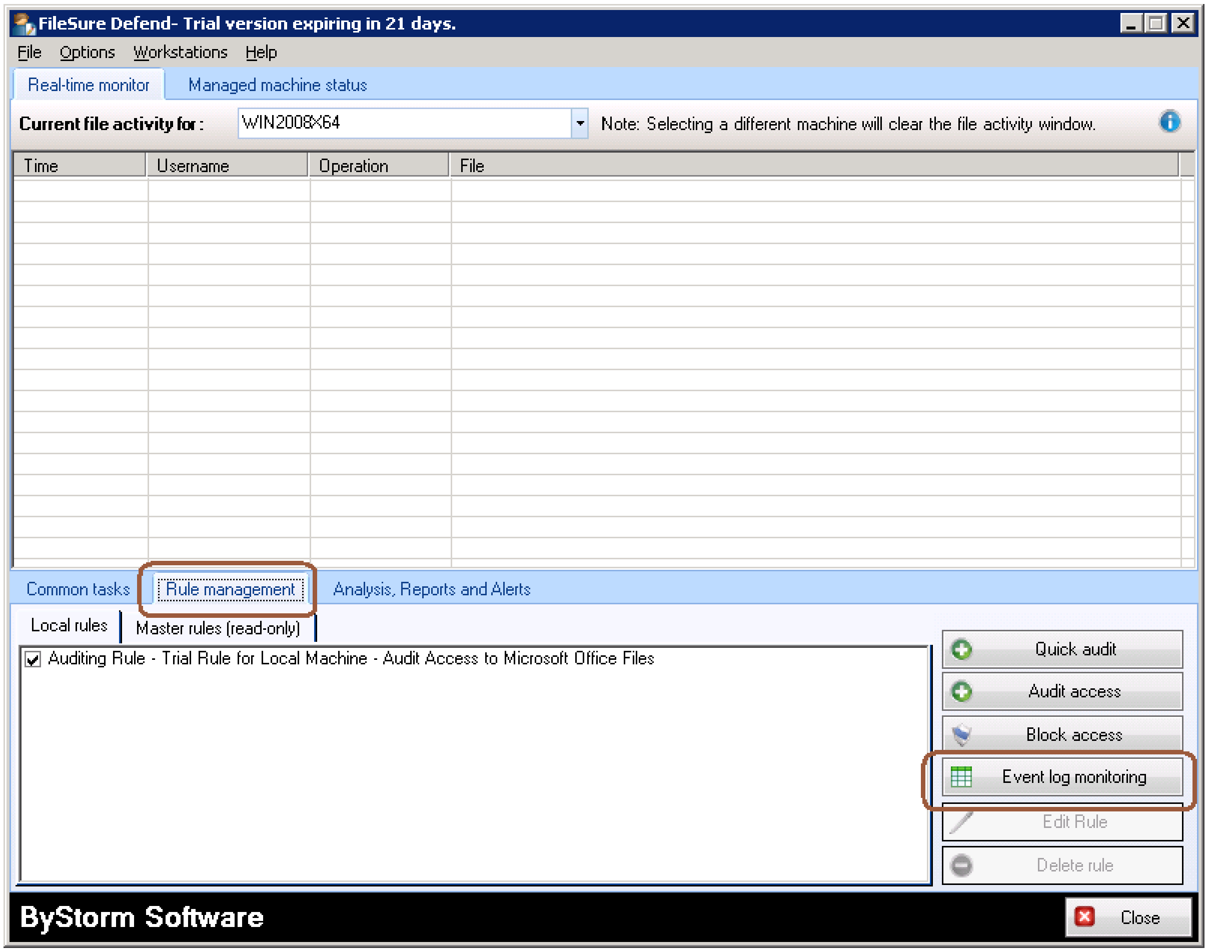
FileSure automatically records 'session based' events; these include logon, logoff, lock, unlock and remote control events. These events are user session based, which means it's not going to pick up authentication events like when a user logons onto the domain from his computer. To audit authentication 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: http://www.youtube.com/watch?v=8Lot58yAEKM]

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


FileSure Defend- Trial version expiring in 21 days.

