

Data restrictions

Understanding permissions

Data access is restricted in two ways

- **Mandatory** permissions granting access to
 - Certain groups of fields (blocks)
 - Records in certain status
- **Optional** filters binding certain data to certain users
 - Owner user (the user that created the record)
 - List of users (dynamic list of users for each record)
 - Per group (group property)

If a user has no active permissions, they will not have any kind of access to the solution. Filters on the other hand is just considered to be additional restrictions, limiting the access granted by permissions.

In both cases the security restrictions always apply, even during system access, API interaction, integration etc.

Permissions [mandatory]

Permissions to solutions are granted as a sum of multiple permissions.

Each permission contains

- Group
- 0-1 Status (records have status)
- 0-1 Blocks (fields belong to blocks)
- Allow read
- Allow write

Permissions stack in an aggregate like manner, allowing to build complex structures from different fragments. This is also the reason that the Allow read and Allow write properties can be set to empty values (typically for generic permissions).

Differentiated FIELD level access

Fields belong to blocks. Permissions may be bound to such a block.

A permission with a block specified will ONLY apply to the fields belonging to this block.

Differentiated STATE level access

Permissions may be bound to a certain status.

A permission with a status specified will ONLY apply to records in this status.

Filters [optional]

All ownership options can be overridden by belonging to a certain group, that ignores all types of filters (3 below).

Access to configuration:

Designer > [solution] > Security - Filters

Ownership by data exclusive group

Designer attribute: Use Exclusive groups for access control

The solution contains a **Exclusive group** that defines a group with access to this piece of data.

- Scope: Group
- Cardinality: One

Ownership by data member lists

Designer attribute: Use Lists of members for each item

The solution contains a **memberlist** field where users can have their access added or removed. Behind the scenes a table with a relation between the record and the user is maintained.

- Scope: User
- Cardinality: Many

Ownership by being the creator

Designer attribute: Use Creator only restriction (ignore group recommended)

You must have created this record in order to see access it.

- Scope: User
- Cardinality: One

Revision #1

Created 3 April 2025 13:18:33 by Theis Villumsen

Updated 7 April 2025 14:20:57 by Theis Villumsen