FSE and FSE-Lite

Product Profile

Software and Computer Systems Company, LLC

What are FSE and FSE-Lite?

FSE and FSE-Lite are file system event monitors. FSE-Lite is included with all base releases of Scannerz (SCSC's hard drive scanning and troubleshooting tool) to assist a user in determining if system slow downs that appear to be drive related may in fact be caused by the operating system or applications running on the operating system, usually in the background. FSE is a much more sophisticated version of FSE-Lite. FSE is much more flexible and can be used to help developers, system administrators, and security administrators isolate problems within a system. FSE is available as a stand-alone product or bundled with Scannerz, whereas FSE-Lite is only included with Scannerz and cannot be obtained in as a stand-alone package.

What's a File System Events Monitor?

All versions of MacOS® since OS X Version 10.4 (Tiger) have a process running named ***fseventsd***. This process is called a ***daemon process***, and runs in the background, unknown to the user. Whenever a change of some type occurs to a file or directory, fseventsd makes note of the change, and broadcasts it to listening clients. Both FSE and FSE-Lite are clients of fseventsd, meaning they can receive information from the daemon and process it. Much information can be obtained about a system by monitoring the daemon. ***Both FSE and FSE-Lite must be run with administrative privileges.***

Why is FSE-Lite, and Optionally FSE Included in Scannerz?

Scannerz is a hard drive scanning tool, which looks not only for existing problems in a system, but also emerging problems. Emerging problems typically start with what Scannerz identifies as an “irregularity,” meaning the measurements and tests Scannerz performs during a test take an abnormally long period of time to complete. This is often a “signature” of a problem in the process of developing. Unfortunately, excessive file activity, particularly from background processes the user doesn't even know are running, can lead a user to believe that their hard drive or system is having problems when in fact it's actually running normally.

FSE and FSE-Lite both expose unusually high file system activity because during such time, fseventsd is usually broadcasting so many messages they can't even be manually monitored using the displays provided in both products. It is not uncommon on some systems for some file system events to be produced with throughputs higher than 10,000 events per minute. Using the logging feature of both products, the user can observe the events taking place and then, if needed, trace back the source of the problem.

Whats the Difference Between FSE and FSE-Lite?

FSE-Lite was developed exclusively for use with Scannerz as a troubleshooting tool. FSE is an outgrowth of FSE-Lite and has numerous enhancements. With both FSE and FSE-Lite, the tools can be used help identify performance problems and (hopefully) trace them back to the source of the problems. This however, is where the similarities end.

The chief strength of FSE is it's use of filtering fseventsd output via user created profiles. FSE supports two modes of operation, *Default Mode* and *Profile Mode*, whereas FSE-Lite supports only *Default Mode*. In *Default Mode*, both products display and optionally log all events coming from the fseventsd daemon. In *Profile Mode*, however, FSE displays and optionally logs only those items identified in the profile. This allows FSE to target and log specific events, as opposed to everything.

Both FSE and FSE-Lite present data about file system events to the user in the following format:

```
File Mode Changed: /private/var/db/shadow/hash/DB3D019E-2AB4-11D8-8D27.......
Modifying Program: DirectoryService      Process ID: 11
Process Owner: System Admin     User ID: 0
Time recorded: 20:08:18, Fri. Mar.  9, 2012

File ownership changed: /private/var/db/shadow/hash/DB3D019E-2AB4-11D8.......
Modifying Program: DirectoryService      Process ID: 11
Process Owner: System Admin     User ID: 0
Time recorded: 20:08:18, Fri. Mar.  9, 2012

File Modified: /private/var/db/shadow/hash/DB3D019E-2AB4-11D8-8D27...........
Modifying Program: DirectoryService      Process ID: 11
Process Owner: System Admin     User ID: 0
Time recorded: 20:08:18, Fri. Mar.  9, 2012

File Modified: /private/var/run/utmpx
Modifying Program: sshd      Process ID: 989
Process Owner: System Admin     User ID: 0
Time recorded: 20:08:18, Fri. Mar.  9, 2012
```

NOTE: The records in the first two listing have their names truncated with a sequence of “.....” to fit on the page.

Each record of a file systems event as presented by FSE and FSE-Lite consists of four lines followed by a new line. The first line indicates the operation performed on the file followed by the name of the file. The second line identifies the name of the application that performed the work and its process ID. The next line identifies the owner of the process and the UID of that user. The last line is the time fseventsd recorded the event. If the process that performed the operation terminated shortly after it completed it's task, the modifying program may be identified as “Process Completed”.

