# Introduction to:

# *Microsoft Windows' Registry*

*A Guide for Administrators and Home Users on the usage and functionality of the Microsoft Windows' Registry.*

By: Robert H. Williams III
CompTIA A+\Net+, Microsoft MCP\MCSA\MCSE (2000), Cisco CCNA

Version 1.7.7.24

## About this paper:

This paper is an introduction to the Microsoft Windows registry. This is intended for two target audiences, administrators, and power users. Administrators may be system administrators, or network administrators, since mass changes to the registry can be propagated via Active Directory to all computers. Power users will mostly want to take note of local use of the registry, and maybe remote functions to control how other pc's on their networks react. For example, locking down IE on your kid's computer.

## Introduction:

The Windows registry is often a topic most people shy away from. They view the registry as some black box that you can not tamper with, or seem to think that it's written in some language no mortal could ever understand. In truth, the registry is very simple. While it may be hard or even impossible to figure out what some keys mean, the registry in it's self is very simple. It is not a mess of configurations with no order. Most settings are placed in a logical location. If you know how the registry works, you can quickly find what you want.

## Requirements:

To use this paper, you need a Windows-based OS, and a tool to edit the registry. Regedit and\or Regedt32 ship with all major versions of Windows. To use local security policy, you need to be on an NT based system, including 2000, XP, or 2K3. To use Active Directory to deploy administrative templates, you must be running an Active Directory domain.

## What programs do I use to edit the registry?

Windows comes with one to three different registry editing tools for you to use:

1. RegEdit
2. Regedt32
3. Reg

Another tool you may wish to have is RegEditX, a free tool from DC Software (http://www.dcsoft.com) RegEditX adds extensions to RegEdit. It does not replace RegEdit, and is not a standalone program.

## What is the registry?

The registry is nothing more then a central place to store all settings on the computer. While a program doesn't have to store any data in the registry, it's free to if it likes. It's like the configuration files for Linux and Unix, but rather then being stored in folders, it's stored in hives, a folder-like structure.

The registry is implemented by the Configuration Manager part of the Windows Kernel.

## What are the registry keys?

When opening the registry in RegEdit, you are presented with 5 keys, or hives. The five keys are:

HKey_Classes_Root (HKCR)
HKey_Current_User (HKCU)
HKey_Local_Machine (HKLM)
HKey_Users (HKU)
HKey_Current_Config (HKCC)
HKEY_DYN_DATA (HKDD) (Win9x Only)

Of the five, three are actually subtrees of other keys. HKey_Users and HKey_Local_Machine are the two "full" keys. The other keys are sub keys of these two, or combinations of two or more keys. HKey_Users holds all "Per User" settings in the registry. If you make a change to a program that records to the registry, and another user is not effect by it, then it must be in this section. You can also use this key to edit .default, the key that is used to make the default keys for all new users. When a new user is made, .default is copied into the new hive, using their SID to tell them apart.

HKey_Current_User is the HKey_Users key for the user running regedit. It is a shortcut to the current users settings, so you don't have to find out what one of the HKey_Users you need to edit.

HKey_Current_Config is the current hardware profile listed in HKey_Local_Machine\System\ControllSet001\Hardware Profiles. HKCC is nothing more then a pointer to this key.

HKey_Classes_Root is a combo of HKEY_LOCAL_MACHINE\Software\Classes and HKEY_CURRENT_USER\Software\Classes keys. The data is a merged, so if there's no data listed for the current user, then the one for the local machine is used.

## What are Keys? Hives? Values?

When most people say hives, they normally mean the five (5) main keys, but sometimes they talk about sub-keys. Keys are the ones that look like small folders in regedit. Values for each of the keys can be binary, string, dword, multi-string ,expandable string, and a few others. In general, you do not need to know what these values mean when editing them , since you have to use the type that value needs. You can not use a string when a dword is called for. Strings and dwords are the most common. On windows 2K, regedit only supports string, dword and binary. You will have to use regedt32 to edit multi and expandable strings.

