Paul McFedries

Covers Release Candidate of Windows 7.

Get a free online edition written on final product.

See inside!

Microsoft® Windows 7

UNLEASHED

SAMS

Microsoft Windows 7 Unleashed

ISBN-13: 978-0-6723-3069-8
ISBN-10: 0-672-33069-5

Library of Congress Cataloging-in-Publication Data:

McFedries, Paul.

Microsoft Windows 7 unleashed / Paul McFedries.

p. cm.

ISBN 978-0-672-33069-8

1. Microsoft Windows (Computer file) 2. Operating systems (Computers) I. Title.

QA76.76.O63M398163 2010

005.4'46—dc22

2009024027

Printed in the United States of America

First Printing: July 2009

Trademarks

Warning and Disclaimer

Bulk Sales

Associate Publisher
Greg Wiegand

Acquisitions Editor
Rick Kughen

Development Editor
Rick Kughen

Managing Editor
Patrick Kanouse

Project Editor
Jennifer Gallant

Copy Editor
Keith Cline

Indexer
Tim Wright

Proofreader
Sheri Cain

Technical Editor
Mark Reddin

Publishing Coordinator
Cindy Teeters

Interior Designer
Gary Adair

Cover Designer
Gary Adair

Compositor
Mark Shirar

Introduction

We shall not cease from exploration
And the end of all our exploring
Will be to arrive where we started
And know the place for the first time.
—T. S. Eliot

Well, *that* was easy. After the "two steps forward, one step back" development process of Windows Vista, after the interminable Vista beta releases, and after the hype and hoopla that accompanied the Vista release, Windows 7 seemed to arrive on our digital doorsteps fully formed, like a kind of electronic Athena from the skull of some programming Zeus (or something like that).

The development and release of Microsoft's latest bouncing-baby operating system was nothing like its older sibling, but does that mean that Windows 7 itself is nothing like Windows Vista? Actually, in many ways, that's true. Sure, if you're familiar with Windows Vista, you'll have a relatively benign learning curve with Windows 7. But Microsoft didn't spend the past 3 years working on new desktop backgrounds! Windows 7 is loaded with new and changed features; some of them are almost too subtle to notice, whereas others represent veritable system sea changes.

Coincidentally (or not, depending on where you fall in the conspiracy theory spectrum), my approach to Windows has also changed in this edition of the book. Unlike in previous editions, *Windows 7 Unleashed* is *not* my attempt to cover all the features of Windows from Aero Glass to AutoPlay. Windows has simply become too big for that kind of book, and most Windows users know (or can figure out) the basics of most features. So in this edition of the book, I've changed

the focus from components (Internet Explorer, Mail, and so on) to subjects: customization, performance, power tools, security, troubleshooting, and networking, and scripting. You get in-depth and useful coverage of these seven areas that will help you unleash the full potential of Windows 7.

Who Should Read This Book

All writers write with an audience in mind. Actually, I'm not sure whether that's true for novelists and poets and the like, but it *should* be true for any technical writer who wants to create a useful and comprehensible book. Here are the members of my own imagined audience:

- **IT professionals—**These brave souls must decide whether to move to Windows 7, work out deployment issues, and support the new Windows 7 desktops. The whole book has information related to your job and Windows 7.
- **Power users—**These elite users get their power via knowledge. With that in mind, this book extends the Windows power user's know-how by offering scripts, Registry tweaks, group policy configurations, and other power tools.
- **Business users—**If your company is thinking of or has already committed to moving to Windows 7, you need to know what you, your colleagues, and your staff are getting into. You also want to know what Windows 7 will do to improve your productivity and make your life at the office easier. You learn all of this and more in this book.
- **Small business owners—**If you run a small or home business, you probably want to know whether Windows 7 will give you a good return on investment. Will it make it easier to set up and maintain a network? Will Windows 7 computers be more stable? Will your employees be able to collaborate easier? The answer turns out to be "yes" for all of these questions, and I'll show you why.
- **Home users—**If you use Windows 7 at home, you probably want to maximize performance, keep your system running smoothly, max out security, and perform customizations that make Windows 7 conform to your style. Check, check, check, check. This book's got your covered in all these areas.

Also, to keep the chapters uncluttered, I've made a few assumptions about what you know and what you don't know:

- I assume that you have knowledge of rudimentary computer concepts, such as files and folders.
- I assume that you're familiar with the basic Windows skills: mouse maneuvering, dialog box negotiation, pull-down menu jockeying, and so on.
- I assume that you can operate peripherals attached to your computer, such as the keyboard and printer.

- I assume that you've used Windows for a while and are comfortable with concepts such as toolbars, scrollbars, and, of course, windows.
- I assume that you have a brain that you're willing to use and a good supply of innate curiosity.

How This Book Is Organized

As I mentioned earlier, I've completely revamped the structure and coverage in this edition, so the next few sections offer a summary of what you'll find in each part.

Part I: Unleashing Windows 7 Customization

Your purchase of this book (a sound and savvy investment on your part, if I do say so myself) indicates that you're not interested in using Windows 7 in its out-of-the-box configuration. If you're looking to make Windows 7 your own, begin at the beginning with the five chapters in Part I. You learn how to customize Windows Explorer (Chapter 1), Internet Explorer (Chapter 2), the file system (Chapter 3), startup and shutdown (Chapter 4), and the Start menu and taskbar (Chapter 5).

Part II: Unleashing Windows 7 Performance and Maintenance

Everybody wants Windows to run faster, so you'll no doubt be pleased that I devote an entire chapter to this important topic (Chapter 6). Everybody wants Windows to run smoother, so you'll also no doubt be pleased that I devote yet another chapter to *that* important topic (Chapter 7).

Part III: Unleashing Windows 7 Power User Tools

The chapters in Part III kick your advanced Windows 7 education into high gear by covering the ins and outs of a half dozen important Windows 7 power tools: Control Panel (Chapter 8), Local Group Policy Editor (Chapter 9), Microsoft Management Console (Chapter 10), the Services snap-in (Chapter 11), the Registry Editor (Chapter 12), and Command Prompt (Chapter 13).

Part IV: Unleashing Windows 7 Security

With threats to our digital lives coming at us from all sides these days, security may just be the most vital topic in technology. So perhaps that's why Part IV is the biggest section in the book, with no less than seven chapters devoted to various aspects of Windows 7 security. Your first learn some general techniques for locking down Windows 7 (Chapter 14), and you then learn how to configure web security (Chapter 15), email security (Chapter 16), file system security (Chapter 17), user security (Chapter 18), wired network security (Chapter 19), and wireless network security (Chapter 20).

Part V: Unleashing Windows 7 Troubleshooting

Windows 7 may represent the state of Microsoft's operating system art, but it *is* still Windows, which means problems, bugs, and glitches are pretty much inevitable. The four chapters in Part V can help when the Windows demons strike. You learn general troubleshooting techniques (Chapter 21), and how to troubleshoot device (Chapter 22), startup (Chapter 23), and networking (Chapter 24).

Part VI: Unleashing Windows 7 Networking

It's a rare home or small office that doesn't have (or doesn't want to have) a network, and Part VI is a reflection of this fact (that I just made up). You learn how to set up a small network (Chapter 25), how to access and use that network (Chapter 26), how to access your network from remote locations (Chapter 27), how to use Windows 7 as a web server (Chapter 28), and how to incorporate Macs into your network (Chapter 29).

Part VII: Unleashing Windows 7 Scripting

To close out the main part of this book, Part VII takes an in-depth look at two methods for automating Windows tasks with scripts: Windows Scripting Host (Chapter 30) and Windows PowerShell (Chapter 31).

Part VIII: Appendixes

To further your Windows 7 education, Part VIII presents two appendixes that contain extra goodies. You'll find a complete list of Windows 7 shortcut keys (Appendix A), and a detailed look at the TCP/IP protocols that underlie Windows 7 networking (Appendix B).

Conventions Used in This Book

To make your life easier, this book includes various features and conventions that help you get the most out of this book and Windows 7 itself:

Steps	Throughout the book, I've broken many Windows 7 tasks into easy-to-follow step-by-step procedures.
Things you type	Whenever I suggest that you type something, what you type appears in a **`bold monospace`** font.
Filenames, folder names, and code	These things appear in a `monospace` font.
Commands	Commands and their syntax use the `monospace` font, too. Command placeholders (which stand for what you actually type) appear in an *`italic monospace`* font.
Pull-down menu commands	I use the following style for all application menu commands: *Menu, Command*, where *Menu* is the name of the menu that you pull down and *Command* is the name of the command you select. Here's an example: File, Open. This means that you pull down the File menu and select the Open command.
Code continuation character	When a line of code is too long to fit on only one line of this book, it is broken at a convenient place and continued to the next line. The continuation of the line is preceded by a code continuation character ([➥]). You should type a line of code that has this character as one long line without breaking it.

This book also uses the following boxes to draw your attention to important (or merely interesting) information:

NOTE

The Note box presents asides that give you more information about the current topic. These tidbits provide extra insights that give you a better understanding of the task. In many cases, they refer you to other sections of the book for more information.

TIP

The Tip box tells you about Windows 7 methods that are easier, faster, or more efficient than the standard methods.

CAUTION

The all-important Caution box tells you about potential accidents waiting to happen. There are always ways to mess things up when you're working with computers. These boxes help you avoid at least some of the pitfalls.

How to Contact Me

If you have any comments about this book, or if you want to register a complaint or a compliment (I prefer the latter), please don't hesitate to send a missive my way. The easiest way to do that is to drop by my website, have a look around, and post a message to the forum: www.mcfedries.com/.

If you do the Twitter thing, you can follow my tweets here: http://twitter.com/paulmcf.

CHAPTER 12

Tweaking the Windows 7 Registry

It is almost everywhere the case that soon after it is begotten the greater part of human wisdom is laid to rest in repositories.
—G. C. Lichtenberg

When you change the desktop background using Control Panel's Personalization window, the next time you start your computer, how does Windows 7 know which image or color you selected? If you change your video display driver, how does Windows 7 know to use that driver at startup and not the original driver loaded during setup? In other words, how does Windows 7 remember the various settings and options either that you've selected yourself or that are appropriate for your system?

The secret to Windows 7's prodigious memory is the Registry. The Registry is a central repository Windows 7 uses to store anything and everything that applies to the configuration of your system. This includes all the following:

- Information about all the hardware installed on your computer
- The resources those devices use
- A list of the device drivers that Windows 7 loads at startup
- Settings that Windows 7 uses internally
- File type data that associates a particular type of file with a specific application
- Backgrounds, color schemes, and other interface customization settings

IN THIS CHAPTER

- Firing Up the Registry Editor
- Getting to Know the Registry
- Understanding the Registry Files
- Keeping the Registry Safe
- Working with Registry Entries
- Finding Registry Entries

- Other customization settings for things such as the Start menu and the taskbar
- Internet and network connections and passwords
- Settings for Windows 7 applications such as Windows Explorer and Internet Explorer
- Settings and customization options for many third-party applications

It's all stored in one central location, and, thanks to a handy tool called the Registry Editor, it's yours to play with (carefully!) as you see fit, and that's what this chapter is all about.

Firing Up the Registry Editor

All the direct work you do with the Registry happens inside the reasonably friendly confines of a program called the Registry Editor, which enables you to view, modify, add, and delete Registry settings. It also has a search feature to help you find settings and export and import features that enable you to save settings to and from a text file.

To launch the Registry Editor, select Start, type **`regedit`** into the Search box, and then press Enter. When the User Account Control dialog box shows up, enter your credentials to continue.

Figure 12.1 shows the Registry Editor window that appears. (Note that your Registry Editor window might look different if someone else has used the program previously. Close all the open branches in the left pane to get the view shown in Figure 12.1.)

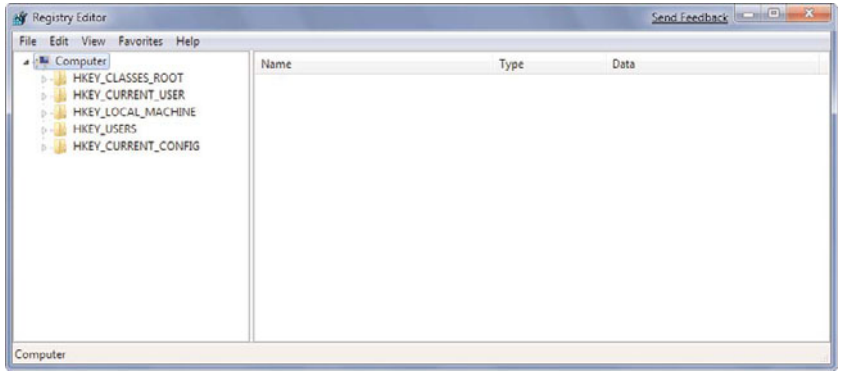

FIGURE 12.1 Run the `regedit` command to launch the Registry Editor, the program that enables you to work with the Registry's data.

CAUTION

The Registry Editor is arguably the most dangerous tool in the Windows 7 arsenal. The Registry is so crucial to the smooth functioning of Windows 7 that a single imprudent change to a Registry entry can bring your system to its knees. Therefore, now that you have the Registry Editor open, don't start tweaking settings willy-nilly. Instead, read the section titled "Keeping the Registry Safe," later in this chapter, for some advice on protecting this precious and sensitive resource.

Getting to Know the Registry

The Registry may be a dangerous tool, but you can mitigate that danger somewhat by becoming familiar with the layout of the Registry and what it various bits and parts are used for. This will help you avoid sensitive areas and stick to those Registry neighborhoods where it's safe to poke around. The next few sections introduce you to the major parts of the Registry.

Navigating the Keys Pane

The Registry Editor is reminiscent of Windows Explorer, and it works in sort of the same way. The left side of the Registry Editor window is similar to Explorer's Folders pane, except that rather than folders, you see *keys*. For lack of a better phrase, I'll call the left pane the *Keys pane*.

