Creatio Academy

Access management

Column permissions

Version 8.0

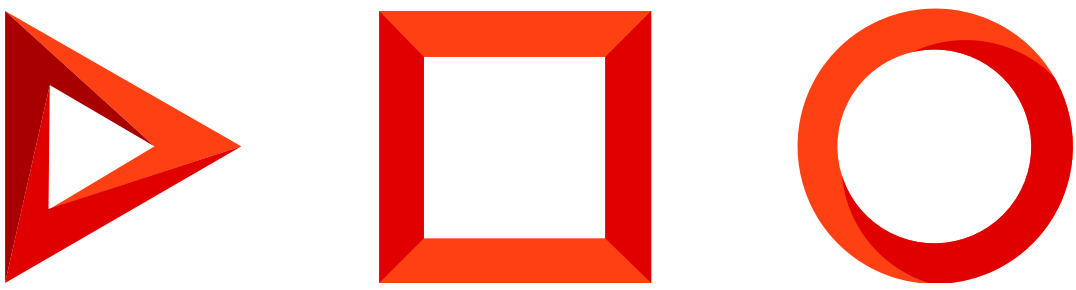


Table of Contents

Column permissions

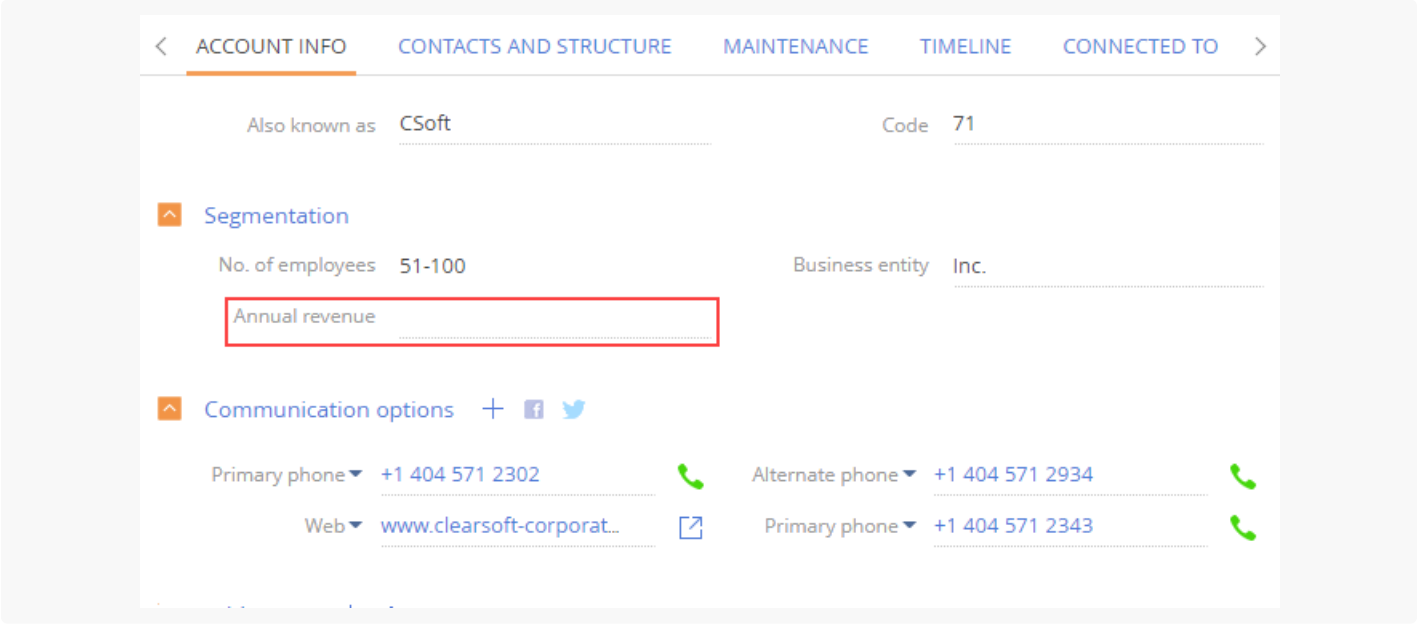
PRODUCTS: ALL CREATIO PRODUCTS

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 the object that uses column permissions, the users, except for system administrators, cannot access the new column by default. Set up permissions for each custom column that you add after enabling column permissions in an object.