The types of values in the registry are listed on by Microsoft as the following: (Note: This is taken directly from Microsoft's site)

REG_BINARY
REG_DWORD
REG_EXPAND_SZ
REG_MULTI_SZ
REG_SZ
REG_RESOURCE_LIST
REG_RESOURCE_REQUIREMENTS_LIST
REG_FULL_RESOURCE_DESCRIPTOR
REG_NONE
REG_LINK
REG_QWORD

REG_BINARY Raw binary data. Most hardware component information is stored as binary data and is displayed in Registry Editor in hexadecimal format.

REG_DWORD Data represented by a number that is 4 bytes long (a 32-bit integer). Many parameters for device drivers and services are this type and are displayed in Registry Editor in binary, hexadecimal, or decimal format. Related values are DWORD_LITTLE_ENDIAN (least significant byte is at the lowest address) and REG_DWORD_BIG_ENDIAN (least significant byte is at the highest address).

REG_EXPAND_SZ A variable-length data string. This data type includes variables that are resolved when a program or service uses the data.

REG_MULTI_SZ A multiple string. Values that contain lists or multiple values in a form that people can read are generally this type. Entries are separated by spaces, commas, or other marks.

REG_SZ A fixed-length text string.

REG_RESOURCE_LIST A series of nested arrays that is designed to store a resource list that is used by a hardware device driver or one of the physical devices it controls. This data is detected and written in the \ResourceMap tree by the system and is displayed in Registry Editor in hexadecimal format as a Binary Value.

REG_RESOURCE_REQUIREMENTS_LIST A series of nested arrays that is designed to store a device driver's list of possible hardware resources the driver or one of the physical devices it controls can use. The system writes a subset of this list in the \ResourceMap tree. This data is detected by the system and is displayed in Registry Editor in hexadecimal format as a Binary Value.

REG_FULL_RESOURCE_DESCRIPTOR A series of nested arrays that is designed to store a resource list that is used by a physical hardware device. This data is detected and written in the \HardwareDescription tree by the system and is displayed in Registry Editor in hexadecimal format as a Binary Value.

REG_NONE - Data with no particular type. This data is written to the registry by the system or applications and is displayed in Registry Editor in hexadecimal format as a Binary Value

REG_LINK A Unicode string naming a symbolic link.

REG_QWORD Data represented by a number that is a 64-bit integer. This data is displayed in Registry Editor as a Binary Value and was first introduced in Windows 2000.

## Why do I have to reboot for some programs?

Most keys fall under HKey_Users and HKey_Local_Machine. HKU should be thought of as the user part of all configuration, while HKLM is the computer part. Many settings that are per computer are looked at when the computer boots, like settings for services, and are then never checked again. A reboot forces all programs to check any changes in the machine section of the registry. This is one of the reasons you may need to reboot, some others may be because a file is locked during normal operation, and needs changed during boot.

Some programs read data in the HKCU key on login, and never again. When changed, these programs will generally tell you to reboot, but actually a login is all that's needed.

## What is group policy?

Group policy is used to ease the change of many registry settings on a Windows computer. This is generally only done on windows 2000, XP, and 2003 or newer machines. Administrative tools should have group policy editor, listed as local policy editor. If not listed there, from the run menu, type in mmc, and file -> Add\Remove Snap in. In the local computer policy, you have two keys, computer and user configuration.

These change settings in HKU and HKLM. There are a fair amount of options here predefined, like computer configuration, windows settings, startup\shutdown scripts. while called scripts, these can be .bat or .exe files ran when the computer starts up\shuts down. This is NOT the same as log on\log off. Most normal users will want to play with the user configurations, computer configuration is more for higher level users.

In the user section, you have options for login\logoff scripts, and administrative templates. The templates are the main thing here that users will want to mess with. Click on desktop, and there's a listing of options. This is mostly simple stuff, hide icons or show them, nothing in there should really be considered advanced. What options you have depends on windows version, 2K has less options then 2K3 and XP.

Lets look in system, under CTRL-ALT-DEL. There's options to control what buttons you get in ctrl-alt-del. There are all sorts of options that you may never known you could do, like network -> network connections.

In almost every key, clicking on it will get you a dialog with three options, enable, disable, and not set. And an explain tab. Make sure you read the explain to understand what the option does.

