the user at all.

If you do not add a column to the detail or do not specify any access permissions for a column on the detail, Creatio grants access to the column according to the operation permissions.

If you add a new column to an object that has column permissions set up, Creatio grants permissions to read the column to all users automatically.

If you are just getting started with Creatio, we recommend familiarizing yourself with the principles of Creatio object permissions in the e-learning course: User and role management, Access permissions.

Attention. Before you set up object column permissions, make sure that the user or role has access to

the corresponding object operations and records. Note that if an object is not managed by operations and records, all users and roles have full access to all operations and all records. Learn more in a separate article: Object operation permissions.

Assign column permissions

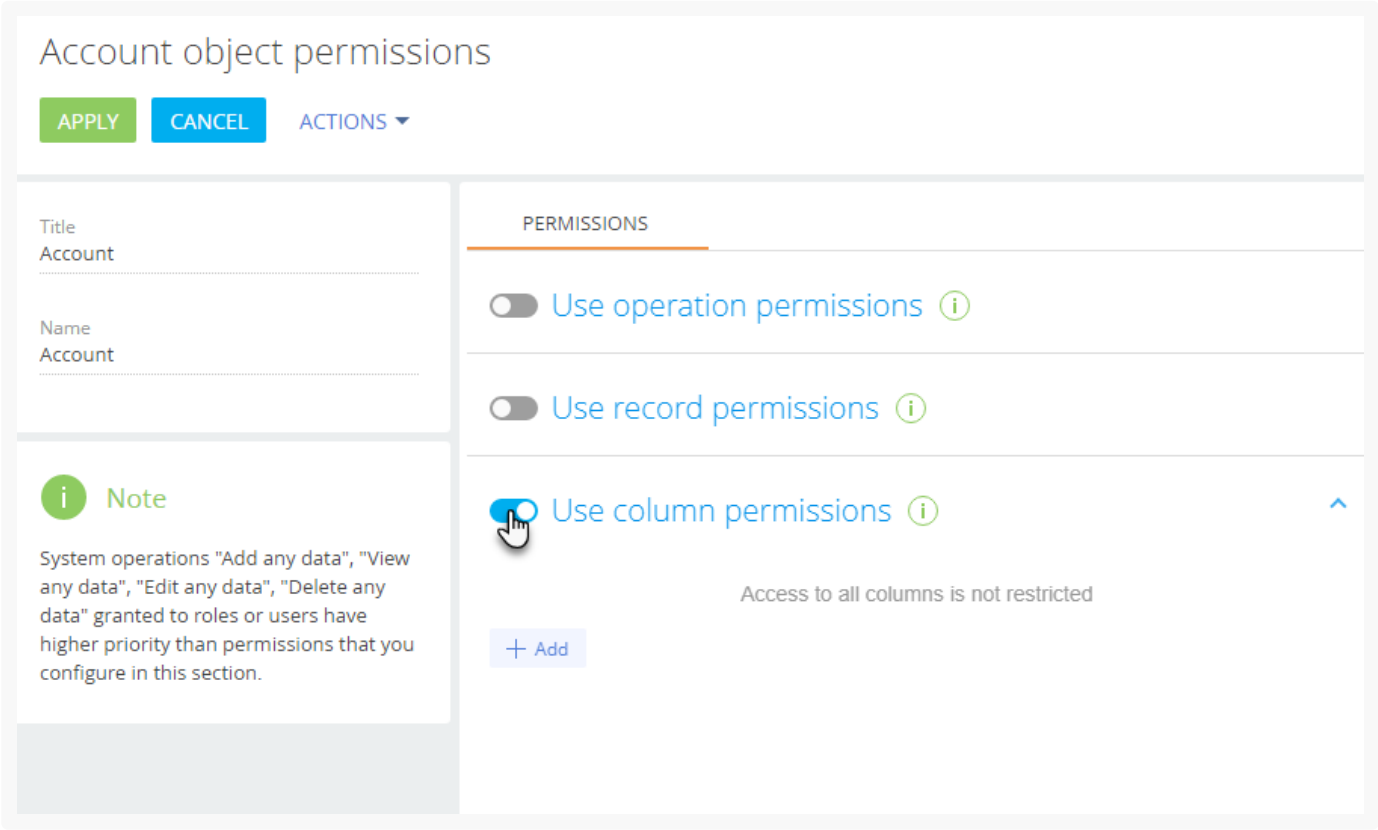
This section covers how to grant or limit access permissions to read and edit data of a particular section record field.

Example. Set up permissions to the [*Annual revenue*] field on the account page. All company's employees, apart from its secretaries, must have permissions to read the data in the [*Annual revenue*] field, while the sales managers must have permissions to read and edit data in that field.

The field value must be hidden for the company's secretaries.

1. Click the button to open the System Designer → the "**Object permissions**" section.
2. Select the necessary object in the list or use the search bar. For example, to configure access permissions to the [*Annual revenue*] field, select the "Sections" filter and choose the "Account" object. Click the name (or title) of the object to open the object permissions settings window.
3. Make sure that the necessary users or roles already have access to object operations or that the object is not administered by operations.
4. Enable the "Use column permissions" toggle (Fig. 2).

