

Copyright (c) 2006 Kenth Nasstrom.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License". Portions of the document like screenshots are from my local computer, some technical aspects fo the document comes from Microsoft knowledgebase, Microsoft Technical articles and independent answers to questions made in forums. Some text is written directly by me and any configuration or change in configuration in this text was made by me on my local computer.

Windows Registry Scan – Fix & Repair

www.RegistryTech.com

Registry Structure	4
HKEY_CLASSES_ROOT	5
HKEY_CURRENT_USER	5
HKEY_LOCAL_MACHINE	6
HKEY_USERS	6
HKEY_CURRENT_CONFIG	7
Editing the Registry	8
Manual editing	8
Command line editing	9
Where is the Registry stored?	10
Windows NT, 2000, 2003, & XP	10
Windows 95 & 98	10
Windows ME	10
Windows 3.11	10
Policy files	11
Policy file editor	11
Useful Registry keys	11
Utilities	12
Spyware , Malware and Adware Damages your Registry	12
Advantages of the Registry concept	13
Criticisms of the Registry concept	14
Registry Alternatives in Other Operating Systems	14
Problems with Windows 9x OS	14
See also	15
References	15
External links	16

Windows Registry Scan – Fix & Repair

www.RegistryTech.com

In computing, the **Windows registry** is a database which stores settings and options for the operating system for Microsoft Windows 32-bit versions, 64-bit versions and Windows Mobile.

It contains information and settings for all the hardware, software, users, and preferences of the PC. Whenever a user makes changes to "Control Panel" settings, or file associations, system policies, or installed software, the changes are reflected and stored in the registry.

The Windows Registry was introduced to tidy up the profusion of per-program INI files that had previously been used to store configuration settings for Windows programs. These files tended to be scattered all over the system, which made them difficult to keep track of.

-- Page 3 (16) --

Visit www.RegistryTech.com for Registry Scan and Repair Tools
Also check out the Top 3 List of AntiSpyware at
www.Free-Spyware-Remover-Reviews.com

Registry Structure

The Registry is split into a number of logical sections. These are generally known by the names of the definitions used to access them in the Windows API, which all begin "HKEY" (an abbreviation for "Handle to a Key"); often, they are abbreviated to a three- or four-letter short name starting with "HK".

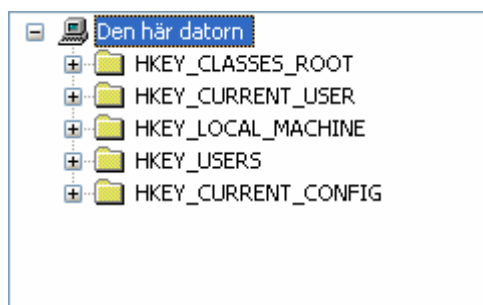
Each of these keys is divided into subkeys, which may contain further subkeys, and so on. Any key may contain values. These values can be:

- String Value
- Binary Value (0 and 1's)
- DWORDValue (numbers between 0 and 4,294,967,295 [$2^{32} - 1$])
- Multi-String value
- Expandable String Value

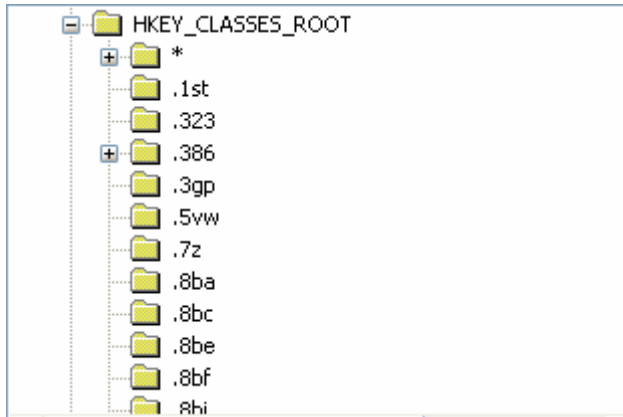
Each key has a default value, which is in effect a value with the same name as the key. Registry keys and values are specified with a syntax similar to Windows' filenames, using backslashes to indicate levels of hierarchy. E.g.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows refers to the subkey "Windows" of the subkey "Microsoft" of the subkey "Software" of the HKEY_LOCAL_MACHINE key.

The HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER nodes have a similar structure to each other; applications typically look up their settings by first checking for them in "HKEY_CURRENT_USER\Software\Vendor's name\Application's name\Version\Setting name", and if the setting is not found looking instead in the same location under the HKEY_LOCAL_MACHINE key. When writing settings back, the reverse approach is used — HKEY_LOCAL_MACHINE is written first, but if that cannot be written to (which is usually the case if the logged in user is not an administrator), the setting is stored in HKEY_CURRENT_USER instead.

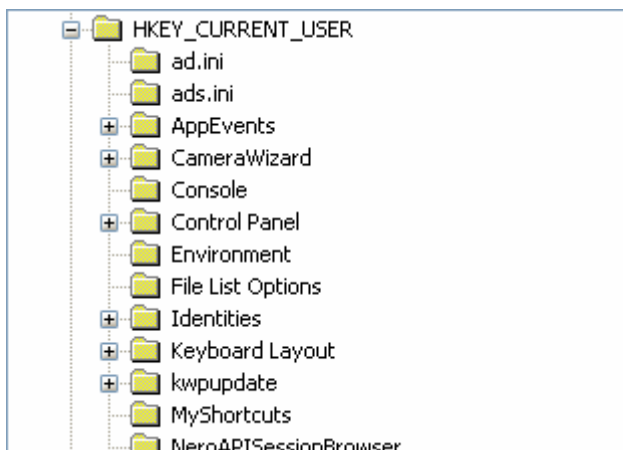


HKEY_CLASSES_ROOT



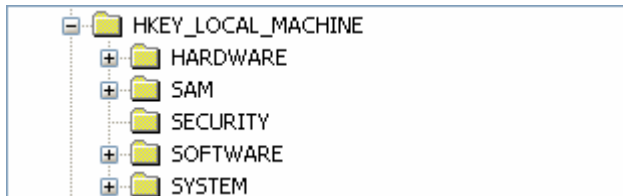
Abbreviated HKCR, HKEY_CLASSES_ROOT stores information about registered applications, including associations from file extensions and OLE object class ids to the applications used to handle these items. On Windows 2000 and above, HKCR is a compilation of HKCU\Software\Classes and HKLM\Software\Classes. If a given value exists in both of the subkeys above, the one in HKCU\Software\Classes is used.

HKEY_CURRENT_USER



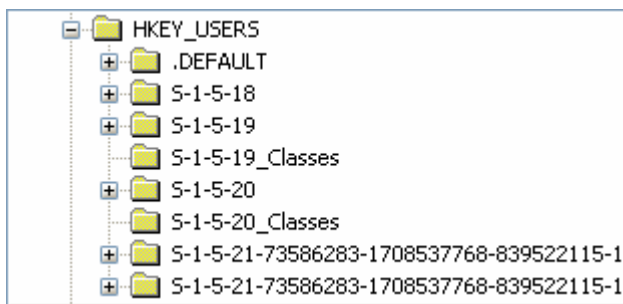
Abbreviated HKCU, HKEY_CURRENT_USER stores settings that are specific to the currently logged in user. HKCU mirrors the current user's subkey of HKEY_USERS.

HKEY_LOCAL_MACHINE



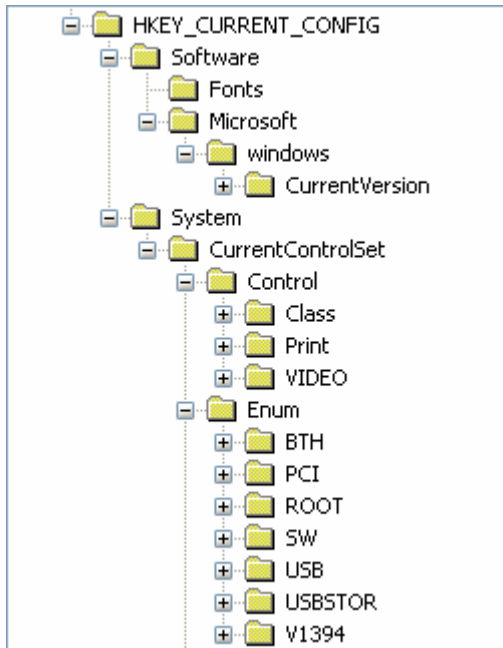
Abbreviated HKLM, HKEY_LOCAL_MACHINE stores settings that are general to all users on the computer. This key is found within the file %SystemRoot%\System32\Config\system on NT-based versions of Windows. Information about system hardware is located under the SYSTEM key.

