

FS FILE SYSTEM AUDITOR™

File System Auditor is a unique, centralized auditing solution that allows administrators to easily record Windows file server activity, audit file access and report and alert on file system events. Meeting compliance objectives and securing sensitive data is easily achieved by creating a secure audit trail of file activity and alerting on unusual or other specified behaviors.

THE CHALLENGE: WHO ACCESSED WHAT?

File systems contain vast amounts of business critical and sensitive information that if left unprotected, could get into the wrong hands and negatively impact your organization. Unplanned downtime, disruptions in service and costly fines stemming from security breaches are all factors that must be taken into consideration when managing these systems. And organizations need to find a way to better control, protect and administer the activity on their file systems without the need to comb through numerous audit entries.

THE SOLUTION: FILE SYSTEM AUDITOR

Audit, report and alert on Windows file server activity, get a clear picture of who accessed what file and when and let File System Auditor take the guessing out of access-related events. Ideal for protecting sensitive information, this solution differentiates itself from the competition by eliminating the need to configure native Windows auditing. And with File System Auditor, you can instantly benefit from the solution with its easy-to-use interface and "Point, Click, Done" deployment that allows you to avoid long and costly implementations often associated with other event log consolidation tools.

INTELLIGENT MONITORING

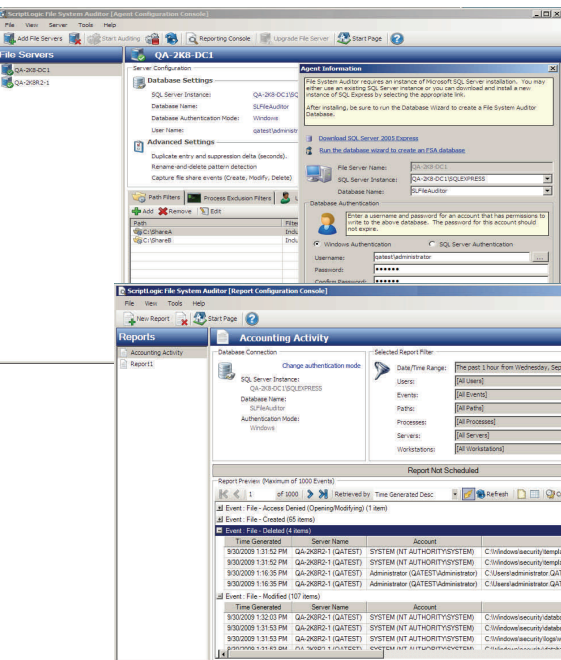
File System Auditor allows administrators to monitor file system activity, return a single entry and avoid manual parsing of what could potentially be dozens of native event log entries. Additionally, not only knowing WHO made the change, but WHERE the user was logged on is easily attained since FSA will also display the IP address and workstation name of the client machine that initiated the event.

FLEXIBLE REPORTING

Audit usage and generate reports based on pre-defined detailed criteria. Reports can be generated and emailed in real-time or scheduled for automatic delivery. Reports can be exported in a variety of formats depending on user needs or preference.

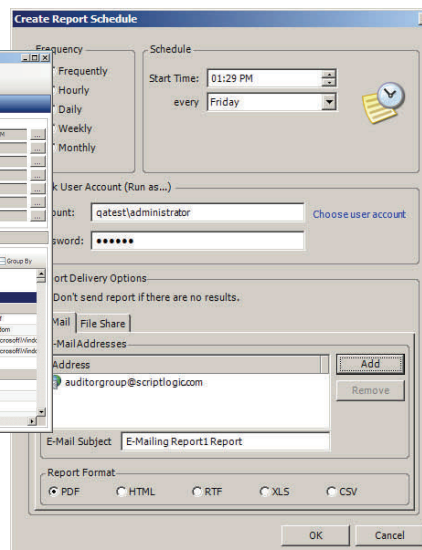
ENHANCED SERVER SECURITY

Validate the strength of security controls and automate reporting for both external compliance requirements and internal security directives. From a single location, administrators can audit all file system changes and store those events for any future investigations, ensuring their systems are protected.



Agents are easily and consistently deployed to multiple file servers across the network. All events are stored in a central database, eliminating the need to configure Windows auditing and monitor event logs across multiple servers.

Schedule specific reports to be sent to recipients via email, or export to a shared location. Reports can be exported in numerous file formats including PDF, HTML, RTF, XLS, and CSV.



FSA displays results (based on the Event Filters) that represent a single file system task and depicts who performed the action on which file, folder, share and server and includes the source and target paths of any data that is moved. FSA also includes the IP address and workstation name of the computer that initiated the event.

KEY BENEFITS

Meet Compliance Requirements
HIPAA, SOX, GLBA and PCI DSS require access controls be implemented for any information pertaining to patient records, financial information or customer data. Easily demonstrate that the proper controls are in-place for any investigations stemming from misuse and tampering of sensitive company data.

Secure Audit Trail

Audit events are stored in a SQL database, maintaining a secured historical record of file access events. Once archived, those records can then be purged based on age, allowing the administrator to more easily manage the growing database.

KEY FEATURES

Centralized Management

Remotely install file server agents to any file server on your network – (without rebooting the server) from a centralized location, and reduce the effort required for establishing audit policies across multiple file servers.

Comprehensive Auditing

Audit events on files, folders and shares and capture who performed an action, what action occurred, which file/folder was tampered with, which server was accessed and from which IP address or workstation the user was logged into at the time.

Robust Reporting

Generate reports for distribution using the event filter in various formats including PDF, XLS, CSV, TIF, TXT, RTF and HTML.

Scheduled Notifications

Schedule reports in 5-minute intervals, daily, weekly, etc. so administrators and other stakeholders can have up-to-date information on file system activity.

SYSTEM REQUIREMENTS

Audit Collection

Windows 2000/2003/2008 & 2008 R2 file server. MSDE, SQL Express, or SQL Server 2000/2005/2008.

Reporting and Agent Configuration Console

Any computer with Windows 2000/XP/2003/Vista/2008 & 2008 R2 and Windows 7.

Licensing

File System Auditor is licensed per server. For pricing, contact your ScriptLogic reseller or call ScriptLogic at 1.800.813.6415