Windows Logger

A Windows application that monitors application usage

[Preliminary Administrators Guide]

Michael A. Todd

7/25/2015

This Users Guide is intended for either personal usage by individuals or for administrator usage in corporate environments. It details the theory and operation of the Windows Logger application.

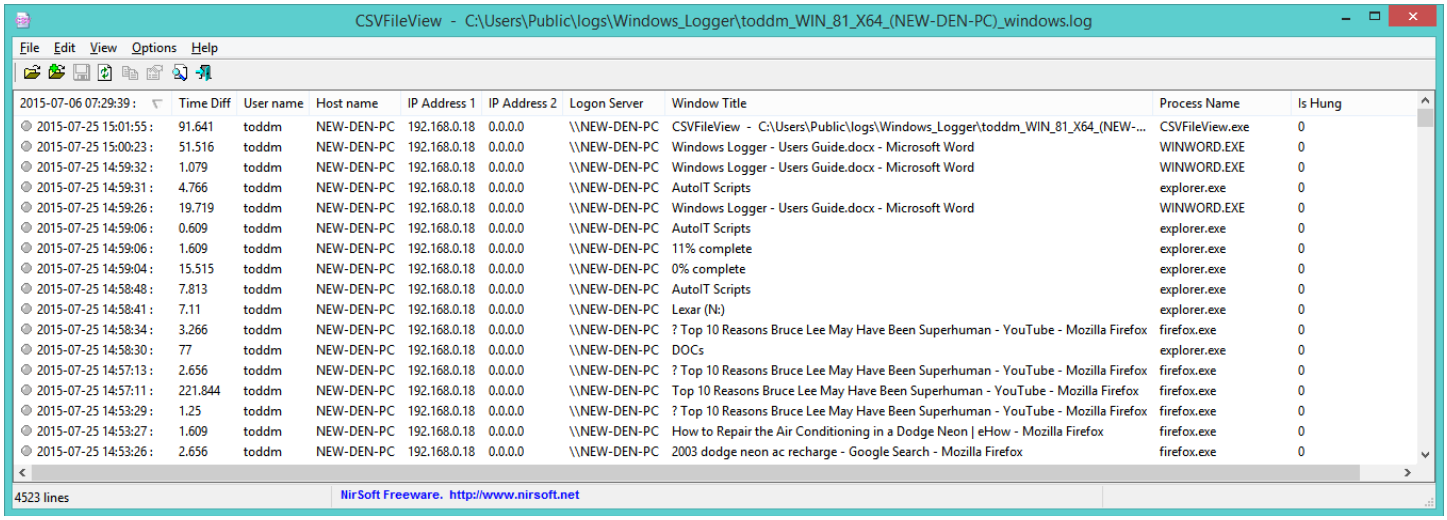
Contents

Purpose:

The purpose of Windows Logger is to scan all visible windows and log every time a user moves from one application to another. The application adds entries into LOG files which are either on users hard drives or on network shares. When run locally, the default folder for LOG files is C:\Temp. On a network, an Administrator determines the default folder location. Email alerts can also be configured.

Sample Log file:

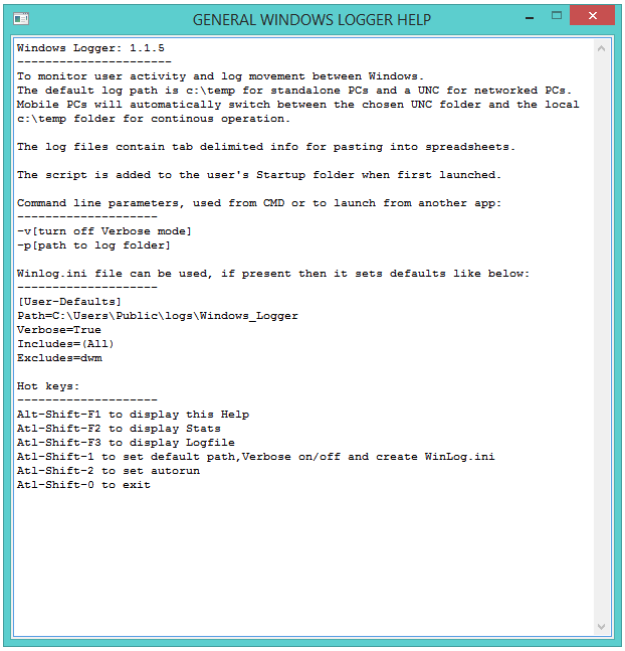
A sample of LOG file output is below. In addition to the date/time and the Window Title, the associated process and other information is logged. The naming convention for the LOG files is Username_OS-Version_32/64bit_(PC name)_process.log.



