Microsoft

Troubleshooting Windows® 7 Inside Out

Mike Halsey

www.it-ebooks.info

Published with the authorization of Microsoft Corporation by:
O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, California 95472

Copyright © 2010 Mike Halsey.

Complying with all applicable copyright laws is the responsibility of the user. All rights reserved. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without express written permission of O'Reilly Media, Inc.

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 M 5 4 3 2 1 0

Microsoft Press titles may be purchased for educational, business or sales promotional use. Online editions are also available for most titles (*http://my.safaribooksonline.com*). For more information, contact our corporate/institutional sales department: (800) 998-9938 or *corporate@oreilly.com*. Visit our website at *microsoftpress.oreilly.com*. Send comments to *mspinput@microsoft.com*.

Microsoft, Microsoft Press, ActiveX, Excel, FrontPage, Internet Explorer, PowerPoint, SharePoint, Webdings, Windows, and Windows 7 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the author, O'Reilly Media, Inc., Microsoft Corporation, nor their respective resellers or distributors, will be held liable for any damages caused or alleged to be caused either directly or indirectly by such information.

Acquisitions and Development Editor: Kenyon Brown
Production Editor: Adam Zaremba
Editorial Production: Octal Publishing, Inc. and Custom Editorial Productions, Inc.
Technical Reviewer: Todd Meister
Indexing: Ginny Munroe
Cover: Karen Montgomery
Illustrator: Robert Romano

978-0-735-64520-2

www.it-ebooks.info

Contents at a Glance

Part 1: Prevention

Chapter 1
Prevention Is Better Than Cure 3

Chapter 2
The Basic Windows 7 Utilities 17

Chapter 3
Basic Windows 7 Security 35

Chapter 4
Backup and Restore 53

Chapter 5
Maintaining Windows 7 69

Chapter 6
Users 79

Chapter 7
Hardware 93

Chapter 8
Virtualization 103

Part 2: Quick Fixes

Chapter 9
Annoyances 121

Chapter 10
Viruses, Malware, and Other Threats 137

Chapter 11
Easy Ways to Fix Windows 7 163

Part 3: Technical Fixes

Chapter 12
What Is Windows 7 Anyway? 199

Chapter 13
Identifying the Source of a Problem 205

Chapter 14
Advanced Diagnostic Tools in Windows 7 . . . 217

Chapter 15
Advanced Repair Methods 231

Chapter 16
Windows Problems Demystified 257

Chapter 17
Remote Help 273

Chapter 18
Where to Find More Help and Support 289

Chapter 19
Diagnosing Hardware Problems 295

Part 4: Disaster Recovery

Chapter 20
Windows and Data Recovery Tools 313

Chapter 21
Restoring from Another PC 319

Chapter 22
Linux: An Operating System on a Disc 325

Chapter 23
Third-Party Rescue Tools and Services 337

Chapter 24
When You Can't Recover Data 347

Part 5: Power Utilities

Chapter 25
Advanced Windows Diagnostic Tools in Depth 369

Chapter 26
Windows Firewall in Depth 401

Chapter 27
Advanced Registry Work 413

www.it-ebooks.info

Part 6: Appendices

Appendix A
Windows 7 Editions 423

Appendix B
Windows 7 Features by Edition 425

Appendix C
Windows 7 Shortcut Keys 431

Appendix D
BIOS Beep Codes 439

Glossary 447

Index 455

www.it-ebooks.info

Table of Contents

Part 1: Prevention 1

Chapter 1: **Prevention Is Better Than Cure 3**

Upgrade or Clean Install? 4
How to Install Windows 7 to Prevent Problems 4
Keeping Your Installation of Windows XP or Windows Vista 6
How Big Should Partitions Be? 7
What To Do When Windows 7 Is Installed 7
Useful Windows 7 Settings to Change 8
MSConfig 11
Moving Your Files Away from Windows 12
Backing Up Windows 7 14
Summary 16

Chapter 2: **The Basic Windows 7 Utilities 17**

Action Center 17
Action Center Settings 19
What Can You Do with Action Center? 19
Windows Update 20
Controlling Windows Update Through Group Policy 22
Windows Firewall 23
Diagnose/Repair 26
Windows Defender 26
Windows 7 and Anti-Virus Software 27
Legacy Program Compatibility 28
The Program Compatibility Assistant 29
Windows XP Mode 31
Summary 33

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

www.it-ebooks.info

Chapter 3: **Basic Windows 7 Security** 35
The Reality of Virtualization 36
Windows vNext 37
Anti-Virus Software for Windows 7 38
Microsoft Security Essentials 38
Norton Internet Security/Norton 360 39
Malwarebytes Anti-Malware 39
Windows Defender 39
Microsoft Windows Malicious Software Removal Tool 39
User Account Control 40
BitLocker and BitLocker To Go 43
Method 1: Encrypting a Hard Disk or Partition with Hardware Support 43
Method 2: Encrypting a Hard Disk or Partition Without Hardware Support 43
Method 3: Encrypting a USB Flash Drive or External Hard Disk 43
Using BitLocker with Non-Windows 7 Computers 45
Why Use BitLocker? 47
Beware the Weak Link at the Keyboard 47
Keep Your Anti-Virus Software Up to Date 47
Make Sure You Have a Good, Up-to-Date Firewall 47
Get Anti-Spyware Software 48
Keep Windows Up to Date 48
Keep Your Software Up to Date 48
Always Check Email Attachments Before Opening Them 48
Use a Secure Internet Browser 48
Get Spam and Phishing Filtering for Your Email Software 48
Never Click Anything You Don't Explicitly Mean To 49
Look for the Padlock or the Green Bar 49
Never Give Private Details Online Unless You Have To 49
Keep Backups 49
Keep the Driver CDs and Manuals for Your PC 50
Keep Windows Maintained 50
Be Careful When You Throw Away Your PC 50
Guest Mode 50
Gibson Research 51
Summary 51

Chapter 4: **Backup and Restore** 53
Moving Your Files Away from Windows 7 53
The Disk Cleanup Wizard 53
Shrinking, Extending, and Creating Partitions 55
Moving the Shell User Folders 57
Using Backup and Restore 57
Backing Up Files and Data 57
Restoring Files and Data from a Backup 61
Third-Party Backup Solutions 62
Backing Up to the Cloud 62
Version Control 63

www.it-ebooks.info

Backing Up the Operating System 63
Restoring Windows from a Windows System Image 63
Restoring Windows 7 from a System Repair or Install Disc 64
Corporate Image Backups 65
Determining How Many Backups You Need and Where to Store Them 66
Summary 67

Chapter 5: **Maintaining Windows 7 . . . . . 69**

Defragmenting Your Hard Disks 69
Which Hard Disks and Partitions Do You Defragment? 71
Maintaining Windows 71
Disk Cleanup 71
Internet and Other Temporary Files 72
Third-Party Tools and Utilities 73
Don't Install Too Much Software 75
Keeping Windows 7 Updated 76
Keeping Auto-Running Software to a Minimum 76
The One Year Reinstall Rule 77
Summary 78

Chapter 6: **Users 79**

How Windows 7 Controls Users 79
Managing User Accounts 80
Setting an Administrator Password 81
What Is the Guest Account? 83
Parental Controls 84
What's Missing from Parental Controls? 87
Group Policies 87
Local Security Policies 88
Computer Management 89
Blocking CDs, DVDs, Flash Drives, and External Hard Disks 90
Summary 91

Chapter 7: **Hardware 93**

What's in a PC? 93
Motherboard 94
Processor 96
Memory 97
Expansion Cards and Riser Cards 97
Optical Drives and Hard Disks 97
Power Supply 98
The PC Case 98
How Can You Clean the Inside of Your PC? 98
Hardware Health 99
Desktops 99
Laptops 99
All-in-Ones 99

www.it-ebooks.info

SMART Monitoring of Hard Disks 100
Peripherals 100
Keyboards and Mice 100
Monitors 101
Other Devices 101
Surge Protectors, UPS, and Power Supply 102
Summary 102

Chapter 8: **Virtualization 103**

Virtualization vs. Dual Booting 104
Are There Any Benefits to Virtualization? 105
Virtual Hard Disks and Windows 7 105
Creating a VHD in Windows 7 105
Reattaching the VHD 110
Booting From a Virtual Copy of Windows 7 110
Windows Virtual PC and Windows XP Mode 115
Installing Another Operating System in Windows Virtual PC 116
Summary 118

Part 2: Quick Fixes 119

Chapter 9: **Annoyances 121**

Common Windows 7 Problems 121
You Don't Have Permission to Write Files to a Disk 121
You Can't See Your New Wi-Fi Network 125
Incorrect File Associations 125
Problematic Graphics, Sound, Keyboard, or Mouse Drivers 126
This Copy of Windows 7 Is Not Genuine 128
Windows Update Won't Install Anything 129
Search Isn't Finding Your Files 129
Service Pack or Update Install Was Interrupted 130
Windows Starts Up Very Slowly 131
Windows Shuts Down Very Slowly 132
Problems with Sleep 133
Hardware Annoyances 134
Windows Gets Stuck at Its Loading Screen 135
No Operating System Found 135
A New Monitor Results in No Picture 135
Your USB3 Device Doesn't Work 135
You've Installed a Fresh Copy of Windows 7 and Can't Get Online 135
Your Headphones or Microphone Won't Work 136
Summary 136

www.it-ebooks.info

Chapter 10: **Viruses, Malware, and Other Threats 137**

Repelling an Attack 137
Action Center 137
Anti-Virus Software 138
Anti-Malware Software 140
Identifying an Attack 144
Look for the Padlock 144
Do You Really Need Another Toolbar? 147
Do You Need that Extra Browser Plug-in or Download? 148
Malicious Websites 149
Malicious and Fake Anti-Malware Software 150
What Goes on the Internet, Might Stay There Forever 152
Repairing the Damage 153
Use Your Existing Anti-Malware Software 153
Try a Free Online Virus Scanner 153
McAfee Stinger 154
Safe Mode 155
Manually Removing a Virus Infection 157
Virus Removal Using Another PC 158
Restoring Windows 7 from a Backup 159
Viruses Corrupting the BIOS 159
Where Can Viruses Hide? 161
Summary 162

Chapter 11: **Easy Ways to Fix Windows 7 . . . . . 163**

Restore Previous Versions of Files 163
System Restore 166
Configuring System Restore 167
Restoring Windows 7 Using System Restore 168
Can I Undo System Restore Changes? 169
Troubleshooting Software Compatibility 170
Manually Setting Program Compatibility 170
The Automatic Program Compatibility Troubleshooter 172
Program Compatibility Notifications in Action Center 173
Windows XP Mode 175
Windows Won't Start 175
Last Known Good Configuration 176
Safe Mode 176
Windows Startup Repair 177
Startup Repair from an Install DVD or a System Repair Disc 178
You Did Back It Up, Didn't You? 179
Working with Device Drivers 180
Common Problems with Device Drivers 180
Graphics Driver Problems 181
Device Manager 182
Installing Device Drivers 187
Removing and Reinstalling Device Drivers 190

www.it-ebooks.info

Updating Device Drivers 192
Rolling Back Device Drivers 193
Action Center Troubleshooter 194
Microsoft Fix It Center 195
Summary 195

Part 3: Technical Fixes 197

Chapter 12: **What Is Windows 7 Anyway? 199**
The Windows 7 File and Folder Structure 199
How Does Windows Compare to Other Operating Systems? 202
Summary 203

Chapter 13: **Identifying the Source of a Problem 205**
Taking a Step-by-Step Approach 205
Minimum Windows Configuration 206
Safe Mode 208
Unplug Your Hardware 209
Why Problems Occur with Windows 211
Keep Things Simple 211
What Are the Causes of Common Problems? 213
The Domino Effect 213
Have You Tried Turning It Off and On Again? 214
The Blue Screen of Death 214
The Perpetual Restart 215
Summary 216

Chapter 14: **Advanced Diagnostic Tools in Windows 7 . . . . . 217**
Performance Information and Tools 217
Event Log 219
How to Read the Event Log 221
Performance Monitor 222
Resource Monitor 223
Windows Task Manager 224
System Information 224
System Health Report 226
Computer Management 227
Using the Windows 7 Performance Tools 229
Take Time to Step Back 230
Summary 230

www.it-ebooks.info

Chapter 15: **Advanced Repair Methods 231**

Repairing Microsoft Internet Explorer 231
Disable Your Add-Ons 231
How to Factory Reset Internet Explorer 235
Can You Reinstall Internet Explorer? 237
Updating Internet Explorer via Windows Update 238
Alternatives to Internet Explorer 238
System File Checker 239
Using MSConfig for Diagnostic Startups 241
Managing Windows Services 244
Working with the Windows Registry 246
Removing the Registry Settings for an Uninstalled Program 248
Using the System Repair Disc for Advanced Restore 249
BootRec.exe 251
Windows Memory Diagnostic 253
Using Safe Mode 254
Summary 255

Chapter 16: **Windows Problems Demystified 257**

Windows 7 Core Operating System Files 257
Windows 7 Security and Policy Folders 260
The Windows 7 Registry 260
Personalization Folders 261
Windows 7 Logs 261
Temporary Files Stores 262
Advanced File Restore 262
System File Checker 263
Creating a Slipstreamed Install DVD 263
What You Will Need 264
Step 1: Creating a Windows Pre-Installation Environment Startup Disc 264
Step 2: Installing a Fresh Copy of Windows 7 267
Step 3: Creating a New Windows Image File 270
Step 4: Creating a New Windows 7 Installation DVD 270
Third-Party Slipstreaming Software 272
Summary 272

Chapter 17: **Remote Help 273**

Using the Internet to Find Solutions to Problems 273
Where Else to Get Help 274
Windows Remote Desktop 278
Windows Remote Assistance 281
Problem Steps Recorder 285
Summary 288

www.it-ebooks.info

Chapter 18: **Where to Find More Help and Support 289**
Windows Help 289
Third-Party Software 289
Sisoftware Sandra Utilities 289
Windows Sysinternals 290
Zinstall zPOD 290
GoToAssist 290
SpinRite 291
Windows Memory Diagnostic 291
Norton Ghost 291
Acronis True Image 291
Paragon Partition Manager 291
Acronis Disk Director Suite 292
Third-Party Websites 292
Tom's Hardware 292
Tech PC Forums 292
Computing.net 292
How-To Geek 292
Annoyances.org 293
Gibson Research 293
ATI Support 293
nVidia Support 293
MSDN Diagnostics 293
Within Windows 293
The Long Climb 294
Summary 294

Chapter 19: **Diagnosing Hardware Problems 295**
PC Hardware Guide 295
Desktop PC Case 295
Power Supply 295
Motherboard 296
Processor 297
Memory 298
Hard Disk 298
Optical Drive 300
Graphics Card 300
Expansion Card(s) 301
Fans 301
Keyboards and Mice 301
Laptops, Netbooks, and All-in-One PCs 301
Safe Working 304
Is Everything Plugged In? 305
Minimal Hardware Boot 306
Resetting the BIOS 307
Jump-Starting Your PC 309
Summary 310

www.it-ebooks.info

Part 4: Disaster Recovery 311

Chapter 20: **Windows and Data Recovery Tools 313**

You Did Back It Up, Didn't You?! 313
Restoring Windows and Data from a Backup 313
Data Restore Through Over-the-Top Reinstall 315
RAID Drives 318
Summary 318

Chapter 21: **Restoring from Another PC 319**

Restoring a Windows Image on Another PC 319
zPOD 320
Restoring Windows File by File 320
Restoring Your Data by Using Another PC 321
Summary 324

Chapter 22: **Linux: An Operating System on a Disc 325**

System or Data Restore Using Another Operating System 325
Useful Software in Linux 330
Remote Desktop 330
System Monitor 331
System Testing 332
CD and DVD Burning in Linux 333
Compatible Linux Operating Systems to Run from a Disc 334
Ubuntu 334
Other Variants of Linux 335
Creating a Linux Installation Disc or Pen Drive 335
Summary 336

Chapter 23: **Third-Party Rescue Tools and Services 337**

Zinstall and zPOD 337
GRC SpinRite 341
Other Third-Party Tools 344
O&O Disk Recovery 344
Ashampoo WinOptimizer 344
Other Third-Party Services 344
Summary 345

Chapter 24: **When You Can't Recover Data 347**

Encrypted File System 347
Setting Up EFS 348
Restoring an EFS Key 352
Turning EFS Off 354
EFS Certificates 354
Smart Cards and EFS Certificates 356
File Encryption Certificate Manager 359

www.it-ebooks.info

Recovering EFS-Encrypted Files . . . 359
Cipher.exe . . . 360
BitLocker and BitLocker To Go . . . 361
Creating a Copy of Encrypted Data . . . 364
Summary . . . 365

Part 5: Power Utilities . . . 367

Chapter 25: **Advanced Windows Diagnostic Tools in Depth . . . 369**

Computer Management . . . 369
System Tools . . . 370
Storage . . . 378
Services and Applications . . . 378
Performance Information and Tools . . . 380
Visual Effects . . . 380
Indexing Options . . . 383
Power Settings . . . 383
Disk Cleanup . . . 385
Advanced Tools . . . 385
Control Panel Troubleshooters . . . 398
Summary . . . 400

Chapter 26: **Windows Firewall in Depth . . . 401**

Windows Firewall . . . 401
Windows Firewall with Advanced Security . . . 403
Managing Firewall Rules . . . 405
Adding New Inbound or Outbound Firewall Rules . . . 406
Setting a Connection Security Rule . . . 410
Monitoring . . . 410
Port Control for Routers . . . 411
Summary . . . 412

Chapter 27: **Advanced Registry Work . . . 413**

Registry Sections . . . 414
HKEY_CLASSES_ROOT . . . 414
HKEY_CURRENT_USER . . . 414
HKEY_LOCAL_MACHINE . . . 414
HKEY_USERS . . . 414
HKEY_CURRENT_CONFIG . . . 414
Registry Keys and Settings . . . 415
Backing Up and Restoring the Registry . . . 416
Working with the Registry . . . 416
Editing, Deleting, or Adding Registry Keys . . . 417
Backing Up Specific Registry Keys . . . 418
Finding Information in the Windows Registry . . . 419
Summary . . . 419

www.it-ebooks.info

Part 6: Appendices 421

Appendix A: **Windows 7 Editions 423**

Appendix B: **Windows 7 Features by Edition 425**

Appendix C: **Windows 7 Shortcut Keys 431**

Appendix D: **BIOS Beep Codes 439**

Glossary 447

Index 455

www.it-ebooks.info

www.it-ebooks.info

Acknowledgments

I would like to thank the following people without whom this book would have not been possible, or at least very difficult, or perhaps a little bit of a problem, or that who helped in some intangible way that might be better explained later.

Everton Blair
Martin Brinkmann
Kenyon Brown
Duncan Buchanan
Mary Cholerton
Fran Gilbane
Richard Gilbane
Vipin Goyal
Larry Hall
Phil 'Fileas' Smith
Megan Smith-Creed
Darren Webber
Jake Webster
Rory Webster
Michael Weir
Adam Zaremba

And, most of all, my dog Jed.

www.it-ebooks.info

www.it-ebooks.info

Conventions and Features Used in This Book

This book uses special text and design conventions to make it easer for you to find the information you need.

Text Conventions

Convention	Feature
Abbreviated menu commands	For your convenience, this book uses abbreviated menu commands. For example, "Choose Tools, Forms, Design A Form" means that you should click the Tools menu, point to Forms, and select the Design A Form command.
Boldface type	Boldface type is used to indicate text that you enter or type.
Initial Capital Letters	The first letters of the names of menus, dialog boxes, dialog box elements, and commands are capitalized. Example: The Save As dialog box.
Italicized type	Italicized type is used to indicate new terms.
Plus sign (+) in text	Keyboard shortcuts are indicated by a plus sign (+) separating two key names. For example, Shift+F9 means that you press the Shift and F9 keys at the same time.

Design Conventions

Note

Notes offer additional information related to the task being discussed.

Cross-references point you to other locations in the book that offer additional information on the topic being discussed.

CAUTION!

Cautions identify potential problems that you should look out for when you're completing a task, or problems that you must address before you can complete a task.

www.it-ebooks.info

INSIDE OUT

This statement illustrates an example of an "Inside Out" problem statement

These are the book's signature tips. In these tips, you'll get the straight scoop on what's going on with the software—inside information on why a feature works the way it does. You'll also find handy workarounds to different software problems.

TROUBLESHOOTING

This statement illustrates an example of a "Troubleshooting" problem statement

Look for these sidebars to find solutions to common problems you might encounter. Troubleshooting sidebars appear next to related information in the chapters. You can also use the Troubleshooting Topics index at the back of the book to look up problems by topic.

Sidebar

The sidebars sprinkled throughout these chapters provide ancillary information on the topic being discussed. Go to sidebars to learn more about the technology or a feature.

www.it-ebooks.info

Errata & Book Support

We've made every effort to ensure the accuracy of this book and its companion content. If you do find an error, please report it on our Microsoft Press site at Oreilly.com:

1. Go to *http://microsoftpress.oreilly.com*.
2. In the Search box, enter the book's ISBN or title.
3. Select your book from the search results .
4. On your book's catalog page, under the cover image, you'll see a list of links.
5. Click **View/Submit Errata.**

You'll find additional information and services for your book on its catalog page. If you need additional support, please e-mail Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

We Want to Hear from You

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://www.microsoft.com/learning/booksurvey

The survey is short, and we read *every one* of your comments and ideas. Thanks in advance for your input!

Stay in Touch

Let's keep the conversation going! We're on Twitter:

http://twitter.com/MicrosoftPress

www.it-ebooks.info

www.it-ebooks.info

Introduction

Despite Microsoft founder Bill Gates' early desire to have "a computer on every desk and in every home," the PC has never been and is still not a consumer electronics device. We use them at work because the flexibility and power they offer as productivity tools offsets the expense of maintaining IT support departments, and we use them in the home because they are, at least for the moment, the best way of getting online.

This will change in the coming years, especially in the home space, as devices such as game consoles and tablets become cheaper and integrate better functionality. In both home and work spaces, things have already changed drastically since the early days of computing. Back then, you usually needed to understand programming in order to be able to use a PC.

There were also huge issues with supporting those early machines. The operating systems and software were custom made, with each program, for instance, coming with its own set of hardware drivers, and with technologies such as external communications ports sometimes requiring expert knowledge to configure.

Modern operating systems take almost all of the pain out of configuring and working with your computer, and Windows 7 is an excellent example. It is more stable, configurable, and reliable than any version of Windows that has come before it.

Things can and still do go wrong, however, and the more complex the machine, the more difficult it can be to diagnose the problem. That's where this book comes in.

Whether you're working in a support department in a corporate business, providing support to smaller clients, or just using Windows 7 at home, this book will guide you through the process of diagnosing and repairing the types of problems you can encounter with Windows 7, and discuss what you can do to prevent more problems from occurring.

www.it-ebooks.info

www.it-ebooks.info

PART 1

Prevention

CHAPTER 1
Prevention Is Better Than Cure 3

CHAPTER 2
The Basic Windows 7 Utilities 17

CHAPTER 3
Basic Windows 7 Security. 35

CHAPTER 4
Backup and Restore. 53

CHAPTER 5
Maintaining Windows 7 69

CHAPTER 6
Users 79

CHAPTER 7
Hardware 93

CHAPTER 8
Virtualization 103

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 1

Prevention Is Better Than Cure

Upgrade or Clean Install? 4
Keeping Your Installation of Windows XP or Windows Vista 6
How Big Should Partitions Be? 7
What To Do When Windows 7 Is Installed 7
Moving Your Files Away from Windows 12
Backing Up Windows 7 14
Summary 16

It's always a good idea to prevent problems before they occur, but knowing where to start can be a problem. When you first install **Windows 7**, you encounter a blank **desktop** with just a few items visible on the new **taskbar** and in the Start menu. You may be tempted to get working straight away, and you can do this if you like. However, Windows 7 comes with a great many tools that you can use to help prevent problems from occurring and to make sure that when problems do occur, you can be back up and running quickly. I recommend spending the time to configure your system and software after you first install Windows. Then back up this initial configuration to quickly restore later should you need to.

INSIDE OUT

Why spend time configuring and backing up Windows?

Windows 7 constantly makes small changes and adjustments to its files and settings as you work. The more you do, the more changes Windows makes. After a period of time, these changes can cause software or Windows components to misbehave or malfunction, and they can become extremely difficult to undo. If you back up your copy of Windows 7 after the changes are entrenched, you preserve potential problems.

The benefit of taking time to back up a clean, unused Windows 7 installation is that when something goes wrong, your backup will be an exact copy of a fully working Windows 7 setup, including all of your software and settings. There will be no need to reinstall everything one piece at a time. Plus, you only need to make the initial backup once.

www.it-ebooks.info

Upgrade or Clean Install?

The minor settings changes described in the previous section are a good reason to install a clean version of Windows 7 rather than upgrading your PC in place from Windows Vista to Windows 7. (The Windows 7 install DVD doesn't support in-place upgrading from **Windows XP**). Although it may be convenient to install Windows 7 over your current operating system, keeping all of your programs and settings intact, any problems that exist on the previous Windows installation can carry forward to the new one. Most IT professionals recommend that you always format your **hard disk** and reinstall Windows 7 on a clean drive or **partition**, unless you've lost **software** installation media or you really don't have the time to spend on a clean install.

How to Install Windows 7 to Prevent Problems

Your hard disk is one big area where you can store Windows, programs, files, data, and **backup**s. But it's not a good idea to keep all of your data in the same place without making a backup and storing it elsewhere. For instance, if you leave a DVD copy of your **digital** music and photo libraries next to your PC, it could be stolen or destroyed in a fire, along with your PC where the original files are stored. The sensible option is to give your backup **DVD** to a friend or family member to keep it safe. Almost all businesses keep a backup of their data somewhere separate from the originals, because data is the critical part of a computer. **Hardware** is easy to replace, but it's impossible to replace last year's holiday photos, it's difficult to re-enter all of your customer data, and it's annoying to re-**download** all the music and video you've bought.

Although you can fix many Windows 7 problems with no loss of data, some problems require you to restore the **operating system** from a backup or reinstall it completely. Restoring and reinstalling usually require you to wipe the hard disk. What's more, there's no way to know if and when a disaster will occur. If your files, photos, and music are stored on the same hard disk or partition as Windows 7, you could lose them forever.

INSIDE OUT Hard disks and partitions

Think of a hard disk as one big plate for all the food at a party buffet. No matter how careful you are in laying out the food, it will always end up mixed together; and if somebody spills the garlic mayonnaise, it'll go over everything.

www.it-ebooks.info

What you really need are different plates to separate the food. If you use one long plate that's split into several compartments, you can put a different food in each space, safe in the knowledge that these compartments will help keep the garlic mayonnaise off the chocolate profiteroles.

It's a similar story with computer hard disks. You can split your hard disk into partitions, one for Windows 7, a second for your files and data, and a third for backups, including a backup of your Windows 7 installation. Splitting them between partitions keeps them apart for safety.



A normal hard disk



A partitioned hard disk, split into three "logical" drives

If you have a desktop PC and access to two or more hard disks, it's even better if you can split your Windows installation, files, and backups across them. This means that if you have a real catastrophe, such as the physical disk containing your Windows installation failing, you don't lose your backup copy of Windows, too. You can also use two hard disks to keep identical copies of your files and data, again just in case a physical disk fails.

Laptops and most PC systems include only one physical disk, however, so you won't have the option of splitting your data across different physical drives. You may instead want to purchase a separate **USB** external hard drive.

When you install Windows 7, you can choose the Custom Install option and repartition your hard disk using the tools available in the Windows 7 installer to delete the current single-drive partition and create new partitions. Once you have done this, select the partition onto which you want to install Windows 7 and press Next (see Figure 1-1).

www.it-ebooks.info

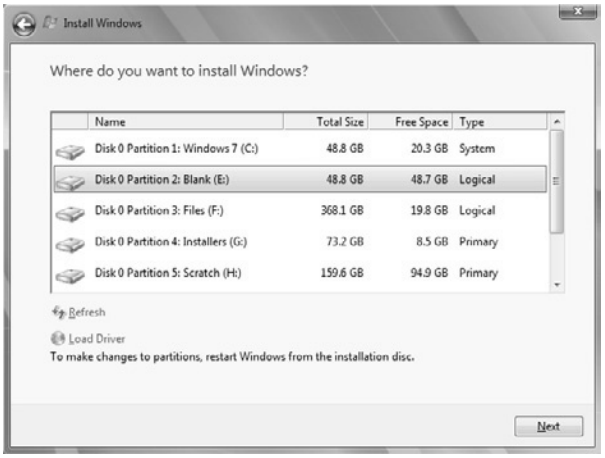


Figure 1-1 Creating and choosing a hard disk and partition for Windows 7 during setup

Keeping Your Installation of Windows XP or Windows Vista

If you really *must* keep your Windows XP or Windows Vista installation, you have two options. First, if you have a spare partition or hard disk large enough to accommodate Windows 7 on your computer, you could install Windows 7 there and create a **dual-boot** system where you can choose at startup which operating system you want to run.

However, many people find this setup clunky and want to be able to use both systems simultaneously. Certain software, such as Zinstall, can help. This software will turn your previous operating system into a virtual machine that will run in a window on your Windows 7 desktop. You need a large hard disk or partition for this since you will essentially have two operating systems installed.

> **Note**
>
> **You can get Zinstall at *www.zinstall.com*.**

www.it-ebooks.info

How Big Should Partitions Be?

The size of your hard disk and how you intend to use your computer will determine how big you should make your partitions. Your backup partition should be the same size as your Windows 7 partition if you only want to keep a backup copy of Windows 7 on it. It should be bigger if you also want to keep files and software installers there.

Use Table 1-1 as a guide to how large your Windows 7 partition should be. Please note these figures are a guide only. If you use development software (web, programming, or design), you might find you will need more space for your programs.

Table 1-1 Recommended partition sizes for Windows 7 in different uses

PC Usage	Windows 7 partition size
General Business	30 **GB**, Enter 30000 in the partition size box
General Home	30 GB, Enter 30000 in the partition size box
Power User	50 GB, Enter 50000 in the partition size box
Developer	100 GB, Enter 100000 in the partition size box
Gaming	100 GB, Enter 100000 in the partition size box

Note: Suggested numbers for entering into Windows are approximate sizes and not exactly the same partition size in GB.

What To Do When Windows 7 Is Installed

After Windows 7 is installed, you should install your other software and configure the system to your preferences. I suggest following the following guide.

- Install **anti-virus** and **malware** protection first. Even though you're just loading and configuring your computer, any software you install could be infected with a **virus** or **Trojan**.
- Install only software you will definitely use regularly. Skip loading software you will use only rarely or might not use at all; when you are ready to use it, you may find it's been upgraded anyway.
- Try to avoid installing shareware or trial version software. While amateur software authors do write some excellent software, it rarely goes through the same quality control procedures as commercial packages. **Shareware** and similar software can cause problems on a PC.

www.it-ebooks.info

- Update all the installed software to get any upgrades. This is especially important for Adobe Acrobat Reader because **PDF** files are often used to hide viruses.
- Activate your software and enter required product keys to keep the software from becoming crippled if you need to restore it from a backup.

For a new installation of Windows 7, I recommend a series of steps.

- Run **Windows Update** to make sure you have the latest updates to the operating system. Do this several times, restarting the PC after each update to make sure your computer is fully up to date. You can access Windows Update from the Start menu.
- Make sure Windows 7 is activated. If you don't activate Windows 7, it might become inoperable if you eventually restore from a backup. To activate Windows 7 from **Control Panel**, click System And Security, then click System. The option to activate Windows 7 is at the bottom of the window.
- Modify Windows 7 settings to your preferences (regional settings, for example). Read the following section for details about how to do this.

CAUTION!

It's important you don't do too much regular work while getting Windows 7 ready to create a system image backup. Avoiding regular work helps make sure nothing can go wrong during this important period.

Useful Windows 7 Settings to Change

By default, Windows 7 is efficient to set up and needs fewer options customized than previous versions of Windows, although there are a small few options that, if changed, will make for a happier experience using the operating system. You can access these settings by pressing Start on the taskbar or on your keyboard and selecting Control Panel from the Start menu.

In Control Panel, click the first option, System And Security, and a list of options appears as shown in Figure 1-2.

www.it-ebooks.info



Figure 1-2 The System and Security panel in the Windows 7 Control Panel

Windows 7 uses a space on your hard disk called **virtual memory** to help better manage the computer's physical **memory** and to load programs quickly. By default, Windows manages the size of the virtual memory file (also known as the paging file), but this means it can grow and shrink and cause problems that ultimately slow down access to the files and data on the hard disk.

To change the virtual memory size follow these steps.

1. In the Control Panel, click System And Security, and then click System. A new list of options appears.
2. Click Advanced System Settings in the blue panel on the left side of the window.
3. In the System Properties dialog box, click the Advanced tab.
4. In the Performance section, click Settings as shown in Figure 1-3.

www.it-ebooks.info

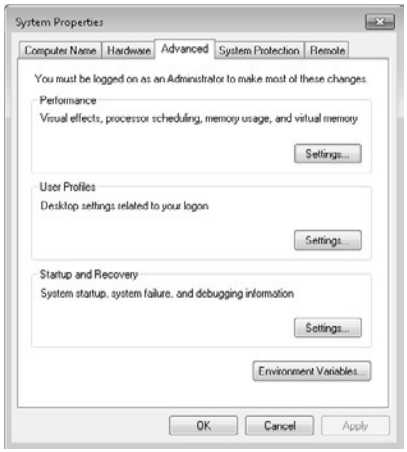


Figure 1-3 The Advanced tab in the System Properties dialog box in Control Panel

You can change the virtual memory settings in the Virtual Memory dialog box as shown in Figure 1-4.



Figure 1-4 Setting the virtual memory paging file size

Clearing the Automatically Manage Paging File Size For All Drives option and selecting the Custom Size option tells Windows to keep this paging file the same size all the time. This can help keep access to your files fast.

The recommended amount of disk space is displayed toward the bottom of the Virtual Memory dialog box (1534 **MB** in the example in Figure 1-4). Enter the recommended paging file size for your computer in both the Initial Size (MB) box and Maximum Size (MB) box, click Set, and then click OK to close the dialog box.

www.it-ebooks.info

In Control Panel, you can also change regional and language settings and get access to Device Manager to check that the drivers for all of your hardware are installed (see Figure 1-5).



Figure 1-5 Settings to adjust in Control Panel, including regional settings

MSConfig

One of the most useful hidden features in Windows 7, and indeed in every version of Windows, is **MSConfig** (see Figure 1-6). To access MSConfig, click Start on the taskbar or on your keyboard. Key **msconfig** in the Start menu search box, and press Enter on your keyboard. When the MSConfig window appears, click the Startup tab. On this tab, you will see a list of all the programs that start automatically when Windows 7 starts up. You can clear all the programs you don't want to run every time you use your PC. These could include the iTunes Updater or the Adobe Acrobat Loader.

The advantage of minimizing the number of programs that run automatically at startup is that the more software your computer is running at one time, the slower it will become and the longer it will take to start up.

www.it-ebooks.info

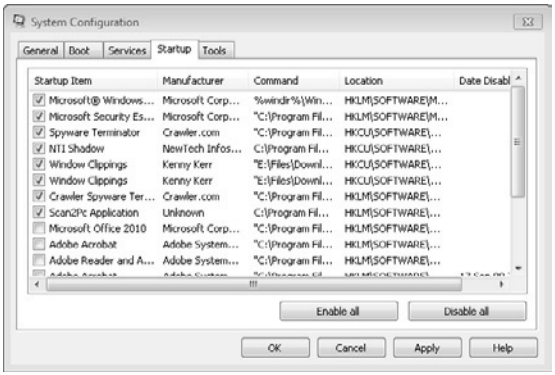


Figure 1-6 Stopping third-party programs from running at startup using MSConfig

> **Note**
>
> **You can resize the columns in the MSConfig window (and in many other parts of Windows) by dragging the vertical line between the columns.**

Moving Your Files Away from Windows

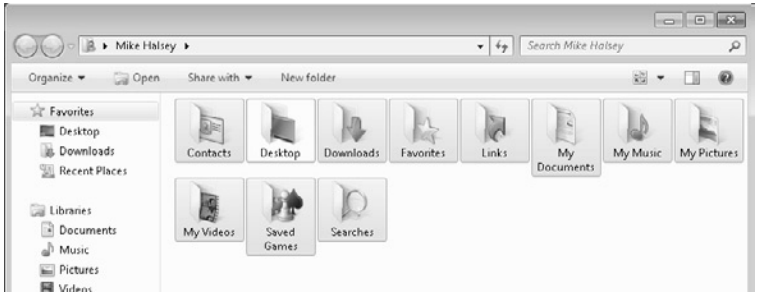
By default, every version of Windows stores your My Documents folder(s) on the same hard disk or partition as the Windows installation. Windows developers recognize, however, that it's useful and important to keep Windows and your files separate, and they have finally made this easy to do in Windows 7 with four simple steps.

1. On the Start menu, click your name in the top right.



www.it-ebooks.info

2. In the explorer window that appears, select all the folders (except Desktop, which should not be moved since doing so can cause problems with the operating system).



3. Right-click in the window and select Cut.

CAUTION!

Be sure to select Cut and not Copy in step 3, because Copy will not move the files; it will simply duplicate them.

4. Navigate to the drive or folder where you want to relocate the files (for example, E:\Files), right-click in an empty space in that window, and select Paste.

All of your files and documents are moved to the new location.

INSIDE OUT

Why move your files away from Windows 7?

Although Windows 7 is a very stable operating system, your PC is still not a consumer electronic device. Windows could become corrupt with little or no notice. If you must reinstall Windows at some point, you could lose all of your files and data if they are stored on the same drive or partition where you originally put the operating system. That's why it is important to separate your data and Windows on your PC.

www.it-ebooks.info

Backing Up Windows 7

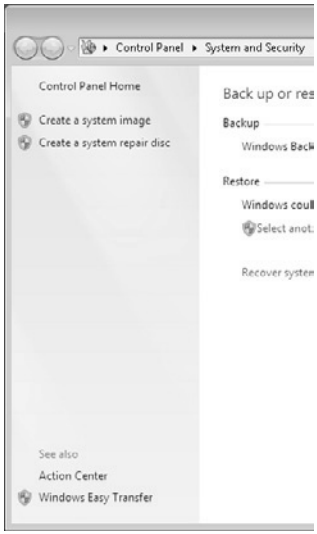
When you finish loading and configuring Windows 7, you are ready to create a backup and lock it down by creating an image of the operating system. When you create a backup, you essentially create a snapshot of all the Windows files and settings on your computer. Do not run programs while preparing to back up Windows 7 since this could create unreported errors in the backup file.

1. In the Start menu search box, type **Backup**.
2. Select Backup And Restore from the list of search results that appear.

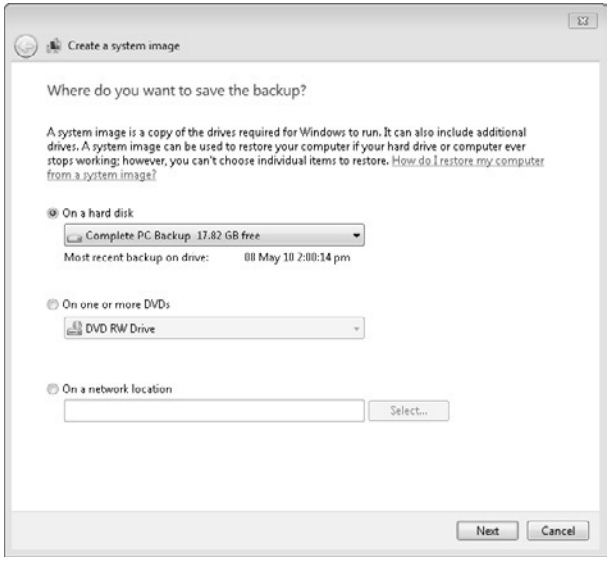


3. In the Control Panel Backup and Restore window that appears, select Create A System Image from the blue panel on the left side of the window.

www.it-ebooks.info



4. In the Create A System Image dialog box, select a location for the backup. You can choose to save the backup to another hard disk or partition on your computer, on a selection of DVDs (note that if you have a lot of software or games installed on your computer, you will need quite a few DVDs), or to a **network** location.



5. Click Next to start the backup

www.it-ebooks.info

INSIDE OUT Network backup precautions

Don't back up your operating system to a network location if your PC connects to the network only via Wi-Fi, because you will be unable to see the backup if you need to restore it. Only do a network backup if you connect via a physical network cable.

Windows 7 is now backed up. If Windows 7 becomes unresponsive, you can restore this backup and get working again quickly. You'll learn more about restoring Windows 7 in Chapter 11, "Easy Ways to Fix Windows 7."

Summary

It's very important to make sure that you have a working copy of Windows 7 backed up somewhere accessible. You never know when and under what circumstances Windows 7 might become unusable or malfunction. Following the steps described in the chapter can ensure that you're never far from being up and running when you need to be.

www.it-ebooks.info

CHAPTER 2

The Basic Windows 7 Utilities

Action Center 17
Windows Update 20
Windows Firewall 23
Windows Defender 26
Windows 7 and Anti-Virus Software 27
Legacy Program Compatibility 28
Summary 33

WINDOWS 7 ships with more easily accessible help and diagnostic utilities than any previous version of Windows, but the **wizard**-based utilities that were popular in the 1990s are gone. Windows 7 developers aimed to create a diagnostic system that doesn't require the user to move through a lot of steps to fix problems. They wanted things to be as simple and automatic as possible. The result of their efforts is a compromise between old diagnostic systems that maintain compatibility with older Windows versions and new features that provide help and advice to users.

Action Center

Action Center is a new Windows 7 feature designed in response to complaints from users of previous Windows versions that the notification area, the area next to the clock on the far right of the taskbar, can easily become cluttered with program **icons** and pop-up balloon tips. Action Center integrates all of these balloon tips into a more manageable centralized location (see Figure 2-1).

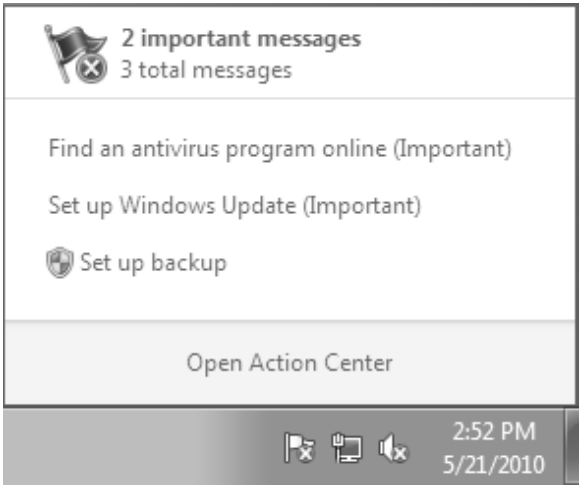


Figure 2-1 Action Center notification

www.it-ebooks.info

Action Center is represented by a small, white flag on the taskbar. The icon includes a small *x* when there are Windows messages in the Action Center. Although it is more subtle than the balloon tips in previous versions of Windows, the discreet Action Center icon can make important messages from Windows easy to miss. When providing technical support, I frequently discover that people have out-of-date anti-virus protection or that they have not installed vital software updates on their PCs because they've either not noticed the flag or not realized what it means.

You can control what messages the Action Center displays and respond to messages by clicking the Action Center icon and clicking Open Action Center.

The main Action Center panel includes a list of color-coded Windows messages, as shown in Figure 2-2. Red messages are critical, and amber messages are important.

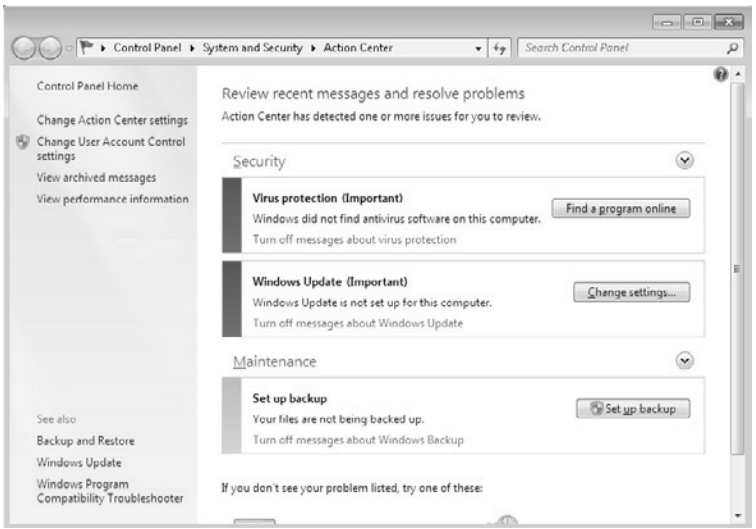


Figure 2-2 Color-coded messages in Action Center

When things go wrong with Windows 7, such as when a program or a driver crashes, the operating system stores information about these errors in a log and displays the log in Action Center. If there are any error logs in Action Center, you will see a Check For Solutions option under Maintenance. Click this option to search for a matching error log and, hopefully, a solution in Microsoft's database. You can also use the Maintenance section to change the Backup Settings and Troubleshooting Settings. It's possible in a corporate environment that the IT department will turn off these settings, perhaps to conserve **Internet bandwidth** or because of their own update management policy.

www.it-ebooks.info

Action Center Settings

To control what messages appear in Action Center, click Change Action Center Settings in the blue pane on the left of the Action Center panel. On the window that appears, indicate which items you want Windows to notify you about when there are problems (see Figure 2-3).

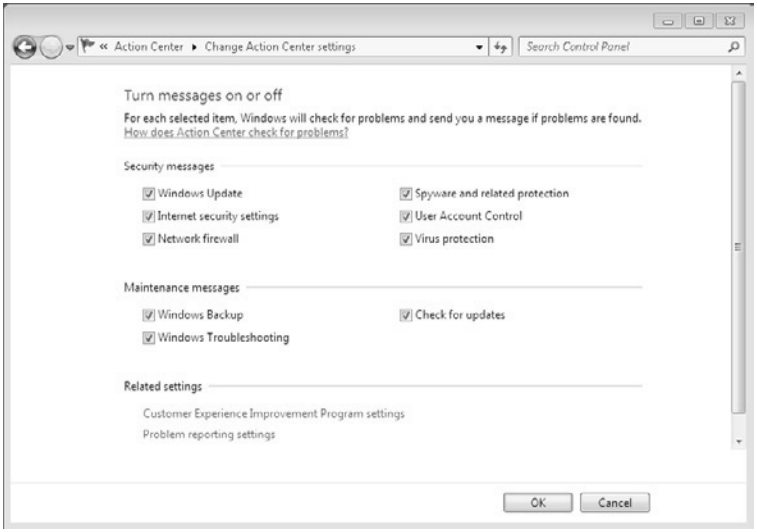


Figure 2-3 Turning notifications on and off in Action Center

What Can You Do with Action Center?

Action Center should be your first resource when diagnosing problems with Windows 7, because it is not only the central place for diagnostic and maintenance messages from the operating system, it is also a centralized place from which you can control essential Windows 7 features, such as the User Account Control security system and Network Access Protection.

You can also view archived Action Center messages from the main Action Center panel. Problems that have occurred with Windows 7 in the past can give you clues to a solution for a current problem.

In Action Center, you can also view the operating system's reliability history by clicking View Reliability History in the Maintenance section. As I said earlier, Windows 7 tracks problems caused by software, drivers and Windows components and represents this information in a chart (see Figure 2-4).

www.it-ebooks.info

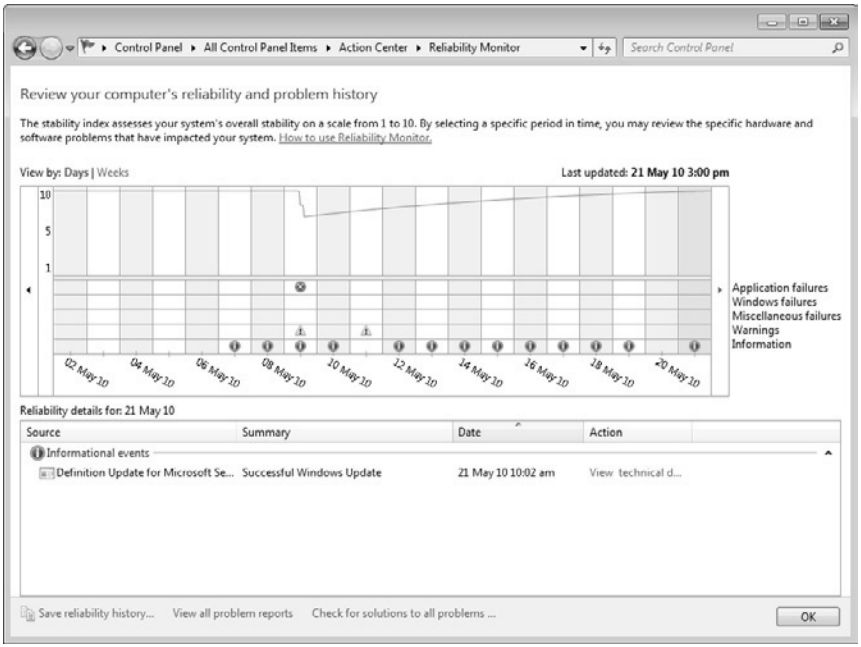


Figure 2-4 The Windows 7 Reliability History window

The chart in Figure 2-4 shows that this copy of Windows was installed on May 2, 2010, and ran perfectly until May 9, 2010, when, as indicated by an *x* and a yellow warning triangle, it encountered a problem. You can click the warning icons to review details about the problems that occurred. Next to each problem, if you need it, is a link to automatically check for a solution to the problem.

Windows Update

By the time the first service pack launches for a Windows operating system, there can be 80 or more security and software updates included in it. These updates address issues related to:

- virus and malware attacks
- hacking attacks
- other security vulnerabilities
- Windows Product Key cracks
- faults found in Windows
- incompatibilities with third-party and other Microsoft software

www.it-ebooks.info

- updates for programs and features in Windows 7
- updated drivers for hardware
- updates for other Microsoft software supported by Windows Update
- legacy code updates

Most updates address security vulnerabilities and legacy code. Around four billion people worldwide use Windows, so it's a huge target for **hackers** and criminals. They regularly exploit software, such as Microsoft **Internet Explorer**.

Legacy code updates, the other largest contributor to service packs, cover vulnerabilities that date back to previous versions of Windows and problems caused by maintaining compatibility with them. For instance, not long after Windows 7 launched, Microsoft released an update for a twenty-year-old DOS vulnerability that nobody had spotted before.

For a stand-alone PC or for a computer on a small, unmanaged network, I recommend turning on automatic Windows updates, as shown in Figure 2-5. This can help prevent problems on your computer by automatically updating Windows components as updates become available.

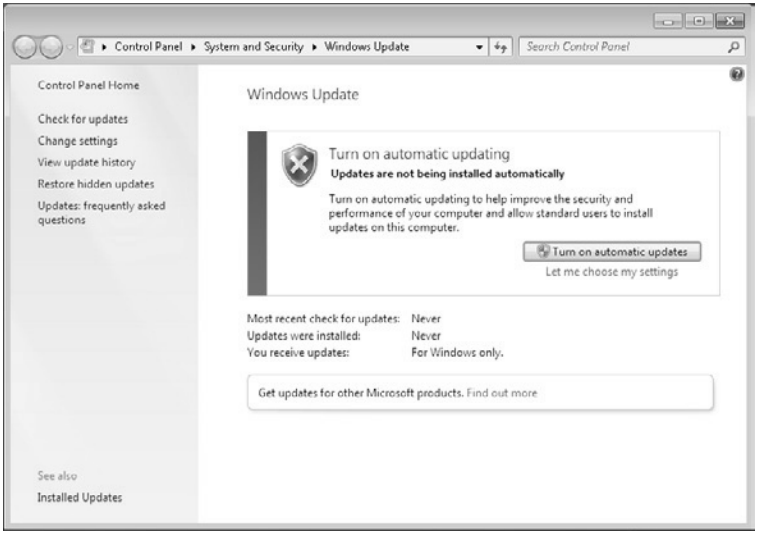


Figure 2-5 Windows Update

You can access Windows Update by selecting Action Center or looking in the System and Security section of Control Panel. You can also open Windows Update by clicking All Programs on the Start menu.

www.it-ebooks.info

Controlling Windows Update Through Group Policy

Windows Update sometimes causes problems, especially with older, legacy hardware or software where an update introduces an incompatibility, preventing older software or hardware from working properly or making Windows 7 unstable when software runs.

In the corporate environment or on a small Windows Server network with multiple users, you can disable the Windows Update service and instead use Windows Server features to download and test all updates before they are rolled out across the network.

To help you disable the Windows Update service, every version of Windows comes with a utility called **Group Policy** Editor. To access Group Policy Editor, type **GPEdit.msc** (not case-sensitive) in the Start menu search box and press Enter. The Local Group Policy Editor window appears as shown in Figure 2-6.

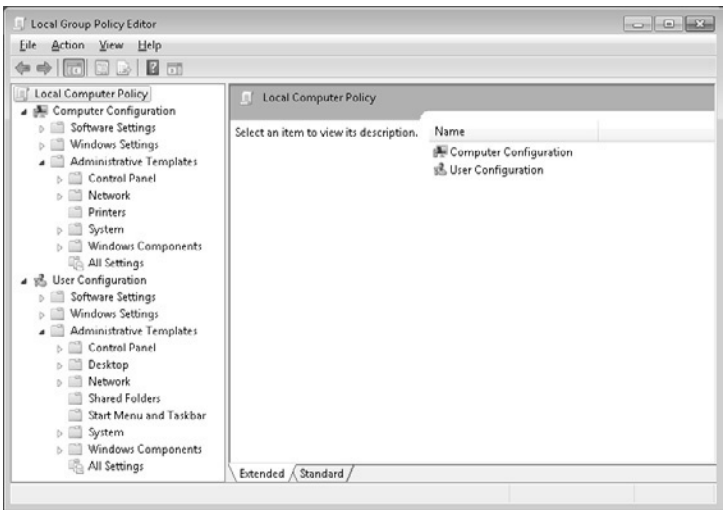


Figure 2-6 The Local Group Policy Editor window

Group Policy Editor allows you to independently control policies for the computer and for individual users. This is important because you want to grant systems **administrators** full control of the PC but limit access by other users.

www.it-ebooks.info

To control Windows Update and set the policy for all users, in Group Policy Editor click Computer Configuration, click Administrative Templates, click Windows Components, and then click Windows Update (see Figure 2-7). In this window, you can configure Windows Update to stop receiving automatic updates or to receive updates only from your company's server, among various other options that are available for controlling Windows Update.

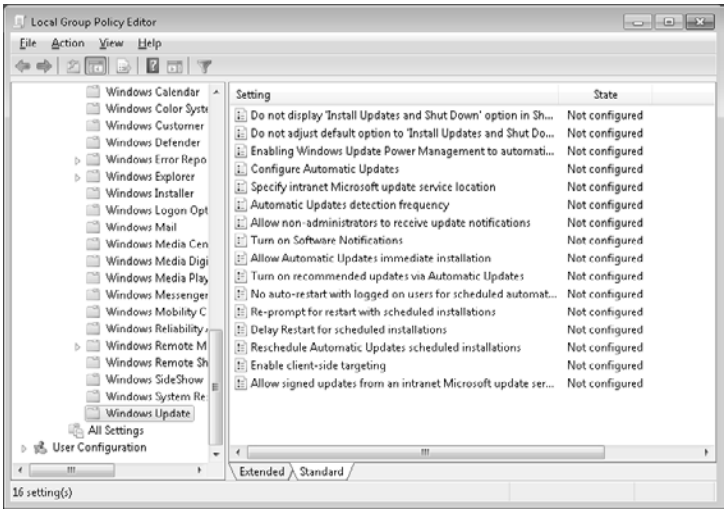


Figure 2-7 Windows Update settings in Group Policy Editor

Windows Firewall

Many people prefer to use a third-party **firewall** with Windows. Third-party firewalls can offer more features and more protection than the standard Windows firewall, but they can also be quite intrusive and complicated to use. For advanced PC users, or for people who are always careful about what they click and open when browsing the Internet, the standard firewall that comes with Windows 7 is perfectly adequate.

Windows Firewall, shown in Figure 2-8, is a two-way firewall that will block incoming and outgoing traffic, unlike the inbound-only block included in Windows XP. I recommend that you always have a firewall turned on, whether it's Windows Firewall or a third-party product. This is an essential security requirement that can prevent many types of problems and attacks on your PC.

www.it-ebooks.info

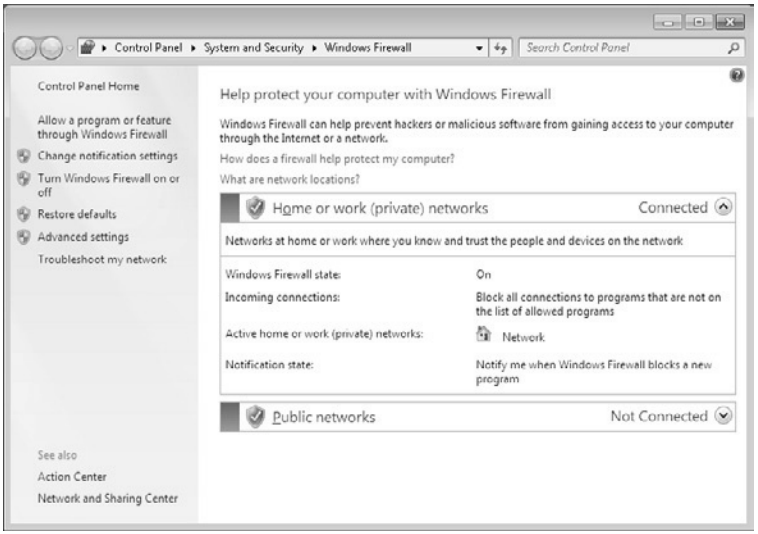


Figure 2-8 Windows Firewall

By default, Windows Firewall settings provide adequate protection for most situations; however, more advanced controls might be necessary in certain environments, such as in a home where people play Internet games or share files, or in an office where Windows Firewall could block access to a network or fileshare.

To correct some Windows issues, especially network connection problems where a program or service cannot communicate with the outside world or your network, you might need to set more appropriate permissions for the program or service.

To change these permissions, you will need to access the advanced settings. Click Advanced Settings in the blue pane of the Windows Firewall main window. The Windows Firewall With Advanced Security window opens with a whole array of options for controlling your firewall and access to and from your PC (see Figure 2-9).

INSIDE OUT Basic Windows Firewall control

Windows Firewall alerts you when a program wants to be allowed through the firewall.

If you accidentally give permission to a program and later want to deny it access through your firewall, you can do this on the main Windows Firewall options panel by clicking Allow A Program Or Feature Through Windows Firewall. A list of programs that have firewall access appears. Clear the check boxes for the programs and features you want to block.

www.it-ebooks.info

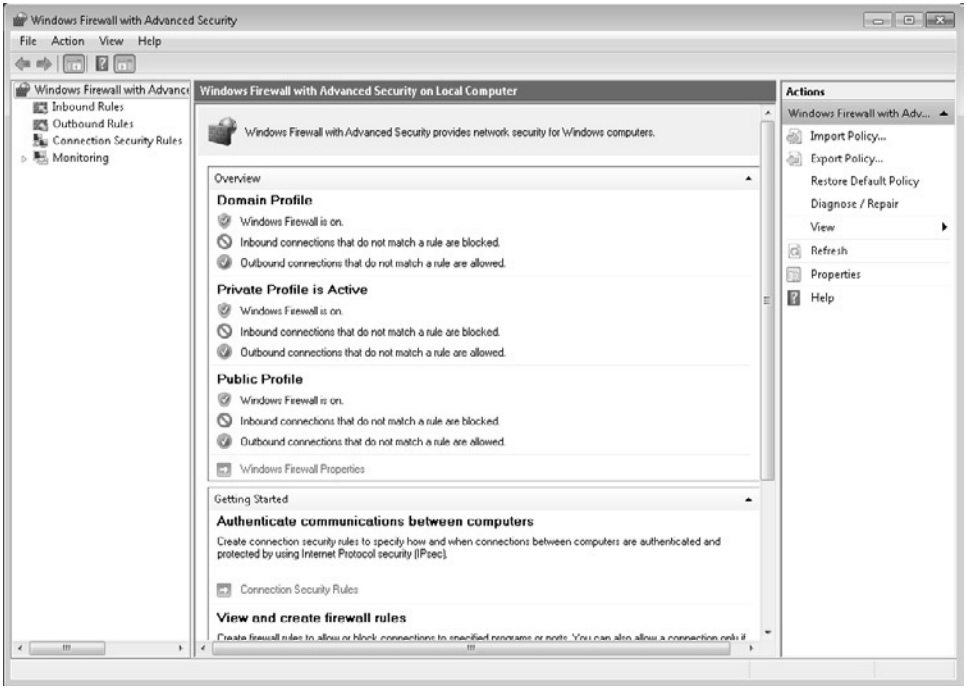


Figure 2-9 The Windows Firewall With Advanced Security window

The advanced firewall controls let you access and set inbound and outbound rules (see Figure 2-10). You can do this by selecting Inbound Rules or Outbound Rules from the left panel and clicking the New Rule link that will then appear in the right panel. The most common rules control access by a program or opening a port. Rules for opening a port would most commonly be used in one of the following circumstances.

- Connecting to a VPN (Virtual Private Network) in a company
- Sharing files across a network
- Allowing a gaming utility (such as PunkBuster) access to the Internet

www.it-ebooks.info

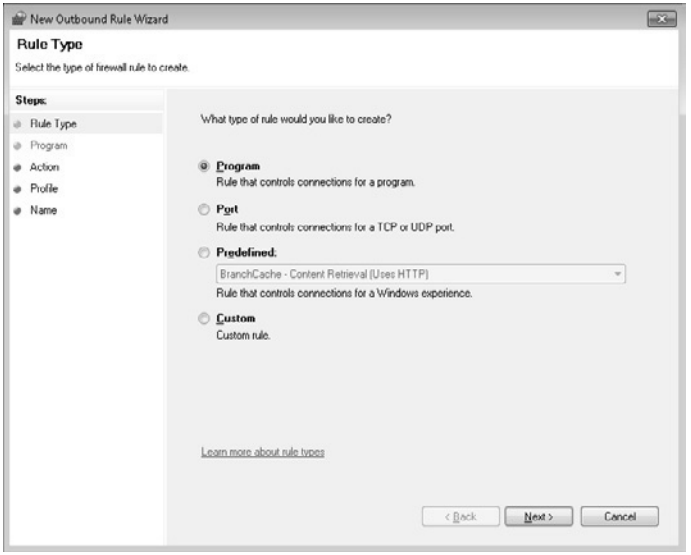


Figure 2-10 Setting new rules in Windows Firewall

Diagnose/Repair

A useful advanced firewall properties tool is the Diagnose/Repair feature in the Actions pane on the Windows Firewall With Advanced Security window (shown in Figure 2-9). This feature automatically troubleshoots, diagnoses, and repairs common problems with connections to networks and the Internet. However, Diagnose/Repair finds and fixes only basic, well-known errors, usually by restoring the appropriate settings to their defaults.

Windows Defender

Although Windows 7 does not come bundled with anti-virus software, it does include Windows Defender, an anti-**spyware** and anti-malware product, as shown in Figure 2-11. Windows Defender will protect your computer against some malware, but it's not enough on its own to defend your PC. I recommend installing a second anti-malware package, such as MalwareBytes' Anti-Malware or Spyware Terminator.

Windows Defender needs to be updated regularly, like all anti-virus and anti-malware products, and you can do this through Windows Update. Accordingly, you should make sure that Windows Update is set to download updates automatically.

www.it-ebooks.info

Some anti-malware products included with anti-virus packages turn off the Windows Defender service. You should not worry too much about this; it's only anti-virus software that can do this, not malware. You can turn Windows Defender back on, but doing so could cause a conflict with your other anti-malware package.

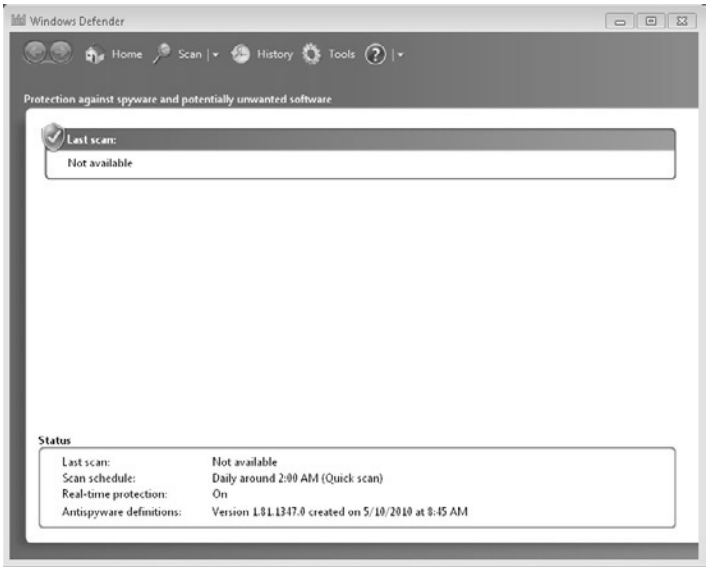


Figure 2-11 Windows Defender

Windows 7 and Anti-Virus Software

As mentioned earlier, Windows 7 does not include anti-virus software, so you need to add an independent anti-virus package when you install the operating system on your computer. Unfortunately, many users do not know this and do not notice the Action Center notification that indicates anti-virus software is missing. Thus, some people unknowingly operate PCs with no anti-virus protection at all.

For users who do notice and click the Action Center notification when Windows is first installed, the operating system helpfully lists anti-virus packages to download and install (see Figure 2-12). Note, you need to be connected to the Internet to see this list.

www.it-ebooks.info

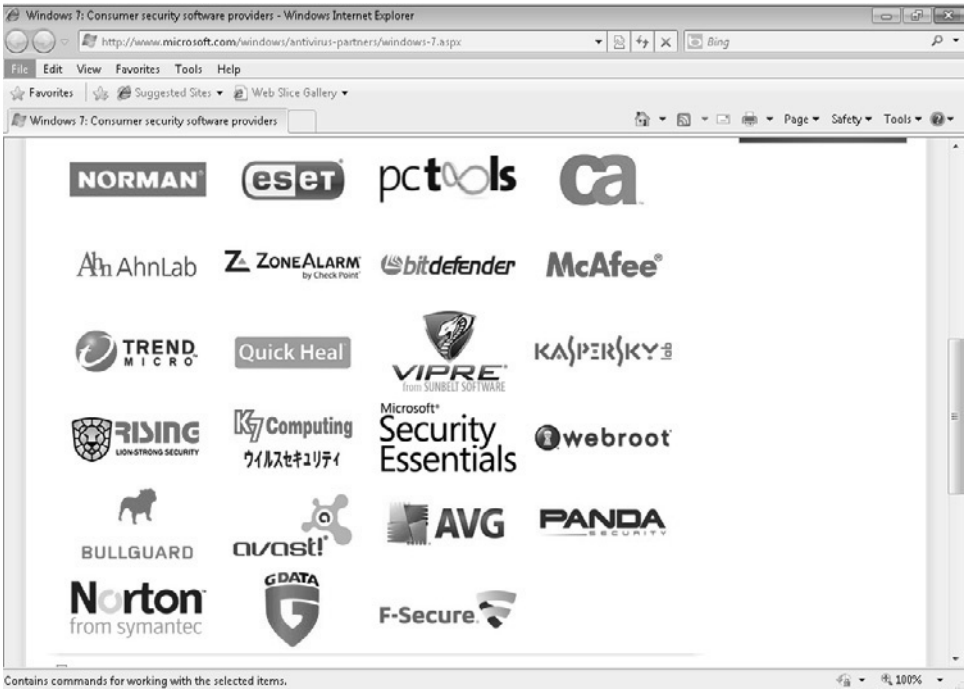


Figure 2-12 Windows 7 will help you find anti-virus software.

These packages range in price and vary in quality. Some are free and others are quite expensive (although many allow you to install the software on several PCs and include other features, such as firewall protection and backup utilities).

My recommendation for anti-virus software includes the following.

- **Microsoft Security Essentials** A lightweight anti-virus and anti-malware package that won't consume your computer's resources and includes an excellent scanning engine (Free)
- **Norton Internet Security/Norton 360** Another excellent scanning engine complete with firewall, malware protection, and other services (Paid-for suite)

Legacy Program Compatibility

One of the biggest strengths of Windows throughout the years, something that has enabled it to maintain market dominance over other desktop operating systems, has also been one of its biggest failings: compatibility with older programs. Windows 7 is capable of

www.it-ebooks.info

running programs designed for every version of Windows and some programs designed for DOS, too. That doesn't mean that everything will install and work correctly, or even install and work at all. There are several ways to get around problems caused by incompatible software.

The Program Compatibility Assistant

Windows 7 is extremely good at detecting software that won't install or run properly and has a new feature designed to help, called the Program Compatibility Assistant (see Figure 2-13).

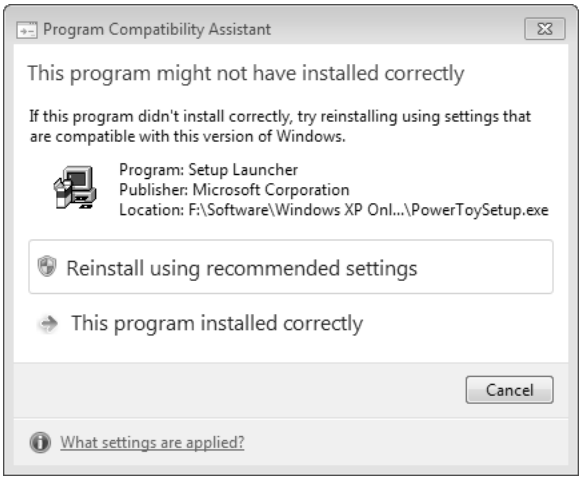


Figure 2-13 The Program Compatibility Assistant

If there is a compatibility problem with software you are installing, Windows 7 displays the Program Compatibility Assistant, as shown in Figure 2-13. It will offer some safe settings to try to install the program correctly.

The Program Compatibility Assistant is a good start, but it's not a solution for every software incompatibility you will encounter, and it's also not guaranteed to set settings and parameters correctly for every program it claims to have fixed. To do this manually, you can modify the program's compatibility settings yourself.

First, right-click the program's icon on the Start menu and select Properties. On the Compatibility tab, under **Compatibility Mode**, you can indicate what version of Windows the program ran on previously. In compatibility mode, Windows 7 runs the program using settings from the previous version of Windows you indicate. The drop-down menu includes every version of Windows dating back to Windows 95 (see Figure 2-14).

www.it-ebooks.info



Figure 2-14 Program compatibility settings

The Settings options might help programs that do not display properly on **32-bit** color screens or at large resolutions.

You can also choose to run the program with full administrator settings. Be careful when choosing this setting. See the Inside Out sidebar, "Administrator mode."

INSIDE OUT Administrator mode

The default user account in every version of Windows before Windows Vista is 'Administrator.' In administrator mode, absolutely everything in Windows can be changed, moved, or deleted with impunity, and viruses take advantage of this. User Account Control (UAC), introduced with Windows Vista, adds a layer of security to prevent these changes from being made automatically, but it can stop some programs from running correctly.

Some programs require access to root Windows files and areas that UAC protects. If a program can't write files to these parts of Windows, the software can become unresponsive. You should be careful giving administrator rights to any program, especially one you do not know well, because bypassing the essential UAC security feature can potentially cause damage. Some older programs, however, must have administrator permissions to operate properly.

www.it-ebooks.info

When troubleshooting program compatibility in Windows 7, you might need to try several different compatibility settings before a program runs properly.

Windows XP Mode

For programs that won't run, or won't run properly in compatibility mode, there's a new Windows 7 feature called Windows **XP Mode**.

Windows XP Mode is a downloadable extra that uses a modified version of Microsoft's free Windows Virtual PC software to run a free, licensed copy of Windows XP Professional in Windows 7.

Originally only for PCs with hardware **virtualization** support on the **processor** and **motherboard**, the Windows XP Mode add-in is now available for all Windows 7 users, although it will run quicker and more efficiently if your PC has hardware virtualization support.

The main advantage of Windows XP Mode is that, although the programs are running on a virtual machine, they appear on the Windows 7 Start menu (see Figure 2-15) and run on the Windows 7 desktop as though they were installed in Windows 7 (see Figure 2-16).



Figure 2-15 Windows XP Mode and its installed programs on the Start menu

www.it-ebooks.info

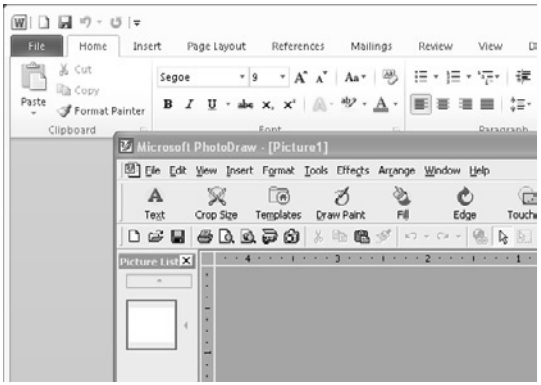


Figure 2-16 Windows XP programs on the Windows 7 desktop

Windows XP Mode offers tremendous advantages, particularly in organizations where users might be unfamiliar with the concept of running software in a virtualized environment or in a dual-boot operating system environment.

Windows XP Mode is capable of seeing all the drives and hardware on a computer and network, so you can use it seamlessly with your existing files and hardware, for instance, USB devices such as **flash drives**.

INSIDE OUT Windows XP Mode and security

Windows XP Mode is a full copy of Windows XP Professional running in its own virtual environment inside Windows 7. Like any version of Windows, however, it is not a consumer electronics device and must be protected and defended in the usual way.

You should always make sure that the Windows XP Mode environment is up to date with Windows Update and is protected by anti-virus and anti-malware software. I recommend a free, lightweight option, such as Microsoft Security Essentials.

Failure to protect your virtualized system could result in a virus or malware infection within the virtual machine that could infect files across your computer or network.

To run programs in Windows XP Mode, launch Windows XP Mode from the Start menu, and install the programs in Windows XP in the usual way. The programs will automatically appear in the Windows 7 Start menu, listed under Windows Virtual PC, Windows XP Mode **Applications**.

www.it-ebooks.info

Because Windows XP Mode is a full copy of Windows XP Professional, you will need to make sure that there is enough space to install Windows XP and any other programs you intend to install in it on the hard disk or partition where Windows 7 is already installed.

> **Note**
>
> **Windows XP Mode is available as a free download at *http://www.microsoft.com/windows/virtual-pc/download.aspx*.**

Summary

The standard utilities in Windows 7 are the most useful of all the comparable utilities that have ever shipped with Windows. As you become more confident troubleshooting Windows 7, however, you might find them limiting. In later chapters, I'll describe much more powerful features that are included with these utilities and how to get the full benefit from using them.

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 3

Basic Windows 7 Security

The Reality of Virtualization 36
Anti-Virus Software for Windows 7 38
User Account Control 40
BitLocker and BitLocker To Go 43
Beware the Weak Link at the Keyboard 47
Guest Mode 50
Gibson Research 51
Summary 51

Microsoft Windows, in its various guises, is used by approximately four billion people worldwide. Currently, Microsoft Internet Explorer, the standard **web browser** that's bundled with Windows, sits at 60 percent market share; that means almost 2.5 billion people worldwide use Internet Explorer.

Both of these facts make Windows and Internet Explorer tempting targets for criminals, hackers, and virus writers. Frankly, security problems in Windows have nothing to do with how secure or insecure it is and everything to do with criminals wanting to hit as many computers as possible in a single attack. Why go for attacks on another web **browser** or another operating system when you can hit a theoretical maximum of only 80 million people? It's a simple return on investment calculation for the criminal gangs who target computers.

All this isn't to say that there aren't problems with the security of Windows 7. Ironically, what makes Microsoft so successful in the operating system market is also the source of most Windows security problems: legacy code.

Legacy code is the substructure of Windows that allows you to continue to use hardware and software from the earlier days of PC computing when you update your operating system. If you run a DOS application, such as WordStar, from the heady days of the IBM PC, it will run fine and very speedily on a modern, Windows-based computer. If you want to plug in an old **parallel** printer and have the appropriate interface on your base unit, you can get it all working fine.

The need for legacy support is to service Microsoft's biggest customer, business. Many large corporations and businesses that collectively pay billions of dollars in subscription royalties every year to Microsoft commonly use software packages that were written many years ago.

The reasons businesses don't update software regularly are many and varied but stem from two simple principles: 1) It's expensive to develop customized software, and 2) if it isn't broken, don't fix it.

www.it-ebooks.info

At one point in my career, I provided second and third-line information and communications technology (ICT) support for blue-chip corporate clients, including a major international banking group. Every single client used custom-made software, even my employer, who used it for call processing and audit tracking. Some clients, including one of the United Kingdom's biggest supermarket chains, used hardware that was decades old to run their checkout systems. All of this software and hardware needed technical support, and all of it is most likely still in use today since it does the job the companies need it to do.

These examples of companies that are reluctant to update software regularly also demonstrate the problems businesses face in developing updates for custom-made software. During my time at the supermarket company, management tried to implement new software across all of the checkouts. Despite extensive testing, unforeseen bugs caused extensive downtime for the upgraded machines.

These types of problems can be unavoidable and can cost millions of dollars in reduced productivity, lost sales, and extra support time.

The Reality of Virtualization

The new Windows 7 feature Windows XP Mode is able to push forward with new virtualization technology because modern multi-core processors can now handle running two or more operating systems side by side, usually with no noticeable loss in performance. I discuss this free add-in for Windows 7 briefly in Chapter 2, "The Basic Windows 7 Utilities."

Windows XP Mode is a fully licensed copy of Windows XP, which allows you to run software, installed in and fully compatible with Windows XP, on a Windows 7 desktop. You can run Windows XP Mode from the Windows 7 Start menu, as shown in Figure 3-1.

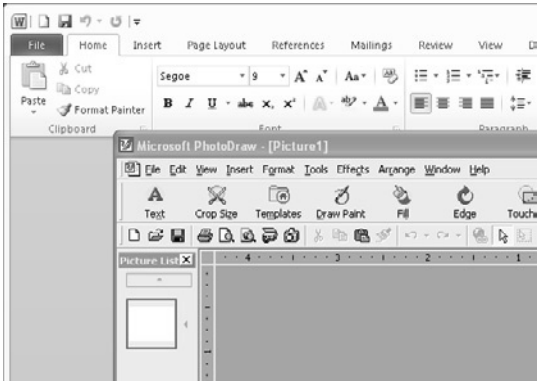


Figure 3-1 Outlook 2003 and Outlook 2010 running side by side in Windows XP Mode

www.it-ebooks.info

On the downside, this is very much an early version of the product and doesn't yet get around the problems that come with having more than one full operating system installed on your computer. For example, you must still download and install Windows XP updates. Also, you must separately install anti-virus and anti-malware software.

INSIDE OUT What is virtualization?

Modern computers come with multi-core processors. Your PC might have an Intel Core 2 Duo chip with two cores or a quad-core processor with four cores. Server chips commonly now have six, eight, or even twelve cores.

Each core is its own processor, essentially the heart of its own PC, and is capable of running a full operating system and accompanying software on its own. Virtualization can take advantage of this, running your "host" operating system on one core, while allowing other operating systems to run on other cores. It is not necessary to have a multi-core processor to run a virtual machine, however.

Windows vNext

Windows vNext is the code-name for the next version of Windows. While there are no details at the time of this writing, strong rumors indicate the legacy code will finally be dropped from Windows with all support for older software and hardware moving to Windows XP Mode. Developers will have to make some serious changes to the Windows XP Mode software to do this; specifically, they will need to address the issues related to updating and protecting Windows XP Mode separately from the "main" operating system. If the legacy code is dropped and support for older versions is moved entirely to Windows XP Mode, however, you can assume that these issues will be addressed.

Removing legacy support from Windows will cut the number of updates for the operating system significantly and make the whole operating system considerably more secure in the process.

While this is something we can all look forward to, we still have to deal with the security problems that exist today. Fortunately, there are some useful features within Windows 7 that can help.

www.it-ebooks.info

Anti-Virus Software for Windows 7

The most basic security requirement for a modern PC, anti-virus software, doesn't come bundled with Windows 7. But Action Center will alert you and help you choose a package to run when you install the operating system, as shown in Figure 3-2. Choosing an anti-virus package can be complicated, however, so I thought I would make my own personal recommendations at this point.