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

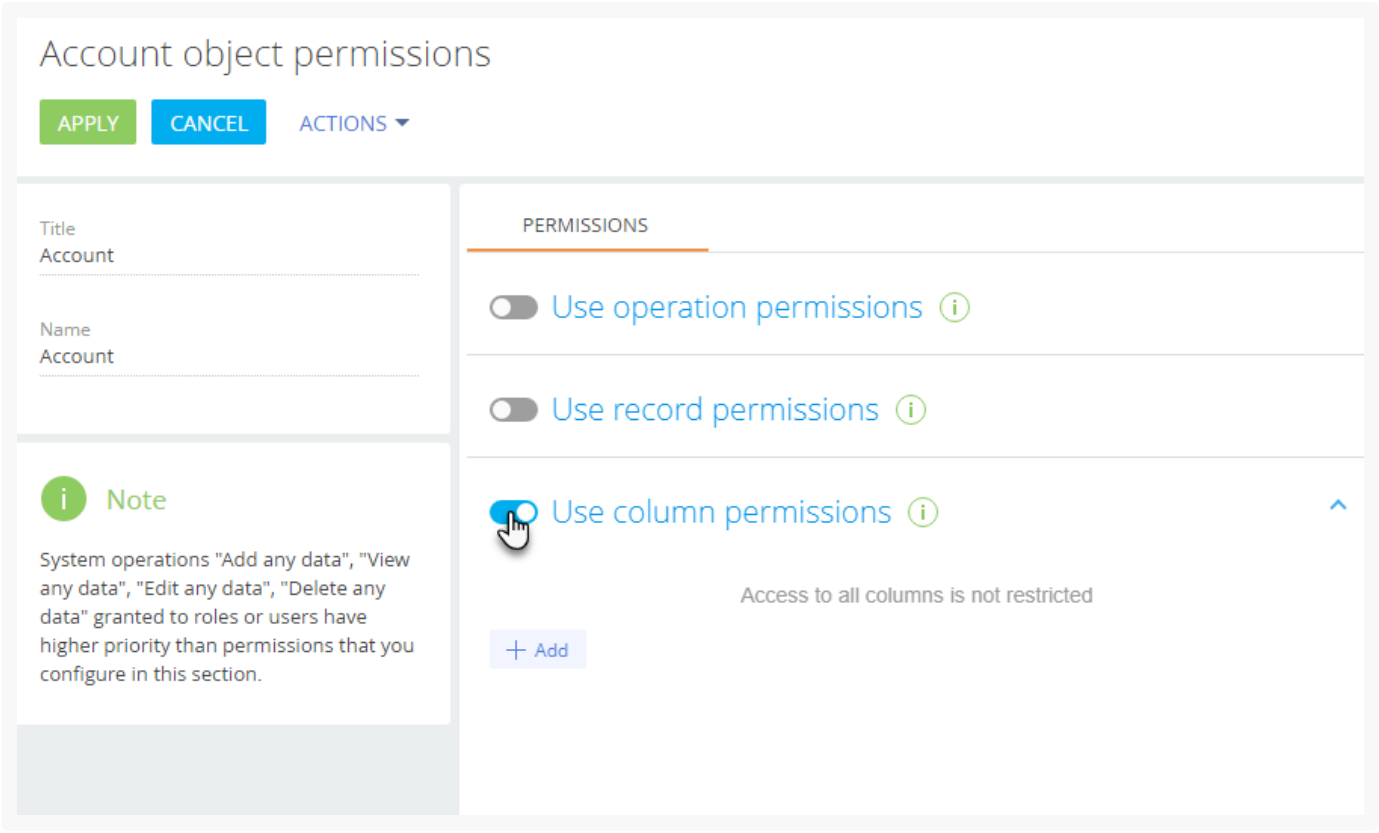
This section covers how to grant or limit access permissions to read and edit data of a particular section record field.

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).