HKEY_USERS



Abbreviated HKU, HKEY_USERS contains subkeys corresponding to the HKEY_CURRENT_USER keys for each user registered on the machine.

HKEY_CURRENT_CONFIG



Abbreviated HKCC, HKEY_CURRENT_CONFIG contains information gathered at runtime; information stored in this key is not permanently stored on disk, but rather regenerated at boot time.

Editing the Registry

Manual editing

The registry can be edited manually in Microsoft Windows by running regedit.exe or regedt32.exe in the Windows directory. However, careless registry editing can cause irreversible damage. Many optimization and "hacking" tools are available to modify this portion of the Windows operating system. It is preferable to use one of the many registry cleaners available.



 Windows 3.11 Registration Editor

A simple implementation of the current registry tool appeared in Windows 3.x, called the "Registration Info Editor" or "Registration Editor". This was basically just a database of applications used to edit embedded OLE objects in documents.

Windows NT introduced permissions for Registry editing. Windows NT 4 and Windows 2000 were distributed with both the Windows 9x REGEDIT.EXE program and Windows NT 3.x's REGEDT32.EXE program. There are several differences between the two editors on these platforms:

- REGEDIT.EXE had a left-side tree view that began at "My Computer" and listed all loaded hives. REGEDT32.EXE had a left-side tree view, but each hive had its own window, so the tree displayed only keys. * REGEDIT.EXE represented the three components of a value (its name, type, and data) as separate columns of a table. REGEDT32.EXE represented them as a list of strings.
- REGEDIT.EXE was written for the Win32 API and supported right-clicking of entries in a tree view to adjust properties and other settings. REGEDT32.EXE was written for the Win32 API and required all actions to be performed from the top menu bar.

Windows Registry Scan – Fix & Repair

www.RegistryTech.com

- Because REGEDIT.EXE was directly ported from Windows 95, it did not support permission editing (permissions do not exist on Windows 9x). Therefore, the only way to access the full functionality of an NT registry was with REGEDT32.EXE.
- REGEDIT.EXE only supports string (REG_SZ), binary (REG_BINARY), and DWORD (REG_DWORD) values. REGEDT32.EXE supports those, plus expandable string (REG_EXPAND_SZ) and multi-string (REG_MULTI_SZ). **Attempting to edit unsupported key types with REGEDIT.EXE on Windows 2000 or Windows NT 4 will result in registry corruption and, possibly, an unbootable system.**^[1]

Windows XP was the first system to integrate these two programs into one, adopting the old REGEDIT.EXE interface and adding the REGEDT32.EXE functionality. The differences listed above are not applicable on Windows XP and newer systems; REGEDIT.EXE is the improved editor, and REGEDT32.EXE simply invokes REGEDIT.EXE.

Command line editing

On NT-based systems the registry can be manipulated from the command line with the reg.exe utility. It is included in Windows XP and can be downloaded separately for previous versions.

```
reg.exe Operation [Parameter List]
Operation
[ QUERY | ADD | DELETE | COPY | SAVE | LOAD | UNLOAD | RESTORE | COMPARE | EXPORT | IMPORT ]
```

Also, a .reg file (a text-based human-readable file format for storing portions of the registry) can be imported from the command line with the following command:

```
regedit.exe /s file
```

The /s means the file will be *silent merged* to the Registry. If the /s parameter is omitted the user will not be asked to confirm the operation. In windows 98 and windows 95 the /s switch also caused regedit.exe to ignore the setting in the registry that allows administrators to disable it. When using the /s switch Regedit does not return an appropriate return code if the operation fails, unlike reg.exe which does. This makes it hard to script, however a possible workaround is to add the following lines into your batch file:

```
regedit /s file.reg
regedit /e test.reg "key"
if not exist test.reg goto REGERROR
del test.reg
```

The default association for .reg files in many versions of Microsoft Windows, starting with Windows 98 does require the user to confirm the merging to avoid user mistake.

Where is the Registry stored?

The Registry is stored in several files; depending upon the version of Windows, there will be different files and different locations for these files, but they are all on the local machine, except for the NTuser or user file which may be placed on another computer to allow for roaming profiles.

