Process Monitor

A Windows application that monitors misbehaving processes

[Preliminary Administrators Guide]

Michael A. Todd

7/11/2015

Contents

Purpose:

The purpose of Process Monitor is to scan all visible windows and look for hung or misbehaving processes that are associated with those windows. The Windows function used is IsHungAppWindow. The default time between scans is 20 seconds. 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.

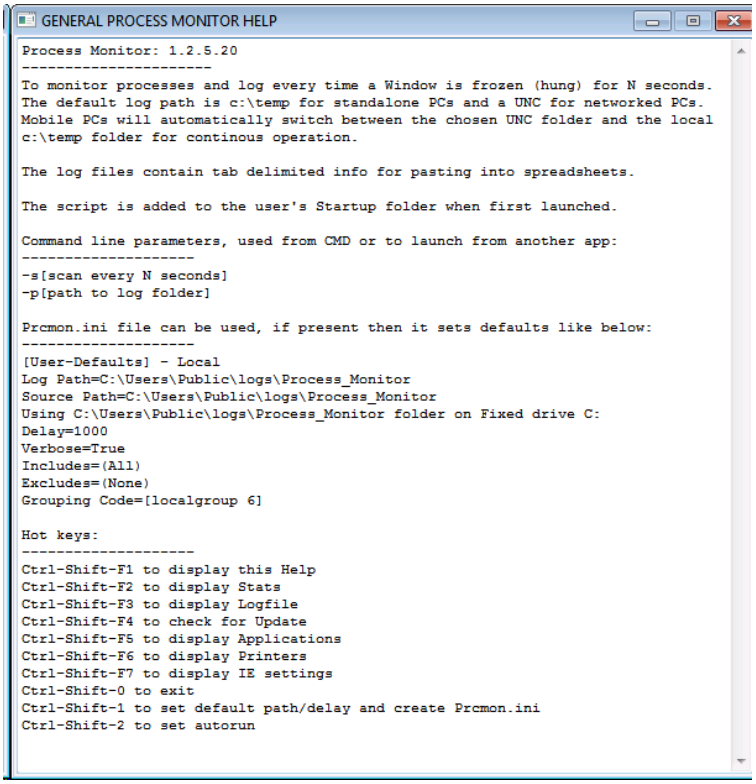
Sample Log file:

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.

2015-07-09 13:27:16 :	User name	Host name	Group Code	IP Address 1	IP Address 2	Logon Server	Window ...	Process Name	Process RAM (...	System Free R...	Scan Speed (sec)
2015-07-11 09:07:29 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	TreeDBN...	TreeDBNotes.exe	16.30	84	2
2015-07-11 09:07:31 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	frmStartup	theword.exe	27.38	83	2
2015-07-11 09:07:31 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	theWord	theword.exe	27.38	83	2
2015-07-11 09:07:31 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	TreeDBN...	TreeDBNotes.exe	16.39	83	2
2015-07-11 09:07:31 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	TreeDBN...	TreeDBNotes.exe	16.39	83	2
2015-07-11 09:07:33 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Adobe Ph...	PhotoshopElementsEditor.exe	55.91	82	2
2015-07-11 09:07:34 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	TreeDBN...	TreeDBNotes.exe	16.41	82	2
2015-07-11 09:07:34 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	TreeDBN...	TreeDBNotes.exe	16.41	82	2
2015-07-11 09:07:36 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	frmStartup	theword.exe	43.11	82	2
2015-07-11 09:07:36 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	theWord	theword.exe	43.16	82	2
2015-07-11 09:07:36 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	TreeDBN...	TreeDBNotes.exe	19.04	82	2
2015-07-11 09:07:36 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	TreeDBN...	TreeDBNotes.exe	19.04	82	2
2015-07-11 09:07:39 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	theWord	theword.exe	45.51	82	2
2015-07-11 09:07:39 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Adobe Ph...	PhotoshopElementsEditor.exe	76.14	82	2
2015-07-11 09:07:41 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Adobe Ph...	PhotoshopElementsEditor.exe	76.17	82	2
2015-07-11 09:07:43 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Adobe Ph...	PhotoshopElementsEditor.exe	77.47	82	2
2015-07-11 09:07:45 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Adobe Ph...	PhotoshopElementsEditor.exe	86.54	81	2
2015-07-11 09:08:03 :	toddm	NEW-DEN-PC	[local-PlainYogurt]	192.168.0.18	0.0.0.0	\\NEW-DEN-PC	Logos Bib...	Logos.exe	195.99	79	2

