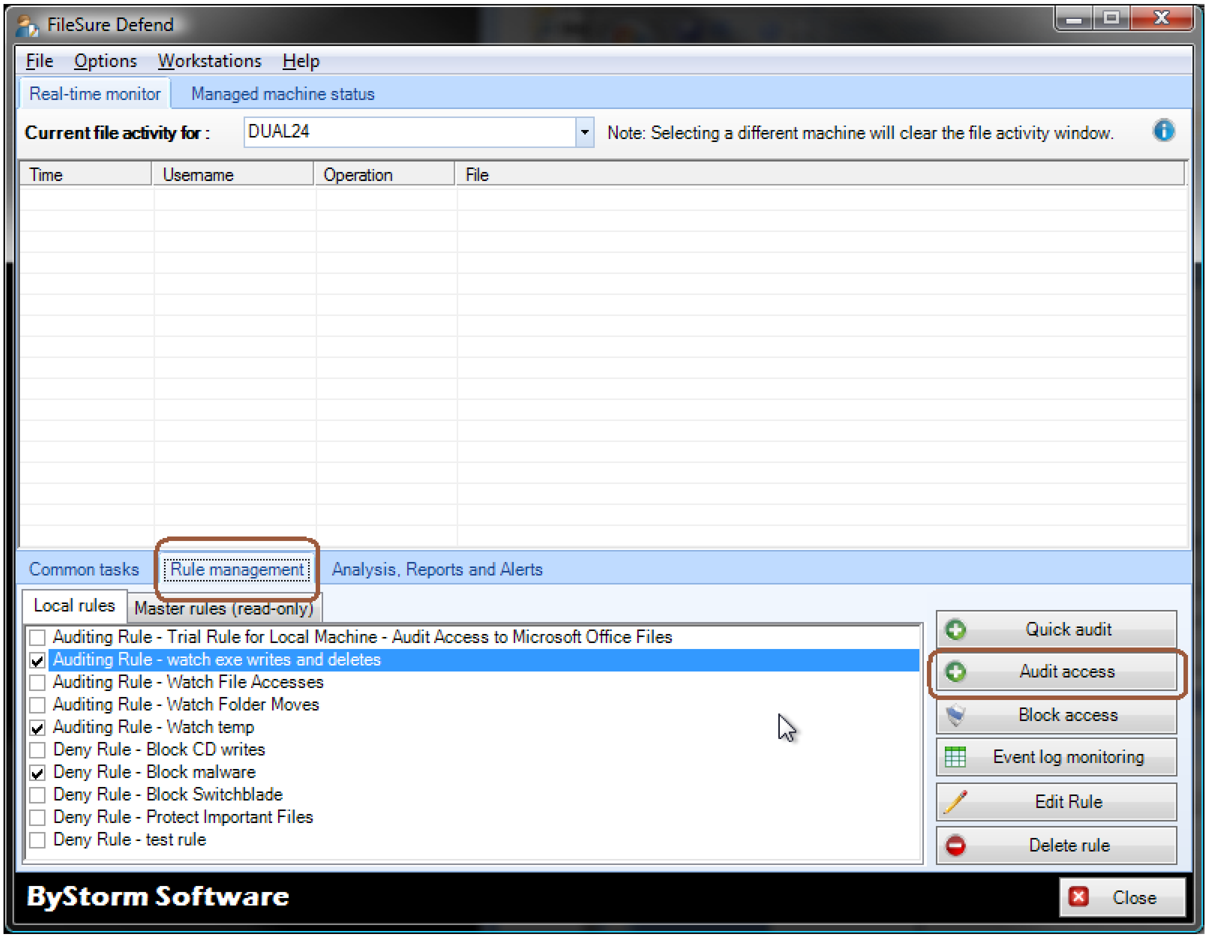
This ‘How-to’ will show how to configure FileSure to audit AutoCAD files. We will generate an e-mail alert when an AutoCAD file is either written to a removable drive or attached to an e-mail. We will also set up an automatic daily possible theft report.

1. Start FileSure, switch to the ‘Rules management’ tab and click the ‘Audit access’ button:

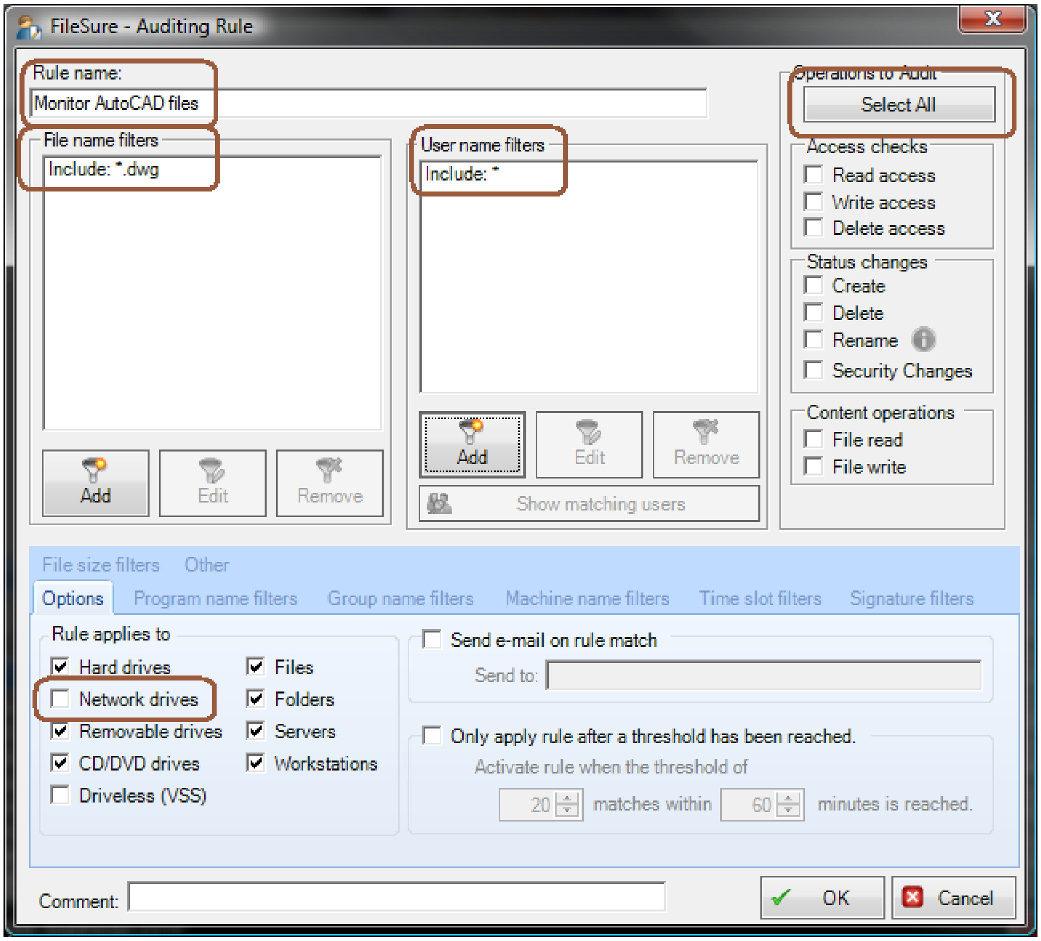


Current file activity for : DUAL24

Note: Selecting a different machine will clear the file activity window.

