

## CPTRAX TECHNICAL BRIEF



### Why choose CPTRAX for File System Auditing and Control?

<b>Does not use Windows Event Logs</b>
<b>Does not use Polling</b>
<b>Low Overhead – No Windows configuration changes required</b>
<b>Real-Time Reporting and Optional Blocking of unwanted activity</b>

You have many choices when selecting a file system auditing and control solution for your Windows® network. We created CPTRAX to give you a *better* choice. This document has been prepared to provide a technical review of file system auditing methods and how CPTRAX for Windows is a better choice.

### CPTRAX *versus*: Windows Event Log Readers

Several file system auditing products available rely upon Windows Event Logs to provide input for their reporting. And, many of these products require you to do your own Event Log “auditing” configuration. This is performed via a tedious manual process that involves visiting each folder (directory) to audit, select audit options and *repeat* for each user and/or group to audit. The following image reveals file system audit options for Windows event logs.

As you can see, the list of options to audit is not entirely self-descriptive, for instance, what would you select to watch files being opened? What about file renames? What about tracking when files are really deleted versus simply moved to the Recycle Bin?

As shown in the image the “Name” to audit is “Everyone” which is a special group indicating all objects.

Notice the “Name” field is singular, it is *not* a list. Further, you can only define auditing options for single object (group, user or other) at a time! If you do not want to track Everyone, but instead track selected accounts, you will either need to create and



## CPTRAX TECHNICAL BRIEF

maintain a group that contains those objects or directly add each account, one at a time. And you will need to modify the objects being audited each time an object is added or deleted from your environment. Remember, when an object is deleted, anywhere it is defined for auditing will remain as there is no auto-clean up performed by Windows.

Continuing, what if you only want to know when certain files are changed? You could define auditing on select files, but, files are often deleted and re-created as part of normal operations making it difficult if not logistically impossible to audit at the file level. Not to mention new files would not be audited at all until auditing was established for each new file. All this means auditing options must be defined at the folder / directory level. Thus, if you simply wanted to track *only* activity upon XLS or DOC files you cannot define it within the Windows Event Log system. And it is the Windows Event Log system that many file system auditing products rely upon. Most of these tools offer report filtering so you can receive reports of just what you want but the Event Log files will be full of data you did not want to track.

All of this puts the Windows file system auditing process *in charge of you* because you have to constantly work for what you want and need.

Event Log details include:

- File name (all events are curiously listed as being for a file even when it is for a Folder)
- Event Type
- Account (user) and Domain name
- If Account was local or remote
- Time of Event
- Permissions changed (if event is modification of security (DACL or ACL) there is no record in the Event Log of what changes were made, only that the DACL was changed)
- Owner changed (new owner identity is not recorded)

**Event Log details *do not include* (these are included by CPTRAX):**

- For remote events, name of workstation where user was
- For remote events, IP address of where user was
- For remote events, Share name access was initiated upon
- For terminal server sessions, remote workstation where user was
- For terminal server sessions, IP address of where user was
- Account's Security Identifier or SID
- Account's Distinguished Name or LDAP style name
- Permissions that were changed (when DACL is updated)
- Account Name of new Owner
- Renames are not tracked, only the original filename is recorded as being deleted but no create is recorded for the new filename (or folder name)

And, lastly, Event Log readers do not have the ability to block undesirable file actions.

## CPTRAX TECHNICAL BRIEF

### CPTRAX *versus*: Polling and Snapshot Captures

Some of the available file system auditing products gather file system activity independently of Windows Event Logs via polling and snapshot captures. These products do not require auditing to be configured within the Windows event system. Some of these products include the option to add events to the Windows Event Log based upon activity independently gathered.

As implied by this section's header, polling and snapshot capture file system activity auditing products only report on what is found after the fact. Though some of the products in this group claim to have real-time auditing abilities, it is still based on polling technology. The limitations are consequential as only the bare minimum of file system activity is revealed. On the plus side, due to the lack of direct involvement in auditing file system activities, polling and snapshot products will record fewer events than the Windows Event Log system.