Group policy isn't really meant to change settings on a single computer. It's meant to change settings on hundreds, or thousands of computers at once. In a Windows Active Directory network, you have what's called OU's. They're basically folders, and the network administrators can put computers and users into these OU's. For example, maybe you're in the Sales\Users OU. All people in the Sales department are required to have the same desktop settings. The administrator makes a group policy setting, and hooks the group policy onto Sales\Users. It now effects all users in sales. What if a user moved to Tech\Desktop Administrators? The administrator simply change what OU the user is in, and the settings for their desktop change based on the new rules. With the group policy templates, plus security settings, and the ability to assign permissions and programs to users and\or computers, group policy is a powerful tool. Any registry changes learned here can be applied via group policy to effect all users in a company with a few clicks of the mouse.

## How do I back-up the registry?

A simple way to backup the registry without third-party tools is this: open Regedit, and on the computer icon, right click and hit export. Make sure you're using the icon for the computer, and not one of the 5 keys, otherwise you won't export all the keys. This creates a .reg file. Simply clicking on it in explorer will import it back. This will cause it to MERGE with the current registry, so any new keys created after the backup will not be affected. There are other ways, many other ways, to back up the registry, like a system state backup using the built in windows backup tool. But exporting can be the simplest.

You can use the export to export any key. Make a neat change to the registry and want to share it? Right click the key, and export just that key. The .reg files are nothing more then text files, and can be edited with ease. If you have any sort of basic programming skills, you can make a program that makes .reg files to change registry settings.

## What is the structure of the registry?

HKey_Classes_Root is where file types are stored. It's how the computer knows what to use to open .bmp files, and it's how it knows what items to put on it's context menu, the menu you get when you right click the file. Open regedit and open HKCR, the first one you get is *.

This as you may have guessed, is a wild card. It basically effects all files. Click on the + sign to open the key, and you get openwith, shell, and shellex. Shell might not be there, so don't worry. Shellex keys are ones you don't want to mess with, at least not with a registry editor, They're com based, and can be very easy to mess up. The shell key is the main one you'll hand edit, and the most fun. If you don't have the shell key, right click the *, and hit new -> key. It should say New Key #1, rename it to shell.

Now right click shell, and hit new key. Name this one OpenCMD. This doesn't really matter, it can be any name you want. On the right pane, double click (Default) and in value data, type in Open Command Line Here. Now highlight the OpenCMD on the left pane, and hit new key. Name this one command, and it MUST be named command. Then click on command, and double click (Default) again. Set this value to "cmd /k ver & date /t & time /t" without the quotes. Now right click any file, except folders, and you now have the option to open a command window in that folders directory.

Next, right click the OpenCMD key, and hit export. Save it on your desktop to whatever you want. Right click the file, and hit edit. You can now change anything in the key, and import it back in. You can also take this file with you, and add this command to any computer you wish, with ease.

Let's try another one. Find the Folder key. NOT .folder, just folder. Under shell, make a new key, OpenNewWin. Change it's default to Open Folder In New Window. Make a new sub key, command. Change it's default to explorer %1. Now when you open a folder up on your desktop, if you want to open a second folder inside the same tree, just right click it. Doesn't seem like much, but I'm sure you'll use it more then you expect.

## How does software use the registry?

Think of the registry as a directory structure holding all the .ini files used for programs. If you open a programs .ini file, you may understand some of the settings in it, but without some sort of list of commands you can never figure out anything not listed. When you look at the keys made in the registry by a program, some of the keys you can understand, others you will never figure out without looking up or trial and error.

Software can store it's settings in one of two areas, HKey_Current_User, or HKey_Local_Machine. If it's in current user, it's a per-user setting, while local machine stores settings for all users. HKCU\Software and HKLM\Software is the default key for this information. HKCU settings override conflicting HKLM settings.

Now let's try an example of software settings. Go to HKey_Current_User\Software\Microsoft Then from there, pick Windows\CurrentVersion. Inside here there are 5 different run keys, Run, RunEX, RunOnce, RunOnceEX, and RunServices. Depending on the systems, not all these keys may be there by default. These keys control programs that start at logon. If you have some program starting up at logon that you want to kill, if it's not in the start menu then chances are it's located in the run key. Like most software settings, the HKCU\Software\Microsoft\Windows\CurrentVersion\Run key is only for the current user, while HKLM\Software\Microsoft\Windows \CurrentVersion\Run is for all users.

