fSeries User Security

fSeries provides a number of options for user security from simple user id / password entry to integration with authentication services. It also has different options for pre-registration and authorisation of user, and whether or not personal data is held by fSeries.

This document outlines the options and how they interact.

Note that a user in fSeries is a user across all accounts, but each account's administration may give access to their account. This means that on multi-account systems a user need only held once and have one set of credentials.

Logging In

There are three ways for a user to log in to fSeries:

External Authentication Service

By using an external service the user logs in via that service and fSeries is informed that the user is a legitimate person. fSeries further checks that the user is known to it (by pre-registration or authorisation – see below) before directing the user to the appropriate start page.

User Id / Password

The user is challenged by fSeries end required to enter their user id and password. The user id may be either the id allocated to them or the email address used to add them. Optionally they may also need to enter an authenticator code (see Two Factor Authentication below).

Active Directory Identity

An option permits users to be identified by their Active Directory identity and passed directly through to fSeries without challenge. A recommended option will check that the user is permitted (e.g. they are in a specific AD group). Note that this is a sub-option of User Id / Password so a user approaching fSeries from outside their network will revert to the User Id / Password method. This makes it possible for network users to log in externally, if the server permits.

Auth Method

The Auth Method is an app setting which applies to the whole of fSeries and indicates which method of authentication is in operation.

"Forms" method provides User Id/ Password and optionally Active Directory authentication.

External methods such as "Auth0" use the specified external authentication service (e.g. Auth0)

Please see separate documentation on fSeries App Setting.

New User (External Service)

If the Auth Method is an external service users may be pre-register and/or optionally self-registered, requiring authorisation.

Pre-Registration

Pre-registration of a user requires their email address and a user id.#

The email address is used to connect the user to their external service identity. The user must sign on to the service using this email address. The first time they log in to fSeries they will be found using this email address and their service authentication id will be capture. In future only the service authentication id will be used to identify them.

Note that when pre-registering a user, if a user already exists with the same email address, the current account is added to that user's list of permitted accounts.

The user id uniquely identifies the user within fSeries. The value entered may be adjusted to make it unique if another user already has the same id.

The administrator may ask for an email to be send to the user immediately. User Registration page also lets the administrator review registrations and re-send invitation emails.

Self Registration

An app setting indicates that only pre-registration is permitted for the system. If set, users must be pre-registered as above. Otherwise they may apply via the external service.

This option relies on your external authentication service having a means of allowing users (or administrators) to add users to or connect to the fSeries application.

The first time the user logs in to fSeries their user record will be set up (against the account to which they logged in) but the user will not be able to log in fully until an administrator has authorised the user.

An option in the administration system (fAdmin) lets the administrator view authorisation requests and permit or reject them.

New User (User Id / Password)

New users who will log in with a user id and password are added by the administrator, entering at least a unique user id and their email address.

fSeries checks if the user already exists with the same email address. If they exist they will be added to the current account, if not a record will be created for them.

It is for the administrator to notify new users. When the user first attempts to log in they should use the "Forgot Password" option to reset the initial random password set for them. They need only know the email address with which they were added in order to do this.

The administrator may also enter then user's AD Login. This is the Active Directory identity which, if the Auto Authentication app setting is true, is checked and will allow the user access without challenge. This makes it possible for a user to have AD access when on the network but also gain access with user id / password externally (if the server permits).

New User (Active Directory)

If a user opens a link to fSeries and their Active Directory identity can be discovered by fSeries the user will be added to the account to which they entered, subject to some restrictions.

- The Auto Authentication app setting must be set to true. This indicates that users may be passed through without challenge based on a matching AD login.

- The Auto Authorisation app setting must be set to true. This indicates that all network users are potentially permitted access and so may be added automatically.
- The optional Authentication DSD (Auto) must be set to a valid DSD and is executed to check the user. This is user defined but typically check, for example, that the user is a member of a designated AD group.

If all tests are passed, the user is added to the account and (if not already present) to fSeries.

If external access is required for such a user, the administrator must add their email address (which must not be in use by any other user) to their profile. This will permit them to use the "Forgot Password" option to obtain access.

Two Factor Authentication

If "Forms" authentication method is in operation, an additional factor may be added. This may be applied to all user, optionally at the user's choice, or not at all, based on the Two Factor app setting (on, optional or off respectively). If set to optional, the user may opt in or out using the option displayed on the fAdmin home page. Optional two factor is not possible for non-admin users.

When the user has logged in with User Id and Password will request a further entry of an authenticator code from an app such as Google Authenticator or Microsoft Authenticator.

Block and Remove

Users may be blocked from having access to an account and subsequently unblocked. This is useful to retain a user's identity in order to prevent repeated self-registration or AD login access.

A user may be removed from an account's list of users. If the user is no longer a member of any accounts their entire record will be removed.