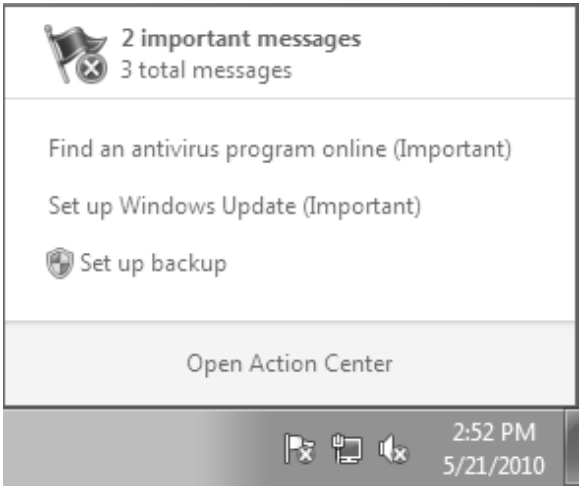


Figure 3-2 The Action Center anti-virus alert

Microsoft Security Essentials

www.microsoft.com/security_essentials

Microsoft's free anti-virus and anti-malware package, Microsoft Security Essentials, has several advantages beyond just being free. The first and major advantage is that it delays computer-slowing virus scans while you are using your computer. The second advantage is that the package is incredibly lightweight, using very little memory and hardly any system resources, and it won't slow down your computer.

www.it-ebooks.info

Norton Internet Security/Norton 360

www.symantec.com

The scanning engine in Norton 360 has won as many awards as Microsoft's own Forefront, a corporate anti-virus scanning engine. This is a more comprehensive suite, with more notifications and warnings, so you'll notice it more when using your PC, which some people might find annoying. It contains many useful features and additions, however, and comes with a license that allows you to install it on several PCs.

Malwarebytes Anti-Malware

www.malwarebytes.org

I recommend several anti-malware products, including SpyBot Search & Destroy and Spyware Terminator. Only Malwarebytes, however, has consistently dealt with hard-to-remove malware from PCs I've encountered. There are also free and for-purchase versions of the product.

Windows Defender

First introduced as an optional add-in for Windows XP, Windows Defender is Microsoft's free, anti-malware product, and it's integrated into Windows Vista and Windows 7.

Windows Defender offers only very basic protection and has some flaws. Most notably, it receives its updates only through Windows Update. If you have Windows Update turned off (which you shouldn't unless you're in a managed corporate environment), or if you do not check Windows Update very often, you could compromise any minimal protection Windows Defender offers.

I recommend always using a third-party, anti-malware package such as Malwarebytes (see the previous section) or Spyware Terminator, which you can find at *www.spywareterminator.com*.

Microsoft Windows Malicious Software Removal Tool

If you review the updates your computer receives through Windows Update, you might notice something called the Microsoft Windows Malicious Software Removal Tool. This is an extra tool in addition to Windows Defender that's updated monthly by Microsoft and runs automatically on your PC. It can also be downloaded from the Microsoft website.

www.it-ebooks.info

As another anti-malware tool, it will check your computer for viruses and malware, try to remove any it finds, and report this information to Microsoft. This is a useful tool but should not be considered a replacement for separate anti-virus and anti-malware products.

User Account Control

ehas been much criticized since its introduction in Windows Vista. This is the security system that prevents users from making critical changes to the operating system and installing software or plug-ins that could be potentially harmful.

In Windows Vista, UAC notifications appear whenever users try to do just about anything and are generally considered annoying. As a result, people simply turn off the feature, making their PCs as vulnerable to attack as they were before the tool was introduced.

When UAC appears, as shown in Figure 3-3, all desktop items and running programs are unavailable until you click Yes or No on the User Account Control dialog box.

With Windows 7, UAC is tamed so that it now appears only when a critical change is being made, such as turning off UAC itself. Most of the time, you are alerted by a yellow shield icon (see Figure 3-4), which can appear on screen anywhere next to a link or on a button. The main UAC alert won't appear for these items. Instead, Windows simply warns you that changing a setting here is something you might want to be careful about.



Figure 3-3 A User Account Control alert

www.it-ebooks.info

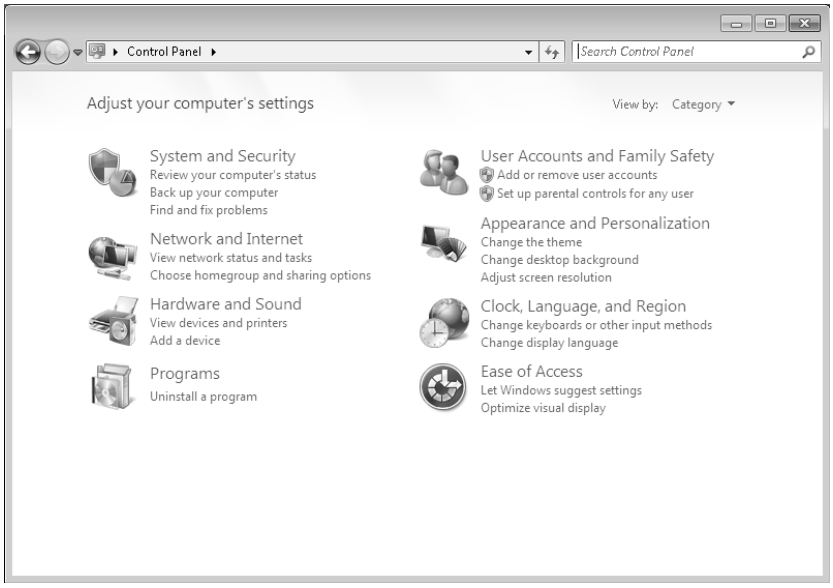


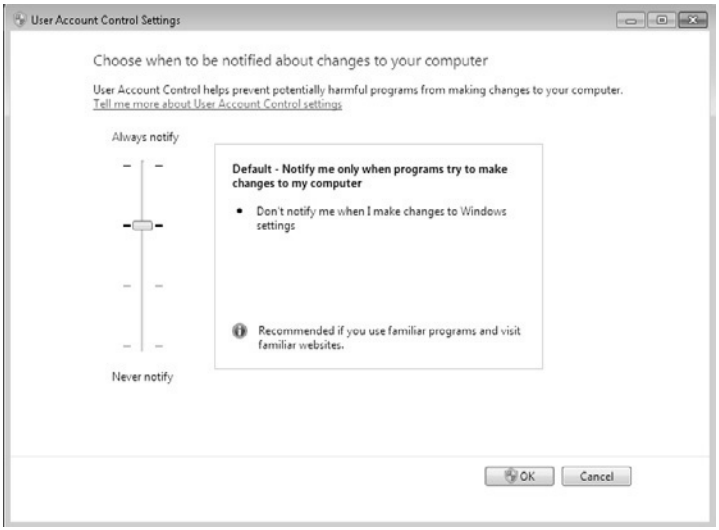
Figure 3-4 Yellow shields next to items to be wary of

By default, UAC is set to what is probably the most sensible level. It alerts you to critical changes being made to your PC but doesn't annoy you with pop-up alerts when you do something like change the time or install software.

You can change the UAC setting to reduce or increase security by following these steps.

1. On the Start menu, click Control Panel.
2. Select System And Security on the window that appears.
3. Under Action Center, click Change User Account Control Settings.
4. Change the UAC level control to suit your needs.

www.it-ebooks.info



There are four settings for UAC in Windows 7.

- **Never Notify** UAC is turned off, so you are not alerted to any changes to your PC or software or attempts to access critical operating system files.
- **Programs Only** You are notified only when programs try to make changes to your operating system settings. You are not notified about other settings changes.
- **Default** With the standard and recommended setting, you are notified when programs and other features try to change system settings, but not when you make changes yourself.
- **Always Notify** You are notified when any system setting changes.

INSIDE OUT The benefit of UAC

As I previously said, many people find UAC irritating. Many people using Windows Vista disable UAC because the only setting is to always notify the user of all system setting changes or nothing at all. However, in Windows 7 it's easy to leave the system turned on. I recommend this because UAC is an essential defense against viruses, malware, and other malicious software on your PC.

www.it-ebooks.info

BitLocker and BitLocker To Go

BitLocker, first introduced with Windows Vista, is available only in the Enterprise and Ultimate editions of Windows 7. It is a full disk **encryption** system that uses the Advanced Encryption Standard (AES) cryptography method.

BitLocker works several different ways in Windows 7, depending on what you are encrypting and what hardware you have in your PC.

Method 1: Encrypting a Hard Disk or Partition with Hardware Support

If your computer's motherboard has a Trusted Platform Module (TPM) chip, it stores the cryptographic keys needed to encrypt and decrypt your hard disk or partition. This encryption key (cipher) is unique to this chip. This means that if an encrypted disk is removed, it can never be decrypted on another computer because the encryption key has been left behind on the old computer.

Method 2: Encrypting a Hard Disk or Partition Without Hardware Support

If your PC does not have a TPM chip on the motherboard, then the cryptographic keys are stored within Windows and are not locked to specific hardware. This method allows you to use the password to access the hard disk if it is plugged into another Windows 7 computer.

Method 3: Encrypting a USB Flash Drive or External Hard Disk

This method of encryption is similar to the non-TPM–based hard disk described in method 2. Windows uses standard BitLocker cryptographic keys to make sure that an encrypted flash drive or hard disk can be used on other Windows 7-based PCs. This method uses the new Windows 7 BitLocker To Go feature.

www.it-ebooks.info

INSIDE OUT What is 128-bit AES encryption?

Advanced Encryption Standard (AES) is a method of encoding a disk drive, partition, external disk, or files. It divides data into block sizes of 128 characters (bits of data) and performs encryption on each block 10 times to secure it and scramble the data so it cannot be read without unscrambling it.

The blocks of data can only be decrypted with a cipher and a password combination, which is never openly displayed. When you type your password to decrypt data, it is converted into a hash key, a random string of characters created by a set algorithm (or formula) that can never be converted back into the password. The server or computer that contains the AES encryption algorithm does the same with the password it has stored in its password vault. If the two hash codes match, then the password is accepted.

You can encrypt a disk using BitLocker only if you have a copy of Windows 7 Enterprise or Ultimate, but the encrypted disk can be read and accessed on any version of Windows 7.

To encrypt a disk, on the Start menu, click Control Panel and then System And Security. BitLocker Drive Encryption settings appear. Click Turn On BitLocker to encrypt a disk, as shown in Figure 3-5.

In the main BitLocker Drive Encryption window you will see details about the hard disks attached to your computer. You can select what drive to encrypt.

Note

If you have a lot of data on the hard disk, it will take longer to encrypt, possibly overnight. Moving the data off the hard disk temporarily will speed up the process.

www.it-ebooks.info

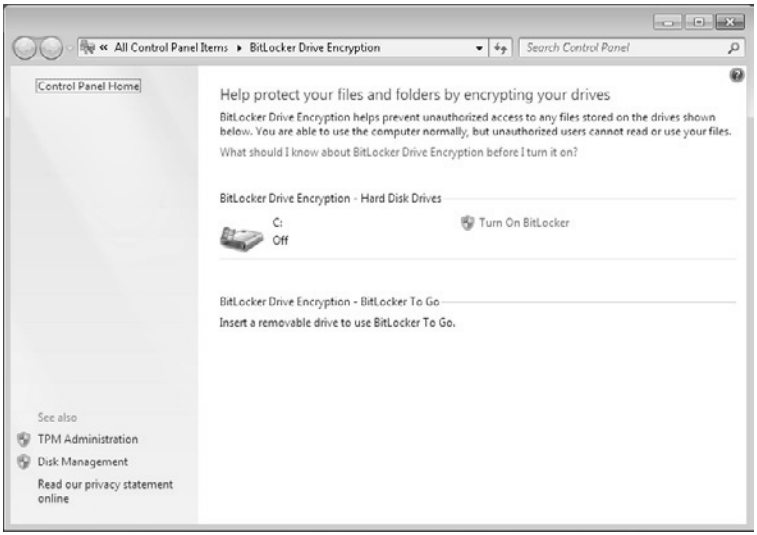


Figure 3-5 Encrypting a disk with BitLocker

CAUTION!

BitLocker provides an extremely high level of security and encryption. If you forget the password or if your TPM-equipped motherboard fails and has to be replaced, you may never be able to access that data again. *Do not* encrypt data using BitLocker if you do not have a backup copy of the data elsewhere!

Using BitLocker with Non-Windows 7 Computers

One of the biggest advantages of using BitLocker is the ability to store sensitive files on devices such as USB flash drives for transport to other machines. Unfortunately, older versions of Windows, namely Windows XP and Windows Vista, do not support BitLocker To Go natively and won't be able to read the files on an encrypted device unless you download and install the BitLocker To Go Reader (see below).

www.it-ebooks.info

Note

Microsoft supplies a free plug-in for Windows XP and Windows Vista, which you can download from *http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=64851943-78c9-4cd4-8e8d-f551f06f6b3d*. You can also search the web for BitLocker To Go Reader.

As its name suggests, you can use this plug-in to read files on a device encrypted with BitLocker To Go, but you cannot write anything to the disk.

INSIDE OUT Alternatives to BitLocker To Go

Many people find the inability to write to a USB flash drive or external hard disk that has been encrypted with BitLocker To Go annoying. So what are the alternatives?

TrueCrypt (*www.truecrypt.org*) is a free, third-party program for encrypting your files and data. You can carry a copy of the TrueCrypt software on your flash drive or hard disk for installation on a host PC. This software is compatible with all versions of Windows and the Apple Mac, and it will allow you to read and write files on the disk.

The limitation of TrueCrypt is that you may not be allowed to install the software on computers where user policies are set up to prevent users from installing software. If you intend to use TrueCrypt in a business or educational environment, you should first verify with the organization's IT department that it is supported.

Cloud storage is another way to store files in one place and access them from different locations. Microsoft's SkyDrive service (*www.skydrive.com*) offers 25 GB of free storage space.

The advantages of cloud storage are that you never need to carry a physical device with you, your files will always be safe and encrypted, and you can access your data anywhere you have an Internet connection.

The downside of cloud storage is that you *must* have a working Internet connection to access the files. If you commonly work remotely with a laptop, or if your Internet connection goes down, you will not have access to your cloud-based files.

www.it-ebooks.info

Why Use BitLocker?

BitLocker is something I recommend people use on laptop computers and sometimes for USB flash drives and external hard disks. If you carry critical information, such as personal data about other people, you will be subject to the data protection laws for your country. Breaking these laws by not properly protecting the data could lead to heavy fines or even imprisonment.

BitLocker is also useful for everyday PC users who not only carry a great deal of personal information in their files, but also commonly store passwords for websites in Internet browsers. If you have a laptop and Windows 7 Enterprise or Ultimate, it is well worth encrypting your disk. If you are considering buying a laptop and can afford to do so, purchase one with a TMP chip and Windows 7 Enterprise or Ultimate. I believe the peace of mind is worth the extra expense incurred.

If you manage a business where employees carry sensitive business or customer-related data on their laptops, these should all be encrypted using BitLocker or another system. Failure to do so is inviting data loss, embarrassment, and possible criminal prosecution.

Beware the Weak Link at the Keyboard

If you have anti-virus software installed in Windows 7 and UAC enabled, your operating system should be perfectly secure. However, the weakest link in all computer security will always be the user. Here are my top tips for avoiding the user errors that can undermine your computer's security.

Keep Your Anti-Virus Software Up to Date

First things first: Make sure you are protected from external attacks by installing anti-virus software.

Make Sure You Have a Good, Up-to-Date Firewall

Just as important as anti-virus software is a firewall. This is your first line of defense against attack from outside. Again, you need to make sure it's kept up to date as well. If you're running Windows XP, don't rely solely on the built-in firewall; it's not enough.

www.it-ebooks.info

Get Anti-Spyware Software

Anti-spyware bsoftware isn't like a firewall or anti-virus software. There's no reason why you couldn't install all three packages. The more protection you get, the better. But make sure you keep them up to date. Also note that most of the free packages will require you to run regular scans manually.

Keep Windows Up to Date

It's essential that you turn on Windows Update and leave it on. Updates are released by Microsoft on a monthly basis and, although some might require you to reboot your PC, the slight inconvenience is well worth it for the added security and peace of mind.

Keep Your Software Up to Date

Make sure you regularly check for general and security updates for the software you use the most. You can find these on the manufacturers' websites.

Always Check Email Attachments Before Opening Them

It's always a good idea to check all **email** attachments for viruses. Save them to your hard disk first, then, in Windows Explorer, right-click the file and select Scan With [*Your Anti-Virus Software*] before you open it.

If you receive a suspicious-looking email attachment from someone you know, you could email that person to ask if she did intend to send it to you. It could be that a virus on her computer has forwarded itself to people in her address book, in which case she would probably like to be notified.

Use a Secure Internet Browser

Browsers like the latest versions of Firefox or Internet Explorer provide much of the protection you need. In Windows 7, the protected mode in Internet Explorer that denies any software running in the browser access to the rest of the operating system is an extra bonus.

Get Spam and Phishing Filtering for Your Email Software

Everyone knows what **spam** is. **Phishing** emails, however, are the messages that purport to be from a real bank or credit card company asking you to type your personal details into a website. I've seen some of the most net-savvy people caught out like this.

www.it-ebooks.info

Never Click Anything You Don't Explicitly Mean To

If you haven't gone to a website with the express intention of clicking items, maybe to install a browser plug-in or get a specific download, for instance, *never* click anything unless you know exactly what it is.

Beware of reputable websites, such as YouTube, where viruses are occasionally posted disguised as a codec that is required to play a video. If you are ever in doubt, simply *don't* click it!

Look for the Padlock or the Green Bar

When shopping online or when visiting any website that requires you to enter personal information, look for the padlock, which is a visual method for your browser to tell you that the website is encrypting any data sent back and forth using a valid security certificate. What browser you use will determine where this is located. The latest security convention in browsers is to color code the address bar. The address bar is displayed as green if the site is okay and orange or red if you should use caution or avoid the site.

> **Note**
>
> **Not all web browsers will use colored address bars, and they may display the padlock in different ways and in different areas of the browser. You should refer to the Help menu for your specific browser for more advice on this.**

Never Give Private Details Online Unless You Have To

Shopping for a credit card or car insurance is one thing, but many websites will unnecessarily ask for personal details that too many people are all too willing to give away. At best, these details are used to send you spam; at worst, they are used to steal your identity.

Keep Backups

Make sure you keep regular backups of your data somewhere away from your Windows installation, maybe on an external USB hard drive, for instance. Windows has a built-in backup utility (which is much improved in Windows 7), but third-party packages offer backup solutions, too.

www.it-ebooks.info

Keep the Driver CDs and Manuals for Your PC

Always safeguard the discs and manuals that come with your PC. These will prove invaluable if Windows ever needs to be reinstalled. Make sure you keep them somewhere safe and together.

Keep Windows Maintained

You will have much more fun on your PC if you keep it tidy and maintained. Make sure you uninstall programs you don't need, use the built-in tools or third-party tools to remove unnecessary files, and keep the **registry** clean.

Be Careful When You Throw Away Your PC

When your PC comes to the end of its useful life, make sure you download a utility that will securely erase the hard disk by overwriting the data several times. If you can, also remove the erased hard disk and dispose of it separately. Discarded PCs can contain a wealth of sensitive information that makes them a bargain find for identity thieves.

Guest Mode

Guest Mode was an extremely promising feature in the Windows 7 **beta** that was sadly removed from the final release. But it may appear in a future version of Windows, and certainly hardware and software vendors have products that fill the void until then.

Guest Mode was a special user account within Windows 7 that created a temporary environment for users on your computer. When the user logged off, every change he made to the operating system, every program he installed, and every file he created or downloaded was rolled back so that everything was returned to the way it was before the user logged on. In short, it was as if that user had never used the PC.

This would be an excellent way to protect a PC from the dangers posed by a guest user, maybe someone visiting your home or office, over whom you have no control.

A similar feature in the Apple OS X operating system caused users to complain that a bug was also wiping out all of the user files from their main accounts. Clearly, this type of feature is not without its problems, but there are some excellent third-party solutions.

www.it-ebooks.info

I have always liked Magic Card, a product by Rogev, which you can find at *www.rogev.co.il*. This is a small expansion card that sits inside your PC and handles real-time encryption and decryption of data on one or more hard disks, similar to a TPM chip and BitLocker but handled entirely by the hardware. In addition, the product is capable of saving a snapshot of your Windows installation and restoring any changes made in just a few seconds. It can do this every time the computer is restarted or on a set schedule, such as once a month.

This type of product is especially useful for businesses, libraries, training companies, and internet cafés where changes to an operating system are made rarely and where any down-time for a PC can prove costly.

Gibson Research

The market for PC security is enormous and includes every type of product that you can imagine. One website that I've found invaluable over the years is Gibson Research Corporation at *www.grc.com*.

Steve Gibson is a highly respected PC security expert, probably the best. His website includes his ShieldsUP! tools, which he accurately describes as, "the Internet's quickest, most popular, reliable and trusted, free Internet security checkup and information service."

There are also a host of other tools at the website for testing the security of your PC, Internet connection, and firewall. I cannot recommend the tools on this website highly enough.

Summary

Once your security is set up in Windows 7, this is not the end of the story. You must always be vigilant about what you click and careful about other people using your computer. It's very easy for even the most ardent computer security expert to accidently or carelessly click something he shouldn't.

Making certain you have your anti-virus and anti-malware protection up to date at all times is also essential, but don't rely solely on the scheduled scans. If you have some time, run a full scan manually. You never know when it might just save more than you might realize.

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 4

Backup and Restore

Moving Your Files Away from Windows 7 53
Using Backup and Restore 57
Backing Up the Operating System. 63
Determining How Many Backups You Need and Where to Store Them. 66
Summary 67

Keeping regular backups of your files and data is essential as more and many of us keep irreplacable files such as photographs and corporate documentation. Windows 7 makes backing up your files and data easier than ever.

You should also make sure that Windows itself is backed up; this can be invaluable in helping you get working again quickly in the event of a crisis.

In this chapter I'll talk about how to back up your files safely and securely, where you can and should do this, and I'll also talk about how to make sure that Windows 7 itself is backed up.

Moving Your Files Away from Windows 7

In Chapter 1, "Prevention Is Better than Cure," I wrote about how it's essential to move your files and data to a different partition from the one on which Windows 7 is installed. If there is a critical failure with Windows 7, and it needs to be restored from a backup or reinstalled, you could lose *all* of your files if they are stored on the same partition.

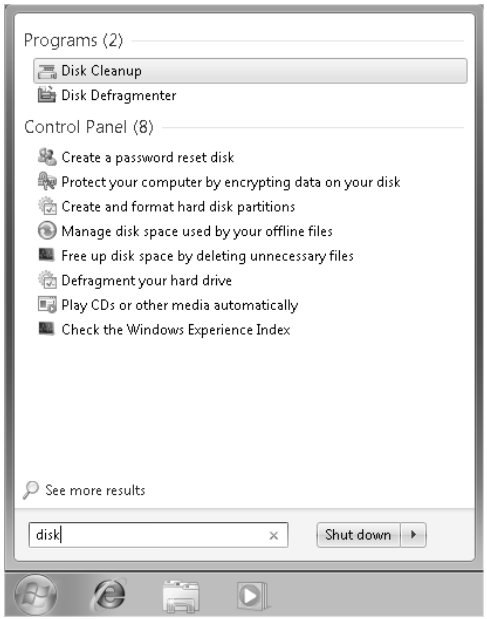
In Chapter 1, I describe how to create a new partition when installing Windows. But what if you want to move your data to a separate partition after you have already installed Windows 7? To help you do this, Windows 7 includes a feature to grow and shrink the size of partitions and then allows you to make extra partitions in the available disk space created.

The Disk Cleanup Wizard

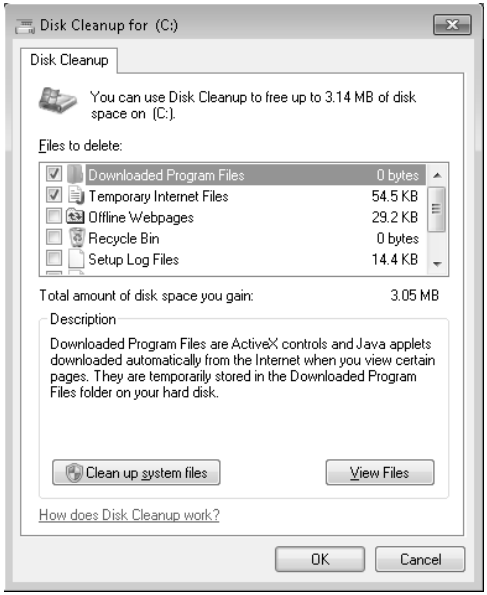
In preparation for moving your data to a new partition, delete any **temporary files** that consume space. Windows 7 can shrink the partition it's installed on by only so much. The more files and programs you have installed on the partition, the less Windows 7 will be able to shrink the drive.

1. In the Start menu search box, type **disk** to find Disk Cleanup, and select Disk Cleanup from the results that appear (as seen in the image on the next page). You can also access this utility on the Start menu by clicking All Programs, clicking Accessories, and then clicking System Tools.

www.it-ebooks.info



2. Run the wizard, indicating which drive you want to clean. This will usually be the C drive. You will be able to select various options in the Disk Cleanup dialog box for recovering wasted space on your hard disk or Windows 7 partition. It is safe to choose any of the available options in Desk Cleanup.



www.it-ebooks.info

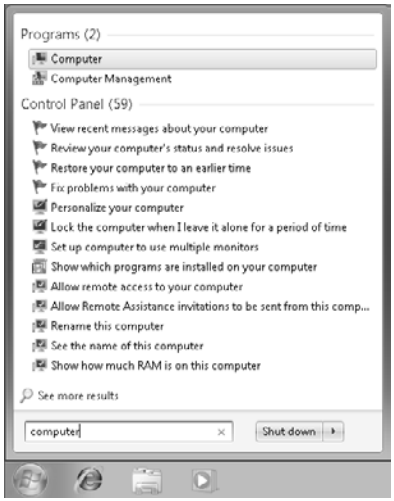
You may also want to use a third-party utility to help clean up your drives. I recommend CCleaner from *www.piriform.com/ccleaner* and Glary Utilities from *www.glarysoft.com*.

Shrinking, Extending, and Creating Partitions

The next step in creating a new partition for your data is to shrink the size of the Windows 7 partition so you can create space for a separate partition. You can also extend a partition if there is any available space that it can be expanded into, although you will not need to do this in this instance.

If your files are already on the same partition or drive as Windows 7, you should move them to a separate disk or partition if possible. Having a copy of your files on the same partition you are trying to shrink will severely limit how much it can contract.

1. In the Start menu search box, type **computer** and select Computer Management from the results that appear. You can also access Computer Management by right-clicking Computer on the Start menu and clicking Manage.



2. In the Computer Management window, click Disk Management in the left pane.

   A list of the available hard disks and their partitions appears in the central panel of the window. Refer to the image that follows step 3 for an example. The example shows that I have two hard disks on this particular PC and two backup partitions on a different hard disk than my main copies of Windows and my files. One backup partition is for files and one is for a copy of Windows. I also keep a second backup of my files separate from my PC.

www.it-ebooks.info

3. Right-click the partition you want to shrink, and select Shrink Volume. Windows 7 determines the maximum amount it can shrink the partition. On a new installation of Windows 7 with no additional files, this can be quite a lot. Choose a new partition size that will meet your needs (see Chapter 1 for suggestions about partition size), and then click OK.



4. In the blank volume that you have created, right-click anywhere in the empty space and select Create Volume from the context menu that appears. You will want to format the new volume you create so that you can write files to it using the NTFS option. This is the default disk formatting type in Windows 7.

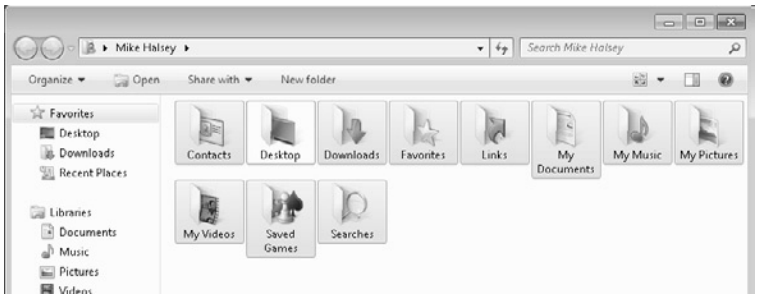
www.it-ebooks.info

Moving the Shell User Folders

If you followed the procedure in the previous section, you now have a spare partition onto which you can move your files. But first you need to move the shell **user folders** to the new partition that you have created. **Shell user folders** are the pointers within Windows 7 that open the correct folder on the correct disk or partition when you click My Documents, My Pictures, and so on.

1. On the Start menu, click your name at the top right. Your user folders appear.

2. Select all the user folders, but don't select Desktop because this folder might not function properly if you move it. Right-click the selected user folders, and select Cut.



3. Navigate to the hard disk, partition, and folder where you want to store your files, right-click in a blank space in the folder, and select Paste. Your files and data are now moved to the new location. If you moved any files to an external hard disk at the very beginning of this process, you can now move them to the new location.

Using Backup and Restore

Windows has always included a utility for backing up your files and folders, and the good news is that it's easier and simpler than ever to use in Windows 7.The bad news is that you might not want to use it!

Backing Up Files and Data

Backup and Restore saves your files as a secure, compressed archive. Backup and Restore can be very useful if you don't want other people looking through the files you've backed up. However, if you will eventually want to access these files on another computer, for

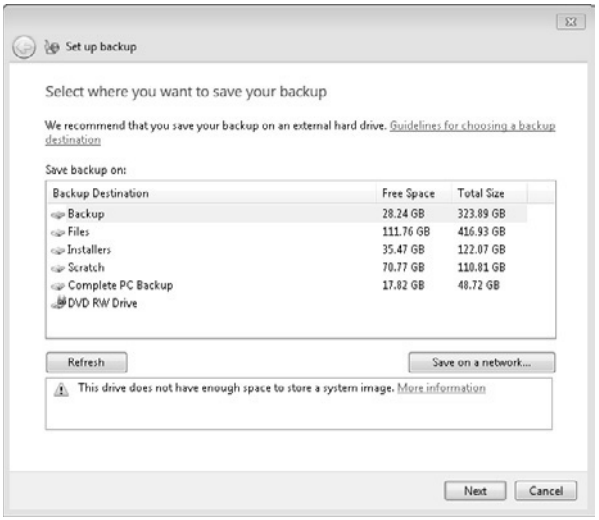
www.it-ebooks.info

example if you want to save the backup to a network-attached storage drive on a home or office network or to an external USB hard disk for working in different locations, you won't be able to access them. If you want to save your backup to an external hard disk, you should consider a third-party backup solution instead of Backup and Restore, and I will cover some of these solutions later in this chapter.

1. Access Backup and Restore on the Start menu by clicking All Programs and then clicking Maintenance, or by typing **backup** into the Start menu search box and selecting Backup and Restore from the results that appear.

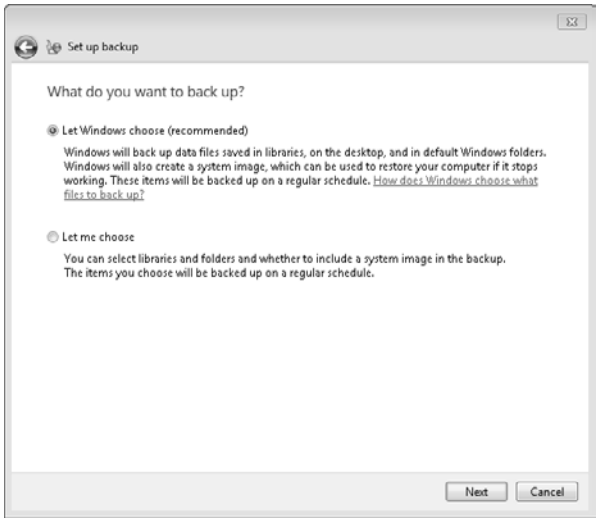
2. In the Backup and Restore window, click Set Up Backup.

3. The Set Up Backup dialog box appears with a list of locations on which you can store your backup. This list includes any hard disks and partitions on your computer. You can also choose to save your backup to a network by clicking Save On A Network. Indicate a location for your backup, and press Next.



4. Next, decide what to back up. If you want to let Windows choose which files and folders to back up, select Let Windows Choose. If you want more control over what is backed up, select Let Me Choose. You should note that the default option will also create a full backup of your Windows 7 installation. If you have already done this separately, you should select Let Me Choose.

www.it-ebooks.info



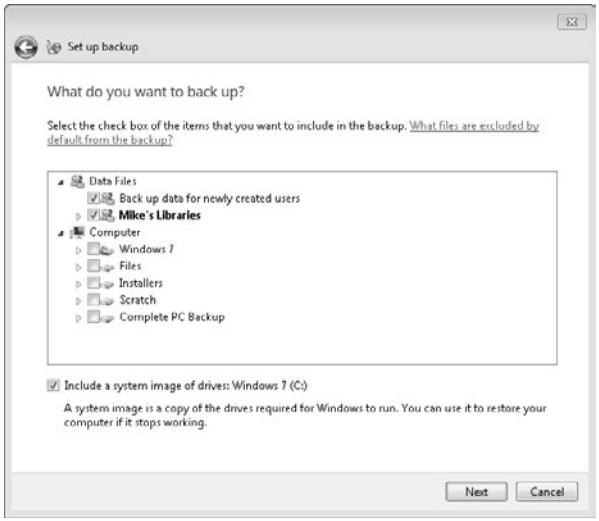
INSIDE OUT

Be careful backing up Windows 7 over a network

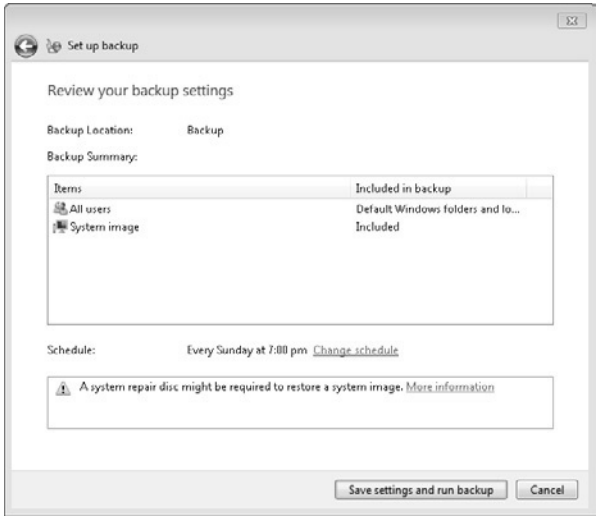
You should only let Windows Backup and Restore make a backup copy of your Windows 7 installation over a network if your PC is connected to the network by a physical cable. If you connect only via Wi-Fi, the restore software will be unable to see the backup if it eventually must be restored. This is because the Windows 7 System Image Restore tool doesn't run on the Windows 7 desktop and, therefore, cannot load any Wi-Fi hardware drivers. It can only rely on wired networking support provided by the computer's BIOS.

5. Next, choose what files and folders you want to back up. The item in bold (Mike's Libraries, for example, in the following figure) includes all of your standard shell user folders for documents, music, photos and pictures, and videos. Select and clear the check boxes, as appropriate, to indicate which items to back up.

www.it-ebooks.info



6. Finally, review the backup settings, including the scheduled time. You can change the schedule to suit your own needs and preferences by clicking Change Schedule. Also note whether Windows will perform a system image backup of your Windows 7 installation. When you are ready to perform the first backup, click Save Settings And Run Backup.



www.it-ebooks.info

INSIDE OUT

Backing up to external hard disks, **CDs**, and DVDs using Windows Backup and Restore

If you want to back up to an external hard disk on a regular basis, you will need to make sure that the drive is connected to your computer when the regular backup is scheduled.

Windows Backup and Restore cannot save regular backups to blank CDs, DVDs, or Blu-Ray discs. You will need a third-party solution if you want to store your backups to these media. You can manually copy any backups stored on an external hard disk to an optical disc.

Restoring Files and Data from a Backup

You can restore your files and data from a backup by using the Backup and Restore tool accessed in the same way detailed earlier in the chapter, by typing **backup** into the Start menu search box and selecting Backup and Restore from the search results that appear, or on the Start menu by clicking All Programs and then clicking Maintenance.

If you have performed any backups, they will appear in the Restore section of the Backup and Restore window that appears. You can see in Figure 4-1 that there are currently no backups to be restored because Windows Backup has not yet been set up and configured.

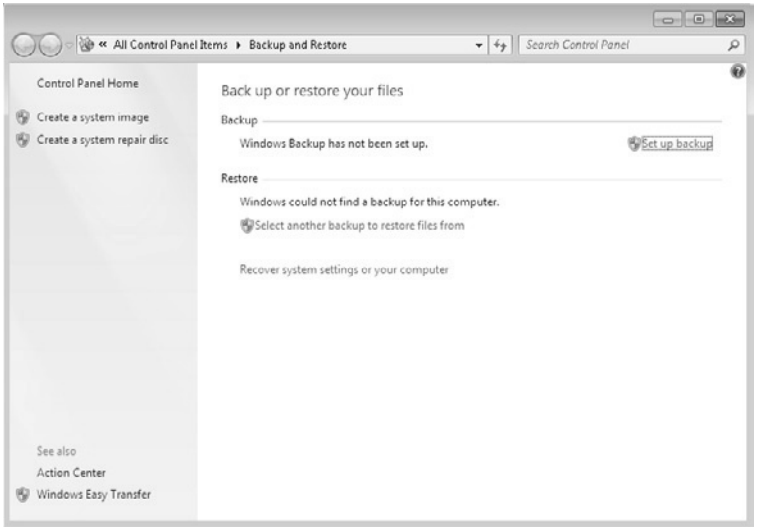


Figure 4-1 Backup and Restore

www.it-ebooks.info

The Backup and Restore tool is automated and will give you the option of choosing to restore all of your files and data or only selected items. The Restore tool will find your most recent backup very quickly and will restore all of your files to their original locations.

Third-Party Backup Solutions

If Windows Backup and Restore isn't the solution that best suits your needs, there are plenty of others. If you have an advanced security suite installed, such as Norton 360, it might include its own backup program. You might also get a backup tool with CD, DVD, or Blu-Ray burning software, such as Nero.

You might find third-party software the best option if you regularly want to back up to CDs, DVDs, or Blu-Ray discs, because the backup program in Windows 7 won't do this.

I use NTI Shadow, which you can purchase at *www.newtechinfosystems.com*. I find it offers an excellent range of features, all of which are extremely customizable.

Backing Up to the Cloud

Cloud storage is becoming increasingly popular, and there are many benefits to keeping a backup of your files online, not the least of which is that your files and data will always be secure if you have a fire at home or at work. It is the ultimate offsite backup.

On the downside, many people are concerned about the privacy and security of files sitting who knows where, accessible by who knows whom. However, for the most part, services from providers such as Microsoft, Google, and Amazon are very trustworthy.

INSIDE OUT Slow backups to the cloud

The rate at which you can back up your files and data to the cloud is dependent on the speed of your Internet connection. If you have a large number of files, you could find it takes many weeks to complete the initial backup, after which time the software should back up only new or modified files.

Cloud-based backup services include Amazon S3, Mozy, and Microsoft SkyDrive. SkyDrive offers a massive 25 GB of free storage space. Generally, though, you will need to pay a subscription fee to maintain your online backup. The price will depend on the service you use and how much data and the number of files you back up.

www.it-ebooks.info

Version Control

Some backup programs and cloud services offer version control. This means that if a file changes, for instance, if you update a Word file, the backup program keeps a copy of the older version of the file instead of replacing it at the next backup. This can be useful if a file is changed accidentally or if you later want to undo a change you didn't mean to make.

Another useful feature in versioning is the ability to temporarily recover a copy of a file that you have deleted from your computer. This means that if you accidentally delete something and then do another backup before you've noticed, you will still be able to recover the deleted file from a versioning folder for a certain amount of time.

Backing Up the Operating System

In Chapter 1, I wrote about how you can back up Windows 7. This is essential because if Windows 7 ever fails, you can be up and running with all of your programs installed and all settings correctly configured quickly.

Restoring Windows from a Windows System Image

If you have used the Windows 7 imaging tool to create your backup copy of Windows 7, you will need to either boot your PC from the Windows 7 installation DVD or from a **system rescue disc** that you create.

To create a system rescue disc, you will need a blank CD or DVD (either will do). In the Start menu search box, type **repair**, and then choose Create A System Repair Disc from the search results that appear, or on the Start menu click All Programs, click Maintenance, and then click Create A System Rescue Disc.

INSIDE OUT The system repair disc

There are several ways to create a system repair disc. In addition to the two methods detailed in this chapter, you can also use the main Backup and Restore window. You can also create a system repair disc when you create a full system image of Windows 7.

The benefit of having a system repair disc is that if you ever need to recover Windows 7 from a backup, you won't need to access your original Windows 7 install DVD. The original media is valuable and should be kept somewhere it will be safe from scratches, loss, and other damage.

www.it-ebooks.info

You can see in Figure 4-2 that creating a system repair disc is an extremely simple operation. You only need to indicate which CD/DVD burner you want to use on your PC to create the disc and then click Create Disc.



Figure 4-2 The Create A System Repair Disc dialog box

You should keep your system repair disc safe. In some circumstances, you may even feel it's appropriate to create more than one of these discs for future use.

Restoring Windows 7 from a System Repair or Install Disc

Before you boot your machine from a system repair or Windows 7 installation disc, you will need to verify that your computer's BIOS is set to boot from the CD/DVD drive before the hard disk. You can access the BIOS by pressing F2 or Delete on your keyboard when you turn on the computer. The setting to verify is called Boot Order or Boot Priority.

As shown in Figure 4-3, the system repair disc first determines if there is a copy of Windows on the PC that won't start. Once this process is complete, you will have the option to repair the faulty installed version of Windows 7 or restore it from a previously backed up copy.

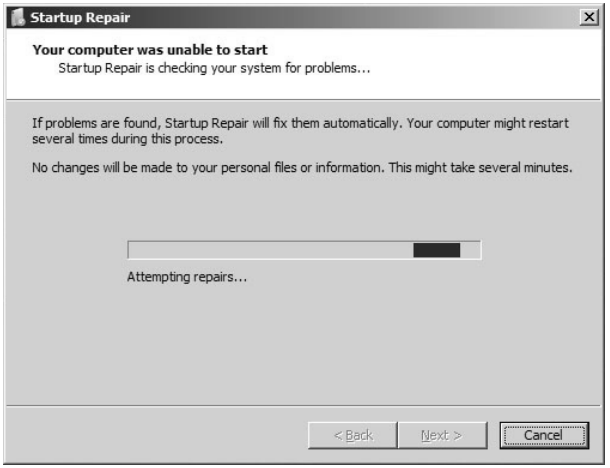


Figure 4-3 Windows Startup Repair

www.it-ebooks.info

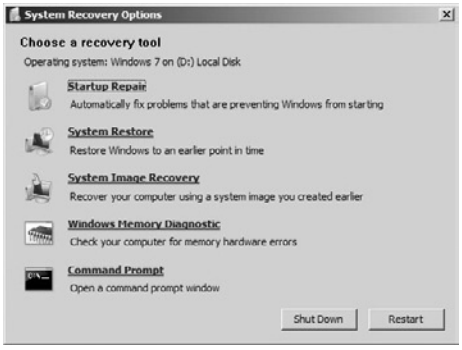
INSIDE OUT

Differences between a system repair disc and a Windows 7 installation DVD

A system repair disc and the Windows 7 install DVD present different options when repairing Windows 7 or restoring it from a backup image. When you boot your PC from the Windows 7 installation DVD, you need to click Repair Your Computer on the initial screen.



Booting from the Windows 7 installation DVD also provides more options for repairing your computer. For simple repair and reimaging, it can be much easier to restore from a system repair disc.



Corporate Image Backups

In the corporate workspace, it's uncommon to use Windows 7 imaging software for creating system backups. The common software packages used by large organizations for creating full system images of Windows are Norton Ghost (*www.symantec.com/norton/ghost*) and Acronis True Image (*www.acronis.com/homecomputing/products/trueimage*). Both of these packages will do the same job and can also offer additional file and data backup software as an extra.

www.it-ebooks.info

Determining How Many Backups You Need and Where to Store Them

The 19th century playwright and author Oscar Wilde famously said, "To expect the unexpected shows a thoroughly modern intellect," and it's a good motto to live by when deciding how many copies of files, data, and Windows to have backed up and where to keep them.

I keep three backups of my files and data.

- One is on a second hard disk inside my main PC for quick restore.
- One is on a network attached storage (NAS) box in my home office.
- An incremental backup made to DVD is periodically mailed to a friend.

I don't currently keep a copy in the cloud because I have far too many files to upload efficiently. This strategy covers all the basics for me, from getting back files in a hurry to guarding against fire and theft.

I recommend that you always keep two backups of your files and data. You should keep one with your PC, or close to it, in case you inadvertently lose files that you want back in a hurry. You should store a second backup either with friends or relatives or in a cloud service such as Carbonite, Amazon S3, or Microsoft SkyDrive.

Offsite backup is more important in business where the data a business owns is probably the single most important asset it possesses.

It's not worth keeping backup images of your copy of Windows 7 remotely because, in the case of a fire or theft, you would need a replacement computer, so your existing backup wouldn't work unless all the hardware in the replacement machine was identical to the one that had been lost.

CAUTION!

If you keep critical copies of backups on removable optical discs, be aware that they can degrade over time, eventually becoming unreadable. My advice is to periodically verify that the discs are readable and replace them with other full backups at least once every 12 months.

www.it-ebooks.info

Summary

As you will see in later chapters, recovering data from a corrupt copy of Windows or a damaged computer can be extremely problematic and sometimes cost considerable amounts of money.

Keeping safe and regular backups of your files and data is always the best policy and the best way to ensure that, whatever problems you face, you can always be back up and running quickly and without hassle.

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 5

Maintaining Windows 7

Defragmenting Your Hard Disks 69
Maintaining Windows 71
Don't Install Too Much Software 75
Keeping Windows 7 Updated 76
Keeping Auto-Running Software to a Minimum 76
The One Year Reinstall Rule 77
Summary 78

It's not enough to just install Windows 7, load your programs, and configure all of the settings and backups. Windows 7 is, as I've already mentioned, sadly not a consumer electronics system where you can take your PC out of the box, plug it in, and have it work happily for years. It will eventually be clogged and bogged down with temporary files, discarded settings, and assorted debris that can slow down the operating system and cause program and other instabilities. However, some tools built into Windows 7 can help prevent a slowdown. The bulk of such programs are from third parties, and there are some excellent free utilities available to clean and optimize your copy of Windows and its installed software.

Defragmenting Your Hard Disks

There is some argument about whether **defragmenting** your hard disks actually makes a difference these days.

As seen in Figure 5-1, some files on your hard disk can become fragmented after a period of time.



Figure 5-1 Fragmentation diagram

www.it-ebooks.info

Fragmentation occurs when files are deleted from your PC. To make the best use of the available space, Windows can split new files into chunks. It will try to save all of these chunks together as a single block of data, but sometimes Windows will scatter them to fill the available space.

When the PC was new in the 1980s and early 1990s, disk fragmentation caused considerable slowdowns, but it's much less of an issue with modern hard disks. If you have a solid state disk in your PC, fragmentation shouldn't affect you at all, because fragmented data will still be read from a solid state disk at the same speed as contiguous data.

CAUTION!

Defragmenting hard disks puts enormous stress on them. They're designed to easily cope with these stresses, but I have had an older hard disk explode inside its metal case because of the physical stresses that defragmentation put on it. It's wise not to defragment your disks too often.

The Windows utility Disk Defragmenter is set to automatically defragment your drives on a schedule. You can access Disk Defragmenter on the Start menu by clicking All Programs, then clicking Accessories, and then clicking System Tools or by typing **defrag** into the Start menu search box. You can change what disks and partitions are defragmented and on what schedule by using the settings in the Disk Defragmenter dialog box, as shown in Figure 5-2.

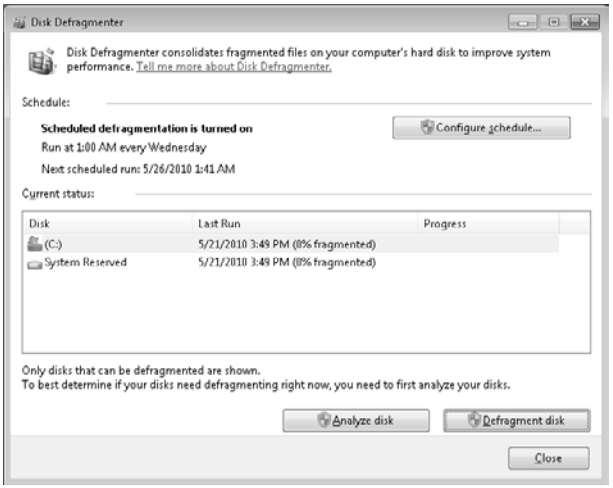


Figure 5-2 The Windows 7 Disk Defragmenter dialog box

www.it-ebooks.info

Which Hard Disks and Partitions Do You Defragment?

It's not always necessary to defragment all the disks and partitions in your PC. If, for instance, you have a partition containing only a backup image of your copy of Windows 7, the data on that partition is not going to change. This disk would not need defragmenting. You need to defragment only the disks where you store files that change regularly, such as your Windows 7 drive and the drive on which you store your files and data.

INSIDE OUT When not to defragment

There are some circumstances when you should not defragment your hard disk. If you have a solid state disk that contains memory chips instead of an actual spinning disk, defragmenting will give you no performance benefit whatsoever, and so it isn't worth it.

As mentioned earlier, there is some discussion about whether defragmenting offers any real benefits on modern hard disks due to their speed and efficiency, so you may decide that you don't need to defragment your own PC at all.

Maintaining Windows

Over a period of time, Windows 7 folders get clogged up with all types of old and temporary files, assorted files left over from uninstalled programs, and dead files. These can slow down the computer and certain software. Windows 7 contains a tool called Disk Cleanup that you can use to delete some of these unnecessary files, but other third-party tools are also excellent for keeping Windows 7 healthy.

Disk Cleanup

You can access Disk Cleanup on the Start menu by clicking All Programs, clicking Accessories, and then clicking System Tools (see Figure 5-3). You can also find this tool by typing **clean** into the Start menu search box. You may be prompted to indicate what drive you want to clean; in most cases, you will choose the C drive. Disk Cleanup will delete some of the temporary and other unwanted program files that can slow down Windows 7.

www.it-ebooks.info

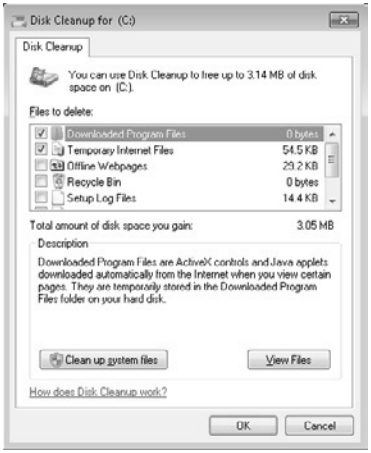


Figure 5-3 Disk Cleanup

By default, Disk Cleanup recommends what items it can delete, but it also offers additional options if you want to reclaim even more space.

Clicking Clean Up System Files will display additional options, including the choice to delete operating system restore files. However, you should remove these only if you are very confident that Windows 7 is running completely fine.

Internet and Other Temporary Files

Many of the temporary files on your computer are from your web browser. The method to clear these temporary files differs from browser to browser, but with Microsoft Internet Explorer 8, which ships with Windows 7, you can easily locate them for removal and cleaning by clicking Safety on the browser **toolbar** and selecting Delete Browsing History. You can also access the Delete Browsing History dialog box by pressing **Ctrl**+Shift+Delete on your keyboard when in Internet Explorer.

In the Delete Browsing History dialog box, shown in Figure 5-4, you can delete temporary Internet files and other items that are not deleted by Disk Cleanup while preserving the data you want to keep.

www.it-ebooks.info

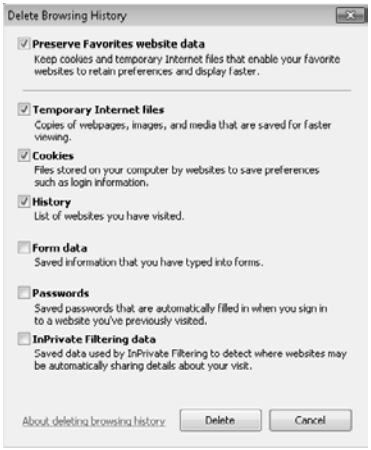


Figure 5-4 Deleting the browsing history in Internet Explorer 8

Third-Party Tools and Utilities

Almost all of the tools and utilities for keeping Windows 7 running efficiently are made by third parties. Here is a selection of some of the best, both free and for purchase.

CCleaner

www.piriform.com/ccleaner

CCleaner is widely considered one of the best programs available for tidying up Windows files. By default, it has very sensible settings, but there are some advanced options, too, which should be used only by advanced users. These advanced features include the ability to clean old and unwanted items from the Windows 7 registry.

Glary Utilities

www.glarysoft.com

There have been numerous all-in-one programs for fixing problems with Windows over the years, including the famous PC Tools. Glary Utilities is a very small and lightweight utility that does one job and does it very well, providing simple, one-click cleanups of unnecessary files in Windows.

www.it-ebooks.info

Ashampoo WinOptimizer

www.ashampoo.com

Another all-in-one program is the excellent Ashampoo WinOptimizer. Their marketing emails can be a bit of a nuisance, but the software itself is extremely well featured with many more controls than Glary Utilities and many advanced controls, too.

PC Tune-Up

www.largesoftware.com

One of the finest PC maintenance packages I've ever had the pleasure to use is PC Tune-Up. This software is simple to use with a series of Next buttons that take you through simple steps to clean up and repair issues with your PC. It's also very powerful, frequently catching problems and rogue files that other optimizers miss.

INSIDE OUT Do registry optimizers work?

The registry is a database that stores all Windows settings (user profiles, permissions, and so on) and all the settings for the software you have installed. As settings change and programs are uninstalled, the registry can become fragmented in the same way a hard disk can.

There is some debate, however, about whether optimizing (defragmenting) this database actually provides any speed improvements. The answer is twofold and can depend on how old your computer is and how much memory it has.

When Windows starts, it loads many of its files, including the registry, into your PC's memory. The more memory your PC has, the more files it can accommodate. Files loaded into memory can be read much faster than those on the hard disk.

There's also the issue of stability. It's a known fact that a database that gets very fragmented can eventually become corrupt. This could happen to the registry, too, and defragmenting it could be a good option.

However, the simple fact is that nobody really knows for sure what effect, if any, optimizing your registry has. It's something that some software packages do, and you might find it works for you. However, I wouldn't be too worried if your clean-up tool is unable to do it.

www.it-ebooks.info

Don't Install Too Much Software

People used to say that Windows had a ceiling of 30 programs that could be installed before the operating system became unstable. Whether there is any truth to this is a great computing mystery. There is no doubt, however, that the more software you install in Windows 7, the more unstable it becomes. The point at which this happens will depend entirely on the software you install. For instance, if you install no software on a PC, which isn't very likely, it will run for an extremely long time. This is because there's nothing installed that can be incompatible with anything else.

Windows often fails or crashes because of incompatibilities with a software component or a hardware driver. This happens because there are so many hundreds of thousands of software packages, and hundreds of thousands of hardware devices, that no manufacturer or Microsoft could ever test every possible combination for stability. Microsoft offers certification programs for software and hardware in Windows 7, but this still won't test against how a specific piece of hardware or software will interact with other hardware and software, especially packages that haven't been through the optional certification.

Windows is built on an open platform and anyone, including enthusiastic amateurs, can write applications for it. This is why Windows is now the most flexible and extensible computing platform in the world.

The other reason is that custom-made software written for organizations also does not always go through the sometimes very expensive Microsoft certification program. Why send your software to Microsoft to certify when you'll only be using it yourself?

So, a limitless number of combinations of hardware and software can be installed on a PC. This makes the whole system unpredictable, and, although Microsoft has made great strides to make Windows 7 as stable as it can possibly be, problems can still occur.

My tips for avoiding problems with installed software and hardware are as follows.

- Don't buy any hardware that has not passed Windows 7 certification and does not carry the Certified for Windows 7 logo.
- Avoid shareware and **freeware** that's written by small software houses and individuals if you can.
- Avoid installing trialware that will sit unused on your PC and expire after a while.
- Install only software that you'll actually use!

www.it-ebooks.info

Keeping Windows 7 Updated

One of the most important ways to avoid instabilities with Windows 7 is to turn on Windows Update and have it download updates on a regular schedule. Periodically, incompatibilities are reported and fixed by Microsoft and then distributed through Windows Update on what is frequently referred to as Patch Tuesday, the second Tuesday of every month. These updates can fix all types of issues that can cause Windows to become unstable or unresponsive. It is important to leave Windows Update turned on.

Keeping Auto-Running Software to a Minimum

By default, a great many programs you install run automatically every time you start your PC. This includes common favorites such as Adobe Acrobat Reader and Apple iTunes software.

Some of these software packages are updaters. People have been asking Microsoft to allow third-party vendors to distribute their updates via Windows Update for years now, but it has not happened yet. For some software, it is worth keeping the updater running. Adobe Acrobat PDF files, for instance, are a frequent source of virus infection, so, although you may not want the Adobe Updater software running every time Windows starts, you should run it manually at least every month. However, there's a strong argument to run other updaters, such as iTunes, only when you actually want to run the software.

The problems caused by auto-running software aren't just that they can slow down your computer and even push up your carbon footprint. (You'd be surprised how much extra money you're paying on your electricity bill by running these things!). They can cause other issues, such as file fragmentation and temporary file clutter, just by being in the background. With the Windows 7 MSConfig tool you can disable some of these unwanted programs.

To access the MSConfig tool, type **msconfig** in the Start menu search box. After MSConfig loads, click the Startup tab. Here you will see a list of all the programs that run every time you turn on your PC. There may be programs you want to keep. As shown in Figure 5-5, I leave Spyware Terminator (an anti-malware package) and NTI Shadow (my automatic backup software) running on my computer for obvious reasons. You will also need to run other software packages at startup. You may want to deselect some packages, however, to save file clutter, processor cycles, and money on your electricity bill.

www.it-ebooks.info

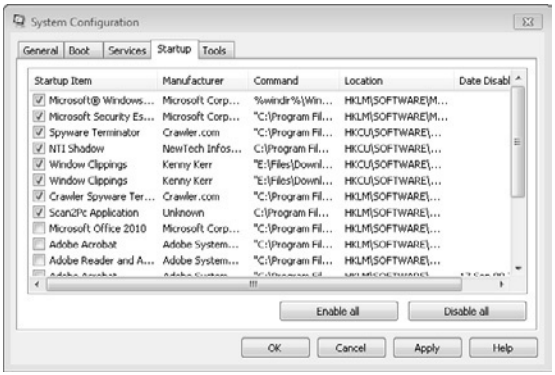


Figure 5-5 Preventing programs from running at startup by using MSConfig

The One Year Reinstall Rule

With earlier versions of Windows, you needed to format your hard disk and reinstall the operating system regularly as it became unstable. Since the introduction of Windows XP this has become less of an issue, but for PCs that are used frequently, amassed temporary files and incompatibilities can cause problems over time. For this reason I recommend that, if possible, you restore Windows 7 from a backup every twelve months or so.

In Chapter 1, "Prevention Is Better Than Cure," I talked about how to back up a working copy of the operating system, complete with all of your programs and hardware installed. You know that the copy you have backed up will be fresh and working fine, so I advise that you restore this backup, update it by using Windows Update, update any programs as necessary, and then back up this new system.

CAUTION!

Remember, don't use the computer too much while preparing it to be backed up. This will help prevent buildups of temporary files or incompatibilities that would then be locked into your backup.

You should set aside one half day or so to reinstall Windows and take your time updating your system thoroughly before locking it down again in a fresh operating system image backup.

www.it-ebooks.info

Summary

Windows 7 is not quite yet a system that can maintain itself. It still needs you to provide some input now and again. However, Windows 7 is not very good at reminding you to provide maintenance, and you will probably only notice that the operating system needs attention when it or your other software begins to slow down. It's not difficult to perform simple maintenance on your copy of Windows 7, though, and the benefits to performance, stability, and security can be enormous. This is definitely time well spent.

www.it-ebooks.info

CHAPTER 6

Users

How Windows 7 Controls Users 79
Managing User Accounts 80
Group Policies 87
Blocking CDs, DVDs, Flash Drives, and External Hard Disks 90
Summary 91

In IT support circles, a great many issues are blamed on a PEBCAK, an acronym for the phrase "Problem Exists Between Chair And Keyboard." It's impossible to have a computer problem without a user being involved in some way and usually as the cause, inadvertently or otherwise. This is why IT support departments have such strict rules about how users operate their computers. It's also why the people who manage and work in IT departments are often regarded as aggressive and authoritarian. But if a system goes down, it could cost an organization hundreds, maybe thousands, of dollars in lost revenue or productivity, and the IT department is ultimately responsible for mitigating such losses.

This is why the first part of this book has been devoted to helping prevent problems before they occur. It doesn't matter if you're reading this book to help fix problems with your PC at home or if you manage a corporate network with thousands of terminals, downtime costs in one way, shape, or form, be it in money or in frustration.

This brings us back to the user, the weakest part of any computer system's integrity. I say this because computers can only do things the way they are programmed to. A piece of software or hardware will do things the same way every time. Human beings, on the other hand, are unpredictable, driven by emotion, mood, and circumstance. To prevent issues, you have to be able to control the user, even if it's yourself!

How Windows 7 Controls Users

With every version of Windows up to and including Windows XP, users are, by default, administrators. This means they have complete control over everything in the operating system and can install programs and delete or move files without restriction. This is still the case with Windows 7, but User Account Control (UAC) adds a layer of protection.

Because of problems running legacy software in Windows, the full security afforded to other operating systems, such as Apple OS X and **Linux**, isn't possible. But Windows developers recognize that users may occasionally make changes to the operating system either unintentionally or without understanding the true repercussions. More importantly, Windows developers know that malicious software and viruses will want to do this too!

www.it-ebooks.info

UAC helps prevent inadvertent or malicious changes to critical system processes by putting a security layer between the user and any action that Windows determines could cause harm to or destabilize the operating system. In Figure 6-1 you can see that when UAC is activated by a questionable action, Windows 7 drops into a secure desktop where only the UAC dialog box is active and where only a user, not software, can make a selection.



Figure 6-1 The User Account Control dialog box

UAC is a useful but not a foolproof way to protect Windows 7 from attack. As comedy science fiction author Douglas Adams once famously said, "A common mistake people make when trying to design something completely foolproof is to underestimate the ingenuity of complete fools." While this observation fails to take into account the simple fact that many people are often bemused or confused by technology, it does apply to some degree to UAC. It's still too easy for a user to click Yes without reading or properly understanding the implications of making such a decision. What isn't helpful is that UAC messages are frequently unclear, and it can be difficult to determine what is trying to change what. Hopefully, this will change in the next edition of Windows due in 2012, but for now there is a potential weak link in Windows security that you should be aware of.

Managing User Accounts

There are a great many ways to manage users on a PC and to prevent anyone from installing unauthorized software, making unnecessary changes, and downloading and opening harmful files from the Internet. But managing user accounts can be a complex process. This section covers some ways to manage user accounts.

www.it-ebooks.info

Setting an Administrator Password

With UAC, a user can bypass security warnings by simply clicking through a dialog box. For better security on a multiuser desktop, you can set the main user as an administrator and all other users as standard users. Standard users have far fewer privileges to change Windows. They are even further restricted if you establish a password for the administrator account so nobody can click through a UAC dialog box without entering the password, as shown in Figure 6-2.

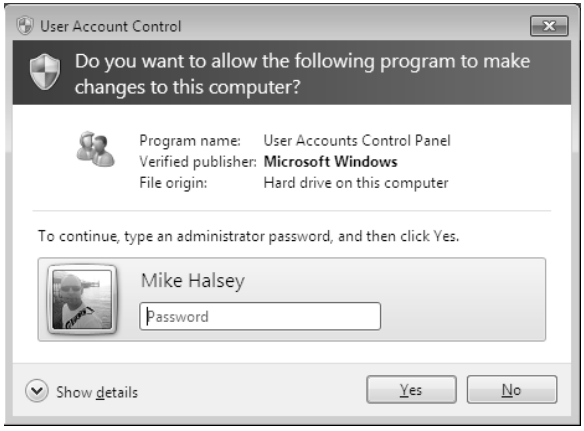


Figure 6-2 UAC controls with an administrator password set

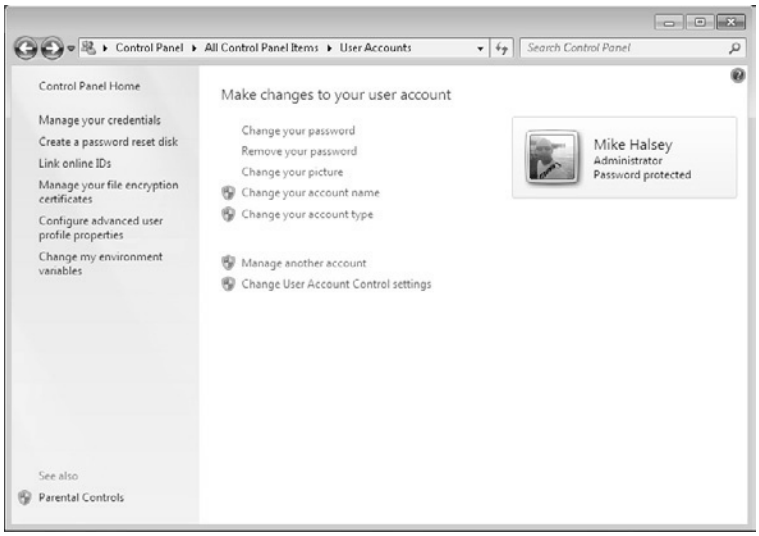
INSIDE OUT The pros and cons of setting an administrator password

On a multiuser PC, protecting the main administrator account with a password prevents other users from logging in as the administrator and upgrading their own accounts from standard users to administrators. But be aware that setting an administrator password can have a downside. Password protection for the administrator account prevents users from making even legitimate changes to Windows or other software that may be required.

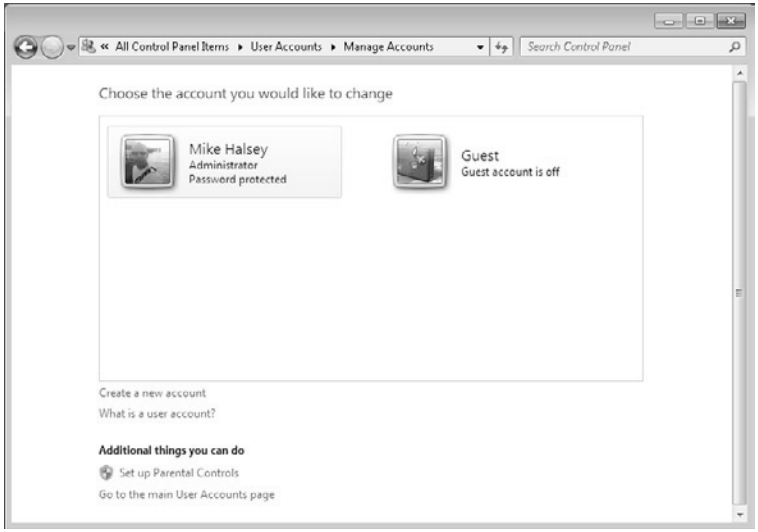
To set up additional user accounts on your PC, follow these simple instructions.

1. On the Start menu, click Control Panel, click Add Or Remove User Accounts in the User Accounts And Family Safety section, and then click Manage Another Account.

www.it-ebooks.info

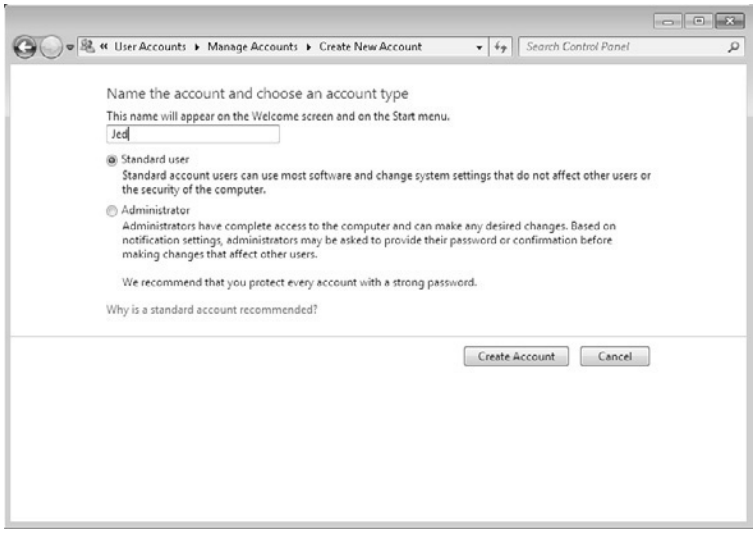


2. Click Create A New Account near the bottom of the window that appears.



3. Enter a name for the new user, select Standard User or Administrator, and then click Create Account.

www.it-ebooks.info



What Is the Guest Account?

In Chapter 3, "Basic Windows 7 Security," I wrote about Guest Mode, a potentially very useful feature that was dropped from the Windows 7 beta which rolls back changes made to Windows and your PC when a guest user logs off or shuts down the PC. The guest account setting in Windows 7 is not as useful, but it can prevent occasional visitors from making changes on your PC.

> **Note**
>
> **A guest account is simply an existing standard user account that can be switched on and off as needed. It should be noted that unless you have a password on your administrator account, anyone logged in as the guest user will be able to click Yes on UAC security prompts.**

www.it-ebooks.info

INSIDE OUT Can other users see your files?

By default, Windows 7 stores your files and data on the same hard disk or partition as your Windows 7 installation. In Chapter 1, "Prevention Is Better Than Cure" and Chapter 4, "Backup and Restore," I talked about how to move your files away from your Windows installation to secure them in the event of a catastrophe with Windows 7 itself.

Unfortunately, there's a downside to this when it comes to multiuser systems. When user files are located on the Windows drive, the operating system will hide them from other users. When you move those files to another disk or partition, they become visible to everyone.

Windows 7 does not come with a tool for hiding disks or partitions from specific users, but you can set individual user permissions on folders to deny access to other users. Also, there are many third-party tools and tips, most of them free, for hiding disks or partitions and user files.

Parental Controls

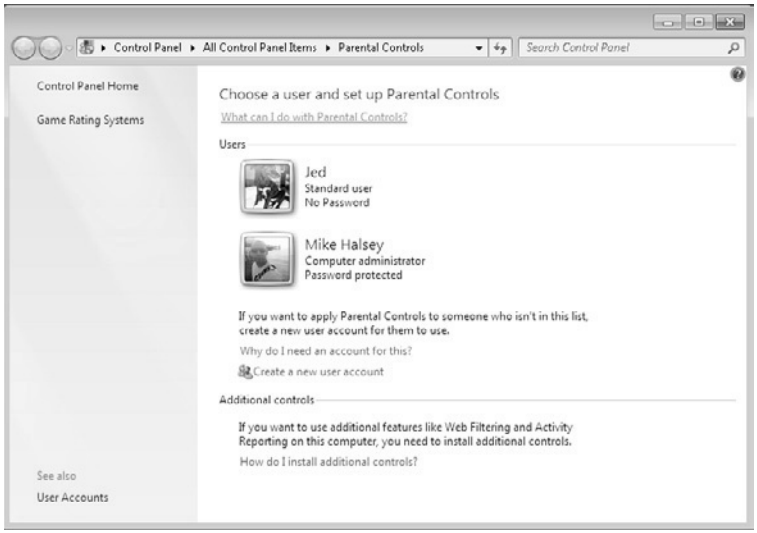
Parental Controls has many more uses than simply stopping your children from playing games late at night. It can also be used to limit access to certain software packages. You might, for instance, have some work-related software on your home PC that you don't want other users to access. Follow these steps to configure Parental Controls.

1. To access Parental Controls from the Start menu, click Control Panel, and then click Set Up Parental Controls For Any User. You can also access the feature by typing **parental** in the Start menu search box and selecting Parental Controls from the results that appear, as shown in the following figure.

www.it-ebooks.info

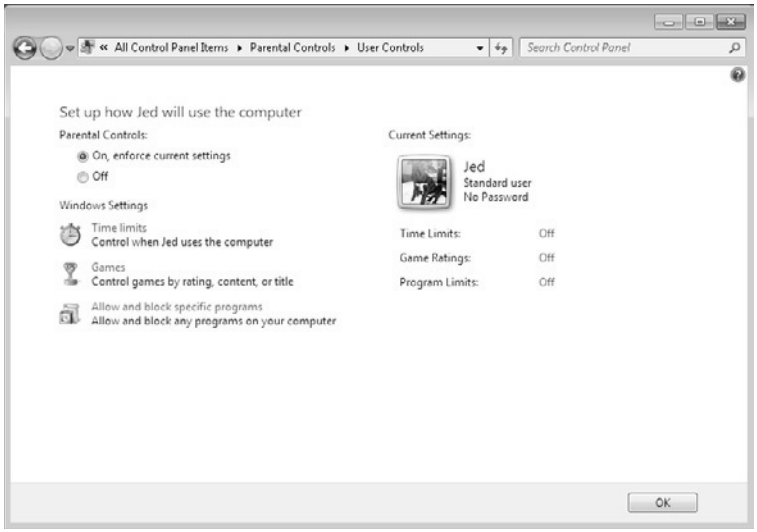


2. In the window that appears, select the user account you want to apply Parental Controls to.



3. Select On, Enforce Current Settings to turn on Parental Controls for this user, and adjust the settings as necessary.

www.it-ebooks.info



4. To control what a user can do on the PC, click Allow And Block Specific Programs and select the programs you want to block (see Figure 6-3).

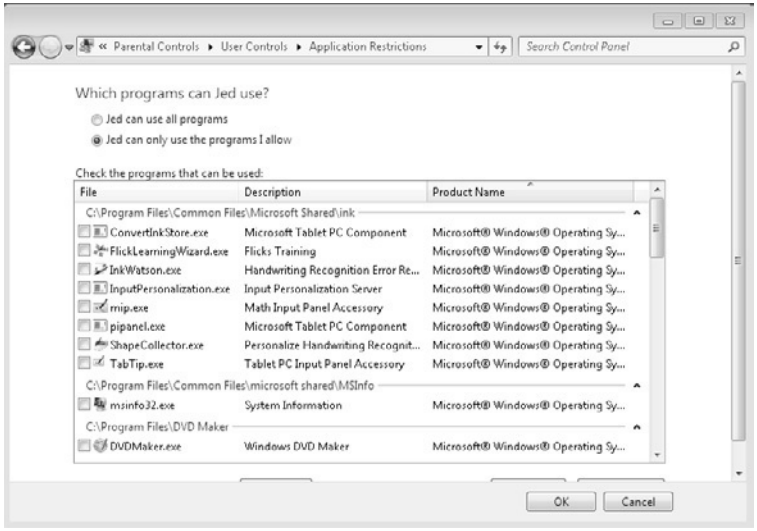


Figure 6-3 Using Parental Controls to stop standard users from accessing certain software

www.it-ebooks.info

What's Missing from Parental Controls?

Unfortunately, one of the most useful features you could add to Parental Controls, web filtering, is not included with Windows 7. This feature allows you to completely or temporarily block access to certain websites or groups of websites (for example, social networking or adult content sites). The software usually works from blacklists and whitelists maintained by third-party companies, with the PC administrator simply selecting which categories to block and when. There are plenty of web filtering packages available for Windows, including some free packages. Microsoft Live Essentials includes free, basic web filtering software.

Group Policies

The Windows tool called Group Policy Editor is used almost exclusively in business and corporate IT environments. It is accessed by typing **gpedit.msc** in the Start menu search box, as shown in Figure 6-4.



Figure 6-4 Accessing Group Policy Editor from the Start menu search box

The Group Policy Editor interface is split into two main sections: Computer Configuration and User Configuration (see Figure 6-5). Each of these sections is subdivided further into Software Settings, Windows Settings, and Administrative Templates.

- Computer Configuration covers settings for the entire PC. You will probably not want to change these unless, for example, you are turning off Windows Firewall or Windows Update in a corporate IT environment.

www.it-ebooks.info

- User Configuration covers the settings that apply to specific users. These will normally be specified remotely by a Windows Server configuration, but if you are changing these settings within Windows 7, you must do so on a per-user basis while logged in to that specific user account.

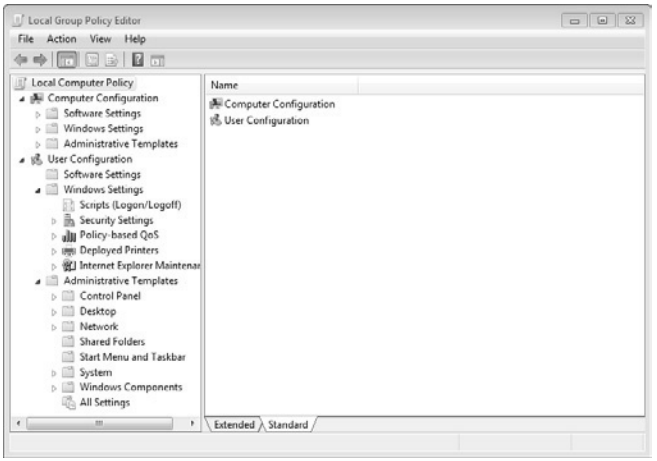


Figure 6-5 Group Policy Editor

It is unlikely that you will ever want to change settings in Group Policy Editor unless you are a system administrator on a company network. However, there might be circumstances where, to enhance security, you want to block user access to the Run command on the Start menu, deny user access to common Windows features such as Windows Media Player, or change the default Windows security level for opening email attachments.

Fortunately, all of the available options in Group Policy Editor are clearly labeled, and all include detailed descriptions of what happens when you edit them. This can help you understand how each selection will affect you and other users on your PC so you can make informed choices.

Local Security Policies

Another tool used almost exclusively in business and corporate IT environments is the Local Security Policy window, shown in Figure 6-6. You can access this tool by typing **security** in the Start menu search box and selecting Local Security Policy from the search results.

www.it-ebooks.info

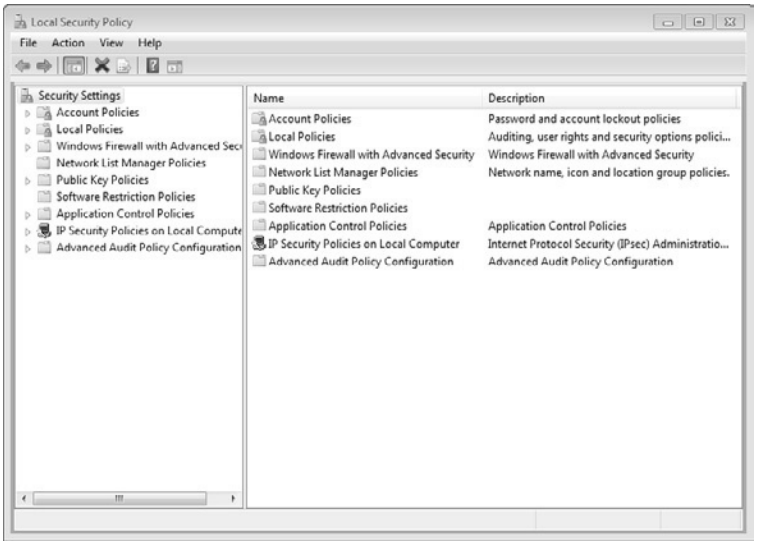


Figure 6-6 Local Security Policy Editor

There is very little that you would want to change in the Local Security Policy window. However, you can access two useful features.

- **Windows Firewall with Advanced Security** This is where you can set and configure specific rules to allow hardware or software through the Windows 7 firewall. This might include games or access to network storage.

- **Application Control Policies** If you have the Enterprise or Ultimate version of Windows 7, you have access to a feature called AppLocker. This feature lets you control what specific software can be installed on your PC, right down to the version number. This can prove useful for features like **graphics card** drivers for games and for some plug-ins, such as Adobe's Flash, that will work only with specific software versions. This feature allows you to block the installation of other versions of those pieces of software.

As with Group Policy Editor, all of the available options in the Local Security Policy Editor are clear and display detailed descriptions when you click their properties. This makes it easy to understand how each option will affect you and other users on the PC and helps you make informed choices.

Computer Management

More widely used in Windows is the **Computer Management** console, shown in Figure 6-7. This is a centralized location for a wide range of useful Windows 7 settings.

www.it-ebooks.info

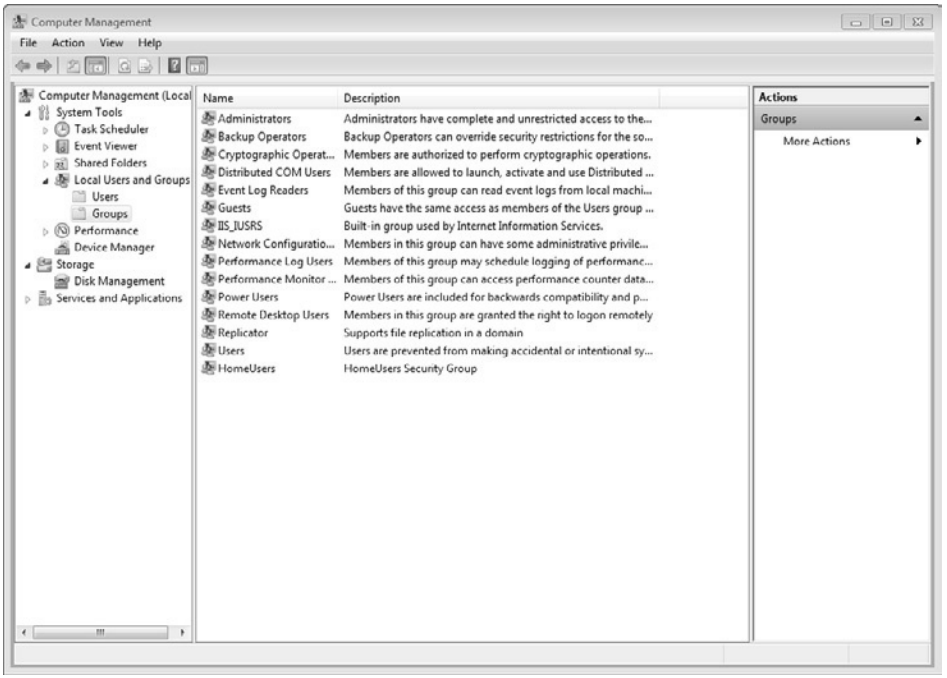


Figure 6-7 The Computer Management console

- **Task Scheduler** You might find that you want Windows 7 to run certain tasks, such as disk cleanup, on a set schedule. You can set any task or program to run on a schedule you define by clicking Task Scheduler in the Computer Management console.
- **Event Viewer** This is a useful tool for viewing error and other reports from the operating system.
- **Shared Folders** You can use Shared Folders to allow and deny access to folders that are shared between users on the same or across different PCs in a home network.