The previous set of records illustrate the files that get modified when a remote login is performed on a system. In this particular case, this was done using FSE with a profile created to deliberately target such events. Without filtering, if another file intensive application capable of produce several hundred records per minute (such as Safari®) was also running, these records would be interspersed among the set of records and the user would need to go through log files to find them. FSE-Lite would list everything as just described, whereas FSE would show only those events the user wishes to have displayed. FSE can thus be used to not only monitor events in general, but it can also be used to monitor the occurrence of specific events.

Both FSE and FSE-Lite list incoming events on their graphical user interface displays, but due to the potentially high speed of incoming events, the number of events showing on a display at a given instance is limited. The user should rely on the products abilities to activate and deactivate logging of events to a log file for analysis. The displays used by both FSE and FSE-Lite are extremely high speed and allow data to keep up with the number of incoming events without losing any data from fseventsd. All logs generated by FSE-Lite are assigned the name FSE.log and stored in the users *Documents* directory. FSE allows the user the ability to rename the log file to fit the situation at hand.

Because FSE can be configured to target specific events, it can be useful for many things, including the following things:

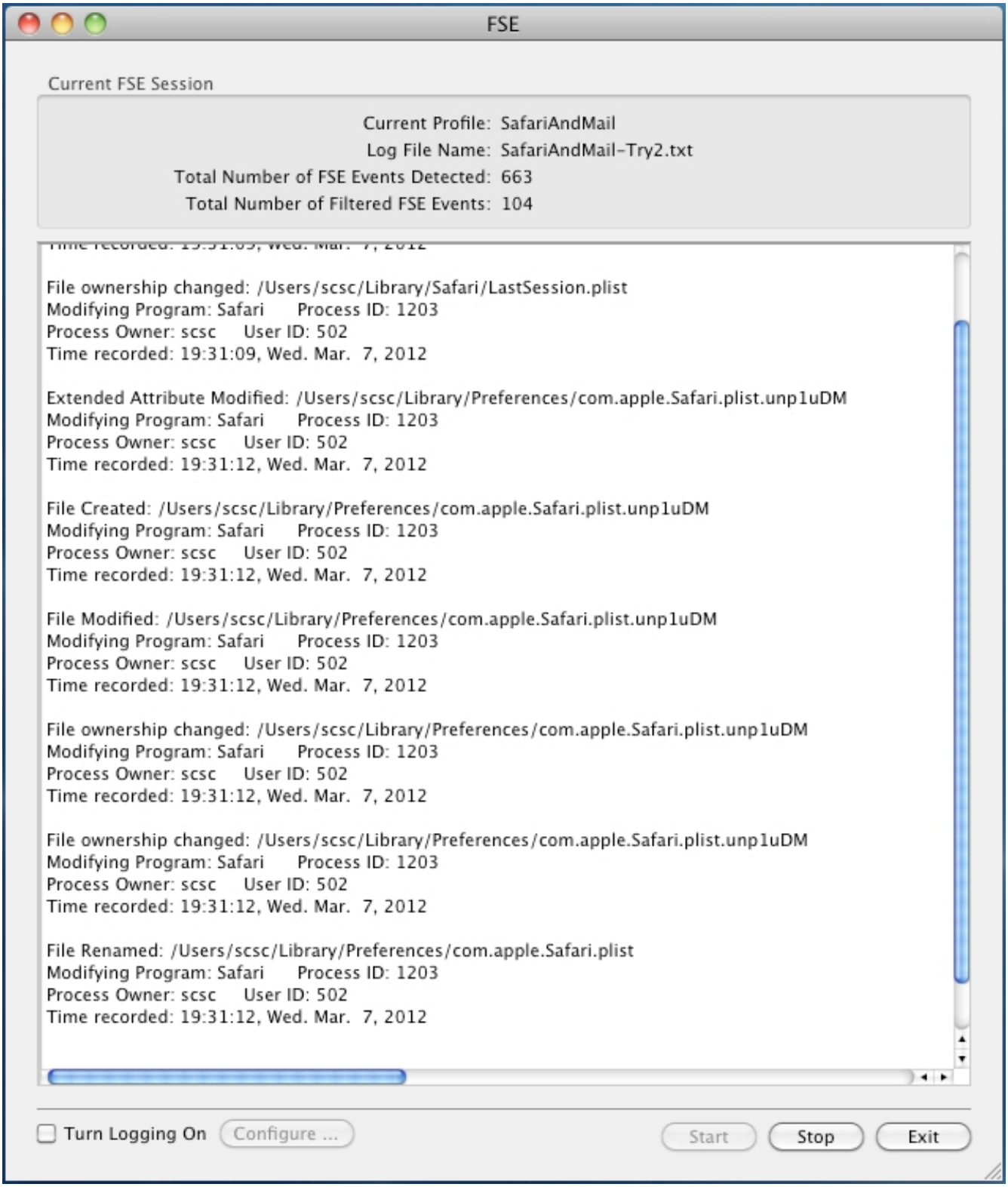
- Determining if a particular process or application has become excessively active with respect to drive I/O.
- Assist in identifying and monitoring unauthorized access to a system.
- Monitoring system or application crashes.
- Recording installation activities for some applications.
- Identifying unwanted or unauthorized processes or programs that are launching programs in the background without the users consent or knowledge.
- Identifying processes or applications that may be recording user data without their knowledge.
- Identifying when certain applications are launched and in some cases, terminated.
- Assist in identifying system slow downs.
- Assist in determining when background processes launch and how often.
- Identifying the applications a user is using.
- Understanding how some applications work.
- Tracking the creation and deletion of files by applications and users