2015-07-06 07:29:39 :	Time Diff	User name	Host name	IP Address 1	IP Address 2	Logon Server	Window Title	Process Name	Is Hung
2015-07-25 15:01:55 :	91.641	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	CSVFileView - C:\Users\Public\logs\Windows_Logger\toddm_WIN_81_X64_(NEW-...	CSVFileView.exe	0
2015-07-25 15:00:23 :	51.516	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Windows Logger - Users Guide.docx - Microsoft Word	WINWORD.EXE	0
2015-07-25 14:59:32 :	1.079	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Windows Logger - Users Guide.docx - Microsoft Word	WINWORD.EXE	0
2015-07-25 14:59:31 :	4.766	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	AutoIT Scripts	explorer.exe	0
2015-07-25 14:59:26 :	19.719	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Windows Logger - Users Guide.docx - Microsoft Word	WINWORD.EXE	0
2015-07-25 14:59:06 :	0.609	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	AutoIT Scripts	explorer.exe	0
2015-07-25 14:59:06 :	1.609	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	11% complete	explorer.exe	0
2015-07-25 14:59:04 :	15.515	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	0% complete	explorer.exe	0
2015-07-25 14:58:48 :	7.813	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	AutoIT Scripts	explorer.exe	0
2015-07-25 14:58:41 :	7.11	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Lexar (N:)	explorer.exe	0
2015-07-25 14:58:34 :	3.266	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	? Top 10 Reasons Bruce Lee May Have Been Superhuman - YouTube - Mozilla Firefox	firefox.exe	0
2015-07-25 14:58:30 :	77	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	DOCs	explorer.exe	0
2015-07-25 14:57:13 :	2.656	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	? Top 10 Reasons Bruce Lee May Have Been Superhuman - YouTube - Mozilla Firefox	firefox.exe	0
2015-07-25 14:57:11 :	221.844	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Top 10 Reasons Bruce Lee May Have Been Superhuman - YouTube - Mozilla Firefox	firefox.exe	0
2015-07-25 14:53:29 :	1.25	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	? Top 10 Reasons Bruce Lee May Have Been Superhuman - YouTube - Mozilla Firefox	firefox.exe	0
2015-07-25 14:53:27 :	1.609	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	How to Repair the Air Conditioning in a Dodge Neon | eHow - Mozilla Firefox	firefox.exe	0
2015-07-25 14:53:26 :	2.656	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	2003 dodge neon ac recharge - Google Search - Mozilla Firefox	firefox.exe	0

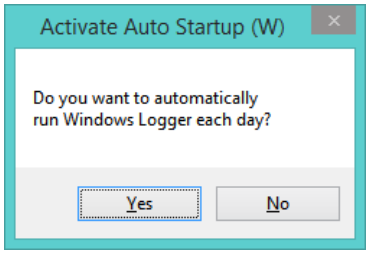
General Help Information (Alt-Shift-F1):

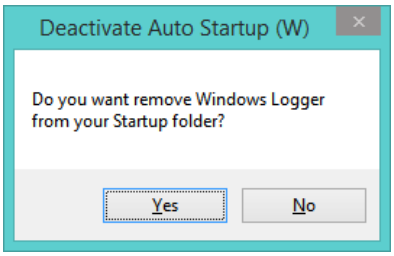
While the user does not need to interact with the program, there are various hotkeys that display information or allow various settings to be changed. Pressing Alt-Shift-F1 displays the Help screen below.



Auto start option (Alt-Shift-2):

When the program is first launched it creates a shortcut in the current user's Startup folder. This shortcut may be modified to specify both the LOG file folder and the delay time between Scans. The auto start option can be removed later via Alt-Shift-2 key combination. Depending on whether the shortcut is active will determine which option below is displayed.