Have windows 2K, and use the command prompt? It has the ability to automatically fill out file and directory names for you, like in XP. If your in XP, and you type in win while in c:\, pressing tab will complete win to windows. This can be of great help if you have some really large file\folder names. 2K does not come with this option enabled. (HKCU|HKLM)\Software\Microsoft\Command Processor holds the settings for cmd, the command processor in windows 2K\XP. Inside there, you will see a completion char key. Double click it, change the value to the key you want, for example, TAB key has a hex value of 9, so put in a 9 if you want tab to complete file names. Quick and simple.

A list of different software keys will be on the bottom of this FAQ.

## I see a number like this: {A671EBA0-895B-11D4-98B2-00A0C9EE6FD9} what is it?

This is a GUID, a Globally Unique Identifier. It's used to identify this item from any other item like it int he world. The GUID is generated in part by the MAC address on the current machine, and time, among other items. This helps to make sure that no two GUID's are the same.

GUIDs are used mostly for COM programming, a special type of Object programming. Without getting into too much depth, GUIDs are normally used on complex keys in the registry, and are a good sign to stay away from that item. They're always the same length, with 4 hyphens in them.

This lets you tell them apart from SID's used to identify user accounts.

In general, items with GUIDs are more complex, and have more then one piece of software that interfaces with them. Stay away from GUIDs unless you know what your doing.

## How can I restrict access to the registry?

There are many ways to restrict access to the registry. To disable registry tools, such as regedit and regedt32, try (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\System and add the key DisableRegistryTools with a REG_DWORD value of 1. On many systems, you will have to create the system sub key. These policies will in general require you to reboot to take effect. Be warned about using this key! You will NOT be able to use registry editing tools to fix this key. You can import a .reg file like normal, however, and most 3rd party registry editing software will work. Only the regedit and regedt32 programs check this key. This does not make the registry secure, it just disables a simple path to it. They can use 3rd party tools, .reg files, the reg command from the command prompt, or even regedit on another machine connected remotely. This key has the same effect as removing file-level access to regedit.exe and regedt32.exe, just a different error message.

The hives in the registry have DACLs (discretionary access-control lists) just like the NTFS file system in windows. As long as your not using windows XP home, right clicking any key will give the permissions... option. From there, it's just like the file system, set up permissions for users or groups, and used advanced for finer control. Giving a use read-only access to their own HKCU key will break some programs, but will also prevent them from changing any settings. Check out the Active Directory section for more info on this.

XP home CAN edit registry permissions like this, it requires an add-on program for windows NT to enable the security tab for explorer. Google can show you how to do this.

## How can I access another computers registry?

Remotely accessing a registry is almost the same as any other remote administrative task. Open regedit, then file->connect network registry... key. Like other networking tools, you need rights on the other machine. If you are on a domain, then your domain account needs to be mapped to an administrative group, or if not on a domain, you need to have the same username\password as an account on the target. Otherwise you're asked for a username\password with the permissions.

For massive registry changes over groups of computers, group policy is recommended.

## How do Active Directory and Group Policies work with the registry?

Active Directory is Microsoft's directory services system based on LDAP. It's used to manage users, computers, and other objects in large (50~5,000+) networks. By using group policy, you can apply changes to many Windows settings, such as password policies and different program restrictions. To understand the relationship between Active Directory and the registry, you will need to cover three topics: Preferences vs. Policies, Registry Tattooing, and .adm files.

## Preference or Policy? What's the difference?

Group policy can be divided into two sections, a setting may be a preference, or it may be a policy. The difference? A preference is a default setting. When a user is logged on, the preference stored in group policy is applied. However, the user has full control over changing the settings. For example, you may set a font for Windows Notepad, and after they load up notepad, the user is free to make changes to the font size. Once the user logs off and back on, the preferences are reapplied, and Notepad reverts to the default domain settings.

