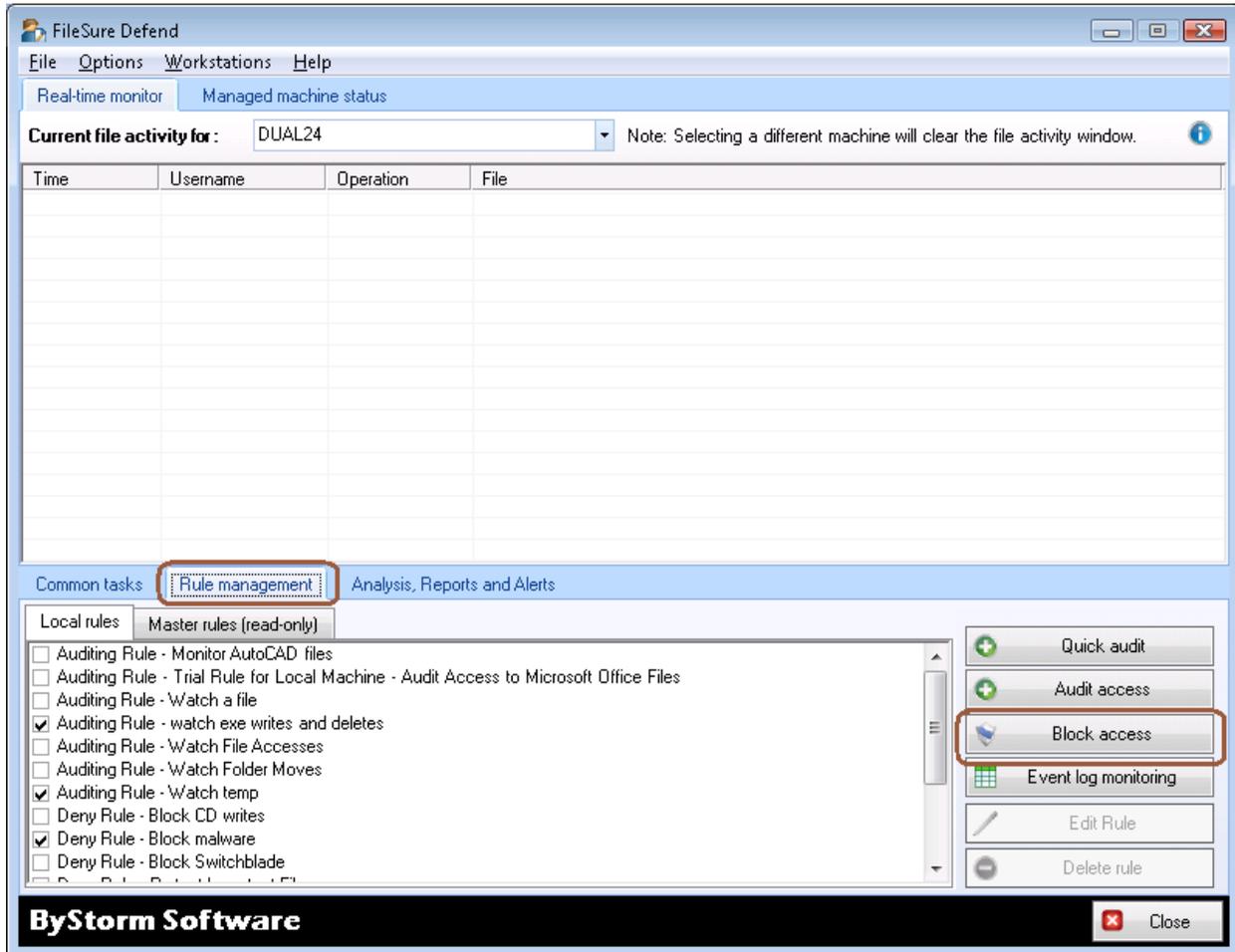
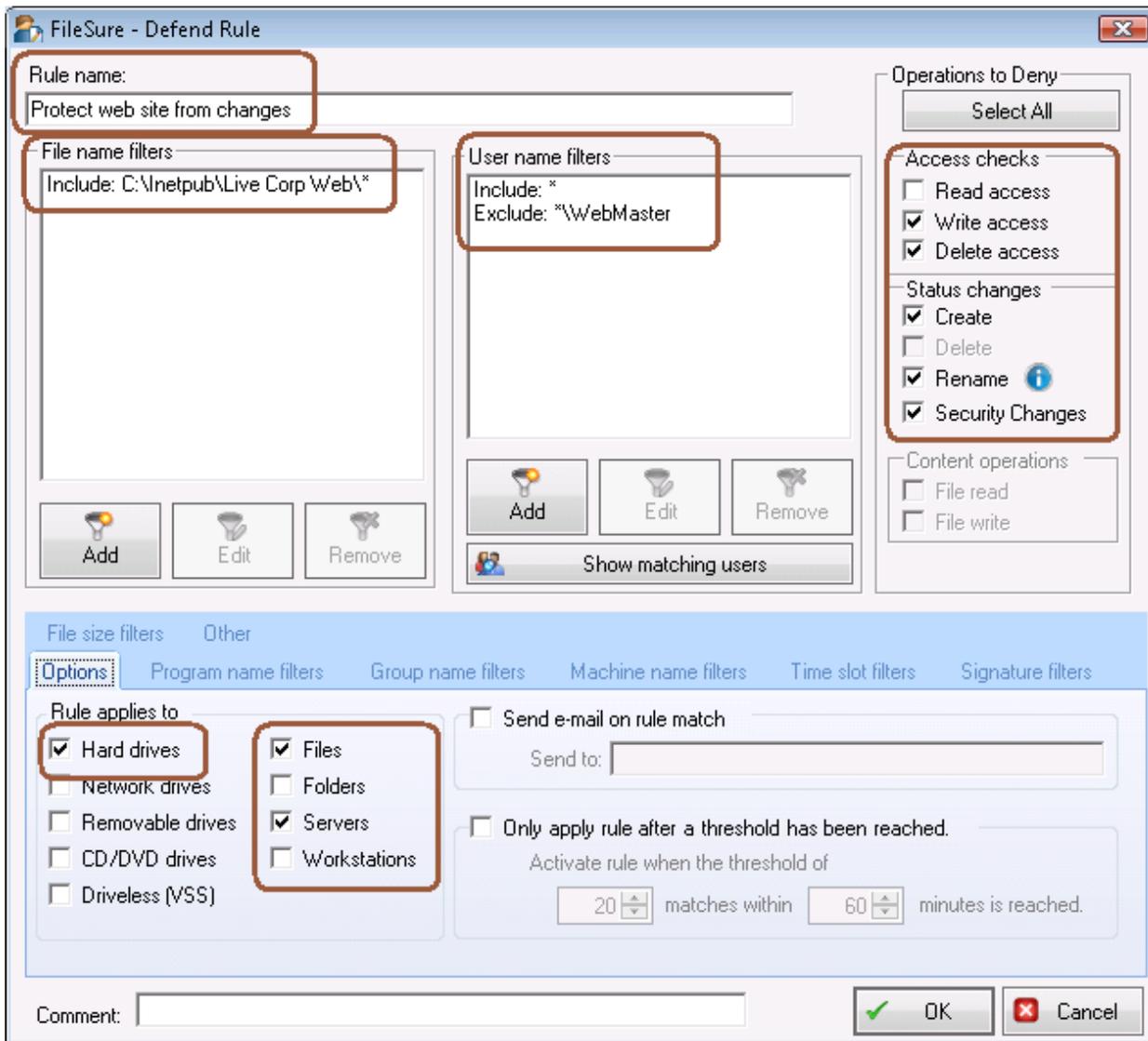


