

- **RegEdit.com : Windows Registry Guide** -



RegEdit.com : Windows Registry Guide

Please visit RegEdit.com for all the latest tips, tricks and tweaks to get the most out of your Windows™ 95, 98 and NT system!



Enhancements

Settings to Enhance Functionality



Security

Security Restrictions and Policies



Files

Other Files With Windows Settings



Tips and Tricks

Hidden and Useful Windows Functions



Performance

Settings to Optimize Performance



Troubleshooting

Windows Bugs and Fault Resolution

Got a Question? Try the [Windows Registry FAQ](#) or join our [Mailing List](#)!

Disclaimer:

Modifying the registry can cause serious problems that may require you to reinstall your operating system. We cannot guarantee that problems resulting from the incorrect use of the registry can be solved. Use the information provided at your own risk. Any trademarks mentioned herein are the property of their respective owners.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Enhancements -

Categories:



[Applications](#)

Application Specific Enhancements



[Network](#)

Network Based Enhancements



[Hardware](#)

Hardware Functionality Enhancements



[Windows](#)

Microsoft Windows Enhancements

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Enhancements/index.shtml - (1)

- RegEdit.com : Files -

Categories:



[BOOT.INI](#)
Windows NT Configuration File



[MSDOS.SYS](#)
Windows 9x Configuration File

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Files/index.shtml - (2)

- RegEdit.com : Performance -

Categories:



File System Performance Settings



Internet and Networking Performance Settings

Registry Keys:



Changing the Menu Show Delay (*Windows 9x and NT*)

Windows normally delays menus before they are shown. For regular users this delay can become annoying, with this setting you to change the delay or remove it altogether.



Control the Windows Animation Function (*Windows 9x and NT*)

Although the Windows animation function, can look good it can slow down your PC if you have a slower graphics card. This settings allows you to control the Windows animation function.



Optimizing L2 Caches Over 256K (*Windows NT*)

Windows NT by default is optimized for a 256K size L2 cache. With most computers now having L2 caches larger than 256K it pays to take the time to change the SecondLevelDataCache setting to correspond to the size of the L2 cache installed.



Control Whether Windows Performs Smooth Scrolling (*Windows 9x and NT*)

This setting allow you to disable the Windows smooth scrolling function, which on an low-powered system can cause performance degradation.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Security -

Categories:



[Applications](#)

Application Specific Security Settings



[Network](#)

Network and Workgroup Security Settings



[Control Panel](#)

Control Panel Security Restrictions



[System](#)

System Security Restrictions and Settings



[Explorer](#)

Windows Explorer and Desktop Restrictions

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/index.shtml - (4)

- RegEdit.com : Tips and Tricks -

Categories:

[Windows 9x](#)

Windows 95 and 98 Tips

[Windows NT](#)

Windows NT Tips and Tricks

Registry Keys:



[Automatically View Thumbnails of Bitmap Files](#) *(Windows 9x and NT)*

Makes Explorer show a thumbnail version of bitmaps files in the current folder rather than the generic icon ordinarily used. This is a great way to preview .BMP files without having to open them first.



[Enable Live Scrolling in Microsoft Word](#) *(Windows 9x and NT)*

Normally when you move through a Word document using the scroll bar the page doesn't update until you release the mouse button. With this tweak the document location is updated as you move.



[Change the Location of System and Special Folders](#) *(Windows 9x and NT)*

Windows keeps a number of special folders such as "My Documents", "Desktop", "Favorites" and the "Start Menu". These folders can be moved anywhere on you system and the new location updated in this key.



[Expand and Contract Folders With Ease](#) *(Windows 9x and NT)*

It can be a time-consuming process to expand a folder by clicking on the (+) for each and every sub-directory. This tip lets you expand and contract them all at once, with one keystroke.



[Launching Programs When Windows Starts](#) *(Windows 9x and NT)*

You can automatically start programs whenever Windows launches. If you have programs automatically starting that you have not loaded then you can remove them using this tip as well.



[Avoid Accidental Registry Imports](#) *(Windows 9x and NT)*

By default, if you double-click on a file with a '.REG' extension the file will be imported into the system registry. You can change the default so it opens the file for editing instead.



[Removing Item Types from the New Menu](#) *(Windows 9x and NT)*

When you right-click on your desktop or other selected applications there is a *New* sub-menu which contains a list a default templates. This list can be modified to include only the templates you want.



[Close Parent Windows Automatically](#) *(Windows 9x and NT)*

Have you ever had a screen full of explorer windows on your desktop after digging through heaps of directories? This tip lets you close the current window and all it's parent windows in one easy step.



[Including Manufacturer and Support Details](#) *(Windows 9x and NT)*

This tip lets you include a company logo and contact information in the System Properties dialog box. This is especially useful if you run a computer store and want your customers to be reminded where they bought their PC and where to get technical support.



[Default Name and Company Information](#) *(Windows 9x and NT)*

When you install a new application, using MS Setup, a default Name and Company are shown, these values can be changed when the details have changed or are incorrect.



[Add Your Own Tips](#) *(Windows 9x and NT)*

Are you sick of seeing the same tips again and again when you first logon to Windows? Now you can change them to whatever you want, whether it's quotes, jokes or a to-do list, anything is possible.



[Make the Columns Fit](#) *(Windows 9x and NT)*

Want to quickly see all the column in explorer without having to resize them individually? This tip does it for you.



Removing Icons from your Desktop (Windows 9x and NT)

This key contains a number of subkeys which hold information about the namespace extensions of icons on your desktop. Through this key you can control which icons are visible on the desktop, including the My Computer, Inbox, MSN and Internet icons.



Creating a Shortcut to the System Folders (Windows 9x and NT)

This function allow you to add a shortcut to various system folders on your Desktop or Start Menu.



Desktop Icon Redraw Frequency (Windows 9x and NT)

If you desktop icons are redrawing too frequently, change this setting.



Remove Cached Command Lines from the Run Menu (Windows 9x and NT)

Got a lot of items in the Start Menu's run command history? This tip will allow you to remove any extraneous commands.



Add the QuickView Option to All Files (Windows 9x and NT)

If you ever wanted to add QuickView to the context menu of all file types, it may be a tedious task doing so using Windows Explorer's Options - File Type window. This tip shows how to do it in a couple of easy steps.



Change the Recycle Bin Icons (Windows 9x and NT)

Would you like to make you Recycle Bin into something a bit more exciting? Maybe a glowing toxic waste bin? With this tweak you can change the icon to be whatever you like.



Remove the Arrow from Shortcuts (Windows 9x and NT)

Would you prefer to show your shortcuts without the arrow in the bottom left hand corner? This tip will show you how to change the arrow icon or remove it completely.



Rename or Delete Special Folders (Windows 9x and NT)

This setting allows you to rename and delete special folders (such as the Recycle Bin) as if it was a normal folder by rick-clicking the icon.



Add Custom Folder to My Computer or the Desktop (Windows 9x and NT)

Create your own custom system folder on the desktop or in My Computer, that can't be deleted or renamed.



Full Window Drag Option (Windows 9x and NT)

This setting enables the Full Windows Drag function, which allow you to view the contents of window while dragging it across the screen, instead of just the standard outline.



Removes the Start Banner on the Taskbar (Windows 9x and NT)

Hides the arrow and "Click here to start" caption that appears on the taskbar when you start Windows.



Changing the Registered Owner and Organisation (Windows 9x and NT)

If you entered the wrong registration information when you installed Windows you can change it and other miscellaneous settings such as ProductID and ProductName.



Change the Wallpaper Shown Prior to Logon (Windows 9x and NT)

This key lets you change the wallpaper that appears prior to anyone logging in to the system.

Related Categories:

- [Enhancements : Windows](#)

Source: C:/helpfile/Tips_and_Tricks/index.shtml - (5)

- RegEdit.com : Troubleshooting -

Categories:



[File System](#)

File System Troubleshooting



[Windows Bugs](#)

Windows Bugs and Fault Resolution



[Logging](#)

Device and Application Logging Functions

Registry Keys:



[MS-DOS Compatibility Mode Problems with PCI-IDE Controllers](#) *(Windows 9x)*

If your computer contains a PCI-IDE hard disk controller that employs serialization between the two IDE channels, this tip may help you resolve a MS-DOS compatibility mode problem in Device Manager.



[Removing Programs listed in the Add/Remove Programs Box](#) *(Windows 9x and NT)*

All Windows 9x or NT compatible programs must include an Uninstall program, sometimes though the program may get removed but entry in Add/Remove programs doesn't, from this key you can remove those orphaned entries.



['Failure Writing to the System Registry...' Error Message](#) *(Windows 95)*

When you run a setup program that was created using the Application Setup Wizard, you may receive an error message indicating the registry may be corrupt or you do not have the required permissions to write to the registry.



[Has Your Taskbar Disappeared?](#) *(Windows 9x and NT)*

If your taskbar has disappeared from the desktop then it may be due to a corrupt registry key.



[Are You Missing Fonts from the Fonts Folder?](#) *(Windows 9x and NT)*

A font may seem to be installed correctly but does not appear in the Fonts folder because the Fonts key in the registry is missing or damaged.



[Delay Occurs When Unlocking Workstation](#) *(Windows NT)*

Sometimes a noticeable delay occurs when the logged on user or an administrator attempts to unlock a workstation. This because when you unlock the workstation Windows NT will update the domain list if the cached list's age exceeds two minutes (by default). This age limit can be modified.



[Yellow '!' On PCMCIA Network Adapter](#) *(Windows 9x)*

When using a PCMCIA network adapter under Windows 98 you might not be able to connect the computer to the network, and under Control Panel >System there is a yellow exclamation mark next to the card.



[Changing the Default State of the NUMLOCK Key](#) *(Windows NT)*

The NUMLOCK key is usually only turned on before the user has logged into the computer, this can cause problem for people with portable computers that do not check the status of the NUMLOCK key before typing their password. The default behaviour can be changed with this setting.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Windows Registry FAQ -

1. [What is the Registry?](#)
2. [Where is the Registry found?](#)
3. [How can you edit the Registry?](#)
 - [Create a Shortcut to Regedit](#)
 - [Using Regedit to modify your Registry](#)
 - [Regedit Command Line Options](#)
4. [What's the structure of the Registry?](#)
5. [How can you backup and restore the Registry?](#)
6. [Importing and Exporting Registry Settings](#)
7. [What to do if you get a Corrupted Registry](#)
 - [Windows 95](#)
 - [Windows NT](#)
8. [How can I clean out old data from the Registry?](#)

What is the Registry?

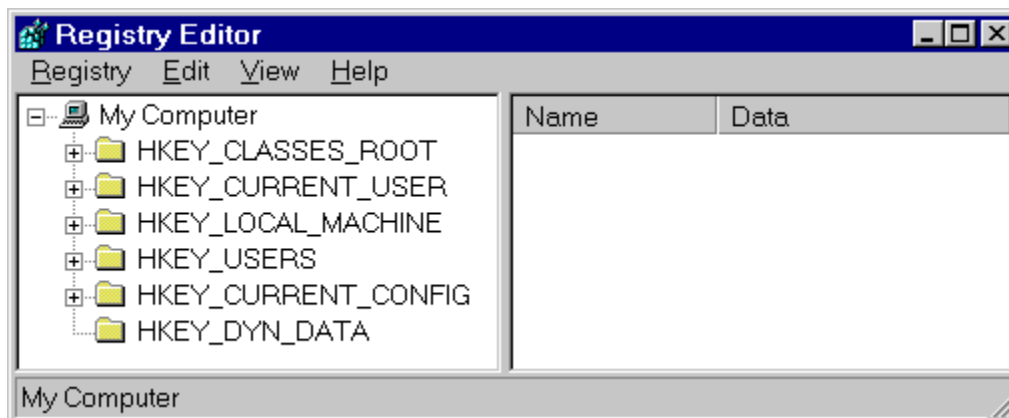
The Registry is a database used to store settings and options for the 32 bit versions of Microsoft Windows; including Windows 95, 98 and NT. It contains information and settings for all the hardware, software, users, and preferences of the PC. Whenever a user makes changes to a Control Panel settings, or File Associations, System Policies, or installed software, the changes are reflected and stored in the Registry.

Where is the Registry found?

The physical files that make up the registry are stored differently depending on your version of Windows; under Windows 95 & 98 it is contained in two hidden files in your Windows directory, called **USER.DAT** and **SYSTEM.DAT**, while under Windows NT the files are contained separately in the "Windows / System32 / Config" directory.

How can you edit the Registry?

The Registry Editor (REGEDIT.EXE) is included with most version of Windows (although you won't find it on the Start Menu) it enables you to view, search and edit the data within of the Registry. There are several methods for starting the Registry Editor, the simplest is to click on the START button, then select RUN, and in the OPEN: box type "regedit", and if the Registry Editor is installed it should now open and look like the image below.



• Create a Shortcut to Regedit

This can be done by simply right-clicking on a blank area of your desktop, selecting New, then Shortcut, then in the Command line box enter "regedit.exe" and click Next, enter a friendly name (e.g. 'Registry Editor') then click Finish and Presto!

• Using Regedit to modify your Registry

Once you have started the Regedit you will notice that on the left side there is a tree with folders, and on the right the contents (values) of the currently selected folder.

To expand a certain branch (see the [structure of the registry](#) below), click on the plus sign [+] to the left of any folder, or just double-click on the folder. To display the contents of a key (folder), just click the desired key, and look at the values listed on the right side. You can add a new key or value by selecting New from the Edit menu, or by right-clicking your mouse. And you can rename any value and almost any key with the same method used to rename files; right-click on an object and click rename, or click on it twice (slowly), or just press F2 on the

keyboard. Lastly, you can delete a key or value by clicking on it, and pressing Delete on the keyboard, or by right-clicking on it, and choosing Delete.

Note: it is always a good idea to backup your registry (see below) before making any changes to it. It can be intimidating to a new user, and there is always the possibility of changing or deleting a vital setting causing you to have to reinstall the whole operating system. It's much better to be safe than sorry!

• Regedit Command Line Options

Regedit has a number of command line options to help automate its use in either batch files or from the command prompt. Listed below are some of the options, please note the some of the functions are operating system specific.

```
regedit.exe [options] [filename]
filename      Import .reg file into the registry
/s            Don't display dialog box when importing .reg files
/e            Export registry file
              e.g. regedit /e filename.reg HKEY_LOCAL_MACHINE\SYSTEM
/L:system     Specify the location of the system.dat to use
/R:user       Specify the location of the user.dat to use
/C            Compress [filename] (Windows 98)
```

What's the structure of the Registry?

The Registry has a hierarchal structure, although it looks complicated the structure is similar to the directory structure on your hard disk, with Regedit being similar to Windows Explorer. Each main branch (denoted by a folder icon in the Registry Editor, see below) is called a **Hive**, and Hives contains **Keys**. Each key can contain other keys (sometimes referred to as sub-keys), as well as **Values**. The values contain the actual information stored in the Registry. There are three types of values; *String*, *Binary*, and *DWORD* - the use of these depends upon the context. There are six main branches, each containing a specific portion of the information stored in the Registry. They are as follows:

- **HKEY_CLASSES_ROOT** : This branch contains all of your file association types, OLE information and shortcut data.
- **HKEY_CURRENT_USER** : This branch links to the section of HKEY_USERS appropriate for the user currently logged onto the PC.
- **HKEY_LOCAL_MACHINE** : This branch contains computer specific information about the type of hardware, software, and other preferences on a given PC, this information is used for all users who log onto this computer.
- **HKEY_USERS** : This branch contains individual preferences for each user of the computer, each user is represented by a SID sub-key located under the main branch.
- **HKEY_CURRENT_CONFIG** : This branch links to the section of HKEY_LOCAL_MACHINE appropriate for the current hardware configuration.
- **HKEY_DYN_DATA** : This branch points to the part of HKEY_LOCAL_MACHINE, for use with the Plug-&-Play features of Windows, this section is dynamic and will change as devices are added and removed from the system.

How can you backup and restore the Registry?

Microsoft included a utility on the Windows 95 CD-ROM that lets you create backups of the Registry on your computer. The Microsoft Configuration Backup program, CFGBACK.EXE, can be found in the `\Other\Misc\Cfgback` directory on the Windows 95 CD-ROM. This utility lets you create up to nine different backup copies of the Registry, which it stores, with the extension RBK, in your Windows directory. If your system is set up for multiple users, CFGBACK.EXE won't back up the USER.DAT file.

After you have backed up your Registry, you can copy the RBK file onto a floppy disk for safekeeping. However, to restore from a backup, the RBK file must reside in the Windows directory. Windows 95 stores the backups in compressed form, which you can then restore only by using the CFGBACK.EXE utility.

Importing and Exporting Registry Settings

A useful feature of the Registry Editor is its ability to import and export registry settings to a text file, this text file, with the .REG extension, can then be saved or shared with other people to easily modify local registry settings. You can see the layout of these text files by simply exporting a key to a text file and opening it in Notepad, to do this using the Registry Editor select a key, then from the "Registry" menu choose "Export Registry File...", choose a filename and save. If you open this file in notepad you will see a file similar to the example below:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SYSTEM\Setup]
"SetupType"=dword:00000000
"CmdLine"="setup -newsetup"
"SystemPrefix"=hex:c5,0b,00,00,00,40,36,02
```

The layout is quite simple, **REGEDIT4** indicated the file type, **[HKEY_LOCAL_MACHINE\SYSTEM\Setup]** indicated the key the values are from, **"SetupType"=dword:00000000** are the values themselves the portion after the "=" will vary depending on the type of value they are; *String*, *Binary*, or *DWORD*.

So by simply editing this file to make the changes you want, it can then be easily distributed and all that need to be done is to double-click, or choose "Import" from the Registry menu, for the settings to be added to the system Registry (see [Regedit Command Line Options](#) above).

What to do if you get a Corrupted Registry

Firstly don't try ringing Microsoft Technical Support, they most probably won't help you. Luckily though both Windows 95, 98 and NT have a simple registry backup mechanism that is pretty reliable, although don't count on it, always make a backup first!

• Windows 95

In the Windows directory there are several hidden files, four of these will be **SYSTEM.DAT & USER.DAT**, your current registry, and **SYSTEM.DA0 & USER.DA0**, a backup of your registry. Windows 9x has a nice feature in that every time it appears to start successfully it will copy the registry over these backup files, so just in case something goes wrong you can restore it to a known good state. To restore the registry follow these instructions:

1. Click the Start button, and then click Shut Down.
2. Click Restart The Computer In MS-DOS Mode, then click Yes.
3. Change to your Windows directory. For example, if your Windows directory is C:\Windows, you would type the following:

```
cd C:\Windows
```

4. Type the following commands, pressing ENTER after each one. (Note that SYSTEM.DA0 and USER.DA0 contain the number zero.)

