<b>FileSure</b>	How to Audit Logon/Logoff Events	s on Windows Server 2008 R2
ByStorm Software	www.bystorm.com	877-BYSTORM

FileSure automatically records 'session based' events; these include logon, logoff, lock, unlock and remote control events. These events are user session based, which means it's not going to pick up authentication events like when a user logons onto the domain from his computer. To audit authentication events, FileSure needs to be configured to monitor the Windows security event log. This How-to will show you how to audit authentication events using FileSure.

[Note: by default, Windows 2008 R2 is configured to audit authentication events; if object auditing isn't turned on in your environment, here is a video that explains how to turn it on: <u>http://www.youtube.com/watch?v=8Lot58yAEKM</u>]

1. Start FileSure, switch to the 'Rules management' tab and click the 'Event log monitoring' button:

🌯 FileSure De			piring in 21 da	iys.				_ 🗆 ×
r	<u>W</u> orkstations							
Real-time monit	tor Mana	iged machir	ne status					
Current file activity for: WIN2008X64				<ul> <li>Note: Selecting a different r</li> </ul>	machine will clear t	he file activity window.	0	
Time	Username	•	Operation	File				
Common tasks	Rule mar	nagement	Analysis, Rep	orts and Alerts				
Local rules	Master rules	(read-only)						
			Machine - Audit /	Access to Microsol	t Office Files		😳 🛛 Quick audit	
							Audit access	
							Block access	
							Event log monitor	ing
						1	/ Edit Rule	
							Delete rule	
ByStorm	Softwa	are						Close

2. This will bring the 'Event Log Filters' screen. When it's up, click on the 'Enable Event Log Monitoring' box:

🗞 Event Log Filters					_ 🗆 >
	- <b>f</b>	nt log hilter, dehni			d.
Event Log	Source	Event ID	Description	String 1	String 2
Security	*Security*	4624	*		
Security	*Security*	4625	*		
Security	*Security*	4634	*		
Security	*Security*	528	*		
Security	*Security*	529	*		
Security	*Security*	540	*		
*					
* Additional Windo generate desired e	ws configuration may be n vent log entries.	ecessary to	😫 Select eve	ent from log	r OK 🛛 Cancel

3. FileSure is 'pre-configured' to gather authentication events on Windows 2003, so we'll need to change the filters a bit. Just delete all the 'Replacement string' filters (scroll to the right in the interface); some are circled below.

💑 Event Log Filters	
- How to use Event log filters	
To begin, check this box: 🔽 Enable Event Log Monitoring*	
Each row below represents a separate event log filter, defining what event lo Type your filter details directly into the fields below, standard FileSure wildca	
String 5 String 6 String 7 String 8	String 9 String 10 String 11
	2
* Additional Windows configuration may be necessary to generate desired event log entries.	Select event from log V OK 🛛 Cancel

4. Click 'OK' to close the Event Log Filters screen and now FileSure will now be gathering authentication events for the current computer. I recommend that you wait for a while for users to authenticate against the server.

5. After 'a while' switch to the 'Analysis, Reports and Alerts' tab and click on the 'Reports' button:

わ FileSure Defe	nd- Trial vei	rsion ex	piring in 2	l days.					
Eile Options W	orkstations į	<u>H</u> elp							
Real-time monitor	Manage	d machin	e status						
Current file activ	vity for : V	√IN2008	×64			•	Note: Selecting a diff	erent r	nachine will clear the file activity window. 🛛 🌀
Time	Username		Operation	F	file				
						_			
Common tasks	Rule manag	jement	Analysis,	Reports a	and Alerts				
Analysis		6		Reports		-			Alerts
	ts recorded to	-	37			0	Total alerts: 0		
Operations denied today: 0			0	Active scheduled reports: 0			· · · · · · · · · · · · · · · · · · ·		Active alerts: 0
						Rep	ort recipients:	0	Machines monitored: 0
						_			Machines managed: 0
🔍 View Data						Reports			
				1	-				
Search for Trends					2	Scheduled report	S	O Manage alerts	
ByStorm 3	Softwar	е							🗵 Close

6. This will bring up the 'Run Report' screen. After it is up, click on the 'Check website for new reports' to get an updated 'Event log: Logon Report'

💦 Run Report
Quick Report Date Range Machines
Range: Custom 🔽 Report: Event Log: Logon Report 🔄 🧠 Run
🛛 🕼 🚱 Check website for new reports 🔹 🔹 🔤 Ordered by time of activity, this report shows Windows log-on and log-offs. Windows
account logon policy needs to be configured for this report.
E   M 4 1 of > >   + 3 2   - 100% - Find   Next
The source of the report definition has not been specified
The source of the report dominion has not been spearred

7. This will download and update the available reports:



8. After the reports are 'reloaded' into FileSure, select 'Previous 7 days' in the Range dropdown and pick the 'Event Log: Logon Report' in the Report dropdown. Then click the 'Run' button and the Logon Report will show just like below:

Run Report Quick Report Date Range	Machines			
Range: Previous 7 days	Report: E	vent Log: Logon Report		Run
💋 Check website for n	ew reports	dered by time of activity, this repor count logon policy needs to be cor	t shows Windows log on and log offs. Windows pliqued for this separt	
Schedule Recurring		count logon policy needs to be con		🛛 Close
📰   🕅 🖣 1 of 1 🕨	H   + 🛛 🛃 🖂	100%	• Find   Next	
	L	.ogon Report		
	From 11/11/20	10 1:37 PM to 11/18/2010 1:3	37 PM	
Time	User	From machine	Event	
Machine:WIN2008X64				_
11/17/2010 7:43:07 PM	FRANK	WIN2008X64	Logon at keyboard	
11/17/2010 8:03:10 PM	ALLENGB	NEWMACHINE	Successful logon	
11/17/2010 8:06:42 PM	ALLENGB	WIN2008X64	Remote Control	
11/17/2010 8:06:42 PM	ALLENGB	WIN2008X64	Remote Control	
11/18/2010 8:39:33 AM	ALLENGB	WIN2008X64	Remote Control	
11/18/2010 8:39:33 AM	ALLENGB	WIN2008X64	Remote Control	
11/18/2010 12:51:18 PM	ALLENGB	WIN2008X64	Remote Control	
11/18/2010 12:51:18 PM	ALLENGB	WIN2008X64	Remote Control	
			FileSure from ByStorm Softwar	e