- ☐ Auditing Rule - Trial Rule for Local Machine - Audit Access to Microsoft Office Files
- ☑ Auditing Rule - watch exe writes and deletes
- ☐ Auditing Rule - Watch File Accesses
- ☐ Auditing Rule - Watch Folder Moves
- ☑ Auditing Rule - Watch temp
- ☐ Deny Rule - Block CD writes
- ☑ Deny Rule - Block malware
- ☐ Deny Rule - Block Switchblade
- ☐ Deny Rule - Protect Important Files
- ☐ Deny Rule - test rule

2. This will bring up the ‘Auditing Rule’ screen:



FileSure - Auditing Rule

Rule name: Monitor AutoCAD files

File name filters: Include: *.dwg

User name filters: Include: *

Operations to Audit

Access checks: □ Read access □ Write access □ Delete access

Status changes: □ Create □ Delete □ Rename □ Security Changes

Content operations: □ File read □ File write

Rule applies to:

☑ Hard drives ☑ Files

□ Network drives ☑ Folders

☑ Removable drives ☑ Servers

☑ CD/DVD drives ☑ Workstations

□ Driveless (VSS)

□ Send e-mail on rule match

Send to:

□ Only apply rule after a threshold has been reached.

Activate rule when the threshold of 20 matches within 60 minutes is reached.

Comment:

a. Change the Rule Name to be ‘Monitor AutoCAD files’

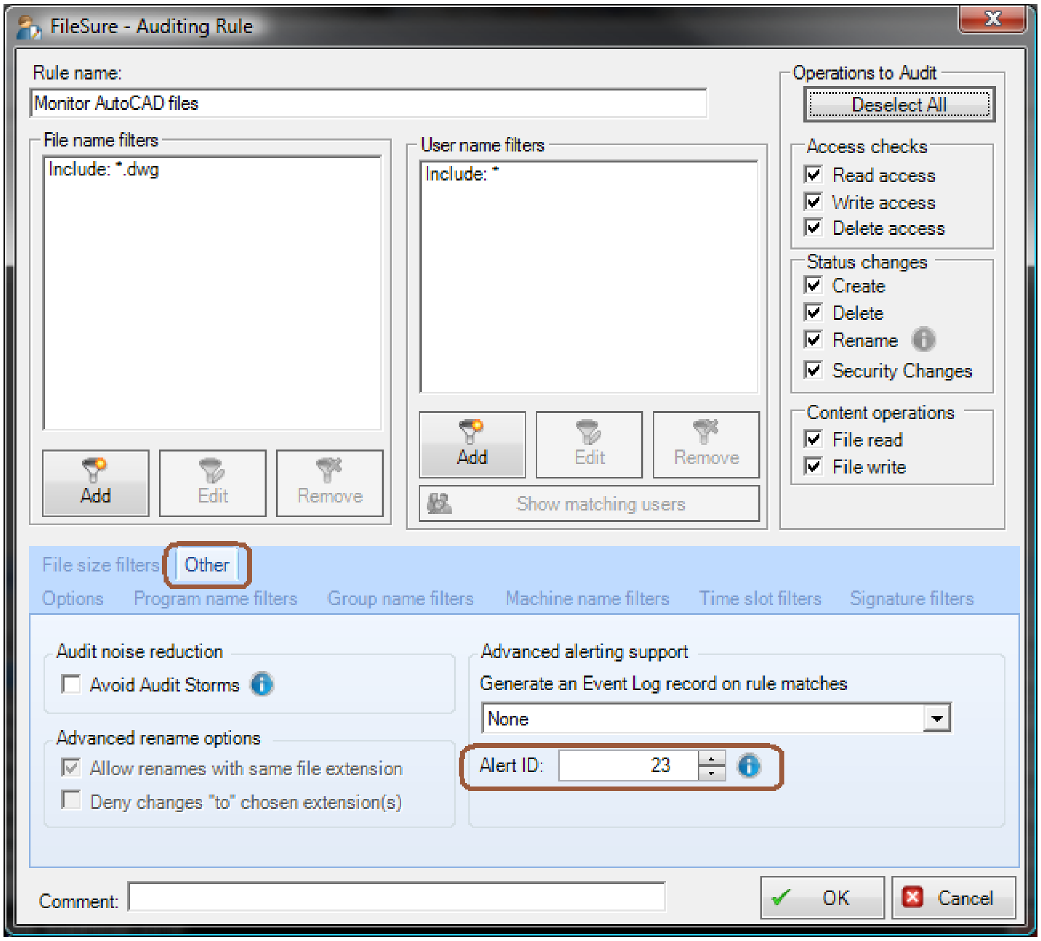
b. Click the ‘Select All’ button to turn on auditing for all the operations

c. Check the ‘Network drives’ so we pick up operations that occur on network drives

d. Use the ‘Add’ button in the ‘File name filters’ area to enter a file name filter of ‘*.dwg’. This filter will limit auditing to AutoCAD files.

e. Use the ‘Add’ button in the ‘User name filters’ are to enter a user name filter of ‘*’; this will cause the rule to be applied to all users.

f. Click the ‘Other’ tab and enter ‘23’ for the ‘Alert ID’ filter



Rule name: Monitor AutoCAD files

File name filters: Include: *.dwg

User name filters: Include: *

Access checks
☑ Read access
☑ Write access
☑ Delete access

Status changes
☑ Create
☑ Delete
☑ Rename
☑ Security Changes

Content operations
☑ File read
☑ File write

Audit noise reduction
□ Avoid Audit Storms

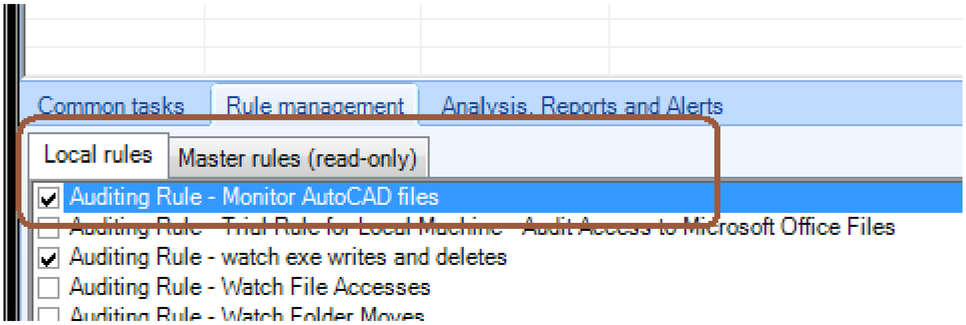
Advanced rename options
☑ Allow renames with same file extension
□ Deny changes "to" chosen extension(s)

Advanced alerting support
Generate an Event Log record on rule matches: None
Alert ID: 23

Comment:

g. Click ‘OK’ to close the rule.