Email Address

The user's email address is used as their identity for checking access via external services and to discover users already registered to other accounts. It must also be unique across all fSeries users.

It should therefore only be changed if necessary. As a result, only administrators may change a user's email address.

User Profile

If the Hold Personal Data app setting is true then fSeries will hold the user's name and telephone number. This is optional and may be maintained by the administrator.

If the setting is false and an external authentication service is in use and set up for management access to user information, fSeries will, as required, obtain the user's name from the service.

Super Users

Super users are a different class of user.

- Access to different administration tasks
- Members of the Fibonacci Support account and no other
- Can act on behalf of any account

Super users must be set up by another super user. Set up is similar to the User Id / Password setup but they can still gain access via and external authentication service.

Super users can be removed but there is means to block a super user (this is an account level action and super users operate across all accounts).

Common Security Scenarios

The following are typical scenarios for setting up user security.

Azure AD Pre-Registered

In this scenario users may be added by the fSeries administrator (via the fAdmin > Users > New User button), providing their email address as registered with Azure AD and a User Id (this is only used to find a user when searching later; the user need not know it). An email may be sent to the user inviting them to log in.

App Settings

AuthMethod	AzureAD	
PreRegistrationOnly	true	Only pre-registered users may log in

When a user who has an Azure AD account logs in to fSeries they are checked using their Azure AD identity or if not found, by the email address you entered (the next time fSeries will have a record of their Azure AD identity). Because you have pre-registered them they may enter.

Auth0 Self-Registered

If you wish to let users request access to your fSeries account by logging in through Auth0, this option does not require pre-registration.

When a user attempts to log in, their details are recorded in fSeries and the user is told that their request has been received and is awaiting authorization.

The fSeries administrator can see users awaiting authorization by going to the fAdmin > Users > User Authorization page. Click on a user and either authorize or deny. Once authorized the user may log in an email is sent to the user and they may now log in.

Note that you must have set the Authentication DSD in fAdmin > Account and that it must return one row in to verify that the user is permitted to be added by self registration.

App Settings

AuthMethod	Auth0	
PreRegistrationOnly	false	Users may request access without being pre-registered

Azure B2C Auto-Authorised

In this scenario users may log in using their B2C credentials, and are added to fSeries users automatically. This is on the basis that having passed through B2C they are a legitimate user of fSeries. The user is added with a role of “User” only.

If a default group has been set up the user is added to this group. If a default group has not been set up the user will have no group and therefore open access to outputs and data. If your fSeries has

groups it is essential that you create a default group with limited access. The user's group and roles may be changed later. Groups are added in fAdmin and the default group is indicated by checking the "Default Group" option.

App Settings

AuthMethod	AzureB2C	
PreRegistrationOnly	false	Allow unregistered access
AutoAuthorise	true	Automatically authorise users on login

By Designated Active Directory Group

In this scenario users are logged in based on their Active Directory (network) identity but they must be a member of a specific group in order to proceed.

This is achieved by selecting an Authentication DSD in fAdmin > Account. The DSD will check the AD Group and is set up as follows:

- Create an LDAP source that connects to your Active Directory
- In Settings set the AD LDAP User Group to the AD group to which the users must belong
- Create a Data Group in the DSD called "User" that uses the AD Security data gatherer

The DSD will look at your Active Directory based on the user's AD Login value and return a row to confirm that the user is in the designated AD LDAP User Group.

App Settings

AuthMethod	Forms	
AutoAuthorise	true	Allow users to be added based on their network id
Forms:AutoAuthenticate	true	Allow users to gain access based on their network id

Active Directory Validated Against Another Database

In this scenario users are logged in based on their Active Directory (network) identity but they must be validated by checking a third party application database.

This is achieved by selecting an Authentication DSD in fAdmin > Account. The DSD can take any actions required but must return a single row in the "User" data group in order to proceed.

Typically this will involve passing the user AD Login identity to a query that looks up the user's record in the other database.

App Settings

AuthMethod	Forms	
AutoAuthorise	true	Allow users to be added based on their network id
Forms:AutoAuthenticate	true	Allow users to gain access based on their network id

Permits Access When Outside the Network

If you are using one of the Active Directory options users will be logged in automatically unless they are outside of the network when the system cannot discover their identity.

In order to permit access, make sure user's email addresses are added to their record (Edit button from user details page).

The user will be taken to the User Id / Password page. On the first occasion they should click the Forgot Password option to reset their password.

User Id and Password

This is the least practical option as the login starts a session which times out, requiring a login again. This is particularly impractical for document downloads as the system will need to authenticate the user repeatedly as they download documents.

App Settings

AuthMethod	Forms	
AutoAuthorise	false	Prevent users being added based on their network id
Forms:AutoAuthenticate	false	Prevent users gaining access based on their network id

Add users via the fAdmin > Users > New User button. Enter their email address and a user id. AD Login is not of use unless you turn on AutoAuthorise and/or AutoAuthicate.