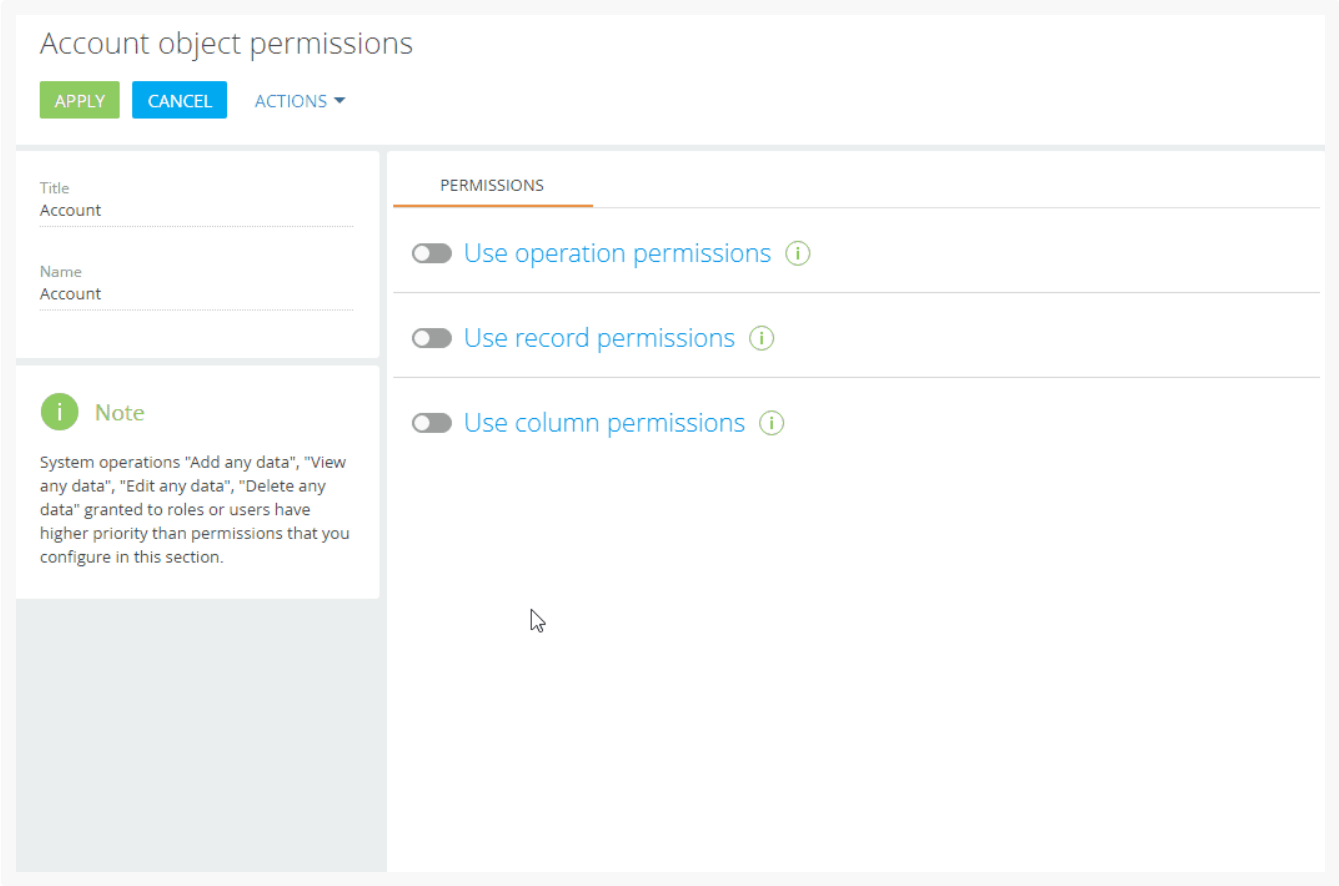
Fig. 2 Enable the column permissions



5. Click [*Add*] and select the necessary column. For example, to limit access to the [*Annual revenue*] field, type “Annual revenue” in the search box and click [*Select*]. The selected column will be displayed in the list on the left. The list on the right lets you select users and roles to configure access permissions (Fig. 3). You can add other columns, if necessary. Select a column in the list to configure its access permissions.
6. Click [*Add*] in the list on the right, then select users and roles. You can use the search bar or the [*Organizational roles*], [*Functional roles*] and [*Users*] tabs to quickly find users and roles in the selection box (Fig. 3). In this example, the roles are as follows:

   - the “All employees” role (added automatically)
   - the “Sales managers” organizational role
   - the “Secretaries” organizational role

Fig. 3 Selecting the [*Annual revenue*] column and adding users and roles to configure access permissions



By default, each user or role added to the list gets permissions to read, update and delete the object field. Modify permissions to restrict access. For example:

a. Change access permissions for the “**All employees**” role to “Permit reading”. As a result, all company’s employees will be able to see the [*Annual revenue*] field value on the account page without the ability to edit it.
b. Select the “Permit reading and editing” access permission level for the ”**Sales managers**” role. As a result, the sales managers will be able to read and edit the value of the [*Annual revenue*] field.
c. Select the “Deny reading and editing” access permissions level for the “**Secretaries**” role. As a result, the company’s secretaries will not be able to see the value of the [*Annual revenue*] field.

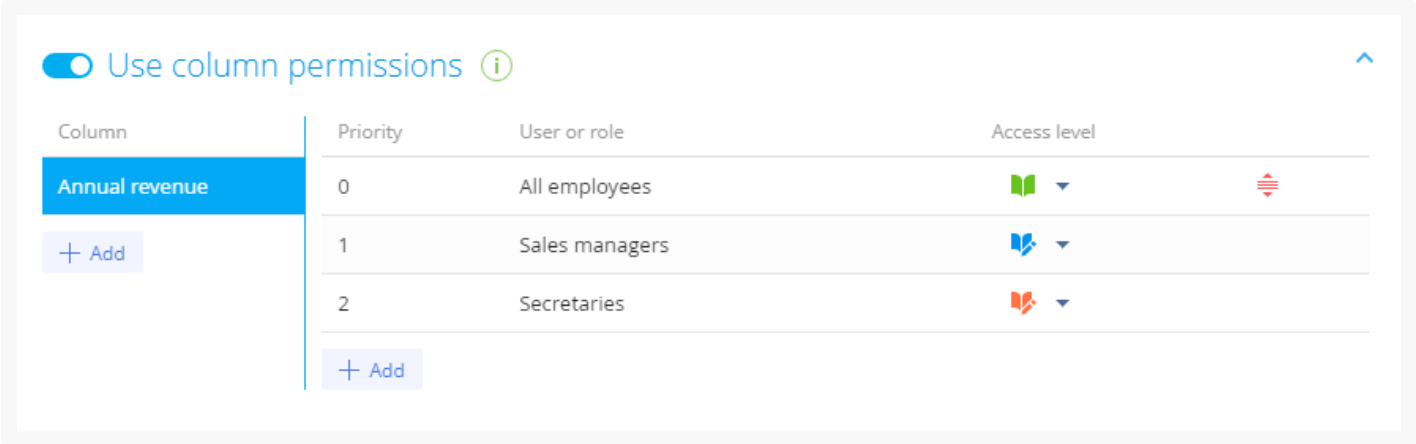
After you apply the settings, the icon can appear next to some permissions. This means the permissions are in conflict. Change their priority so that Creatio can apply the permissions correctly.

Hierarchy of column permissions

Sometimes, different access permissions applied to the same user or role can contradict each other.

For example, the “Sales Managers” and the “Secretaries” roles are included in the “All Employees” role. Sales managers have more permissions than regular employees (Fig. 4).

Fig. 4 Permission levels that contradict each other



The higher the permission is in the list, the higher the permission priority. The priority is shown in the [*Priority*] column, and the highest possible priority is “0”. An icon next to some of the rules indicates that they overlap. Lower or raise a rule in the list to ensure other rules work correctly.

Follow these rules while configuring access permission priorities:

- Object operation permissions and record permissions have higher priority.
- A user who has several roles will get the access permissions of the highest role in the list.

  For example, you can deny editing access for all employees, and grant sales managers the permissions to read and edit this field. To do this, place the “Sales managers” role higher than “All employees” in the list.
- If you want to deny column access for a role that is included in the role that has a higher permission level, place the role to deny access higher than the parent role.

  For example, to deny access to read and edit column data for all secretaries, place the “Secretaries” role higher than the “All employees” role that has permissions to read the column data in the list. In this case, Creatio will display the icon next to the “Secretaries” role.

Note. In this case, you do not need to change the priority, since the contradiction means the secretaries will be unable to view the column value, which is the intended behavior.

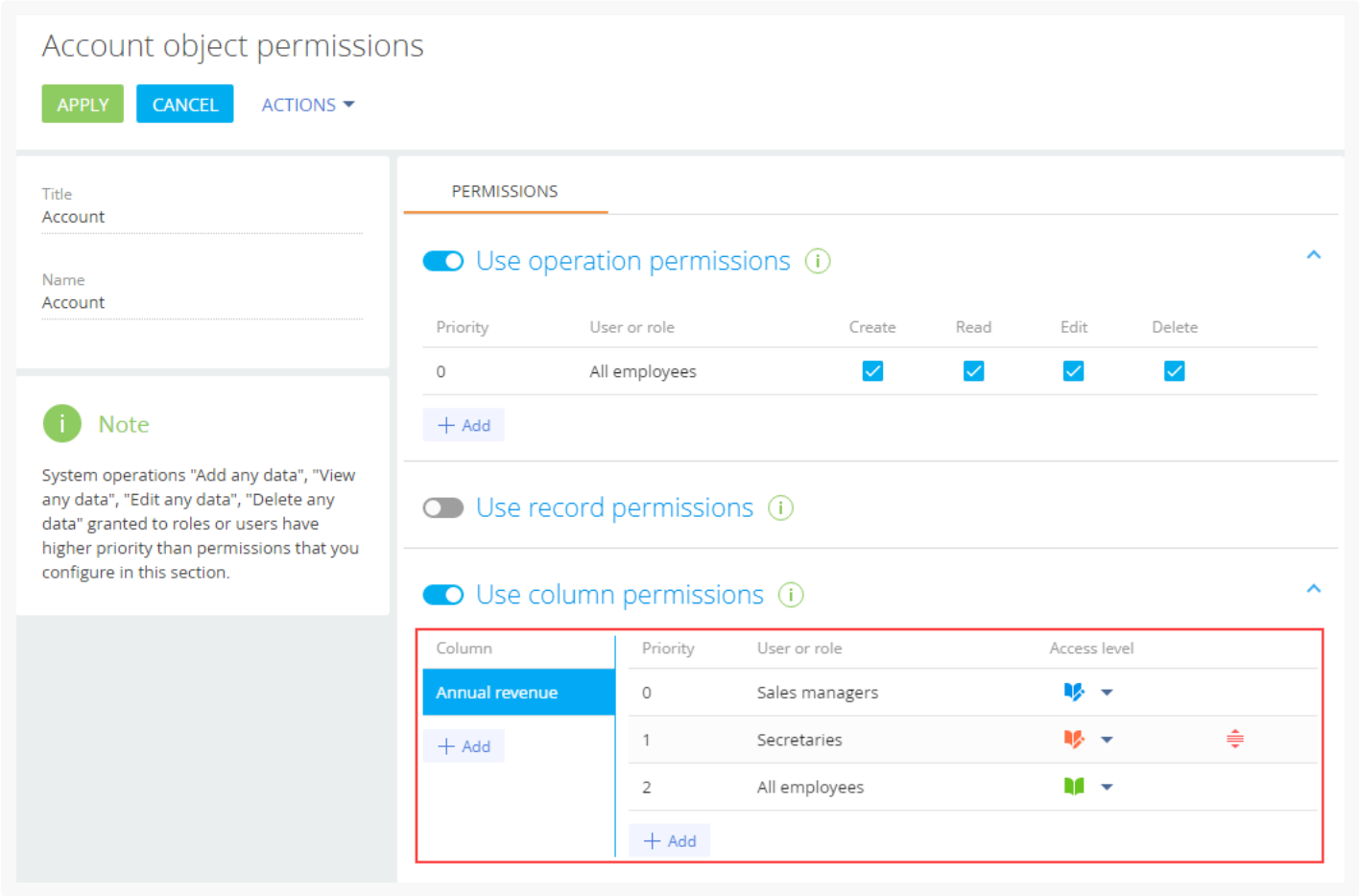
- The access permissions for users or roles that have not been added to the column permissions settings area correspond to the object operation permissions that are configured for them.