A policy, however, can not be changed by the end user. The difference between the two is simple as permissions: a user has control over his or her registry key in a preference, but only have read permission to the registry with a policy. By using Active Directory, you can propagate registry permissions, changing a key to read-only, allowing you to set any key as a policy, rather then a preference. This is generally done when making your own .adm files, as the Microsoft programs in general use a special set of sub keys that will be talked about in the Registry Tattooing section.

To change a preference into a policy, you can change the users permission on the key from full to read-only. Doing this can be a task onto itself however. While group policy allows you to edit registry permissions, it only allows it on Classes, Hardware, and Users. Because there is no current user key, it can only set permissions via SID.

## Registry Tattooing: What is it?

Registry Tattooing is one of the issues you face when using group policy to change the registry. If the group policy makes a new key in the registry, when you remove the policy, it does not remove the new key. Also, if you change a setting via group policy, removing the setting does not revert the setting to what it once was. This process is called tattooing, and can cause unforeseen problems.

If you make a change to the registry that causes a program to act in an unforeseen manner, removing the key is not possible via group policy. It can only change keys, not remove them. So make sure you have tested the results of the key ahead of time. Making changes to firefox's registry settings, for example, shouldn't change how any other programs on your computer work, so it's a minor threat.

To help prevent this issue, Microsoft has made four special keys in the registry, the policy keys:
*HKEY_LOCAL_MACHINE\Software\Policies*
*HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies*
*HKEY_CURRENT_USER\Software\Policies*
*HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies*

As you can see, there are two keys each for HKLM and HKCU. These keys have two special changes to them that make them different then most keys. First, normal users only have read permissions to these keys, so they can not change them. Second, these keys are purged when certain evens occur, such as when group policy is reapplied. This means that any changes to these keys will be undone when a policy is removed.

While most pieces of Microsoft software will read the information in these keys, 3rd party software normally will not. This means if you want to change settings in third party software, you must be fully aware of registry tattooing. Also, these settings will be preferences, not policies, unless set at HKLM level or permissions are set (And that is a whole new can of worms).

If you are making software with settings that an administrator may wish to control, you may want to allow the software to query these keys too. Anything found in these keys should overwrite the normal, non-policy keys. For example, if HKCU\Software\Program\Execute key is 0, and HKCU\Software\Policies\Program\Execute is 1, then it should have an effective value of 1. So, when you make a program, HKLM\Software\Policies should override all other settings, then HKCU\Software\Policies, then HKLM\Software and HKCU\Software should both be controlled how you see fit. You may wish to allow HKCU to overwrite HKLM, you may not, it depends on how you wish for the software to work. Also, if the program discovers a policy on one of these keys, you may wish to disable the options that allow you to change these options, so they are enforced as a policy. By doing this, and shipping the program with an .adm file, you can now say your software is fully managed via Active Directory. If you're selling a program, this is sure to get you a whole lot more cooperate buyers then if you didn't list it.

## What are .adm files?

Adm files are add-ons to group policy. They allow you to have an easy, GUI driven control of registry settings. All parts of administrative templates are controlled via .adm files. To add or remove .adm files, first open group policy MMC snap in, and right click one of the two administrative templates, one for computer, one for users. From there, you can import your .adm file.

Many applications, such as Microsoft Office, come with their own .adm files. These programs may even import them for you, depending on the installer. In most cases, these adm files are what's known as "fully managed". This is simply a nice way of saying they use the policy keys and do not have issues with tattooing. It also means that it allows you to set them as policies, not preferences.

If you import an .adm file and it doesn't seem to show up, then it might not be fully managed. When programs are not fully managed, then they are, by default, filtered. To remove this filtering, right click in the right hand side of the administrative templates section (Where the templates themselves are displayed) and hit view -> filtering... and uncheck "Only show policy settings the can be fully managed".