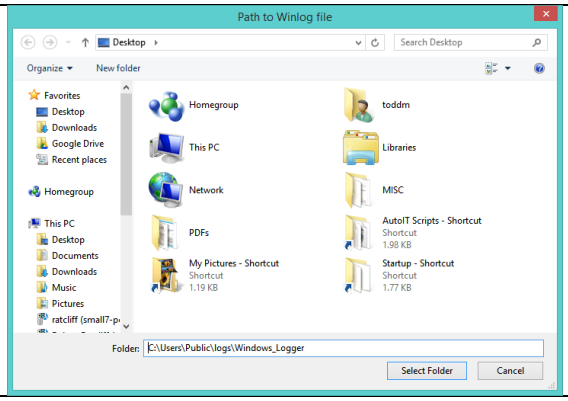
Internal default settings:

The program will set defaults to Verbose title logging and use the c:\temp folder to store LOG files when off a network. While connected to a network (i.e. not IP 192.168.x.x), the program will use the compiled network share folder (UNC format).

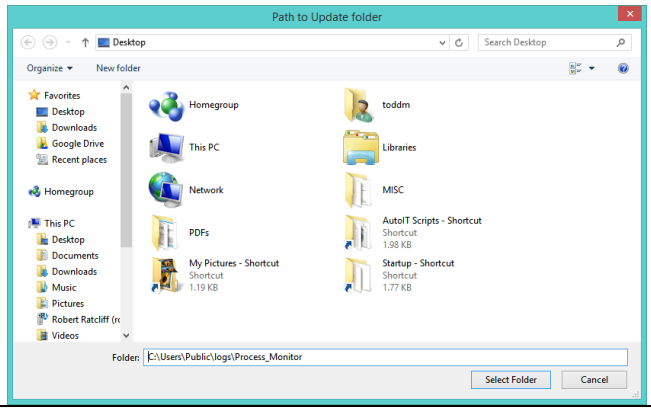
Local settings file – winlog.ini (Alt-Shift-1):

If the user or an administrator wishes to change the default LOG folder and other settings, pressing Alt-Shift-1 displays the following series of prompts. The settings file prcmon.ini will be created in order to save this information and will override the built-in default settings.

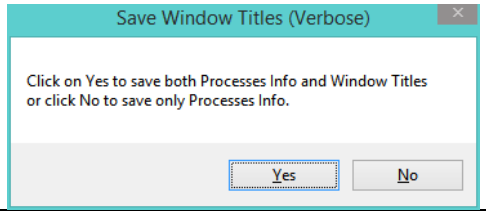
Path to the LOG file folder =>
[example filename:
toddm_WIN_81_X64_(HOME-PC)_process.log]



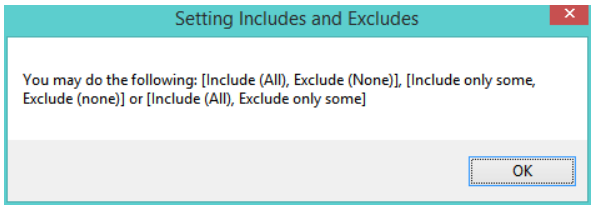
[Not Yet] Path to the Application Updater folder =>
(A newer version placed here will automatically update the version currently running on the user's computer.)



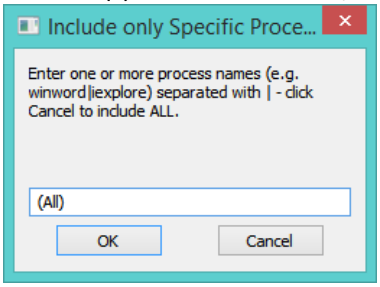
Save Window Titles =>
[Click Yes to save Titles for each logged process or click No to only save the process names.]



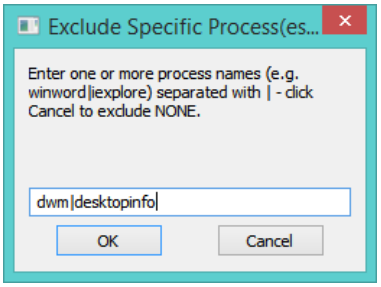
Setting Processes to Include or Exclude =>



[By default, (All) processes are included (i.e. (None) are excluded), but if you only wanted to watch one or more processes then enter their names in the Includes. If you have one or more processes that you need to be ignored then enter their name(s) into the Excludes, separated with vertical bars (|). You cannot use both at the same time.]