The Keys pane, like Explorer's Folders pane, is organized in a tree-like hierarchy. The five keys that are visible when you first open the Registry Editor are special keys called *handles* (which is why their names all begin with `HKEY`). These keys are collectively referred to as the Registry's *root keys*. I'll tell you what to expect from each of these keys later (see the section called "Getting to Know the Registry's Root Keys" later in this chapter).

These keys all contain subkeys, which you can display by clicking the arrow to the left of each key, or by highlighting a key and pressing the plus-sign key on your keyboard's numeric keypad. To close a key, click the minus sign or highlight the key and press the minus-sign key on the numeric keypad. Again, this is just like navigating folders in Explorer.

You often have to drill down several levels to get to the key you want. For example, Figure 12.2 shows the Registry Editor after I've opened the `HKEY_CURRENT_USER` key, and then the `Control Panel` subkey, and then clicked the `Mouse` subkey. Notice how the status bar tells you the exact path to the current key, and that this path is structured just like a folder path.

NOTE

To see all the keys properly, you likely will have to increase the size of the Keys pane. To do this, use your mouse to click and drag the split bar to the right. Alternatively, select View, Split, use the right-arrow key to adjust the split bar position, and then press Enter.

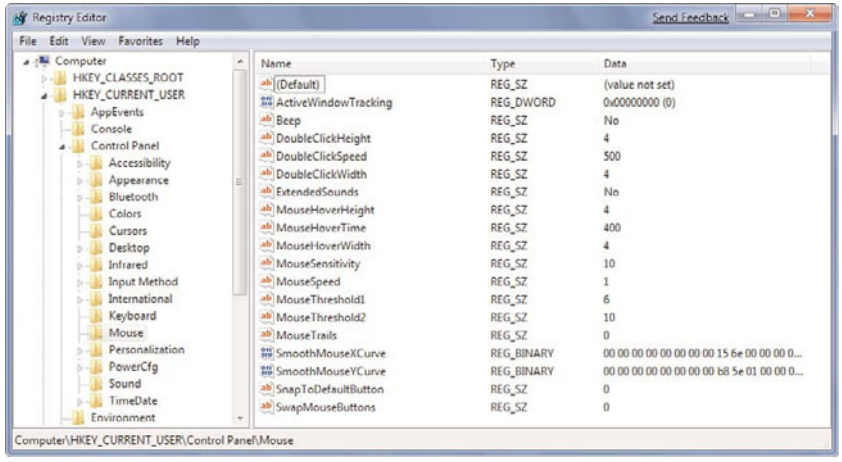

FIGURE 12.2 Open the Registry's keys and subkeys to find the settings you want to work with.

Understanding Registry Settings

If the left side of the Registry Editor window is analogous to Explorer's Folders pane, the right side is analogous to Explorer's Contents pane. In this case, the right side of the Registry Editor window displays the settings contained in each key (so I'll call it the *Settings pane*). The Settings pane is divided into three columns:

- **Name**—This column tells you the name of each setting in the currently selected key (analogous to a filename in Explorer).
- **Type**—This column tells you the data type of the setting. There are six possible data types:

  `REG_SZ`—This is a string value.

  `REG_MULTI_SZ`—This is a series of strings.

  `REG_EXPAND_SZ`—This is a string value that contains an environment variable name that gets "expanded" into the value of that variable. For example, the `%SystemRoot%` environment variable holds the folder in which Windows 7 was installed. So, if you see a Registry setting with the value `%SystemRoot%\System32\`, and Windows 7 is installed in `C:\Windows`, the setting's expanded value is `C:\Windows\System32\`.

  `REG_DWORD`—This is a double word value: a 32-bit hexadecimal value arranged as eight digits. For example, 11 hex is 17 decimal, so this number would be represented in `DWORD` form as 0x00000011 (17). (Why "double word"? A 32-bit value represents four bytes of data, and because a *word* in programming circles is defined as two bytes, a four-byte value is a *double word*.)

  `REG_QWORD`—This is a quadruple word value: a 64-bit hexadecimal value arranged as 16 digits. Note that leading zeros are suppressed for the high 8 digits. Therefore, 11 hex

appears as 0x00000011 (17), and 100000000 hex appears as 0x1000000000 (4294967296).
REG_BINARY—This value is a series of hexadecimal digits.

- **Data**—This column displays the value of each setting.

Getting to Know the Registry's Root Keys

The root keys are your Registry starting points, so you need to become familiar with what kinds of data each key holds. The next few sections summarize the contents of each key.

HKEY_CLASSES_ROOT

HKEY_CLASSES_ROOT—usually abbreviated as HKCR—contains data related to file extensions and their associated programs, the objects that exist in the Windows 7 system, as well as applications and their automation information. There are also keys related to shortcuts and other interface features.

The top part of this key contains subkeys for various file extensions. You see `.bmp` for bitmap (Paint) files, `.txt` for text (Notepad) files, and so on. In each of these subkeys, the `Default` setting tells you the name of the registered file type associated with the extension. (I discussed file types in more detail in Chapter 3, "Customizing the File System.") For example, the `.txt` extension is associated with the `txtfile` file type.

- **See** "Understanding File Types," **p. 46**.

These registered file types appear as subkeys later in the HKEY_CLASSES_ROOT branch, and the Registry keeps track of various settings for each registered file type. In particular, the shell subkey tells you the actions associated with this file type. For example, in the `shell\open\command` subkey, the `Default` setting shows the path for the executable file that opens. Figure 12.3 shows this subkey for the `txtfile` file type.

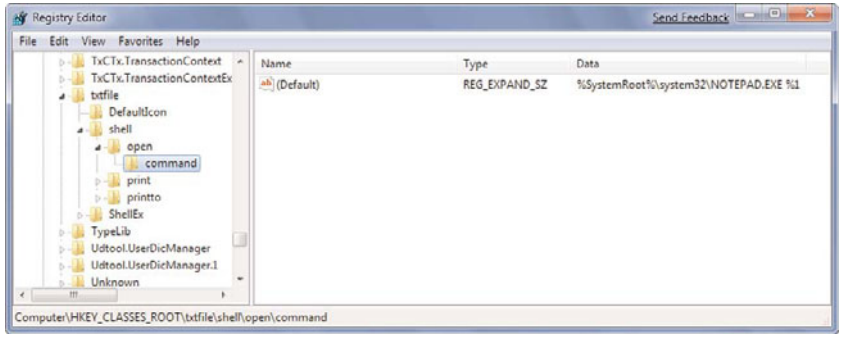

FIGURE 12.3 The registered file type subkeys specify various settings associated with each file type, including its defined actions.

HKEY_CLASSES_ROOT is actually a copy (or an *alias*, as these copied keys are called) of the following HKEY_LOCAL_MACHINE key:

```
HKEY_LOCAL_MACHINE\Software\Classes
```

The Registry creates an alias for HKEY_CLASSES_ROOT to make these keys easier for applications to access and to improve compatibility with legacy programs.

HKEY_CURRENT_USER

HKEY_CURRENT_USER—usually abbreviated as HKCU—contains data that applies to the user that's currently logged on. It contains user-specific settings for Control Panel options, network connections, applications, and more. Note that if a user has group policies set on his account, his settings are stored in the HKEY_USERS*sid* subkey (where *sid* is the user's security ID). When that user logs on, these settings are copied to *HKEY_CURRENT_USER*. For all other users, HKEY_CURRENT_USER is built from the user's profile file, ntuser.dat (located in %UserProfile%).

TIP

How do you find out each user's SID? First, open the following Registry key:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\
```

Here you'll find a list of SIDs. The ones that begin S-1-5-21 are the user SIDs. Highlight one of these SIDs and then examine the ProfileImagePath setting, which will be of the form %SystemDrive%\Users*user*, where *user* is the username associated with the SID.

Here's a summary of the most important HKEY_CURRENT_USER subkeys:

AppEvents	Contains sound files that play when particular system events occur (such as maximizing of a window)
Control Panel	Contains settings related to certain Control Panel icons
Keyboard Layout	Contains the keyboard layout as selected via Control Panel's Keyboard icon
Network	Contains settings related to mapped network drives
Software	Contains user-specific settings related to installed applications and Windows

HKEY_LOCAL_MACHINE

HKEY_LOCAL_MACHINE (HKLM) contains non-user-specific configuration data for your system's hardware and applications. You'll use the following three subkeys most often:

Hardware	Contains subkeys related to serial ports and modems, as well as the floating-point processor.

`Software`	Contains computer-specific settings related to installed applications. The `Classes` subkey is aliased by `HKEY_CLASSES_ROOT`. The `Microsoft` subkey contains settings related to Windows (as well as any other Microsoft products you have installed on your computer).
`System`	Contains subkeys and settings related to Windows startup.

HKEY_USERS

`HKEY_USERS` (`HKU`) contains settings that are similar to those in `HKEY_CURRENT_USER`. `HKEY_USERS` is used to store the settings for users with group policies defined, as well as the default settings (in the `.DEFAULT` subkey) which get mapped to a new user's profile.

HKEY_CURRENT_CONFIG

`HKEY_CURRENT_CONFIG` (`HKCC`) contains settings for the current hardware profile. If your machine uses only one hardware profile, `HKEY_CURRENT_CONFIG` is an alias for `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001`. If your machine uses multiple hardware profiles, `HKEY_CURRENT_CONFIG` is an alias for `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet`*nnn,* where *nnn* is the numeric identifier of the current hardware profile. This identifier is given by the `CurrentConfig` setting in the following key:

```
HKLM\SYSTEM\CurrentControlSet\Control\IDConfigDB
```

Understanding Hives and Registry Files

The Registry database actually consists of a number of files that contain a subset of the Registry called a *hive*. A hive consists of one or more Registry keys, subkeys, and settings. Each hive is supported by several files that use the extensions listed in Table 12.1.

TABLE 12.1 Extensions Used by Hive Supporting Files

Extension	Descriptions
None	A complete copy of the hive data.
`.log1`	A log of the changes made to the hive data.
`.log`, `.log2`	These files are created during the Windows 7 setup, but remain unchanged as you work with the system.

NOTE

To see all of these files, you must display hidden files on your system. In Windows Explorer, select Organize, Folder and Search Options, select the View tab, and then activate the Show Hidden Files, Folder, and Drives option. While you're here, you can also deactivate the Hide Extensions for Known File Types check box. Click OK.

Table 12.2 shows the supporting files for each hive. (Note that not all of these files might appear on your system.)

TABLE 12.2 Supporting Files Used by Each Hive

Hive	Files
HKLM\BCD00000000	%SystemRoot%\System32\config\BCD-Template
	%SystemRoot%\System32\config\BCD-Template.LOG
HKLM\COMPONENTS	%SystemRoot%\System32\config\COMPONENTS
	%SystemRoot%\System32\config\COMPONENTS.LOG
	%SystemRoot%\System32\config\COMPONENTS.LOG1
	%SystemRoot%\System32\config\COMPONENTS.LOG2
HKLM\SAM	%SystemRoot%\System32\config\SAM
	%SystemRoot%\System32\config\SAM.LOG
	%SystemRoot%\System32\config\SAM.LOG1
	%SystemRoot%\System32\config\SAM.LOG2
HKLM\SECURITY	%SystemRoot%\System32\config\SECURITY
	%SystemRoot%\System32\config\SECURITY.LOG
	%SystemRoot%\System32\config\SECURITY.LOG1
	%SystemRoot%\System32\config\SECURITY.LOG2
HKLM\SOFTWARE	%SystemRoot%\System32\config\SOFTWARE
	%SystemRoot%\System32\config\SOFTWARE.LOG
	%SystemRoot%\System32\config\SOFTWARE.LOG1
	%SystemRoot%\System32\config\SOFTWARE.LOG2
HKLM\SYSTEM	%SystemRoot%\System32\config\SYSTEM
	%SystemRoot%\System32\config\SYSTEM.LOG
	%SystemRoot%\System32\config\SYSTEM.LOG1
	%SystemRoot%\System32\config\SYSTEM.LOG2
HKU\.DEFAULT	%SystemRoot%\System32\config\DEFAULT
	%SystemRoot%\System32\config\DEFAULT.LOG
	%SystemRoot%\System32\config\DEFAULT.LOG1
	%SystemRoot%\System32\config\DEFAULT.LOG2

Also, each user has his or her own hive, which maps to HKEY_CURRENT_USER during logon. The supporting files for each user hive are stored in \Users*user,* where user is the username.

In each case, the `ntuser.dat` file contains the hive data, and the `ntuser.dat.log1` file tracks the hive changes. (If a user has group policies set on her account, the user data is stored in an `HKEY_USERS` subkey.)

Keeping the Registry Safe

The sheer wealth of data stored in one place makes the Registry convenient, but it also makes it very precious. If your Registry went missing somehow, or if it got corrupted, Windows 7 simply would not work. With that scary thought in mind, let's take a moment to run through several protective measures. The techniques in this section should ensure that Windows 7 never goes down for the count because you made a mistake while editing the Registry.

Preventing Other Folks from Messing with the Registry

Do you share your computer with other people? How brave! In that case, there's a pretty good chance that you don't want them to have access to the Registry Editor. In Windows 7, User Account Control automatically blocks Standard users unless they know an administrator's password. For other administrators, you can prevent any user from using the Registry Editor by setting a group policy:

1. Select Start, type **`gpedit.msc`**, and then press Enter.
2. Open the User Configuration, Administrative Templates, System branch.
3. Double-click the Prevent Access to Registry Editing Tools policy.
4. Click Enabled.
5. In the Disable Regedit from Running Silently? list, click Yes.
6. Click OK.

Note that *you* won't be able to use the Registry Editor, either. However, you can overcome that by temporarily disabling this policy prior to running the Registry Editor. Even better, you can run the following script, which toggles the Registry Editor between enabled and disabled:

NOTE

The file that contains the code for this script (`ToggleRegistryEditing.vbs`) is available on my website at www.mcfedries.com/Windows7Unleashed.

