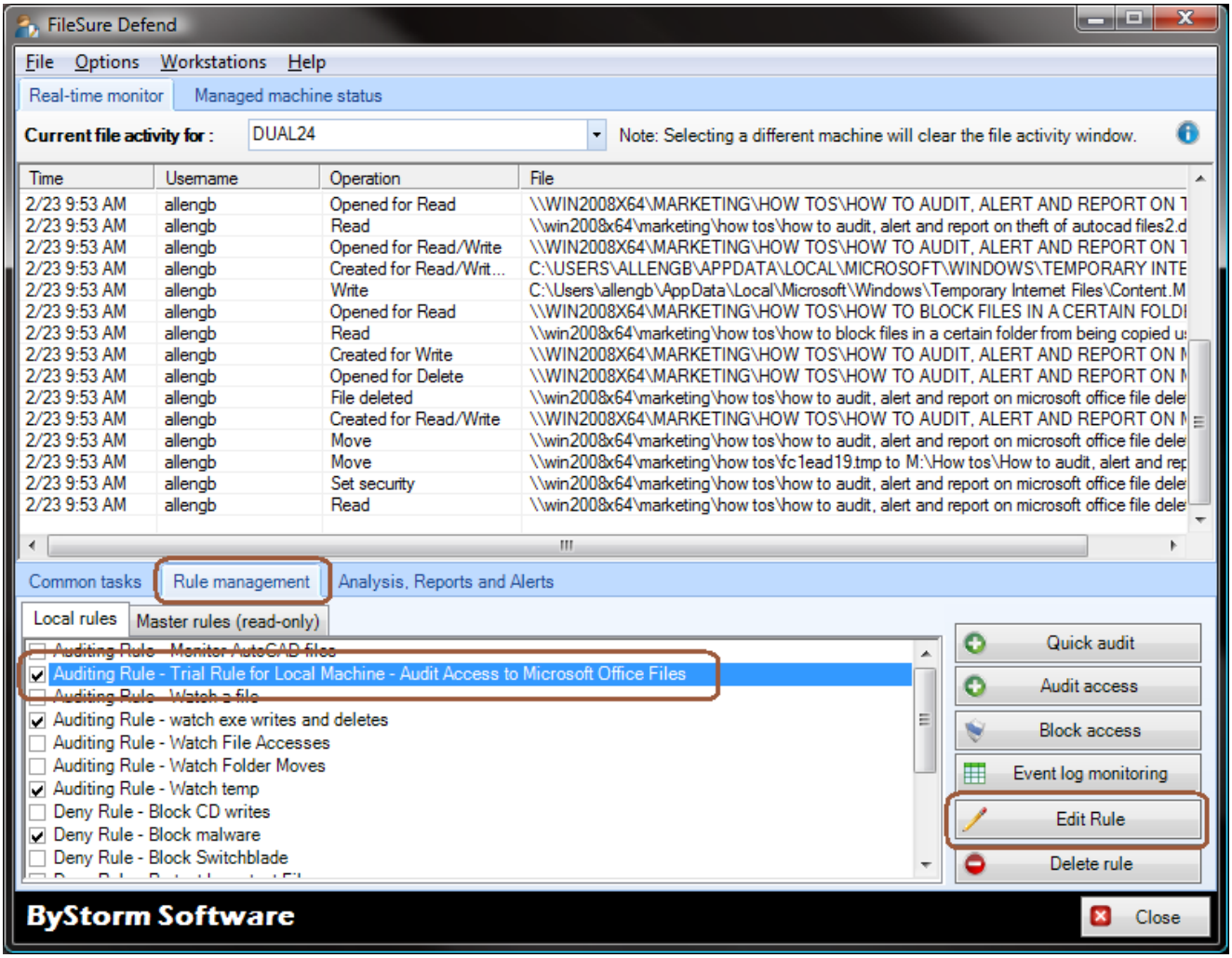
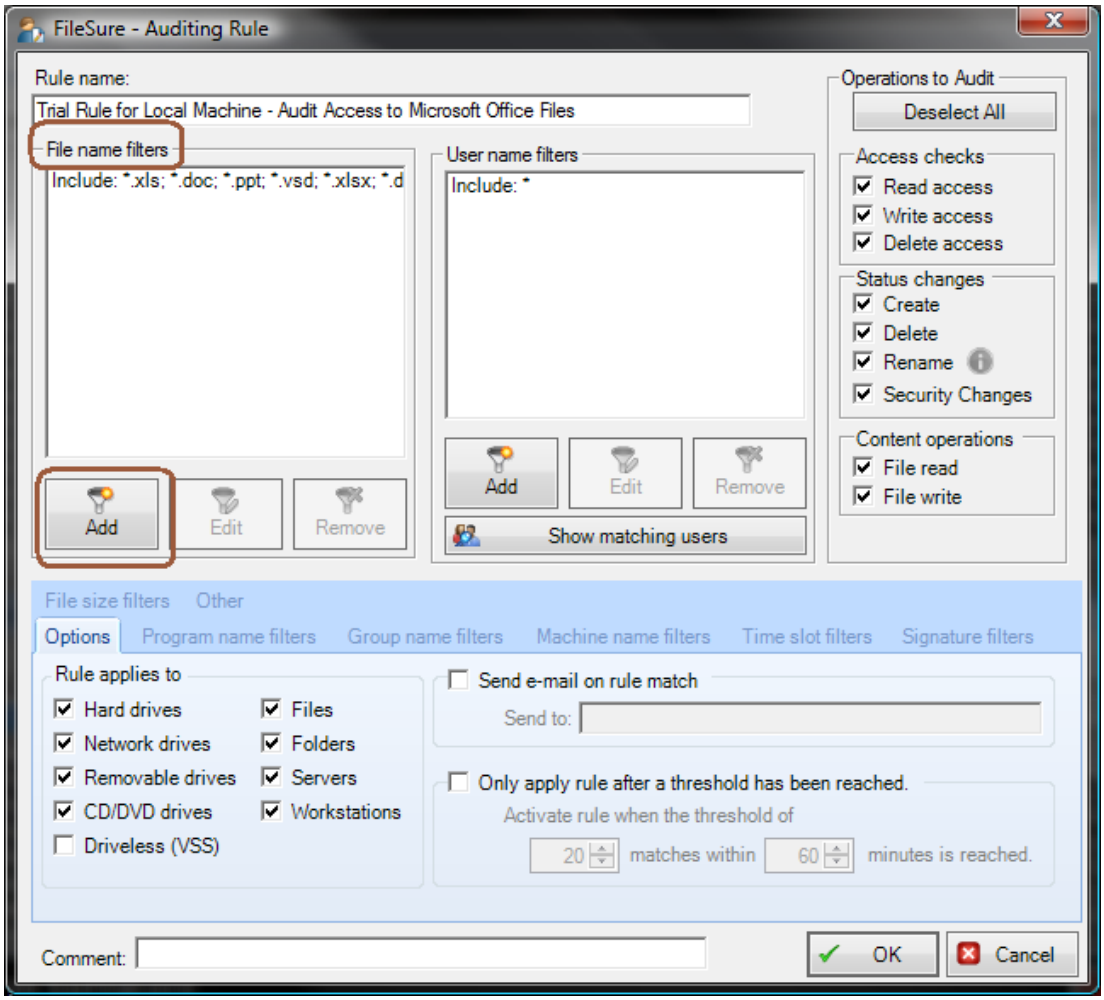
This 'How-to' will show how to configure FileSure to audit Microsoft Office files. We will generate an e-mail alert when an Office file is deleted. We will also set up an automatic daily "deleted files" report.