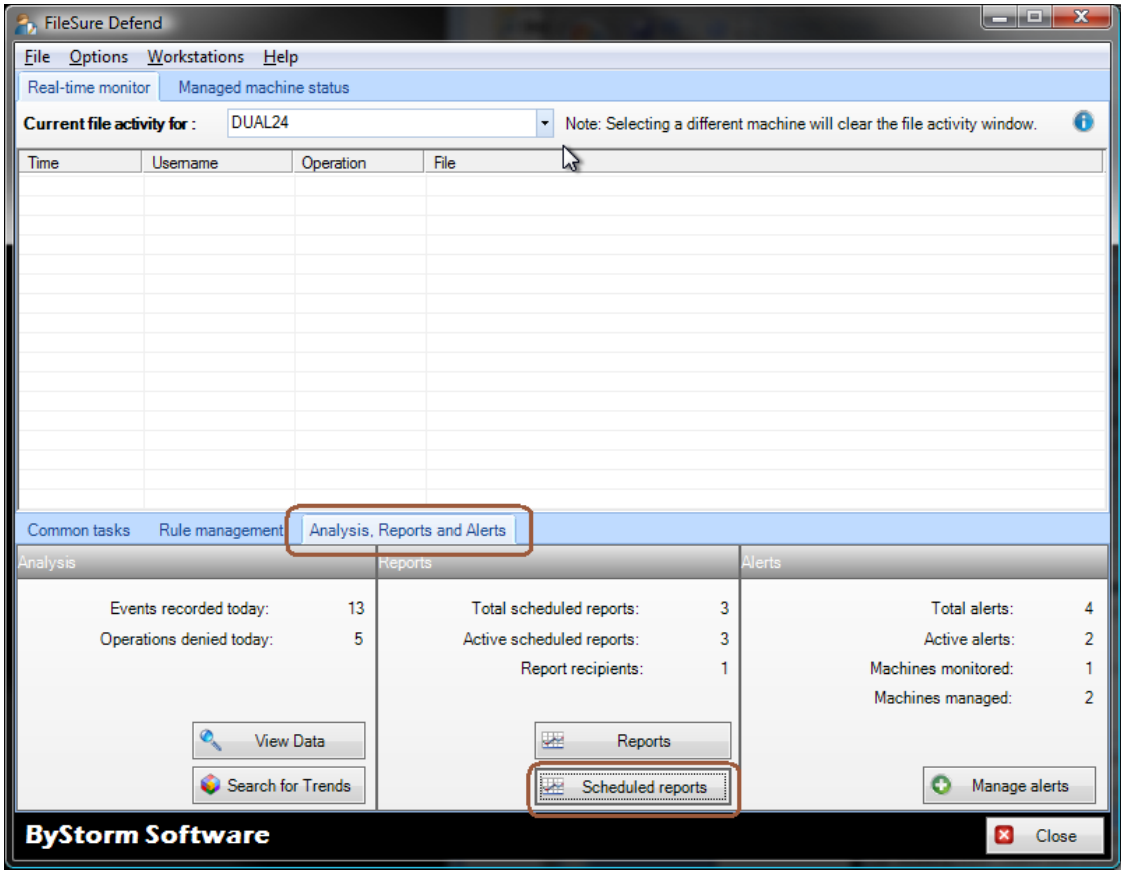
3. Find the newly created rule and enable it by clicking the checkbox next to the rule name



☑ Auditing Rule - Monitor AutoCAD files
□ Auditing Rule - Trial Rule for Local Machine - Audit Access to Microsoft Office Files
☑ Auditing Rule - watch exe writes and deletes
□ Auditing Rule - Watch File Accesses
□ Auditing Rule - Watch Folder Moves

At this point, FileSure is recording access to all files with the extension ‘DWG’ 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 repots’ button.

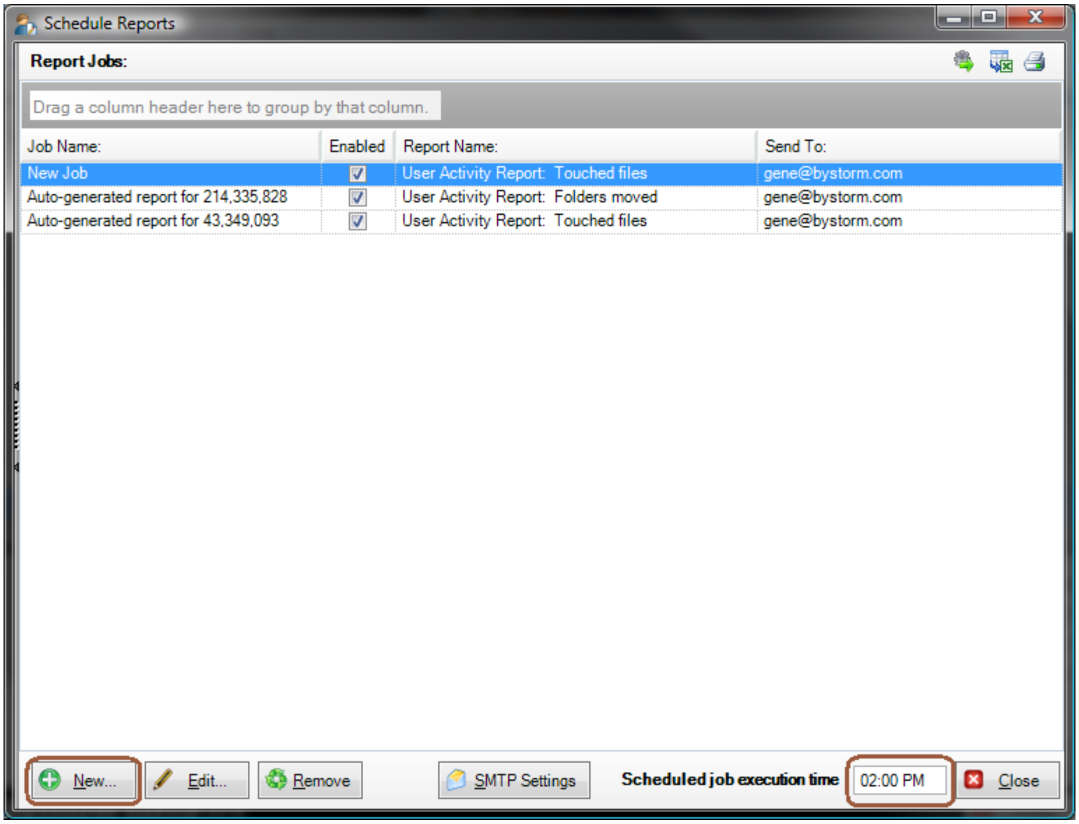


Current file activity for : DUAL24

Note: Selecting a different machine will clear the file activity window.

