

An Introduction to the Windows Registry

Ву

David Hartsock

www.davescomputertips.com

An Introduction to The Windows Registry

You have heard about it. You have been warned about the dangers of messing with it. What is it?

The purpose of this ebook is to remove some of the mystic and fear associated with the registry. Often times tweaks or fixes are published on the internet, which require editing the registry. If you decide to do these you will have a little knowledge about where you are, what the hive does, and what the instructions mean. As a Daves Computer Tips reader I know you will make a <u>backup</u> of your system before you do edit the registry (grin).

What is it?

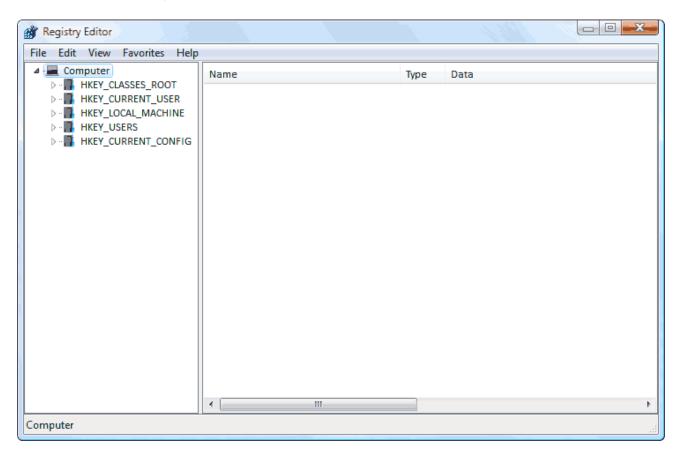
The Windows registry is a central database for the Windows operation system. Settings and information that control hardware configuration, operating system configuration, installed software configuration, and user preferences are all stored in the registry. If you make a change to a program setting, or something as simple as changing display settings, it is likely those changes are stored in the Windows registry. The registry is very important to Windows! Even with the dire warnings of gloom and doom when editing the registry aren't anything to be afraid of. In fact you interact with it daily, you just didn't know it.

With that said, the registry is full of thousands of entries. The chances of one tiny mistake bringing Windows to its knees is slim, but possible. It is always a good idea to have a current <u>disk image</u> before jumping into the registry.

Now that I've scared the pants off you feel free to follow along as I discuss the registry, just don't make any changes.

The Registry Structure

To view or edit the registry Windows includes a program called RegEdit. In Windows 2000 and XP click Start>Run and enter regedit.exe in the run box and then click OK. In Vista click Start and type "regedit" in the search box, at the bottom of the Start Menu, followed by the Enter key. The window below will open.



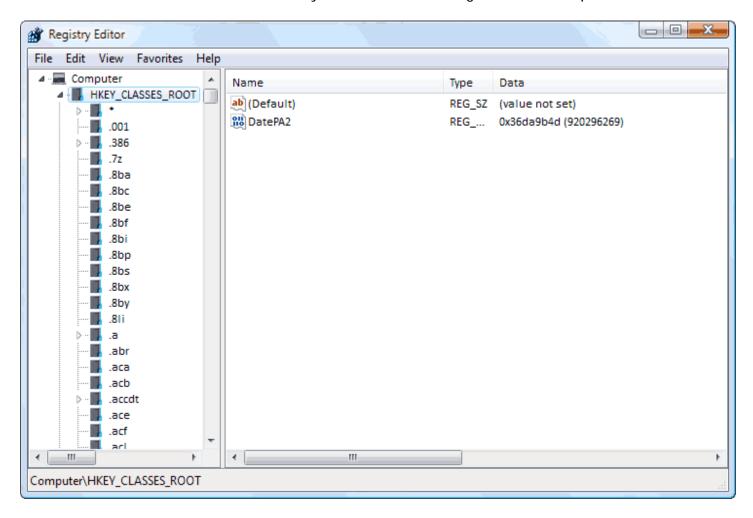
It's very apparent that all this HKEY stuff in the left hand column is gibberish. Computer refers to your computer and each entry under that is a specific section or hive. Let's take a look at each hive and see what it does.

- HKEY_CLASSES_ROOT storage for information about registered programs and file associations.
- HKEY_CURRENT_USER storage for settings specific to the current user. If your computer is set up with multiple user accounts this is where the settings for each user are kept.
- HKEY_LOCAL_MACHINE storage for settings that apply to all users of the computer.
- **HKEY_USERS** storage for subkeys which correspond to the HKEY_CURRENT_USER keys for each user account.
- HKEY_CURRENT CONFIG storage for keys generated during boot. This hive is actually created when the computer boots and is not stored on your hard drive.