These and the other features in the Computer Management console will be discussed later in this book.

Blocking CDs, DVDs, Flash Drives, and External Hard Disks

One of the biggest security problems, certainly in the corporate space, is the use of external flash drives, CDs, DVDs, and external hard disks. If not carefully vetted, these media can transfer viruses and other malware onto a computer or be used to steal information.

www.it-ebooks.info

This is because, although computer equipment within an organization can be controlled using group and security policies, external hardware, especially personal flash drives, is not subject to the same rules and could also be used on a third-party or home PC with little or no virus and malware protection. You can use Group Policy Editor to deny access to these devices for specific users or for everyone (see Figure 6-8).

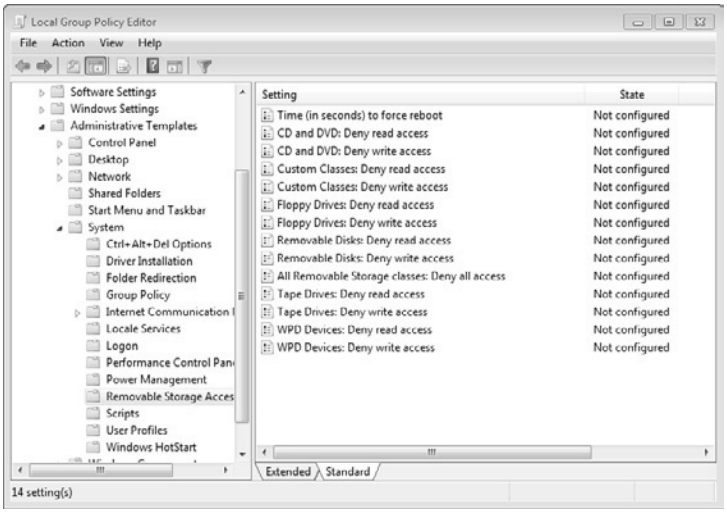


Figure 6-8 Blocking access to removable storage in Group Policy Editor

To access Group Policy Editor, type **gpedit.msc** in the Start menu search box. Find the relevant settings by clicking Administrative Templates, clicking System, and then clicking Removable Storage Access.

> **Note**
>
> **USB flash drives and external hard disks are classified as *removable disks*. To allow or deny access to a wide range of plug-in drives, right-click any of the settings, click Edit, and then click Disable to block access to the selected group of drives.**

Summary

The complex set of tools in Windows required to manage users, policies, and security is a good example of how a PC running Windows 7 is not a consumer electronics device. Windows 7 contains tens of millions of lines of code and is extremely complex.

www.it-ebooks.info

The weakest point in keeping Windows 7 running smoothly is clearly the user. It's unreasonable to assume that users will know what is good practice and what they should do. You only have to look at the rates of botnet and virus infections worldwide and the volumes of people who buy bogus products from spam emails to see that lack of education is at fault.

Users should be properly educated in good PC practice and in what is and isn't safe to do both **online** and **offline**. If you are an IT professional, you should always be patient with users you support, because any problems they cause are hardly ever intentional.

www.it-ebooks.info

CHAPTER 7

Hardware

What's in a PC? 93
How Can You Clean the Inside of Your PC? 98
Hardware Health. 99
SMART Monitoring of Hard Disks 100
Peripherals. 100
Surge Protectors, UPS, and Power Supply 102
Summary 102

Sometimes, when you ask someone to point at his PC, he'll point at the **monitor**. Some people need a visual interface, and, for these people, unless they have all-in-one devices, the screen *is* the computer. They often forget that the base unit is actually the brains and brawn of the computer, be it a big black box under a desk or components under a laptop keyboard.

Whatever the size or shape of your computer's components, there are many of them, and they all need care to ensure that they don't fail and leave you with a dead machine, unable to work or play. In this chapter, I'll talk about the hardware in your PC, what it does, what can go wrong with it, and how you can help prevent problems from occurring.

CAUTION!

You should always make sure you are grounded before working inside a PC to avoid static electricity from your hands shorting out sensitive components. You can do this by wearing an antistatic wristband, but I recommend leaving the PC plugged into the electric source while you remove the case (make sure the power is turned off) and touching your fingers to the power supply inside the case before unplugging the main power lead. This will ensure that the computer is properly grounded to prevent static electricity from damaging components.

What's in a PC?

Your PC is a mass of different components, and it's very rare to find any machine, be it a laptop or desktop, that has every component integrated onto a single board. What are these components, and what are the potential problems that can occur with them?

www.it-ebooks.info

Motherboard

The motherboard is where everything connects in your PC. All the other components plug into the motherboard, and chips and circuits on the board regulate all processes. There are generally no problems associated with motherboards, but some components (listed below) can cause problems.

Sockets

Sometimes it can be very difficult to push plugs into the sockets on a motherboard. Take care that the motherboard is properly supported when plugging cables and devices into it to avoid cracking the board.

One good thing about the sockets on motherboards is that each component has its own unique plug shape. This prevents users from inadvertently plugging a cable or device into the wrong socket and damaging the system.

BIOS

The Basic Input Output System (BIOS) is software on a chip that regulates the computer and gets it started. It initializes all the hardware and allows the software to communicate with it. BIOS checks the components for errors at startup, a process referred to as the POST (Power On Self-Test), and reports any issues either through warning lights or, more commonly, through a series of warning beeps. BIOS software is made by several companies, including AMI, Phoenix, and Award. The name and possibly the logo of the BIOS manufacturer appears when you start your PC.

Warning Beeps

There are many different beep codes, and the warning sounds they make will vary depending on your BIOS manufacturer and the manufacturer of your motherboard.

When you start your PC, it will sound one short beep to indicate that the POST has completed and all is well. If you hear combinations of short and long beeps, you should check the manual for your motherboard or the manufacturer's website for the cause.

> **Note**
>
> **A full list of BIOS beep codes is included in Appendix D, "BIOS Beep Codes." This list should not be considered definitive due to variations by manufacturer.**

www.it-ebooks.info

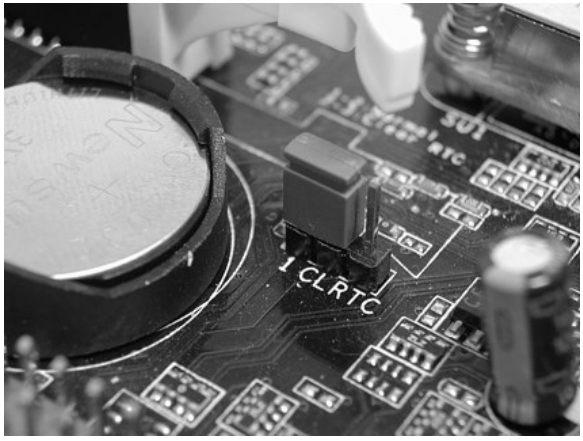
The BIOS beeps can give you clear information about where a fault or potential fault lies with your hardware.

Resetting the BIOS

The BIOS is a program stored on a chip (commonly referred to as ***firmware***) on the motherboard, and sometimes it can become corrupt. The BIOS can be reset to its factory default settings easily. You might need to do this if your PC cannot detect a specific piece of hardware, will not start, or sometimes when you install new hardware.

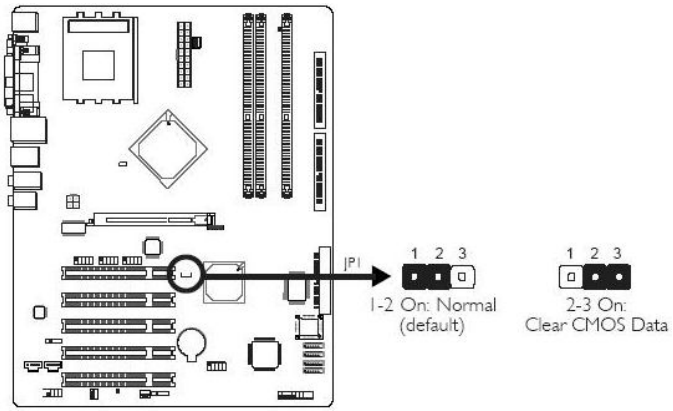
1. Make sure the PC is turned off and disconnected from the main power source. Ground yourself by touching an unpainted area on the PC case with your fingertips, using an anti-static wristband, if possible, and open the side of the PC to expose the motherboard, placing the PC on a level, firm surface.

2. Find the battery on the motherboard. It looks like (and, indeed, is) a large watch battery. Unclip the battery to remove it from the motherboard.



3. There will be a Clear CMOS jumper somewhere on the motherboard, close to the battery; check the motherboard manual for the exact location. The Clear CMOS jumper is a three pin socket with a small connector covering two of the pins (shown in the image following step 2). Remove the connector on the jumper and move it to cover the center pin and the uncovered pin. A small pair of tweezers is useful for doing this.

www.it-ebooks.info



4. Leave the jumper as described in step 3 for 10 seconds, and then move it back to its original position.

5. Replace the motherboard battery.

6. Reassemble the PC case, and reconnect it to the main power supply.

Northbridge and Southbridge

Two of the hottest components on the motherboard, and those that have their own heat sinks or fans, are the Northbridge and Southbridge chipsets. These regulate all the communications between components in the PC and, therefore, have a lot of work to do.

You should occasionally check that the heat sink or fan is free from dust and obstructions like stray wires or cables and that there is good airflow inside the computer.

As one of the hottest components, this chipset is also the most prone to failure. This is because the chip and all of its circuitry expand and contract as it heats and cools. Over a long period of time, this will cause physical wear and tear on the chip and will eventually be the cause of its demise. Fortunately, these chipsets are designed to operate under extremely hot conditions over a very long period of time and are extensively stress tested by the manufacturers.

Processor

The brain of your PC is the processor. The processor is the hottest component in the PC. It has its own heat sink and fan and might also be water cooled, although this is reserved for high-specification, gaming PCs and certain servers.

www.it-ebooks.info

You should check that the processor fan and heat sink are free from dust and obstructions such as wires and cables. You should also check that the PC has ample airflow inside the case.

Memory

Memory cards are thin cards approximately six inches long that protrude from the motherboard. They can be difficult to fit, so you should always make certain that the PC and motherboard are properly supported when placing or removing memory cards.

Memory cards are also very prone to damage from static electricity. When you touch them (or any component in your PC, for that matter), make sure you are grounded by touching an unpainted area on the PC (preferably by using an anti-static wristband) to avoid damaging the components with an electric shock.

Expansion Cards and Riser Cards

As with other components, it can be difficult to correctly place expansion cards and riser cards (mini expansion cards). Make sure that the PC is level and well supported, because the motherboard can snap under extreme pressure.

You should also make sure that expansion cards are correctly screwed in or otherwise secured to the inside of the PC case.

Graphics Cards

Graphics cards are another component that might have their own heat sink and/or fan. Make sure that these are free from dust and that there are no wires or cables causing an obstruction.

Graphics cards may also require their own power supply and will have a socket on the top of the card if this is the case. You should also check that there is a power cable connected to this socket and that the lead is not obstructing any fans.

Optical Drives and Hard Disks

Optical drives and hard disks are the only components, other than fans, that contain moving parts and, therefore, can suffer from wear and tear after extensive use.

www.it-ebooks.info

Power Supply

Although fans are the only moving parts of the power supply, they are some of the most common PC components to fail. It may be that the power supply fans work, but the power supply itself is no longer capable of providing enough electricity to power the computer. Fortunately, the power supply is one of the cheapest and easiest components to replace.

The PC Case

The case for your PC can contain several fans that can be blocked by dust and carpet fibers. Other moving parts in the case might fail, including the power button, which can stick or break.

How Can You Clean the Inside of Your PC?

The best way to clean the inside of a PC case is with a good, strong puff of breath, but you can also use a vacuum cleaner to clean dust from inside. Another good tool for cleaning dust inside your computer is a small, unused paintbrush.

You should always be very careful when using a vacuum inside your PC. The computer should be turned off and disconnected from the main power supply. The PC should be on a firm and level surface. You should use a small attachment on the end of the vacuum with a soft brush, and the suction power on the vacuum should be turned to the lowest level.

Carefully vacuuming the inside of your PC, including all fans and heat sinks, can extend its life and reduce heat buildup and power consumption.

When performing these actions, always be careful to avoid touching components inside the PC case or knocking cables from their housings. If you can use a small, battery-powered vacuum, you are less likely to cause any damage.

INSIDE OUT Where should you keep your PC?

Keeping your computer on or near a carpet can attract dust and carpet fibers. Your computer can also attract dust if you keep it on a laminate or tiled floor.

A good location for a main PC case is on a raised platform at least six inches off the floor or on a desk. These locations will help minimize the buildup of dust and other particles that may be drawn in by the fans and reduce the risk of static electricity buildup.

www.it-ebooks.info

Hardware Health

Different types of computers can require different care. This section covers the three main types of hardware, although these types also vary by manufacturer.

INSIDE OUT Turn off your PC when cleaning your room

If you are dusting or vacuuming the room where your computer is set up, it is a good idea to turn off the computer because the case fans can draw in any dust that is thrown up by the vacuum.

Desktops

For PCs where the monitor is separate from the base unit, you can usually open the side of the PC via an access panel (although for very small form factor computers this may not be possible). The components are usually accessible for a good blast of air to remove dust and other debris that can find its way inside, and you can carefully open the computer without causing any damage.

Laptops

Laptop and notebook computers use many different components than desktop PCs do, and they are often fixed permanently to the motherboard. There is usually an access port or two on the underside of the laptop you can open to upgrade and change components like the memory and hard disk, but otherwise you should not attempt to open a laptop case for cleaning or maintenance. If you need to clean dust from the computer, you can carefully place a vacuum against the heat vents on the sides of the laptop and use low to medium suction.

All-in-Ones

All-in-one PCs, a desktop machine where the computer and monitor are built into the same housing unit, share many similarities with laptops and, accordingly, you should not attempt to open them for cleaning or maintenance. You can clean dust from the vents in the same way as described for laptops in the previous section.

www.it-ebooks.info

SMART Monitoring of Hard Disks

Most motherboard BIOS software (shown in Figure 7-1) supports a feature called Self-Monitoring, Analysis, and Reporting Technology, or SMART, monitoring of hard disks. SMART monitoring reports hard disk reliability indicators to the BIOS with the aim of anticipating any disk failure before it occurs. The benefit of SMART monitoring is that it allows a user to move any data and files off the disk before it fails.

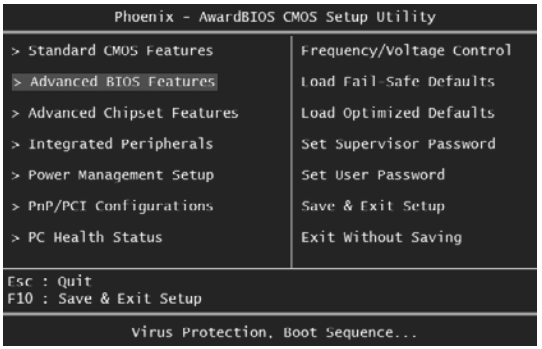


Figure 7-1 An example BIOS screen on a PC

The SMART monitoring feature may be turned off for your hard disks in your computer's BIOS. You can normally access the BIOS when starting the machine by pressing F2 or Delete on your keyboard. The exact location of the SMART monitoring utility varies depending on your BIOS. You should consult your motherboard manual to determine if this feature is supported and where you can find it.

Peripherals

Without peripherals, keyboards, mice, and so on, your computer would simply sit in a corner, whirring all day. These important devices also need care and attention to prevent them from causing trouble.

Keyboards and Mice

A commonly reported Windows problem is "my keyboard and/or mouse won't work." Is this problem due to a fault with the hardware driver for the device, or with the hardware itself, or is it just because the hardware is dirty?

It's good practice to keep your keyboard clean by using a small brush to sweep between the keys. Keep your mouse clean by occasional wiping it with a dry cloth or cotton ball. If your mouse contains a ball, pop out the ball, and clean the rollers it runs against.

www.it-ebooks.info

CAUTION!

While I was providing second-line IT support a few years ago, a client from a major British bank was talking on the phone with a colleague of mine about his keyboard. He'd decided it was dirty and needed to be cleaned.

The night before, he'd filled his sink with hot, soapy water and given the keyboard a good scrub. Realizing it was an electrical device, he hung it up to dry overnight, but was concerned when his computer didn't work the following morning.

My colleague had to break the bad news that the reason his keyboard didn't work was because it was built into the rest of his laptop!

Monitors

Probably the least problematic piece of hardware on your PC is the monitor. If a problem does occur, such as there is no display, the source of the issue is often caused by something easy to fix such as one of the following.

- The power cable has fallen out of the monitor.
- The video cable is not properly attached to the monitor.
- The monitor has accidentally been switched to a different video input.

Other Devices

You may need to troubleshoot other device problems when a specific device refuses to function or because Windows can't see that device. A useful method for troubleshooting such devices is to test the device by plugging it into another port on your PC, into a USB, for example. If that doesn't work, try the device with a different connecting cable.

INSIDE OUT The Wi-Fi USB dongle won't work

After moving a computer, some people find that their Wi-Fi USB dongle won't connect them to the Internet. Because of the way Windows loads drivers for hardware, you might find that it's just because the dongle is plugged into a different USB port than it was before. Usually, changing to a different USB port on the PC solves the problem.

www.it-ebooks.info

Surge Protectors, UPS, and Power Supply

Your PC should always be plugged into a spike or surge protector. This will stop any sudden spikes in the power supply from passing through your computer and damaging sensitive components. Some surge protectors also protect computer components such as network and telephone cabling. Most uninterruptable power supplies (UPS) have this feature built in. These devices can maintain your electricity supply in the event of a power drop or brownout.

I also recommend that you do not plug your PC into the same outlet as any appliance. Some large appliances, such as refrigerators, can cause spikes in the power supply, which can disrupt other electrical devices. For instance, in an older house, sometimes the lights flicker when the cooling element in a refrigerator or freezer comes on.

Summary

A PC is a complex set of assorted components, some of which include components that are incredibly tiny and are measured in nanometers. Consequently, these components are very susceptible to electrical fluctuations and heat.

It's important to keep your PC clean and protected from electrical and heat damage. Performing a few simple actions now and again can greatly increase the lifespan of a computer.

www.it-ebooks.info

CHAPTER 8

Virtualization

Virtualization vs. Dual Booting. 104
Are There Any Benefits to Virtualization? 105
Virtual Hard Disks and Windows 7 105
Windows Virtual PC and Windows XP Mode. 115
Summary 118

As computers and processors become more powerful, they're able to do more tasks simultaneously. The advent of multi-core processors made this even easier, and now virtualization is everywhere.

But what is it? Virtualization is an operating system running on software-based, emulated hardware and sharing the same hardware. To do this, the host operating system shares the computer's resources between the different virtual machines (VMs). This includes isolating areas of memory for each VM and, in the case of a multi-core processor, sometimes even assigning a specific processor core to each VM. Each VM then has its own hardware resources and can operate at near the full speed of the computer.

Where does each VM sit? Each VM exists within a file on your hard drive, a bit like a compressed zip folder. The operating system sees this file as a hard disk and runs perfectly from within it.

Using VMs at home or at work affords many advantages. For example, if your copy of Windows 7 fails, the downtime can be long and frustrating. Even if you have a backup image of that copy of Windows, you'll be completely offline for a while until you restore it. If you are running Windows on a VM, however, you simply log into the master operating system and replace the VM file with a clean backup copy. Essentially, all you do is copy or rename a single file, and you're still able to get things done on your PC while the VM is being restored.

Another advantage of using VMs is that you only need a single PC or server to run different operating systems and tasks simultaneously. This can reduce a whole bank of servers to just a single computer. The effect this has on your electricity consumption and your carbon footprint can be enormous, not to mention the impact it has on your IT costs.

All of this is made possible because modern processors and computers are almost never used to their full potential by everyday computing and server tasks. Why have five computers using only 20 percent of their computing power but consuming 80 percent of their maximum electricity consumption when you can have a single machine running full out?

www.it-ebooks.info

Virtualization vs. Dual Booting

To dual boot a computer, you must have different operating systems installed on different hard disks or partitions. This is how Boot Camp manages Windows and OS X on an Apple Mac. The disadvantages of dual booting are twofold. First, if the boot sector or boot menu of the computer changes, you might lose access to one of the operating systems, because **Startup Repair** might not rebuild entries correctly for non-Windows operating systems, and those operating systems might not be able to write to the Windows boot loader.

Second, if you want to switch from one operating system to another, you have to close all of your programs, shut down the machine, and then restart it.

Virtualization allows you to run different operating systems side by side on your Windows desktop or full screen and makes it easy to switch between them. Furthermore, you still have only one operating system in your Windows boot loader (unless you choose to boot from a virtual hard disk, but more on this later in the chapter).

Also, VMs are very easy to back up. They are just files (think of a really large **zip file**) that can be copied from one place to another when the VM isn't running. This makes them considerably simpler to back up and restore than operating systems installed on a separate hard disk or partition.

While you can dual boot between Windows and other operating systems, such as Linux, there are limitations on the order in which you can install these operating systems. This is because Microsoft changed the boot loader with Windows Vista to make it much more secure. Many other operating systems use a different, older style of boot loader. This means Windows 7 should always be the last operating system you install because, although it can incorporate the other operating boot loaders into itself, not all operating systems can incorporate the Windows 7 boot loader into themselves. Windows 7 wouldn't be able to start if a non–Windows 7 boot loader has overwritten the Windows 7 boot loader.

Virtualization gets around this problem by running all of the operating systems from within Windows 7. You can install any other version of Windows or Linux using Windows Virtual PC. Apple Mac OS X isn't supported, but you can get third-party virtualization packages such as VirtualBox and VMWare, which may support a wider range of operating systems.

www.it-ebooks.info

Are There Any Benefits to Virtualization?

Virtualization offers significant benefits, one of which is booting into a virtual copy of Windows 7 to keep your main copy clean, protected, and running smoothly. I will detail this later in this section.

Two other benefits of virtualization are software and hardware compatibility. You may, for instance, like to use an older printer or **scanner** that isn't supported with Windows 7 drivers. If there's nothing wrong with the hardware, you could use virtualization to install an earlier operating system with drivers that support the hardware and install the hardware into that virtualized operating system instead.

Similarly, you might require the use of software that won't run in Windows 7, maybe a Linux application that won't run even in Windows XP Mode. You can use virtualization to create safe test computers into which you can install and test new software, updates, security updates, and hardware. This is becoming common practice in environments where system administrators want to know what impact an update or new software package will have on the organization's PCs.

Virtual Hard Disks and Windows 7

With Windows 7, support for **virtual hard disks** (VHD) is built into the operating system for the first time. A VHD is different from a VM but can be used like a VM. Let me explain.

In its basic form, a VHD is simply a file that you can "attach" to a copy of Windows 7 so that it appears in Windows Explorer as another hard disk. You can store any type of file or data on a VHD just as you can a regular hard disk.

Creating a VHD in Windows 7

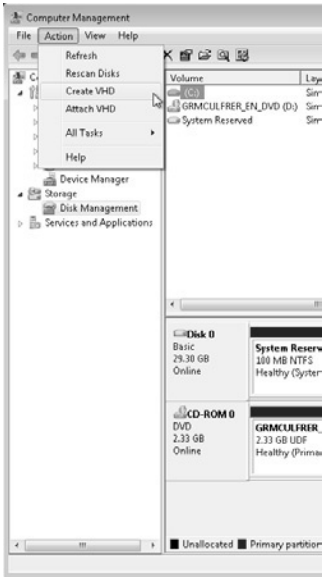
To create a VHD in Windows 7, follow these steps.

1. Open Computer Management by typing **computer** in the Start menu search box and selecting Computer Management from the results that appear.

2. In Computer Management, select Disk Management from the panel on the left.

www.it-ebooks.info

3. On the Action menu, select Create VHD.

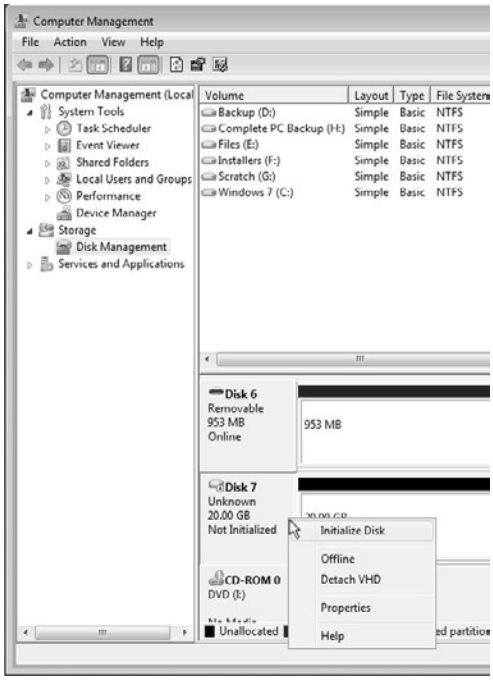


4. You will need to select where on your hard disk(s) the VHD file will go, what it will be called, and how big it will be. You can choose whether the file is dynamically expanding or of a fixed size. The first option doesn't create the full size file but expands it as files are added to it until it reaches its maximum size. This can be useful if hard disk space is short. The recommended option is to create the full size file to begin with.

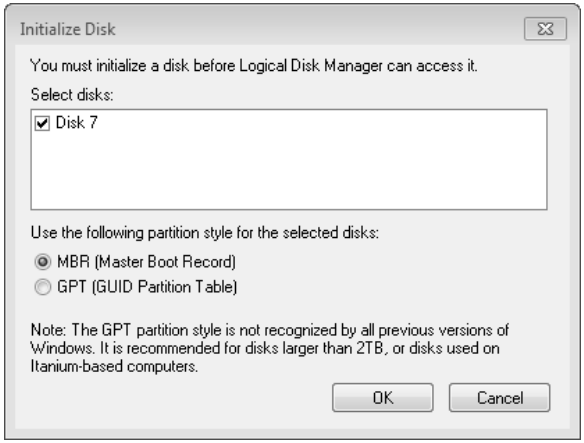


www.it-ebooks.info

5. The new VHD appears in the list of available disks in the Disk Management console. You need to initialize this disk, which you can do by right-clicking its information panel (to the left of the black, disk size block) and selecting Initialize Disk.

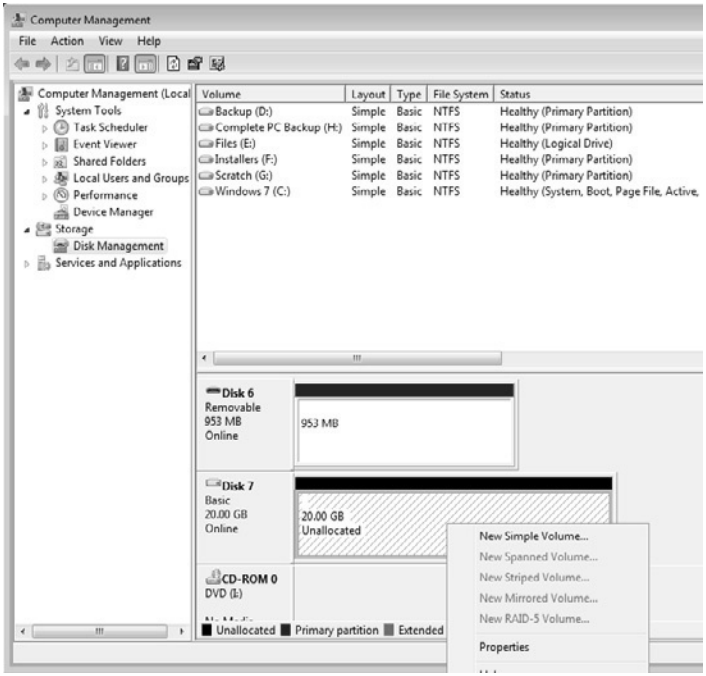


6. Select a partition style for the disk (I recommend MBR), and click OK.

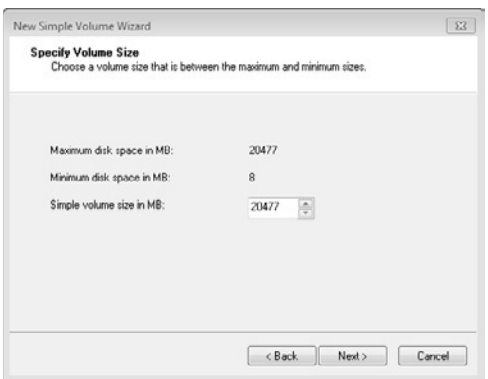


www.it-ebooks.info

7. You next need to place a partition on the VHD so you can write files to it. To do this, right-click the VHD in the Disk Management Console, and select New Simple Volume.

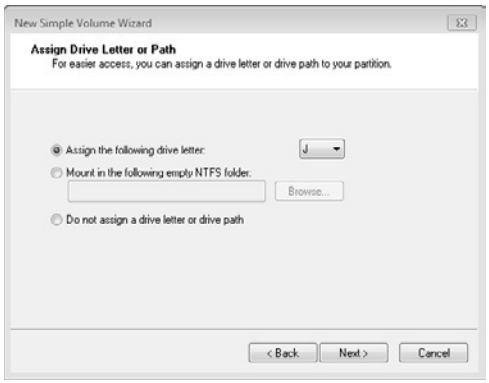


8. You will be asked to select a size for the volume. For a VHD, you should use the default (maximum) size available.



www.it-ebooks.info

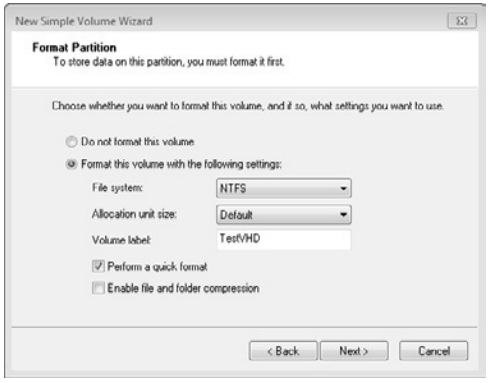
9. You can either assign a **drive letter** for the VHD or have it mounted automatically as a subfolder onto another drive. You can also choose not to associate a drive letter with a disk or partition, although this will prevent it from appearing in Windows Explorer views.



10. Finally, give the VHD a name (Volume Label), and format it using either a quick or standard format. I recommend the NTFS file structure.

Note

NTFS (New Technology File System) is a disk file system that Microsoft first introduced with Windows NT and has since refined. It is more stable and reliable than other formats, including FAT (File Allocation Table), and it supports larger drives than FAT or FAT32 drives as well. It also supports, and is required for, the folder and disk encryption technologies in Windows 7.



www.it-ebooks.info

Reattaching the VHD

You will probably need to reattach the VHD you created in the previous section the next time you start Windows. This is normal behavior for Windows 7. If you want to automatically reattach a VHD whenever Windows 7 starts, you can set this up as a task in the Task Scheduler. See Chapter 25, "Advanced Windows Diagnostic Tools in Depth," for details about how to use this feature.

To attach a VHD, follow these steps.

1. Access the Computer Management console by typing **computer** in the Start menu search box and selecting Computer Management from the results that appear. Select Disk Management from the left pane of the Computer Management console.

2. On the Action menu, select Attach VHD.



3. Select the VHD file from the location where it is stored on your PC. It appears as a drive in Windows Explorer.



Booting From a Virtual Copy of Windows 7

With the Enterprise and Ultimate editions of Windows 7, it's possible to install another copy of Windows 7 inside a VHD and boot from it. You can find an official guide to creating a bootable VHD by searching for **Demonstration: Windows 7 VHD Boot** at *www.microsoft.com*, but this method is very complex. There is actually a much simpler way to do it.

www.it-ebooks.info

Creating a bootable VHD is an excellent way to keep your main copy of Windows 7 clean and problem free. Quite simply, in this scenario, you'll never use it except for making back-ups of the VHD and restoring it if you need to. This also allows you to have a multi-boot environment on your PC that's easier to manage than a traditional dual-boot system.

INSIDE OUT Licensing and booting Windows 7 from a VHD

Note that if you want to install a copy of Windows 7 on a VHD, you will need an additional valid product key for that extra copy of Windows 7.

Also, you can use only the Enterprise and Ultimate editions of Windows 7 to boot from a VHD. You cannot use this feature to install another, earlier version of Windows (such as Windows XP or Windows Vista) or another edition of Windows 7 (such as Starter, Home Premium, and so on) on the VHD.

INSIDE OUT Breaking the 32-bit barrier with bootable VHDs

Windows Virtual PC and Windows XP Mode support only the 32-bit (x86) editions of Windows and other operating systems. Creating a bootable VHD allows you to install a 64-bit (x64) version of Windows 7. This is something you would want to consider if your PC has more than 4 GB of RAM so that Windows will be able to see all of your installed memory.

To install Windows 7 on a VHD, follow these steps.

1. Boot your PC from your Windows 7 installation DVD.

> **Note**
> **You cannot install Windows 7 this way from within a currently loaded copy of Windows 7. You have to start your PC from the installation disc.**

2. Select your installation language.

www.it-ebooks.info

3. At the install screen, press Shift+F10 to open the DOS command window.

4. Type **diskpart** and press Enter.

Using an Existing VHD

To use an existing VHD, follow these steps.

1. Type **Select vdisk file=C:\path1\path2\disk.vhd**, substituting the drive letter and paths where the VHD is stored on your computer as necessary.

2. Type **attach vdisk**.

Creating a New VHD

To create a new VHD, follow these steps.

1. Type **Create vdisk file=C:\path1\path2\disk.vhd maximum=20000 type=fixed**, substituting the drive letter and the paths indicating where you want the VHD stored on your hard disk. The 20000 in the example here would create a VHD of 20 GB, so for a 15-GB VHD, type **15000**. Note that these numbers are not precise calculations of 15 GB and 20 GB but are rounded here for clarity.

2. Type **select vdisk file=C:\path1\path2\disk.vhd**.

3. Type **attach vdisk**.

INSIDE OUT Fixed vs. expandable VHD files

When you create a VHD file, you can make it a fixed size or expandable. This latter option will create a small file that the copy of Windows 7 on the VHD can expand as needed up to its maximum size.

The downside is that if you run short of available disk space on the drive where the VHD file is located, the copy of Windows 7 in the VHD may report errors when it cannot access disk space that it sees as being available to it.

4. Type **exit** and press Enter.

www.it-ebooks.info

5. Type **exit** again and press Enter.

6. Click Install and then select a Custom (Advanced) install.

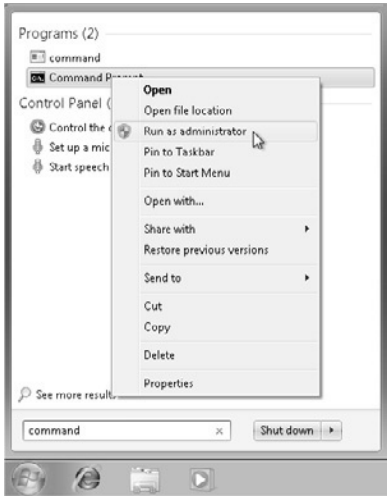
7. In the panel where you indicate which hard disk to install Windows 7 on, the hard disks in your computer are normally referred to as Disk 0 or Disk 1. The VHD will have a different disk number and will stand out. You will probably find it at the bottom of the list of available drives. Click the VHD and select Drive Options (Advanced).

8. Create a new partition in the space available for the partition by clicking New and selecting its size, then format this new drive.

9. Make sure the VHD drive is highlighted, and then click Next to install Windows 7 on it.

Windows 7 will install and automatically configure the boot loader; however, you will now have two copies of Windows 7 to choose from when you start your PC. Follow these steps to change the names of the programs after either copy of Windows starts.

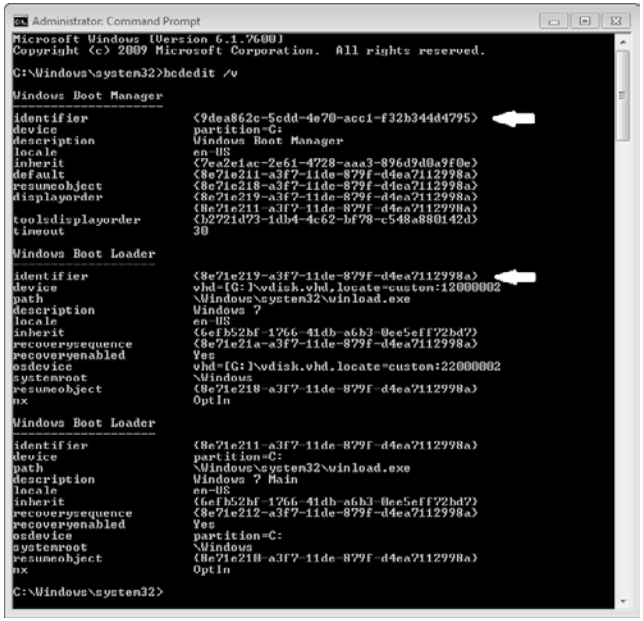
1. Type **command** in the Start menu search box, and when Command Prompt appears in the results, right-click it and select Run As Administrator. Click Yes through the UAC security alert.



2. In the command window that appears, type **bcdedit/v**, and then click Enter.

www.it-ebooks.info

3. Locate the VHD copy of Windows 7 in the list. It will be associated with a Globally Unique Identifier (GUID), a long string of numbers and letters.



In the example above, there are two entries listed in the Windows Boot Manager section: one for the main copy of Windows 7 and one for the VHD copy. The GUID of the VHD in this example is 8e71e219-a3f7-11de-879f-d4ea7112998a, and it is identified as VHD=[G:]\vdisk.vhd.

4. Type **bcdedit /set {GUID} description "Windows 7 VHD"**.

INSIDE OUT Cutting and pasting in a Command Prompt window

You can select text in a Command Prompt window by right-clicking anywhere in the window and selecting Mark. Move the insertion point to the beginning of the text you want to select, and press and hold the Shift key while you select the text. Now press CTRL+C to copy the text.

To paste this text, right-click in the window and select Paste. This can be very helpful when writing long GUIDs.

www.it-ebooks.info

5. Optionally, you may want your VHD copy of Windows 7 to be the operating system that loads by default when you start your PC. To do this with any of the entries listed, type **bcdedit /default {GUID}**.

INSIDE OUT Why boot your PC from a VHD?

The primary reason to boot your PC from a VHD is to protect your main copy of Windows 7. When you boot from a VHD, you can use the full features of your PC and still be able to restore it if something goes wrong simply by booting into your *original* copy of Windows 7 and restoring the VHD file from a backup. Restoring your operating system takes no longer than the time required to reboot Windows 7 a couple of times and rename a file.

Your VHD copy of Windows 7 will be able to see all of your hard disks and all of your hardware. There will be no way of knowing that you are actually running a VM. This can be very useful in organizations where getting up and running quickly after a crash and preventing people from damaging a copy of Windows 7 is paramount.

Windows Virtual PC and Windows XP Mode

The ability to boot from a VHD is useful in some situations, but it won't let you run several operating systems side by side on your Windows 7 desktop. For this purpose, there's Windows Virtual PC and Windows XP Mode. They are not shipped with or integrated into Windows 7, but both tools can be downloaded for free from Microsoft at *www.microsoft.com/windows/virtual-pc*.

I covered Windows XP Mode at some length in Chapter 2, "The Basic Windows 7 Utilities," and Chapter 3, "Basic Windows 7 Security," so I won't repeat all of that information here. Windows Virtual PC is a component that comes with Windows XP Mode and allows you to install other versions of Windows and other operating systems, such as Linux, that can run in a window on your Windows 7 desktop or full screen. This is helpful when you want to run software separately to protect your main operating system, perhaps for testing purposes.

For software that is incompatible with Windows 7, you can install it in Windows XP Mode. With this feature, you can see all of your computer's files and hard disks and have access to all of your hardware, including USB devices. Windows Virtual PC is more limited and cannot, by default, see these.

www.it-ebooks.info

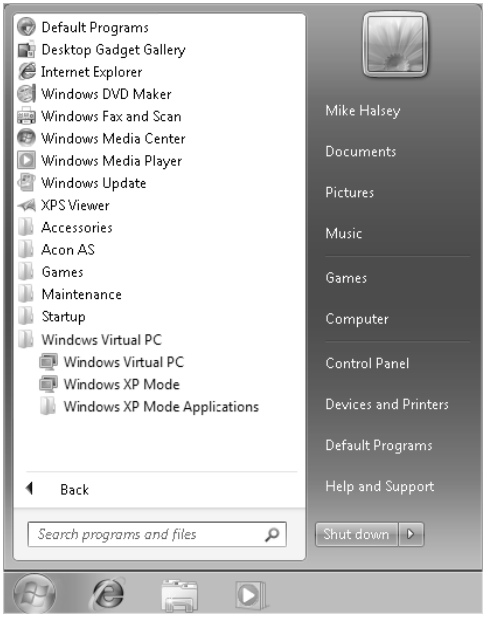
Installing Another Operating System in Windows Virtual PC

You can also install other operating systems in Windows Virtual PC. These include earlier versions of Windows and different versions of Linux. This can be useful for running different operating systems side by side if, as I mentioned at the beginning of the chapter, you have older hardware for which there is no compatible Windows driver or if you like using software in another operating system.

The first step in installing another operating system in Windows Virtual PC is creating a container into which you can install the guest operating system and telling Windows 7 what hardware resources (such as memory) it should be allowed.

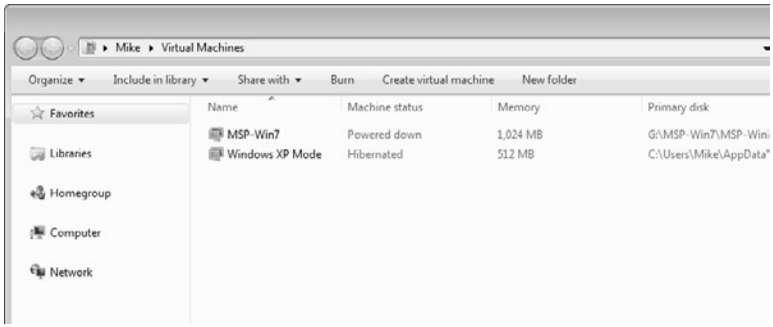
To install another operating system in Windows Virtual PC from the Start menu, follow these steps.

1. Click Windows Virtual PC, and then click Windows Virtual PC again.



2. In the window that appears, you have some options along the blue toolbar near the top of the window. Click Create Virtual Machine. Installing an operating system into a VM here is very similar to creating a VHD in Windows 7 as detailed earlier in the chapter.

www.it-ebooks.info



To launch the operating system after it is installed, you will need to launch it from within the Virtual PC Management console. Note that any programs you install in Windows Virtual PC will *not* appear in your Windows 7 Start menu as they do when you use Windows XP Mode. You will also need a valid product key and license for any operating system you install.

Once this window loads, you will see that it has its own BIOS and will appear, for all intents and purposes, to be a full PC running inside Windows on your computer. In the Settings options, accessed on the Tools menu at the top of the window, you can give the VM control of your optical drive or attach an ISO (disc image) file as a disk. You can install your guest operating system from this ISO file. You do this in the DVD Drive section of the Settings options.

Other options on the Settings panel control permissions and resources for the VM.

CAUTION!

It's important to remember that the version of Windows XP in Windows XP Mode and any operating system you install in Windows Virtual PC will need to have its own anti-virus and anti-malware software installed. You will need to make sure it is updated using its own Windows Update rather than relying on Windows Update for your copy of Windows 7. Failure to do this could result in your files, data, and your copy of Windows 7 being vulnerable to attack and virus infection.

www.it-ebooks.info

Summary

In the right circumstances, there are great benefits to be gained from using virtual machines, perhaps even as your main operating environment. There's a great deal they can offer you, from maintaining hardware and software compatibility to providing safe test environments. They can also have a significant role in reducing the number and types of problems that you might experience with your PC.

The good news is even the least expensive modern PC is capable of running at least two operating systems side by side. Plus, using virtualization can significantly cut your electricity consumption. Virtualization is definitely the way forward in more ways than one.

www.it-ebooks.info

PART 2

Quick Fixes

CHAPTER 9
Annoyances 121

CHAPTER 10
Viruses, Malware, and Other Threats 137

CHAPTER 11
Easy Ways to Fix Windows 7 163

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 9

Annoyances

Common Windows 7 Problems 121
Hardware Annoyances 134
Summary 136

Windows 7 and your PC can be annoying! As much as we'd all like them to be, and for as much effort as Microsoft puts into it, your PC is still not a consumer electronics device. Despite the best efforts of enthusiastic sales staff in your local computer store, reassuring you that you can simply take home a PC loaded with Windows 7, plug it in, and use it happily for years, you can't.

The problem is that Windows 7 has to be everything to everybody. It has to support older legacy software and hardware as well as incorporate the very latest software and hardware standards. It has to be easy to use for novices but powerful enough for system administrators. And it must bring all of this together in a way that's stable, solid, and dependable.

Despite all of the challenges, Microsoft has done an admirable job developing Windows 7, but annoyances still occur. Most of the problems people encounter with Windows are relatively minor. In this chapter, you'll learn to deal with the issues that you may come across.

Common Windows 7 Problems

As I've already said, Windows 7 has to be all things to all people, which makes the system extremely complex and creates, inevitably, a huge ecosystem of help, support, and training businesses and resources, including this book. This chapter focuses on annoyances that you can troubleshoot to fix or repair. These annoyances appear in no particular order.

You Don't Have Permission to Write Files to a Disk

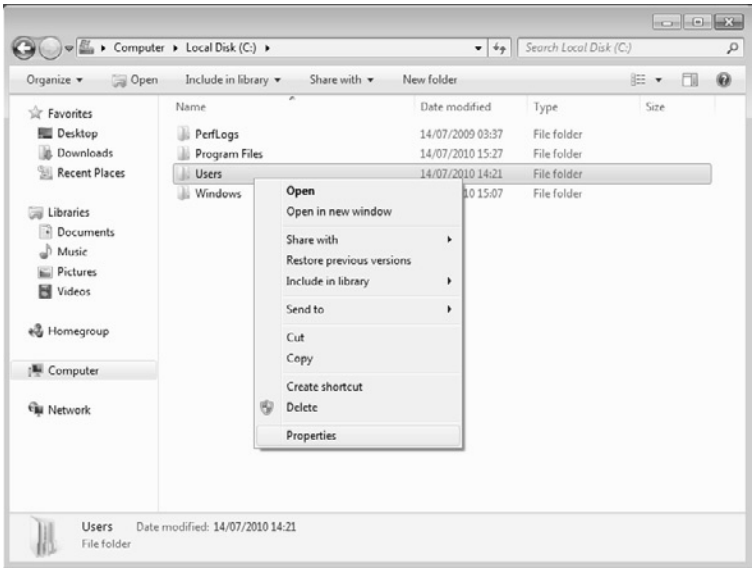
One of the things I recommend most often is keeping your files and data on a separate hard disk or partition from Windows 7 (see Chapters 1 through 4). Keeping Windows 7 and your files on separate disks or partitions means that if something catastrophic happens with Windows 7 and it needs to be reinstalled from scratch, you don't lose any data.

However, sometimes doing this leaves you in a position where you suddenly can't write files to the disk where you have moved your items. Although the files probably transferred with no problem, you suddenly start receiving Windows messages indicating that you don't have permission to write to the disk when you try to save a new file.

www.it-ebooks.info

This commonly happens after upgrading to Windows 7 from a previous version such as Windows XP or Windows Vista. If this is the case, the previous operating system has set permissions for the disk and files. To correct the problem, you must reset those permissions for your copy of Windows 7.

1. Right-click the folder or drive you want to set new permissions for, and select Properties.

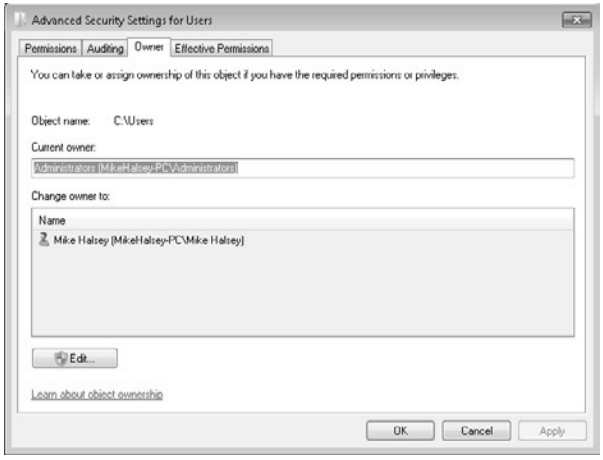


2. On the Security tab, click Advanced.

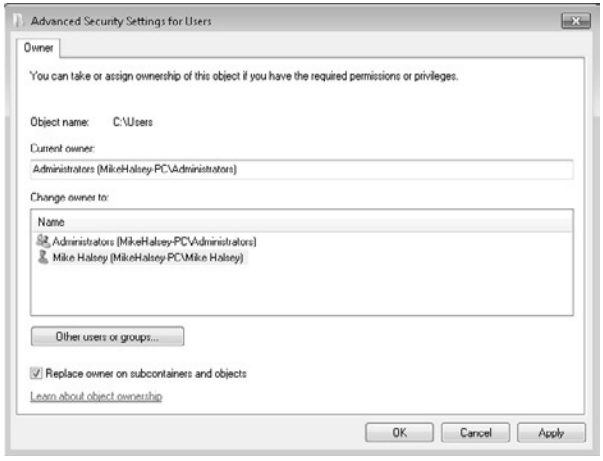


www.it-ebooks.info

3. In the dialog box that appears, on the Owner tab, click Edit.



4. Next, select the user whom you want to take ownership of the folder or drive. Select the Replace Owner On Subcontainers And Objects check box, click Apply, and then click OK twice.

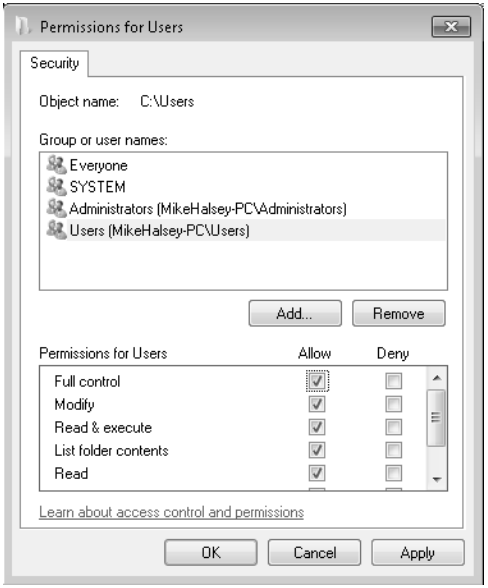


www.it-ebooks.info

5. In the User Properties dialog box, make sure the Security tab is active, and click Edit.



6. In the Permissions For Users dialog box, select the user you want to have control of the disk or folder. Under Allow, select the check box next to Full Control, and then click Apply.



It could take some time to set permissions for all your files; don't click Cancel in the progress window that appears.

www.it-ebooks.info

INSIDE OUT Setting permissions on single user PCs

If you are the only user on your PC, you may only have to follow steps 5 and 6 to reassign full control of a disk to your account.

You will now have full read and write control of the disk or folder in which your files are located.

You Can't See Your New Wi-Fi Network

If you have a new **broadband** router that's already been configured using another PC, or if you are connecting to a router for the first time via Wi-Fi, you may find that your computer can't see it. This problem is caused by one or two firewalls that are blocking the connection. The simple way to fix this is to temporarily shut down Windows Firewall and, if necessary, the router firewall.

1. Access Windows Firewall settings from Control Panel by clicking System And Security and then clicking Windows Firewall or by typing **firewall** into the Start menu search box and selecting Windows Firewall from the results that appear.
2. Turn off Windows Firewall, and then try again to connect to the router.
3. If you still can't see your router, you should plug your computer into the router via a physical network cable so you can log on to its configuration panel. You normally do this by typing **192.168.1.1** or **192.168.2.1** into your web browser. Once connected, turn off the router firewall too.
4. Next, connect your PC to the router via Wi-Fi. The two devices will see each other fine.
5. Finally, turn both firewalls back on. Your PC will continue to connect to your router each time you access it via Wi-Fi once you follow this procedure.

Incorrect File Associations

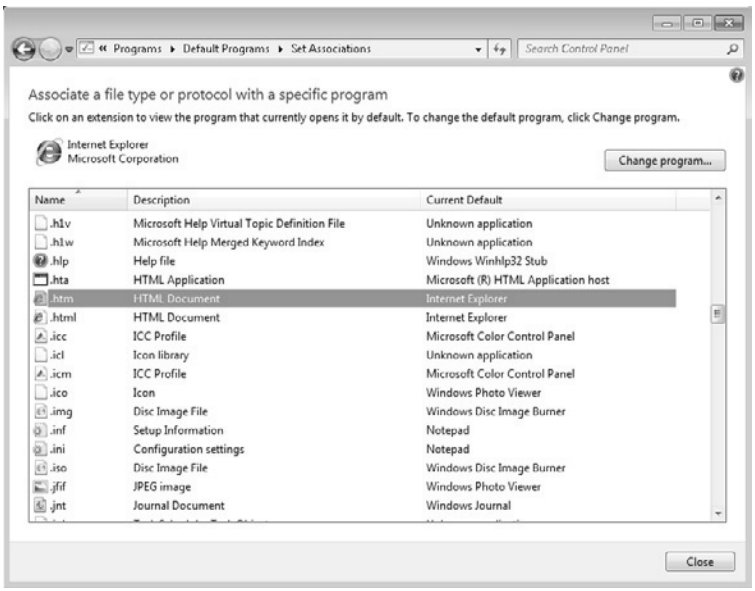
One of the most annoying things when using Windows is clicking on a file only to see a message that there is no program associated with this type of file. This is easy to fix.

1. On the Start menu, click Control Panel, click Programs, and then click Default Programs.

www.it-ebooks.info

2. For simple file association problems, for instance if Microsoft Office Word has lost its association to *.docx files, click the Set Your Default Programs link. In the dialog box that appears, select an installed program, and then click Set This Program As Default.

   For more difficult file association problems, click the Associate A File Type Or Protocol With A Specific Program link. Now you will be presented with a list of all the file types Windows recognizes. Select the appropriate file type from the list, and then click Change Program. Next, select the program from the list that appears, or browse the Programs Files (or Programs Files x86) folders to find the correct one. Click OK when you're done.

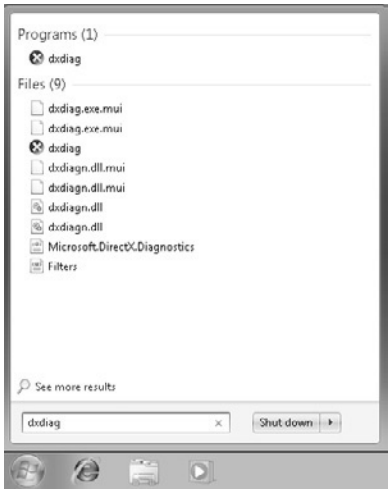


Problematic Graphics, Sound, Keyboard, or Mouse Drivers

Sometimes, **graphics** or sound drivers can cause problems with Windows. **DirectX** Diagnostic Tool can identify problems with them.

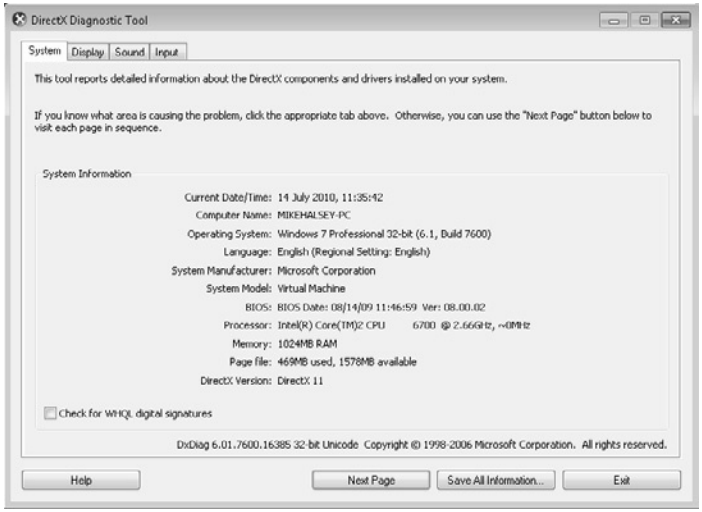
1. Type **dxdiag** in the Start menu search box, and click Dxdiag under Programs in the search results.

www.it-ebooks.info



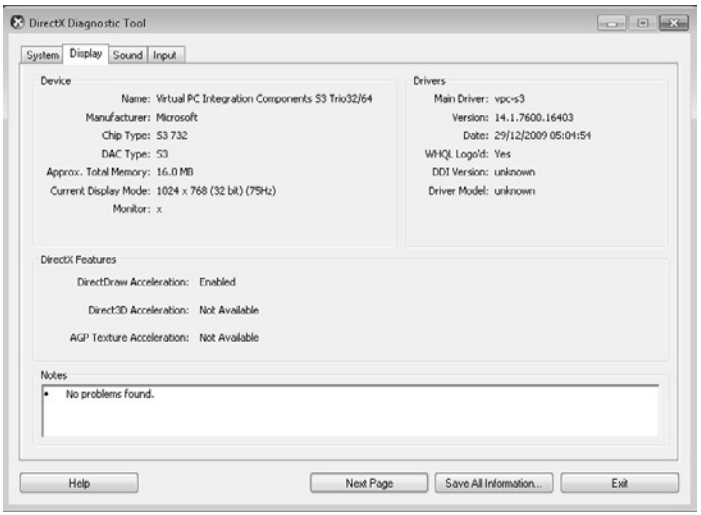
2. Click Yes if you are asked if you want to check if your hardware drivers are digitally signed. This verifies that the drivers have been approved by Microsoft for compatibility with Windows 7.

3. Now the DirectX Diagnostic Tool launches. This checks your display, sound, and input devices for problems.



www.it-ebooks.info

4. If DirectX Diagnostic Tool identifies any problems, they are displayed and you can click the tabs along the top of the screen to review the reports. If problems are found, you will be alerted so that you can use an appropriate diagnostic tool or method to rectify it.



This Copy of Windows 7 Is Not Genuine

Sometimes, even though you have a completely legitimate, fully activated copy of Windows 7, you will be greeted by the message shown in Figure 9-1 when you turn on your PC.

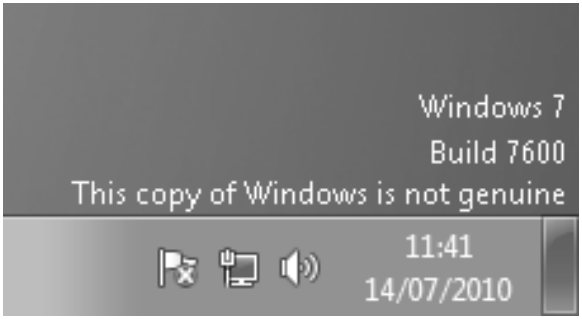


Figure 9-1 Is this copy of Windows genuine or not?

www.it-ebooks.info

Fixing this is incredibly simple; just restart your PC by shutting it down normally and rebooting. This almost always sorts out this minor glitch caused by a file being read incorrectly at startup.

Windows Update Won't Install Anything

Sometimes Windows Update gets stuck, unable to install any updates. This happens because the temporary files store for the program has become corrupt. To fix this problem, navigate to the *X*:\Windows\Software Distribution folder, where *X* represents the hard disk on which Windows 7 is installed. Delete the contents of this folder to reset Windows Update. This will delete all the temporary files associated with Windows Update. It will also reset Windows Update to the default settings, so any updates you've previously hidden will reappear.

Search Isn't Finding Your Files

You know a file is there, but it doesn't show up in a Windows search. This is probably because Search in Windows 7 displays only files it has indexed. You can add files and folders to the index through the Control Panel by typing **index** or **indexing options** in the Start menu search box (see Figure 9-2).

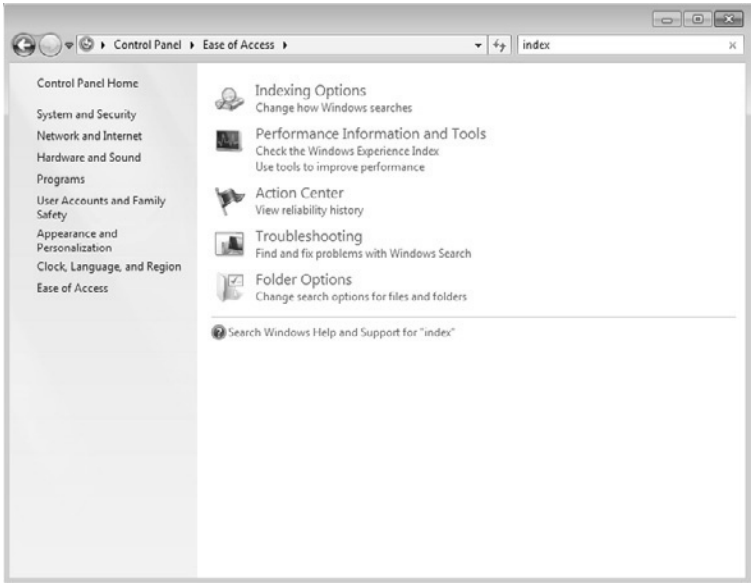


Figure 9-2 Accessing Indexing Options in Control Panel

www.it-ebooks.info

Click Indexing Options, and a list of all the currently indexed drives and folders appears (Figure 9-3). If you do not see the correct location, for instance if you have moved your files to another hard disk or partition, click Modify to add the new location. It will take a while for Windows to add the new files to its index.

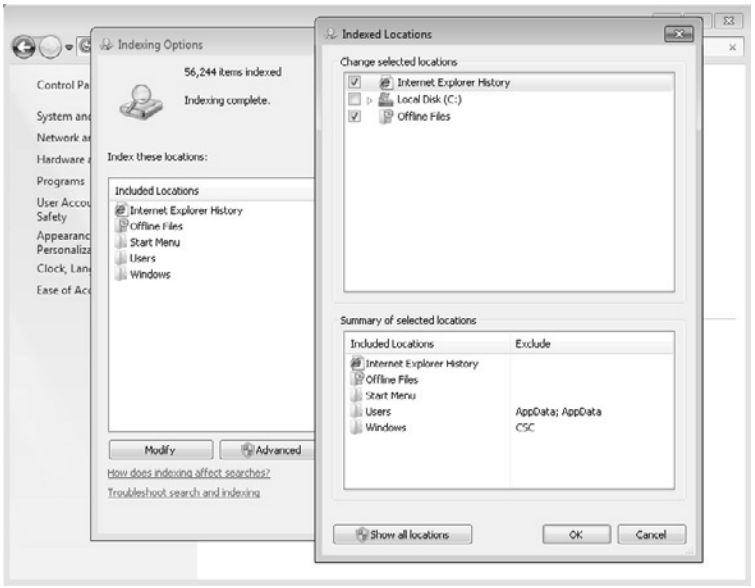


Figure 9-3 Changing the indexing options

INSIDE OUT Indexing is taking ages!

Indexing in Windows 7 only works at full speed when you're not. If you are using your computer while Windows is indexing files, the speed at which Windows 7 builds its index is greatly reduced. Sometimes it's worth leaving your PC on overnight so it can build its index properly.

Service Pack or Update Install Was Interrupted

We've all seen it: the message indicating that Windows is configuring updates and warning us not to turn off the computer (see Figure 9-4). But what if the computer does shut off while Windows is configuring updates, perhaps due to a poorly timed power failure?

www.it-ebooks.info

Windows 7 is remarkably resilient when installing updates. While writing this book, I deliberately turned off the computer while Windows was configuring updates, and I was unable to make the system crash even after several attempts.



Figure 9-4 What happens if the power gets cut here?

However, it's possible that a power interruption at the wrong time will render your copy of Windows 7 inoperable. If this happens, the automated rescue service should start since it shouldn't be touched by any update.

If the automatic restore feature doesn't start, you can opt to manually perform a **system restore**. This will roll back critical Windows files to the point just before the update was installed (Windows 7 will always create a fresh restore point before installing updates). This should get you up and running so that you can try installing the update(s) again.

Windows Starts Up Very Slowly

If Windows 7 is taking a long time to start, it's probably because you have a lot of programs running at startup. To turn off startup programs, access MSConfig by typing **msconfig** in the Start menu search box. See Chapter 15, "Advanced Repair Methods," for more information on this.

www.it-ebooks.info

Another good solution to this problem is Soluto Anti-Frustration Software, which you can download from *www.soluto.com*. This tool will analyze the programs that run on your PC at startup and recommend what programs you can safely turn off (see Figure 9-5).

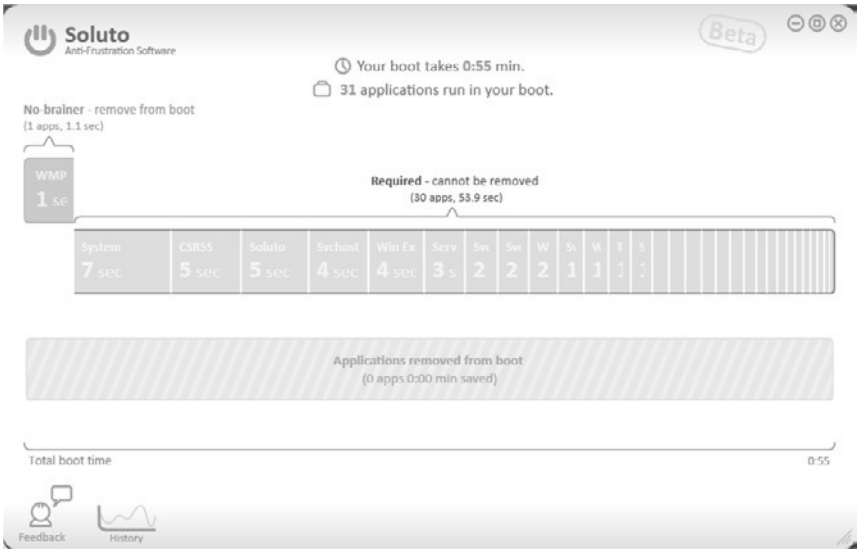


Figure 9-5 Soluto Anti-Frustration Software

Windows Shuts Down Very Slowly

Changing a registry setting might fix a slow shutdown problem. Open Registry Editor by typing **regedit** in the Start menu search box and selecting Registry Editor from the search results that appear. In the left pane of the Registry Editor window, click HKEY_LOCAL_MACHINE, click SYSTEM, click CurrentControlSet, and then click Control.

Here you can lower the WaitToKillServiceTimeout setting (see Figure 9-6) to a lower number by right-clicking it and selecting Modify. The recommended setting is 3000. (This is the number of milliseconds Windows will wait before terminating the program.) This will close programs more quickly when Windows shuts down.

www.it-ebooks.info

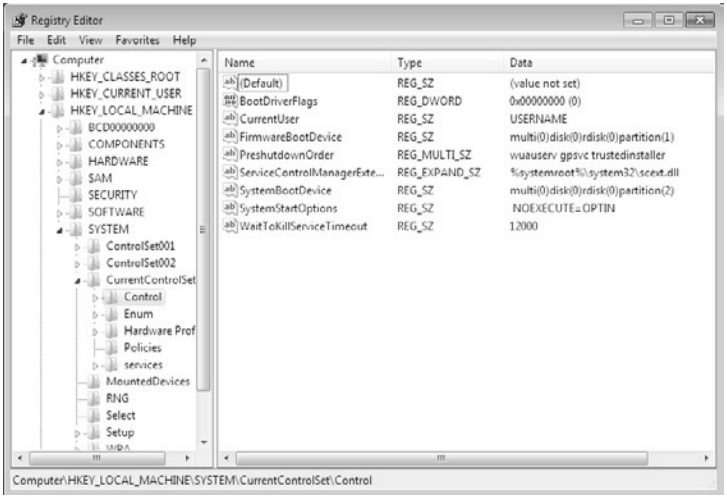


Figure 9-6 Changing the Wait to Kill setting

CAUTION!

Changing the Wait to Kill setting can prevent some software from saving files or shutting down properly. This can cause problems with the software and perhaps make it unstable.

Problems with Sleep

Some people have problems when Windows 7 goes to sleep, ranging from Wi-Fi reconnection problems to issues with the computer not coming out of sleep mode at all.

If you have problems with Windows in sleep mode, especially if the PC is not coming out of sleep mode, you can change the default action to either turn it off or use hibernate mode instead. To do this in Control Panel, click Hardware And Sound, and then, under the Power Options section, click Change When The Computer Sleeps (see Figure 9-7). You will now be presented with several options.

www.it-ebooks.info

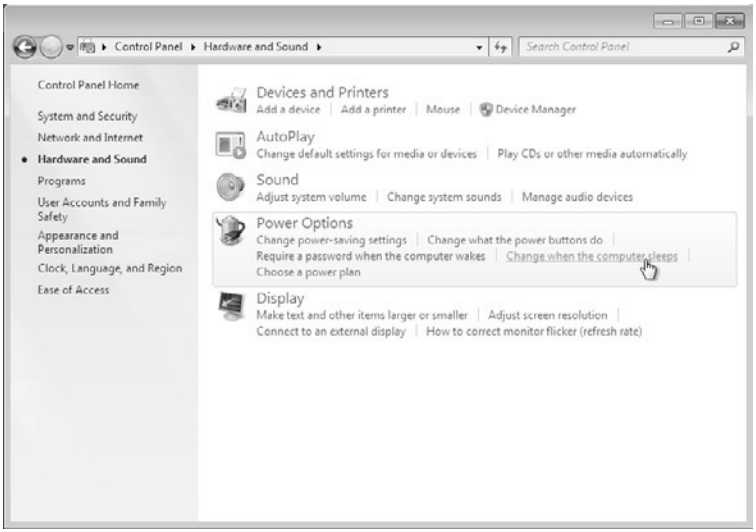


Figure 9-7 Changing the sleep options

You can also change the advanced power settings by clicking the link Change Advanced Power Settings and setting the Sleep Button Action setting to either Do Nothing or to Hibernate (see Figure 9-8).



Figure 9-8 Changing the Sleep Button Action setting

Hardware Annoyances

Some common annoyances with Windows 7 can be caused and/or fixed by the hardware you have attached to your PC.

www.it-ebooks.info

Windows Gets Stuck at Its Loading Screen

There are occasions when Windows gets as far as its loading screen and just sits there. It doesn't crash, it doesn't load, it doesn't do anything, and no matter how many times it gets this far, it just flatly refuses to go any further.

This sometimes happens when you have a network cable plugged into your PC. Simply unplugging this cable will allow Windows to start. You can then plug the cable back in. Windows should operate properly after this fix.

No Operating System Found

If you get a message such as, "No Operating System Found," you probably have a floppy disc, CD, or USB flash drive plugged into your computer, and the PC's BIOS is set to boot from this device before your main hard disk. Just unplug or remove the media and restart the PC.

A New Monitor Results in No Picture

If you connect a new monitor and it won't display anything on the screen, it's probably because the maximum resolution of your new screen is less than Windows 7 was set to on your old screen. Windows 7 does a good job of auto-detecting screen resolutions, but a quick way around this is to boot into **Safe Mode**. (Press F8 after the BIOS screen disappears but before you see the Windows loading logo.) While in Safe Mode you can change the resolution to a setting supported by your new monitor.

Your USB3 Device Doesn't Work

USB3 devices aren't natively supported in Windows 7; this is a feature added with Service Pack 1. If you plug in a USB3 device and nothing happens, it's probable that there is no driver installed for the USB3 controller. You will need the third-party driver that came with your motherboard or USB3 expansion card. Alternatively, you can get this support with Windows 7 Service Pack 1.

You've Installed a Fresh Copy of Windows 7 and Can't Get Online

Windows 7 doesn't come with built-in support for every type of Wi-Fi adapter. This could leave you unable to get online at all unless you have a physical network cable with which to connect to your router. This can be really annoying.

www.it-ebooks.info

The rule here is to always make sure you have a copy of the drivers for your hardware available when reinstalling any operating system. You can normally download these from the support section of the computer manufacturer's website.

Your Headphones or Microphone Won't Work

Sometimes a pair of headphones or a microphone won't work when you plug it in. To fix this, you need to set the headphones or the microphone as the default device.

In Control Panel, click Hardware And Sound, and then click Sound. In the window that appears, set the default sound and recording devices (see Figure 9-9).



Figure 9-9 Setting the default audio devices

Summary

There are lots of little things that can cause problems in Windows 7, none of which are *really* problems but all of which can prove frustrating. In this chapter, I've written about the most common issues I have encountered, and I think you'll agree that some seem to defy all logic.

You will undoubtedly find additional annoyances, and I encourage you to send them to me through my website, *www.thelongclimb.com*.

www.it-ebooks.info

CHAPTER 10

Viruses, Malware, and Other Threats

Repelling an Attack 137
Identifying an Attack 144
Repairing the Damage 153
Summary 162

THE avenues of attack on Windows 7 range from viruses to human error, but the simple fact remains that the world's most popular operating system is cyber criminals' biggest target, and the user is what they're looking to exploit.

An attack on your Windows 7-based computer is something that can bring down your system quickly and, sometimes, for long periods of time. Criminals can attack your personal files, the operating system, or even the computer's BIOS. You have to be prepared for attacks, and you have to know both how to repel them and how to fix any problems that occur as a result of them.

Repelling an Attack

Although Windows 7 isn't bundled with anti-virus software, it does come with some anti-malware software in the form of Windows Defender, and further virus and malware protection is distributed through Windows Update.

Action Center

When you first install Windows 7, it will immediately warn you that you don't have any anti-virus software installed on your PC, as shown in Figure 10-1. This warning notification isn't always immediately obvious to all users, however, and some could miss it.

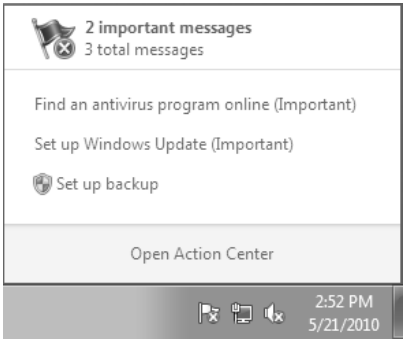


Figure 10-1 Action Center warning you when you install Windows 7 that you need anti-virus software

www.it-ebooks.info

Action Center is represented by a white flag that sits on the far-right side of the Windows 7 taskbar, next to the clock. When Windows has something to tell you, it will highlight this flag with a small white *x* on a red circle. Some people might miss this subtle notification, and if you are providing technical support to someone else, you may find that they have a great many Action Center notifications that they've never noticed.

Anti-Virus Software

Clicking the Action Center icon opens a small dialog box with clickable messages. The anti-virus software warning reads "Find an antivirus program online (Important)." Clicking this message launches Microsoft Internet Explorer and takes you to a website (you will need to have an active Internet connection at this point) listing many anti-virus software recommendations. Clicking any of these icons takes you to a purchase or download link for the software, as shown in Figure 10-2.

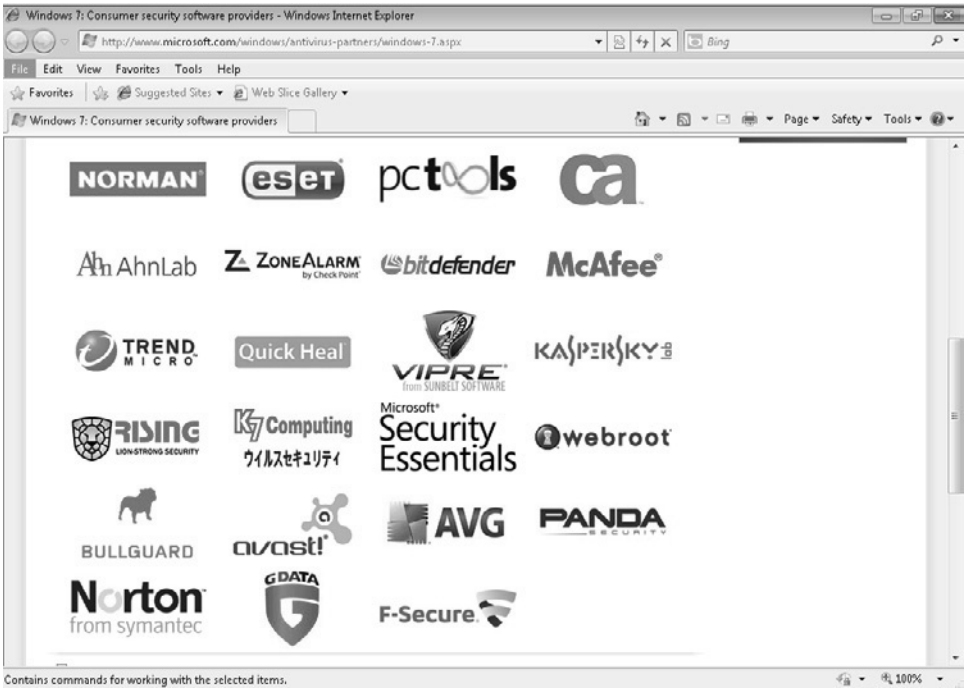


Figure 10-2 Windows 7 helps you find anti-virus software.

My first experience with a computer virus was in 1991 when my PC was infected with a small virus that played the tune *Yankee Doodle Dandy* through the PC's speaker every day at five o'clock. But a decade later, there was a much worse year. In 2001, several major

www.it-ebooks.info

viruses suddenly attacked computer systems worldwide. The Kournikova, Sircam, and Code Red viruses are just three of the viruses that everybody in the technology industry was talking about in 2001.

That year, I was exchanging regular emails with other technical people working in my area via a bulletin board system that allowed hundreds of people to quickly and easily keep in regular contact. It quickly became apparent from member reports that the AVG anti-virus package was the only one to consistently stop all of these threats. Other packages were stopping one or two of the viruses, but only AVG stood firm against all of the major attacks of that year.

AVG built its reputation on its success that year, and millions of PC users around the world still hold the software in high regard today. There's an important lesson to be learned from this, however, and that is that no matter how good your anti-virus software is, there's still no guarantee that you're completely safe and protected from viruses on your PC.

Many factors determine how effective your anti-virus software is at detecting and removing virus attacks. These include:

- How regularly you update the software.
- How regularly and extensively the manufacturer updates the virus definitions.
- How good the software's heuristic scanning engine is for detecting virus-like activity.

The simple rule is that no anti-virus software can ever guarantee 100 percent protection against viruses and malware. So how do you choose the software that's best for you? Organizations like Virus Bulletin conduct rigorous and regular testing of anti-virus products to verify that they provide the protection that they claim they do. Virus Bulletin test results, known as the VB100, are the mainstay of anti-virus reviews and can be found online at *www.virusbtn.com* where free registration is required.

You may be unfamiliar with any of the software packages Windows recommends. In truth, most people choose anti-virus software based on a recommendation from a friend or colleague. The following section about anti-virus software reflects my recommendations.

Microsoft Security Essentials

www.microsoft.com/security_essentials

Microsoft's free anti-virus and anti-malware package, Microsoft Security Essentials, has several advantages beyond just being free. The first and major advantage is that it delays computer-slowing virus scans while you are using your computer. The second advantage is that the package is incredibly lightweight, using very little memory and hardly any system resources, and it won't slow down your computer.

www.it-ebooks.info

Norton Internet Security/Norton 360

www.symantec.com

The scanning engine in Norton 360 has won as many awards as Microsoft's own scanning engine. This is a more comprehensive suite, so you'll notice it more when using your PC, as it is more intrusive for the user than other packages. It contains many useful features and additions, however, and comes with a license that allows you to install it on several PCs.

AVG Anti-Virus/AVG Security Suite

www.avg.com

For years, AVG was the market leader in free anti-virus software and the program most people are likely to have installed on their PCs. In recent years, Symantec and Microsoft have rivaled AVG as the top-rated anti-virus package providers, but AVG remains one of the most popular packages and with good reason.

INSIDE OUT Only run one anti-virus package

Although there are generally no limits to the number of anti-malware packages you can run on your PC, you should have only a single anti-virus package installed. This is because anti-virus packages can interfere with one another and compromise your PC's security.

Anti-Malware Software

Malware takes many different forms. Sometimes it is spyware that reports what you do online to certain websites, or records what you do on its own site, or does something much worse.

Some forms of malware include keyloggers that record everything you type on your PC, including passwords and credit card numbers, and then transmit that information to criminals. Trojans can take control of your PC, sometimes without you even realizing it. These Trojans then use your computer to send spam emails or even to launch distributed denial of service (DDOS) attacks on popular websites for extortion or blackmail purposes.