The following table identifies the differences between FSE-Lite and FSE with regard to their capabilities:

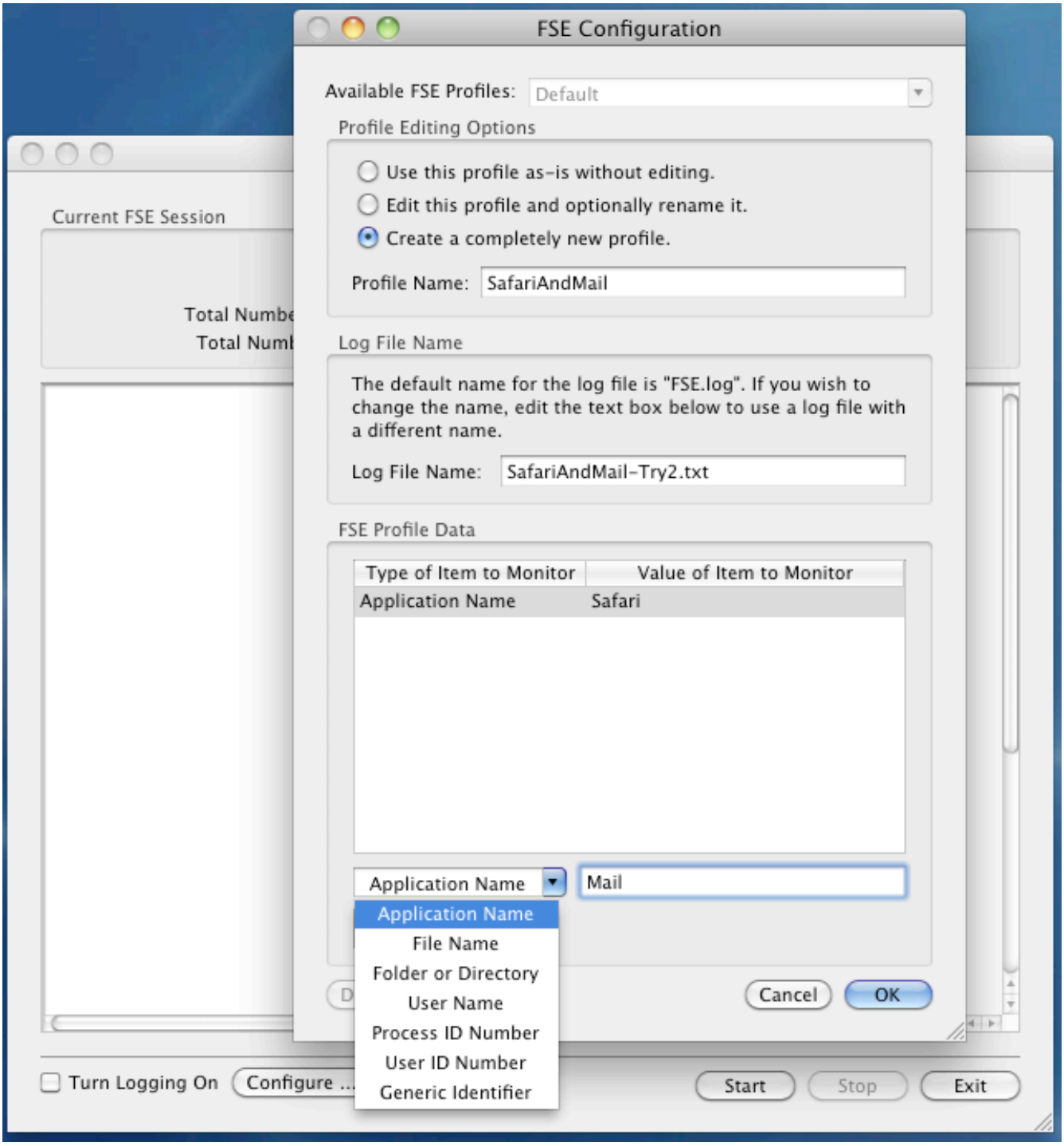
Capability	FSE-Lite	FSE
User can enable/disable communications with fseventsd	●	●
User can enable/disable logging at will.	●	●
Detects creation of a file	●	●
Detects creation of a directory or folder	●	●
Detects deletion of a file or directory	●	●
Detects modification of a files contents	●	●
Detects permission changes to a file or directory	●	●
Detects ownership changes to a file or directory	●	●
Detects attribute changes to a file or directory	●	●
Detects the renaming of a file or directory	●	●
Detects data exchange between files	●	●
Capable of filtering events by application name		●
Capable of filtering events by process ID number		●
Capable of filtering events by user name		●
Capable of filtering events by user ID number		●
Capable of filtering events by file name		●
Capable of filtering events by folder or directory name		●
Capable of filtering events using generic identifiers		●
Allows creating and editing of profiles to filter specific events		●
Allows user to rename log file		●
Maintains count of received and filtered events		●
High speed display area	●	●
Available as a stand-alone product		●