```
Set objWshShell = WScript.CreateObject("WScript.Shell")
'
' Get the current setting
'
intDisableRegistryTools = Int(objWshShell.RegRead("HKCU\Software\Microsoft\
➥Windows\CurrentVersion\Policies\System\DisableRegistryTools"))
'
' Toggle the current setting
'
If intDisableRegistryTools = 0 Then
    objWshShell.RegWrite "HKCU\Software\Microsoft\Windows\CurrentVersion\
➥Policies\System\DisableRegistryTools", 2, "REG_DWORD"
    WScript.Echo "The Registry Editor is disabled."
Else
    objWshShell.RegWrite "HKCU\Software\Microsoft\Windows\CurrentVersion\
➥Policies\System\DisableRegistryTools", 0, "REG_DWORD"
    WScript.Echo "The Registry Editor is enabled."
End If
```

Note that you need to run this script as the administrator. I show you how to do this in Chapter 30, "Programming the Windows Scripting Host."

▶ **See** "Running a Script as the Administrator," **p. 664**.

Backing Up the Registry

Windows 7 maintains what is known as the *system state*: the crucial system files that Windows 7 requires to operate properly. Included in the system state are the files used during system startup, the Windows 7–protected system files, and, naturally, the Registry files. Windows 7's Backup utility has a feature called a system image backup that enables you to easily back up the current system state, so it's probably the most straightforward way to create a backup copy of the Registry should anything go wrong. See Chapter 7, "Maintaining Your Windows 7 System," for the details.

▶ **See** "Creating a System Image Backup," **p. 157**.

Saving the Current Registry State with System Restore

Another easy way to save the current Registry configuration is to use Windows 7's System Restore utility. This program takes a snapshot of your system's current state, including the Registry. If anything should go wrong with your system, the program enables you to restore a previous configuration. It's a good idea to set a system restore point before doing any work on the Registry. I show you how to work with System Restore in Chapter 7.

▶ **See** "Setting System Restore Points," **p. 149**.

TIP

Another way to protect the Registry is to ensure that its keys have the appropriate permissions. By default, Windows 7 gives members of the Administrators group full control over the Registry. A standard user gets Full Control permission only over the HKCU key when that user is logged on and Read permissions over the rest of the Registry. To adjust the permissions, right-click the key in the Registry Editor, and then click Permissions. Make sure that only administrators have the Full Control check box activated.

Protecting Keys by Exporting Them to Disk

If you're just making a small change to the Registry, backing up all of its files might seem like overkill. Another approach is to back up only the part of the Registry that you're working on. For example, if you're about to make changes within the HKEY_CURRENT_USER key, you could back up just that key, or even a subkey within HKCU. You do that by exporting the key's data to a registration file, which is a text file that uses the .reg extension. That way, if the change causes a problem, you can import the .reg file back into the Registry to restore things the way they were.

Exporting the Entire Registry to a .reg File

The easiest way to protect the entire Registry is to export the whole thing to a .reg file on a separate hard drive or network share. Note that the resulting file will be about 150MB on a default Windows 7 system, and possibly twice that size (or more) if you have lots of other programs installed, so make sure the target destination has enough free space.

Here are the steps to follow:

1. Open the Registry Editor.
2. Select File, Export to display the Export Registry File dialog box.
3. Select a location for the file.
4. Use the File Name text box to type a name for the file.
5. Activate the All option.
6. Click Save.

Exporting a Key to a .reg File

Here are the steps to follow to export a key to a registration file:

1. Open the Registry Editor and select the key you want to export.
2. Select File, Export to display the Export Registry File dialog box.
3. Select a location for the file.
4. Use the File Name text box to type a name for the file.
5. Activate the Selected Branch option.
6. Click Save.

Finding Registry Changes

One common Registry scenario is to make a change to Windows 7 using a tool such as the Group Policy Editor, and then try and find which Registry setting (if any) was affected by the change. However, because of the sheer size of the Registry, this is usually a needle-in-a-haystack exercise that ends in frustration. One way around this is to export some or all the Registry before making the change and then export the same key or keys after making the change. You can then use the FC (file compare) utility at the command prompt to find out where the two files differ. Here's the FC syntax to use for this:

```
FC /U pre_edit.reg post-edit.reg > reg_changes.txt
```

Here, change *pre_edit.reg* to the name of the registration file you exported before editing the Registry; change *post_edit.reg* to the name of the registration file you exported after editing the Registry; and change *reg_changes.txt* to the name of a text file to which the FC output is redirected. Note that the `/U` switch is required because registration files use the Unicode character set.

Importing a `.reg` File

If you need to restore the key that you backed up to a registration file, follow these steps:

1. Open the Registry Editor.
2. Select File, Import to display the Import Registry File dialog box.
3. Find and select the file you want to import.
4. Click Open.
5. When Windows 7 tells you the information has been entered into the Registry, click OK.

NOTE

You also can import a `.reg` file by locating it in Windows Explorer and then double-clicking the file.

CAUTION

Many applications ship with their own `.reg` files for updating the Registry. Unless you're sure that you want to import these files, avoid double-clicking them. They might end up overwriting existing settings and causing problems with your system.

Working with Registry Entries

Now that you've had a look around, you're ready to start working with the Registry's keys and settings. In this section, I'll give you the general procedures for basic tasks, such as modifying, adding, renaming, deleting, and searching for entries, and more. These techniques will serve you well throughout the rest of the book when I take you through some specific Registry modifications.

Changing the Value of a Registry Entry

Changing the value of a Registry entry is a matter of finding the appropriate key, displaying the setting you want to change, and editing the setting's value. Unfortunately, finding the key you need isn't always a simple matter. Knowing the root keys and their main subkeys, as described earlier, will certainly help, and the Registry Editor has a Find feature that's invaluable. (I'll show you how to use it later.)

To illustrate how this process works, let's work through an example: changing your registered owner name and company name. In earlier versions of Windows, the installation process probably asked you to enter your name and, optionally, your company name. These registered names appear in several places as you work with Windows:

- If you select Help, About in most Windows 7 programs, your registered names appear in the About dialog box.
- If you install a 32-bit application, the installation program uses your registered names for its own records (although you usually get a chance to make changes).

Unfortunately, if you install a clean version of Windows 7, Setup doesn't ask you for this data, and it takes your username as your registered owner name. (If you upgraded to Windows 7 for Windows XP, the owner name and company name were brought over from your previous version of Windows.) With these names appearing in so many places, it's good to know that you can change either or both names (for example, to put in your proper names if Windows 7 doesn't have them or if you give the computer to another person). The secret lies in the following key:

```
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion
```

To get to this key, you open the branches in the Registry Editor's tree pane: `HKEY_LOCAL_MACHINE`, and then `SOFTWARE`, and then `Microsoft`, and then `Windows NT`. Finally, click the `CurrentVersion` subkey to select it. Here, you see a number of settings, but two are of interest to us (see Figure 12.4):

`RegisteredOrganization`	This setting contains your registered company name.
`RegisteredOwner`	This setting contains your registered name.

TIP

If you have keys that you visit often, you can save them as favorites to avoid trudging through endless branches in the keys pane. To do this, navigate to the key and then select Favorites, Add to Favorites. In the Add to Favorites dialog box, edit the Favorite Name text box, if desired, and then click OK. To navigate to a favorite key, pull down the Favorites menu and select the key name from the list that appears at the bottom of the menu.

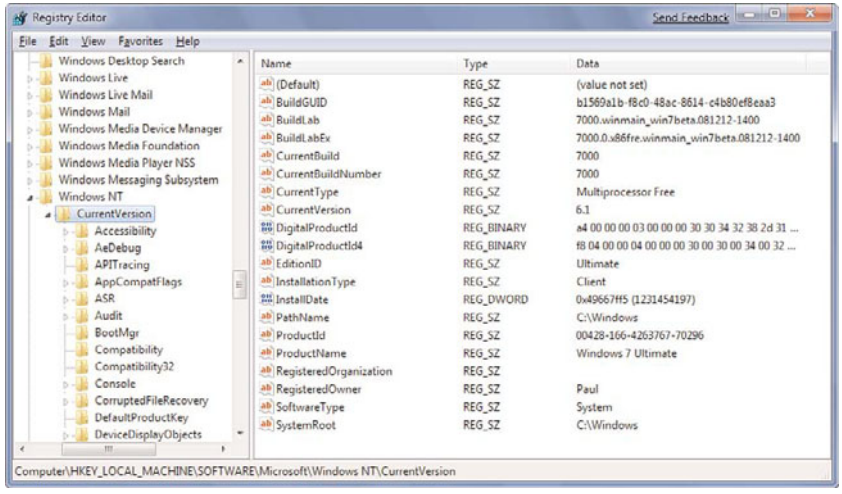

FIGURE 12.4 Navigate to `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion` to see your registered names.

Now you open the setting for editing by using any of the following techniques:

- Select the setting name and either select Edit, Modify or press Enter.
- Double-click the setting name.
- Right-click the setting name and click Modify from the context menu.

The dialog box that appears depends on the value type you're dealing with, as discussed in the next few sections. Note that edited settings are written to the Registry right away, but the changes might not go into effect immediately. In many cases, you need to exit the Registry Editor and then either log off or restart Windows 7.

Editing a String Value

If the setting is a `REG_SZ` value (as it is in our example), a `REG_MULTI_SZ` value, or a `REG_EXPAND_SZ` value, you see the Edit String dialog box, shown in Figure 12.5. Use the Value Data text box to enter a new string or modify the existing string, and then click OK. (For a `REG_MULTI_SZ` multistring value, Value Data is a multiline text box. Type each string value on its own line. That is, after each string, press Enter to start a new line.)

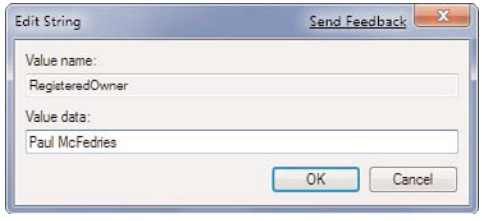

FIGURE 12.5 You see the Edit String dialog box if you're modifying a string value.

Editing a DWORD or QWORD Value

If the setting is a `REG_DWORD`, you see the Edit DWORD (32-Bit) Value dialog box shown in Figure 12.6. In the Base group, select either Hexadecimal or Decimal, and then use the Value Data text box to enter the new value of the setting. (If you chose the Hexadecimal option, enter a hexadecimal value; if you chose Decimal, enter a decimal value.) Note that editing a `QWORD` value is identical, except that the dialog box is named Edit QWORD (64-Bit) Value, instead.

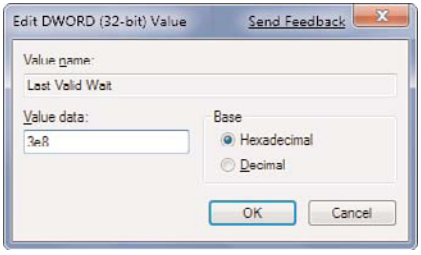

FIGURE 12.6 You see the Edit DWORD Value dialog box if you're modifying a double word value.

Editing a Binary Value

If the setting is a `REG_BINARY` value, you see an Edit Binary Value dialog box like the one shown in Figure 12.7.

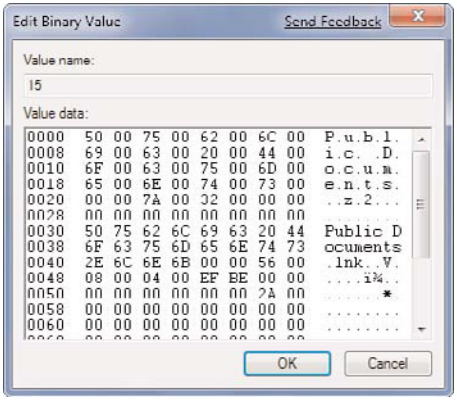

FIGURE 12.7 You see the Edit Binary Value dialog box if you're modifying a binary value.

For binary values, the Value Data box is divided into three vertical sections:

- **Starting Byte Number—**The four-digit values on the left of the Value Data box tell you the sequence number of the first byte in each row of hexadecimal numbers. This sequence always begins at 0, so the sequence number of the first byte in the first row is 0000. There are eight bytes in each row, so the sequence number of the first byte in the second row is 0008, and so on. You can't edit these values.
- **Hexadecimal Numbers (Bytes)—**The eight columns of two-digit numbers in the middle section display the setting's value, expressed in hexadecimal numbers, where

which each two-digit number represents a single byte of information. You can edit these values.

- **ANSI Equivalents—**The third section on the right side of the Value Data box shows the ANSI equivalents of the hexadecimal numbers in the middle section. For example, the first byte of the first row is the hexadecimal value 54, which represents the uppercase letter *T*. You can also edit the values in this column.

Editing a `.reg` File

If you exported a key to a registration file, you can edit that file and then import it back into the Registry. To make changes to a registration file, find the file in Windows Explorer, right-click the file, and then click Edit. Windows 7 opens the file in Notepad.

TIP

If you need to make global changes to the Registry, export the entire Registry and then load the resulting registration file into WordPad or some other word processor or text editor. Use the application's Replace feature (carefully!) to make changes throughout the file. If you use a word processor for this, be sure to save the file as a text file when you're done. You can then import the changed file back into the Registry.

Creating a `.reg` File

You can create registration files from scratch and then import them into the Registry. This is a handy technique if you have some customizations that you want to apply to multiple systems. To demonstrate the basic structure of a registration file and its entries, Figure 12.8 shows two windows. The top window is the Registry Editor with a key named Test highlighted. The Settings pane contains six sample settings: the (`Default`) value and one each of the five types of settings (binary, DWORD, expandable string, multistring, and string). The bottom window shows the `Test` key in Notepad as an exported registration file (`Test.reg`).

NOTE

The file that contains the test Registry code (`test.reg`) is available on my website at www.mcfedries.com/Windows7Unleashed.

Windows 7 registration files always start with the following header:

```
Windows Registry Editor Version 5.00
```

TIP

If you're building a registration file for a Windows 9x, Me, or NT 4 system, change the header to the following:

```
REGEDIT4
```

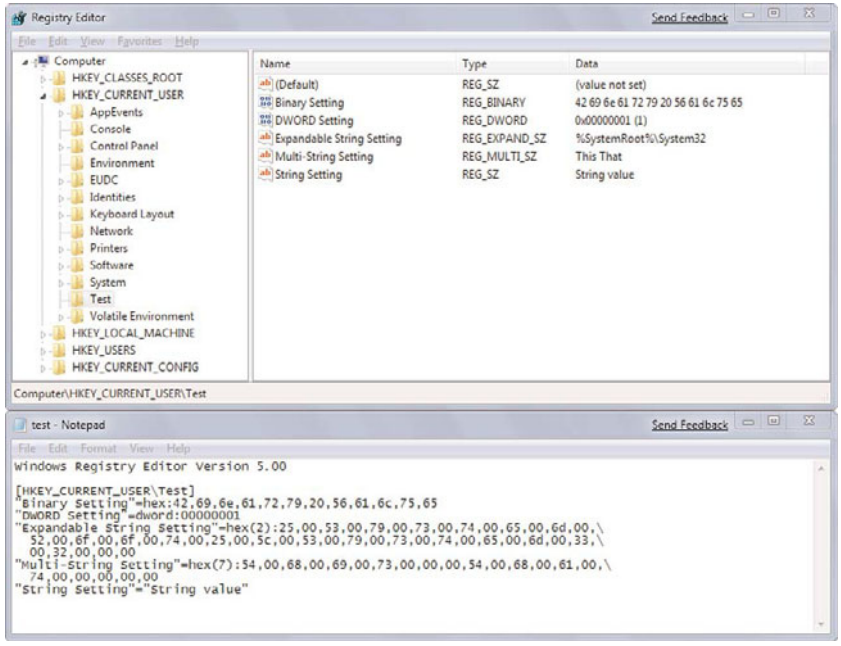

FIGURE 12.8 The settings in the `Test` key shown in the Registry Editor correspond to the data shown in `Test.reg` file shown in Notepad.

Next is an empty line followed by the full path of the Registry key that will hold the settings you're adding, surrounded by square brackets:

```
[HKEY_CURRENT_USER\Test]
```

Below the key are the setting names and values, which use the following general form:

TIP

If you want to add a comment to a `.reg` file, start a new line and begin the line with a semicolon (`;`).

```
"SettingName"=identifier:SettingValue
```

`SettingName`	The name of the setting. Note that you use the `@` symbol to represent the key's `Default` value.
`identifier`	A code that identifies the type of data. `REG_SZ` values don't use an identifier, but the other four types do:
`dword`	Use this identifier for a `DWORD` value.
`hex(b)`	Use this identifier for a QWORD value.
`hex`	Use this identifier for a binary value.

	`hex(2)`	Use this identifier for an expandable string value.
	`hex(7)`	Use this identifier for a multistring value.
SettingValue	This is the value of the setting, which you enter as follows:	
	String	Surround the value with quotation marks.
	DWORD	Enter an eight-digit `DWORD` value.
	QWORD	Enter eight two-digit hexadecimal pairs, separated by commas, with the pairs running from highest order to lowest. For example, to enter the QWORD value 123456789abcd, you would use the following value: `cd,ab,89,67,45,23,01,00`
	Binary	Enter the binary value as a series of two-digit hexadecimal numbers, separating each number with a comma.
	Expandable string	Convert each character to its hexadecimal equivalent and then enter the value as a series of two-digit hexadecimal numbers, separating each number with a comma, and separating each character with 00.
	Multistring	Convert each character to its hexadecimal equivalent and then enter the value as a series of two-digit hexadecimal numbers, separating each number with a comma, and separating each character with 00, and separating each string with space (00 hex).

TIP

To delete a setting using a `.reg` file, set its value to a hyphen (-), as in this example:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Test]
"BinarySetting"=-
```

To delete a key, add a hyphen to the start of the key name, as in this example:

```
Windows Registry Editor Version 5.00

[-HKEY_CURRENT_USER\Test]
```

Renaming a Key or Setting

You won't often need to rename existing keys or settings. Just in case, though, here are the steps to follow:

1. In the Registry Editor, find the key or setting you want to work with, and then highlight it.
2. Select Edit, Rename, or press F2.
3. Edit the name and then press Enter.

CAUTION

Rename only those keys or settings that you created yourself. If you rename any other key or setting, Windows 7 might not work properly.

Creating a New Key or Setting

Many Registry-based customizations don't involve editing an existing setting or key. Instead, you have to create a new setting or key. Here's how you do it:

1. In the Registry Editor, select the key in which you want to create the new subkey or setting.
2. Select Edit, New. (Alternatively, right-click an empty section of the Settings pane and then click New.) A submenu appears.
3. If you're creating a new key, select the Key command. Otherwise, select the command that corresponds to the type of setting you want: String Value, Binary Value, DWORD Value, Multi-String Value, or Expandable String Value.
4. Type a name for the new key or setting.
5. Press Enter.

Deleting a Key or Setting

Here are the steps to follow to delete a key or setting:

1. In the Registry Editor, select the key or setting that you want to delete.
2. Select Edit, Delete, or press Delete. The Registry Editor asks whether you're sure.
3. Click Yes.

CAUTION

Again, to avoid problems, you should delete only those keys or settings that you created yourself. If you're not sure about deleting a setting, try renaming it instead. If a problem arises, you can also return the setting back to its original name.

Finding Registry Entries

The Registry contains only five root keys, but they contain hundreds of subkeys. The fact that some root keys are aliases for subkeys in a different branch only adds to the confusion. If you know exactly where you're going, the Registry Editor's tree-like hierarchy is a reasonable way to get there. If you're not sure where a particular subkey or setting resides, however, you could spend all day poking around in the Registry's labyrinthine nooks and crannies.

To help you get where you want to go, the Registry Editor has a Find feature that enables you to search for keys, settings, or values. Here's how it works:

1. In the Keys pane, select Computer at the top of the pane (unless you're certain of which root key contains the value you want to find; in this case, you can highlight the appropriate root key instead).
2. Select Edit, Find or press Ctrl+F. The Registry Editor displays the Find dialog box, shown in Figure 12.9.

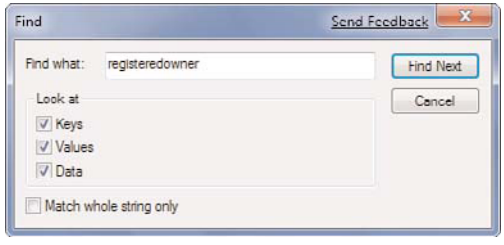

FIGURE 12.9 Use the Find dialog box to search for Registry keys, settings, or values.

3. Use the Find What text box to enter your search string. You can enter partial words or phrases to increase your chances of finding a match.
4. In the Look At group, activate the check boxes for the elements you want to search. For most searches, you want to leave all three check boxes activated.
5. If you want to find only those entries that exactly match your search text, activate the Match Whole String Only check box.
6. Click the Find Next button. The Registry Editor highlights the first match.
7. If this isn't the item you want, select Edit, Find Next (or press F3) until you find the setting or key you want.

When the Registry Editor finds a match, it displays the appropriate key or setting. Note that if the matched value is a setting name or data value, Find doesn't highlight the current key. This is a bit confusing, but remember that the current key always appears at the bottom of the Keys pane.

Index

Symbols & Numerics

| (pipe operator), 714

.reg files

creating, 240-242

editing in Registry, 240

importing, 236

8.3 filename creation, disabling, 130

9-step maintenance plan, setting up, 162-163

A

accelerator keys, defining for new actions, 51

access points, signal leakage, 428-430

Accessibility group (Internet Explorer, Advanced Tab), 38

accessing, 554-556, 615-617, 635-636

homegroups, 521

Network and Sharing Center, 516-518

Network Connections window, 530

router setup pages, 299

acknowledgments (TCP), 758

ACPI (Advanced Configuration and Power Interface), 479

Action Center icon (Control Panel), 168

activating

Administrator account, 76-79

InPrivate Filtering, 326

ad hoc wireless networks, creating, 543-545

add-ons (Internet Explorer), managing, 336
adding
applications to Open With dialog box, 62
Control Panel to Start menu, 176-177
memory, 124
search engines to Internet Explorer, 30-31
security zone sites, 329-330
shortcuts to Start menu, 97-98
snap-ins, 200-202
users with User Accounts dialog box, 386-387
Address Bar, 108
list, clearing, 320-322
searching, configuring, 32-34
addresses (networks), 556-558
adjusting, processor scheduling, 124-125
administrative passwords, specifying for routers, 428
Administrative Tools icon (Control Panel), 168
Administrator account, 390
disabling, 307-308
elevated Command Prompt sessions, 246-247
enabling, 76-79
scripts, running, 664, 680
Advanced Boot Options menu, customizing startup options, 73-76
advanced options (Internet Explorer), 37-38
Advanced tab (Internet Explorer)
Accessibility group, 38
Browsing group, 39-42
HTTP 1.1 Settings group, 42
Multimedia group, 42-43
Printing group, 43
Security group, 43
security options, 337-339
AirPort, 643-644
aliases (cmdlets), 706-709
anonymous access (IIS websites), 635-636
AntiSpyware (MS). *See* Windows Defender, 304
application layer (TCP/IP stack), 743
applications
adding to Open With menu, 62
assocating with multiple file types, 55-56
boot applications, 64, 72
optimizing, 125-126
removing from Open With menu, 61-62
AQS (Advanced Query Syntax), 22-23
Boolean operators, 24-25
operators, 23
ARP cache, viewing contents of, 502
arp command, 499
assigning
Full Control permissions to folders, 20-22
objects to variables, 668
permissions, 363-364
PowerShell objects to a variable, 722
special permissions, 364-366
users to security groups, 361-363
associating
applications with multiple file types, 55-56
extensions with different applications, 53-57
attrib utility, 278-279
authentication, 637
author mode (MMC), 207
AUTOCHK utility, 139-140
AutoComplete feature (Internet Explorer), 41
automatic file backups, configuring, 155-156
automatic IP addressing, configuring, 531-534
automatic logins, 123
override, disabling, 80
setting up, 79
automatic service startup, configuring, 212
Automatic Sleep mode, 587
automation objects, creating, 672-674
AutoPlay icon (Control Panel), 169

B

background colors, changing for Command Prompt sessions, 249

backing up

- BCD store, 72
- files, 153-154
- Registry, 234
- system image, 157

Backup and Restore icon (Control Panel), 169

Backup Operators group, 360

backups, 648

base priority, 126

batch files, 260

- comments, adding, 261
- conditions, handling, 266-269
- creating, 260
- jumping to a line, 265-266
- looping, 264
- messages, displaying from, 261-262
- parameters, 263-264
- pausing, 262
- strings, comparing, 267

BCD (Boot Configuration Data)

- modifying with System Configuration Utility, 66-68
- startup, customizing, 64-66

BCDEDIT, customizing startup options, 69-73

best practices, general troubleshooting tips, 447-448

binary values, editing in Registry, 239

Biometric Devices icon (Control Panel), 169

BIOS

- checks, reducing, 121
- DVD-based bootup, enabling, 487
- startup, troubleshooting, 482

bit bucket, 257

BitLocker

- disks, encrypting, 368
- enabling
  - on non-TPM systems, 369-371
  - on TPM systems, 369

BitLocker Drive Encryption icon (Control Panel), 169

blocking

- email messages, 349
- email messages from specific countries, 349-350
- pop-up windows, 327-328
- read receipts, 352

Boolean operators

- AND, 750
- AQS, 24-25
- natural language search queries, 25-26

boot applications, 64, 72

boot configuration data, customizing startup, 63

Broderick, Matthew, 423

broken services, resetting, 222-224

browsers, accessing router setup pages, 299

Browsing group (Internet Explorer, Advanced Tab), 39-42

browsing history, deleting, 316, 318-319

BSOD (blue screen of death), 443-444

bugs, 440

built-in accounts, renaming, 405-406

bypassing Windows Security screen, 114

C

cables, troublesooting, 506-507

caret browsing, 38

CDO (Collaboration Data Objects), sending email messages via, 343-344

changing
default SSID value, 435-436
security zone security level, 330-331
changing folders in command line, 253
changing Registry entries, 237
channels, 353
Check Disk GUI, starting, 138-139
checking
free disk space on hard drive, 140-142
for updates, 158-160
chard drive for errors, 135-136
chkdsk utility, 270-271
chkntfs utility, 271-274
class instances (WMI), returning, 696-699
classes of IP addresses, 746-748
clearing
Address Bar list (Internet Explorer), 320-322
recent programs from Start menu, 94
clocks, displaying multiple for different time zones, 106-107
clusters
cross-linked, 138
invalid, 138
lost, 137
cmd command, 247-250
cmdlets, 705
aliases, 706-709
Get-Member, 714-715
Get-Process, 715-717
running, 709-713
collections, 669
enumerators, 670
For Each....Next loops, 669
PowerShell, 724-725
Color Management icon (Control Panel), 169
command line, 561
accessing, 246
Control Panel icons, launching, 173-174
doskey utility, 254
command lines, editing, 255
command recall, 254-255
multiple commands, running on single line, 255
Command Prompt
Autocomplete, 250
elevated sessions, running, 246-247
external commands, 251
folders, changing, 253
internal commands, 251
launching, 247-248
long filenames, 252
opening, 246
services, controlling, 212-213
sessions, changing background colors, 249
switches, 248, 250
command-line utilities, 499
ipconfig, 500-502
ping, 502-504
tracert, 504-505
commands
batch files, 260
comments, adding, 261
conditions, handling, 266-269
creating, 260
jumping to a line, 265-266
looping, 264
messages, displaying from, 261-262
parameters, 263-264
pausing, 262
cmd, 247-250
echo, 261-262
for, 264
goto, 265-266
if, 266-269
input, redirecting, 258
NET CONTINUE, 212