If you buy a comprehensive security suite, it will most likely include anti-malware protection, but free anti-virus packages do not usually provide anti-malware software.

www.it-ebooks.info

Windows 7 comes with two, free anti-malware packages.

Windows Defender

First introduced with Windows XP as an optional extra, Windows Defender is Microsoft's free anti-malware package that comes bundled with Windows 7 (see Figure 10-3). You should not consider it the only anti-malware product for your computer; I make recommendations for some others later in this chapter.

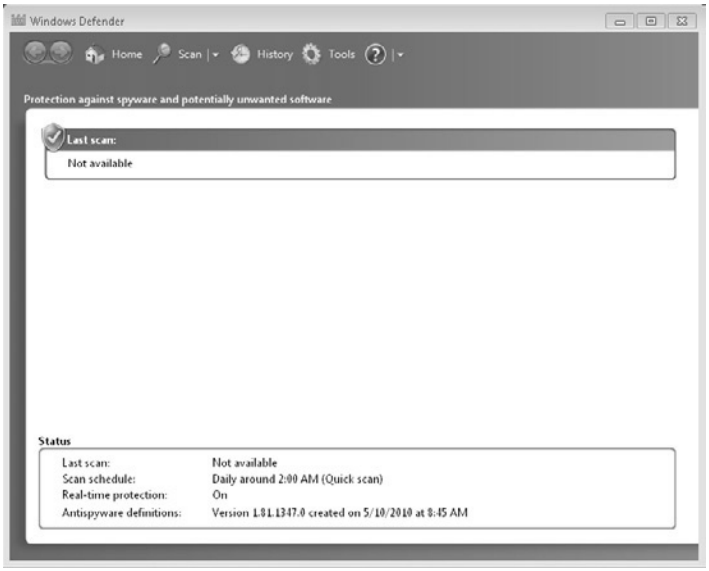


Figure 10-3 Windows Defender

INSIDE OUT

Only one anti-virus package to two or more anti-malware packages?

Anti-virus and anti-malware software operate differently, with the former embedded more deeply into Windows. Anti-malware software usually runs just like an application that you can easily shut down. It is much more difficult to turn off anti-virus software.

Because multiple anti-malware software packages don't interfere with each other the way multiple anti-virus packages do, you can and should have more than one anti-malware package running on your PC.

www.it-ebooks.info

Although Windows Defender is a competent package, it does have a potential flaw: It's updated through Windows Update unlike the Microsoft Security Essentials anti-virus package. This means that if Windows Update is turned off, the package won't receive the latest malware definitions. This could leave your computer unprotected against the most recent malware threats.

Despite this potential weakness, Windows Defender is a useful addition to Windows, and you should keep it activated and updated even if you are running additional anti-malware software.

Some anti-virus packages, such as Microsoft Security Essentials, disable Windows Defender because they perform the same actions, sometimes using the Windows Defender scanning engine. If this is the case, you will see the message that appears in Figure 10-4 when you run Windows Defender.

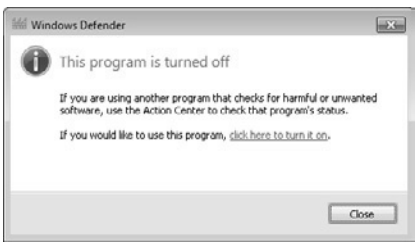


Figure 10-4 Some anti-virus programs disable Windows Defender.

Do not worry about this; there are no recorded instances of viruses and malware being able to turn off this program.

Windows Malicious Software Removal Tool

Once a month, on what is known as Patch Tuesday, Microsoft releases the latest updates for the various versions of Windows and Office. Included in these updates is a program called the Microsoft Windows Malicious Software Removal Tool.

This program, updated only through Windows Update and not available to run separately from the Start menu, works as additional virus and malware protection on your PC. The program is also available to download separately from the Microsoft website (see Figure 10-5) at *www.microsoft.com/security/malwareremove/default.aspx*.

www.it-ebooks.info



Figure 10-5 The Microsoft Windows Malicious Software Removal Tool

The Malicious Software Removal Tool scans for and removes only a limited number of viruses and malware. It is not a replacement for other anti-virus and anti-malware programs. I recommend the following third-party anti-malware software.

Malwarebytes Anti-Malware

www.malwarebytes.org

Although there are a great many excellent anti-malware products available, Malwarebytes is the only one I have ever encountered that is able to identify and remove some of the more unpleasant malware, and I strongly recommend this product.

Spyware Terminator

www.spywareterminator.com

Spyware Terminator is an extremely comprehensive package that offers all types of protection, and I can thoroughly recommend it as it protects my own PCs. Some users find the Host Intrusion Protection System in Spyware Terminator, which prevents malware from installing things on or making changes to your PC, to be, pardon the pun, intrusive, and you may want to select the Advanced options when installing it so you can choose not to have this feature running.

www.it-ebooks.info

Spyware Blaster

www.javacoolsoftware.com

Another excellent and free package is Spyware Blaster, a small, lightweight program that provides excellent protection against malware and Trojans.

INSIDE OUT

Always keep anti-virus and anti-malware software up to date

Your anti-virus and anti-malware software packages can keep your PC protected only if you keep them up to date and set them to run regular scans. It's always wise to be proactive and not reactive with your computer's security.

Identifying an Attack

It's almost impossible for a PC to be infected with a virus or Trojan without a human being permitting the infection at some point. In this section, I share some guidelines for making sure you can keep your computer safe from unwanted software.

Look for the Padlock

Most attacks will come from the Internet. Since this is where you probably spend more time than ever before, shopping, banking, and visiting websites where you provide all types of personally and commercially sensitive information, you need to be careful about what information you give and to whom you give it.

Figure 10-6 shows a standard web form, in this case the Microsoft **Hotmail** account sign-up screen. This is a good example of a website that requires you to provide all types of personal information and to create a password. In this case, you can see that the website is safe because there is a padlock in the address bar. Clicking the padlock will bring up details about the security certificate associated with the website. You can see in the figure that the certificate is registered to the address *signup.live.com*, which matches the address of the website in the address bar.

www.it-ebooks.info

INSIDE OUT Stay Safe Online

You should never submit personal or sensitive information (such as a password) to a website that does not display the padlock. Some pages do not display a padlock because they may consider the information you are entering, your name for instance, to not need to be encrypted when it's collected through the website, but any page where you enter details like date of birth or credit card numbers should display the padlock. Note that different web browsers may display the padlock in different locations at the top or bottom of the browser window.

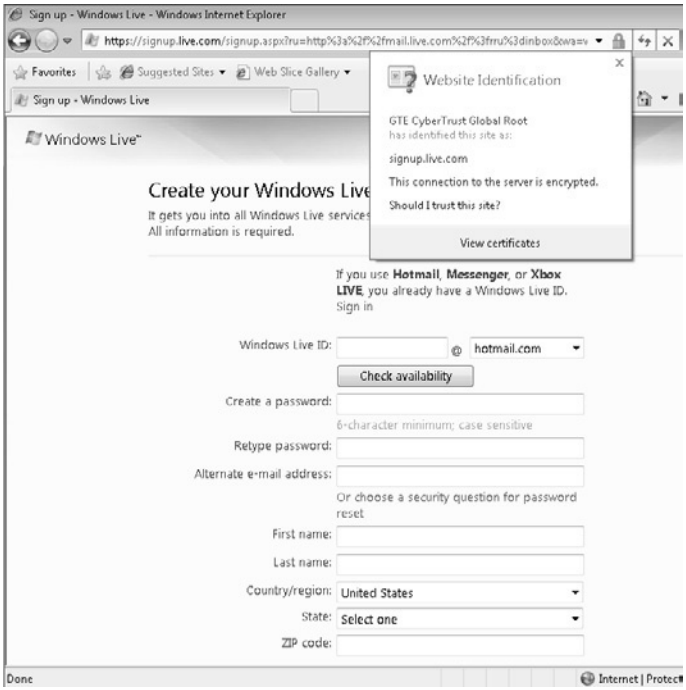


Figure 10-6 Always check for the padlock on secure websites.

www.it-ebooks.info

Beware of Spam and Phishing Emails

Spam and phishing emails commonly lead to websites that ask you to enter personal information in a form. Spam emails usually try to sell you goods, such as generic drugs, that are almost always counterfeit. Spam is a multimillion dollar business for criminals. If you want to buy something legitimate, you should visit a reputable website shop or search for the product through the shopping section of a legitimate **search engine** like Google, Yahoo!, or Bing.

INSIDE OUT What is a phishing email?

A phishing email is a message that purports to be from a reputable bank or website asking you to log in to confirm security details. Instead, you are redirected to a fake website that may look and operate exactly or in a similar way to the real one, but anything you type into the website will be sent to criminals instead. Phishing emails commonly ask for information such as your first and last name, date of birth, mother's maiden name, account number, and password.

It is important that you use a secure password and, if possible, have different passwords for each website you use. If you inadvertently give criminals your "standard" password, they could access all of your accounts, from banking to PayPal, Amazon, eBay, and so on.

CAUTION!

No website or bank will *ever* email its customers asking them to log in to their account for the purposes of confirming account or security details. If you ever receive an email asking you to do so, *never* click on the link in the email. If you want to log in, open your browser, and type the address of the website.

The one exception to this is some websites will send you a confirmation link when you first set up an account with them to confirm your identity. This activation link is acceptable to click, and the website will always tell you to expect one of these emails when you create an account.

www.it-ebooks.info

How to Create a Strong Password

Many people use common dictionary words and names as passwords. These are the weakest passwords you can use, and they can be cracked within seconds by any modern computer. To create a strong password, you should use a mixture of uppercase and lowercase letters, numbers, and symbols.

Examine your password to determine where you can substitute letters for other characters. Can you slip a capital letter into the middle, substitute an *i* or an *L* for a *1*, or use a * instead of an *o*? For example, the password "microsoft" could be spelled "m1cr*S0ft" with a *1*, a *, a capital *S*, and *0* used to make the password much more secure.

Table 10-1 shows how long it could take a criminal with an ordinary computer to crack passwords with different numbers of characters. Where do your passwords fit in the chart?

Table 10-1 How long does it take for a PC to crack a password?

Number of Characters	Numbers Only	Upper or Lower Case Letters	Upper or Lower Case Letters Mixed	Numbers, Upper, Lower Case Letters	Numbers, Upper, Lower Case Letters, Symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	4 seconds	9 seconds	1.25 minutes
6	Instantly	3 seconds	3.25 minutes	9.5 minutes	2 hours
7	Instantly	1.25 minutes	3 hours	10 hours	8.5 days
8	10 seconds	35 minutes	6 days	25.25 days	2.25 years

I recommend that any password(s) you use be a minimum of eight characters long.

Do You Really Need Another Toolbar?

Many free software packages, such as Adobe Flash Player shown in Figure 10-7, offer additional toolbars for your web browser as a way of helping to finance their development. Some of these toolbars, such as toolbars from Google or Bing, are perfectly harmless, but I would not recommend installing additional toolbars into any web browser for three reasons.

- They can only serve to slow down your web browser.
- They commonly replicate functionality that is already in your browser, such as search.
- Some are malicious.

www.it-ebooks.info

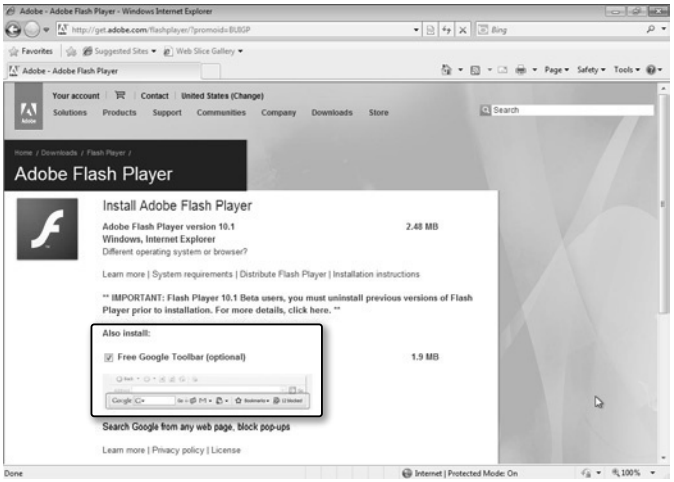


Figure 10-7 Do you really need an extra toolbar?

Malicious Toolbars

To say that some toolbars are malicious is probably overstating the case, but there are good reasons to avoid most of them. Often they block any attempts you make to access search engines like Google and Bing and instead redirect you to their own websites; this is because they make their money through people using their sites to search the web. These web search engines are often not as good or as comprehensive as the big three, Google, Yahoo!, and Bing.

The other thing toolbars can do is insist you install additional software on your PC. At best, this added software will automatically run at startup and slow down your PC. At worst, it will cause problems on your PC, either by being poorly written or by doing something deliberately malicious, such as recording what you type and broadcasting it to criminals.

Do You Need that Extra Browser Plug-in or Download?

All Internet browsers these days will warn you if a website wants to install a plug-in for your browser or if it wants you to download software. In Internet Explorer (and several other browsers, such as Mozilla Firefox), an information bar like the one shown in Figure 10-8 warns you of this.

www.it-ebooks.info

INSIDE OUT The web browser information bar

The location and color of the information bar will vary depending on the browser you use. In Internet Explorer 8, which ships with Windows 7, it is at the top of the browser window, see Figure 10-8. In Internet Explorer 9 it appears at the bottom of the browser window.

In other browsers such as Mozilla Firefox and Google Chrome this can also vary; the information bar color in Chrome is blue.

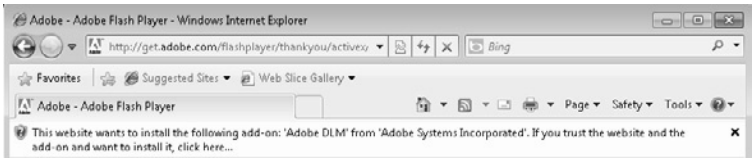


Figure 10-8 Only download plug-ins and software you specifically need.

The simple rule is to *never* install or download anything you didn't specifically visit a website to get. A common trick is for a fake security site to try and get you to download a Trojan (more on this later in the chapter) or for malicious videos on websites like YouTube to try and convince you that you need a special codec to play a video. These websites will all use a single standard for playing video, and you will never need to install another. If you find a video on YouTube, Hulu, or any other website that asks you to use a special codec, you should email, for example, abuse@paypal.com, and inform the website immediately. They will all monitor an abuse@... email address.

Malicious Websites

There are many malicious and fake websites that will try to do everything from getting you to surrender sensitive information to getting you to download viruses and Trojans. Many of these are quickly blocked by security and Internet browser vendors. The web address shown in Figure 10-9 was used as part of an email phishing scam, but Internet Explorer blocked access to the website.

www.it-ebooks.info

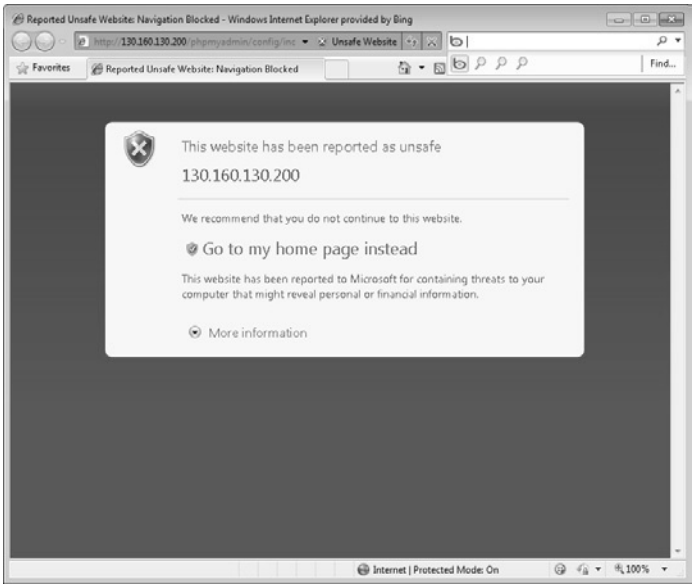


Figure 10-9 Security vendors can be quick to block harmful websites.

The web address bar in Figure 10-9 is red to indicate a warning and, in this example, the words "Unsafe Website" appear in the address bar. Clicking this warning will bring up additional information about the threat (see Figure 10-10).

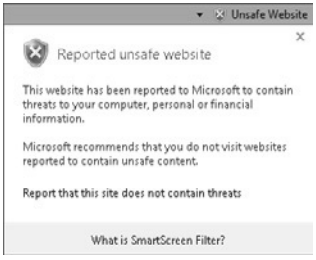


Figure 10-10 If a vendor finds a website unsafe, it warns you.

Malicious and Fake Anti-Malware Software

Figure 10-11 shows a common Trojan called Antivirus 2010. I have known many people to be fooled by this and similar products.

www.it-ebooks.info



Figure 10-11 This apparently innocuous anti-virus package is actually a nasty Trojan.

A Trojan like Antivirus 2010 is usually downloaded from a website that claims it has detected harmful software on your computer (something that is impossible when you first visit an anti-virus website) and advises you to download and install what looks like a perfectly legitimate anti-virus product.

What this software *really* does is falsely identify dozens, maybe even hundreds, of viruses and Trojans on your computer. It will claim that it can get rid of all of them, but only if you upgrade to the full product. It will direct you to a website where you can pay for and download the fake software.

In reality you have just one Trojan on your computer: this one! The download you pay for will remove it, but it will probably install other malicious software such as keyloggers and botnet clients. At this point, not only do the criminals responsible for the fake anti-virus software have a back door into your PC, but they also have your personal details, credit cards details, and, most likely, the password you commonly use on the Internet as well.

CAUTION!

Unless you specifically visit a website to perform a scan, a website cannot automatically detect malicious software on your PC without first installing a plug-in to do so (more on this later in the chapter). Never let a website trick you into downloading a Trojan or virus in this way.

www.it-ebooks.info

What Goes on the Internet, Might Stay There Forever

Internet privacy is a contentious issue, with privacy activists and even governments wading into the debate about what websites and online companies should do to protect the privacy of their customers and users and how they should do it.

In Figure 10-12, you can see a typical website privacy settings page, in this case for Facebook, which has received more criticism than most in recent years.

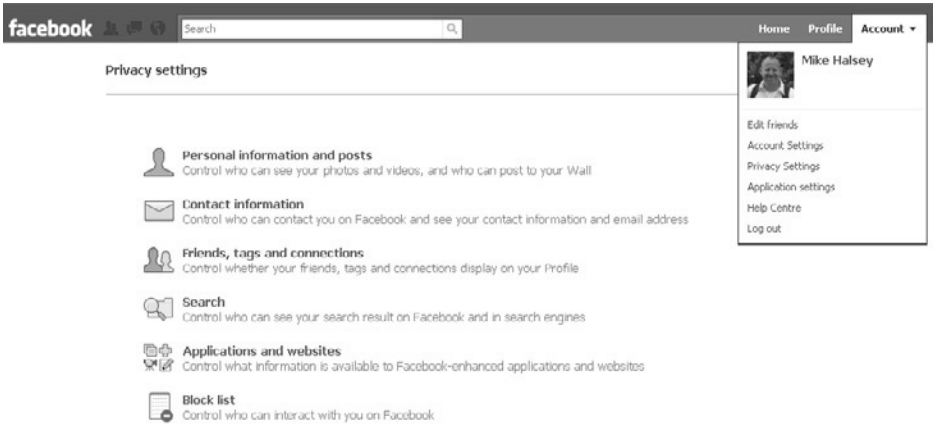


Figure 10-12 A typical website privacy settings page

Internet search engines are brilliant for finding out all sorts of information, but they can also be used to find out information about you. You could one day find personal information about yourself or others close to you, such as addresses, your mother's maiden name, or your date of birth, available on Google, Yahoo!, or Bing. You might also find personal comments you have written (privately, so you thought) published for the world to see. Any information about you can be harvested by criminals, and exposed private comments could even cost you your job. If you are suddenly receiving large amounts of spam email, it could be because your email address is exposed on a website and has been harvested by criminals.

You should always guard your privacy online. Often, you display personal information on social networking websites or on sites like YouTube. Although these websites are improving their default privacy settings, you should always check the settings yourself.

www.it-ebooks.info

Repairing the Damage

Malicious software can put up all types of barriers when it comes to removal. It can prevent you from accessing anti-virus and anti-malware websites or redirect you from a legitimate to a malicious website. In some instances, it can even disable your existing anti-virus and anti-malware software or prevent you from updating it. However, you *can* take action to remove these viruses.

Use Your Existing Anti-Malware Software

If you suspect your computer has been infected with a virus or malware and want to remove it, the very first thing to try is updating your existing anti-virus and anti-malware packages and performing full scans with them. You might find they are still functioning and able to remove the infections on your PC.

INSIDE OUT

Always run your anti-virus and anti-malware scans twice

After you run full scans of your PC with your anti-virus and anti-malware packages and they have removed infections, you should always restart your PC and run these full tests again. This way you can be certain that any and all malware has been removed and your system is clean.

Try a Free Online Virus Scanner

Many Internet security companies offer free online virus scanners. These normally run via a plug-in from the website, and you can search for them online. Unless you know and trust the name of the vendor whose service you are using, I recommend using one of the following vendors.

- **Trend Micro HouseCall** *http://housecall.trendmicro.com*
- **BitDefender Online Scanner** *www.bitdefender.com/scanner/online/free.html*
- **ESET Online Scanner** *www.eset.com/online-scanner*
- **Norton Security Scan** *security.symantec.com/sscv6*

www.it-ebooks.info

- **Kaspersky Online Scanner** *www.kaspersky.com/virusscanner*
- **McAfee FreeScan** *http://home.mcafee.com/Downloads/FreeScan.aspx*
- **Panda ActiveScan** *www.pandasecurity.com/homeusers/solutions/activescan*

These free online services are very efficient and competent. However, they are not a substitute for a full anti-virus package, since they will commonly be able to scan for only the biggest and most well-known viruses, not the full range of viruses that your own anti-virus software can scan for.

McAfee Stinger

A useful tool for detecting and removing malware and viruses is McAfee Stinger software (see Figure 10-13). You can download it from *http://vil.nai.com/vil/stinger*. This utility does not need to be installed on your PC to run. Since viruses often block the installation of new anti-virus software, you can run Stinger from a removable device such as USB flash drive or a CD.

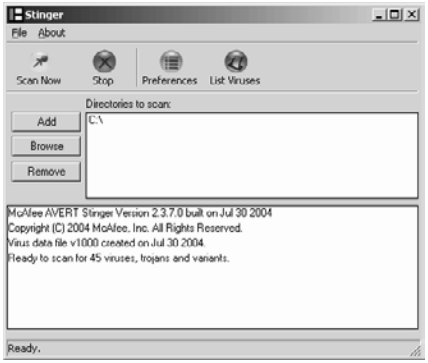


Figure 10-13 McAfee Stinger stand-alone anti-malware software

As with the online scanners, Stinger can scan for only a limited number of threats. Always make certain that you download the latest version of Stinger, perhaps from a different PC, before running it.

www.it-ebooks.info

INSIDE OUT

Rerun tests with your own anti-virus software

After using an online scanner or Stinger to remove a virus, always update your own anti-virus and anti-malware software, and run full scans to be certain the malware has been removed.

Safe Mode

All versions of Windows have a special diagnostic mode you can start up in called Safe Mode. This is a reduced functionality mode where only the basic hardware drivers are loaded and where all startup software is disabled.

Many viruses and malware packages that run automatically when Windows starts up will not run in Safe Mode. You can, therefore, run your anti-virus scans in Safe Mode without fear of interference. This can be especially useful if you want to download an anti-virus or anti-malware software package but are being blocked or redirected to fake websites instead.

You enter Safe Mode when you start your computer by pressing F8 on your keyboard to bring up the Advanced Boot Options screen, as shown in Figure 10-14. If you see the Starting Windows logo, you have gone too far and will need to restart.

The Advanced Boot Options menu presents a series of options. You should usually choose Safe Mode, but if you need to get online to download anti-malware software or to use an online virus scanner, you should choose Safe Mode With Networking.

With Windows running in Safe Mode, you should be able to do tasks such as updating your malware protection (remember to select Safe Mode With Networking to do this) and running full scans of your PC with both anti-virus and anti-malware packages.

www.it-ebooks.info

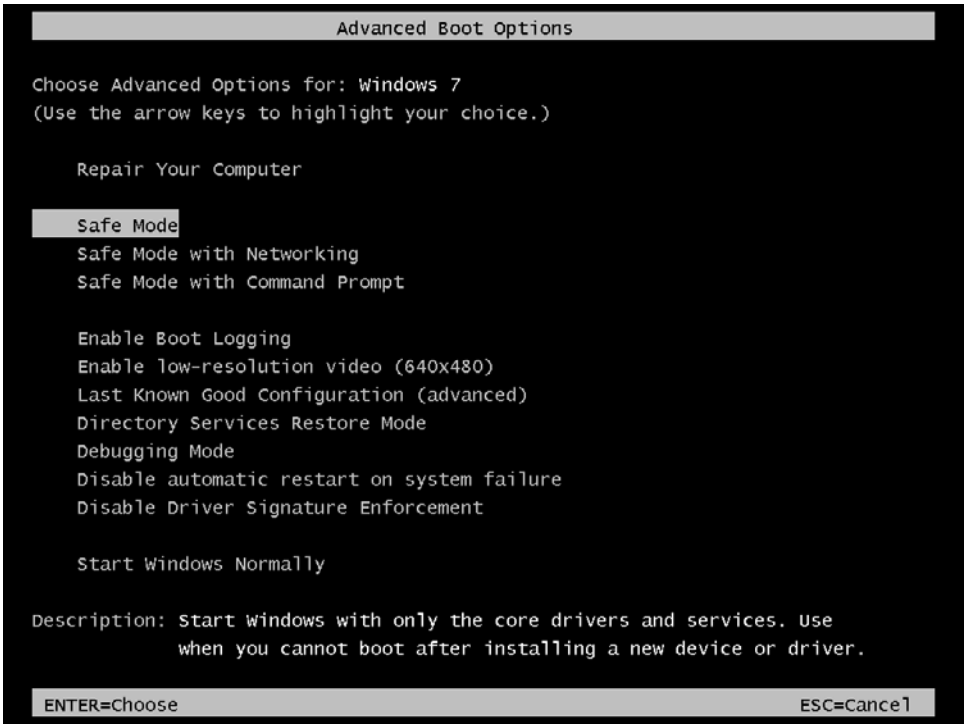


Figure 10-14 Starting Windows 7 in Safe Mode

If your anti-malware package reports that it has found and removed the malware, you can reboot your machine normally. You should always run a second full scan using your anti-virus and anti-malware software after restarting, however, to be sure the malware is removed.

INSIDE OUT My anti-malware software can't remove the virus

If your anti-virus or anti-malware software cannot remove a virus or malware infection, try another package or one of the free online scanners listed in this chapter.

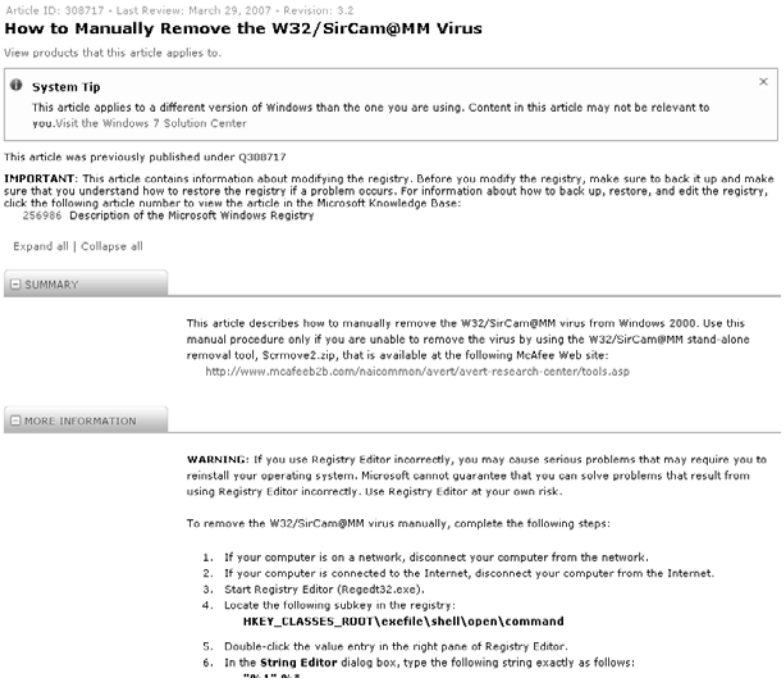
www.it-ebooks.info

Manually Removing a Virus Infection

If your anti-virus software cannot remove a virus, then the time may have come to remove it manually. This can be a complex process and will usually involve deleting files, removing Windows services, and removing entries from the Windows 7 registry.

The first thing to do, either in Safe Mode with Networking or, preferably, on an uninfected PC, is to search the Internet for instructions on manually removing the virus, using the name of the virus provided by your anti-virus software.

In Figure 10-15, you can see an example of the instructions Microsoft provides on its web-site for manually removing the W32/SirCam@MM Virus. This is one of the major viruses from 2001 that I mentioned at the beginning of the chapter.



Article ID: 308717 - Last Review: March 29, 2007 - Revision: 3.2

How to Manually Remove the W32/SirCam@MM Virus

View products that this article applies to.

System Tip

This article applies to a different version of Windows than the one you are using. Content in this article may not be relevant to you.Visit the Windows 7 Solution Center

This article was previously published under Q308717

IMPORTANT: This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, click the following article number to view the article in the Microsoft Knowledge Base:

256986 Description of the Microsoft Windows Registry

Expand all | Collapse all

SUMMARY

This article describes how to manually remove the W32/SirCam@MM virus from Windows 2000. Use this manual procedure only if you are unable to remove the virus by using the W32/SirCam@MM stand-alone removal tool, Scrmove2.zip, that is available at the following McAfee Web site:

http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/tools.asp

MORE INFORMATION

WARNING: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

To remove the W32/SirCam@MM virus manually, complete the following steps:

1. If your computer is on a network, disconnect your computer from the network.
2. If your computer is connected to the Internet, disconnect your computer from the Internet.
3. Start Registry Editor (Regedt32.exe).
4. Locate the following subkey in the registry:
   HKEY_CLASSES_ROOT\exefile\shell\open\command
5. Double-click the value entry in the right pane of Registry Editor.
6. In the **String Editor** dialog box, type the following string exactly as follows:

Figure 10-15 Typical virus manual removal instructions

The instructions provided by Microsoft or other third-party anti-virus vendors like Symantec and McAfee can sometimes be complicated. However, the following instructions may help you make sense of a complicated procedure.

1. Note the name of the virus or malware infection on your PC, as provided by your anti-virus or anti-malware program.

www.it-ebooks.info

2. On an uninfected PC if possible, search online for ***virusname*** **manual remove**. Choose a link from Microsoft or one of the major security vendors I mentioned in the free online scanner section earlier in the chapter.

3. Print out the instructions, if possible, so you have them in hand.

4. Boot your PC in Safe Mode as described in the section titled, "Safe Mode."

You may need four Windows tools to manually remove the virus.

- Windows Explorer, accessed by clicking Computer on the Start menu.

- MSConfig, accessed by typing **msconfig** in the Start menu search box. On the MSConfig Startup tab, clear programs that are set to start automatically when Windows starts. This may include malware. You can also use the Services tab to remove malware services in Windows, but I would recommend instead using the Services Panel (see below) for disabling Windows 7 services.

- Services panel, accessed by typing **services.msc** in the Start menu search box. This will provide a list of all the Windows 7 components, including plug-in and third-party services, that make up the operating system. You can view them by status, which you may find helpful since Windows 7 on your PC will not need every service that ships with the operating system. Right-click any service, and select Properties from the context menu that appears. In the dialog box that opens, you can disable the service.

- Windows registry, accessed by typing **regedit** in the Start menu search box. This is the database of settings for the operating system and all of your software. I will cover advanced tasks with Windows registry in Chapter 27, "Advanced Registry Work."

CAUTION!

You should always exercise caution when disabling a Windows service or changing a registry setting. Changing a setting that is critical to the operation of Windows or a program can cause a malfunction or even lead to the entire operating system becoming unresponsive, even after restarting the PC.

Virus Removal Using Another PC

If Windows 7 cannot start even in Safe Mode because of an infection, you can still remove the virus, but you will need another PC or laptop to do so. You can physically remove the infected hard disk from your PC by unplugging its power and data cables. (Always make sure your PC is switched off and disconnected from the main power source before you do

www.it-ebooks.info

this.) You can connect this hard drive to another PC either by plugging it in inside the case of the alternative desktop PC or by putting it into a USB-removable hard disk caddy (recommended). You can then start this other PC, making sure its anti-virus and anti-malware software has been updated in advance, and run full scans passively on the infected disk. I say "passively" because you need to make certain you don't open or run any files on the infected drive during this process, since this will risk infecting the second PC with the virus or malware.

Restoring Windows 7 from a Backup

A good way to quickly and easily remove virus infection is to restore Windows 7 from a clean system image backup. If you created such a backup, you can use it to restore your copy of Windows and all of your software exactly as they existed when the backup was made.

This may be inconvenient, especially if the backup was created a long time ago, because there will be many updates and new software to install. However, it can be a quick and easy way to remove a virus infection.

INSIDE OUT

Run a full virus scan after restoring from a backup

You should always make sure your anti-virus and anti-malware packages are fully up to date and run full scans with them after restoring Windows 7 from a system image backup, because a virus infection might sit in a file on your hard drive. If this is the case, you could reinfect your PC the next time you open the file.

Viruses Corrupting the BIOS

Most modern BIOS come with built-in protection to defend against viruses rewriting or erasing the BIOS code (see Figure 10-16). Although this feature can, on rare occasions, interfere with certain hardware, it can also be very useful. You will need to turn off this feature to update the firmware in your BIOS.

In some extreme cases, viruses have been known to rewrite a computer's BIOS chip on the motherboard. If this happens, your computer will no longer communicate with Windows and won't be able to start (see Figure 10-17).

www.it-ebooks.info

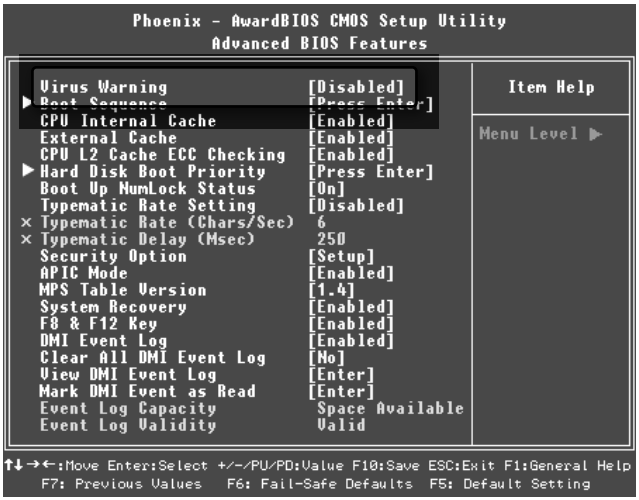


Figure 10-16 BIOS-level virus protection

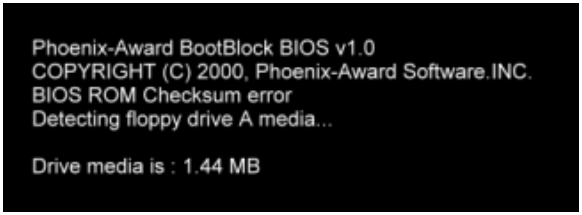


Figure 10-17 A corrupt BIOS preventing a PC from booting

In Chapter 7, "Hardware," I wrote about how to reset the computer's BIOS, and this should be the first thing to try if your PC does not start after a virus attack. Sometimes, however, this won't be enough, and you will need to upgrade the firmware in the BIOS using a utility provided by your motherboard manufacturer. This software is usually on a CD that comes with your motherboard or PC, and the firmware update can be found on the manufacturer's website.

You should consult the motherboard manual for instructions on exactly how to update the BIOS firmware, but normally you need to create a bootable CD or **floppy disk** on another PC using the supplied software. You start the infected PC using this disk, and the utility upgrades the BIOS firmware. This usually fixes the problem.

www.it-ebooks.info

CAUTION!

You should always be very careful upgrading the firmware for your motherboard's BIOS, because if the process is not done exactly as directed in the manual or if it is interrupted for some reason, your motherboard can become completely unusable.

Fortunately, virus attacks on the BIOS are extremely rare, but they can cause devastating damage to your PC. If upgrading the firmware for your BIOS does not fix this type of attack, you should contact an IT professional for further assistance.

Where Can Viruses Hide?

Simply getting rid of a virus is sometimes not enough. There are places where viruses can hide.

- **Email** A virus or malware can sit in an infected email, usually as an attachment, and can reinfect your computer the next time you open it. You should delete all infected emails.
- **Files** Files on your PC may contain viruses. Microsoft Office and PDF files are commonly used to hide viruses. If your anti-virus software cannot remove the infection from a file, you should either delete the file or quarantine it (this choice is usually offered by anti-virus software) until it can be healed in the future.
- **Backups** Have you backed up your files since your PC became infected? You should check the dates of your backed-up files to see if the virus infection sits there, ready to reinfect your PC if you restore them. If this is the case, consider deleting and redoing the backup.
- **System Restore** This is a Windows service that can roll back critical operating system files in the event of a failed driver or software install. You can access System Restore in the Control Panel by clicking System And Security, then clicking System, and then clicking Advanced System Settings. You should turn off System Restore on all drives and restart your computer. Reactivate System Restore only when the virus infection is gone. To do this, in the System Properties dialog box, on the System Protection tab, click Configure in the System Restore panel, and then disable protection for all drives.

www.it-ebooks.info



Summary

No matter how up-to-date or effective your anti-virus or anti-malware software is on your PC, and no matter how good your firewall is, the weakest point of entry to your PC will always be the user. That user might not always be you. Some people guard their PCs carefully and are wary of letting friends or family members use them because of horror stories they've heard or because of their own experiences online. In the end, however, computers and the Internet are for you to enjoy and not fear. While it's easy to download a virus, it's usually equally as easy to get rid of it without it causing any permanent damage. If you want more information about PC and Internet security, log on to my website at *www.thelongclimb.com* for updates on the latest threats, scams, and fixes.

www.it-ebooks.info

CHAPTER 11

Easy Ways to Fix Windows 7

Restore Previous Versions of Files 163
System Restore 166
Troubleshooting Software Compatibility 170
Windows Won't Start 175
Working with Device Drivers 180
Action Center Troubleshooter 194
Microsoft Fix It Center 195
Summary 195

You might be surprised how easily the operating system can fix many of the common problems and annoyances you might experience with Windows 7. These problems can range from software and drivers not working to corrupt files to Windows not starting. Fortunately, the operating system includes a tool for dealing with just about every situation you encounter.

Restore Previous Versions of Files

First seen in Windows Server 2003 for use across networks, Previous Versions is a system that uses the System Restore feature in Windows 7 to save previous versions of files that have been changed. You access Previous Versions through Control Panel by clicking System and Security\System and then clicking Advanced System Settings in the left pane.

In the dialog box that appears, select the System Protection tab, as shown in Figure 11-1. Here you can control what drives are protected by Previous Versions. By default, the Windows drive is protected, but if you've moved your files and data to another drive, you need to switch on system protection for that drive as well.



Figure 11-1 Controlling previous versions of files in Windows 7

www.it-ebooks.info

To turn on system protection for a drive, click the drive you want from the Available Drives in the Protection Settings area of the System Protection tab, and click Configure. A dialog box like the one shown in Figure 11-2 opens for that drive and includes three options.

- **Restore system settings and previous versions of files.** Choose this option only on the hard disk or partition that contains your copy of Windows 7.
- **Only restore previous versions of files.** Use this option for drives or partitions that contain files and data that will change, but no operating system.
- **Turn off system protection.** Select this option for drives on which the files won't change, such as a Windows 7 Image backup, and no operating system is installed.

The Disk Space Usage section lets you adjust how much space on your hard disk you want to allocate for backups. The default amounts are very low.



Figure 11-2 Controlling settings for previous versions

INSIDE OUT Why isn't Previous Versions saving my files?

By default, Previous Versions reserves 3 percent of the space on any drive it is activated on, but this amount of space might not be enough for your needs. I have tens of thousands of files on my PC, many of which I am constantly updating and changing. When I want to use the Previous Versions feature to restore an earlier copy of a file, I often find that no previous copies of the file are backed up.

www.it-ebooks.info

You need to decide how much disk space you're prepared to reserve for the Previous Versions feature and what files you want it to save. To work effectively with a heavy volume of files, you should be prepared to allocate 10 percent of your disk space for Previous Versions.

You can also restore a previous version of a document by right-clicking the file and selecting Restore Previous Versions from the shortcut menu, as shown in Figure 11-3.

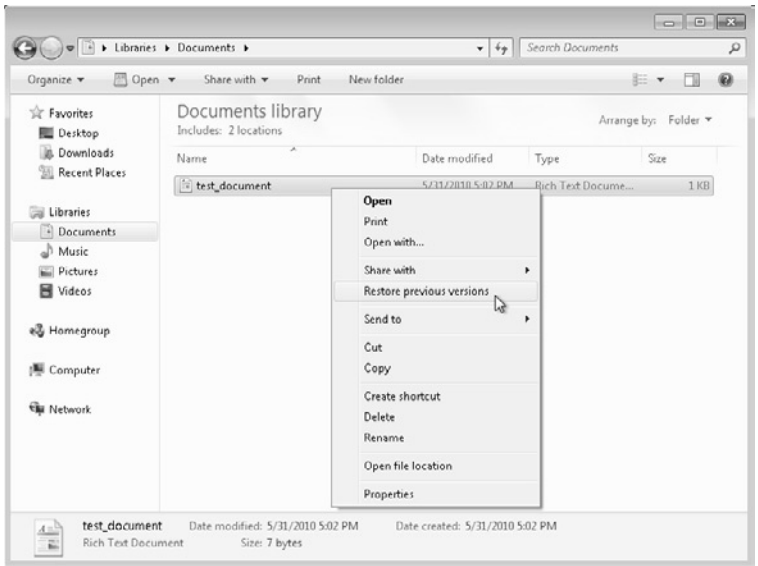


Figure 11-3 Accessing previous versions of files

You shouldn't rely on Previous Versions as the sole way to keep backup copies of your files and documents. As you can see in Figure 11-4, no previous versions of files are available for the file I have selected, despite the fact that this file has been edited many times. Previous Versions cannot tell the difference between files you deem critical and minor changes, which could include the "last accessed" date and time stamp made to all files when you open them.

This means that playing a music track or viewing a photo also counts as a file change, and there could be a great many more of these changes than there would be to files you edit and work with.

www.it-ebooks.info

As a result, the files you have edited most recently, for instance a group of music tracks or viewed photos, will cause the files you have worked on, spreadsheets for instance, to be moved down the priority list for Previous Versions until the backups are automatically deleted when no more disk space for them is available. In this case, I would have been disappointed if I had not kept my own backups. You should *always* keep your own backups of files. Because of the way the Previous Versions feature works, you can't guarantee that it will have the backed-up versions of the file you want to restore.



Figure 11-4 The Previous Versions restore window

As I said, you should never use Previous Versions as an alternative to backing up your files because it doesn't keep a backup copy of every file, only the most recently changed few (depending on how much disk space it has available). You also need to allocate a reasonable amount of space on your hard disk or partition for storing the backups for the feature to work at its best.

System Restore

The System Restore function has been in Windows since Windows XP. It was originally criticized as being a nice hiding place for viruses, because Windows XP didn't have a security system in place to prevent viruses from being written there, and anti-virus software couldn't easily remove any viruses that were planted. Also, while performing a system restore after cleaning the virus, the virus would also be restored., The addition of the User Account Control security system means this feature can now be trusted to restore important and critical Windows 7 files—and nothing nasty.

www.it-ebooks.info

System Restore takes snapshots of critical Windows 7 operating system files when changes are made, such as installing new software or a driver for a new hardware device. Should something go wrong—for instance, the driver causes Windows 7 to misbehave—you can restore all critical Windows operating system files to the point just before the driver was installed.

INSIDE OUT

Does System Restore affect my files and documents?

System Restore doesn't roll back any changes to your files or documents, nor does it delete any of them. It makes changes only to Windows 7 operating system files.

Configuring System Restore

As shown in Figure 11-5, you access System Restore through Control Panel by clicking System and Security\System and then clicking Advanced System Settings in the left pane.



Figure 11-5 System Restore in Windows 7

In the System Protection tab, you can set the options for System Restore by clicking Configure. You want to make sure the hard disk or partition on which you have Windows 7 installed is set to "Restore system settings and previous versions of files." The system works automatically in the background, protecting your computer.

www.it-ebooks.info

INSIDE OUT Don't deactivate System Restore

Anybody who had a bad experience with System Restore in Windows XP doesn't need to worry anymore. System Restore in Windows 7 is an essential tool, and you should leave it on. It is the quickest and easiest way to get Windows 7 back up and running if you make a change that causes the system to become unstable.

Manually Creating Restore Points

You can also create your own restore points. You might want to do this if you're changing some operating system settings and are not certain what the result will be or if you're installing a piece of software or a hardware driver that you suspect will cause a problem and you want to ensure that a particular restore point is saved. To create your own restore point, click Create in the System Protection tab of the System Properties dialog box shown in Figure 11-5.

Restoring Windows 7 Using System Restore

The quickest way to get into System Restore to restore Windows 7 to an earlier time is to type **system restore** in the Start menu search box.

The System Restore window lists the date and time at which restore points were made and describes what triggered them. You can see in Figure 11-6 that one restore point was an automatically scheduled backup and the other two occurred when Microsoft Virtual PC 2007 was installed and later removed.

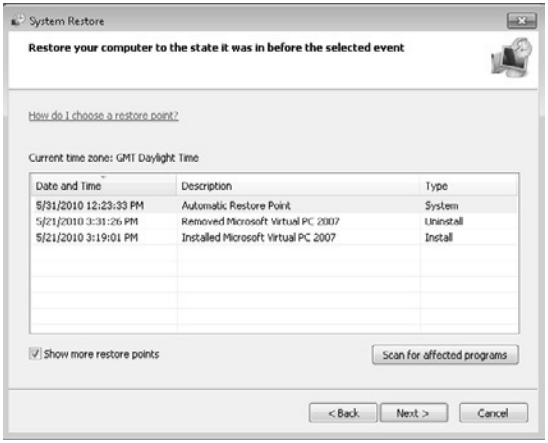


Figure 11-6 Restoring Windows 7 files using System Restore

www.it-ebooks.info

You want to choose the restore point that best reflects the change you want to undo, such as when you installed a new **device driver** or a piece of software. You can click Next to start the process. Your PC needs to restart during this process.

INSIDE OUT Don't worry about picking the wrong restore point

If you err on the side of caution and don't choose a System Restore point that goes back far enough to undo the changes you want to make, don't worry. You can simply repeat the process.

When your PC has restarted and the System Restore has successfully completed, you will see a message like the one in Figure 11-7. You will also be notified if System Restore has been unable to restore your Windows 7.



Figure 11-7 Successful System Restore message

Can I Undo System Restore Changes?

The simple answer is yes, provided you're not using System Restore from Windows Startup Repair (more on this service later in the chapter) or from Safe Mode. As shown in Figure 11-8, a new restore point is created just before your changes are rolled back.

Running System Restore again will give you an option to undo any changes you've made and restore the system to the state it was in before you used System Restore. You would use this option if you realized that restoring older files has, for example, uninstalled a critical program you need.

You can try again with your other restore points until you find one that provides a stable operating system that you can work in.

www.it-ebooks.info

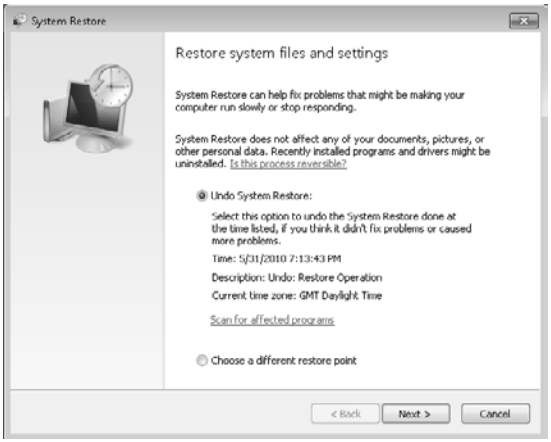


Figure 11-8 Undoing System Restore changes

Troubleshooting Software Compatibility

Recall from Chapter 2, "The Basic Windows 7 Utilities," that when you install software in Windows 7, you will receive a message if the system detects that the software won't work properly. (Older software is especially prone to compatibility issues.) You will receive a prompt that asks whether the software has installed properly and offers to reinstall it automatically in compatibility mode if it hasn't.

This automated feature is extremely useful, but it appears only when you first go to install the software. But what happens if you click Yes, and you then find that the software doesn't work properly, or if it doesn't configure the software properly to begin with?

Manually Setting Program Compatibility

To access the program compatibility options, right-click a program's icon (either on the desktop or in Windows Explorer) or on its entry in the Start menu, and select Properties from the shortcut menu. Click the Compatibility tab in the Properties dialog box, as shown in Figure 11-9, and choose the settings you want to use. Some applications, especially those that ship as part of Windows 7, don't have this option available.

www.it-ebooks.info



Figure 11-9 Adjusting the compatibility settings for a program

Compatibility mode allows you to emulate every version of Windows going back to Windows 95. You should choose the option for the most recent version of Windows in which the software you want to install worked properly.

If you're not sure which version of Windows to choose, try different settings until you find one that works with the software you want to load.

INSIDE OUT

Is there a full list of compatible software and hardware in Windows 7?

A list of software and hardware that is compatible with Windows 7 is located on the Microsoft website at the following address:

http://www.microsoft.com/windows/compatibility/windows-7/en-us/default.aspx

This list isn't exhaustive, but it is comprehensive and a good way to find out whether your software and hardware are compatible with an upgrade to Windows 7.

You can also download a program from this website that checks your software and hardware for compatibility with Windows 7 and produces a report for you.

www.it-ebooks.info

The program compatibility settings offer more options, most importantly the ability to run a program as an administrator (Figure 11-10). You should always be careful with this option because it means the program has complete access to and can modify the Windows 7 system files. Some older software, however, especially custom business software, requires this level of access in order to function.



Figure 11-10 More program compatibility options

You will probably never need the remaining options, which exist for particularly old or problematic software, such as a program that causes an error when run under the Aero Glass Windows 7 interface or doesn't function properly on high-resolution screens.

The Automatic Program Compatibility Troubleshooter

You access the Program Compatibility troubleshooter by typing **program compatibility** into the Start menu search box, as shown in Figure 11-11. Many users may find this an easier way to troubleshoot program compatibility in Windows 7 than by using the manual methods I detailed earlier in this chapter.

The Program Compatibility troubleshooter, shown in Figure 11-12, detects all the software you have installed on your PC and asks which program is causing problems. It then tries different compatibility settings for the program, changing them automatically, and asks you each time whether the program is now working properly.

www.it-ebooks.info

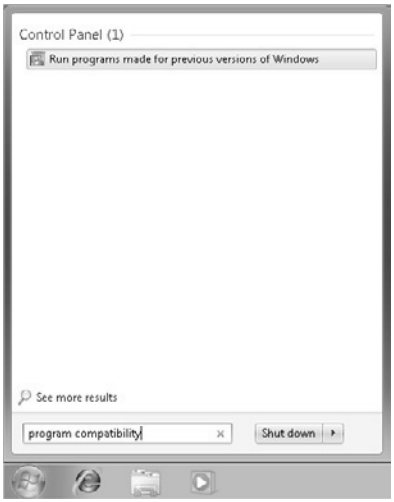


Figure 11-11 Launching the automated Program Compatibility troubleshooter

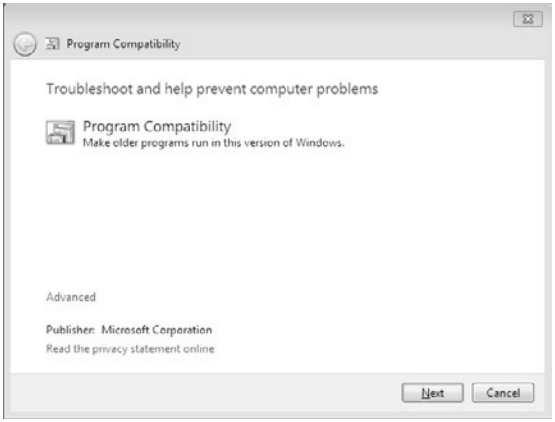


Figure 11-12 The automated Program Compatibility troubleshooter

This troubleshooter is an automated version of the program compatibility options mentioned earlier, but it isn't as flexible as modifying the program compatibility settings yourself.

Program Compatibility Notifications in Action Center

Occasionally, Action Center in Windows 7, signified by the white flag next to the clock on the taskbar, alerts you to a potential program compatibility problem.

www.it-ebooks.info

In Figure 11-13, you can see that Windows has detected that the Adobe Flash Player software has stopped working. Microsoft gathers a significant amount of detail about programs that fail to work. When applications don't work on your computer, you are asked whether you want to send the error information to Microsoft.

Sometimes a fix is suggested. As you can see in Figure 11-13, links are provided to both the Flash Player uninstaller and a website that has the Flash Player update.

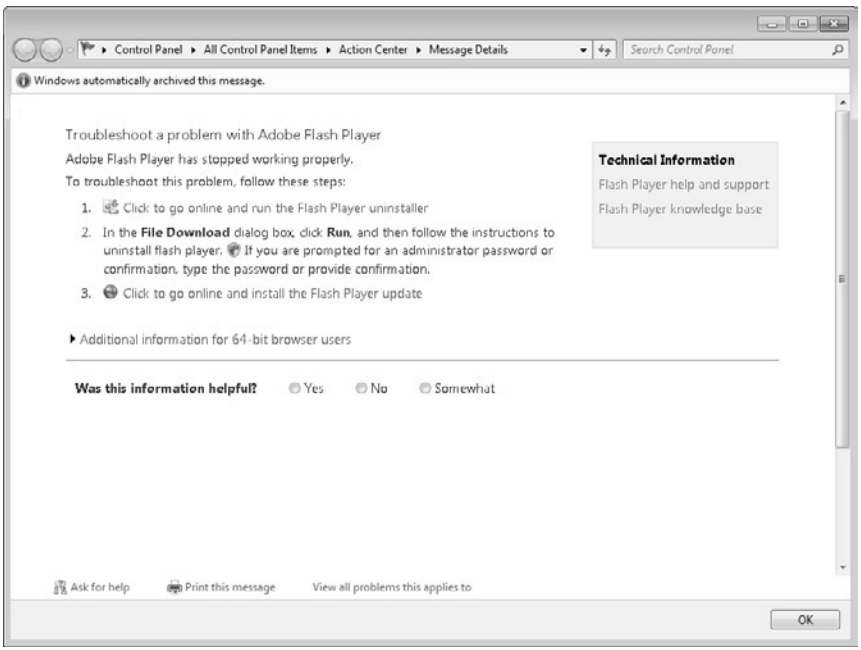


Figure 11-13 The automatic program troubleshooter in Action Center

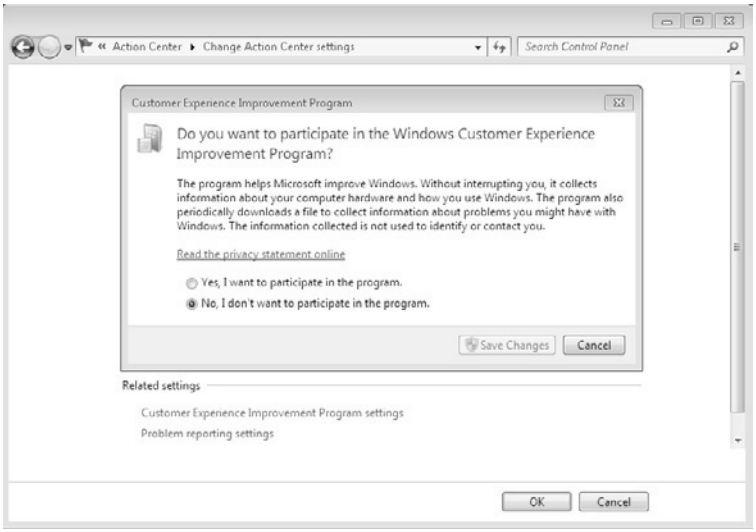
INSIDE OUT

Can you opt out of Windows automatically sending information about your PC to Microsoft?

Some people guard their privacy jealously and don't want Windows sending any information to Microsoft. The data sent to Microsoft doesn't include any personally identifiable information, but you can opt out of sending any information in Action Center.

In Action Center, select Change Action Center Settings in the left pane, and then click Customer Experience Improvement Program Settings. As shown here, you can opt out of this program by selecting "No, I don't want to participate in the program."

www.it-ebooks.info



I recommend that you leave it switched on. This tool is useful, and turning it off might mean that you don't automatically receive useful troubleshooting advice about Windows 7 from Microsoft.

Windows XP Mode

For software that doesn't work in Windows 7, there's always Windows XP Mode. I talked about this add-in at some length in Chapters 2, 3, and 8. Windows XP Mode is a fully licensed copy of Windows XP Professional that allows you to install software that runs in Windows XP, complete with blue windows, but is accessible from your Windows 7 Start menu and runs on your Windows 7 desktop.

Windows Won't Start

Occasionally, Windows 7 just won't start. A configuration file or some other minor issue is usually what prevents Windows 7 from starting correctly in such cases. You can get frustrated when even restarting your computer several times doesn't work. Sometimes the answer is as simple as turning off your machine and turning it on again.

www.it-ebooks.info

Last Known Good Configuration

When you start your computer, press the F8 key just after the BIOS screen has disappeared. If you see the "Starting Windows" logo, you've gone too far and will have to try again. Pressing F8 brings up the Windows startup options, as shown in Figure 11-14.

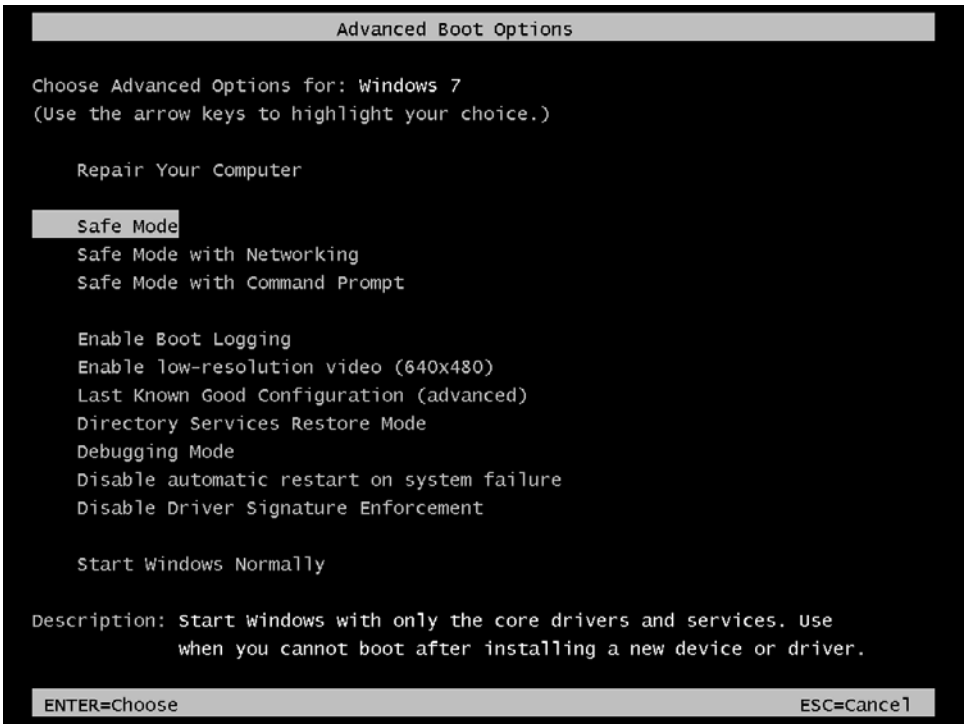


Figure 11-14 Windows startup options

From these options, select Last Known Good Configuration (advanced) to reset the current Windows 7 instance in favor of the one recorded the last time Windows successfully started.

Windows 7 should now start. Note that this option won't change any Windows settings since you last started the operating system, so it's perfectly safe to use.

Safe Mode

If the Last Known Good Configuration doesn't get Windows 7 started, you can choose another option from the Advanced Boot Options. Again, press F8 when starting your computer, and this time choose the Safe Mode option.

www.it-ebooks.info

If Windows 7 loads to the Safe Mode desktop, shut down your computer and restart it. Many startup problems with the operating system are fixed using this option.

INSIDE OUT Avoid the reset button

You should avoid restarting your computer by using the reset button, especially if you're restarting only because you haven't pressed F8 in time to show the Advanced Boot Options. If possible, let Windows load to the desktop, and then restart your computer using the Restart option from the Start menu.

Pressing your computer's reset button at the wrong time can cause essential Windows 7 startup files to become corrupt.

Windows Startup Repair

If Windows 7 fails to start after three tries, Windows Startup Repair will appear the next time you start your computer. Windows Startup Repair is a fully automated feature that replaces the Recovery Console from previous versions of Windows. Figure 11-15 shows the dialog box you'll see when the Startup Repair tool appears.

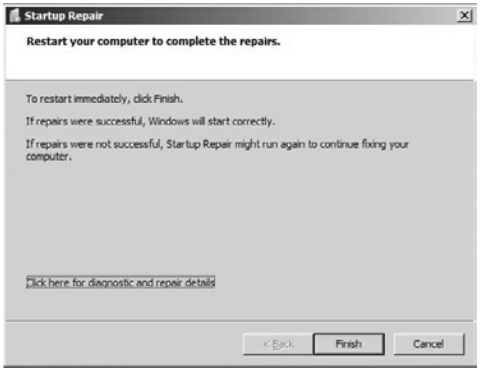


Figure 11-15 Windows Startup Repair

This service looks at your Windows 7 installation and tries to identify and fix any problems that are preventing Windows 7 from starting. If the service finds something wrong, it attempts to repair the problem and then prompts you to restart the computer if the problem is fixed.

www.it-ebooks.info

If Startup Repair is unable to fix the problem, it asks whether you want to restore Windows from a System Restore point, as shown in Figure 11-16. A faulty hardware driver or a recently installed piece of software are common culprits that prevent Windows 7 from starting.

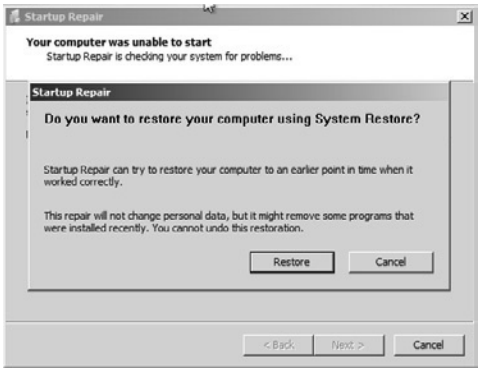


Figure 11-16 System Restore option in Startup Repair

As a final option, you can restore Windows 7 from an image backup, as shown in Figure 11-17. If you use this option, you lose any updates and new software installed since the backup was made. Startup Repair offers this option only if it can't repair the problem any other way.



Figure 11-17 Image backup option in Startup Repair

Startup Repair from an Install DVD or a System Repair Disc

You can also run Startup Repair from your Windows 7 install DVD or a System Repair disc. These approaches offer you more options for fixing your computer when it won't start. When starting from your Windows 7 install DVD, at the install screen, click Repair Your Computer, as shown in Figure 11-18.

www.it-ebooks.info

You can also access Repair Your Computer from the boot menu (by pressing F8 at startup). You will only be able to access this if the Windows boot loader on the hard disk has not been deleted or corrupted.



Figure 11-18 Install DVD screen showing the Repair Your Computer option

As shown in Figure 11-19, you have additional options for system recovery on the installation DVD, such as diagnosing your computer's memory or using manual commands through a Command Prompt. Chapter 15, "Advanced Repair Methods," has more details about the Command Prompt options.



Figure 11-19 Additional repair options from the install DVD

You Did Back It Up, Didn't You?

If you still can't get Windows 7 to start, you should choose System Image Recovery and restore Windows 7 from a backup. I covered backups in Chapter 1, "Prevention Is Better Than Cure." Sadly, if you don't have a system image of your Windows 7 installation, you will need to reinstall your operating system, including all of your programs and updates.

www.it-ebooks.info

Working with Device Drivers

There are hundreds of thousands of hardware devices for PCs, ranging from super-cheap components to extremely expensive graphics cards. Microsoft has a certification program for hardware drivers, but it isn't mandatory for the 32-bit versions of Windows 7, and many hardware manufacturers don't want to pay for it.

With the 64-bit editions of Windows 7, driver certification is mandatory, but you can still install drivers that are uncertified. Once you realize that hardware drivers control your whole experience with Windows, you won't be surprised to discover that uncertified device drivers can cause problems with Windows or even cause the operating system to fail to start. They are one of the biggest causes of computer problems.

Fortunately, Microsoft has made working with hardware drivers easy in Windows 7, so if you need to remove, reinstall, or update one, you shouldn't encounter any problems. Before explaining how you handle device drivers in Windows 7, I'll warn you of some of the issues that can occur with device drivers.

Common Problems with Device Drivers

Device driver problems are at the root of many issues with Windows 7. Here are some of the most common ones.

- Windows doesn't start.
- A device stops working.
- A device starts misbehaving.

A problem often occurs for the first time after you've performed one of the following actions.

- Installed hardware for the first time.
- Updated the hardware driver manually.
- Updated the driver through Windows Update.

Recently, a media PC of mine, which had always been extremely stable, suddenly began crashing regularly. The crashes began shortly after a Windows Update that had included a new driver for the networking card. So I rolled back that driver to the previous version, and the problem immediately went away.

www.it-ebooks.info

I was lucky I found the problem so quickly. Sometimes device problems can be difficult to diagnose. On this same PC, Windows Update had recently installed numerous updates because I had just restored this PC from a backup that I had made a year ago. I had also placed a Nintendo Wii games console on top of it, which could have caused overheating or electrical interference that could also have been the source of the problem. If the driver rollback had not worked, I could have spent hours diagnosing the problem that was causing my media PC to crash.

In Chapter 13, "Advanced Troubleshooting," I'll tackle the topic of diagnosing device problems in more detail. For now, let's deal with troubleshooting techniques for specific drivers.

Graphics Driver Problems

Some of the most common driver problems occur with the computer's graphics drivers. The graphics card driver differs from other Windows drivers because it is the first driver to load when Windows starts.

Here are a few common problems caused by graphics drivers.

- Windows loads but has no picture.
- Windows shows the **Blue Screen of Death (BSOD)** while loading, as shown here.



- Your screen resolution is stuck at its lowest settings.
- Windows 7 crashes while loading games.
- You can't use the Aero Glass interface in Windows 7.

www.it-ebooks.info

If you encounter one of the problems I have described, it's best to start your PC in Safe Mode. As mentioned earlier in the chapter, you do this by pressing F8 when Windows starts but before the Starting Windows screen appears (see Figure 11-20.) If you see this screen, you have gone too far and need to restart your PC again.



Figure 11-20 Windows 7 loading screen

Pressing the F8 key brings up the Advanced Boot Options screen (shown earlier in Figure 11-14). Choose Safe Mode, and press Enter. This is a reduced functionality mode where Windows loads the minimum drivers and software.

Refer to the "Windows Won't Start" section earlier in this chapter for more options.

Device Manager

Device Manager, shown in Figure 11-21, is where you can see and control all the drivers for the hardware installed on your PC. You access Device Manager through Control Panel. Click Hardware and Sound\Device Manager. Alternatively, you can type **device manager** in the Start menu search box.

www.it-ebooks.info

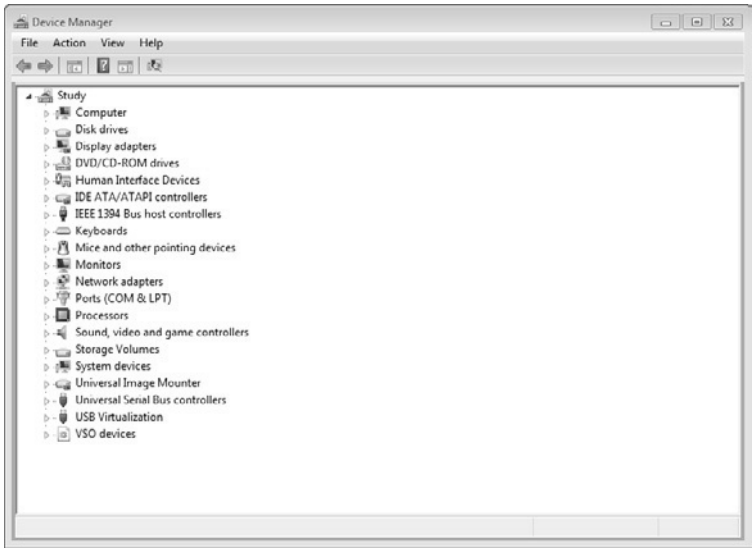


Figure 11-21 Device Manager

The hardware is organized into categories, most of which are self-explanatory: disk drives, display adapters, DVD/CD-ROM drives, keyboards, network adapters, and so on.

Some categories need more explanation.

- **Human Interface Devices** is where drivers for hardware such as USB input devices (such as graphics tablets and remote control sensors) are located.
- **Sound, video and game controllers** includes everything from your PC's sound card and gaming joystick to TV tuner cards and **webcams**.

A white arrow precedes each category. Clicking it expands the category to display all the hardware within it, as shown in Figure 11-22. Here you can see any drivers that may not be working (they will be highlighted with a yellow warning triangle or a red cross) or see whether they're even listed.

www.it-ebooks.info



Figure 11-22 Viewing specific hardware in Device Manager

A yellow warning triangle next to a device, as shown in the Generic volume items in Figure 11-23, means that the driver either isn't installed or isn't working properly. If any devices have warning triangles, these groups will expand automatically when Device Manager starts.

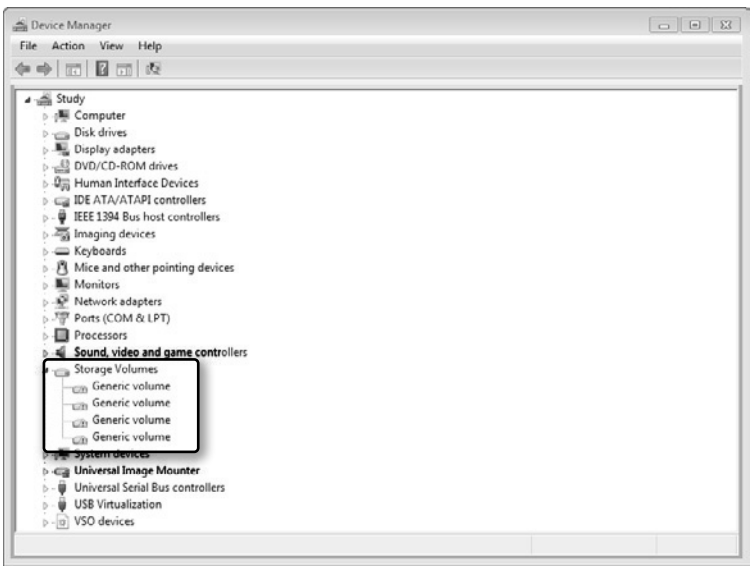


Figure 11-23 Problem hardware indicated by a warning triangle

www.it-ebooks.info

If your hardware isn't listed, on the Action menu, select Scan For Hardware Changes, as shown in Figure 11-24. After the scan, your hardware should appear in the list, and Windows 7 might automatically install the correct driver for that hardware. Windows will inform you whether an appropriate driver has been found and installed or whether no driver could be found.

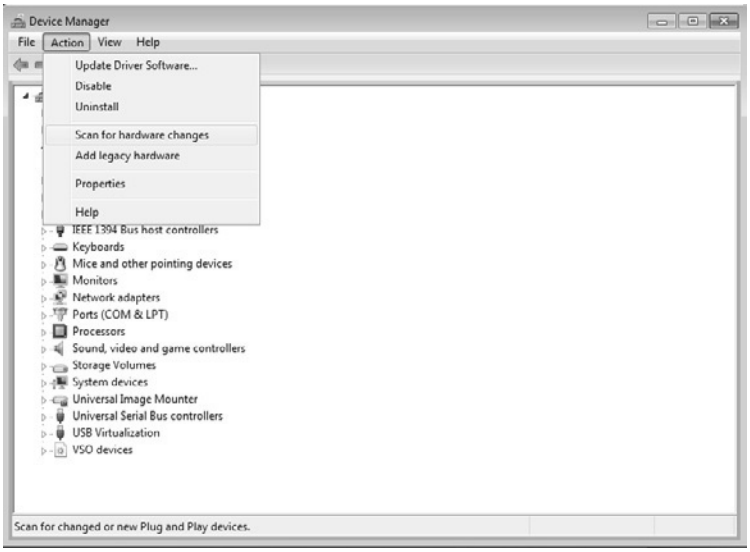


Figure 11-24 Searching for new hardware in Device Manager

If your hardware still doesn't show up, on the View menu, select Show Hidden Devices, as shown in Figure 11-25. The hidden devices are usually hardware drivers for Windows components, but they can also include your PC's hardware.

In the recent example I mentioned in which a network device driver was causing my computer to crash, the driver, which had been digitally tested and distributed through Windows Update, didn't appear in Device Manager until I clicked Show Hidden Devices.

www.it-ebooks.info

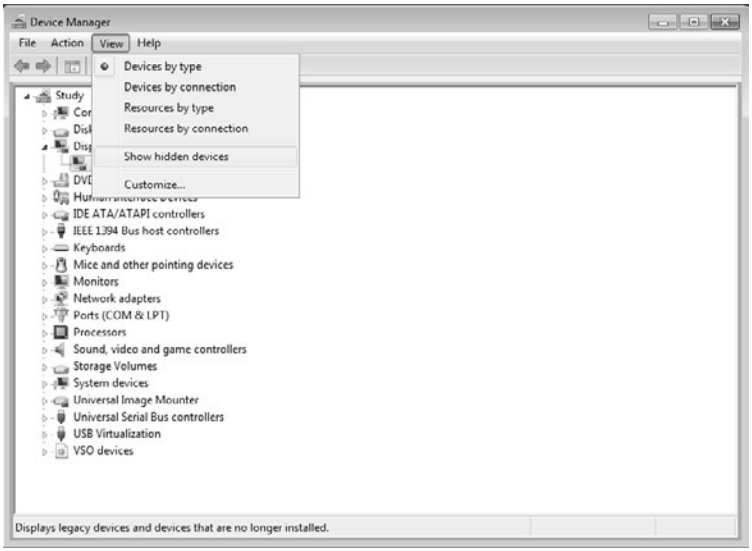


Figure 11-25 Viewing hidden devices in Device Manager

What If My Hardware Still Doesn't Appear?

There are a few situations in which your hardware still doesn't appear in the device list. At this point, ask yourself the following questions.

- Could my hardware be called something else in Device Manager? Look through the list to see whether your hardware shows up with a different name from the one you're expecting. For example, many devices are simply called "Human Interface Device."
- If my device is removable, such as a USB device, does unplugging it cause something to disappear from the device list?
- Is my device firmly plugged in, and are all the relevant power and data cables attached to it? Make sure your PC is turned off and disconnected from the main electrical supply before checking this.

With USB and other removable devices, if Windows doesn't make any sound when you plug in your device or you don't see a small notification window on the right of the taskbar

www.it-ebooks.info

telling you the hardware has been found, Windows might not be seeing the device. There are several things you can try at this point.

- Plug your device into a different port. For example, if your device is USB, check the ports on the front of your PC as well as the ones at the back.
- Try a different connecting cable.
- If your device requires its own external power supply, make sure that it is connected, turned on, and receiving power.
- Leave the device plugged in, and restart your computer.

INSIDE OUT Using older USB devices

Some older USB devices (and possibly some new ones) require that you install the device driver from the supplied CD before plugging the device into the computer for the first time. Check the manual that came with your hardware, or look for FAQs on the manufacturer's website.

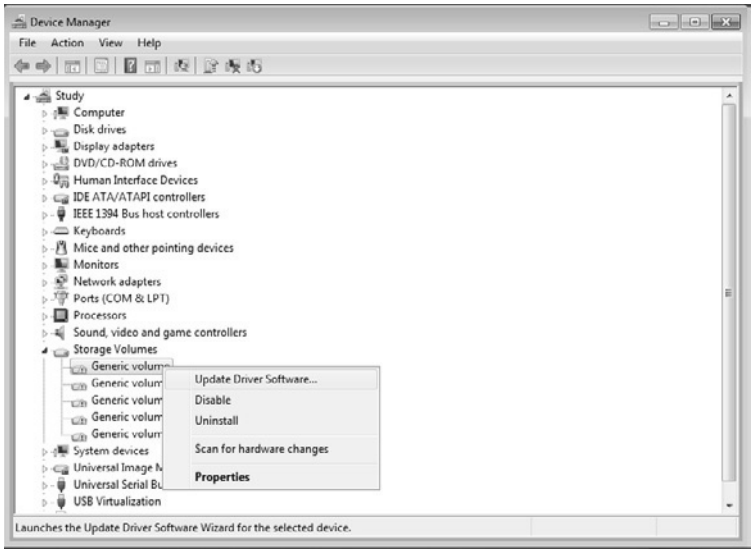
If you still can't get your device to work, the device might be faulty. Try to use the device on another PC. This test will be much easier with a USB or other removable device. If the device is a graphics card, however, you might want to check the manufacturer's website for support and check out some help forums before trying to install it on a different PC.

Installing Device Drivers

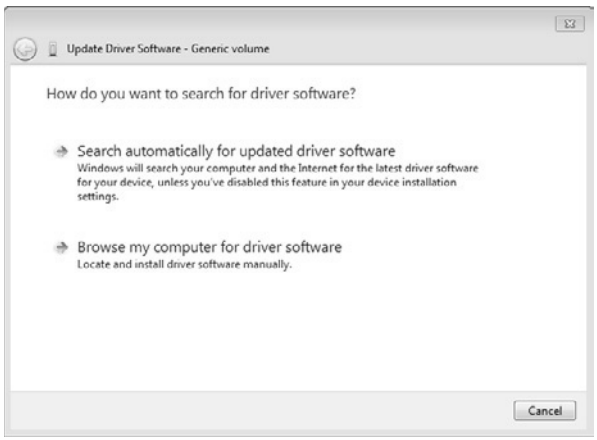
Windows normally updates the drivers for new hardware automatically. Even though Windows 7 comes with more hardware drivers than any earlier version of Windows, it still might encounter drivers it won't find or be able to install automatically.

1. To install the driver for a device, right-click it in Device Manager, and select Update Driver Software from the shortcut menu.

www.it-ebooks.info



2. You can choose to have Windows 7 find and install the driver or to install it manually from a disk or another location. If you have a copy of the driver on CD or DVD, select Browse My Computer For Driver Software.



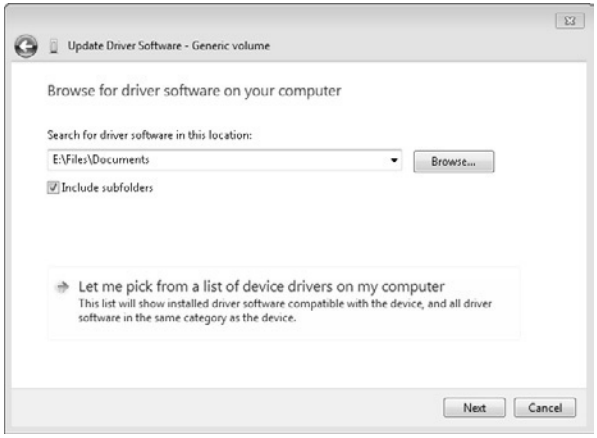
www.it-ebooks.info

INSIDE OUT

Always make sure you have a copy of your network/Wi-Fi driver

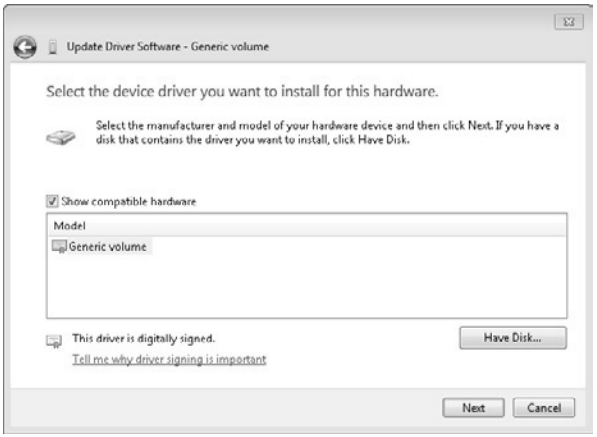
If Windows doesn't come with a suitable driver for your network or Wi-Fi card, you must make certain that you have a copy on a disk ready to install. If you don't, Windows won't be able to search online for a driver for you, and the hardware will not work.

3. Windows 7 will ask where it should look for a driver. You can browse to the location on your hard disk or CD where the driver is located. Sometimes you want to manually select which driver you want Windows to install, for example, if Windows 7 has been unable to find the exact driver for your hardware when looking automatically. In that case, select Let Me Pick From A List Of Device Drivers On My Computer.