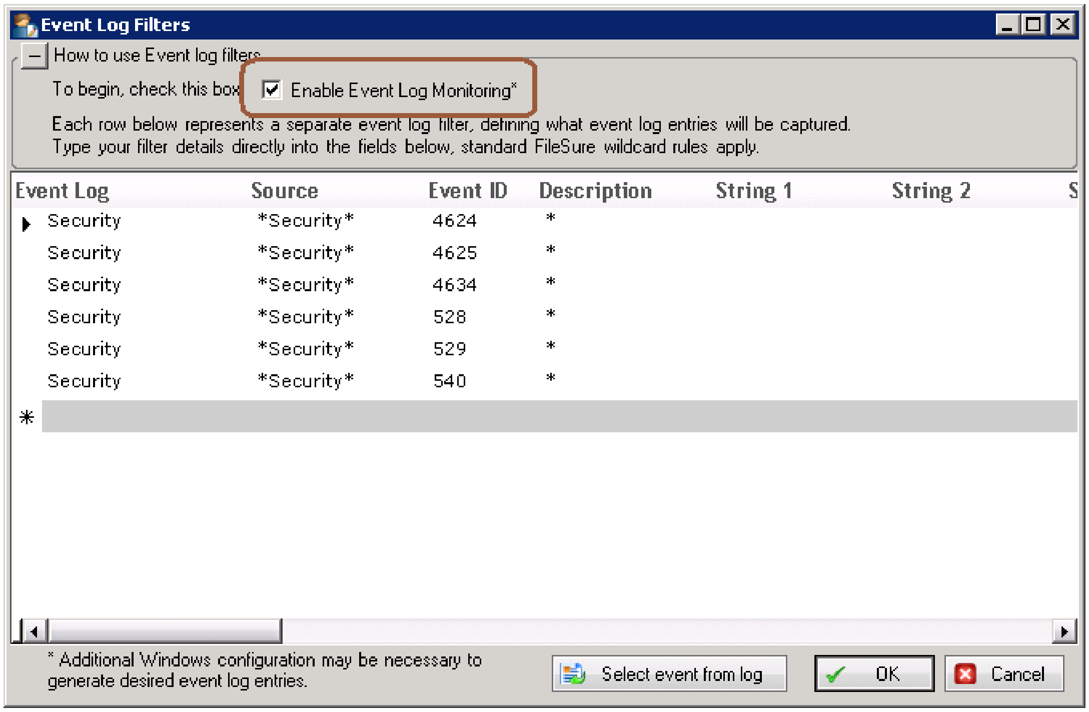
Current file activity for : WIN2008X64

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

Time	Username	Operation	File

☑ Auditing Rule - Trial Rule for Local Machine - Audit Access to Microsoft Office Files

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



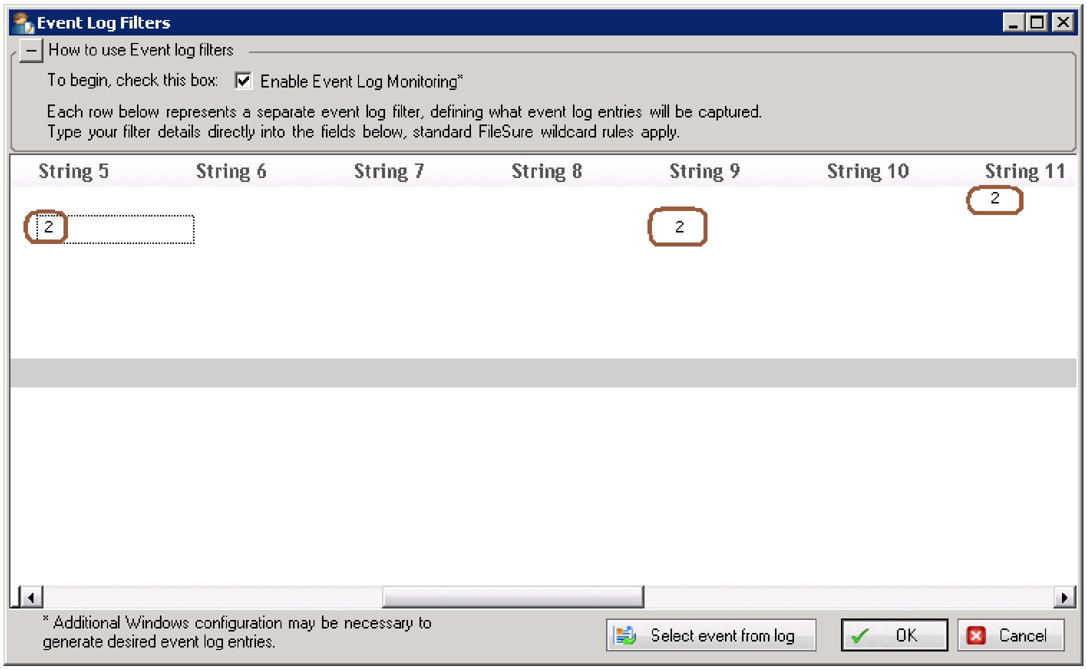
To begin, check this box ☑ Enable Event Log Monitoring*

Each row below represents a separate event log filter, defining what event log entries will be captured.
Type your filter details directly into the fields below, standard FileSure wildcard rules apply.