A Comparison of FSE and FSE-Lite Capabilities

The images on the following pages illustrate what the FSE graphical user interface and configuration menus look like. FSE-Lite is similar, but it does not have the ability to configure profiles or log names, it does not have a profile information box at the top (since profiles don't exist on FSE-Lite) and it does not have the ability to scroll the display area.



In this screen capture, FSE is using a profile named SafariAndMail to monitor the applications Safari and Mail. It has a custom log file named SafariAndMail-Try2.txt, and although the fseventsd daemon has sent 663 events total, this profile has filtered out only those associated with Safari and Mail, which has an event count of 104. Logging is currently deactivated.



The screen shot above illustrates a profile being created that will monitor file activity associated with Safari and Mail. The name of the profile is “SafariAndMail.” A new log file name is being assigned as “SafariAndMail-try2.txt.” An entry to monitor the application Safari has already been entered into the profile, and the user is about to add the Mail application. This profile will monitor all file modification activity performed by these applications. **This configuration menu and the ability to configure profiles does not exist with FSE-Lite.**

Who Should Use FSE and FSE-Lite?

FSE-Lite is provided as a convenience tool at no cost in the Scannerz package. If Scannerz, which is supposed to be run when a system is in a reasonably quiescent state, detects a large number of timing irregularities, it indicates that something is wrong with the system or there are drive intensive background processes running the user is unaware of. FSE-Lite is provided to allow the user to monitor general file system activity, and if it's brought up and the “display goes wild showing file activity” it indicates there are, indeed, background processes running the user is unaware of. For those familiar with the more advanced details of the operating system, Scannerz disables spotlight activity while it's running, thus a problematic application would likely have to have been installed with the user unaware of it.

FSE can perform all the tasks of FSE-Lite, but because of its ability to use profiles it can be used for much, much more. Unfortunately, however, it requires a fair amount of skill and a reasonably advanced understanding of the operating system to take advantage of FSE's benefits. ***FSE is not a tool for the novice or casual, non-technical user of a Mac.*** An individual that will likely be able to use FSE to its fullest advantage should be at least reasonably familiar with the following:

1. **Process ID number**
2. **User ID number**
3. **root user/super user**
4. **Familiarity with navigating the operating system by command line.**
5. **File ownership, permissions, and attributes**
6. **System monitors such as *Activity Monitor* and *top***
7. **System background processes**

Both FSE and FSE-Lite require administrative access levels to run.

Contact Information

If you have more questions, please visit our web site at:

http://www.scsc-online.com

For specific questions about the product, feel free to drop us a line at the following e-mail addresses:

Sales: sales@scsc-online.com
Support: support@scsc-online.com

Thank you for your interest in FSE and FSE-Lite.

Legal Information