NET PAUSE, 212
NET START, 212
NET STOP, 212
net user, 393-394
output, redirecting, 256-257
pause, 262
piping, 259
reg, 289-291
rem, 261
ren, 281-282
replace, 282-283
running, 251
SHUTDOWN, 81
sort, 258, 283-284
subst, 253
systeminfo, 256-257, 292-293
tracert, 751
typeperf, 293-295
whoami, 295-296, 407
xcopy, 284-288

comments, adding to batch files, 261

commit limit, 451

comparing strings in batch files, 267

Component Services icon (Control Panel), 168

compression, disabling, 128

Computer Management icon (Control Panel), 168

computer name, configuring for peer-to-peer networks, 513

computers, locking, 300-302

conditions, handling in batch files, 266-269

configuring

automatic file backups, 155-156
automatic IP addressing, 531-534
automatic logon, 79
automatic service startup, 212
group policies, 233-234
Internet Explorer
address bar searching, 32-34
page history, 29-30
logon hours for users, 420-422
one-click restarts/shutdowns, 81-83
peer-to-peer networks, 512-513
homegroups, 518-522
wireless, 514-515
workgroup name, 513
permissions
security permissions, 414-415
shared permissions, 411-414
policies, 185-186
PowerShell
execution policy, 726
ISE, 726-727
prefetcher, 123
remote shutdowns, 84-86
Start menu, default programs, 94-95
static IP addressing, 534-537
Task Manager, program priority, 125-126
UAC, 377-380
user accounts
lockout policies, 391-392
parental controls, 395-400
security policies, 389-390
user rights policies, 391
Windows Live Mail
email, blocking from senders, 349
email, blocking from specific countries, 349-350
junk email protection level, 347-348
Safe Sender list, 348
wireless networks
ad hoc, 543-545
properties, 545-548

connecting to hidden wireless networks, 434

connection bar, 598

connections (TCP), opening, 758
connectivity, verifying with ping command, 502-504
console root, adding snap-ins, 200-202
consoles, 197
saving, 202-203
content indexing, disabling on hard drive, 128
Content view, Windows Explorer icons, 9
Control Panel
adding to Start menu, 176-177
dialog boxes, launching, 172
displaying, 166
files, 172
icons
hiding, 178
launching, 173-174
opening, 175-176
removing, 177-178
policies, 179
controlling
services at command prompt, 212-213
services with scripts, 213-217
snap-ins with group policies, 207
web pages cache in Internet Explorer, 28-29
CONVERT utility, 129
converting
FAT16/FAT32 partitions to NTFS, 129-130
Start menu links to menus, 96-97
cookies, 317, 322-325
counters, 119-120
CPL files, 172
CPU tab (Resource Monitor), 118
crackers, 424
thwarting, 298-300
computers, locking, 300-302
Ctrl+Alt+Delete, requiring at startup, 302
crawlers, 346
CreateObject method, 672-674
CreateShortcut methods, 682
creating
.reg files, 240-242
batch files, 260
exception for Windows Firewall, 309-313
new actions for file types, 50-53
new file types, 56-57
password reset disk, 383
Registry keys, 243
restart shortcut, 83-84
script jobs, 661
shortcuts in Windows Script Host, 682-685
shutdown shortcut, 84
strong passwords, 381
system image backup, 157
system recovery disc, 153
toolbars, 109
wireless network connections, user-specific, 549-550
Credential Manager icon (Control Panel), 169
critical update restore points, 458
cross-linked clusters, 138
Cryptographic Operators group, 360
CScript, 661-662
script properties, 663
Ctrl+Alt+Delete, requiring at startup, 302
custom taskpad view, creating in MMC, 203-205
customizing
icons in Windows Explorer, 8
Internet Explorer, advanced options, 37-43
New menu, 57-59
page file size, 131-132, 134
Start menu, 90
default programs, 94-95
favorite programs, 91-93
links, converting to menus, 96-97
power button, 86-87

recent programs, clearing, 94
shortcuts, adding/removing, 97-98
startup, 63-66
startup with Advanced Boot Options menu, 73-76
startup with BCDEDIT, 69-73
taskbar, 98-104
Windows Explorer, view options, 16-19
your network, 528-529
cycles, 126, 138

D

data collector sets, 121
data link layer (TCP/IP stack), 743
Data Sources icon (Control Panel), 168
data transfer rate, 119, 526
datagrams, 743-745
TTL value, 751
Date and Time icon (Control Panel), 169
DCHP lease, releasing, 501
DDNS (Dynamic DNS), 604
Debugging Mode, when to use, 484
default action, setting for file types, 49-50
default documents, 631-634
default gateway, 750
default programs, configuring, 94-95
Default Programs icon (Control Panel), 169
default search provider, preventing changes to, 31
default TTL value, changing, 505
Defender (Windows), accessing, 304
defrag utility, 274-276
defragmenting the hard drive, 145-149
delaying service shutdown, 222
delete confirmations, turning off, 13-15
deleting
browsing history, 316-319
file types from New menu, 59
Registry keys, 243
services, 223
unnecessary files, 143-145
dependent services, 211
Desktop Gadgets icon (Control Panel), 169
Desktop toolbar, 108
desktops, 649-652
Details view, Windows Explorer icons, 8-10
device drivers
downloading, 478-479
updating, 124
upgrading, 123
Device Manager, 462
device drivers, exporting to text file, 469-471
device properties, viewing, 463
devices
troubleshooting, 473-474
uninstalling, 471
drivers, updating, 465-466
nonpresent devices, displaying, 464
nonworking devices, displaying, 474-477
unsigned device drivers, ignoring, 466-469
views, 463
Device Manager icon (Control Panel), 169
devices
drivers
exporting list to text file, 469-471
troubleshooting, 477-478
power cycling, 494
routers, displaying setup pages, 424-427
security policies, 472
troubleshooting with Device Manager, 473-474
uninstalling, 471
viewing on network, 523-524

Devices and Printers icon (Control Panel), 169

DHCP (Dynamic Host Configuration Protocol), 531, 751

dialog boxes

keyboard shortcuts, 734

User Accounts, 386-387

digital IDs, obtaining, 354-355

directories (virtual), adding folders as (IIS), 626-627

Directory Services Restore Mode, when to use, 484

Disable Automatic Restart on System Failure option, when to use, 484

Disable Driver Signature Enforcement option, when to use, 485

disabling

8.3 filename creation on hard drive, 130

Administrator account, 307-308

automatic logon override, 80

compression, 128

content indexing on hard drive, 128

Delete Confirmation Dialog check box, 14

encryption, 128

hidden shares, 417-418

homegroup connections, 522

network connections, 541

notification area, 105-106

Open With check box, 62

services, 212, 217

Sharing Wizard, 410-411

SSID broadcasting on wireless networks, 432-433

startup splash screen, 122

unnecessary services, 217-221

unsigned drivers, 478

user accounts, 402-403

disconnecting, 561, 599

discovering logged in users with whoami command, 407

Disk Cleanup, 143-145

Disk Defragmenter, 146

disks, selecting, 148-149

schedule, changing, 147

disk diagnostics, 449

disk management tools, 269

chkdsk, 270-271

chkntfs, 271-274

defrag, 274-276

Disk tab (Resource Monitor), 119

disks, encrypting, 368

Display icon (Control Panel), 169

displaying

Control Panel, 166

current IP address, 533

DNS addresses, 535-536

file extensions, 11-13

folder properties, 10

Internet Options dialog box (Internet Explorer), 28

multiple clocks for different time zones, 106-107

network status, 525-527

router setup pages, 424-427

selected Control Panel icons, 178

taskbar, toolbars, 108

Windows Explorer menu full-time, 8

Distributed COM Users group, 360

dithering, 43

DNS, 751-754

gTLDs, 753

LMHOSTS file, 752

top-level domains, 753-754

DNS addresses, displaying, 535-536

DNS servers, 754

documents, 631-634

keyboard shortcuts, 733

opening with unassociated applications, 59-60

domains, logging on to, 76
doskey utility, 254
command lines, editing, 255
command recall, 254-255
keyboard shortcuts, 738
multiple commands, running on single line, 255
dotted-decimal notation, 745-746
double output redirection, 256
double-clicking, 555-556
downloading
device drivers, 478-479
drivers from manufacturer, 478
DPS (Diagnostic Policy Service), 450
drag-and-drop operations, keyboard shortcuts, 735
drive-by downloads, 304
protecting against, 345
drivers
downloading, 478-479
exporting list to text file, 469-471
rolling back, 478
troubleshooting, 477-478
unsigned, ignoring, 466-469
updates, checking for, 465-466
updating, 466
DVD-based bootup, enabling, 487
DWORD, editing in Registry, 239
dynamic IP addressing, 751

E

Ease of Access Center icon (Control Panel), 169
echo command, 261-262
Echo method, 671
editing
command lines, 255
Registry
.reg files, 240
binary values, 239
string values, 238
elements, 669
elevated Command Prompt sessions, running, 246-247
elevating privileges, 375-376
email
blocking
from senders, 349
from specific countries, 349-350
CDO, sending messages via, 343-344
digital ID, obtaining, 354-355
encrypting, 353-354
phishing, protecting against, 350-351
public key, obtaining, 355-356
read receipts, blocking, 352
scanning with Windows Defender, 345
secure messages
receiving, 356-357
sending, 356
spam, thwarting, 345-346
viruses, protecting against, 341, 343-345
web bugs, suppressing, 352-353
Enable Boot Logging option, when to use, 483
Enable VGA Mode option, when to use, 484
enabling
Administrator account, 76-79
DVD-based bootup, 487
full-screen mode, 15
MAC address filtering, 436-438
network discovery, 495-497
password-protected sharing, 410
write caching on hard drive, 128-129

encrypting
disks, 368
email, 353-354
digital ID, obtaining, 354-355
public key, obtaining, 355-356
files, 366-367
encryption, 577
disabling, 128
reversible, 383
WPA, 430-432
enumerators, 670
environment variables, 687-689
erratic services, resetting, 222-224
error detection, 758
error messages, troubleshooting, 441
essential services, 211
Event Log Readers group, 361
Event Viewer
troubleshooting error messages, 441
logs, reviewing, 160-162
Event Viewer icon (Control Panel), 168
events, 581-582, 714
examples
of group policies
Places bar, customizing, 191-193
Recent Items list, increasing size of, 193-194
Shutdown Event Tracker, enabling, 194-195
Windows Security window, customizing, 189-191
of Internet Explorer scripts, 691-692
exceptions, creating for Windows Firewalls, 309-313
execution policy (PowerShell), configuring, 726
exporting
device driver list to text file, 469-471
Registry keys to disk, 235-236
exposing VBScript/JavaScript objects, 675
extensions, 46
associating applications with multiple file types, 53-57
hiding, 52-53
external commands, 251

F

false positives, 347
FAT16/FAT32 partitions, converting to NTFS, 129-130
favorite destinations, pinning to jump list, 101-102
favorite programs (Start menu)
increasing displayed number of, 91-92
pinning to Start menu, 92-93
pinning to taskbar, 100-101
features of TCP, 758
file and Registry virtualization, 377
file extensions, displaying, 11-13
file fragmentation, 145
file management tools
attrib, 278-279
find, 279-281
ren, 281-282
replace, 282-283
sort, 283-284
xcopy, 284-288
file system
cycles, 138
permissions, setting, 360
file types, 46
creating, 56-57
default action, setting, 49-50
deleting from New menu, 59

extensions
associating with different applications, 53-55
hiding, 52-53
new actions, creating, 50-53
files, 572-582, 622-623
backing up, 153-154
encrypting, 366-367
FileSystemObject object, 675-677
filtering
policies, 187-189
PowerShell object instances, 719-720
find utility, 279-281
finding
MAC address, 537-539
Registry entries, 244
firewalls, 588, 601, 614-615
firmware, updating, 497-498
Flash drives, 559
flow control, 758
folder management tools
attib, 278-279
find, 279-281
ren, 281-282
replace, 282-283
sort, 283-284
xcopy, 284-288
Folder Options icon (Control Panel), 170
folders, 572-582, 585, 623-627
changing in command line, 253
encrypting, 366-367
Full Control permissions, assigning, 20-22
hidden, disabling, 417-418
keyboard shortcuts, 735
moving, 19
network, 558-561
properties, displaying, 10
remote, 562
shared folders
hiding, 415-417
security permissions, configuring, 414-415
Fonts icon (Control Panel), 170
for command, 264
For Each...Next loops, 669
For loops, 670
foreground colors, changing for Command Prompt sessions, 249
forgotten passwords, recovering, 383-384
form data, 317
formatting PowerShell scripting output, 717-719
forwarding, 602
fragmentation, 145
free disk space, checking on hard drive, 140-142
FTP (File Transfer Protocol), 742
Full Control permission, 360
assigning to folders, 20-22
full-screen mode, enabling, 15

G

games, configuring parental controls, 397-400
gateways (network), 606
general keyboard shortcuts, 732
general troubleshooting tips, 447-448, 494
Get-Member cmdlet, 714-715
Get-Process cmdlet, 715-717
GetObject method, 674-675
Getting Started icon (Control Panel), 170
ghosted devices, displaying in Device Manager, 464
goto command, 265-266

granting temporary access with Guest account, 406-407
group policies, 181-182
configuring, 185-186, 233-234
filtering, 187-189
Places bar, customizing, 191-193
Recent Items list, increasing size of, 193-194
Shutdown Event Tracker, enabling, 194-195
snap-ins, controlling, 207
Start menu, modifying, 109-110
Windows Security window, customizing, 189-191
Group Policy Editor, 14, 182
device security policies, 472
launching, 183
panes, 184
policies
configuring, 185-186
filtering, 187-189
Group Policy Settings Reference, 182
gTLDs, 753
Guest account, 406-407
Guests group, 361