Configure access permission priorities for the example above. To change the rule display order, drag the rule to

the necessary position in the list (Fig. 5).

1. Place the organizational role that has the highest permission level (in this example, “Sales managers”) at the top of the list.
2. Place the “Secretaries” role directly below the “Sales managers” role.
3. Place the “All employees” role at the very bottom of the list.
4. Save the settings.

Fig. 5 Configure the priority of column access permissions



As a result:

- Users that are part of the “**Sales managers**” role will be able to read and edit the [*Annual revenue*] field value.
- All **secretaries** will not be able to see the [*Annual revenue*] field value on the account page.
- **All company’s employees** will be able to see the [*Annual revenue*] field value on the account page, without the ability to edit it.

Learn more in an e-learning course: [User and role management. Access permissions](#).

Record permissions

PRODUCTS: ALL CREATIO PRODUCTS

Configure object permissions on several levels:

- **Operation permissions**. Learn more in a separate article: Object operation permissions.
- **Column permissions**. Learn more in a separate article: Column permissions.
- **Record permissions**. This article explains how to configure permissions to read, edit, and delete **individual records** of a particular object.

The system administrator can manage permissions to read, edit, or delete **individual records**, as well as the ability to delegate these permissions.

To enable the record permissions, toggle on the “Use record permissions” switch in the [*Object permissions*] section of the System Designer. The permission mechanism is based on the record authorship. If the record author is a member of the role specified in the “Record author” column, Creatio will grant permissions to the receiving role specified in the “User or role who obtains permissions” column. If the receiving role is subordinate, its management role will inherit the granted permissions.

By default, Creatio grants maximum access permissions to the following users:

- The **system administrators** with permissions to the “Add any data,” “View any data,” “Edit any data,” and “Delete any data” system operations. These settings have a higher priority than the settings specified in the [*Object permissions*] section.
- The **record author** and the **management role of the author**, including the ability to delegate permissions to other users.
- The **record owner** and the **management role of the owner**, including the ability to delegate permissions to other users.

  Learn more in a separate article: Share records.

Note. If object record permissions are disabled, the records will be available to all users that have sufficient object operation permissions.

If record permissions are enabled, but there are no permission rules set up, the records will be available only to the author, the author’s management role, the record owner, the owner’s management role, as well as the system administrators.

If you are just getting started with Creatio, we recommend familiarizing yourself with the principles of Creatio object permissions in the e-learning course: User and role management, Access permissions.

Example. Configure access permissions to the [*Opportunities*] section.

If a sales associate creates a record, all employees with this organizational role must have permission to view the record with the ability to delegate this permission, as well as edit the record, but not delete it.

If a supervisor creates the record, the associates must have permission to view and edit the record without the ability to delegate these permissions. The other supervisors must have full access to the record, including the ability to delegate permissions.

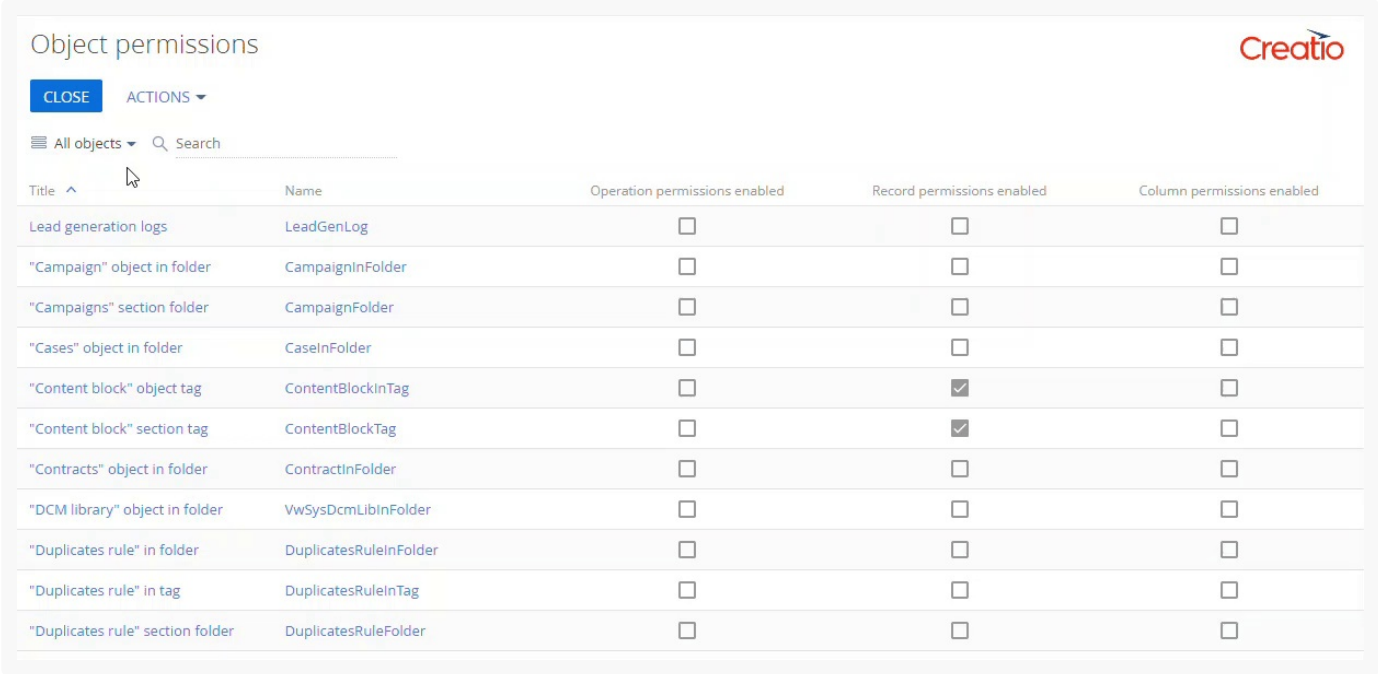
In this example, the record authors and the users who receive permissions are the members of the “Sales associates” and “Sales associates. Managers group” organizational roles.

Note. If you use a load balancer to ensure fault tolerance of your Creatio application, perform the setup on one Creatio instance, then transfer settings to other instances. The setup process applies to Marketplace apps, custom packages, and other settings that require compilation. Learn more in a separate article: Compile an app on a web farm.

1. Click the button to go to the System Designer, then open the “**Object permissions**” section.
2. Select the “Sections” filter and choose the “Opportunity” object to configure access permissions to the [*Opportunities*] section. Click the object name or title to open the permission setup page of the [*Opportunity*] object (Fig. 1).