Windows NT, 2000, 2003, & XP

The following Registry files are stored in %SystemRoot%\System32\Config\:

- Sam
- Security
- Software
- System
- Default
- Userdiff
- NTUSER.dat
- The NTUSER.dat file is stored in the profile folder.

Windows 95 & 98

The registry files are named `User.dat` and `System.dat` and are stored in the `\Windows\` directory. The old ini files `win.ini` and `system.ini` are still used quite heavily in these versions of windows. Making it even harder to keep it running ok as no registry tools even look inside the ini files. And there are no real fix utilites for the ini files.

Windows ME

The registry files are named `Classes.dat`, `User.dat`, and `System.dat` and are stored in the `\Windows\` directory. It is important that you notice that windows ME have more files then windows 95 and 98. It is easy to overlook the new `classes.dat` file if you have been working with the older versions of windows.

Windows 3.11

The registry file is called `Reg.dat` and is stored in the `\Windows\` directory. This knowledge is now quite outdated as you will have a hard time finding any windows 3.11 in use.

Windows Registry Scan – Fix & Repair

www.RegistryTech.com

Policy files

Since Windows 95 administrators can include a special file in the registry, a policy file. The policy file allows administrators to enforce registry settings such as preventing users from changing the background picture of the desktop. The default extension for the policy file is .pol. The policy file filters the settings it enforces on a per user basis and per user group basis. To do that the policy file merges into the registry, preventing users from circumventing it by simply changing back the settings. The policy file is usually distributed through a LAN, but can be placed on the local computer.

Policy file editor

The policy file is created by a free tool by Microsoft that goes by the filename `poledit.exe` for Windows 95/Windows 98 and with a computer management module for NT- based systems. The module will not work in Windows XP Home, but it does work in the Pro edition. The editor requires administrative permissions to be run on systems that uses permissions. The editor can also directly change the current registry settings of the local computer and if the remote registry service is installed and started on another computer it can also change the registry on that computer. The policy editor loads the settings it can change from .adm files, of which one is included, that contains the settings the Windows shell provides. The .adm file is plain text and supports easy localisation by allowing all the strings to be stored in one place.

Useful Registry keys

The following registry keys may be of interest to users attempting to customize their Windows systems.

- **HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate** Creating this (as a DWORD) and setting it to 1 will prevent Windows (NT, 2000 or XP) from tracking the last access time of files, which speeds up a lot of operations (especially opening folders of items with previews).
- **HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\SizReqBuf** Specifies the size of buffers used for storing requests to the file/print server. Increasing this from the default of 4356 bytes can improve network performance: a figure of 14596 is frequently recommended.
- **HKLM\Software\Microsoft\Windows\CurrentVersion\Run** (and the **HKCU** equivalent) specifies applications to run whenever a user logs in. These can include desirable programs, such as printer monitoring programs or frequently-used tools, but a lot of Malware uses this registry key to ensure it is automatically run. This key is a good place to start looking for evidence of malware if you think your computer has been infected.

Windows Registry Scan – Fix & Repair

www.RegistryTech.com

Utilities

- Registry inspection and monitoring tools
 - [ErrorNuker](#) – Scan, find and repair errors in the registry. Will also clean the registry at the same time.
 - [ErrorKiller](#) —A system optimization tool that, among other things, detects and corrects application-related registry problems
 - [Regclean](#)—An unsupported tool, originally from [Microsoft](#), to remove old Registry entries
 - [Registry Toolkit](#) —A system tuning utility that includes registry cleaning

A review of various Registry cleaners was carried out by Fred Langa and published in *Information Week* on October 10, 2005.

Spyware , Malware and Adware Damages your Registry

This type of software is know to be the source of many of your problems with the registry.

Especially spyware and Malware as they normally try to install a large number of files and services in your operating system, without you noticing it. And they have no reason to use normal installation routines, with a full fledge uninstall routine, cleaning your computer complete when you remove it.

You will have to rely on software like [Adwarealert](#) to scan all of your registry to find all bad entries the spyware have put in there, then clean and fix any of the errors the cleaning created. To fix all of the registry errors a program like [ErrorNuker](#) or [ErrorKiller](#) should be run afterwards to correct as many problems as possible.