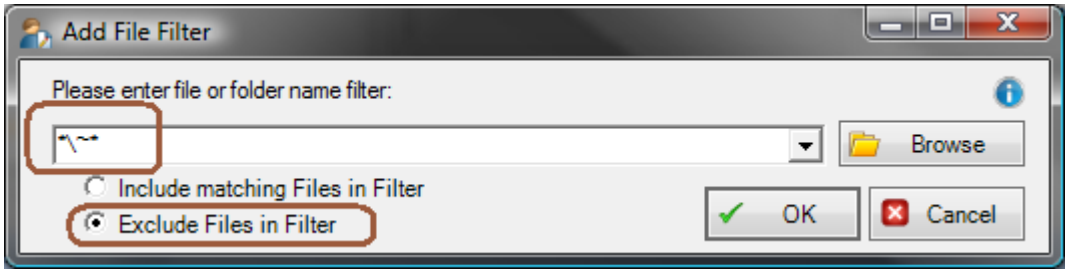
1. Start FileSure, switch to the 'Rules management' tab, select the rule titled 'Audit rule – Trial Rule for Local Machine – Audit Access to Microsoft Office Files' and click 'Edit Rule'. The rule is pre-installed.



2. This will bring up the 'Auditing Rule' screen, and we need to make a small tweak to the rule.

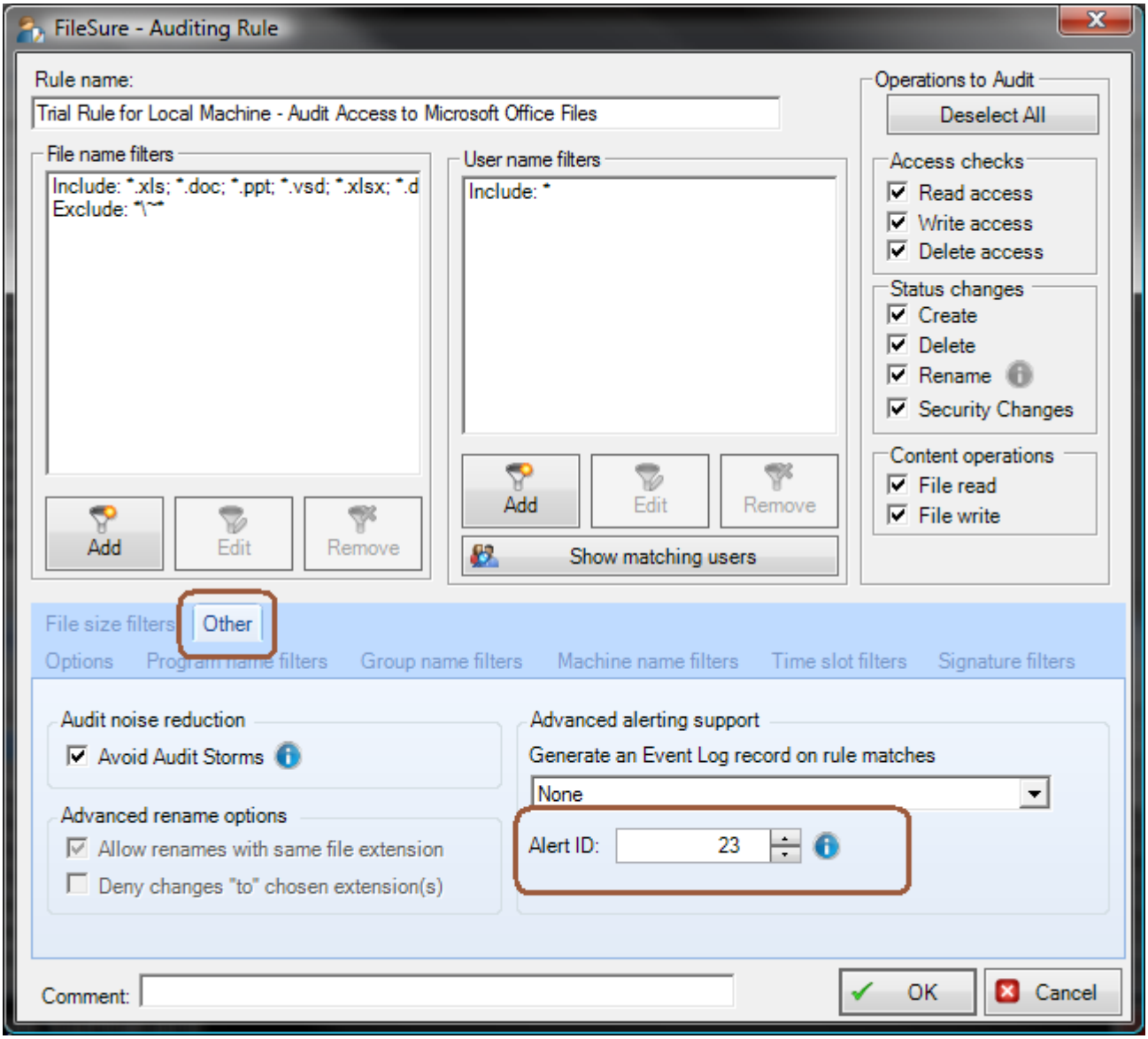


a. Click the 'Add' button in the 'File name filters' area. This will bring a little screen where you can enter the file filter:



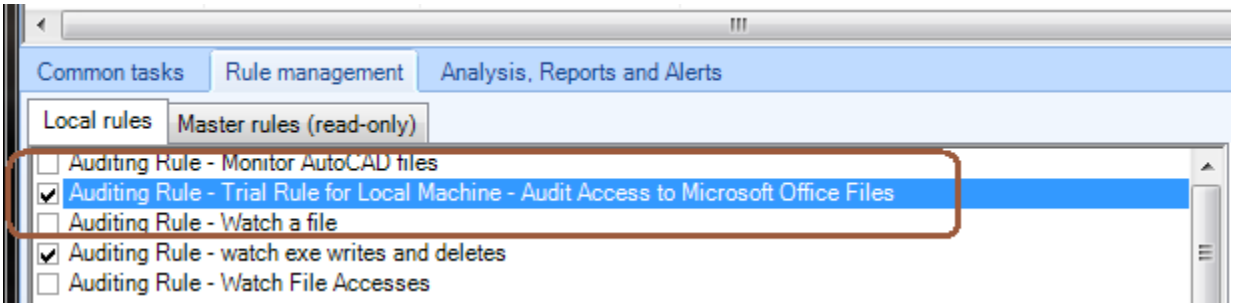
b. Enter '*\~*' and check the 'Exclude Files in Filter' option. **Microsoft Office creates these '~' files while a file is being used and we want to ignore them.**