```
attrib -h -r -s system.dat
attrib -h -r -s system.da0
copy system.da0 system.dat
attrib -h -r -s user.dat
attrib -h -r -s user.da0
copy user.da0 user.dat
```

5. Restart your computer.

Following this procedure will restore your registry to its state when you last successfully started your computer.

If all else fails, there is a file on your hard disk named SYSTEM.1ST that was created when Windows 95 was first successfully installed. If necessary you could also change the file attributes of this file from read-only and hidden to archive to copy the file to C:\WINDOWS\SYSTEM.DAT.

• Windows NT

On Windows NT you can use either the "Last Known Good" option, or RDISK to restore to registry to a stable working configuration.

How can I clean out old data from the Registry?

Although it's possible to manually go through the Registry and delete unwanted entries, Microsoft provides a nifty tool to automate the process, the program is called RegClean. RegClean analyzes Windows Registry keys stored in a common location in the Windows Registry. It finds keys that contain erroneous values, and after recording those entries in the Undo.Reg file, it removes them from the Windows Registry. You can download this free utility from our [downloads page](#).

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Enhancements : Applications -

Categories:



Internet Explorer

Internet Explorer Specific Enhancements



pcANYWHERE

Tweaks for Symantec pcANYWHERE



Outlook Express

Tweaks for Outlook Express

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Enhancements/Applications/index.shtml - (8)

- RegEdit.com : Enhancements : Hardware -

Categories:



Printing

Windows Printing Enhancements

Registry Keys:



Enable or Disable the CD-ROM Autorun Feature (Windows 9x and NT)

You can enable the CD-ROM autorun function by changing this registry setting, this will stop applications from auto launching when you insert a CD-ROM disc into your drive.



PC Speaker Beeping on Errors (Windows 9x and NT)

If you get annoyed by the beeps and noises coming from your PC speaker but can't find a way to turn it off, then use this tip to disable it.



Adjust IntelliMouse Scroll Function (Windows 9x and NT)

This entry determines the number of lines scrolled for each rotation of the mouse wheel on a Microsoft IntelliMouse! 22 when no modifier keys (such as <Ctrl> or <Shift>) are pressed.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Enhancements/Hardware/index.shtml - (9)

- RegEdit.com : Enhancements : Network -

Registry Keys:



Dial-Up Networking Password Box Grayed Out (Windows 9x)

If you are having problems trying to get DUN to remember your password and you find the option grayed out then there are a few things you can try.



Removing or Adding Items to Your Persistent Connections List (Windows NT)

Windows stores the names of previously mapped drives, this can be a security threat if vulnerable hidden shares are listed. An advantage is that this key can also be used to set default items for list, if for example inexperienced users where required to map common drives, you could store them here.



Specifying a Preferred Netware Server (Windows 9x)

Specifying a default Netware is possible using this setting.



Modifying LAN Based Auto-disconnect Time-Out (Windows NT)

Windows NT can be configured to automatically disconnect idle LAN sessions are a set number of minutes.



Disable Automatic Netware Logon (Windows 9x)

This setting disabled the automatic logon to Netware servers.



Display Domain Logon Confirmation (Windows 9x and NT)

When this option is enabled, a dialog box is shown upon successful validation by a Windows NT domain.



Automatically Detect Slow Network Connections (Windows NT)

By default, Windows NT will attempt to detect the time-out on network links to determine their speed (high or low). This functionality can be disabled if Windows NT is having problems determining the speed of your link.



Define the Slow Link Time-Out (Windows NT)

Windows NT uses this setting to define what is a low speed, and what is a high speed connection. The default time-out is 2000 milliseconds, any connection slower is considered a low speed link.



Support Long Filenames on Netware Servers (Windows 9x)

This setting controls whether long filenames (LFN) are supported on Netware servers, and if supported which versions.



Disable SAP advertising for Netware Networks (Windows 9x)

By default Windows will send SAP packets to advertise available file and print shares when 'File and Print Sharing for Netware Networks' is enabled, this setting disables those packets.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Enhancements : Windows -

Categories:



Windows 95 & 98 Specific Enhancements



Windows NT Specific Enhancements

Registry Keys:



[Displaying Hi-Color Icons without the Plus Pack](#) *(Windows 9x and NT)*

If you like a bit more colour and detail in your icons, then step up to hi-color mode. With this setting your Windows icons are shown in all their hi-resolution glory.



[Add an Expanding Control Panel to Start Menu](#) *(Windows 9x and NT)*

Want easy access to the Control Panel options? With this tip you can add an expanding Control Panel folder to the start menu. This trick will work with most special folders too.



[Easily Use Notepad to Open a File](#) *(Windows 9x and NT)*

Enabling this setting will allow you to use Notepad to open a file by simply right clicking on the icon. Also the Notepad will be used to open the files by default if no association already exists.



[Add Explore From Here to Every Folder](#) *(Windows 9x and NT)*

When you right click on any folder this will give you an option to *Explore From Here*, which will open up an explorer window of that folder.



[Control Network Browser Elections](#) *(Windows 9x and NT)*

A browser election is a normal network occurrence and provides a means to guarantee there is never more than one master browser present in a domain / workgroup.



[Add Command Prompt Here to Every Folder](#) *(Windows 9x and NT)*

If you're from the old school and still use the DOS prompt regularly, then this tip is for you! It creates a new right-click option to open a command prompt window at the directory you are currently working from.



[Creating Program Aliases in Windows](#) *(Windows 9x and NT)*

A hidden feature in the Windows registry allows you to create program aliases. Allowing you to create, for example, an alias called JBLOGGS.EXE that when executed actually runs another program, e.g. NOTEPAD.EXE



[Active Window Tracking \(X-Mouse\)](#) *(Windows 9x and NT)*

This tweak makes you most control the Window focus, therefore wherever you move your mouse the window will become active, similar to X-Windows on Unix.



[Automatic Logon without Name or Password](#) *(Windows 9x)*

This setting allows Windows clients to logon without entering a user name or password, therefore bypassing the logon box.



[Adjust the Double-Click Sensitivity Area](#) *(Windows 9x and NT)*

This setting controls the amount of movement allowed between clicks, for two clicks to be counted as a double-click.



[Removing the 'Shortcut to...' Text on Shortcuts](#) *(Windows 9x and NT)*

Don't like having 'Shortcut to...' appended to every Shortcut? You're not alone. With this tip you can stop Windows for adding this text when creating links.



[Change the Alignment of Drop-Down Menus](#) *(Windows 9x and NT)*

By default, Windows drop-down menus are aligned to the left, with this tip you can change the default behaviour to make all drop-down aligned to the right instead.



Change the Size of Desktop Icons (Windows 9x and NT)

Are your icons too small? Or too big? This setting will let you resize them to suit your desktop preference.



Change the Position of the Desktop Wallpaper (Windows 9x and NT)

Unfortunately Windows only gives you the limited options of center or tile for the placement of the desktop wallpaper. With this setting you can move the image anyway on your desktop.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Enhancements/Windows/index.shtml - (11)

- RegEdit.com : Files : BOOT INI -

Registry Keys:



Boot Windows NT in Safe Mode *(Windows NT)*

Windows NT can be very temperamental sometimes are you add new software or install a new driver. The option allows you the create a Windows NT alternative to the Windows 9x Safe Mode. In this mode extra checks are performed and not all third party drivers are loaded.



Disable Detection of Devices on Serial Ports *(Windows NT)*

Windows NT attempts to probe the serial ports on boot-up to detect any serial mice. This can cause problems with other serial devices such as UPS's.



Enable the 4GT RAM Tuning Feature of NT Enterprise Edition *(Windows NT)*

With standard Windows NT Server, the per-process address limit is 2 gigabytes (GB) of random access memory (RAM). The 4GT feature of Windows NT Server/E increases this limit to 3 GB without introducing new APIs. 4GT does this by reducing the potential RAM allocated to the Windows NT kernel from 2 GB to 1 GB.



Boot Windows NT with the Default VGA Video Driver *(Windows NT)*

This explains how to create an a safe VGA video mode start-up option, especially useful when your video adapter or driver is causing problems.



Change the Default Operating System *(Windows NT)*

This key controls which operating system the NT Boot Loader launches by default.



Change Default OS Selection Timeout *(Windows NT)*

This setting controls the amount of time Windows NT will wait before loading the Default OS choice as define by the "default=" option.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Files : MSDOS SYS -

Registry Keys:



Running Scandisk on Boot Up (Windows 9x)

If Windows 9x is shutdown incorrectly, or the turn power turned off without shutting down, the system will attempt to run Scandisk on the next boot. You can control whether Scandisk doesn't run, prompts whether to run, or runs automatically.



Modifying the [Paths] Section of MSDOS.SYS (Windows 9x)

The [Paths] section lists the locations for other Windows 95 files (such as the registry) and can be modified if files are moved.



Enable / Disable Function Keys on Boot Up (Windows 9x)

By default Windows 9x enables the function keys on boot, these allow you to control the boot process. For example pressing F5 while the "Starting Windows 95..." message is displayed will boot Windows in Safe Mode.



Change the Amount of Time that Function Keys are Available (Windows 9x)

By default Windows 9x enables the function keys on boot for 2 seconds, these keys allow you to control the boot process.



Control Whether the Windows 9x GUI is Loaded Automatically (Windows 9x)

By default Windows 9x automatically loads the GUI (or Windows Desktop) with this key you can control whether the GUI is loaded or if you just want the MS-DOS 7.0 prompt.



Display the Windows Splash Screen While Loading (Windows 9x)

When Windows is loading normally you see the Windows clouds splash screen, this can be disabled to show the background DOS boot process.



Allow Booting to the Previous Operating System (Windows 9x)

If you installed an upgrade version of Windows 9x, you can normally press F4 to boot your previous version of Windows. This option can be disabled.



Showing the Windows Boot Menu (Windows 9x)

By default Windows 9x does not show the boot menu unless you press F8. The boot menu allows you to boot Windows in different modes, including Safe Mode and Command Prompt Mode. You can configure the boot menu to be shown automatically on every boot.



Forces Your Computer to Boot in Safe Mode (Windows 9x)

This setting when enabled forces your computer to always boot in Safe Mode.



Suppress Safe Mode Warning Message (Windows 9x)

Enabling the setting suppress the safe mode warning message when booting up, and bypasses the Startup menu.



Control Windows Double Buffering Support (Windows 98)

Windows 98 includes double buffering support, some systems may have an incompatibility between the computer's BIOS and the Dblbuff.sys file.



Loading Double / Drive Space Compression into Low Memory (Windows 9x)

A setting of 0 does not let Windows 95 load COMMAND.COM or DRVSPACE.BIN/DBLSPACE.BIN at the top of 640K. If you are having compatibility problems with software that makes assumptions about the available memory try setting this to 0.

Source: C:/helpfile/Files/MSDOS_SYS/index.shtml - (13)

- RegEdit.com : Performance : File System -

Registry Keys:



Speed Up File System Caching *(Windows NT)*

If you have some extra RAM and an active file system, you can speed up file system activity by increasing the IoPageLockLimit from the default 512K bytes to 4096K bytes or more.



Configure the Contiguous File Allocation Size *(Windows 9x and NT)*

This setting optimizes the contiguous file allocation size for the file system. This is especially useful for disk intensive applications.



Disable 8.3 Name Creation (NTFS) *(Windows NT)*

This key stops the NTFS volume from generating MS-DOS compatible 8.3 file names. Disabling this feature can increase the performance on heavily used NTFS partitions that have large amount of files with long filenames.



Increase NTFS Peformance by Disabling the Last Access Time Stamp *(Windows NT)*

When Windows NT lists a directory (Explorer, DIR command, etc.) on an NTFS volume, it updates the LastAccess time stamp on each directory it detects. If there are a very large number of directories, this can affect performance.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Performance/File_System/index.shtml - (14)

- RegEdit.com : Performance : Network and Internet -

Registry Keys:



Optimizing the DefaultRcvWindow & DefaultTTL Settings (Windows 9x)

The optimization of RcvWindow and DefaultTTL along with other registry settings such as MaxMTU and MaxMSS can speed up TCP/IP modem networking connections (eg. Internet connections).



Optimizing Dial-Up Modem Connection Speed (Windows 9x)

By optimizing the MaxMTU & MaxMSS settings along with the RWIN and TTL settings you can increase dialup modem connection reliability and performance by as much as 200%.



Increase Network Performance (Windows NT)

If you increase the number of buffers that the redirector reserves for network performance, it may increase your network throughput. Each extra execution thread that you configure will take 1k of additional nonpaged pool memory, but only if your applications actually use them.



Optimize Windows NT TCP/IP Data Retransmissions (Windows NT)

This parameter controls the number of times TCP will retransmit an individual data segment (not connection request segments) before aborting the connection.



Change the Maximum Transmission Unit (MTU) Size (Windows NT)

By optimizing the MTU setting you can gain substantial network performance increases, especially when using dial-up modem connections.



Optimize Windows NT TCP/IP Connection Retransmissions (Windows NT)

This parameter determines the number of times TCP will retransmit a connect request (SYN) before aborting the attempt. The retransmission timeout is doubled with each successive retransmission in a given connect attempt.



Optimize the Windows NT TCP/IP Window Size (Windows NT)

This parameter determines the maximum TCP receive window size offered by the system. The receive window specifies the number of bytes a sender may transmit without receiving an acknowledgment.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Changing the Menu Show Delay -

Detailed Information:



Changing the Menu Show Delay (*Windows 9x and NT*)

Windows normally delays menus before they are shown. For regular users this delay can become annoying, with this setting you to change the delay or remove it altogether.

Open your registry and find the key below. Modify the value of 'MenuShowDelay' according to the delay you would like before the menus are shown (the value is time in milliseconds).

If the value doesn't already exist, then simply create a new string value and name it 'MenuShowDelay'.

Note: *You may need to restart Windows for the changes to take affect.*

Key: [HKEY_CURRENT_USER\Control Panel\Desktop]

Value Name: MenuShowDelay

Data Type: REG_SZ

Data: 0-999 (milliseconds)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Control the Windows Animation Function -

Detailed Information:



Control the Windows Animation Function (*Windows 9x and NT*)

Although the Windows animation function, can look good it can slow down your PC if you have a slower graphics card. This settings allows you to control the Windows animation function.

Open your registry and change the value of 'MinAnimate' found in the key below, set the value to '0' for disabled or '1' for enabled.

If the value doesn't already exist simply create a new string value and name it 'MinAnimate'.

Key: [HKEY_CURRENT_USER\Control Panel\Desktop]

Value Name: MinAnimate

Data Type: REG_SZ

Data: (0=disable, 1=enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/19.html - (17)

- Optimizing L2 Caches Over 256K -

Detailed Information:



Optimizing L2 Caches Over 256K (*Windows NT*)

Windows NT by default is optimized for a 256K size L2 cache. With most computers now having L2 caches larger than 256K it pays to take the time to change the SecondLevelDataCache setting to correspond to the size of the L2 cache installed.

1. Using Regedit open the key below.
2. Find the value named 'SecondLevelDataCache', double-click to modify.
3. Click the 'Decimal' radio button, and enter your L2 cache size in Kb's.
4. Exit Regedit and reboot.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]

Value Name: SecondLevelDataCache

Data Type: REG_DWORD

Data: Cache (in Kb) using Decimal Notation

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/116.html - (18)

- Control Whether Windows Performs Smooth Scrolling -

Detailed Information:



Control Whether Windows Performs Smooth Scrolling (Windows 9x and NT)

This setting allow you to disable the Windows smooth scrolling function, which on an low-powered system can cause performance degradation.

1. Using RegEdit find the key below.
2. Modify the value of 'SmoothScroll' to either '00 00 00 00' for disabled, or '01 00 00 00' for enabled. If the value doesn't already exist create a new REG_BINARY value, naming it 'SmoothScroll'.

Key: [HKEY_CURRENT_USER\Control Panel\Desktop]

Value Name: SmoothScroll

Data Type: REG_BINARY

Data: (00 00 00 00 = disabled, 01 00 00 00 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/121.html - (19)

- RegEdit.com : Security : Applications -

Categories:



[DOS](#)

MS-DOS and Windows 3.x Application Restrictions



[Internet Explorer](#)

Internet Explorer Security Restrictions

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Applications/index.shtml - (20)

- RegEdit.com : Security : Control Panel -

Categories:



[Display](#)

Display Properties Restrictions



[Printers](#)

Printer Properties Restrictions



[Network](#)

Network Properties Restrictions



[System](#)

System Properties Restrictions



[Passwords](#)

Password Properties Restrictions

Registry Keys:



[Deny Access to the Display Settings](#) (*Windows 9x and NT*)

This option disables the display settings control panel icon, and stops users from accessing any display settings.



[Disable Network Control Panel](#) (*Windows 9x*)

Enabling this option disables access to the Network Control Panel icon.



[Disable Printers Control Panel Icon](#) (*Windows 9x*)

This option disables access to the Printers icon in control panel, therefore stopping users from changing Printer settings.



[Restrict Access to the Passwords Control Panel](#) (*Windows 9x*)

This options disables access to the Passwords icon on the the control panel, therefore stopping users from changing security related settings.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Control_Panel/index.shtml - (21)

- RegEdit.com : Security : Explorer -

Registry Keys:



Disable the Shut Down Command *(Windows 9x and NT)*

This option allows you to stop users from being able to shutdown the computer, by disabling the shut down command.



Remove common program groups from Start menu *(Windows 9x and NT)*

Disables the display of common groups when the user selects Programs from the Start menu.



Hide All Items on the Desktop *(Windows 9x and NT)*

Enabling this options hides all the items and programs on the Windows desktop.



Hide Drives in My Computer *(Windows 9x and NT)*

This setting controls which drives are visible in 'My Computer', it is possible to hide all drives or just selected ones.



Remove the Favorites Folder from the Start Menu *(Windows 9x and NT)*

To remove the Favorites folder from the Start menu, modify this registry key.



Remove File menu from Explorer *(Windows NT)*

Removes the File option from Explorer's toolbar. (This option was added in Service Pack 2.)



Remove the Find Command From the Start Menu *(Windows 9x and NT)*

When enabled, this setting removes the 'Find' command from the Start Menu.



Hide the Network Neighborhood Icon *(Windows 9x and NT)*

The Network Neighborhood icon is shown on the Windows desktop whenever Windows networking is installed, by enabling this setting the icon will be hidden.



Remove the Documents Folder from the Start Menu *(Windows 9x and NT)*

This key will remove the recent Documents folder from the Start Menu.



Remove the Run Command from the Start Menu *(Windows 9x and NT)*

Removes the user's ability to start applications or processes from the Start menu by removing the option completely.



Save Explorer Window Settings *(Windows 9x and NT)*

With this function you can control whether your desktop settings will be saved when you exit Windows.



Don't Save Settings at Exit *(Windows 9x and NT)*

Normally when Windows exits it saves the desktop configuration, including icon location, appearance etc. This setting disables these changes from being saved, this is useful in both a secure environment and when you don't want people to change the appearance of your desktop once you have it setup the way you like it.



Remove Folders from Settings on the Start Menu *(Windows 9x and NT)*

Removes the Control Panel and Printers folders from the Settings menu. Note: Removing the Taskbar, Control Panel, and Printer folders causes the Settings menu to be removed completely.



Remove the Taskbar from Settings on the Start Menu *(Windows 9x and NT)*

Enabling this option, removes the Taskbar option from Settings on the Start Menu, therefore stopping users from changing the taskbar properties. Note: Removing the Taskbar, Control Panel, and Printer folders causes the Settings menu to be removed completely.



Disable context menus for the Taskbar *(Windows NT)*

Removes the context menus for the tray, including the Start button, Tab control, and Clock. (This option was added in Service Pack 2.)



Disable Explorer's default context menu (Windows NT)

Removes the context menu that would normally appear when the user right clicks on the desktop or in the Explorer right results pane. (This option was added in Service Pack 2.)



Restricting Applications Users Can Run (Windows 9x and NT)

Windows gives the ability to restrict the applications that can be run by users on a workstation.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Explorer/index.shtml - (22)

- RegEdit.com : Security : Network -

Categories:



[Remote Access](#)

Remote Access Security Settings

Registry Keys:



[Disable File and Printer Sharing](#) (Windows 9x and NT)

When 'File and printer sharing...' is installed it allows users to make services available to other users on a network, this functionality can be disabled by changing this setting.



[Automatic Hidden Shares](#) (Windows NT)

This key controls whether the administration shares are created ie. c\$ and d\$. Set AutoShareServer to "0" to disable admin shares for a server. Set AutoShareWks to "0" to disable admin shares for a workstation.



[Disabling Save Password option in Dial-Up Networking](#) (Windows NT)

When you dial a phonebook entry in Dial-Up Networking (DUN), you can use the 'Save Password' option so that your DUN password is cached and you will not need to enter it on successive dial attempts. This key disables that option.



[Don't Display Last User Name](#) (Windows NT)

Enabling this key will blank the username box on the logon screen. Preventing people that are logging on from knowing the last user on the system.



[Sending Unencrypted Passwords](#) (Windows NT)

Connecting to SMB servers (such as Samba and LAN Manager for UNIX) with an unencrypted (plain text) password fails after upgrading to Windows NT 4.0 Service Pack 3. This is because the SMB redirector in Service Pack 3 handles unencrypted passwords differently than previous versions of Windows NT. Beginning with Service Pack 3, the SMB redirector will not send an unencrypted password unless you add a registry entry to enable unencrypted passwords.



[Hiding Servers from the Browser List](#) (Windows NT)

If you have a secure server or workstation you wish to hide from the general browser list, add this registry setting.



[Hide Share Passwords with Asterisks](#) (Windows 9x and NT)

This setting controls whether the password typed when accessing a file share is shown in clear text or as asterisks.



[Changing LAN Manager Authentication on Windows NT](#) (Windows NT)

Windows NT supports two kinds of challenge/response authentication: LanManager (LM) and Windows NT (NTLM). LM authentication is not as strong as Windows NT authentication so some customers may want to disable its use, because an attacker sniffing the network traffic could attack the weaker protocol.



[Setting a Minimum Password Length](#) (Windows 9x and NT)

You can force Windows to reject passwords that do not meet a minimum password length. Useful to help stop people from using trivial passwords where security is an issue.



[Require Validation by Network for Windows Access](#) (Windows 9x)

By default Windows doesn't require a valid network username and password combination for a user to create and use a local Windows machine. This functionality can be change to require validation by the network.



[Disable Caching of Domain Password](#) (Windows 9x and NT)

Enabling this setting, disables the caching of the NT domain password, and therefore it will need to be re-entered to access additional domain resources.



[Defining Local and Remote Drive Visibility Under WinNT](#) (Windows NT)

Administrators may use the NODRIVES entry to disable access to floppy drives on a per-user basis. The NODRIVES entry uses a 32-bit word to define local and network drive visibility for each logical drive in the computer. The lower 26 bits of the 32-bit word correspond to drive letters A through Z. Drives are visible when set to 0 and hidden when set to 1.



Remove Entire Network from Network Neighborhood (Windows 9x and NT)

Entire Network is an option under Network Neighborhood that allows users to see all the Workgroup and Domains on the network. Entire Network can be disabled, so users are confined to their own Workgroup or Domain.



Remove Log Off <Username> from the Start Menu (Windows 9x and NT)

To remove the Log Off <Username> command from the Start menu, use Registry Editor to modify the following key.



Remove the Map and Disconnect Network Drive Options (Windows NT)

Prevents users from making additional network connections by removing the Map Network Drive and Disconnect Network Drive buttons from the toolbar in Explorer and also removing the menu items from the Context menu of My Computer and the Tools menu of Explorer. (This option was added in Service Pack 2.)



Hide Workgroup Content from Network Neighborhood (Windows 9x and NT)

Enabling this option, hides all Workgroup content from being displayed in Network Neighborhood.



Changing the Default 14 day Password Expiry Warning (Windows NT)

This entry specifies the number of days that a warning message is displayed before the user's password expires.



Restricting Information Available to Anonymous Logon Users (Windows NT)

Windows NT has a feature where anonymous logon users can list domain user names and enumerate share names. Customers who want enhanced security have requested the ability to optionally restrict this functionality.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Security : System -

Registry Keys:



Restricting Access to the Event Logs (Windows NT)

The Windows NT event log contains records documenting application, security and system events taking place on the machine. These logs can contain sensitive data, and by default, the Guest account has access to view them. This tweak allows you to restrict access to administrators and system accounts only.



Secure Network Access to the Windows NT Registry (Windows NT)

Windows NT supports accessing a remote registry via the Registry Editor across a network. The default setting allows for users to connected and modify data within the remote registry.



Securing Network Access to CD-ROM Drives (Windows NT)

This setting determines whether data in the CD-ROM drive is accessible to other users. This value entry satisfies, in part, the C2 security requirement that you must be able to secure removable media.



Securing Network Access to Floppy Drives (Windows NT)

This setting determines whether data in the floppy disk drive is accessible to other users. This value entry satisfies, in part, the C2 security requirement that you must be able to secure removable media.



Require Alphanumeric Windows Password (Windows 9x and NT)

Windows by default will accept anything as a password, including nothing. This setting controls whether Windows will require a alphanumeric password, i.e. a password made from a combination of alpha (A, B, C...) and numeric (1, 2, 3 ...) characters.



Control the Automatic Restarting of the Shell (Windows NT)

By default if the Windows NT user interface or one of its components fails, the interface is restarted automatically, the can be changed so that you must restart the interface by logging off and logging on again manually.



Clear the Page File at System Shutdown (Windows NT)

Windows normally does not clear or recreate the page file. On a heavy used system this can be both a security threat and performance drop. Enabling this setting will cause Windows to clear the page file whenever the system is shutdown.



Disable the Change Password Button (Windows NT)

This setting disables the 'Change Password' button on the Windows NT Security dialog box. Enabling this setting stops casual users from being able to change the password.



Disable the Lock Workstation Button (Windows NT)

Add this setting to the registry to stop unauthorized users from locking machines from the Windows NT Security dialog box.



Disabled Password Caching (Windows 9x and NT)

Normally Windows caches a copy of the users password on the local system to allow for additional automation, this leads to a possible security threat on some systems. Disabling caching means the users passwords are not cached locally. This setting also removes the second Windows password screen and also remove the possibility of networks passwords to get out of sync.



Disable Registry Editing Tools (Windows 9x and NT)

This setting disables user's ability to run Regedit.exe or Regedt32.exe to modify the registry.



Disable Task Manager (Windows NT)

Enables or disables the user's ability to start Task Manager to view processes, applications running, and make changes to the priority or state of the individual processes. (This option was added in Service Pack 2.)



Legal Notice Dialog Box Before Logon (Windows 9x and NT)

Use these fields to create a dialog box that will be presented to any user before logging onto the system. This is useful where you are required by law to warn people that it is illegal to attempt to logon without being an authorized user.



Change the Message Shown on the Logon Box (Windows NT)

You can personalize (or legalize) the message displayed on the logon box above the user name and password.



Determines which drives the Autorun feature is enabled on (Windows 9x and NT)

Determines whether the Autorun feature is enabled on each drive connected to the system. When Autorun is enabled, media is started automatically when it is inserted in the drive.



Stopping the KnownDLLs Vulnerability (Windows NT)

In Windows NT, core operating system DLLs are kept in virtual memory and shared between the programs running on the system. This has exposed a vulnerability that could allow a user to gain administrative privileges on the computer the user is interactively logged onto.



Preventing the Logon Screen Saver from Launching (Windows NT)

Windows NT has a default screen saver called login.scr, which runs even if no screen saver has been selected. This can present a security risk, as it can allow a local user to replace login.scr with another program and have it launched with system privileges.



Enable Shutdown from Authentication Dialog Box (Windows NT)

When this setting is enabled, you can click 'Shutdown' from the authentication dialog box when the system first starts without having to log in.



Specify executable files to be run by Winlogon (Windows NT)

This setting Specifies executable files to be run by Winlogon in the system context, and can be modified by simply editing the value.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Tips and Tricks : Windows 9x -

Registry Keys:



Order the Menu

It's easy to reorder the items on any Win98 cascading menu by holding down the mouse button and drag a highlighted file or folder up or down the list. With this tip it's even easier to force the entire list into permanent alphabetical order.



Speed Up ISP Logon Time (Windows 9x)

On some systems it can take a long time to connect to the Internet, you can decrease the time required to connect to your ISP by trying these simple steps.



Faster Modem Dialing (Windows 9x)

Waiting to long for your modem to dial? This tip lets you reduce the time it takes your modem to dial, and increase your overall modem connection speed.



Restart Windows Quickly without Rebooting (Windows 9x)

Tired of waiting for Windows to restart? Sometimes it can take ages to completely shutdown, then your have to wait for the PC to reset as well. Try this tip to speed up your computer's shutdown procedure.



Change the Startup and Shutdown Screens (Windows 9x)

Microsoft has a nack for making the Windows startup and shutdown screens pretty boring. Luckily it's relatively easy to replace these images with pictures of your own.



Make Windows Start Without Asking for a Password (Windows 9x)

Does Windows prompt you for a password every time you boot up even though you're the only one using the PC? Follow these instructions to make Windows automatically start up without prompting you for a password.



Re-Initailize Your Registry Without Rebooting (Windows 9x)

Some registry changes require you to restart Windows before they are enabled. This tip lets you reinitialize your registry and refresh your desktop without having to leave Windows.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Tips_and_Tricks/Windows_9x/index.shtml - (25)

- RegEdit.com : Tips and Tricks : Windows NT -

Registry Keys:



[View Which HotFix Patches Have Been Installed](#) *(Windows NT)*

Periodically Microsoft releases HotFix's to patch bugs in Windows NT and other products, this key contains information about which Hotfix's have been installed.



[Removing Windows NT Devices and Services](#) *(Windows NT)*

Sometimes it is possible to get orphaned services remaining in the registry. These services can be removed by modifying this key.



[Reduce the Time the Startup List is Shown on Boot](#) *(Windows NT)*

30 Seconds is a long time when you're waiting for Windows NT to boot. With this tip you can decrease the time the system waits for a selection, or remove the time-out all together.



[Change Directories Without Typing the Whole Name](#) *(Windows NT)*

Changing directories at the command prompt can be a hit and miss process when long filenames are involved. This tip let you change directories with ease, not matter how long the directory name.



[Launch the Task Manager Quickly](#) *(Windows NT)*

Launching the Task Manager can sometimes be difficult depending on the situation. Some people didn't know that the Task Manager can actually be launched in at least three different ways to make it easier to use when you need it the most.



[Enable Plug-and-Play on Windows NT](#) *(Windows NT)*

By default Windows NT 4.x doesn't support plug-and-play devices, but it can be configured to at least partially support them with a little help.



[Change System Environment Variables](#) *(Windows NT)*

This key contains the Windows NT system environment variables, variables include Path, Temp, Windir and any other defined values.



[Changing the Behaviour of the Dr. Watson Utility](#) *(Windows NT)*

By default whenever an application error occurs under Windows NT, Dr. Watson is launched and the debugger started automatically. The extra resources needed for the debugger can sometimes push the system over the edge. It is possible to stop the debugger from launching by changing this setting.



[Disable Automatic Cache Updates in NT's DNS Server](#) *(Windows NT)*

This value disables that automatic cache updated from the DNS root servers. Useful when there is a problem with the root servers, or if you wish to completely control DNS updates.



[Change Background Color During Logon](#) *(Windows NT)*

Change the default background color of the logon screen.



[Configuring Unimodem Support](#) *(Windows NT)*

Windows NT 4.0 and greater support Unimodem modems, if your device is not supported though Windows can be configured to use the MODEM.INF file instead.



[Remove the Tildes in Short Filenames](#) *(Windows 9x and NT)*

The setting removes the tildes "~" from short filenames.



[Stop Error Messages When Booting](#) *(Windows NT)*

Stops the annoying Windows pop-up messages notifying you a device is not functioning when you boot-up Windows NT.



Define Whether Windows Parses Autoexec.bat (Windows NT)

When this value is 1, the environment variables declared in the Autoexec.bat file are included in the user's environment.



Suppress the 'domain controller can not be reached' Message (Windows NT)

If Windows is unable to contact a domain controller when a user logs in a message is displayed, this message can be suppressed by modifying this setting.



PS2 Mouse Port Rate Adjustment (Windows NT)

Ever noticed how your mouse cursor flickers sometimes, or doesn't run as smoothly as a mouse cursor on a Macintosh? That's because the refresh rate is set too low, modify this key to speed things up and make your mouse cursor move smoothly.



Changing the Startup Mode of a Service (Windows NT)

All services have a setting controlling how they are started, i.e. manually, automatically or disabled. This setting can be changed through the registry.

Related Categories:

- [Enhancements : Windows : NT](#)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Tips_and_Tricks/Windows_NT/index.shtml - (26)

- Automatically View Thumbnails of Bitmap Files -

Detailed Information:



Automatically View Thumbnails of Bitmap Files (*Windows 9x and NT*)

Makes Explorer show a thumbnail version of bitmaps files in the current folder rather than the generic icon ordinarily used. This is a great way to preview .BMP files without having to open them first.

Find the key below and modify the value of (Default) to equal '%1'.

Key: [HKEY_CLASSES_ROOT\Paint.Picture\DefaultIcon]

Value Name: (Default)

Data Type: REG_SZ

Data: %1

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/29.html - (27)

- Enable Live Scrolling in Microsoft Word -

Detailed Information:



Enable Live Scrolling in Microsoft Word (*Windows 9x and NT*)

Normally when you move through a Word document using the scroll bar the page doesn't update until you release the mouse button. With this tweak the document location is updated as you move.

Open your registry and find the key below.

Create a new string value named 'LiveScrolling', or modify the existing value, to equal '1' for live scrolling enabled or '0' for disabled. Close the registry and restart Word.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Office\8.0\Word\Options]

Value Name: LiveScrolling

Data Type: REG_SZ

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/228.html - (28)

- Change the Location of System and Special Folders -

Detailed Information:



Change the Location of System and Special Folders (*Windows 9x and NT*)

Windows keeps a number of special folders such as "My Documents", "Desktop", "Favorites" and the "Start Menu". These folders can be moved anywhere on your system and the new location updated in this key.

1. Using Regedit open the key below, listed are all the special folders Windows uses.
2. Note the current location of the folder you want to move, and then using explorer move the folder to the new location.
3. Edit the value in the key below for the folder you moved to reflect the new directory location.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/107.html - (29)

- Expand and Contract Folders With Ease -

Detailed Information:



Expand and Contract Folders With Ease (*Windows 9x and NT*)

It can be a time-consuming process to expand a folder by clicking on the (+) for each and every sub-directory. This tip lets you expand and contract them all at once, with one keystroke.

While in any application that is based on the explorer interface (e.g. Windows Explorer) simply highlight the parent folder you wish to expand and press '*' (asterix on the keypad) and all the sub folders will expand out, press '-' (minus on the keypad) and they'll all contract back again.

Hint: *This works in regedit.exe as well!*

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/242.html - (30)

- Launching Programs When Windows Starts -

Detailed Information:



Launching Programs When Windows Starts (*Windows 9x and NT*)

You can automatically start programs whenever Windows launches. If you have programs automatically starting that you have not loaded then you can remove them using this tip as well.

1. Open your registry and find the key below.
2. For each program you wish to start automatically create a new string value using a descriptive name, and set the value of the string to the program executable.

For example, to automatically start Notepad, add a new entry of "Notepad"="c:\windows\notepad.exe".

Note: Remember to include the full path to the file, if the directory is not included in your default search path.

If you're trying to remove a program and can not find it in the default key, then additionally try these keys as well:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit]
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows]
```

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Avoid Accidental Registry Imports -

Detailed Information:



Avoid Accidental Registry Imports (*Windows 9x and NT*)

By default, if you double-click on a file with a '.REG' extension the file will be imported into the system registry. You can change the default so it opens the file for editing instead.

From either Explorer or My Computer click on View | Options, then the 'File Types' tab. Scroll down the list of registered file type until you find 'Registration Entries', highlight it and click 'Edit'. Listed in the 'Actions' box should be three actions: Edit, Merge and Print. Highlight 'Edit' and click 'Set Default', Edit should become **Bold**.

Next time you double-click on a .REG file, notepad should open instead. You can still import a file by simply right-click on it and select 'Merge'.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/253.html - (32)

- Removing Item Types from the New Menu -

Detailed Information:



Removing Item Types from the New Menu (*Windows 9x and NT*)

When you right-click on your desktop or other selected applications there is a *New* sub-menu which contains a list of default templates. This list can be modified to include only the templates you want.

Each template exists in the [HKEY_CLASSES_ROOT] hive associated with a file extension. Whether it is visible or not in the *New* menu is controlled by whether the related entry has a sub-key called 'ShellNew'.

For example on the *New* menu there is usually an entry for "Text Document". This is visible because of the key: [HKEY_CLASSES_ROOT\.txt\ShellNew] If you were to rename the key so it no longer had a sub-key called 'ShellNew' by changing it to [HKEY_CLASSES_ROOT\.txt\ShellNewOld] it would disappear from the *New* menu.

1. Open Regedit, and using the *Find* function (Ctrl+F) search for any values of 'ShellNew'.
2. Several should be found under the [HKEY_CLASSES_ROOT] hive, if you do not want them to be displayed rename 'ShellNew' to 'ShellNewOld'.

Note: *Changes should take place immediately without needing to reboot.*

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Close Parent Windows Automatically -

Detailed Information:



Close Parent Windows Automatically (*Windows 9x and NT*)

Have you ever had a screen full of explorer windows on your desktop after digging through heaps of directories? This tip lets you close the current window and all its parent windows in one easy step.

To close a folder and all its open parent folders, simply press the SHIFT key while clicking on its Close box or alternatively press ALT + SHIFT + F4.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/241.html - (34)

- Including Manufacturer and Support Details -

Detailed Information:



Including Manufacturer and Support Details (*Windows 9x and NT*)

This tip lets you include a company logo and contact information in the System Properties dialog box. This is especially useful if you run a computer store and want your customers to be reminded where they bought their PC and where to get technical support.

To add the manufacturer and support information you need to create two new files in the Windows system directory, normally 'c:\windows\system' for Windows 9x and 'c:\winnt\system32' for Windows NT.

The first file is a text file called 'OEMINFO.INI'. To create the file open notepad and copy the template below, make any changes and save the file in the System directory.

OEMINFO.INI Template

```
[General]
Manufacturer=Enter the Company Name Here
Model=Enter the Computer Model Name Here
[Support Information]
Line1=first line of support information
Line2=second line
Line3=third line
Line4=fourth line
; Create as many lines as you need by incrementing the Line number
```

The other file you need to create is a logo file. This is a standard Windows bitmap file, but it must be saved as 'OEMLOGO.BMP' in the System directory.

Once you've created both these files, open System Properties from Control Panel, and your logo and company name will be listed. The details you entered in the [Support Information] section will show up when you click on the Support Information button.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Default Name and Company Information -

Detailed Information:



Default Name and Company Information (*Windows 9x and NT*)

When you install a new application, using MS Setup, a default Name and Company are shown, these values can be changed when the details have changed or are incorrect.

1. Using Regedit open the key below.
2. Modify the two values of 'DefName' and 'DefCompany', and change the values to your current Name and Company respectively.
3. Next time you install a program these new values will be used.

Note: *This will not affect the registered names of existing applications, it only affects new installations.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\MS Setup (ACME)\User Info]

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Add Your Own Tips -

Detailed Information:



Add Your Own Tips (Windows 9x and NT)

Are you sick of seeing the same tips again and again when you first logon to Windows? Now you can change them to whatever you want, whether it's quotes, jokes or a to-do list, anything is possible.

Simply open your registry and find the key below.

To create a new tip, click on Edit | New | String Value and name the value by incrementing the existing values. Double click on your newly created entry and enter any text you want.

To delete, simply highlight the enter and either hit the <Delete> key or choose Edit | Delete.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Tips]

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/223.html - (37)

- Make the Columns Fit -

Detailed Information:



Make the Columns Fit (*Windows 9x and NT*)

Want to quickly see all the column in explorer without having to resize them individually? This tip does it for you.

Simple press CTRL + + (press the plus button twice on the numeric keypad), this will adjust the column width so you can view the info in each column.

This tip may also work with programs based on the Windows explorer interface. Try it out!

Note: *You may have to expand the window borders to see all the columns.*

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/240.html - (38)

- Removing Icons from your Desktop -

Detailed Information:



Removing Icons from your Desktop (*Windows 9x and NT*)

This key contains a number of subkeys which hold information about the namespace extensions of icons on your desktop. Through this key you can control which icons are visible on the desktop, including the My Computer, Inbox, MSN and Internet icons.

The name of each key is a globally unique identifier (GUID), and the default value of each key is a human-readable name for the namespace extension, although this is not the same name as the icon on the desktop.

To delete an icon from your desktop:

1. Step through the subkeys until you find the key representing the icon you want to remove from your desktop, delete the key and the icon should disappear.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Creating a Shortcut to the System Folders -

Detailed Information:



Creating a Shortcut to the System Folders (*Windows 9x and NT*)

This function allow you to add a shortcut to various system folders on your Desktop or Start Menu.

Create a new folder on your desktop and name it "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" It should look like the normal Control Panel icon (not a shortcut). You can now move the icon anywhere on your desktop or start menu.