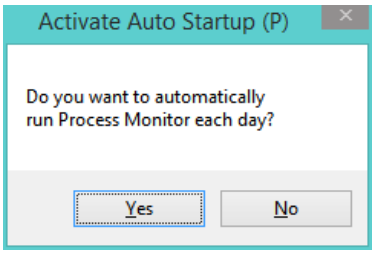
General Help Information (Ctrl-Shift-F1):

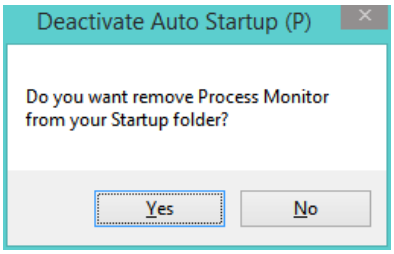
While the user does not need to interact with the program, there are various hotkeys that display information or allow various settings to be changed. Pressing Ctrl-Shift-F1 displays the Help screen below.



Auto start option (Ctrl-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 Ctrl-Shift-2 key combination. Depending on whether the shortcut is active will determine which option below is displayed.





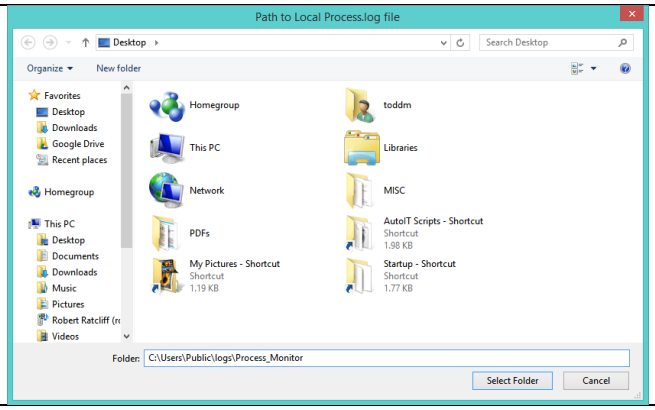
Internal default settings:

The program will set defaults to 20 second delay 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).

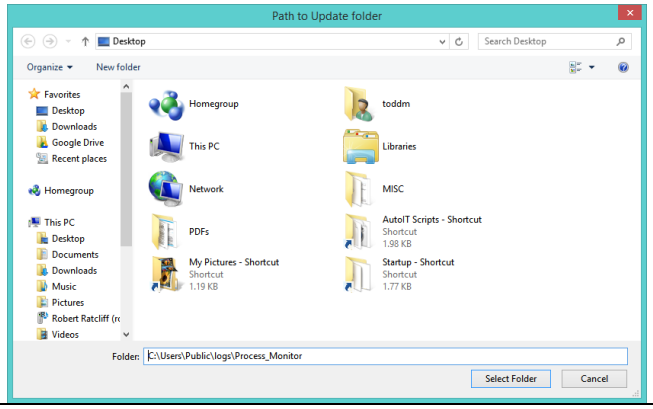
Local settings file – prcmon.ini (Ctrl-Shift-1):

If the user or an administrator wishes to change the default LOG folder and other settings, pressing Ctrl-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.

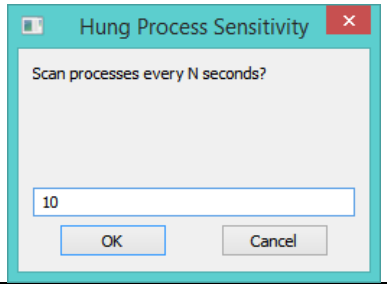
Path to the LOG file folder =>
[example filename:
toddm_WIN_81_X64_(HOME-PC)_process.log]



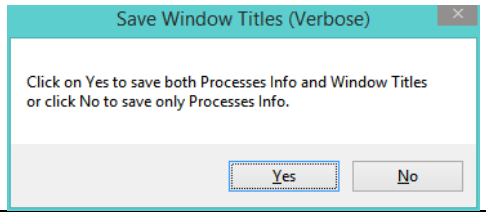
Path to the Application Updater folder =>
(A newer version placed here will automatically update the version currently running on the user's computer.)



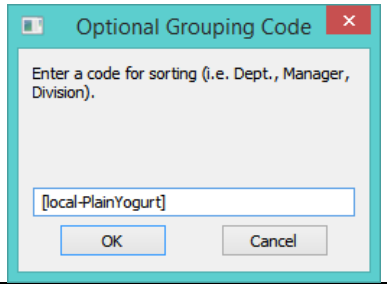
Scan running processes every N seconds =>
[This setting determines the delay time between the scan of open Windows. 10 seconds is a good minimum as smaller values will generate unrealistic output.]