The Windows registry is actually made up of several files named SAM, SOFTWARE, SECURITY, and SYSTEM (notice no file extension) located in the c:\windows\system32\config folder. There is also a file named NTUSER.DAT, which is located in c:\Documents and Settings\<your user name> for Windows XP and c:\Users\<your user name> for Windows Vista. These files relate to the above hives.

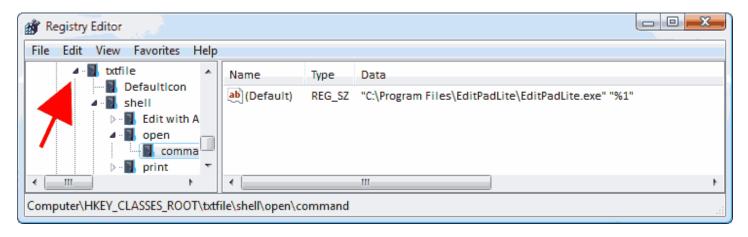
- NTUSER.DAT contains the HKEY_CURRENT_USER hive.
- SAM contains the HKEY_LOCAL_MACHINE\SAM hive.
- SECURITY contains the HKEY_LOCAL_MACHINE\SECURITY hive.
- SOFTWARE contains the HKEY_LOCAL_MACHINE\SOFTWARE hive.
- SYSTEM contains all other sub hives of THE HKEY_LOCAL_MACHINE hive.

We know where the files are and what they do. Let's go back to Regedit and look around. Click the arrow next to HKEY_CLASSES_ROOT and you will see something similar to the picture below.



These are all of the file extensions which have been registered on your computer. File extensions tell Windows which program to use for a specific file type.

Scroll down (a lot of scrolling) to txtfile. This is the entry responsible for how your computer handles text files.



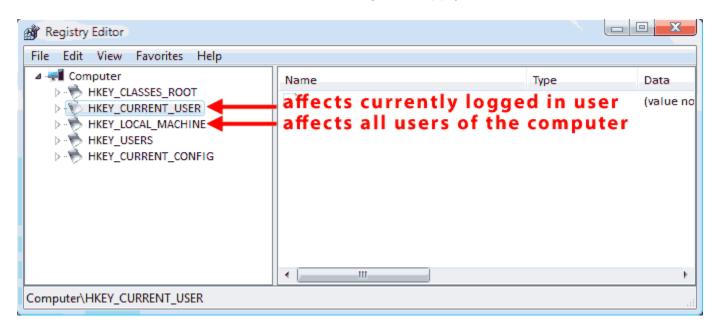
This is a screenshot of my registry. Yours will be similar, but different. Next to txtfile you will see another arrow. Clicking this arrow will expand the tree below the txtfile entry. Under shell you will see that I use a program named EditPad Lite to view and edit text files. Yours will most likely be notepad.exe.

You will notice the second column is labeled Type. Here is a list of common Types and what they represent:

- **REG_BINARY** The value will be in Binary format. Usually used for hardware component entries.
- REG_DWORD These values are commonly a "0" for a disabled option or a "1" for an enabled option.
- **REG_SZ** These values are stored in a readable format like the one above.

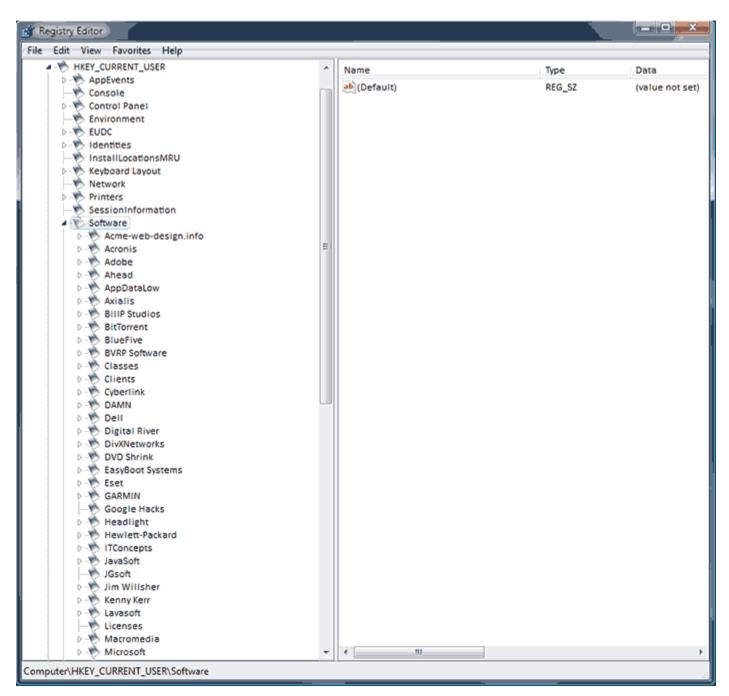
How software relates to the Windows Registry