The same can be achieved for others by substituting these values:

For Dial Up Networking

Dial-Up Networking.{992CFFA0-F557-101A-88EC-00DD010CCC48}

For Printers

Printers.{2227A280-3AEA-1069-A2DE-08002B30309D}

For Control Panel

Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}

My Computer

My Computer.{20D04FE0-3AEA-1069-A2D8-08002B30309D}

For Network Neighborhood

Network Neighborhood.{208D2C60-3AEA-1069-A2D7-08002B30309D}

For the Inbox

InBox.{00020D75-0000-0000-C000-000000000046}

For the Recycle Bin

Recycle Bin.{645FF040-5081-101B-9F08-00AA002F954E}

For more check out the HKEY_CLASSES_ROOT\CLSID key.

Key: [HKEY_CLASSES_ROOT\CLSID]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Desktop Icon Redraw Frequency -

Detailed Information:



Desktop Icon Redraw Frequency (*Windows 9x and NT*)

If you desktop icons are redrawing too frequently, change this setting.

Try editing:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer

Add Value of "Max Cached Icons" with type REG_SZ. Set it to "8000".

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer]

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/57.html - (41)

- Remove Cached Command Lines from the Run Menu -

Detailed Information:



Remove Cached Command Lines from the Run Menu (*Windows 9x and NT*)

Got a lot of items in the Start Menu's run command history? This tip will allow you to remove any extraneous commands.

Delete the value corresponding to the command you want to remove, or remove all the entries to clear the list completely.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/76.html - (42)

- Add the QuickView Option to All Files -

Detailed Information:



Add the QuickView Option to All Files (Windows 9x and NT)

If you ever wanted to add QuickView to the context menu of all file types, it may be a tedious task doing so using Windows Explorer's Options - File Type window. This tip shows how to do it in a couple of easy steps.

Open your registry and create a sub-key called QuickView under [HKEY_CLASSES_ROOT*].

Change the (Default) value of the new sub-key to equal '*'.

Close the registry and open an Explorer window. Right-click on any file and the QuickView command should now appear.

Note: You need to have QuickView installed on your PC. If not, Go to Control Panel, Add/Remove Programs and add it from the Accessories group in the Windows Setup tab.

Key: [HKEY_CLASSES_ROOT*\QuickView]

Value Name: (Default)

Data Type: REG_SZ

Data: *

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/115.html - (43)

- Change the Recycle Bin Icons -

Detailed Information:



Change the Recycle Bin Icons (*Windows 9x and NT*)

Would you like to make you Recycle Bin into something a bit more exciting? Maybe a glowing toxic waste bin? With this tweak you can change the icon to be whatever you like.

Open you registry and find the key below.

Within the key are three values: '(Default)', 'Empty' and 'Full'. Set the values to equal the icon you'd like to display for the various states of the Recycle Bin.

Note: *These changes should take place immediately, you may need to refresh your desktop by clicking on a blank area and pressing F5.*

Key: [HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\DefaultIcon]

Value Name: (Default), Empty, Full

Data Type: REG_SZ

Data: Path to Icon File

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/291.html - (44)

- Remove the Arrow from Shortcuts -

Detailed Information:



Remove the Arrow from Shortcuts (*Windows 9x and NT*)

Would you prefer to show your shortcuts without the arrow in the bottom left hand corner? This tip will show you how to change the arrow icon or remove it completely.

Open your registry and find the key below.

Create a new string value called '29', or modify the exist value, so that the data equal the icon you want to use for the shortcut arrow. If you don't want an icon simply leave the value blank. **Note:** *Restart your computer for the changes to take effect.*

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Icons]

Value Name: 29

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/75.html - (45)

- Rename or Delete Special Folders -

Detailed Information:



Rename or Delete Special Folders (Windows 9x and NT)

This setting allows you to rename and delete special folders (such as the Recycle Bin) as if it was a normal folder by right-clicking the icon.

Set the value of "Attributes" in the appropriate key below to "70 01 00 20", you will then be able to rename and/or delete any special folders by right-clicking them.

Recycle Bin

[HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\ShellFolder]

Search the [HKEY_CLASSES_ROOT\CLSID] key for any other folders you want to modify.

Value Name:

Attributes

Data Type: REG_BINARY

Data: (70 01 00 20=enable, 40 01 00 20=default)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Add Custom Folder to My Computer or the Desktop -

Detailed Information:



Add Custom Folder to My Computer or the Desktop (*Windows 9x and NT*)

Create your own custom system folder on the desktop or in My Computer, that can't be deleted or renamed.

Add the following series of keys and values to the registry at ([HKEY_CLASSES_ROOT\CLSID] or [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID]). The entry can be a random number. In this example 'FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345'

```
[HKEY_CLASSES_ROOT\CLSID\{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}]
@='My Menu'
```

```
[HKEY_CLASSES_ROOT\CLSID\{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}\DefaultIcon]
@='c:\winnt\myicon.ico'
```

```
[HKEY_CLASSES_ROOT\CLSID\{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}\InProcServer32]
@='shell32.dll'
'ThreadingModel'='Apartment'
```

```
[HKEY_CLASSES_ROOT\CLSID\{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}\Shell\Open My Menu\
Command]
@='"c:\winnt\explorer /n /root,c:\MyFolder"
```

```
[HKEY_CLASSES_ROOT\CLSID\{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}\ShellEx\PropertySheetHandler\
{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}]
```

```
[HKEY_CLASSES_ROOT\CLSID\{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}\ShellFolder]
"Attributes"=hex:00,00,00,00
```

To place the folder (which is now a system folder) on the desktop and in My Computer, add the following keys:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\
{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\NameSpace\
{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}]
```

The folder cannot be deleted from the desktop or My Computer, nor can it be renamed other than removing the CLSID and the entries under NAMESPACE.

Key: [HKEY_CLASSES_ROOT\CLSID]

Value Name: CLSID

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Full Window Drag Option -

Detailed Information:



Full Window Drag Option (Windows 9x and NT)

This setting enables the Full Windows Drag function, which allow you to view the contents of window while dragging it across the screen, instead of just the standard outline.

Open your registry and find the key below.

Create a new string value named 'DragFullWindows', or modify the existing value, to equal '1' for enabled, or '0' for disabled.

Close the registry and restart Windows.

Key: [HKEY_CURRENT_USER\Control Panel\Desktop]

Value Name: DragFullWindows

Data Type: REG_SZ

Data: (0=disable, 1=enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Removes the Start Banner on the Taskbar -

Detailed Information:



Removes the Start Banner on the Taskbar (Windows 9x and NT)

Hides the arrow and "Click here to start" caption that appears on the taskbar when you start Windows.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoStartBanner

Data Type: REG_BINARY

Data: (00 00 00 00 = disabled, 01 00 00 00 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/155.html - (49)

- Changing the Registered Owner and Organisation -

Detailed Information:



Changing the Registered Owner and Organisation (*Windows 9x and NT*)

If you entered the wrong registration information when you installed Windows you can change it and other miscellaneous settings such as ProductID and ProductName.

Using Regedit, open the key appropriate for your operating system:

Windows 9x:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion]

Windows NT:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion]

Then modify the values of 'RegisteredOwner' and 'RegisteredOrganization'.

Value Name:

RegisteredOwner, RegisteredOrganization

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Change the Wallpaper Shown Prior to Logon -

Detailed Information:



Change the Wallpaper Shown Prior to Logon (*Windows 9x and NT*)

This key lets you change the wallpaper that appears prior to anyone logging in to the system.

1. Using Regedit, open the key below.
2. Modify 'Wallpaper' to equal the BMP you want to use as the background (e.g. 'c:\windows\mylogo.bmp').
3. Reboot your PC for the changes to take affect.

Note: *In the same key, you should also be aware of, and possibly set: "Pattern"="(None)" "TileWallpaper"="0"*

Key: [HKEY_USERS\DEFAULT\Control Panel\Desktop]

Value Name: Wallpaper

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/103.html - (51)

- RegEdit.com : Troubleshooting : File System -

Registry Keys:



Use Asynchronous or Synchronous Buffer Commits (Windows 9x)

This setting changes function calls to the File-Commit API to return immediately back without checking the data has been correctly written to the disk drive. By default Windows uses synchronous buffer commits, this setting allows you to enable asynchronous as an alternative for applications that may need this functionality.



Control Write Behind Caching (Windows 9x)

For increased performance write behind caching is used to write data to the fixed disks, this means that in the event of a system failure there is a possibility that data would not be completely written to the disk. If you have a system critical application you can disable this functionality to be sure that data is written directly to the disk bypassing the cache.



Configure 32-bit Protected Mode IO Drivers (Windows 9x)

This setting controls whether fixed disk access is performed through Windows protected mode drivers or through real mode drivers and BIOS routines. If you are experiencing drive IO errors enabling this setting may be a possible solution.



Preserving Long Filenames for Legacy Applications (Windows 9x)

Windows normally preserves the long filenames of files accessed by legacy applications. This functionality can be disabled if you are experiencing LFN errors with a legacy application.



Configure New File Sharing and Locking Symantics (Windows 9x)

This setting controls the file locking mechanisms of Windows 9x, disable this setting only if you are currently experiencing problems with specific applications.



Configure Protected-Mode Hard Disk Interrupt Handling (Windows 9x)

This switch allows Windows to terminate interrupts from the hard disk controller, bypassing the ROM routine that handles these interrupts. Some hard drives might require that this setting be disabled in order for interrupts to be processed correctly. If this setting is disabled, the ROM routine handles the interrupts.



Turn On / Off Long Filename Support (Windows 9x and NT)

Windows 9x and NT introduced the use of long filenames on existing FAT partitions. Some legacy software maybe incompatible with this new filesystem, and may require the use of 8.3 filenames. Enabling this setting turn off long filename support.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Troubleshooting/File_System/index.shtml - (52)

- RegEdit.com : Troubleshooting : Logging -

Registry Keys:



Remote Access Service (RAS) Device Logging (Windows NT)

Creates a file called DEVICE.LOG in the %SYSTEMROOT%\SYSTEM32\RAS folder for information about commands that the modem is sending and errors that are reported. This file can be very useful in debugging RAS failures.



Remote Access Service (RAS) PPP Logging (Windows NT)

Creates a file called PPP.LOG in the %SYSTEMROOT%\SYSTEM32\RAS folder to help diagnose connectivity problems between a PPP server and a PPP client when one of the computers is a Windows NT Remote Access Service client.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Troubleshooting/Logging/index.shtml - (53)

- RegEdit.com : Troubleshooting : Windows Bugs -

Registry Keys:



[New Command Missing in Windows Explorer](#) (Windows 9x and NT)

After you install Internet Explorer with the Windows Desktop Update component you may notice that the New command is missing from the right-click context menu. This tip will help you fix the problem.



[Change the Default Mailbox Sound Setting](#) (Windows 9x and NT)

When you receive a new message, a sound may not be played even though "Play sound when new messages arrive" is enabled.



[Addition of New LAN Interface in RRAS Causes Event Message](#) (Windows NT)

When you install an additional network interface card (NIC) and the Routing and Remote Access Service (RRAS) is already installed, you receive an error 20101 in the System Log in Event Viewer.



[Shortcuts Created Resolve to UNC Paths](#) (Windows NT)

A Windows NT user may click a program's shortcut and be prompted to Enter Network Password, yet the properties of the shortcut indicate a relative path to the local computer.



[Windows 98 Problem - Long File Names Need to be Enabled](#) (Windows 98)

If you are receiving an error when installing Windows 98 that long file names need to be enabled in order for Windows 98 to install successfully try this.



[CD-ROM Does Not Run Automatically When Inserted](#) (Windows 9x)

When you insert a CD-ROM into the CD-ROM drive, it may not be run automatically, changing this registry key should correct the problem.



[Unable to Connect More Than 10 Clients](#) (Windows NT)

If you have a retail version of Windows NT server, and you are still unable to connect more than 10 users concurrently, then have a look at this tip.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Troubleshooting/Windows_Bugs/index.shtml - (54)

- MS-DOS Compatibility Mode Problems with PCI-IDE Controllers -

Detailed Information:



MS-DOS Compatibility Mode Problems with PCI-IDE Controllers (*Windows 9x*)

If your computer contains a PCI-IDE hard disk controller that employs serialization between the two IDE channels, this tip may help you resolve a MS-DOS compatibility mode problem in Device Manager.

To cause Windows to attempt to reinitialize the protected-mode IDE driver, remove the 'NoIDE' entry from the registry key below.

After you update the registry, restart Windows. Windows will then attempt to initialize the protected-mode driver for the controller.

If no problems are encountered, the file system and virtual memory will operate in 32-bit mode, and Device Manager will not display an exclamation point in a yellow circle for the IDE channels.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\IOS]

Value Name: NoIDE

More info: <http://support.microsoft.com/support/kb/articles/q151/9/11.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/288.html - (55)

- Removing Programs listed in the Add/Remove Programs Box -

Detailed Information:



Removing Programs listed in the Add/Remove Programs Box (*Windows 9x and NT*)

All Windows 9x or NT compatible programs must include an Uninstall program, sometimes though the program may get removed but entry in Add/Remove programs doesn't, from this key you can remove those orphaned entries.

Using Regedit open the key below. Under this key will be a number of sub-keys, each representing an installed application.

To see which application each sub-key represents, open it and there should be at least two values 'DisplayName' and 'UninstallString'. 'DisplayName' is the name used in the Add/Remove programs list, and 'UninstallString' is the program used to uninstall the application.

To remove a program from the list you can simple delete the sub-key representing that program.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- 'Failure Writing to the System Registry...' Error Message -

Detailed Information:



'Failure Writing to the System Registry...' Error Message (Windows 95)

When you run a setup program that was created using the Application Setup Wizard, you may receive an error message indicating the registry may be corrupt or you do not have the required permissions to write to the registry.

As the error message indicates, the problem may be due to a corrupt registry or incorrect permissions to write to the registry. In addition, the problem occurs on computers running Windows 95 when the Setup program tries to add an entry to a registry key and the key will exceed 64K in size as a result. Registry keys are limited to 64K in Windows 95.

When the problem occurs on a Windows 95 computer, it usually happens when Setup tries to add entries to the key below.

Try running the RegClean utility provided by Microsoft, a link can be found at our [downloads page](#). Alternatively have a look at the Microsoft Knowledge Base article referenced below.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs]

More info: <http://support.microsoft.com/support/kb/articles/q186/8/97.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Has Your Taskbar Disappeared? -

Detailed Information:



Has Your Taskbar Disappeared? (*Windows 9x and NT*)

If your taskbar has disappeared from the desktop then it may be due to a corrupt registry key.

Open the registry and find the key below. Highlight the key and press the DELETE key to remove it from the registry.

Restart Windows to restore the taskbar.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StuckRects]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/277.html - (58)

- Are You Missing Fonts from the Fonts Folder? -

Detailed Information:



Are You Missing Fonts from the Fonts Folder? (Windows 9x and NT)

A font may seem to be installed correctly but does not appear in the Fonts folder because the Fonts key in the registry is missing or damaged.

Move the contents of the Fonts folder to an empty folder. By opening the Fonts folder, select all the fonts, copy them, and paste them to a new folder.

Open your registry and find the key below appropriate to your operating system. Highlight the key and press DELETE. Once the key has been deleted create a new key to replace it, by selecting Edit | New | Key and name the new key [Fonts].

Restart the computer, then re-install the fonts by opening the Control Panel, double-click on 'Fonts'. And from the File menu select 'Install New Fonts...' adding the fonts that were previously copied to the temporary directory.

Windows 95

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Fonts]

Windows NT

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts]

More info:

<http://support.microsoft.com/support/ntserver/serviceware/nts40/e9mskcv/q.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Delay Occurs When Unlocking Workstation -

Detailed Information:



Delay Occurs When Unlocking Workstation (Windows NT)

Sometimes a noticeable delay occurs when the logged on user or an administrator attempts to unlock a workstation. This because when you unlock the workstation Windows NT will update the domain list if the cached list's age exceeds two minutes (by default). This age limit can be modified.

1. Open the registry and find this key and value, if they don't exist already create them.
2. Modify the value of 'DcacheMinInterval' to equal the new cache time-out.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: DcacheMinInterval

Data Type: REG_DWORD

Data: 120-86400 (decimal) (expressed in seconds)

More info: <http://support.microsoft.com/support/kb/articles/q160/8/39.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Yellow '!' On PCMCIA Network Adapter -

Detailed Information:



Yellow '!' On PCMCIA Network Adapter (*Windows 9x*)

When using a PCMCIA network adapter under Windows 98 you might not be able to connect the computer to the network, and under Control Panel >System there is a yellow exclamation mark next to the card.

1. Click on START>RUN >
2. Type REGEDIT and click OK
3. Go to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VCOMM
4. Doubleclick on 'EnablePowerManagement' - change it to '0' based on the following:
 - If the current value is '0000 01 00 00 00' change it to '0000 00 00 00 00' (Full Version).
 - If the current value is '0x00000001 (1)' change it to '0x00000000 (0)' (Upgrade Version)
5. Close Registry Editor
6. Restart Windows

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VCOMM]

Value Name: EnablePowerManagement

Data: (0=disable, 1=enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/80.html - (61)

- Changing the Default State of the NUMLOCK Key -

Detailed Information:



Changing the Default State of the NUMLOCK Key (*Windows NT*)

The NUMLOCK key is usually only turned on before the user has logged into the computer, this can cause problem for people with portable computers that do not check the status of the NUMLOCK key before typing their password. The default behaviour can be changed with this setting.

1. Open your registry and find the key below.
2. Change the value of 'InitialKeyboardIndicators' to either '0' for off, or '2' for on.

Note: *This change will affect all users but value can also be changed on a user basis by modifying [HKEY_CURRENT_USER\Control Panel\Keyboard] and the same registry key.*

Key: [HKEY_USERS\DEFAULT\Control Panel\Keyboard]

Value Name: InitialKeyboardIndicators

Data Type: REG_SZ

Data: 0 = NUMLOCK off, 2 = NUMLOCK on

More info: <http://support.microsoft.com/support/kb/articles/q170/9/03.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Enhancements : Applications : Internet Explorer -

Registry Keys:



[How to Restore the Animated Internet Explorer Logo](#) *(Windows 9x and NT)*

When you browse the Internet using Internet Explorer, the animated logo spins indicating that activity is taking place. This registry setting controls which logo is being shown.



[Internet Explorer Intercepts the FTP Command](#) *(Windows 9x and NT)*

When you enter a FTP command such as "FTP ftp.regedit.com" IE 4.0 launches instead of the DOS based FTP program.



[Modifying the Internet Explorer Partial Address Feature](#) *(Windows 9x and NT)*

The Internet Explorer partial address feature, scans common domains for a match to a keyword entered in the Address bar. The feature is limited by default to searching only .COM, .EDU and .ORG domains. This tip allows you to add new domains and modify their priorities.



[Change the Internet Explorer Search Engine](#) *(Windows 9x and NT)*

Normally when you type 'go keyword' in the Internet Explorer address bar IE will search the web using a Microsoft selected search engine. By modifying this key you can select which search engine to use.



[Add a Background Bitmap to the Internet Explorer ToolBar](#) *(Windows 9x and NT)*

Want to have you own bitmap shown on the Internet Explorer toolbar? It's simple with the Registry setting.



[Hide the Internet Explorer Icon](#) *(Windows 9x and NT)*

This option hides the Internet Explorer icon from the Windows desktop.



[Proxy Server Configuration](#) *(Windows 9x and NT)*

If you need to configure a proxy server on multiple computers, or would just like to automate the procedure through the registry then this tip will explain how.



[Change the Location of the Outlook Express Mail and News Files](#) *(Windows 9x and NT)*

If you have installed Windows on a separate partition and want to keep it free of any unnecessary files, you can change the location of the mail and news files stored by Outlook Express to another partition.



[Changing the Internet Explorer Window Title](#) *(Windows 9x and NT)*

This setting allows you to customize Internet Explorer by using your own window title. For example you could rename IE to 'My Browser' or anything else you like!

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

**- RegEdit.com : Enhancements : Applications : Outlook Express -
Registry Keys:**



Remove the Outlook Express Splash Screen (Windows 9x and NT)

Sick of the Outlook Express splash screen everytime you start? This tip will help you remove it.



Colorful Message Backgrounds (Windows 9x and NT)

This setting enables colorful backgrounds with Outlook Express.



Change the Outlook Express Window Title (Windows 9x and NT)

This setting allows you to customize Outlook Express by using your own window title. For example you could rename Outlook Express to 'My Mail Reader' or anything else you like!

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Enhancements : Applications : pcANYWHERE -

Registry Keys:



Use Computer Name Instead of Caller Name (pcANYWHERE) *(Windows 9x and NT)*

When this key is set, if a host has the "Prompt to confirm connection" option checked, the host computer's prompt dialog will display the remote's computer name instead of the caller's name when a connection is made.



Confirm File Delete (pcANYWHERE) *(Windows 9x and NT)*

When this setting is disabled, the remote does not display the confirm prompt when deleting a file.



Confirm File Send (pcANYWHERE) *(Windows 9x and NT)*

When this setting is disabled, the remote does not display the confirm prompt when sending a file.



Display Host in List (pcANYWHERE) *(Windows 9x and NT)*

The registry entry allows the host to respond to remote requests for names. Thus, by disabling the registry item, you can hide the host from users scanning the network.



Hide the Record Session Button (pcANYWHERE) *(Windows 9x and NT)*

Use this registry key to hide the Record Session icon from the remote session toolbar.



Configure IPX Search Mode (pcANYWHERE) *(Windows 9x and NT)*

This registry item enables the SAP method of network search instead of using the bindery when making IPX connections.



Host Connection Time-Out (pcANYWHERE) *(Windows 9x and NT)*

If pcANYWHERE host does not respond, hang up. This is useful for scripts that call systems where a modem will answer, but the pcANYWHERE host may not be running.



Wait for Call After Disconnect (pcANYWHERE) *(Windows 9x and NT)*

If enabled, the host will not wait for a call when the remote disconnects.



Compatibility with the OnNet 2.1 TCP/IP Stack (pcANYWHERE) *(Windows 9x and NT)*

This registry item resolves an issue where pcANYWHERE displayed the wrong host IP address when using FTP's OnNet 2.1 TCP/IP stack.



Configure Persistent Cache (pcANYWHERE) *(Windows 9x and NT)*

This setting turns pcANYWHERE's persistent cache feature on or off.



Configure Legacy Remote Print Mode (pcANYWHERE) *(Windows 9x and NT)*

This setting specifies the default print destination when connecting to a pcANYWHERE 2.0 or 5.0 host.



Remote Printer Inactivity Time-out (pcANYWHERE) *(Windows 9x and NT)*

Use this setting if a print job is being separated into multiple jobs during remote printing. This item sets the inactivity time-out for the remote printing facility.



Multi-Processor Options (pcANYWHERE) *(Windows 9x and NT)*

This registry item specifies which processors pcANYWHERE32 8.0 will run on.



Prompt for TCP/IP Host (pcANYWHERE) *(Windows 9x and NT)*

This registry item allows a TCP/IP remote to specify an IP address or name when you leave the "Host To Connect To" field blank.



Prompt If Logged Out (pcANYWHERE) *(Windows 9x and NT)*

This registry key allows you to specify how pcANYWHERE32 will handle a remote connection when the pcANYWHERE32 host is waiting at the Windows NT login screen and the "Prompt On Connection" and "Disconnect

On Timeout" options have been checked.



Ignore DSR on Serial Devices (pcANYWHERE) *(Windows 9x and NT)*

Use this item for modems or other serial devices that do not initialize correctly because their DSR is not initially set. It is also useful if the modem connection does not have a DSR line.



Change Serial 56K Connection Speed (pcANYWHERE) *(Windows 9x and NT)*

Use this item when a serial connection can be made at 38,400 bps and 115,000 bps, but not at 57,600 bps.



Run the pcANYWHERE Service in Stealth Mode (pcANYWHERE) *(Windows 9x and NT)*

Use this setting to hide the Host Waiting icon and Waiting dialog.



Show Full Screen Reminder Message (pcANYWHERE) *(Windows 9x and NT)*

This setting turns the Full Screen Reminder Message on or off.



Run Smart Setup (pcANYWHERE) *(Windows 9x and NT)*

This setting controls whether SmartSetup is run when pcANYWHERE is loaded for the first time.



Speed Send File Size Limits (pcANYWHERE) *(Windows 9x and NT)*

The minimum size a file must be for SpeedSend to work is 10K. You can change this value.



Add an Additional Delay to Browse Packets (pcANYWHERE) *(Windows 9x and NT)*

Use this setting when remotes display an incomplete list of TCP/IP hosts in the host list over a WAN or LAN connection.



Connect to TCP/IP Hosts With Unknown Status (pcANYWHERE) *(Windows 9x and NT)*

This registry entry allows a remote to try to connect to a host if the host's status is unknown. The usual reason for not knowing the host's status is that direct packets have been filtered by a firewall between the host and the remote.



Configure the TCP/IP Data Port (pcANYWHERE) *(Windows 9x and NT)*

Use this setting to select which TCP data port pcANYWHERE32 uses.



Adapter Binding Mode (pcANYWHERE) *(Windows 9x and NT)*

This registry item allows a waiting host to bind to a new adapter, such as a dial-up adapter, without reinitializing the host.



Specify Host Mode TCP/IP Address (pcANYWHERE) *(Windows 9x and NT)*

This registry item allows you to specify which TCP/IP address index the host will wait on.



TCP/IP Host Binding Mode (pcANYWHERE) *(Windows 9x and NT)*

This registry item allows you to specify whether the host will wait on the first TCP/IP address given by the operating system, or whether it will wait on the TCP/IP index as indicated by TCPIPHostAddressIndex.



Multicast Packet Delay (pcANYWHERE) *(Windows 9x and NT)*

This sets the delay in milliseconds between each send. This is useful if multicast error correction is disabled.



Configure the Multicast Data Port (pcANYWHERE) *(Windows 9x and NT)*

This setting selects the port that the multicast data is sent to.



Multicast Error Correction (pcANYWHERE) *(Windows 9x and NT)*

This sets the level of error correction used on the host. The host specifies which level of error correction the remotes will use.



Configure Multicast Send and Receive Buffers (pcANYWHERE) *(Windows 9x and NT)*

These registry items set the number of receive and send buffers when using an error correction multicast session. For slow remotes, a larger value may lead to less data loss.



Multicast Adapter Selection (pcANYWHERE) *(Windows 9x and NT)*

Use this registry item for a multihomed, multicast host that is not binding to the correct network card. This can be why none of the remotes receive the multicast packets.



Multicast Maximum Transmission Unit (pcANYWHERE) *(Windows 9x and NT)*

This registry item sets the Maximum Transmission Unit (MTU) in bytes. The MTU is the maximum bytes that may be sent as one IP multicast packet.



Multicast Winsock Receive Buffer (pcANYWHERE) *(Windows 9x and NT)*

This registry item sets the size in bytes of the Winsock receive buffer.



TCP/IP Broadcast Mode (pcANYWHERE) *(Windows 9x and NT)*

Use this setting to turn off or modify pcANYWHERE32's broadcast options to limit network traffic when the remote browses for a host.



Port Compatibility with Legacy Versions (pcANYWHERE) *(Windows 9x and NT)*

pcANYWHERE32 8.0 hosts and remotes can connect to earlier hosts and remotes without any registry changes. You may want to turn off compatibility to limit network traffic or allow third party applications that have registered the ports that earlier versions of pcANYWHERE32 7.x and pcANYWHERE 2.0 were using.



TCP/IP Query Interval (pcANYWHERE) *(Windows 9x and NT)*

Use this setting to limit network traffic. Sometimes the additional network queries to refresh the browse list will interfere with getting status lights or making connections.



Configure the TCP/IP Status Port (pcANYWHERE) *(Windows 9x and NT)*

Use this setting to select which TCP status port pcANYWHERE uses.



Configure the Winsock Buffer Size (pcANYWHERE) *(Windows 9x and NT)*

Use this registry item to set the size in bytes of TCP's Winsock buffer. Using a large value may increase the throughput of connections where the delay is large in relation to the bandwidth. This includes Internet, ISDN, RAS, dial-up networking, WAN and satellite connections.



TAPI Modem Errors (pcANYWHERE) *(Windows 9x and NT)*

Each time you add a TAPI modem, it generates a unique TAPI Permanent Line ID which is stored in pcANYWHERE32's connection items. If you no longer have a modem with this unique ID, pcANYWHERE32 displays an error message. This registry key tells pcANYWHERE32 how to handle this situation.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Enhancements : Hardware : Printing -

Registry Keys:



Beep on Printer Errors *(Windows NT)*

When this setting is enabled the machine will beep (every 10 seconds) when a remote job error occurs on a print server.



Changing the Default Printer Spool Directory *(Windows NT)*

Windows using the hard drive to spool information before sending it to a printer. If the system is acting as a print server, it is possible that the default location may have insufficient disk space.



Change a Users Default Printer *(Windows 9x and NT)*

This setting will allow you the change the default printer of a user by modifying the registry.



Disable printer browse thread on the computer *(Windows NT)*

When this option is enabled, the print spooler does not send shared printer information to other print servers.



Disable Print Job Notification in Event Viewer *(Windows NT)*

By default Windows NT server adds an entry in the event log for every print job occurring on the spooler. This can quickly fill up the event log with redundant information.



Define the Scheduler Priority *(Windows NT)*

The setting controls the overall priority of the printer scheduler.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Enhancements/Hardware/Printing/index.shtml - (66)

- Enable or Disable the CD-ROM Autorun Feature -

Detailed Information:



Enable or Disable the CD-ROM Autorun Feature (*Windows 9x and NT*)

You can enable the CD-ROM autorun function by changing this registry setting, this will stop applications from auto launching when you insert a CD-ROM disc into your drive.

Open your registry and find the key below.

Change to value of 'Autorun', or create a new DWORD value if it doesn't already exist, and set the data to equal '0' for Autorun disabled.

Restart your computer for the changes to take affect.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom]

Value Name: Autorun

Data Type: REG_DWORD

Data: (0=disable, 1=enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- PC Speaker Beeping on Errors -

Detailed Information:



PC Speaker Beeping on Errors (Windows 9x and NT)

If you get annoyed by the beeps and noises coming from your PC speaker but can't find a way to turn it off, then use this tip to disable it.

1. Find the key below using Regedit.
2. Located the value 'Beep' if it doesn't already exist create it, by selecting Edit | New | String Value and naming the new value 'Beep'.
3. Modify the value of 'Beep' to either 'Yes' beeping enabled, or 'No' beeping disabled.

Key: [HKEY_CURRENT_USER\Control Panel\Sound]

Value Name: Beep

Data Type: REG_SZ

Data: 'Yes' or 'No'

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/120.html - (68)

- Adjust IntelliMouse Scroll Function -

Detailed Information:



Adjust IntelliMouse Scroll Function (*Windows 9x and NT*)

This entry determines the number of lines scrolled for each rotation of the mouse wheel on a Microsoft IntelliMouse! 22 when no modifier keys (such as <Ctrl> or <Shift>) are pressed.

If the value of this entry is 0, the screen will not scroll when the mouse wheel is turned. If the value of this entry is greater than the number of lines visible in the window, the screen will scroll up or down by one page. To direct Windows NT to interpret all wheel rotations as page-up or page-down commands, set the value of this entry to 0xFFFFFFFF.

Key: [HKEY_CURRENT_USER\Control Panel\Desktop]

Value Name: WheelScrollLines

Data Type: REG_SZ

Data: 0 - 0xFFFFFFFF

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/53.html - (69)

- Dial-Up Networking Password Box Grayed Out -

Detailed Information:



Dial-Up Networking Password Box Grayed Out (*Windows 9x*)

If you are having problems trying to get DUN to remember your password and you find the option grayed out then there are a few things you can try.

1. Make sure you have Client for Microsoft Networks installed on your system. Control Panel / Networking / Add / Client / Microsoft / Microsoft Networking.
2. Your Windows startup is configured to ask for a password and you are hitting the esc key when the logon box is displayed.
3. You have a corrupted password file. Do a search for *.pwl in the Windows folder and rename all the files you find. Note - this will force you to rebuild your password files from scratch.
4. Check the Registry:
 - Run the Registry Editor (REGEDIT.EXE).
 - Find HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Network\Real Mode Net.
 - If you see autologon (on the right side) with a value of "00 00 00 00", double-click on it, and change the value to "01 00 00 00 00".
 - Exit RegEdit and restart the PC.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Network\Real Mode Net]
Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/77.html - (70)

- Removing or Adding Items to Your Persistent Connections List -

Detailed Information:



Removing or Adding Items to Your Persistent Connections List (*Windows NT*)

Windows stores the names of previously mapped drives, this can be a security threat if vulnerable hidden shares are listed. An advantage is that this key can also be used to set default items for list, if for example inexperienced users where required to map common drives, you could store them here.

1. Open the registry and find the key below.
2. Listed under this key are all the shares Windows has stored for the current user, simply delete the entries you don't want to store. Or add new ones by adding a new string value, and name it by incrementing the alpha values already in the list. Set the data to equal the drive share you wish to add.

Note: *This change affects only the current user, to change the defaults for all users modify [KEY_USERS\DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Network\Persistent Connections] instead.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Network\Persistent Connections]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/200.html - (71)

- Specifying a Preferred Netware Server -

Detailed Information:



Specifying a Preferred Netware Server (*Windows 9x*)

Specifying a default Netware is possible using this setting.

1. Using Regedit find the key below, if it doesn't exist, create it.
2. Create new String value and name it 'AuthenticatingAgent', set the value to the name of your preferred Netware server.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NWNP32\NetworkProvider]

Value Name: AuthenticatingAgent

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/127.html - (72)

- Modifying LAN Based Auto-disconnect Time-Out -

Detailed Information:



Modifying LAN Based Auto-disconnect Time-Out (*Windows NT*)

Windows NT can be configured to automatically disconnect idle LAN sessions after a set number of minutes.

1. Open your registry and find the key below.
2. Modify the value of 'Autodisconnect' to equal the time in minutes before a session is disconnected. If this value doesn't already exist create a new string value.
3. Restart Windows NT.

Note: To disable Autodisconnects set the value to 'Oxffffffff'.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

Value Name: Autodisconnect

Data Type: REG_DWORD

Data: 0 to 4,294,967,295 (Oxffffffff) in minutes

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/194.html - (73)

- Disable Automatic Network Logon -

Detailed Information:



Disable Automatic Network Logon (*Windows 9x*)

This setting disabled the automatic logon to Netware servers.

1. Using Regedit open the key below, if it doesn't already exist, create it.
2. Create a new DWORD value of 'DisableDefaultPasswords', and modify the value to equal '1' for disabled automatic logon, or '0' for automatic logon.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NWNP32\NetworkProvider]

Value Name: DisableDefaultPasswords

Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/128.html - (74)

- Display Domain Logon Confirmation -

Detailed Information:



Display Domain Logon Confirmation (*Windows 9x and NT*)

When this option is enabled, a dialog box is shown upon successful validation by a Windows NT domain.

Key: [HKEY_LOCAL_MACHINE\Network\Logon]

Value Name: DomainLogonMessage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/133.html - (75)

- Automatically Detect Slow Network Connections -

Detailed Information:



Automatically Detect Slow Network Connections (Windows NT)

By default, Windows NT will attempt to detect the time-out on network links to determine their speed (high or low). This functionality can be disabled if Windows NT is having problems determining the speed of your link.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: SlowLinkDetectEnabled

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/143.html - (76)

- Define the Slow Link Time-Out -

Detailed Information:



Define the Slow Link Time-Out (*Windows NT*)

Windows NT uses this setting to define what is a low speed, and what is a high speed connection. The default time-out is 2000 milliseconds, any connection slower is considered a low speed link.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: SlowLinkTimeOut

Data Type: REG_DWORD

Data: Time (milliseconds)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/144.html - (77)

- Support Long Filenames on Netware Servers -

Detailed Information:



Support Long Filenames on Netware Servers (*Windows 9x*)

This setting controls whether long filenames (LFN) are supported on Netware servers, and if supported which versions.

1. Using Regedit open the key below, if it doesn't already exist, create it.
2. Create a new DWORD value, and name it 'SupportLFN'.
3. Modify the value of 'SupportLFN' to either '0', '1' or '2' depending on the table below:

Value	Description
0	LFN Disabled
1	LFN Enabled on Netware 3.12 and above
2	LFN Enabled on all Netware servers that support LFN

4. Exit Regedit and reboot.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\NWREDIR]

Value Name: SupportLFN

Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Disable SAP advertising for Netware Networks -

Detailed Information:



Disable SAP advertising for Netware Networks (*Windows 9x*)

By default Windows will send SAP packets to advertise available file and print shares when 'File and Print Sharing for Netware Networks' is enabled, this setting disables those packets.

In addition to changing the value of 'Use_Sap' you also may be required to create another key and value:

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NcpServer\Parameters\Ndi\Params\Use_Sap] @="0"
```

