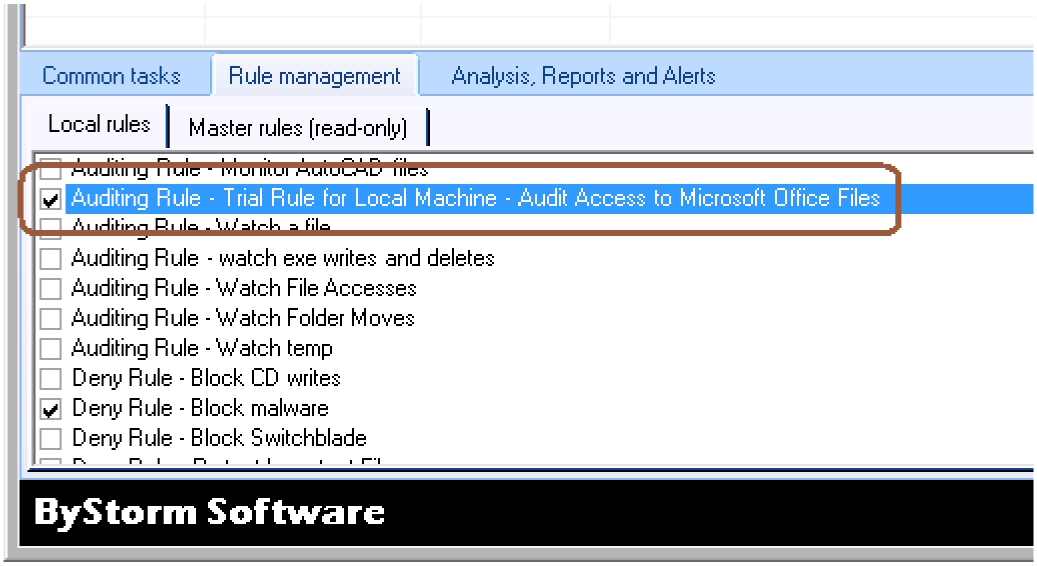
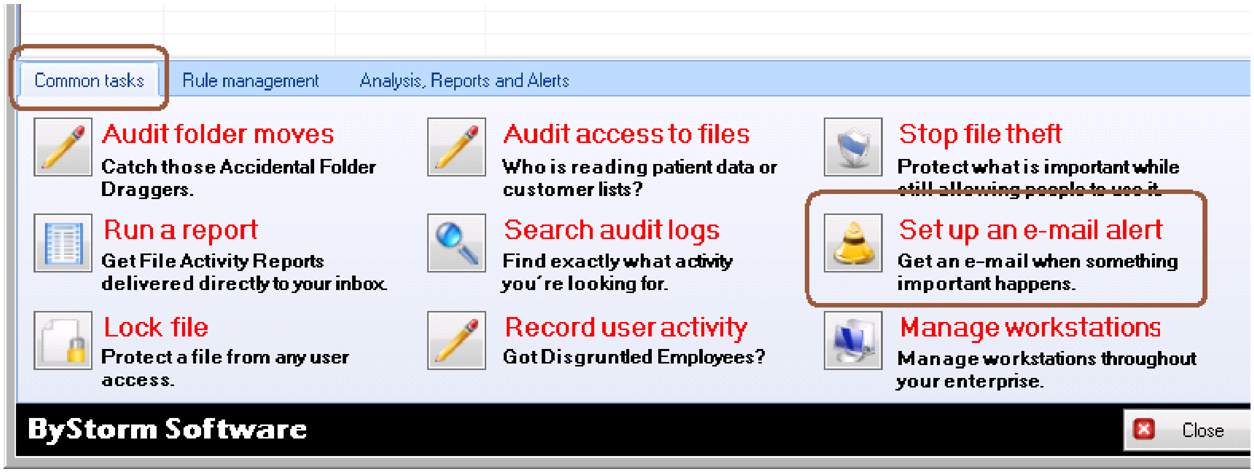
How to get an e-mail alert when someone deletes more than 10 files

1. First we need to define what files we want to monitor for deletes, for my example I'm going to use the trial rule: Audit Access to Microsoft Office Files. Just look in the Rule Management screen and make sure it is checked (turned on).