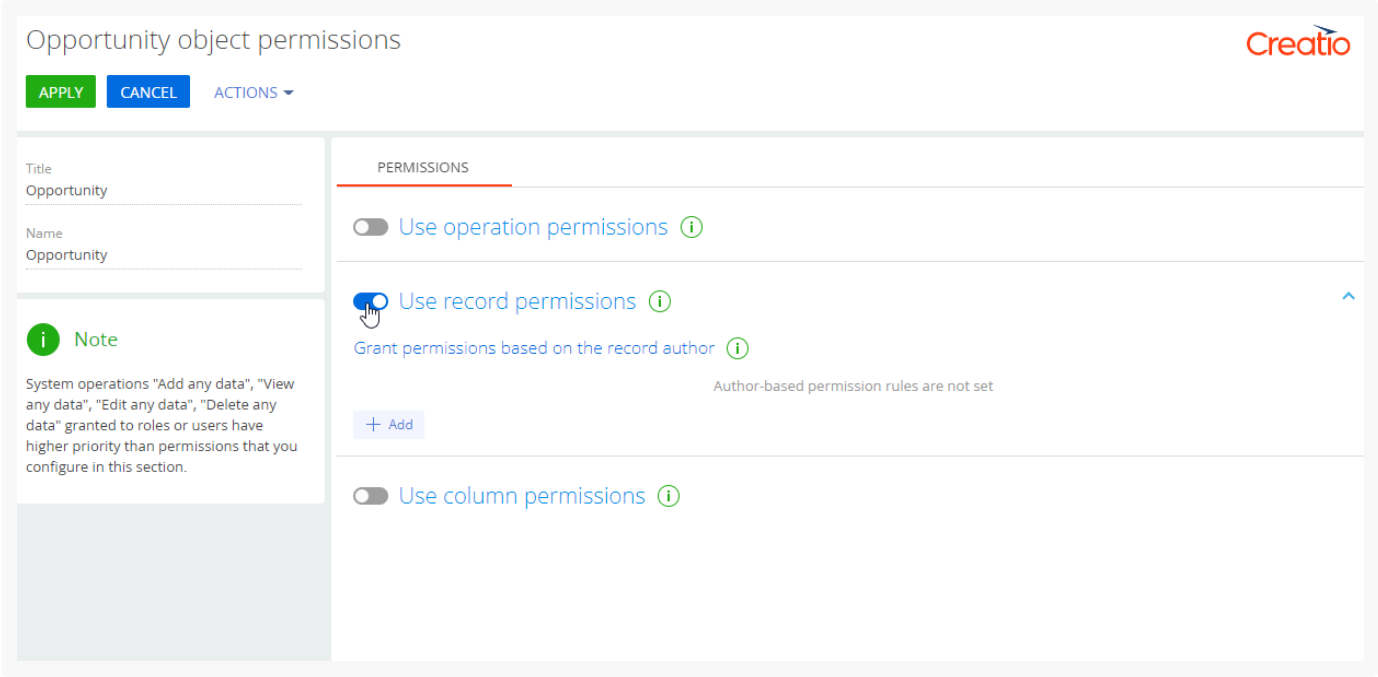
   Learn more in the e-learning course: Object permissions.

Fig. 1 Selecting the section object and opening the permission setup page



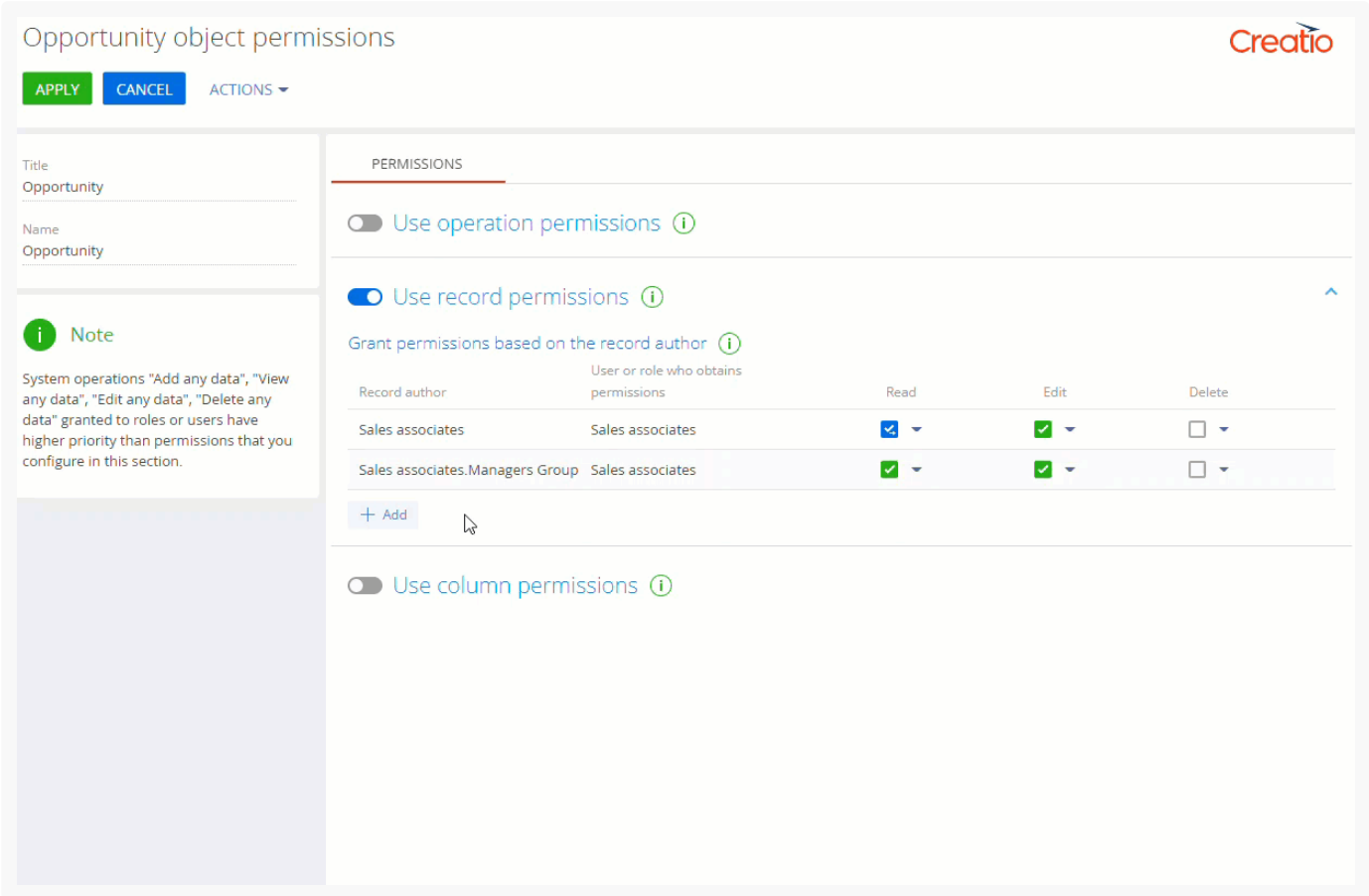
3. Toggle on the “Use record permissions” switch to enable record permissions (Fig. 2).

Fig. 2 Toggle on the record permissions



4. Click the [*Add*] button. In the box that opens, specify the record author user or role and the user or role that will receive permissions for the record. Use the search bar to quickly find the needed role or user. In this example, you need to add three records (Fig. 3).

