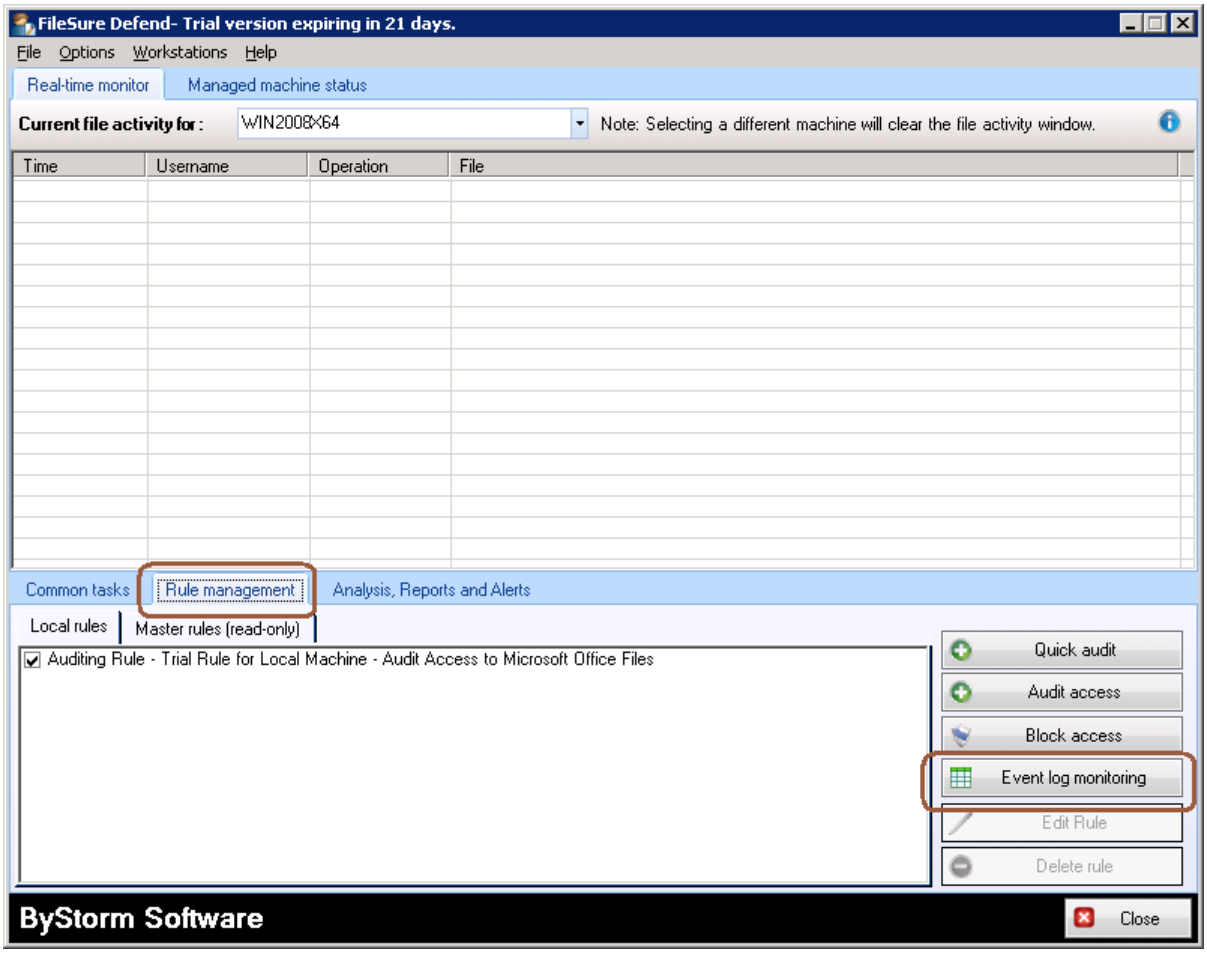
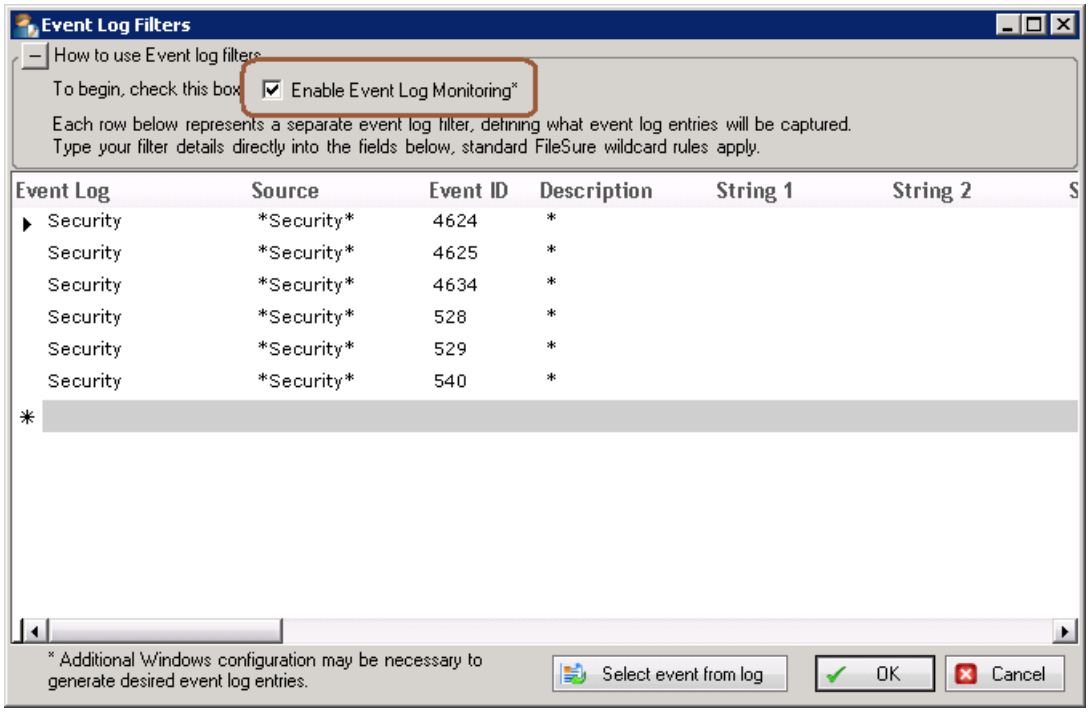
With FileSure 2.5, we added the ability to audit Windows event logs. The captured events are securely stored right with your other FileSure auditing data in FileSure's encrypted, compressed data store. In this How-To, I'm going to configure FileSure to monitor and record when Firewall changes occur on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