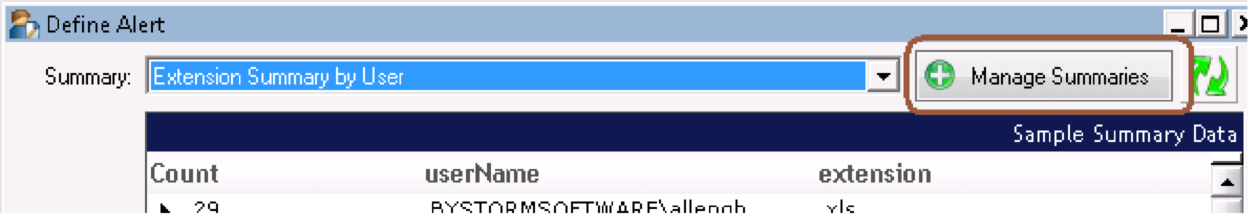
□ Auditing Rule - Monitor AutoCAD files
☑ Auditing Rule - Trial Rule for Local Machine - Audit Access to Microsoft Office Files
□ Auditing Rule - Watch a file
□ Auditing Rule - watch exe writes and deletes
□ Auditing Rule - Watch File Accesses
□ Auditing Rule - Watch Folder Moves
□ Auditing Rule - Watch temp
□ Deny Rule - Block CD writes
☑ Deny Rule - Block malware
□ Deny Rule - Block Switchblade

2. Now, that we've set up our auditing rule, we need to set up the e-mail alert. On the Common Tasks tab, select the 'Set up an e-mail alert' task.


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

[Note: if you are prompted to set up your SMTP settings, select 'Yes' and enter them]

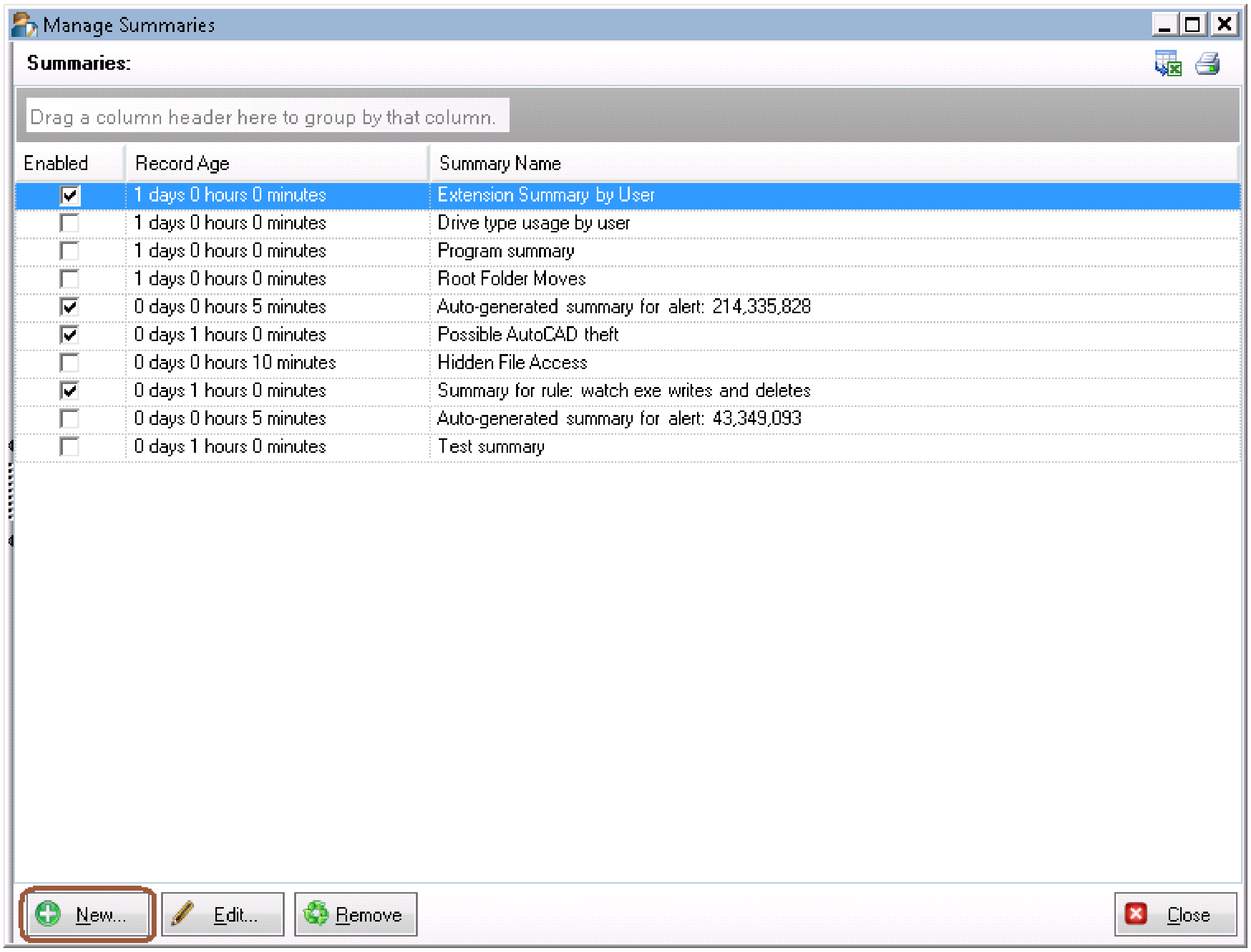
3. This will bring up the 'Define alert' screen, click the 'Manage Summaries' button in the upper right:



Summary: Extension Summary by User

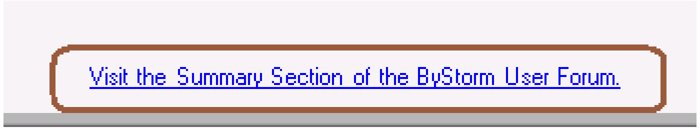
Count	userName	extension
29	BYSTORMSOFTWARE\allengb	xls

4. Now on the Manage Summaries screen, click ‘New…’ at the bottom, since we need to set up a new summary for what we want to be alerted on:

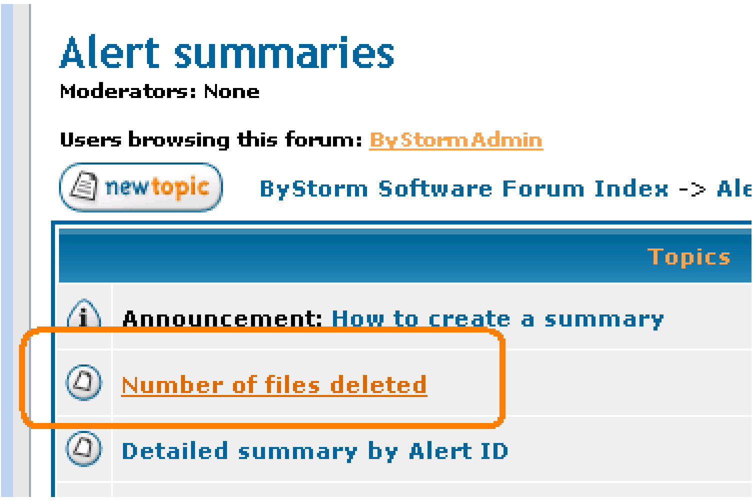


Enabled	Record Age	Summary Name
☑	1 days 0 hours 0 minutes	Extension Summary by User
□	1 days 0 hours 0 minutes	Drive type usage by user
□	1 days 0 hours 0 minutes	Program summary
□	1 days 0 hours 0 minutes	Root Folder Moves
☑	0 days 0 hours 5 minutes	Auto-generated summary for alert: 214,335,828
☑	0 days 1 hours 0 minutes	Possible AutoCAD theft
□	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

5. This will bring up the ‘Define Summary’ screen and since we’re lucky enough that this is a pretty popular request, click on the ‘ Visit the Summary Section of the ByStorm User Forum’ link at the bottom:



6. Clicking on the link will open a browser and navigate to the ByStorm User Forum. The summary you want is this one:



Alert summaries

Moderators: None

Users browsing this forum: ByStormAdmin

ByStorm Software Forum Index -> Ale

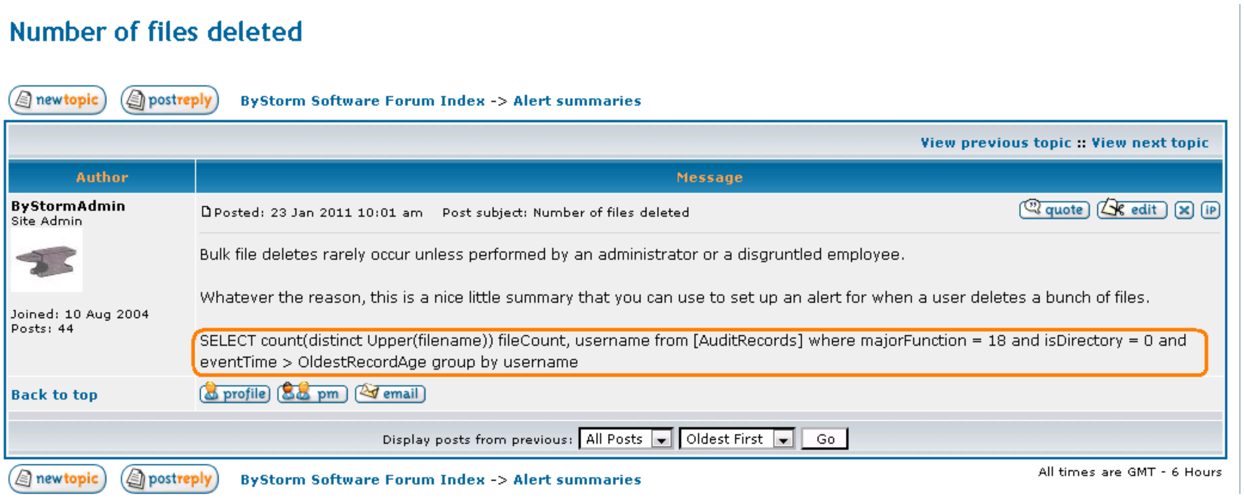
Topics

Announcement: How to create a summary

Number of files deleted

Detailed summary by Alert ID

and it will bring up the following screen:



Number of files deleted

ByStorm Software Forum Index -> Alert summaries

View previous topic :: View next topic

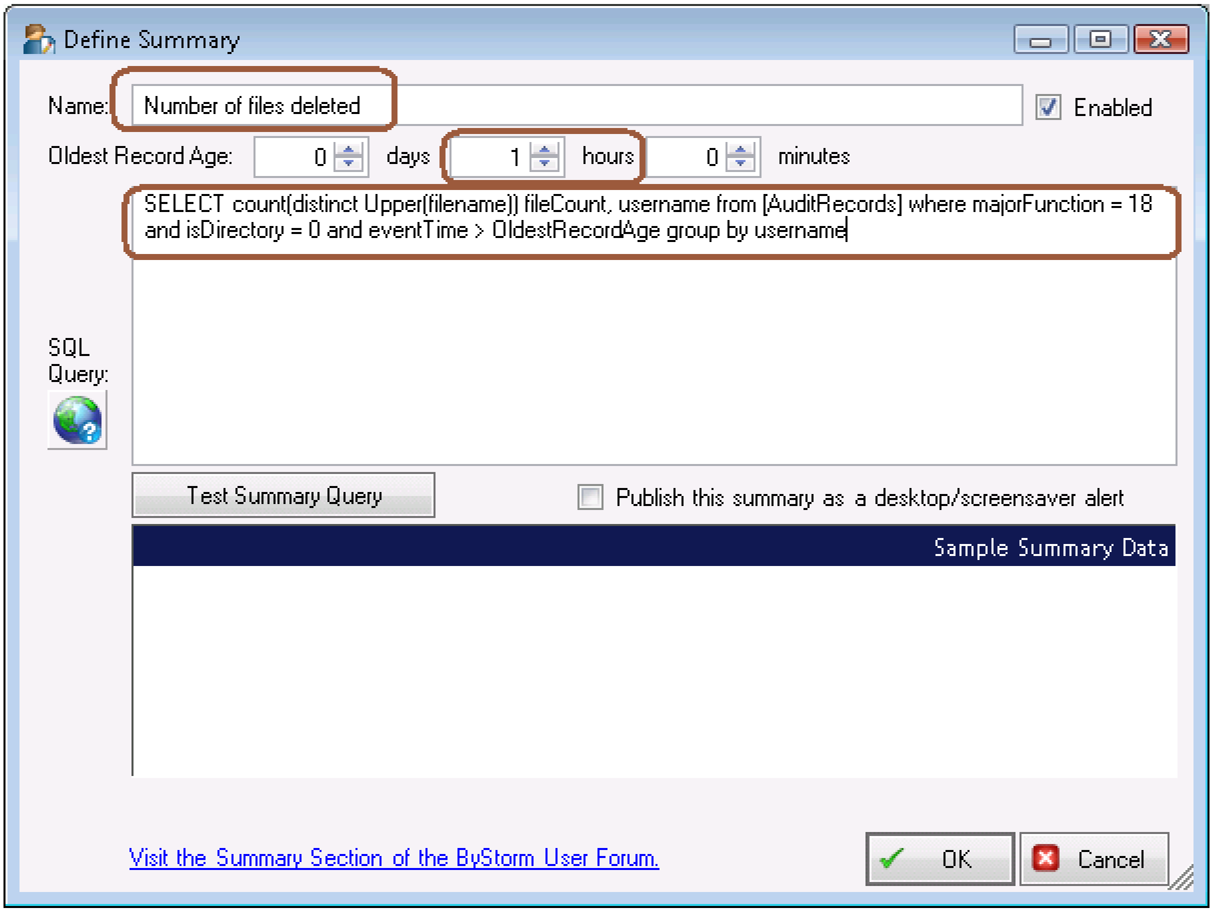
Author	Message
ByStormAdmin Site Admin Joined: 10 Aug 2004 Posts: 44	Posted: 23 Jan 2011 10:01 am Post subject: Number of files deleted Bulk file deletes rarely occur unless performed by an administrator or a disgruntled employee. Whatever the reason, this is a nice little summary that you can use to set up an alert for when a user deletes a bunch of files. SELECT count(distinct Upper(filename)) fileCount, username from [AuditRecords] where majorFunction = 18 and isDirectory = 0 and eventTime > OldestRecordAge group by username
Back to top	

Display posts from previous: All Posts | Oldest First | Go

ByStorm Software Forum Index -> Alert summaries

All times are GMT - 6 Hours

7. Cut and paste the 'Summary title' from the web page to the 'Define summary' screen in FileSure. Do the same thing for the SQL query. Leave the OldestRecordAge at 1 hour and when you're done, you should have something looking like this:



Name: Number of files deleted ☑ Enabled

Oldest Record Age: 0 days 1 hours 0 minutes

SQL Query:

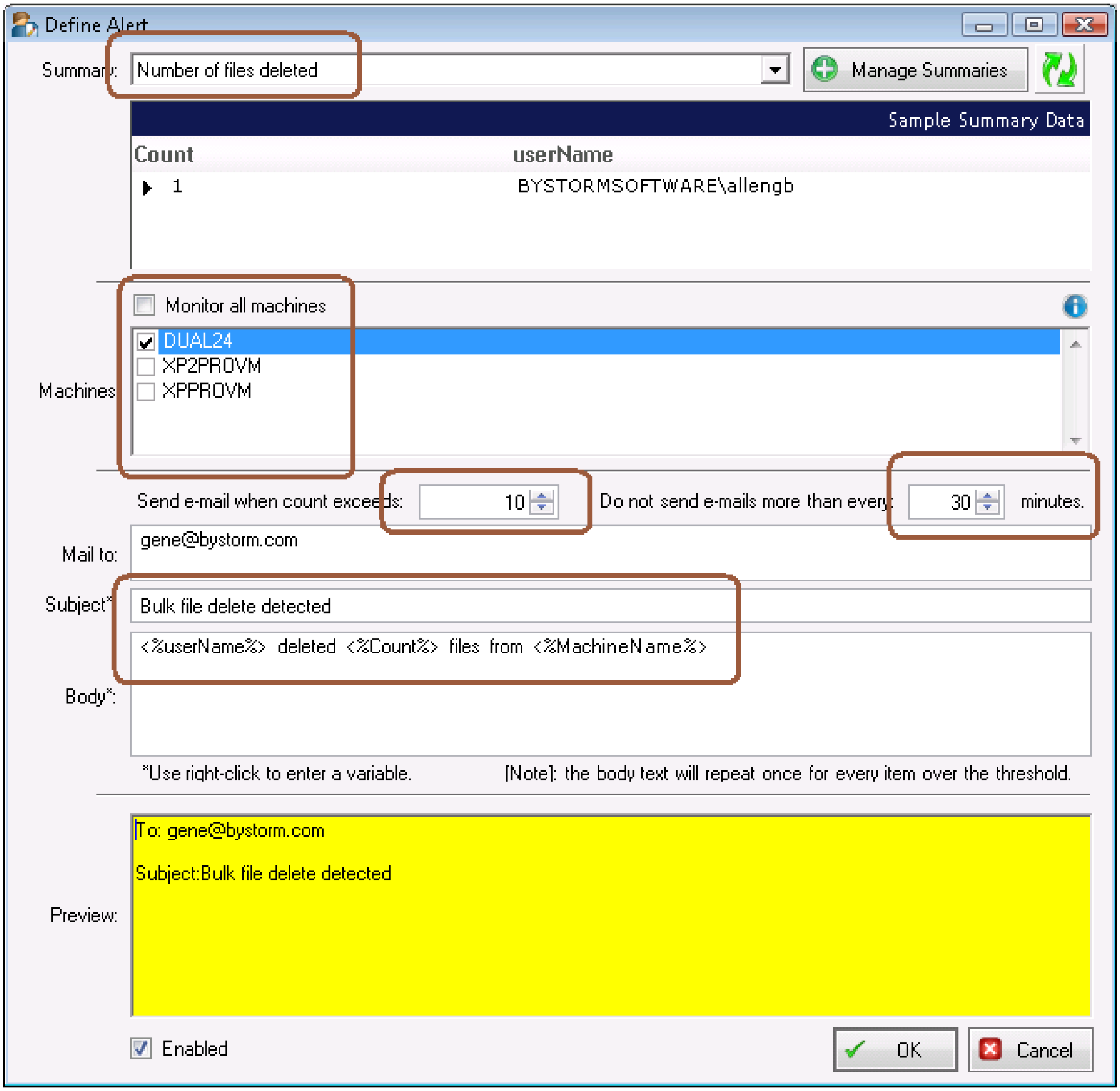
```
SELECT count(distinct Upper(filename)) fileCount, username from [AuditRecords] where majorFunction = 18
and isDirectory = 0 and eventTime > OldestRecordAge group by username
```

Test Summary Query
□ Publish this summary as a desktop/screensaver alert
Sample Summary Data
Visit the Summary Section of the ByStorm User Forum.
OK
Cancel

[Note: You might have a little trouble copying the title from the webpage into the Name field since the copy sometimes picks up a blank line before the title.]

8. Click OK to close the Define Summary screen, click 'Close' to close the Manage Summaries screen and click 'Ok' on the message box saying you might need to wait a few minutes for the summary to be published.

9. After a couple of minutes, click the 'Summary' drop down at the top and select our new 'Number of Files Deleted' summary. Fill out the rest of the form per your requriments; if you right click in the Subject and Body sections, you can select values from the summary. Here is how I set up my example:



Summary: Number of files deleted

Count	userName
1	BYSTORMSOFTWARE\allengb

Machines

□ Monitor all machines

☑ DUAL24
□ XP2PROVM
□ XPPROVM

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

Mail to: gene@bystorm.com

Subject*: Bulk file delete detected

Body*: <%userName%> deleted <%Count%> files from <%MachineName%>

*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:Bulk file delete detected

☑ Enabled

10. Make sure that "enabled" is checked, and click OK.

11. Go ahead and try to delete some Microsoft Office files. You should get an email if you delete more than 10.