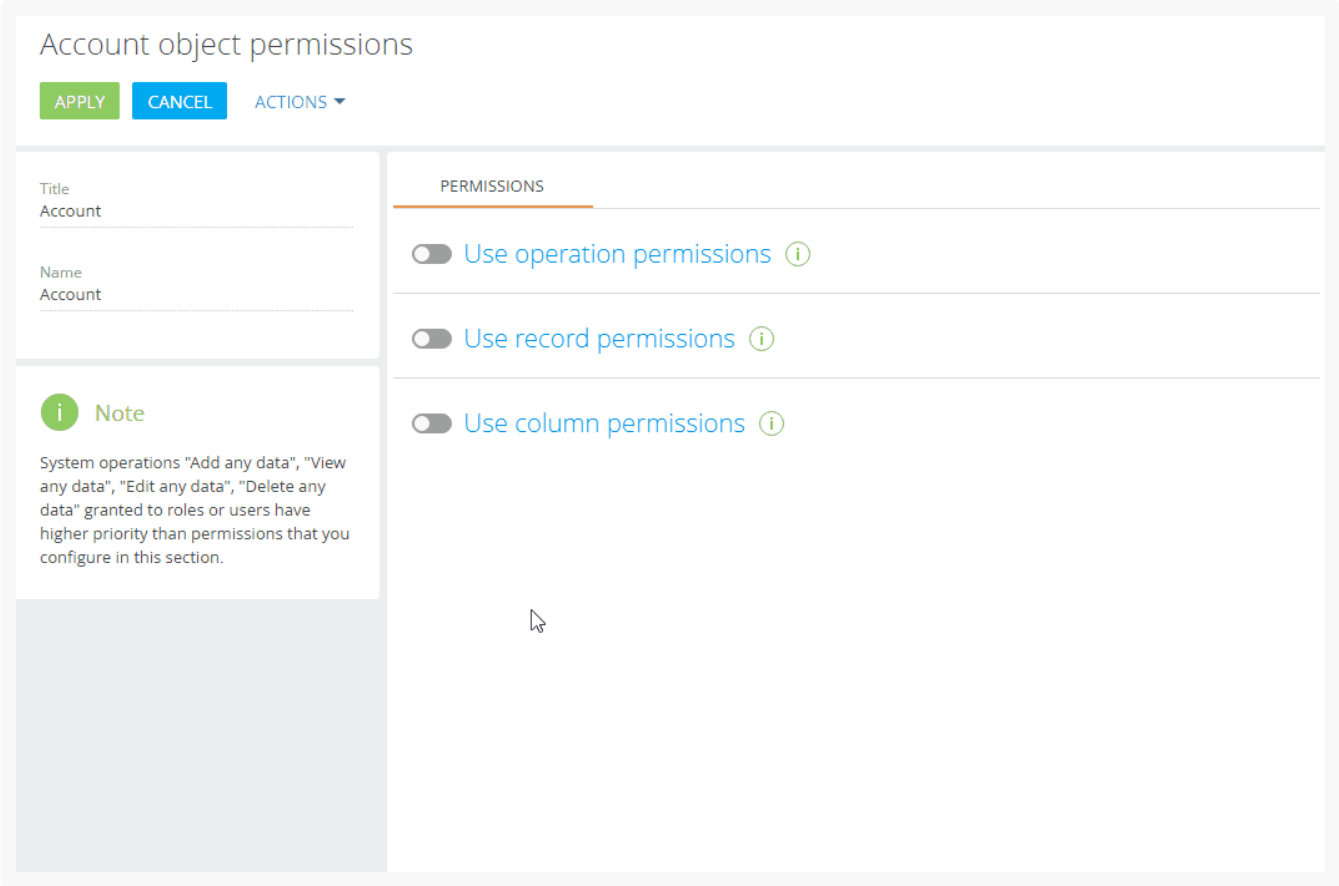
Fig. 2 Enable the column permissions



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.

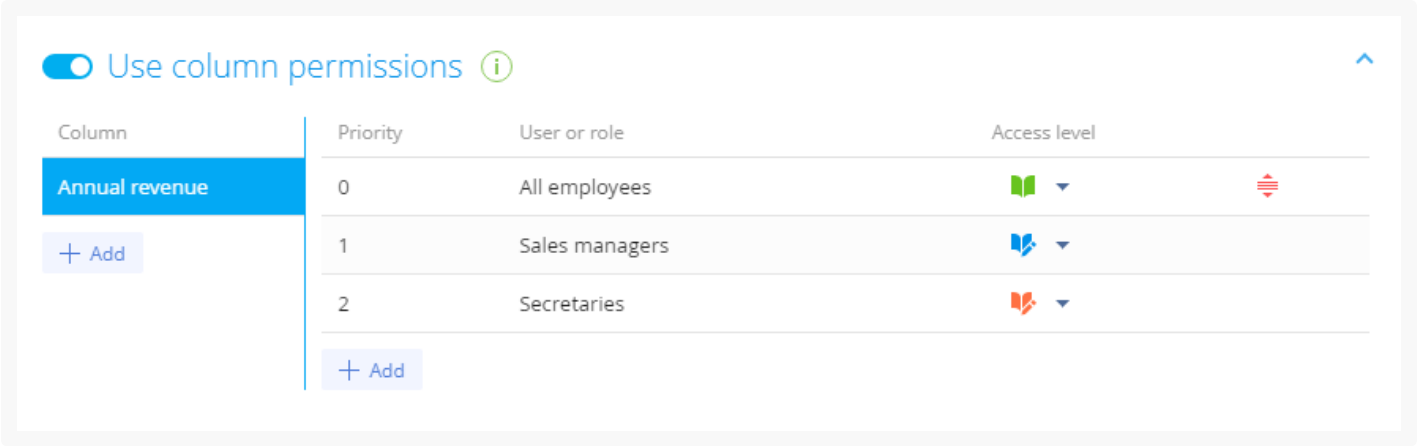
After you apply the settings, the icon can appear next to some permissions. This means the permissions are in conflict. Change their priority so that Creatio can apply the permissions correctly.

