

## File System Auditor™ vs Native Windows Auditing

Product Feature	File System Auditor	Native Windows Auditing
<b>Auditing</b>		
Enabling Auditing	Auditing of both files and folders is centrally accomplished within the Service Configuration Console on a per server basis.	Auditing is enabled first at the system policy level and then individual folders and files need to be configured to be audited.
View Auditing Configuration	File System Auditor provides a single listing of all folders and files audited on a server.	It is necessary to navigate to the Advanced security settings for each folder (and potentially file) audited to see if auditing is enabled.
Storage	Events are centrally stored in a secure SQL database providing a secure audit trail.	Events are stored per server within insecure Event Logs
Entries per event	Intelligent Auditing yields a single event for both simple events, such as a file read, as well as complex events, such as a file move.	Tens of entries are created for each event. For example, in a simple test of creating a text file and immediately deleting it, native auditing yielded 42 entries with File System Auditor showing 2 – the creation and deletion of the file.
<b>Reporting</b>		
Filtering	<p>Events can be filtered based on:</p> <ul style="list-style-type: none"> <li>● Date/Time Range</li> <li>● User(s)</li> <li>● Event Type(s)</li> <li>● Path(s)</li> <li>● Process(es)</li> <li>● Server(s)</li> </ul>	Limited event filtering is available based on Event ID and date/time range. (While event filtering in Windows supports other filter criteria, they have no effect on file system auditing events.)
Filter Scope	Filters apply enterprise-wide covering all servers configured to use the same SQL database.	Filters apply to a single server's events.
Reporting	Reports are generated based on filtered criteria.	No reporting – can copy a single event to the clipboard.
Exporting Report Results	Reports can be exported to the following formats: RTF, PDF, HTML, XLS, TIF, TXT and RDF	Filtered event logs can be exported to EVT, CSV and TXT formats.
<b>Notification</b>		
Real-Time Notification	Reports can be emailed to designated recipients at 5 minute intervals for real-time notification of occurring events. (5 minute intervals are used to avoid having a new report emailed every second a file is accessed, etc).	No notification capabilities.
Historical Notification	Reports can be scheduled daily or weekly to be emailed to the designated recipients for review by management, security staffo notification capabilities.	