

# FRAUD DETECTOR

The three key approaches to ensuring an ERP system is not the subject of internal fraud are controlling access, setting up Segregation of Duties, and setting up alerts on critical data. With EnterpriseOne, there are ways to monitor transactions at the database layer, but changes to critical and master data cannot be monitored effectively with this method. The database simply does not show the before values and does not identify the user who did the modification.

Fraud Detector fits very well with the Q Software tools for Access control and SoD, by enabling the user to selectively set up alerts against areas of the system that are concerning. Changes to key data entities such as the Address Book or even Payroll data can be monitored, and Management informed of suspicious activity. These tools together provide a complete pro-active control over fraudulent activity on the system.

## PROACTIVELY MONITOR FOR COMMON FRAUDS

Unauthorized changes to master data should be investigated promptly as they could be a sign of fraudulent activity.

For example:

- Changes to the Address Book and/or Vendor Bank Account details could be symptomatic of "Dummy Company" fraud
- A large increase in a Vendor Credit Limit may indicate procurement fraud
- A high percentage rise in an employee's salary may be suspicious and need investigating!

But native JD Edwards doesn't alert you, so such activity can go undetected for a long time and result in huge losses.

**Fraud Detector** gives you powerful auditing tools which can alert you instantly to suspicious changes and make it easy for you to view and investigate them.

## HOW IT WORKS

Although many JD Edwards customers are not aware of it, the native EnterpriseOne system contains a Data Change Tracker module, also known as 21 CFR 11. Its tracking functionality can be valuable to any organization who needs to monitor critical data. But the audit data that it produces is not very meaningful in its raw form – so identifying significant changes can be a bit like looking for a needle in a haystack.

## ALL THE POWER WITHOUT THE PAIN

Our **Fraud Detector** harnesses the power of the native Data Change Tracker, and provides tools that alert you promptly to significant changes and enable you to drill down to investigate them.

## USER-FRIENDLY TRACKING WITH AUDITING ALERTS

Data Change tracker allows you to specify **exactly** which columns on which tables should be audited, then every time those columns are updated, the details are automatically logged.

With **Fraud Detector** you can set up alerts to notify relevant people of significant changes that may need to be investigated promptly as they could indicate suspicious activity – for example changes to bank account details or system configuration files.

Audit data can be viewed through easy-to-use enquiries and reports, with filters that allow you to pinpoint events that are of interest, investigate changes and make notes to explain changes to auditors.



## BENEFITS

- Instant notification of changes to critical data greatly reduces the risk of fraud
- Quickly and easily see all audited data in one place
- Detailed audit trail of who changed what and when (including before and after values)
- You decide exactly what to audit and monitor
- All changes to audited data are logged, even if made by programs external to JDE

Changed By	Date	Date and Time Stamp	Column	Column Description	Is Key	Action	Image ID	
BRIGANS	06/08/2016	2016-06-08 15:01:39	ALPH1	Alpha Name	N	Added	P0101	
BRIGANS	06/08/2016	2016-06-08 15:01:39	AT1	Search Type	N	Added	P0101	
BRIGANS	06/08/2016	2016-06-08 15:01:39	ANB	Address Number	Y	Added	P0101	
BRIGANS	06/08/2016	2016-06-08 15:02:47	ALPH1	Alpha Name	N	Added	P0101	
BRIGANS	06/08/2016	2016-06-08 15:02:47	AT1	Search Type	N	Added	P0101	
BRIGANS	06/08/2016	2016-06-08 15:02:47	ANB	Address Number	Y	Added	P0101	
Line of Business	BRIGANS	06/08/2016	2016-06-08 15:07:45	ACL	Credit Limit	N	Changed	P0301
Line of Business	BRIGANS	06/08/2016	2016-06-08 15:07:45	ANB	Address Number	Y	Changed	P0201
Line of Business	BRIGANS	06/08/2016	2016-06-08 15:07:45	CO	Company	Y	Changed	P0301
Line of Business	BRIGANS	06/08/2016	2016-06-08 15:09:27	ACL	Credit Limit	N	Changed	P0301
Line of Business	BRIGANS	06/08/2016	2016-06-08 15:09:27	ANB	Address Number	Y	Changed	P0301
Line of Business	BRIGANS	06/08/2016	2016-06-08 15:09:27	CO	Company	Y	Changed	P0301
SARASV	06/07/2016	2016-06-07 13:38:18	ALPH1	Alpha Name	N	Changed	P0101	
SARASV	06/07/2016	2016-06-07 13:38:18	AT1	Search Type	N	Changed	P0101	
SARASV	06/07/2016	2016-06-07 13:38:18	ANB	Address Number	Y	Changed	P0101	
SARASV	06/07/2016	2016-06-07 13:44:54	ALPH1	Alpha Name	N	Changed	P0101	
SARASV	06/07/2016	2016-06-07 13:44:54	ANB	Address Number	N	Changed	P0101	
SARASV	06/07/2016	2016-06-07 13:44:54	AT1	Search Type	N	Changed	P0101	

## MAIN FEATURES

### USING DATA CHANGE TRACKER TO DEFINE YOUR AUDIT REQUIREMENTS

Fraud Detector works on audit data collected by the JD Edwards Data Change Tracker (21 CFR 11), which needs to be configured and running in the current environment.

You can specify exactly which tables and columns you want to audit. Every time a change is made, audit data is logged.

- Which column was changed
- Action type (e.g. add, update, delete)
- Previous value
- New value
- Who made the change (User ID)
- Time and date
- Plus key data and User-specified columns

### AUDIT DATA VIEWER

As records are added to the 21 CFR 11 audit files, Fraud Detector collates them into a central repository for simplified enquiry and reporting.

Audit Data Viewer enables you to filter and sort results by Table, User ID, Date or Environment.

Sets of audit records that are created as the result of a single change/add/delete transaction are colour-banded for easy viewing.

### ALERT MANAGER

This allows users to view current Alerts so that they can investigate issues and document any findings or actions taken/required as a result of the alert.

The status of Alerts can be updated as they are progressed.

### ALERT BUILDER

This enables you to create alerts on particular audit tables and columns. A range of comparison operators give you the ability to monitor for broad or detailed change conditions:

- FT (From/To): checks if a value has changed from 'X' to 'Y'.
- GT (Greater Than): checks if a value is above a specified number (eg when a credit limit has been raised to more than \$20,000).
- LT(Less Than): checks if a value is below specified number.
- PU (Percentage Up): checks if a numeric value has increased by more than a specified percentage.
- PD (Percentage Down): checks if a numeric value has reduced by more than a specified percentage.
- You can also build an Alert which will be triggered if a record on a specified table is simply added, deleted or changed.

Alerts can be given a severity level to indicate the urgency of action required.

If the criteria is met, an email will be sent immediately to the person nominated to be responsible for changes to the table.

### PERFORMANCE

By its very nature, creating an audit trail will always have some effect on performance. Fraud Detector runs as a subsystem and it has been designed to minimize system overheads.