



SecurTrac

Why build An Audit Trail For Your Notes Application?

Background

Traditionally, you may come across some Notes applications that provide typical simple edit history field or section information at the bottom of the document.

You may think this is useful; however, when there are 10 modifications made by different people, changes become more difficult to monitor.

You just know that somebody made the change, but you will never know exactly who.

A comprehensive audit trail should provide you the following information:

- Who made the change
- When the change was made
- What was the change
- Where the alteration occurred. Was the change made on my server or did it come from another server through replication?

Imagine that if you have an application which stores some sensitive information, say employees' salary.

It will be beneficial if you can:

- Keep track of who has read the records
- Keep track of who had updated the records with highlights of what was changed.
- Automatic Email notification to the head of HR if someone makes changes on certain records

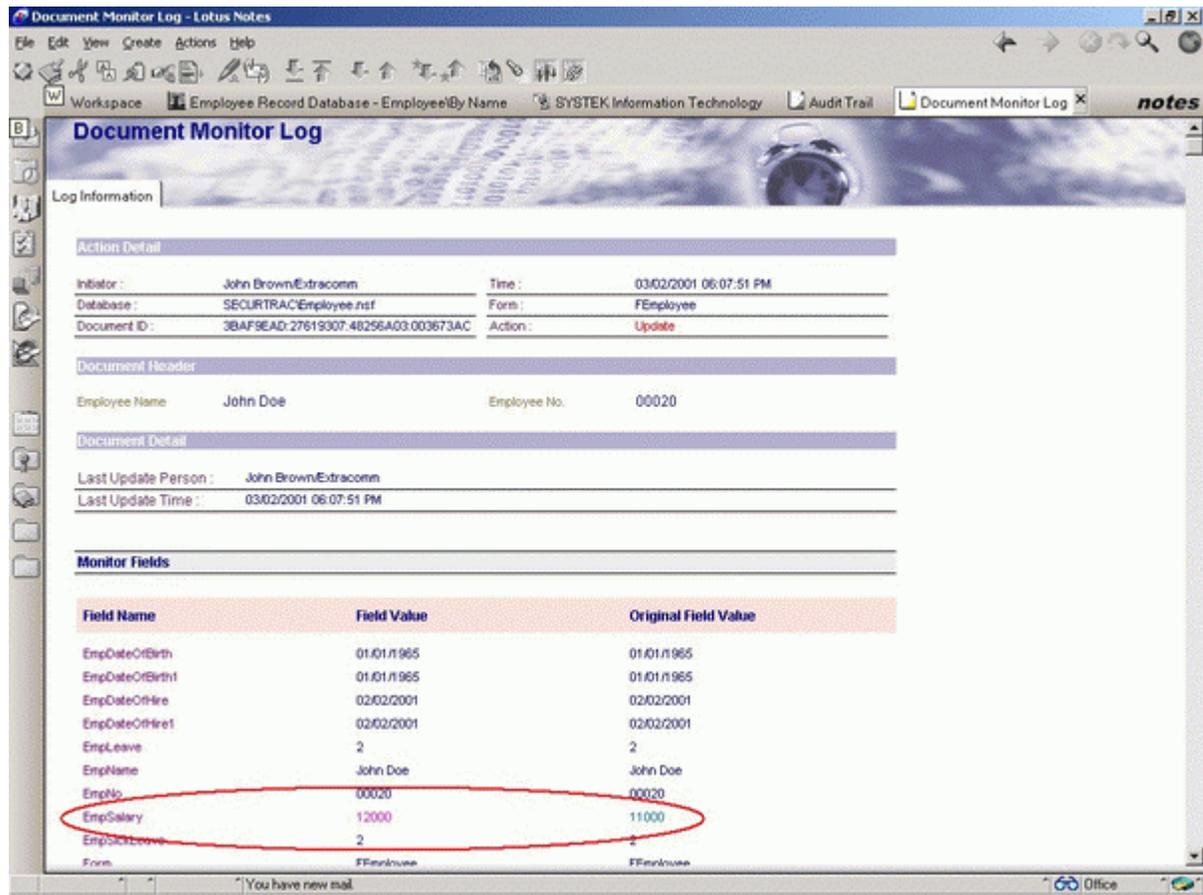
How SecurTrac solves this problem?