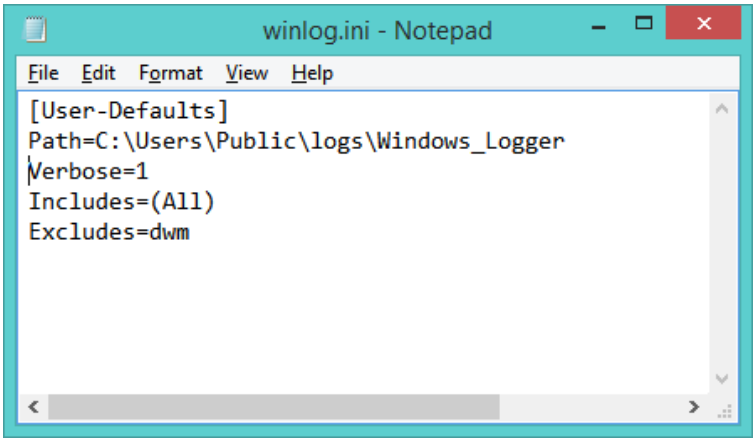


[All is the default; using iexplore, for example, would only log records for Internet Explorer.]



[Using (None) excludes nothing. Using dwm|desktopinfo excludes those two processes from being logged.]

After filling out all of this information, the file **winlog.ini** is created with the contents below. Any time this file is edited, either inside the program or with an outside editor, Windows Logger will update its running defaults automatically.



Once a winlog.ini file has been created, the program will defer to it for all settings. These values are also displayed in the General Help screen via Alt-Shift-F1.

[not yet] Global settings file for network users – global_winlog.ini:

For usage primarily on a network, a Global INI file may be created and placed into the Updater folder. It uses the same format as prcmon.ini and is called global_winlog.ini. The program will auto detect the global INI file and its values supersede both the internal and the winlow.ini settings. This global file enables an administrator to change settings in real time for a large group of computers that are running Windows Logger.

Off Network process logging:

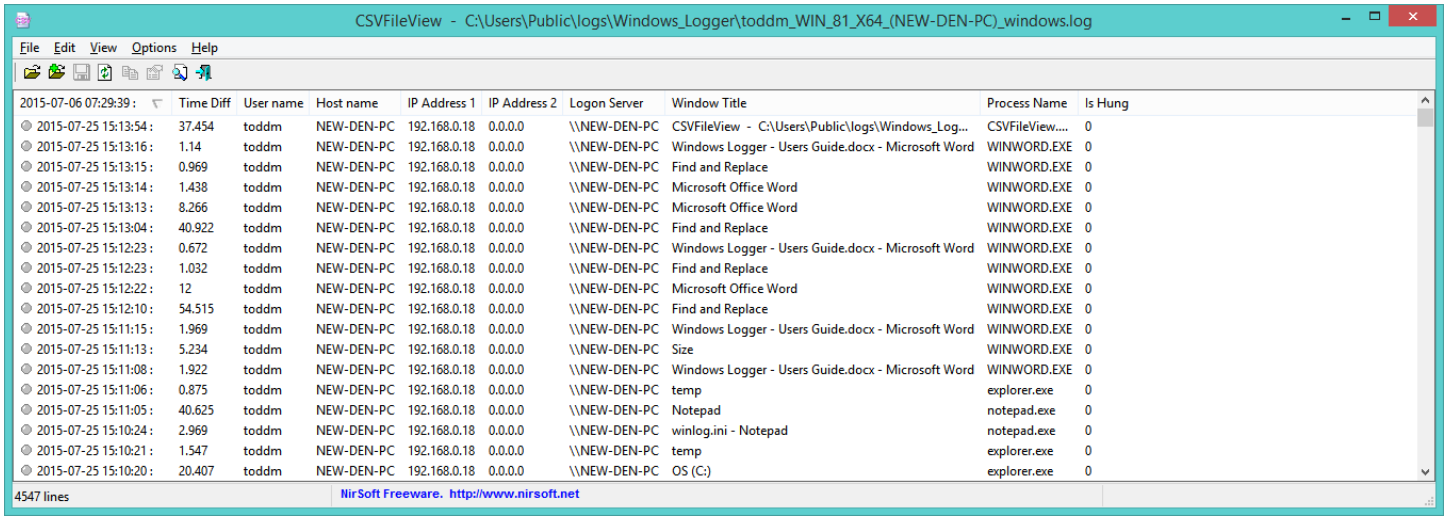
If the program detects it is running from a home network (i.e. not IP 10.x.x.x) then it will keep logging information into the c:\temp folder. Once the computer is back on our network, it will switch back to the network share folder and continue logging.