## How can I see what programs access what keys in the registry?

Regmon is a free program from Sysinternals that monitors all registry activity. Be ready for a shock at how often the registry is accessed. You will need to use filters to find any one single program\key's access. The program itself can be found here:

http://www.sysinternals.com/ntw2k/source/regmon.shtml

# Sample Registry Keys

*Notes: Keys with (1) and (2) need to be used together.*

## System Settings

Notes: *The settings here apply to system-wide configurations. These settings are all applied to computers, not users.*

**Registered Owner**
Key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
Value Name: RegisteredOwner
Value Type: REG_SZ
Set To: **New Owner's Name**
Notes: *This key controls the Owner's name in the system tab of control panel, and in any programs that reads this data. This has little to no effect in Windows, it's merely a cosmetic change.*

## Explorer Settings

Notes: *All the settings here work with explorer. They should not be used for a sole means of security, as they do not remove the rights to perform actions. They merely remove the ability to do an action via Explorer.*

**Disable Desktop Right Click**
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Value Name: NoViewContextMenu
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 Default)**
Notes: *Use this to disable right click context menu on the desktop.*

**Show Windows Version On Desktop**
Key: HKCU\Control Panel\Desktop
Value Name: PaintDesktopVersion
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 Default)**
Notes: *Displays the current Windows version on top of the desktop wallpaper.*

**Disable Shutdown**
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Value Name: NoClose
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 Default)**
Notes: *Removes the shutdown option from the start menu. This should be used with removal the shutdown system right. This key does not prevent the user from turning off the computer, it only removes the shutdown button from the start menu.*

**Disallow These Programs From Running (1)**
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Value Name: DisallowRun
Value Type: REG_DWORD
Set To: **1**
Notes: *This enables disallow run. Any programs later added to the DisallowRun subkey will not be ran from explorer. Programs can still be ran by other means, and they can be renamed to bypass this.*

**Disallow These Programs From Running (2)**
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun
Value Name: 1+
Value Type: REG_SZ
Set To: **Application's Name**
Notes: *This is the container for the DisallowRun. Each program should be placed in the DisallowRun key. The first program's value should be called 1. And if the program was, for example, cmd.exe, then the string value should be cmd.exe. Renaming files will bypass this.*

**Allow ONLY These Programs To Run (1)**
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Value Name: RestrictRun
Value Type: REG_DWORD
Set To: **1**
Notes: *This enables RestrictRun. This is like Disallow Run, but explorer will only run programs listed in this key. Make sure you enable regedit for your account, or have some other means to reverse this. This is Opt-In security.*

**Allow ONLY These Programs To Run (2)**
Key: (HKCU|HKLM)\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun
Value Name: 1+
Value Type: REG_SZ
Set To: **Application's Name**
Notes: *This is the container for the Restrict Run. Each program should be placed in the Restrict Run key. The first program's value should be called 1. And if the program was, for example, cmd.exe, then the string value should be cmd.exe. Renaming files will bypass this.*

**Shell Folders**
Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Value Name: Various
Value Type: REG_SZ
Set To: **New Path**
Notes: *This key contains different paths to special folders for the user, such as desktop, CD Burning, Programs, Start Menu and the like. I personally like to use NTFS Junctions rather then change the folder location, since some programs write to the default location without checking for the correct value.*

## Application Specific

Notes: *The settings here are for the listed applications only. These can be used to set options on all computers on a network remotely, or to lock in settings by disabling the write permission to the key.*

**Application: Notepad**

**Set Font (Notepad)**
Key: HKCU\Software\Microsoft\Notepad
Value Name: lfFaceName
Value Type: REG_SZ
Set To: **Font name (For example: Lucida Console)**
Notes: *Sets the default font used in notepad.*

**Italics (Notepad)**
Key: HKCU\Software\Microsoft\Notepad
Value Name: lfItalic
Value Type: REG_DWORD
Set To: **0 to disable, 1 to enable (default is 0)**
Notes: *Sets the italics for notepad.*

**Font Size (Notepad)**
Key: HKCU\Software\Microsoft\Notepad
Value Name: iPointSize
Value Type: REG_DWORD
Set To: **Desired font size.**
Notes: *This setting controls the font size. The value should be 10x the desired size. For example, to set a font of size 24, then enter a decimal value of 240.*

**Window Size (Notepad)**
Key: HKCU\Software\Microsoft\Notepad
Value Name: iWindowPosDX & iWindowPosDY
Value Type: REG_DWORD
Set To: **Desired Window Size**
Notes: *Change these two values to control the default size of notepad when opened.*