We now know that the HKEY_CURRENT_USER hive stores settings for the currently logged on user and the HKEY_LOCAL_MACHINE hive stores settings that apply to all users.



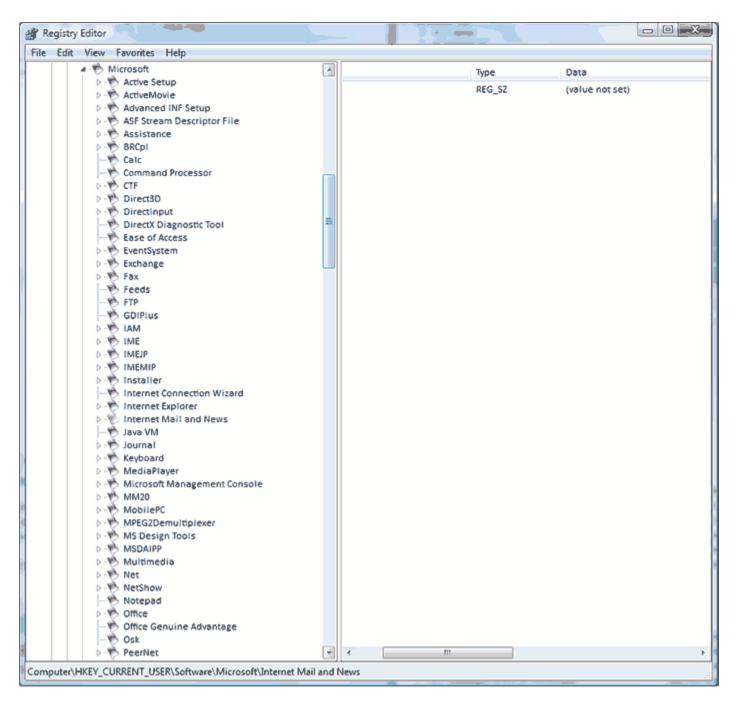
When you install software on your computer settings for that software are often times stored in the registry. This isn't the best solution because registry corruption can render programs useless. Another problem is that programs writing to the registry could possibly overwrite an important entry rendering the computer unbootable. Microsoft has tried to eliminate this in Vista by providing a specific directory (c:\program data) for software authors to store program settings and information.

Software is either installed for a specific user or for all users of the computer. It is a 50/50 change whether software will be installed for the current user, or all users, though some programs allow you to choose. Navigate by clicking the "+" or triangle beside each hive to HKEY_CURRENT_USER>SOFTWARE