This 'How-to' will show how to configure FileSure-Defend to protect your website from change--except to certain users or at certain times. We will generate an e-mail alert when a change was blocked, and set up an automatic daily report showing all the changes that were attempted.

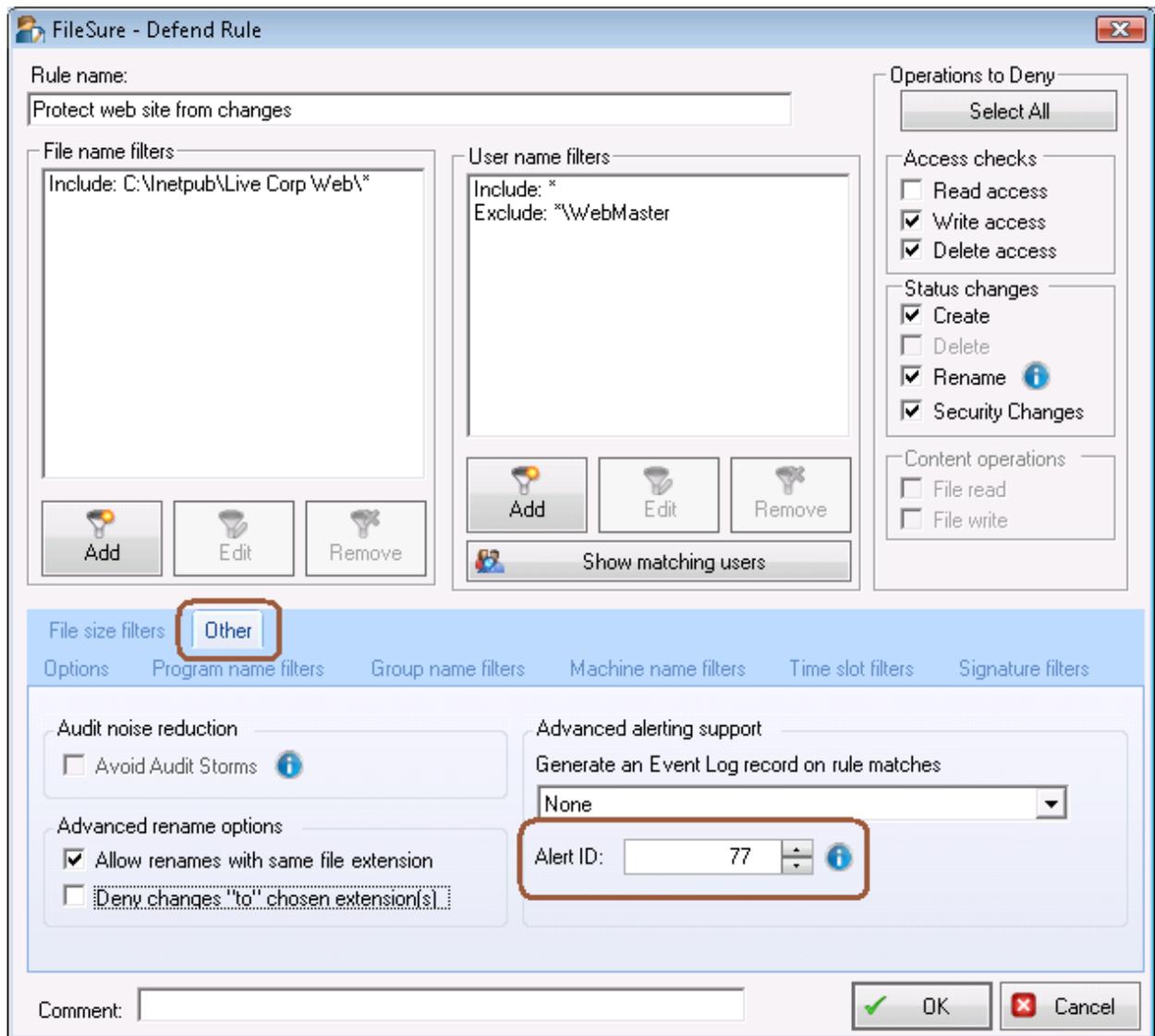
1. Start FileSure, switch to the 'Rules management' tab and click the 'Block access' button:



2. This will bring up the 'Defend Rule' screen (next page). We are going to configure an example rule involving only allowing access to the webmaster and only at a certain time of the week. You can tweak the criteria to fit your needs.

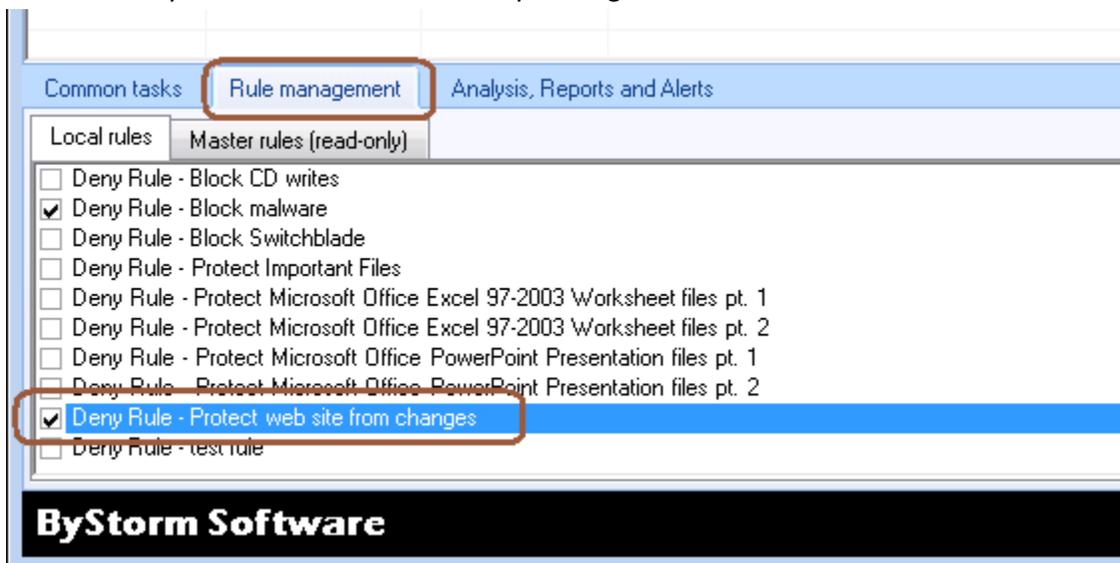


- a. Change the Rule Name to be 'Protect web site from changes'
- b. Check all the 'Operations to Deny' except for Read Access. This is telling FileSure not to allow any changes, but to let users read the files.
- c. In the 'Rule applies to' section, check only 'Hard drives', 'Files' and 'Servers'.
- d. Use the 'Add' button in the 'File name filters' area to enter a filter that points to your website on the hard drive. In my example, I'm protecting 'C:\inetpub\live corp\web*'. The '*' at the end means the rule applies to ALL files in that folder and any subfolder.
- e. Use the 'Add' button in the 'User name filters' area to enter a user name filter of '*'; this will cause the rule to be applied to all users.
- f. Use the 'Add' button in the 'User name filters' area to enter a user name filter of '*\WebMaster', this time click the 'Exclude' option instead of the default 'Include'. This will exclude the user 'WebMaster' from the rule.
- g. Click the 'Time slot filters' tab and select every time slot except for Saturday morning from 8AM to 12PM. [Note: if you click on the day, all time slots for that day will be selected]. This tells FileSure to enforce this rule all the time, except for Saturday mornings...say for scheduled maintenance.