## Internet Explorer

**Disable ability to close browser (Internet Explorer)**
Key: (HKCU|HKLM)\Software\Policies\Microsoft\Internet Explorer\Restrictions
Value Name: NoBrowserClose
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 by default)**
Notes: *When the user presses the close button, or tries to close view the file menu, the action is denied with a message stating "The operation has been canceled due to restrictions in effect on this computer. Please contact your system administrator" IE can still be closed by killing the process. If this restriction is in place on a user account, and IE is ran under the context of a different user, the first user can not kill the process of the second user. This allows internet explorer to be always active in kiosk computers.*

**Remove Favorites**
Key: (HKCU|HKLM)\Software\Policies\Microsoft\Internet Explorer\Restrictions
Value Name: NoFavorites
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 by default)**
Notes: *Removes the Favorites menu from Internet Explorer.*

**Disable Context Menu (Right Click)**
Key: (HKCU|HKLM)\Software\Policies\Microsoft\Internet Explorer\Restrictions
Value Name: NoBrowserContextMenu
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 by default)**
Notes: *Removes the ability to right click in IE*

**Remove File -> Open Menu**
Key: (HKCU|HKLM)Software\Policies\Microsoft\Internet Explorer\Restrictions
Value Name: NoFileOpen
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 by default)**
Notes: *Removes the File -> Open that can be used to launch other programs. Helps keep a cleaner look in a Kiosk machine, but NTFS permissions should still be used to limit what programs the end user may run.*

**Remove File -> Save As Menu**
Key: (HKCU|HKLM)Software\Policies\Microsoft\Internet Explorer\Restrictions
Value Name: NoBrowserSaveAs
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 by default)**
Notes: *Removes the File -> Save As that can be used to launch other programs. Helps keep a cleaner look in a Kiosk machine, but NTFS permissions should still be used to limit what programs the end user may run.*

**Remove Address Bar**
Key: HKLM\Software\Policies\Microsoft\Internet Explorer\Toolbars\Restrictions
Value Name: NoAddressBar
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 by default)**
Notes: *By removing the address bar, and disabling Explorer, you can use a single HTML page as the computers interface on a kiosk machine.*

## Automatic Update Settings

Notes: *These settings allow the user to fine-tune how Automatic Updates run on a system. Most of these settings can be set via Group Policy using default templates shipped in 2K and 2K3.*

**Automatic Updates**
Key: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Value Name: NoAutoUpdate
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 by default)**
Notes: *This is the key to DISABLE auto updates. So setting it to 1 enables disable automatic updates. In other words, set it to 1 to turn off automatic updates.*

**Automatic Updates - Options**
Key: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Value Name: AUOptions
Value Type: REG_DWORD
Set To: **2, 3, 4, 5**
Notes: *These options control if it downloads the updates on it's own, or if it just tells the user when downloads are out. It also controls if the service will install the updates, or prompt the user to install them later. 2 will tell you when there are updates to download. 3 will download them automatically, and ask for an install. 4 will fully automate the process, but may not finish the installs till you reboot. To use 4, you must have* ScheduledInstallDay *and* ScheduledInstallTime *set. 5 forces automatic updates to be enabled, but allows the end users to configure it.*

**Automatic Updates - Install Options**
Key: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Value Name: ScheduledInstallDay
Value Type: REG_DWORD
Set To: **0~7**
Notes: *Controls on what day the updates will be installed. 0 is daily, while 1~7 is a set day of the week, Sunday to Saturday.*

**Automatic Updates - Install Options 2**
Key: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Value Name: ScheduledInstallTime
Value Type: REG_DWORD
Set To: **0~23**
Notes: *Controls at what time Windows will install the updates, in 24 hour format.*

**Automatic Updates - Auto Reboot When Logged On**
Key: HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
Value Name: NoAutoRebootWithLoggedOnUsers
Value Type: REG_DWORD
Set To: **0 or 1**
Notes: *Controls if Windows will automatically reboot when a user is logged on. Setting to 1 will prompt the user to reboot, while setting to 0 will cause Automatic Updates to notify the user that the computer will reboot. Default time till reboot is five (5) minutes.*