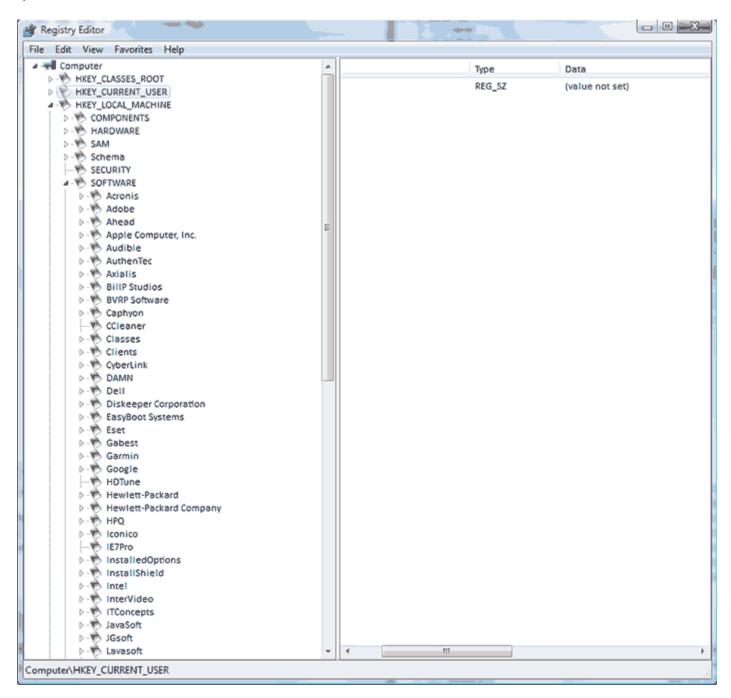


Here you will see quite a few of the programs you have installed on your computer. Each of the entries in this tree is a software author. If you have more than one program installed from the same author you will find entries for each under the software author's folder. Settings in this tree will be user specific.

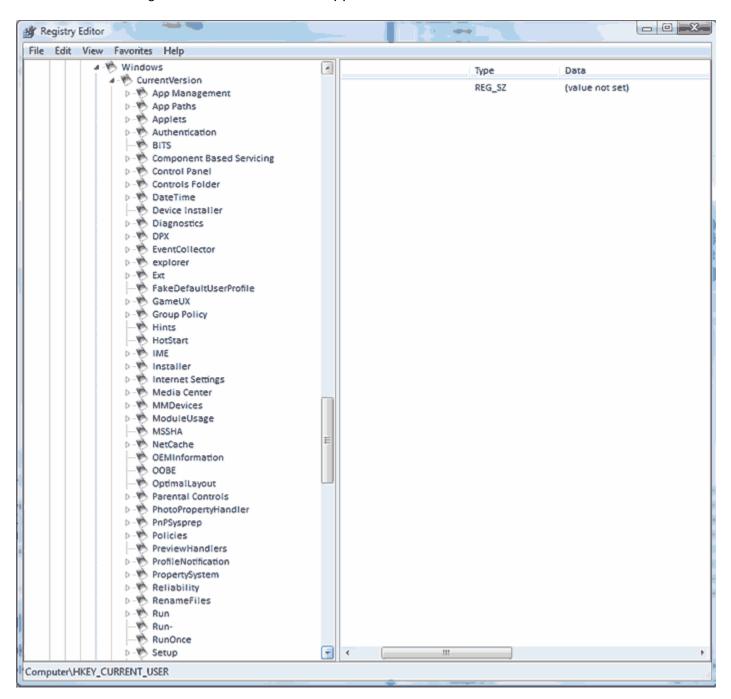
Scroll down to the Microsoft entry and expand (HKEY_CURRENT_USER>SOFTWARE>MICROSOFT). Very interesting to note that Microsoft lists most of the programs and features of the OS here. Windows itself is listed under the Microsoft folder. Feel free to have a look around.



Ok, Let's check out the HKEY_LOCAL_MACHINE hive. Click the "-" or tilted triangle next to all entries you have expanded to close them. Click the "+" or triangle next to HKEY_LOCAL_MACHINE to expand the tree and scroll down to software. You will notice there are many similar entries and quite a few that don't show in HKEY_CURRENT_USER.



Scroll down to Microsoft and expand the tree (HKEY_LOCAL_MACHINE>SOFTWARE>MICROSOFT). Scroll down again to Windows (HKEY_LOCAL_MACHINE>SOFTWARE>MICROSOFT>WINDOWS) and expand. CurrentVersion should be the first entry (HKEY_LOCAL_MACHINE>SOFTWARE>MICROSOFT>WINDOWS>CurrentVersion). Here is where you will find most settings that control Windows appearance and function.



Most entries are self explanatory. Control Panel contains settings for the Control Panel, Run contains settings that cause programs to run at startup, Uninstall will contain the uninstallation strings for most programs, etc. Have a look around. You will be surprised at what may look familiar. The next time you make a settings change you'll have a better idea of what is going on behind the scenes.