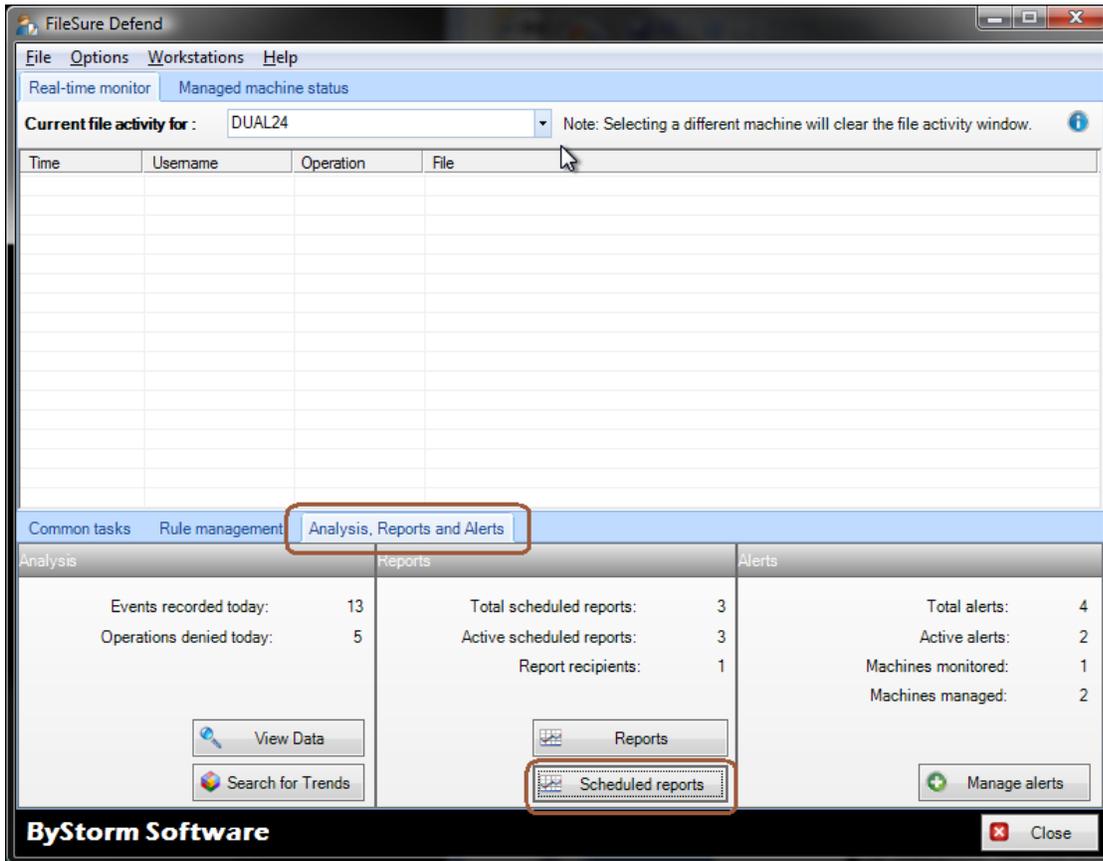
i. Click 'OK' to close the rule.

3. Find the newly created rule and enable it by clicking the checkbox next to the rule name



At this point, FileSure is protecting your website from changes and recording any attempts in the auditing 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.



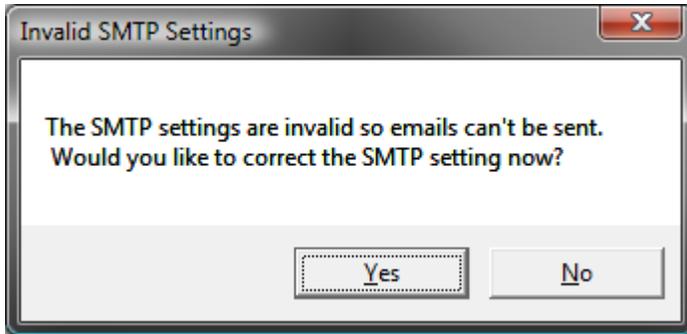
5. This will bring up the 'Schedule Reports' where you need to click the 'New' button. Note the 'Scheduled job execution time' as this is the time that the reports will run everyday.