c. Click the 'Other' tab and enter '23' for the 'Alert ID' filter



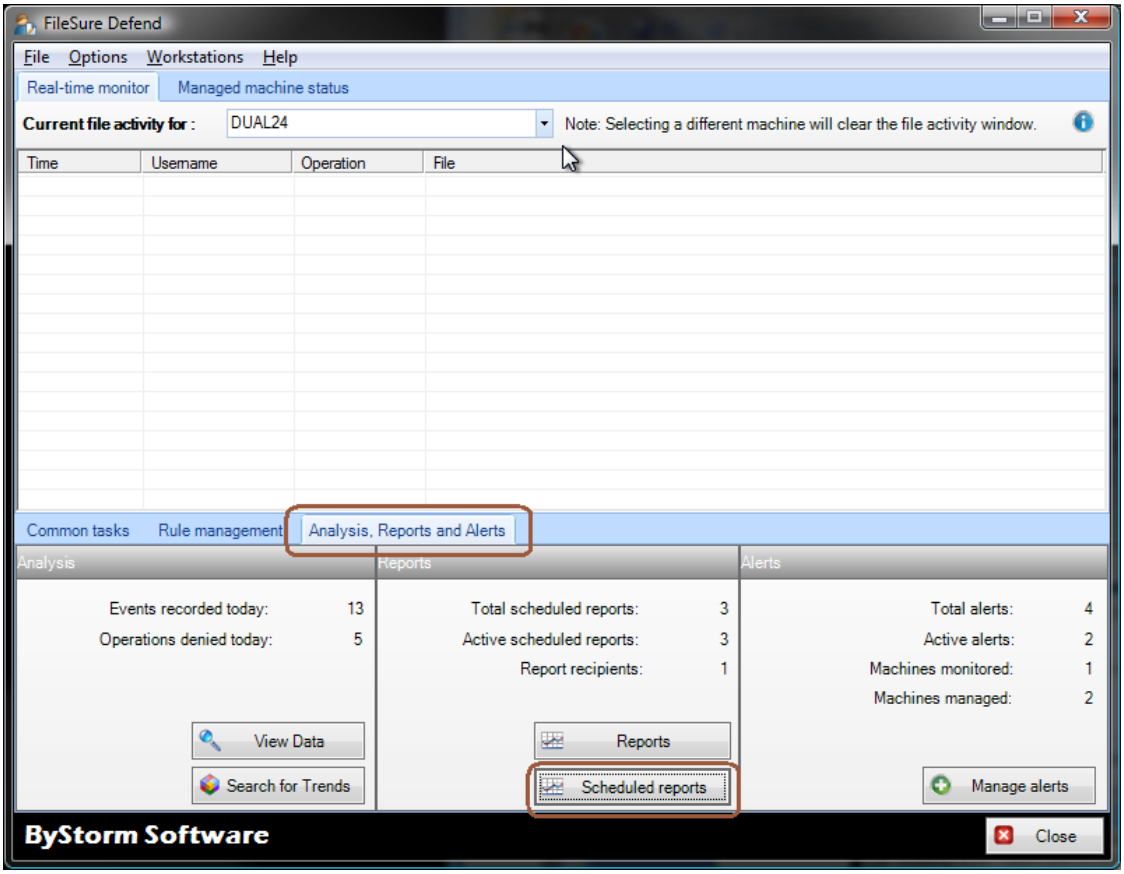
d. Click 'OK' to close the rule.

3. Find the newly created rule and make sure that it is enabled by clicking the checkbox next to the rule name, if necessary.

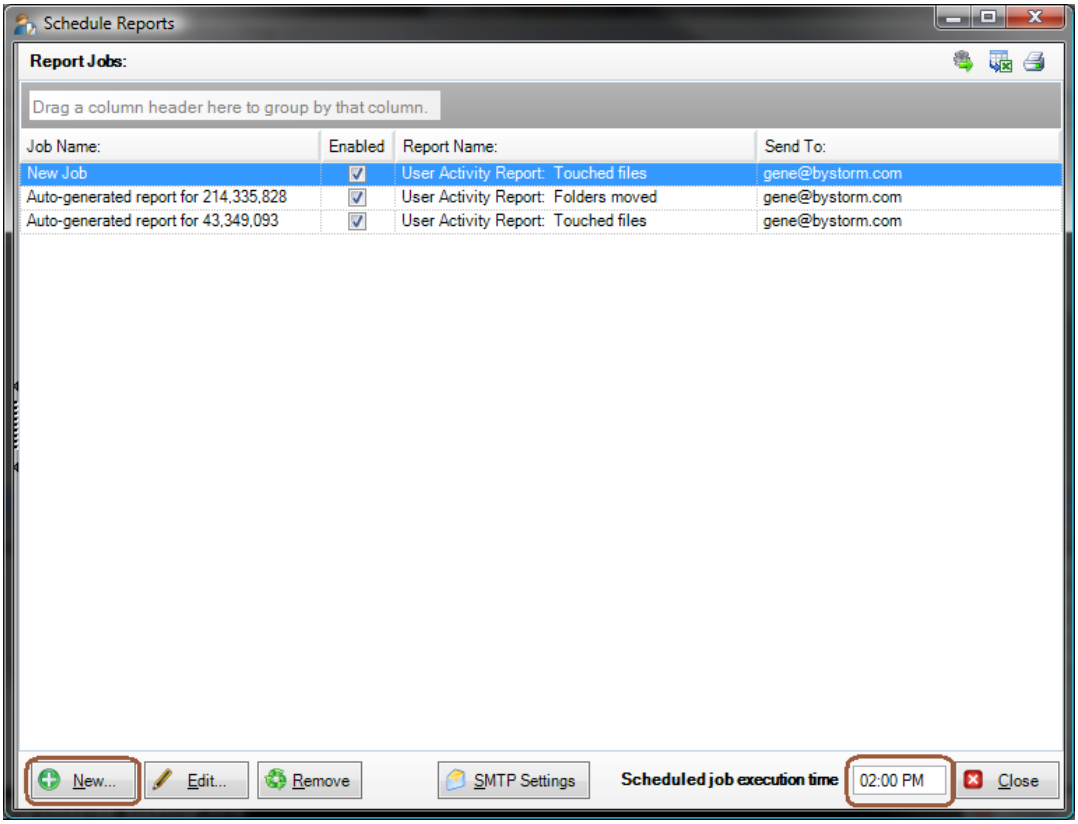


At this point, FileSure is recording access to Office files and storing those accesses in the data store. Now, let's see if we can't use that data for an alert and a daily report.

