# *Object Permission*

iQ-BASIS provides an extensive permissions concept named form permissions. It can be used to define, if a user who is currently logged in can edit, view or even not access at all the data within the context of a specific form because of a membership in one or multiple permissions groups. However, this context does still not provide a solution for the requirement if a user may edit or view specific objects but possibly not any other objects.

The iT-OBJEKTE module allows extending the permissions concepts to the data level to find solutions for even complex permission requirements in conjunction with the form permissions.

**Workflow**

Object permissions center the object. The object is a record from an iQ-BASIS data table that has been activated for the object permissions system. The system is defined using a so called object model that groups the data within this table according to a specific criterion. The criterion is expressed by an object number. In many situations the object number is equal to the plant ID to specify that the object belongs to a specific plant.

The object permission refers to the object number. To establish a relation to the active user, the system is configured with person groups that have specific permissions for each of the object numbers. When accessing an object for editing or viewing purposes, the system will check if the user belongs to a configured person group for the object number stored within the object to find out if the record should be editable for the user or perhaps even not displayed at all. Because it is possible to specify any number of person groups for each object number and equip the group with different permissions any kind of permissions concept should be implementable.

In practice, this means that a concrete object number needs to be assigned and stored in each record of a table with activated object permissions at the end of the creation of the record. If the object is not assigned to any object number then it would be accessible for everybody (i. e. public)! If a user has access to multiple object numbers then the system will prompt for selecting one of those numbers manually when storing a new record ensuring a correct data handling in this situation, too.

**Important Features at a Glance**

*Definition*

*Model*
- It is possible to define models for almost any iQ-BASIS table.

*Object numbers*
- Generally it is possible to choose any form of grouping (such as a separation of plants or a functional separation).
- The definition of standard models such as when implementing a plant separation is supported by automatic functions.

*Person groups*
- Possible person groups are: plant (any cost centers, any persons of a plant), cost centre (any persons of a cost centre), person group (any contained persons), single persons.
- It is possible to automatically take over a specific person group with its defined permissions into any defined object numbers.

*Permissions*
- The different kinds of permission levels are (with an increasing significance): view, change, add, change object number and delete.
- When defining a person group it is mandatory to specify one of these levels.
- The user gets the highest permission if he or she belongs to multiple person groups defined for the object number.

- More significant permissions contain less significant permissions.

*Application*

*Specifying the object number*
- Processes that create data in the background can assign object numbers automatically.
- If a record is created manually then the object number will be assigned automatically if the user is member of exactly one person group for the object.
- If the user belongs to multiple person groups the suitable object number needs to be assigned manually.
- For creating new objects it is necessary to own the add permission.
- If an object should be reassigned to a new object number (for example because it becomes property of a different plant) then the user will need the change object number permission for the old and the new object number as well.
- The permission of changing object numbers can be refined by additionally setting form permissions on the form that is used for changing the number.

*Checking permissions*
- The permissions are checked whenever reading a record from a table with active object permissions.
- If the result of the check is that the user does not belong to a person group assigned to the object number then displaying the record will be suppressed with a corresponding message.

- If the result of the check is that the user belongs to one or multiple person groups then the most signifi- cant permission is determined and applied to the record or the table.
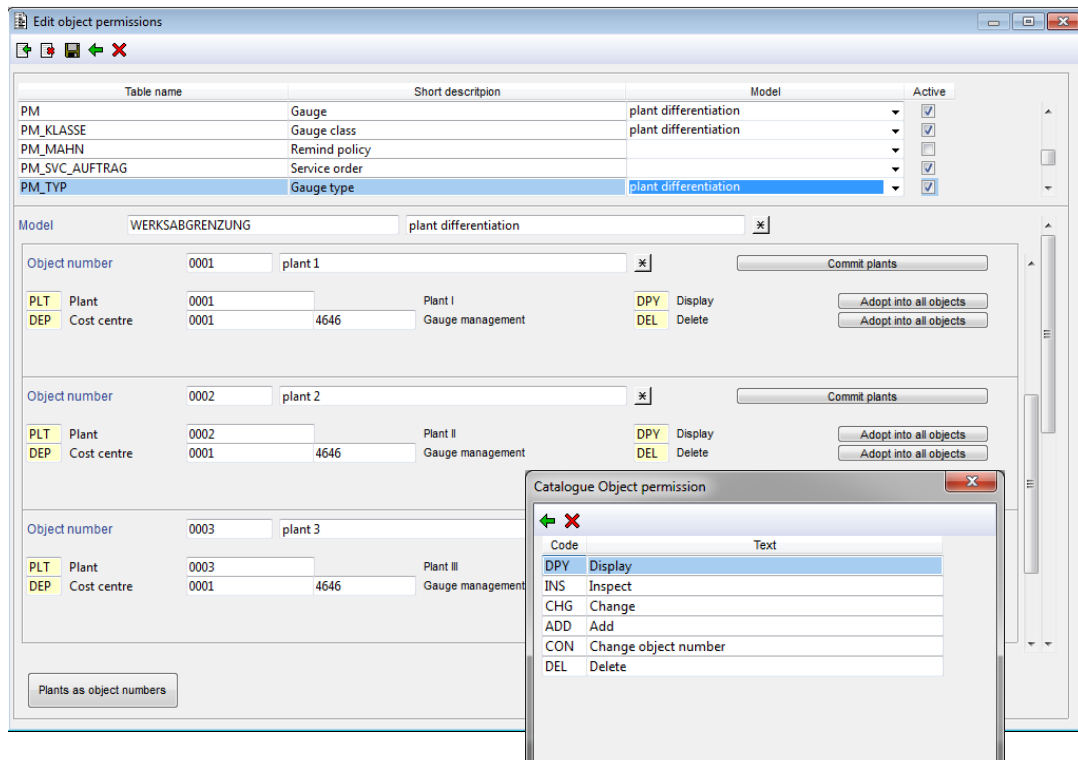


## Interfaces to Other Modules

- *iQ-KONFIG* for managing users and permissions as well as other administrative data
- *iQ-GL* for centrally maintaining master data relevant in any existing modules