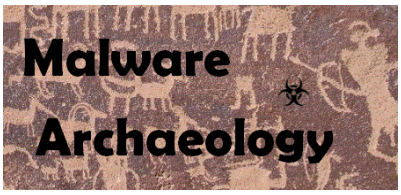
WINDOWS REGISTRY AUDITING CHEAT SHEET - Win 7/Win 2008 or later

This "**Windows Registry Auditing Cheat Sheet**" is intended to help you get started with basic and necessary Registry 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 THE REGISTRY

The registry is a database used by Windows to keep track configurations and settings. One of the types of settings found in the registry are places to auto launch applications like Windows services, startup applications and task bar items. These are referred to as "autorun" locations and are frequently used by attackers to load malware on system startup and should be audited. By auditing autorun registry locations, any attempt to maintain persistence by a hacker can be captured in the logs, harvested by a log management solution, or security logging tool and potentially alerted on or gathered during an investigation.

Building a base configuration for registry 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.MalwareManagement.com***

DEFINITIONS:

1. HKCU: The HKEY_Current_User keys are settings specific to a user and only apply to a specific or currently logged on user. Each user gets their own user key to store their unique settings.
2. HKU: The HKEY_Users keys are settings that apply to all user accounts. All HKCU keys are maintained under this key.
3. HKLM: The HKEY_Local_Machine keys are where settings for the machine or system that applies to everyone and everything are stored.
4. HKCR & HKCC: The HKEY_CLASSES_ROOT and HKEY_Current_Config keys are not used in this cheat sheet

RESOURCES: Places to get more information

1. ***MalwareArchaeology.com/cheat-sheets*** - More Windows cheat sheets and scripts to assist in your audit settings. PowerShell scripts that set, remove and check your auditing are available for download.
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***" to help with configuring your audit policy and refine registry and file auditing. List Event ID's 4663 and 4657 to see what keys might be noise and can be removed from your audit policy.
3. technet.microsoft.com – Information on Windows auditing.
4. Google! – But of course.

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

ENABLE AND CONFIGURE:

1. REGISTRY AUDITING: In order to collect registry auditing events (Event ID 4663 and 4657) 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 keys that have auditing enabled.

ENABLE:

2. 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's: There are two Event ID's that will appear in the Security log when registry auditing is enabled, 4663 and 4657
   a. 4663 - An attempt was made to access an object. This Event ID will not provide much security value for registry keys and can be filtered out of your log management solution for ONLY registry items (Task Category = Registry or Object Name = "\REGISTRY*"). This Event ID is needed for file auditing, so do not filter out for file and folder items.
   b. 4657 - A registry value was modified. This is the primary Event ID that you will want to focus your registry auditing investigations on as they contain the key, value, data added or changed and the process that made the change providing the details most needed for registry monitoring.

REFINING AUDITING:

When using registry auditing, refinement will be needed in order to collect only the entries having actual security value. Enabling keys that have a high rate of changes will fill up your logs causing them to rotate faster than you might want to retain them. In addition, logging more than you need when using a log management solution will have an impact to licensing and storage requirements. It is important to test and refine registry auditing before applying it across your organization. Use ***Log-MD*** to assist you in refining your registry 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 keys that are overly noisy and do not contain autorun items or have significant security importance.

When setting auditing of registry keys there are some decisions on what to monitor. Using Regdit.exe to select the key 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 registry auditing on well-known keys and autorun locations 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 key value creation.

WINDOWS REGISTRY 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 Key and subkeys***" – Audit all items in this key and all subkeys
  OR
- "***This Key only***" - Audit only the items in this key and NOT the subkeys