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 Windows configuration may be necessary to generate desired event log entries.

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.



To begin, check this box: ☑ Enable Event Log Monitoring*

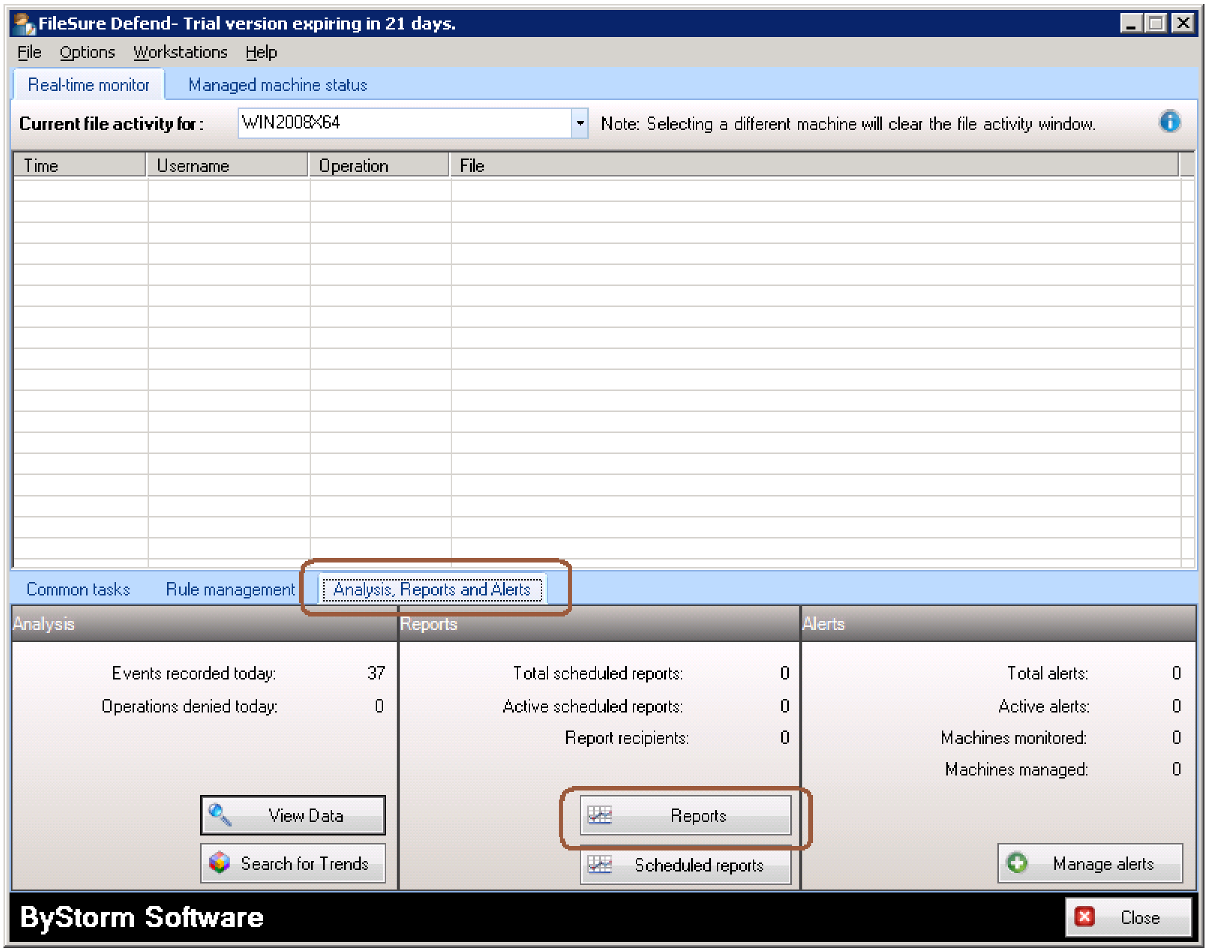
Each row below represents a separate event log filter, defining what event log entries will be captured.
Type your filter details directly into the fields below, standard FileSure wildcard rules apply.

