Audit Log

*f*Series Audit Log is an optional feature that lets you record a log of user access to data gathering throughout the *f*Series product range. Logs are recorded in the AuditLog table of the *f*Series database.

What is logged and the information recorded is entirely under your control. *f*Series will automatically capture standard details such as the date, the user and the context but in addition you can add a log type and value for analysis together with extensive data about what was delivered to the user.

Logging is defined by adding data groups to DSDs that, instead of returning data, add a record to the AuditLog table based on your definition of the data group. Because every *f*Series product uses DSDs, by adding logging to DSDs you can obtain a record of user access to data throughout the product range.

Since *f*Series security is also based on DSDs, login records can be created by audit logging the security DSD (more detail on this specific use is provided later).

AuditLog Table Contents

The *f*Series database's AuditLog table is used to record all logging. The contents are as follows:

Id	Automatically generated unique identity for a log record (GUID)
AuditDate	Automatically captured date/time stamp
UserId	The User Id of the logged in user
DSD	The id of the DSD being processed
DataGroup	The id of the Audit Log data group that created the log (there may be more than one per DSD)
Context	Identifies the context in which the DSD is being used (e.g. Security or fDocs)
ContextData	Provides more detail about the context (e.g. the fDocs template being generated)
LogType	User defined classification of the log (e.g. Client)
LogValue	User defined value for the LogType (e.g. the client's id)
AuditData	A user defined collection of key/value data (separated by &) to record more details of the data gathered.

The LogType and LogValue are intended for use when analysing or searching the log. Use the log type to classify the logs and the LogValue to identify the data gathered. A good example is to log user access to client data, so the LogType would be Client and the LogValue would be the client's id. It would then be simple to view a list of all access made to a specific client by a specific user, or view a specific user's pattern of client views.

The AuditData lets you record more detail about the data gathered. For example, you may wish to record the from/to date range selected by a user when viewing transactions for a client. The LogType and LogValue might record the client and the AuditData could then be used to record the from and to dates entered by the user. Any data within the DSD may be included here.

Setting up the Log

All that’s needed to log activity is to add an AuditLog type data group to the DSD you wish to log. *f*Series will automatically add a record to the log every time the DSD is processed. For a basic log, that’s all that’s required. However, there are a number of additional options.

Log Type and Value

When you add the AuditLog data group you can enter these two values to be recorded, each of which may contain placeholders. Log Type is typically a classification (e.g. Client) and the Log Value is the value of that classification (e.g. #ClientId# to record the client’s id, if this were a user entry).

Audit Data

The Audit Data recorded in the database record is based on the data items you add to the data group. Each data item is added to the Audit Data as a key=value pair, separated by &. For example:

From=14/03/2013&To=21/03/2013&Status=open

By simply adding data items in the normal way you can record this extra detail about the data gathered.

Execute If

Don’t forget to use the standard features of a data group. The Execute If option lets you decide whether or not to record a log based on, for example, whether another data group has returned any rows (=COMPARE(=DGROWS(Transaction),gt,0,1)).

Also, you can add as many Audit Log data groups as you wish, each of which may have complimentary Execute If options if appropriate.

Data Group Order

Remember that the order of data groups in the DSD is important. Make sure your Audit Logs are after the data groups whose data you want to record as Log Type/Value and Audit Data.

Internal Data

The Audit Log data group type returns one row of data that contains the values saved to the database. You may not wish to show this in outputs so remember to check the Internal Data option in Data Group Settings to hide the data group.

Always Include

If your DSD is potentially for use in fDocs generated documents make sure you tick the Always Include option under fDocs Settings. fDocs automatically excludes data groups whose data does not feature in the generated document unless this is ticked. As you are unlikely to include the log data in most or any documents, make sure this is ticked to ensure logging.

Security

*f*Series security is based on a DSD being used to check a user's credentials and roles. It is therefore possible to use the Audit Log feature to record users' access to the system. The *f*Series recommended method is to have two Audit Log data groups, one for successful login and one for failure. This is done by including a condition in the Execute If option to check that the "User" data group returned a single record or not respectively.

A configuration setting (fSeriesSecurityLogging) is provided in order to activate or deactivate logging within the security DSD globally. Include a condition in the Execute If options of each Audit Log data group to check the setting.

The full Execute If condition recommended is as follows:

Success:
=IFAND(=IF(=CONFIG(fSeriesSecurityLogging),true),=COMPARE(=DGROWS(User),eq,1,1))

Fail:
=IFAND(=IF(=CONFIG(fSeriesSecurityLogging),true),=COMPARE(=DGROWS(User),ne,1,1))

It is recommended that the Log Type and Log Value are used to record the success/failure of the login and the identity of the user (the automatically logged UserId will not be present as the user has not yet logged in).

	Success	**Failure**
Log Type	UserAccess	AccessFailed
Log Value	#Id#	#Id#

Note that a placeholder of #Id# is used for the user's identity. Use a global placeholder to obtain either the UserId or Login user entry, whichever has been supplied.

Finally it is suggested to add data items to the Access Failed data group to record the UserId, Password and Login user entries in order to be able to determine why a user's login has failed.

The security DSDs supplied with *f*Series will include these features.

Contexts

Context and Context Data are added to Audit Log records automatically according to where the DSD is being used, such as security, fDocs, fPanels, lookups and so on. Below is a list of the contexts you will find in the table and and explanation of the associated data for each.

Context	**Data**	**Explanation**
ClearCore	“AsyncErrors”“XRefs” “BestView”	ClearCore data plugin
fAdmin	“UserSearch”“UserDetails” “CheckUserId”	
fDocs	Template file	Generated document
fPanels	Presentation Id	
Jontek	Ids	Jontek data plugin
Lookup	The Id of the main DSDThe id of the Presentation“WS” (web service request)	Lookups for option lists (e.g. in user entries)
Menu	Menu Id	DSD run in fSeries menus
PermissionSets		Data access permission details
PivotFields	DSD Id and Data Group Id	Fields expected in pivoted data group record
Security	First URL and web page requested“Designer” – fDocs Designer“DSD” – fData“User” – via web service “Admin” (not currently used) “WS” – undetermined from web service	User authentication from browser or web service
SQLLibrary	Queries	Obtaining SQL query from library
WS	“GetData”“Structure” (fTest analyse)	Various options executed from the web service

Note that these contexts will only appear if you add logging to the DSDs that serve these purposes. In most cases it is unlikely that they will be used.

Configuration

The following configuration settings are provided, under fSeries in fAdmin.

fSeriesDatabaseSource	The configured data source for the optional fSeries database (default: ‘fSeries’)
fSeriesSecurityLogging	May be used to indicate to your security DSD that user accessing logging is to be done