Events recorded today:	13
Operations denied today:	5
Total scheduled reports:	3
Active scheduled reports:	3
Report recipients:	1
Total alerts:	4
Active alerts:	2
Machines monitored:	1
Machines managed:	2

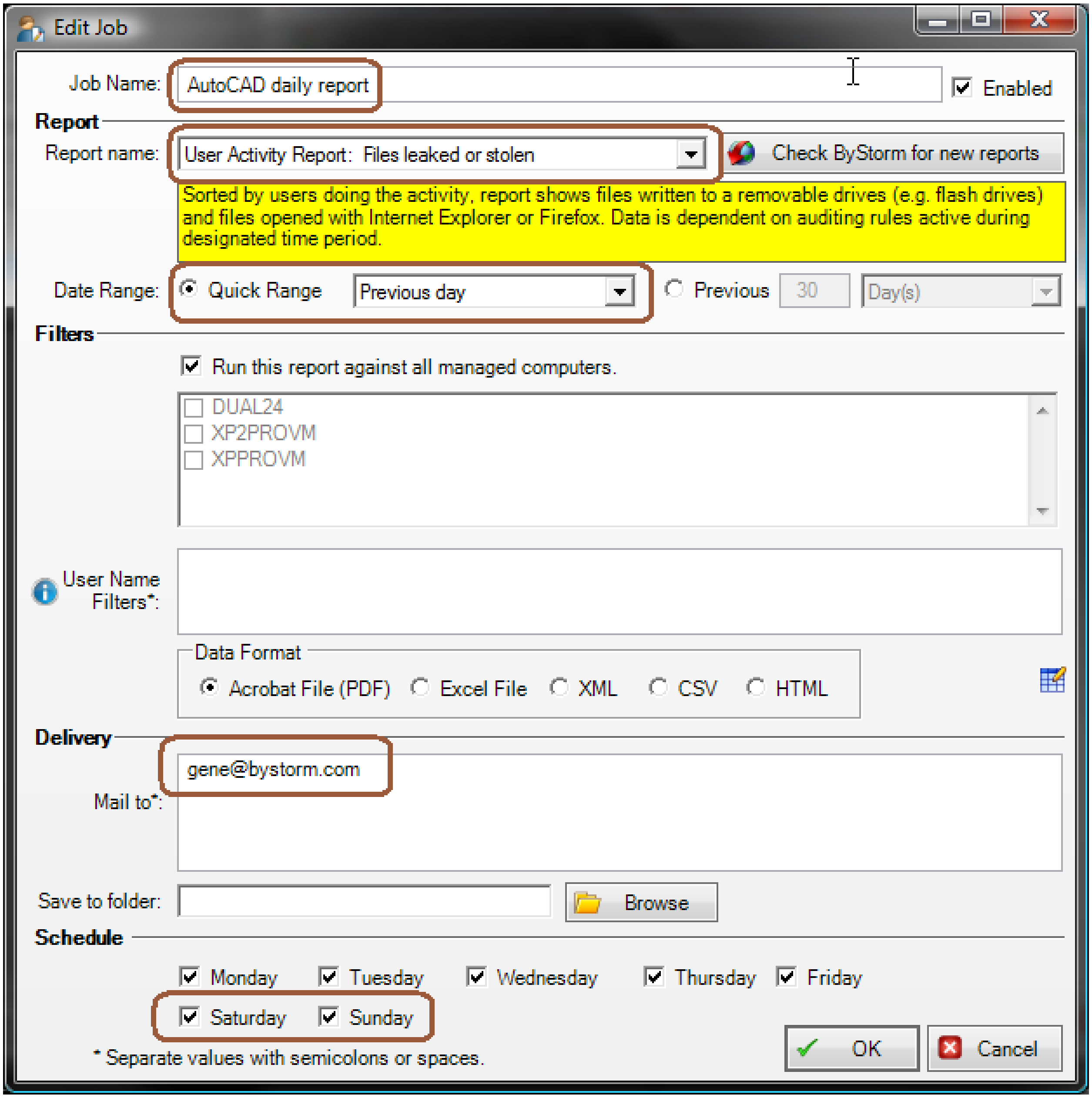
5. This will bring up the ‘Schedule Reports’ where you need to click the ‘New’ button. Note the ‘Scheduled job execution time’ as this is the time that the reports will run everyday.



Job Name:	Enabled	Report Name:	Send To:
New Job	☑	User Activity Report: Touched files	gene@bystorm.com
Auto-generated report for 214,335,828	☑	User Activity Report: Folders moved	gene@bystorm.com
Auto-generated report for 43,349,093	☑	User Activity Report: Touched files	gene@bystorm.com

Scheduled job execution time 02:00 PM

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



Edit Job

Job Name: AutoCAD daily report ☑ Enabled

Report

Report name: User Activity Report: Files leaked or stolen

Sorted by users doing the activity, report shows files written to a removable drives (e.g. flash drives) and files opened with Internet Explorer or Firefox. Data is dependent on auditing rules active during designated time period.

Date Range: ● Quick Range Previous day ○ Previous 30 Day(s)

Filters

☑ Run this report against all managed computers.

□ DUAL24
□ XP2PROVM
□ XPPROVM

User Name Filters*:

Data Format: ● Acrobat File (PDF) ○ Excel File ○ XML ○ CSV ○ HTML

Delivery

Mail to*: gene@bystorm.com

Save to folder:

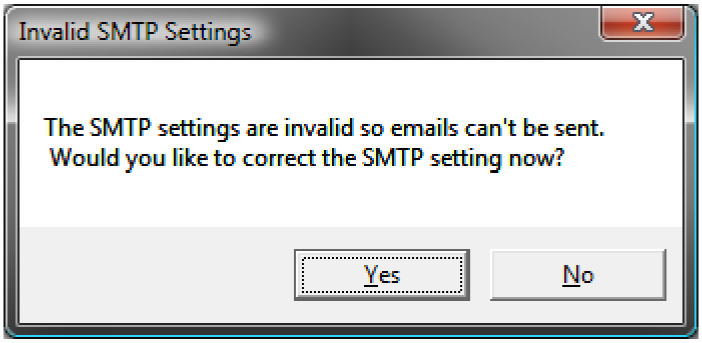
Schedule

☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday
☑ Saturday ☑ Sunday

* Separate values with semicolons or spaces.