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NcpServer\Parameters]

Value Name: Use_Sap

Data Type: REG_SZ

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/129.html - (79)

- RegEdit.com : Enhancements : Windows : 9x -

Registry Keys:



[Use Windows Update Without Registering](#) (*Windows 98*)

Windows Update is a handy feature of Windows 98, having to register your personal details before being able to use it isn't as good! With this tip you can bypass the registration process.



[Changing the Location of Windows 9x's Installation Files](#) (*Windows 9x*)

Modifying the string will change the path that the Windows 95 setup program will look for the installation files.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Enhancements/Windows/9x/index.shtml - (80)

- RegEdit.com : Enhancements : Windows : NT -

Registry Keys:



Enable Command Line Completion *(Windows NT)*

Command completion allows you to type only a portion of a file name, and then have the system complete the rest by pressing the TAB key. This is similar to the the UNIX shell command completion feature.



Change the Display Color of Compressed Files and Folders *(Windows NT)*

When a file is compressed in Windows NT, there is an option in Explorer to display it in a different color to easily distinguish them. This setting defines what color to use, the default is blue.



Auto Logon to a Windows NT Machine *(Windows NT)*

Windows NT includes a feature that allows you to automatically logon to the machine and network, bypassing the Winlogon dialog box.



Automatically Shutdown Not Responding Applications *(Windows NT)*

Often when Windows NT shutdown, a task will return as 'Not Responding' and you are given the choice to 'End Task' enabling this function automatically ends the task.



Automatically Reboot on the 'Blue Screen of Death' *(Windows NT)*

Windows NT workstation will halt by default when you get a dreaded 'Blue Screen of Death' (BSOD). Changing this setting will force Windows NT to automatically reboot when it crashes instead.



Changing Default Colors for Command Prompt *(Windows NT)*

The value DefaultColor controls the foreground and background colors used in command prompt windows. It has a default value of 0, for standard white text on a black background.



Run 16bit apps in a Separate VDM by Default *(Windows NT)*

When starting a 16bit application you have the option of running it in a separate virtual machine. From this setting you can change the default setting for using VDM's.



Delete Cached Copies of Roaming Profiles *(Windows NT)*

If this settings is enabled, when users with roaming profiles log off, the system will delete the cached copy of their roaming profile. This will help to save disk space where that are lots of roaming users.



Hard Disk Free Space Warning *(Windows NT)*

By default, Windows NT posts an alert when the amount of free space remaining on your hard disk falls below 10 percent.



Configure the DHCP Settings of a Network Adapter *(Windows NT)*

This setting controls whether TCP/IP should use DHCP to automatically assign an IP address, or if it should use the statically defined address.



Configure the TCP/IP Settings of a Network Adapter *(Windows NT)*

These values control the TCP/IP parameters of the network interface cards. Configurable parameters include IP Address, Subnet Mask and Default Gateway.



Allow extended characters in 8.3 filenames *(Windows NT)*

This setting allows extended characters to be used in 8.3 filenames. Short file names with extended characters may not be viewable on computers that do not have the same character code page.



Power the Computer Off After Shutdown *(Windows NT)*

Enabling the setting will cause Windows NT to automatically powerdown your computer once it has finished the shutdown process.



Time-out for NT User Profile Dialog Boxes (Windows NT)

When the user is presented with a dialog box requesting User Profile information, this specifies the amount of time in seconds before the dialog box is closed and the default is accepted. The default value is 30 seconds.



Run Logon Scripts Synchronously (Windows NT)

This setting defines whether the system should wait for the logon scripts to complete before starting the user's shell.



Windows NT Short File Extensions (Windows NT 4.x)

Windows NT evaluates file extensions on the first three characters, therefore 'filename.html' is actually treated as 'filename.htm'. The side affect is that if you use a command such as 'del *.htm' to delete all the '.htm' files, you will also delete all '.html' files as well. This functionality can be disabled by modifying the registry.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Enhancements/Windows/NT/index.shtml - (81)

- Displaying Hi-Color Icons without the Plus Pack -

Detailed Information:



Displaying Hi-Color Icons without the Plus Pack (*Windows 9x and NT*)

If you like a bit more colour and detail in your icons, then step up to hi-color mode. With this setting your Windows icons are shown in all their hi-resolution glory.

Create a new string value named "Shell Icon BPP" in the key below. Change the value to equal the color depth supported by your video card (e.g. '16' for 16-bit graphics cards or '24' for 24-bit graphics cards)

Note: *You need a graphics card capable of displaying above 256 colors for this to be useful.*

Key: [HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics]

Value Name: Shell Icon BPP

Data Type: REG_SZ

Data: 16

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/39.html - (82)

- Add an Expanding Control Panel to Start Menu -

Detailed Information:



Add an Expanding Control Panel to Start Menu (*Windows 9x and NT*)

Want easy access to the Control Panel options? With this tip you can add an expanding Control Panel folder to the start menu. This trick will work with most special folders too.

The first step is find the system ID of the folder you want to add, these ID's can be found under the [HKEY_CLASSES_ROOT\CLSID] key. The Control Panel's key is called [HKEY_CLASSES_ROOT\CLSID\{21EC2020-3AEA-1069-A2DD-08002B30309D}] and the ID is the last set of number after CLSID, in this case '{21EC2020-3AEA-1069-A2DD-08002B30309D}'.

Once you've found the ID the hard work is done, now all you need to do is right-click on the Start button and chose open.

Now create a new folder with the name of the folder followed by a dot and the folder ID. For Control Panel create a new folder called 'Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}'. The new folder should now change into the Control Panel logo. Close the explorer window and click on the Start button, and there should now be a new expanding folder for the Control Panel.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/294.html - (83)

- Easily Use Notepad to Open a File -

Detailed Information:



Easily Use Notepad to Open a File (*Windows 9x and NT*)

Enabling this setting will allow you to use Notepad to open a file by simply right clicking on the icon. Also the Notepad will be used to open the files by default if no association already exists.

1. Go to the key "HKEY_CLASSES_ROOT*\shell", if it doesn't exist create it.
2. Under *shell* create a new key called *open*, and edit the string "(Default)" to read "Open With Notepad".
3. Under *open* create a new key called *command*, and edit the string "(Default)" to read "notepad.exe %1".

Now when you right click on a file you should see "Open with Notepad" as one of the options.

Key: [HKEY_CLASSES_ROOT*\shell]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/40.html - (84)

- Add Explore From Here to Every Folder -

Detailed Information:



Add Explore From Here to Every Folder (Windows 9x and NT)

When you right click on any folder this will give you an option to *Explore From Here*, which will open up an explorer window of that folder.

Open your registry and find the key below. If it doesn't exist create it.

Change the value of '(Default)' to equal 'E&xplore From Here'.

Create a new key under the [Explore] key called *command*, and edit the '(Default)' value to equal 'explorer.exe /e,/root,/idlist,%i'.

Key: [HKEY_CLASSES_ROOT\Directory\shell\Explore]

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/41.html - (85)

- Control Network Browser Elections -

Detailed Information:



Control Network Browser Elections (*Windows 9x and NT*)

A browser election is a normal network occurrence and provides a means to guarantee there is never more than one master browser present in a domain / workgroup.

Controlling which PC is the Domain Master Browser is set using the "IsDomainMaster" key the options are "Yes" or "False".

To prevent an NT Workstation or Server (non-PDC) from acting as a browser, set the "MaintainServerList" key to "No", other options are "Yes", "No" or "Auto".

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\Parameters]

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/54.html - (86)

- Add Command Prompt Here to Every Folder -

Detailed Information:



Add Command Prompt Here to Every Folder (Windows 9x and NT)

If you're from the old school and still use the DOS prompt regularly, then this tip is for you! It creates a new right-click option to open a command prompt window at the directory you are currently working from.

Open your registry and find the key below.

Create a new sub key called 'CommandPrompt' as in [HKEY_CLASSES_ROOT\Directory\shell\CommandPrompt]. Change the value of '(default)' within the key to equal the text you would like on the right-click menu, for example 'Command Prompt Here'.

Create another new sub-key under the key created above, name this subkey 'command' as in: [HKEY_CLASSES_ROOT\Directory\shell\CommandPrompt\command]. Change the value of '(default)' within this key depending on your operating system to equal either:

Windows 9x

command.com /k cd "%1"

or

Windows NT

cmd.exe /k cd "%1"

Now right-click on a folder and the new option of 'Command Prompt Here' should be available.

Key: [HKEY_CLASSES_ROOT\Directory\shell]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/260.html - (87)

- Creating Program Aliases in Windows -

Detailed Information:



Creating Program Aliases in Windows (*Windows 9x and NT*)

A hidden feature in the Windows registry allows you to create program aliases. Allowing you to create, for example, an alias called JBLOGGS.EXE that when executed actually runs another program, e.g. NOTEPAD.EXE

1. Open your registry and find the key below. Under it should be a number of sub-keys.
2. To create a new alias create a sub-key, and call it the name of the alias you wish to create (e.g. 'JBLOGGS.EXE').
3. Modify the (default) value of the sub-key to equal the fully qualified path and filename of the application you want to be launched when you execute the alias (e.g. 'c:\windows\notepad.exe').
4. Exit Regedit, and to test use the Start | Run command type in the name of your alias (i.e. 'JBLOGGS.EXE') and the aliased program should be launched, in this case Notepad.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths]

Value Name: (Default)

Data Type: REG_SZ

Data: Fully Qualified File Name (e.g. c:\windows\notepad.exe)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Active Window Tracking (X-Mouse) -

Detailed Information:



Active Window Tracking (X-Mouse) (*Windows 9x and NT*)

This tweak makes you most control the Window focus, therefore wherever you move your mouse the window will become active, similar to X-Windows on Unix.

Open you registry and find the key below.

Create a new DWORD value called 'ActiveWindowTracking', or modify the existing value, to equal '1' for enabled.

Note: *Restart your computer for the changes to take affect.*

Key: [HKEY_CURRENT_USER\Control Panel\Mouse]

Value Name: ActiveWindowTracking

Data Type: REG_DWORD

Data: (0=disable,1=enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/18.html - (89)

- Automatic Logon without Name or Password -

Detailed Information:



Automatic Logon without Name or Password (*Windows 9x*)

This setting allows Windows clients to logon without entering a user name or password, therefore bypassing the logon box.

1. Using Regedit, open the key below.
2. Create a new String Value, and name it 'Default Password'.
3. Modify the data of 'Default Password' to match the default users password.

The default username is stored at:

[HKEY_LOCAL_MACHINE\Network\Logon] - Username

4. Reboot and the system should automatically logon.

Note: *The password is stored in clear text, therefore anyone with access to the registry can see the default password!*

Key: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon]

Value Name: Default Password

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/125.html - (90)

- Adjust the Double-Click Sensitivity Area -

Detailed Information:



Adjust the Double-Click Sensitivity Area (Windows 9x and NT)

This setting controls the amount of movement allowed between clicks, for two clicks to be counted as a double-click.

Open your registry and find the key below.

Create two new string values named: 'DoubleClickHeight' and 'DoubleClickWidth'. Set these values to equal the size in pixels of the double-click area.

Log-off, or restart Windows for the changes to take effect.

Key: [HKEY_CURRENT_USER\Control Panel\Desktop]

Value Name: DoubleClickHeight, DoubleClickWidth

Data Type: REG_SZ

Data: Size in Pixels

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/341.html - (91)

- Removing the 'Shortcut to...' Text on Shortcuts -

Detailed Information:



Removing the 'Shortcut to...' Text on Shortcuts (*Windows 9x and NT*)

Don't like having 'Shortcut to...' appended to every Shortcut? You're not alone. With this tip you can stop Windows from adding this text when creating links.

Open your registry and find the key below.

Create a new BINARY value name 'link', or modify the existing value, to equal '00 00 00 00' to have the Shortcut text disabled.

This tweak can also be applied to the [HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer] key, to change all users.

Note: *Restart your computer before creating any new shortcuts.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer]

Value Name: link

Data Type: REG_BINARY

Data: (00 00 00 00 = No Shortcut Text)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/339.html - (92)

- Change the Alignment of Drop-Down Menus -

Detailed Information:



Change the Alignment of Drop-Down Menus (Windows 9x and NT)

By default, Windows drop-down menus are aligned to the left, with this tip you can change the default behaviour to make all drop-down aligned to the right instead.

Open your registry and find the key below.

Create a new string value named 'MenuDropAlignment', or modify the existing value to equal '1' for right alignment or '0' for left alignment.

Restart or Log Off your PC for the changes to take affect.

Key: [HKEY_CURRENT_USER\Control Panel\Desktop]

Value Name: MenuDropAlignment

Data Type: REG_SZ

Data: (0 = Left, 1 = Right)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/340.html - (93)

- Change the Size of Desktop Icons -

Detailed Information:



Change the Size of Desktop Icons (Windows 9x and NT)

Are your icons too small? Or too big? This setting will let you resize them to suit your desktop preference.

Open the registry and find the key below.

Create a new value named 'Shell Icon Size' and set the value, or modify the existing value, to equal the size of your icons in pixels. Smaller values = smaller icons!

Key: [HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics]

Value Name: Shell Icon Size

Data Type: REG_SZ

Data: Size in Pixels (Default = 32)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/263.html - (94)

- Change the Position of the Desktop Wallpaper -

Detailed Information:



Change the Position of the Desktop Wallpaper (*Windows 9x and NT*)

Unfortunately Windows only gives you the limited options of center or tile for the placement of the desktop wallpaper. With this setting you can move the image anyway on your desktop.

Open your registry and find the key below.

Create two new string values of 'Wallpaperoriginx' and 'Wallpaperoriginy'. If the values already exist then you simply modify them.

Set the value of 'Wallpaperoriginx' to equal the horizontal offset, and set the value of 'Wallpaperoriginy' to equal the vertical offset. Then either restart Windows, or change your background image through the Control Panel.

Note: *The image is offset from the center of your desktop, so you can use positive and negative values.*

Key: [HKEY_CURRENT_USER\Control Panel\Desktop]

Value Name: Wallpaperoriginx, Wallpaperoriginy

Data Type: REG_SZ

Data: Distance in Pixels

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/290.html - (95)

- Boot Windows NT in Safe Mode -

Detailed Information:



Boot Windows NT in Safe Mode (*Windows NT*)

Windows NT can be very temperamental sometimes are you add new software or install a new driver. The option allows you the create a Windows NT alternative to the Windows 9x Safe Mode. In this mode extra checks are performed and not all third party drivers are loaded.

1. Change the attributes for BOOT.INI so it is not 'Read Only', BOOT.INI is found in the root directory of the first partition. And open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Listed under the [operating systems] section are all the OS's the NT boot loader can launch. To create a new safe mode entry copy one of the existing NT entries and paste it on a new line.
3. At the end of the new entry add '/sos' (without the quotation marks), change the description of the entry to reflect that it is safe mode. Additional adding '/basevideo' will launch NT with the default VGA driver.

The new entry should look similar to:

```
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Workstation Version 4.00 [Safe Mode]" /sos /basevideo
```

4. Changes will take place on the next reboot.

Key: [BOOT.INI]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/87.html - (96)

- Disable Detection of Devices on Serial Ports -

Detailed Information:



Disable Detection of Devices on Serial Ports (*Windows NT*)

Windows NT attempts to probe the serial ports on boot-up to detect any serial mice. This can cause problems with other serial devices such as UPS's.

1. Change the attributes for BOOT.INI so it is not 'Read Only', BOOT.INI is found in the root directory of the first partition. And open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Listed under the [operating systems] section are all the OS's the NT boot loader can launch.
3. At the end of the each entry add '/NoSerialMice' (without the quotation marks).

The new entry should look similar to:

```
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Workstation Version 4.00" /NoSerialMice
```

4. Changes will take place on the next reboot.

Key: [BOOT.INI]

More info: <http://support.microsoft.com/support/ntserver/service/10141848.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Enable the 4GT RAM Tuning Feature of NT Enterprise Edition -

Detailed Information:



Enable the 4GT RAM Tuning Feature of NT Enterprise Edition (*Windows NT*)

With standard Windows NT Server, the per-process address limit is 2 gigabytes (GB) of random access memory (RAM). The 4GT feature of Windows NT Server/E increases this limit to 3 GB without introducing new APIs. 4GT does this by reducing the potential RAM allocated to the Windows NT kernel from 2 GB to 1 GB.

1. Change the attributes for BOOT.INI so it is not 'Read Only', BOOT.INI is found in the root directory of the first partition. And open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Listed under the [operating systems] section are all the OS's the NT boot loader can launch.
3. At the end of the each entry add '/3GB' (without the quotation marks).

The new entry should look similar to:

```
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Server Version 4.00" /3GB
```

4. Changes will take place on the next reboot.

Note: *This change is only effective if you are using Windows NT Server/E. On standard Windows NT, this flag will relocate the kernel, but applications will be unable to access more than 2 GB.*

Key: [BOOT.INI]

More info: <http://support.microsoft.com/support/kb/articles/Q171/7/93.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Boot Windows NT with the Default VGA Video Driver -

Detailed Information:



Boot Windows NT with the Default VGA Video Driver (*Windows NT*)

This explains how to create an a safe VGA video mode start-up option, especially useful when your video adapter or driver is causing problems.

1. Change the attributes for BOOT.INI so it is not 'Read Only', BOOT.INI is found in the root directory of the first partition. And open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Listed under the [operating systems] section are all the OS's the NT boot loader can launch. To create a new safe VGA entry copy one of the existing NT entries and paste it on a new line.
3. At the end of the new entry add '/basevideo' (without the quotation marks), change the description of the entry to reflect that it is VGA mode.

The new entry should look similar to:

```
multi(0)disk(0)rdisk(0)partition(1)WINNT="Windows NT Workstation Version 4.00 [VGA mode]" /basevideo
```

4. Changes will take place on the next reboot.

Key: [BOOT.INI]

Value Name: [operating systems]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Change the Default Operating System -

Detailed Information:



Change the Default Operating System (*Windows NT*)

This key controls which operating system the NT Boot Loader launches by default.

1. Change the attributes for BOOT.INI so it is not 'Read Only', BOOT.INI is found in the root directory of the first partition. And open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Change the 'default=' option to an operating system listed under the [operating systems] sub section of BOOT.INI
ie. to load Windows NT from the first partition on the first IDE hard drive in the /WINNT directory the option would look like: "default=multi(0)disk(0)rdisk(0)partition(1)WINNT"
3. Changes will take affect on the next reboot.

Key: [BOOT.INI]

Value Name: default

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Change Default OS Selection Timeout -

Detailed Information:



Change Default OS Selection Timeout (*Windows NT*)

This setting controls the amount of time Windows NT will wait before loading the Default OS choice as define by the "default=" option.

1. Change the attributes for BOOT.INI so it is not 'Read Only', BOOT.INI is found in the root directory of the first partition. And open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Change the default value of '30' to a number representing a timeout in seconds. ie. to have a timeout of 5 seconds change the value to 'timeout=5'.
3. The change will take affect on the next reboot.

Hint: To have an Windows NT wait indefinitely for a choice change this value to 'timeout=-1'.

Key: [BOOT.INI]

Value Name: timeout

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/84.html - (101)

- Running Scandisk on Boot Up -

Detailed Information:



Running Scandisk on Boot Up (*Windows 9x*)

If Windows 9x is shutdown incorrectly, or the turn power turned off without shutting down, the system will attempt to run Scandisk on the next boot. You can control whether Scandisk doesn't run, prompts whether to run, or runs automatically.

1. Change the attributes for MSDOS.SYS so it is not 'Read Only', MSDOS.SYS is found in the root directory of your C:\ drive. Open the file using Notepad or another text editor (not Microsoft Word or any word processor).

2. Change the value of 'AutoScan=' to:

- AutoScan=0 : Scandisk is Disabled
- AutoScan=1 : Scandisk Prompts First
- AutoScan=2 : Scandisk Runs Automatically

3. Changes will take place on the next reboot.

Note: *It is advisable to run Scandisk after an incorrect shutdown to avoid file corruption.*

Note: *This feature is only available on Windows 95 OSR 2 and greater.*

Key: [MSDOS.SYS]

Data: AutoScan=1 (default)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/95.html - (102)

- Modifying the [Paths] Section of MSDOS.SYS -

Detailed Information:



Modifying the [Paths] Section of MSDOS.SYS (Windows 9x)

The [Paths] section lists the locations for other Windows 95 files (such as the registry) and can be modified if files are moved.

The [Paths] section can contain the following settings:

HostWinBootDrv=<Root of Boot Drive>

Default: C

Purpose: Specifies the location for the root of the boot drive.

UninstallDir=<Root of Boot Drive>

Default: C

Purpose: Specifies the location of the W95undo.dat and W95undo.ini files. These files are necessary to uninstall Windows 95.

NOTE: This setting is present only if you back up your system files when you are prompted during Windows 95 Setup.

WinBootDir=<Windows Directory>

Default: Directory specified during Setup (for example, C:\WINDOWS)

Purpose: Lists the location of the necessary files for booting.

WinDir=<Windows Directory>

Default: Directory specified during Setup (for example, C:\WINDOWS)

Purpose: Lists the location of the Windows 95 directory specified during Setup.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Enable / Disable Function Keys on Boot Up -

Detailed Information:



Enable / Disable Function Keys on Boot Up (*Windows 9x*)

By default Windows 9x enables the function keys on boot, these allow you to control the boot process. For example pressing F5 while the "Starting Windows 95..." message is displayed will boot Windows in Safe Mode.

1. Change the attributes for MSDOS.SYS so it is not 'Read Only', MSDOS.SYS is found in the root directory of your C:\ drive. Open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Change the value of 'BootKeys=' to 'BootKeys=1' for enabled or 'BootKeys=0' for disabled.
3. Changes will take place on the next reboot.

Key: [MSDOS.SYS]

Data: BootKeys=1 (default)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/90.html - (104)

- Change the Amount of Time that Function Keys are Available -

Detailed Information:



Change the Amount of Time that Function Keys are Available (*Windows 9x*)

By default Windows 9x enables the function keys on boot for 2 seconds, these keys allow you to control the boot process.

1. Change the attributes for MSDOS.SYS so it is not 'Read Only', MSDOS.SYS is found in the root directory of your C:\ drive. Open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Change the value of 'BootDelay=' to a value representing the number of seconds to make the keys available. eg. To enable the keys for 5 seconds change the value to 'BootDelay=5'
3. Changes will take place on the next reboot.

Key: [MSDOS.SYS]

Data: BootDelay=2 (default)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Control Whether the Windows 9x GUI is Loaded Automatically -

Detailed Information:



Control Whether the Windows 9x GUI is Loaded Automatically (*Windows 9x*)

By default Windows 9x automatically loads the GUI (or Windows Desktop) with this key you can control whether the GUI is loaded or if you just want the MS-DOS 7.0 prompt.

1. Change the attributes for MSDOS.SYS so it is not 'Read Only', MSDOS.SYS is found in the root directory of your C:\ drive. Open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Change the value of 'BootGUI=' to 'BootGUI=1' for GUI enabled or 'BootGUI=0' GUI disabled.
3. Changes will take place on the next reboot.