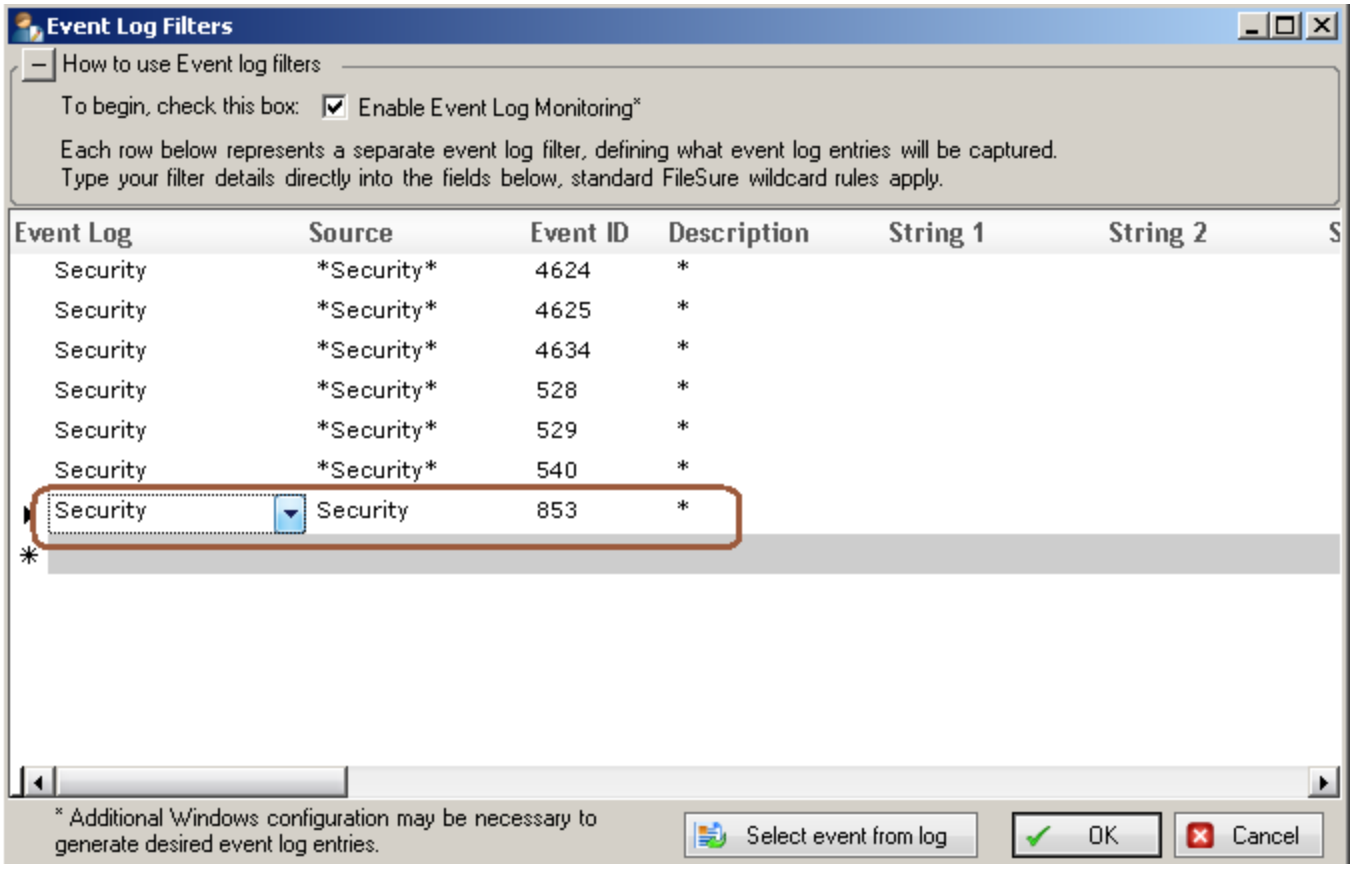
1. Start FileSure, switch to the 'Rules management' tab and click the 'Event log monitoring' button:



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

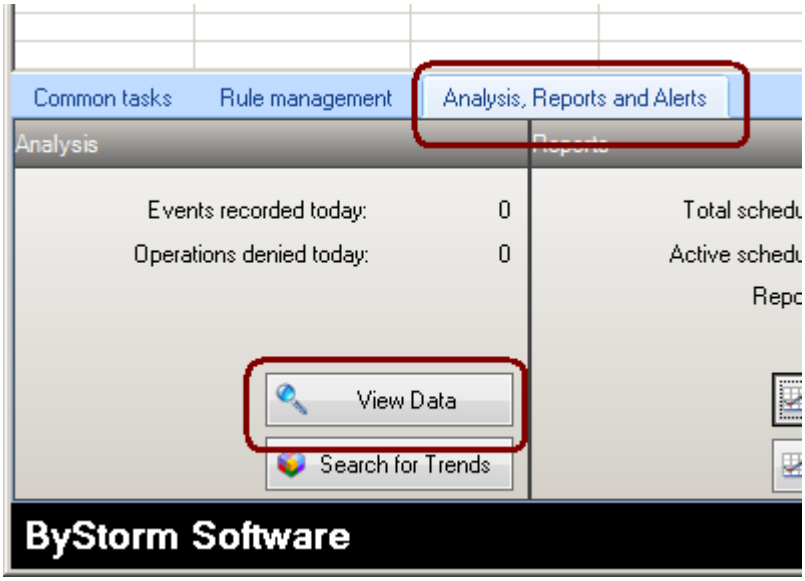


FileSure is 'pre-configured' to gather authentication events on Windows 2003, but we need to add a new entry for the enrties we're interested in. According to http://technet.microsoft.com/en-us/library/cc736708%28WS.10%29.aspx and http://technet.microsoft.com/en-us/library/cc737845%28WS.10%29.aspx, Firewall 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.

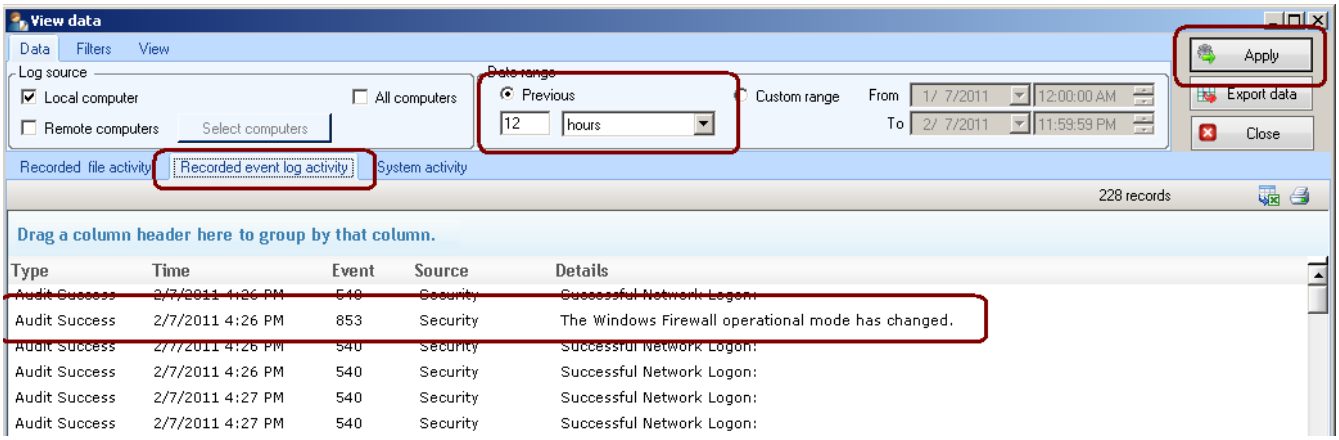


3. Click 'OK' to close the Event Log Filters screen and now FileSure will now be gathering Firewall operational change events for the current computer. As a test, turn the Firewall off and on to generate the events.