4. Click Have Disk, as shown in the following screen, and navigate to the folder on your hard disk or CD where the driver is located. The folder should be something like Device Name\Driver\Win7. Only device drivers will appear in this list—not any other files that might be there. Choose the correct driver, and click OK.

www.it-ebooks.info



Sometimes when you're installing a driver manually the drivers folder will include several driver (.inf) files. You may have to go through the manual driver install process several times to find the correct one.

INSIDE OUT

Why not just install drivers using the setup program on the supplied CD?

Installing a driver from the CD the manufacturer supplies with it can be quick and easy. In certain situations, however, you shouldn't install the driver this way. For example, if the hardware is older and the supplied CD doesn't include Windows 7 drivers, don't install the driver via the CD (although most of the time Windows Vista drivers will still work).

There are also manufacturers—especially those who make Wi-Fi, graphics, and printer/scanner hardware—that include extra software on the driver CD that, by default, is set to load every time you start Windows.

Removing and Reinstalling Device Drivers

You might want to remove a device driver from Windows when you are updating it. One of the reasons for doing this is that when you reinstall the driver, Windows might automatically reinstall the previous version of the driver that doesn't work and that you don't want.

To uninstall a device driver in Device Manager, right-click the device and select Uninstall from the shortcut menu, as shown in Figure 11-26.

www.it-ebooks.info

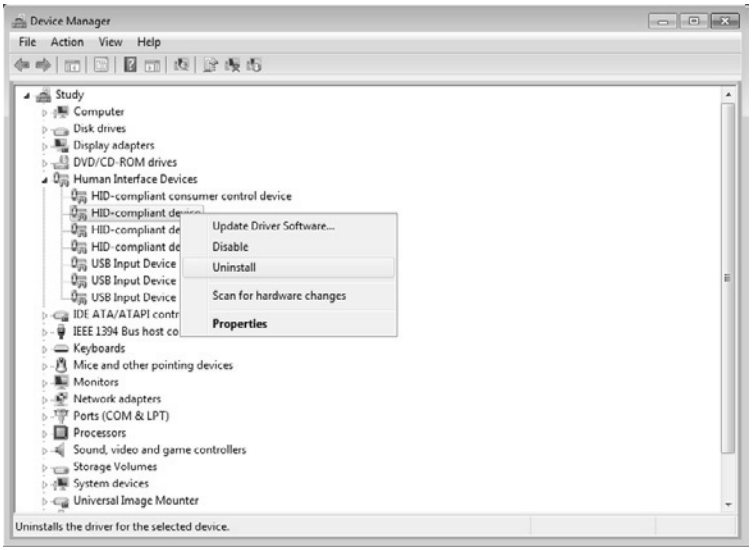


Figure 11-26 Removing a device driver from Windows

With many devices, Windows then asks if you want to delete the driver software for this device (see Figure 11-27). You should select this option if you want to reinstall a specific driver and not have Windows reinstall this one. The installed driver files are then deleted from your hard disk.



Figure 11-27 Deleting the driver from Windows

You can now reinstall the driver.

www.it-ebooks.info

Updating Device Drivers

Windows sometimes offers updates to device drivers through Windows Update, but at times you will have downloaded the driver from the manufacturer's website.

INSIDE OUT If it isn't broken, don't fix it!

Do you really need the latest driver for your hardware? If you use your PC for gaming, you probably want to keep your graphics drivers updated for speed and stability. For most hardware, however, you may not want to install the latest drivers.

Remember my cautionary tale from earlier about the media PC, which sat under my living room TV, and the new networking driver for it that was pushed down, admittedly as an optional update, by Windows Update.

I didn't actually need this driver; the PC ran fine with the existing driver. And as it turned out, this new driver caused my machine to constantly crash.

To update the driver for a specific piece of hardware, in Device Manager, right-click the device and select Update Driver Software from the shortcut menu, as shown in Figure 11-28. Now you can follow the process described in the preceding "Installing Device Drivers" section.

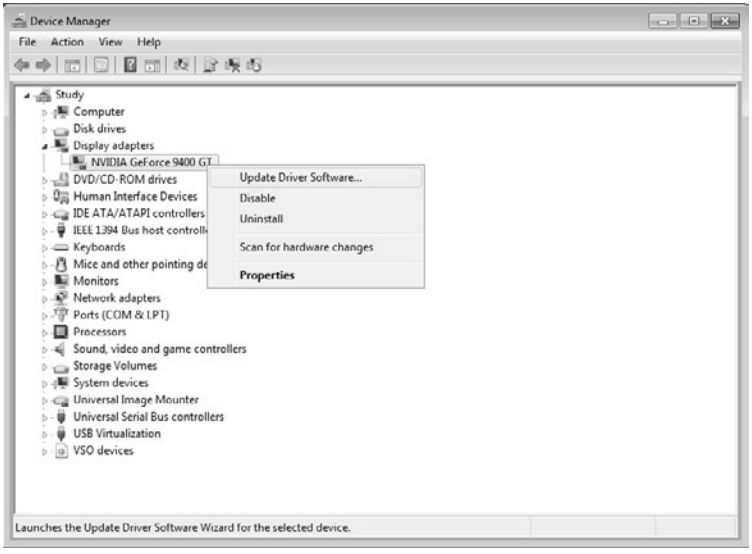
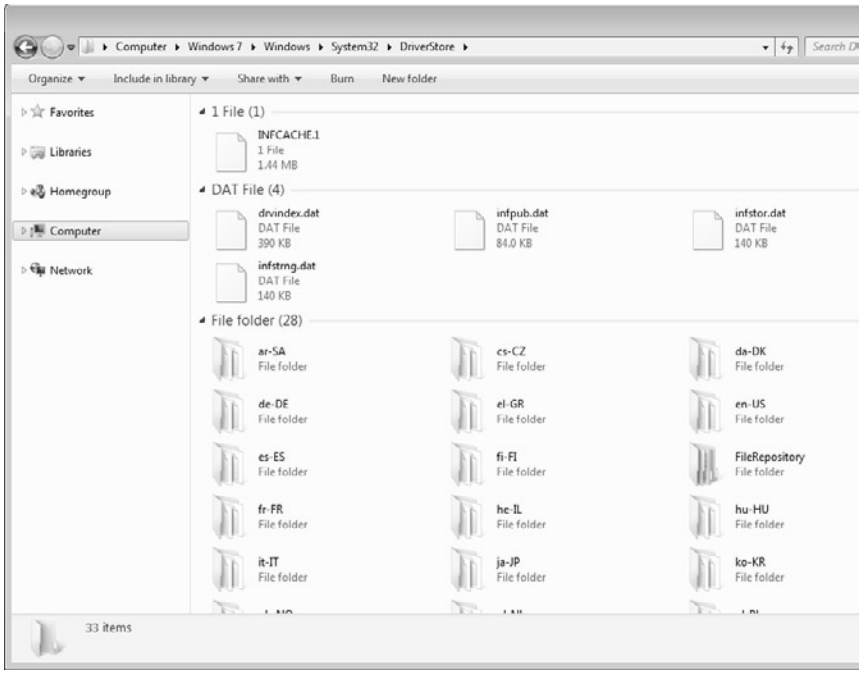


Figure 11-28 Updating a driver in Device Manager

www.it-ebooks.info

INSIDE OUT How to back up device drivers in Windows 7

You can back up all of your device drivers if you want to—for example, because you've lost the original driver CD for a piece of hardware. You can find these device drivers on your Windows drive (usually C:\) in the Windows\System32\DriverStore folder.



You can back up this entire folder and copy it back if you need to reinstall Windows. After doing this and restarting the PC, Windows should be able to install the correct drivers for all of your installed hardware.

Rolling Back Device Drivers

Sometimes, as in the case of the updated network driver that caused my media PC to crash, you want Windows 7 to reinstall the previous driver, the one that worked. This is easy to do.

In Device Manager, right-click the correct device and select Properties from the shortcut menu. The dialog box in Figure 11-29 appears. Click the Driver tab. Here, if there is a previous driver that Windows 7 can roll the system back to, you can click Roll Back Driver. This starts an automated process that removes the current driver and reinstates the previous one. Your PC might need to reboot during this process.

www.it-ebooks.info

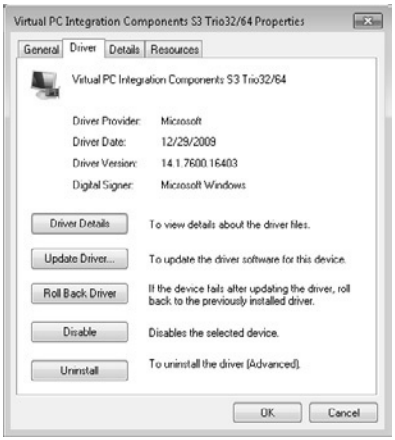


Figure 11-29 Rolling back a device driver

Action Center Troubleshooter

The new Action Center in Windows 7, indicated by the white flag next to the clock on the right side of the Windows 7 taskbar, has an excellent Troubleshooting panel that helps you fix common problems in Windows 7. You access it by clicking the flag and opening Action Center. Next click the Troubleshooting (Find and fix problems) link at the bottom of the Action Center window (you might have to scroll down the window) to bring up the trouble-shooters, as shown in Figure 11-30.

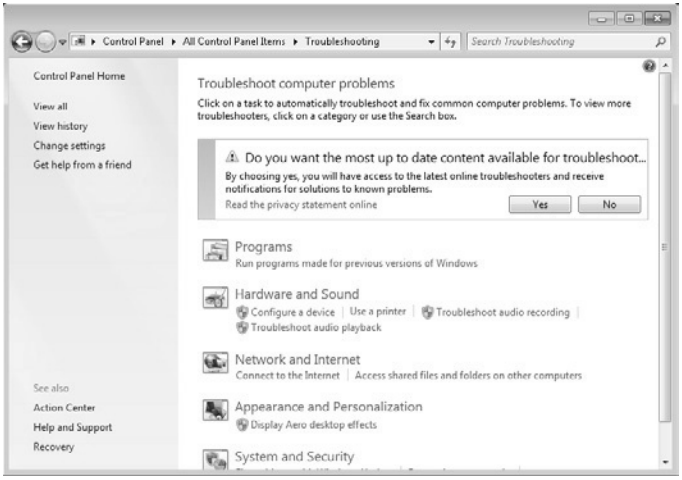


Figure 11-30 Action Center troubleshooters

www.it-ebooks.info

This panel contains many automated Windows 7 troubleshooters that are easy to run. They don't always find and fix the problem with your PC, but this panel is an excellent place to start troubleshooting minor issues.

Microsoft Fix It Center

Microsoft provides an automated problem-solving solution for all versions of Windows. The Microsoft Fix it Center can be downloaded from **support.microsoft.com/fixit** and is an automated service that attempts to detect and repair problems with Windows, as shown in Figure 11-31.

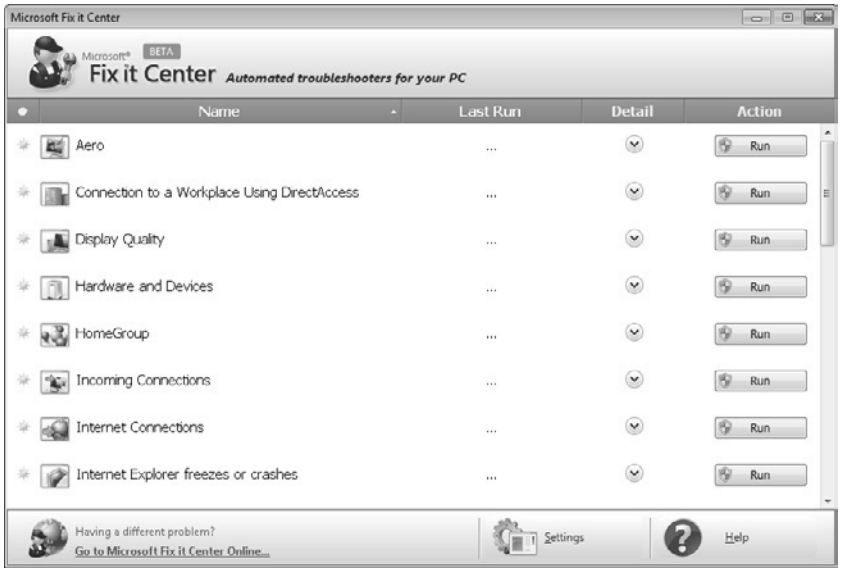


Figure 11-31 The Microsoft Fix it Center

This is an excellent piece of software that I would recommend you run periodically to check for solutions to problems on your PC.

Summary

There are many simple and easy ways to fix problems in Windows 7. Microsoft provides a great set of tools, both in the operating system and downloadable, for doing so. It's worth familiarizing yourself with these tools, especially if you provide support to other people, as they can save significant amounts of time. Even PC novices can use these tools.

www.it-ebooks.info

www.it-ebooks.info

PART 3

Technical Fixes

CHAPTER 12
What Is Windows 7 Anyway? 199

CHAPTER 13
Identifying the Source of a Problem 205

CHAPTER 14
Advanced Diagnostic Tools in Windows 7 . . 217

CHAPTER 15
Advanced Repair Methods 231

CHAPTER 16
Windows Problems Demystified 257

CHAPTER 17
Remote Help 273

CHAPTER 18
Where to Find More Help and Support 289

CHAPTER 19
Diagnosing Hardware Problems 295

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 12

What Is Windows 7 Anyway?

The Windows 7 File and Folder Structure. 199
How Does Windows Compare to Other Operating Systems?. 202
Summary 203

Windows 7 is the latest edition in a series of desktop operating systems and graphical user interfaces (GUI) from Microsoft. Windows 1.0 was released in 1985 as a GUI that sat on top of Microsoft's popular DOS disk operating system. Over the years Windows has been changed and refined, finally subsuming DOS and becoming a full operating system in its own right with the launch of Windows 98.

Windows 7 was released in October 2009. It is not exactly the seventh version of Windows. Rather it is the seventh version from its particular branch of the software. There have been two branches of Windows: the original consumer versions and the New Technology (NT) business versions. The original consumer lineup included the popular Windows 3.1, Windows 95, and Windows 98. It ended with Windows Me. The NT series began in 1993 as an offshoot of Windows 3.1, with much of the underlying code reengineered to make it more stable and suitable for business users. This NT development tree has split off further with the Server, Desktop, and Home Server variations of the operating system. In turn, the NT branch spawned various server versions of the operating system and then Windows XP, Windows Vista, and most recently, Windows 7.

There is some debate about whether Windows 7 really is the seventh iteration of the NT family, but it's not the most important concern facing the world today. Windows 7 is *officially* the seventh iteration if you follow the tree Windows 1.0, Windows 2.0, Windows NT 3.1, Windows NT 4.0, Windows XP, Windows Vista, and Windows 7. Depending on your view, there have been as many as 28 versions of Windows since it first launched, up to 2010.

Windows in its various versions is currently used by approximately four billion people worldwide.

The Windows 7 File and Folder Structure

Windows runs from a series of files and folders on your computer's hard disk. The basic folder structure is extremely logical and has been simplified immensely over the years. There are three basic Windows 7 folders with some extra folders for user and configuration data and temporary files, as shown in Figure 12-1.

www.it-ebooks.info

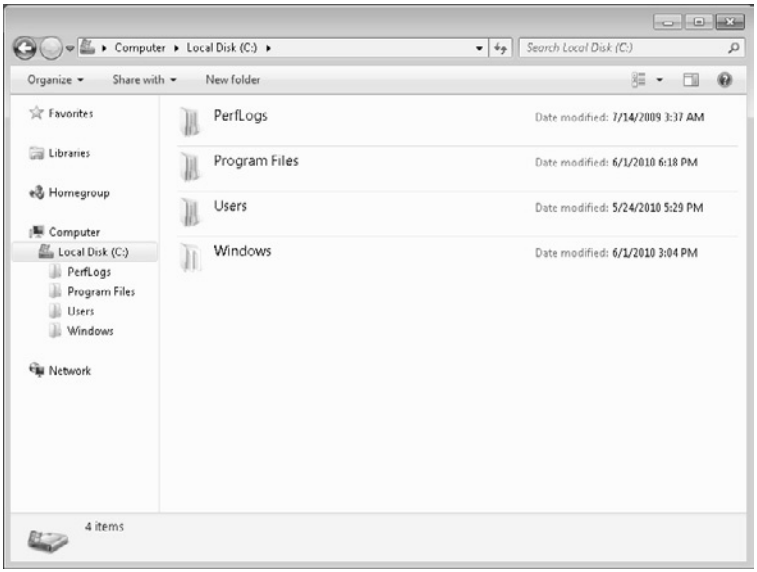


Figure 12-1 The folder structure in Windows 7

- **Program Files** This is where all the files for any programs and software you install in Windows 7 sit. There are two Program Files folders in the 64-bit version of Windows 7: Program Files x86 for 32-bit software and Program Files for newer 64-bit software. Each program sits in its own custom folder under one of these folders. In the 32-bit version, there is only a Program Files folder.

- **Users** This is where, by default, all of your documents and files sit, and it is also the location of the Windows registry, the database of settings for Windows and your software. Within the main Users folder, there is one subfolder for each user and another folder called Public, where shared files and folders are kept. There are also hidden user folders called Default and All Users.

- **Windows** This is the main folder into which the operating system is installed.

Windows also installs hidden system files across the disk (seen slightly dimmed in Figure 12-2), including the Root folder.

www.it-ebooks.info

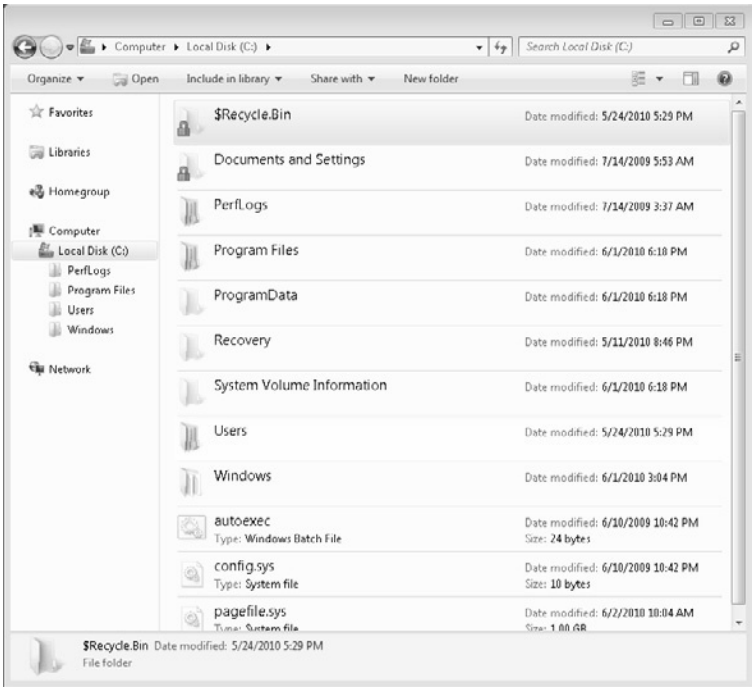


Figure 12-2 Hidden system files installed by Windows 7

These hidden files and folders are where Windows stores operating system recovery software and folders to support legacy software, including Documents and Settings and the Autoexec.bat and Config.sys files that date back to the earliest versions of DOS.

Inside the main Windows folder are a great many different folders, some of which exist to maintain compatibility with legacy hardware and software and some of which service specific features within the operating system (see Figure 12-3).

www.it-ebooks.info

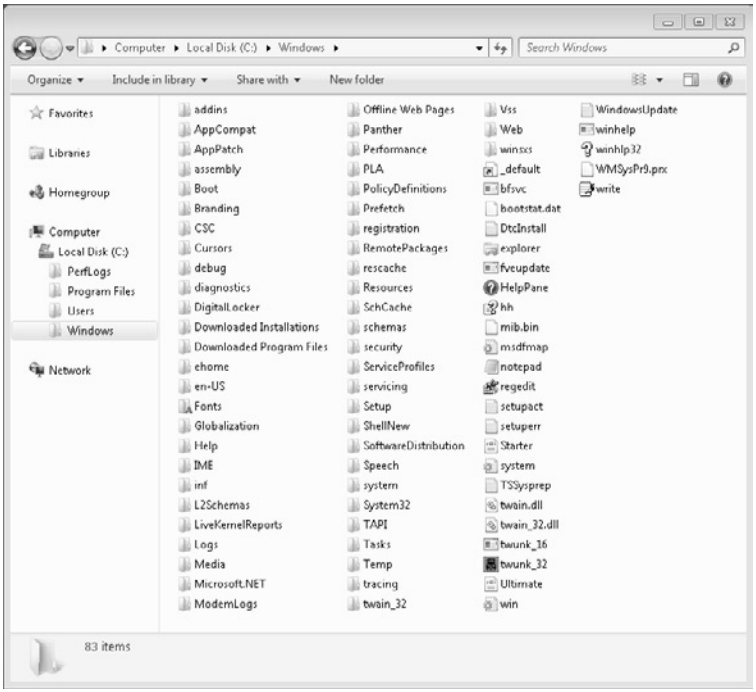


Figure 12-3 The main Windows operating system files and folders

All of these files and folders are essential, and you should not move, rename, or delete any of them. Folders you might find of particular interest include the following.

- **Globalization** This is where you will find the desktop wallpapers in Windows.
- **Resources** This is a similar folder to Globalization but is for Windows desktop themes.
- **System32** The main operating system files, including hardware device drivers, are located in this folder.

How Does Windows Compare to Other Operating Systems?

Windows was built over the foundation of the DOS disk operating system that shipped with the very first PCs from IBM in the early 1980s. This brought with it several problems, many of which still exist today. The biggest issue is the need to maintain compatibility with legacy hardware and software. DOS did not support or need to support multiple users or multi-tasking. Support for these has been added with later versions of Windows.

www.it-ebooks.info

As computers have changed in the last 30 years, and with the introduction of new technologies such as the Internet, the need for extra security has come to the forefront of operating system design. Unfortunately, this has meant having to build security over the top of the existing Windows system. This has inevitably led to some compromises and security flaws, which have been exploited by the authors of malicious software.

With Windows 8, it is rumored that the legacy support will be moved into a virtual machine. This means that the security subsystem in Windows 8 will be able to be treated differently, making it much more secure.

Most other desktop and server operating systems, including Linux, Apple OS X, and Google Chrome OS, are all built on top of an operating system called UNIX. This operating system was developed in 1969 and was initially designed to accommodate multitasking and multiusers on mainframe computers.

This means that user permissions and overall operating system security have always been handled differently in UNIX, with users never being given default administrator access to the operating system files. UNIX has slowly made its way from mainframe and minicomputers over the years to the desktop market, during which time this security system has remained unchanged.

None of this means that Windows 7 is an insecure and unstable operating system, quite the opposite. It is the most secure and stable operating system that Microsoft has ever released, and many experts believe it to be every bit as secure as a UNIX-based operating system. It is the vast popularity of Windows that has made it such a security target in the past.

Summary

Windows is, as I have said, a hugely complicated piece of software engineering that is built on many layers to provide backward compatibility and stability. Occasionally, however, you'll still need to find something within its thousands of files. Fortunately, the operating system is logically and sensibly organized. This will help you troubleshoot problems and can make someone else describing a problem to you much simpler.

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 13

Identifying the Source of a Problem

Taking a Step-by-Step Approach 205
Why Problems Occur with Windows 211
What Are the Causes of Common Problems? 213
Have You Tried Turning It Off and On Again? 214
The Blue Screen of Death 214
The Perpetual Restart 215
Summary 216

In Sir Arthur Conan Doyle's novel *The Sign of Four*, the second story featuring the world's greatest detective, Sherlock Holmes, the gallant hero makes one of his most famous statements when addressing his loyal friend, Doctor Watson:

"When you have eliminated the impossible, whatever remains, however improbable, must be the truth."

I have always used this theory as the basis for all technical support because it implies that you have to take a methodical, step-by-step approach to diagnosing problems. I find it much easier and quicker to diagnose what *isn't* causing a problem than to identify what actually *is* causing it. This is especially true when diagnosing problems with computers, operating systems, and software, all of which can be extremely complex.

Taking a Step-by-Step Approach

The first step in taking this approach with a Windows 7 problem is to eliminate the impossible. For example, if you suspect Windows is causing an instability issue with a hardware device, unplug all the devices that you can (USB flash drives, joysticks, and so on), leaving only the keyboard, the mouse, and the monitor attached. If the problem persists, you have very quickly established that the unplugged devices *aren't* part of the problem, and you can investigate another cause. But if the problem goes away, you know that one of the unplugged devices is the cause. Plug in the devices one at a time. When the problem resurfaces, you will have identified which of the devices is at fault.

Similarly, if you suspect that software is causing a problem, you can shut down all of the software at once. If the problem persists, you can eliminate software as the source of the issue. However, if the problem goes away when all of the software is shut down, you can be reasonably sure that software is the root of the problem. To identify which program is at fault, shut down each software package one at a time until the problem goes away.

www.it-ebooks.info

This all sounds incredibly simple and straightforward, I know, but I recognize that there are a great many occasions when a technique as simple as unplugging hardware and shutting down software doesn't work. However, this process is an essential first step to identifying what really *is* causing a problem.

At this point in a troubleshooting book, you probably expect to find a large and very complex flowchart to follow: Is it A or B? If it's B, then go this way and do X, Y, and Z. However, with PCs, there are countless possible causes for the problems you might encounter, and so any such flowchart would cover a football field and might not help you diagnose the problem.

You would be amazed how frequently I encounter a problem that neither I nor my colleagues have ever seen before, even after years of providing IT support. There are simply millions of possible things that can go wrong with your PC and your copy of Windows. The Microsoft Knowledge Base at *http://support.microsoft.com* contains several hundred thousand articles about Windows problems and still does not address them all. This is where taking a more structured and step-by-step approach can help enormously. Because of the structured nature of the diagnosis, you can be certain all of the time where your troubleshooting is at.

Minimum Windows Configuration

Sometimes it's a good idea to begin with the minimum amount of software running and hardware installed to help diagnose what's causing an issue. The basis of this approach is this statement: Reduce your operating Windows system to its minimum configuration to diagnose the problem. You can reduce the amount of running software in several ways. One way is to use the system tray. Click the small up arrow on the right side of the taskbar to access the system tray. As shown in Figure 13-1, the system tray displays some, but not all, of the programs that are currently running on the computer. To exit a program, right-click and select Exit, or open it if an exit option doesn't appear, so you can close the program appropriately.

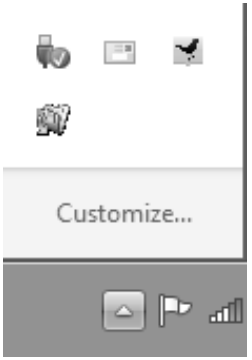


Figure 13-1 Shutting down programs from the system tray

www.it-ebooks.info

You can also shut down programs through Windows Task Manager. To access Task Manager, right-click the taskbar and select Start Task Manager, or press Ctrl+Alt+Del on your keyboard and select Start Task Manager. You can view running applications on the Applications tab or by examining the processes on the Processes tab. To shut down a program from the Applications or Processes tab, right-click its corresponding process and select End Task (on the Applications tab) or End Process (on the Processes tab), as shown in Figure 13-2.



Figure 13-2 Shutting down programs from Task Manager

As shown in Figure 13-2, End Process Tree is another option on the context menu you access by right-clicking a process on the Processes tab. This option can be useful if you have either a series of similar processes (one Internet Explorer process for each of several tabs in your browser, for instance) or a series of processes that rely on one another. Selecting End Process Tree quickly shuts down these programs.

Note

If you aren't sure what a certain process is doing, you should not shut it down. Each process on the Processes tab of Windows Task Manager includes a description. If necessary, you can maximize the Task Manager window and adjust the column widths to read the descriptions. Sometimes even the descriptions on the Processes tab aren't enough to identify a process. In these cases, you can right-click a process and select Open File Location to see where the file associated with the process is stored. If it is in your Windows folder, you might want to leave it alone. Shutting down the wrong process can cause Windows to become unresponsive or crash.

www.it-ebooks.info

What is the difference between an application, a process, and a service?

- An *application* is a program running on your computer. It is typically installed separately from Windows, but Windows 7 does include some applications, including Internet Explorer.
- A *process* is a component for a program or service. Sometimes an application is constructed from several programs that run together, providing different functions for the application, for example, one process for running the application and another for updating it.
- A *service* is a program that does not require user interaction and that performs a specific task within Windows, such as running a print spooler or aggregating a media library.

INSIDE OUT Finding out what process does what

You can do a quick Internet search using a process name to find out what it is. For example, a search on the process 'vmusrvc.exe,' shown in Figure 13-2, returned the result, "vmusrvc.exe is a VMUSrvc belonging to Virtual Machine Additions from Microsoft Corporation."

CAUTION!

Shutting down Windows services can be troublesome. Unless you suspect a specific service is causing the problem, you shouldn't shut down any Windows service because doing so can cause Windows 7 to crash or become unresponsive.

Each time you shut down an application, process, or service, see if the problem you are troubleshooting goes away. Doing so can eliminate programs from your investigation and might even help you quickly identify the cause of the problem.

Safe Mode

Another way to shut down all running programs is to restart Windows 7 in Safe Mode by pressing F8 on your keyboard after the BIOS screen disappears but before the Starting Windows logo appears upon startup. This method is probably less useful than other methods since no software will be running (unless it's set as a Windows service, such as anti-virus

www.it-ebooks.info

software) and only minimal hardware drivers will be loaded at this point in startup. However, if you do restart in Safe Mode and everything is working fine, you can eliminate Windows 7 itself as the cause of the problem you are troubleshooting.

Unplug Your Hardware

As I mentioned earlier, you should also remove any hardware that you can from the machine when you're troubleshooting a problem. I'm not suggesting that you pull out your graphics card or anything like that. Do not remove anything from inside the PC case, but do remove hardware devices such as printers, USB flash drives, scanners, joysticks, and anything else that simply plugs in. After removing each element, see if the problem you're troubleshooting persists.

Hardware and Interrupt Requests (IRQ)

Windows 7 handles IRQs (interrupt requests) far more effectively than other versions of Windows before it, so problems almost never occur. You can never tell, however, if a poorly written hardware driver may still cause a problem, and IRQ conflicts can be worth checking occasionally.

In Device Manager, on the View menu, select Resources By Type, and then expand the list of device IRQs by clicking the plus sign next to Interrupt Request (IRQ). Right-click a device to open its Properties dialog box. On the Resources tab, you will see a list of the IRQ assignments for your hardware, as shown in Figure 13-3.

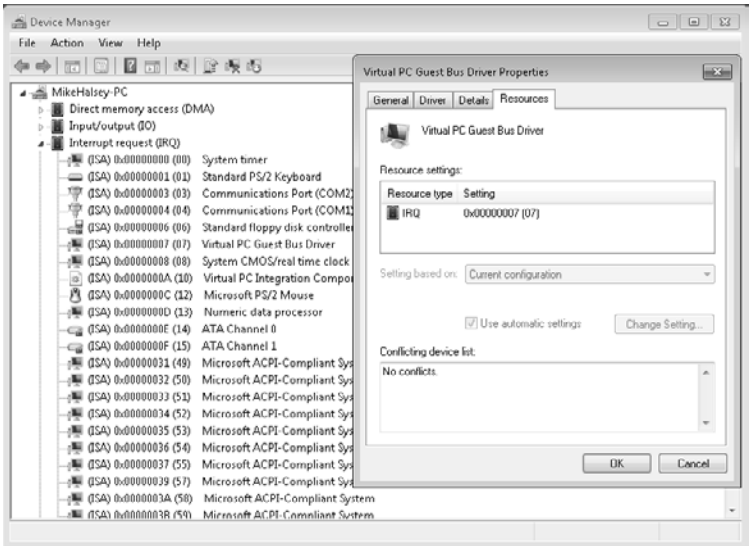


Figure 13-3 Viewing devices by IRQ

www.it-ebooks.info

IRQs are essentially communications channels that your hardware uses to send and receive data. They're called *interrupts* because a computer can't allow every device to talk to the motherboard simultaneously, so these communications channels take turns, with one channel 'interrupting' another to take over. IRQs also allow Windows 7 to manage the power usage on a PC, ensuring that all devices receive the power they require to function.

There are 15 IRQ channels in a PC; any IRQs you see above this number are virtual channels where Windows 7 is handling all the communication.

The more hardware devices you have plugged into a computer, the more they have to share the IRQs. Windows 7 is extremely good at sharing the IRQs, but occasionally two pieces of hardware sharing the same IRQ cause communication problems with each other. By viewing the resources by type in the Device Manager as described earlier in this section, you will be able to see if one or more IRQs are being shared by multiple devices. On the Resources tab, the Conflicting Device List box will indicate if there are any conflicts for this device caused by IRQ sharing (refer to Figure 13-3).

In Windows 7, you can't manually change the IRQ of a device. However, you can move the device to a different socket. This might involve moving a **PCI** card inside your computer to a different slot (make sure your PC is switched off and disconnected from power before you do this). This will force Windows 7 to reassign the device a new IRQ, and it may fix the problem.

With some motherboards, you can manually set IRQs for devices in the BIOS. It's entirely possible, however, that Windows 7 will simply ignore this BIOS setting and reassign the IRQ anyway.

Tip

Sometimes IRQ conflicts are caused by a device appearing twice in Device Manager. To resolve this issue, right-click one of the devices and select Remove.

These are the basics of diagnosing Windows problems, and you should find that they will enable you to quickly resolve a great many problems and issues. Chapter 14, "Advanced Diagnostic Tools in Windows 7," through Chapter 19, "Diagnosing Hardware Problems," will provide greater detail on how to diagnose more complex problems with Windows 7 and your PC.

www.it-ebooks.info

Why Problems Occur with Windows

So many things can go wrong with Windows because every single PC is unique. It is highly unlikely, especially outside of a business space, that another PC exists with exactly the same hardware, installed software specification, and updates as yours. Your PC will contain a unique mix of software and hardware components, and there would be no way for any person or any company to ever test all of the possible combinations for stability. There are logo certification programs for Windows hardware and software, and a great many vendors do indeed put their products forward for testing by Microsoft. All that these tests prove, however, is that on a basic Windows system, they will be stable and not cause the system to crash. What can't be tested is how a certain piece of software or hardware will interact with other software or hardware on your machine, some of which might not have been submitted for certification.

Keep Things Simple

The sheer number of software packages you have installed or the number of hardware devices you have plugged in can also cause problems on your computer. I always keep my Windows systems simple and uncomplicated. When it comes to hardware, I like multifunctional devices such as printer/scanner combinations, and I avoid unnecessary USB devices, such as USB attached speakers. Your PC already comes with audio out jacks that are perfectly good.

I also try to avoid installing all the software that comes with a new device. Wi-Fi adapters and printers are common culprits for loading your PC with *bloatware*. You may also find, if you have a new PC, that it came preloaded with lots of software that you don't need and will never use. The software packages that come bundled with hardware devices broadly fall into the following categories.

- **Trialware** Software that will expire after a period, normally 30 days. If you do not intend to buy the software after this time, you should uninstall it because it might, especially in the case of trial anti-virus software, leave programs and services running that can slow down Windows 7 or cause other problems.

- **Dupliware** Programs that duplicate Windows features, such as Wi-Fi connection software, media players, or CD/DVD burners.

- **Craplets** 'Useful' utilities that your PC supplier might have preloaded onto your computer. They are intended to simplify certain tasks, such as writing notes or accessing media files. They will always run when Windows launches at startup, although you will probably never use them.

www.it-ebooks.info

Note

Occasionally, you will find a utility that comes with hardware useful, for example, printer status (and ink/toner) monitoring, a document scanning utility, or a tweaking/overclocking utility for your gaming graphics card. These programs are perfectly fine, and you may find them very useful.

Don't Install Programs that Duplicate Features in Windows

Why would you want to install a software package that simply duplicates Windows functionality? By default, the operating system can burn CDs and DVDs (including audio discs and ISO image files), play media (video, TV, and audio), display photos and images, and much more.

Although a few Windows functionalities available in Windows Vista have been removed from Windows 7, such as the Calendar and Email software, a great many functions still exist. (Note that these programs have been moved to the excellent Microsoft Live Essentials Suite, which you can get from *http://download.live.com*.)

The more software you install on your PC, the more problems you invite. If at all possible, avoid having software packages installed that duplicate functionality that's already in Windows. CD/DVD burning software is a good example. You should need these only if you have a Blu-Ray burner in your machine.

INSIDE OUT The media player exception

The only possible exception I would make to the rule about not installing duplicate programs is media player software. If you have an iPhone, iPad, or iPod, you will need to install Apple iTunes software on your PC to synchronize your device. Many people also find the iTunes software very good and like shopping in the iTunes store.

Another example is the Zune media software, which is not only far better than the media player software bundled with Windows 7, but is also required if you want to synchronize with a Windows Phone 7 mobile device or a Zune Media Player.

www.it-ebooks.info

> **Note**
>
> **A case can be made for choosing only Microsoft software when you have a choice of suppliers. I would argue this is true for Microsoft Live Essentials Suite and Microsoft Office, especially. Microsoft has complete access to the Windows base code, so you can be confident that Microsoft software will almost always operate without causing any problems in Windows 7. Installing a third-party package will not give you the same peace of mind.**

What Are the Causes of Common Problems?

It's very rare for Windows 7 to fail. Windows will fail on its own only if something disastrous happens, such as a power surge or a sudden reset while Windows is modifying a critical system file. Problems are more commonly caused by something outside of Windows, such as software, updates, and drivers. Physical hardware almost never causes problems in Windows. (But I *will* talk about diagnosing hardware problems in Chapter 19.)

A great many of the problems with Windows are caused by poorly written software or hardware drivers or by having too many devices or programs installed on or in your PC. In my experience, the most common problems within Windows are caused, in order, by:

1. Device drivers
2. Poorly written software
3. Poor security
4. BIOS corruption (see more information on resetting the BIOS in Chapter 7, "Hardware")

The Domino Effect

Some problems can cause what is called a *domino effect*, where one event sets off a string of other events, so it's always advisable to diagnose and repair problems as early as you can after they first appear. One unchecked problem can then lead to others, because a malfunctioning process, service, or driver can cause other programs or Windows functions to fail, since these processes, services, or drivers are often shared by several applications or Windows components. For instance, you might have a problem with Internet Explorer

www.it-ebooks.info

crashing repeatedly. This could be because a component Internet Explorer shares with another Windows program, such as Windows Explorer, is corrupt or because another program or process is causing it to crash. I'll cover the sometimes complex process of repairing Internet Explorer in Chapter 15, "Advanced Repair Methods." The point is that the source of a problem is not always obvious; a failing program may not be the root cause of the issue. In these cases, you can use more advanced diagnostic methods and tools to diagnose an issue. I will cover these in Chapter 14, "Advanced Diagnostic Tools in Windows 7," through Chapter 16, "Windows Problems Demystified."

Have You Tried Turning It Off and On Again?

If you've ever called an IT support department, the first question the support person probably asked you is, "Have you tried turning it off and on again?" This is a running joke with IT support professionals, because you might be amazed how often it fixes problems!

It might not be a permanent fix if there is something more serious happening, but for odd occasions when a software package suddenly crashes, restarting the PC will often fix the problem. Software crashes are common, and just because a program crashes once does not mean it will continue to do so. Crashes can be caused by freak conditions that are unlikely to recur, such as two programs trying to access the same file simultaneously.

With all IT problems, be they hardware or software, this is a good thing to try. You should also restart all external hardware devices attached to your PC when you restart the computer by manually switching them off and on again when you restart your computer.

The Blue Screen of Death

The Blue Screen of Death (BSOD) is notorious and, although not frequently seen in Windows 7, is still feared by many Windows users. The BSOD is the ultimate sign that Windows has died. However, the BSOD can provide some very useful information when you are troubleshooting problems that have caused it.

Figure 13-4 shows an example of a BSOD. I have marked two useful messages within the screen. The top one is the error type that caused the critical stop, in this case a PAGE_FAULT_IN_NONPAGED_AREA, indicating a memory problem.

www.it-ebooks.info

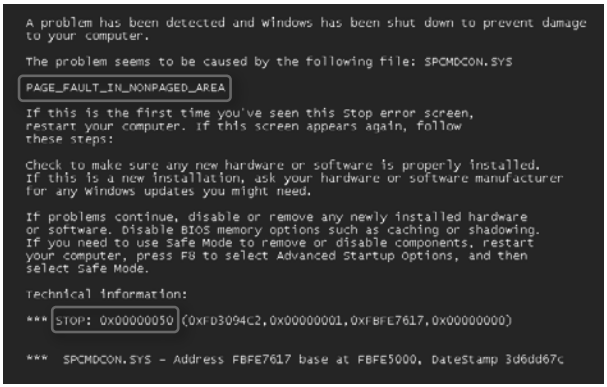


Figure 13-4 The Blue Screen of Death

The second callout, located in the Technical Information section of the screen, is the actual error code, in this case STOP: 0x00000050. A BSOD may also provide additional information. The BSOD in Figure 13-4 indicates the Windows service that has failed: SPCMDCON.SYS.

If a BSOD provides this type of information, you can use it to search online for more information on the error. In this case, SPCMDCON.SYS is a "mini command console," which isn't the most useful description, but a search for the error code reveals that there are several problems with Windows 7 that can cause this specific error. You can search through the results to find a fix that works for you and your PC.

By far the most common cause of BSOD in Windows is a hardware driver error, especially from unsigned drivers that have not been tested and certified by Microsoft. On occasion, other issues, such as a poorly written piece of software or even a power drop, can cause the dreaded BSOD.

The Perpetual Restart

Sometimes Windows 7 will automatically restart when it encounters a critical error. This can cause terrible problems, with a PC constantly restarting and never loading the desktop.

You can disable automatic restart on the boot menu shown in Figure 13-5. To access this menu, press F8 on your keyboard after the BIOS screen disappears but before the Starting Windows logo appears.

www.it-ebooks.info

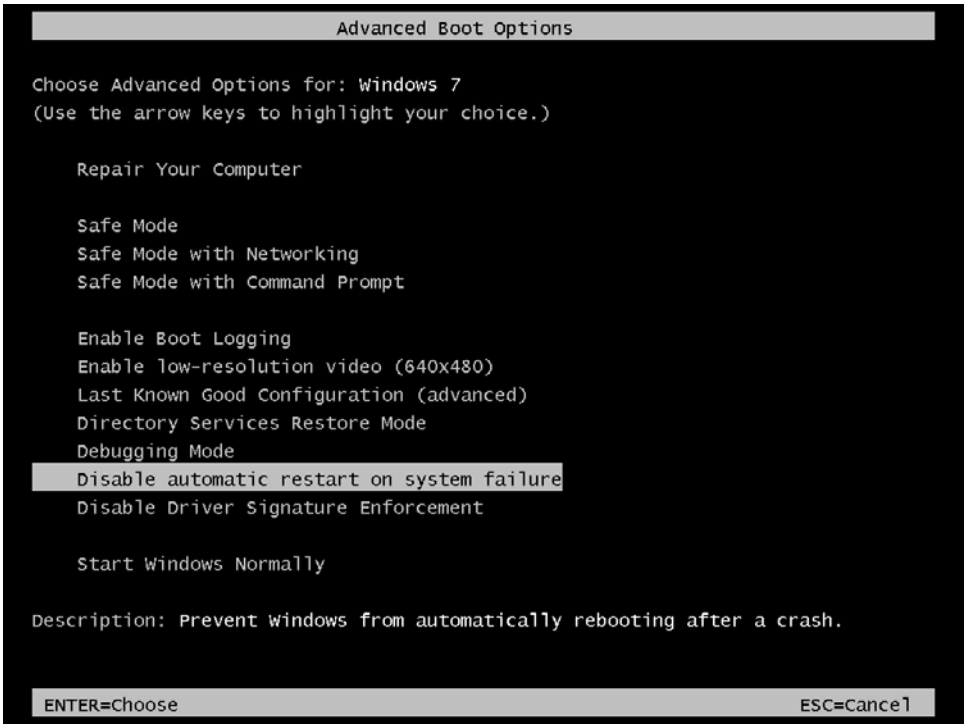


Figure 13-5 Disabling Windows automatic restart on system failure

Select Disable Automatic Restart On System Failure from the options list, as shown in Figure 13-5. At the next critical stop, Windows will display the error message on the BSOD instead of automatically restarting. You may discover (unless you're having an extremely bad day) that after making a note of the stop error code, you can start your PC in Safe Mode.

Summary

Honing your troubleshooting techniques is one of the most useful computer skills you can develop; every person will find a method that works best for him or her. Because computers are so complex, using a step-by-step approach and attempting to eliminate first what a problem cannot be, will ultimately help you to identify the source of a problem. This is by no means the only way to troubleshoot a PC. You should never forget that sometimes you need to take a step back and sleep on a problem, or you may never find it.

www.it-ebooks.info

CHAPTER 14

Advanced Diagnostic Tools in Windows 7

Performance Information and Tools 217
Event Log 219
Performance Monitor 222
Resource Monitor 223
Windows Task Manager 224
System Information 224
System Health Report 226
Computer Management 227
Using the Windows 7 Performance Tools 229
Summary 230

In Chapter 2, "The Basic Windows 7 Utilities," you learned about the basic diagnostic and help utilities included with Windows 7. In this chapter, I cover some of the advanced tools that come with Windows 7, describing the features and capabilities of each one and explaining how you can use them to help you troubleshoot your Windows 7 system.

Performance Information and Tools

Performance Information and Tools is a central location for many types of information about your PC and how Windows 7 performs on it. The easiest way to access Performance Information and Tools is by typing **performance** in the Start menu search box, as shown in Figure 14-1. You can access its components separately in Control Panel by selecting System and Security\Administrative Tools.

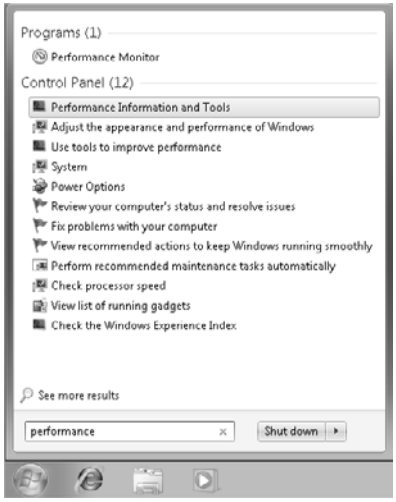


Figure 14-1 Accessing Performance Information and Tools

www.it-ebooks.info

The basic function of Performance Information and Tools is to provide a front end to features such as the Windows Experience Index and options for adjusting the visual effects, power settings, and indexing options of your copy of Windows. Once you're in the Performance Information and Tools window, which is shown in Figure 14-2, click Advanced Tools in the left pane to access the advanced tools, which are shown in Figure 14-3.

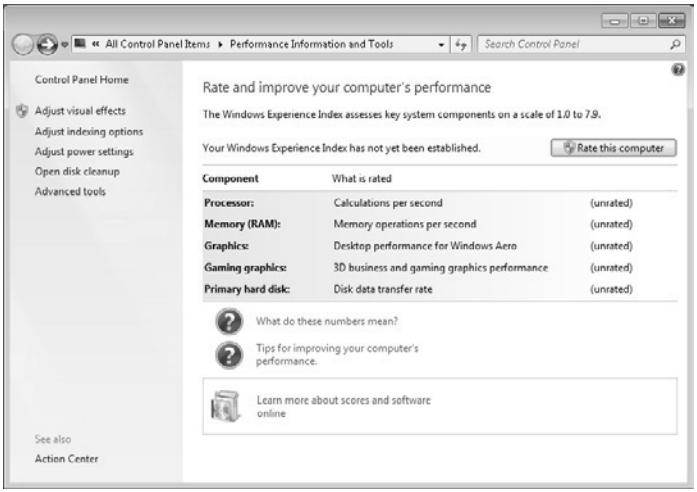


Figure 14-2 Performance Information and Tools window

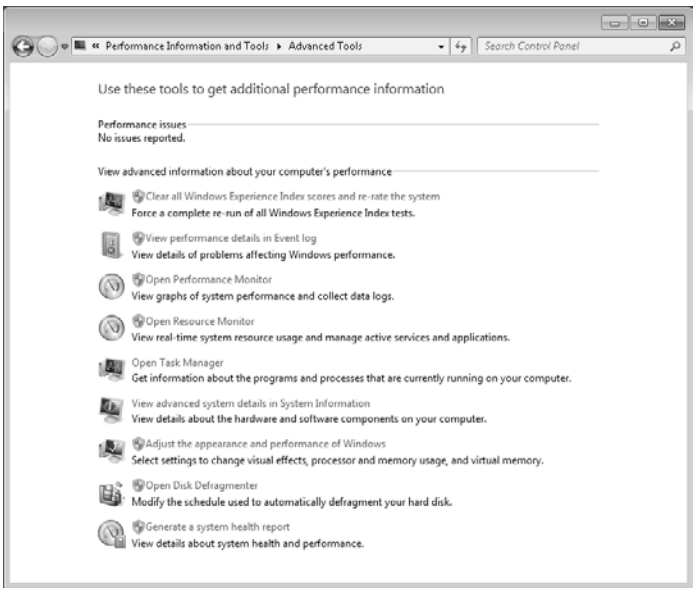


Figure 14-3 Advanced tools in Performance and Information Tools

www.it-ebooks.info

These advanced tools are extremely useful in diagnosing performance problems with Windows 7 and your software and hardware drivers. I don't provide details for every tool in this chapter, but I do cover what I consider the vital ones individually: **Event Log**, **Performance Monitor**, **Resource Monitor**, Task Manager, System Information, **System Health Report**, and the Computer Management console.

Event Log

Everything that happens in Windows 7 from user log-ins to program component failures that the users never even know about is logged and recorded. You would be amazed by how much information is stored in the Event Log. The two most important views, however, are the ones where you will see most Windows 7 errors recorded.

In the Event Viewer, you can find all the events and errors that Windows 7 has recorded on your computer by clicking Event Viewer (Local), then clicking Windows Logs, and then clicking System. Warnings are highlighted with yellow triangles, and errors are indicated with red icons, as shown in Figure 14-4.

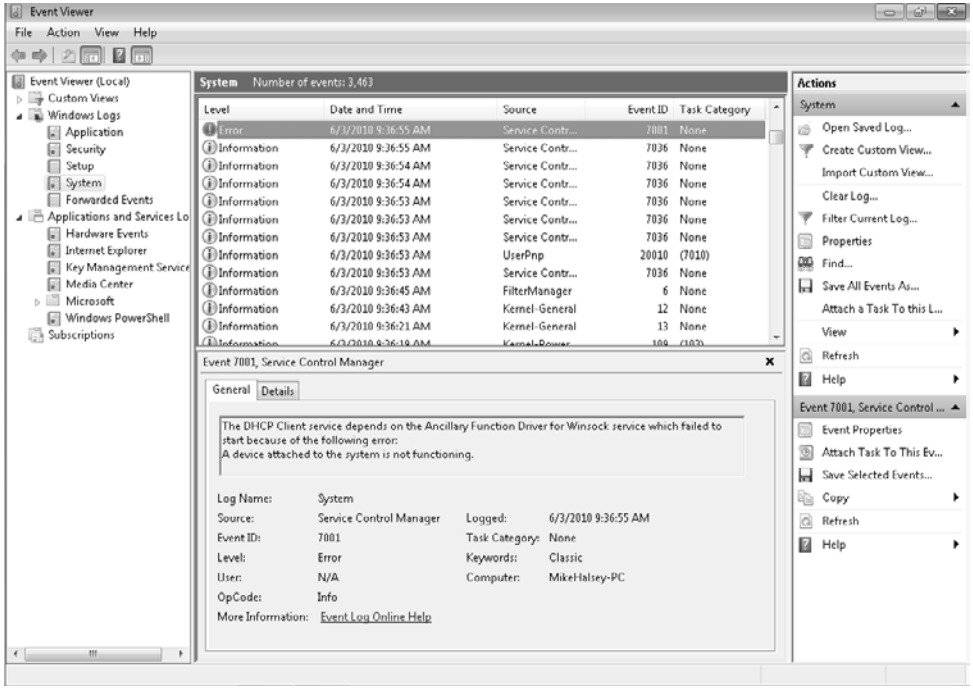


Figure 14-4 Event Viewer showing system activity and errors

www.it-ebooks.info

In Figure 14-5, notice the error highlighted in the first line of the Administrative Events pane. Below the list is a description of this PrintService error that includes enough information to help you track down the source of the problem and fix it.

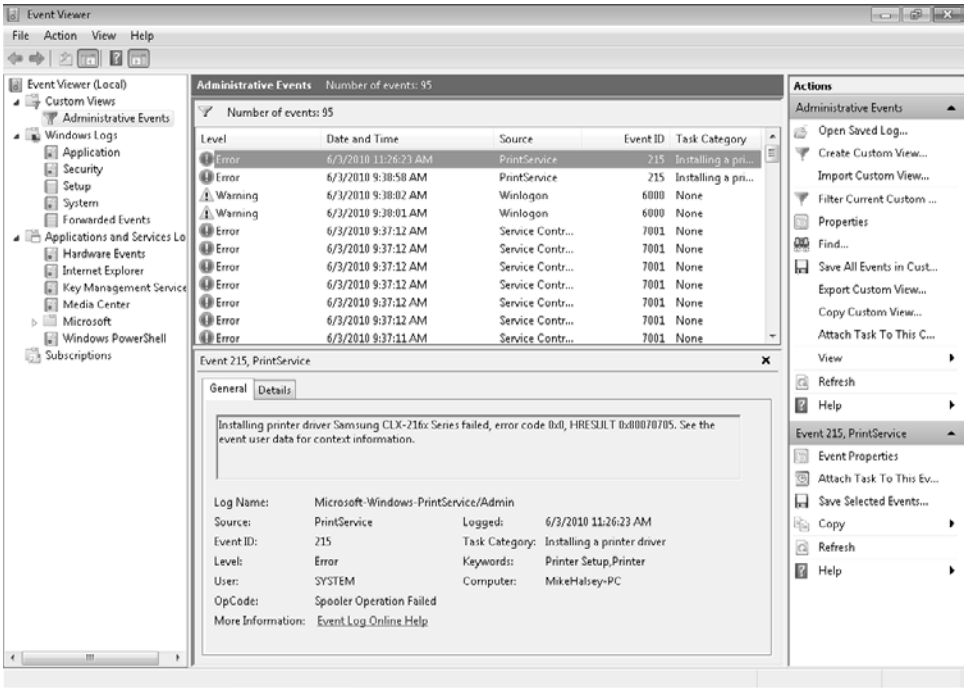


Figure 14-5 Administrative errors in the Event Log

Another useful place to see errors listed in the Event Log is under Event Viewer (Local)\ Custom Views\Administrative Events, as shown in Figure 14-6. These errors include events for which you or Windows didn't have permission to perform the specified action.

In the bottom pane of the Event Viewer are two tabs, General and Details. By default, the General tab is selected, and here you find general information about errors and events. You can get much more information by clicking the Details tab. You can also expand this panel upward to read more.

This information can be useful if you need to send specific data about an error to a third-party support person. You can cut and paste it into an email or select an option from the right pane such as Save Selected Events to email.

www.it-ebooks.info

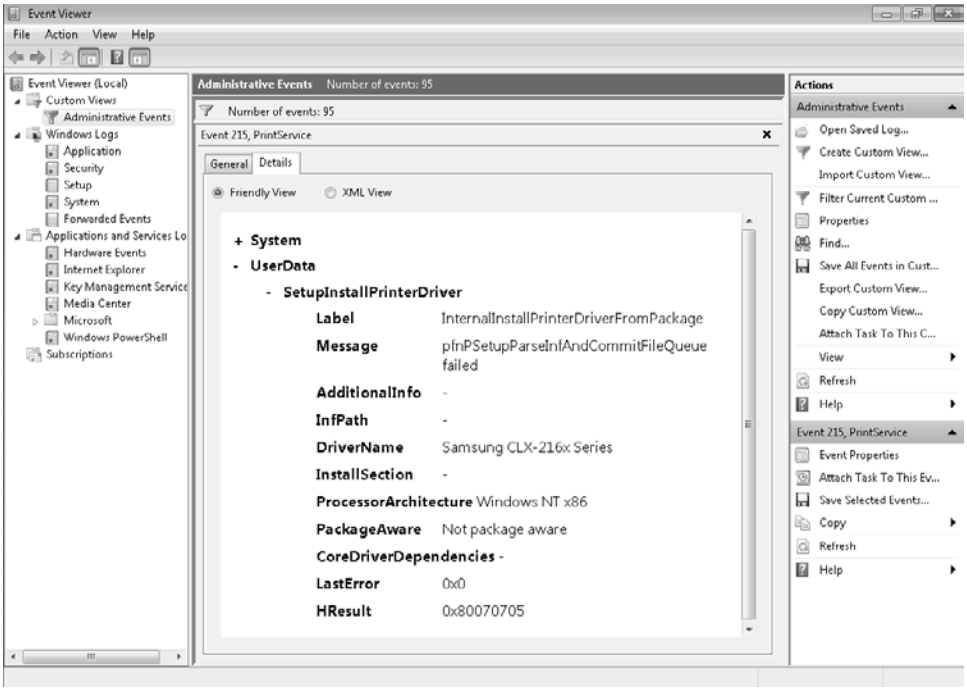


Figure 14-6 Formatted error information, which you can send to third parties

INSIDE OUT The Event Log is your friend

The Event Log is probably the single most useful feature in Windows 7 when it comes to troubleshooting problems. It is certainly the most useful feature in the advanced toolset in Performance Information and Tools because the amount of useful information it provides is far greater than other Windows utilities.

How to Read the Event Log

By default, the events in the Event Log are ordered by date. If your computer has recently encountered an error, you can check for it by date and time. It's probably near the top of the event list. The Event Log provides essential information about the source of errors, helping you diagnose problems much more quickly than you could by trial and error.

www.it-ebooks.info

Performance Monitor

Performance Monitor, shown in Figure 14-7, provides real-time information about a wide range of Windows and hardware components and events. You can also use it to check whether the Windows reporting tools are activated.

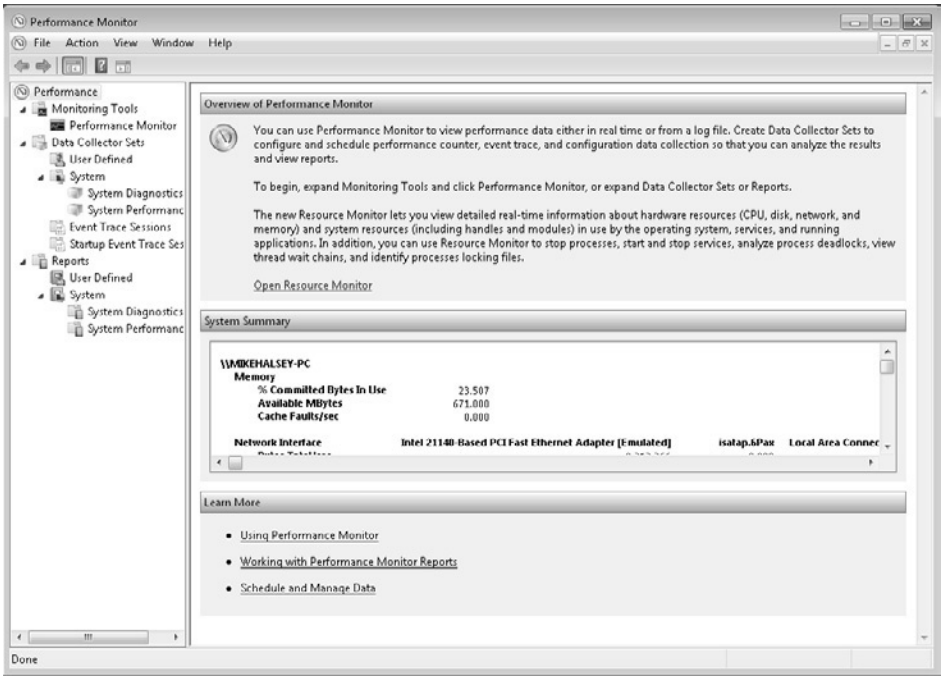


Figure 14-7 Performance Monitor in Windows 7

You can use the real-time monitoring tools in Performance Monitor to add information about specific things, for instance, the read/write data for your hard disk or the power distribution to individual components, seen in Figure 14-8. In Chapter 25, "Advanced Windows Diagnostic Tools in Depth," I will talk about these tools in much greater depth.

For most users, the information provided by Performance Monitor is extremely complex and difficult to interpret. If you need specific information about how a certain component is working—say, for example, you suspect the **ReadyBoost** cache isn't working properly—you can monitor this feature in real time via Performance Monitor.

www.it-ebooks.info

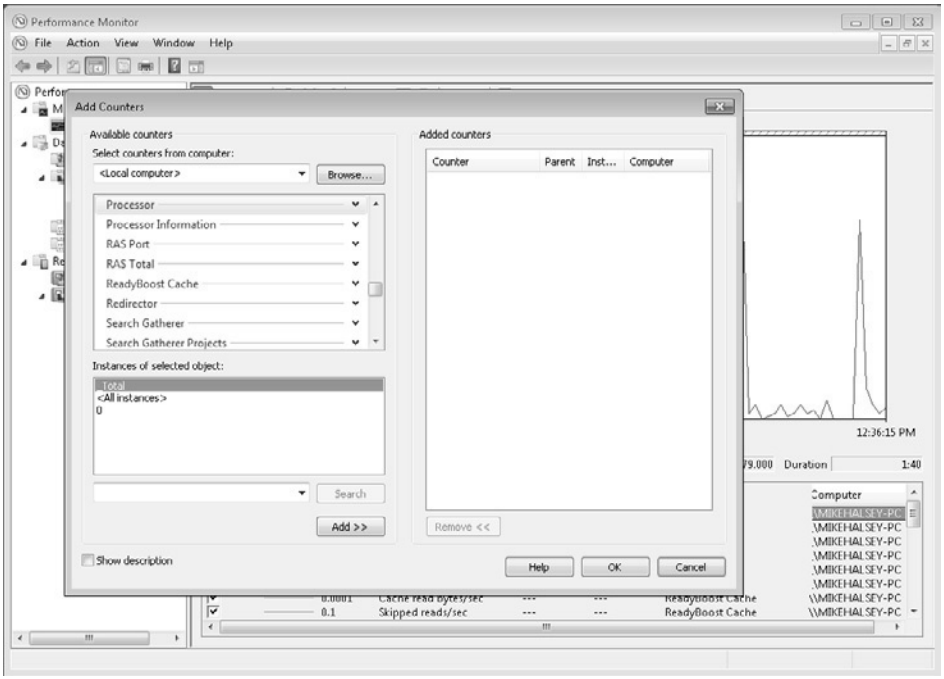


Figure 14-8 Adding custom counters to Performance Monitor

Resource Monitor

Whereas Performance Monitor helps you diagnose problems with Windows services and components, Resource Monitor gives you extensive real-time information about your processor, memory, hard disks, and networking. Figure 14-9 shows the information you find on the Memory tab of Resource Monitor. If one of your applications is consuming vast amounts of memory, you would find information about it here. Each tab lets you know exactly what's going on at a given moment in a different part of your system, from the status of processes and services running (or not running) on your CPU to the current activity on your network.

www.it-ebooks.info

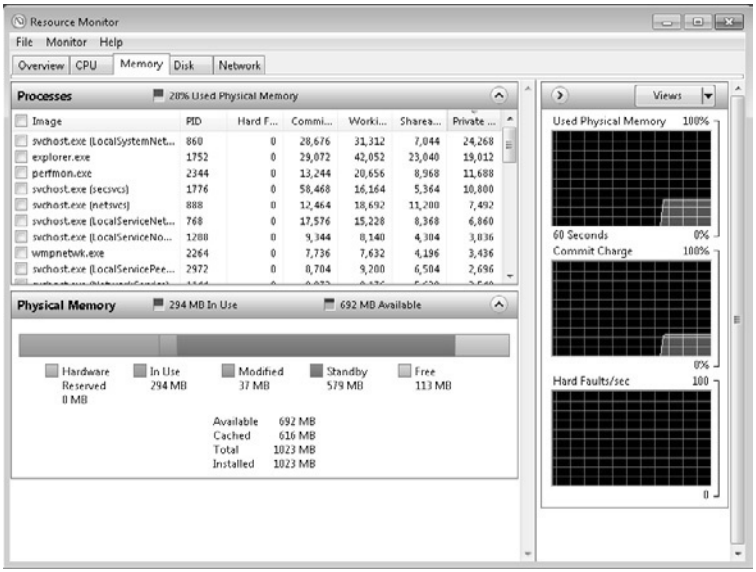


Figure 14-9 Resource Monitor in Windows 7

Resource Monitor provides information similar to what Windows Task Manager gives you but supplies many more details, which can be useful when you're diagnosing advanced problems in Windows or in your applications.

Windows Task Manager

If you've used Windows before, you're probably familiar with Windows Task Manager. One of the fastest ways to access Windows Task Manager is by right-clicking the Windows taskbar and selecting Start Task Manager.

The information you find in Windows Task Manager is less detailed than what you see in Resource Manager but can provide information that is not shown in Performance Monitor, including what services are currently running and what users are logged in to the computer.

System Information

If you need to provide a third party with information about your PC, including data on Windows, your hardware, and your installed software, the System Information tool, shown in Figure 14-10, is the place to find it.

www.it-ebooks.info

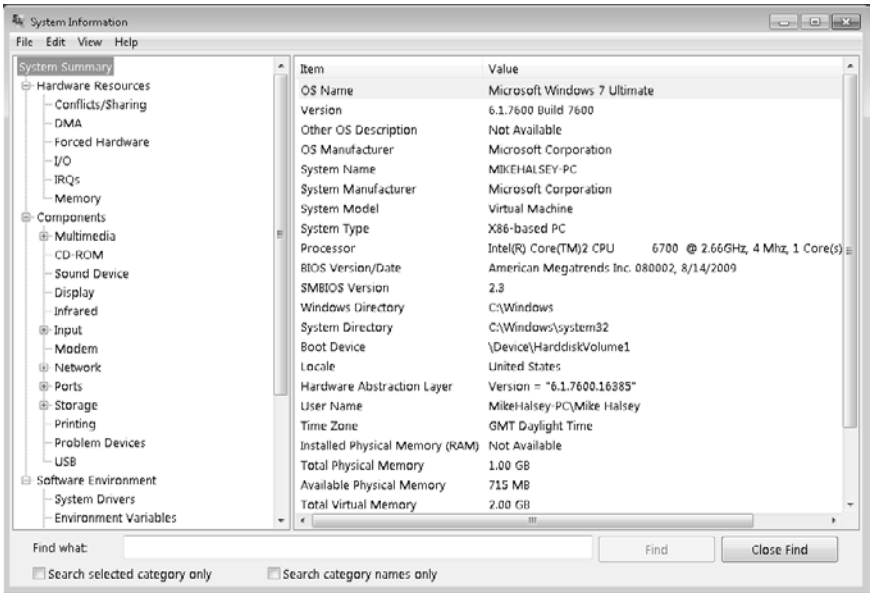


Figure 14-10 System Information tool

The system information is divided into three sections.

- **Hardware Resources** Contains information about hardware conflicts, IRQs (interrupt requests), memory allocations, and so on.
- **Components** Includes information about the hardware attached to your PC, with a separate section, Problem Devices, for devices that Windows 7 has identified as problematic.
- **Software Environment** Includes information about everything from installed software and drivers to startup programs and recent Windows error reporting.

To export any or all of the data from the System Summary as a text file that can be read on any computer, go to File\Export, name the text file, and save it.

www.it-ebooks.info

System Health Report

One of the most useful automatic diagnostic features in Windows 7 is the system health report tool you find when you click Generate A System Health Report in the Advanced Tools section of Performance Information and Tools. Figure 14-11 shows the Resource and Performance Monitor window that appears when you click the link. This tool produces thorough and detailed reports of the current status of your PC, checking every part of Windows, your hardware, and your installed software and highlighting any problems.

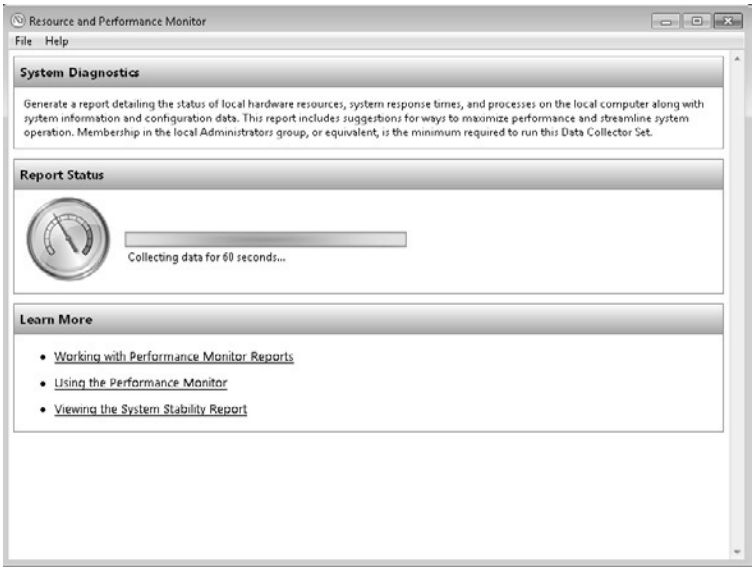


Figure 14-11 Tool for generating system health reports in Windows 7

The File menu includes options to send the report to an **email client** configured on your PC, save it as a file, or send it through a web mail application when you can attach the file manually to an email in the same way you would any other attachment you send. This method will vary depending on your email provider.

Before you dive into the details of the system health report, you should read the information that appears in the Diagnostic Results panel, as shown in Figure 14-12. Here you'll see information on currently detected problems as well as links to helpful articles about these problems on the Microsoft website.

www.it-ebooks.info

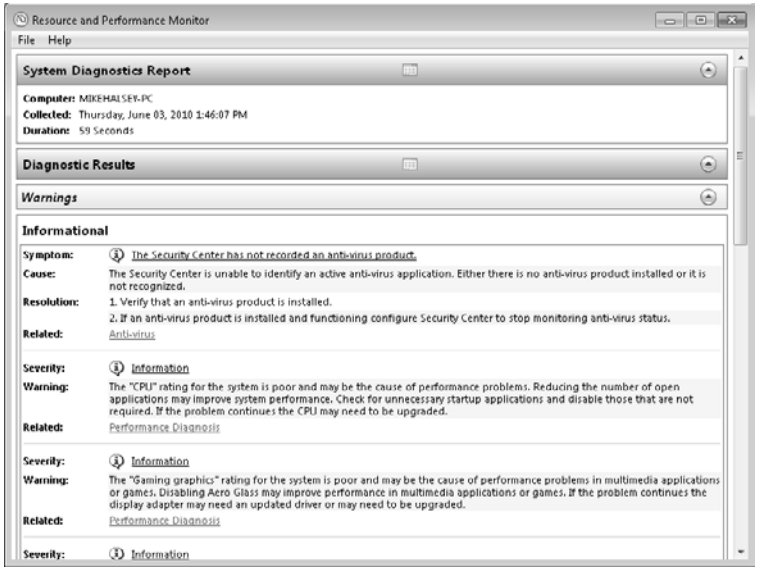


Figure 14-12 Sample system health report

Computer Management

You can access the Computer Management console through Control Panel (click System and Security, click Administrative Tools, and then click Computer Management), but the easiest way to get to it is by right-clicking the Computer link in the Start menu and selecting Manage, as shown in Figure 14-13.



Figure 14-13 Accessing the Computer Management console

www.it-ebooks.info

From the Computer Management window, shown in Figure 14-14, you can view and control System Tools such as Task Scheduler, Event Viewer, Performance, Device Manager, and the Disk Management storage tool.

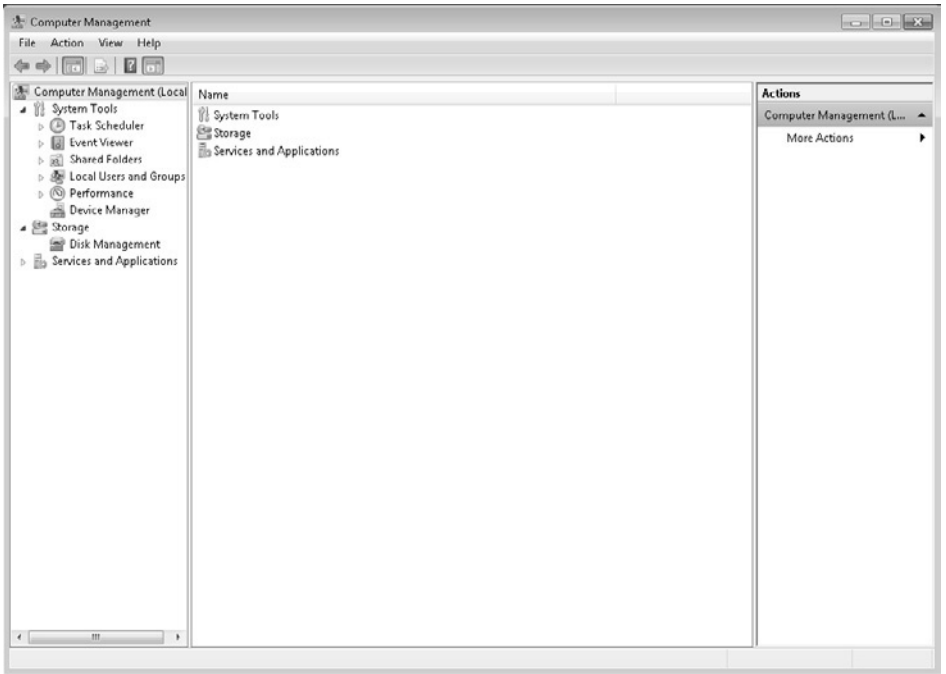


Figure 14-14 The Computer Management console

When you click Disk Management, the pane in Figure 14-15 appears. Here you can view all the fixed and removable drives in your PC and find problems with them. For example, you might see that a disk isn't being recognized or is being reported as unformatted.

INSIDE OUT

Be careful when working with suspected faulty disks

Just because Windows is reporting a disk as "unformatted" or "not initialized" doesn't mean that the disk is really faulty. If the disk has been working fine until now, the problem is more likely with a driver or a corrupt BIOS. Reformatting or reinitializing the disk might not fix the problem.

www.it-ebooks.info

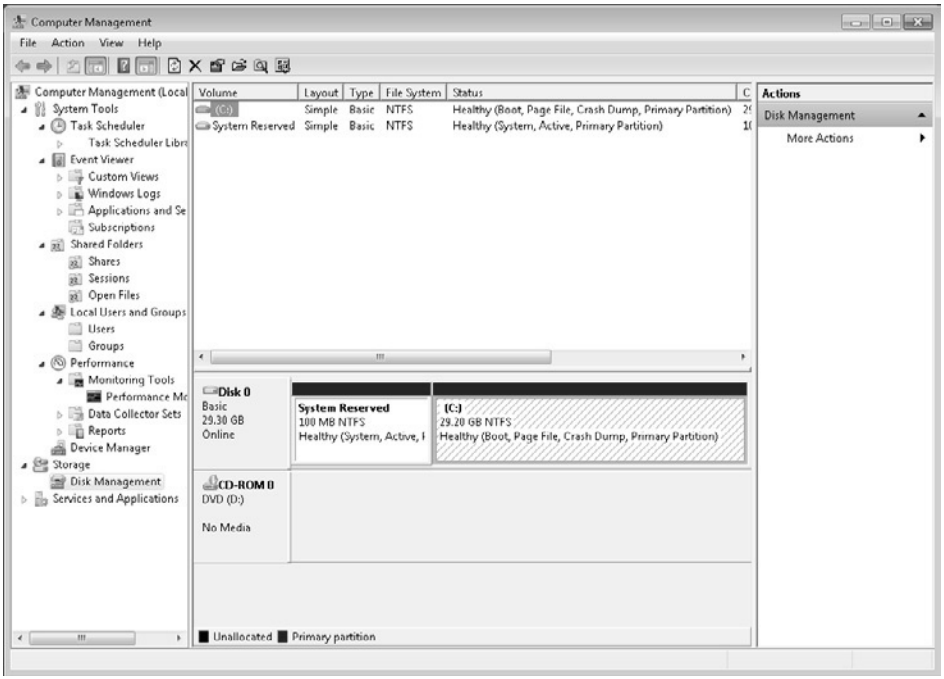


Figure 14-15 Disk Management console

As I have said, the Computer Management Console is a good and centralized place for finding the tools that come with Windows that can be used for repairing problems with the operating system and your hardware.

Using the Windows 7 Performance Tools

The performance tools in Windows 7 offer some extremely advanced information that may be primarily used by IT professionals, either remotely or when accessing the PC directly, but that are of use to anyone working with diagnosing and repairing problems on a PC. One of the most useful functions of these tools is their ability to quickly display a huge amount of data about your PC, your copy of Windows, and your hardware.

They are especially useful because of the different ways they can present this information and the different levels of detail they goes into depending on your requirements. For most of your troubleshooting needs, the Event Log will suffice. If you're going to a third party for additional help or guidance or if you're helping someone else, a system health report might be required.

www.it-ebooks.info

Take Time to Step Back

Sometimes the best troubleshooting tool isn't built into the system. If you're stuck on a troubleshooting problem that you just can't figure out, I would advise you to step away from your computer. Take a break, maybe even a day, and come back to the problem with a clear mind. I've found that if I keep staring at a PC screen trying to figure out or fix a challenging problem, my mind can become muddled and I can tend to miss things that I would normally catch. If you (or your company) can't justify such a respite, try reading some of the reports you generated with Performance Information and Tools offline. The reports that the Advanced Performance Information and Tools utilities can provide make for excellent reading when you're away from your PC and can't be tempted to try quick fixes. This can give you time to digest a problem and read the logs thoroughly.

Summary

I will talk about the advanced tools included in Performance Information and Tools in much more depth in Chapter 25. These tools are versatile and useful in many contexts as well as highly customizable. What I hope to have shown in this chapter is that even a novice user can gain useful data and information from the advanced maintenance and troubleshooting tools in Windows 7.

www.it-ebooks.info

CHAPTER 15

Advanced Repair Methods

Repairing Microsoft Internet Explorer 231
System File Checker 239
Using MSConfig for Diagnostic Startups 241
Managing Windows Services 244
Working with the Windows Registry 246
Using the System Repair Disc for Advanced Restore . . 249
Using Safe Mode 254
Summary 255

Windows 7 includes many ways to help you perform advanced repairs when malfunctions and failures occur. These include tools that are bundled within Windows itself, additional modes you can start Windows 7 in, and utilities that you can run from a CD or DVD.

Repairing Microsoft Internet Explorer

Microsoft Internet Explorer shares many components with other parts of Windows, such as Windows Explorer. Internet Explorer is one of the most heavily used components in the operating system, and one of the biggest targets of attack, so a lot can go wrong with it. But as an integrated Windows component, it can be very hard to fix problems with the browser. So how do you fix Internet Explorer when it misbehaves?

Disable Your Add-Ons

Many problems with Internet Explorer, or any web browser, are caused by plug-ins and toolbars. These elements cause many problems, including a very slow startup time. It's easy to turn off problematic plug-ins and toolbars from within the browser.

With Internet Explorer open, click Tools in the top right of the toolbar, and select Manage Add-ons (see Figure 15-1).

A window appears with details about all of your add-ons and toolbars (see Figure 15-2). Disable each suspicious add-on one at a time, restarting Internet Explorer each time to see if the problem persists.

www.it-ebooks.info



Figure 15-1 Managing add-ons in Internet Explorer

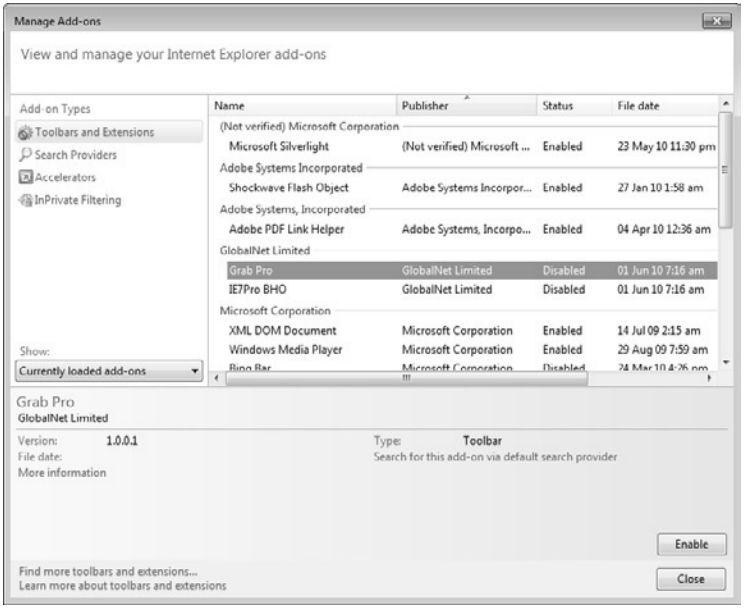


Figure 15-2 Disabling add-ons in Internet Explorer

www.it-ebooks.info

INSIDE OUT Keep add-ons and toolbars to a minimum

Add-ons can very quickly slow down your Internet browser, whichever one you use. I recommend keeping installed add-ons and toolbars to a minimum to help with speed and efficiency and to minimize problems and errors.