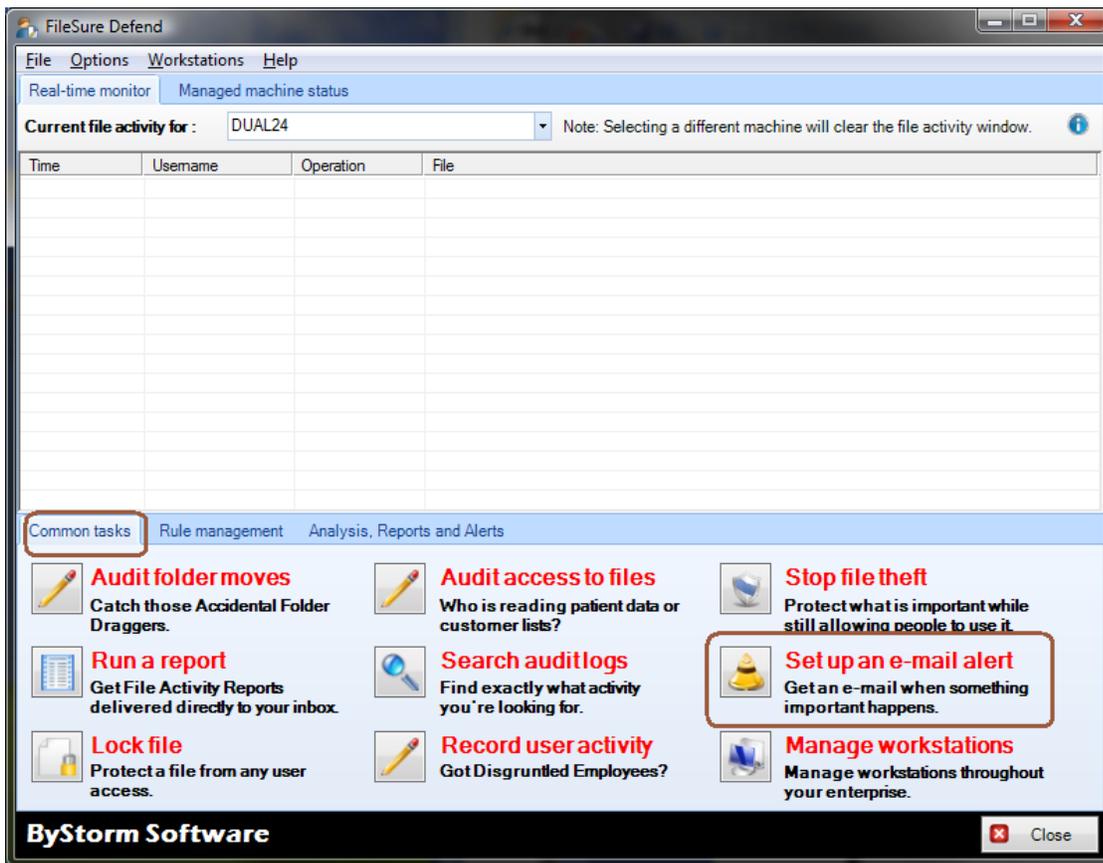
6. This will bring up the 'Edit Job' screen. This is where we will configure the scheduled report. Change the following things:

- Enter 'Attempted web site changes' for the 'Job Name'
- Select the 'User Activity Report: Write access denied' in the 'Report name' drop down.
- For the 'Date Range', select the 'Quick Range' of 'Previous day'
- In the 'Mail to' area, enter the e-mail address of who should get the report.
- In the 'Schedule' area, select the additional options of 'Saturday' and 'Sunday'

