www.bystorm.com

877-BYSTORM

With FileSure 2.5, we added the ability to audit Windows event logs. The captured events are securely stored right with your other FileSure auditing data in FileSure's encrypted, compressed data store. In this How-To, I'm going to configure FileSure to monitor and record when Firewall changes occur on a Window 2003 server.

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

FileSure Def	end- Trial version e	xpiring in 21 days	5.	
Real-time monito	or Managed mach	ine status		
Current file act	ivity for: WIN200	18×64	 Note: Selecting a different machine will clean 	ear the file activity window. 🛛 🌀
Time	Username	Operation	File	
Common tasks	Rule management	Analysis, Report	ts and Alerts	
Local rules	Master rules (read-only)	1		
Auditing Rule	e - Trial Rule for Local	Machine - Audit Ac	cess to Microsoft Office Files	
				Block access
				Event log monitoring
				Edit Rule
				Delete rule
ByStorm	Software			🗵 Close

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

🌯 Event Log I	Filters					_ 🗆 🗙
- How to use	e Event log filters		<u> </u>			
To begin, c	heck this box 🔽 Enable Eve	ent Log Monitoring*				
Each row t Type your	pelow represents a separate ev filter details directly into the fie	ent log tilter, detini Ids below, standar	ng what event log e d FileSure wildcard r	entries will be capt rules apply.	ured.	
Event Log	Source	Event ID	Description	String 1	String 2	S
Security	*Security*	4624	*			
Security	*Security*	4625	*			
Security	*Security*	4634	*			
Security	*Security*	528	*			
Security	*Security*	529	*			
Security	*Security*	540	*			
*						
X A LINC 1	<u></u>					<u> </u>
" Additional generate de	Windows configuration may be sired event log entries.	e necessary to	📄 Select ev	ent from log	🖌 ОК 🛛 🛛	Cancel

FileSure is 'pre-configured' to gather authentication events on Windows 2003, but we need to add a new entry for the enrties we're interested in. According to http://technet.microsoft.com/en-us/library/cc736708%28WS.10%29.aspx and http://technet.microsoft.com/en-us/library/cc736708%28WS.10%29.aspx and http://technet.microsoft.com/en-us/library/cc737845%28WS.10%29.aspx, Firewall events are between 848-861 in the security log. Below I've selected event 853, which is written to the security log when the operation mode changes. Select the 'Security' log for the Event Log, type in 'Security' for the source, '853' for the Event ID and '*' for the Description.

🌯 Event Log	Filters					
- How to u	e Event log filters					
To begin,	check this box: 🔽 Enable Eve	ent Log Monitoring [*]				
Each row Type you	below represents a separate ev r filter details directly into the fie	vent log filter, defini elds below, standar	ng what event log er d FileSure wildcard m	ntries will be capt ules apply.	ured.	
Event Log	Source	Event ID	Description	String 1	String 2	S
Security	*Security*	4624	*			
Security	*Security*	4625	*			
Security	*Security*	4634	*			
Security	*Security*	528	*			
Security	*Security*	529	*			
Security	*Security*	540	*			
Security	👻 Security	853	*			
*						
* Additiona	Windows configuration may be	e necessary to				
generate o	lesired event log entries.		😫 Select eve	ent from log	🖌 ОК	Cancel

- 3. Click 'OK' to close the Event Log Filters screen and now FileSure will now be gathering Firewall operational change events for the current computer. As a test, turn the Firewall off and on to generate the events.
- 4. After 'a while' switch to the 'Analysis, Reports and Alerts' tab and click on the 'View Data' button:



5. This will bring up the 'View Data' screen. Select to run a query for the 'Previous 12 hours' and click the 'Apply' button. After the data comes back [Note: the Recorded file activity might be blank], select the 'Recorded event log activity' tab and we see our test event.

🌯 View data					
Data Filters	View			Polo ranco	🗳 Apply
Local compute	r		computers	Custom range From 1/ 7/2011 12:00:00 AM	Export data
🗖 Remote compu	uters Select computers			12 hours To 2/ 7/2011 11:59:59 PM	🛛 Close
Recorded file activ	vity Recorded event log a	activity Sys	stem activity		
				228 records	🤹 🎒
Drag a column	header here to group	by that col	umn.		
Туре	Time	Event	Source	Details	-
Audit Cussess	2/7/2011 4:26 PM	548	Coourity	Cussossful Nativark Lagoni	
Audit Success	2/7/2011 4:26 PM	853	Security	The Windows Firewall operational mode has changed.	
Audit Success	2/7/2011 4:26 PM	540	Security	Successful Network Logon:	
Audit Success	2/7/2011 4:26 PM	540	Security	Successful Network Logon:	
Audit Success	2/7/2011 4:27 PM	540	Security	Successful Network Logon:	
Audit Success	2/7/2011 4:27 PM	540	Security	Successful Network Logon:	

6. If you hover over the event details, a tool tip will show you the event description and if you double click on the event itself, you'll get the full details for the event.

» Event Detai	ls							
Machine: Category:	ALLENGB-BTYICCI 0	Event Time: Event Type:	2/7/2011 4:26:08 PM Audit Success	🛛 Close				
Event ID:	853	Source:	Security					
User name:	NT AUTHORITY\SY	NT AUTHORITY\SYSTEM						
Event text:	Policy origin: Local F Profile changed: Sta Interface: All interfac New Setting:							
	Name		Value					
	String 1	Local Policy						
	String 2 Standard							
Replacement strings:	String 3	tring 3 All interfaces						
	String 4	Off						
	String 5	On						
	String 6							
	String 7							
	String 8			-				

You can follow this format to track any sort of event in which you're interested (just look up the number), and the data is saved right with your audit log.