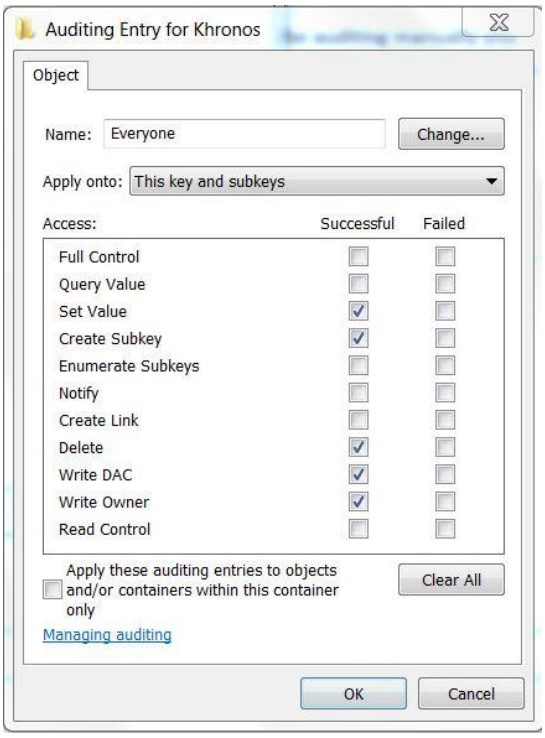
Access:

- Set Value – Registry value changes
- Create Subkey – A key is created
- Delete – A key is deleted
- Write DAC – The permissions change
  - Same as ***Change Permissions*** in the MMC
- Write Owner – The owner changes
  - Same as ***Change ownership*** in the MMC

CONFIGURE:

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

1. Apply onto – "***THIS KEY ONLY"*** or "***THIS KEY and SUBKEYS***" (or what you want/need).
2. Select '***Set Value***', '***Create Subkey***', '***Delete***', '***Write DAC***' & '***Write Owner***' to audit.
3. Be careful setting auditing to '***Keys and subkeys***' as this can generate a lot of data and thus noise.



Select	To audit
Query Value	Any attempts to read a entry from a registry key
Set Value	Any attempts to set entries in a registry key
Create Subkey	Any attempts to create subkeys on a selected registry key
Enumerate Subkeys	Any attempts to identify the subkeys of a registry key
Notify	Any notification events from a key in the registry
Create Link	Any attempts to create a symbolic link in a particular key
Delete	Any attempts to delete a registry object
Write DAC	Any attempts to write a discretionary access control list on the key
Write Owner	Any attempts to change the owner of the selected key
Read Control	Any attempts to open the discretionary access control list on a key

CONFIGURE:

1. KEYS TO AUDIT - HKU: Settings that apply ONLY to the default user when a ***new*** user is created.
2. ***Note:*** The Current User Key (HKCU) cannot be set using a security template due to needing the users SID, but you can set the auditing using a PowerShell script as the current logged on user run with administrator access.

THIS KEY ONLY: (none)

- USERS\.DEFAULT\Control Panel\Desktop
- HKCU\<SID>\Environment — Changes to the enviro variables
- HKCU\<SID>\Control Panel\Desktop
- HKCU\<SID>\Software\Microsoft\Windows NT\CurrentVersion\Accessibility

THIS KEY AND SUBKEYS: (containerinherit)

- USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
- USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\RunOnce
- USERS\.DEFAULT\Software\Microsoft\Office\Outlook\Addins
- USERS\.DEFAULT\Software\Microsoft\Office\PowerPoint\Addins
- USERS\.DEFAULT\Software\Microsoft\Office\Word\Addins
- USERS\.DEFAULT\Software\Microsoft\Internet Explorer\UrlSearchHooks

- HKCU\<SID>\Software \ALPS — ALPs Touchpad
- HKCU\<SID>\Software\Policies\Microsoft\Windows\System\Scripts — Logon/Logoff
- HKCU\<SID>\Software\Synaptics — Synaptics Touchpad
- HKCU\<SID>\Software \Microsoft\CTF
- HKCU\<SID>\Software \Microsoft\MultiMedia
- HKCU\<SID>\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\<SID>\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\<SID>\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached
- HKCU\<SID>\Software\Microsoft\Office\14.0\Word — 11.0,12.0,14.0,15.0
- HKCU\<SID>\Software\Microsoft\Office\Outlook\Addins
- HKCU\<SID>\Software\Microsoft\Office\PowerPoint\Addins
- HKCU\<SID>\Software\Microsoft\Office\Word\Addins
- HKCU\<SID>\Software\Microsoft\Office Test\ — if exists
- HKCU\<SID>\Software\Microsoft\Internet Explorer\UrlSearchHooks
- HKCU\<SID>\Software\Nico Mak Computing — WinZip
- HKCU\<SID>\Software\Classes\CLSID\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}
- HKCU\<SID>\Software\Classes\Wow6432Node\CLSID\{BCDE0395-E52F-467C-8E3D-C4579291692E}
- HKCU\<SID>\Software\Microsoft\Windows\CurrentVersion\Explorer
- HKCU\<SID>\Software\WinRAR — WinRAR

