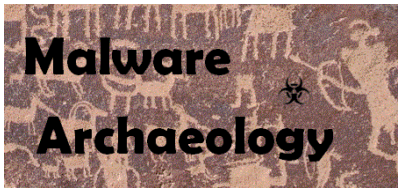
WINDOWS FILE AUDITING CHEAT SHEET - Win 7/Win 2008 or later

This "**Windows File Auditing Cheat Sheet**" is intended to help you get started with basic and necessary File and Folder Auditing. This cheat sheet includes some very common items that should have auditing enabled, configured, gathered and harvested for any Log Management, Information Security program or other security log gathering solution. Start with these settings and add to the list as you understand better what is in your logs and what you need to monitor and alert on.



WHY AUDIT FILES AND FOLDERS:

Files are often added or changed by hackers and malware. By auditing key file and folder locations, any additions or changes made by an attacker can be captured in the logs, harvested by a log management solution and potentially alerted on or gathered during an investigation.

Building a base configuration for file and folder auditing provides you a great starting point to build upon. As you mature your logging program, you can build upon and develop it as you find new locations that are important to monitor. We recommend as a part of any Information Security program that you implement and practice "***Malware Management***". You can read more on what "***Malware Management***" is and how to begin doing in here:

- ***www.MalwareManagementFramework.com***

The basic idea of Malware Management is, as you find file and folder locations reported in an incident response firm's malware analysis, virus/malware reports and your own incidents and investigations, you can expand on the base auditing listed in this cheat sheet and make it more mature and applicable to your specific needs or requirements.

RESOURCES: Places to get more information

1. ***MalwareArchaeology.com/cheat-sheets*** - More Windows cheat sheets and scripts to assist in your audit settings.
2. ***Log-MD.com*** – The ***Log Malicious Discovery*** tool reads security related log events and settings. Use ***Log-MD*** to audit your log settings compared to the "***Windows Logging Cheat Sheet***" and Center for Internet Security (CIS) to help with configuring your audit policy and refine file and registry auditing. List Event ID 4663 to see what files and folders might be noise and can be removed from your audit policy.
3. technet.microsoft.com – Information on Windows auditing
4. https://msdn.microsoft.com/en-us/library/bb742512.aspx - Using Security Templates to set audit policies
5. Google! – But of course.

WINDOWS FILE AUDITING CHEAT SHEET - Win 7/Win 2008 or later

ENABLE AND CONFIGURE:

1. FILE AUDITING: In order to collect file and folder auditing events (Event ID 4663) you must first apply the settings found in the "***Windows Logging Cheat Sheet***". These settings will allow a Windows based system to collect any events on files and folders that have auditing enabled.

CONFIGURE:

1. LOCAL LOG SIZE: Increase the maximum size of your local Security log. Proper auditing will increase log data beyond the default settings, your goal should be to keep local security logs for around 7 days.
   - Security log set to 1GB (1,000,000KB) or larger (yes this is huge compared to defaults)

INFORMATION:

1. EVENT ID: There is only one Event ID that will appear in the Security log when file and folder auditing is enabled, 4663.
   - 4663 - An attempt was made to access an object. This is the only Event ID that will record the details of the folder(s) and file(s) created as well as the process name that performed the actions.

REFINING AUDITING:

When using file and folder auditing, refinement will be needed in order to collect only the entries having actual security value. Enabling folders that have a high rate of changes will fill up your logs causing them to rotate faster than you might want to retain them and miss files you might actually want to catch. In addition, logging more than you need when using a log management solution will have a potential impact to licensing and storage requirements. It is important to test and refine file and folder auditing before applying it across your organization. Use ***Log-MD*** to assist you in refining your file and folder audit policy which can be found here:

- ***Log-MD.com***

If you are examining malware in a lab for example, or doing an incident response investigation, over auditing may be perfectly acceptable. Use the built-in Windows wevtutil.exe utility, PowerShell (get-eventlog), a security log tool like ***Log-MD*** or your log management solution to review what is being captured and remove files and folders that are excessively noisy and do not have significant security importance.

When setting auditing of files and folders there are some decisions on what to monitor. Using Explorer to select the folder and set the auditing manually, you can see what options there are as seen from the image below. The goal of this cheat sheet is to get you started using file and folder auditing on well-known folders and to enable just enough to provide security value, but not too much as to create a lot of useless noise. What follows is our recommendation to get started which you may tweak and improve as you need. The main goal is to look for things that are newly added by hackers and/or malware. Monitoring for all changes is rather noisy and excess noise could cause you to miss a simple file creation.

WINDOWS FILE AUDITING CHEAT SHEET - Win 7/Win 2008 or later

CONFIGURE:

These are the only items that are recommended be set to optimize what is needed security wise and keep noise to a minimum. You may expand on these settings as necessary for your environment, but these settings are a good place to start.