[not yet] Automatic program updates:

When a newer version of Windows Logger.exe is found in the Source Path directory, it will be used to update the running copy in the c:\temp folder. Users will not notice when the update takes place. The update_winlog.exe program must be in the source path directory as it does the actual updating.

Viewing log files (Alt-Shift-F3):

Users may open the log file with a variety of programs since it is a tab-delimited text file. Importing into Excel allows a variety of statistics and charts to be created. For convenience, the free program CSVFileView (from www.Nirsoft.net) is packed into Windows Logger. When Alt-Shift-F3 is pressed CSVFileView is used to open and display the log file currently configured in the INI or Internal settings. You can sort and copy/paste data from this window to Excel.



2015-07-06 07:29:39 :	Time Diff	User name	Host name	IP Address 1	IP Address 2	Logon Server	Window Title	Process Name	Is Hung
2015-07-25 15:13:54 :	37.454	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	CSVFileView - C:\Users\Public\logs\Windows_Log...	CSVFileView....	0
2015-07-25 15:13:16 :	1.14	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Windows Logger - Users Guide.docx - Microsoft Word	WINWORD.EXE	0
2015-07-25 15:13:15 :	0.969	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Find and Replace	WINWORD.EXE	0
2015-07-25 15:13:14 :	1.438	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Microsoft Office Word	WINWORD.EXE	0
2015-07-25 15:13:13 :	8.266	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Microsoft Office Word	WINWORD.EXE	0
2015-07-25 15:13:04 :	40.922	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Find and Replace	WINWORD.EXE	0
2015-07-25 15:12:23 :	0.672	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Windows Logger - Users Guide.docx - Microsoft Word	WINWORD.EXE	0
2015-07-25 15:12:23 :	1.032	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Find and Replace	WINWORD.EXE	0
2015-07-25 15:12:22 :	12	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Microsoft Office Word	WINWORD.EXE	0
2015-07-25 15:12:10 :	54.515	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Find and Replace	WINWORD.EXE	0
2015-07-25 15:11:15 :	1.969	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Windows Logger - Users Guide.docx - Microsoft Word	WINWORD.EXE	0
2015-07-25 15:11:13 :	5.234	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Size	WINWORD.EXE	0
2015-07-25 15:11:08 :	1.922	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Windows Logger - Users Guide.docx - Microsoft Word	WINWORD.EXE	0
2015-07-25 15:11:06 :	0.875	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	temp	explorer.exe	0
2015-07-25 15:11:05 :	40.625	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Notepad	notepad.exe	0
2015-07-25 15:10:24 :	2.969	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	winlog.ini - Notepad	notepad.exe	0
2015-07-25 15:10:21 :	1.547	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	temp	explorer.exe	0
2015-07-25 15:10:20 :	20.407	toddm	NEW-DEN-PC	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	OS (C:)	explorer.exe	0

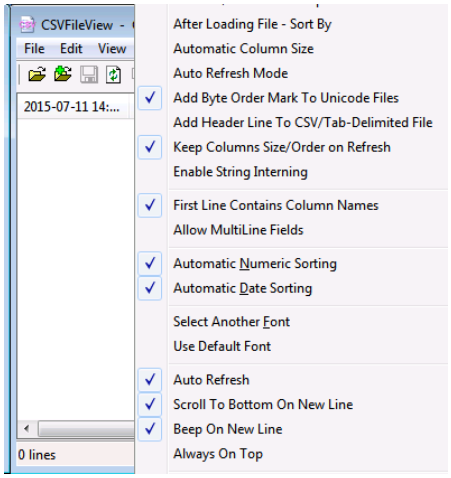
Installing Windows Logger:

Users may open the ZIP file and copy the Windows Logger.exe to any folder. The Temp folder on C drive is recommended as a starting point. You can later move the executable file somewhere less conspicuous. You can modify the INI file Alt-Shift-2 to include a different path for the LOG file as shown previously. The program installs into the user's Startup folder automatically.