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.

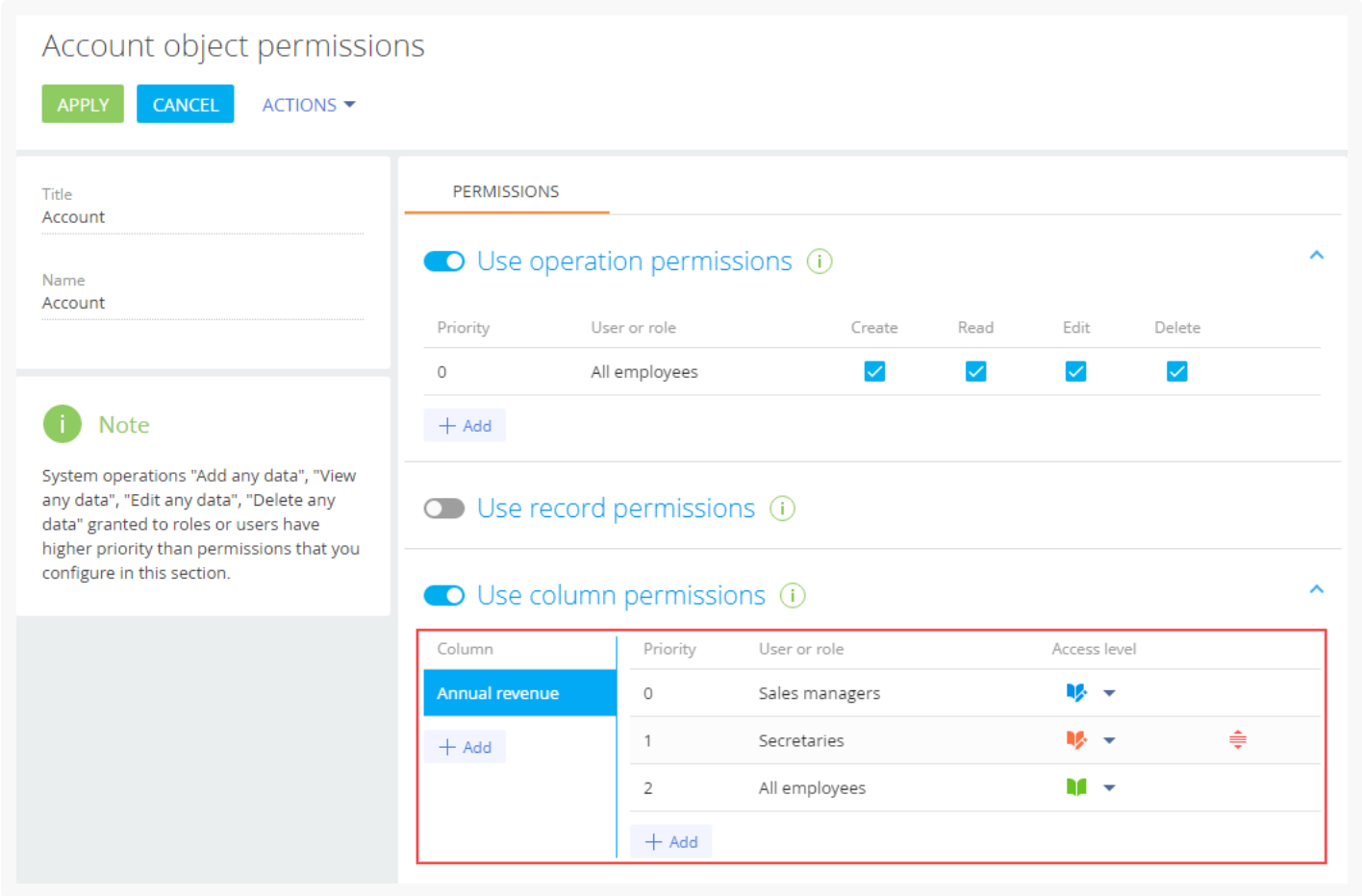
Note. In this case, you do not need to change the priority, since the contradiction means the secretaries will be unable to view the column value, which is the intended behavior.

- 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.