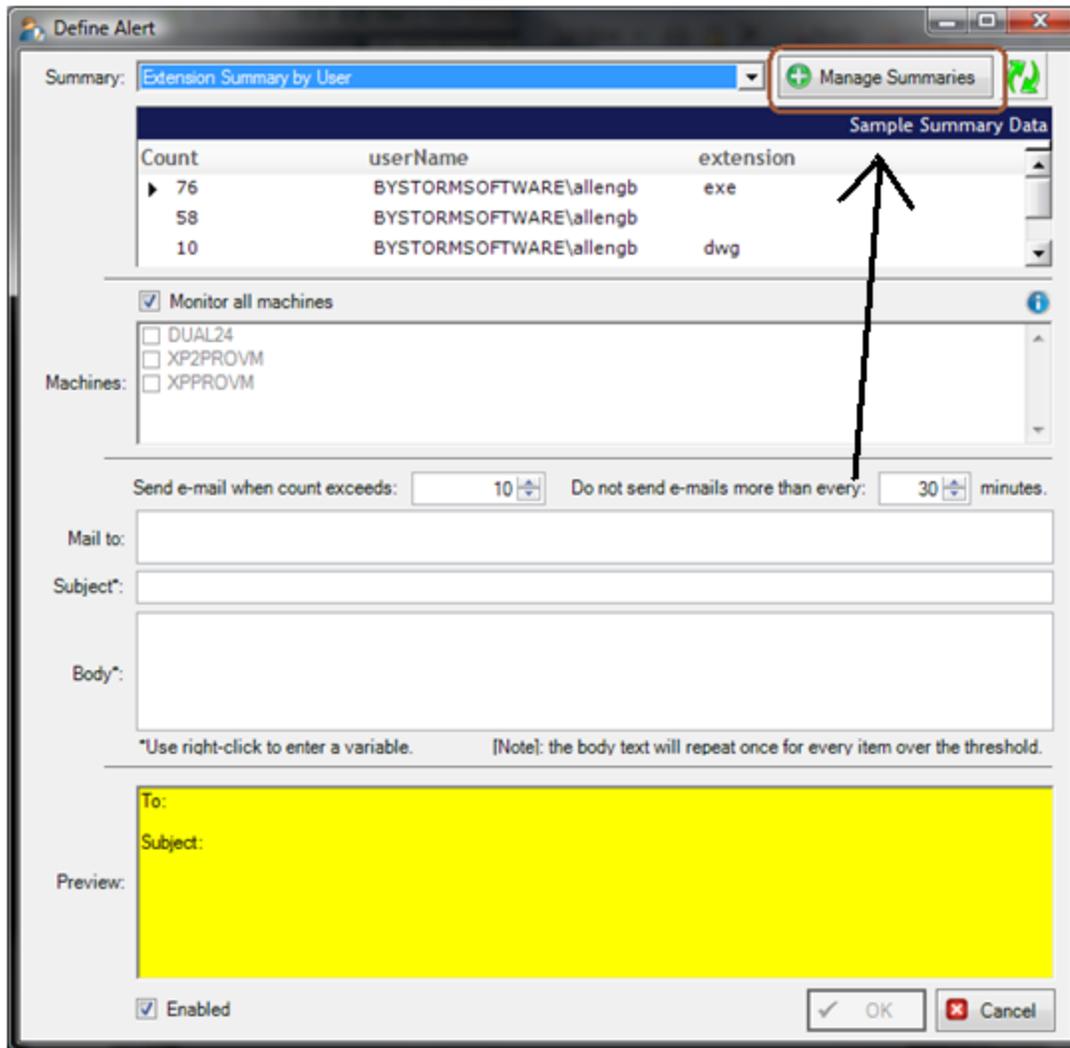
- Click OK to close the screen and save the report job. Click 'Close' on the 'Schedule Reports' screen. If haven't already configured your SMTP settings, you will be prompted to do so.



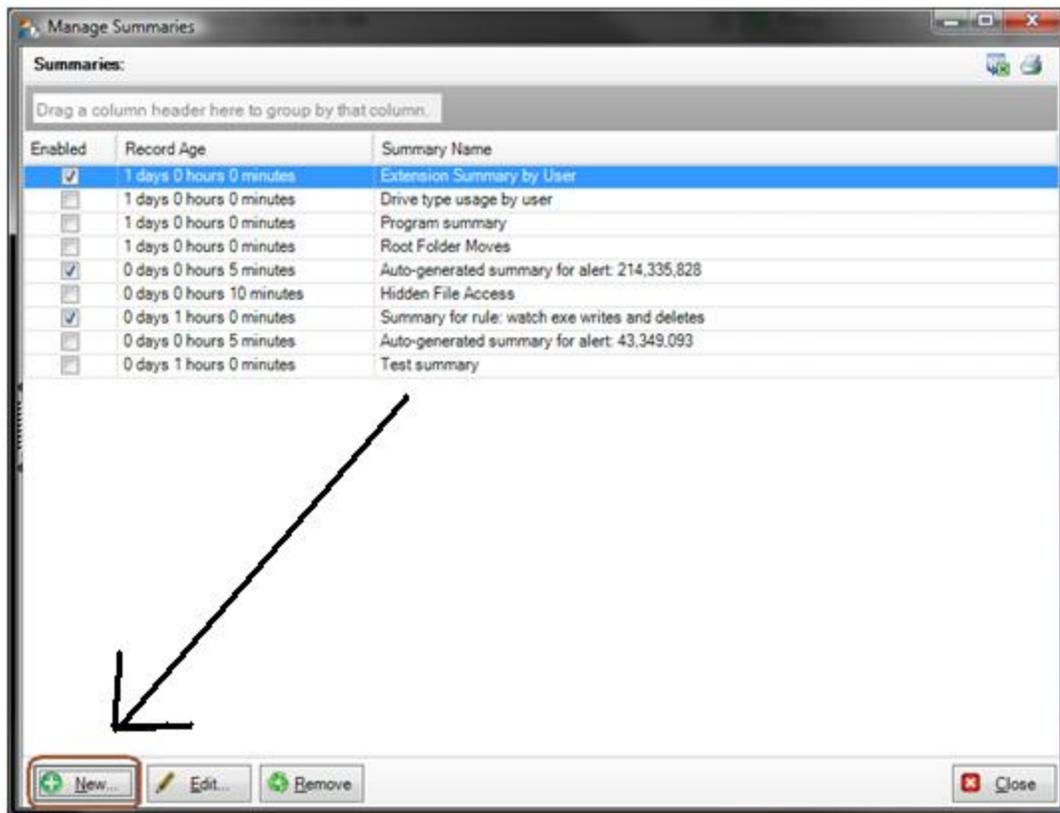
- Now we have a daily report scheduled, but we want to know about the change attempts as they are happening. For that, we need to set up an Alert. Back on the main screen, select the 'Common tasks' and click the 'Set up an e-mail alert' button.