Key: [MSDOS.SYS]

Data: BootGUI=1 (default)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/92.html - (106)

- Display the Windows Splash Screen While Loading -

Detailed Information:



Display the Windows Splash Screen While Loading (*Windows 9x*)

When Windows is loading normally you see the Windows clouds splash screen, this can be disabled to show the background DOS boot process.

1. Change the attributes for MSDOS.SYS so it is not 'Read Only', MSDOS.SYS is found in the root directory of your C:\ drive. Open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Change the value of 'Logo=' to 'Logo=1' for splash screen enabled or 'Logo=0' for disabled.
3. Changes will take place on the next reboot.

Hint: Pressing <Esc> while the splash screen is showing will have the same effect for that session.

Key: [MSDOS.SYS]

Data: Logo=1 (default)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/93.html - (107)

- Allow Booting to the Previous Operating System -

Detailed Information:



Allow Booting to the Previous Operating System (*Windows 9x*)

If you installed an upgrade version of Windows 9x, you can normally press F4 to boot your previous version of Windows. This option can be disabled.

1. Change the attributes for MSDOS.SYS so it is not 'Read Only', MSDOS.SYS is found in the root directory of your C:\ drive. Open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Change the value of 'BootMulti=' to 'BootMulti=1' for F4 enabled or 'BootMulti=0' for disabled.
3. Changes will take place on the next reboot.

Key: [MSDOS.SYS]

Data: BootMulti=1 (default)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/94.html - (108)

- Showing the Windows Boot Menu -

Detailed Information:



Showing the Windows Boot Menu (*Windows 9x*)

By default Windows 9x does not show the boot menu unless you press F8. The boot menu allows you to boot Windows in different modes, including Safe Mode and Command Prompt Mode. You can configure the boot menu to be shown automatically on every boot.

1. Change the attributes for MSDOS.SYS so it is not 'Read Only', MSDOS.SYS is found in the root directory of your C:\ drive. Open the file using Notepad or another text editor (not Microsoft Word or any word processor).
2. Change the value of 'BootMenu=' to 'BootMenu=1' for enabled or 'BootMenu=0' for disabled.
3. If the boot menu is enabled you can control how long it waits before continuing to boot with the 'BootMenuDelay=' option. Set 'BootMenuDelay=' to the amount of time to wait in seconds. i.e. 'BootMenuDelay=5' would wait 5 seconds before continuing to load Windows.
4. Changes will take place on the next reboot.

Note: *BootKeys must also be enabled for this option to function i.e. 'BootKeys=1'*

Data:

BootMenu=0 (default)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Forces Your Computer to Boot in Safe Mode -

Detailed Information:



Forces Your Computer to Boot in Safe Mode (Windows 9x)

This setting when enabled forces your computer to always boot in Safe Mode.

1. Add a new value of 'BootSafe=' to MSDOS.SYS.
2. Set the value to '1' to always boot in Safe mode, or '0' to run normally.

Value Name:

BootSafe

Data: (1=enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/213.html - (110)

- Suppress Safe Mode Warning Message -

Detailed Information:



Suppress Safe Mode Warning Message (*Windows 9x*)

Enabling the setting suppress the safe mode warning message when booting up, and bypasses the Startup menu.

1. Add a new value of 'BootWarn=' to MSDOS.SYS.
2. Set the value to '1' to ignore the Safe mode warning, or '0' to run normally.

Value Name:

BootWarn

Data: (1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/214.html - (111)

- Control Windows Double Buffering Support -

Detailed Information:



Control Windows Double Buffering Support (*Windows 98*)

Windows 98 includes double buffering support, some systems may have an incompatibility between the computer's BIOS and the Dblbuff.sys file.

A setting of 1 is a conditional setting that enables double-buffering for controllers that need it (for example, SCSI controllers). A setting of 2 is an unconditional setting that enables double-buffering regardless of whether the controller needs it or not.

Note: *that some computers, especially those that use a SCSI hard disk, may require double buffering to work properly.*

Key: [MSDOS.SYS]

Value Name: DoubleBuffer

Data: (0 = disabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/211.html - (112)

- Loading Double / Drive Space Compression into Low Memory -

Detailed Information:



Loading Double / Drive Space Compression into Low Memory (*Windows 9x*)

A setting of 0 does not let Windows 95 load COMMAND.COM or DRVSPACE.BIN/DBLSPACE.BIN at the top of 640K. If you are having compatibility problems with software that makes assumptions about the available memory try setting this to 0.

Value Name: LoadTop

Data: (0 = load in low memory)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/215.html - (113)

- Speed Up File System Caching -

Detailed Information:



Speed Up File System Caching (*Windows NT*)

If you have some extra RAM and an active file system, you can speed up file system activity by increasing the IoPageLockLimit from the default 512K bytes to 4096K bytes or more.

This entry is the maximum number of bytes that can be locked for I/O operations. When the value is 0, the system defaults to 512K. The largest value is based on the amount of memory in your system.

RAM (MB)	IoPageLockLimit
32	4096000
64	8192000
128	16384000
256+	65536000

Before making changes, get a baseline by using performance monitor for a representative period of time. Make your changes in small increments and measure performance after each change.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]
Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/55.html - (114)

- Configure the Contiguous File Allocation Size -

Detailed Information:



Configure the Contiguous File Allocation Size (Windows 9x and NT)

This setting optimizes the contiguous file allocation size for the file system. This is especially useful for disk intensive applications.

Open your registry and find the key below.

Create a new DWORD value named 'ContigFileAllocSize', set the value to equal '200' (in hex).

Close the registry and restart the computer for the change to take affect.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]

Value Name: ContigFileAllocSize

Data Type: REG_DWORD

Data: 200 (hex) or 512 (decimal)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/344.html - (115)

- Disable 8.3 Name Creation (NTFS) -

Detailed Information:



Disable 8.3 Name Creation (NTFS) (Windows NT)

This key stops the NTFS volume from generating MS-DOS compatible 8.3 file names. Disabling this feature can increase the performance on heavily used NTFS partitions that have large amount of files with long filenames.

Warning: Some 16 bit installation programs may have problems with this option enabled, you can either re-enabled 8.3 creation during the install or use directory names in the non LFN format i.e. "c:\progra~1\applic~1"

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]

Value Name: NtfsDisable8dot3NameCreation

Data Type: REG_DWORD

Data: (0=disable, 1=enable)

More info: <http://support.microsoft.com/support/kb/articles/q121/0/07.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Increase NTFS Performance by Disabling the Last Access Time Stamp -

Detailed Information:



Increase NTFS Performance by Disabling the Last Access Time Stamp (*Windows NT*)

When Windows NT lists a directory (Explorer, DIR command, etc.) on an NTFS volume, it updates the LastAccess time stamp on each directory it detects. If there are a very large number of directories, this can affect performance.

To control this feature use Regedit to edit the key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem

Add Value name "NtfsDisableLastAccessUpdate" of type REG_DWORD. Set it to "1" to prevent the LastAccess time stamp from being updated.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]

Value Name: NtfsDisableLastAccessUpdate

Data Type: REG_DWORD

Data: (0 = disable, 1 = enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/50.html - (117)

- Optimizing the DefaultRcvWindow & DefaultTTL Settings -

Detailed Information:



Optimizing the DefaultRcvWindow & DefaultTTL Settings (*Windows 9x*)

The optimization of RcvWindow and DefaultTTL along with other registry settings such as MaxMTU and MaxMSS can speed up TCP/IP modem networking connections (eg. Internet connections).

RWIN (Receive WINdow) is the buffer your machine waits to fill with data before attending to whatever other TCP transactions are occurring on the other threads and sockets WinSock has open while a connection is in progress.

The value of TTL (Time To Live) defines how long a packet can stay active before being discarded. The default value is '32'.

1. Open the registry and find the key below.
2. Create a new string value named 'DefaultRcvWindow' and set it to '4288'. If 'DefaultRcvWindow' already exists, then simply modify the current value.
3. Also create another string value named 'DefaultTTL' under the same key and set that to '128'. Again if it already exist, simply modify the value.
4. Exit the registry and reboot your PC.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP]

Value Name: DefaultRcvWindow, DefaultTTL

Data Type: REG_SZ

More info: <http://support.microsoft.com/support/kb/articles/q120/6/42.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Optimizing Dial-Up Modem Connection Speed -

Detailed Information:



Optimizing Dial-Up Modem Connection Speed (Windows 9x)

By optimizing the MaxMTU & MaxMSS settings along with the RWIN and TTL settings you can increase dialup modem connection reliability and performance by as much as 200%.

What is the MTU and MSS?

MTU stands for Maximum Transmission Unit and in basic terms, it defines the maximum size of a packet that can be transferred in one frame over a network.

MSS or Maximum Segment Size defines how much actual data can put in that packet, and it is therefore a marginally smaller value than MTU to allow for packet addressing and other information.

Why do the default values need to be changed?

By default Windows hardcodes the value of MTU to equal 1500 bytes. This value is adequate for normal LAN networking, but when your connecting to the Internet with a modem this value is too high. This can show itself in different ways, the most noticeable affect is less than peak performance.

By adjusting this value to more closely match the requirements of a modem Internet connection huge performance gains can be achieved.

Below are the instructions on how to modify these values for yourself. Please remember though, modifying the Windows registry is not for the faint hearted. Always remember to back it up first!

1. To change the settings you first have to find the details of your Dial-Up Adapter.
2. Find the key HKEY_LOCAL_MACHINE\Enum\Root\Net and within there will be one or more sub-keys such as 0000, 0001 ...
3. Open each key and find the one that contains the value of 'DeviceDesc' equal to 'Dial-Up Adapter'.
4. Within that key there will also be another sub-key named 'Bindings'. Open the 'Bindings' sub-key and you will find a string name like 'MSTCP\0000'. Take note of the four digit number after 'MSTCP' (in this case 0000) and use it in the next step.
5. Now go to the key 'HKEY_LOCAL_MACHINE\Enum\Network\MSTCP' and expand the sub-key with the same four digit number as from the previous step.
6. In this key you will find a value called 'Driver' and it will be equal to something similar to 'NetTrans\0002'. Take note of this four digit number (in this case 0002) and use it in the next step.
7. Now open the key [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans] below there will be one or more sub-key's. Expand the key with the name equal to the four digit number from the previous step.
8. Within this key create a new string value named 'MaxMTU' and set it to '576', and also add a string value named 'MaxMSS' and set it to '536'.
9. Then exit the registry and restart your computer.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans]

Value Name: MaxMTU, MaxMSS

Data Type: REG_SZ

More info: <http://support.microsoft.com/support/kb/articles/q120/6/42.asp>

Source: C:/helpfile/detail/30.html - (119)

- Increase Network Performance -

Detailed Information:



Increase Network Performance (*Windows NT*)

If you increase the number of buffers that the redirector reserves for network performance, it may increase your network throughput. Each extra execution thread that you configure will take 1k of additional nonpaged pool memory, but only if your applications actually use them.

To configure additional buffers and threads, edit:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters

Modify or Add Value of type REG_DWORD for:

'MaxCmds' The range is 0 - 255 and the default is 15

'MaxThreads' Set it to the same value as MaxCmds

You may also want to increase the value of 'MaxCollectionCount'. This REG_DWORD is the buffer for character-mode named pipes writes. The default is 16 and the range is 0 - 65535.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]

Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/56.html - (120)

- Optimize Windows NT TCP/IP Data Retransmissions -

Detailed Information:



Optimize Windows NT TCP/IP Data Retransmissions (*Windows NT*)

This parameter controls the number of times TCP will retransmit an individual data segment (not connection request segments) before aborting the connection.

The retransmission timeout is doubled with each successive retransmission on a connection. It is reset when responses resume. The base timeout value is dynamically determined by the measured round-trip time on the connection.

Note: *The Windows NT TCP/IP implementation is largely self tuning. Adjusting registry parameters may adversely affect system performance.*

Key: [TcpMaxDataRetransmissions]

Value Name: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Data Type: REG_BINARY

Data: 0 - 0xFFFFFFFF (default = 5)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/267.html - (121)

- Change the Maximum Transmission Unit (MTU) Size -

Detailed Information:



Change the Maximum Transmission Unit (MTU) Size (*Windows NT*)

By optimizing the MTU setting you can gain substantial network performance increases, especially when using dial-up modem connections.

MTU stands for Maximum Transmission Unit and in basic terms, it defines the maximum size of a packet that can be transferred in one frame over a network.

Open the registry and find the key below. Add a new value, or edit the existing value, to equal the new MTU size. For modem connections a MTU of '576' would be a good size.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]

Value Name: MTU

Data Type: REG_DWORD

Data: Default = 0xFFFFFFFF

More info: <http://support.microsoft.com/support/ntserver/serviceware/nts40/E9MSLS8FW.ASP>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Optimize Windows NT TCP/IP Connection Retransmissions -

Detailed Information:



Optimize Windows NT TCP/IP Connection Retransmissions (*Windows NT*)

This parameter determines the number of times TCP will retransmit a connect request (SYN) before aborting the attempt. The retransmission timeout is doubled with each successive retransmission in a given connect attempt.

Note: *The Windows NT TCP/IP implementation is largely self tuning. Adjusting registry parameters may adversely affect system performance.*

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]

Value Name: TcpMaxConnectRetransmissions

Data Type: REG_DWORD

Data: 0 - 0xFFFFFFFF (Default = 3)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/266.html - (123)

- Optimize the Windows NT TCP/IP Window Size -

Detailed Information:



Optimize the Windows NT TCP/IP Window Size (*Windows NT*)

This parameter determines the maximum TCP receive window size offered by the system. The receive window specifies the number of bytes a sender may transmit without receiving an acknowledgment.

In general, larger receive windows will improve performance over high delay, high bandwidth networks. For greatest efficiency, the receive window should be an even multiple of the TCP Maximum Segment Size (MSS).

Reducing the TCP Window size effectively causes an acknowledgment to be sent to the sender for data received sooner. This will lower the possibility that the sender will time out while waiting for an acknowledgment. However it will also increase the amount of network traffic and cause slower throughput.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]

Value Name: TcpWindowSize

Data Type: REG_DWORD

Data: 0 - 0xFFFF (default = 8760 for Ethernet)

More info: <http://support.microsoft.com/support/kb/articles/q140/5/52.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- RegEdit.com : Security : Applications : DOS -

Registry Keys:



Disable the MS-DOS Command Prompt *(Windows 9x and NT)*

This setting allows you to disable the use of the MS-DOS command prompt in Windows.



Disable Single Mode MS-DOS Applications in Windows *(Windows 9x and NT)*

This setting allows you to disable the use of real mode DOS applications from within the Windows shell.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Applications/DOS/index.shtml - (125)

- RegEdit.com : Security : Applications : Internet Explorer -

Registry Keys:



Remove the Content Advisor and Ratings Password *(Windows 9x and NT)*

If you've forgotten the Internet Explorer content advisor password and want to change the ratings settings then follow these instructions to change the settings back to their defaults.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Applications/Internet_Explorer/index.shtml - (126)

- RegEdit.com : Security : Control Panel : Display -

Registry Keys:



Hide the Display Appearance Page *(Windows 9x and NT)*

This setting, once enabled, hides the display settings appearance page.



Hide the Display Background Page *(Windows 9x and NT)*

This option hides the background page, stopping users from changing any background display settings.



Hide the Screen Saver Settings Page *(Windows 9x and NT)*

This option hides the screen saver page from the display settings control, which stops users having access to change screen saver settings.



Hide the Display Settings Page *(Windows 9x and NT)*

This option hides the Settings page from the display properties control.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Control_Panel/Display/index.shtml - (127)

- RegEdit.com : Security : Control Panel : Network -

Registry Keys:



Hide the File and Printer Sharing Controls (Windows 9x)

Enabling this options hides the file and printer sharing controls, stopping users from disabling or creating new file or printer shares.



Hide Network Identification Page (Windows 9x)

The Network Identification page include options to set the Computer Name, Workgroup and Description, enabling this option disables access to the Network ID page.



Hide Network Access Control Page (Windows 9x)

The Access Control Page, defines whether the computer support User-Level access or Share-Level access, enabling this option removes access to the Access Control Page.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Control_Panel/Network/index.shtml - (128)

- RegEdit.com : Security : Control Panel : Passwords -

Registry Keys:



Hide the Remote Administration Page (Windows 9x)

Enabling this function stops users from being able to change the remote administration settings for the computer.



Hide the User Profiles Page (Windows 9x)

The user profile page controls whether all users share or have separate user profiles, access to this page can be disabled by enabling this setting.



Hide the Change Passwords Page (Windows 9x)

When this setting is enabled, users are no longer able to access the Change Passwords page.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Control_Panel/Passwords/index.shtml - (129)

- RegEdit.com : Security : Control Panel : Printers -

Registry Keys:



Disable the Addition of Printers (*Windows 9x*)

Any user can add a new printer their system, this option once enabled disables the addition of new printers to the computer.



Disable the Deletion of Printers (*Windows 9x*)

Printers can be deleted simply by anyuser pressing the delete key, enabling this setting stops users from being able to delete printers.



Hide the General and Details Printer Pages (*Windows 9x*)

This option hides the printer details and general printer information pages. Once enabled this option stops users from changing specific printer settings.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Control_Panel/Printers/index.shtml - (130)

- RegEdit.com : Security : Control Panel : System -

Registry Keys:



Hide the Hardware Profiles Page *(Windows 9x)*

The settings when enabled hides the Hardware Profiles page from the System icon on the Control Panel.



Hide the Device Manager Page *(Windows 9x)*

This setting controls whether the Device Manager, under Control Panel / System is visible.



Hide the File System Button *(Windows 9x)*

This option hides the File System button from the System icon on the Control Panel.



Hide the Virtual Memory Button *(Windows 9x)*

This option hides the Virtual Memory button from the System icon on the Control Panel.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Control_Panel/System/index.shtml - (131)

- Deny Access to the Display Settings -

Detailed Information:



Deny Access to the Display Settings (*Windows 9x and NT*)

This option disables the display settings control panel icon, and stops users from accessing any display settings.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoDispCPL

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/167.html - (132)

- Disable Network Control Panel -

Detailed Information:



Disable Network Control Panel (*Windows 9x*)

Enabling this option disables access to the Network Control Panel icon.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: NoNetSetup

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/174.html - (133)

- Disable Printers Control Panel Icon -

Detailed Information:



Disable Printers Control Panel Icon (*Windows 9x*)

This option disables access to the Printers icon in control panel, therefore stopping users from changing Printer settings.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoPrinters

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/177.html - (134)

- Restrict Access to the Passwords Control Panel -

Detailed Information:



Restrict Access to the Passwords Control Panel (Windows 9x)

This options disables access to the Passwords icon on the the control panel, therefore stopping users from changing security related settings.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoSecCPL

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/181.html - (135)

- Disable the Shut Down Command -

Detailed Information:



Disable the Shut Down Command (*Windows 9x and NT*)

This option allows you to stop users from being able to shutdown the computer, by disabling the shut down command.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoClose

Data Type: REG_DWORD

Data: (0 = shutdown enabled, 1 = shutdown disabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/146.html - (136)

- Remove common program groups from Start menu -

Detailed Information:



Remove common program groups from Start menu (*Windows 9x and NT*)

Disables the display of common groups when the user selects Programs from the Start menu.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoCommonGroups

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/158.html - (137)

- Hide All Items on the Desktop -

Detailed Information:



Hide All Items on the Desktop (*Windows 9x and NT*)

Enabling this options hides all the items and programs on the Windows desktop.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoDesktop

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/147.html - (138)

- Hide Drives in My Computer -

Detailed Information:



Hide Drives in My Computer (*Windows 9x and NT*)

This setting controls which drives are visible in 'My Computer', it is possible to hide all drives or just selected ones.

The value of 'NoDrives' defines which drives are visible. The low order (right most) bit is drive A: while the 26th bit is Drive Z: To hide a drive, turn on it's bit.

If your not happy working in Hex, add these decimal numbers to hide the drive(s):

A: 1, B: 2, C: 4, D: 8, E: 16, F: 32, G: 64, H: 128, I: 256, J: 512, K: 1024, L: 2048, M: 4096, N: 8192, O: 16384, P: 32768, Q: 65536, R: 131072, S: 262144, T: 524288, U: 1048576, V: 2097152, W: 4194304, X: 8388608, Y: 16777216, Z: 33554432, ALL: 67108863

Note: *These drives will still appear in File Manager, to remove File Manager, delete winfile.exe.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoDrives

Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/148.html - (139)

- Remove the Favorites Folder from the Start Menu -

Detailed Information:



Remove the Favorites Folder from the Start Menu (*Windows 9x and NT*)

To remove the Favorites folder from the Start menu, modify this registry key.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoFavoritesMenu

Data Type: REG_DWORD

Data: (0=disable, 1=enable)

More info: <http://support.microsoft.com/support/kb/articles/q177/3/32.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Remove File menu from Explorer -

Detailed Information:



Remove File menu from Explorer (Windows NT)

Removes the File option from Explorer's toolbar. (This option was added in Service Pack 2.)

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoFileMenu

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/157.html - (141)

- Remove the Find Command From the Start Menu -

Detailed Information:



Remove the Find Command From the Start Menu (*Windows 9x and NT*)

When enabled, this setting removes the 'Find' command from the Start Menu.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoFind

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/149.html - (142)

- Hide the Network Neighborhood Icon -

Detailed Information:



Hide the Network Neighborhood Icon (*Windows 9x and NT*)

The Network Neighborhood icon is shown on the Windows desktop whenever Windows networking is installed, by enabling this setting the icon will be hidden.

In addition, disables UNC capability from within the Explorer interface, including the Start menu's Run command, UNC paths configured by the administrator in Policies for shared folders, desktop icons, the Start command, and so forth. This does not impair the functionality of the command line Net.exe command.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoNetHood

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/150.html - (143)

- Remove the Documents Folder from the Start Menu -

Detailed Information:



Remove the Documents Folder from the Start Menu (*Windows 9x and NT*)

This key will remove the recent Documents folder from the Start Menu.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoRecentDocsMenu

Data Type: REG_DWORD

Data: (0=disable, 1=enable)

More info: <http://support.microsoft.com/support/kb/articles/q181/3/42.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Remove the Run Command from the Start Menu -

Detailed Information:



Remove the Run Command from the Start Menu (Windows 9x and NT)

Removes the user's ability to start applications or processes from the Start menu by removing the option completely.

Note: *If the user still has access to the MS-DOS prompt icon or command prompt, the user can start unauthorized applications.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoRun

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/151.html - (145)

- Save Explorer Window Settings -

Detailed Information:



Save Explorer Window Settings (Windows 9x and NT)

With this function you can control whether your desktop settings will be saved when you exit Windows.

To change this option find the key below in your registry and edit the value as required.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoSaveSettings

Data Type: REG_BINARY

Data: (00 00 00 00=disable, 01 00 00 00=enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/21.html - (146)

- Don't Save Settings at Exit -

Detailed Information:



Don't Save Settings at Exit (Windows 9x and NT)

Normally when Windows exits it saves the desktop configuration, including icon location, appearance etc. This setting disables these changes from being saved, this is useful in both a secure environment and when you don't want people to change the appearance of your desktop once you have it setup the way you like it.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoSaveSettings

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/152.html - (147)

- Remove Folders from Settings on the Start Menu -

Detailed Information:



Remove Folders from Settings on the Start Menu (*Windows 9x and NT*)

Removes the Control Panel and Printers folders from the Settings menu. Note: Removing the Taskbar, Control Panel, and Printer folders causes the Settings menu to be removed completely.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoSetFolders

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/153.html - (148)

- Remove the Taskbar from Settings on the Start Menu -

Detailed Information:



Remove the Taskbar from Settings on the Start Menu (*Windows 9x and NT*)

Enabling this option, removes the Taskbar option from Settings on the Start Menu, therefore stopping users from changing the taskbar properties. Note: Removing the Taskbar, Control Panel, and Printer folders causes the Settings menu to be removed completely.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoSetTaskbar

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/154.html - (149)

- Disable context menus for the Taskbar -

Detailed Information:



Disable context menus for the Taskbar (*Windows NT*)

Removes the context menus for the tray, including the Start button, Tab control, and Clock. (This option was added in Service Pack 2.)

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoTrayContextMenu

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/159.html - (150)

- Disable Explorer's default context menu -

Detailed Information:



Disable Explorer's default context menu (*Windows NT*)

Removes the context menu that would normally appear when the user right clicks on the desktop or in the Explorer right results pane. (This option was added in Service Pack 2.)

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoViewContextMenu

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/160.html - (151)

- Restricting Applications Users Can Run -

Detailed Information:



Restricting Applications Users Can Run (*Windows 9x and NT*)

Windows gives the ability to restrict the applications that can be run by users on a workstation.

Open your registry and find the key:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Change the value of 'RestrictRun' to '1' for enabled or '0' for disabled. Create the value if it doesn't already exist.

Then define the applications they are allowed to be run at:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun].

Creating a new value for each application, and name them consecutive numbers.

Reboot the computer for the changes to take effect.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: RestrictRun

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/113.html - (152)

- RegEdit.com : Security : Network : Remote Access -

Registry Keys:



Maximum Number of Remote Access Authentication Attempts (Windows NT)

This setting controls the number of authentication retries before the remote access connection is terminated.



Maximum Time Limit for Authentication (Windows NT)

A time limit can be enforced on the length of time given to logon via Remote Access.



Automatically Disconnect Remote Access Callers (Windows NT)

Specifies the amount of idle time in minutes to wait before disconnecting the RAS client.



Define the length of time before callback is initiated (Windows NT)

When callback is required or requested this setting defines how long to wait before initiating the callback connection.



Disable Dial-In Access (Windows 9x and NT)

It's possible for users to setup a modem on a Windows machine, and by using Dial-up Networking allow callers to connect to the internal network. Especially in a corporate environment this can cause a major security risk.



Automatically Use Dial-Up Networking to Logon (Windows NT)

There is an option that is available on the logon dialog box and allows you to dial into your logon server for authentication of your user account, this can be enabled by default.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/Security/Network/Remote_Access/index.shtml - (153)

- Disable File and Printer Sharing -

Detailed Information:



Disable File and Printer Sharing (Windows 9x and NT)

When 'File and printer sharing...' is installed it allows users to make services available to other users on a network, this functionality can be disabled by changing this setting.

1. Using Regedit find the key below, if it doesn't already exist, create it.
2. Create two new DWORD values of 'NoFileSharing' and 'NoPrintSharing'.
3. Modify the values of 'NoFileSharing' and 'NoPrintSharing' to either '1' sharing disabled, or '0' sharing enabled. Both settings do not have to be the same, it is possible to have one disabled and the other enabled.
4. Exit Regedit and reboot.

Key: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/132.html - (154)

- Automatic Hidden Shares -

Detailed Information:



Automatic Hidden Shares (Windows NT)

This key controls whether the administration shares are created ie. c\$ and d\$. Set AutoShareServer to "0" to disable admin shares for a server. Set AutoShareWks to "0" to disable admin shares for a workstation.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters]

Value Name: AutoShareServer, AutoShareWks

Data Type: REG_DWORD

Data: (0=disable, 1=enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/4.html - (155)

- Disabling Save Password option in Dial-Up Networking -

Detailed Information:



Disabling Save Password option in Dial-Up Networking (*Windows NT*)

When you dial a phonebook entry in Dial-Up Networking (DUN), you can use the 'Save Password' option so that your DUN password is cached and you will not need to enter it on successive dial attempts. This key disables that option.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters]

Value Name: DisableSavePassword

Data Type: REG_DWORD

Data: (0=disable, 1=enable)

More info: <http://support.microsoft.com/support/ntserver/serviceware/10140908.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Don't Display Last User Name -

Detailed Information:



Don't Display Last User Name (Windows NT)

Enabling this key will blank the username box on the logon screen. Preventing people that are logging on from knowing the last user on the system.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: DontDisplayLastUserName

Data Type: REG_SZ

Data: (1=enable, 0=disable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/1.html - (157)

- Sending Unencrypted Passwords -

Detailed Information:



Sending Unencrypted Passwords (Windows NT)

Connecting to SMB servers (such as Samba and LAN Manager for UNIX) with an unencrypted (plain text) password fails after upgrading to Windows NT 4.0 Service Pack 3. This is because the SMB redirector in Service Pack 3 handles unencrypted passwords differently than previous versions of Windows NT. Beginning with Service Pack 3, the SMB redirector will not send an unencrypted password unless you add a registry entry to enable unencrypted passwords.

1. Add a new value of "EnablePlainTextPassword" to the key below, modify the value to be a DWORD value of "1".
2. Exit Regedit and Reboot.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters]

Value Name: EnablePlainTextPassword

Data Type: REG_DWORD

Data: (0=disable, 1=enable)

More info: <http://support.microsoft.com/support/kb/articles/q166/7/30.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Hiding Servers from the Browser List -

Detailed Information:



Hiding Servers from the Browser List (*Windows NT*)

If you have a secure server or workstation you wish to hide from the general browser list, add this registry setting.

To hide a server from the browser, edit:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Add value "Hidden" (REG_DWORD) and set it to "1".

Reboot the server. It may take up to ½ hour for the server to disappear from the browse lists.

(Same result can be achieved by executing NET CONFIG SERVER /HIDDEN:YES on the workstation.)

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

Value Name: Hidden

Data Type: REG_DWORD

Data: (0=disable, 1=enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/58.html - (159)

- Hide Share Passwords with Asterisks -

Detailed Information:



Hide Share Passwords with Asterisks (*Windows 9x and NT*)

This setting controls whether the password typed when accessing a file share is shown in clear text or as asterisks.

Key: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: HideSharePwds

Data Type: REG_DWORD

Data: (0 = disabled, 1=enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/122.html - (160)

- Changing LAN Manager Authentication on Windows NT -

Detailed Information:



Changing LAN Manager Authentication on Windows NT (*Windows NT*)

Windows NT supports two kinds of challenge/response authentication: LanManager (LM) and Windows NT (NTLM). LM authentication is not as strong as Windows NT authentication so some customers may want to disable its use, because an attacker sniffing the network traffic could attack the weaker protocol.