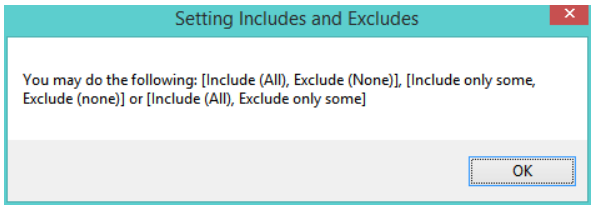
Save Window Titles =>
[Click Yes to save Titles for each logged process or click No to only save the process names.]



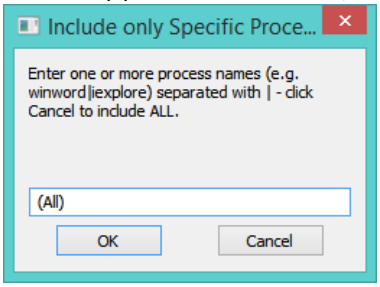
Optional Grouping Code =>
[Within the INI file a grouping code may be saved and it will be output to the LOG file. This can be the type of PC, a Dept. code, Manager / Supervisor name, etc. for the purpose of sorting / filtering logs.]



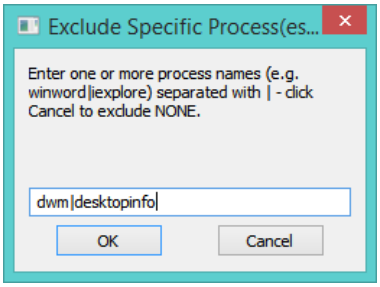
Setting Processes to Include or Exclude =>



[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.]

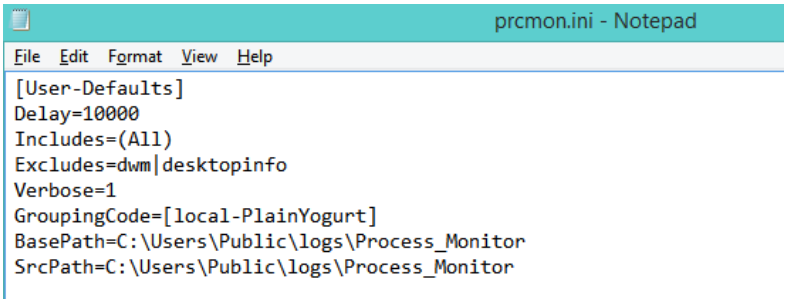


[All is the default; using iexplore, for example, would only log records for Internet Explorer.]



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

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



Once a prcmoni.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 Ctrl-Shift-F1.

Global settings file for network users – global_prcmon.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_prcmon.ini. The program will auto detect the global INI file and its values supersede both the internal and the prcmon.ini settings. This global file enables an administrator to change settings in real time for a large group of computers that are running Process Monitor.

Off Network process logging:

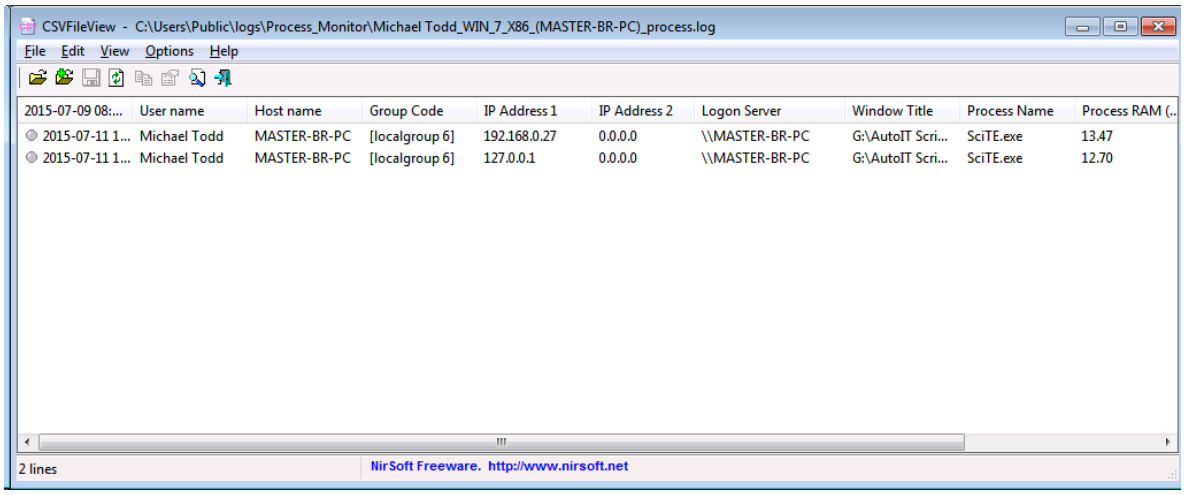
If the program detects it is running from a home network (i.e. not IP 10.x.x.x) then it will keep logging information into the c:\temp folder. Once the computer is back on our network, it will switch back to the network share folder and continue logging.