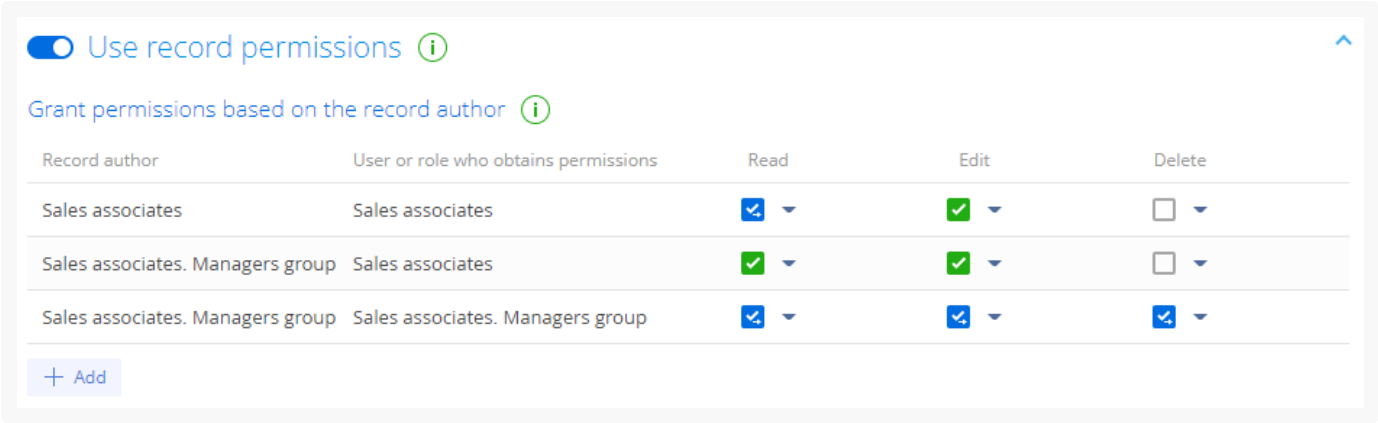
Fig. 3 Adding the record permission roles



5. Click the ☐ ▾ button and select “Granted” ✅ or “Granted with right to delegate” ☑ options in the column

that corresponds to specific permissions (read, edit or delete) for each user to determine access levels. By default, access permissions are not specified. In this example, grant the following permissions (Fig. 4):

Fig. 4 Configure the record permissions



a. Select the “Granted with right to delegate” checkbox for the “**Sales associates**” role in the [*Read*] column, and the “Granted” checkbox in the [*Edit*] column to enable sales associates to view records created by their colleagues and delegate this permission to other users, as well as edit the records, but not delete them.

b. Select the “Granted” checkbox in the [*Edit*] and [*Read*] columns for the “**Sales associates**” role to enable sales associates to view and edit records created by their managers, but not delete them.

c. Select the “Granted with right to delegate” checkbox for the “**Sales associates. Managers group**” role in the [*Read*], [*Edit*], and [*Delete*] columns of the records created by the “Sales associates. Managers group” role to allow managers to view, edit and, delete records created by their colleagues, as well as delegate these permissions.

> **Note.** Unlike object operation permissions, the order of the record permissions does not affect their priority.

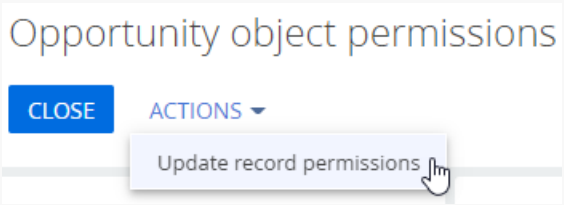
6. Click [*Apply*].

> **Attention.** If you configure access permissions for a section with existing records, you will need to run a permission update. Otherwise, the new permissions will apply only to newly created section records.

Permission update is a resource-intensive procedure. Depending on the number of section records, as well as the number of affected users and roles, the update may take 3 minutes or more and affect Creatio performance. We recommend updating record permissions when the load on Creatio is the lowest to avoid this.

Open the access permissions setup page and select “Update record permissions” in the [*Actions*] menu to apply new access permissions to existing section records (Fig. 5).

Fig. 5 Start the update of object record permissions



As a result of the update, Creatio will delete the default permissions and add new permissions. During the update, Creatio will not delete permissions you added manually to the record permission page or those configured as part of a business process.

Note. One role can have several record permissions. For example, these may be permissions you added by running the [*Update record permission*] action and obtained as part of a business process, as well as permissions you added manually and obtained as part of a business process.

Data export permissions

PRODUCTS: ALL CREATIO PRODUCTS

Grant permissions to export lists of either specific objects or all Creatio sections to roles and individual users.

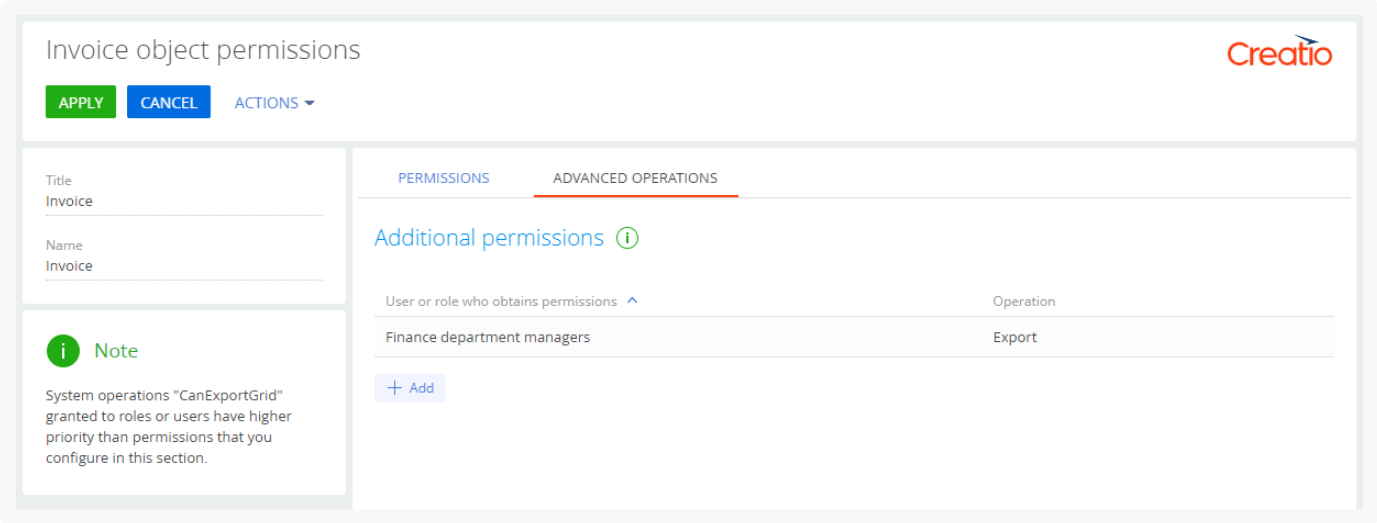
Data export permissions are a subset of Creatio object permissions. You can grant full data export permissions to some roles and users. For example, the company management. To do this, grant them permission to the “Export list records” (the “CanExportGrid” code) system operation. If the information is confidential and sensitive, we recommend setting up export permissions for specific objects. For example, grant permission to export invoices to the finance department managers.

Example. Set up permission to export only the invoice list for the “Finance department managers” role.

1. Go to the System designer. For example, click the button.
2. Go to the “Users and administration” block → “Object permissions.”
3. Find the needed section, lookup, or detail object in the Creatio object list. Apply the “Sections” filter and select the “Invoice” object.
4. Click the name or title of the object to open the permission setup page of the [*Invoices*] section object.
5. Go to the [*Advanced operations*] tab of the permission setup page.
6. Click the [*Add*] button. This will open a dialog box. Specify the role or user to whom to grant the list export permission in the box.
   a. Click in the [*User or role who obtains permissions*] field. Select the needed organizational role, functional role, or user, then click [*Select*] to confirm the action.
   b. Specify “Export” in the [*Entity operation*] field.
   c. Click the [*Add*] button to confirm the selection.
7. Repeat step 6 to grant the export permission to other roles and users, if needed.

8. Click the [*Apply*] button to save the settings (Fig. 1).

Fig. 1 Set up the list export permission



As a result, employees that have the “Finance department managers” role will be able to export only the [*Invoices*] section list. They will not be able to export other Creatio lists.

System operation permissions

PRODUCTS: ALL CREATIO PRODUCTS

Access to a number of Creatio functions cannot be managed via permissions to add, view, edit and delete data in objects. Examples of such functions are import and export operations, creating business processes, configuring workplaces, system configuration, etc. Use **system operations** to manage access to these functions. A system operation can have one of the two access levels: a user or role either have access to perform the operation, or they do not. For example, if you grant the “All employees” role permission to perform the “Export list records” system operation, all users will be able to export section list data as Excel files.

The **Operation permissions** section of the System Designer is designed for managing access to system operations. Although standard folders are not available in the list of system operations, you can use either a standard or an advanced filter to find the needed operation.