## TCP\IP Settings in Windows 2003

Notes: *These settings are based off of Windows 2003. Some may apply to 2K and XP, and a few keys may work on 9x based systems. But these are primarily aimed for Windows 2K3 servers. All keys listed here, plus many many more, can be found inside the paper "*Microsoft Windows Server 2003 TCP/IP Implementation Details", *listed in the references section of this paper.*

**Allow Raw Sockets For Users (Windows 2003)**
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: AllowUserRawAccess
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 by default)**
Notes: *By default, only Administrators can access raw sockets on a Windows 2003 system. Setting this value to 1 allows raw-socket usage for all users.*

**Arp Cache Keep Alive**
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: ArpCacheLife
Value Type: REG_DWORD
Set To: **0 to 0xFFFFFFFF (4,294,967,295 Decimal)**
Notes: *Controls the time, in seconds, that an entry stays within the ARP cache. Without this key, defaults are two minutes for unused entries, and ten minutes for used entries.*

**Data Base Path**
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: DatabasePath
Value Type: REG_EXPAND_SZ
Set To: **Path to files. (Default: %SystemRoot%\system32\drivers\etc)**
Notes: *This controls the path to TCP\IP's database files, Hosts, Lmhosts, Network, Protocols, Services. Sometimes changed by malware to bypass restrictions on the hosts file.*

**Default Time To Live**
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: DefaultTTL
Value Type: REG_DWORD
Set To: **0~0xFF (0~255 Decimal, 128 Default)**
Notes: *Adjusts the TTL of outgoing IP packets. Raising TTL can cause larger broadcast storms if routing loops are formed in network topology.*

**Disable Offloading to Network Card**
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: DisableTaskOffload
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 by default)**
Notes: *Allows functions in the TCP\IP stack to be performed by the hardware in the network card. Disabling this will cause greater load onto the CPU as the system must handle all functions. This is used for troubleshooting only.*

**Enable Detect Dead Gateway**
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: EnableDeadGWDetect
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (1 by default)**
Notes: *This causes TCP to detect if the main gateway has went down, and will switch to any secondary gateways configured in TCP\IP properties.*

**Enable Multicast Forwarding**
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: EnableMulticastForwarding
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (0 by default)**
Notes: *This controls if the computer will forward Multicasts across other networks. This is only used when the computer is running as a Routing and Remote Access Server (RRAS).*

**Enable Path MTU Discovery**
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: EnablePMTUDetect
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (1 by default)**
Notes: *Controls if windows will try to discover the Maximum Transmission Unit (MTU) over the path to a remote host. If the MTU used is larger then what is supported, then the packet will become fragmented in transport. Fragmentation can cause network congestion and excess load on networking devices as they assemble the packets back into whole units of data.*

**Syn Attack Protection**
Key: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Value Name: SynAttackProtect
Value Type: REG_DWORD
Set To: **1 to enable, 0 to disable (1 by default on Windows 2K3 with SP1, 0 by default on 2K3 with SP0)**
Notes: *Enables the SYN attack protection in SYN-ACK floods. Please see the Windows 2003 TCP\IP Implementation in the References section for more information. It is recommended that it is set to 1 on all SP0 configurations, if SP1 can not be installed for some reason.*

## References used:

Configure Automatic Updates in a Non–Active Directory Environment:
*http://technet2.microsoft.com/WindowsServer/en/Library/75ee9da8-0ffd-400c-b722-aeafdb68ceb31033.mspx*

Microsoft Windows Server 2003 TCP/IP Implementation Details:
*http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/networking/tcpip03.mspx*

Description of the Microsoft Windows registry:
*http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986*

Differences between Regedit.exe and Regedt32.exe:
*http://support.microsoft.com/kb/141377/*

Registry Functions:
*http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/registry_functions.asp*

Inside the Registry - By Mark Russinovich (Windows NT Magazine)
*http://www.microsoft.com/technet/archive/winntas/tips/winntmag/inreg.mspx*

Understanding Policy "Tattooing":
*http://www.gpoguy.com/FAQs/tattoo.htm*