How to audit, alert and report on Microsoft Uffice file deletes
---

**ByStorm Software** 

**FileSure** 

www.bystorm.com

877-BYSTORM

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.

 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.

FileSure Defe File Options	end Workstatio	ons Help		
Real-time monitor	or Manag	ed machine status		
Current file acti	vity for :	DUAL24	-	Note: Selecting a different machine will clear the file activity window.
Time	Usemame	Operation	File	•
2/23 9:53 AM 2/23 9:53 AM	allengb allengb allengb allengb allengb allengb allengb allengb allengb allengb allengb	Opened for Read Read Opened for Read/Writ Created for Read/Writ Write Opened for Read Read Created for Write Opened for Delete File deleted Created for Read/Write	\\WIN20 \\win200 e \\WIN20 C:\USER C:\USER \\WIN20 \\win200 \\WIN20 \\WIN20 \\WIN200 e \\WIN200	D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 &x64\marketing\how tos\how to audit, alert and report on theft of autocad files2.d D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 \$\ALLENGB\APPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTE allengb\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.M D8X64\MARKETING\HOW TOS\HOW TO BLOCK FILES IN A CERTAIN FOLD! &x64\marketing\how tos\how to block files in a certain folder from being copied u: D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 &x64\marketing\how tos\how to audit, alert and report on microsoft office file delei D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 &x64\marketing\how tos\how to audit, alert and report on microsoft office file delei D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 &x64\marketing\how tos\how to audit, alert and report on microsoft office file delei D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 &x64\marketing\how tos\how to audit, alert and report on microsoft office file delei D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 &x64\marketing\how tos\how to audit, alert and report on microsoft office file delei D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 &x64\marketing\how tos\how to audit, alert and report on microsoft office file delei D8X64\MARKETING\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 &x64\marketing\how tos\how to audit, alert and report on microsoft office file delei D8X64\MARKETING\HOW TOS\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 &x64\marketing\how tos\how to audit, alert and report on microsoft office file delei D8X64\MARKETING\HOW TOS\HOW TOS\HOW TOS\HOW TO AUDIT, ALERT AND REPORT ON 1 &x64\marketing\how tos\how to audit AUDIT
2/23 9:53 AM 2/23 9:53 AM 2/23 9:53 AM 2/23 9:53 AM 4 Common tasks	allengb allengb allengb allengb	Move Move Set security Read agement Analysis, Reports an	\\win200 \\win200 \\win200 \\win200	ax64 \marketing \how tos \now to audit, alert and report on microsoft office file dele 8x64 \marketing \how tos \fc lead 19.tmp to M:\How tos \How to audit, alert and rep 8x64 \marketing \how tos \how to audit, alert and report on microsoft office file dele 8x64 \marketing \how tos \how to audit, alert and report on microsoft office file dele 8x64 \marketing \how tos \how to audit, alert and report on microsoft office file dele 8x64 \marketing \how tos \how to audit, alert and report on microsoft office file dele •
Local rules M	aster rules ( Monitor A - Trial Rule	read-only) uteCAD files for Local Machine - Audit Access	s to Microsoft	Office Files Quick audit
Auditing Rule Auditing Rule Auditing Rule Auditing Rule Auditing Rule Deny Rule - I Deny Rule - I Deny Rule - I Deny Rule - I	- watch exe - Watch File - Watch Fo - Watch ten Block CD wr Block malwa Block Switch	e writes and deletes e Accesses Ider Moves np ites re Iblade		<ul> <li>Block access</li> <li>Event log monitoring</li> <li>Edit Rule</li> <li>Delete rule</li> </ul>
ByStorm	Softw	are		Close

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

Rule name:       Trial Rule for Local Machine - Audit Access to Microsoft Office Files       Deselect All         File name filters       User name filters       Access checks         Include: *.xls; *.doc; *.ppt; *.vsd; *.xlsx; *.d       Include: *       Virte access         Virte access       Vir	🐴 FileSure - Auditing Rule		
Image: Show matching users     Image: Show matching users	Rule name: Trial Rule for Local Machine - Audit Access to Mix File name filters Include: *.xls; *.doc; *.ppt; *.vsd; *.xlsx; *.d Made Edit Remove	crosoft Office Files User name filters Include: *	Operations to Audit         Deselect All         Access checks         ✓ Read access         ✓ Write access         ✓ Delete access         ✓ Create         ✓ Delete         ✓ Rename         ✓ Security Changes         ✓ File read         ✓ File write
File size filters       Other         Options       Program name filters       Group name filters       Machine name filters       Time slot filters       Signature filters         Rule applies to       Image: Send e-mail on rule match       Send e-mail on rule match       Send to:       Image: Send to:         Image: Removable drives       Image: Servers       Image: Servers       Image: Only apply rule after a threshold has been reached.         Image: Driveless (VSS)       Image: VSS)       Image: Only apply rule after swithin       Got minutes is reached.			