SecurTrac tracks the entire life cycle of the document, from creation to deletion. You can click on the Smarticon and you will see the complete audit trail of the document. This document trail can include events such as creation, update, open or deletion.

The screenshot displays the Lotus Notes interface. On the left, the 'Employee Information' form is visible, containing fields for Employee Name (John Doe), Employee Number (00020), Date of Birth (01/01/1965), Date of Hire (02/02/2001), Leave Taken (2), Sick Leave Taken (2), and Salary (\$11,000.00). A red circle highlights a Smarticon in the top toolbar, with a red arrow pointing to the 'Audit Trail' window. The 'Audit Trail' window shows a table titled 'Audit Trail for Document Change Log' with columns for Action Time, Action, and Initiator. The table contains the following data:

Action Time	Action	Initiator
03/02/2001 05:55:07 PM	Create	CN=John Brown/O=Extracom
03/02/2001 05:55:09 PM	Open	CN=John Brown/O=Extracom
03/02/2001 05:55:10 PM	Open	CN=John Brown/O=Extracom
03/02/2001 05:55:26 PM	Open	CN=John Brown/O=Extracom
03/02/2001 05:55:31 PM	Open	CN=John Brown/O=Extracom
03/02/2001 05:55:31 PM	Open	CN=John Brown/O=Extracom
03/02/2001 05:55:31 PM	Update	CN=John Brown/O=Extracom
03/02/2001 05:55:39 PM	Open	CN=John Brown/O=Extracom

If you wish to see the details of an entry, you can double click on the log entry.



For example, in the Update Log, you will find out:

- Who changed the document
- When it was changed
- What was exactly changed (at field level).

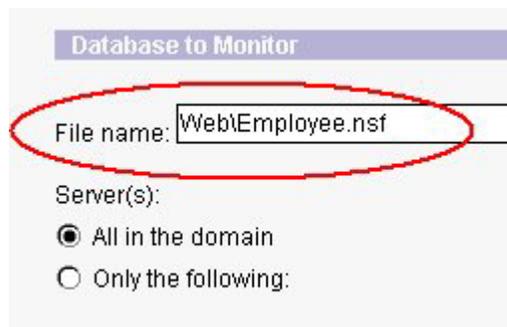
The modified field will also be highlighted. The original and new value of the field will be shown.

In addition, SecurTrac can be configured to notify you or anyone you assign to receive notification by e-mail, pager or Short Message Service (SMS).

How SecurTrac works?

There is no programming required to enable an audit trail in your application. It is very easy to setup Database Monitor.

1. Specify which database you want to monitor.



Database to Monitor

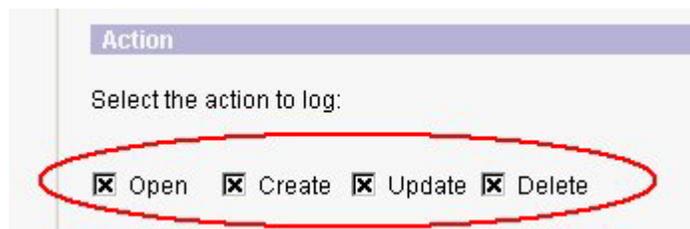
File name:

Server(s):

All in the domain

Only the following:

2. Select the action(s) that you want to log.



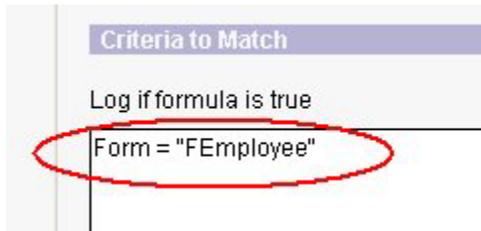
Action

Select the action to log:

Open Create Update Delete

In the above example a new log entry will be generated each time the document is opened, created, updated or deleted.