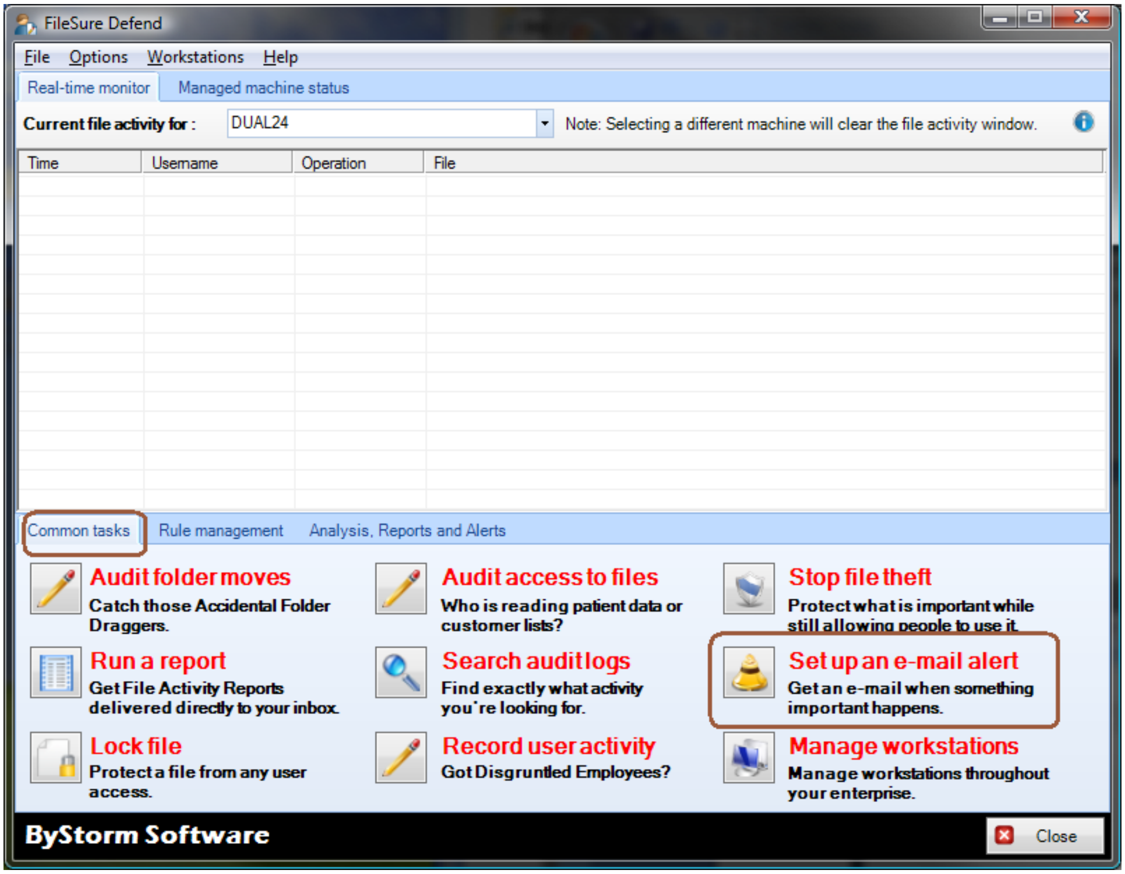
a. Enter 'AutoCAD daily report' for the 'Job Name'
b. Select the 'User Activity Report: Files leaked or stolen' in the 'Report name' drop down.
c. For the 'Date Range', select the 'Quick Range' of 'Previous day'
d. In the 'Mail to' area, enter the e-mail address of who should get the report.
e. In the '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.



The SMTP settings are invalid so emails can't be sent.
Would you like to correct the SMTP setting now?

8. Now we have a daily report scheduled, but we need to know about theft as it's happening. For that, we need to set up an Alert. Back on the main screen, select the 'Common tasks' tab and click the 'Set up an e-mail alert' button.

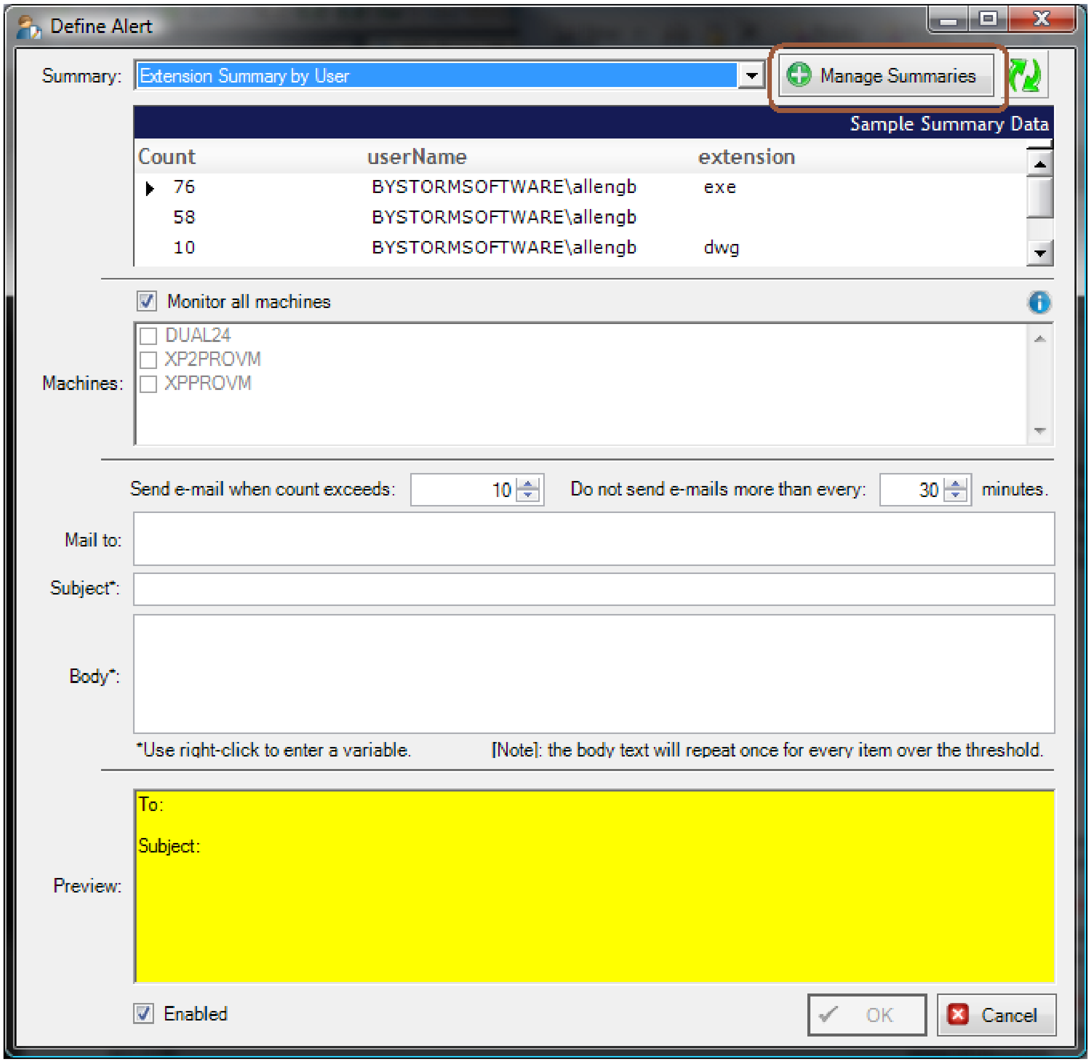


FileSure Defend
File Options Workstations Help
Real-time monitor
Managed machine status
Time
Username
Operation
File
Common tasks
Rule management
Analysis, Reports and Alerts
Audit folder moves
Catch those Accidental Folder Draggers.
Audit access to files
Who is reading patient data or customer lists?
Stop file theft
Protect what is important while still allowing people to use it.
Run a report
Get File Activity Reports delivered directly to your inbox.
Search audit logs
Find exactly what activity you're looking for.
Set up an e-mail alert
Get an e-mail when something important happens.
Lock file
Protect a file from any user access.
Record user activity
Got Disgruntled Employees?
Manage workstations
Manage workstations throughout your enterprise.
ByStorm Software
Close

Current file activity for : DUAL24

Note: Selecting a different machine will clear the file activity window.

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.



Summary: Extension Summary by User

Sample Summary Data

Count	userName	extension
76	BYSTORMSOFTWARE\allengb	exe
58	BYSTORMSOFTWARE\allengb	
10	BYSTORMSOFTWARE\allengb	dwg

☑ Monitor all machines

Machines:
□ DUAL24
□ XP2PROVM
□ XPPROVM

Send e-mail when count exceeds: 10 Do not send e-mails more than every: 30 minutes.