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

🏠 FileSure - Auditing Rule		×
Rule name: Trial Rule for Local Machine - Audit Access to Mic	crosoft Office Files	Operations to Audit Deselect All
File name filters         Include: *.xls; *.doc; *.ppt; *.vsd; *.xlsx; *.d         Exclude: *\~*         Image: *\*         Ima	User name filters	Access checks         ✓ Read access         ✓ Write access         ✓ Delete access         ✓ Create         ✓ Delete         ✓ Rename         ✓ Security Changes         ✓ File read         ✓ File write
File size filters Other Options Program name filters Group name	ne filters Machine name filters Time slot	t filters Signature filters
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 None Alert ID: 23	e matches
Comment:		✓ OK 🛛 Cancel

- 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.

<u>File Options Workstations H</u> elp						
Real-time monitor Managed machine s	status					
Current file activity for : DUAL24   Note: Selecting a different machine will clear the file activity window.						0
Time Usemame Op	peration	File	3			
Common tasks Rule management A	Analvsis, Rep	orts and Alerts				
Analysis	Rep	orts		Alerts		
Events recorded today:	13	Total schedule	ed reports:	3	Total alerts:	4
Operations denied today:	5	Active schedule	ed reports:	3	Active alerts:	2
		Report	recipients:	1	Machines monitored:	1
					Machines managed:	2
🔍 🛛 View Dat	ta		Reports			
Search for Tr	rends		Scheduled reports		Manage al	lerts
ByStorm Software						Close

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.

Schedule Reports						-   <b>D</b>   X
Report Jobs:						촉 🌄 🍊
Drag a column header here to group b	y that colum	n.				
Job Name:	Enabled Re	port Name:		Send To:		
New Job	🔽 Us	er Activity Report:	Touched files	gene@bysto	orm.com	
Auto-generated report for 214,335,828	🔽 Us	er Activity Report:	Folders moved	gene@bysto	orm.com	
Auto-generated report for 43,349,093	🔽 Us	er Activity Report:	Touched files	gene@bysto	orm.com	
🚯 <u>N</u> ew 🖊 <u>E</u> dit 🔇 <u>R</u> em	ove	SMTP Set	ings Schedu	led job execution time	02:00 PM	S <u>C</u> lose

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

わ Edit Job	
Job Name	Deleted files report 🔽 Enabled
Report name:	User Activity Report: Files deleted  Check ByStorm for new reports
	Sorted by users doing the activity, report shows files deleted. 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
o User Name Filters*:	
	Data Format     O Acrobat File (PDF) O Excel File O XML O CSV O HTML
Delivery	gene@bystorm.com
Mail to*:	
Save to folder:	🖆 Browse
Schedule -	<ul> <li>✓ Monday</li> <li>✓ Tuesday</li> <li>✓ Wednesday</li> <li>✓ Thursday</li> <li>✓ Friday</li> <li>✓ OK</li> <li>✓ Cancel</li> </ul>

- 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.

ਨ FileSure Defe	nd						
<u>File</u> Options	Workstations Hel	р					
Real-time monito	Managed machin	ne status					
Current file activ	vity for : DUAL24		<ul> <li>Note: Selecting a diff</li> </ul>	ferent machine will clear the file activity	r window. 🕚		
Time	Usemame	Operation	File				
Common tasks	Rule management	Analysis, Report	s and Alerts				
Audi	, t folder moves	ß	Audit access to files	Stop file theft			
Catch Dragg	those Accidental F ers.	older	Who is reading patient data or customer lists?	Protect what is importa still allowing people to	ntwhile use it		
Run	a report		Search auditlogs	🔝 Set up an e-mail a	alert		
GetFil	e Activity Reports	-	Find exactly what activity	Getan e-mail when so	mething		
delive	delivered directly to your inbox. you're looking for. important happens.						
Lock file         Record user activity         Manage workstations           Protect a file from any user         Got Disgrunted Employees?         Manage workstations throughout							
acces	S			your enterprise.			
ByStorm	Software				Close		

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.