Running Internet Explorer with No Add-ons

Sometimes you can't even start Internet Explorer and turn off the add-ons and toolbars without it crashing. There's a solution to this problem as well.

There's a special entry for Internet Explorer in the Windows 7 Start menu to run the program with all add-ons, toolbars, and ActiveX controls disabled. To find this special mode, simply type **add** in the Start menu search box (see Figure 15-3), or look for it on the Start menu by clicking Accessories and then clicking System Tools.

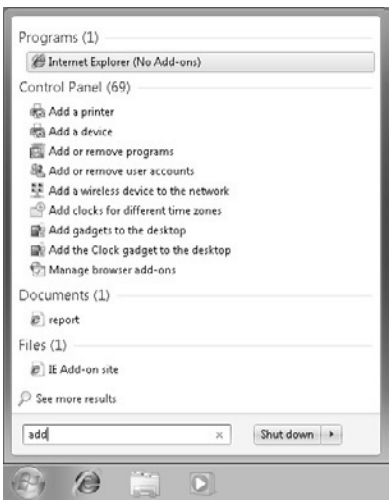


Figure 15-3 Running Internet Explorer with no add-ons

You will be notified when the program starts that no add-ons are running, and a yellow information bar will appear. You can click the information bar to manage your add-ons (see Figure 15-4).

www.it-ebooks.info

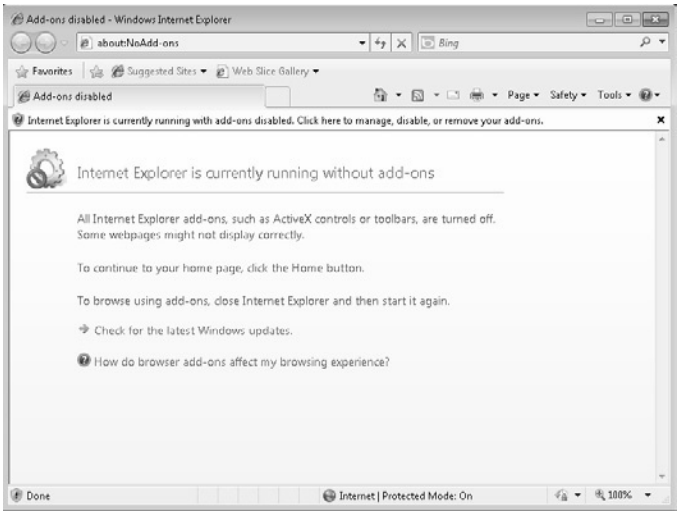


Figure 15-4 Managing add-ons settings in Internet Explorer with add-ons disabled

Again, if you are unsure what add-ons or toolbars are causing the problem, you might want to shut them down one at a time, restarting Internet Explorer in normal mode each time to see if the problem has been rectified.

Managing Add-Ons from the Control Panel

Another way to manage add-ons in Internet Explorer is through Control Panel (see Figure 15-5).

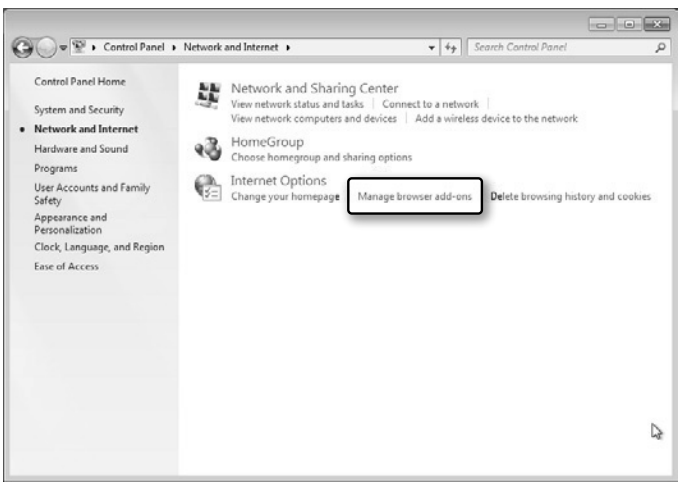


Figure 15-5 Managing Internet Explorer add-ons from Control Panel

www.it-ebooks.info

You can access the settings by clicking Network And Internet and then clicking Manage Browser Add-ons. A window opens with options for Internet Explorer. Here you will see a Manage Add-ons button.

How to Factory Reset Internet Explorer

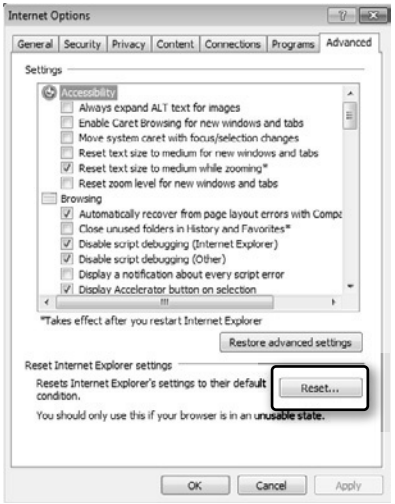
If the problem with Internet Explorer is not caused by add-ons or toolbars, you can use a Windows 7 option to reset Internet Explorer to its default settings. This will restore the web browser to the state it was in when it was first run.

1. To access the reset option from within Internet Explorer, click Tools on the toolbar, and select Internet Options.



2. A dialog box appears. Click the Advanced tab, and then click Reset in the Reset Internet Explorer Settings section.

www.it-ebooks.info



An alert window will open asking if you really want to reset all Internet Explorer settings. This is a safeguard against pressing the button accidentally, since resetting Internet Explorer will remove all of your add-ons and toolbars and can, optionally, delete all of your settings for the program. Review the information and then click Reset.



INSIDE OUT

Resetting Internet Explorer will not delete Internet **favorites**

Because your favorite websites are stored in your Windows users folder and are not a part of Internet Explorer, resetting the browser will not delete them. You can perform this action safe in the knowledge that your favorites and bookmarks are safe.

www.it-ebooks.info

Resetting Internet Explorer When You Can't Start It

Sometimes you can't start Internet Explorer at all and need to reset it from Control Panel. To do this, open Control Panel and click Network And Internet, and then click Internet Options (see Figure 15-6).

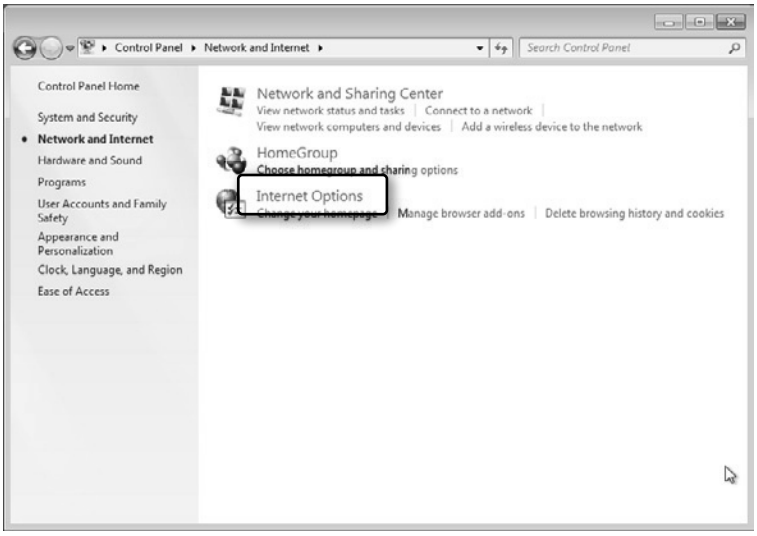


Figure 15-6 Accessing Internet Options from Control Panel

On the next screen, click Internet Options again. The Internet Options dialog box appears where you can click the Advanced tab and reset the browser.

Can You Reinstall Internet Explorer?

You can't actually reinstall Internet Explorer 8 in Windows 7 because Microsoft does not provide a download to support it. If you try to download the Internet Explorer versions for Windows Vista, you will be notified that they are not compatible with Windows 7.

You can also reset Internet Explorer by running the **System File Checker**, which will replace any corrupt files for the program. If it still malfunctions after this is done, you might need to switch it off and use a different web browser if you cannot restore Windows 7 from a backup made at a time when everything was working fine.

You can turn off Internet Explorer by clicking Programs And Features and then clicking Turn Windows Features On (or Off).

www.it-ebooks.info

INSIDE OUT Internet Explorer 9

You will be able to install Internet Explorer 9 over a damaged version of Internet Explorer 8 when it is released. (It is due to be released in 2011.) The reset options for this new browser will be the same as they currently are for Internet Explorer 8.

Updating Internet Explorer via Windows Update

In other chapters of this book, I have stressed the importance of having Windows Updates switched on. If you are experiencing browser problems, Windows Update may provide an update that will fix them. It's also worth performing a manual update by selecting Windows Update on the Start menu to see if any new updates for the browser are available.

Alternatives to Internet Explorer

Internet Explorer isn't for everyone. Windows users in the European Union can use the Browser Ballot Screen to choose which browser to use with Windows (see Figure 15-7).

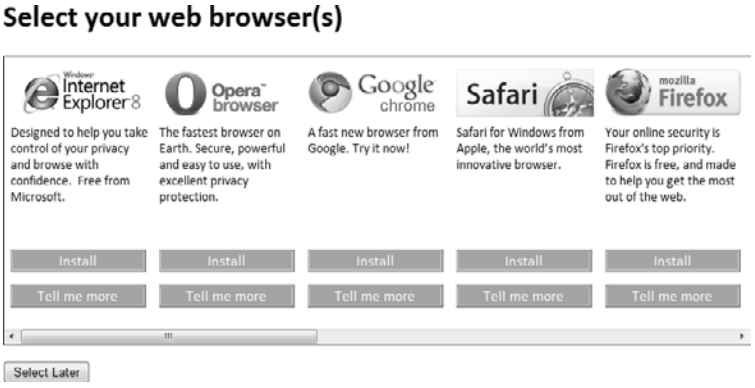


Figure 15-7 The European Browser Ballot Screen

www.it-ebooks.info

This gives European users a choice between the most popular web browsers and allows them to download and install one if they don't want to use Internet Explorer. The web browsers appear in a random order, although the five most popular browsers always appear first in the list.

Following are my recommendations for alternatives to Internet Explorer.

- **Mozilla Firefox** An open-source browser that's excellent if you want to use plug-ins and add extra features to your browser (*www.firefox.com*)
- **Google Chrome** Designed to be a fast, lightweight browser for people who like quick, unfussy web browsers (*chrome.google.com*)

System File Checker

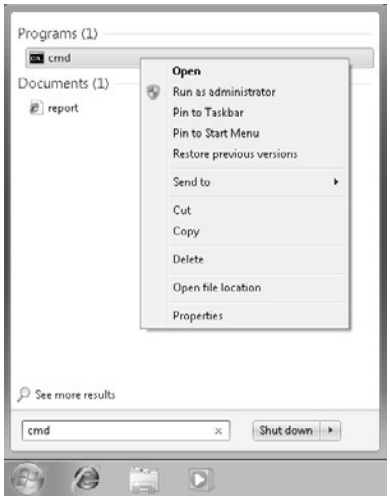
One of the hidden gems in Windows is System File Checker. This utility checks the integrity of every file that was installed in Windows against the original copy of the file on the installation DVD.

> **Note**
> **You will need to have your installation DVD in your computer's optical drive when you run this utility.**

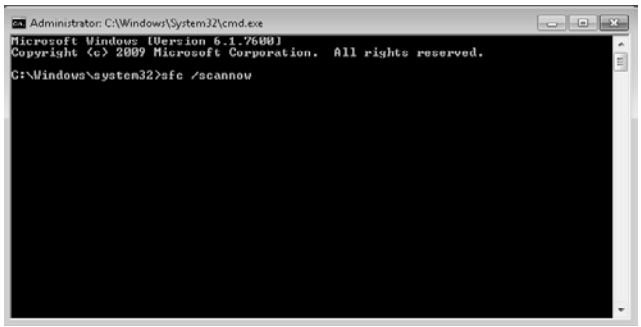
If System File Checker finds any file that's changed or become corrupt, it will restore the original file from the DVD. This process can take from 10 minutes to an hour, but it is one of the quickest and simplest ways to repair problems with Windows 7.

1. To access System File Checker, place the Windows 7 installation DVD in your computer's optical drive, but do not run anything on the disk.
2. Type **cmd** in the Start menu search box. When cmd (or Command Prompt) appears in the search results, right-click it and select Run As Administrator.

www.it-ebooks.info



3. A DOS window appears. Type **SFC /SCANNOW** (this is not case sensitive) and press Enter on your keyboard.



System File Checker checks the integrity of every Windows system file, including all Internet Explorer 8 files, and replaces any corrupted files it finds.

INSIDE OUT System File Checker and Windows 7 service packs

To run System File Checker, you must have an installation DVD containing the service pack that's currently installed in your copy of Windows 7. This may mean that you need to create a new installation DVD. See Chapter 16, "Windows Problems Demystified," for instructions on how to do this.

www.it-ebooks.info

Using MSConfig for Diagnostic Startups

MSConfig, accessed by typing **msconfig** in the Start menu search box, can be used for so much more than just turning off startup programs. On the Boot tab of the System Configuration dialog box are several options you may find useful.

Select the Safe Boot check box to start the computer in Safe Mode the next time you restart it. This can be useful if you have a keyboard fault or if you keep missing the chance to press F8 at restart.

Select Boot Log (see Figure 15-8) to create a text file on the next startup that will report on everything that worked (and didn't). This can be an invaluable tool for diagnosing drivers or services that are failing to start when Windows loads. You can find this boot log on your Windows drive in the root folder; it is called ntblog.txt (see Figure 15-9).

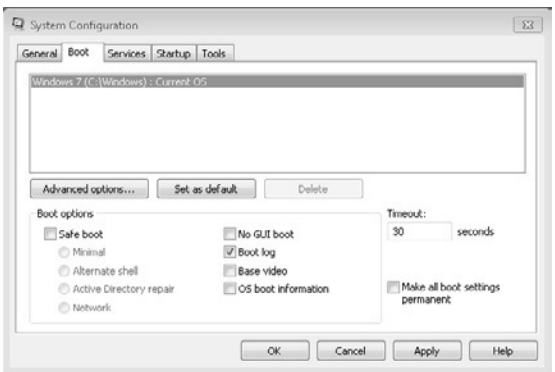


Figure 15-8 Diagnostic startups in MSConfig

Double-clicking the boot log will open it in Notepad (see Figure 15-10). The boot log shows a complete list of every system file and driver that loaded, or failed to load, when Windows started. This can be extremely useful information for diagnosing problematic services or drivers.

www.it-ebooks.info

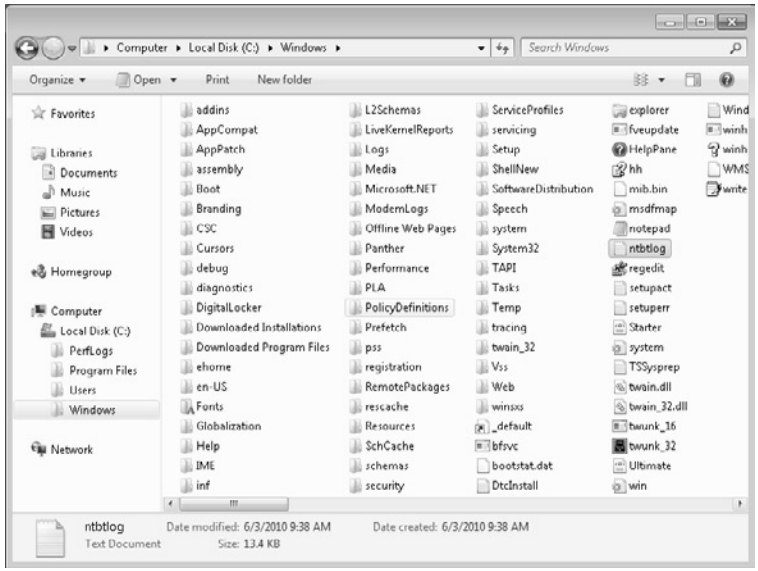


Figure 15-9 Finding the boot log in Windows

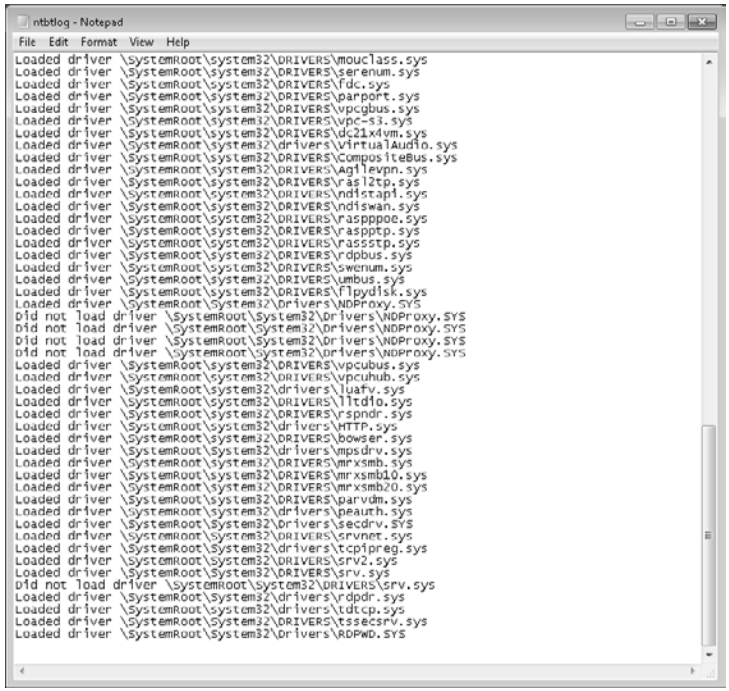


Figure 15-10 The boot log

www.it-ebooks.info

More startup options in MSConfig are on the General tab in the System Configuration dialog box (see Figure 15-11). Here you can disable startup programs and some services to start Windows 7 in a diagnostic mode that offers more functionality than Safe Mode. This diagnostic mode is a simple version of Windows 7 you can use to troubleshoot problems (see Figure 15-12).

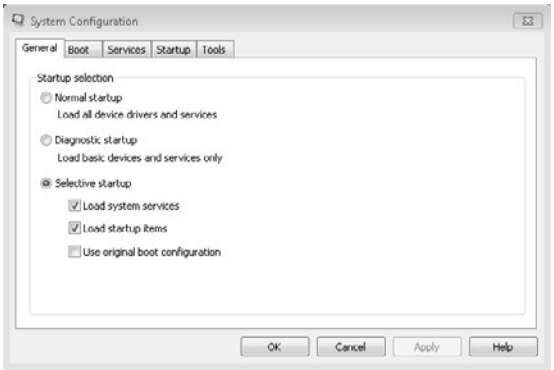


Figure 15-11 Additional startup options in MSConfig



Figure 15-12 MSConfig offers an additional startup diagnostic mode.

www.it-ebooks.info

Managing Windows Services

Services are operating system components that start when Windows loads or when you perform an action that requires a specific feature within the operating system. These services include managing the desktop interface, the firewall, and printer spooling.

CAUTION!

You should always be very careful when working with services in Windows 7 because deactivating the wrong one can make Windows unresponsive or even unable to start.

You can access the Services panel by typing **services.msc** in the Start menu search box (see Figure 15-13). The icon for this panel is a small blue cog.

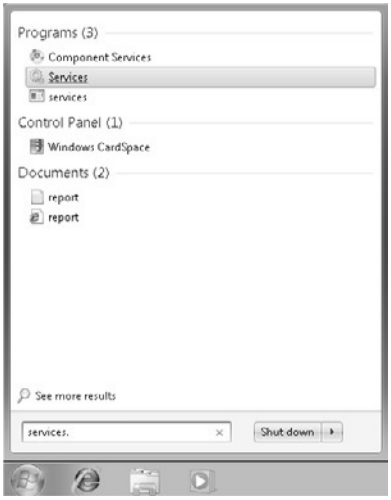


Figure 15-13 Accessing Windows services with the Start menu search box

In the main Services panel, shown in Figure 15-14, all Windows services are listed alphabetically. You can make columns wider to more easily read the content. The descriptions of the services are very helpful in making sure you do not disable the wrong one.

www.it-ebooks.info

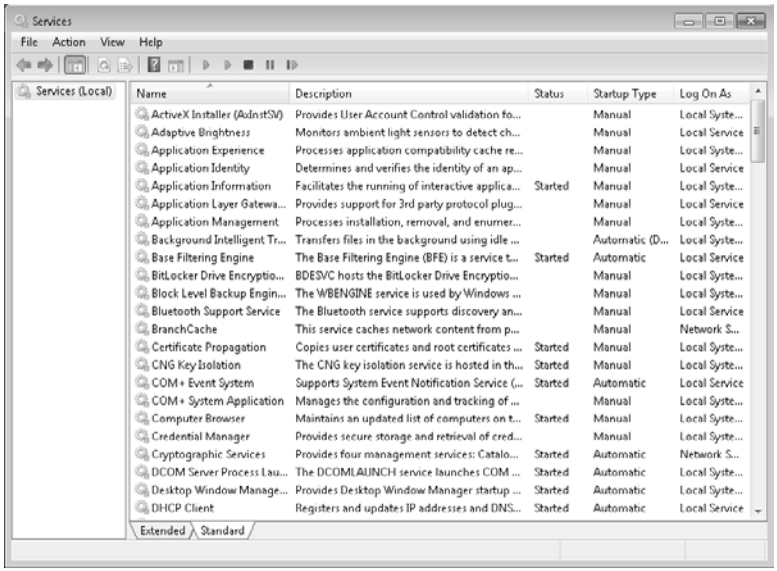


Figure 15-14 The Services panel

INSIDE OUT

When would you want to disable a service?

I would not recommend turning off any services that are part of Windows, but you might want to turn off third-party software services, for example trialware anti-virus software, that are causing slowdowns or other problems. In the Services panel you can stop these services from running or change the startup type to manual (so they will start only when called).

Right-click a service to access its Properties dialog box. On the General tab, you can disable the service if required (see Figure 15-15). Also, on the Recovery tab, you can choose what actions Windows should take if this service stops working for any reason.

Finally, on the Dependencies tab, you can check if this service cannot run without other services being active. You can check here if you are shutting down a service that, because it won't start the next time you start Windows, will cause another service to crash.

www.it-ebooks.info

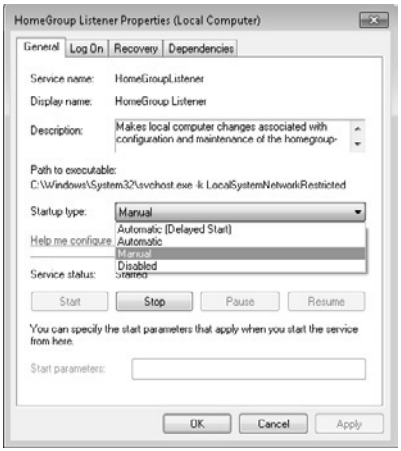


Figure 15-15 Setting the properties for a service

Working with the Windows Registry

The registry is a database where the settings for Windows and all of your installed software are kept. There is one copy of the registry for each user in hidden files called ntuser.dat located in the root of each user account folder on your Windows drive.

The Windows registry can be manually edited using Registry Editor (see Figure 15-16). To open this panel, type **registry** in the Start menu search box, and then select Registry Editor from the search results that appear.

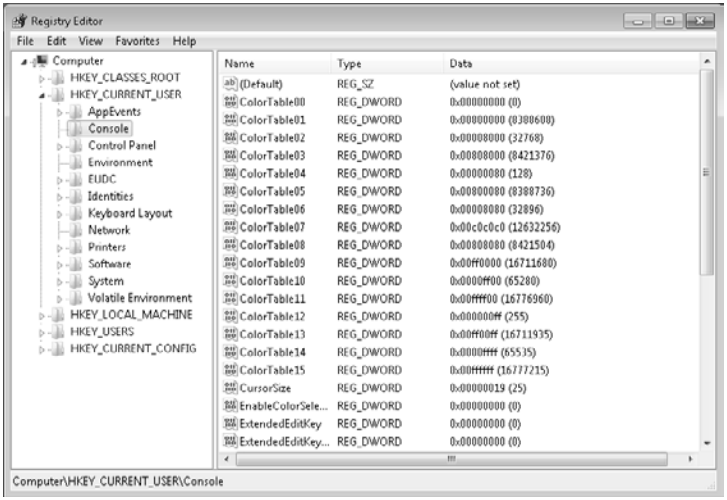


Figure 15-16 The Windows registry

www.it-ebooks.info

Occasionally, you may have to change or remove a setting in the Windows registry. You should always be very careful when you do this, because changing the wrong setting in the registry can cause Windows 7 to become unresponsive or unable to boot.

I will cover how to use the registry in depth in Chapter 27, "Advanced Registry Work." It is separated into five different sections.

- **HKEY_CLASSES_ROOT** You should not change these settings. They include essential Windows system settings along with other things such as file associations.
- **HKEY_CURRENT_USER** These are the custom settings for the currently logged-in user. These will include settings for Windows and installed software. These are the most commonly changed settings.
- **HKEY_LOCAL_MACHINE** This section is for general Windows and software settings. You may need to make changes in this section.
- **HKEY_USERS** This section is for general controls for user accounts; you will not need to change these settings.
- **HKEY_CURRENT_CONFIG** These are additional settings related to your current configuration; you will not need to change these settings.

There are only two situations when you will really need to change or remove settings in the Windows registry.

- When you are following specific written instructions on dealing with a problem, or tweaking advanced (hidden) settings in Windows 7
- When you are removing settings left behind by an uninstalled program that are causing problems with Windows 7 or other programs

As mentioned earlier, I will explain modifying the registry properly in Chapter 27, but the most common things you will need to do are create a new setting or change an existing one. You can do this by navigating to the correct place in the registry (you may be following specific instructions from a website or manual, which will guide you to exactly the right place in the registry) and right-clicking either a blank space to create a new setting or an existing setting to change it (see Figure 15-17).

www.it-ebooks.info

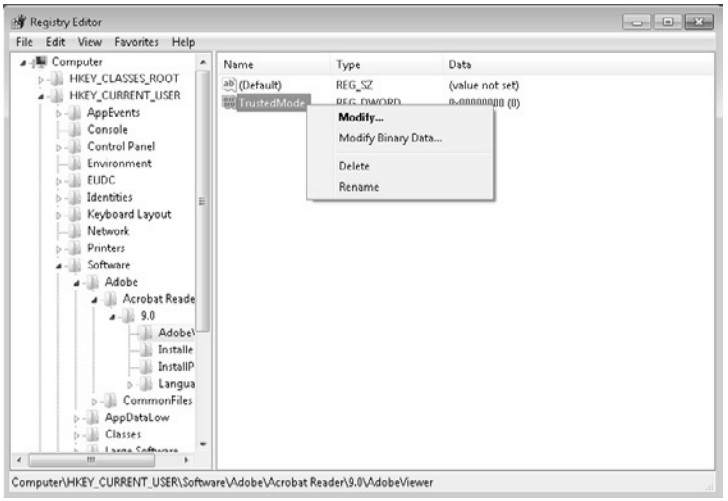


Figure 15-17 Changing a setting in the Windows registry

Removing the Registry Settings for an Uninstalled Program

There are two ways to find settings left behind by an improperly uninstalled program. The simplest way is to use the Find and Find Next controls on the Edit menu in Registry Editor (also available by pressing Ctrl+F [Find] or Ctrl+F3 [Find Next]).

You can also search for the settings manually. You will find them in the following two locations.

- HKEY_CURRENT_USER/Software
- HKEY_LOCAL_MACHINE/SOFTWARE

You can right-click a setting for a specific program and select Delete to remove it from the registry (see Figure 15-18). You should always be careful when you do this and back up the registry before you make any changes.

www.it-ebooks.info

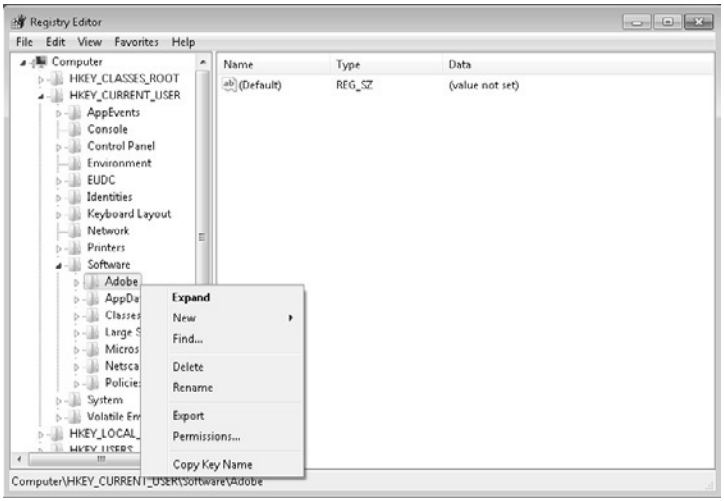


Figure 15-18 Removing unwanted software settings in the Windows registry

INSIDE OUT

Backing up the registry before making changes

You can create a backup copy of the registry by selecting Export on the File menu. You should always create a backup before making any changes to the registry. You can restore this backup the same way by selecting Import on the File menu. (Note that you may have to do this in Safe Mode if the changes you have made make Windows 7 unstable.)

Using the System Repair Disc for Advanced Restore

In Chapter 11, "Easy Ways to Fix Windows 7," I talked about Windows Startup Repair. This will automatically start when Windows has failed to load three times, but you can get more repair options by starting your PC from your Windows 7 installation DVD or by creating a system repair disc.

www.it-ebooks.info

INSIDE OUT Accessing System Recovery Options without a CD or DVD

You can access System Recovery Options on PCs where it has not been disabled by pressing F8 on your keyboard after the BIOS screen disappears but before you see the Starting Windows logo and selecting Repair Your Computer from the boot options. System Recovery Options may not function properly, however, if there is a problem with Windows or your hard disk.

Starting your PC from these discs gives you many more options for diagnosing and troubleshooting problems with Windows 7 startup.

INSIDE OUT Finding advanced options on the system repair disc

These advanced options do exist on the system repair disc, but they're hidden. To find them, you must direct Windows to restore your computer from a backup and then cancel that action when the options appear.

Click Command Prompt (see Figure 15-19) to access some very useful options for repairing your computer. You may be pleased to hear that **chkdsk** is still available at the command prompt in Windows 7. You can use it with the following command line switches.

- **/F** To fix errors on the disk
- **/R** To locate and attempt repairs on bad disk sectors
- **/X** To force, if necessary, the disk to dismount before checking

www.it-ebooks.info

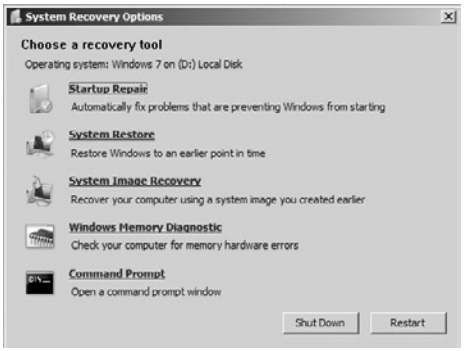


Figure 15-19 System Recovery Options on a Windows 7 system repair disc

There are several other options available by typing **chkdsk /?**.

BootRec.exe

For anyone who's missing the Recovery Console from Windows XP, fear not; it's still in Windows 7, but in a different form. The new Bootrec.exe command is accessed from Command Prompt in System Recovery Options. This will allow you to perform various actions by adding command line switches.

Repairing the Boot Menu by Using BootRec

The boot menu is the list of operating systems that appears when Windows starts. You will not see this menu if you have only one operating system installed. It can become corrupt, however, and will need to be rebuilt. You can do this by typing **bootrec /RebuildBcd** into a Command Prompt window (see Figure 15-20).



Figure 15-20 Rebuilding the Windows boot menu

www.it-ebooks.info

Sometimes this command won't work, and you will need to delete the boot menu and rebuild it from scratch. To do this from Command Prompt in System Recovery Options, type the following commands, and Windows will rebuild and restore the boot menu.

```
Bcdedit /export c:BCD_Backup
c:
cd boot
attrib bcd -s -h -r
ren c:\boot\bcd bcd.old
bootrec /RebuildBcd
```

There are other useful switches for use with the BootRec command.

/FixMbr

This switch, used at **bootrec /fixmbr**, will repair the master boot record (MBR) in Windows 7.

/FixBoot

This option, used at **bootrec /fixboot**, will write a new boot sector to the system disk. This can be useful if the boot sector has become corrupt or damaged, perhaps by trying to install an earlier version of Windows on the disk.

/ScanOS

This option, used at **bootrec /scanos**, will scan your hard disks for any compatible operating systems that may not be viewable on the boot menu.

BCDEdit

This is a program used for maintaining, changing, and rebuilding the boot menu in Windows 7. You should not need to use BCDEdit to repair your copy of Windows 7, because the tools I have mentioned already should repair any problems. However, if you need to use this tool, you can find detailed instructions on the Microsoft support website at *http://technet.microsoft.com/en-us/library/cc709667(WS.10).aspx*.

When you are finished with Command Prompt in System Recovery Options, type **exit** to close the window.

www.it-ebooks.info

Other DOS Commands in System Recovery Options

Other DOS commands are available in the Command Prompt window of System Recovery Options.

- **Copy** Copies files from one location to another
- **Move** Moves files from one location to another
- **Rd** Removes an empty **directory**
- **Ren** Renames a file or directory
- **More** Shows the contents of a file
- **Type** Shows all the contents of a file without pausing the screen
- **Xcopy** Copies a folder and all of its contents to another location
- **Mkdir** Makes a new directory
- **Diskpart** Loads the Windows disk management program
- **Dir** Displays a list of files and folders
- **Cd** Allows you to move to a different folder
- **Attrib** Allows you to change the attributes of the file (Read only etc.)
- **Del** Deletes a file

The switch options for each command are available by using the /? switch after the command.

Windows Memory Diagnostic

Another option in System Recovery Options is Windows Memory Diagnostic. This will scan your computer's physical memory to see if it can find any errors that are preventing Windows 7 from starting or running properly (see Figure 15-21).

www.it-ebooks.info

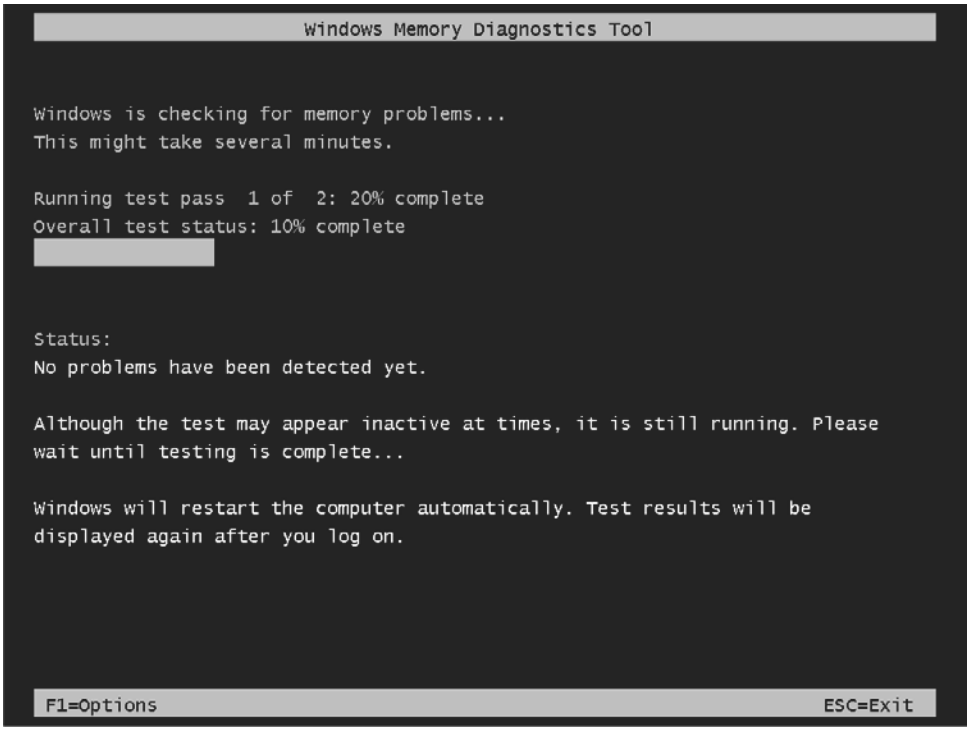


Figure 15-21 Windows Memory Diagnostic

While physical hardware problems are rare, a memory problem would certainly cause Windows to encounter a critical stop error and show the Blue Screen of Death (BSOD) during startup.

If you get BSOD messages when starting Windows, it is a good idea to try the Windows Memory Diagnostic tool.

Using Safe Mode

You may also want to start your PC in Safe Mode by pressing the F8 key during startup to open the boot options menu. Here, you'll see a stripped-down diagnostic mode of Windows in which you can run tests and check to see if the operating system is functioning correctly.

> **Note**
>
> **You can see the tools that I have described in Chapter 14, "Advanced Diagnostic Tools in Windows 7," and earlier in this chapter.**

www.it-ebooks.info

Summary

Windows 7 contains a great many components, each of which is very complex and many of which have dependencies on each other. Some of the fixes described in this chapter have been specifically designed by Microsoft to allow you to repair and maintain the components, such as Internet Explorer, that have traditionally caused the most problems. Others are more generic fixes.

When an installed component or a bundled piece of software fails, it can be very difficult to repair, because some components cannot be uninstalled. However, there is usually a way to repair the problem when it occurs.

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 16

Windows Problems Demystified

Windows 7 Core Operating System Files 257
Advanced File Restore 262
System File Checker 263
Creating a Slipstreamed Install DVD 263
Summary 272

WINDOWS 7 includes a huge number of files and folders, and I could write an entire book about what each one does. In this chapter, however, I deal with the most important folders and file types, explaining the significance of each one.

INSIDE OUT

Show hidden system files and file extensions in Windows Explorer

By default, Windows 7 hides certain system files and file extensions so that you can't see them when you explore files and folders on your computer. To view these hidden files and extensions, press Alt on your keyboard in any Windows Explorer window and select Folder Options on the Tools menu in a Windows Explorer window. The Folder Options dialog box appears. (Alternatively, you can open the Organize menu from the Windows Explorer toolbar and select Folder And Search Options.) On the View tab in the Folder Options dialog box, select the Show Hidden Files, Folders And Drives option, the (Un)Hide Extensions For Known File Types option, and the (Un)Hide Protected Operating System Files option.

Windows 7 Core Operating System Files

Figure 16-1 shows the full Windows 7 folder structure. Some of these folders contain files for specific functions. For example, the ehome folder includes Windows Media Center files and the **Fonts** folder stores Windows fonts.

www.it-ebooks.info

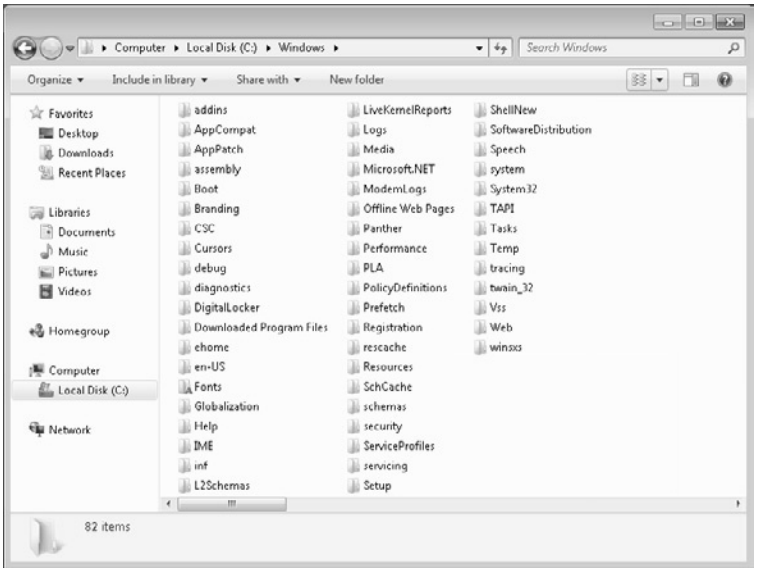


Figure 16-1 The folder structure for Windows 7

A few of these folders contain core operating system files, and it's worth focusing on these folders, because this is where file corruptions are most likely to occur.

X:\Windows\Boot This folder contains files necessary for starting Windows 7.

X:\Windows\Help The Windows 7 help files are located in the Help folder. If you cannot start Help, these files might be corrupt or missing.

X:\Windows\inf Windows uses the INF files in this folder when installing hardware and software drivers.

X:\Windows\System32 This folder contains the guts of Windows 7. All the main Windows components are located here. If you have a problem with a Windows file, it is likely located in this folder.

The following files are commonly located within the X:\Windows\System32 folder sub-structure.

ActiveX Files (*.ocx) ActiveX is a programming framework that software authors use to design reusable components to be shared across applications. Sometimes these controls are shared across programs from different software houses, and in older software, there might be incompatibilities with various versions of the .ocx files. For example, one program might require a specific version of the file, but another program needs a different version. Windows 7 is much better at handling these conflicts than previous versions of Windows; however, such conflicts can still occur.

www.it-ebooks.info

Applications Applications are the main programs that comprise Windows 7. If you are trying to launch a built-in Windows feature and it cannot be found, the associated application file might be missing from the Applications folder.

Application Extensions (*.dll) Dynamic Link Library (.dll) files are shared library files. Like .ocx files, .dll files are program and Windows components that can be shared across software applications. Occasionally, Windows becomes unresponsive because a .dll file is corrupt or is an incorrect version that is not supported by the program or feature trying to access it.

As with .ocx files, Windows 7 is much better than previous versions of Windows at handling .dll file conflicts, but issues with these files can still occur. Windows 7 includes more .dll files than any other type of file.

Control Panel Item (*.cpl) Windows 7 launches .cpl files when you access features in Control Panel. If an item cannot be found, the associated .cpl file might be missing or corrupt.

Device Driver (*.drv) The Device Driver folder contains certain Windows 7 software and hardware drivers. These files can occasionally become corrupt.

Boot The Boot folder contains the programs required to start Windows. If these files are deleted or become corrupt, Windows will not start.

Drivers and DriverStore These folders contain all of the software drivers for your hardware. You can back up these folders and restore them manually if an event such as a driver malfunction or faulty driver upgrade causes problems with Windows 7.

Microsoft Common Console Document The Microsoft Management Console (MMC) programs are stored in this folder. If you cannot start an MMC item, the program file might be corrupt or missing from this folder.

VBScript Script File (*.vbs) Visual Basic VBScript scripts can be a target for virus writers. Some VBScript scripts are stored in the main Windows 7 folders.

X:\Windows\winsxs Earlier, I discussed side-by-side compatibility protection for different versions of .dll, .ocx, and other files in Windows 7. Windows stores and organizes compatible duplicate versions of files in the winsxs folder. This folder is usually very large and even bigger than the System32 folder.

X:\Users\AppData In each user's folder is a subfolder named AppData, as shown in Figure 16-2. Application-specific files and settings are stored in this folder.

www.it-ebooks.info

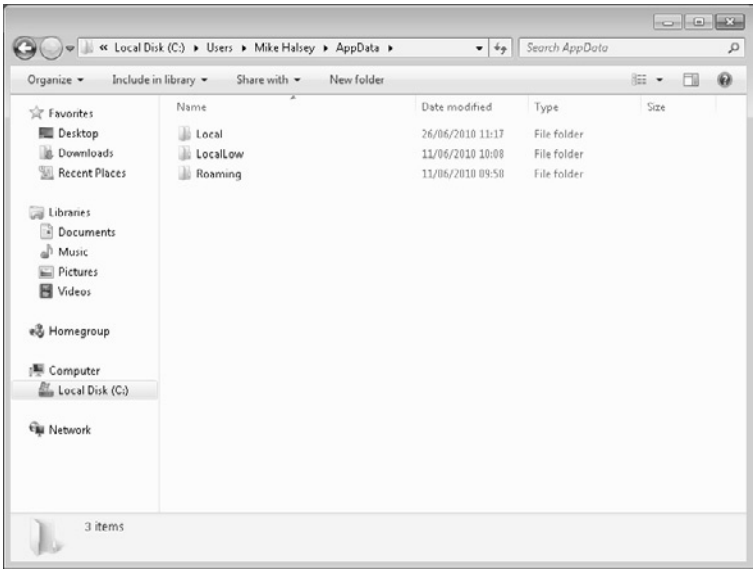


Figure 16-2 The AppData subfolders

The AppData folder is hidden by default, so you will need to change the default setting to show hidden files to see the folder contents. See the Inside Out sidebar "Show hidden system files and file extensions in Windows Explorer" earlier in this chapter for details.

Windows 7 Security and Policy Folders

Windows security and other policies that control login, software, and user behavior and permissions are stored in the following folders.

- X:\Windows\Security
- X:\Windows\ServiceProfiles

The Windows 7 Registry

The registry is a database that contains configuration options and settings for Windows and your installed programs. There is one registry folder named NTUSER.DAT for each user. You can see one hidden registry file in Figure 16-3 and can make all of them visible by showing hidden and operating system files. See the Inside Out sidebar "Show hidden system files and file extensions in Windows Explorer" earlier in this chapter for details.

www.it-ebooks.info

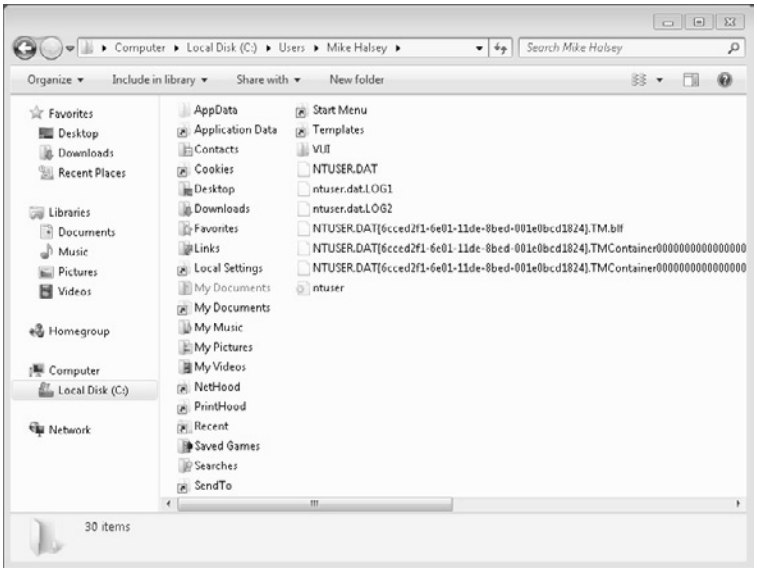


Figure 16-3 The registry files are hidden in user folders.

Personalization Folders

The main folders containing wallpapers and other personalization options are:

- X:\Windows\Globalization
- X:\Windows\Media
- X:\Windows\Resources
- X:\Windows\Web

Windows 7 Logs

Several folders contain Windows 7 logs. You can normally access these logs through Control Panel and Microsoft Management Console. You can also access the logs manually if you can't get Windows 7 to start. You can find the logs in the following folders.

- X:\Windows\debug
- X:\Windows\diagnostics

www.it-ebooks.info

- X:\Windows\LiveKernelReports
- X:\Windows\Logs
- X:\Windows\ModemLogs

Temporary Files Stores

You can delete all the contents in several Windows 7 folders if you suspect they are causing problems.

- **X:\Windows\Downloaded Program Files** Windows does not usually use this folder, so it will normally be empty anyway.
- **X:\Windows\Prefetch** Windows tracks what programs and files you frequently use and stores this information in the Prefetch folder to preload them when appropriate (for instance, when starting a program you run often). Sometimes the prefetch files can become corrupt. If you suspect this has happened, you can safely delete the contents of this folder. Windows will then rebuild the prefetch database.
- **X:\Windows\SoftwareDistribution** This folder contains Windows Update configuration options and downloaded files. If Windows Update will not install updates, you can delete the contents of this folder to try to fix the problem.
- **X:\Windows\Temp** This folder is the temporary files store. Its contents can be deleted at any time if you suspect one or more temporary files is causing a problem.

Advanced File Restore

As I stated previously, I could write an entire book on the Windows 7 file and folder structure. But the guide presented in the previous section should be enough to help you restore Windows 7 files and folders on a file-by-file, folder-by-folder basis. You can infer from this discussion that you do not need to restore folders that contain temporary files; temporary files are unnecessary when restoring Windows to working order, and you could run the risk of restoring a corrupt file. You can also use the descriptions above to decide which folders containing user personalization options to specifically include or ignore in a restore.

The most important folders, and the ones you are most likely to restore, are the Boot, INF, System32, and WinSxS folders. These folders contain the essential parts of the operating system. Most likely, problems are caused by corrupt or missing files in these essential folders.

www.it-ebooks.info

CAUTION!

If you restore the folders containing security or other computer policies, be certain that there have been no changes since the backup was made. If changes were made, you could encounter additional problems, such as a faulty smart card or fingerprint reader.

System File Checker

I wrote about the extremely useful System File Checker in Chapter 15, "Advanced Repair Methods." This utility checks every system file in Windows against the original version on the installation DVD. If it finds a file that has changed or become corrupt, it restores the original file.

System File Checker quickly repairs problems with Windows 7, but if you have a service pack installed on your computer, you will also need to **slipstream** the service pack onto the installation DVD before running System File Checker. The following section details how to create a slipstreamed DVD.

Creating a Slipstreamed Install DVD

Slipstreaming is the process of integrating a service pack into the original installation DVD. You might want to do this for a couple of reasons. First, a slipstreamed installation DVD is useful when you need to reinstall Windows or install it on a new PC. A slipstreamed version of the software is far better updated than the original install. You may also want to create a slipstreamed installation DVD if you want to use System File Checker as mentioned previously. The installation DVD you use with System File Checker must include the service pack that matches the one installed on your PC. If it doesn't, some operating system files will not match, and System File Checker will abort with an error.

Sadly, creating a slipstreamed service pack installation DVD for Windows 7 isn't as simple as it is for Windows XP. With Windows XP, you simply copy the contents of your Windows XP installation disc to your hard drive and use an /integrate switch with the service pack to build it into the file structure. Then you burn back to a bootable DVD. This procedure changed with Windows Vista, and while you can still slipstream, it's a significantly more complex process. Here, however, I'll describe how to do it step by step.

www.it-ebooks.info

What You Will Need

Before beginning the slipstream procedure, gather the following items.

- A spare hard disk or partition on which you can install a fresh copy of Windows 7.
- The Windows 7 Automated Installation Kit (AIK), which you can download for free from *http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34* or by searching the Microsoft website for Windows 7 AIK. You will need approximately 1.5 GB of free disk space to install the Windows AIK on your PC.
- A blank CD or DVD.
- Software for creating an ISO file such as UltraISO, (available from *www.ezbsystems.com/ultraiso*) or WinISO (available from *www.winiso.com*). You might be able to download a free trial version of the software, which will be fine for a quick job.

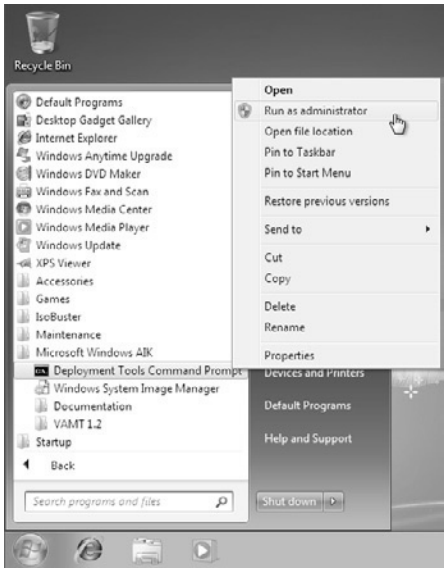
Step 1: Creating a Windows Pre-Installation Environment Startup Disc

1. You first need to create a startup disc for the Windows Pre-Installation Environment (WinPE). To do this, run the Windows 7 AIK installer and select Windows AIK Setup.



2. When the Windows 7 AIK is installed, select Microsoft Windows AIK from the Start menu, right-click Deployment Tools Command Prompt, and select Run As Administrator.

www.it-ebooks.info



3. In the command prompt window that appears, type **C:** and press Enter. Then type **cd .\Program Files\Windows AIK\Tools**, and press Enter again to access the AIK folder.

4. Use the Copype.cmd script, changing the arguments as necessary to match the locations for your WinPE files and the desired destination folder. (Valid versions include 32-bit [x86] or 64-bit [x64]. Other supported types are amd64 and ia64.)

   Type **copype.cmd x86 C:\winpe_x86** or **copype.cmd x64 C:\winpe_x64**, and press Enter.

5. The command in step 4 creates a folder structure in a new folder. (For the purposes of this tutorial, we'll assume this is C:\winpe_x86.)

   Next, to copy the base WinPE image to this folder structure, type **copy C:\winpe_x86\winpe.wim C:\winpe_x86\ISO\sources\bot.wim**, and press Enter.

6. Next, you need to add disk boot files to the files you have created in steps 4 and 5, ready for burning to a CD or DVD.

   a. Type **dism /Mount-wim /Winfile:C:\winpe_x86\ISO\sources\boot.wim /index:1 /MountDir:C:\winpe_x86\mount**, and press Enter.

   b. Type **copy C:\winpe_x86\ISO\bootmgr C:\winpe_x86\mount**, and press Enter.

www.it-ebooks.info

c. Type **mkdir C:\winpe_x86\mount\boot**, and press Enter.

d. Type **xcopy /cherky C:\winpe_x86\ISO\boot C:\winpe_x86\mount\boot**, and press Enter.

7. Add the ImageX disc image creation program to the folder by typing **copy "C:\Program Files\Windows AIK\Tools\x86\ImageX.exe" C:\winpe_x86\mount**, and pressing Enter.

8. Next, create the boot configuration data (BCD) file for the disc. Type the following commands, pressing Enter after each one.

   a. **Del c:\winpe_x86\mount\boot\BCD**

   b. **Bcdedit /createstore c:\winpe_x86\mount\boot\BCD**

   c. **Bcdedit /store c:\winpe_x86\mount\boot\BCD -create {bootmgr} /d "Boot Manager"**

   d. **Bcdedit /store c:\winpe_x86\mount\boot\BCD -set {bootmgr} device boot**

   e. **Bcdedit /store c:\winpe_x86\mount\boot\BCD -create /d "WINPE" -application osloader**

9. The command in step 8e returns a GUID value. Type the following commands, substituting the GUID value returned by step 8e for {GUID}. The GUID should look similar to *{21EC2020-3AEA-1069-A2DD-08002B30309D}* but will contain different numbers and letters. Press Enter on your keyboard after each step.

   a. **Bcdedit /store c:\winpe_x86\mount\boot\BCD -set {GUID} osdevice boot**

   b. **Bcdedit /store c:\winpe_x86\mount\boot\BCD -set {GUID} device boot**

   c. **Bcdedit /store c:\winpe_x86\mount\boot\BCD -set {GUID} path \windows\system32\winload.exe**

   d. **Bcdedit /store c:\winpe_x86\mount\boot\BCD -set {GUID} systemroot \windows**

   e. **Bcdedit /store c:\winpe_x86\mount\boot\BCD -set {GUID} winpe yes**

   f. **Bcdedit /store c:\winpe_x86\mount\boot\BCD -displayorder {GUID} -addlast**

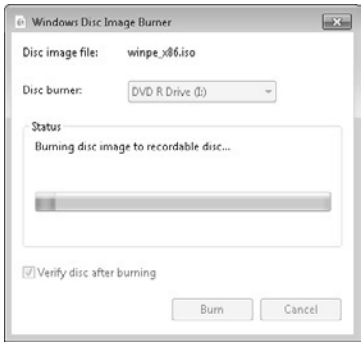
www.it-ebooks.info

10. Finally, create an ISO disc image that you can burn to a CD or DVD. Type **oscdimg –n –m –o –bC:\winpe_x86\etfsboot.com C:\winpe_x86\mount C:\winpe_x86\winpe_x86.iso**, and press Enter.

    For Intel Itanium–based architecture, replace **etfsboot.com** with **efisys.bin**.

    If you are building an ISO to an AMD Extensible Firmware Interface (EFI) ISO instead, type **oscdimg.exe –bC:\winpe-x64-efi\efisys.bin –pEF –u1 –udfver102 C:\winpe-x64-efi\ISO x64-efi-winpe.iso**, and press Enter.

11. You will now have an ISO file in the C:\winpe_x86 folder that you can double-click to start Windows Disc Image Burner.



Note

You only ever need to create a single WinPE startup disc (and disc image). You can use the same disc to install a slipstreamed version of Windows 7 on any computer.

Step 2: Installing a Fresh Copy of Windows 7

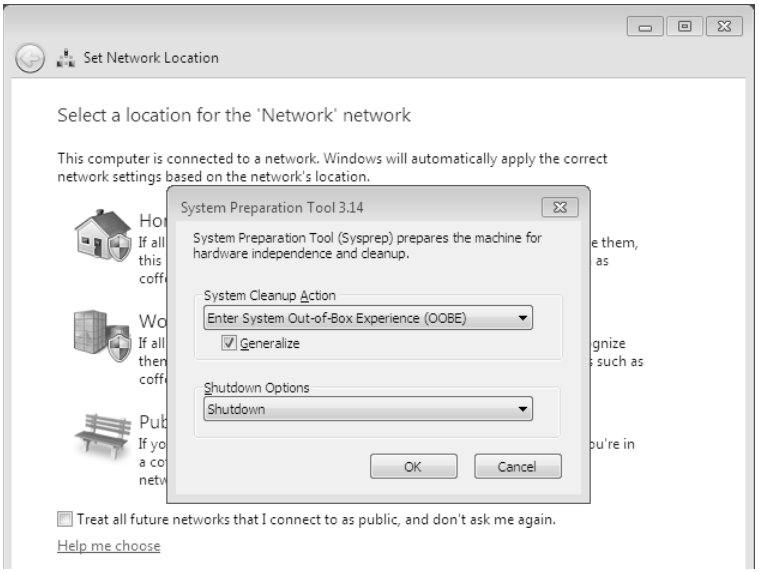
1. Using your Windows 7 installation DVD, install a fresh copy of Windows 7 onto a spare hard disk or partition. Use the version you want to create the slipstreamed disc for, that is Home Premium, Professional, Enterprise, and so on.

2. When Windows 7 is installed and the screen asking for your username and password appears, press Ctrl+Shift+F3 on your keyboard.

www.it-ebooks.info

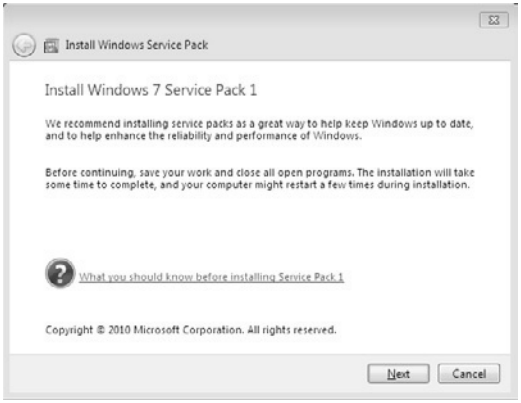


3. The system restarts in audit mode. *Do not* close the System Preparation Tool window that appears; you will need it later.



4. Install the appropriate service pack. (You can either download the service pack or install it from a CD, network, or USB pen drive).

www.it-ebooks.info



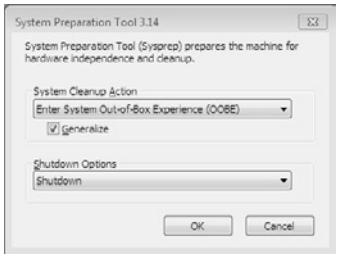
5. Windows may restart during the service pack installation. If the Windows 7 password screen appears again, press Ctrl+Shift+F3 again to re-enter Audit Mode.

INSIDE OUT Performing other actions in Audit Mode

You can also perform other actions in Audit Mode, such as installing software, changing Windows settings, or installing device drivers. Be careful installing drivers if you intend to use this new install image to install Windows on a different PC from the one you are creating the image on, because the hardware will likely be different. Also take care when installing software; you must leave enough space for the final disc image to fit on a single blank DVD.

6. In the System Preparation Tool window, select Enter System Out-Of-Box Experience (OOBE) from the System Cleanup Action menu, and select the Generalize option.

   Place the WinPE startup disc in the CD/DVD drive. In the System Preparation Tool dialog box, select Restart under Shutdown Options, and then click OK when you are ready to create the new Windows image.



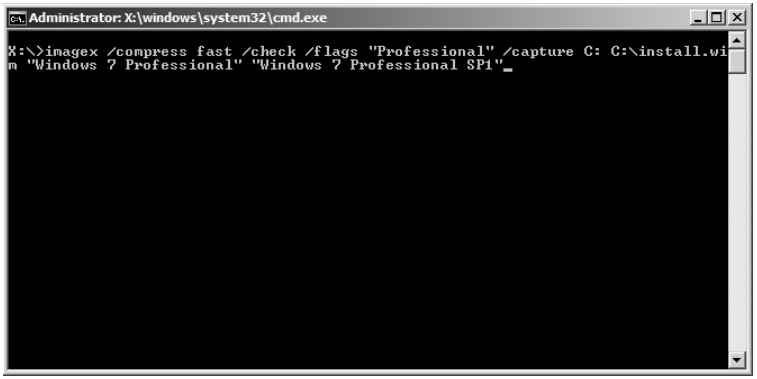
www.it-ebooks.info

Step 3: Creating a New Windows Image File

1. After you follow the previous procedure, the system will start in the WinPE environment, and a command prompt window will appear.

   Noting the following substitution guidelines, type **E:\imagex /compress fast /check /flags "Professional" /capture D: E:\install.wim "Windows 7 Professional" "Windows 7 Professional Custom"** at the command prompt.

   - If necessary, substitute the name of your Windows 7 edition for *Professional* in the command.
   - Substitute the drive letters of the disks on which you have the second copy of Windows 7 installed and the disk where you want WinPE to store the new Windows 7 Image file. The file will be approximately 2 to 2.5 GB.



Step 4: Creating a New Windows 7 Installation DVD

1. Use ISO creation software (see the Inside Out sidebar below for more information about where you can get this) to make an ISO file from your original Windows 7 installation DVD.

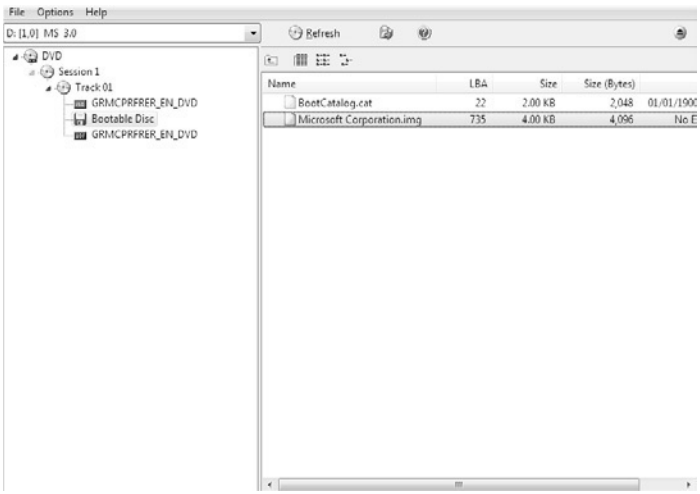
2. Using the same ISO creation software, locate the newly created Install.wim file you created in the previous procedure and add it to the disc image file, overwriting the one that exists there in the \sources\ folder. Double-click the image to burn it to the DVD using the Windows Disc Image Burner.

www.it-ebooks.info

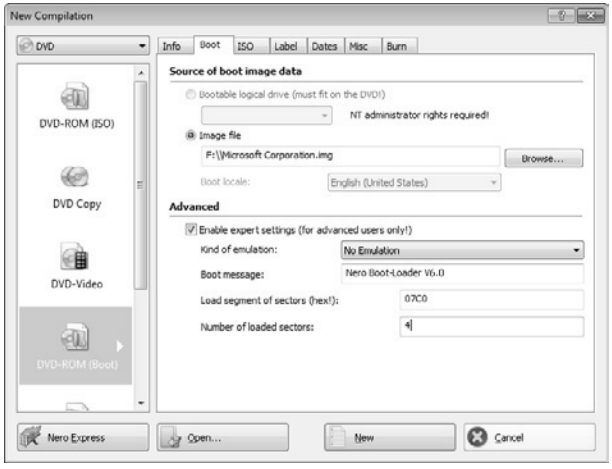
INSIDE OUT

Extracting a Windows 7 DVD to your hard disk

Depending on what ISO creation software you are using, you may need to extract the contents of the installation DVD to your hard disk and then add the new Install.wim file to it there. To re-burn your image to a disc, you may need a Microsoft bootable disc image. You can use software such as ISOBuster (available at *www.isobuster.com*) to extract the Microsoft Corporation.img file from the disc.



You will also need DVD burning software such as Nero (*www.nero.com*) or Roxio (*www.roxio.com*) to burn this new replacement Windows 7 install disc. In Nero, use the options shown in the following image.



www.it-ebooks.info

> **Tip**
>
> **You can delete the second copy of Windows 7 once you are done with the procedures, although I always recommend testing the install disc before deleting anything that's taken a long time to install and configure.**

Third-Party Slipstreaming Software

Third-party solutions are available for slipstreaming Windows service packs. Two popular programs for Windows Vista are vLite (*www.vlite.com*) and Vista Update Integrator (*www.winvistaside.de*), which may be updated to support Windows 7. These third-party programs can simplify the Windows 7 service pack slipstreaming process and can also offer support for creating discs that will install into any edition of Windows 7.

When software becomes available to make slipstreaming Windows 7 service packs simple, I will announce it on my website, *www.thelongclimb.com*.

Summary

Windows 7 is an extremely complex piece of software engineering. Third-party tools can streamline some processes, such as creating a slipstreamed service pack installation DVD, but, generally, the file, folder, and maintenance structure of Windows 7 makes file-level work very difficult.

The complexity of Windows 7 is due in large part to the need to maintain compatibility with legacy hardware and software, which is why so many empty folders sit on your Windows drive. If particular files and folders not listed in this chapter are causing problems, I suggest a quick search online or on a website such as *http://technet.microsoft.com* where you will commonly find that you are not the first person to encounter your problem.

www.it-ebooks.info

CHAPTER 17

Remote Help

Using the Internet to Find Solutions to Problems. 273
Windows Remote Desktop 278
Windows Remote Assistance 281
Problem Steps Recorder 285
Summary 288

You can get help with Windows 7 and your PC in many places outside your home or office. In this chapter, I'll cover how you can quickly find solutions yourself and how you can easily get help from other people over a broadband connection.

Using the Internet to Find Solutions to Problems

You're never alone as long as you have an Internet connection. Whatever problem you face with your computer, you're almost certainly not the first person to encounter it. A great many websites exist to help with computer problems, and technical experts can be very generous about sharing solutions to problems they've encountered.

The major search engines are extremely good at recognizing search queries and providing relevant results. Searching for **network driver for dell laptop**, for instance, brings up a whole page of results, all offering appropriate drivers to download.

Sometimes, however, your search entry is more imprecise and returns too many results. This means you might not immediately find the information you need. In these instances, there are some simple search techniques you can use in all the major search engines to improve the results you get.

- **Searching "in quotes"** Putting text into double inverted commas (as in "text") is a useful way to make certain that the search engine treats the text inside the quotes as a string and not as separate words.
- **Adding a plus (+) or minus (–) sign** Adding a plus (+) or minus (–) in front of a word or phrase will ensure that term definitely *is* or *is not* in the search results. For instance, if you are searching for a driver for specific hardware but don't want search results advertising the item, adding **–shop** could help filter consumer sites from the search results.

www.it-ebooks.info

- **AND, OR, and NOT** These are other terms you can use in search entries to tailor your results (although I find the plus [+] and minus [–] signs easier to use). For example, if you are looking for a driver and know the name of your hardware but not the name of the generic driver you need, you might search for **connexant OR dynamode BT878a driver** (where *BT878a* is the name of your hardware). Adding the qualifiers linked with *OR* narrows the search more than just searching for **BT878a**.

Of course, you first need to know what to search for when trying to find a solution to a problem. Try to pick up clues from the information provided by anti-virus or anti-malware software, the Windows event log, or a Windows or other software error message. If you notice a code or the name of a program, virus, or service, write it down right away. You never know when that onscreen message might disappear accidentally or otherwise.

Try not to use irrelevant words in your search terms; keep things short and to the point. If your search item includes characters like periods or forward slashes (common in virus names), enclose the term in quotes, for example **"Win32.Gattman.A"**.

Finally, use plus (+) signs before specific terms to ensure that they appear in the search results. For example, the search phrase **+"win32.Gattman.A" +"windows 7" +remove** provides only results that include the terms *win32.Gattman.A* and *Windows 7* and *remove*.

Where Else to Get Help

Plenty of websites provide excellent help and support, including Microsoft sites, and you might be surprised just how good these sites are and how quickly people can answer your questions.

Microsoft's main support website, found at *support.microsoft.com*, features a huge amount of help and support in an easy-to-navigate interface (see Figure 17-1).

You can customize the Microsoft Support center depending on whether you are a home user, an IT professional, or a developer. There are also advanced search tools.

The Microsoft Windows 7 Solution Center, shown in Figure 17-2, is easily accessed through the Microsoft Support website. It contains a whole host of Windows 7 problems and solutions, all helpfully categorized and written in simple language.

www.it-ebooks.info



Figure 17-1 The Microsoft Support website



Figure 17-2 The Microsoft Windows 7 Solution Center

www.it-ebooks.info

Also available through the Microsoft Support website is Microsoft Answers (see Figure 17-3). This is an advanced forums tool where experts can help you find the answers to the problems you have. This site will only grow over time and already contains a vast array of knowledge, all presented in a helpful and friendly way. You can access Microsoft Answers directly at *answers.microsoft.com*.



Figure 17-3 The Microsoft Answers website

For advanced users, there's also Microsoft TechNet, accessed at *technet.microsoft.com* (see Figure 17-4). Here you can get advanced help in real time from experts and other users on every aspect of every Microsoft product. You might be surprised how quickly people will reply to your questions here, too. The direct link to Windows 7 Troubleshooting in Microsoft TechNet is *technet.microsoft.com/en-us/library/dd349347(WS.10).aspx*.

www.it-ebooks.info

INSIDE OUT Subscribing to Microsoft TechNet

If you subscribe to Microsoft TechNet, in addition to evaluation copies of Microsoft software and operating systems, you get access to online training courses and forums that are open only to other technical professionals. You can subscribe to Microsoft TechNet at *http://technet.microsoft.com/en-us/subscriptions/*.

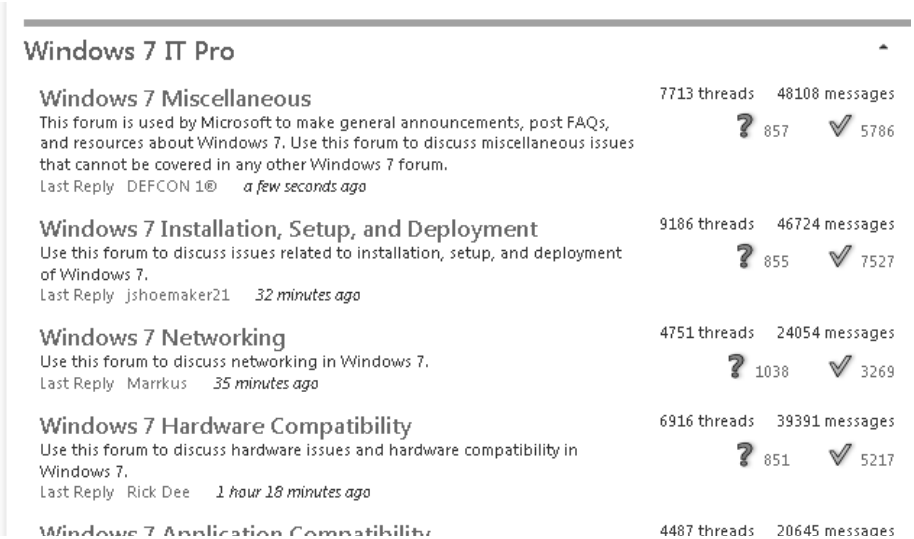


Figure 17-4 Microsoft TechNet

Third-party hardware and software manufacturers almost always host help forums on their own websites as well. These sites are, if nothing else, a good way to reduce a company's support costs by helping customers to help each other. These manufacturers also have their own experts available to help with problems, and a great many companies offer email and technical support, too.

You can find other online forums and articles containing help and advice. The best ones are always free; I don't suggest that you pay to join a help forum. You will need to decide for yourself how valuable a particular website or service is.

I'll talk more about these forums and websites in Chapter 18, "Where to Find More Help and Support."

www.it-ebooks.info

Windows Remote Desktop

If your PC is in a corporate environment, your IT helpdesk might be able to use Windows **Remote Desktop** or a similar system to gain access to your computer. You might consider it slightly disconcerting to see the pointer moving around the screen apparently on its own, but this is a good way for an organization to provide support and reduce overall costs.

Before beginning a remote help session, make sure that your PC is on. If you want to set up a remote desktop connection to another PC, you can access Remote Desktop by typing **remote** in the Start menu search box and selecting Remote Desktop Connection from the results that appear (see Figures 17-5 and 17-6).



Figure 17-5 Accessing Windows Remote Desktop

INSIDE OUT Third-party firewalls and remote help

Third-party firewalls can block Remote Desktop or Windows Remote Assistance attempts to connect to your PC. You can temporarily disable the firewall to allow connection if required. If you are using the Windows 7 built-in firewall, it is already correctly configured for remote help and won't give you any problems.

www.it-ebooks.info



Figure 17-6 The Remote Desktop Connection dialog box

The PC you want to connect to must be on your network or virtual private network (VPN), and you will need to know its name on the system to connect. Some organizations use Remote Desktop across the Internet to provide support for customers, although others may use **Remote Assistance** (see "Windows Remote Assistance" later in this chapter).

The target PC will also need to be configured to receive Remote Desktop connections. These settings can be found in Control Panel by clicking System And Security, clicking System, and then clicking the Advanced System Settings link. The options to allow remote connections can be found on the Remote tab of the dialog box that appears (see Figure 17-7).

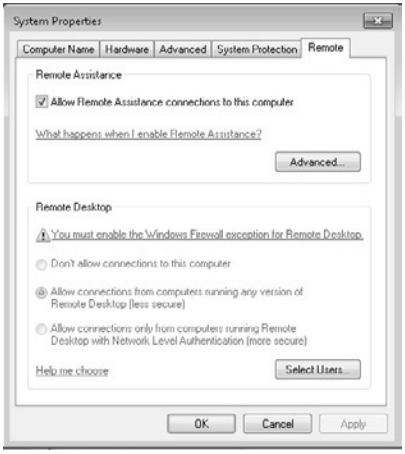


Figure 17-7 Advanced System Settings for remote connections

www.it-ebooks.info

You might need to allow Remote Desktop through your firewall. You can access Windows Firewall settings from the Control Panel by clicking System And Security, and then clicking Windows Firewall. Click Allow A Program Or Feature Through Windows Firewall to allow Remote Desktop (see Figure 17-8).

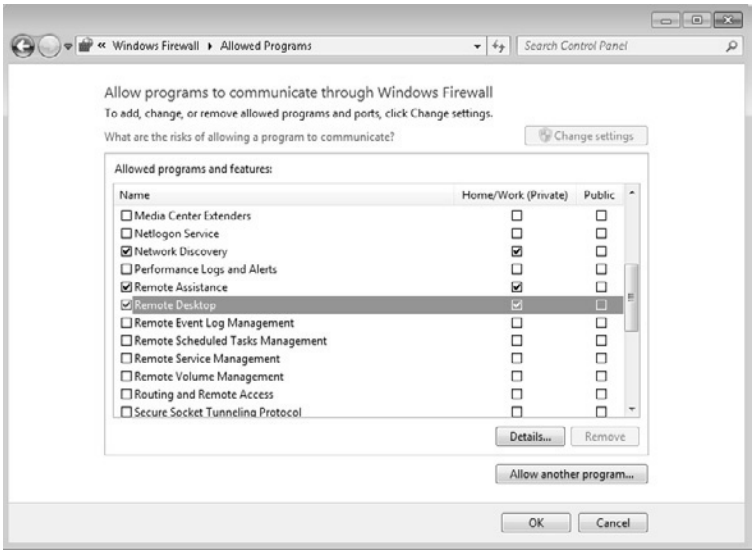


Figure 17-8 Allowing Remote Desktop through Windows Firewall

If Remote Desktop is unable to verify the identity of the computer when you try to connect to a remote PC, a warning appears, as shown in Figure 17-9. This will happen if Windows suspects that connecting to this PC could pose a security risk to your system.



Figure 17-9 Windows alert to potential security threats when using Remote Desktop

www.it-ebooks.info

Once connected, the person who initiated the Remote Desktop connection has full access to your PC to remotely diagnose any problems.

> **Note**
>
> **By default, most routers allow a Remote Desktop connection across the Internet. If you cannot connect, however, you may have to log in to your router and change certain router settings, such as opening a connection port or permitting Remote Desktop. You should consult your router manual or help document for details on how to do this.**

Windows Remote Assistance

Although Remote Desktop is helpful and common in organizations where the computers are owned by the employer and people do not keep personal files and data on their machines, home users need something that can give them more control over what a remote user can access. Furthermore, Remote Desktop grants complete, unfettered control of a PC to a remote user for long periods of time, but it isn't so user-friendly for the person sitting in front of the computer. He is logged out of the computer and unable to see what is happening.

Windows Remote Assistance addresses this issue by enabling the user receiving the support to monitor exactly what's being done throughout the remote help session. Remote Assistance also provides controls to enable a user to regain full control of the PC and terminate the remote connection at any time.

Remote Assistance is intended for use over the Internet; you will need a broadband connection that's not busy with other activities, such as downloading files.

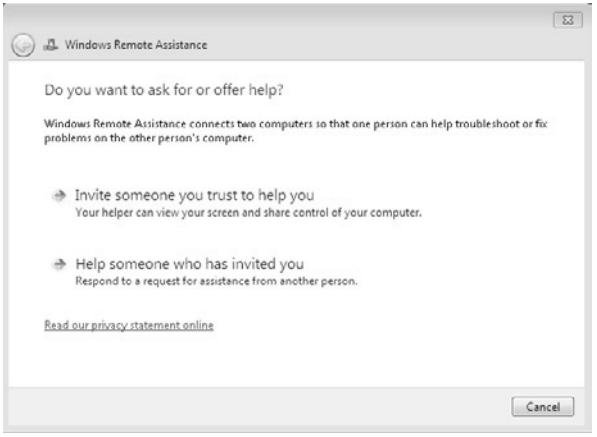
> **Note**
>
> **The PC offering the remote assistance does not need to be running Windows 7. It could be running an older version of Windows that supports this feature.**

www.it-ebooks.info

1. Access Remote Assistance by typing **remote assistance** in the Start menu search box and selecting Windows Remote Assistance from the results that appear (the easiest method) or by pressing F1 on your keyboard to open Windows Help, clicking More Support Options in the bottom-left corner of the window, and then clicking Windows Remote Assistance when the options change.



2. When Windows Remote Assistance opens, you can select either Invite Someone You Trust To Help You or Help Someone Who Has Invited You. Click the second option to help someone if you received an invitation through Easy Connect.



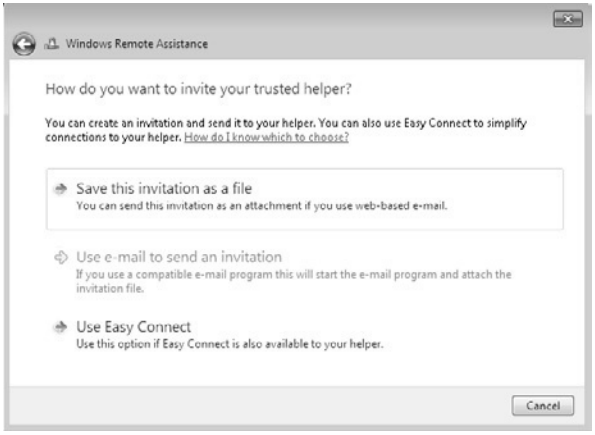
www.it-ebooks.info

INSIDE OUT Remote assistance using Easy Connect

Easy Connect allows two computers running Windows 7 to connect using Remote Assistance without the need to send an invitation file. This may not always be available depending on whether your router supports the Peer Name Resolution Protocol.

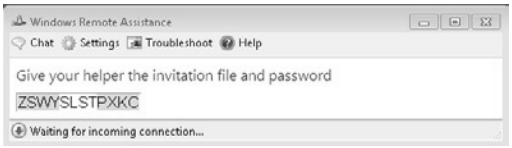
Easy Connect is a very useful and easy way to connect two computers for remote assistance and is worth trying to see if you can get it to work. It uses a secure peer-to-peer network managed by Microsoft to handle the connection.

3. If you are requesting assistance, you will need to indicate how to send a remote assistance invitation. This will commonly be sent via email. If you have an email program installed on your PC, such as Windows Live Mail or Microsoft Office Outlook, click Use E-Mail To Send An Invitation. Otherwise, click Save This Invitation As A File, and then send it via webmail. Alternatively, you can click Use Easy Connect. See the previous Inside Out sidebar entitled, "Remote Assistance Using Easy Connect."