Polling/Snapshot details can include:

- File/Folder name
- Event Type – limited to:
  - File/Folder Added
  - File/Folder Deleted
  - File Size Changed
  - Permissions Changed (only if product saves these data before the change)
  - Owner Changed (only if product saves these data before the change)
- Time of Event (for 'real time polling' only, otherwise, time is approximate or "best guess")

**Polling/Snapshot details *do not include* (these are included by CPTRAX):**

- All File/Folder Events occurring between polling or snapshot periods
- Account (User) performing event / action
- Name of workstation where user was
- IP address of where user was
- For remote events, Share name access was initiated upon
- For terminal server sessions, remote workstation where user was
- For terminal server sessions, IP address of where user was
- Account Security Identifier or SID
- Account Distinguished Name or LDAP style name
- File/Folder Renames
- File Open / Read events
- File Change events as they occur

And, lastly, Polling and Snapshot Capture products do not have the ability to block undesirable file actions.

## CPTRAX TECHNICAL BRIEF

### CPTRAX *versus*: File System Drivers

A few of the available file system auditing products use a kernel-level File System Driver to gather file system activity independently of Windows Event Logs. These products do not require auditing to be configured within the Windows event system.

These File System Driver products gather events by being directly involved with file system actions as each occurs. File System Drivers are kernel-level agents that, when in use, become part of the Windows file system. This means each file system activity is passed through the agent before it is applied to the affected file or folder. This “low level” of involvement with the Windows file system means nothing is missed. However, the only critical detail tracked is the name of the user (or other account) performing the file action. This means details of remote access are not recorded, no workstation name, no IP address.

File System Driver recorded details include:

- File/Folder name
- Event Type
- Account (user) and Domain name plus Distinguished Name
- Time of Event
- Permissions changed with full change details
- Owner changed and new owner identity

**File System Driver recorded details generally *do not include*** (these are included by CPTRAX):

- No direct indication of action was performed locally or remotely
- For remote events, name of workstation where user was
- For remote events, IP address of where user was
- For remote events, Share name access was initiated upon
- For terminal server sessions, remote workstation where user was
- For terminal server sessions, IP address of where user was

And, lastly, File System Driver products do have the innate ability to block undesirable file actions, but we have not found any such commercial products that offer this functionality.

## CPTRAX TECHNICAL BRIEF



### Choice: CPTRAX for Windows

Unique among Windows File System Auditing products, CPTRAX provides an integrated approach that fully connects with the server's communications channels. This allows CPTRAX to record all details regarding file system activity.

Benefited by kernel-level development design experience stretching back to the late 1980's and all versions of Windows since, CPTRAX offers a better choice for Windows File System Auditing. With CPTRAX you will receive reports that include:

- File/Folder name
- Event Type
- Account (user) and Domain name plus Distinguished Name
- Account SID
- Time of Event
- Permissions changed with full change details
- Owner changed and new owner identity
- For remote events, name of workstation where user was
- For remote events, IP address of where user was
- For remote events, Share name access was initiated upon
- For terminal server sessions, remote workstation where user was
- For terminal server sessions, IP address of where user was

And, unlike any other commercial Windows File System Auditing product, CPTRAX offers active blocking of undesirable create, delete and modification activity.

Additionally, the deep level of experience and expertise provided by the Visual Click Software Team gives you the power of CPTRAX without requiring any superfluous technologies on your servers such as the .NET framework, SQL Server, specific MSI Installer versions or any other add-on.

Contact us today to schedule your customized free online demonstration of CPTRAX.

[sales@visualclick.com](mailto:sales@visualclick.com)

Toll-free: (877) 902-5425  
Direct dial: (512) 330-0542

<http://www.visualclick.com/content/cptraxw.htm>