H

handles, 116
Handley, Pete, 704
hard drive, 558-561
8.3 filename creation, disabling, 130
cache, 127
checking for errors, 135-136
clusters
cross-linked, 138
invalid, 138
lost, 137
compression, disabling, 128
content indexing, disabling, 128
defragmenting, 145-149
encryption, disabling, 128
free disk space, checking, 140-142
maintenance, performing, 128
NTFS, disabling Last Access Timestamp, 130
partitions, converting to NTFS, 129-130
sectors, 137
seek time, 127
speed, 127
troubleshooting, 449
write caching, enabling, 128-129
Hibernate mode. *See* Sleep mode (Start menu)
hidden shares
disabling, 417-418
viewing, 417
hidden wireless networks, connecting to, 434
hiding
Control Panel icons, 178
extensions, 52-53
shared folders, 415-417
user names in logon screen, 403-405
History list, configuring in Internet Explorer, 29-30
hives, 231-233
HKEY_CLASSES_ROOT key, 47-48
HKEY_CLASSES_ROOT root key, 229-230
HKEY_CURRENT_CONFIG root key, 231
HKEY_CURRENT_USER root key, 230
HKEY_LOCAL_MACHINE root key, 230
HKEY_USERS root key, 231
home networks, 528
home pages, 624-625
opening multiple at startup (Internet Explorer), 35-37
HomeGroup icon (Control Panel), 170

homegroups
configuring, 518-522
connections, disabling, 522
homograph spoofing, 333
Hopper, Grace, 440
host computers (Remote Desktop), 586-591, 602
hot spots, 515
HTTP (HyperText Transfer Protocol), 742
HTTP 1.1 Settings group (Internet Explorer, Advanced Tab), 42

I

ICMP echo packets, 502
icons
Control Panel
launching, 173-174
opening, 175-176
removing, 177-178
customizing in Windows Explorer, 8
Details view, 9-10
Network icon, operational states, 493-494
pinning to Start menu, 92-93
IDN spoofing, 333-335
if command, 266-267, 269
ignoring unsigned device drivers, 466-469
IIS (Internet Information Services), 612-639
IIS_IUSRS group, 361
IMAP, 742
importing .reg files, 236
increasing displayed number of favorite programs, 91-92
Indexing Options icon (Control Panel), 170
inetpub folder (IIS default website), 618
InPrivate browsing, 325
InPrivate filtering, 318, 326
input redirection operator, 258
install restore points, 458
installing, 613
instances (PowerShell)
filtering, 719-720
sorting, 720-722
internal commands, 251
Internet, 599-603, 617
Internet Explorer
add-ons, 336
Address Bar list, clearing, 320-322
address bar searching, configuring, 32-34
advanced security options, 337-339
Advanced tab (Internet Options dialog box), 37-38
Accessibility group, 38
Browsing group, 39-42
HTTP 1.1 Settings group, 42
Multimedia group, 42-43
Printing group, 43
Security group, 43
AutoComplete feature, 41
browsing history, deleting, 316-319
cookies, managing, 322-325
default search provider, preventing changes to, 31
home page, opening multiple at startup, 35-37
IDN spoofing, preventing, 334-335
InPrivate browsing, 325
InPrivate filtering, 326
Internet Options dialog box, displaying, 28
keyboard shortcuts, 736
page history, configuring, 29-30
Phishing Filter, 332-334
pop-up windows, blocking, 327-328
protected mode, 331
search engines, adding, 30-31

security zones, 328-329
security level, changing, 330-331
sites, adding/removing, 329-330
SmartScreen Filter, 333-334, 350-351
tabbed browsing, 34-35
web pages
cache, controlling, 28-29
displaying with scripts, 691-692
navigating with scripts, 692
Internet Options (Control Panel), 170
Internet Options dialog box (Internet Explorer)
Advanced tab, 37
Accessibility group, 38
Browsing group, 39-42
HTTP 1.1 Settings group, 42
Multimedia group, 42-43
Printing group, 43
Security group, 43
displaying, 28
Internet zones, 328
InternetExplorer object properties, 693
invalid clusters, 138
IP (Internet Protocol), 742. *See also* IP addressing; IP routing
datagrams, 743-745
DNS, 751-754
dynamic IP addressing, 751
IP addressing
addresses, displaying displaying, 533
classes, 746-748
conflicts, resolving, 513
DNS, 751-754
dotted-decimal notation, 745-746
dynamic, 751
IP routing
default gateway, 750
subnet masks, 748-750
ipconfig command, 500-502
iPod halo effect, 641
IPSec (IP Security) protocol, 606
IRQs (interrupt requests), troubleshooting resource conflicts, 479-480
iSCSI Initiator icon (Control Panel), 168
ISE (Integrated Scripting Environment), 726-727
isolating source of problems, 440-447
Event Viewer, 441
System Information utility, 442

J

JavaScript
collections, enumerators, 670
FileSystemObject object, 675-677
joining homegroups, 520
jump drives, 559
jump list, pinning favorite destinations to, 101-102
jumping to a specific batch file line, 265-266
Junk Filter (Windows Live Mail), 345-349

K

keyboard, launching pinned taskbar icons from, 102-103
Keyboard icon (Control Panel), 170
keyboard shortcuts, 731-739
keys
creating in Registry, 243
deleting from Registry, 243
exporting to disk, 235-236
renaming, 243
Keys pane (Registry), 227

killing slow services, 222
Knittel, Brian, 659
Kopczynski, Tyson, 704

L

Last Access Timestamp, disabling, 130
Last Known Good Configuration
starting Windows 7 with, 456
when to use, 484
launching
Command Prompt sessions, 247-248
Control Panel dialog boxes, 172-174
Group Policy Editor, 183
Memory Diagnostics tool, 451
MMC, 200
pinned taskbar icons from keyboard, 102-103
PowerShell ISE, 727
Registry Editor, 226
Windows Backup, 154
least-privileged user account, 375
left pane (Group Policy Editor), 184
limited users, 374
links (Start menu), converting to menus, 96-97
Links toolbar, 108
List Folder Contents permission, 360
List view, Windows Explorer icons, 8
listening ports, 600-601
LMHOSTS file, 752
loading
Services snap-in, 209
services into system hive, 224
Local Intranet zones, 328
Local Security Policy Editor, 185
Local Security Policy icon (Control Panel), 168
Local Users and Groups MMC snap-in, 388-389
locating Registry entries, 244
Location and Other Sensors icon (Control Panel), 170
locking
computers, 300-302
taskbar, 99
lockout policies, configuring on user accounts, 391-392
logging on to domains, 76
logon hours for users, configuring, 420-422
logon screen, hiding user names, 403-405
logs, 637-639
long filenames, 252
looping
batch files, 264
JavaScript, For loops, 670
VBScript, For Each...Next loops, 669
lost clusters, 137

M

MAC addresses
filtering, 436-438
finding, 537-539
Macs, 641-655
maintenance, performing on hard drive, 128
maintenance plan, setting up, 162-163
malware, 303
Manage Wireless Networks window, opening, 542
managing
cookies, 322-325
Internet Explorer add-ons, 336
user accounts, 384-386

Windows Firewall, 308-309
exception, creating, 309-310
ports, adding as new exception, 311-313
programs, adding as new exception, 310-311
manual restore points, 458
mapping, 558-561
members, 714
memory
adding, 124
shareable, 118
memory cards, 559
Memory Diagnostics tool, 451-452
Memory tab (Resource Monitor), 118
messages, displaying from batch files, 261-262
methods, 667-668
CreateObject, 672-674
Echo, 671
GetObject, 674-675
Quit, 671
PowerShell, 724
RegDelete, 686
RegRead, 685
RegWrite, 686
metrics, WinSAT, 112-114
MFT (Master File Table), 137
Microsoft AntiSpyware. *See* Windows Defender
Microsoft Knowledge Base, 455
Microsoft Product Support Services, 455
Microsoft Security, 455
Microsoft TechNet, 455
MMC (Microsoft Management Console), 197
author mode, 207
consoles, saving, 202-203
custom taskpad view, creating, 203-205
launching, 200
smart modems, 513
snap-ins, 198-199
adding, 200-202
controlling with group policies, 207
Local Users and Groups, 388-389
organizing, 201
Modify permission, 360
modifying
BCD with System Configuration Utility, 66-68
default SSID value, 435-436
Start menu with Group Policies, 109-110
monitoring performance
with Performance Monitor, 119-120
data collector sets, 121
reports, 121
with Resource Monitor, 117
with Task Manager, 114-117
Mouse icon (Control Panel), 170
moving folders, 19
Multimedia group (Internet Explorer, Advanced Tab), 42-43

N

name servers, 754
natural language search queries, 25-26
navigating, 558, 623
nbstat command, 499
NDE (Network Diagnostics Engine), 492
NDF (Network Diagnostics Framework), 492
NET CONTINUE command, 212
NET PAUSE command, 212
NET START command, 212
NET STOP command, 212
net user command, 393-394
NetBIOS, 502

netstat command, 499
network, customizing, 528-529
Network and Sharing Center
accessing, 516-518
Network Map feature, 524
network status, viewing, 526-527
Network and Sharing Center icon (Control Panel), 170
Network Center, 517-518
Network Configuration Operators group, 361
network connections, 529
automatic IP addressing, configuring, 531-534
disabling, 541
renaming, 531
sleeping computers, waking up, 539-541
static IP address, configuring, 534-537
wireless, 542
ad hoc, configuring, 543-545
properties, configuring, 545-548
removing, 551
renaming, 548
reordering, 548-549
user-specific, creating, 549-550
Network Connections window, 530
Network Diagnostic tool, 492
network discovery, enabling, 495-497
network gateways, 606
Network icon, operational states, 493-494
network layer, 743
network locations, 562
Network Map (Network Center), 517, 523-524
network status, viewing, 525-527
networking interface, 517-518, 524
networks, 554-582, 605, 615, 641-655. *See also* IP addressing
new actions, creating for file types, 50-53
New menu
customizing, 57, 59
file types, deleting, 59
newsgroups, 455
NICs
MAC addresses
filtering, enabling, 436-438
finding, 537-539
troubleshooting, 507
NNTP (Network News Transport Protocol), 743
nodes, 197
non-TPM, enabling BitLocker, 369-371
nonpresent devices, viewing in Device Manager, 464
nonworking devices, displaying in Device Manager, 474-475, 477
notebook computers, customizing power buttons, 87-88
notification area, 103
customizing, 104
disabling, 105-106
Notification Area Icons icon (Control Panel), 170
NTFS file system, 367
Last Access Time, disabling, 130

O

objects
assigning to a variable, 668
collections, 669
exposing, 675
FileSystemObject, 675-677
InternetExplorer
properties, 693
sample script, 693-694
JavaScript, exposing, 675
members, 714

methods, 667-668
PowerShell, 714
collections, 724-725
instances, filtering, 719-720
instances, sorting, 720-722
members, returning, 714-715
members, selecting, 715-717
methods, 724
properties, 666
value, returning, 667
value, setting, 666
VBScript, exposing, 675
WScript
CreateObject method, 672-674
Echo method, 671
GetObject method, 674-675
Quit method, 671
WshNetwork, 689
network drives, mapping, 690-691
network printers, mapping, 689
properties, 689
referencing, 689
WshShell, 677
Popup method, 677-681
RegDelete method, 686
RegRead method, 685
RegWrite method, 686
Run method, 681
WshShortcut, 683-685

Offline Files icon (Control Panel), 170

offline file/folder management, 572-582

one-click restarts/shutdowns, configuring, 81-83

online troubleshooting resources, 455-456

Open command, 555

Open With check box, disabling, 62

Open With dialog box, 60-61
adding programs to, 62
removing applications from, 61-62
unassociated applications, opening documents with, 59-60

opening
Command Prompt, 246
Control Panel icons, 175-176
documents with unassociated applications, 59-60
Manage Wireless Networks window, 542
multiple home pages at startup (Internet Explorer), 35-37
Network and Sharing Center, 517
Network window, 523
tabs in Internet Explorer, 34
TCP connections, 758

operators, AQS, 23

optimizing
applications, 124-126
page file storage, 131

organizing snap-ins, 201

OS Choices menu, reducing timeouts, 122

Overview tab (Resource Monitor), 118

P

packets, tracing with tracert, 504-505

page file, 116
size, customizing, 131-134
size of, monitoring, 132
splitting, 131

page history, configuring in Internet Explorer, 29-30

panes, Group Policy Editor, 184

parameters
for batch files, 263-264
WScript, 660-661

parental controls, configuring on user accounts, 395-400
Parental Controls icon (Control Panel), 170
partitions
clusters
cross-linked, 138
invalid, 138
lost, 137
FAT16/FAT 32, converting to NTFS, 129-130
passthroughs (VPN), 606
password reset disk, creating, 383
password-protected sharing, enabling, 410
passwords, 317, 560
hints, 385
policies, 382-383
recovering, 383-384
specifying for wireless routers, 428
strengthening, 381
UAC, options, 381-382
patches, checking for, 158-160
PATH environment variable, 253
pause command, 262
pausing
batch files, 262
services, 210
peer-to-peer networks
configuring, 512-513
homegroups
configuring, 518-522
connections, disabling, 522
wireless, configuring, 514-515
workgroup name, configuring, 513
Pen and Touch icon (Control Panel), 170
performance
applications, optimizing, 124-126
automatic logins, 123
device drivers, upgrading, 123
encryption, disabling, 128
hard drive
8.3 filename creation, disabling, 130
cache, 127
compression, disabling, 128
content indexing, disabling, 128
Last Access Timestamp, disabling, 130
seek time, 127
speed, 127
write caching, enabling, 128-129
monitoring
with Resource Monitor, 117
with Task Manager, 114-117
prefetcher, configuring, 123
startup BIOS checks, reducing, 121
virtual memory
optimizing page file storage, 131
page file size, customizing, 131-134
WinSAT, metrics, 112-114
Performance Information and Tools icon (Control Panel), 170
Performance Log Users group, 361
Performance Monitor, 119
counters, 119-120
data collector sets, 121
reports, 121
Performance Monitor icon (Control Panel), 168
Performance Monitor Users group, 361
Performance tab (Task Manager), 115
peripherals, 563-565
permissions, 621
assigning, 363-364
security permissions, configuring, 414-415
setting, 360
shared permissions, configuring, 411-414
special permissions, 360
assigning, 364-366