User:

- EVERYONE

Applies to:

- "***This folder, subfolders and files***" – Audit all items in this folder and all subfolders
  OR
- "***This folder and files***" - Audit only the files in this folder and NOT the subfolders

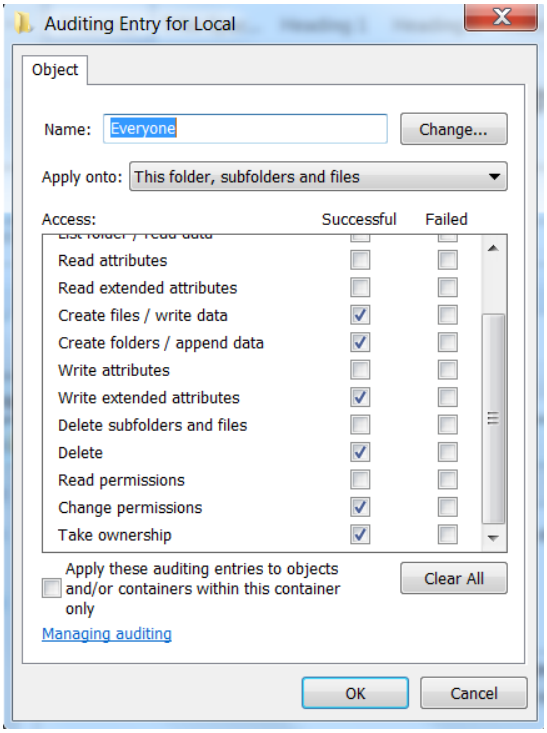
Access: Only select these items to keep down on the noise

- Create files / write data – File created
- Create folders / append data – Folder created
- Write extended attributes – Metadata that can be placed in a file
- Delete – File is deleted
- Change permissions – permissions of a file change
- Take ownership – ownership changed

CONFIGURE:

Select a Folder or file you want to audit and monitor. Right-Click the Folder, select Permissions – Advanced – Auditing – Add – EVERYONE – (check names), OK.

1. Apply onto – "***THIS FOLDER and FILES"*** or "***THIS FOLDER, SUBFOLDERS and FILES***" (or what you want/need).
2. Select '***Create files / write data***', '***Create folders / append data***', '***Write extended attributes***', '***Delete***', '***Change permissions***' & '***Take ownership***' to audit.
3. Be careful, setting auditing to '***This folder, subfolders and files***' as this can generate a lot of data and thus noise.



WINDOWS FILE AUDITING CHEAT SHEET - Win 7/Win 2008 or later

CONFIGURE: Recommend Folder and Files to enable auditing on

1. FOLDERS TO AUDIT:

THIS FOLDER AND FILES ONLY: Do ***NOT*** audit subfolders on these directories

- C:\Program Files
- C:\Program Files\Internet Explorer
- C:\Program Files\Common Files
- C:\Program Files (x86)
- C:\Program Files (x86) \Common Files
- C:\ProgramData
- C:\Windows
- C:\Windows\System32
- C:\Windows\System32\Drivers
- C:\Windows\System32\Drivers\etc
- C:\Windows\System32\Sysprep
- C:\Windows\System32\wbem
- C:\Windows\System32\WindowsPowerShell\v1.0
- C:\Windows\Web
- C:\Windows\SysWOW64
- C:\Windows\SysWOW64\Drivers
- C:\Windows\SysWOW64\wbem
- C:\Windows\SysWOW64\WindowsPowerShell\v1.0

THIS FOLDER, SUBFOLDERS AND FILES:

- C:\Boot
- C:\Perflogs
- Any Anti-Virus folder(s) used for quarantine, etc.
- C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Startup
- C:\Users\Public
- C:\Users*\AppData\Local
- C:\Users*\AppData\Local\Temp
- C:\Users*\AppData\LocalLow
- C:\Users*\AppData\Roaming
- C:\Windows\Scripts
- C:\Windows\System
- C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup — Consider Scripts if no other dirs
- C:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown
- C:\Windows\System32\GroupPolicy\User\Scripts\Logon — Consider Scripts if no other dirs
- C:\Windows\System32\GroupPolicy\User\Scripts\Logoff
- C:\Windows\System32\Repl — Servers only

WINDOWS FILE AUDITING CHEAT SHEET - Win 7/Win 2008 or later

CONFIGURE:

EXCLUDE NOISY ITEMS: These folders will create events that do not provide much value. After setting auditing on the parent folder, remove auditing from these folders and any other files and folders you find overly noisy with little security benefit.