String 5	String 6	String 7	String 8	String 9	String 10	String 11
						2
2				2		

* Additional Windows configuration may be necessary to generate desired event log entries.

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:



Current file activity for : WIN2008X64

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

Events recorded today: 37

Operations denied today: 0

Total scheduled reports: 0

Active scheduled reports: 0

Report recipients: 0

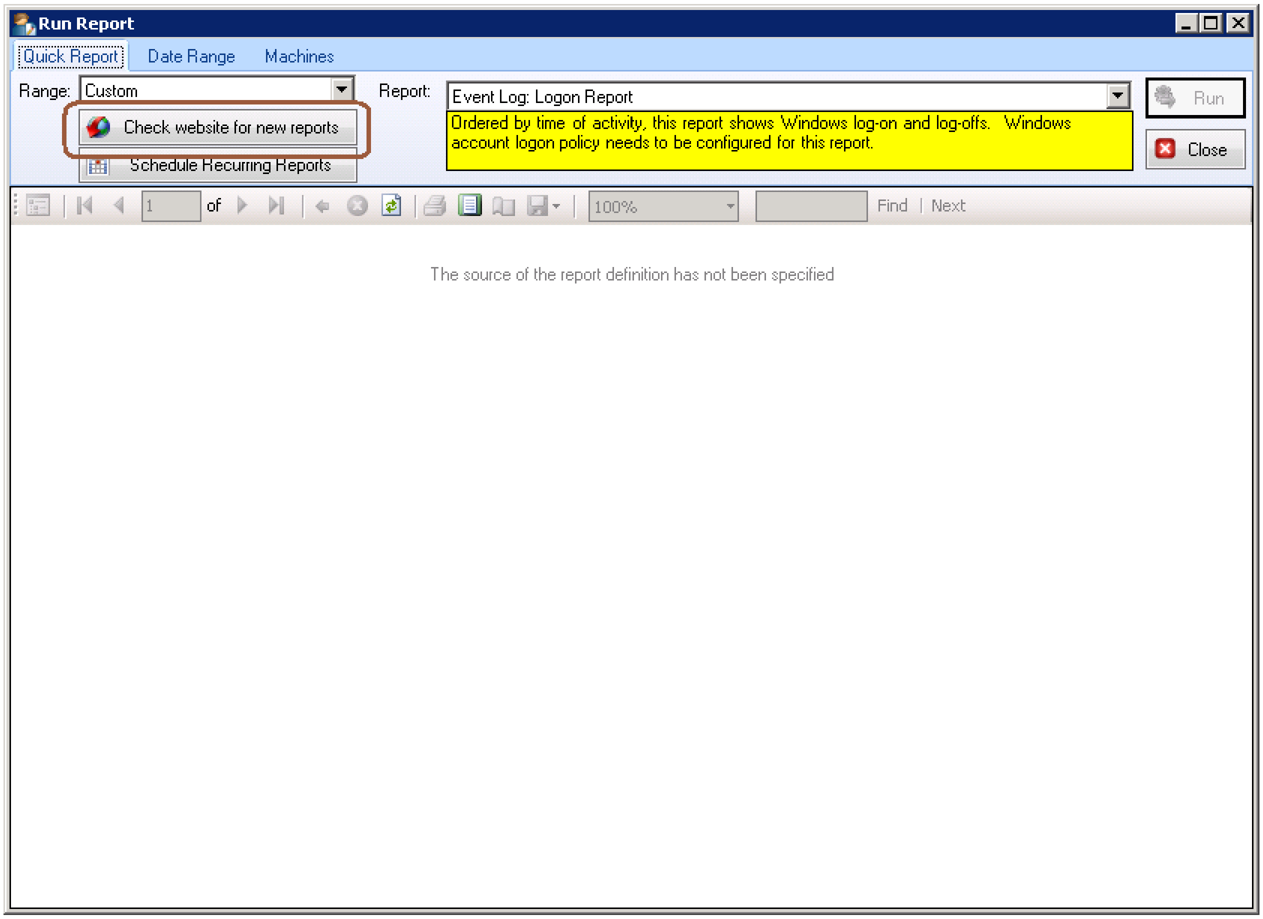
Total alerts: 0

Active alerts: 0

Machines monitored: 0

Machines managed: 0

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’



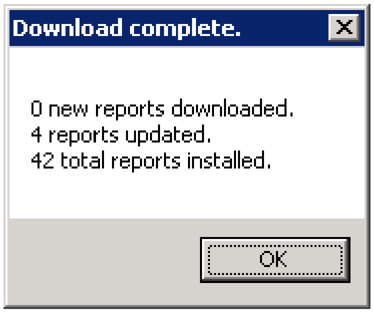
Range: Custom

Report: Event Log: Logon Report

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.