Personalization icon (Control Panel), 170
phishing, protecting against, 350-351
Phishing Filter (Internet Explorer), 332-334
Phone and Modem Options icon (Control Panel), 171
physical layer (TCP/IP stack), 743
piggybackers, 423
ping command, 499
connectivity, verifying, 502-504
pinned taskbar icons, launching from keyboard, 102-103
pinning
favorite destinations to jump list, 101-102
favorite programs
to Start menu, 92-93
to taskbar, 100-101
piping commands, 259
policies, 14
configuring, 185-186
filtering, 187-189
for passwords, 382-383
for user accounts, configuring, 389-390
UAC, 379-380
user rights policies, configuring, 391
POP, 742
Pop-up Blocker, 327
pop-up windows, blocking, 327-328
Popup method, 677
intType parameter options, 678-680
return values, 680-681
port forwarding, 602
ports, 600-601
adding as new Windows Firewall exception, 311-313
POST (power on self-test), 121
power button, 86-88
power cycling, 494
Power Options icon (Control Panel), 171
Power Users group, 361
PowerShell
cmdlet
aliases, 706-709
running, 709-713
cmdlets, 705
execution policy, configuring, 726
ISE, 726-727
objects, 714
assigning to a variable, 722
collections, 724-725
members, returning, 714-715
members, selecting, 715-717
methods, 724
properties, 723-724
output, formatting, 717-719
scripts, running, 728-729
sessions, starting, 704-705
***PowerShell Unleashed, Second Edition*, 704**
PPTP (Point-to-Point Tunneling Protocol), 606
pre-shared keys, 431
prefetcher, configuring, 123
presentation layer (TCP/IP stack), 743
preventing
IDN spoofing, 334-335
privilege escalation, 400-402
signal leakage, 428-430
Print Management icon (Control Panel), 168
printing, 563-565
Printing group (Internet Explorer, Advanced Tab), 43
privacy
Address Bar list, clearing, 320-322
browsing history, deleting, 316-319
cookies, managing, 322-325

InPrivate browsing, 325
InPrivate filtering, 326
Windows Media Player, options, 320
private-key encryption, 354
privileges, elevating, 375-376, 400-402
Problem Reporting, 452-455
Processes tab (Task Manager), 114
processor scheduling, adjusting, 124-125
program priority, setting in Task Manager, 125-126
programmatic identifiers, 672
programming, objects
methods, 667-668
properties, 666-667
programs
adding to Open With list, 62
keyboard shortcuts, 732
removing from Open With list, 61-62
Programs and Features icon (Control Panel), 171
programs. *See also* services
properties
of devices, viewing, 463
of objects
returning, 667
setting, 666
of PowerShell objects
returning value of, 723
setting value of, 723-724
protected mode (Internet Explorer), 331
protecting against
drive-by downloads, 345
email viruses, 341-345
phishing, 350-351
public key, obtaining, 355-356
public networks, 528
public-key encryption, 354
Punycode, 334

Q-R

Quit method, 671
QWORD, editing in Registry, 239

RADAR (Resource Exhaustion Detection and Resolution) tool, 450
RDP, 742
Read and Execute permission, 360
Read permission, 360
read receipts, blocking, 352
recalling commands, 254-255
receiving secure email messages, 356-357
recent programs, clearing from Start menu, 94
recovering forgotten passwords, 383-384
recovering with System Restore, 457-459
recovery disc, creating, 153
Recovery icon (Control Panel), 171
Recycle Bin, turning off delete confirmations, 13-15
redirecting
command input, 258
command output, 256-257
reducing
BIOS checks, 121
OS Choices menu timeout, 122
reg command, 289-291
RegDelete method, 686
Regional and Language Options icon (Control Panel), 171
Registry
.reg files
creating, 240-242
editing, 240
importing, 236
backing up, 234
binary values, editing, 239
default action, setting for file types, 49-50

DWORD, editing, 239
entries
changing, 237
finding, 244
group policies, 233-234
Group Policy Settings Reference, 182
hives, 231
supported files, 232-233
HKEY_CLASSES_ROOT key, 47-48
keys
creating, 243
deleting, 243
exporting to disk, 235-236
renaming, 243
Keys pane, 227
new action, setting for file types, 50-53
root keys, 227
HKEY_CLASSES_ROOT, 229-230
HKEY_CURRENT_CONFIG, 231
HKEY_CURRENT_USER, 230
HKEY_LOCAL_MACHINE, 230
HKEY_USERS, 231
securing, 233-235
settings
deleting with scripts, 686
reading with scripts, 685
storing with scripts, 686
ShellNew subkey, 58
string values, editing, 238
system hive, loading services, 224
Registry Editor
launching, 226
Settings pane, 228-229
slow services, killing, 222
RegRead method, 685
RegWrite method, 686
reinstalling drivers, 477
releasing DHCP lease, 501
rem command, 261
Remote App and Desktop Connections icon (Control Panel), 171
remote computers, 578
scripting, 700-702
Remote Desktop, 586-609
stored desktop credentials, removing, 418-420
Remote Desktop Users group, 361
remote desktops, 649-652
remote folders, 562
remote shutdowns, configuring, 84-86
removable drives, 559
removing
applications from Open With dialog box, 61-62
icons from Control Panel, 177-178
security zone sites, 329-330
shortcuts from Start menu, 97-98
stored desktop credentials, 418-420
wireless connections, 551
ren command, 281-282
renaming, 629
boot applications, 72
built-in accounts, 405-406
network connections, 531
wireless network connections, 548
renaming Registry keys, 243
renewing DHCP lease, 501
reordering wireless network connections, 548-549
replace command, 282-283
Replicator group, 361
reports, 121
resetting erratic services, 222-224
resolving IP address conflicts, 513
resource conflicts, troubleshooting, 479-480

resource exhaustion detection, 450
Resource Monitor, monitoring performance, 117
restarting, 629
shortcut, creating, 83-84
restore points
reverting to, 457-459
setting, 149-152
Restricted Sites, 329
restricting
computer usage with parental controls, 395-400
login times for users, 420-422
results pane, 197
custom taskpad view, creating, 203-205
resuming paused services, 210
return codes for StartService method, 216-217
return codes for StopService method, 216-217
returning
value of PowerShell object properties, 723
WMI class instances, 696-699
returning object members (PowerShell), 714-715
reversible encryption, 383
reviewing Event Viewer logs, 160-162
right pane (Group Policy Editor), 184
rolling back drivers, 478
root keys, 227
HKEY_CLASSES_ROOT, 229-230
HKEY_CURRENT_CONFIG, 231
HKEY_CURRENT_USER, 230
HKEY_LOCAL_MACHINE, 230
HKEY_USERS, 231
rotational latency, 127
route command, 499
routers
administrative passwords, specifying, 428
firmware, updating, 497-498
setup pages
accessing, 299
displaying, 424-427
routing
default gateway, 750
subnet masks, 748-750
RPC (Remote Procedure Call) protocol, 605
Run method, 681
running
commands, 251-252
Internet Explorer without add-ons, 336
PowerShell cmdlets, 709-713
PowerShell scripts, 728-729

S

Safe mode
troubleshooting, 485
when to use, 483
Safe mode with Command Prompt, when to use, 483
Safe mode with Networking, when to use, 483
Safe Senders, specifying in Windows Live Mail, 348
sample scripts, 693-694
saving consoles, 202-203
scanning email with Windows Defender, 345
scheduling Disk Defragmenter, 147-149
script jobs, creating, 661
scripting
Administrator account, running scripts from, 664, 680
examples
InternetExplorer object, 693-694
web pages, displaying, 691-692
web pages, navigating, 692
PowerShell

cmdlets, 705-713
collections, 724-725
execution policy, configuring, 726
ISE, 726-727
methods, 724
object instances, filtering, 719-720
object instances, sorting, 720-722
objects, 714-717, 723-724
objects, assigning to a variable, 722
output, formatting, 717-719
scripts, running, 728-729
services, controlling, 213-217
Windows Script Host, 658-659
CScript, 661-662
WScript, 660-661
WMI, 695
class instances, returning, 696-699
remote computers, scripting, 700-702
search engines, adding to Internet Explorer, 30-31
search queries
AQS, 22-23
Boolean operators, 24-25
operators, 23
natural language queries, 25-26
sectors, 137
security, 560, 577, 637
Administrator account, disabling, 307-308
BitLocker, enabling
on non-TPM systems, 369-371
on TPM systems, 369
crackers, thwarting, 298-300
computers, locking, 300-302
Ctrl+Alt+Delete, requiring at startup, 302
email, encrypting, 353-356
encrypting disks, 368
encrypting files, 366-367
file system, setting permissions, 360
group policies, 181
Group Policy Manager, device security policies, 472
hidden shares, disabling, 417-418
Internet Explorer
advanced options, 337-339
IDN spoofing, preventing, 334-335
Phishing Filter, 332-334
pop-up windows, blocking, 327-328
protected mode, 331
running without add-ons, 336
security zones, 328-331
SmartScreen Filter, 333-334
MAC address filtering, enabling, 436-438
on wireless networks, preventing signal leakage, 428-430
password-protected sharing, enabling, 410
passwords
policies, 382-383
recovering, 383-384
strengthening, 381
permissions
assigning, 363-364
configuring, 414-415
privilege escalation, preventing, 400-402
receiving secure email, 356-357
Registry, 233-235
reversible encryption, 383
sending secure email, 356
shared folders, hiding, 415-417
shared permissions, configuring, 411-414
Sharing Wizard, disabling, 410-411
snoops, thwarting, 298-300, 302
special permissions, assigning, 364-366
SSID
broadcasting, disabling on wireless networks, 432-433
default value, modifying, 435-436

TCI, 316
UAC, 374
configuring, 377, 379-380
elevating, 375-376
least-privileged user account, 375
password options, 381-382
privileges, 375-376
verifying operation, 307
user accounts
built-in, renaming, 405-406
disabling, 402-403
Guest account, 406-407
lockout policies, 391-392
managing, 384-386
policies, configuring, 389-390
restricting login times, 420-422
user names, hiding in logon screen, 403-405
user rights policies, configuring, 391
WEP, 516
Windows Defender
accessing, 304
settings, 306-307
spyware scanning, 305
Windows Defender, verifying operation, 303-305
Windows Firewall, verifying operation, 303
Windows Service Hardening, 368
wireless networks, WPA, 430-432
WPA, 516

Security group (Internet Explorer, Advanced Tab), 43

security groups, 360
assigning users to, 361-363

security zones, 328-329
security level, changing, 330-331
sites, adding/removing, 329-330

seek time, 127

segments (TCP), 756-757

selecting object members (PowerShell), 715-717

sending
email messages via CDO, 343-344
secure email messages, 356

sequencing TCP segments, 758

Server Too Busy error messages, 612

servers, 612-615, 637-639

services
automatic startup, configuring, 212
controlling at command prompt, 212-213
controlling with scripts, 213-215, 217
deleting, 223
dependent, 211
disabling, 212, 217-221
essential, 211
killing, 222
pausing, 210
resetting, 222-224
starting, 210
status of, changing, 210
stopping, 210