- C:\ProgramData\Microsoft\RAC\Temp
- C:\ProgramData\Microsoft\RAC\PublishedData\RacWmiDatabase.sdf
- C:\ProgramData\Microsoft\RAC\StateData\RacDatabase.sdf
- C:\ProgramData\<Anti-Virus>\Common Framework Insert your AV folder(s)
- C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.chk
- C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.log
- C:\Users*\AppData\Local\GDIPFONTCACHEV1.DAT
- C:\Users*\AppData\Local\Google\Chrome\User Data
- C:\Users*\AppData\Local\Microsoft\Windows\Explorer\thumbcache_*
- C:\Users*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
- C:\Users*\AppData\Local\Microsoft\Office
- C:\Users*\AppData\Local\Microsoft\Outlook
- C:\Users*\AppData\Local\Microsoft\Windows\PowerShell\CommandAnalysis
- C:\Users*\AppData\Local\Mozilla\Firefox\Profiles
- C:\Users*\AppData\LocalLow\Microsoft\CryptnetUrlCache
- C:\Users*\AppData\Roaming\Microsoft\Excel
- C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache
- Any other normal applications that you have installed that produce a lot of log entries without significant security value.

OPTIONS TO SET FILE AUDITING:

There are four ways to set file and folder auditing on each folder:

1. Create a security template that is applied using Group Policy and/or secedit. This is the most effective way of doing it for a large amount of systems.
    a. https://msdn.microsoft.com/en-us/library/bb742512.aspx
2. Set with a PowerShell script. Though this method does not work on certain directories owned by TrustedInstaller and changing the ownership is not recommended
3. Set with a ***SetACL.exe***, a utility by ***www.helgeklein.com***
4. Set manually via Explorer. This does not scale as each system must be set manually, but may be fine for a malware lab or investigation of a single or a few systems.

PREFETCH FOLDER AUDITING:

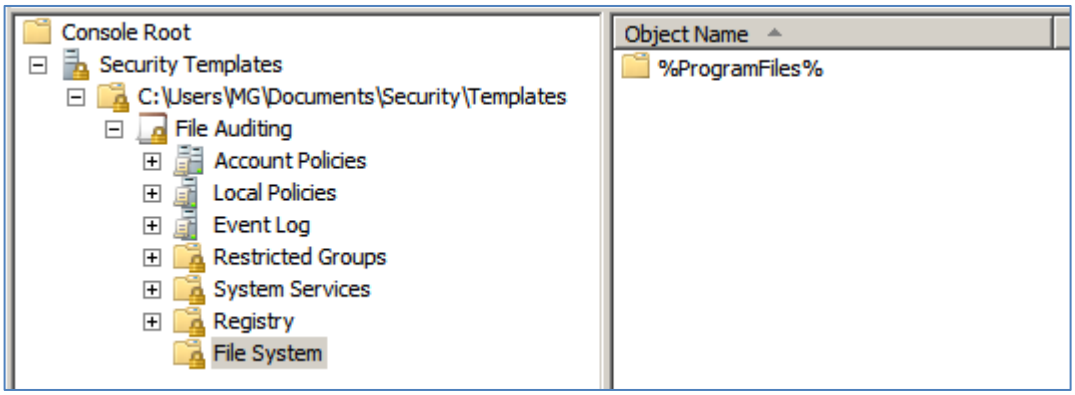
Auditing the Windows Prefetch or Superfetch folder is a good forensic addition since it will not generate very much log data. In Win 7 and later with systems with an SSD, it is disabled. Enabling on Servers is an option. Enable the "***Superfetch***" service on Workstations to Automatic and Start and enable the "***EnableSuperfetch***" key is set to "***3***".

- HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

USING SECURITY TEMPLATES TO SET AND REMOVE FILE AUDITING:

The following is how to create a Security template using the Microsoft Management Console (MMC). To create a custom security template using the MMC snap-in:

1. Open the MMC console, choose ***Start***, and then choose ***Run***
2. Type "***mmc***" in the Open box, and then choose ***OK***
3. From the ***File*** menu, choose ***Add/Remove Snap-in***
4. Select ***Add/Remove Snap-in*** dialog box, choose ***Add***
5. Select the list of available snap-ins, select ***Security Templates***, choose ***Add***, choose ***Close***, and then choose ***OK***
6. In the MMC main window, under the Console Root node, expand the Security Templates node, right-click the root templates folder, and then choose ***New Template***
7. Type a name and description for the template, and then choose ***OK***
8. Choosing ***OK*** saves your template as an .inf file in:
    - C:\Users\<username>\Documents\Security\Templates
    - Or you may save them anywhere you would like
9. Add each folder and/or file you want to audit with the appropriate audit settings listed above



SETTING AUDITING OF USER FOLDERS KEYS:

You can use a script stored on MalwareArchaeology.com to help you set the auditing for user folders mentioned in this cheat sheet. You may edit the list of folders in the cmd file provided to meet your needs.

1. You must be logged into the system as the user you want to set the registry auditing for:
    - ***Set_User_Folder_Auditing.cmd*** – Calls the PowerShell script to set auditing for specific folders listed in the cmd script
    - ***WARNING:*** Test this on other folders as there are some permissions that will cause issue if you try to use this with C:\Windows directories
    - The script is available at ***www.Malwarearchaeology.com/logging***