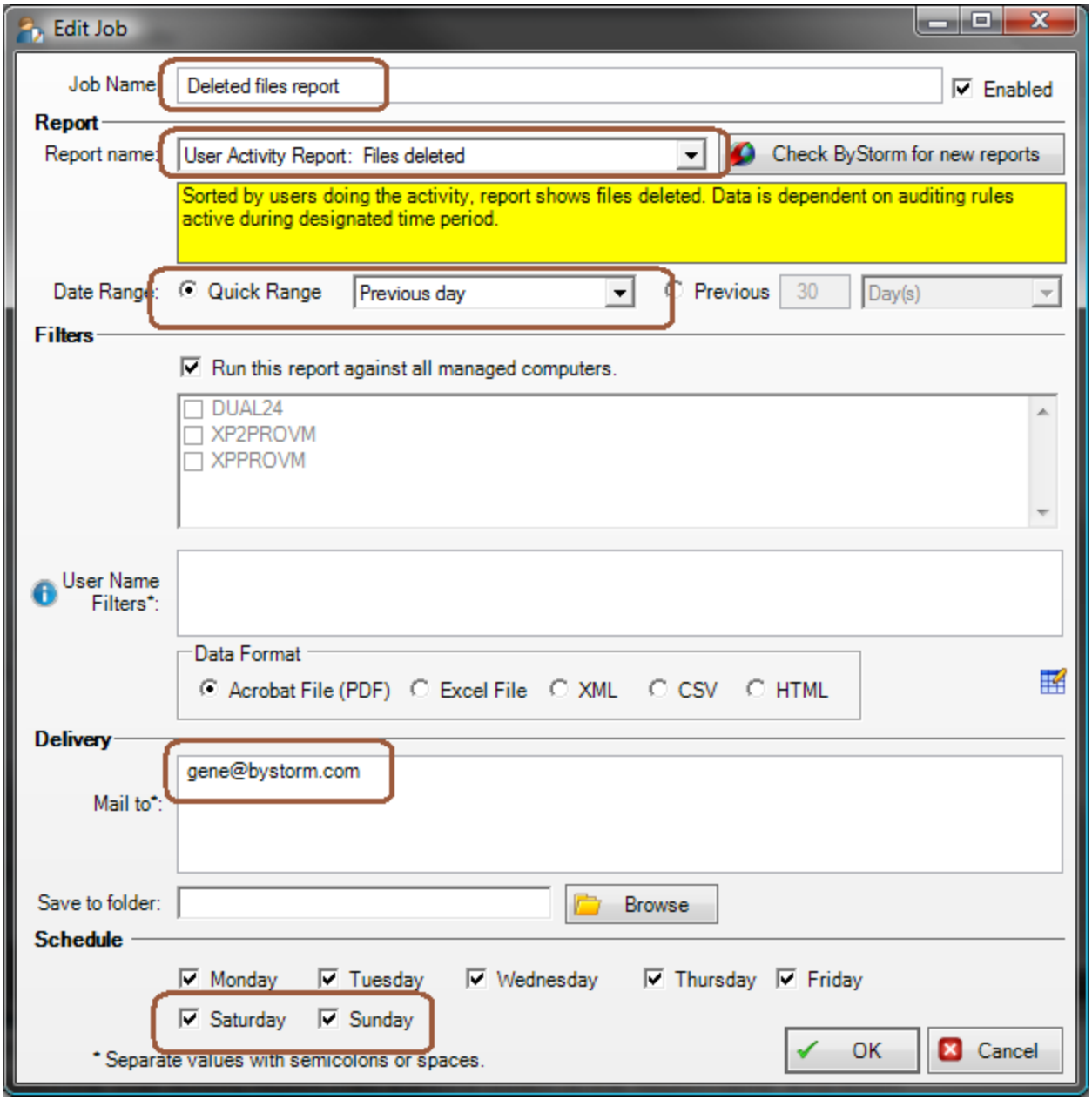
4. Select the 'Analysis, Reports and Alerts' tab and click the 'Scheduled reports' button.



5. This will bring up the 'Schedule Reports' where you need to click the 'New' button. Note the 'Scheduled job execution time' as this is the time that the reports will run everyday.

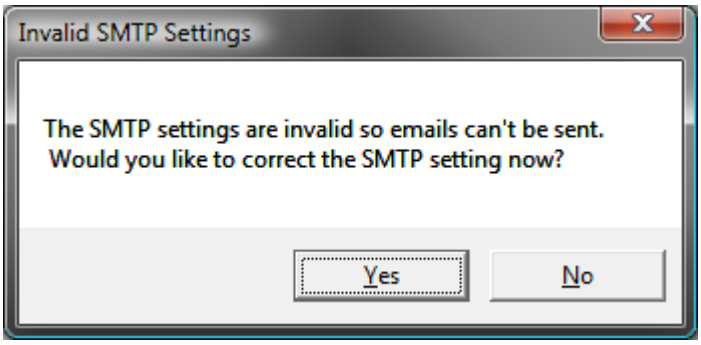


6. This will bring up the 'Edit Job' screen. This is where we will configure the scheduled report. Change the following things:

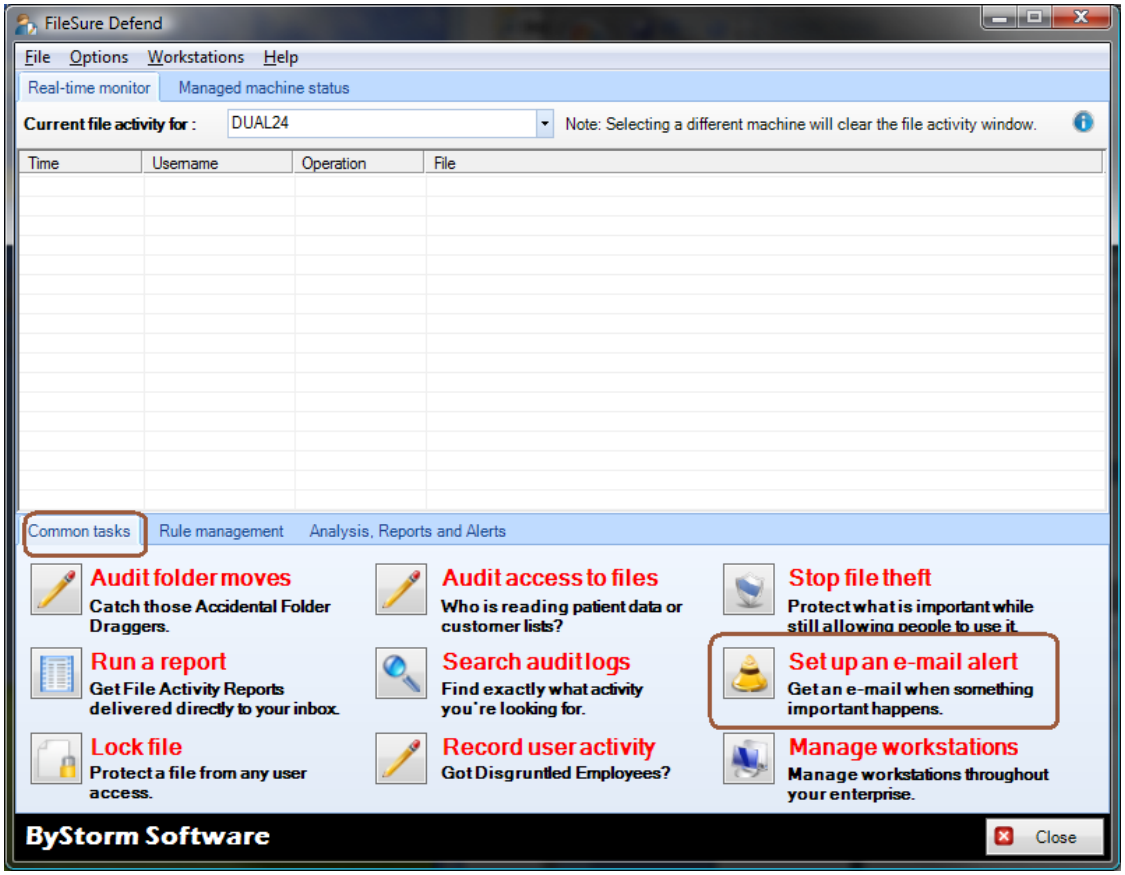


   a. Enter 'Deleted files report' for the 'Job Name'
   b. Select the 'User Activity Report: Files deleted' in the 'Report name' drop down.
   c. For the 'Date Range', select the 'Quick Range' of 'Previous day'
   d. In the 'Mail to' area, enter the e-mail address of who should get the report.
   e. In the 'Schedule' area, select the additional options of 'Saturday' and 'Sunday'

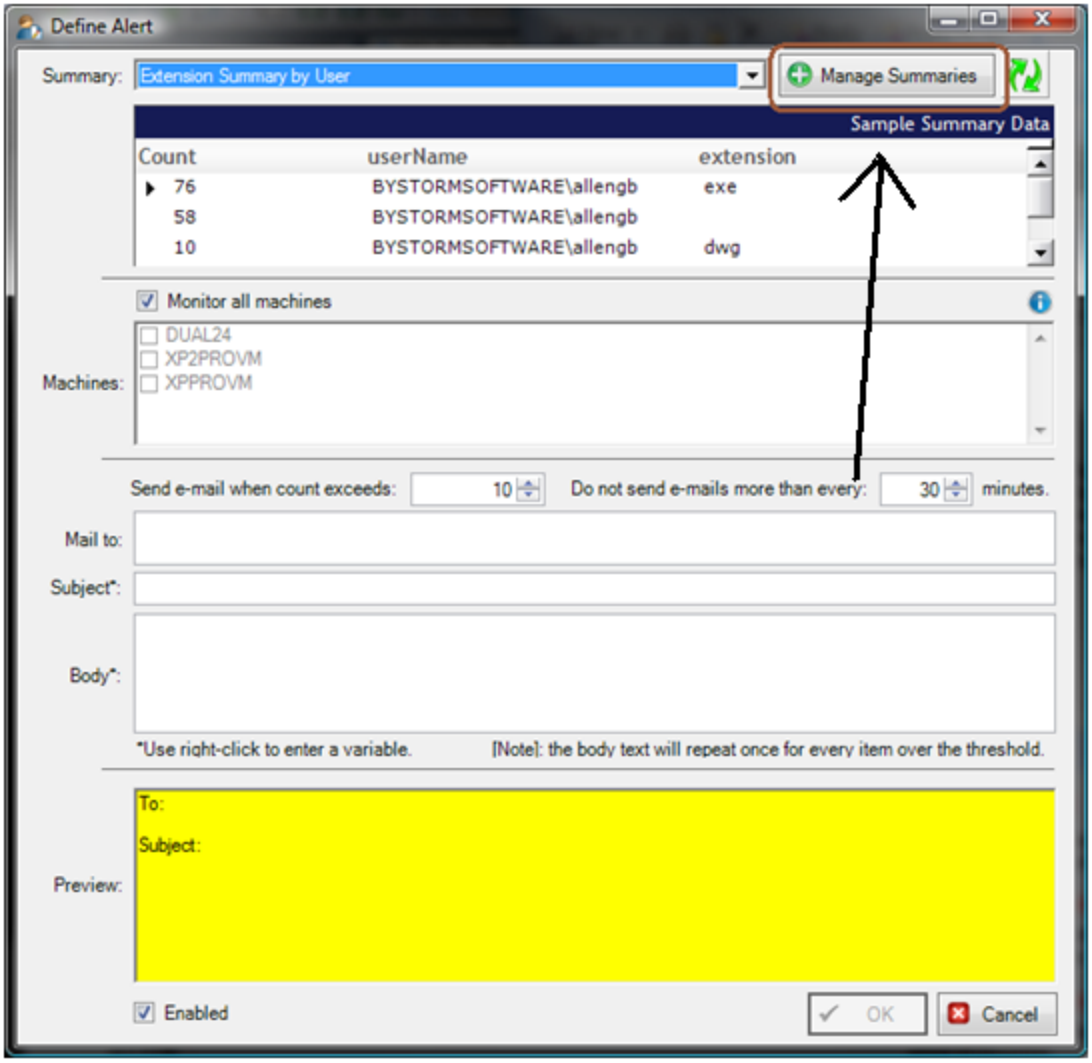
7. Click OK to close the screen and save the report job. Click 'Close' on the 'Schedule Reports' screen. If haven't already configured your SMTP settings, you will be prompted to do so.



