

Monitor and Audit Changes to Your Critical Data



The Highlights

- Allows you to decide exactly what should be monitored
- Eliminates the need to comb through reams of irrelevant data to find items of interest
- Alerts you to actions that may need to be investigated as soon as they occur
- It is now easy for both business and technical users to define monitoring rules and enquire on significant changes
- Output results to a report or export them at the touch of a button.

Fraud Detector

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.

To satisfy compliance regulations requirements, many companies also need to be able to track changes to data in certain files.

Fully integrated within JD Edwards World, **Fraud Detector** is an auditing and monitoring tool which allows you to:

- specify the database items that you wish to monitor
- track all changes to those items
- receive timely notification of unusual activity.

Simple Definition of Auditing Rules

You can set up straightforward auditing rules to identify which data to track, which actions you wish to monitor, and which users should either be monitored or excluded from monitoring (e.g. those who are permitted to make these changes).

Monitoring can be as granular as you need, as rules can be defined at the File (Table), Row (Record) or Column (Field) level. Fraud Detector will then track ALL changes to those items, even if the updates are made by functions external to JD Edwards World.

For each rule you can specify up to three email addresses to be notified in the event that the monitored change takes place.

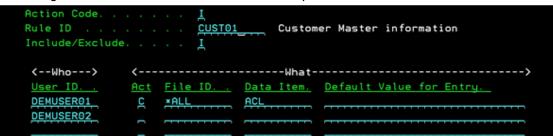
User-friendly Ad Hoc Queries

Both business and technical users can define their own enquiries to find out what changes have been made to a database item, or what changes particular users have made. Once you have defined your query criteria, you can automatically create a new rule that uses those parameters.

Generate Reports / Export Results

Query results can be output to a report or to a data extract file for external analysis – simply choose the relevant button from the results screen.

Below is an example of **Column Level monitoring**, tracking changes to the data dictionary item ACL (Account Credit Limit), on whichever JDE table it resides. This rule states that only users DEMUSER01 and DEMUSER02 have permission to change the value of ACL. If anyone else changes this item, notifications will be sent to the specified email addresses.



The rule below illustrates **Row Level Monitoring**. Changes to any data element of Address Book ID 12345, in whichever table it resides, will be monitored.

Action Code <u>ADDR01</u> Address Book Rule 1 Rule ID <u>ADDR01</u> Address Book Rule 1 Include/Exclude <u>I</u>				
<who></who>				
<u>User ID</u>	Act	<u>File ID</u>	<u>Data Item.</u>	Default Value for Entry.
DEMUSER01	*	*ALL	AN8	12345
DEMUSER02	_			
DEMUSER03	_		·····	

When reviewing event details, you can display multiple files on a single screen. As you highlight a record in the top half of the screen, the 'Before' and 'After' details are displayed in the bottom half:





US Headquarters

4600 S Syracuse Street, 9th Floor Denver, CO 80237-2719 Tel: 303-256-6630

UK & EMEA Headquarters

Connect House, Kingston Road Leatherhead KT22 7LT United Kingdom Tel: +44 (0)1372 700850



Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.