The implementation of the NTLM Security Service Provider (SSP) in Server Pack 4 has been enhanced to allow clients to control which variants of NTLM are used, and to allow servers to control which variants they will accept.

To change the type of authentication to be used modify the key below with the following values:

Level 0 - Send LM response and NTLM response; never use NTLMv2 session security

Level 1 - Use NTLMv2 session security if negotiated

Level 2 - Send NTLM response only

Level 3 - Send NTLMv2 response only

Level 4 - DC refuses LM responses

Level 5 - DC refuses LM and NTLM responses (accepts only NTLMv2)

Note: Currently only Windows NT 4.0 (SP4 and greater) support NTLMv2, before making any changes to this key please read the Microsoft Knowledge base article below.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]

Value Name: LMCompatibilityLevel

Data Type: REG_DWORD

Data: 0 (default) to 5 as defined above

More info: <http://support.microsoft.com/support/kb/articles/q1477/06.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Setting a Minimum Password Length -

Detailed Information:



Setting a Minimum Password Length (*Windows 9x and NT*)

You can force Windows to reject passwords that do not meet a minimum password length. Useful to help stop people from using trivial passwords where security is an issue.

1. Using Regedit, open the key below, if the Network sub-key does not already exist then create it.
2. Add a new REG_BINARY value of 'MinPwdLen', and set the data to the minimum number of characters required for a password to be accepted.

Note: *This does not affect existing passwords, only new or changed.*

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: MinPwdLen

Data Type: REG_BINARY

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/108.html - (162)

- Require Validation by Network for Windows Access -

Detailed Information:



Require Validation by Network for Windows Access (Windows 9x)

By default Windows doesn't require a valid network username and password combination for a user to create and use a local Windows machine. This functionality can be change to require validation by the network.

Key: [HKEY_LOCAL_MACHINE\Network\Logon]

Value Name: MustBeValidated

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/130.html - (163)

- Disable Caching of Domain Password -

Detailed Information:



Disable Caching of Domain Password (*Windows 9x and NT*)

Enabling this setting, disables the caching of the NT domain password, and therefore it will need to be re-entered to access additional domain resources.

Key: [HKEY_LOCAL_MACHINE\Network\Logon]

Value Name: NoDomainPwdCaching

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/134.html - (164)

- Defining Local and Remote Drive Visibility Under WinNT -

Detailed Information:



Defining Local and Remote Drive Visibility Under WinNT (*Windows NT*)

Administrators may use the NODRIVES entry to disable access to floppy drives on a per-user basis. The NODRIVES entry uses a 32-bit word to define local and network drive visibility for each logical drive in the computer. The lower 26 bits of the 32-bit word correspond to drive letters A through Z. Drives are visible when set to 0 and hidden when set to 1.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NODRIVES

Data Type: REG_DWORD

Data: A bit mask of 11111111111111111111111111111111 (0x3FFFFFFh) would hide all drive letters.

More info: <http://support.microsoft.com/support/kb/articles/q158/4/57.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/11.html - (165)

- Remove Entire Network from Network Neighborhood -

Detailed Information:



Remove Entire Network from Network Neighborhood (*Windows 9x and NT*)

Entire Network is an option under Network Neighborhood that allows users to see all the Workgroup and Domains on the network. Entire Network can be disabled, so users are confined to their own Workgroup or Domain.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: NoEntireNetwork

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/172.html - (166)

- Remove Log Off <Username> from the Start Menu -

Detailed Information:



Remove Log Off <Username> from the Start Menu (*Windows 9x and NT*)

To remove the Log Off <Username> command from the Start menu, use Registry Editor to modify the following key.

Note: *This setting relies in Internet Explorer 4.0 or greater being installed.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoLogOff

Data Type: REG_BINARY

Data: 01 00 00 00

More info: <http://support.microsoft.com/support/kb/articles/q177/9/03.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Remove the Map and Disconnect Network Drive Options -

Detailed Information:



Remove the Map and Disconnect Network Drive Options (Windows NT)

Prevents users from making additional network connections by removing the Map Network Drive and Disconnect Network Drive buttons from the toolbar in Explorer and also removing the menu items from the Context menu of My Computer and the Tools menu of Explorer. (This option was added in Service Pack 2.)

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoNetConnectDisconnect

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/161.html - (168)

- Hide Workgroup Content from Network Neighborhood -

Detailed Information:



Hide Workgroup Content from Network Neighborhood (*Windows 9x and NT*)

Enabling this option, hides all Workgroup content from being displayed in Network Neighborhood.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: NoWorkgroupContents

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/173.html - (169)

- Changing the Default 14 day Password Expiry Warning -

Detailed Information:



Changing the Default 14 day Password Expiry Warning (*Windows NT*)

This entry specifies the number of days that a warning message is displayed before the user's password expires.

1. Open the registry, and find the key below.
2. Create a new DWORD value and name it 'PasswordExpiryWarning' set the value to equal the number of days at which the Password Change Notification is presented.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: PasswordExpiryWarning

Data Type: REG_DWORD

Data: (Number of Days)

More info: <http://support.microsoft.com/support/kb/articles/q135/4/03.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/209.html - (170)

- Restricting Information Available to Anonymous Logon Users -

Detailed Information:



Restricting Information Available to Anonymous Logon Users (*Windows NT*)

Windows NT has a feature where anonymous logon users can list domain user names and enumerate share names. Customers who want enhanced security have requested the ability to optionally restrict this functionality.

1. Run Registry Editor (regedit.exe).
2. Go to the following key in the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

3. On the Edit menu, click Add Value and use the following entry:

Value Name: RestrictAnonymous
Data Type: REG_DWORD
Value: 1

4. Exit the Registry Editor and restart the computer for the change to take effect.

Note: It is only possible to control this operation after installing Windows NT 4.0 Service Pack 3 or the Windows NT 3.51 hotfix.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Data: (0=disabled, 1=enabled)

More info: <http://support.microsoft.com/support/kb/articles/q143/4/74.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Restricting Access to the Event Logs -

Detailed Information:



Restricting Access to the Event Logs (*Windows NT*)

The Windows NT event log contains records documenting application, security and system events taking place on the machine. These logs can contain sensitive data, and by default, the Guest account has access to view them. This tweak allows you to restrict access to administrators and system accounts only.

Open your registry and find the key below.

Under this key are three sub-keys: Application, Security and System. These subkeys represent each section of the event log. To restrict access to each section create a new DWORD value of 'RestrictGuestAccess' under each sub-key and set it to equal '1'. To restrict access to only certain sections, then only add the value to that specific key.

Restart the machine for changes to take affect.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog]

Value Name: RestrictGuestAccess

Data Type: REG_DWORD

Data: (0 = Guest Access, 1 =Restricted Access)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Secure Network Access to the Windows NT Registry -

Detailed Information:



Secure Network Access to the Windows NT Registry (*Windows NT*)

Windows NT supports accessing a remote registry via the Registry Editor across a network. The default setting allows for users to connect and modify data within the remote registry.

By creating the new key listed below, or modifying the existing key if it already exists, it is possible to control access to the registry remotely.

Use REGEDT32 to modify the permissions on the key below to suit your security requirements, the permissions on this key represent the remote access permissions to the registry.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg]

More info: <http://support.microsoft.com/support/kb/articles/Q155/3/63.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/249.html - (173)

- Securing Network Access to CD-ROM Drives -

Detailed Information:



Securing Network Access to CD-ROM Drives (*Windows NT*)

This setting determines whether data in the CD-ROM drive is accessible to other users. This value entry satisfies, in part, the C2 security requirement that you must be able to secure removable media.

Because the CD-ROM drive is a volume, by default, it is shared as an administrative share on the network. If the value of this entry is 1, the CD-ROM drive is allocated to the user as part of the interactive logon process and, therefore, only the current user can access it. This prevents administrators and remote users (and even the same user at a different workstation) from accessing the drive while the current user is logged on to the computer. The drive is shared again when the current user logs off the computer.

Value Meanings:

- '0' = Compact discs in the CD-ROM drive can be accessed by all administrators in the domain.
- '1' = Only the user logged on locally can access data on the compact discs in the CD-ROM drive.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: AllocateCDRoms

Data Type: REG_SZ

Data: (0 = enabled, 1 = disabled)

More info: <http://support.microsoft.com/support/kb/articles/q172/5/20.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Securing Network Access to Floppy Drives -

Detailed Information:



Securing Network Access to Floppy Drives (*Windows NT*)

This setting determines whether data in the floppy disk drive is accessible to other users. This value entry satisfies, in part, the C2 security requirement that you must be able to secure removable media.

Because the floppy disk drive is a volume, by default it is shared as an administrative share on the network. If the value of this entry is 1, the floppy disk drive is allocated to the user as part of the interactive logon process and, therefore, only the current user can access it. This prevents administrators and remote users (and even the same user at a different workstation) from accessing the drive while the current user is logged on. The drive is shared again when the current user logs off.

Value Meanings:

- '0' = Floppy disks in the floppy disk drive can be accessed by all administrators in the domain.
- '1' = Only the user logged on locally can access data on the floppy disks in the floppy disk drive.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: AllocateFloppies

Data Type: REG_SZ

Data: (0 = enabled, 1 = disabled)

More info: <http://support.microsoft.com/support/kb/articles/q172/5/20.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Require Alphanumeric Windows Password -

Detailed Information:



Require Alphanumeric Windows Password (*Windows 9x and NT*)

Windows by default will accept anything as a password, including nothing. This setting controls whether Windows will require a alphanumeric password, i.e. a password made from a combination of alpha (A, B, C...) and numeric (1, 2, 3 ...) characters.

Key: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: AlphanumPwds

Data Type: REG_DWORD

Data: (0 = disabled, 1=enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/123.html - (176)

- Control the Automatic Restarting of the Shell -

Detailed Information:



Control the Automatic Restarting of the Shell (*Windows NT*)

By default if the Windows NT user interface or one of its components fails, the interface is restarted automatically, the can be changed so that you must restart the interface by logging off and logging on again manually.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: AutoRestartShell

Data Type: REG_DWORD

Data: (0 = disable, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/205.html - (177)

- Clear the Page File at System Shutdown -

Detailed Information:



Clear the Page File at System Shutdown (*Windows NT*)

Windows normally does not clear or recreate the page file. On a heavy used system this can be both a security threat and performance drop. Enabling this setting will cause Windows to clear the page file whenever the system is shutdown.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]

Value Name: ClearPageFileAtShutdown

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/244.html - (178)

- Disable the Change Password Button -

Detailed Information:



Disable the Change Password Button (Windows NT)

This setting disables the 'Change Password' button on the Windows NT Security dialog box. Enabling this setting stops casual users from being able to change the password.

Note: *This functionality requires Windows NT Service Pack 4 or higher.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: DisableChangePassword

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

More info: <http://support.microsoft.com/support/kb/articles/q174/8/40.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/265.html - (179)

- Disable the Lock Workstation Button -

Detailed Information:



Disable the Lock Workstation Button (Windows NT)

Add this setting to the registry to stop unauthorized users from locking machines from the Windows NT Security dialog box.

Note: *This functionality requires Windows NT Service Pack 4 or higher.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: DisableLockWorkstation

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

More info: <http://support.microsoft.com/support/kb/articles/q174/8/40.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/264.html - (180)

- Disabled Password Caching -

Detailed Information:



Disabled Password Caching (Windows 9x and NT)

Normally Windows caches a copy of the users password on the local system to allow for additional automation, this leads to a possible security threat on some systems. Disabling caching means the users passwords are not cached locally. This setting also removes the second Windows password screen and also remove the possibility of networks passwords to get out of sync.

Key: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: DisablePwdCaching

Data Type: REG_DWORD

Data: (0 = disabled, 1=enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/124.html - (181)

- Disable Registry Editing Tools -

Detailed Information:



Disable Registry Editing Tools (*Windows 9x and NT*)

This setting disables user's ability to run Regedit.exe or Regedt32.exe to modify the registry.

Warning: *Be careful with this setting and make sure you don't lock yourself of the registry.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: DisableRegistryTools

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/190.html - (182)

- Disable Task Manager -

Detailed Information:



Disable Task Manager (Windows NT)

Enables or disables the user's ability to start Task Manager to view processes, applications running, and make changes to the priority or state of the individual processes. (This option was added in Service Pack 2.)

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: DisableTaskMgr

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/163.html - (183)

- Legal Notice Dialog Box Before Logon -

Detailed Information:



Legal Notice Dialog Box Before Logon (*Windows 9x and NT*)

Use these fields to create a dialog box that will be presented to any user before logging onto the system. This is useful where you are required by law to warn people that it is illegal to attempt to logon without being an authorized user.

1. Using Regedit find the appropriate key for your operating system.

Windows 9x:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon

Windows NT:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

2. Modify the data of 'LegalNoticeCaption' to represent the caption on the dialog box (e.g. 'WARNING!'). If this value doesn't already exist create it.

3. Then modify the data of 'LegalNoticeText' to represent the body of the dialog box (e.g. 'Do Not Attempt to Logon to this system unless you are an authorized user!')

4. Exit Regedit, reboot, and the next time you boot up you should be presented with the dialog box before logging on.

Note: *This value is limited to 256 characters, you need to install the latest Windows NT service pack to allow up to 1024 characters.*

Value Name:

LegalNoticeCaption, LegalNoticeText

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Change the Message Shown on the Logon Box -

Detailed Information:



Change the Message Shown on the Logon Box (*Windows NT*)

You can personalize (or legalize) the message displayed on the logon box above the user name and password.

Simply create a new string value named 'LogonPrompt' in the key below, and enter the text you want to display. The default message is: 'Enter a user name and password that is valid for this system.'

This feature can be used in conjunction with: [Legal Notice Dialog Box Before Logon](#).

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: LogonPrompt

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/247.html - (185)

- Determines which drives the Autorun feature is enabled on -

Detailed Information:



Determines which drives the Autorun feature is enabled on (Windows 9x and NT)

Determines whether the Autorun feature is enabled on each drive connected to the system. When Autorun is enabled, media is started automatically when it is inserted in the drive.

This value is comprised of 32 bits. The lower 26 bits each represent a drive, with the lowest (right- most) bit representing drive A and the 26th bit from the right representing drive Z. If a bit is set to 0, the autorun feature is enabled on that drive. If a bit is set to 1, the autorun feature is disabled on that drive.

For example, if the value of this entry is 0x8 (1000 binary), autorun is disabled on drive D. Note that a value of 1 in the bit representing the CD- ROM drive takes precedence over the value of Autorun.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoDriveTypeAutoRun

Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/156.html - (186)

- Stopping the KnownDLLs Vulnerability -

Detailed Information:



Stopping the KnownDLLs Vulnerability (*Windows NT*)

In Windows NT, core operating system DLLs are kept in virtual memory and shared between the programs running on the system. This has exposed a vulnerability that could allow a user to gain administrative privileges on the computer the user is interactively logged onto.

To enable stronger protection on system base objects such as the KnownDLLs list, change the value of 'ProtectionMode' to equal '1' in the registry key below.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager]

Value Name: ProtectionMode

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

More info: <http://support.microsoft.com/support/kb/articles/q218/4/73.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/281.html - (187)

- Preventing the Logon Screen Saver from Launching -

Detailed Information:



Preventing the Logon Screen Saver from Launching (*Windows NT*)

Windows NT has a default screen saver called login.scr, which runs even if no screen saver has been selected. This can present a security risk, as it can allow a local user to replace login.scr with another program and have it launched with system privileges.

1. Change the value of 'ScreenSaveActive' to '0' to disable the screen saver.
2. Exit Regedit and Reboot.

Note: An alternative screen saver can be used, if disabling is not an option, simply change the value of 'SCRNSAVE.EXE' in the same to key, to equal the full path of the screen saver you wish to use. A reboot is required for the changes to take affect.

Key: [HKEY_USERS\.DEFAULT\Control Panel\Desktop]

Value Name: ScreenSaveActive

Data Type: REG_SZ

Data: (0 = disabled, 1 =enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/112.html - (188)

- Enable Shutdown from Authentication Dialog Box -

Detailed Information:



Enable Shutdown from Authentication Dialog Box (Windows NT)

When this setting is enabled, you can click 'Shutdown' from the authentication dialog box when the system first starts without having to log in.

Default: *NT Server = Disabled, NT Workstation = Enabled.*

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: ShutdownWithoutLogon

Data Type: REG_SZ

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/135.html - (189)

- Specify executable files to be run by Winlogon -

Detailed Information:



Specify executable files to be run by Winlogon (*Windows NT*)

This setting Specifies executable files to be run by Winlogon in the system context, and can be modified by simply editing the value.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: System

Data Type: REG_SZ

Data: (default = lsass.exe)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/210.html - (190)

- Order the Menu -

Detailed Information:



Order the Menu

It's easy to reorder the items on any Win98 cascading menu by holding down the mouse button and drag a highlighted file or folder up or down the list. With this tip it's even easier to force the entire list into permanent alphabetical order.

Open the Registry Editor and find the key below.

Highlight the Order entry in the Contents pane, then delete it. The list will be in alphabetical order the next time Windows opens.

You'll find a similar Menu subkey under each of the &Program subkeys Accessories, Games and so on). Follow the same procedure to alphabetize those lists, too.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu\&Programs\Menu]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/231.html - (191)

- Speed Up ISP Logon Time -

Detailed Information:



Speed Up ISP Logon Time (Windows 9x)

On some systems it can take a long time to connect to the Internet, you can decrease the time required to connect to your ISP by trying these simple steps.

Open the Dial-Up Networking folder, right click on the icon for your ISP and select 'Properties'.

Chose the 'Server Types' tab, and then under *Advanced Options* uncheck the 'Log on to network' box, and make sure that 'Enabled Software Compression' is checked. From under *Allowed Network Protocols* uncheck 'NetBEUI' and 'IPX/SPX Compatible'.

Next time you connect to your ISP, the connection should be a little faster.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/237.html - (192)

- Faster Modem Dialing -

Detailed Information:



Faster Modem Dialing (*Windows 9x*)

Waiting to long for your modem to dial? This tip lets you reduce the time it takes your modem to dial, and increase your overall modem connection speed.

Open Control Panel | Modems, select your modem and click on Properties. Select the *Connection* tab, and click on 'Advanced'.

In the text box that is labelled 'Extra Settings' at the following text (without the quotation marks) 'S11=40'.

The number specified after S11= (in this case 40) is the time for each tone in milliseconds. Lower numbers equals faster dialling. If your having problems connecting try increasing the number until it works.

Note: *This may not work as planned in some countries and with some modems.*

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/238.html - (193)

- Restart Windows Quickly without Rebooting -

Detailed Information:



Restart Windows Quickly without Rebooting (*Windows 9x*)

Tired of waiting for Windows to restart? Sometimes it can take ages to completely shutdown, then you have to wait for the PC to reset as well. Try this tip to speed up your computer's shutdown procedure.

You can reduce the time it takes for Windows to restart by holding down the SHIFT key while you select 'Shutdown'. This will restart Windows only, and not your whole computer.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/236.html - (194)

- Change the Startup and Shutdown Screens -

Detailed Information:



Change the Startup and Shutdown Screens (*Windows 9x*)

Microsoft has a knack for making the Windows startup and shutdown screens pretty boring. Luckily it's relatively easy to replace these images with pictures of your own.

There are three files which makeup the startup and shutdown screens, they are:

- **LOGO.SYS** - The startup screen, usually located in your C:\ directory.
- **LOGOW.SYS** - The 'Please wait...' screen, usually located in your c:\windows directory.
- **LOGOS.SYS** - The 'It's now safe to turn off your computer.' screen, usually located in your c:\windows directory.

These files are standard 256 color Windows bitmap files with dimensions of 320(w) x 400(h). You can use basically any image editing program to change them (as long as it supports BMP files).

Warning: Before getting started make sure to take a backup copy of all three files (LOGO.SYS may or may not already exist).

1. Copy LOGOW.SYS and LOGOS.SYS to a temporary folder, and rename their extensions to .BMP
2. Using your favourite graphics editor, open the files and modify them to your liking.
3. Once your finished, save the files, change their extensions back to .SYS, and copy them back over the original files in the Windows directory (which you've already backed-up) and you're done.

Alternatively you can create three new BMP files for each screen, just make sure that the proportions of 320(w) x 400(h) are maintained. The file once finished should be 129,078 bytes.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Make Windows Start Without Asking for a Password -

Detailed Information:



Make Windows Start Without Asking for a Password (*Windows 9x*)

Does Windows prompt you for a password every time you boot up even though you're the only one using the PC? Follow these instructions to make Windows automatically start up without prompting you for a password.

Windows 9x passwords are stored in a Password List file, these files are stored in the Windows directory and named after your username, they can be recognised by their .PWL extension.

For example if your username was 'John' then your password file would probably be 'c:\windows\john.pwl'

To remove the password prompt start by finding the PWL file relating to your username and delete it.

Now restart Windows and you'll be prompted for a password, don't type anything in the Password box and simply click OK.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/272.html - (196)

- Re-Initailize Your Registry Without Rebooting -

Detailed Information:



Re-Initailize Your Registry Without Rebooting (*Windows 9x*)

Some registry changes require you to restart Windows before they are enabled. This tip lets you reinitialize your registry and refresh your desktop without having to leave Windows.

Save your work before attempting this tip!

Press CTRL + ALT + DELETE, to bring up the Windows task list. Highlight 'Explorer' and click on 'End Task', if the Shutdown screen is shown, click 'Cancel'. After a few seconds an error message will popup, click on 'End Task' and the Windows explorer will be reloaded along with any new registry settings.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/239.html - (197)

- View Which HotFix Patches Have Been Installed -

Detailed Information:



View Which HotFix Patches Have Been Installed (*Windows NT*)

Periodically Microsoft releases HotFix's to patch bugs in Windows NT and other products, this key contains information about which Hotfix's have been installed.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/104.html - (198)

- Removing Windows NT Devices and Services -

Detailed Information:



Removing Windows NT Devices and Services (*Windows NT*)

Sometimes it is possible to get orphaned services remaining in the registry. These services can be removed by modifying this key.

1. Open your registry and find the key below.
2. Under this key are subkeys representing each device and service installed on the machine.
3. To remove, first stop the service through Control Panel / Services, then locate the subkey corresponding to device or service and delete it.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/197.html - (199)

- Reduce the Time the Startup List is Shown on Boot -

Detailed Information:



Reduce the Time the Startup List is Shown on Boot (*Windows NT*)

30 Seconds is a long time when you're waiting for Windows NT to boot. With this tip you can decrease the time the system waits for a selection, or remove the time-out all together.

The simple way to modify the time-out is to open Control Panel >System. Then click on the 'Startup/Shutdown' tab and change the value of 'Show list for'. Any value between 1-999 is valid, if you choose '0' the system will wait forever for you to make a selection.

If you would like to boot Windows without waiting for the time-out the process is slightly more difficult.

Using Windows explorer find the file called BOOT.INI on your system drive. Make the file writeable, by right clicking on it and choosing Properties, and then under Attributes, uncheck 'Read-only' and click OK. Now double-click on BOOT.INI, and it should open in Notepad.

There is a line under the `[boot loader]` section labeled `timeout=`. The number after the '=' sign is the time in seconds Windows will wait for a selection. To make Windows boot instantly change this value to '-1' (i.e. `timeout=-1`). Save the file, and the next time you reboot Windows NT won't wait for a selection and just load the default OS choice.

For more information about the BOOT.INI file see: http://www.regedit.com/Files/BOOT_INI/

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Change Directories Without Typing the Whole Name -

Detailed Information:



Change Directories Without Typing the Whole Name (*Windows NT*)

Changing directories at the command prompt can be a hit and miss process when long filenames are involved. This tip let you change directories with ease, not matter how long the directory name.

To change a directory quickly you can use wildcards, for example, to change to the 'C:\Program Files' directory simply type:

```
cd c:\prog*
```

Note: *This will work in alphabetical order, therefore if you have two directories named 'c:\dir1' and 'c:\dir2' and you type `cd dir*`, you will be moved to the 'c:\dir1' directory.*

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/245.html - (201)

- Launch the Task Manager Quickly -

Detailed Information:



Launch the Task Manager Quickly (*Windows NT*)

Launching the Task Manager can sometimes be difficult depending on the situation. Some people didn't know that the Task Manager can actually be launched in at least three different ways to make it easier to use when you need it the most.

First Method:

Press CTRL + ALT + DELETE and click on the 'Task Manager...' button on the Windows NT Security dialog.

Second Method:

Right click on the Windows NT taskbar and chose 'Task Manager...'

Third Method:

Press CTRL + SHIFT + ESC and the Task Manager will be launched instantly.

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/246.html - (202)

- Enable Plug-and-Play on Windows NT -

Detailed Information:



Enable Plug-and-Play on Windows NT (*Windows NT*)

By default Windows NT 4.x doesn't support plug-and-play devices, but it can be configured to at least partially support them with a little help.

Find the directory on your Windows NT CD-ROM called \Drvlib\Pnpisa, then open the directory for your system type (standard PC's are x86 or i386). In this directory are two files. To install plug-and-play support, right-click on the file called 'Pnpisa.inf' and select install. You'll need to reboot for the changes to take affect.

Note: *Windows NT should now detect PnP devices, but you may have to configure the settings manually.*

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/248.html - (203)

- Change System Environment Variables -

Detailed Information:



Change System Environment Variables (*Windows NT*)

This key contains the Windows NT system environment variables, variables include Path, Temp, Windir and any other defined values.

Open your registry and find the key below. Modify the value of any existing variables by double-clicking the value name. To create a new variable, select Edit | New | String Value.

Note: A reboot may be required for these changes to take affect.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment]

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/282.html - (204)

- Changing the Behaviour of the Dr. Watson Utility -

Detailed Information:



Changing the Behaviour of the Dr. Watson Utility (*Windows NT*)

By default whenever an application error occurs under Windows NT, Dr. Watson is launched and the debugger started automatically. The extra resources needed for the debugger can sometimes push the system over the edge. It is possible to stop the debugger from launching by changing this setting.

1. Open your registry and find the key below.
2. Change the value of 'Auto' to '0' to disable the automatic debugger.

Note: *To disable Dr. Watson, simply delete the AeDebug subkey and to re-enable simply execute the command 'drwtsn32 -i'.*

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug]

Value Name: Auto

Data Type: REG_SZ

Data: (0 = message, 1 = debugger & message)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/195.html - (205)

- Disable Automatic Cache Updates in NT's DNS Server -

Detailed Information:



Disable Automatic Cache Updates in NT's DNS Server (*Windows NT*)

This value disables that automatic cache updated from the DNS root servers. Useful when there is a problem with the root servers, or if you wish to completely control DNS updates.

1. Open Regedit, find the key below.
2. Change the value of "AutoCacheUpdate" = "00000000" to disable, if it doesn't exist create a new DWORD value.
3. Exit RegEdit and Reboot.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters]

Value Name: AutoCacheUpdate

Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/79.html - (206)

- Change Background Color During Logon -

Detailed Information:



Change Background Color During Logon (*Windows NT*)

Change the default background color of the logon screen.

Modify the value according to the color you want: "0 0 0" for black, "255 255 255" for white, and everything in between.

Key: [HKEY_USERS\.Default\ControlPanel\Colors]

Value Name: Background

Data Type: REG_SZ

Data: 0 0 0 - 255 255 255

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/72.html - (207)

- Configuring Unimodem Support -

Detailed Information:



Configuring Unimodem Support (*Windows NT*)

Windows NT 4.0 and greater support Unimodem modems, if your device is not supported though Windows can be configured to use the MODEM.INF file instead.

1. Open you registry and find the key below.
2. Create a new DWORD value and name it 'EnableUnimodem' set the data to equal to '0' for disabled.
3. Restart Windows NT.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RAS\PROTOCOLS]

Value Name: EnableUnimodem

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/202.html - (208)

- Remove the Tildes in Short Filenames -

Detailed Information:



Remove the Tildes in Short Filenames (*Windows 9x and NT*)

The setting removes the tildes "~" from short filenames.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]

Value Name: NameNumericTail

Data Type: REG_DWORD

Data: (0=disable,1=enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/64.html - (209)

- Stop Error Messages When Booting -

Detailed Information:



Stop Error Messages When Booting (Windows NT)

Stops the annoying Windows pop-up messages notifying you a device is not functioning when you boot-up Windows NT.

Create a REG_DWORD value of 'NoPopupsOnBoot' in the key below (if it doesn't already exist). Set the value to '1' to disable pop-up messages from appearing.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows]

Value Name: NoPopupsOnBoot

Data Type: REG_DWORD

Data: (1 = disable messages)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/98.html - (210)

- Define Whether Windows Parses Autoexec.bat -

Detailed Information:



Define Whether Windows Parses Autoexec.bat (*Windows NT*)

When this value is 1, the environment variables declared in the Autoexec.bat file are included in the user's environment.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: ParseAutoexec

Data Type: REG_SZ

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/162.html - (211)

- Suppress the 'domain controller can not be reached' Message -

Detailed Information:



Suppress the 'domain controller can not be reached' Message (*Windows NT*)

If Windows is unable to contact a domain controller when a user logs in a message is displayed, this message can be suppressed by modifying this setting.

1. Open the registry and find the key below.
2. Create a new DWORD value, name it 'ReportDC' and set the data to equal '1' for the message to be suppressed.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: ReportDC

Data Type: REG_DWORD

Data: (0 = message enabled, 1 = message disabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/208.html - (212)

- PS2 Mouse Port Rate Adjustment -

Detailed Information:



PS2 Mouse Port Rate Adjustment (*Windows NT*)

Ever noticed how your mouse cursor flickers sometimes, or doesn't run as smoothly as a mouse cursor on a Macintosh? That's because the refresh rate is set too low, modify this key to speed things up and make your mouse cursor move smoothly.

