Data Access Control

From 3.4.2

*f*Series includes facilities for detailed control over the data gathered, down to row and field level, based on roles and rules. This allows for Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) to be implemented when gathering data.

How It Works

When *f*Series gathers data, as each data group is gathered, *f*Series Data Access Control (DAC) checks against rules set for the data group in the DSD. DAC applies each rule and either clears corresponding field values or removes rows accordingly. Several rules may be set for a data group and all will be checked and applied.

DAC restricts fields and rows in a data group based on either the user's data access role (established at login) or any condition expressed as an *f*Series function, or a combination of both. The function is evaluated immediately after the base data is gathered and any data items have been calculated, so that the condition may be based on values in the row.

Here are some examples of conditions that may be applied:

- Remove all restricted clients from a list for users who have a role of “Admin”
- Clear the date of birth and age of clients who are over 18 years old
- Clear the name fields if the client is aged under 18 and the user's role is “Adults”.

Access Roles

A user's access roles are different from their *f*Series roles. Access roles are specified by the system administrator. Each role is defined by a simple text or numeric code (e.g. “Adults”).

Establishing a user's access roles is done at log in. A feature of *f*Series authentication is the ability to record information about the user that may then be used later in the system. A designated value (default “AccessRoles”) in the user data is used to store the user's access roles.

So in the security DSD, the data group designated as containing the user defined values must have a field containing the logged in user's roles as a comma separated list. The name of the field may be specified in the *f*Admin Settings Data Access Control section if it is not “AccessRoles”.

Setting the Conditions

One of the options in *f*Data for setting up a data group is "Access Control". This is where the conditions are set. Each condition is either the id of an access role or an *f*Series function. A description may also be recorded for each as a note of the purpose of the condition.

There are two types of conditions: those that apply to field restrictions and those that apply to the entire row. If you check the "Apply to row" option, the entire row will be removed if the condition applies. Otherwise select the fields from the list provided to clear the value of the selected fields if the condition applies.

A further option (Apply All Restrictions, at the top of the form) lets you specify a function that if true enforced all conditions to be treated as true. The purpose is to provide a failsafe option. A further "Apply All" option in *f*Admin settings that imposes a similar failsafe to all access control settings in all DSDs. In both cases the function is evaluated at the same time as the conditions and if true, all condition are deemed to be true.

The effect is that all fields specified in any conditions are cleared and if any condition is marked as "Apply to row" all rows will be cleared! An example of a function that could be used here is "=HasNoAccessRoles()". If there has been a failure in gathering access roles then this will fall back on applying all conditions and preventing inappropriate inclusion of any restricted data.

*f*Admin Settings

The following settings apply to Data Access Control.

DataAccessControl – switches access control on and off

DACApplyAll – a function which if evaluated to true enforces all condition to evaluate as true as a failsafe

DACRolesDSD – a DSD that contains a list of available access rules that may be selected when setting up a data group. Must have a "Roles" data group with Id and Description fields.

DACRolesField – the name of the user defined values field captured at login that contain a comma separated list of the user's access roles. Default is "AccessRoles".