

Access management

System operation permissions

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

System operation permissions

4

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

Export list records

SAVE
CANCEL

Name*
Code*

Description

+ Operation permission

| User/role | Access level | Position |
|-----------------------|--------------|----------|
| System administrators | Yes | 1 |

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.