



## What's New in File System Auditor 2.5?

### Windows File Auditing Made Easy

File System Auditor, a unique solution for recording Windows file server activity, allows administrators to audit file access, generate easy-to-understand reports, and create alerts tied to file system events all from a centralized management console. Ideal for protecting confidential or sensitive data, File System Auditor assists in compliance reporting by creating an audit trail of file activity on sensitive information such as patient records or financial reports. File System Auditor assists in security management by sending email alerts whenever specific file system events occur such as access denied events, or modifications of a particular set of files and folders.

### New Feature highlights

#### **\*NEW\*** File Share Auditing

Shared folders provide end users the ability to remotely access data stored on file servers. Any changes to these shared folders or the permissions associated with them can have a serious affect on user productivity and network security. In order to ensure the proper access is maintained to network data, it is imperative to monitor any changes that occur to file shares.

File System Auditor 2.5 now provides the ability to audit changes to file shares. Audit all events related to file shares including share creations, deletions, and security modifications. With this new functionality File System Auditor can help to ensure the proper access is maintained to shared data by auditing all changes to shares in real time, and alerting administrators when changes do occur.

Audit and report on file share change events on all servers across the network to show an audit trail of all changes that have occurred over time.

### File System Auditor - Audit Report

**Summary:** 4 Events  
**Date Range:** The past 1 hour from Wednesday, September 30, 2009 1:46 PM  
**Events:** File Share - Created, File Share - Deleted, File Share - Modified, File Share - Modified Security  
**Paths:** [All Paths]  
**Users:** [All Users]  
**Processes:** [All Processes]  
**Servers:** [All Servers]  
**Workstations:** [All Workstations]

ScriptLogic Corporation - File System Auditor

**Wednesday, September 30, 2009**

Date:	Time:	User:	Event:
9/30/2009	1:44:26 PM	Administrator (QATEST\Administrator)	File Share - Modified
<b>Server:</b> QA-2K8R2-1 (QATEST)			
<b>Process:</b> System			
<b>Workstation:</b> QA-2K8R2-1.qatest.local (192.168.163.139)			
<b>Path:</b> [Share1] C:\Share1			
9/30/2009	1:15:01 PM	Administrator (QATEST\Administrator)	File Share - Deleted
<b>Server:</b> QA-2K8R2-1 (QATEST)			
<b>Process:</b> System			
<b>Workstation:</b> QA-2K8R2-1.qatest.local (192.168.163.139)			
<b>Path:</b> [Share3] C:\Share3			
9/30/2009	1:13:28 PM	Administrator (QATEST\Administrator)	File Share - Modified
<b>Server:</b> QA-2K8R2-1 (QATEST)			

Configure alerts to be sent when changes are made to file shares, enabling administrators to respond to potential issues right away.

### Event Viewer - File System Auditor

Event Viewer

Server Name: QA-2K8R2-1 (QATEST)

Time Generated: 9/30/2009 1:55:24 PM

Account: Administrator (QATEST\Administrator)

Event Name: File Share - Modified Security

Source Path: [Share1] C:\Share1

Rename To:

Process Name: System

Client Workstation: QA-2K8R2-1.qatest.local (192.168.163.139)

Security Changes

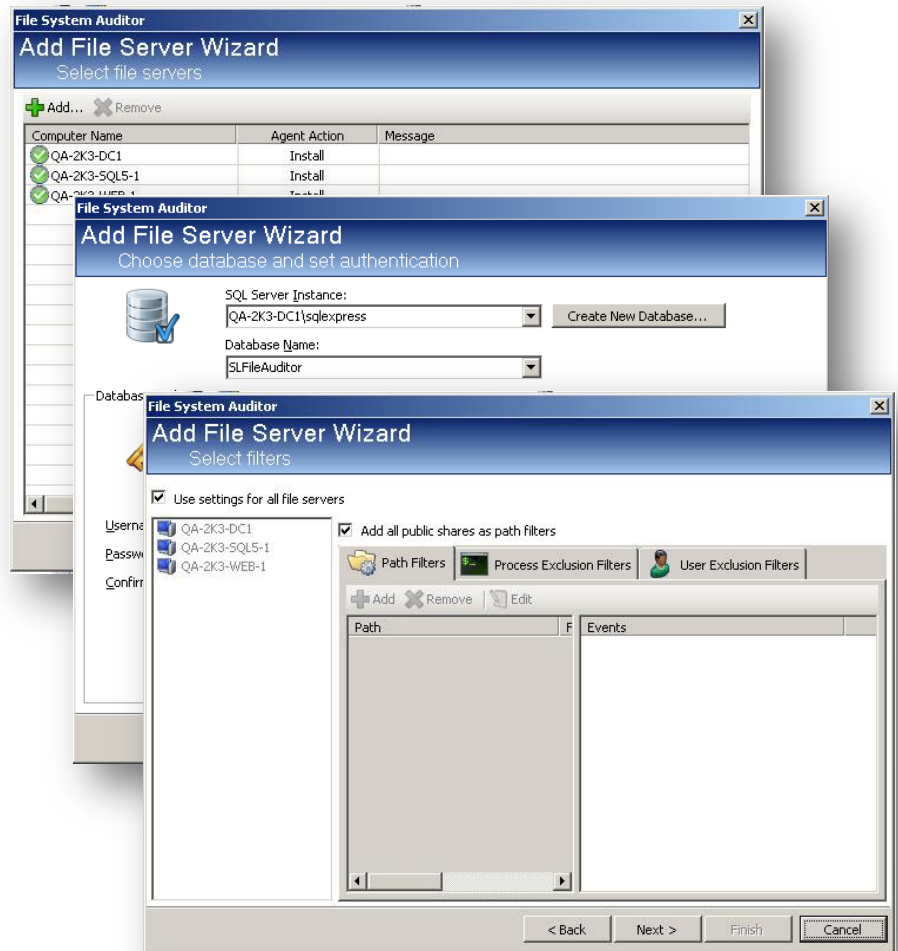
Name	Type	Permissions	Applies To
<b>Permissions Removed</b>			
Everyone	Allow	Full Control, Read, Write, Execute, De...	This folder, subfold...
<b>Permissions Added</b>			
Everyone	Allow	Read, Execute, List Folders, Read Attr...	This object only