Mail to:

Subject*:

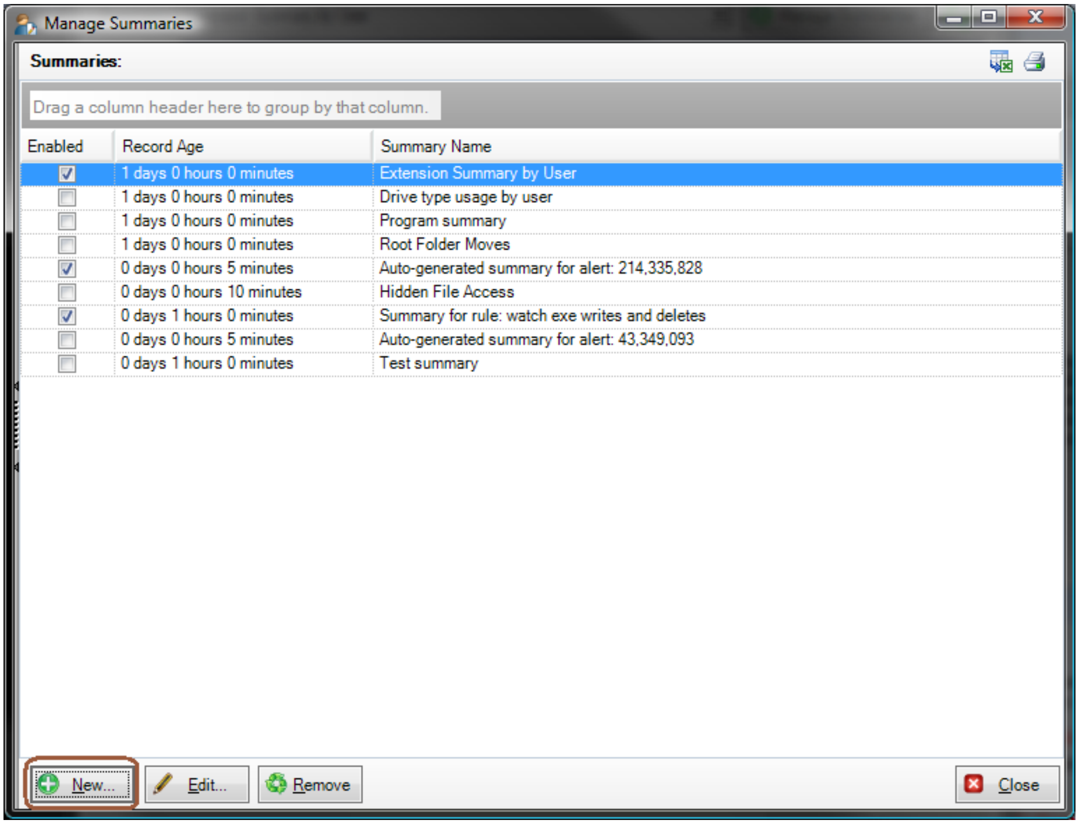
Body*:

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

Preview:
To:
Subject:

☑ Enabled

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



Summaries:

Drag a column header here to group by that column.

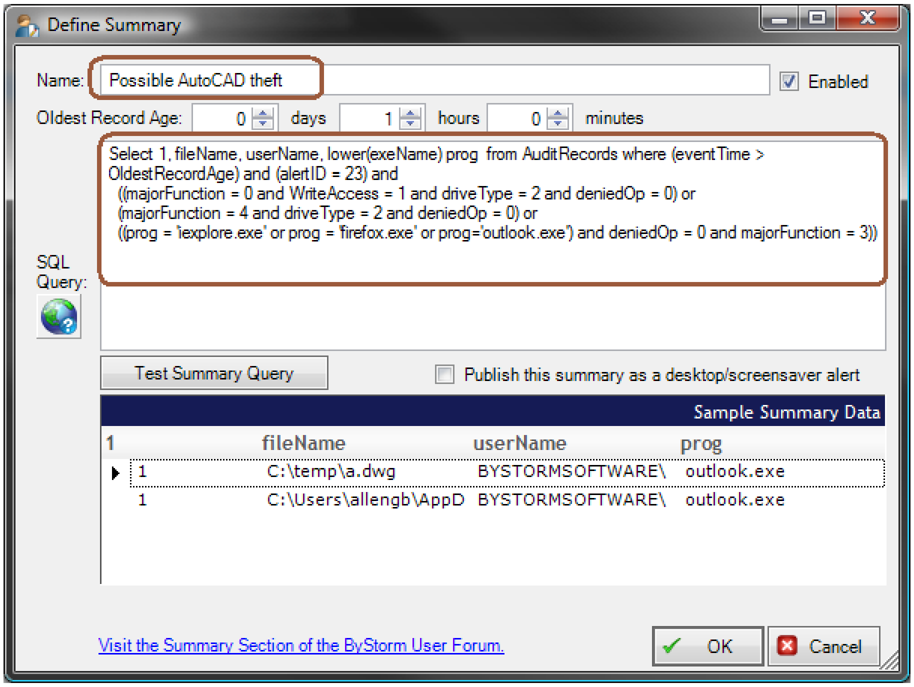
Enabled	Record Age	Summary Name
☑	1 days 0 hours 0 minutes	Extension Summary by User
□	1 days 0 hours 0 minutes	Drive type usage by user
□	1 days 0 hours 0 minutes	Program summary
□	1 days 0 hours 0 minutes	Root Folder Moves
☑	0 days 0 hours 5 minutes	Auto-generated summary for alert: 214,335,828
□	0 days 0 hours 10 minutes	Hidden File Access
☑	0 days 1 hours 0 minutes	Summary for rule: watch exe writes and deletes
□	0 days 0 hours 5 minutes	Auto-generated summary for alert: 43,349,093
□	0 days 1 hours 0 minutes	Test summary

11. This will bring up the 'Define Summary' screen. Here is how to configure the alert:
    a. Enter 'Possible AutoCAD theft' for the 'Name'
    b. For the 'SQL Query' enter the following:

```
Select 1, fileName, userName, lower(exeName) prog  from AuditRecords where (eventTime > OldestRecordAge) and (alertID = 23) and

((majorFunction = 0 and WriteAccess = 1 and driveType = 2 and deniedOp = 0) or  (majorFunction = 4 and driveType = 2 and deniedOp = 0) or

((prog = 'iexplore.exe' or prog = 'firefox.exe' or prog='outlook.exe') and deniedOp = 0 and majorFunction = 3))
```



Name: Possible AutoCAD theft ☑ Enabled

Oldest Record Age: 0 days 1 hours 0 minutes

SQL Query:

```
Select 1, fileName, userName, lower(exeName) prog  from AuditRecords where (eventTime >
OldestRecordAge) and (alertID = 23) and
  ((majorFunction = 0 and WriteAccess = 1 and driveType = 2 and deniedOp = 0) or
  (majorFunction = 4 and driveType = 2 and deniedOp = 0) or
  ((prog = 'iexplore.exe' or prog = 'firefox.exe' or prog='outlook.exe') and deniedOp = 0 and majorFunction = 3))
```