Services icon (Control Panel), 168

Services snap-in, loading, 209

session layer, 743

setting
restore points, 149-152
toolbar options, 109
value of PowerShell object properties, 723-724

settings for Windows Defender, 306-307

Settings pane (Registry Editor), 228-229

shareable memory, 118

shared folders, 585, 644-648
hiding, 415-417
security permissions, configuring, 414-415

shared network resources, 554-558, 563-570
shared permissions, configuring, 411-414
Sharing Wizard, disabling, 410-411
Shaw, Marco, 704
ShellNew subkey, 58
shortcuts, 52
adding/removing from Start menu, 97-98
creating in Windows Script Host, 682-685
extensions, hiding, 52
restarts, creating, 83-84
shutdown, creating, 84
Shut Down command, customizing, 86-87
SHUTDOWN command, 81
remote shutdowns, configuring, 85-86
restart shortcut, creating, 83-84
shutdown shortcut, creating, 84
shutting down slow services, 222
signal leakage, 428, 430
Signature Verification tool, 478
signed drivers, upgrading, 478
single-key encryption, 354
Size slider (Remote Desktop), 595
sleep button, customizing on notebooks, 87-88
sleeping computers, waking up with network connection, 539-541
slow services, killing, 222
SMART (Self-Monitoring, Analysis, and Reporting Technology), 450
smart modems, 513
SmartScreen Filter (Internet Explorer), 333-334, 350-351
SMB (Server Message Blocks), 642
smooth scrolling, 42
SMTP (Simple Message Transfer Protocol), 742
snap-ins, 197-199
adding, 200-202
controlling with group policies, 207
Local Users and Groups, 388-389
organizing, 201
Services, loading, 209
snoops, thwarting, 298-299
computers, locking, 300-302
Ctrl+Alt+Delete, requiring at startup, 302
sockets, 755-756
solutions to problems, checking for, 452-455
sort command, 258, 283-284
sorting PowerShell object instances, 720-722
Sound icon (Control Panel), 171
source of problems, isolating, 440-447
spam
blocking from specific countries, 349-350
junk email protection level, configuring Windows Live Mail, 347-348
senders, blocking, 349
thwarting, 345-346
Special Edition Using JavaScript (Que, 2001), 659
special permissions, 360
assigning, 364-366
specifying Safe Senders in Windows Live Mail, 348
splitting page file, 131
spoofing
homograph spoofing, 333
IDN spoofing, 333-335
spyware, 304-305
SSIDs
broadcasting, preventing on wireless networks, 432-433
default value, modifying, 435-436
Standby mode. *See* Sleep mode (Start menu), 539
Start menu
Control Panel, adding, 176-177
customizing, 90
default programs, configuring, 94-95

favorite programs
increasing displayed number of, 91-92
pinning to, 92-93
links, converting to menus, 96-97
modifying with Group Policies, 109-110
power button, customizing, 86-87
recent programs, clearing, 94
shortcuts, adding/removing, 97-98
starting
Check Disk GUI, 138-139
Command Prompt sessions, 246
Group Policy Editor, 183
MMC, 200
PowerShell sessions, 704-705
services, 210
Windows 7 with last known good configuration, 456
StartService method, return codes, 216-217
startup
BIOS checks, reducing, 121
customizing, 63-66
with Advanced Boot Options menu, 73-76
with BCDEDIT, 69-73
Debugging Mode, when to use, 484
Directory Services Restore Mode, when to use, 484
Disable Automatic Restart on System Failure option, when to use, 484
Disable Driver Signature Enforcement option, when to use, 485
Enable Boot Logging option, when to use, 483
Enable VGA Mode option, when to use, 484
Last Known Good Configuration, when to use, 484
OS Choices menu timeout, reducing, 122
Safe mode, 483
Safe mode with Command Prompt, 483
Safe mode with Networking, 483
splash screen, turning off, 122
System Configuration utility options, 488-490
troubleshooting, 481-482
static IP addressing, configuring, 534-537
status of services, changing, 210
stop errors, 442
stopping services, 210
StopService method, return codes, 216-217
stored desktop credentials, removing, 418-420
storing page file optimally, 131
strengthening passwords, 381
string values, editing in Registry, 238
strings, comparing in batch files, 267
strong passwords, creating, 381
subkeys
HKEY_CLASSES_ROOT key, 48
ShellNew, 58
subnet masks, 748-750
subst command, 253
suppressing web bugs, 352-353
Sync Center, 578
Sync Center icon (Control Panel), 171
synchronizing, 579-582
System Configuration icon (Control Panel), 168
System Configuration utility, 487
startup options, 488-490
system hive, copying services into, 224
System icon (Control Panel), 171
system image backup, creating, 157
System Information utility, troubleshooting error messages, 442
system management tools
reg, 289-291
systeminfo, 292-293
typeperf, 293-295
whoami, 295-296

system recovery disc, creating, 153
System Recovery Options, 485-487
System Restore, 457-459
Registry, backing up, 234
restore points, setting, 149-152, 458
system tray. *See* notification area
systeminfo command, 256-257, 292-293

T

tabbed browsing, 34-35
opening multiple home pages at startup, 35-37
Tablet PC Input Panel toolbar, 108
Tablet PC Settings icon (Control Panel), 171
Task Manager
Performance tab, 115
performance, monitoring, 114-117
Processes tab, 114
program priority, configuring, 125-126
Task Scheduler icon (Control Panel), 168
taskbar
customizing, 98-100
favorite programs, pinning to, 100-101
jump list, pinning destinations to, 101-102
modifying with Group Policies, 109-110
notification area, 103
customizing, 104
disabling, 105-106
pinned icons, launching from keyboard, 102-103
toolbars
creating, 109
displaying, 108
options, setting, 109
Taskbar and Start Menu icon (Control Panel), 171
taskpad view, customizing, 203-205
Tasks pane (Network Center), 518
TCI (Trustworthy Computing Initiative), 316
TCP (Transmission Control Protocol), 742, 755
features, 758
segments, 756-757
sockets, 755-756
TCP/IP, 742-743, 755
IP
datagrams, 743-745
DNS, 752-754
dynamic IP addressing, 751
IP addresses, 745-748
IP routing, 748-750
TCP
features, 758
segments, 756-757
sockets, 755-756
temporary access, granting with Guest account, 406-407
temporary Internet files, 316
text files, exporting device driver list to, 469-471
threads, 116
thwarting
crackers, 298-300
computers, locking, 300-302
Ctrl+Alt+Delete, requiring at startup, 302
snoops, 298-300
computers, locking, 300-302
Ctrl+Alt+Delete, requiring at startup, 302
spam, 345-346
Tiles view, Windows Explorer icons, 8
time, 579-581
TLD (top-level domain), 349
TLS (Transport Layer Security), 338

toolbars
creating, 109
displaying, 108
options, setting, 109
top-level domains, 753-754
TPM, enabling BitLocker, 369
TPM chip, verifying installation, 368
tracert command, 499, 504-505, 751
tracing packets with tracert, 504-505
transport layer, 743
tree panes, 197
troubleshooters, 448
Device Manager, 473-474
nonworking devices, displaying, 474-477
disk diagnostics, 449
Memory Diagnostics tool, 451-452
Problem Reporting, 452-455
RADAR, 450
troubleshooting, 582
BSOD, 444
cables, 506-507
device drivers, 477-478
error messages, 441
in Event Viewer, 441
in System Information utility, 442
from command-line, 499
ipconfig, 500-502
ping, 502-504
tracert, 504-505
last known good configuration, 456
NIC, 507
online resources, 455-456
resource conflicts, 479-480
Safe Mode, 485
source of problem, isolating, 440-447
startup, 481-482
Debugging Mode, when to use, 484
Directory Services Restore Mode, when to use, 484
Disable Automatic Restart on System Failure option, when to use, 484
Disable Driver Signature Enforcement option, when to use, 485
Enable Boot Logging option, when to use, 483
Enable VGA Mode option, when to use, 484
Last Known Good Configuration, when to use, 484
Safe mode with Command P rompt, when to use, 483
Safe mode with Networking, when to use, 483
Safe mode, when to use, 483
with System Configuration utility, 487-490
tips, 447-448
wireless networks, 508-509
Troubleshooting icon (Control Panel), 171
Trusted Sites, 328
TTL (Time-to-Live) value, 751
default value, changing, 505
turning off
delete confirmations, 13-15
startup splash screen, 122
turning on network discovery, 495-497
typeperf command, 293-295

U

UAC (User Account Control), 374
configuring, 377-379
least-privieleged user account, 375
limited users, 374
passwords, options, 381-382

policies, configuring, 379-380
privileges, elevating, 375-376
verifying operation, 307
unassociated applications, opening documents with, 59-60
UNC (Universal Naming Convention), 558
undo restore points, 458
uninstall restore points, 458
uninstalling devices, 471
unknown restore points, 458
unmounting, 648
unnecessary files, deleting, 143-145
unnecessary services, disabling, 217-221
unreliable protocols, 755
unsigned drivers
disabling, 478
ignoring, 466-469
updates
checking for, 158-160
for drivers, checking for, 465-466
updating
device drivers, 124, 466
router firmware, 497-498
upgrading
device drivers, 123
signed drivers, 478
UpNP routers, accessing setup pages, 426-427
user accounts, 567-570, 586
Administrator, 390
elevated Command Prompt sessions, 246-247
scripts, running, 664, 680
built-in, renaming, 405-406
disabling, 402-403
Guest account, 406-407
lockout policies, configuring, 391-392
logged in users, discovering, 407
managing, 384-386
net user command, 393-394
parental controls, 395-400
privilege escalation, preventing, 400-402
security policies, configuring, 389-390
user names, hiding in logon screen, 403-405
user rights policies, configuring, 391
User Accounts dialog box, 386-387
User Accounts icon (Control Panel), 171
user folders, moving, 19
user rights policies, configuring, 391
user-specific wireless connections, creating, 549-550
usernames, 560
users
assigning to security groups, 361, 363
permissions, assigning, 363-364
special permissions, assigning, 364-366
utilities, 499
attrib, 278-279
AUTOCHK, 139-140
chkdsk, 270-271
chkntfs, 271-274
defrag, 274-276
Disk Defragmenter, 146
disks, selecting, 148-149
schedule, changing, 147
find, 279-281
ipconfig, 500-502
ping, 502-504
System Configuration utility, 487
BCD, modifying, 66-68
startup options, 488-490
System Recovery Options, 485-487
System Restore, setting restore points, 149-152

tracert, 504-505
Windows Backup, configuring automatic file backups, 155-156

V

variables
assigning PowerShell objects to, 722
objects, assigning to, 668
***VBA for the 2007 Microsoft Office System* (Que, 2007), 659**
VBScript, 659
FileSystemObject object, 675-677
verifying
connectivity with ping command, 502-504
UAC operation, 307
Windows Defender operation, 303-305
settings, 306-307
spyware scanning, 305
Windows Firewall operation, 303
view options, customizing in Windows Explorer, 16-19
viewing, 554-556
computers on network, 523-524
device properties, 463
hidden shares, 417
network status, 525-527
nonpresent devices in Device Manager, 464
viewing contents of ARP cache, 502
views, Device Manager, 463
virtual directories (IIS), adding folders as, 626-627
virtual memory, 116
commit limit, 451
page file
size of, monitoring, 132
size, customizing, 131-134
splitting, 131
storing optimally, 131
viruses, protecting against, 341-345
VPN (Virtual Private Networks), 529, 605-609

W

waking up sleeping computers, 539-541
War Games (1983), 423
warchalking, 424
wardialing, 423
wardriving, 423
web bugs, suppressing, 352-353
web pages cache, controlling in Internet Explorer, 28-29
web servers, 612-615, 637-639
websites, 614—639
channels, 353
WEP (Wired Equivalent Privacy), 516, 430
whoami command, 295-296, 407
wildcards, AQS, 23
Win32 Service, 213
***Windows 7 and Vista Guide to Scripting, Automation, and Command Line Tools* (Que, 2009), 659**
Windows Backup, 154
automatic file backups, configuring, 155-156
Windows CardSpace icon (Control Panel, 171
Windows Defender
accessing, 304
configuring to scan email, 345
settings, 306-307
spyware scanning, 305
verifying operation, 303-305
Windows Defender icon (Control Panel), 172

Windows Explorer
file extensions, displaying, 11-13
folders, moving, 19
Full Control permissions, assigning to folders, 20, 22
full-screen mode, enabling, 15
icons
customizing, 8
Details view, 9-10
menu, displaying full-time, 8
view options, customizing, 16-19
Windows Firewall, 588, 601, 614-615
exception, creating, 309-310
managing, 308-309
ports, adding as new exception, 311-313
programs, adding as new exception, 310-311
verifying operation, 303
Windows Firewall icon (Control Panel), 172
Windows Firewall with Advanced Security icon (Control Panel), 168
Windows Live Mail
countries, blocking, 349-350
digital ID, obtaining, 354-355
email, encrypting, 353-356
junk email protection level, configuring, 347-348
Junk Filter, 345-346
public key, obtaining, 355-356
read receipts, blocking, 352
Safe Senders, specifying, 348
secure messages, receiving, 356-357
senders, blocking, 349
viruses, protecting against, 343-345
web bugs, suppressing, 352-353
Windows Logo Key, keyboard shortcuts, 739
Windows Media Player
keyboard shortcuts, 737
privacy options, 320
Windows Memory Diagnostic icon (Control Panel), 168
Windows Mobility Center icon (Control Panel), 172
Windows networks, 641-655
Windows Script Host, 658-659
CScript, 661-663
object
assigning to a variable, 668
methods, 667-668
properties, 666-667
objects, collections, 669
WScript, 660
parameters, 660-661
programming, 671-675
script properties, 663
shortcuts, creating, 682
WshNetwork object, 689-691
WshShell object, 677-681, 685-686
WshShortcut object, 683-685
Windows Security screen, bypassing, 114
Windows Service Hardening, 368
Windows shared folder, 644-648
Windows Update, 455
Windows Update icon (Control Panel), 172
Windows Update website, checking for updates, 158-160
Windows XP, 590-591
WINS (Windows Internet Name Service), 755
WinSAT (Windows System Assessment Tool), 112-114
wireless network connections, 542, 643-644
wireless networks
access points, signal leakage, 428-430
ad hoc, configuring, 543-545
connecting to, 514-515
default SSID value, changing, 435-436
hidden, connecting to, 434

hot spots, 515
MAC address filtering, enabling, 436-438
properties, configuring, 545-548
removing, 551
renaming, 548
reordering, 548-549
routers
administrative passwords, specifying, 428
setup pages, displaying, 424-427
SSID broadcasting, disabling, 432-433
troubleshooting, 508-509
user-specific, creating, 549-550
WPA, 430-432

WishNetwork object
network drives, mapping, 690-691
network printers, mapping, 689
properties, 689
referencing, 689

WMI (Windows Management Instrumentation), 695
class instances, returning, 696-699
remote computers, scripting, 700-702
services, controlling, 213-217

work networks, 528

workgroup name, configuring on peer-to-peer networks, 513

WPA (Wireless Protected Access), 430-431, 516
security properties, modifying on wireless networks, 431-432

write caching, enabling on hard drive, 128-129

Write permission, 360

WScript, 660
environment variables, 687-689

WScript
objects
CreateObject method, 672-674
Echo method, 671
GetObject method, 674-675
Quit method, 671
parameters, 660-661
script properties, 663
WshNetwork object
network drives, mapping, 690-691
network printers, mapping, 689
properties, 689
referencing, 689

WshShell object
Popup method, 677
intType parameter options, 678-680
return values, 680-681
RegDelete method, 686
RegRead method, 685
RegWrite method, 686
Run method, 681

WshShortcut object, 683-685

wwwroot folder (IIS default website), 618, 623

X-Y-Z

xcopy command, 284-288

XOR (Boolean Exclusive Or), 750

zones. *See* security zones