🇞 Define Al	ert		a second	
Summary:	Extension Summary by User		Manage Su	mmaries 🔀
			Sample	Summary Data
	Count	userName	extension	-
	▶ 76	BYSTORMSOFTWARE\allengb	exe	
	58	BYSTORMSOFTWARE\allengb	4	
L _	10	BTSTORMSOFTWARE (allenge	awg	<u> </u>
	Monitor all machines			0
	DUAL24			~
Machines:	XP2PROVM			
_	1			-
	Send e-mail when count exc	eeds: 10 🗢 Do not send	e-mails more than every:	30 ≑ minutes.
Mail to:				
Subject	[			
oubject .	[			
Body*:				
_	*Use right-click to enter a v	ariable. [Note]: the body text wi	ill repeat once for every item of	ver the threshold.
	To:			
	Subject:			
Previous	outport.			
Fleview.				
	Enabled		✓ OK	S Cancel

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

👌 Manage	Summaries	· · · · · · · · · · · · · · · · · · ·	- 0 ×
Summari	es:		<b>W</b> 4
Drag a c	blumn header here to group by	that column	
Enabled	Record Age	Summary Name	
V	1 days 0 hours 0 minutes	Extension Summary by User	
17	1 days 0 hours 0 minutes	Drive type usage by user	
10	1 days 0 hours 0 minutes	Program summary	
173	1 days 0 hours 0 minutes	Root Folder Moves	
1	0 days 0 hours 5 minutes	Auto-generated summary for alert: 214,335,828	
E9	0 days 0 hours 10 minutes	Hidden File Access	
2	0 days 1 hours 0 minutes	Summary for rule: watch exe writes and deletes	
<b>F</b> 1	0 days 0 hours 5 minutes	Auto-generated summary for alert: 43,349,093	
173	0 days 1 hours 0 minutes	Test summary	
	$\checkmark$		
New	Edit	·e	

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

2. Define Summary	_ 🗆 🗙
Name: Watching for Office file deletes	Enabled
Oldest Record Age: 0 🚖 days 1 🚖 hours 0 🚖 minutes	
select count(extension), extension from AuditRecords where extension <> "" and eventTime : OldestRecordAge group by Upper(extension);	>
SQL Query:	
Test Summary Query Dublish this summary as a desktop/scree	ensaver alert
Sample S	Summary Data
Visit the Summary Section of the ByStorm User Forum.	Cancel

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

## Detailed summary by Alert ID

(a) newtopic (a) postreply ByStorm Software Forum Index -> Alert summaries							
View previous topic :: View next							
Author	Message						
ByStormAdmin Site Admin	D Posted: 09 Nov 2009 09:33 am Post subject: Detailed summary by Alert ID						
	This summary is useful for alerting on a rule match.						
Joined: 10 Aug 2004 Posts: 46	Change the 'alertID = 10' in the SQL below to match what is defined in the rule.						
	select 1 count, fileName, userName from AuditRecords where alertID = 10 and eventTime > OldestRecordAge						
Back to top	🚨 profile) (😹 pm) (🎯 email)						

- 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:

Define Alert						
Summary:	Watching for Office file deletes		•	Manage Sumr	naries 💫	
	Sample S	ummary Data				
	Count f	fileName	userName			
	• 1	C:\Users\allengb\App	BYSTORMSOFTW	VARE\allengb		
- 1	Manitas all anakinas					
					0	
					^	
Machines:						
					~	
	Send e-mail when count exceeds:	1 🖂 Do no	send e-mails more th	an every: 3	0 inimites	
6	gene@bystorm.com				U V Innitico.	
Mail to	geneebyetennicenn					
Subject*	Office file deleted					
(	<%userName%> deleted <%fileName%	%>				
Body*:						
	*Use right-click to enter a variable.	[Note]: the body	text will repeat once fo	or every item over	r the threshold.	
	Ter and Ohuston and					
	ro.gene@bystom.com					
	Subject:Office file deleted					
Preview: BYSTORMSOFTWARE\allengb deleted C:\Users\allengb\AppData\Local\Microsoft\Windows\Temporary In						
	Enabled			🖌 ОК	🛛 Cancel	

- 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.