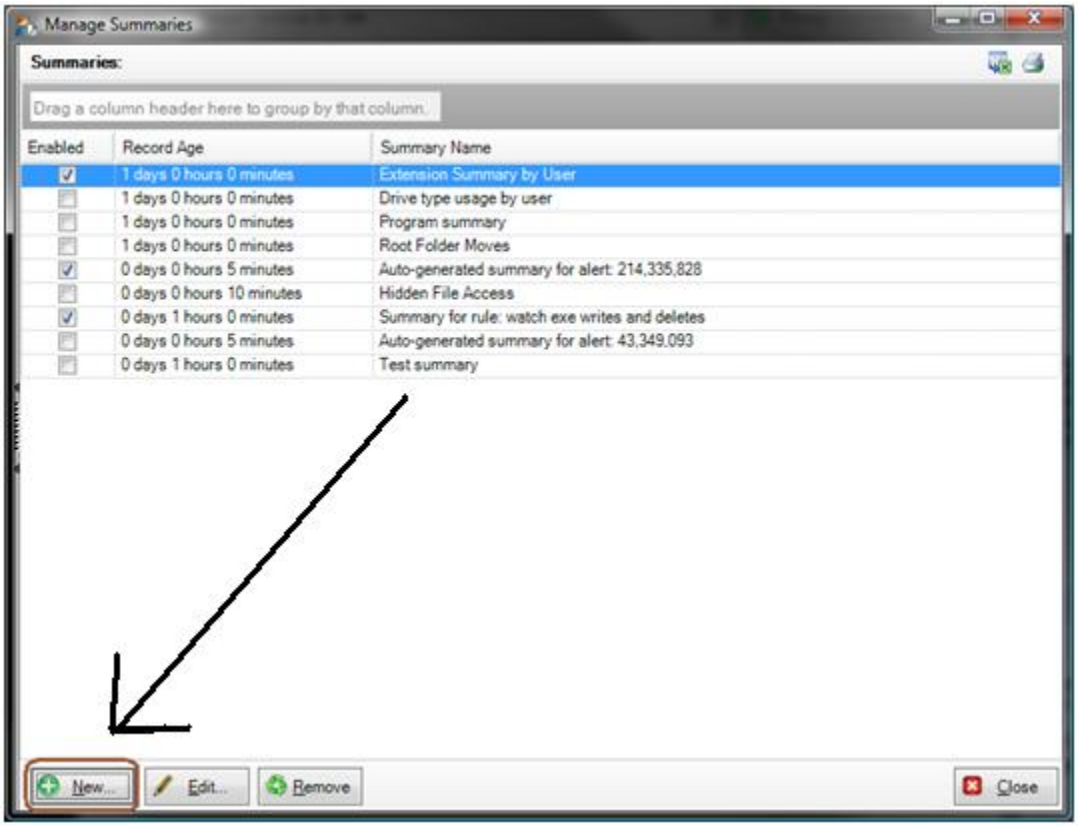
8. Now we have a daily report schedule handled, but we need to know about file deletions as they happen. For that, we need to set up an Alert. Back on the main screen, select the 'Common tasks' and click the 'Set up an e-mail alert' button.



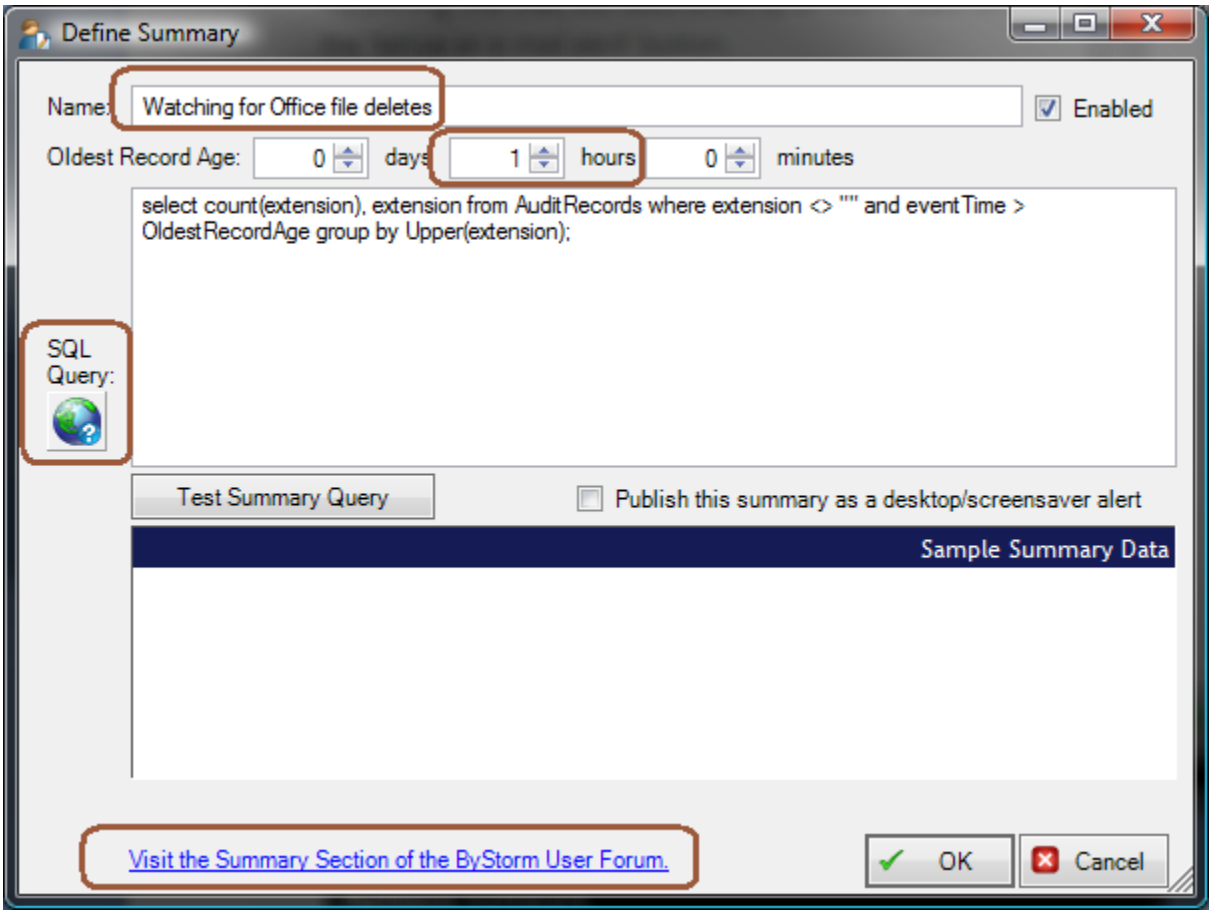
9. This will bring up the ‘Define Alert’ screen which is where we will configure the alert but before we can do that we need to set up a summary. Click the ‘Manage Summaries’ button.



10. This will bring up the 'Manage summaries' screen which shows all the current summaries. On this screen, click the 'New' button.