Previous Event    Next Event    Close

### \*NEW\* Agent Deployment Wizard

File System Auditor 2.5 adds a new agent deployment wizard which simplifies the installation and configuration process when deploying auditing agents to file servers. The agent deployment wizard allows for deploying the auditing agent to multiple servers simultaneously, eliminating the need to deploy and configure auditing agents independently.

Agent configuration settings including path, user and process filters as well as database settings can be set for multiple file servers at one time. This will help to ensure agents are deployed quickly and consistently across the network.



### \*ENHANCED\* Audit events now display workstation name and IP address for client workstation

All audit events collected by the File System Auditor agent will now include the workstation name and IP address of the client machine that initiated the event. This provides administrators and auditors with the information to know not only WHO made the change, but also WHERE the user was logged in at the time the change occurred.

Filter results and generate reports to show all events that originated from a specific workstation or IP address.

Account	Event	Path	Client Workstation	IP Address
Administrator (QATEST\Administrator)	File - Created	C:\Share\Join_domain.vbs	QA-2K8-DC1.qatest.local	192.168.163.135
Administrator (QATEST\Administrator)	File - Modified	C:\Share\Join_domain.vbs	QA-2K8-DC1.qatest.local	192.168.163.135
Administrator (QATEST\Administrator)	File - Created	C:\Share\GetTableSizesSpac	QA-2K8-DC1.qatest.local	192.168.163.135
Administrator (QATEST\Administrator)	File - Modified	C:\Share\GetTableSizesSpac	QA-2K8-DC1.qatest.local	192.168.163.135
Administrator (QATEST\Administrator)	File - Created	C:\Share\createfiles.kix	QA-2K8-DC1.qatest.local	192.168.163.135
Administrator (QATEST\Administrator)	File - Modified	C:\Share\createfiles.kix	QA-2K8-DC1.qatest.local	192.168.163.135
Administrator (QATEST\Administrator)	File - Created	C:\Share\CreateADGroupsUs	QA-2K8-DC1.qatest.local	192.168.163.135
Administrator (QATEST\Administrator)	File - Modified	C:\Share\CreateADGroupsUs	QA-2K8-DC1.qatest.local	192.168.163.135
Administrator (QATEST\Administrator)	File - Created	C:\Share2\Share.xps	QA-2K8R2-1.qatest.local	192.168.163.139
Administrator (QATEST\Administrator)	File - Modified	C:\Share2\Share.xps	QA-2K8R2-1.qatest.local	192.168.163.139
Administrator (QATEST\Administrator)	File - Read	C:\Users\administrator.QATES	QA-2K8R2-1.qatest.local	192.168.163.139
Administrator (QATEST\Administrator)	File - Read	C:\Users\administrator.QATES	QA-2K8R2-1.qatest.local	192.168.163.139
Administrator (QATEST\Administrator)	File - Read	C:\Users\Public\Desktop\deskt	QA-2K8R2-1.qatest.local	192.168.163.139
Administrator (QATEST\Administrator)	File - Read	C:\Users\Public\Desktop\deskt	QA-2K8R2-1.qatest.local	192.168.163.139
Administrator (QATEST\Administrator)	File - Read	C:\Users\desktop.ini	QA-2K8R2-1.qatest.local	192.168.163.139
Administrator (QATEST\Administrator)	File - Read	C:\Users\desktop.ini	QA-2K8R2-1.qatest.local	192.168.163.139

### **\*NEW\*** Automatically purge audit data once it reaches a certain age

Audit trail history typically must be retained for a certain period of time for compliance reasons. However, as time goes by old audit data may be backed up and archived so that it no longer needs to be stored in the audit database. Once archived, purging old data will help maintain the size of the auditing database which will conserve disk space and increase reporting performance. File System Auditor provides the ability to manually purge data at any time through the configuration console interface but previously did not provide the ability to automatically purge old data. With version 2.5, File System Auditor adds the ability to purge all data past a certain age on a scheduled basis.

Combined with a database maintenance plan to archive data; purging old information helps to keep the audit database at an efficient size for minimal disk usage and optimal application performance.



### **\*NEW\* Platform support**

File System Auditor 2.5 adds support for auditing Windows Server 2008 R2 systems, along with console support on Server 2008 R2 and Windows 7 operating systems. The auditing database is now supported on SQL Server 2008.

## **Summary**

File System Auditor 2.5 adds a number of features that help enable administrators to meet their compliance and auditing needs more effectively. With this exciting new release administrators can now audit and report on file share changes in real time, determine the computer and IP address of the source workstation for all events, deploy multiple agents quickly and consistently, and more easily remove old audit data to maintain an efficient database size!

In conjunction with Enterprise Security Reporter and Security Explorer, File System Auditor 2.5 provides a complete solution for bringing a file server into compliance. Ask your reseller or ScriptLogic representative about our File Server Compliance Solution, which combines all 3 products at a significant discount.

© Copyright 2009 ScriptLogic Corporation. All Rights Reserved.