Advantages of the Registry concept

Changing from having one or more INI Files per program to one centralised registry has its good points:

- The registry keeps machine configuration separate from user configuration. When a user logs into a Windows NT/XP/2003 computer, their registry settings are merged with the system wide settings. This allows programs to more easily keep per-user configuration, as they can just work with the 'current user' key, whereas in the past they tended to just keep system-wide per-program settings. (This point doesn't apply to programs on *NIX based OSs as they have an accepted standard for per-user settings, where Windows previously did not).
- Group Policy allows administrators on a Windows-based computer network to centrally manage program and policy settings. Part of this involves being able to set what an entry in the registry will be for all the computers on the network, and affect nearly any installed program - something almost impossible with per-program configuration files each with custom layouts, stored in dispersed locations.
- Because the registry is accessed through a special API it is available to scripts and remote management using WMI. Each script does not have to be customised for every application's unique configuration file layouts and restrictions.
- The registry can be accessed as one item over a network connection for remote management/support, including from scripts, using the standard API.
- It can be backed up more easily, in that it is just a small number of files in specific locations.

Criticisms of the Registry concept

However, the centralized Registry introduces some problems as well:

- It is a single point of failure - damage to the Registry can render a Windows system unbootable, in extreme cases to a point that can not be fixed, and requires a full reinstall of Windows.
- Any program which wants to manipulate the registry must use special Windows API functions whereas a configuration file can be manipulated using normal text file-processing techniques. A user must edit the registry using the provided program 'regedit', but they could edit most other configuration files with any standard text editor.
- Configuration files can contain comments to help the user by explaining what values are for and how they can be changed, the registry cannot.
- It is more difficult to backup - it cannot be done 'live' because it is always in use, and thus requires special software such as ntbackup.
- Restoring parts of the registry is hard because you cannot easily extract data from backed up registry files
- Any application that doesn't uninstall properly, or doesn't have an uninstaller, can leave entries in the registry, which can lead over time to increased file size and decreased performance.

Registry Alternatives in Other Operating Systems

Other systems preserve the concept of separate configuration files for separate application subsystems, but group them together in a single filesystem directory for ease of management, such as the Preferences Folder in Mac OS, or the `/etc` and hidden directories (directories that start with a period) within the home directory in Unix-like systems. In those systems, fine-grained access to configuration settings can be controlled by normal filesystem protection mechanisms. Also, the only thing that could cause widespread damage to the configuration system would have to be major filesystem corruption.

Problems with Windows 9x OS

On Windows 9x computers, an older installation can have a very large registry that slows down the computer's startup and can make the computer unstable. This has led to

Windows Registry Scan – Fix & Repair

www.RegistryTech.com

frequent criticisms that the registry leads to instability. However, these problems occur slightly less often on the Windows NT family of systems, including Windows XP.

See also

- Elektra Initiative: A Windows Registry-Like back-end for configuration of the GNU/Linux operating system.
- NetInfo: The Mac OS X system database.

References

1. ^ Microsoft's *Windows 2000 Security Hardening Guide* version 1.3, published May 15, 2003, says "It is highly recommended to use regedt32.exe (a.k.a. the Windows NT registry editor) and not regedit.exe (a.k.a. the Windows 95 registry editor) to modify registry settings. Both editors ship with Windows 2000 and regedit.exe is generally perceived as easier to use. However, regedit.exe does not support all the registry data types and will convert certain types it does not understand. Certain values will not be read properly if they are converted and this can cause serious problems with the system, including failure to boot."

Russinovich, Mark E.; Solomon, David A. (2005). *Microsoft Windows Internals*, Fourth Edition, 183-236, Washington, USA: Microsoft Press. ISBN 0735619174.

External links

- [ErrorNuker](#) – Scan, find and repair errors in the registry. Will also clean the registry at the same time.
- [ErrorKiller](#) — A system optimization tool that, among other things, detects and corrects application-related registry problems
- [Regclean](#)—An unsupported tool, originally from [Microsoft](#), to remove old Registry entries
- [Registry Toolkit](#) — A system tuning utility that includes registry cleaning
- Microsoft Knowledge Base article : "Description of the Microsoft Windows registry"
- Win32 Registry Activity Monitor (Utility and Source code)
- Registry Cleaner/Drive Cleaner, need one NOW Forum discussion on registry cleaners.
- Information on the Windows registry
- [Registry Backup](#) How to back up your registry.
- [AdwareAlert](#) – Free Download and Scan for Adware, Malware and other malicious software in your computer.