Last Known Good Configuration

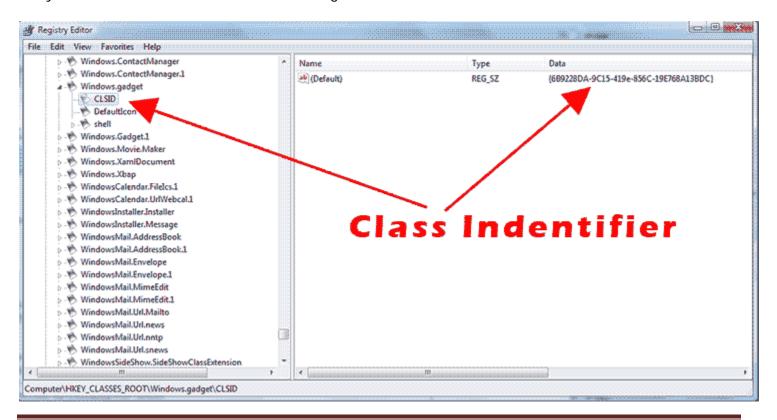
Have you ever had a windows error which caused a reboot? If you have you probably were presented with a black screen that offered several options (none of which seem like a good idea at the time). The screen offers several options: Safe Mode, Safe Mode with Networking, and Last Known Good Configuration.

Exactly what is Last Known Good Configuration? I'll tell you now it isn't a life saver, but it could come in handy. Each time your computer boots normally there is a backup made of the Hkey_Local_Machine\System\CurrentControlSet tree and its' sub keys. Choosing Last Known Good Configuration causes Windows to load that backup in place of the current registry file during boot. If the original problem was a registry issue that affected that tree and/or sub keys then you may be able to recover by choosing that option.

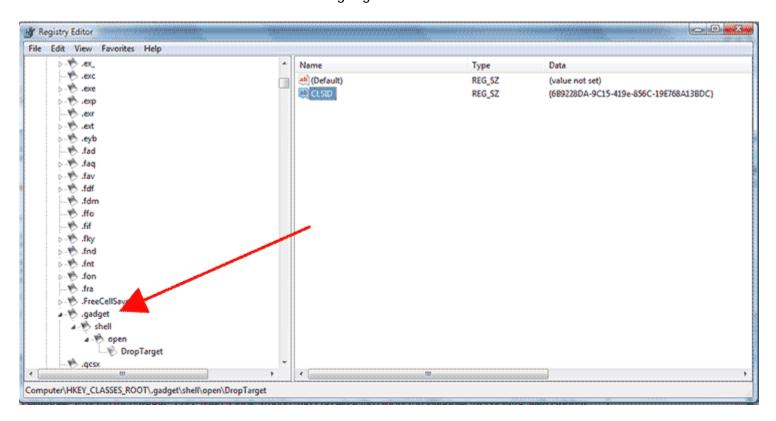
Generally I find that registry entries related to hardware affect this tree, so if you've made a hardware or driver change before the problem this may be a wise choice. If you haven't made any hardware or driver changes I would stay away. It is in no way a substitute for a good backup!

CLSID

There were a few readers who discovered entries labeled CLSID as they were exploring the registry. CLSID is short for Class Identifier or Global Unique Identifier (GUID). Here is an example of a CLSID - {6B9228DA-9C15-419e-856C-19E768A13BDC}. A long (128 bit) number that means nothing to you or I. In actuality it is a unique number which references an executable on your computer. Here is an example. The Vista Sidebar allows you to add Gadgets to your desktop. If we look in Hkey_Classes_Root we will see the following:



So we know the CLSID Windows is using for gadgets. Let's have a look around and see what file extension Windows associates with sidebar gadgets.



I know not everyone has Vista. This was just an example. Look around. Find an extension you are familiar with. Use Edit>Find to locate the associated program.

.reg files

You may run into files on the internet or through emails that have the file extension .reg. These files are meant to add, change, or delete entries from the registry in a way that is much simpler than explaining how to navigate to a specific key(s) and make a specific change(s).It is a simple text file created in a specific format. These files can run the gamut from innocent to evil. Be **VERY** careful if you are ever told to download or execute a file with this extension. Only do so if you are absolutely sure of the source, trust the source, and have a current backup. These can get you in a lot of trouble if you aren't careful!

Let's wrap it up

I hope you've learned a little about the Windows Registry Through this ebook. At least enough so you aren't scared when someone mentions the word "Registry"! I use a program named RegCool in place of the built in registry editor. I've grown to rely of this program. Unfortunately it wasn't compatible with Vista. Thankfully the author recently updated the program! Windows Regedit program provides search results one at a time. This can make removing left over software entries a very lengthy process. What I like about RegCool is it gives search results all at the same time allowing you to delete groups of keys simply. If you would like to try RegCool you can <u>find it here</u>.