Please note that system operation permissions work in conjunction with other access permissions. For example, users can only export data, which they can access according to object permissions.

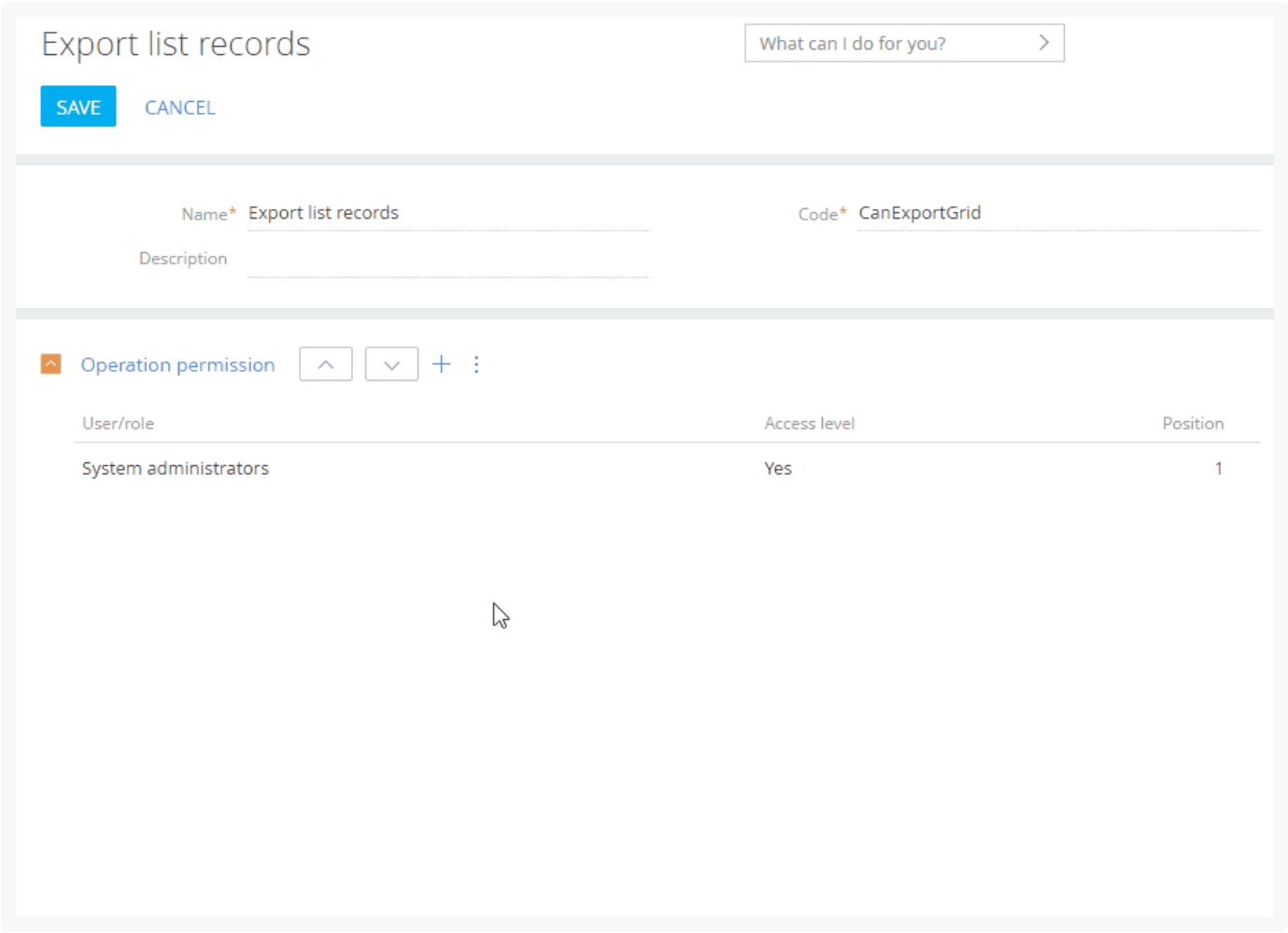
By default, only system administrators have access to key system operations. You can configure access permissions to system operations for individual users or user groups.

Case. Set up access to the [*Export to Excel*] system operation for the sales supervisors.

1. Click → System Designer → **Operation permissions**
2. Apply the “Name = Export list records” (or “Code = CanExportGrid”) filter. **Click the name of the operation** to open it.
3. Click + and specify the necessary **user/role** on the [*Operation permission*] detail. For example the “Sales

managers. Managers group” organizational role. The user/role will show up on the [*Operation permission*] detail with the “Yes” value in the “Access level” column. As a result, the “Sales managers.Managers group” role will be able to export section data to Excel (Fig. 1).

Fig. 1 Granting access permissions to a system operation



Note. To deny access permissions, click a record on the [*Operation permission*] detail and change the value in the “Access level” column to “No”. To do this, select the user or role in the list. The “Access level” column value will be displayed as a checkbox. Clear it to deny access permissions for the selected user/role. Please do not forget to save.

Sometimes a user may be assigned conflicting permissions to system operations. This may happen if the user is a member of several roles, some of which have permission to a system operation, and some are denied that permission. In order for access permissions to work correctly, make sure you properly configure their priority. Use ⌄ or ⌃ on the [*Operation permissions*] detail to change the priority of assigned operation permissions. The role that is the highest in the list will determine the actual access permissions of a user. For example, if you need to deny permission to export list records for all users except sales managers, place the “All Employees” role lower than the “Sales managers” role in the list.

Note. Users or roles that were not added to the [*Operation permission*] detail will not have access to

perform the corresponding system operation. In addition, they will not affect the permission priorities.

System operation reference

PRODUCTS: ALL CREATIO PRODUCTS

System operations to which you can manage access are described below.

User and role administration

System operation name and code	Description
Manage user list “CanManageUsers”	Permissions to add, modify and delete user accounts in the System Designer's user and role management sections.
Manage user licenses “CanManageLicUsers”	Access to the [*License manager*] section. The users that have permission to manage licenses can log into Creatio and redistribute the licenses even if Creatio has been locked due to exceeding the number of distributed licenses.
Change delegated permissions “CanChangeAdminUnitGrantedRight”	The ability to delegate the access rights of some users to others using the [*Delegate permissions*] detail on the user page.

Managing portal users

System operation name and code	Description
Manage portal users “CanAdministratePortalUsers”	Permissions to add, modify and delete portal user accounts in the System Designer's user and role management sections.
Access to portal main page setup module “CanManagePortalMainPage”	Permission to set up the portal main page.

General access

General access operations refer to all records in all objects. General access is usually provided to system administrators.

Attention. Access to these operations overrides object permissions (object operations, records and columns). For example, if a user has access to the [*View any data*] operation, this user will be able to view records of all objects, even those in which the read operation is restricted.

System operation name and code	Description
View any data “CanSelectEverything”	Permission to view any data in any object.
Add any data “CanInsertEverything”	Permission to add records to any object.
Edit any data “CanUpdateEverything”	Permissions to edit any data in any object.
Delete any data “CanDeleteEverything”	Permission to delete any records in any object.

Columns, system operations and default permissions

System operation name and code	Description
Change system operations permissions “CanChangeAdminOperationGrantee”	Ability to manage access permissions to system operations. The scope of rights granted by this operation includes the right to register additional system operations.

Access to special sections

System operation name and code	Description
Access to “Access rights” workspace “CanManageAdministration”	Access to the [*Object permissions*] and [*Operation permissions*] sections. Required for sysAdminUnit record management. Grant access to specific administering operations separately.
Access to “Process design” section “CanManageProcessDesign”	Access to the Process Designer, and the ability to add and modify business processes.
Access to “Change log” section “CanManageChangeLog”	Access to the [*Change log*] section.
Access to “System settings” section “CanManageSysSettings”	Access to the [*System settings*] section.
Access to “Lookups” section “CanManageLookups”	Access to the [*Lookups*] section.
Can manage configuration elements “CanManageSolution”	Access to the System designer's [*Configuration*] section.
View “Audit log” section “CanViewSysOperationAudit”	Permission to to view the contents of the [*Audit log*] section.
Manage “Audit log” section “CanManageSysOperationAudit”	Permission to view the contents of the [*Audit log*] section and to archive the log.

