

Change access rights

[Change access rights] process element

Version 8.0



This documentation is provided under restrictions on use and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this documentation, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Table of Contents

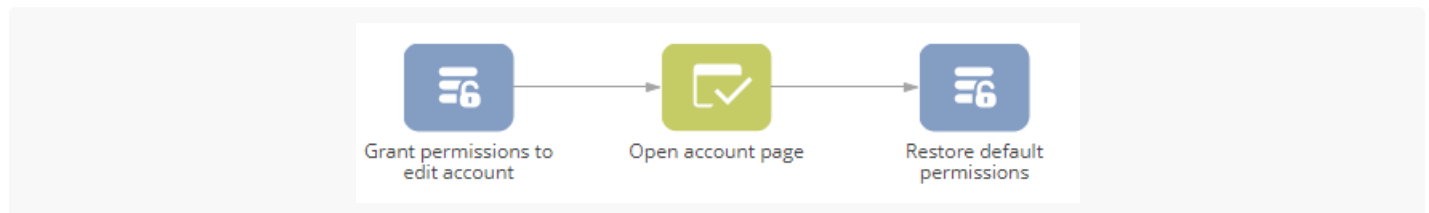
[Change access rights] process element	4
Set up the properties of the Change access rights element	4
Use examples	6

[Change access rights] process element

PRODUCTS: ALL CREATIO PRODUCTS

The [*Change access rights*] element (Fig. 1) is designed to grant or deny permissions to Creatio records.

Fig. 1 [*Change access rights*] elements on a process diagram



Use this element to automate distribution of access permissions for employees, for instance, when an account owner changes.

This element is also used for setting access permissions required for performing a user action in a business process flow. For example, before an [*Open edit page*] action can be performed, a user must be granted access to view the record whose page will open.

Attention. If a user, who is supposed to perform a process action does not have access permissions required to perform that action, the corresponding process task will not be able to complete. Correspondingly, if the completion of this task is required for the process completion, the business process will not be able to complete as well.

Permissions can be granted or revoked:

- [*For a user role*] - revokes permissions for a selected organizational structure element.
- [*For an employee*] - revokes permissions for a specific user. To ensure the correct element operation, specify the contact of the user whose permissions you would like to revoke.
- [*For selected employees*] - revokes permissions for all users who fit the filtering conditions.

When **activated**, the [*Change access rights*] element uses a filter to obtain a list of records in the specified object, then grants or revokes permissions to the specified users or roles.

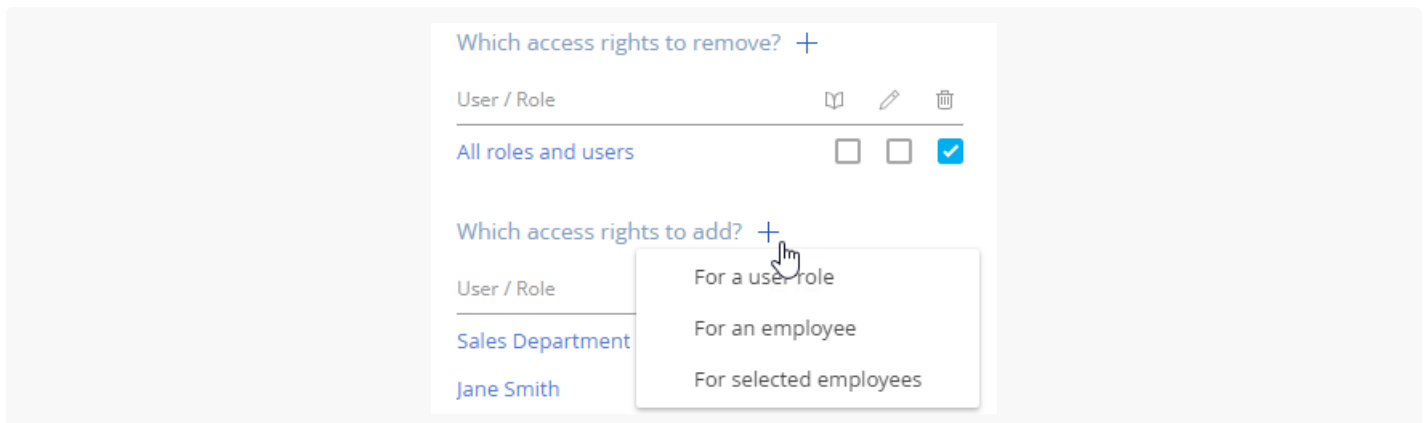
The element completes its operation and activates its outgoing flows after the corresponding permissions have been **updated**.

