



# Dell Change Auditor for FluidFS

Dell software tool to track, audit, report on and alert on critical changes

## Benefits of Change Auditor for FluidFS Storage

- Eliminates unknown security concerns, ensuring continuous access to FluidFS files, folders and users by tracking all events and those changes related to specific incidents
- Enables you to pinpoint problems quickly with robust search and filtering capabilities
- Reduces security risks with real-time alerts to any device for immediate response
- Facilitates auditing and management review by converting cryptic data into intelligently organized, in-depth forensics
- Streamlines internal security policies and external compliance regulations including SOX, PCI DSS, HIPAA, FISMA and SAS 70

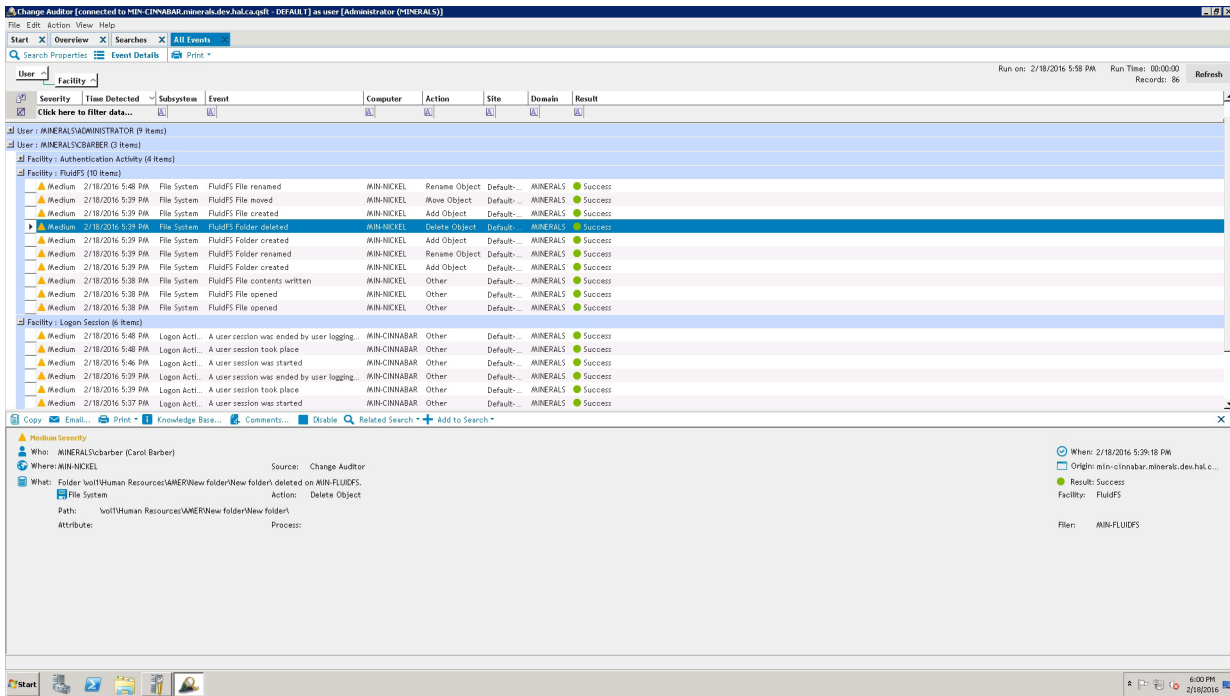
Event logging and change reporting is cumbersome and time-consuming using native auditing tools. Because there's no central console, you have to repeat the process for each server, and you end up with a huge volume of data and a myriad of reports. That means proving compliance or reacting quickly to events is a constant challenge. Your data security is also at risk because native event details are sparse and difficult to interpret. As a result, you may not find out about problems until it is too late. And because native logs can be deleted or overwritten, the integrity of the log data can be compromised, defeating the purpose of auditing in the first place.

Dell is addressing this threat by adding support for integration of Dell™ Fluid File System (FluidFS v5) on the FS8600 platform with Dell Change Auditor™. Dell FluidFS storage offerings are open-standards-based, scale-out, network-attached storage (NAS) solutions that meet the capacity, performance, reliability, flexibility and scalability requirements of modern data centers. Dell FluidFS storage is connected to a back-end Dell Storage SC Series array providing a unified block and file storage offering. This is all centrally managed using the Enterprise Manager console.

The Change Auditor tool helps ensure the security, compliance and control of files and folders by monitoring, auditing, reporting and alerting on all changes in real time. With Change Auditor, administrators can monitor, report on and analyze events and changes without complexity and fear of unknown security concerns. You will instantly know who made what change when, where, from which workstation and all related events to that change. You can then automatically generate intelligent, in-depth forensics and reduce the risk associated with day-to-day modifications.

The screenshot displays the Dell Change Auditor web interface. At the top, it shows the user is logged in as Administrator (MINERALS). The main area is titled 'My Favorite Search: All FluidFS Events' and shows a table of events. The table has columns for Severity, Time Detected, Subsystem, User, Computer, File Server, Action, Domain, and Result. Below the table, there is a detailed view of a specific event: a file rename operation performed by MINERALS\barber on 2/18/2016 at 5:48 PM. The event details include the source (Change Auditor), the file path (\\vol1\Human Resources\AWERFY16 salary awards.xls.txt), the action (Rename Object), and the result (Success).

With Change Auditor, you can gather events from all your Dell FluidFS storage servers in one place, and in one format so you can quickly see the most relevant and potentially dangerous changes.



With Change Auditor, immediately learn more about what a particular event means and its severity.

## Audit all critical changes

Change Auditor for FluidFS provides extensive, customizable auditing and reporting for all critical changes to FluidFS files, including files, folders, servers, permissions and configuration settings. You'll get complete visibility into all changes over the course of time and in chronological order with in-depth forensics on who, what, when, where, why and workstation, including any related events with before and after values. And, with real-time alerts to any device, you'll maintain constant awareness and the ability to respond to vital changes as they occur, reducing the risks associated with day-to-day modifications.

## Track user activity

Change Auditor for FluidFS helps tighten enterprise-wide auditing and compliance policies by tracking user and administrator activity for FluidFS file changes. Change Auditor also provides information on administrators and users who have gained or changed file access rights. You'll see exactly who accessed, deleted, moved, created or renamed files and folders. And with 24x7 real-time alerts, in-depth analysis and reporting capabilities, your FluidFS infrastructure is protected from exposure to suspicious behavior or unauthorized access, and is always in compliance with corporate and government standards.

## Learn More at [Dell.com/FS8600](http://Dell.com/FS8600).

## Turn irrelevant data into meaningful information to drive security and compliance

Change Auditor for FluidFS eliminates guesswork analysis reporting by translating isolated cryptic data into a series of meaningful events. You'll instantly get all information on the change you're viewing and all related events such as what other changes came from specific users. You will also gain a better understanding of event trends with the ability to view, highlight and filter related events over the course of days, months and even years.

## Automate reporting for corporate and government regulations

Utilizing Microsoft's SQL Reporting Services (SRS), Change Auditor for FluidFS provides clean, meaningful security and compliance reports on the fly. With a built-in compliance library and the ability to build your own custom reports, proving compliance for standards such as Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA) and Statement on Auditing Standards No. 70 (SAS 70) is a breeze.