1. Click on START>RUN >
2. Type REGEDIT and click OK
3. Find the key listed below and doubleclick on "SampleRate", choose Base >Decimal, then enter a value from 60 - 200, where a higher number = smoother cursor.
4. Close the Registry Editor and restart your PC.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters]

Value Name: SampleRate

Data Type: REG_DWORD

Data: 0 - 200 (default = 60)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/81.html - (213)

- Changing the Startup Mode of a Service -

Detailed Information:



Changing the Startup Mode of a Service (*Windows NT*)

All services have a setting controlling how they are started, i.e. manually, automatically or disabled. This setting can be changed through the registry.

1. Open your registry, and file the key below.
2. Listed under this key are subkeys representing the devices and services on the system.
3. Open the subkey, corresponding to the service you wish to change, and modify the value of 'Start' as per the table below:

Value	Startup Mode
2	Automatic
3	Manual
4	Disabled

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]

Value Name: Start

Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Use Asynchronous or Synchronous Buffer Commits -

Detailed Information:



Use Asynchronous or Synchronous Buffer Commits (*Windows 9x*)

This setting changes function calls to the File-Commit API to return immediately back without checking the data has been correctly written to the disk drive. By default Windows uses synchronous buffer commits, this setting allows you to enable asynchronous as an alternative for applications that may need this functionality.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]

Value Name: AsyncFileCommit

Data Type: REG_DWORD

Data: (0 = sync, 1 = async)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/222.html - (215)

- Control Write Behind Caching -

Detailed Information:



Control Write Behind Caching (Windows 9x)

For increased performance write behind caching is used to write data to the fixed disks, this means that in the event of a system failure there is a possibility that data would not be completely written to the disk. If you have a system critical application you can disable this functionality to be sure that data is written directly to the disk bypassing the cache.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]

Value Name: DriveWriteBehind

Data Type: REG_BINARY

Data: (00 00 00 00 = protected mode, 01 00 00 00 = real mode)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/221.html - (216)

- Configure 32-bit Protected Mode IO Drivers -

Detailed Information:



Configure 32-bit Protected Mode IO Drivers (*Windows 9x*)

This setting controls whether fixed disk access is performed through Windows protected mode drivers or through real mode drivers and BIOS routines. If you are experiencing drive IO errors enabling this setting may be a possible solution.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]

Value Name: ForceRMIO

Data Type: REG_BINARY

Data: (00 00 00 00 = protected mode, 01 00 00 00 = real mode)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/220.html - (217)

- Preserving Long Filenames for Legacy Applications -

Detailed Information:



Preserving Long Filenames for Legacy Applications (*Windows 9x*)

Windows normally preserves the long filenames of files accessed by legacy applications. This functionality can be disabled if you are experiencing LFN errors with a legacy application.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]

Value Name: PreserveLongNames

Data Type: REG_BINARY

Data: (00 00 00 00 = disabled, ff ff ff = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/219.html - (218)

- Configure New File Sharing and Locking Symantics -

Detailed Information:



Configure New File Sharing and Locking Symantics (*Windows 9x*)

This setting controls the file locking mechanisms of Windows 9x, disable this setting only if you are currently experiencing problems with specific applications.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]

Value Name: SoftCompatMode

Data Type: REG_BINARY

Data: (00 00 00 00 = disabled, 01 00 00 00 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/218.html - (219)

- Configure Protected-Mode Hard Disk Interrupt Handling -

Detailed Information:



Configure Protected-Mode Hard Disk Interrupt Handling (*Windows 9x*)

This switch allows Windows to terminate interrupts from the hard disk controller, bypassing the ROM routine that handles these interrupts. Some hard drives might require that this setting be disabled in order for interrupts to be processed correctly. If this setting is disabled, the ROM routine handles the interrupts.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]

Value Name: VirtualHDIRQ

Data Type: REG_BINARY

Data: (00 00 00 00 = disabled, 01 00 00 00 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/217.html - (220)

- Turn On / Off Long Filename Support -

Detailed Information:



Turn On / Off Long Filename Support (*Windows 9x and NT*)

Windows 9x and NT introduced the use of long filenames on existing FAT partitions. Some legacy software maybe incompatible with this new filesystem, and may require the use of 8.3 filenames. Enabling this setting turn off long filename support.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]

Value Name: Win31FileSystem

Data Type: REG_DWORD

Data: (0 = long file names, 1 = 8.3 filenames)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/216.html - (221)

- Remote Access Service (RAS) Device Logging -

Detailed Information:



Remote Access Service (RAS) Device Logging (Windows NT)

Creates a file called DEVICE.LOG in the %SYSTEMROOT%\SYSTEM32\RAS folder for information about commands that the modem is sending and errors that are reported. This file can be very useful in debugging RAS failures.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters]

Value Name: Logging

Data Type: REG_DWORD

Data: (0=disable, 1=enable)

More info: <http://support.microsoft.com/support/ntserver/serviceware/10141181.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/14.html - (222)

- Remote Access Service (RAS) PPP Logging -

Detailed Information:



Remote Access Service (RAS) PPP Logging (Windows NT)

Creates a file called PPP.LOG in the %SYSTEMROOT%\SYSTEM32\RAS folder to help diagnose connectivity problems between a PPP server and a PPP client when one of the computers is a Windows NT Remote Access Service client.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP]

Value Name: Logging

Data Type: REG_DWORD

Data: (0=disable, 1=enable)

More info: <http://support.microsoft.com/support/ntserver/serviceware/10141179.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/15.html - (223)

- New Command Missing in Windows Explorer -

Detailed Information:



New Command Missing in Windows Explorer (Windows 9x and NT)

After you install Internet Explorer with the Windows Desktop Update component you may notice that the New command is missing from the right-click context menu. This tip will help you fix the problem.

To resolve this issue, use Registry Editor to verify that the registry key listed below has the value listed, and if needed, edit the value to match the value listed.

Note: *This registry entry only exists if the Windows Desktop Update component is installed. If the Windows Desktop Update component is not installed, add the registry entry and (Default) value.*

Key: [HKEY_CLASSES_ROOT\Directory\Background\shellex\ContextMenuHandlers\New]

Value Name: (Default)

Data Type: REG_SZ

Data: {D969A300-E7FF-11d0-A93B-00A0C90F2719}

More info: <http://support.microsoft.com/support/kb/articles/q180/2/57.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Change the Default Mailbox Sound Setting -

Detailed Information:



Change the Default Mailbox Sound Setting (Windows 9x and NT)

When you receive a new message, a sound may not be played even though "Play sound when new messages arrive" is enabled.

This registry key displays the path to the Windows 9x and NT default 'new mail' sound. It is recommended to first check the sound control panel to make sure a sound is selected for New Mail notification.

Key: [HKEY_CURRENT_USER\AppData\Local\Microsoft\Windows\CurrentVersion\Sound\Default\MailBeep\current]

Value Name: (Default)

Data Type: REG_SZ

More info: <http://support.microsoft.com/support/kb/articles/q190/3/04.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/70.html - (225)

- Addition of New LAN Interface in RRAS Causes Event Message -

Detailed Information:



Addition of New LAN Interface in RRAS Causes Event Message (Windows NT)

When you install an additional network interface card (NIC) and the Routing and Remote Access Service (RRAS) is already installed, you receive an error 20101 in the System Log in Event Viewer.

This event will be logged every time RRAS starts yet does not prevent RRAS from starting properly, nor does it cause any loss of functionality within RRAS.

For each value of (x) in the key below, verify the value of 'Enabled' is equal to '1' or '0', the default is '1' Enabled.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Router\Interfaces\{x}]

Value Name: Enabled

Data Type: REG_DWORD

Data: (0 = false, 1 = true)

More info: <http://support.microsoft.com/support/kb/articles/q1877/93.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/252.html - (226)

- Shortcuts Created Resolve to UNC Paths -

Detailed Information:



Shortcuts Created Resolve to UNC Paths (*Windows NT*)

A Windows NT user may click a program's shortcut and be prompted to Enter Network Password, yet the properties of the shortcut indicate a relative path to the local computer.

Shortcuts created on a computer automatically embed a UNC (Universal Naming Convention) path such as \\ <computer>\admin\$ in the .lnk file. The default shortcut resolution method is to resolve the link to the original location of the file (the "absolute" path) before looking at another path of where that file may or may not exist (the secondary or "relative" path). In this case, the UNC path to the original file is always reachable, which prevents the link from being resolved by means of a local path. As a result, the user who is trying to run the shortcut is prompted for the administrator's password of the computer that created the link.

1. Open the registry and find the key below.
2. Create a new DWORD value of 'LinkResolveIgnoreLinkInfo' and set the value to '1' for enabled.
3. Exit the registry editor and reboot for the changes to take place.

Note: To apply this change on a per computer basis modify the same key under the HKEY_LOCAL_MACHINE hive.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: LinkResolveIgnoreLinkInfo

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

More info: <http://support.microsoft.com/support/kb/articles/q158/6/82.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Windows 98 Problem - Long File Names Need to be Enabled -

Detailed Information:



Windows 98 Problem - Long File Names Need to be Enabled (*Windows 98*)

If you are receiving an error when installing Windows 98 that long file names need to be enabled in order for Windows 98 to install successfully try this.

Run Regedit and find the key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem.

Look for an entry in the right pane titled "NameNumericTail" and delete it.

Close RegEdit, reboot and retry the installation.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]

Value Name: NameNumericTail

Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/78.html - (228)

- CD-ROM Does Not Run Automatically When Inserted -

Detailed Information:



CD-ROM Does Not Run Automatically When Inserted (*Windows 9x*)

When you insert a CD-ROM into the CD-ROM drive, it may not be run automatically, changing this registry key should correct the problem.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoDriveTypeAutoRun

Data Type: REG_BINARY

Data: 0000 95 00 00 00

More info: <http://support.microsoft.com/support/kb/articles/q177/8/80.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Unable to Connect More Than 10 Clients -

Detailed Information:



Unable to Connect More Than 10 Clients (*Windows NT*)

If you have a retail version of Windows NT server, and you are still unable to connect more the 10 users concurrently, then have a look at this tip.

Open the key below, and find the value of 'Users', if the value doesn't exist then create a new DWORD value. Change the value to equal 'FFFFFFFF' in hex and reboot.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

Value Name: Users

Data Type: REG_DWORD

Data: (ffffff = unlimited)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/250.html - (230)

- How to Restore the Animated Internet Explorer Logo -

Detailed Information:



How to Restore the Animated Internet Explorer Logo (*Windows 9x and NT*)

When you browse the Internet using Internet Explorer, the animated logo spins indicating that activity is taking place. This registry setting controls which logo is being shown.

To restore the default animated Internet Explorer logo, delete the "BrandBitmap" and "SmBrandBitmap" string values found under the registry key below.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar]

More info: <http://support.microsoft.com/support/kb/articles/q176/7/13.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/83.html - (231)

- Internet Explorer Intercepts the FTP Command -

Detailed Information:



Internet Explorer Intercepts the FTP Command (*Windows 9x and NT*)

When you enter a FTP command such as "FTP ftp.regedit.com" IE 4.0 launches instead of the DOS based FTP program.

To disable this behaviour, use Regedit to find the key below, and delete the value of "ftp".

To re-enable, create a REG_SZ value of "ftp" and set the data to "ftp://".

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/69.html - (232)

- Modifying the Internet Explorer Partial Address Feature -

Detailed Information:



Modifying the Internet Explorer Partial Address Feature (*Windows 9x and NT*)

The Internet Explorer partial address feature, scans common domains for a match to a keyword entered in the Address bar. The feature is limited by default to searching only .COM, .EDU and .ORG domains. This tip allows you to add new domains and modify their priorities.

The values listed under the key below control which domains are auto searched for matches to the keyword entered in the Address bar.

To add a new domain simply create a new string value and name it a sequential number (e.g. '7'). Set the data of the new value to equal the domain you want to search, for example to also search .DE domains add a new value of 'www.%s.de' (%s represents the keyword).

To change their priorities, simply rename the values with sequential numbers where '1' is the site to be checked first.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\UriTemplate]

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/261.html - (233)

- Change the Internet Explorer Search Engine -

Detailed Information:



Change the Internet Explorer Search Engine (*Windows 9x and NT*)

Normally when you type 'go keyword' in the Internet Explorer address bar IE will search the web using a Microsoft selected search engine. By modifying this key you can select which search engine to use.

Open you registry and find the key below.

Modify the value of default to equal the URL for the search engine you want to use, substituting '%s' to represent the keywords.

For example, to use Altavista the value would be:

`http://www.altavista.com/cgi-bin/query?q=%s`

And to use Yahoo! the value would be:

`http://search.yahoo.com/bin/search?p=%s`

Key: [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchUrl]

Value Name: (Default)

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/289.html - (234)

- Add a Background Bitmap to the Internet Explorer ToolBar -

Detailed Information:



Add a Background Bitmap to the Internet Explorer ToolBar (*Windows 9x and NT*)

Want to have you own bitmap shown on the Internet Explorer toolbar? It's simple with the Registry setting.

1. Open Regedit and find the key below.
2. Add a new String Value of "BackBitmap" and set the value to the path and name of bitmap file you wish to use (eg. "C:\WINDOWS\CLOUDS.BMP")
3. Exit Regedit and restart Internet Explorer.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\ToolBar]

Value Name: BackBitmap

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/66.html - (235)

- Hide the Internet Explorer Icon -

Detailed Information:



Hide the Internet Explorer Icon (*Windows 9x and NT*)

This option hides the Internet Explorer icon from the Windows desktop.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoInternetIcon

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/191.html - (236)

- Proxy Server Configuration -

Detailed Information:



Proxy Server Configuration (*Windows 9x and NT*)

If you need to configure a proxy server on multiple computers, or would just like to automate the procedure through the registry then this tip will explain how.

Open the registry and find the key below.

The values that configure the Internet proxy setup are located in this key. To change which proxy server is used, modify the value of 'ProxyServer' to equal the server and port combination. For example if your proxy server was called \\PROXY and it was running on port 80 then the setting would equal 'PROXY:80'.

You may also need to set the value of 'ProxyEnable' to equal '1' for proxy enabled or '0' for disabled. Setting the value of 'ProxyOverride' to equal '<local>' will stop internal addresses from going through the proxy.

Note: Changes should take effect immediately.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]

Value Name: ProxyServer

Data Type: REG_SZ

Data: Server:Port

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/292.html - (237)

- Change the Location of the Outlook Express Mail and News Files -

Detailed Information:



Change the Location of the Outlook Express Mail and News Files (Windows 9x and NT)

If you have installed Windows on a separate partition and want to keep it free of any unnecessary files, you can change the location of the mail and news files stored by Outlook Express to another partition.

Change the value of 'Store Root' in the key below to equal the new path.

Don't forget to move the 'mail' and 'news' folder from the old location to the new.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Outlook Express]

Value Name: Store Root

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/100.html - (238)

- Changing the Internet Explorer Window Title -

Detailed Information:



Changing the Internet Explorer Window Title (*Windows 9x and NT*)

This setting allows you to customize Internet Explorer by using your own window title. For example you could rename IE to 'My Browser' or anything else you like!

Open your registry and find the key below.

Create a new string value, or modify the existing value, to equal the title you would like.

Note: Delete the value of 'WindowTitle' to change the title back to the default.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main]

Value Name: Window Title

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/62.html - (239)

- Remove the Outlook Express Splash Screen -

Detailed Information:



Remove the Outlook Express Splash Screen (Windows 9x and NT)

Sick of the Outlook Express splash screen everytime you start? This tip will help you remove it.

Open your registry and create a new value called 'NoSplash' in the key below.

Change the value to equal '1' to disable the splash screen.

Exit the registry and restart Outlook Express.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Outlook Express]

Value Name: NoSplash

Data Type: REG_DWORD

Data: 1 = No Splash Screen,0 = Splash Screen

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/345.html - (240)

- Colorful Message Backgrounds -

Detailed Information:



Colorful Message Backgrounds (Windows 9x and NT)

This setting enables colorful backgrounds with Outlook Express.

Open your registry and find the key below.

Change the value of 'ColorCycle' to equal '1' for enabled.

Close the registry and open Outlook Express. Open a new message and hold down CTRL + SHIFT, then press the 'Z' key to cycle through the colored backgrounds.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Internet Mail and News]

Value Name: ColorCycle

Data Type: REG_SZ

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/343.html - (241)

- Change the Outlook Express Window Title -

Detailed Information:



Change the Outlook Express Window Title (*Windows 9x and NT*)

This setting allows you to customize Outlook Express by using your own window title. For example you could rename Outlook Express to 'My Mail Reader' or anything else you like!

Open your registry and find the key below.

Create a new string value, or modify the existing value, to equal the title you would like.

Note: Delete the value of 'WindowTitle' to change the title back to the default.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Outlook Express]

Value Name: WindowTitle

Data Type: REG_SZ

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/342.html - (242)

- Use Computer Name Instead of Caller Name (pcANYWHERE) -

Detailed Information:



Use Computer Name Instead of Caller Name (pcANYWHERE) (Windows 9x and NT)

When this key is set, if a host has the "Prompt to confirm connection" option checked, the host computer's prompt dialog will display the remote's computer name instead of the caller's name when a connection is made.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Host]

Value Name: ConfirmComputerName

Data Type: REG_DWORD

Data: (0 = Use Caller name, 1 = Use remote's Computer name)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/327.html - (243)

- Confirm File Delete (pcANYWHERE) -

Detailed Information:



Confirm File Delete (pcANYWHERE) (Windows 9x and NT)

When this setting is disabled, the remote does not display the confirm prompt when deleting a file.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\File Transfer]

Value Name: ConfirmDelete

Data Type: REG_DWORD

Data: (0 = Disabled, 1 = Enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/334.html - (244)

- Confirm File Send (pcANYWHERE) -

Detailed Information:



Confirm File Send (pcANYWHERE) (Windows 9x and NT)

When this setting is disabled, the remote does not display the confirm prompt when sending a file.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\File Transfer]

Value Name: ConfirmSend

Data Type: REG_DWORD

Data: (0 = Disabled, 1 = Enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/333.html - (245)

- Display Host in List (pcANYWHERE) -

Detailed Information:



Display Host in List (pcANYWHERE) (Windows 9x and NT)

The registry entry allows the host to respond to remote requests for names. Thus, by disabling the registry item, you can hide the host from users scanning the network.

Use this setting so the host will not appear in a remote's list when the remote is scanning the network.

If the remote specifies the name of a host that has the DisplayHostInList option disabled, the host will appear in the remote's list, but the name displayed in the remote's list will not change from whatever the remote user entered.

Note: This item currently only refers to TCP/IP hosts.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: DisplayHostInList

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/295.html - (246)

- Hide the Record Session Button (pcANYWHERE) -

Detailed Information:



Hide the Record Session Button (pcANYWHERE) (*Windows 9x and NT*)

Use this registry key to hide the Record Session icon from the remote session toolbar.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Remote Control]

Value Name: HideRecordingButton

Data Type: REG_DWORD

Data: (0 = Visible, 1 = Hidden)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/320.html - (247)

- Configure IPX Search Mode (pcANYWHERE) -

Detailed Information:



Configure IPX Search Mode (pcANYWHERE) (Windows 9x and NT)

This registry item enables the SAP method of network search instead of using the bindery when making IPX connections.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: IPXUseNBSapMethod

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/319.html - (248)

- Host Connection Time-Out (pcANYWHERE) -

Detailed Information:



Host Connection Time-Out (pcANYWHERE) (*Windows 9x and NT*)

If pcANYWHERE host does not respond, hang up. This is useful for scripts that call systems where a modem will answer, but the pcANYWHERE host may not be running.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Remote Control]

Value Name: NonPCAHostTimeout

Data Type: REG_DWORD

Data: Time in Seconds (0 = Forever)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/324.html - (249)

- Wait for Call After Disconnect (pcANYWHERE) -

Detailed Information:



Wait for Call After Disconnect (pcANYWHERE) (Windows 9x and NT)

If enabled, the host will not wait for a call when the remote disconnects.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Host]

Value Name: OnlyOneGoodConnection

Data Type: REG_DWORD

Data: (0 = Host waits for a call after each connection, 1 = Do not wait for a call)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/328.html - (250)

- Compatibility with the OnNet 2.1 TCP/IP Stack (pcANYWHERE) -

Detailed Information:



Compatibility with the OnNet 2.1 TCP/IP Stack (pcANYWHERE) (Windows 9x and NT)

This registry item resolves an issue where pcANYWHERE displayed the wrong host IP address when using FTP's OnNet 2.1 TCP/IP stack.

When this is set to 1, pcANYWHERE32 8.0 uses the default IP address as defined by the FTP software.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Host]

Value Name: OnNet

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/304.html - (251)

- Configure Persistent Cache (pcANYWHERE) -

Detailed Information:



Configure Persistent Cache (pcANYWHERE) *(Windows 9x and NT)*

This setting turns pcANYWHERE's persistent cache feature on or off.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Host]

Value Name: PersistentCache

Data Type: REG_DWORD

Data: (0 = Off, 1 = On)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/329.html - (252)

- Configure Legacy Remote Print Mode (pcANYWHERE) -

Detailed Information:



Configure Legacy Remote Print Mode (pcANYWHERE) (Windows 9x and NT)

This setting specifies the default print destination when connecting to a pcANYWHERE 2.0 or 5.0 host.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Remote Control]

Value Name: Print

Data: (0 = Discard, 1 = Host, 2 = Remote, 3 = Host and Remote)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/322.html - (253)

- Remote Printer Inactivity Time-out (pcANYWHERE) -

Detailed Information:



Remote Printer Inactivity Time-out (pcANYWHERE) (Windows 9x and NT)

Use this setting if a print job is being separated into multiple jobs during remote printing. This item sets the inactivity time-out for the remote printing facility.

If there is no activity on the port being captured for remote printing, pcANYWHERE32 assumes the printing job is done and stop spooling. This may cause a print job to be separated into multiple jobs if there is a long delay during the printing. This DWORD registry item allows you to adjust the length in seconds of the inactivity on the captured port before pcANYWHERE assumes a print job has stopped spooling.

The default is 30 seconds. To adjust the inactivity time-out, add the registry item as a DWORD set to the number of seconds you want.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Remote Control]

Value Name: PrinterFlushTimeout

Data Type: REG_DWORD

Data: Seconds before assuming print job has completed

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Multi-Processor Options (pcANYWHERE) -

Detailed Information:



Multi-Processor Options (pcANYWHERE) (Windows 9x and NT)

This registry item specifies which processors pcANYWHERE32 8.0 will run on.

To have pcANYWHERE32 8.0 run on a specific processor, set this value according to the table below. If you want pcANYWHERE32 8.0 to run on several specific processors, then set this value to the sum of the values below.

Value	Processor
0	All
1	1
2	2
4	3
8	4
16	5
32	6
64	7
128	8

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Host]

Value Name: ProcessorMask

Data Type: REG_DWORD

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/330.html - (255)

- Prompt for TCP/IP Host (pcANYWHERE) -

Detailed Information:



Prompt for TCP/IP Host (pcANYWHERE) (Windows 9x and NT)

This registry item allows a TCP/IP remote to specify an IP address or name when you leave the "Host To Connect To" field blank.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Remote Control]

Value Name: PromptForTCPIPHost

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/305.html - (256)

- Prompt If Logged Out (pcANYWHERE) -

Detailed Information:



Prompt If Logged Out (pcANYWHERE) (Windows 9x and NT)

This registry key allows you to specify how pcANYWHERE32 will handle a remote connection when the pcANYWHERE32 host is waiting at the Windows NT login screen and the "Prompt On Connection" and "Disconnect On Timeout" options have been checked.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Host]

Value Name: PromptIfLoggedOut

Data Type: REG_DWORD

Data: (0 = User Will Connect, 1 = User Won't Connect)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/331.html - (257)

- Ignore DSR on Serial Devices (pcANYWHERE) -

Detailed Information:



Ignore DSR on Serial Devices (pcANYWHERE) (*Windows 9x and NT*)

Use this item for modems or other serial devices that do not initialize correctly because their DSR is not initially set. It is also useful if the modem connection does not have a DSR line.

This registry item forces the computer to ignore the DSR setting of the attached modem or serial device. Thus, you can get around the requirement of setting a modem's DSR high.

The default is to ignore the DSR. To respect the DSR, add the registry item as a DWORD and set it to a value of zero.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: SerialIgnoreDSR

Data Type: REG_DWORD

Data: (0 = Respect DSR, 1= Ignore DSR)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/316.html - (258)

- Change Serial 56K Connection Speed (pcANYWHERE) -

Detailed Information:



Change Serial 56K Connection Speed (pcANYWHERE) (Windows 9x and NT)

Use this item when a serial connection can be made at 38,400 bps and 115,000 bps, but not at 57,600 bps.

This setting changes the default serial speed from 57,600 bps to 56,000 bps when you select 57,600 bps. It does not affect TAPI serial speeds.

The default is not to change the serial speed. To use 56,000 bps instead of 57,600 bps, add the registry item as a DWORD and set it to a value other than zero.

Note: Use only for Digiboards under Windows NT.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: SerialUse56000

Data Type: REG_DWORD

Data: (0 = Do not change, 1 = Change)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Run the pcANYWHERE Service in Stealth Mode (pcANYWHERE) -

Detailed Information:



Run the pcANYWHERE Service in Stealth Mode (pcANYWHERE) *(Windows 9x and NT)*

Use this setting to hide the Host Waiting icon and Waiting dialog.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Host]

Value Name: ServiceStealthMode

Data Type: REG_DWORD

Data: (0 = Show Icon, 1 = Hide Icon)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/326.html - (260)

- Show Full Screen Reminder Message (pcANYWHERE) -

Detailed Information:



Show Full Screen Reminder Message (pcANYWHERE) (Windows 9x and NT)

This setting turns the Full Screen Reminder Message on or off.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\Remote Control]

Value Name: ShowAltEnterMsg

Data Type: REG_DWORD

Data: (0 =disabled, 1 = enabled)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/323.html - (261)

- Run Smart Setup (pcANYWHERE) -

Detailed Information:



Run Smart Setup (pcANYWHERE) (Windows 9x and NT)

This setting controls whether SmartSetup is run when pcANYWHERE is loaded for the first time.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: SmartSetup

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/325.html - (262)

- Speed Send File Size Limits (pcANYWHERE) -

Detailed Information:



Speed Send File Size Limits (pcANYWHERE) (*Windows 9x and NT*)

The minimum size a file must be for SpeedSend to work is 10K. You can change this value.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\File Transfer]

Value Name: SpeedSend Minimum Size

Data Type: REG_DWORD

Data: Size in KB (Default = 10)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/332.html - (263)

- Add an Additional Delay to Browse Packets (pcANYWHERE) -

Detailed Information:



Add an Additional Delay to Browse Packets (pcANYWHERE) (Windows 9x and NT)

Use this setting when remotes display an incomplete list of TCP/IP hosts in the host list over a WAN or LAN connection.

The entry allows you to set the amount of delay used to create the remote's browse list. Technically, it adds 0.01 seconds between broadcast packets, and waits one additional second for the host's response for each unit of delay set.

For example, a setting of 2 means wait .02 additional seconds between each packet and an additional 2 seconds to receive the response from those broadcasts.

If you are having problems over a WAN connection, start with a setting of 1. If the setting does not work correctly, increase the number until the entire host list is displayed.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPBrowseDelay

Data Type: REG_DWORD

Data: Delay in Milliseconds

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Conect to TCP/IP Hosts With Unknown Status (pcANYWHERE) -

Detailed Information:



Conect to TCP/IP Hosts With Unknown Status (pcANYWHERE) (*Windows 9x and NT*)

This registry entry allows a remote to try to connect to a host if the host's status is unknown. The usual reason for not knowing the host's status is that direct packets have been filtered by a firewall between the host and the remote.

An unfortunate side effect of enabling this key is that if the host's status is unknown to the remote, but the host is actually busy, the remote will receive a blank screen when it tries to connect. The remote can cancel from this screen and make another connection without difficulty. Sometimes, due to the length of time that the browse list updates take, updates will be turned off. By setting this item, you ensure that the list delays will not be turned off due to the length of time they take.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPConnectIfUnknown

Data Type: REG_DWORD

Data: (0 = Use UDP directed packets, 1 = Do not use UDP directed packets)

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/297.html - (265)

- Configure the TCP/IP Data Port (pcANYWHERE) -

Detailed Information:



Configure the TCP/IP Data Port (pcANYWHERE) (Windows 9x and NT)

Use this setting to select which TCP data port pcANYWHERE32 uses.

Note: Version 7.52's remote always uses the value in this registry entry. Version 8.0 remotes only use this entry if the TCPIPNetBroadcast entry equals 1.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPDataPort

Data Type: REG_BINARY

Data: 15FF (HEX) = Registered Port (Default)

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/298.html - (266)

- Adapter Binding Mode (pcANYWHERE) -

Detailed Information:



Adapter Binding Mode (pcANYWHERE) (Windows 9x and NT)

This registry item allows a waiting host to bind to a new adapter, such as a dial-up adapter, without reinitializing the host.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPHostAdapterMode

Data Type: REG_DWORD

Data: (0 = bind to the default network adapter, 1 = bind to all network adapters)

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/306.html - (267)

- Specify Host Mode TCP/IP Address (pcANYWHERE) -

Detailed Information:



Specify Host Mode TCP/IP Address (pcANYWHERE) (Windows 9x and NT)

This registry item allows you to specify which TCP/IP address index the host will wait on.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPHostAddressIndex

Data Type: REG_DWORD

Data: TCP/IP address index to wait on

More info: <http://service1.symantec.com/SUPPORT/pca.nsf/docid/19973683442>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- TCP/IP Host Binding Mode (pcANYWHERE) -

Detailed Information:



TCP/IP Host Binding Mode (pcANYWHERE) (Windows 9x and NT)

This registry item allows you to specify whether the host will wait on the first TCP/IP address given by the operating system, or whether it will wait on the TCP/IP index as indicated by TCPIPHostAddressIndex.