□ Publish this summary as a desktop/screensaver alert

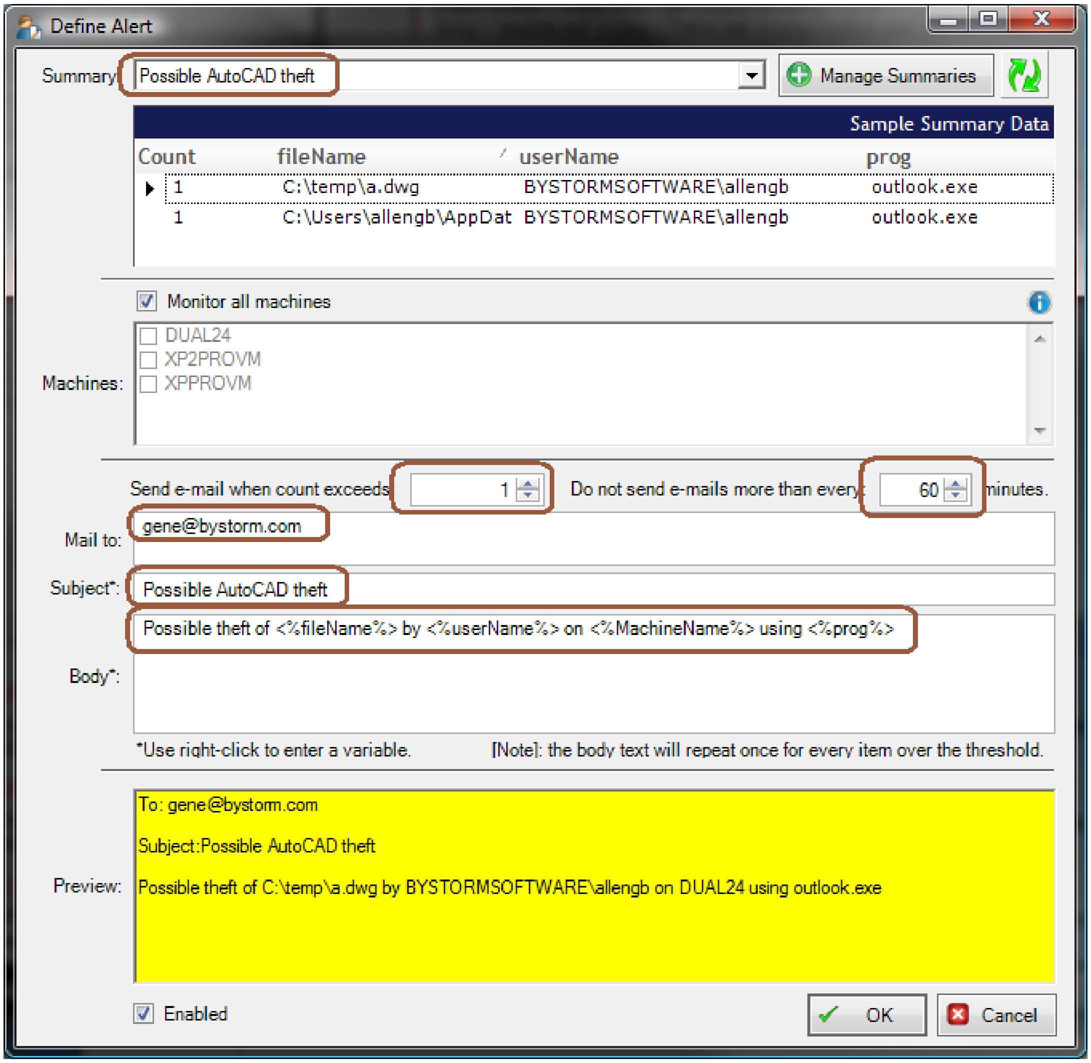
Sample Summary Data

```
1        fileName                 userName            prog
1        C:\temp\a.dwg            BYSTORMSOFTWARE\    outlook.exe
1        C:\Users\allengb\AppD    BYSTORMSOFTWARE\    outlook.exe
```

Visit the Summary Section of the ByStorm User Forum.

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 ‘Possible AutoCAD theft’ summary from the drop down.
    b. Enter ‘1’ for the ‘Send e-mail when count exceeds’
    c. Enter ‘60’ 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 ‘Possible AutoCAD theft’ for the ‘Subject’
    f. For the body enter:

```
Possible theft of <%fileName%> by <%userName%> on <%MachineName%>
using <%prog%> for the body.
```



Summary: Possible AutoCAD theft

Sample Summary Data

Count	fileName	userName	prog
1	C:\temp\a.dwg	BYSTORMSOFTWARE\allengb	outlook.exe
1	C:\Users\allengb\AppDat	BYSTORMSOFTWARE\allengb	outlook.exe

☑ Monitor all machines

Machines:
□ DUAL24
□ XP2PROVM
□ XPPROVM

Send e-mail when count exceeds 1 Do not send e-mails more than every 60 minutes.

Mail to: gene@bystorm.com

Subject*: Possible AutoCAD theft

Body*: Possible theft of <%fileName%> by <%userName%> on <%MachineName%> using <%prog%>

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

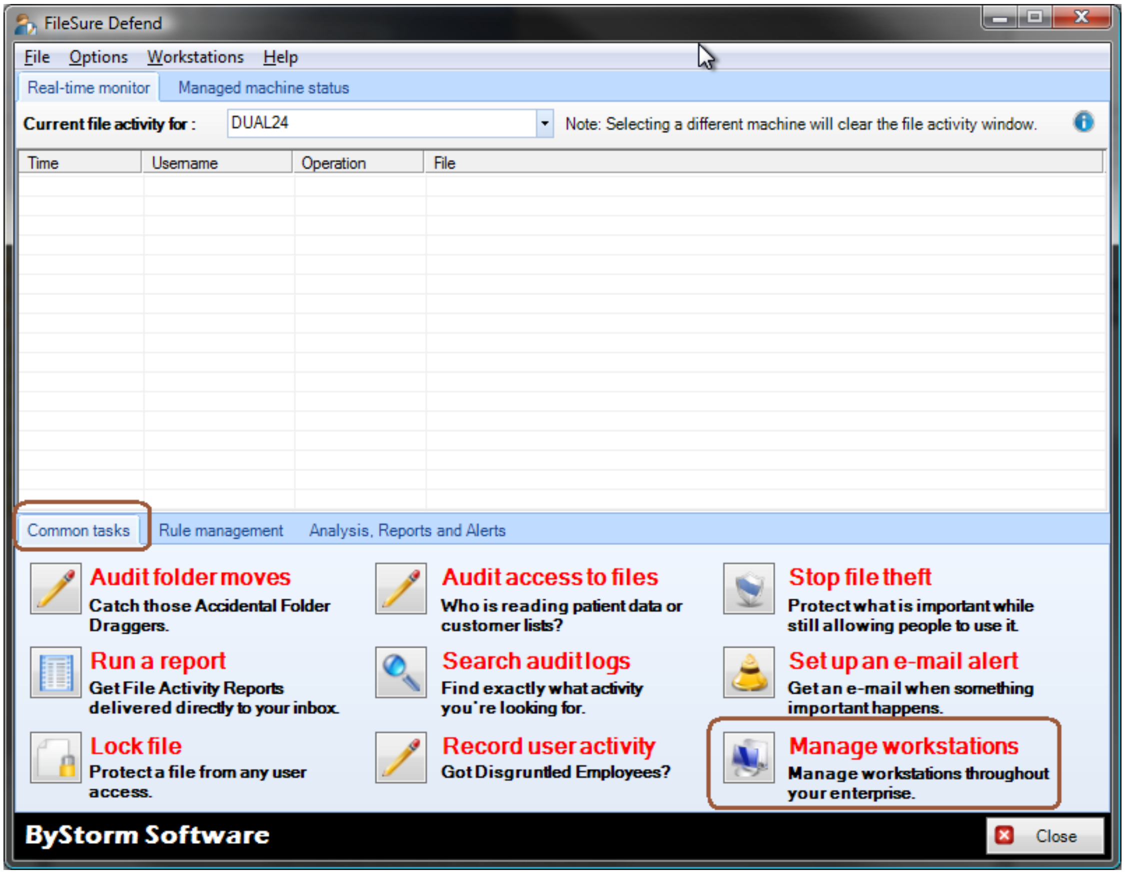
Preview:
To: gene@bystorm.com
Subject:Possible AutoCAD theft
Possible theft of C:\temp\a.dwg by BYSTORMSOFTWARE\allengb on DUAL24 using outlook.exe