Set up the properties of the [*Change access rights*] element




Which object to apply access rights to?	The object that contains records for which the permissions must be updated. For example, to change access permissions to specific activities, select the “Activity” object, to change permissions to certain accounts, select “Account”, etc.
Apply access rights to all records that match conditions	Set up a filter to select records whose permissions must be modified. To change permissions for a specific record, set up a filter by the [<i>Id</i>] column.
Which access rights to remove?	Specify access permissions that will be revoked on the element’s execution. Click [+] to add a new permission. On the element execution, the specified permissions will be revoked for the specified users and roles.
Which access rights to add?	Specify access permissions that will be granted on the element’s execution. Click [+] (Fig. 2) to add a new permission. On the element execution, the specified permissions will be granted for the specified users and roles.

An “access permission” in Creatio implies a certain level of access for a certain user or role to perform certain operations with a record. You can set access permissions for specific users (“**employees**”) or user groups (“**roles**”).

Fig. 2 Adding access permissions

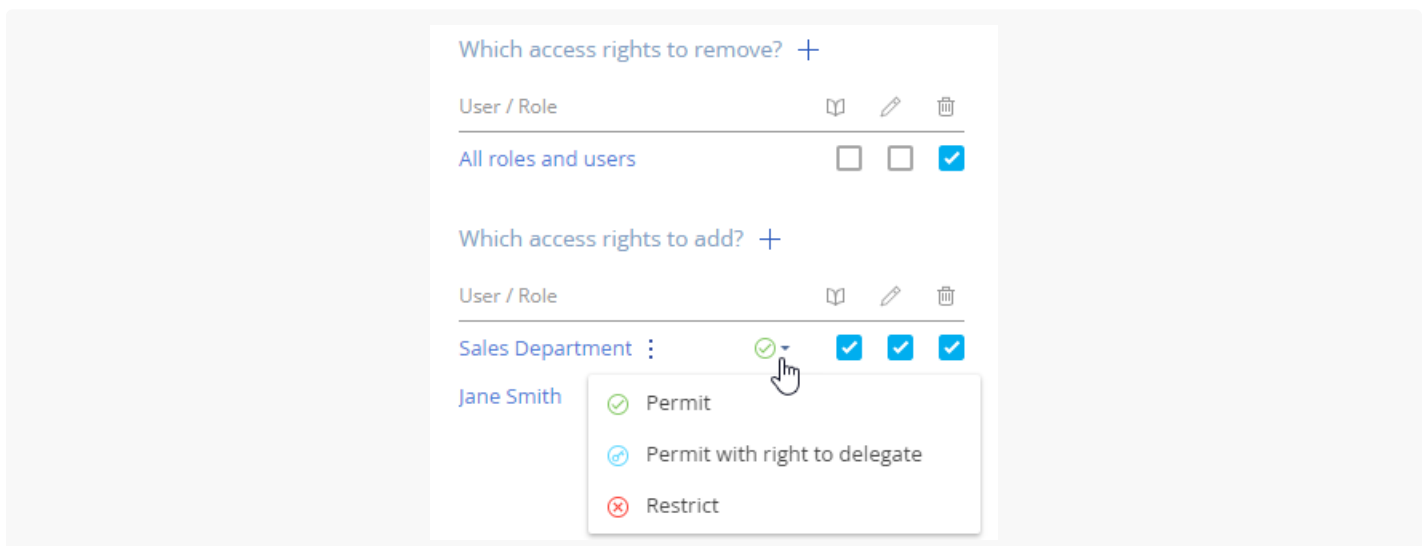




You can set access permissions for the following **operations**:

 Read	<p>Enables viewing the record, without the ability to modify or delete them. Without a permission to view a record, a user is unable to see the record or the values of the record's fields in the list or on a page. The read permission is required to open a record in a record page.</p>
 Edit	<p>Enables populating and modifying a record's field values. The user must have a "read" permission to the record as well, since without one they won't be able to open it for editing. Both permissions are required if the user needs to edit records.</p>
 Delete	<p>Enables deleting records. The user must have a "read" permission to the record as well, since without one they won't be able to select it for deleting. Both permissions are required if the user needs to delete records.</p>

When granting permissions to the mentioned operations, you can also select the **level of access** (Fig. 3):

Fig. 3 Selecting the level of access



-  [*Permit with rights to delegate*] - the user has access to perform the operation with the records, as well as grant access to same operations with the same records to other users.
-  [*Restrict*] - the user is denied access to perform the operation with the records.

Use examples

- [Manage access permissions with business processes](#)