Access to duplicates search

System operation name and code	Description
Duplicates search “CanSearchDuplicates”	Permission to search for duplicates in sections with active duplicate search rules.
Duplicates processing “CanMergeDuplicates”	Permission to merge duplicate records on the duplicate search results page. Additionally, permission to merge records manually in all accessible sections and lookups.
Access to “Duplicates rules setup” “CanManageDuplicatesRules”	Permission to add and edit duplicate search rules.

Access to integration settings

System operation name and code	Description
Access to OData “CanUseODataService”	Permission to use OData protocol for external integration.

General actions

System operation name and code	Description
Email providers list setup “CanManageMailServers”	Permission to create a list of email servers used to send and receive emails.
Shared mailbox synchronization setup “CanManageSharedMailboxes”	Permission to manage shared mailboxes (mailboxes with the [*Allow shared access*] checkbox enabled).
Change access rights to record “CanChangeEntitySchemaRecordRight”	Lets users grant record permissions. The [*Use operation permissions*] switch must be toggled on in the corresponding object for record permissions to work.
Ignore access check by IP address “SuppressIPRestriction”	When a user who has access to this operation logs in to the system, the IP address restrictions will be ignored.
Export list records “CanExportGrid”	Permission to export list data in a *.xlsx file. If a user does not have permission for this operation, the [*Export to Excel*] action in sections and the “List” dashboard tile menu is disabled.
Permission to run business processes. “CanRunBusinessProcesses”	Permission to run business processes in Creatio. All users have permission to perform this operation by default.
Cancel running processes “CanCancelProcess”	Permission to cancel a running business process in the process log.
Access to workplace setup “CanManageWorkplaceSettings”	Permission to create and set up workplaces, i. e., managing the section list available in the side panel.
Access to comments “CanEditOrDeleteComment”	Permission to edit and delete comments on the feed messages.
Permission to delete messages and comments “CanDeleteAllMessageComment”	Permission to delete messages and comments left by other users in the [*Feed*] section, on the [*Feed*] tab of the Notification Panel, and on the [*Feed*] tab of the view and edit pages of system sections. Users can edit and delete their own messages and comments even if they do not have access permissions to this system operation.

Delegate permissions

PRODUCTS: ALL CREATIO PRODUCTS

The functionality of delegating permissions enables granting all access permissions of a user to another user for a limited time. This is useful when, for example, an employee is out of the office or otherwise unavailable and someone should take over their duties. You can delegate permissions of individual users or roles to any number of other users or roles.

To delegate permissions, a user must have access to the “**Manage user list**” (CanManageUsers) and “**Change delegated permissions**” (CanChangeAdminUnitGrantedRight) system operations.

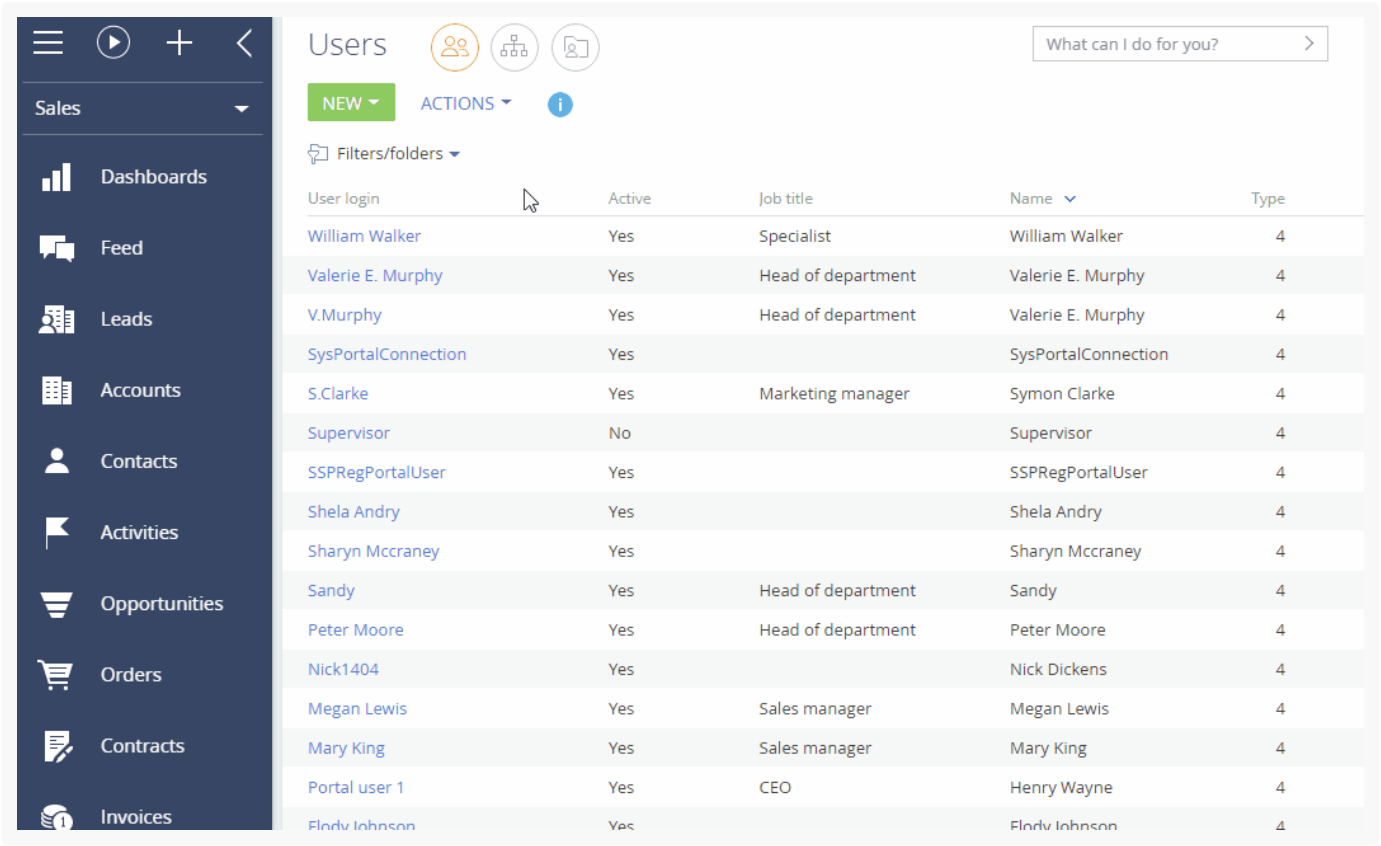
Delegate permissions of a user to other users and roles

To delegate user permissions to another employee or employee group:

1. Click → [***System users***].
2. Open the user page, **whose permissions you want to delegate**.
3. Click [***Rights delegation***] → [***Delegate permissions***].
4. In the opened window, select the user or employee group that **will receive the delegated permissions**, e.g., the “Accounting department” organizational role.
5. Click [***Select***]. Click [***Close***] on the user page.
6. Click [***Actions***] → [***Update roles***] to apply the changes.

   As a result, the users and roles who received the permissions will be displayed in the [***Who receives permissions***] column, and the user/role, whose permissions were delegated, will be displayed in the [***Who grants permissions***] column on the [***Access rights delegation***] detail (Fig. 1).