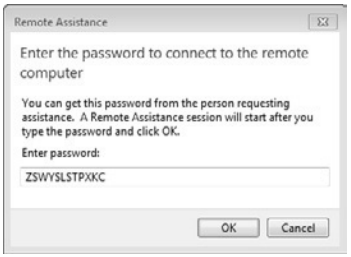


4. You will now be given a password. If you are using Easy Connect, tell or send the password to the person providing the support. Otherwise, email the invitation file that's been saved to your PC.

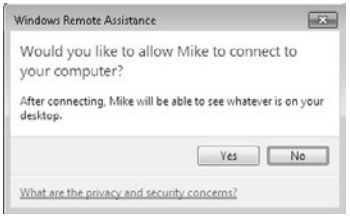
www.it-ebooks.info



5. If you are the person providing the support, either enter the password in the dialog box that appears on your screen, or open the invitation file you received.

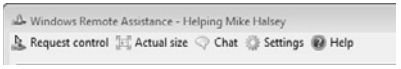


6. If you are the person receiving the support, allow the person providing support access to your computer by clicking Yes in the dialog box that appears.



At this point, the person providing the support can look at what's happening on the other PC but cannot control it by default. This can be a useful security feature and handy when you just want to show someone what's happening on your computer.

7. If you are providing support, in the Remote Assistance console, click Request Control.



If you are receiving support, do not be too alarmed about someone taking control of your computer because you will be able to see at every stage what is going on.

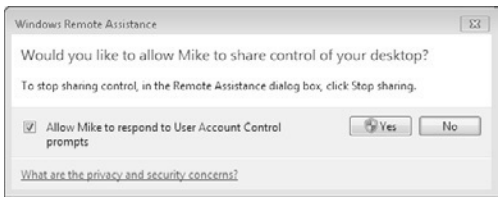
www.it-ebooks.info

Note

In the Remote Assistance settings, you can also set the software to break the connection instantly when you press Escape on your keyboard.



8. When someone requests control of a remote computer, a dialog box appears asking if this is allowable. If you allow the access, you should also select the check box allowing the help provider to respond to User Account Control security prompts. This will mean that the person supplying remote support will have full control of your PC to repair it. If you do not select this option, you will have to respond to the UAC prompts yourself. This is a more secure approach and can be used if you do not completely trust the person providing the support, but it can also slow the process, and you will have to remain at your PC throughout the entire session.



Problem Steps Recorder

The **Problem Steps Recorder** feature was introduced in the Windows 7 beta to enable technical beta testers to more effectively report problems to the operating system development team at Microsoft. It was so well received that Microsoft kept it in the final release of the operating system. This is a hidden feature only available by typing **problem steps** in the Start menu search box.

www.it-ebooks.info

This tool records actions on your screen at key points (such as when you click something or an error appears), saving each event as a screenshot. You can click Add Comment on the Problem Steps Recorder to annotate the screenshots and give more information (see Figure 17-10).



Figure 17-10 Problem Steps Recorder

When you stop the recording, Problem Steps Recorder saves all of the information it captured, complete with additional details about your computer and what software was running at the time, as a zip file that can be sent via email to a support person. This zip file contains a document viewable in any web browser (see Figures 17-11 through 17-13).

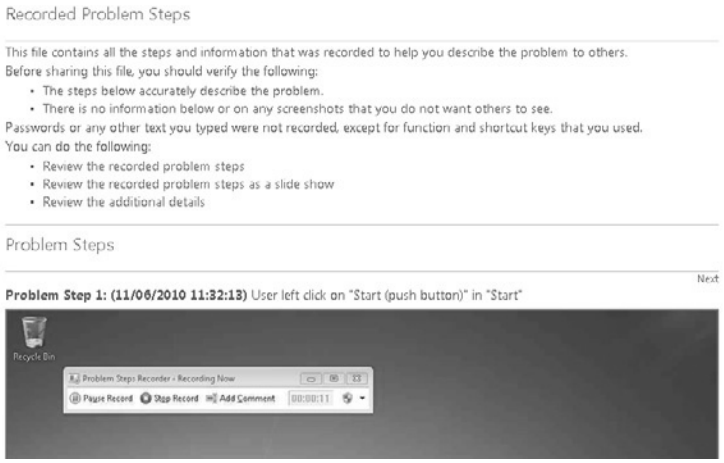


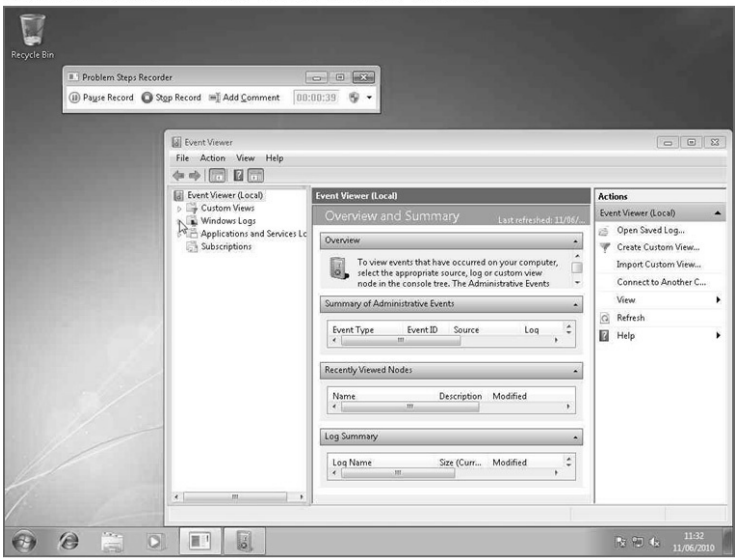
Figure 17-11 The Problem Steps Recorder information file (1 of 3)

As shown in Figure 17-12, Problem Steps Recorder annotates all the screenshots to show what you were clicking when an event occurred. This can be an excellent way to get support for a computer, because it provides a great amount of detail about the state of your PC at the time of an error and simplifies what could be a complicated description by using screenshots.

www.it-ebooks.info

Previous

Problem Step 3: (11/06/2010 11:32:41) User mouse drag start in "Event Viewer"



Return to top of page...

Figure 17-12 The Problem Steps Recorder information file (2 of 3)

Additional Details

The following section contains the additional details that were recorded that can help find a solution for your problem.
These details help accurately identify the programs and UI you used while recording the problem steps.
This section may contain text that is internal to programs that only very advanced users or programmers may understand.
Please review these details to ensure that they do not contain any information that you would not like others to see.

```
Recording Session: 11/06/2010 11:32:01 - 11:33:05

Problem Steps: 3, Missed Steps: 0, Other Errors: 0

Operating System: 7600.16385.x86fre.win7_rtm.090713-1255 6.1.0.0.2.48

Problem Step 1: User left click on "Start (push button)" in "Start"
Program: Windows Explorer, 6.1.7600.16385 (win7_rtm.090713-1255), Microsoft Corporation, EXPL
UI Elements: Start, Start, Button

Problem Step 2: User keyboard input in "Start menu" [... ENTER]
Program: Windows Explorer, 6.1.7600.16385 (win7_rtm.090713-1255), Microsoft Corporation, EXPL
UI Elements: DirectUIHWND, SearchEditBoxWrapperClass, Search Box, Desktop OpenBox Host, Start

Problem Step 3: User mouse drag start in "Event Viewer"
Program:
UI Elements: SysTreeView32, MMCViewWindow, Event Viewer (Local), MMCChildFrm, MDIClient, Ever
```

Figure 17-13 The Problem Steps Recorder information file (3 of 3)

www.it-ebooks.info

Summary

When Remote Help was first introduced with Windows XP, the weak point of this extremely useful system was the fact that broadband Internet connections were typically very slow and unreliable and most people still used dial-up Internet connections. Now, that problem has gone away.

Remote Help has also come a very long way since it first appeared in Windows. If you are receiving remote support, you can now use this feature safe in the knowledge that it is secure, and, if you are still concerned about safety, you can use Remote Assistance, enabling you to terminate a session at any time.

For professionals providing assistance, the new remote help systems in Windows 7 are considerably faster than before and are a reliable alternative to third-party solutions, such as VNC, which people receiving support may not know how to install and configure.

www.it-ebooks.info

CHAPTER 18

Where to Find More Help and Support

Windows Help 289
Third-Party Software 289
Third-Party Websites 292
Summary 294

Microsoft Windows is used by so many people around the world that an enormous ecosystem has built up around it over the years to provide help and support. There's help everywhere and not just on the Microsoft websites I mentioned in Chapter 17, "Remote Help."

Windows Help

You can access Windows Help at any time by pressing F1 on your keyboard or by selecting Help And Support on the Start menu. You might be wondering why I haven't mentioned Windows Help before Chapter 18. The reason is that the help system in Windows is more of a basic manual than anything else. It can be helpful for guiding you through unfamiliar features, but it is not exhaustive. There are other resources you can use for assistance, and I will cover them in this chapter.

Third-Party Software

You can download many different utilities, some for free and others for a fee, that will help solve problems on your PC. Some of these are more helpful than others. You should decide for yourself about the value of individual software packages, but I recommend the following packages.

Sisoftware Sandra Utilities

www.sisoftware.net

Sisoftware Sandra is an excellent information and diagnostic utility. This package's extremely detailed reports about every aspect of your PC, including hardware, drivers, and installed software, can help enormously when diagnosing computer-related problems.

Create Report on the Tools tab in Sandra utilities is a useful tool that generates a complete report about your computer (see Figure 18-1). This tool does everything the Windows 7 System Information panel and System Health Report do, but it provides even more detail about your PC.

www.it-ebooks.info

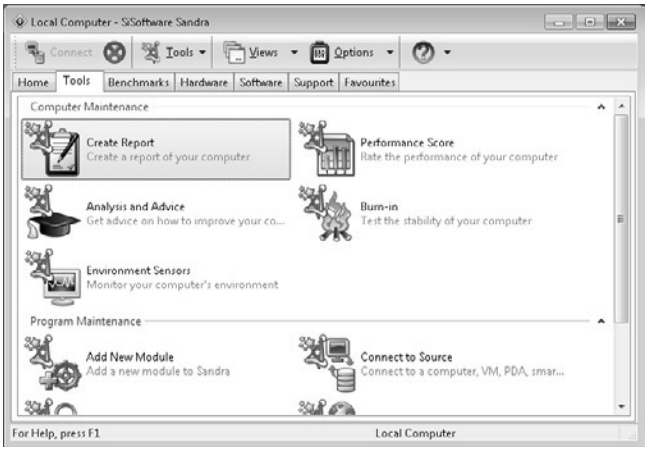


Figure 18-1 Sisoftware Sandra utilities

Windows Sysinternals

www.sysinternals.com

Windows Sysinternals is a suite of tools and applications from Microsoft that help you manage, troubleshoot, and diagnose your Windows systems and applications. These extensive tools provide huge amounts of detail about your PC when troubleshooting problems. However, some of these tools are quite complex and are designed for experienced computer users.

Zinstall zPOD

www.zinstall.com

Zinstall zPOD is an excellent software package that enables you to turn your copy of Windows and all of your software into a virtual machine that can be stored on a removable hard disk or even a USB pen drive. You can then use this virtual machine on any PC. This means you can always have your copy of Windows and your programs (perhaps even your files) with you whenever you need them.

GoToAssist

www.gotoassist.com

GoToAssist is software that performs the same functions as Windows Remote Desktop and Windows Remote Assistance but offers a few additional functions for serious technical support. Most notably, it allows you to restart the remote computer (which can be essential when performing some support functions), and it runs on and from Apple Mac computers.

www.it-ebooks.info

SpinRite

www.grc.com

Another software package held in extremely high regard by many computer professionals is SpinRite from computer security specialist Steve Gibson. This utility runs from a disk or USB flash drive and checks your hard disk for errors, physical or otherwise, that are causing malfunctions and/or data loss, then helps repair problems. I will describe SpinRite in more detail in Chapter 23, "Third-Party Rescue Tools and Services." It is an extremely useful piece of software.

Windows Memory Diagnostic

oca.microsoft.com/en/windiag.asp

The Windows 7 installation DVD contains a memory diagnostic tool (see Chapter 15, "Advanced Repair Methods"), but Microsoft also provides this other memory diagnostic tool if your Windows 7 install DVD is lost or damaged and you can't boot into the computer repair console in Windows 7.

Norton Ghost

www.symantec.com/ghost

Norton Ghost from Symantec is one of two packages on this list that create system images of Windows. Although this functionality is already built into Windows 7, these packages offer additional backup and restore functionality for people who work in a corporate environment.

Acronis True Image

www.acronis.com

Acronis True Image is another system image backup and restore application. This package is useful in business scenarios where you need more control over Windows 7 system images than is available through the Microsoft Windows Image Backup that ships as part of Windows 7.

Paragon Partition Manager

www.paragon-software.com

Sometimes you need a utility to manage the partitions on your hard disks. Windows 7 includes a partitioning tool, but it's not especially powerful. Paragon Partition Manager can make working with partitions much simpler.

www.it-ebooks.info

Acronis Disk Director Suite

www.acronis.com

Acronis Disk Director is another partitioning management package that will make working with and managing partitions on your hard disks much simpler.

Third-Party Websites

There are hundreds of PC help websites, some of which require a subscription (although I wouldn't recommend these). You should decide for yourself about the value of specific websites, but I recommend the following sites.

Tom's Hardware

www.tomshardware.com

Tom's Hardware is a long-standing website devoted to hardware and hardware problems. This site includes extensive forums containing a huge wealth of information, and experts are always available to help diagnose and fix difficult problems.

Tech PC Forums

www.tech-pc.com

Tech PC Forums is a forum website that contains a wealth of valuable information. Experts are available to answer your questions and help solve your computer-related problems.

Computing.net

www.computing.net

Run by the people behind Tom's Hardware, Computing.net is an excellent resource for help with complex and difficult PC problems.

How-To Geek

www.howtogeek.com

How-To Geek helps you perform a wide variety of tasks in Windows 7 and other operating systems and software packages. Many tasks help resolve PC issues and problems.

www.it-ebooks.info

Annoyances.org

www.annoyances.org

This is the accompanying website to the book *Windows 7 Annoyances: Tips, Secrets, and Solutions* by David A. Karp (O'Reilly Media, 2010). It's an excellent archive of problems that you can search through to find solutions to common Windows 7 problems.

Gibson Research

www.grc.com

Steve Gibson is a well-respected IT security expert. On the Gibson Research website, he provides many tools to help diagnose and repair security flaws in your installation of Windows.

ATI Support

support.amd.com

Graphics card problems are common with Windows. Fortunately, there are only two major manufacturers providing the core hardware for graphics card technology, so help is centralized. You can find support for an ATI-based graphics card at the ATI support website.

nVidia Support

www.nvidia.com/page/support.html

Similar to the ATI support page, the nVidia support website is the place to visit if you have an nVidia-based graphics card in your PC.

MSDN Diagnostics

msdn.microsoft.com/en-us/library/ee663269(v=VS.85).aspx

The Microsoft MSDN site offers an extensive section for diagnosing and troubleshooting Windows 7. This includes the Windows Troubleshooting Platform (WTP) that enables system administrators to write custom troubleshooting packs.

Within Windows

www.withinwindows.com

Software author Rafael Rivera has years of experience delving deep into Windows, producing fixes to undocumented features and providing software to enhance the functionality of Microsoft products.

www.it-ebooks.info

The Long Climb

www.thelongclimb.com

The Long Climb is my own website. I offer PC support and updates on security and other issues with PCs and Windows. I will also offer specific help and advice, adding to the content of this book during the lifetime of Windows 7. I can also be contacted through this website with any questions you may have.

Summary

There are a huge number of places online where you can get help and support, usually for free. It's worth asking friends and colleagues where they find help, and I'd also recommend avoiding websites that charge for it (one notable exception being subscriptions to the Microsoft TechNet and MSDN sites).

The sites and software I've mentioned here are extremely comprehensive and trustworthy. You will probably find most of the answers you need on these sites.

www.it-ebooks.info

CHAPTER 19

Diagnosing Hardware Problems

PC Hardware Guide 295
Safe Working. 304
Is Everything Plugged In? 305
Minimal Hardware Boot 306
Resetting the BIOS 307
Jump-Starting Your PC 309
Summary 310

A problem with Windows 7 could be caused by hardware, either inside the PC case, or plugged into the computer externally. In this chapter, I'll talk you through how to diagnose hardware problems and work safely with your PC.

PC Hardware Guide

A PC is a collection of assorted parts, each with its own foibles and individual characteristics. Each of these parts works together in an interdependent way.

Desktop PC Case

The base unit on a PC is the main case that contains all of the parts that make a computer work. In a laptop, notebook, or even an all-in-one desktop, all of these parts are inside the same case as the monitor since there's only a single unit. With a standard desktop PC, however, the base unit is the large case that probably sits on your desk or, more commonly, on the floor. Figure 19-1 shows all of the relevant parts of the PC on the front and back of the desktop case.

Power Supply

The power supply is probably the part of the computer most prone to failure. As shown in Figure 19-1, the power supply is where you plug your computer into the main electrical supply. It regulates and distributes the power going into the computer and extra components, and it is one of only a few components within the PC to have a fan to keep it cool. Fortunately, the power supply is very simple to replace if it does fail.

www.it-ebooks.info



Figure 19-1 A typical desktop PC case

Motherboard

The motherboard is the substrate of the PC. This is the board to which all other components are plugged in or attached (see Figure 19-2).

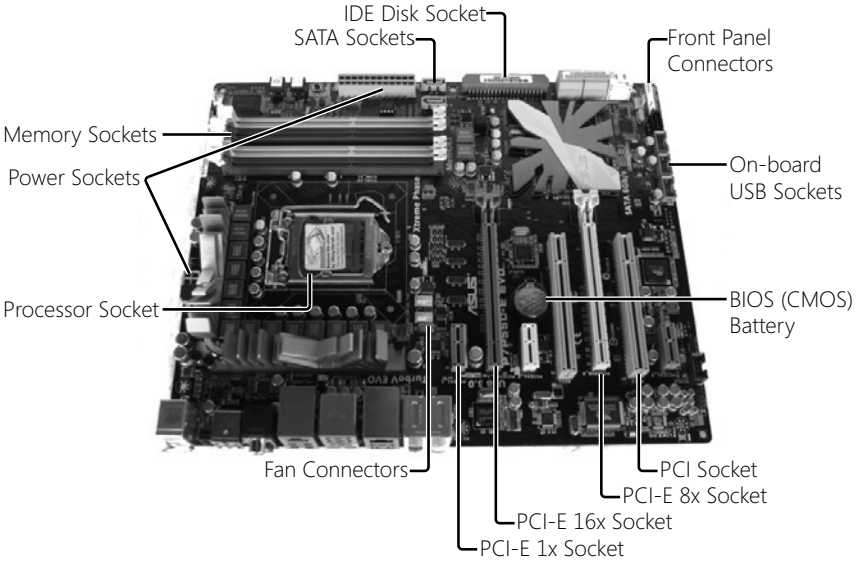


Figure 19-2 A typical PC motherboard

www.it-ebooks.info

As you might expect, the motherboard is the component located at the very bottom of your PC and is the most difficult to remove if something goes wrong with it.

The back-panel connectors on the motherboard shown in Figures 19-1 through 19-3 are where you plug in additional accessories such as your keyboard and mouse, speakers, and any USB accessories.

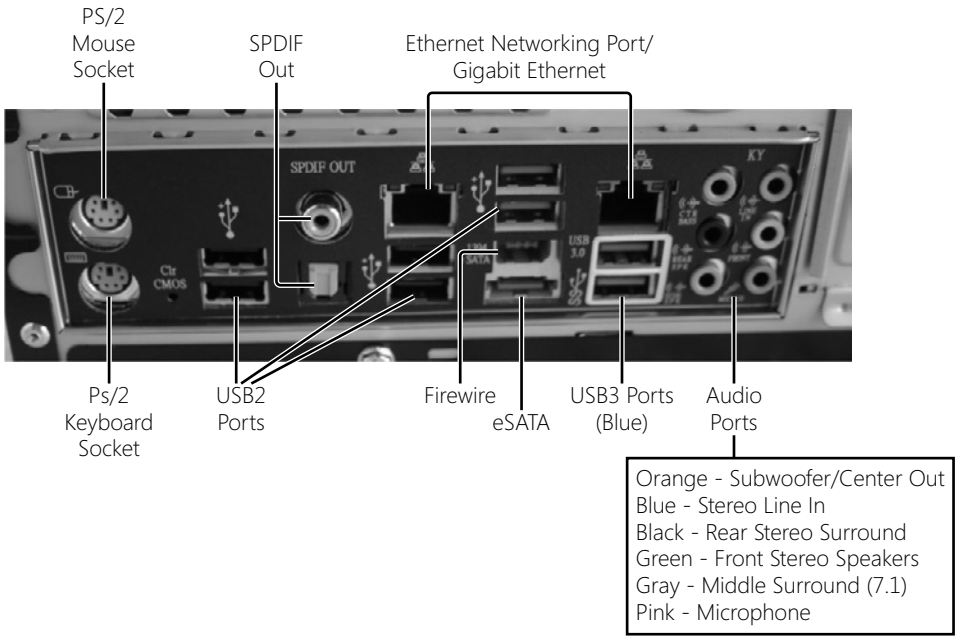


Figure 19-3 The back-panel connectors on a motherboard

Processor

The processor is the brain of the computer, the chip that does all the computational work (see Figure 19-4). The processor is quite fragile and needs to be handled with care.

The processor fits into a socket on the motherboard and requires a heat sink and, normally, a fan to keep it cool. When installing a processor, make sure that there's plenty of silicon paste between it and the heat sink to prevent overheating and cracking.

www.it-ebooks.info

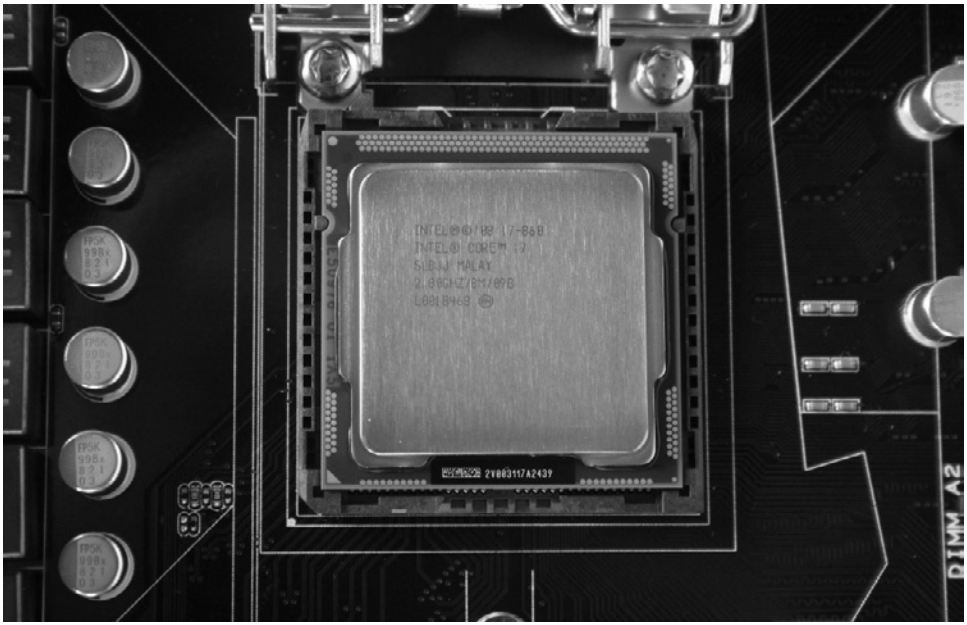


Figure 19-4 A typical PC processor

Memory

Memory in your PC (not to be confused with memory on the hard disk) is where Windows loads files while it works with them. It's a temporary store, and files are wiped from memory when the PC is turned off. Figure 19-5 shows an example of physical memory.

Hard Disk

The hard disk(s) in your PC are the physical storage where Windows 7 and your files reside. Different types of hard disks have different connectors. Figure 19-6 shows a small, 2.5-inch hard disk (which is the smaller of the three on the left side of the image) and two standard 3.25-inch hard disks. All three have SATA (Serial ATA) connectors. Older IDE (Integrated Drive Electronics) drives have a long connector with many pins for data and a smaller connector with large pins for power.

www.it-ebooks.info



Figure 19-5 PC Memory

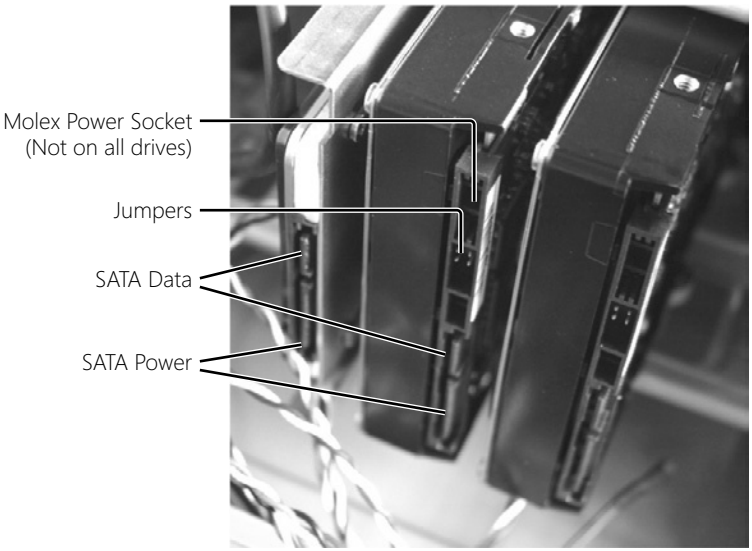


Figure 19-6 Hard disk and optical drive connectors

www.it-ebooks.info

Optical Drive

The optical drive is the CD/DVD or Blu-Ray drive on your computer. An optical drive connects to the motherboard with either the SATA or IDE connectors, as I described for hard disks.

Graphics Card

Your PC probably does not include a separate graphics card if the graphics technology is built into the motherboard or, as is the case with the newest processors, built into the processor itself. If you do have a separate graphics card, it might look similar to the one shown in Figure 19-7.



Figure 19-7 A graphics card

This component connects to the monitor and manages what is displayed on the computer screen.

www.it-ebooks.info

Expansion Card(s)

Expansion cards plug into your PC like graphics cards but likely use a different socket (see Figure 19-2). Expansion cards can do anything from connecting to the Internet, to providing more USB ports, to acting as a television tuner.

CAUTION!

Always make sure your PC is disconnected from the electrical outlet before you work inside the case. This will avoid causing electrical damage to the components, many of which are fragile.

Fans

Your PC has several fans to keep it cool: one or more in the power supply, one on the processor, one on the graphics card, perhaps one on the motherboard, and one or more in the case. Fans are important for keeping the computer cool since some components can heat up to temperatures near 100 degrees Celsius. It's a good idea to make sure these fans are clean and operational. If they are rattling, they might need to be replaced.

Keyboards and Mice

Keyboards and mice don't normally malfunction, but the keyboard will occasionally need to be cleaned, especially if you eat or drink around your computer. I don't recommend washing a keyboard, however. Normally, light vacuuming (on a low setting) and a wipe will do the job.

If you have a ball-mouse, the rollers the ball runs up against can become clogged with dust and debris from your desk. You can remove the ball by removing a small panel on the underside of the mouse and clean the rollers inside.

Laptops, Netbooks, and All-in-One PCs

In a laptop, netbook, or all-in-one PC, things are slightly different from a standard PC in that all of the components and hardware are built into a single case with removable panels on the underside of the computer (see Figure 19-8).

www.it-ebooks.info



Figure 19-8 The underside of a typical laptop computer

Although there are not many user-serviceable components inside a laptop, they can usually be detached simply by removing a few screws. In Figures 19-9 through 19-11 you can see how the optical drive, hard disk, and memory can be replaced quite easily in a laptop after unscrewing the removable panels on the underside of the case.



Figure 19-9 Removing the optical drive from a laptop computer

www.it-ebooks.info



Figure 19-10 Removing the hard disk from a laptop computer

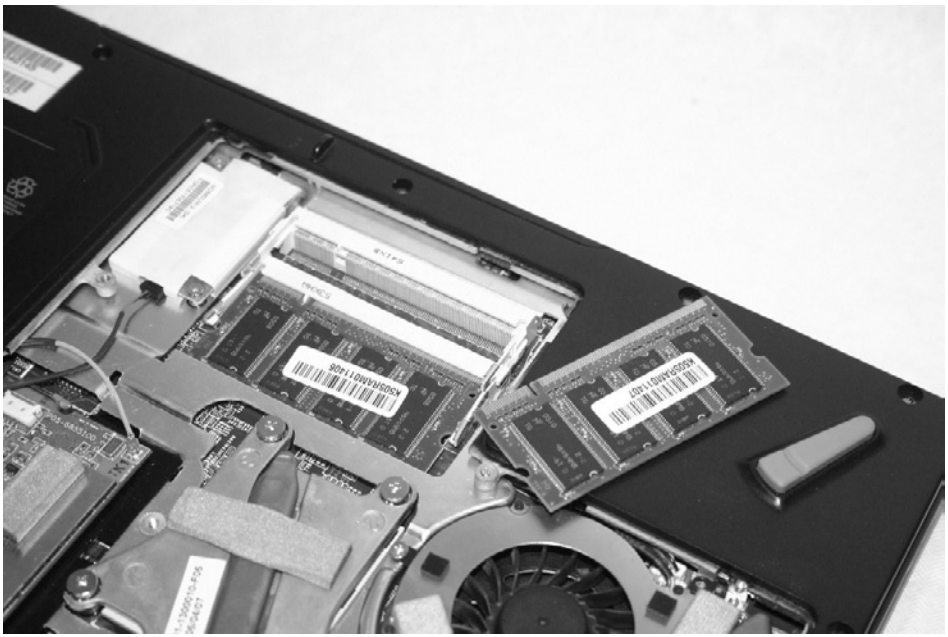


Figure 19-11 Changing the memory cards in a laptop computer

www.it-ebooks.info

CAUTION!

Always make sure that the laptop is not plugged into an electrical outlet and that you have removed the battery before opening the case. This will avoid causing electrical damage to any components.

Safe Working

Many of the components on a motherboard, processor, or memory can be measured in nanometers; they're absolutely tiny and quite susceptible to even tiny voltages of human static electricity. To work safely with a PC, follow these guidelines.

1. Make certain that the computer is turned off but still plugged in to an electrical outlet.
2. If the computer is a laptop or netbook, remove the battery.
3. Make sure you are wearing an anti-static wristband. Remove the side or back panel, and attach the clip on the wristband to the metal frame of the case. This can be difficult with a laptop, but do not clip the wristband to any components.



4. For a desktop PC, touch the power supply inside the case.
5. While still touching the case, pull the power lead out of the back.

You can now work safely with your PC.

www.it-ebooks.info

INSIDE OUT Other things to be careful of when working with a PC

Try to avoid working on a PC in a room with thick or nylon carpet, because these materials can cause buildups of static electricity. Also, always place the PC on a flat and stable surface.

Is Everything Plugged In?

It's not uncommon for a connector in a PC to come loose. If you find, for instance, that the power button has stopped working, check to see if the front panel connectors have come off their mountings. In the bottom right of Figure 19-12, you can see the front panel connectors and connecting wires. Next to the front panel connectors are other connectors for USB and SATA devices. If you are experiencing issues, you can check this area to ensure that all of the cables are properly and securely plugged in.



Figure 19-12 The front panel connectors, seen in the bottom right of the image

www.it-ebooks.info

Minimal Hardware Boot

There are so many components inside a PC that it can sometimes be difficult to determine which one is causing a problem. If your PC won't start or is crashing regularly, the problem could be a hardware fault.

The best way to determine if you have a hardware fault is to perform a minimal hardware boot. To do this, first remove all external devices from your PC except for the mouse and keyboard. This includes USB-attached devices.

If your PC is still malfunctioning after you disconnect all of the external hardware, then open the case and remove the following components.

- The optical drive
- Any hard disks except the one on which Windows 7 is installed
- All but one of the memory cards
- Any expansion cards except the graphics card (if present)

Removing these components enables your PC to start with the minimum number of hardware components. If the computer is still malfunctioning, you can conclude that no external devices are causing the problem. However, if the PC works properly, you can begin adding the components back one at a time, restarting and testing the PC every time you reattach a component. This process of elimination can help you diagnose what hardware component is at fault.

If you perform a minimal boot and the computer still doesn't work, your task is harder because you cannot remove anything else except the graphics card, and that only if your motherboard has on-board graphics. In this case, the first thing to do is try each memory card in turn, turning off the computer to change the card and restarting it each time to see if the computer works. This will establish whether you have a faulty memory card.

> **Note**
>
> **Sometimes changing graphics cards can result in a blank display if the currently set resolution is higher than your screen can support. When you are changing a graphics card or removing one for testing purposes to use the motherboard graphics chip instead, it's a good idea to first lower your screen resolution to 800 x 600 or 1024 x 768. You can do this by right-clicking on any blank area of the Windows 7 desktop and selecting Screen Resolution from the options that appear.**

www.it-ebooks.info

If the problem persists, then it can only be caused by one of four components: the power supply, the primary hard disk, the motherboard, or the processor. I'll cover how to jump-start your PC in the next section, which can help determine if you have a faulty power supply, but how do you check the other components?

You can check the hard disk by plugging it into another computer as an extra drive and seeing if any problems are transferred with it. Don't try to use it as the boot drive on this second PC, because the installed copy of Windows 7 won't have compatible hardware for the new computer and Windows will fail to start.

If you determine that the hard disk is not the problem, then the processor or the motherboard might be the culprit. Because you can't start the PC without either of these, you might consider consulting a technical professional. But before you do so, there are some other things you can try first.

Resetting the BIOS

Sometimes the computer's BIOS (Basic Input Output System) can become corrupt. This can cause Windows to fail to boot or malfunction when the operating system cannot properly communicate with your hardware. On these occasions, you can reset the BIOS to its default configuration.

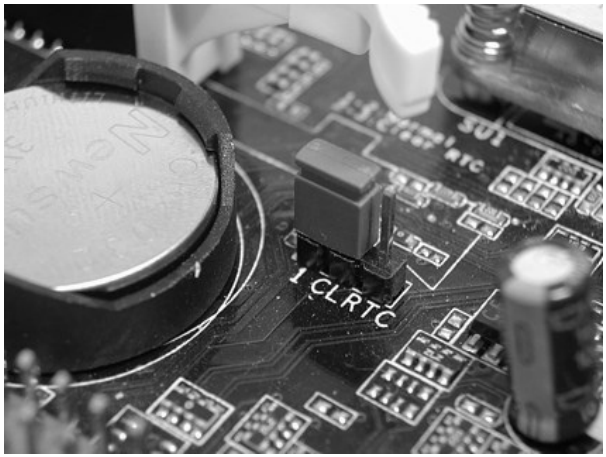
The first and easiest way to reset the computer's BIOS is to access the BIOS by pressing Delete or F2 on your keyboard at startup and then restore the default BIOS settings.

Your motherboard, which houses your BIOS chip, has a CMOS battery and a BIOS/CMOS reset button or jumper. You can remove the battery for between 20 seconds and two minutes to reset the CMOS.

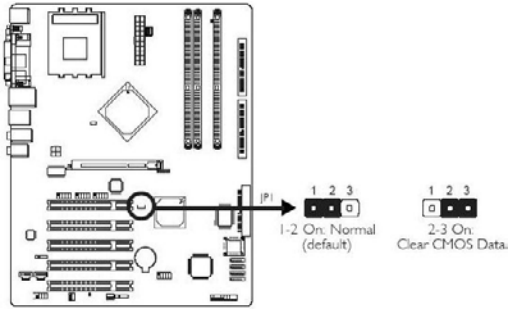
1. Place the PC on a level, firm surface, and make sure it is turned off and disconnected from the electrical outlet. Ground yourself by touching an unpainted area on the PC case, using an anti-static wristband if possible, and open the side of the PC to expose the motherboard.

2. Locate the battery on the motherboard. It looks like (and, indeed, is) a large watch battery. Unclip the battery to remove it from the motherboard.

www.it-ebooks.info



3. There is a Clear CMOS jumper on the motherboard, close to the battery; check the motherboard manual for the exact location. The jumper is three pins with a small connector covering two of them (shown in the image following step 2). Remove the connector, and move it to cover the center pin and the uncovered pin. A small pair of tweezers is useful for doing this.



4. Leave the jumper as described in step 3 for 10 seconds, and then move it back to its original position.

5. Replace the motherboard battery.

6. Reassemble the PC case, and reconnect it to the main power supply.

On some motherboards, instead of a CMOS jumper, there is a small reset button on the back of the panel (see Figure 19-13).

www.it-ebooks.info



Figure 19-13 Some PCs include a Clear CMOS button.

This button, which you can normally press with a paper clip, can make it easier to reset the BIOS.

INSIDE OUT Updating the BIOS firmware

If you find that you can't use new hardware with your PC, you might need to update your computer's BIOS to a newer version. To do this, check your motherboard manual or the support section of the manufacturer's website.

Jump-Starting Your PC

If you suspect that the power supply has failed on your desktop PC, you can try to jump-start it if you have another computer available. To do this, remove the two power connectors from the motherboard in both PCs. Place the computers side by side, and plug the power connectors from the working power supply into the motherboard in the nonworking PC. (If the cables aren't long enough. simply unscrew the working power supply, supporting it carefully, and hold it closer to the other PC.)

Next, try to start the nonworking PC. If lights and fans activate on the motherboard, it is drawing power perfectly well, and you can be certain that the power supply in your PC is not working.

www.it-ebooks.info

Summary

The methods detailed here should help you diagnose the vast majority of computer hardware problems. If you need to do anything beyond the diagnostics in this chapter, such as check voltages, you will need a multi-meter, and, to be honest, it's worth surrendering the PC to a specialist hardware engineer.

www.it-ebooks.info

PART 4

Disaster Recovery

CHAPTER20
Windows and Data Recovery Tools. 313

CHAPTER 21
Restoring from Another PC 319

CHAPTER 22
Linux: An Operating System on a Disc 325

CHAPTER 23
Third-Party Rescue Tools and Services 337

CHAPTER 24
When You Can't Recover Data. 347

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 20

Windows and Data Recovery Tools

You Did Back It Up, Didn't You?! 313
Restoring Windows and Data from a Backup 313
Data Restore Through Over-the-Top Reinstall 315
RAID Drives 318
Summary 318

I've talked several times so far in this book about the importance of making sure all your data and files, and Windows 7 itself, are backed up. Sometimes, though, a recent backup will not be available or your backup media—especially if you back files up to CD or DVD—could itself be corrupt. It can still be possible to reover your files and data, and this chapter will show you how.

You Did Back It Up, Didn't You?!

At some point, something bad will happen with your computer, and you won't be able to access your copy of Windows or your files and data. What's more, this kind of disaster always seems to happen at the worst time, when you're up against a deadline or planning a vacation, for instance.

The easiest and quickest way to get back up and running can be to restore your operating system or files from a backup. Although restoring from a backup can be much faster than diagnosing and fixing the actual problem, you should be wary about restoring your files from a backup too hastily if the backup isn't recent and the originals might still be saved.

If, however, Windows 7 won't start at all and can't be repaired using the conventional tools, you should be prepared to rely on your most recent files and data backups (unless you keep your files and data on a separate hard disk or partition from your copy of Windows).

Even now, though, you might be surprised at just how much you can do to rescue your system and get it working again.

Restoring Windows and Data from a Backup

The first thing to do when your system crashes is to restore Windows. You may have created a system image using the Windows 7 built-in feature Complete PC Backup, or you may have used a third-party solution such as Norton Ghost or Acronis True Image. Any of these back-ups will do.

www.it-ebooks.info

To restore an image created using the built-in Windows 7 backup tool, you will need the Windows 7 system repair disc or the original installation DVD for your operating system.

When restoring from the Windows 7 installation DVD, skip the language selection, and then select Repair Your Computer from the install screen, as shown in Figure 20-1.



Figure 20-1 Restoring Windows 7 from your installation DVD

Startup Repair will first try to repair your Windows installation, but when offered the choice, you should choose to restore your copy of Windows from an image backup, as shown in Figure 20-2.



Figure 20-2 Restoring Windows 7 from an image backup

INSIDE OUT Storing your backups on the same hard disk as Windows

Windows System Image Backup will warn you if you try to store a Windows system image on the same physical hard disk as your copy of Windows (although, on a laptop, this could be unavoidable).

The problem is that if the disk becomes damaged or malfunctions, you could lose your image backup. If you do not have another hard disk in your computer, back up your copy of Windows 7 to a USB-attached external hard disk instead.

www.it-ebooks.info

It doesn't normally take long for Windows 7 to be restored from a backup, after which you can use whatever backup software you have used to make backup copies of your files and data to restore them, too.

In Figure 20-3, you can see the Windows 7 standard backup software quickly finds the location of your backups for restoration.

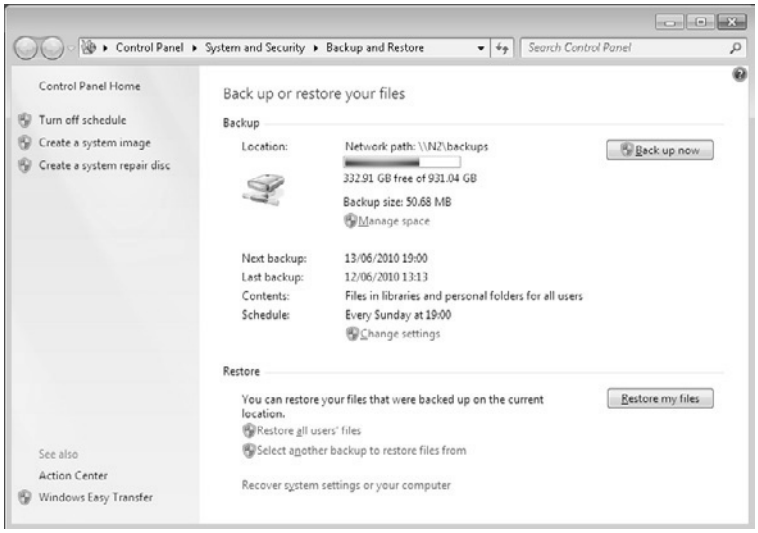


Figure 20-3 Restoring files from a backup using Windows 7 Backup and Restore

INSIDE OUT

Always have at least two backup copies of files

If your only backup copy of your files is on a hard disk inside your PC, there's a chance that it will be lost if disaster strikes. You should always keep at least two copies of backups. Preferably, you should have an extra copy in your home or office for quick restore, perhaps on a network attached storage (NAS) drive or external hard disk, and another copy off-site.

Data Restore Through Over-the-Top Reinstall

Even if all of your files and data are on the same partition as Windows 7 and you must reinstall the operating system, you can still save the files from deletion.

www.it-ebooks.info

To do this, boot your PC from the Windows 7 installation DVD, select your language, and then click Install Now. After this, you will be asked if you want to upgrade Windows 7 or perform a clean install, as shown in Figure 20-4.



Figure 20-4 Upgrading Windows 7 over a previous installation

Oddly, at this point you should select Custom (Advanced), because the upgrade option will work only if you are running the installer from within a working copy of Windows 7 or Windows Vista (see Figure 20-5).

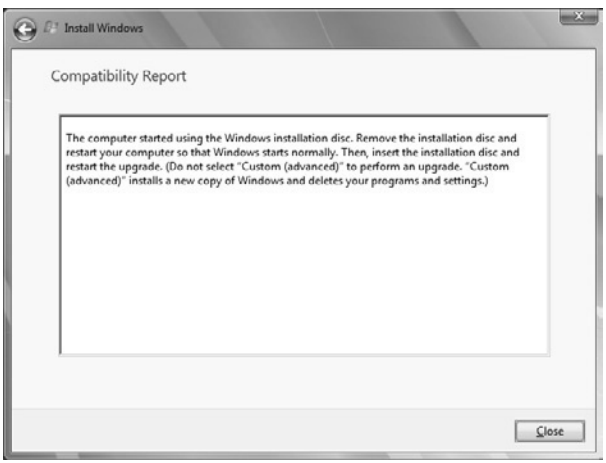


Figure 20-5 You can't upgrade Windows 7 by selecting the upgrade option if you have booted from the installation DVD.

www.it-ebooks.info

When you perform a custom install, select the hard disk or partition on which Windows 7 is installed, but *do not* format the drive. You will then be presented with a message saying that another Windows installation has been found and that it will be archived in a folder called Windows.old, as shown in Figure 20-6.



Figure 20-6 Installing Windows 7 over the top of a previous installation

After you have reinstalled Windows, you will find that all your previous files and data are safe, although you will need to reinstall all of your programs and readjust your settings. Your files are in the Users folder under Windows.old, as shown in Figure 20-7. You should back up these files to a secure location, such as an external hard disk.

INSIDE OUT Do you have enough disk space?

If you are short on disk space in the partition where you are reinstalling Windows 7, it may fail to install. This is because Windows 7 keeps all of the files for the previous version of Windows 7 in a folder called Windows.old. If you cannot install over the top, you may need to try to rescue Windows using another method. Chapter 21, "Restoring from Another PC," through Chapter 23, "Third-Party Rescue Tools and Services," describe ways that you can do this.

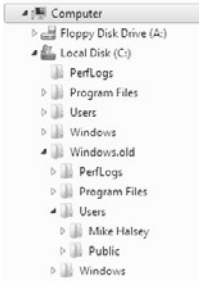


Figure 20-7 Your files are saved inside the Windows.old folder.

www.it-ebooks.info

RAID Drives

Sometimes hard disks are connected using a system called Redundant Array of Independent Disks, or **RAID**. This system can automatically create backups of files or data that can be used in the event that one of the disks fails, or it can span your files across several disks, essentially creating more space.

CAUTION!

RAID is most useful for recovering data when a hard disk fails. If that data is deleted or moved from one drive, however, this action will be copied on the other, and the data will be lost there, too.

Sometimes, one drive fails to appear at startup, and you can't access your files and data. This is not necessarily a crisis, however.

In this situation, turn off your PC, and unplug it from the electrical outlet. Remove the side panel on the PC, and carefully remove and reseat all the data and power cables to the hard disks that are part of the RAID array. This will also involve reseating the cables in their sockets on the motherboard or RAID card. You should be careful to keep plugs in their current sockets.

After doing this, a RAID array will often spring back into life. If you still encounter problems, you should attempt a repair in the diagnostic console for your RAID hardware. Consult your RAID card or motherboard manual for details on how to access the diagnostic panel and perform a repair, since the procedure will vary from one computer to the next.

Summary

The most important thing to remember is to always keep an up-to-date backup of your files and data so that they at least are safe in the event of a disaster. Although I have detailed several methods here for recovering data and files, the success of these recovery attempts depends entirely on individual circumstances. For example, if the partition or partition table on your hard disk is corrupt, you may not be able to perform an over-the-top reinstall.

Always back up your data on a regular schedule, and keep the data somewhere safe, separate from your PC.

www.it-ebooks.info

CHAPTER 21

Restoring from Another PC

Restoring a Windows Image on Another PC 319
Restoring Windows File by File 320
Restoring Your Data by Using Another PC 321
Summary 324

If your own PC is out of commission, you may still need to access files and programs stored on it. You can do this by unplugging the physical hard disk from your PC and connecting it to another computer. You can connect the hard disk to another computer by either plugging it in inside the new host computer as the main or secondary hard disk or by putting it in a USB hard disk caddy.

Restoring a Windows Image on Another PC

If you need to restore an image of Windows 7 from a backup, you can plug the disk(s) containing the corrupt Windows 7 installation and the Complete PC Backup system image into a working PC. You should probably unplug the host computer's hard disk(s) at this point to prevent accidental damage to or deletion of its files.

Next, boot from the Windows 7 installation DVD, and instead of clicking Install Now, click Repair Your Computer (see Figure 21-1).



Figure 21-1 Restoring a system image from the installation DVD

Click through startup repair, and choose the option for restoring your computer from a system image. Select the correct system image backup and the correct restoration location, then click Next. Your copy of Windows should now restore, ready for you to put the hard disk(s) back into your main PC when it is repaired.

www.it-ebooks.info

INSIDE OUT

Can you run Windows 7 from one PC on another computer?

You can run a Windows installation from one PC on another only if the motherboards of both computers match. Any difference between the two will result in a Blue Screen of Death (BSOD), and Windows will not start.

Although you can restore a copy of Windows on another PC, only do so if the host PC is identical to the one you have removed the hard disk from, for example, if they are from the same business environment.

zPOD

Although you cannot run a Windows 7 installation on a PC with a different hardware specification from the original, you can run it in a virtual machine. US-based company Zinstall has developed a piece of software called zPOD that allows you to create a virtual machine out of any Windows installation. The virtual machine you create will also include all of your installed programs. This installation can be loaded onto a USB disk drive or even a pen drive (also known as a thumb drive) and run on any PC, regardless of the installed hardware.

zPOD is available from *www.zinstall.com*. You can find out more about this software in Chapter 23, "Third-Party Rescue Tools and Services."

Restoring Windows File by File

In Chapter 4, "Backup and Restore," I described how Windows Backup encrypts files so they can't be read unless you restore them, discouraging some people from using this feature. Windows Complete PC Backup and third-party solutions from Symantec and Acronis do the same thing.

Many people find it more useful to boot into another operating system, such as a Linux disc (see Chapter 22, "Linux: An Operating System on a Disc"), and create a file-by-file backup copy of Windows on another hard disk or partition.

This approach has many advantages when it comes to restoring a malfunctioning operating system. For instance, you can copy back only the driver store folders or the registry files if they are causing the problem. This means that you can restore all of your critical operating system files, leaving settings and programs intact. Or you could replace only the files for a faulty program.

www.it-ebooks.info

For more information on what file does what in Windows, see Chapter 16, "Windows Problems Demystified."

INSIDE OUT To copy the Windows registry or not?

You can choose to copy back every file from your file-by-file Windows 7 backup to its original location. Doing so restores Windows, but software or settings might not work, because you will have also copied back old Windows registry files.

You can get around this by leaving the existing registry files on the original disk. There is one registry file in each user folder called Ntuser.dat. This is a hidden file, so you might need to set your computer to show hidden files before restoring your backup to the original computer. It is sometimes easier to simply not copy the C:\Windows\Users folder at all, since the only Windows system files it contains are the registry.

Restoring Your Data by Using Another PC

Although a copy of Windows 7 from one computer won't work on another, accessing your data on an alternative PC is much simpler.

CAUTION!

When attaching hardware to a PC, always be careful that the power is switched off and that the PC is disconnected from the main electrical outlet. Use an anti-static wristband when installing an extra disk into a PC case, if possible (see Chapter 19, "Diagnosing Hardware Problems").

Simply plugging the hard disk from your dead PC into a host PC will enable you to access your files and folders. The hard disk and any partitions from the defunct PC will appear in My Computer on the host PC. This way, you will be able to recover lost files, but sometimes you won't be able to write data back to the disk. This is because Windows 7 on the original PC has set access permissions for the drive's files and folders, and the new computer doesn't have permission to write to them. This is simple to fix, however. In My Computer, right-click the relevant drive or folder, and select Properties. In the Properties dialog box that appears, on the Security tab, choose the appropriate user(s) for whom you want to set permissions (see Figure 21-2).

www.it-ebooks.info



Figure 21-2 Taking ownership of files and folders

Click Edit with the specific user or user group highlighted and, in the dialog box that appears, give that user or user group Full Control of the disk or folder.

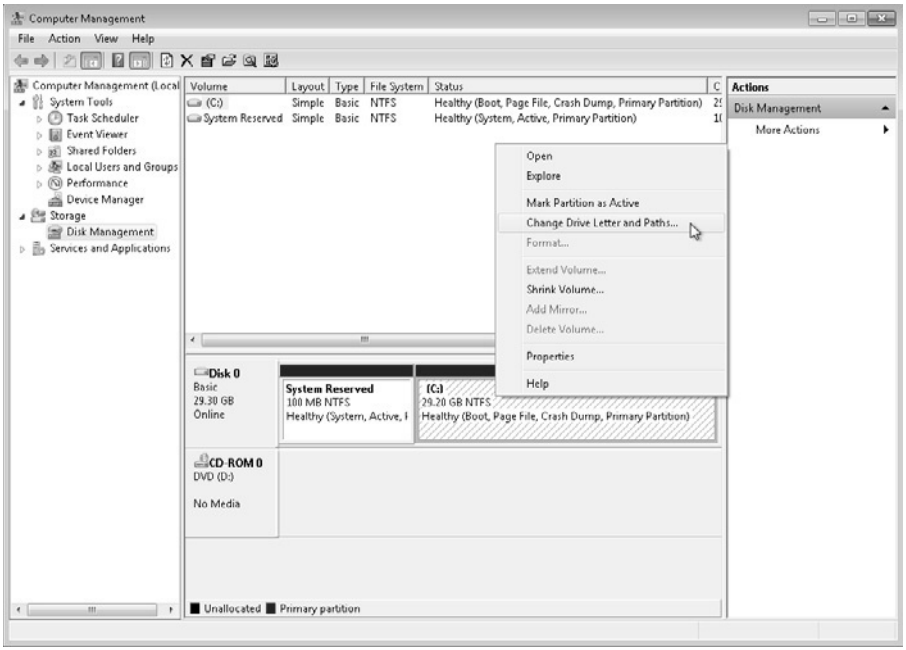
The system will now set the permissions for all files in that drive or folder. You should allow this process to complete and not cancel it. Depending on the number of files in the folder, this could take some time.

INSIDE OUT Your disk isn't appearing in My Computer

Sometimes new hard disks or partitions won't appear immediately in My Computer on a host computer, because they are sharing a drive letter (for example, the D drive) with another drive or partition. This is simple to rectify.

Type Computer Management in the Start menu search box, and run the Computer Management console when it appears in the search results. Then click the Disk Management link in the left pane of the console window.

www.it-ebooks.info



Right-click any drive or partition that is not appearing in My Computer, and select Change Drive Letter And Paths. Designate a new drive letter (only unused drive letters will appear in the choice list), or set it to appear as a folder on another drive.

Unless you store your files and data on a separate partition (which I definitely recommend; see Chapter 1, "Prevention Is Better Than Cure," and Chapter 4, "Backup and Restore"), your files and data are stored in the Users folder on the drive or partition containing your Windows 7 installation. This is shown in Figure 21-3.

www.it-ebooks.info

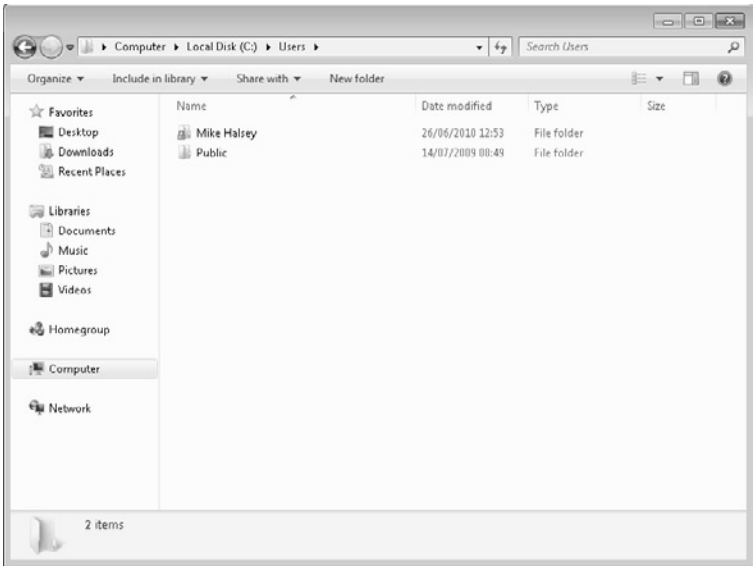


Figure 21-3 The Users folder in Windows 7

Summary

There are a great many ways to restore your files in Windows by using another PC, some complex and time-consuming and others simple and automated. The process you choose will depend on your circumstances and whether there is any important data you need to rescue. You'll learn about some of these methods in more detail in the next few chapters.

www.it-ebooks.info

CHAPTER 22

Linux: An Operating System on a Disc

System or Data Restore Using Another Operating System 325
Useful Software in Linux 330
CD and DVD Burning in Linux 333
Compatible Linux Operating Systems to Run from a Disc 334
Creating a Linux Installation Disc or Pen Drive 335
Summary 336

SURPRISING as this may sound, one of the best ways to rescue a dead Windows installation or your data could be a Linux distribution (commonly known as a distro). There are several advantages to using Linux this way; most importantly, it's nonintrusive in that it won't change or overwrite any files or settings in your Windows installation.

System or Data Restore Using Another Operating System

Many Linux distributions can run from a CD or DVD. For example, Figure 22-1 shows the popular Ubuntu Linux running on a PC, booted from the installation DVD.

When you start up a copy of Linux that can run from a DVD, you are asked whether you want to install the operating system on the hard disk or run it from the DVD to test it. You should choose the second option if your intention is to use Linux to rescue a faulty copy of Windows or your files.

> **Note**
>
> **Linux distributions vary, and the locations of the specific items I cover in this chapter might differ depending on the Linux variant you're using or even the version of that variant. Also, some of the tools mentioned in this chapter might not be available in your particular copy of Linux.**

www.it-ebooks.info

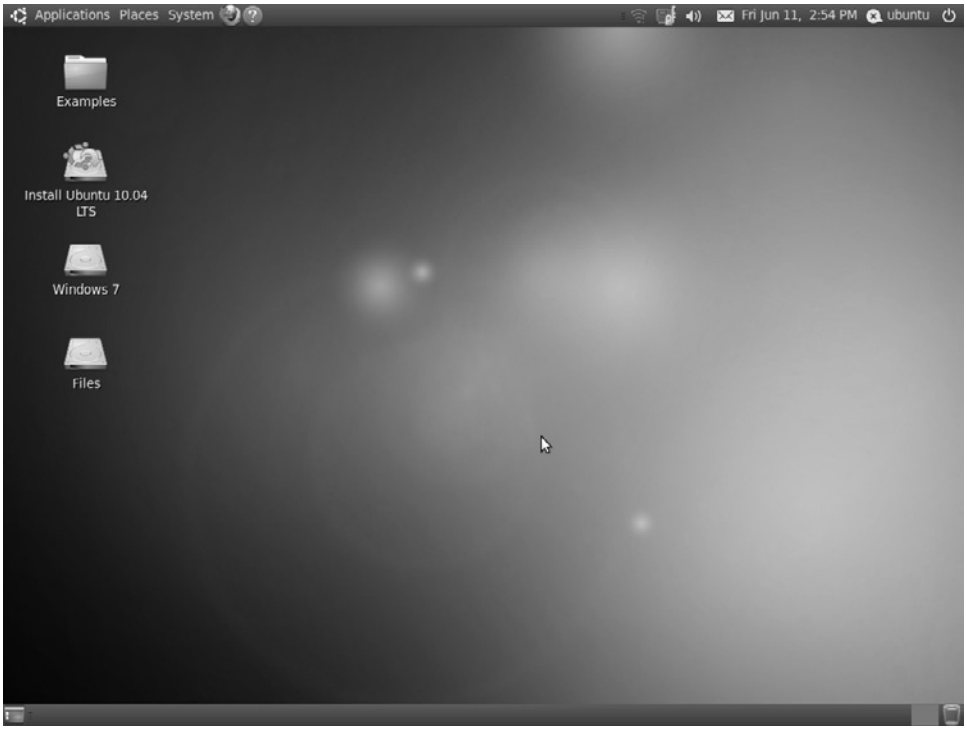


Figure 22-1 The Ubuntu desktop

INSIDE OUT Keep a Linux boot disc on standby

You never know when disaster will strike and you'll need to recover files from your PC or still be able to work with them when up against a tight deadline. I recommend downloading a Linux disc ISO and burning it to a CD or DVD to keep on standby, just in case. You can find download links at the end of this chapter.

One of the biggest advantages of Linux is that it's free to individual users, with the distributors making money by charging for optional support contracts. One disadvantage is that many people do not find Linux as user-friendly as Windows, although variants like Ubuntu have made enormous strides in general usability.

www.it-ebooks.info

Another disadvantage is that the software you usually use in Windows isn't available in Linux. However, most Linux distributions come bundled with some software already installed, including a web browser, a graphics package, and an office productivity package, such as OpenOffice. This software will normally open your files, even the newer Microsoft Office file formats, so you can keep working in the event of a disaster until your own PC or copy of Windows can be repaired.

INSIDE OUT Linux on a flash drive

Some Linux variants include a tool that enables you to boot the operating system from a USB flash drive. As long as your computer's BIOS permits booting from a USB device, this can be a useful tool in the arsenal of any Windows troubleshooter.

Figure 22-2 shows the Ubuntu computer browser, accessed on the Places menu at the top of the desktop.



Figure 22-2 Accessing your Windows drive in Ubuntu

www.it-ebooks.info

You can see all of your unencrypted hard disks and files from within Linux. This means that you can access your files through Linux and back them up to a DVD or to another location, such as a network drive or external USB hard disk. You can also use a Linux installation to restore Windows 7 on a file-by-file basis. See Chapter 21, "Restoring from Another PC" for more information on how to do this; the process from within Windows and Linux is identical.

> **Note**
>
> **If any of your disks or partitions are encrypted by Windows Encrypted File System (EFS) or BitLocker, they will not be readable from within Linux.**

Figure 22-3 shows how some Linux distributions include advanced disk management and diagnostic tools. For example, in Ubuntu you can edit and work with drives, sometimes on a far more advanced level than Windows 7 will allow.

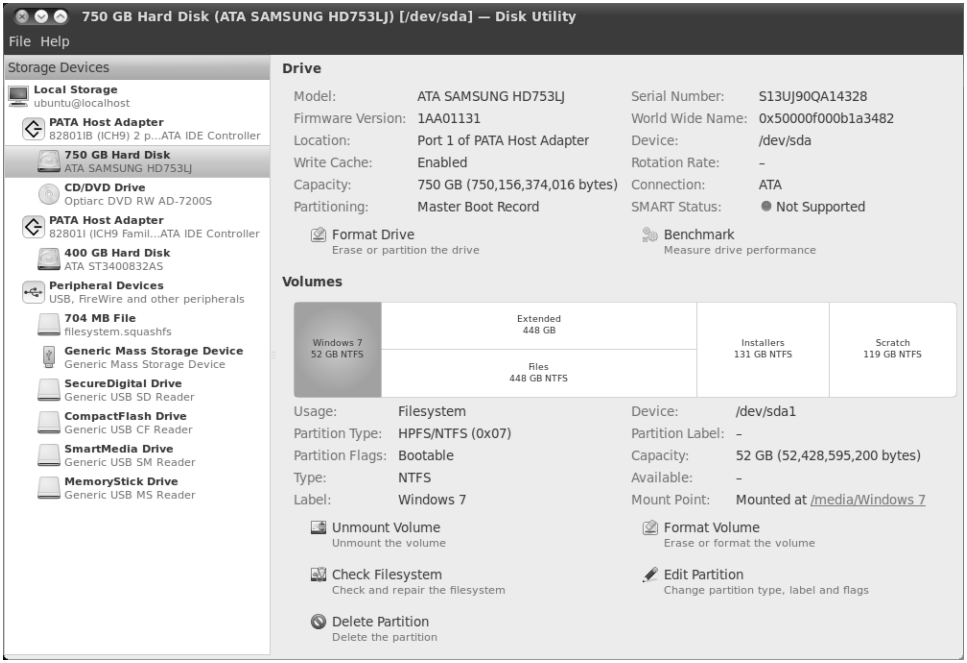


Figure 22-3 Managing drives in Ubuntu

www.it-ebooks.info

You can also run disk file system checks similar to using the Chkdsk command in Windows. Figure 22-3 shows the disk management console that you can access from the System menu at the top of the Ubuntu desktop by clicking Administration and then clicking Disk Utility. (This will vary from one Linux distribution to another.)

> **Note**
>
> **Because many hardware manufacturers do not support Linux, you might be unable to print any documents you need, such as copies of software or Windows product codes.**

Figure 22-4 shows the Ubuntu partitioning utility, accessed from the System menu at the top of the desktop by selecting Administration and then selecting GParted. (Again, this will vary depending on what Linux distribution you use.)

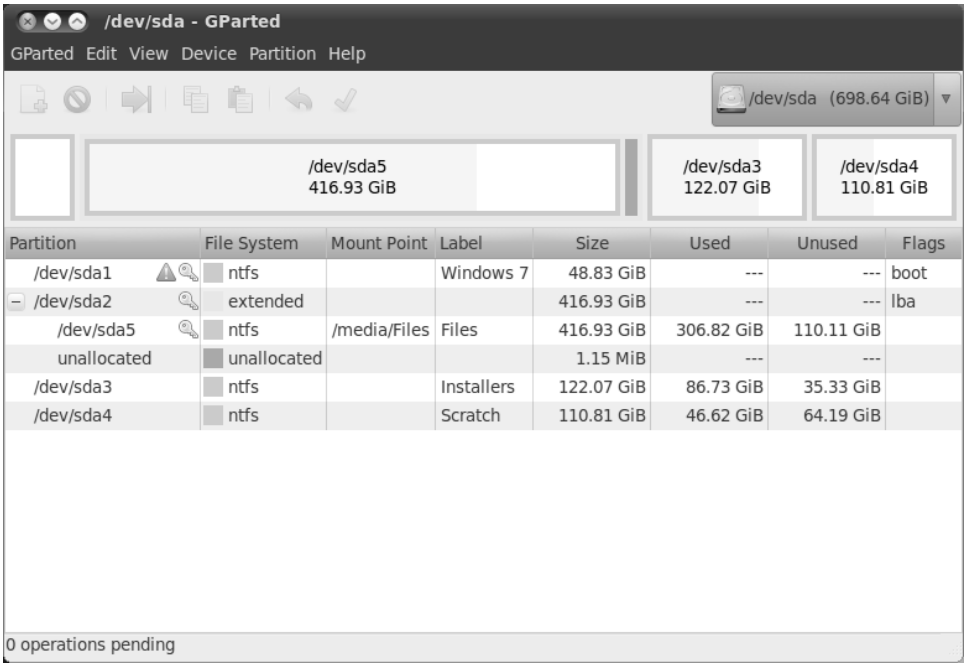


Figure 22-4 Managing partitions in Ubuntu

www.it-ebooks.info

Many Linux distributions contain a disk partitioning tool. Sometimes Windows 7 fails because the partition it sits on has become corrupt. You might be able to repair the partition using a Linux disk partitioning tool, or, if you have a system image backup of Windows 7, you can use Linux to delete the corrupt partition and create a fresh one in its place. You can then restore Windows 7 by booting from the Windows 7 installation DVD and restoring from an image backup using Complete PC Restore.

CAUTION!

When you boot your PC from a Linux CD or DVD, you have full administrator access to Windows and data drives in your computer. Always be careful not to delete critical system files or data that is not backed up or replaceable.

Useful Software in Linux

The software packages covered in this section vary in name, location, and availability depending on the version (distro) of Linux you are using. However, some are very useful tools in the operating system if you have access to them.

Remote Desktop

Some Linux packages include remote access software similar to Remote Desktop in Windows, as shown in Figure 22-5. You can use the Linux version of the remote desktop software to allow a remote support person access to your PC, so they can help diagnose and repair problems with Windows 7. The remote support person might need to be running the same version of Linux that you are, but other operating systems and some third-party remote desktop packages are compatible.

INSIDE OUT Connecting to the Internet in Linux

Hardware driver support for Linux is not as widespread as it is with Windows. You might be unable to get online if you use Wi-Fi on your PC, especially if you connect through a USB dongle. If you intend to use a USB dongle with Linux, from a working PC with Internet access, first visit the manufacturer's website for the USB dongle and see if they supply a Linux driver you can install from a CD or flash drive. The best way to get online when using a Linux disc is with a physical network cable.

www.it-ebooks.info

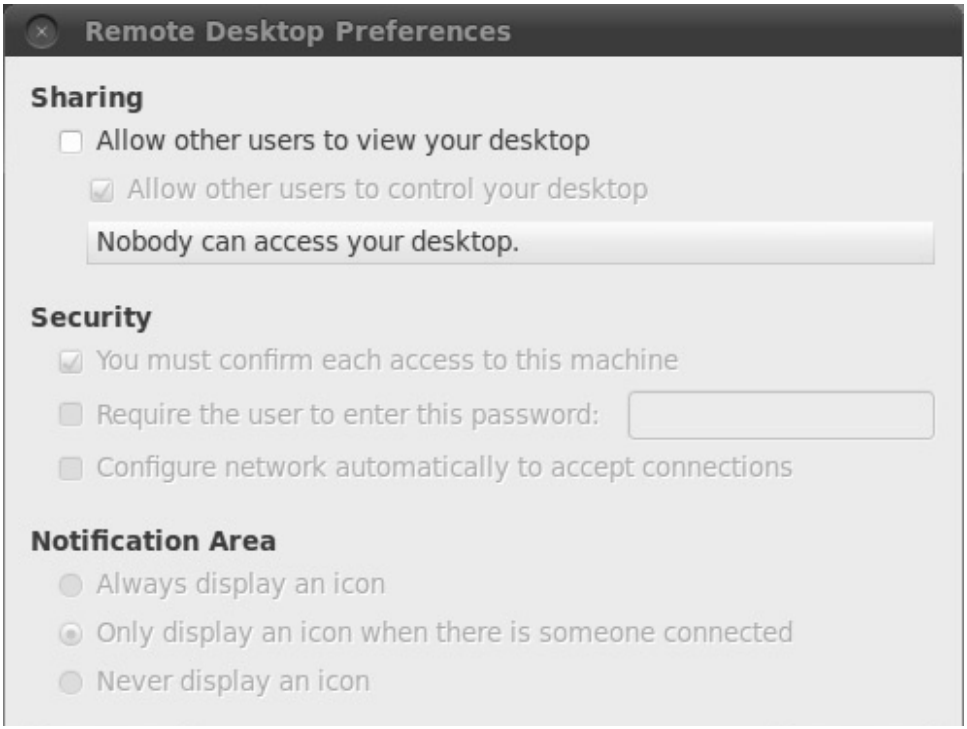


Figure 22-5 Remote Desktop in Ubuntu

System Monitor

System Monitor in Ubuntu, as in many Linux distributions, is very similar to the live System Monitor in Windows (see Figure 22-6). System Monitor provides live details of CPU, memory, and network activity on a PC. This can be useful for helping diagnose hardware errors; for instance, it can help determine if you are having difficulty getting online because of networking problems.

www.it-ebooks.info

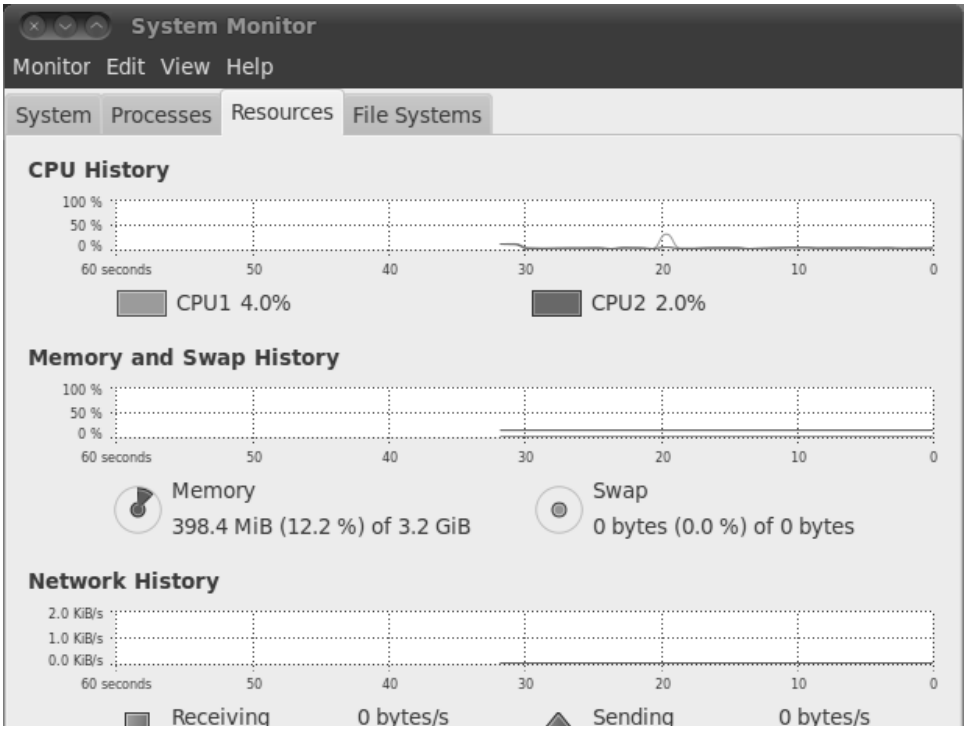


Figure 22-6 System Monitor in Ubuntu

System Testing

Some Linux distributions come with advanced system testers like the one shown in Figure 22-7. These will test many aspects of computer hardware to find and diagnose problems. The system tester in Ubuntu is an excellent example. It tests every aspect of the hardware and guides you through automated diagnostics with a helpful, wizard-based interface.

www.it-ebooks.info



Figure 22-7 The system tester in Ubuntu

CD and DVD Burning in Linux

All Linux distributions come with CD and DVD burning software standard. If you've lost your Windows 7 installation DVD but still have an image of the disc (or of your system repair disc), you can use Linux burning software to make another copy of the Windows disc (see Figure 22-8).

INSIDE OUT Keep an ISO copy of your Windows installation DVD

It is an excellent idea to keep a backup ISO (disc image) of your Windows installation DVD in case you damage or lose your original DVD. A quick search online will reveal a great many software packages, some free, that can create a backup ISO.

You can also burn new Windows installation discs from ISO files from within Windows 7 by double-clicking the ISO file to open the ISO Image Burner.

www.it-ebooks.info



Figure 22-8 Burning a CD or DVD in Linux is usually easy.

Compatible Linux Operating Systems to Run from a Disc

The list of the best and most popular Linux distributions can be found online at *www.linux.org*. They include the following.

Ubuntu

www.ubuntu.com

Ubuntu is the Linux variant that I have used to demonstrate Linux throughout this chapter and is shown in Figures 22-1 to 22-8. I used Ubuntu because it's widely considered to be one of the most user-friendly Linux variants and is shipped with some new PCs by companies such as Dell.

www.it-ebooks.info

Other Variants of Linux

A few other variants of Linux include

- **Debian** *www.debian.org*
- **SuSe** *en.opensuse.org*
- **Fedora** *www.fedoraproject.org*
- **Knoppix** *www.knoppix.com*

Creating a Linux Installation Disc or Pen Drive

All downloadable Linux variants are available as ISO files. Windows 7 now supports these natively and allows you to burn them to a CD or DVD. To burn an ISO file to a CD or DVD in Windows, simply double-click the file, select the appropriate disc burner, and then click Burn (see Figure 22-9).

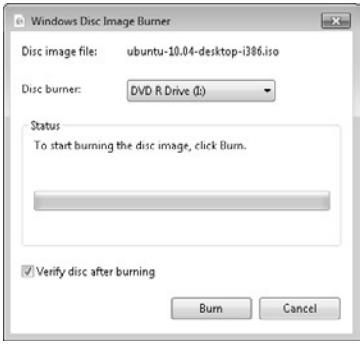


Figure 22-9 Burning a disc image file to CD or DVD in Windows 7

You should check online for the latest utility to write a bootable ISO file to a USB pen drive. Note that if you want to boot your copy of Linux from a USB pen drive, you should check that the computer's BIOS supports booting from a USB device and that this is set in the boot order, as shown in Figure 22-10.

www.it-ebooks.info

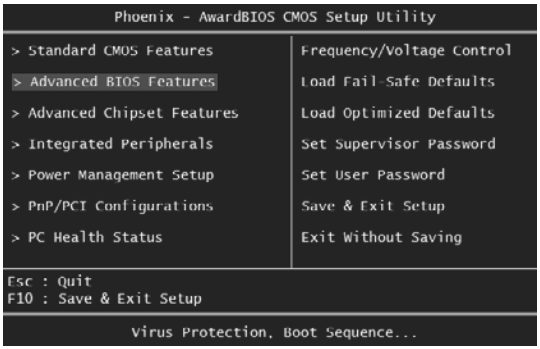


Figure 22-10 Setting the boot options in the BIOS

Summary

Linux is a full operating system in its own right and, with modern distributions like Ubuntu, can keep you working if your copy of Windows fails. Although Linux is not as popular, because most people prefer the familiarity of Windows, it can be extremely useful when rescuing or repairing a Windows system.

www.it-ebooks.info

CHAPTER 23

Third-Party Rescue Tools and Services

Zinstall and zPOD 337
GRC SpinRite 341
Other Third-Party Tools 344
Other Third-Party Services 344
Summary 345

THERE are a huge number of third-party rescue and recovery tools available for Microsoft Windows 7. These tools vary in price considerably from free to hundreds of dollars. They can also vary considerably in quality and functionality. This can make it very difficult to choose the best recovery and rescue option for you. In this chapter, I will highlight some of my favorite software and packages that have received general acclaim.

Zinstall and zPOD

www.zinstall.com

Zinstall and zPOD aren't marketed or sold as Windows rescue tools, but you'd be surprised just how effective both can be when it comes to getting a damaged PC working again. Even if your PC has failed completely, as long as your hard disk or your copy of Windows 7 isn't damaged, you can use Zinstall or zPOD to rescue the system, complete with all of your software, and be back up and running again quickly.

They're slightly different types of software, but both get a copy of Windows running in a virtual machine (VM). Here's a brief description of their primary functions.

Zinstall

Zinstall was designed primarily to ease the upgrade from Windows XP to Windows 7 by creating a VM of your copy of Windows XP to run in the new Windows 7 environment, complete with all of your programs. This means that when upgrading to Windows 7 from Windows XP, you can keep downtime to an absolute minimum and perform a clean install of all of your software and files into Windows 7 in your own time.

www.it-ebooks.info

zPOD

zPOD works in the same way as Zinstall, but it allows you to copy the VM it creates to an external USB hard disk or even to a pen drive and run Windows from that device on any other computer.

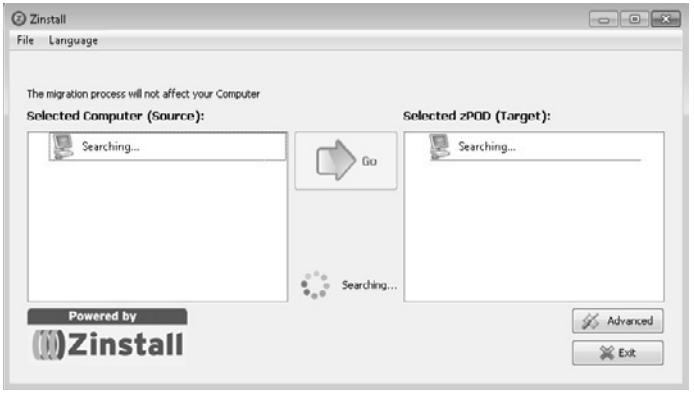
Both programs operate in an incredibly simple way by allowing you to create a VM with a single click. They automatically search for your installed operating systems and then enable you to quickly and easily choose a destination. Both software packages will work with any version of Windows, including Windows 7, and can even rescue a copy of Windows from a dead PC.

To rescue a copy of Windows 7 from a dead PC, follow these instructions.

1. Plug the hard disk from the dead PC into another computer. Remember to make sure both computers are turned off and disconnected from the electrical outlet before working inside the case.

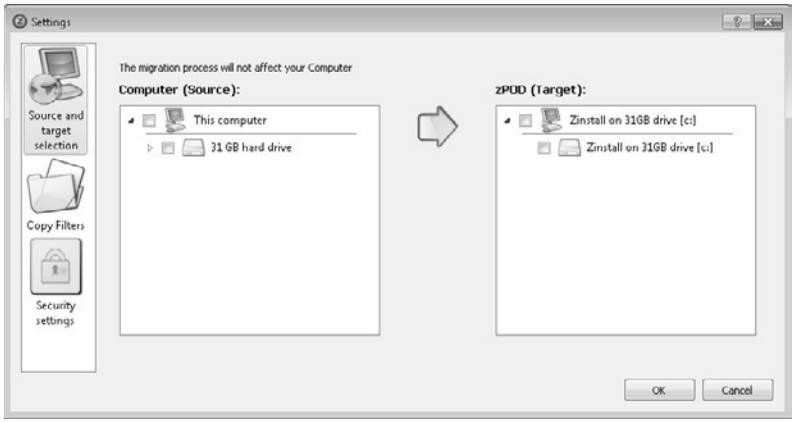
2. Boot the working computer into the copy of Windows that's installed on it.

3. Install the Zinstall or zPOD software on the working PC, and run it.



4. By default, Zinstall or zPOD will find the main, running copy of Windows. To point the software toward the copy of Windows on the imported hard disk, press Advanced.

www.it-ebooks.info



5. You can choose to omit certain file types. By default, Zinstall and zPOD exclude any files in the Users folder. Indicate whether to include or omit other files in the Copy Filters panel of the Advanced settings window.

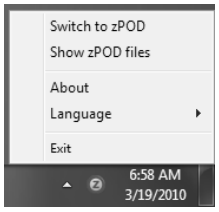


6. zPOD uses 256-bit encryption to secure the VM so you can carry it around with you, safe in the knowledge that only you can access this copy of Windows and your programs. Activate this option by setting up a password in the Security Settings panel of the Advanced settings window.

www.it-ebooks.info



7. It could take several hours for Zinstall or zPOD to create the VM. When the process is complete, a utility for running the VM appears.



