fSeries Outputs Security

The availability of outputs (fDocs, fSheets, fPanels, Menus) may be secured within fSeries by a number of means:

- Disabling or excluding links to it
- Users' access roles
- Permission granted to groups and teams
- Permission granted to individual users

This provides a comprehensive and potentially daunting level of security to ensure users only get to see the outputs they should see.

The different methods work together but you need only implement the methods that suit your organisation.

Disabling Links

Menu items and dashboard commands can be subject to tests to prevent their use (by disabling or hiding).

This improves the appearance of the menus and dashboards but is not a satisfactory method of securing outputs as it removes the option but does not prevent the link itself being run manually.

Access Roles

An access role is a code added by the administrator which may then be allocated to appropriate users. For example, if you add an Access Role of Manager (from the fAdmin > Access Roles page) you may then apply this access role to all users who are managers (go to User Search to select the user and then click on "More Options" and click on Access Roles).

Next, open the Properties page of an entity that is only available to manager and click on the Manager item in the Access Roles section to the right of the page.

Now, only users with the access role of Manager are permitted to see this output.

You can add any number of access roles and apply them in any combination to any entity.

If an entity has no access roles applied then it is considered available to all user, depending on other permissions.

Permission Sets

A permission set is a collection of entities which are granted permission as a whole to selected user groups and / or teams.

Groups and Teams

First, what are groups and teams.

All users may be assigned to a group, or no group at all. Groups are added by the administrator and as well as being a part of permissions, a group also designates the start URL that all members are taken to when opening fSeries.

Groups are optional but may be areas of the organisation, such as Social Care and Education.

Teams are sections of your user community. A team may be assigned to a group, or no group at all. A user may be a member of more than one team (e.g. Management and IT), but only teams associated with the user's group (or no group if the user is not a member of a group).

Setting up groups and teams to match your organisation you have a matrix of your organisation's structure. Of course, you may have no groups, just teams; alternatively you may have no teams, just groups. Whichever way suits your organisation, you can grant permissions based on your own structure.

Permission Set Content

Each permission set that you set up has two aspects: the entities associated with the set and the groups and teams granted access to the set.

Entities

When you open the Permission Set Entities page, a list of all of the entities in the set is displayed to the left.

You can added to the list by clicking on the Search button to the right. This will open a search dialog where you can search by entity types, index labels and entity name or alias to narrow down the search. Note that DSDs is one of the entity types; this relates to generation of an fSheets spreadsheet based directly on the contents of the DSD.

The search results will be displayed to the right and clicking on any item will move it to the left to include it in the permission set's entities.

Click on an entity to the left to remove it from the permission set's entities.

You can also add an entity to permission sets from the "Permissions" option on the entity's property page.

All of the entities included in the permission set may now be granted access as a whole to groups and teams.

Grant

The Permission Set Grant page shows all of the groups and teams granted permission to the set of entities. Where a whole group is granted (no individual teams) only the group name will be shown. Teams are shown within their group.

To the right of the page the select list offer all groups (and no group). Select one to edit the grant related to that group.

A list of checkboxes will appear, one for the whole group and one for each team in the group. Checking the "whole group" option will hide the teams as you cannot grant to a whole group and individual teams.

Once you have set up the granting of permissions it is active. Users will be subject to the conditions from the next time they log in (if they are currently logged in their permissions will not be reset until they log out and back in).

Individual Permissions

For particularly sensitive outputs you can apply permissions for individual users.

Open the entity you wish to secure this way and click on the Permissions option.

From here you can add/remove the entity to/from permission sets by using the check boxes in the left column.

In the centre column is a list of the users who have been granted individual permission to the entity. Use the form to the right to search for users. Click on a user to add to the list of individuals.

Checking Permissions

Whenever an entity is accessed (other than when testing an "In Progress" version from the designer) the permissions are checked. The process is as follows:

- Does the user have the appropriate user role (i.e. User)?
- Is the entity subject to access roles:
    - Does the user have one of the access roles specified for the entity?
- Is the entity associated with any permission sets or individual permissions
    - If the entity a member of any permission sets
        - Does the user belong to a group or team that has been granted access to one of the permission sets to which the entity belongs?
    - or
    - If the entity subject to individual permissions
        - Is the user in the list of individuals granted permission?

If the tests are passed, access is permitted.

Menu Checks

By default if a restricted entity is included in a menu it is only checked if the user selects it.

An option in a menu's design Settings page allows you to do a permissions check on each item in the menu and remove any to which the user is not permitted.

This is a useful option but may impair performance as it has to do a lot of work for each menu item before displaying the menu, so make only sparing use of this feature.

You can also set individual menu items to be checked. This is more efficient as only those that requested are checked but you must know which items are subject to permissions.