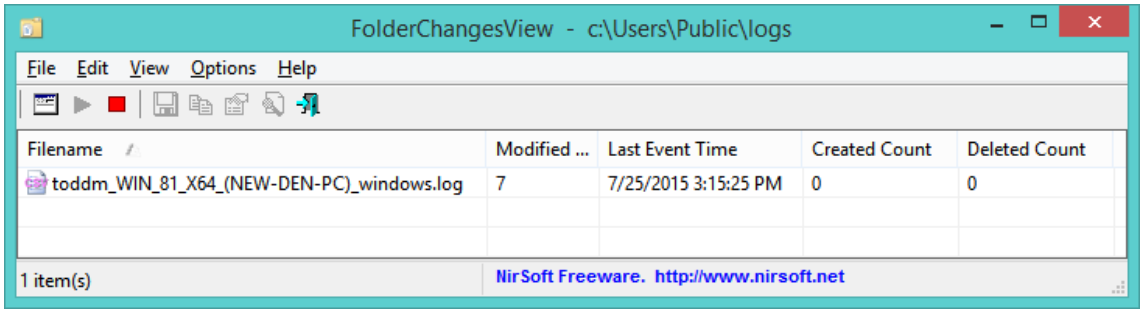
Additional resources:

If you want to get visual notification of log file updates you can do any of the following:

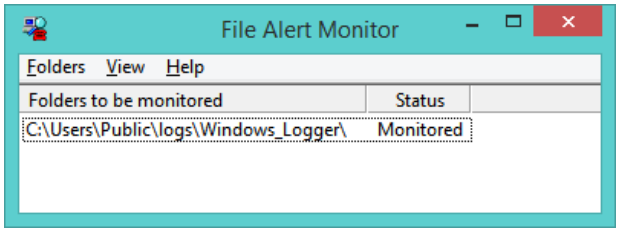
1. In CSVFileView, with the log file opened, click on Auto Refresh and Beep on New Line under Options, then just minimize the viewer and let it run.

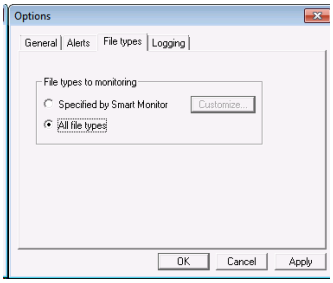


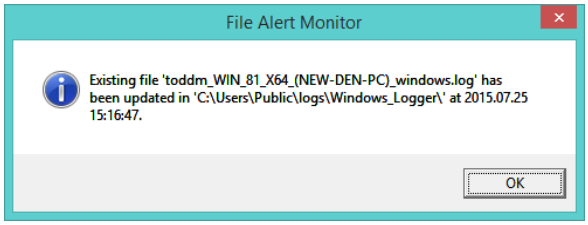
2. Download the free folder change monitor, FolderChangesView.exe, from the www.Nirsoft.net website. They also makes the CSVFileView application. FolderChangesView can monitor a main folder and its subfolders and will display any files that are being added, changed or deleted.



3. For an application that will display a popup window in the middle of your monitor, try File Alert Monitor, which is available from http://www.libertyrecording.com/download/FileMon20.exe. When you run the application, simply add the folder(s) you want to monitor and under Options set File types to All. Now the program will pop up a window whenever a file is changed.







Email interface:

An email interface can be constructed in several ways. Currently, I am using File Alert Monitor (FAM) along with an AutoIT script called Email Alert. Whenever a window is displayed by FAM, its contents are copied by Email Alert, the window is closed and an email is sent to an Administrator. Currently, emails may be sent through SMTP or through a user's Outlook client which has to be installed and running. The content of email is below.

> **Subject:** (S) Windows Logger Alert for toddm1
>
> Existing file 'toddm1_WIN_7_X86_(PBDB22E)_windows.log' has been updated in 'c:\temp\Windows_Logger' at 2015.07.11 14:10:42.

A future version will probably have email alerts built in and won't need Email Alert or FAM.

Exiting the Windows Logger (Alt-Shift-0):

If you want to stop the program from running without having to display Task Manager you may press Alt-Shift-0 (zero) and it will be stopped.