3. KEYS TO AUDIT - HKLM: Settings that apply to the entire system and all users

THIS KEY ONLY: (none)

- HKLM\Software\Microsoft\WBEM\CIMOM (noisy, but can detect WMI attacks)
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\ATs
- HKLM\System\CurrentControlSet\Control
- HKLM\System\CurrentControlSet\Control\Lsa
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SecurityProviders
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SecurityProviders\WDigest
- HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd
- HKLM\System\CurrentControlSet\Control\Terminal Server\AddIns Look for new addins

CONFIGURE:

THIS KEY AND ALL SUBKEYS: (containerinherit)

- HKLM\Software\Classes*\ShellEx
- HKLM\Software\Classes\AllFileSystemObjects\ShellEx
- HKLM\Software\Classes\Directory\ShellEx
- HKLM\Software\Classes\Folder\ShellEx
- HKLM\Software\Classes\Protocols\Filter
- HKLM\Software\Classes\Protocols\Handler
- HKLM\Software\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance
- HKLM\Software\Classes\Htmlfile\Shell\Open\Command
- HKLM\Software\Clients\Mail
- HKLM\Software\Microsoft\.NETFramework
- HKLM\Software\Microsoft\Active Setup\Installed Components
- HKLM\Software\Microsoft\Internet Explorer\Toolbar
- HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{SIP Guid} **NEW**
- HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData\{SIP Guid} **NEW**
- HKLM\Software\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{SIP Guid} **NEW**
- HKLM\Software\Microsoft\Office\Outlook\Addins
- HKLM\Software\Microsoft\Office\Excel\Addins
- HKLM\Software\Microsoft\Office\PowerPoint\Addins
- HKLM\Software\Microsoft\Office\Word\Addins
- HKLM\Software\Microsoft\Terminal Server Client
- HKLM\Software\Microsoft\VBA\Monitors
- HKLM\Software\Microsoft\WBEM\ESS Look for new providers
- HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers
- HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters
- HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers

CONFIGURE:

4. KEYS TO AUDIT - HKLM: continued

THIS KEY AND ALL SUBKEYS: (containerinherit)

- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects
- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\TBDEn
- HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit Audit Command Line log settings
- HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\AeDebug
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\SystemRestore
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options "Debugger" **New**
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\IconServiceLib
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows "Load" **New**
- HKLM\Software\Policies\Microsoft\Windows\System\Scripts Startup/Shutdown
- HKLM\Software\Policies\Microsoft\PowerShell Audit PowerShell log settings
- HKLM\System\CurrentControlSet\Control\SafeBoot
- HKLM\System\CurrentControlSet\Control\Session Manager\Environment
- HKLM\System\CurrentControlSet\Control\Print\Monitors
- HKLM\System\CurrentControlSet\Control\NetworkProvider\Order
- HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms
- HKLM\System\CurrentControlSet\Services
- HKLM\System\CurrentControlSet\services\NTDS
- HKLM\System\CurrentControlSet\Services\RemoteAccess
- HKLM\System\CurrentControlSet\Services\WinSock2
- HKLM\System\CurrentControlSet\Control\Session Manager
- HKLM\System\CurrentControlSet\Control\Print\Monitors
- HKLM\System\CurrentControlSet\Control\NetworkProvider\Order
- HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms

CONFIGURE:

4. KEYS TO AUDIT - HKLM: continued

THIS KEY AND ALL SUBKEYS: (containerinherit)