☑ Enabled

    g. Click ‘OK’ to close the ‘Define Alert’ screen

Now we have an alert configured to send an alert when someone either attaches an AutoCAD file to an email or when one is copied to a removable drive. We have also configured a daily theft report to be sent. Because most theft doesn’t happen on the actual file server which is where FileSure is currently running, we need to manage some workstations.

13. On the main console screen, select the ‘Common tasks’ and click the ‘Manage workstations’ button.



Current file activity for : DUAL24

Note: Selecting a different machine will clear the file activity window.

Audit folder moves Catch those Accidental Folder Draggers.

Audit access to files Who is reading patient data or customer lists?

Stop file theft Protect what is important while still allowing people to use it.

Run a report Get File Activity Reports delivered directly to your inbox.

Search audit logs Find exactly what activity you're looking for.

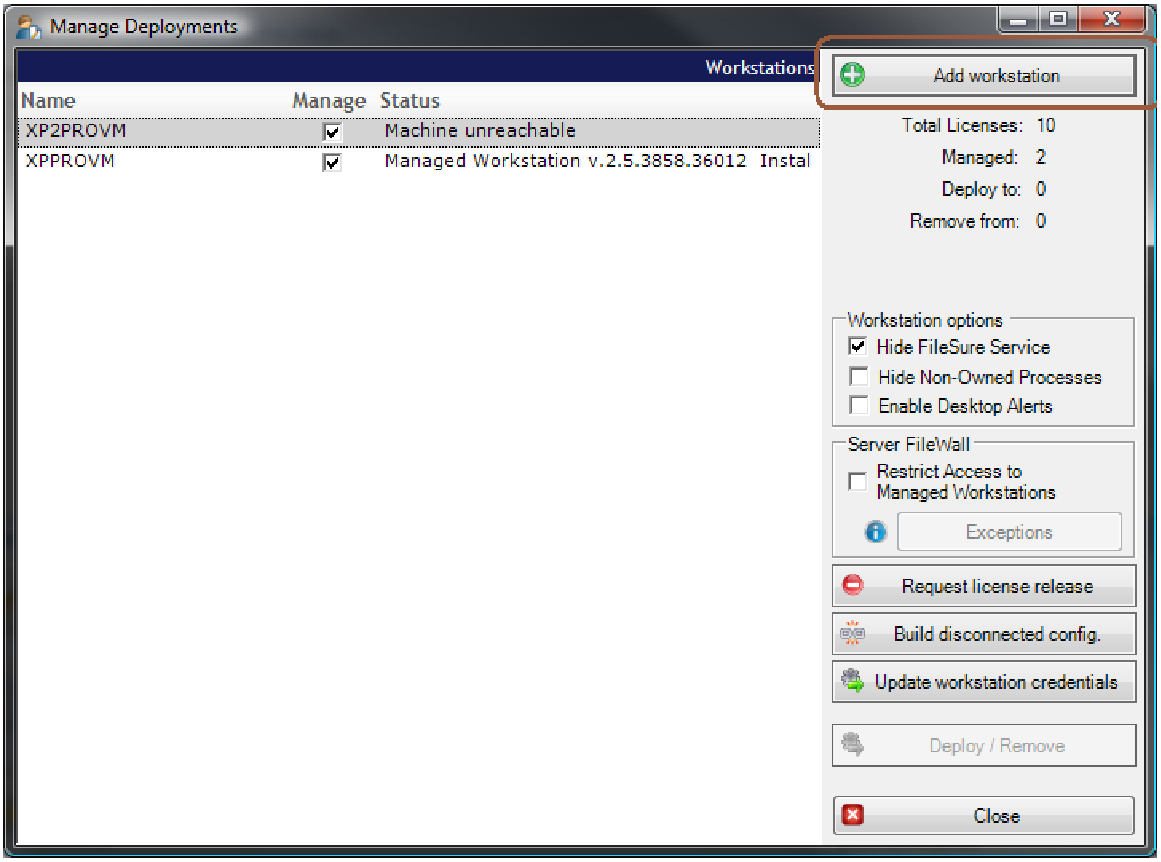
Set up an e-mail alert Get an e-mail when something important happens.

Lock file Protect a file from any user access.

Record user activity Got Disgruntled Employees?

Manage workstations Manage workstations throughout your enterprise.

14. This will bring up the ‘Manage Deployments’ screen, click the ‘Add workstations’.



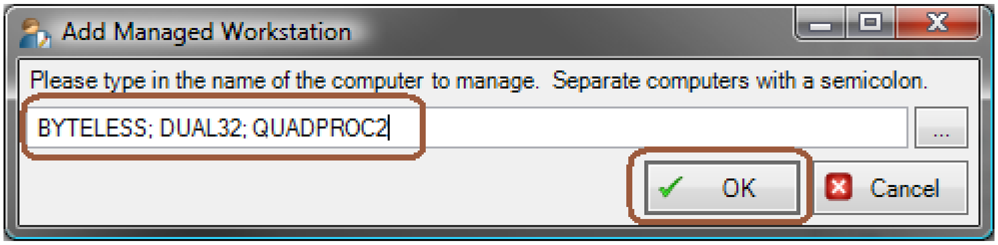
Name	Manage	Status
XP2PROVM	☑	Machine unreachable
XPPROVM	☑	Managed Workstation v.2.5.3858.36012 Instal

Total Licenses: 10
Managed: 2
Deploy to: 0
Remove from: 0

☑ Hide FileSure Service
☐ Hide Non-Owned Processes
☐ Enable Desktop Alerts

☐ Restrict Access to Managed Workstations

15. This will bring up the ‘Add Managed Workstation’ screen. On this screen enter the workstations you want to monitor and click OK.



Please type in the name of the computer to manage. Separate computers with a semicolon.

BYTELESS; DUAL32; QUADPROC2

16. Click the ‘Deploy/Remove’ to install FileSure for Workstation on each workstation.

The managed workstation will pull their rules, configuration and summaries from the server and push their logs to the server. The central FileSure server will monitor the summaries being published by each workstation looking for something to alert on. When it’s time for a scheduled report, the central server will consolidate the logs from the workstations and generate the report.