Fig. 1 Delegating permissions of a user to another user/employee group



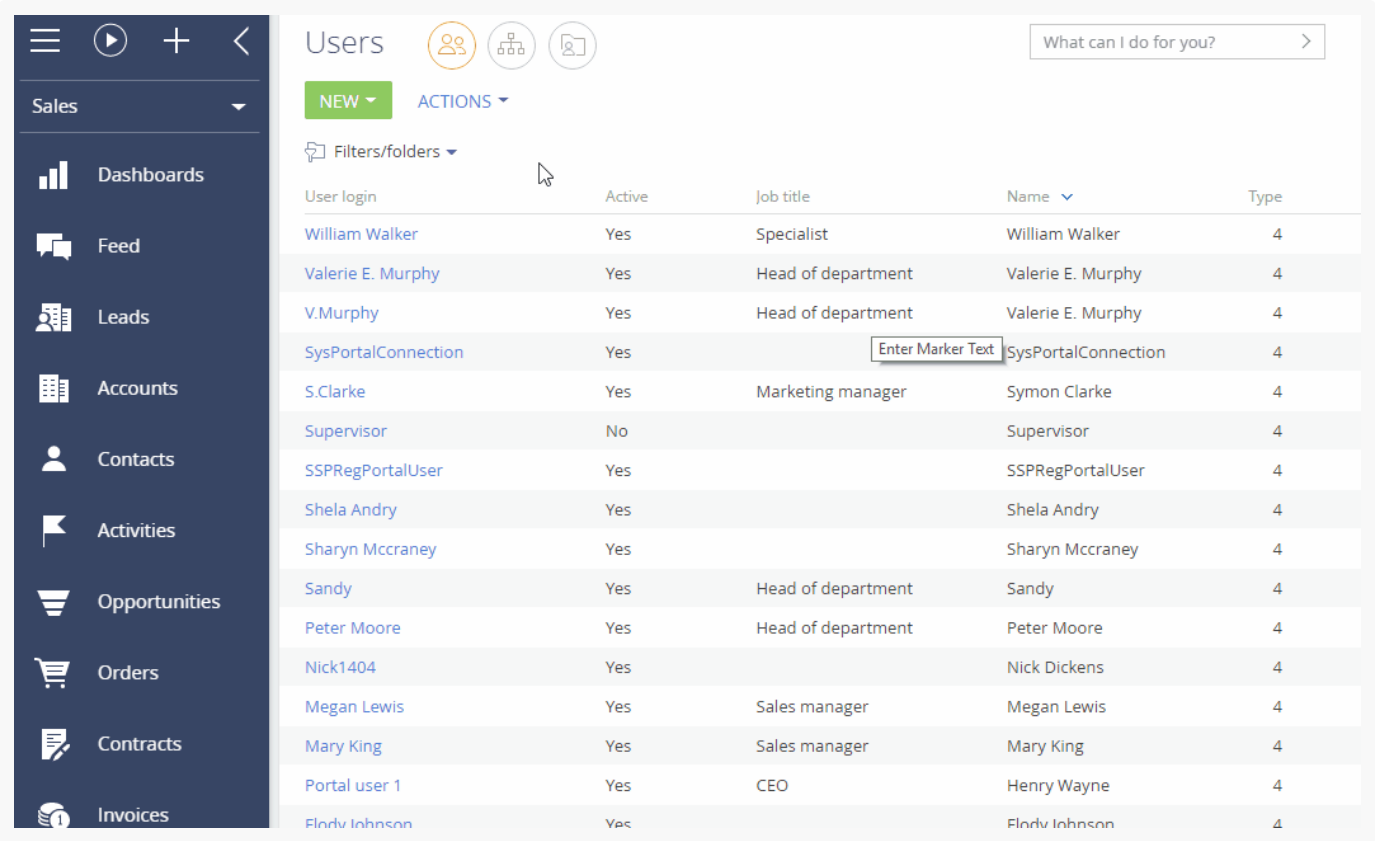
Delegate permissions of other users and roles to a user

To delegate permissions of other users and roles to a user:

1. Click → [***System users***].
2. Open the page of a user, who **will receive the delegated permissions**.
3. Click [***Rights delegation***] → [***Get permissions***].
4. In the opened window, select the user or role whose **permissions must be delegated** to the current user, e.g., the “Accounting department” organizational role.
5. Click [***Select***]. Click [***Close***] on the user page.
6. Click [***Actions***] → [***Update roles***] to apply the changes.

   As a result, the user who received the permissions will be displayed in the [***Who receives permissions***] column, and the user/role, whose permissions were delegated, will be displayed in the [***Who grants permissions***] column on the [***Access rights delegation***] detail (Fig. 1).

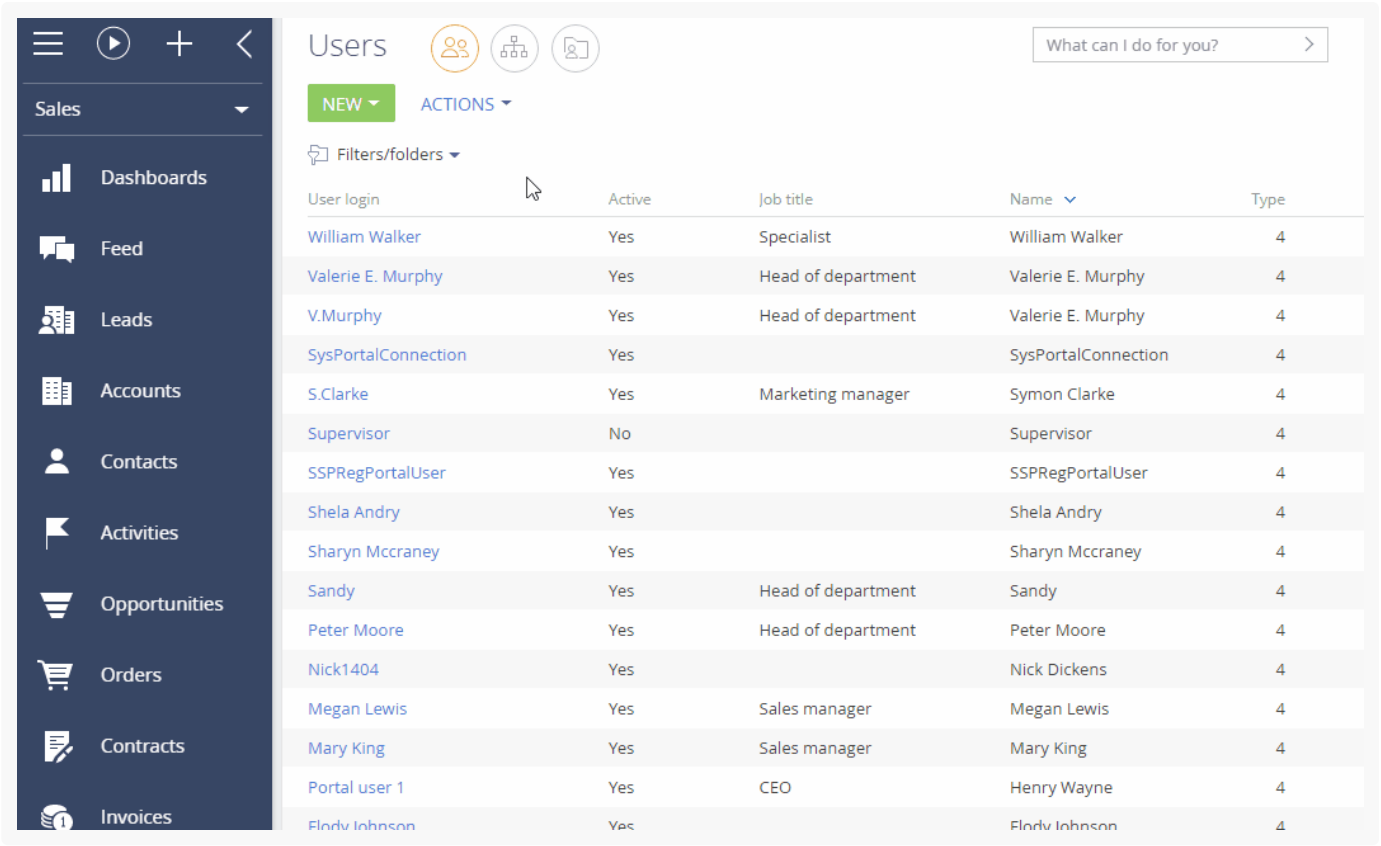
Fig. 1 Delegating permissions of an alternative user/employee group to the current user



Remove the delegated user permissions

1. Click → [***System users***].
2. Open the page of the user, whose **delegated permissions you want to remove**.
3. Open the [***Rights delegation***] tab, **click the record** you want to delete.
4. Click ⋮ → “Delete” (Fig. 1). **Close the user page**.
5. Click [***Actions***] → [***Update roles***] to apply the changes.

Fig. 1 Removing the delegated permissions



As a result, the delegated permissions will be deleted. The user will only have the initially assigned permissions.