- HKLM\Software\Wow6432Node\Classes*\ShellEx
- HKLM\Software\Wow6432Node\Classes\AllFileSystemObjects\ShellEx
- HKLM\Software\Wow6432Node\Classes\Directory\ShellEx
- HKLM\Software\Wow6432Node\Classes\Folder\ShellEx
- HKLM\Software\Wow6432Node\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance
- HKLM\Software\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{SIP Guid} **NEW**
- HKLM\Software\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData\{SIP Guid} **NEW**
- HKLM\Software\ Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{SIP Guid} **NEW**
- HKLM\Software\Wow6432Node\Microsoft\.NETFramework
- HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components
- HKLM\Software\Wow6432Node\Microsoft\Office\Outlook\Addins
- HKLM\Software\Wow6432Node\Microsoft\Office\Excel\Addins
- HKLM\Software\Wow6432Node\Microsoft\Office\PowerPoint\Addins
- HKLM\Software\Wow6432Node\Microsoft\Office\Word\Addins
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
- HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\AeDebug
- HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
- HKLM\Software\ Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options "Debugger" **New**

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

- HKLM\SYSTEM\CurrentControlSet\services\Tcpip
- HKLM\SYSTEM\CurrentControlSet\services\VSS
- HKLM\SYSTEM\CurrentControlSet\services\Netlogon
- HKLM\SYSTEM\CurrentControlSet\services\BITS
- HKLM\SYSTEM\CurrentControlSet\services\WmiApRpl
- HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Epoch
- HKLM\SYSTEM\CurrentControlSet\services\Shared Access\Epoch2
- HKLM\SYSTEM\CurrentControlSet\services\rdyboost\Parameters
- Any other keys that produce a lot of log entries without significant security value.

MUICACHE: This key can provide some forensic details of things that execute on the system by user. Since it generates very little log data, it is a good addition to audit.

- HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache
- HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MUICache
- HKCR\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MUICache

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

OPTIONS TO SET REGISTRY AUDITING:

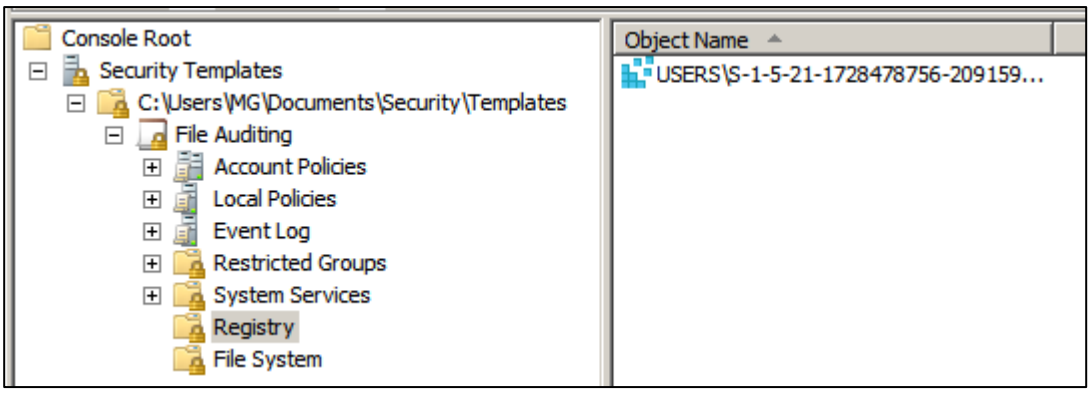
There are four ways to set file and folder auditing on each folder:

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 Regedit.exe. 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.

USING SECURITY TEMPLATES TO SET AND REMOVE REGISTRY 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 registry key you want to audit with the appropriate audit settings listed above



SETTING AUDITING OF USER REGISTRY KEYS:

You can use a script stored on MalwareArchaeology.com to help you set the auditing for registry keys mentioned in this cheat sheet. You may edit the list of keys in the PowerShell script provided to meet your needs. It is launched with the batch file also provided.

1. You must be logged into the system as the user you want to set the registry auditing for:
    - ***Set_User_Registry_Auditing.cmd*** – Calls the PowerShell script to set auditing for specific registry keys
    - It will set the auditing and produce 3 reports of the before, after and items not set
    - The script is available at ***www.Malwarearchaeology.com/logging***