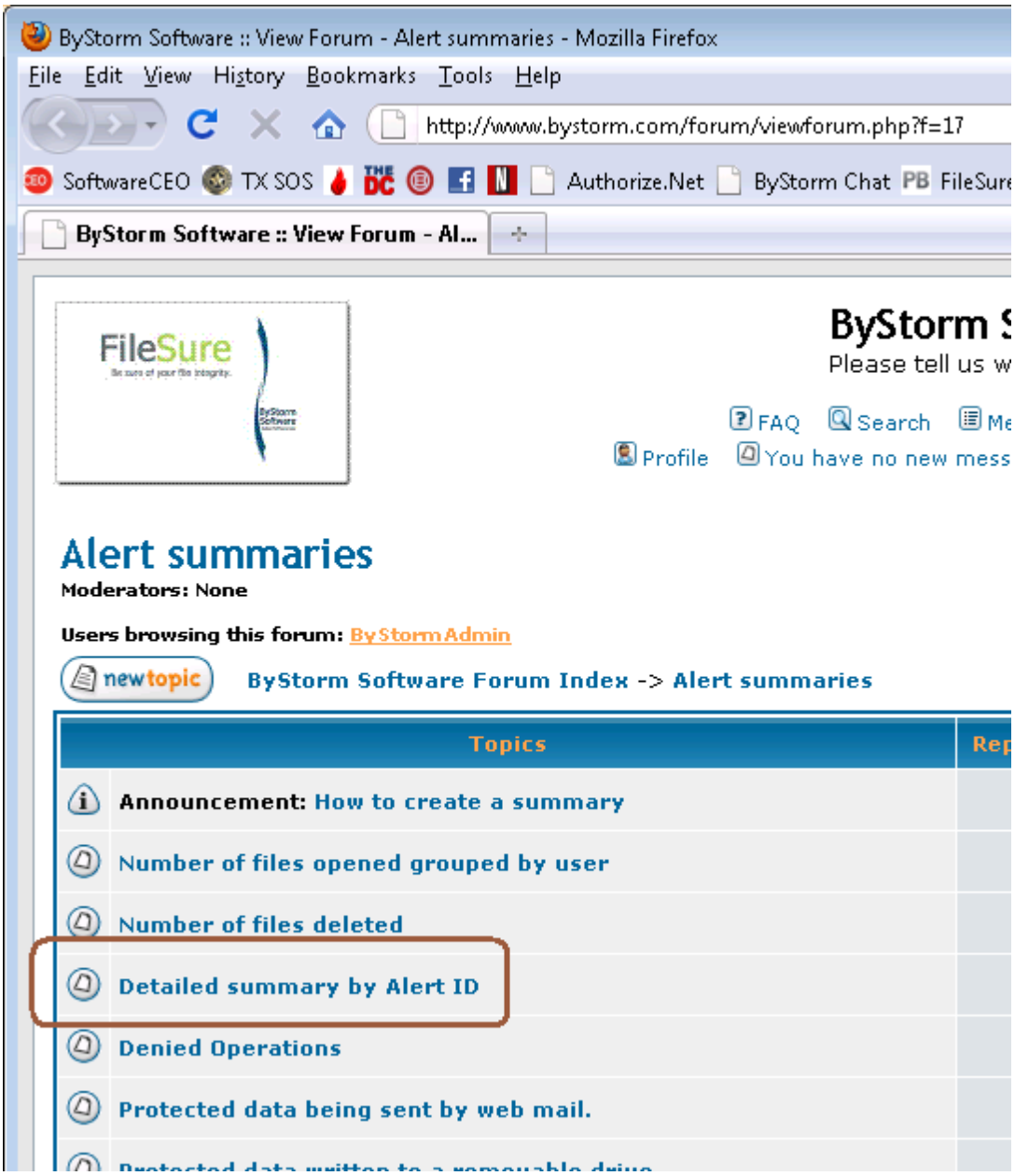
11. This will bring up the 'Define Summary' screen. Here is how to configure the summary:



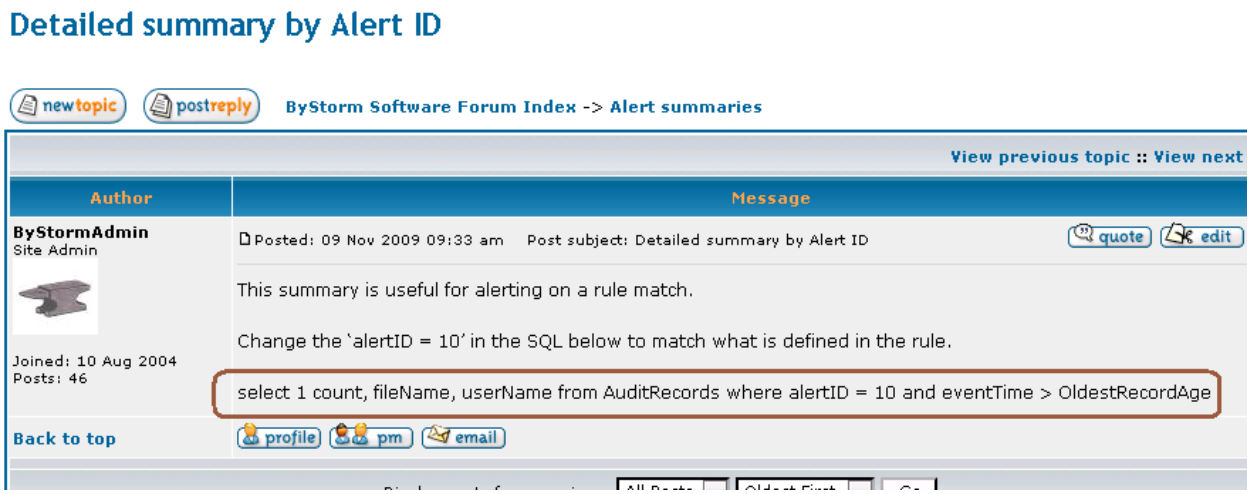
a. Enter 'Watching for Office file deletes' for the 'Name'

b. Enter ‘1’ in the hour section ‘Oldest Record Age’. This tells FileSure that we only want to look in the past hour for events. We do this so we don’t continue to send out alerts for old events.

c. Click either the little ‘world’ button or the ‘Visit the summary section of the ByStorm User Forum’ link. This will open a browser to the ByStorm Forum:



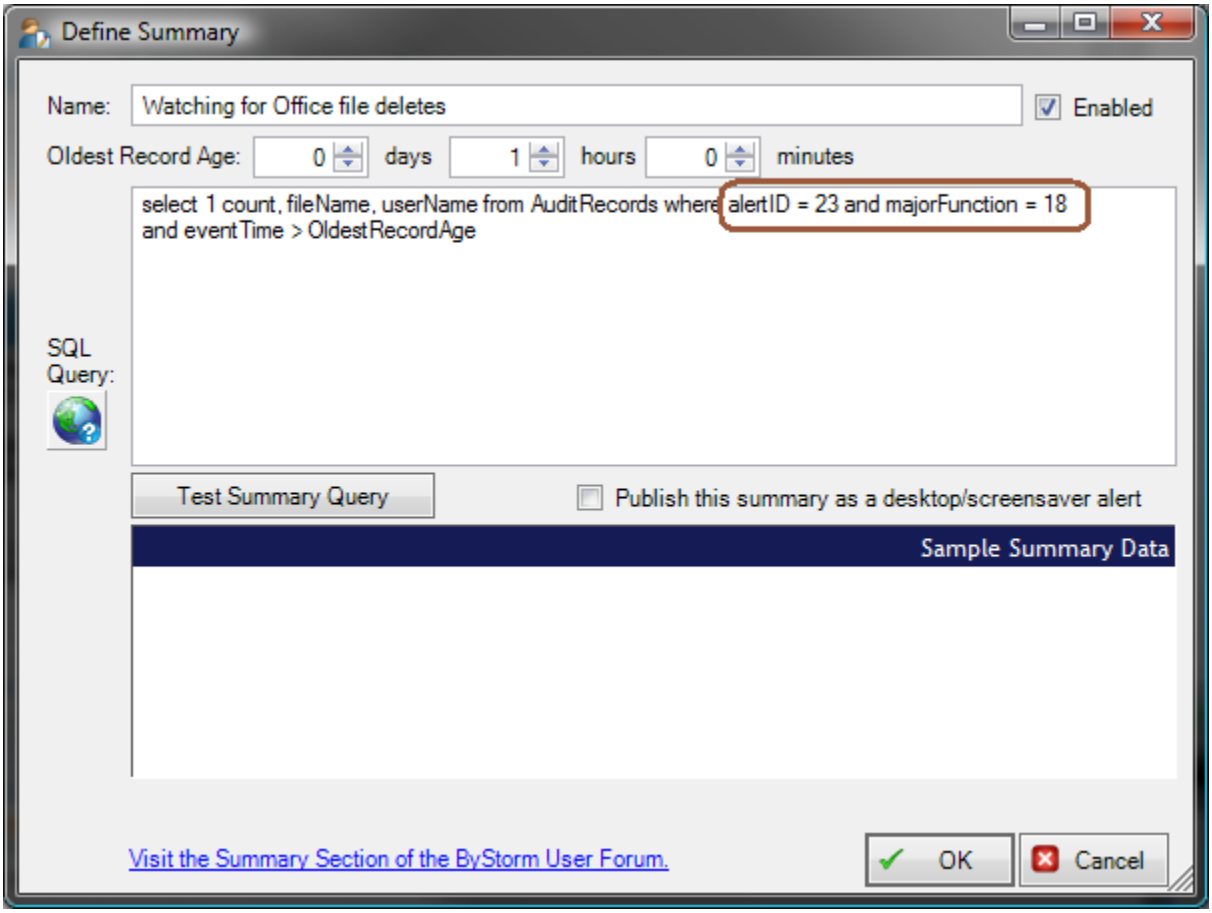
d. Select the ‘Detailed summary by Alert ID’ link