Automatic program updates:

When a newer version of Process Monitor.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_prcmon.exe program must be in the source path directory as it does the actual updating.

Viewing log files (Ctrl-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 Process Monitor. When Ctrl-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.



Setting the scan delay time:

While 20 seconds is a good starting value for the time between processes scanning, 30 seconds or more would indicate processes that are hung or not responding for a noticeable period of time. If you are seeing closely timed, repetitive entries then increase the delay time. If you are seeing applications which are logged when you are not even working at your computer, these may be entered as exclusions to keep the log file entries cleaner.

If you rarely see processes being logged on your computer system, that's good. You can always set the delay time to 1 or 2 seconds then restart your system. You should find several entries logged by the time you are back to your Desktop folder.

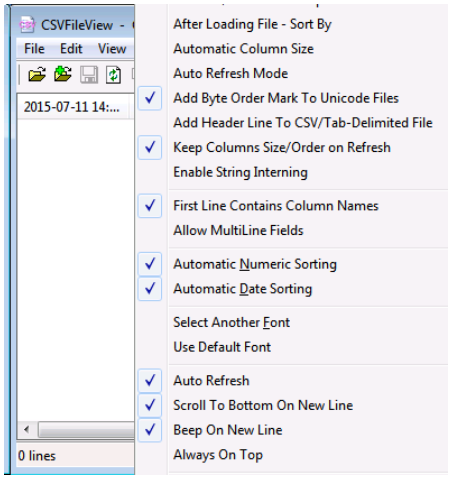
Installing Process Monitor:

Users may open the ZIP file and copy the Process Monitor.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 Ctrl-Shift-2 to include a different path for the LOG file as shown previously. The program installs into the user's Startup folder automatically.

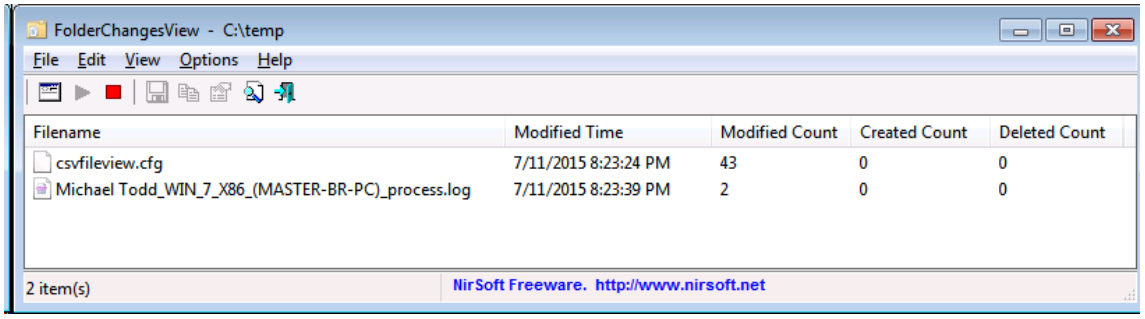
Additional resources:

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

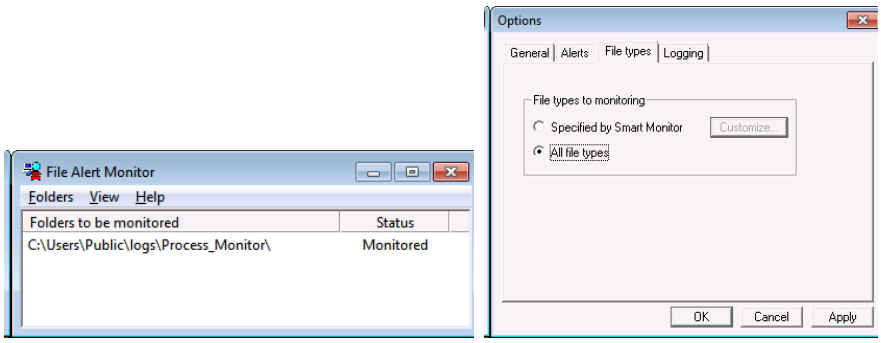
1. In CSVFileView, with the log file opened, click on Auto Refresh and Beep on New Line under Options, then just minimize the viewer and let it run.



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 our SMTP, relay.hrc.corp or through a user's Outlook client which has to be installed and running. The content of email is below.

> **Subject:** (S) Process Monitor Alert for toddm1
>
> Existing file 'toddm1_WIN_7_X86_(PBDB22E)_process.log' has been updated in '\\hrc.corp\dfschs\CHS-data\All Charleston\prclogs\Process_Monitor' 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 Process Monitor (Ctrl-Shift-0):

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