fSeries Safety

The main purpose of fSeries is to get your data from wherever it is and deliver it to whomever needs it in the most appropriate format. Inevitably that requires assurance that the whole process is safe in terms of who gets to see what.

There are four elements to the safety of data in fSeries: User Access, Data Security, Output Generation and Audit of Activity

In each area fSeries provides a flexible range of tools to protect your data to the level you require.

User Access

There are three ways to secure access to the system itself.

- External Authentication Service
  - Azure B2C
  - Azure AD
  - Auth0
- Active Directory
  - Based on membership of designated group
- User Id / Password
  - Backup to AD
  - Two factor authentication available

fSeries maintains a record of individual users and their roles. Users are only permitted to enter if they are a current valid user with appropriate roles registered in fSeries.

Data Security

Data is secured at the point at which it is gathered (not just in the output). There are a number of mechanisms that protect the data.

Data Group Exclusion

Each data group (table within a set of gathered data) may be “switched off” based on a wide range of conditions such as the user’s access roles, or the content of another data group (e.g. permissions from the client’s record).

Filtered Rows

Conditional filters may be applied using any data gathered including values on the row itself. For example, if the subject is under 18 or is restrtcited, and the user does not have the appropriate access role.

Abandon Checks

Perform a test during the gathering process and stop all further gathering. For example, if the first data group gets the current user’s details and some aspect indicates that they should not have access to other data, all further data gathering is cancelled.

Data Access Control

Hide rows and / or fields, such as someone’s confidential address, based on conditions or access roles. Provides for detailed RBAC and ABAC security.

Output Generation

Access to outputs (documents, spreadsheets and dashboards) is through links in menus, dashboards or directly via a URL. Outputs can be secured in a number of ways.

Disabling Links

Menu items and dashboard commands can be conditionally disabled or hidden based on data in the output, such as user access roles or their user group.

Access Roles

User access roles are codes (set up by your administrator) that defined user's access (e.g. Manager, Adoption). A user may have many access roles. Each output's definition includes a list of the access roles that are permitted access to the output (or none for open access). If the current user does not have one of the permitted access roles, the system behaves as if the output dies not exists, preventing access to it.

Permission Sets

A permission set is a collection of entities (outputs, menus and even data set definitions – DSDs) that are considered as a set for the purpose of granting permission to access. This may be a collection of documents covering a particular area of operation, or a set of management reports.

Users may be organised into groups and further in to teams. Access to permission sets may then be granted to groups and teams.

Individual Permissions

For particularly sensitive output you can apply permissions by individual user.

Auditing Activity

As well as preventing unauthorised access to data and outputs it is also important that you can audit access to sensitive data. For example, you may wish to know who is accessing specific client records and how often, or provide a "break the glass" option but record the action.

As part of the data gathering process, one or more audit logs may be recorded.

The audit log data records the following information:

- When the data was accessed
- User Id of the person accessing it
- The Data Set Definition used to gather the data
- The Data Group used to log the data
- The Context of the data access (e.g. fPanels, fDocs)
- Context Id and Data – the id and name of the dashboard, template, etc
- Log Type and Value – a code for the type of action and its identity

In addition, specific values may be recorded from the data itself to further identify the data viewed. For example you may wish to record the client's name. This makes it easier to see what a user has seen.

The Audit Log data is held in the fSeries database and may be accessed to use the data in other outputs such as a history of activity for a client.