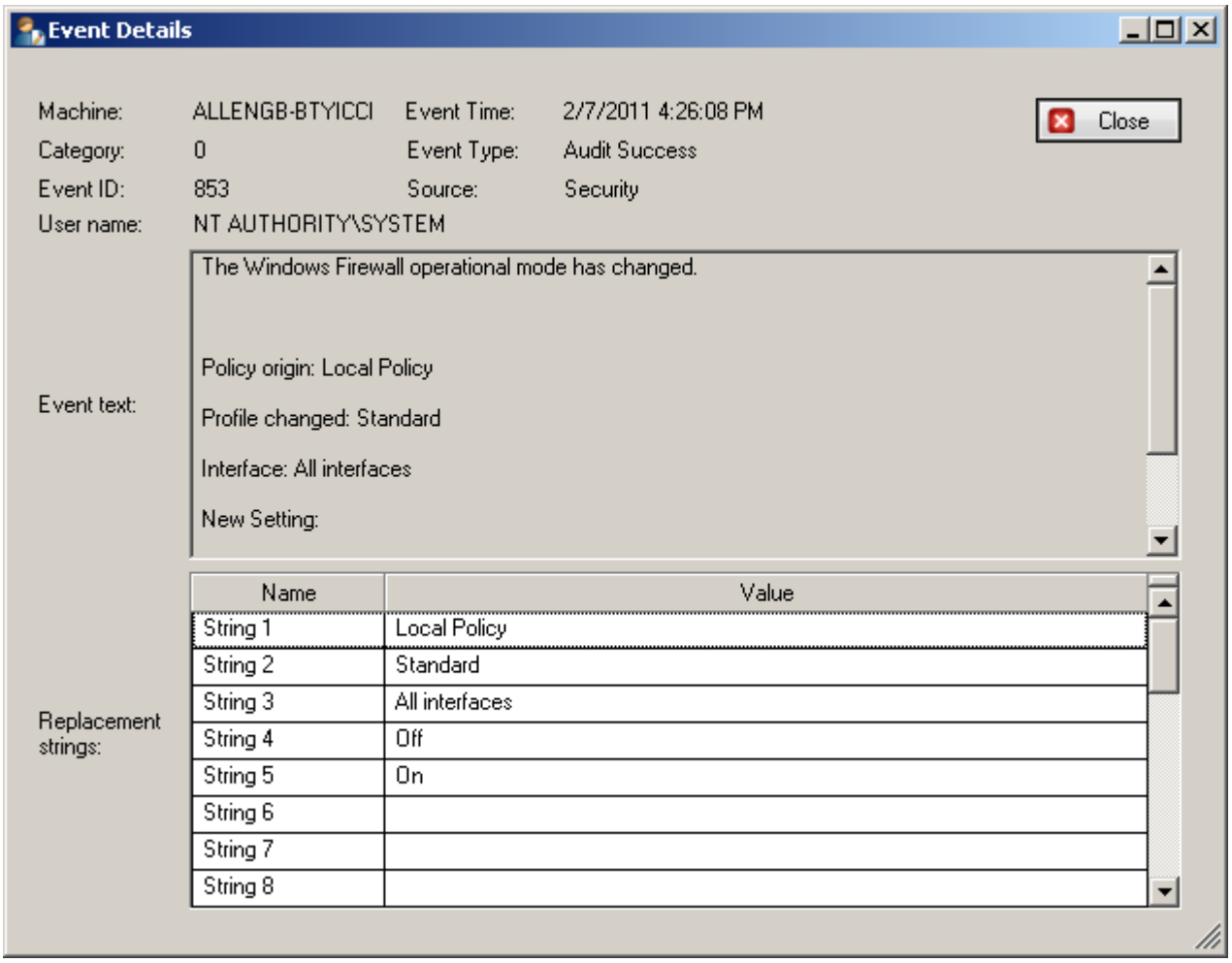
4. After 'a while' switch to the 'Analysis, Reports and Alerts' tab and click on the 'View Data' button:



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.



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.



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.