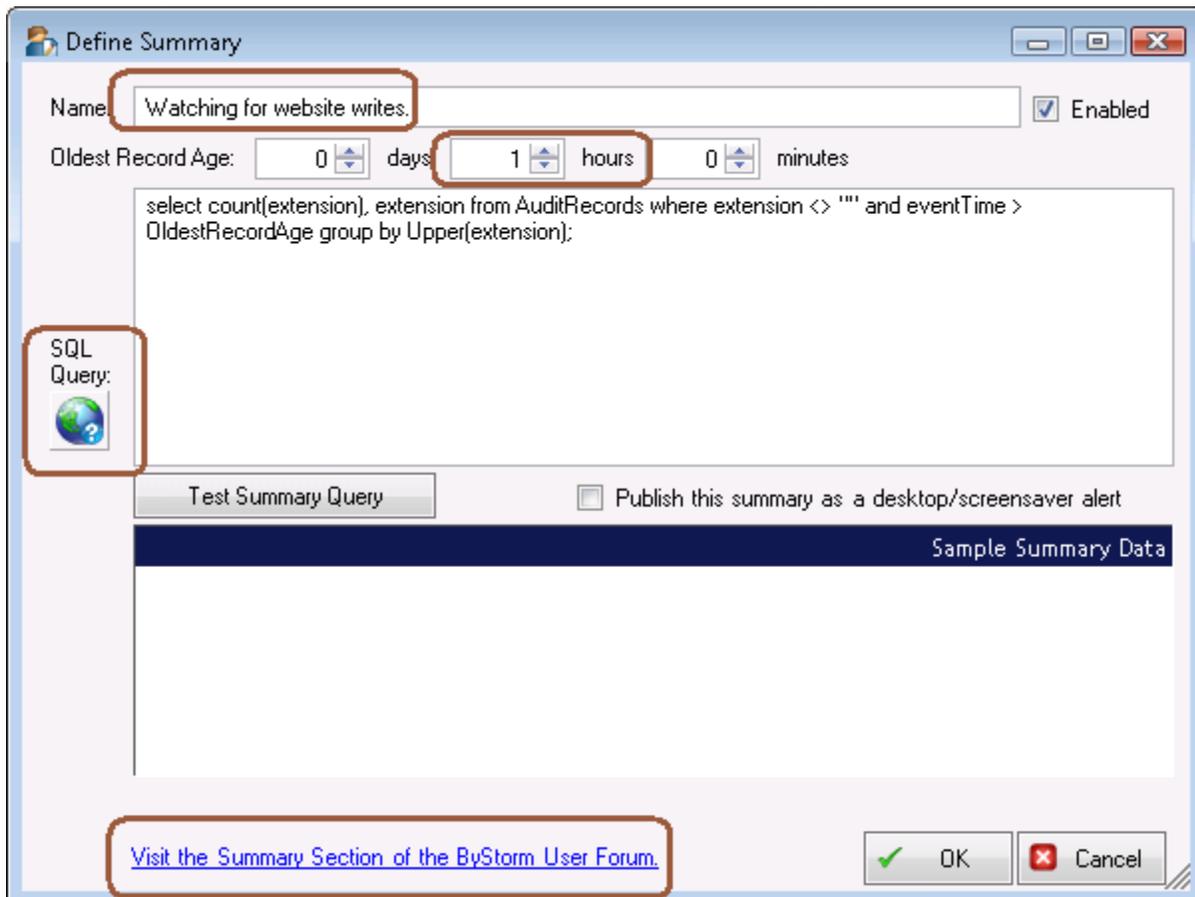
9. This will bring up the 'Define Alert' screen which is where we will configure the alert, but before we can do that we need to set up a summary. Click the 'Manage Summaries' button.



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 website writes' 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:

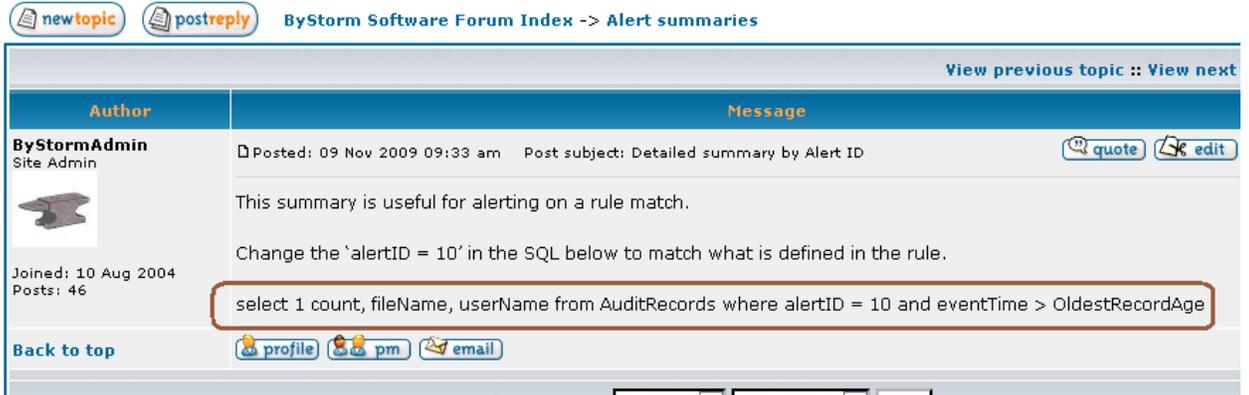
The screenshot shows a Mozilla Firefox browser window with the following details:

- Browser title: ByStorm Software :: View Forum - Alert summaries - Mozilla Firefox
- Address bar: http://www.bystorm.com/forum/viewforum.php?f=17
- Page content:
 - FileSure logo with tagline "Be sure of your file integrity."
 - ByStorm Software logo
 - Navigation links: FAQ, Search, Profile, You have no new messages
 - Section header: **Alert summaries**
 - Moderators: None
 - Users browsing this forum: [ByStormAdmin](#)
 - Buttons: [new topic](#), [ByStorm Software Forum Index -> Alert summaries](#)
 - Table of Topics:

Topics	Rep
Announcement: How to create a summary	
Number of files opened grouped by user	
Number of files deleted	
Detailed summary by Alert ID	
Denied Operations	
Protected data being sent by web mail.	
Protected data written to a removable drive	

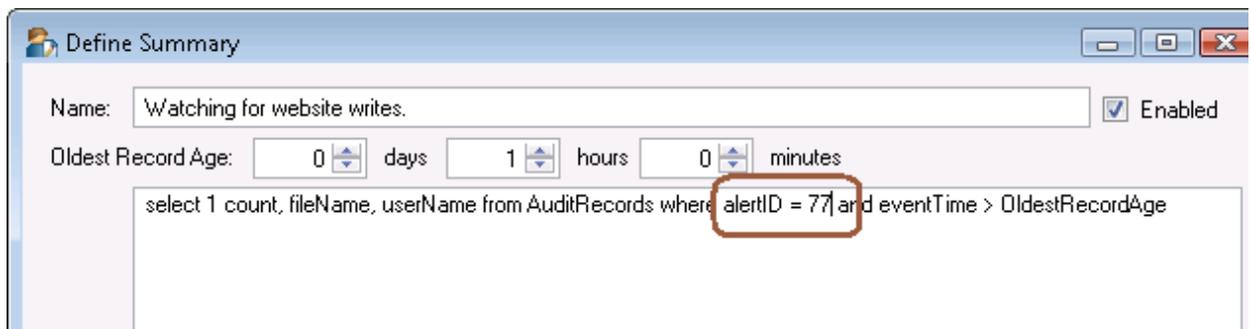
- d. Select the 'Detailed summary by Alert ID' link

Detailed summary by Alert ID



The screenshot shows a forum post from 'ByStormAdmin' (Site Admin) dated 09 Nov 2009. The post subject is 'Detailed summary by Alert ID'. The message content includes a SQL query: `select 1 count, fileName, userName from AuditRecords where alertID = 10 and eventTime > OldestRecordAge`. This query is circled in red. The forum interface includes navigation links like 'new topic', 'postreply', and 'View previous topic :: View next'.

- 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 '77' to match the alert ID we put on the rule.



The screenshot shows the 'Define Summary' dialog box. The 'Name' field contains 'Watching for website writes.' and the 'Enabled' checkbox is checked. The 'Oldest Record Age' is set to 0 days, 1 hour, and 0 minutes. The SQL query field contains: `select 1 count, fileName, userName from AuditRecords where alertID = 77 and eventTime > OldestRecordAge`. The '77' in the query is circled in red.

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:

Define Alert

Summary: Watching for website writes. Manage Summaries

Count	fileName	userName
Sample Summary Data		

Monitor all machines

Machines:

- DUAL24
- XP2PROVM
- XPPROVM

Send e-mail when count exceeds: 1 Do not send e-mails more than every: 30 minutes.

Mail to: gene@bystorm.com

Subject*: Website change denied!

Body*: <%userName%> was denied the ability to change <%fileName%>

*Use right-click to enter a variable. [Note]: the body text will repeat once for every item over the threshold.

Preview:

```
To: gene@bystorm.com
Subject: Website change denied!
```

Enabled OK Cancel

- a. Pick the newly created 'Watching for website writes' 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 'Website change denied!' for the 'Subject'
- f. For the body enter:
 - <%userName%> was denied the ability to change <%fileName%>.
- g. Click 'OK' to close the 'Define Alert' screen

Now we have an alert configured to send an alert when someone is blocked from changing a file on our website.

To recap: We have set FileSure-Defend to block writing, deleting, renaming or changing security on any file on our web site except when those changes are made by the user 'WebMaster' or during our scheduled maintenance time of Saturday morning.

We have scheduled a report to be sent everyday listing all blocked changes.

We have set up an alert to tell us when someone has attempted to change the website, right as it happens.