Note: Requires version 8.02 or higher.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPHostBindMode

Data Type: REG_DWORD

Data: (0 = Use first or default TCP/IP address, 2 = Use TCP/IP address index as indicated by TCPIPHostAddressIndex)

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/307.html - (269)

- Multicast Packet Delay (pcANYWHERE) -

Detailed Information:



Multicast Packet Delay (pcANYWHERE) (Windows 9x and NT)

This sets the delay in milliseconds between each send. This is useful if multicast error correction is disabled.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPiPMcastDataDelay

Data Type: REG_DWORD

Data: Delay in Milliseconds (0 = disabled)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/309.html - (270)

- Configure the Multicast Data Port (pcANYWHERE) -

Detailed Information:



Configure the Multicast Data Port (pcANYWHERE) (Windows 9x and NT)

This setting selects the port that the multicast data is sent to.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPmcastDataPort

Data Type: REG_BINARY

Data: (0x15ff = Default)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/310.html - (271)

- Multicast Error Correction (pcANYWHERE) -

Detailed Information:



Multicast Error Correction (pcANYWHERE) (Windows 9x and NT)

This sets the level of error correction used on the host. The host specifies which level of error correction the remotes will use.

If you set this to '0' (disabled), you should use TCIPMcastDataDelay to slow the sends from the host to minimize the loss on slow remotes.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCIPMcastErrorCorrect

Data Type: REG_DWORD

Data: (0 = disabled, 2 = Full error correction)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/311.html - (272)

- Configure Multicast Send and Receive Buffers (pcANYWHERE) -

Detailed Information:



Configure Multicast Send and Receive Buffers (pcANYWHERE) (Windows 9x and NT)

These registry items set the number of receive and send buffers when using an error correction multicast session. For slow remotes, a larger value may lead to less data loss.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCIPMcastHostNumRecvBuf, TCIPMcastHostNumSendBuf, TCIPMcastRemNumRecvBuf, TCIPMcastRemNumSendBuf

Data Type: REG_DWORD

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/313.html - (273)

- Multicast Adapter Selection (pcANYWHERE) -

Detailed Information:



Multicast Adapter Selection (pcANYWHERE) (Windows 9x and NT)

Use this registry item for a multihomed, multicast host that is not binding to the correct network card. This can be why none of the remotes receive the multicast packets.

To specify a particular network card, specify its number. For example, to force the multicast packet to be sent from the second network card, set this registry item to 2. Although the network card order is fairly stable, the order may change according to current DHCP and RAS status. To display the current network card order, run WINIPCFG.EXE for Windows 95, or IPCONFIG.EXE for Windows NT.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPmcastInterface

Data Type: REG_DWORD

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/312.html - (274)

- Multicast Maximum Transmission Unit (pcANYWHERE) -

Detailed Information:



Multicast Maximum Transmission Unit (pcANYWHERE) (Windows 9x and NT)

This registry item sets the Maximum Transmission Unit (MTU) in bytes. The MTU is the maximum bytes that may be sent as one IP multicast packet.

The largest supported value is 10,239. Do not set this value below its default of 1400 bytes.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPmcastMTU

Data Type: REG_DWORD

Data: 1400 - 10,239 bytes

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/314.html - (275)

- Multicast Winsock Receive Buffer (pcANYWHERE) -

Detailed Information:



Multicast Winsock Receive Buffer (pcANYWHERE) (Windows 9x and NT)

This registry item sets the size in bytes of the Winsock receive buffer.

If error correction is off, set this value to 16384 bytes to minimize loss of data on the view-only remotes.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPmcastWSRecvBuf

Data Type: REG_DWORD

Data: Size in Bytes (Default = 8000)

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/315.html - (276)

- TCP/IP Broadcast Mode (pcANYWHERE) -

Detailed Information:



TCP/IP Broadcast Mode (pcANYWHERE) (Windows 9x and NT)

Use this setting to turn off or modify pcANYWHERE32's broadcast options to limit network traffic when the remote browses for a host.

If this is set to '0', only the hosts specified in Applications Options - TCP/IP host list will appear in a remote's TCP/IP browse list.

If this is set to '1' the default, pcANYWHERE32 sends 254 UDP packets per network. This setting is best when accessing pcANYWHERE TCP/IP hosts through the Internet and on wide area networks. However, this option does send the most TCP/IP packets on the network.

If this is set to '2', pcANYWHERE32 sends one UDP broadcast packet per network. However, if the router filters broadcast packets, you will not see pcANYWHERE32 hosts across the router.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPNetBroadcast

Data Type: REG_DWORD

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/301.html - (277)

- Port Compatibility with Legacy Versions (pcANYWHERE) -

Detailed Information:



Port Compatibility with Legacy Versions (pcANYWHERE) (Windows 9x and NT)

pcANYWHERE32 8.0 hosts and remotes can connect to earlier hosts and remotes without any registry changes. You may want to turn off compatibility to limit network traffic or allow third party applications that have registered the ports that earlier versions of pcANYWHERE32 7.x and pcANYWHERE 2.0 were using.

If compatibility is set to OFF, then the pcANYWHERE32 8.0 host opens one TCP (TCPIPDataPort) and one UDP (TCPIPStatusPort) port. Remotes query and try to connect to one set of TCP and UDP ports.

If compatibility is set to ON, then the pcANYWHERE32 8.0 host opens the TCP port defined in TCPIPDataPort and port 65301, and the UDP port defined in TCPIPStatusPort and port 22. Remotes query and try to connect to the ports defined in the registry and ports 65301 and 22.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPPortCompatibility

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- TCP/IP Query Interval (pcANYWHERE) -

Detailed Information:



TCP/IP Query Interval (pcANYWHERE) (*Windows 9x and NT*)

Use this setting to limit network traffic. Sometimes the additional network queries to refresh the browse list will interfere with getting status lights or making connections.

Set this registry item to a high value if you get a message that a known ready host is busy when you try to connect to the host, and direct packets are not filtered. It is especially important to increase this value if the TCPIPBrowseDelay value has been increased, because it is difficult to connect if the network query is going on at the same time.

The default is 50 seconds. The minimum setting is 30 seconds. A setting of zero turns off all list updates.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPQueryInterval

Data Type: REG_DWORD

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/302.html - (279)

- Configure the TCP/IP Status Port (pcANYWHERE) -

Detailed Information:



Configure the TCP/IP Status Port (pcANYWHERE) (Windows 9x and NT)

Use this setting to select which TCP status port pcANYWHERE uses.

The default is the port for pcANYWHERE is 1600 (hex). For compatibility with previous versions, change the port number to 0016 (hex).

Note: Version 7.52's remote always uses the value in this registry entry. Version 8.0 remote only uses this entry if the TCP/IPNetBroadcast entry equals 1.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPStatusPort

Data Type: REG_BINARY

Data: 1600 (HEX) (Default)

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/299.html - (280)

- Configure the Winsock Buffer Size (pcANYWHERE) -

Detailed Information:



Configure the Winsock Buffer Size (pcANYWHERE) (Windows 9x and NT)

Use this registry item to set the size in bytes of TCP's Winsock buffer. Using a large value may increase the throughput of connections where the delay is large in relation to the bandwidth. This includes Internet, ISDN, RAS, dial-up networking, WAN and satellite connections.

For example, if the delay between two end points is 500 msec (.5 sec), the default throughput will be limited to 8K / .5 sec = 16K/sec. By increasing the value to its maximum setting, the theoretical throughput will be 65535 / .5 sec = 128K/sec.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: TCPIPWSDataBuf

Data Type: REG_DWORD

Data: 1 - 65535 (Default = 8000)

More info: <http://www.symantec.com/techsupp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/303.html - (281)

- TAPI Modem Errors (pcANYWHERE) -

Detailed Information:



TAPI Modem Errors (pcANYWHERE) (Windows 9x and NT)

Each time you add a TAPI modem, it generates a unique TAPI Permanent Line ID which is stored in pcANYWHERE32's connection items. If you no longer have a modem with this unique ID, pcANYWHERE32 displays an error message. This registry key tells pcANYWHERE32 how to handle this situation.

The options are:

- 0 = Always error if TAPI ID does not match.
- 1 = Error if TAPI ID does not match and more than one TAPI modem is present. If only one TAPI modem is installed, then use it if the TAPI IDs do not match.
- 2 = Always use the first TAPI modem if the TAPI ID does not match

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System]

Value Name: UseFirstTapiModem

Data Type: REG_DWORD

More info: <http://www.symantec.com/techsupp/>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Beep on Printer Errors -

Detailed Information:



Beep on Printer Errors (Windows NT)

When this setting is enabled the machine will beep (every 10 seconds) when a remote job error occurs on a print server.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print]

Value Name: BeepEnabled

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/136.html - (283)

- Changing the Default Printer Spool Directory -

Detailed Information:



Changing the Default Printer Spool Directory (Windows NT)

Windows using the hard drive to spool information before sending it to a printer. If the system is acting as a print server, it is possible that the default location may have insufficient disk space.

1. Create a new directory to act as the Printer spool directory.
2. Using Regedit open the key below.
3. Change the value of 'DefaultSpoolDirectory' to equal the full path of the directory created in step 1.
4. Reboot Windows NT, or stop and start the 'Spooler' service.

The default directory is: `%SystemRoot%\system32\spool\PRINTERS`

Note: To change the spool directory for a specific printer only, find the sub-key under the key below that corresponds to the printer in question. Modify the value of 'SpoolDirectory' to equal the directory you want to use.

Note: If the directory doesn't exist, Windows will use the default.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers]

Value Name: DefaultSpoolDirectory

Data Type: REG_SZ

Data: Full path to printer spool directory

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/193.html - (284)

- Change a Users Default Printer -

Detailed Information:



Change a Users Default Printer (Windows 9x and NT)

This setting will allow you the change the default printer of a user by modifying the registry.

Open your registry, and find the key appropriate for your operating system, as shown below.

Add or edit the value of 'Device', to equal the printer you want to become default for the current user.

Windows 95

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Windows]

Windows NT

[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows]

***Note:** The device is the name used to represent the printer in the registry, the name can also be found in the [HKEY_CURRENT_USER\Printers\Settings] key.*

Value Name:

Device

Data Type: REG_SZ

Data:

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/279.html - (285)

- Disable printer browse thread on the computer -

Detailed Information:



Disable printer browse thread on the computer (*Windows NT*)

When this option is enabled, the print spooler does not send shared printer information to other print servers.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print]

Value Name: DisableServerThread

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/164.html - (286)

- Disable Print Job Notification in Event Viewer -

Detailed Information:



Disable Print Job Notification in Event Viewer (*Windows NT*)

By default Windows NT server adds an entry in the event log for every print job occurring on the spooler. This can quickly fill up the event log with redundant information.

To disable this function, change the DWORD value for EventLog to "0".

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers]

Value Name: EventLog

Data Type: REG_DWORD

Data: (0 = disable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/49.html - (287)

- Define the Scheduler Priority -

Detailed Information:



Define the Scheduler Priority (Windows NT)

The setting controls the overall priority of the printer scheduler.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print]

Value Name: SchedulerThreadPriority

Data Type: REG_DWORD

Data: Above normal = 1; Normal = 0, Less than normal = ffffffff

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/165.html - (288)

- Use Windows Update Without Registering -

Detailed Information:



Use Windows Update Without Registering (*Windows 98*)

Windows Update is a handy feature of Windows 98, having to register your personal details before being able to use it isn't as good! With this tip you can bypass the registration process.

Open your registry and find the key below.

Create a new string value called 'RegDone', or modify the existing value, to equal '1'.

Check that the key [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Welcome\RegWiz] exists, if it doesn't then create a new key.

Next time you run Windows Update it shouldn't ask you to complete the registration process.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion]

Value Name: RegDone

Data Type: REG_SZ

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/338.html - (289)

- Changing the Location of Windows 9x's Installation Files -

Detailed Information:



Changing the Location of Windows 9x's Installation Files (*Windows 9x*)

Modifying the string will change the path that the Windows 95 setup program will look for the installation files.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup]

Value Name: SourcePath

Data Type: REG_SZ

Data: D:\WIN95

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/42.html - (290)

- Enable Command Line Completion -

Detailed Information:



Enable Command Line Completion (*Windows NT*)

Command completion allows you to type only a portion of a file name, and then have the system complete the rest by pressing the TAB key. This is similar to the the UNIX shell command completion feature.

1. Open the key below and change the value of "CompletionChar" to "09" for the TAB key.
2. Exit and reboot your PC.

Now when you type the first part of a filename, and press the TAB key and Windows will complete the filename for you.

Note: Changing the value of 'CompletionChar' changes which key executes command completion i.e. '09' is the TAB key.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Command Processor]

Value Name: CompletionChar

Data Type: REG_DWORD

Data: 09 = enabled (TAB Key)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/3.html - (291)

- Change the Display Color of Compressed Files and Folders -

Detailed Information:



Change the Display Color of Compressed Files and Folders (*Windows NT*)

When a file is compressed in Windows NT, there is an option in Explorer to display it in a different color to easily distinguish them. This setting defines what color to use, the default is blue.

1. Open the key below, and modify the value of 'AltColor' to a hexadecimal value representing the color you want the files to be display using.
2. Exit and reboot.

Note: *The option to "Display compressed files and folders with alternate color" must be enabled, this is found under 'View | Options | View' in any explorer window.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer]

Value Name: AltColor

Data Type: REG_BINARY

Data: 00 00 ff 00 (default)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/20.html - (292)

- Auto Logon to a Windows NT Machine -

Detailed Information:



Auto Logon to a Windows NT Machine (*Windows NT*)

Windows NT includes a feature that allows you to automatically logon to the machine and network, bypassing the Winlogon dialog box.

To enable this function you need to add several new values to the [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] key.

1. Add a new value of 'DefaultUserName' and set the data to the username you wish to automatically logon as.
2. Add a new value of 'DefaultPassword' and set this to the password for the username above.
3. Add a new value of 'DefaultDomainName' and set this to the domain of the user. Ignore this value if the NT box is not participating in NT Domain security.
4. Add a new value of 'AutoAdminLogon' and set it to either '1' to enable auto logon or '0' to disable.
5. Exit and reboot, Windows should not ask for a password and automatically show the desktop of the user.

WARNING: The password is stored in registry, which means anyone who has access to the machine has access to the password.

Note: You can bypass this function by holding the <Shift> during the boot process.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: AutoAdminLogon

Data Type: REG_SZ

Data: (0=disable, 1=enable)

More info: <http://support.microsoft.com/support/ntserver/service/10141775.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

- Automatically Shutdown Not Responding Applications -

Detailed Information:



Automatically Shutdown Not Responding Applications (*Windows NT*)

Often when Windows NT shutdown, a task will return as 'Not Responding' and you are given the choice to 'End Task' enabling this function automatically ends the task.

1. Open the registry and find the key below.
2. Modify the value of 'AutoEndTasks' to equal '1' for enabled.
3. The default time-out before ending the task is defined by the value of 'WaitToKillAppTimeout' located in the same key, this value is in milliseconds (default=20000 i.e. 20 seconds). You can therefore additionally change this value to speed the process up.

Note: *This change will affect all users but value can also be changed on a user basis by modifying [HKEY_CURRENT_USER\Control Panel\Desktop] and the same registry key.*

Key: [HKEY_USERS\DEFAULT\Control Panel\Desktop]

Value Name: AutoEndTasks

Data Type: REG_SZ

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/199.html - (294)

- Automatically Reboot on the 'Blue Screen of Death' -

Detailed Information:



Automatically Reboot on the 'Blue Screen of Death' (*Windows NT*)

Windows NT workstation will halt by default when you get a dreaded 'Blue Screen of Death' (BSOD). Changing this setting will force Windows NT to automatically reboot when it crashes instead.

1. Open your registry and find the key below.
2. Change the value of 'AutoReboot' to equal '1' for automatic reboot, or '0' for disabled.
3. Exit the registry editor and reboot for the change to take affect.

Note: *This function can also be enabled from 'Control Panel | System | Startup/Shutdown | Automatically Reboot'. This feature is enabled by default on NT server, and disabled on NT Workstation.*

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]

Value Name: AutoReboot

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/229.html - (295)

- Changing Default Colors for Command Prompt -

Detailed Information:



Changing Default Colors for Command Prompt (*Windows NT*)

The value DefaultColor controls the foreground and background colors used in command prompt windows. It has a default value of 0, for standard white text on a black background.

You can replace this value with a two-digit hexadecimal number, in which the first digit selects a background color and the second a foreground color. A value of F0, for example, would give black text on a white background, and 1E would yield yellow text on a blue background.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Command Processor]

Value Name: DefaultColor

Data Type: REG_DWORD

Data: (0 = default)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/12.html - (296)

- Run 16bit apps in a Separate VDM by Default -

Detailed Information:



Run 16bit apps in a Separate VDM by Default (*Windows NT*)

When starting a 16bit application you have the option of running it in a separate virtual machine. From this setting you can change the default setting for using VDM's.

Having a separate virtual machine, has the advantage that if the application crashes only that one application is affected, on the down side though it takes up a bit more system resources. It's up to you decide which is more important.

1. Open the registry and find the key and value below, if they don't already exist create them.
2. Change the value of 'DefaultSeparateVDM' to either 'Yes' or 'No'.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WOW]

Value Name: DefaultSeparateVDM

Data Type: REG_SZ

Data: 'Yes' or 'No'

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/201.html - (297)

- Delete Cached Copies of Roaming Profiles -

Detailed Information:



Delete Cached Copies of Roaming Profiles (Windows NT)

If this settings is enabled, when users with roaming profiles log off, the system will delete the cached copy of their roaming profile. This will help to save disk space where that are lots of roaming users.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: DeleteRoamingCache

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/142.html - (298)

- Hard Disk Free Space Warning -

Detailed Information:



Hard Disk Free Space Warning (*Windows NT*)

By default, Windows NT posts an alert when the amount of free space remaining on your hard disk falls below 10 percent.

To alter this behavior, edit:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters

Add Value DiskSpaceThreshold with a type of REG_DWORD and set it to the percentage of free disk space remaining before an alert is sent. The allowable range is 0 - 99 percent.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters]

Value Name: DiskSpaceThreshold

Data Type: REG_DWORD

Data: 0 - 99

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/52.html - (299)

- Configure the DHCP Settings of a Network Adapter -

Detailed Information:



Configure the DHCP Settings of a Network Adapter (*Windows NT*)

This setting controls whether TCP/IP should use DHCP to automatically assign an IP address, or if it should use the statically defined address.

Open the registry and find the key below, where {Adapter} equals the service name of the installed NIC.

Change the value of 'EnabledDHCP' to equal either '0' for disabled, or '1' for enabled.

Note: *If you change this setting to disabled, make sure you have IP addressing information defined.*

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{Adapter}\Parameters\Tcpip]

Value Name: EnableDHCP

Data Type: REG_DWORD

Data: (0 = DHCP Disabled, 1= DHCP Enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/270.html - (300)

- Configure the TCP/IP Settings of a Network Adapter -

Detailed Information:



Configure the TCP/IP Settings of a Network Adapter (*Windows NT*)

These values control the TCP/IP parameters of the network interface cards. Configurable parameters include IP Address, Subnet Mask and Default Gateway.

Open the registry and find the key below, where {Adapter} equals the service name of the installed NIC. For example 3COM 905 NIC's service name is 'E190X'.

Modify the values names (listed below) in binary.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{Adapter}\Parameters\Tcpip]

Value Name: IPAddress; SubnetMask; DefaultGateway

Data Type: REG_BINARY

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/269.html - (301)

- Allow extended characters in 8.3 filenames -

Detailed Information:



Allow extended characters in 8.3 filenames (*Windows NT*)

This setting allows extended characters to be used in 8.3 filenames. Short file names with extended characters may not be viewable on computers that do not have the same character code page.

Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]

Value Name: NtfsAllowExtendedCharacterIn8dot3Name

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/166.html - (302)

- Power the Computer Off After Shutdown -

Detailed Information:



Power the Computer Off After Shutdown (Windows NT)

Enabling the setting will cause Windows NT to automatically powerdown your computer once it has finished the shutdown process.

Note: *This feature must be supported by the computer's BIOS.*

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: PowerdownAfterShutdown

Data Type: REG_SZ

Data: (0 = disabled, 1 = enabled)

More info: <http://support.microsoft.com/support/kb/articles/q155/1/17.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/251.html - (303)

- Time-out for NT User Profile Dialog Boxes -

Detailed Information:



Time-out for NT User Profile Dialog Boxes (Windows NT)

When the user is presented with a dialog box requesting User Profile information, this specifies the amount of time in seconds before the dialog box is closed and the default is accepted. The default value is 30 seconds.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: ProfileDlgTimeOut

Data Type: REG_DWORD

Data: 1 to 600 (seconds)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/145.html - (304)

- Run Logon Scripts Synchronously -

Detailed Information:



Run Logon Scripts Synchronously (*Windows NT*)

This setting defines whether the system should wait for the logon scripts to complete before starting the user's shell.

This function can also be controlled on a per user basis by modifying the same value at:

[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]

Note: The value in [HKEY_CURRENT_USER] section take precedence over [HKEY_LOCAL_MACHINE].

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: RunLogonScriptSync

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/141.html - (305)

- Windows NT Short File Extensions -

Detailed Information:



Windows NT Short File Extensions (*Windows NT 4.x*)

Windows NT evaluates file extensions on the first three characters, therefore 'filename.html' is actually treated as 'filename.htm'. The side affect is that if you use a command such as 'del *.htm' to delete all the '.htm' files, you will also delete all '.html' files as well. This functionality can be disabled by modifying the registry.

To turn this setting off, editing the key found below and set the value of 'Win95TruncatedExtensions' to '0', to turn the feature back on, set the value back to '1'.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]

Value Name: Win95TruncatedExtensions

Data Type: REG_DWORD

Data: (0 = disable , 1 = enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/59.html - (306)

- Disable the MS-DOS Command Prompt -

Detailed Information:



Disable the MS-DOS Command Prompt (*Windows 9x and NT*)

This setting allows you to disable the use of the MS-DOS command prompt in Windows.

1. Using Regedit find the key below, creating it if it doesn't already exist.
2. Create a new DWORD value, and name it 'Disabled'.
3. To disable the command prompt modify the value of 'Disabled' to '1', and to re-enable it again later change the value to '0'.

Note: *You need to reboot for this restriction to come into force.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp]

Value Name: Disabled

Data Type: REG_DWORD

Data: (0 = disable, 1 = enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/118.html - (307)

- Disable Single Mode MS-DOS Applications in Windows -

Detailed Information:



Disable Single Mode MS-DOS Applications in Windows (*Windows 9x and NT*)

This setting allows you to disable the use of real mode DOS applications from within the Windows shell.

1. Using Regedit find the key below, creating it if it doesn't already exist.
2. Create a new DWORD value, and name it 'NoRealMode'.
3. To disable the real mode DOS modify the value of 'NoRealMode' to '1', and to re-enable it again later change the value to '0'.

Note: *You need to reboot for this restriction to come into force.*

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp]

Value Name: NoRealMode

Data Type: REG_DWORD

Data: (0 = disable, 1 = enable)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/119.html - (308)

- Remove the Content Advisor and Ratings Password -

Detailed Information:



Remove the Content Advisor and Ratings Password (*Windows 9x and NT*)

If you've forgotten the Internet Explorer content advisor password and want to change the ratings settings then follow these instructions to change the settings back to their defaults.

All the Content Advisor settings are stored in the key below. If you no longer have the password, then simply delete the key, and all the settings will be removed.

Open your registry, find the key below. Single click on the key to highlight it, press the DELETE key, or alternatively select Delete from the Edit menu.

Close Internet Explorer, re-open it, and the Content Advisor feature should be disabled.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ratings]

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/60.html - (309)

- Hide the Display Appearance Page -

Detailed Information:



Hide the Display Appearance Page (*Windows 9x and NT*)

This setting, once enabled, hides the display settings appearance page.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoDispAppearancePage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/168.html - (310)

- Hide the Display Background Page -

Detailed Information:



Hide the Display Background Page (*Windows 9x and NT*)

This option hides the background page, stopping users from changing any background display settings.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoDispBackgroundPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/169.html - (311)

- Hide the Screen Saver Settings Page -

Detailed Information:



Hide the Screen Saver Settings Page (*Windows 9x and NT*)

This option hides the screen saver page from the display settings control, which stops users having access to change screen saver settings.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoDispScrSavPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/170.html - (312)

- Hide the Display Settings Page -

Detailed Information:



Hide the Display Settings Page (*Windows 9x and NT*)

This option hides the Settings page from the display properties control.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoDispSettingsPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/171.html - (313)

- Hide the File and Printer Sharing Controls -

Detailed Information:



Hide the File and Printer Sharing Controls (*Windows 9x*)

Enabling this options hides the file and printer sharing controls, stopping users from disabling or creating new file or printer shares.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: NoFileSharingControl

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/189.html - (314)

- Hide Network Identification Page -

Detailed Information:



Hide Network Identification Page (*Windows 9x*)

The Network Identification page include options to set the Computer Name, Workgroup and Description, enabling this option disables access to the Network ID page.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: NoNetSetupIDPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/175.html - (315)

- Hide Network Access Control Page -

Detailed Information:



Hide Network Access Control Page (*Windows 9x*)

The Access Control Page, defines whether the computer support User-Level access or Share-Level access, enabling this option removes access to the Access Control Page.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: NoNetSetupSecurityPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/176.html - (316)

- Hide the Remote Administration Page -

Detailed Information:



Hide the Remote Administration Page (*Windows 9x*)

Enabling this function stops users from being able to change the remote administration settings for the computer.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoAdminPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/183.html - (317)

- Hide the User Profiles Page -

Detailed Information:



Hide the User Profiles Page (*Windows 9x*)

The user profile page controls whether all users share or have separate user profiles, access to this page can be disabled by enabling this setting.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoProfilePage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/184.html - (318)

- Hide the Change Passwords Page -

Detailed Information:



Hide the Change Passwords Page (*Windows 9x*)

When this setting is enabled, users are no longer able to access the Change Passwords page.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoPwdPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/182.html - (319)

- Disable the Addition of Printers -

Detailed Information:



Disable the Addition of Printers (Windows 9x)

Any user can add a new printer their system, this option once enabled disables the addition of new printers to the computer.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoAddPrinter

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/180.html - (320)

- Disable the Deletion of Printers -

Detailed Information:



Disable the Deletion of Printers (*Windows 9x*)

Printers can be deleted simply by anyuser pressing the delete key, enabling this setting stops users from being able to delete printers.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoDeletePrinter

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/179.html - (321)

- Hide the General and Details Printer Pages -

Detailed Information:



Hide the General and Details Printer Pages (*Windows 9x*)

This option hides the printer details and general printer information pages. Once enabled this option stops users from changing specific printer settings.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Value Name: NoPrinterTabs

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/178.html - (322)

- Hide the Hardware Profiles Page -

Detailed Information:



Hide the Hardware Profiles Page (*Windows 9x*)

The settings when enabled hides the Hardware Profiles page from the System icon on the Control Panel.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoConfigPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/186.html - (323)

- Hide the Device Manager Page -

Detailed Information:



Hide the Device Manager Page (*Windows 9x*)

This setting controls whether the Device Manager, under Control Panel / System is visible.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoDevMgrPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/185.html - (324)

- Hide the File System Button -

Detailed Information:



Hide the File System Button (*Windows 9x*)

This option hides the File System button from the System icon on the Control Panel.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoFileSysPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/187.html - (325)

- Hide the Virtual Memory Button -

Detailed Information:



Hide the Virtual Memory Button (*Windows 9x*)

This option hides the Virtual Memory button from the System icon on the Control Panel.

Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]

Value Name: NoVirtMemPage

Data Type: REG_DWORD

Data: (0 = disabled, 1 = enabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/188.html - (326)

- Maximum Number of Remote Access Authentication Attempts -

Detailed Information:



Maximum Number of Remote Access Authentication Attempts (*Windows NT*)

This setting controls the number of authentication retries before the remote access connection is terminated.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters]

Value Name: AuthenticateRetries

Data Type: REG_DWORD

Data: 1 to 10

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/137.html - (327)

- Maximum Time Limit for Authentication -

Detailed Information:



Maximum Time Limit for Authentication (*Windows NT*)

A time limit can be enforced on the length of time given to logon via Remote Access.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters]

Value Name: AuthenticateTime

Data Type: REG_DWORD

Data: 20 to 600 (seconds)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/138.html - (328)

- Automatically Disconnect Remote Access Callers -

Detailed Information:



Automatically Disconnect Remote Access Callers (Windows NT)

Specifies the amount of idle time in minutes to wait before disconnecting the RAS client.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters]

Value Name: AutoDisconnect

Data Type: REG_DWORD

Data: Time in Minutes

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/139.html - (329)

- Define the length of time before callback is initiated -

Detailed Information:



Define the length of time before callback is initiated (*Windows NT*)

When callback is required or requested this setting defines how long to wait before initiating the callback connection.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters]

Value Name: CallbackTime

Data Type: REG_DWORD

Data: 2 - 12 (seconds)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/140.html - (330)

- Disable Dial-In Access -

Detailed Information:



Disable Dial-In Access (*Windows 9x and NT*)

It's possible for users to setup a modem on a Windows machine, and by using Dial-up Networking allow callers to connect to the internal network. Especially in a corporate environment this can cause a major security risk.

Key: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

Value Name: NoDialIn

Data Type: REG_DWORD

Data: (0 = dial-in enabled, 1 = dial-in disabled)

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/131.html - (331)

- Automatically Use Dial-Up Networking to Logon -

Detailed Information:



Automatically Use Dial-Up Networking to Logon (*Windows NT*)

There is an option that is available on the logon dialog box and allows you to dial into your logon server for authentication of your user account, this can be enabled by default.

1. Open the registry and find the key below.
2. Create a string new value and name it 'RasForce', set the value to equal '1' for enabled.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: RasForce

Data Type: REG_SZ

Data: (0 = disabled, 1 = enabled)

More info: <http://support.microsoft.com/support/kb/articles/q172/1/25.asp>

Copyright © 1998-1999 by Simon Clausen. All Rights Reserved.
Any unauthorized duplication is strictly prohibited.

Source: C:/helpfile/detail/207.html - (332)