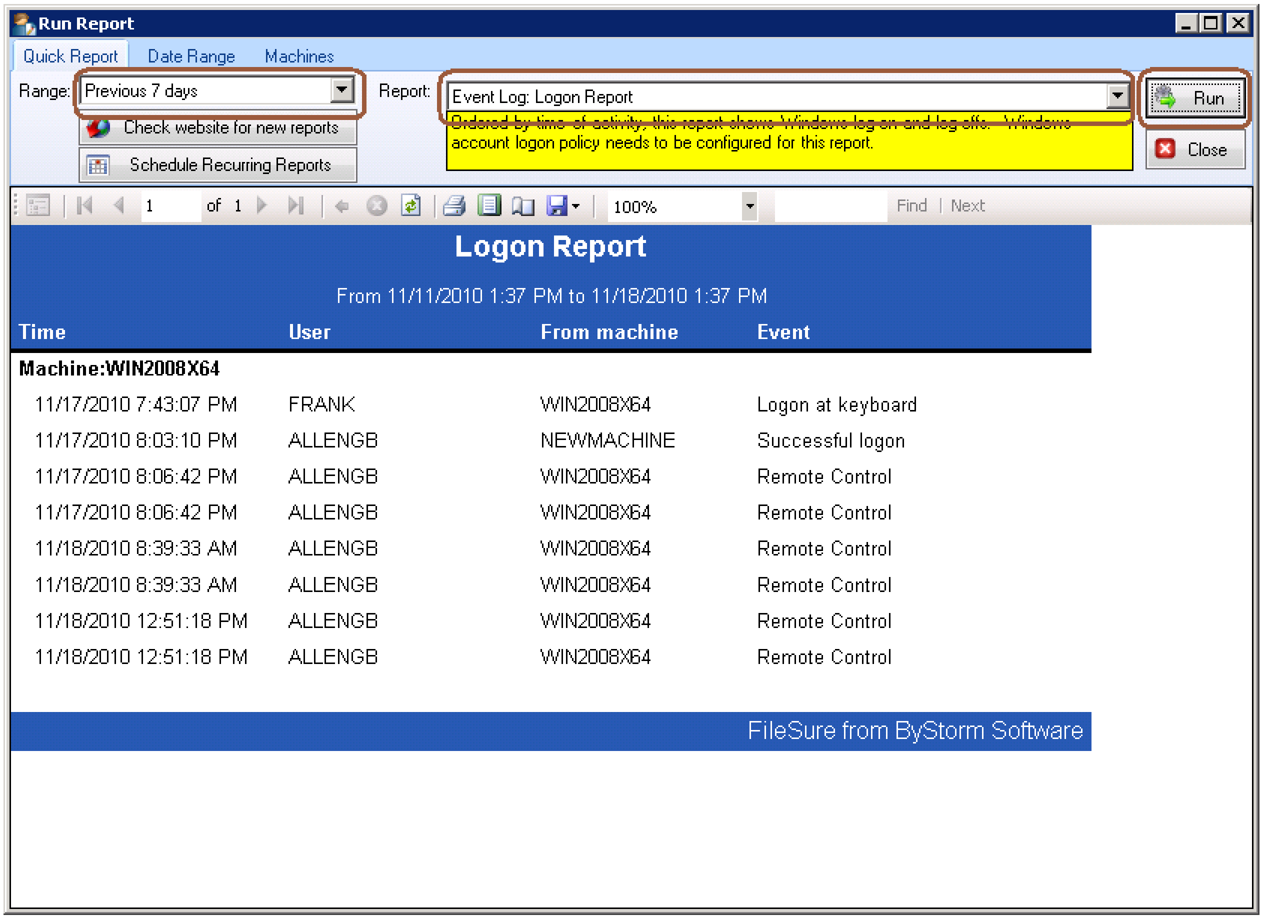
The source of the report definition has not been specified

7. This will download and update the available reports:


Download complete.

0 new reports downloaded.
4 reports updated.
42 total reports installed.

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:



Range: Previous 7 days

Report: Event Log: Logon Report

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.

100%

Logon Report

From 11/11/2010 1:37 PM to 11/18/2010 1:37 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 Software