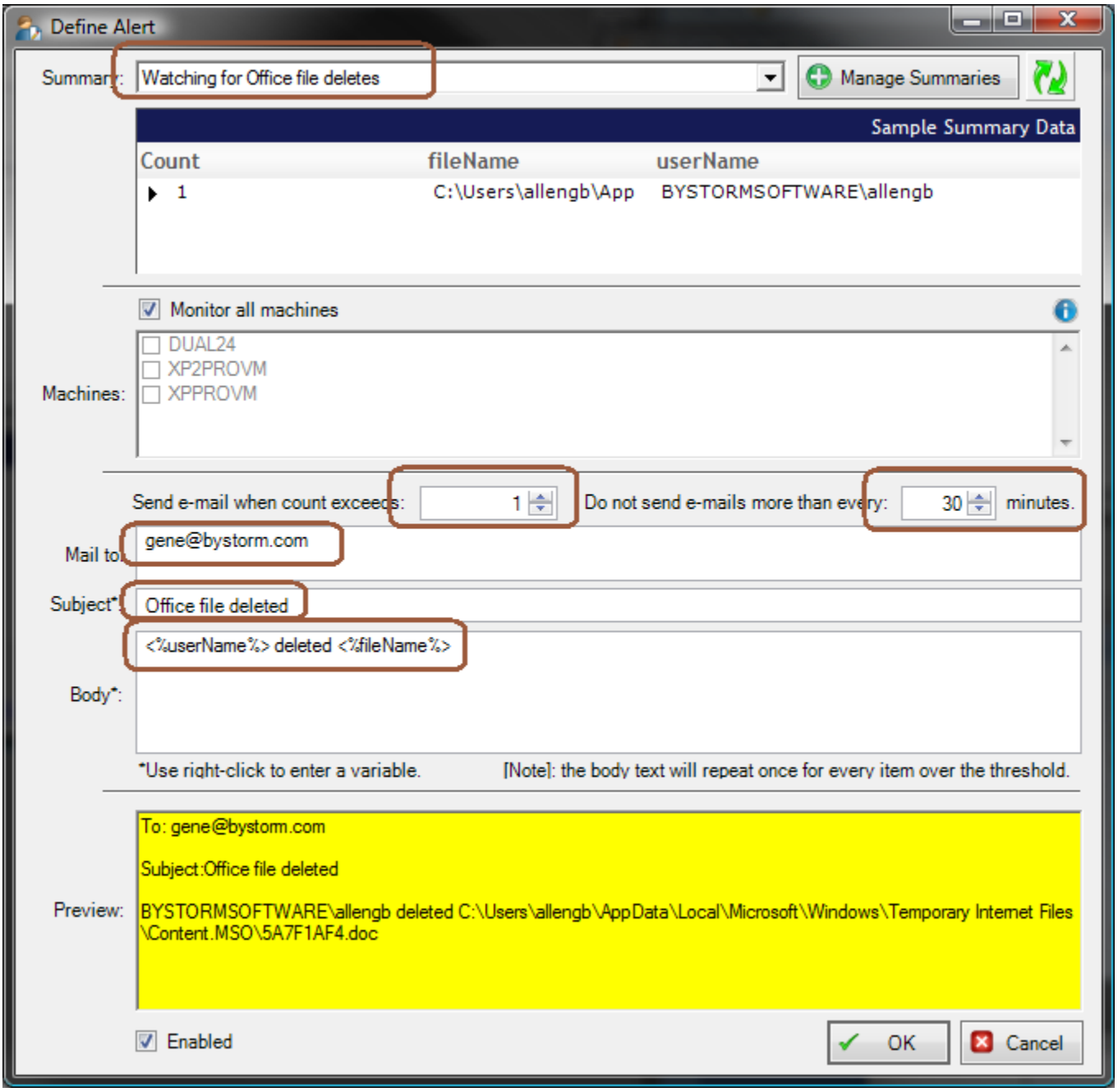
e. Copy the circled area into the clipboard. Here is the actual text: '*select 1 count, fileName, userName from AuditRecords where alertID = 10 and eventTime > OldestRecordAge*'.

f. Paste the text into the SQL Query area of the alert and change the '10' to '23' to match the alert ID we put on the rule. Since our auditing rule watches all operations on Office files, we need to change it just a bit since we only want to pick up delete, so add an additional condition. Here is the final SQL Query:

   i. select 1 count, fileName, userName from AuditRecords where alertID = 23 and majorFunction = 18 and eventTime > OldestRecordAge



12. Click 'OK' to close the summary screen and click 'Close' on the 'Manage Summaries', this will take you back to the 'Define Alert' screen. Define your alert like this:



a. Pick the newly created 'Watching for Office file deletes' summary from the drop down.
b. Enter '1' for the 'Send e-mail when count exceeds'
c. Enter '30' for the 'Do not send e-mails more than every'
d. Enter the email address you want the alert to be sent to
e. Enter 'Office file deleted' for the 'Subject'
f. For the body enter:

```
<%userName%> deleted <%fileName%>.
```

g. Click 'OK' to close the 'Define Alert' screen

Now we have an alert configured to send an alert when someone deletes an Office file anywhere on our server.

To recap, FileSure is recording all activity to Microsoft Office files anywhere on the server, sending out e-mail alerts when someone deletes an Office file and a daily report of all Office files that were deleted is being sent.