3. Specify the type of documents you want to audit (optional).



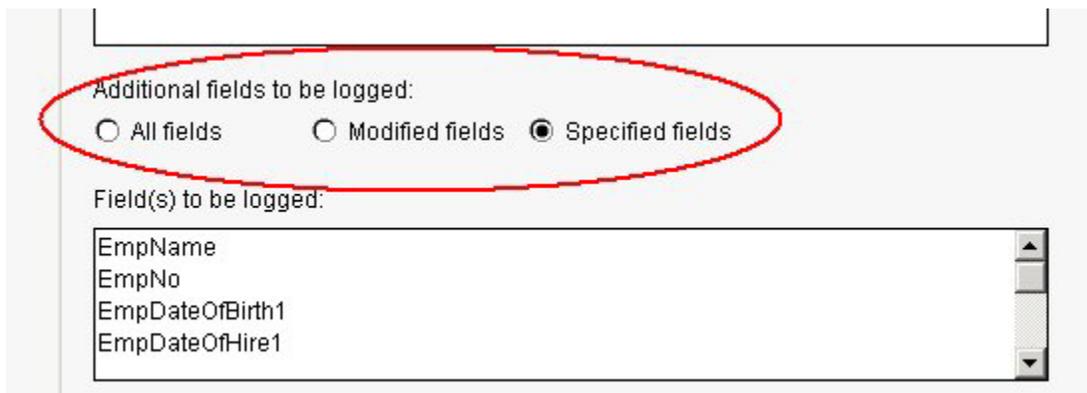
Criteria to Match

Log if formula is true

Form = "FEmployee"

You may wish to track only certain documents in the database. You can specify which documents to audit by using standard Notes formula. Notes formula are very flexible and powerful.

4. You can specify which field(s) to monitor. You can select to log all the fields inside the document, log modified fields, or any specific fields.



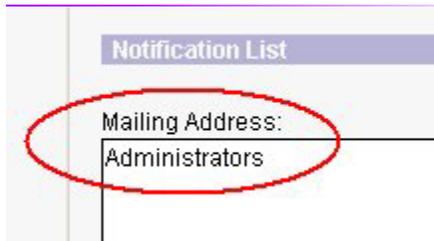
Additional fields to be logged:

All fields Modified fields Specified fields

Field(s) to be logged:

EmpName
EmpNo
EmpDateOfBirth1
EmpDateOfHire1

5. Optionally, you can specify email notification when the log is generated.



Notification List

Mailing Address:
Administrators

It is that simple. The monitor information can now be saved and auditing will begin. You can setup multiple monitors for a single database and have different staff be notified when there are triggered events.

What are the benefits of using SecurTrac?

All levels of administration in an organization benefit from using SecurTrac. The table below outlines the benefits for the company and each employee.

	Benefits
Company	<ul style="list-style-type: none">• Protect valuable information assets. All activities are logged and audited.• Save money.• Save time. SecurTrac shortens the development cycle due to the absence of a programmed audit trail.
Security Officers	<ul style="list-style-type: none">• Audit the activities of users to monitor or predict any irregularities.• Analyze the behavior of users' activities.• In case there is any leakage of information, all the activities will be traceable and users will be accountable for any information leakage.
Administrators	<ul style="list-style-type: none">• Discover why a document suddenly disappeared, who made the change to the document, or what was changed.
Developers	<ul style="list-style-type: none">• Can concentrate on the application development, rather than on the audit trail.

When would you use SecurTrac?

Scenario A

A database contains sensitive business information and assets that, if leaked, could jeopardize the financial future of a company. Strict access control enforcement, periodic review of database access and real-time alert of any irregularity are very important.

Scenario B

Companies use email to send confidential information. Apart from encryption and digital signature for the confidential emails, traceability is also very important. It is required to know:

- who send/receive the information
- entire email routing path
- who read the information
- how many copies of the information in the network
- mail delegation

Scenario C

All production applications need some form of tracking. Writing tracking mechanisms requires quality coding to ensure data fields are captured accurately. However, this process is time consuming. SecurTrac provides an "instant" audit trail for a company's Notes applications, freeing development teams from these tedious routines, allowing them to focus on other tasks, and increasing their productivity.

Scenario D

After administrators establish audit trails or tracking records, they need to manage the resulting data. Maintaining tracking information embedded in multiple databases is complex and time consuming. SecurTrac consolidates all information in one database per server, reducing administrator effort.