INSIDE OUT Zinstall or zPOD: Which is right for you?

If you intend to use the VM only on the PC that you create it on, then Zinstall will do, since it creates the VM to run on the computer where it is created. Use zPOD if you want to use your virtual copy of Windows 7 on other computers, too.

The single biggest advantage of zPOD and Zinstall is continuity of productivity. Simply put, this means that, as long as there is a spare computer available that you can use, you will always be able to keep working.

Although you can't use Complete PC Backup, you can use other disk imaging utilities, such as Norton Ghost or Acronis True Image (see Chapter 18, "Where to Find More Help and Support," for more details) to create an image of the rescued copy of Windows 7. You might also be able to use a third-party tool to rescue programs from the damaged Windows 7 installation that you do not have the original installers for.

www.it-ebooks.info

Either way, you now have a rescued copy of Windows 7 and your programs that you can continue using.

GRC SpinRite

For some years, GRC SpinRite has been widely considered one of the best, if not the best, hard disk rescue and maintenance tool available. SpinRite is a DOS program that runs from a bootable CD, DVD, or other device, such as a floppy disk or USB pen drive. Because you boot your computer into SpinRite, the software has full low-level administrator access to the hard disks on your computer.

SpinRite can perform a broad range of checks on your hard disk(s) and includes the following features.

- A real-time graphical status display, showing the health and status of your hard disk (see Figure 23-1). This graph is updated in real time, displaying data and disk recovery and repair as it happens. All events are also logged so you can review them later.

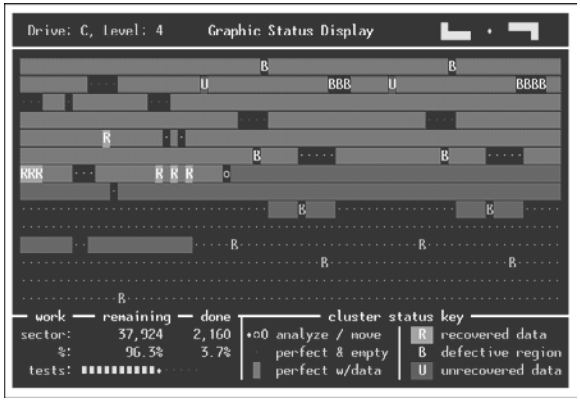


Figure 23-1 Graphical log of the state of a hard disk in SpinRite

- Detailed technical logs of the hard disk (see Figure 23-2). Helpfully, the error information these logs provide includes clear descriptions that can help you determine exactly where errors are located and what they are. GRC boasts about the clarity of the language they use when providing reports on your hard disks, and I can confirm that the quality of the information SpinRite can give you is excellent indeed.

www.it-ebooks.info

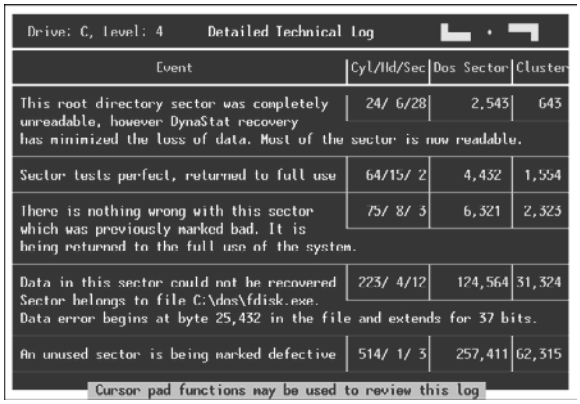


Figure 23-2 Detailed technical information about your hard disk displayed in SpinRite

- The Surface Analysis Monitor uses exhaustive techniques to detect defects on the hard disk (see Figure 23-3). It deliberately creates scenarios on your hard disk to try to replicate the worst types of failure that can occur. This is an extremely thorough and excellent way to check for defects.

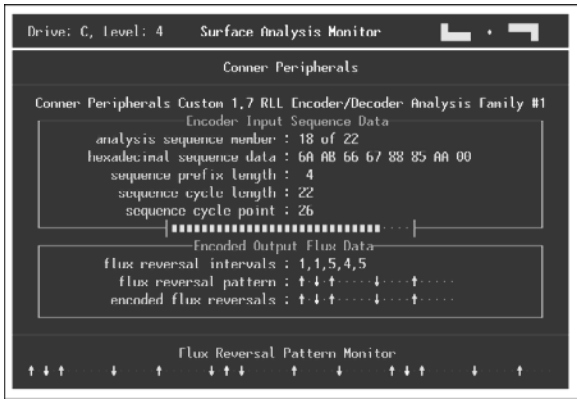


Figure 23-3 Comprehensive disk error checking tools in SpinRite

- Extensive data recovery tools that work tirelessly to recover your data (Figure 23-4). A special tool called Dynastat appears if SpinRite has trouble reading data on a faulty hard disk. This tool provides more detailed information in real time about the software's attempts to recover your files and data.

www.it-ebooks.info

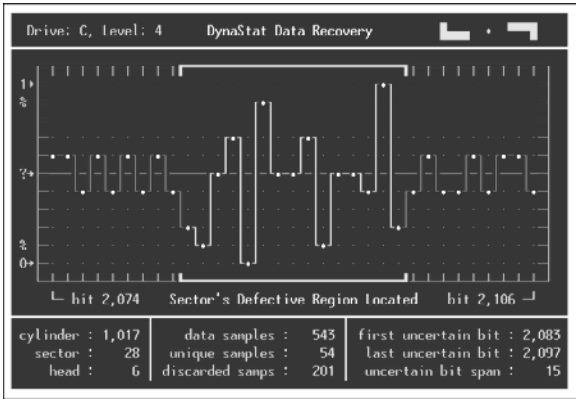


Figure 23-4 SpinRite gives up trying to recover your data only when you do.

- Detailed information about the existing partition structure on hard disks. SpinRite also checks partitions for errors, as shown in Figure 23-5.

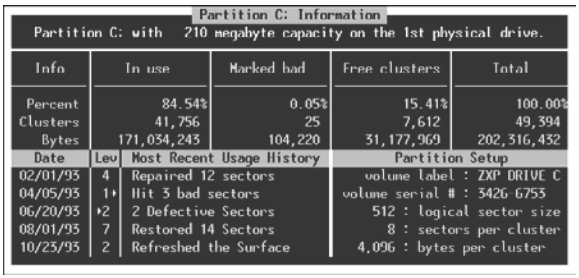


Figure 23-5 SpinRite checking existing partitions on a disk for errors

In all, SpinRite is an invaluable tool for diagnosing and repairing errors on physical hard disks. Its support for different drive formatting options is extensive, and it is, as I have said, held in high regard within the technical community.

INSIDE OUT SpinRite and solid state disks

Solid state disks (SSDs) operate differently from mechanical hard disks in that they store all of your data on silicon chips and include no moving parts. Therefore, SpinRite is not the best tool for diagnosing errors on these types of disk.

www.it-ebooks.info

Other Third-Party Tools

Many companies provide specialist software for rescuing data or hard disks, and you should try the forums mentioned in Chapter 18 for recommendations. Here are details of packages I recommend.

O&O Disk Recovery

www.oo-software.com

O&O Disk Recovery is a comprehensive package that performs several useful functions. The most commonly used function of the software is an unerase program to help recover files and folders that have been accidentally deleted. There are also other functions within the software that can provide recovery in scenarios such as the accidental formatting of a hard disk. This can be extremely useful, as in Windows 7 it can be annoyingly simple to accidentally format disks.

This software can be useful for rescuing data or a faulty disk in your PC, and you can also remove the hard disk from your PC and plug it into another computer to run these rescue tools on it.

Ashampoo WinOptimizer

www.ashampoo.com

Although Ashampoo WinOptimizer traditionally has not been used as a tool for rescuing a hard disk or data, it now contains a small utility that can help you do just that. This tool analyses your hard disk(s) to try to find defective areas or problems with the disk(s). It contains tools that can then be used to apply automatic repairs and fix some of the more common problems that you can encounter.

Other Third-Party Services

At some point, you might reach the stage where there's nothing more you can do with your disk. If the disk includes critical data that you must recover, you will need to go to a professional data recovery specialist.

These companies offer extremely comprehensive services, and they can be hugely successful at recovering data from damaged hard disks, but they will not be inexpensive.

You can find data recovery specialists in your area by searching in your local telephone directory online or through a search engine.

www.it-ebooks.info

Summary

The best way to make sure you can always rescue your files and data is to have at least one backup copy that is regularly refreshed. Windows 7 contains a tool to enable you to do this, and there are also many third-party tools that do the same thing. You can read more about backing up your files and data in Chapter 4, "Backup and Restore."

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 24

When You Can't Recover Data

Encrypted File System 347
BitLocker and BitLocker To Go 361
Creating a Copy of Encrypted Data 364
Summary 365

Sometimes you might encounter a situation where the files and data you are trying to recover are encrypted. Windows provides some tools to aid with unlocking data, but you will need access to the recovery keys specific to the locked data. There are several methods that can be used in Windows 7 for encrypting files, data, and even entire hard disks.

Encrypted File System

The Windows Encrypted File System (EFS) has been around for over a decade and is used to provide file and folder encryption for individual users, for instance, two people who share a computer but want to keep their files private from one another.

EFS uses a public/private key encryption method similar to that used by the popular Pretty Good Privacy (PGP) encryption software and utilizes methods used by digital certificates to send and receive personal information over the Internet. This public/private key encryption technique uses two keys, one stored on the computer and another that the user has access to.

You need to carefully configure EFS to avoid losing access to your files if something goes wrong with Windows.

INSIDE OUT EFS and removable drives

EFS encryption will work only on drives formatted with New Technology File System (better known as NTFS). This means that if you copy any encrypted files to a non-NTFS–formatted device, such as a FAT 32–formatted external hard disk or an exFat-formatted USB pen drive, the encryption on those files will be removed when they are copied.

www.it-ebooks.info

Setting Up EFS

1. To configure EFS, right-click the file(s) or folder(s) you want encrypted, and select Properties.

2. On the General tab, click Advanced.

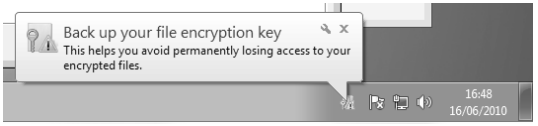
3. In the Advanced Attributes dialog box, select the Encrypt Contents To Secure Data check box, and then click OK. When prompted, make sure you apply the action to the folder and all files and subfolders.



4. The files and folders will be automatically encrypted, and when this process is complete, a message in the taskbar notification area prompts you to back up your file encryption key.

CAUTION!

If you do not back up your file encryption key to a safe location, you might never be able to access your files again if you need to reinstall Windows.



www.it-ebooks.info

You can choose to back up your key immediately, or Windows can remind you to do so the next time you log on. I recommend you make a backup immediately.



5. The Certificate Export Wizard appears.



6. The standard options will probably serve your needs, but Windows 7 does offer additional backup options when you save a copy of your file encryption key. Here you can choose what aspects of your security key you want to back up.

www.it-ebooks.info

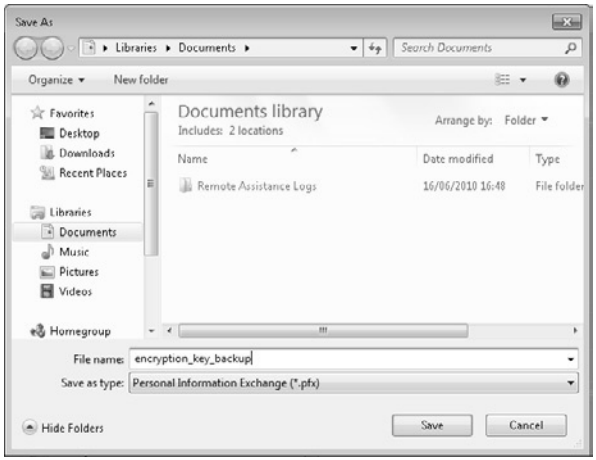


7. Set a password for your backup. You won't need to enter this password to read encrypted files, but you will need it if you must restore the file encryption key. You should not lose a record of or forget this password.



8. Enter a file name, and decide where to store your backed-up file encryption key. Make sure it is kept in a safe location and that you have more than one copy.

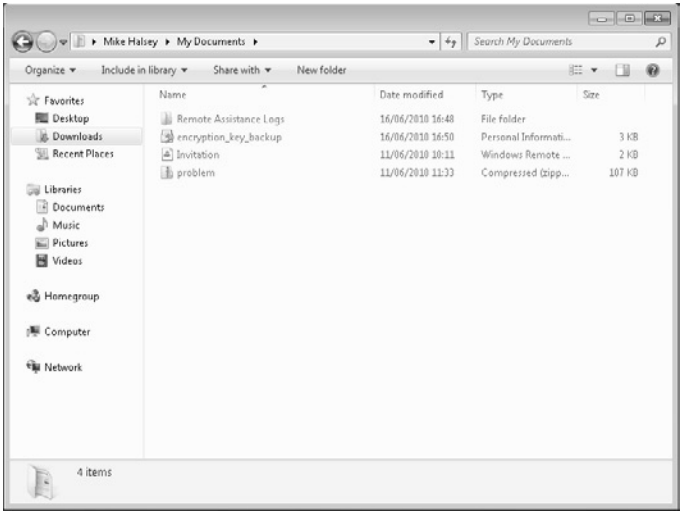
www.it-ebooks.info



CAUTION

In the example in the above procedure, I mistakenly backed up my file encryption key to a folder that is encrypted using EFS. Windows won't prevent you from doing this, so be careful. Any key backed up to an encrypted drive will not be accessible if something goes wrong or if you have to reinstall Windows.

Your files and folders will now be encrypted.



www.it-ebooks.info

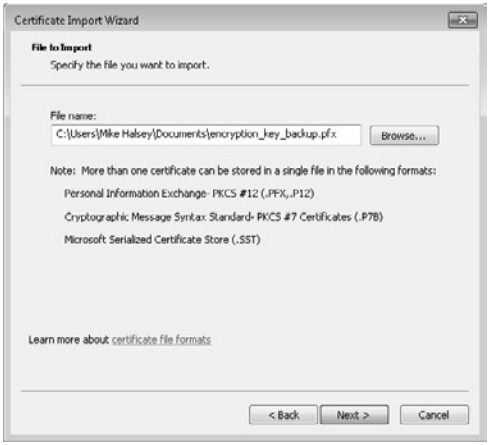
INSIDE OUT EFS and user passwords

EFS does not require that a user password is set up on your Windows account; however, it provides no protection if your user account is not password-protected since anyone can log in to your account and have unrestricted access to the files.

Restoring an EFS Key

If you have to reinstall Windows 7, perhaps because of a critical error, then your EFS-encrypted files are unreadable until you restore your EFS encryption key using the following steps.

1. Double-click the backed-up EFS encryption key to open it, and then click Next on the first two pages.



2. Enter the password you set when you created the EFS encryption key, and then click Next.

www.it-ebooks.info



3. Restore the certificate to the default store in Windows 7 or to a different location if your network requires this.



The EFS encryption certificate will now be restored, and you will again have access to your files and data.

www.it-ebooks.info

INSIDE OUT When might you need to restore your EFS key?

If the Windows default password store becomes corrupt, you will need to restore your EFS key. Or, if someone tries to forcibly reset your password to access your files and folders, the system will lock out the EFS-encrypted files until you can restore the correct key.

Turning EFS Off

You may want to turn off EFS encryption for files or folders after it has been set up. You use almost the same procedure as when you set up the encryption.

1. Right-click the file(s) and folders(s) you wish to decrypt, and select Properties.
2. On the General tab, click Advanced.
3. In the Advanced Attributes dialog box, clear the Encrypt Contents To Secure Data check box, and then click OK. When prompted, make sure you apply the action to the folder and all files and sub-folders.

EFS Certificates

If your encryption key is damaged or lost, you might be able to recover your files and folders using an encryption key certificate. You can create one of these when you encrypt your files or at any time afterward.

1. Type **command** in the Start menu search box, and when Command Prompt appears in the search results, right-click it, and run it as an administrator.
2. Navigate to the folder on a spare hard disk or removable drive where you want to store your EFS certificate. Do this by typing the drive letter and colon (for example, type **E:** to move to the E drive), and then use the CD command to move to the correct folder (for example **CD ./Files/Backups** to move to the Backups folder in the Files folder).
3. Type **cipher /r: *file name*** (where *file name* is the name you want to assign to the backed-up EFS certificate), and then press Enter on your keyboard.

www.it-ebooks.info

Windows creates a backup of the EFS certificate, which can be restored using the following method.

1. In the Start menu search box, type **secpol.msc**, and run the secpol (Security Policies) program when it appears.



2. Open the Public Key Policies section in the left pane of the Local Security Policy window that appears, right-click Encrypting File System, and select Add Data Recovery Agent. Use the wizard that appears to select and install the EFS certificate.



www.it-ebooks.info

3. In the Start menu search box, type **command** and open Command Prompt.

4. Type **gpupdate**, and then press Enter on your keyboard.

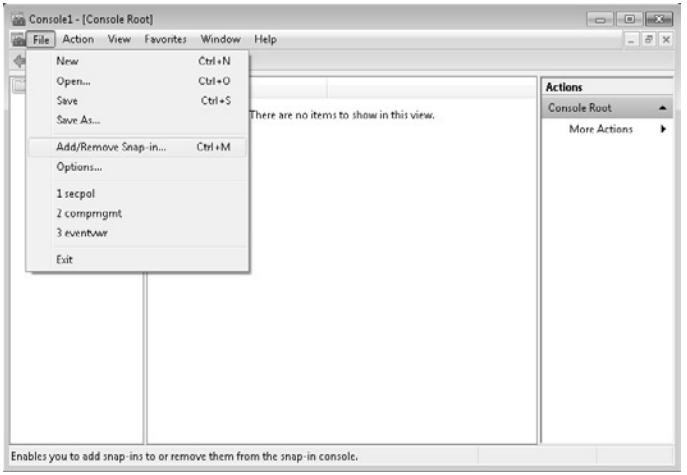
Smart Cards and EFS Certificates

If you use a smart card with EFS to access your data, you will need to back up the certificate for your smart card. To do this, follow these steps.

1. Type **mmc** in the Start menu search box, and open Microsoft Management Console (MMC).

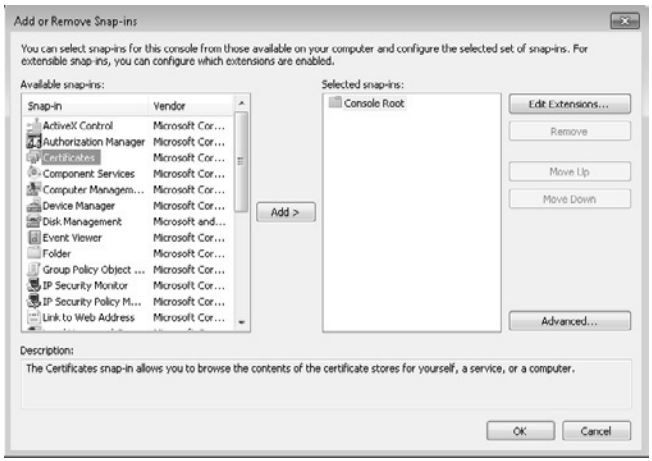


2. On the File menu, click Add/Remove Snap-in.

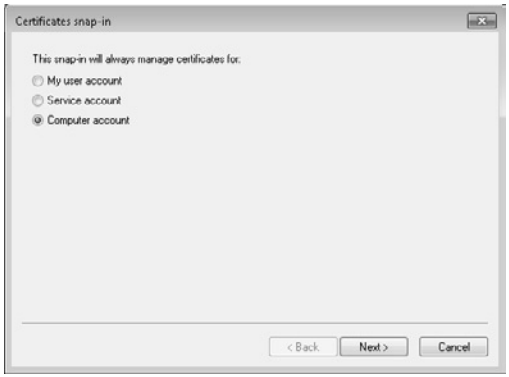


www.it-ebooks.info

3. Select Certificates in the left pane, click Add, and then click OK.

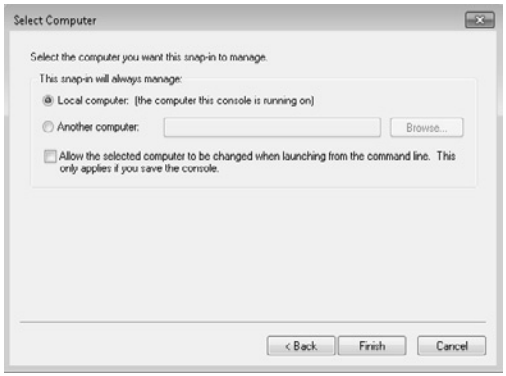


4. Select Computer Account on the next screen, and then click Next.

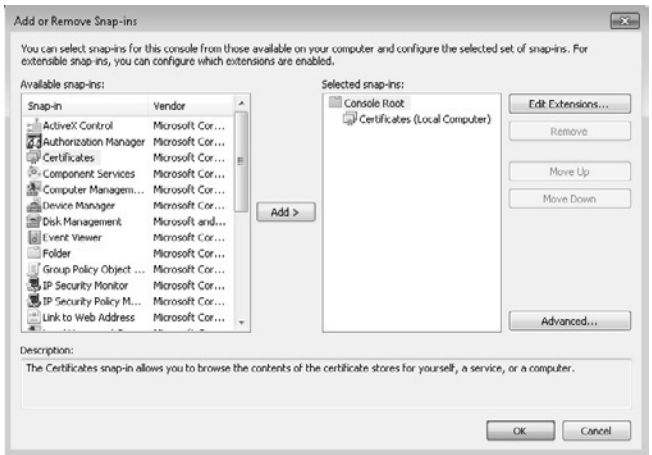


5. Make sure Local Computer is selected on the next screen, and then click Finish.

www.it-ebooks.info



6. Certificates appears in the Selected Snap-ins section. Click OK to exit this window.



7. In the main MMC window, click Certificates.
8. Click the certificate that lists Encrypting File System under the Intended Purposes section. If there is more than one, select them all.
9. On the Action menu, select All Tasks, and then click Export.
10. In the Export Wizard, select Export Private Key.
11. Click Personal Information Exchange, and then click Next.
12. Assign a password for this file; don't forget this password.
13. When prompted, indicate where you want to save your backed-up security certificate, and then click Finish.

www.it-ebooks.info

To restore your security certificate, follow steps 1 through 6 in the previous procedure, and then follow these instructions.

1. On the Action menu, click All Tasks, and then click Import.
2. Click Next, and navigate to the location of your backed-up security certificate. In the list next to the file name box, select Personal Information Exchange.
3. Type the password you set when creating the certificate, and then finish the wizard.

File Encryption Certificate Manager

By typing **file encryption** in the Start menu search box, you can open the File Encryption Certificate Manager (see Figure 24-1).

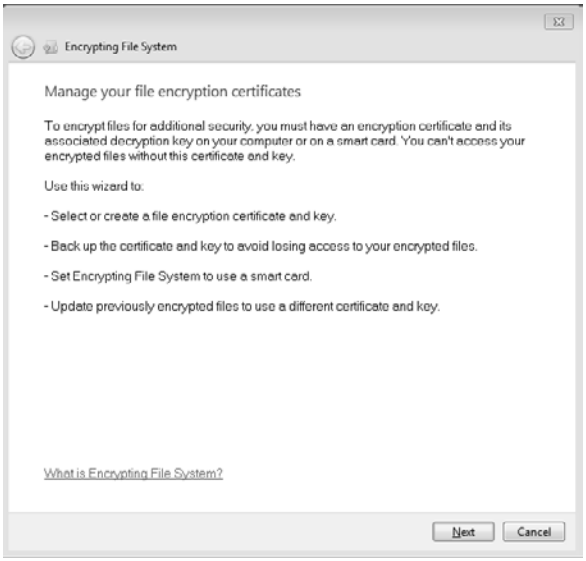


Figure 24-1 Managing your file encryption certificates in Windows 7

This dialog box allows you to view, back up, update, and restore EFS certificates in Windows 7 by using a friendly interface; however, you may not find it as powerful or flexible as the methods described previously in this chapter.

Recovering EFS-Encrypted Files

You should always keep a copy of your EFS encryption key and your password safe. If you lose the backed-up copy of your key, you won't be able to gain access to your files, and if you lose your password, you won't be able to restore the key.

www.it-ebooks.info

Although EFS is very secure, employing a 256-bit ECC (Elliptic-Curve Cryptographic) algorithm cipher to secure your data, it may still be possible to recover your password by purchasing special software or by taking your computer to a computer security specialist. Following are two examples of software you can use to recover a password.

Advanced EFS Data Recovery

www.elcomsoft.com/aefsdr.html

Advanced EFS Data Recovery is advanced software for cracking EFS passwords. The company claims that even if data is damaged or if someone has attempted to tamper with the encryption key, it can still recover data.

EnCase Forensic

www.guidancesoftware.com/computer-forensics-ediscovery-software-digital-evidence.htm

EnCase Forensic is password-cracking software for EFS drives and much more. EnCase Forensic includes a full suite of analysis, bookmarking, and reporting features.

Cipher.exe

Cipher.exe is a command-line tool accessed through Command Prompt in Windows 7, as shown in Figure 24-2. (Type **CMD** or **command** in the Start menu search box, right-click Command Prompt or CMD in the search results that appear, and run the Command Prompt as an administrator.)

Cipher is a powerful tool for managing encryption and decryption in Windows 7. You can access a list of switches that you can use with the program by typing **cipher /?** Into the Command Prompt window.

One of the most useful features of Cipher in Windows 7 is the ability to completely and securely wipe data from a disk. This is a very powerful tool and must be used with caution, because you cannot later recover files that have been wiped.

You access this facility by typing **cipher /w *x*:\folder**, where *x* indicates what you want to wipe. For instance, if you want to wipe your D drive, type **cipher /w D:**. If you want to wipe a folder called Personal in your C drive users folder, type **cipher /w C:\Users*Mike Halsey*\Personal**.

www.it-ebooks.info

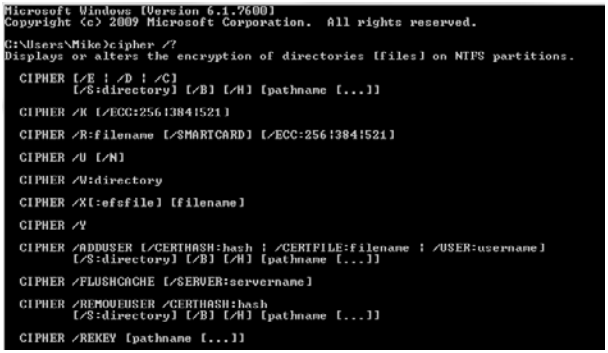


Figure 24-2 Cipher.exe

BitLocker and BitLocker To Go

BitLocker is a full-drive encryption method that was introduced with Windows. It encrypts data using a 128-bit AES (Advanced Encryption Standard) key and works at its most secure if your computer's motherboard contains a TPM (Trusted Platform Module) chip.

There are three modes that BitLocker works in when authenticating the user.

- **Transparent Operation mode** This is used when you have a TPM chip on your motherboard; the encryption key is stored on the chip.
- **User Authentication mode** This mode requires the user to type a password before the operating system boots to provide authentication.
- **USB Key mode** In this mode, the user must insert a USB pen drive containing the encryption key.

You can use BitLocker in Windows 7 to encrypt internal partitions, hard disks, external hard disks, or USB pen drives. These drives can be encrypted only in the Enterprise or Ultimate versions of Windows 7, but they can then be used in any other Windows 7 version and on any other PC running Windows 7 by entering a password or by using a smart card or USB pen drive containing the decryption key. (See the Inside Out sidebar titled "Reading BitLocker-encrypted hard disks on another computer" on the next page.)

www.it-ebooks.info

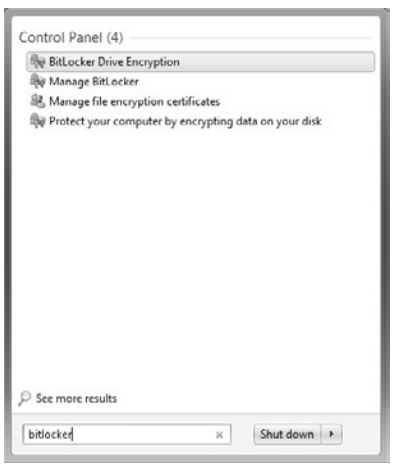
INSIDE OUT Reading BitLocker-encrypted hard disks on another computer

You can read a BitLocker-encrypted disk on another computer running Windows 7 unless you have encrypted it using a TPM chip. This chip will lock that hard disk to that specific motherboard, rendering it unreadable on another computer.

In Windows XP you can read, but not write to, drives protected by BitLocker To Go by downloading the BitLocker To Go Reader from the Microsoft website. You can find it at *www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=64851943-78c9-4cd4-8e8d-f551f06f6b3d*.

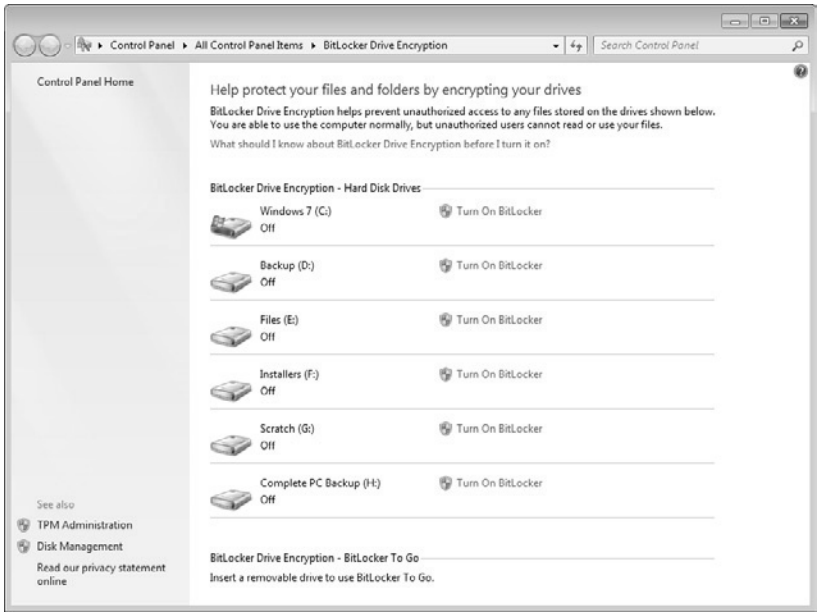
BitLocker is also more flexible than EFS for encrypting drives because you can easily carry a BitLocker drive from one computer to another without having to go through the rigamarole of exporting and importing security keys and certificates using complex management consoles.

1. Access BitLocker by typing **BitLocker** into the Start menu search box or, from Control Panel, by clicking System And Security, and then clicking BitLocker Drive Encryption.



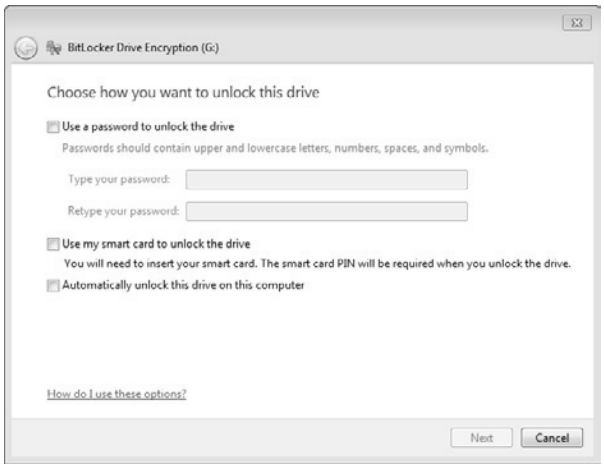
2. In the BitLocker Drive Encryption window, you can manage the drives that are encrypted using BitLocker. Click the TPM Administration link in the bottom left of the window to manage a TPM chip on your motherboard if you have one.

www.it-ebooks.info



3. When you encrypt a drive, you will have several options, including setting a password or using a smart card. These options will allow you to access the drive on another computer. Choose which options you want to use.

Select Automatically Unlock This Drive On This Computer if you intend to use the drive only on the computer where it was encrypted (such as a laptop). For this option to work, the copy of Windows 7 on that computer must also be encrypted with BitLocker.



www.it-ebooks.info

From the BitLocker Management Console, you can change your password, disable BitLocker for a drive, or temporarily suspend BitLocker encryption.

CAUTION!

Unlike EFS, which encrypts specific files and folders, BitLocker encrypts entire disks or partitions and is extremely secure. A hard disk encrypted using BitLocker will be completely inaccessible on another PC without the password or correct smart card or USB pen drive access.

Some security and data recovery companies may offer professional services to recover lost BitLocker encryption keys. Commercial software is also now available. One such program is Passware Kit Forensic (available at *www.lostpassword.com*). This software can quickly recover encryption keys for drives protected with BitLocker. Passware also offers other security software that can, for example, recover lost Windows user passwords.

Creating a Copy of Encrypted Data

Sometimes it can be difficult to tell whether data you encrypt will still be encrypted when you make a copy of it. You can use the information in Table 24-1 to determine if your data will still be encrypted in different scenarios.

Table 24-1 **Will your encrypted data still be encrypted when you make a copy of it?**

	EFS-Encrypted Folder	Bitlocker-Encrypted Drive	Unencrypted Folder or Drive	CD/DVD
FAT32-Formatted	Not Supported	Yes	No	Not Supported
exFat-Formatted	Not Supported	Yes	No	Not Supported
CDFS-Formatted	Not Supported	Not Supported	Not Supported	No
NTFS-Formatted	Yes	Yes	No	Not Supported

www.it-ebooks.info

Summary

You should always keep backups of your files and data, whether encrypted or not, in secure locations where they cannot be affected by disasters such as fire or theft.

The encryption systems available in Windows 7 are extremely useful but can very easily render your data forever beyond your reach, especially if you cannot afford the services of a professional data recovery company. They should always be used with care.

www.it-ebooks.info

www.it-ebooks.info

PART 5

Power Utilities

CHAPTER 25
Advanced Windows Diagnostic Tools in Depth 369

CHAPTER 26
Windows Firewall in Depth 401

CHAPTER 27
Advanced Registry Work 413

www.it-ebooks.info

www.it-ebooks.info

CHAPTER 25

Advanced Windows Diagnostic Tools in Depth

Computer Management 369
Performance Information and Tools 380
Control Panel Troubleshooters 398
Summary 400

In this chapter I'll look in more depth at the specific diagnostic and troubleshooting tools in Windows 7 and examine how you might use them for detailed problem solving and analysis.

Computer Management

The Computer Management console is the central location for managing and monitoring Windows 7. You can access the Computer Management console either by right-clicking Computer on the Start menu and clicking Manage (see Figure 25-1) or by typing **manage** in the Start menu search box and running Computer Management from the results that appear.

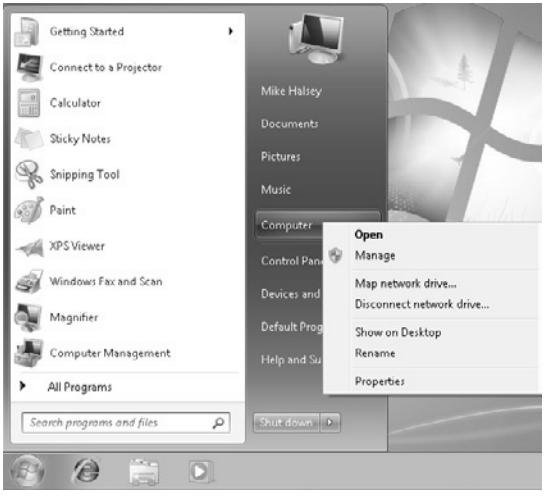


Figure 25-1 Accessing the Computer Management console

www.it-ebooks.info

In the main Computer Management window, the tools are divided into three categories: System Tools, Storage, and Services and Applications (see Figure 25-2).

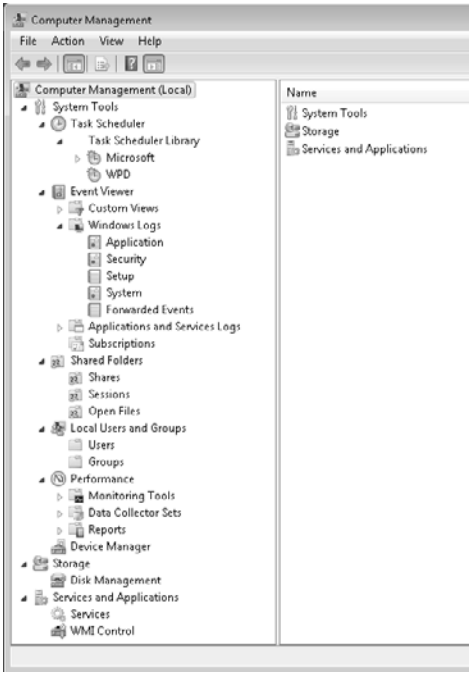


Figure 25-2 The Computer Management console

System Tools

System Tools manages events, tasks, file and folder sharing, users, and user groups and monitors the performance of your PC.

Task Scheduler

Task Scheduler in Windows, shown in Figure 25-3, isn't just the place where you can set your programs to run automatically at startup or on a schedule; a great many Windows components also use this feature.

www.it-ebooks.info

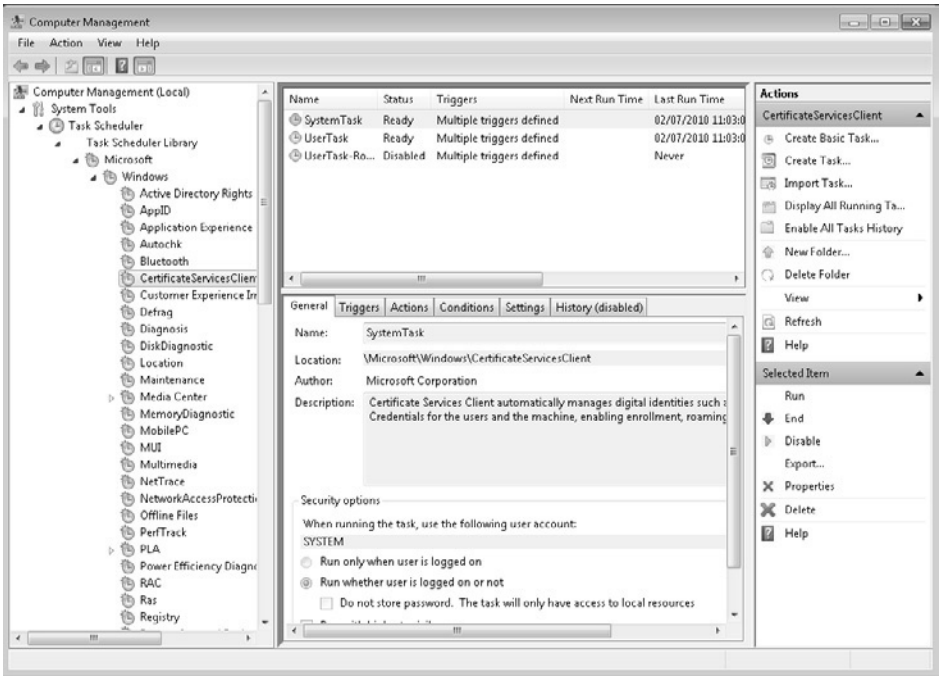


Figure 25-3 Task Scheduler

You can expand any item on the list of Windows components under Task Scheduler to see its scheduled tasks. You can use the tabs across the center of the window to modify and set up tasks.

- **General** This tab summarizes information about the task and also contains some basic security options for the task. A useful feature on this tab is the option to run a task in compatibility mode for Windows Server 2008 or Windows Vista.
- **Triggers** On this tab you can specify what (if appropriate) will trigger the task.
- **Actions** This tab indicates what happens when the task activates. You can set programs to launch and commands to run on this tab.
- **Conditions** The settings on this tab give you more control over a task, allowing you, for instance, to only run the task if the computer is idle or if it is plugged into an electrical outlet.
- **Settings** This tab includes additional settings associated with the task.
- **History** If any events are associated with the task, they appear on this tab.

www.it-ebooks.info

Adding New Tasks

You can create a new task by selecting Create Basic Task or Create Task from the Actions pane on the right of the Computer Management console. The Create Basic Task option launches a simpler wizard, but Create Task gives you more control. Clicking Import Task in this pane imports tasks that you have created previously and saved using the Export Task options in the Task Scheduler (see "Exporting Tasks" below).

You can also select Display All Running Tasks to display all of the currently running tasks or Enable All Tasks History to enable or disable the event history recording for tasks.

In business or corporate environments where tasks have been created using the AT.exe tool, it may be necessary to click the AT Service Account Configuration link to set what user account (that is, privilege level) these tasks will run at (see Figure 25-4).

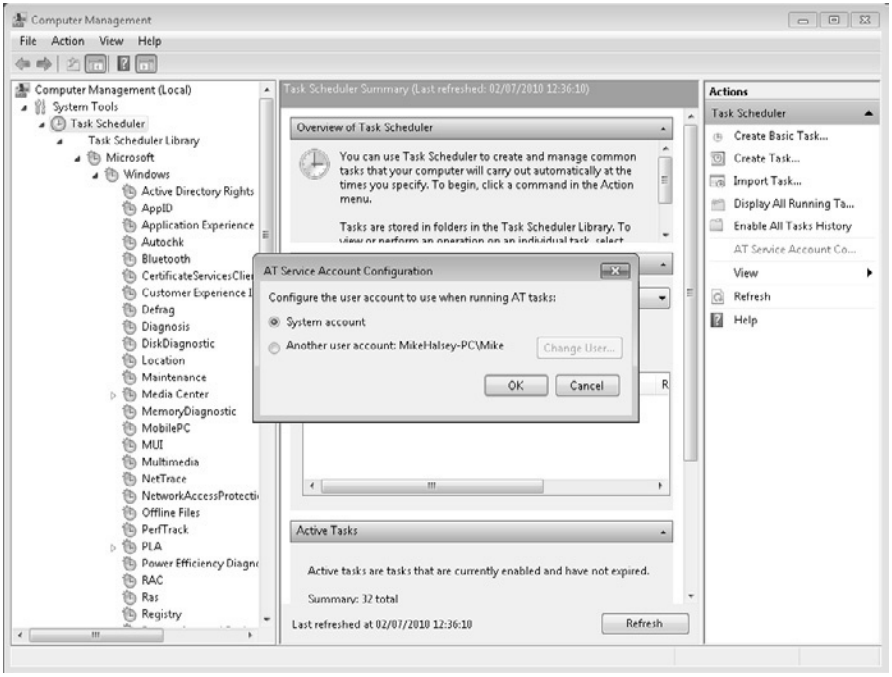


Figure 25-4 Assigning tasks to specific user accounts

Exporting Tasks

You can right-click any task and select Export to export the task to a file (see Figure 25-5). This can be useful if you want to use a task on different computers, or if you want to keep a backup of the task in case you need to later reinstall Windows 7.

You can also right-click a task and select Properties to see more detail and have more control over the task.

www.it-ebooks.info

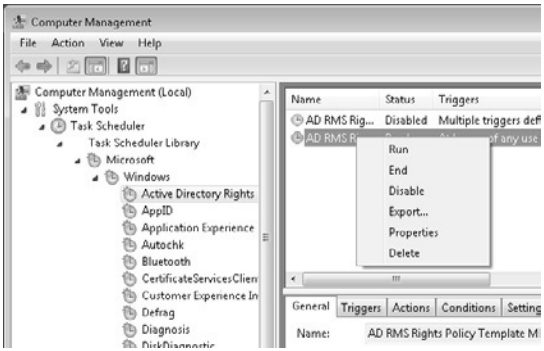


Figure 25-5 Exporting tasks

Event Viewer

Event Viewer is probably the most useful troubleshooting component in Windows 7, and it's highly configurable. The Actions pane on the right of the Computer Management console includes options to save and reopen event logs and to search for specific events (see Figure 25-6).

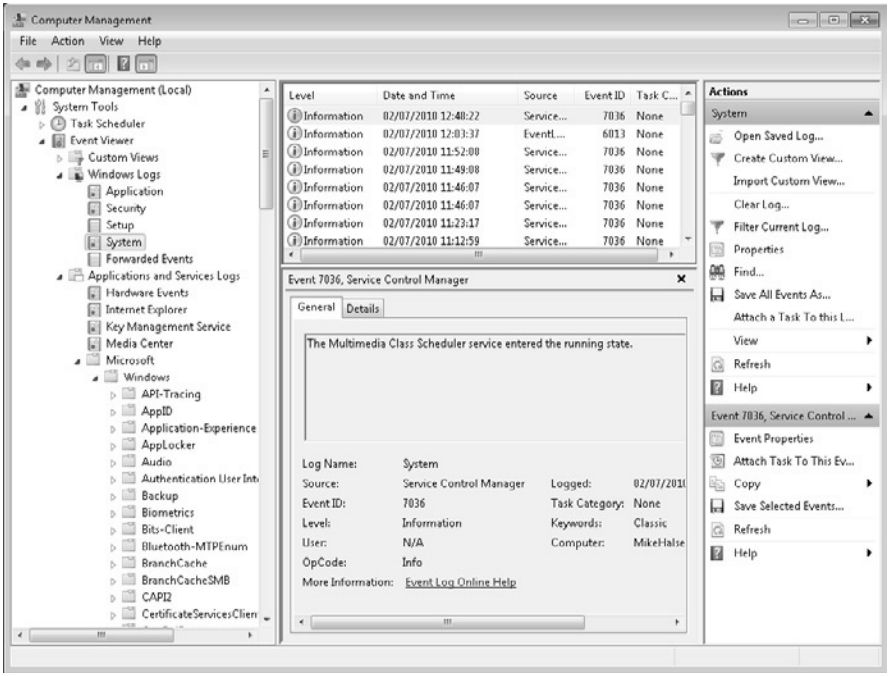


Figure 25-6 Event Viewer

www.it-ebooks.info

Event Log Filtering

Also in the right pane is the Filter Current Log option. This can be extremely useful for displaying certain types of logs, for instance critical and error logs (see Figure 25-7).

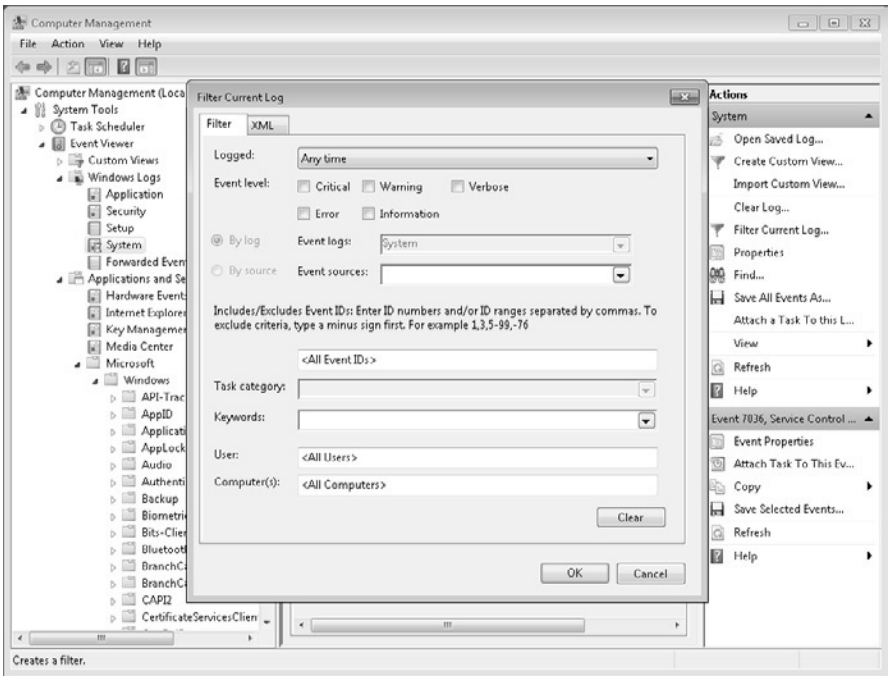


Figure 25-7 Filtering events

Windows 7 stores a great deal of information in its event logs; being able to filter the information by using the Filter Current Log option can prove a real timesaver when troubleshooting problems.

You can also filter by the event source, namely by Windows component and by user.

Attaching a Task to an Event

You can attach tasks to specific events so that they happen automatically when the event occurs. This could include automatically running Problem Steps Recorder to alert you that something is happening you want to see or to send an email to a support person letting

www.it-ebooks.info

them know that a specific error or event has recurred. This is useful for problems that occur occasionally and are difficult to diagnose.

You can also trigger an on-screen message when an event occurs (see Figure 25-8). You may want to use this as an alert that something has happened (remember, not all errors are immediately obvious) and include instructions on what to do when it does happen. You can do this by highlighting an event and clicking Attach Task To This Event in the Actions pane.

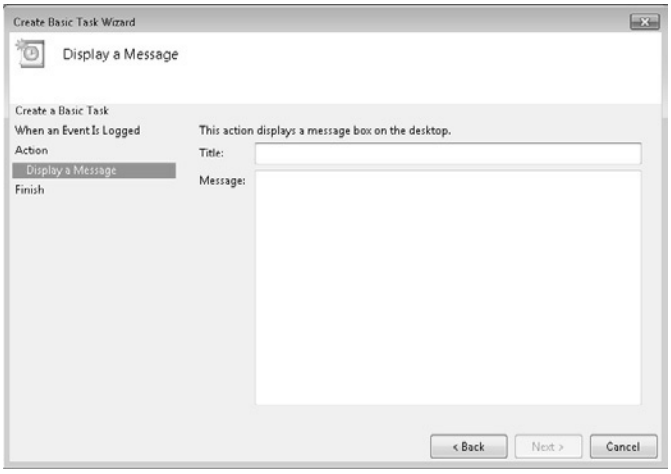


Figure 25-8 Displaying a message for an event

For instance, these instructions could direct a user to send an email to a support person detailing exactly what software was running, what was happening when the error occurred, what hardware was plugged into the computer, and what user account was being used.

Creating Custom Views

In the Custom Views section in the left pane, you can create new views in Event Viewer (see Figure 25-9). You can do this by right-clicking Custom Views or by selecting Create Custom View from the Action menu.

www.it-ebooks.info

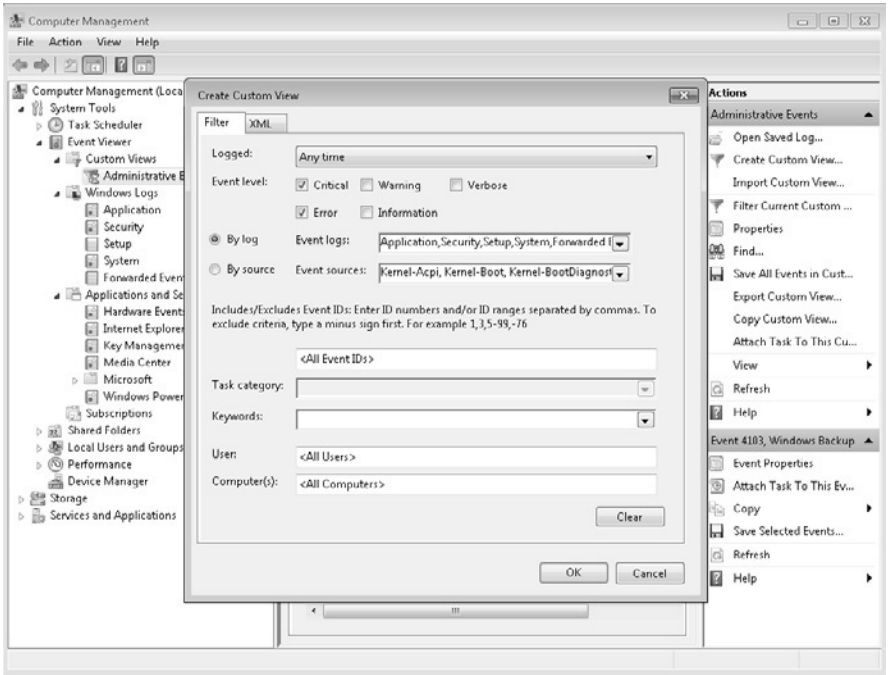


Figure 25-9 Creating custom event views

For the example in Figure 25-9, I created a custom view that reports all errors and critical events associated with the Windows Kernel (startup). If you are troubleshooting a specific part of Windows, this can be an invaluable timesaver and allow you to create a very detailed and concise error log that can then be exported and emailed to a support person if necessary.

Shared Folders and Local Users and Groups

The Shared Folders and Local Users And Groups options are very similar, so I will deal with them together. They give you control over file and folder shares and any users or groups of users on the PC. You can right-click any item in the central panel of this window to review its properties.

This can be useful, for instance, in the following scenarios.

- Shared files are not showing on another computer.
- A file is being reported as open by Windows but does not appear so.
- You want to set specific security or other policies for a user or a group of users.

www.it-ebooks.info

Performance

I will talk about the performance tools in more depth later in this chapter.

Device Manager

The Device Manager, shown in Figure 25-10, is a quick and easy way to get access to the hardware drivers in Windows 7.

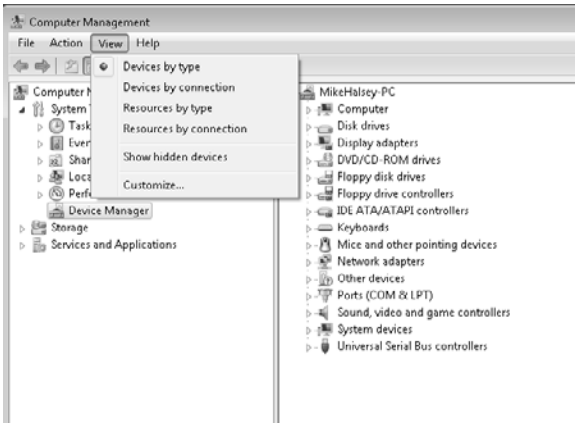


Figure 25-10 Device Manager in Computer Management

On the View menu are several options that you may find helpful.

- **Devices By Type** This is the default Device Manager view, showing your hardware devices grouped by their device type.
- **Devices By Connection** This view shows core Windows hardware devices for your computer.
- **Resources By Type** This can be an extremely useful view, showing you, for instance, what devices are sharing Interrupt Requests (IRQs), memory segments, and Input/Output (I/O) connections with your motherboard. Some hardware problems are caused by IRQ conflicts, and here you can see if any exist.
- **Resources By Connection** This view shows core Windows hardware devices by I/O, IRQ, and memory connections.
- **Show Hidden Devices** Probably the most useful tool on the View menu, this option shows hidden devices. By default, not all devices appear in Device Manager, and sometimes a device may disappear from the list. With Show Hidden Devices, you can force Device Manager to display all of the devices that are attached to, or are a part of, your PC.

www.it-ebooks.info

Storage

I covered the Disk Management feature in Chapter 14, "Advanced Diagnostic Tools in Windows 7." You use Disk Management to see all fixed and removable drives that are attached to your PC and to partition, format, and initialize new disks.

Services and Applications

Services are programs that require no interaction from the computer user and that perform specific tasks within Windows, such as searching for Windows updates or print spooling. In the Services panel you can see what services are installed in Windows 7 and which are running, and you can perform actions on them.

I find it useful to click the Status column heading to sort the processes by status to easily see which are currently started (see Figure 25-11).

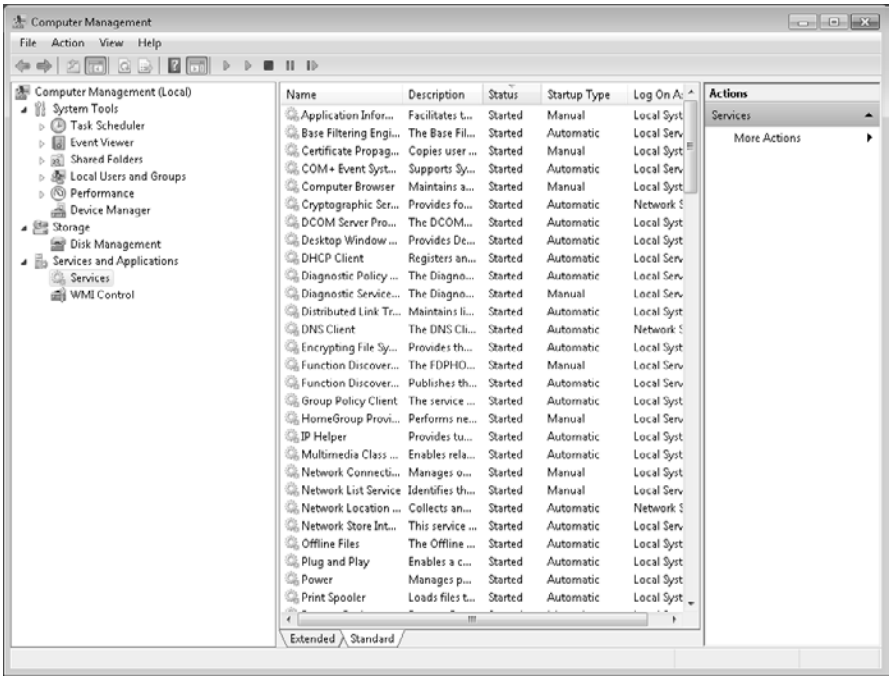


Figure 25-11 Windows Services

The useful service descriptions can help you determine what they are and what they do.

www.it-ebooks.info

You can right-click any service and select Properties to view the service's settings. In the Properties dialog box, you can set the service's status and disable it if necessary.

Figure 25-12 shows the Recovery tab in the Properties dialog box for a service. On the Recovery tab, you can set what Windows should do if a service causes a problem and fails. One option is to run a program, Problem Steps Recorder, for instance.

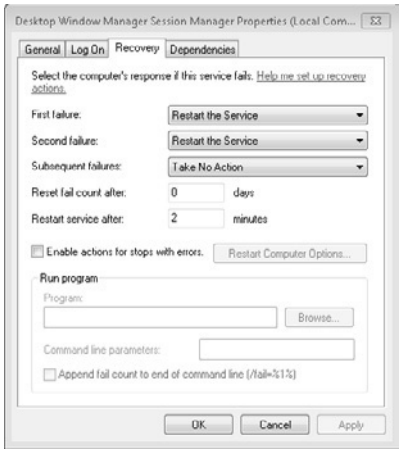


Figure 25-12 Recovery tab in a service's Properties dialog box

INSIDE OUT

Launching Problem Steps Recorder in response to an action

Although you can launch Problem Steps Recorder by typing *Problem Steps* into the Start menu search box, where do you find it if you want to auto-launch it in response to an event?

You will find the program listed on your Windows drive as \Windows\System32\psr.exe.

WMI Control

Windows Management Instrumentation (WMI) is a way for your computer to access and share management information over an enterprise network. It is used by management tools like Windows Systems Management Server and will probably not display anything on your Windows 7 PC when you click WMI Control in the Computer Management console.

www.it-ebooks.info

Performance Information and Tools

On the surface, Performance Information and Tools offers a way for gamers and PC enthusiasts to rate their computers so that they can compare their Windows Experience Index score with their friends (see Figure 25-13). Delve a little deeper, however, and you quickly find a large number of powerful help and diagnostic tools.

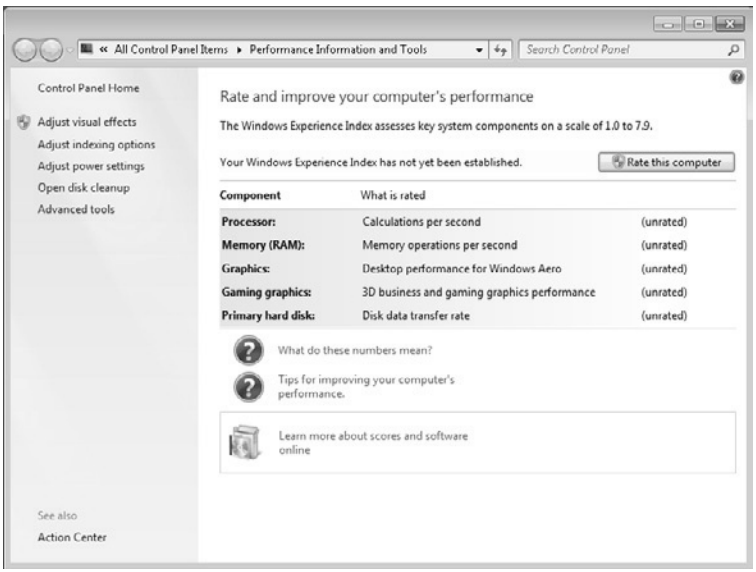


Figure 25-13 Performance Information and Tools

In Chapter 14, I wrote about the features in Performance Information and Tools, but here I will go into more detail about specific features that can prove invaluable for diagnosing and repairing problems with Windows.

Visual Effects

You can access the Visual Effects options by clicking the Adjust Visual Effects link in the blue pane on the left side of the Performance Information and Tools panel. The options do much more than just change the way some Windows components look.

On the main Visual Effects tab (see Figure 25-14), you can turn off effects that are causing Windows to behave sluggishly, such as animation settings. On some computers, particularly older machines or low-power computers such as netbooks and tablets, changing some of these settings improves the performance of the operating system.

www.it-ebooks.info

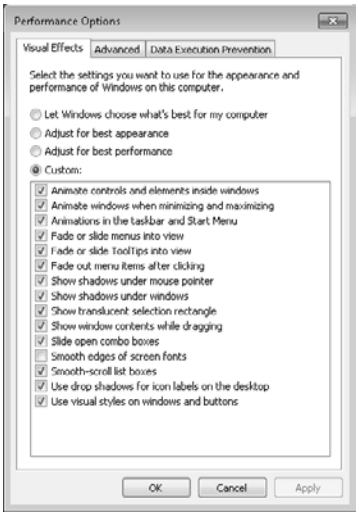


Figure 25-14 Adjusting Visual Effects

The Visual Effects tab also includes default settings for running Windows 7 optimized for best appearance and best performance.

On the Advanced tab (see Figure 25-15), you will see the virtual memory settings. (See Chapter 1, "Prevention Is Better Than Cure," for details on how to change these settings.) On this tab, you can also adjust the performance of Windows for the benefit of either programs or background services.



Figure 25-15 Virtual memory and processor scheduling setting

www.it-ebooks.info

You should select the Programs option unless you are running a dedicated device for a specific task, such as a file or print server.

On the **Data Execution Prevention** tab, you will find the settings for Data Execution Prevention (DEP) (see Figure 25-16). These settings are related directly to visual settings. DEP is a system to prevent viruses and other malware from running code from nonexecutable memory. Code run in this way could cause a buffer overflow in the memory stack and crash the operating system. A buffer overflow is where a program writes data to memory reserved and/or being used by another program or service.



Figure 25-16 Data Execution Prevention settings

Unfortunately, some software will occasionally be blocked by DEP, especially certain games. If you are having a problem with a program or game, you could try allowing it through DEP to see if it fixes the problem.

To do this, follow these instructions.

1. On the Data Execution Prevention tab, select Turn On DEP For All Programs And Services Except Those I Select.
2. Click Add, and navigate to the folder where the program is located. This will commonly be in the Program Files folder on the C drive.
3. Select the program you want to allow through DEP, and then click OK.
4. Add any other related programs (multi-player mode, for example) the same way, and then click OK on the Data Execution Prevention tab when you are done.

www.it-ebooks.info

Indexing Options

The Windows 7 Index is a database of all of your files and their contents. If this database becomes corrupt, it can prevent the search facility in Windows 7 from operating correctly.

You can reset the index by clicking Advanced in the Indexing Options dialog box and then clicking Rebuild in the Advanced Options dialog box (see Figure 25-17).

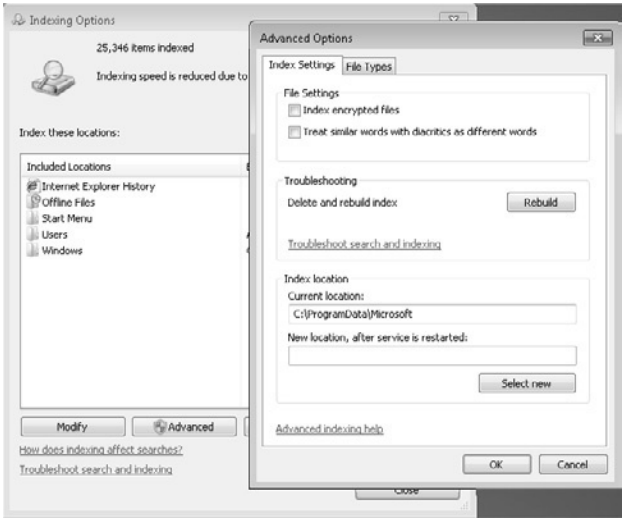


Figure 25-17 Rebuilding the index

Power Settings

I have a problem on one of my own self-built PCs that causes it to continually go to sleep every few seconds. The only way around this is to keep wiggling the mouse and pressing a key on the keyboard until I can get into the power options and disable the Sleep function. This can be an annoying first step each time I reinstall Windows 7.

In the Power Options panel (see Figure 25-18), you can change a great many settings for Windows 7 that go far beyond choosing power options for running a laptop on battery power or changing the default action of the Start menu power button.

www.it-ebooks.info

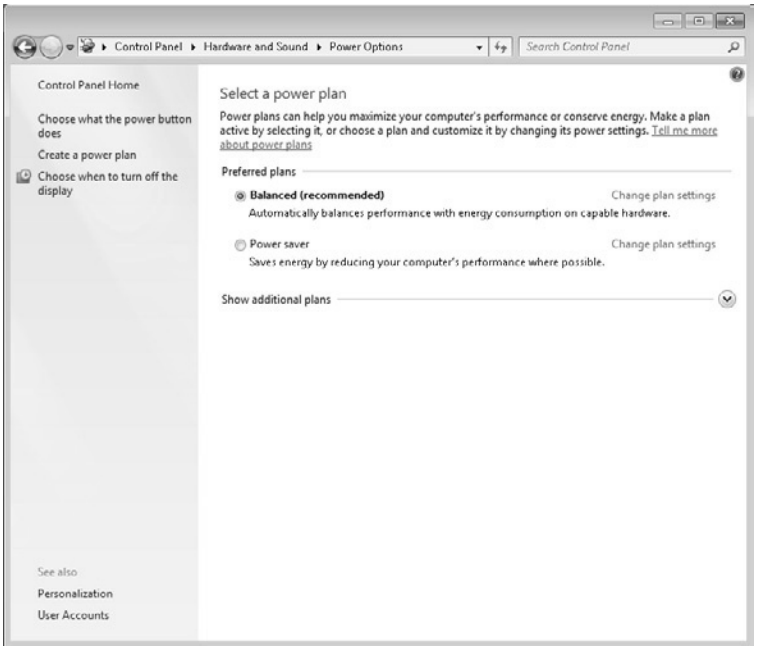


Figure 25-18 Windows 7 Power Options

By clicking Choose When To Turn Off The Display in the left panel, you open the Advanced Settings panel. Click Change Advanced Power Settings to change the power settings for a wide variety of Windows components (see Figure 25-19).

INSIDE OUT

Windows 7 on a laptop, netbook, or tablet

On a portable computer, the Power Options dialog box displays additional options by default, giving you much more control over power consumption and battery life.

www.it-ebooks.info



Figure 25-19 Advanced power management options

Sometimes a hard disk or network adapter doesn't function properly after being brought out of sleep. In the Power Options dialog box, you can disable settings such as Sleep and Hibernate modes for your PC.

You might also see a link in the Power Options dialog box to Change Settings That Are Currently Unavailable. Clicking this link will lead to more power options to choose from.

Disk Cleanup

Disk Cleanup is a useful utility that can delete temporary files and other items that can cause Windows to run slowly, including items in the Recycle Bin. Too many deleted files in the Recycle Bin can cause Windows 7 to slow down if you do not have much free hard disk space.

Advanced Tools

I wrote about Advanced Tools (see Figure 25-20) in Chapter 14, but in this section I go into more detail about what each tool does and how it can help you troubleshoot problems on your PC.

www.it-ebooks.info

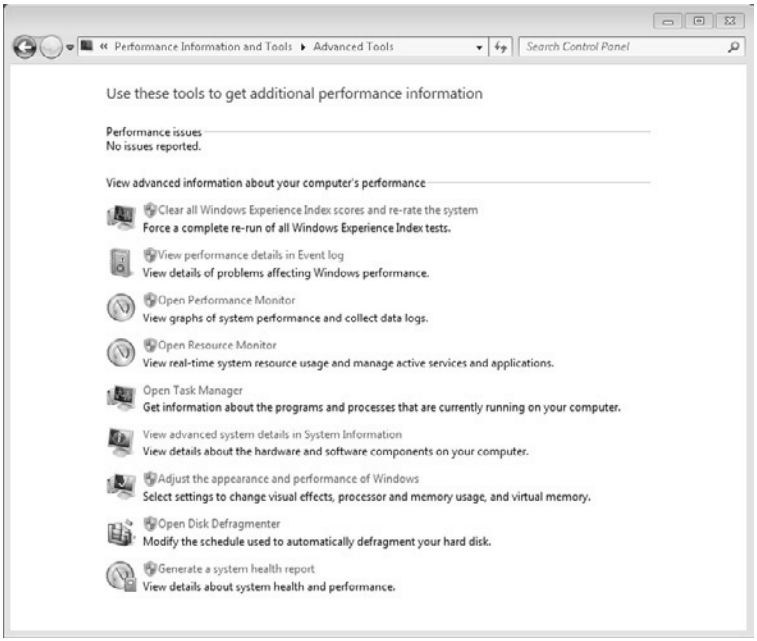


Figure 25-20 Advanced Tools

Event Log

You can read all about Event Log in the "Event Viewer" section earlier in this chapter.

Performance Monitor

By default, the Windows 7 Performance Monitor shows you only the current processor usage on your PC (see Figure 25-21). It's extremely customizable, however, and all sorts of other tools and features can be added to it.

By pressing the green plus (+) sign on the top toolbar, you can add counters to the Performance Monitor, and there are many to choose from (see Figure 25-22).

www.it-ebooks.info

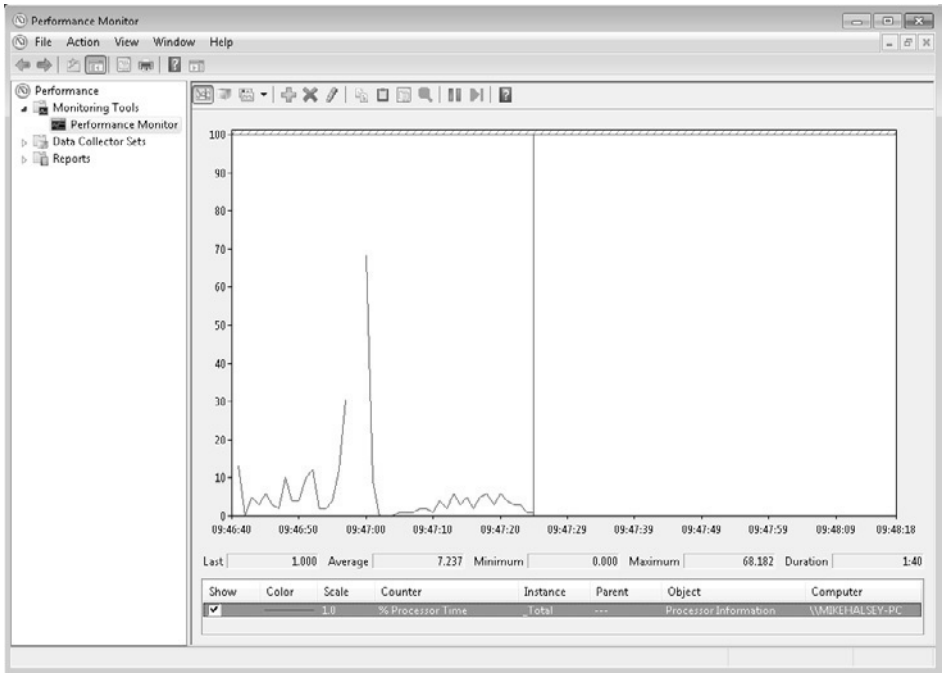


Figure 25-21 Performance Monitor

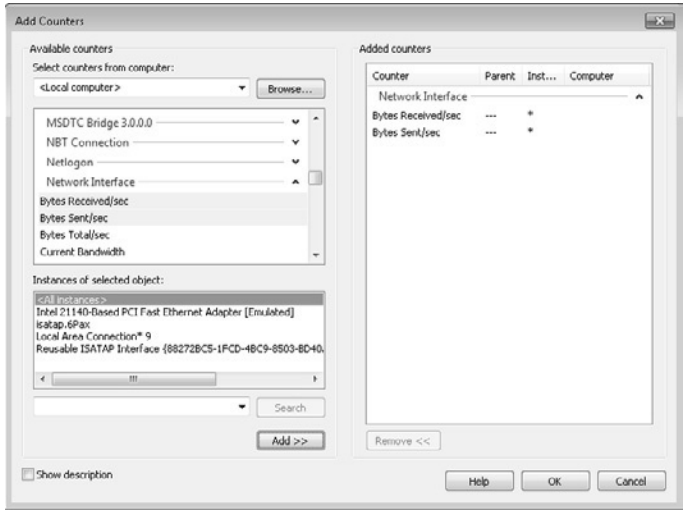


Figure 25-22 Adding counters to Performance Monitor

www.it-ebooks.info

Some of the most useful counters you can add are for the network interface. One of the glaring omissions from Windows over the years has been any kind of useful and easy-to-access Internet traffic monitor. The network status monitor can tell you how much data is being sent and received, but the network traffic monitor in Task Manager, which presents the information more usefully as a graph, doesn't show Internet traffic.

By adding some of the network interface tools counters to Performance Monitor, you can see a better real-time interpretation of what is going on.

This graph view can be more useful than a numeric counter, because it makes it easier to see what effect different devices or software are having on your Internet connection.

The pen icon in the toolbar allows you to highlight one or more indicators on the graph to make them stand out.

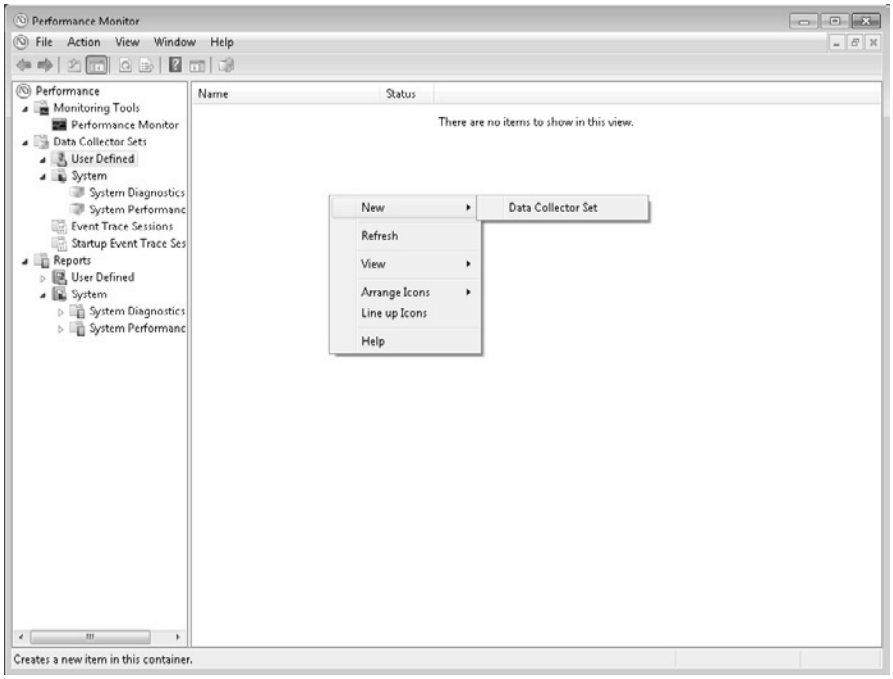
Data Collector Sets

You can save data from Performance Monitor as Data Collector Sets. These are accessed from the left pane in Performance Monitor and include predefined system and user-configurable options.

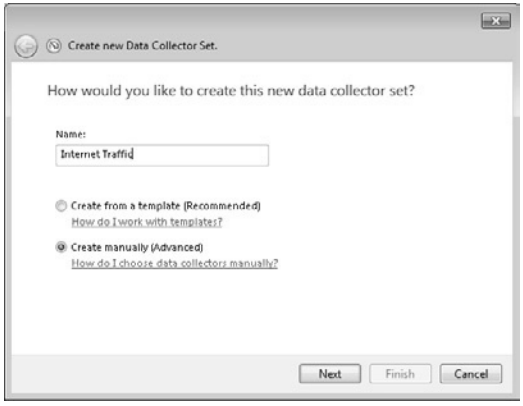
These can be exported to be viewed on another PC by a support technician or imported and viewed in Performance Monitor on your own PC. Data Collector Sets are invaluable in providing specific detail about parts of Windows 7 that cause problems.

1. In Performance Monitor, click Data Collector Sets and then User Defined in the left pane.
2. Right-click anywhere in the blank space in the main panel. Select New, and then select Data Collector Set from the context menu that appears.

www.it-ebooks.info

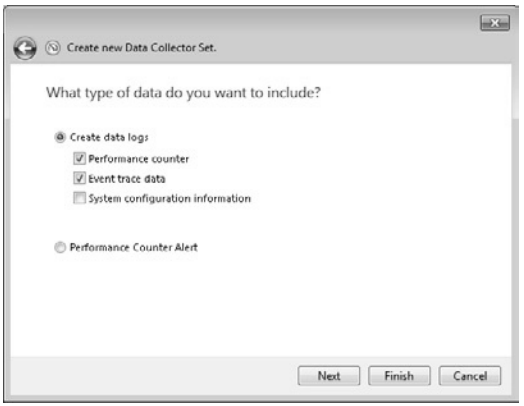


3. Choose to create your Data Collector Set from a template or to have more control by creating it manually.

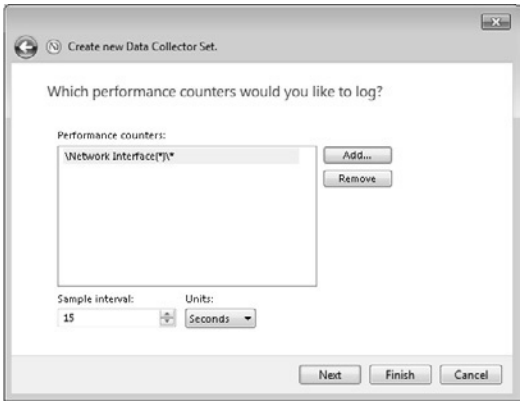


www.it-ebooks.info

4. Next, choose the type of information you want collected.

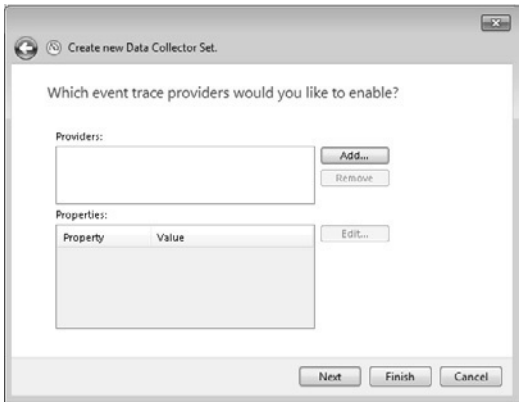


5. Now add specific counters to the Data Collector Set. Here I have added the networking monitors.

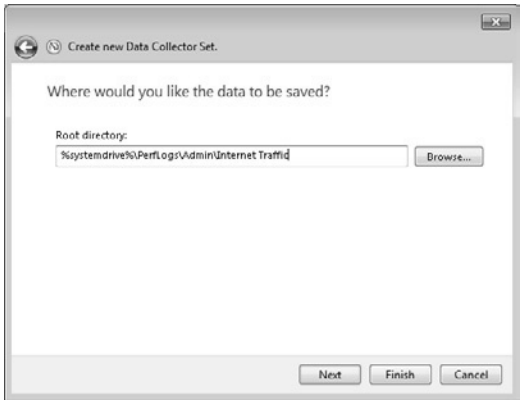


6. Optionally, add event logs to the Data Collector Set.

www.it-ebooks.info

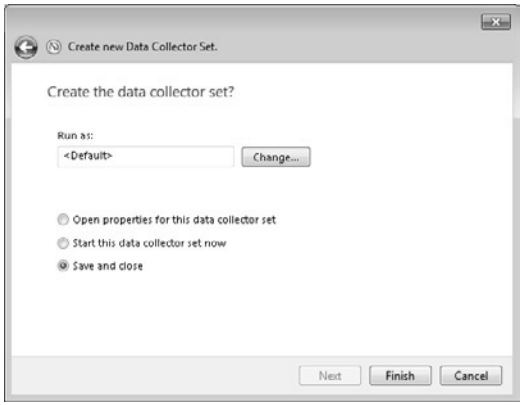


7. Choose a file name and storage location for the logs. This can be on your PC or on a network location.



8. Choose a user that the Data Collector Set runs as, or leave it as the default (current) user. Click Finish when you are done.

www.it-ebooks.info



Viewing Data Collector Sets

The Performance Logs for Windows 7, shown in Figure 25-23, are kept by default on the Windows drive under the *X*:\PerfLogs folder. Here you can find and either open the files to read or email them to a support person.

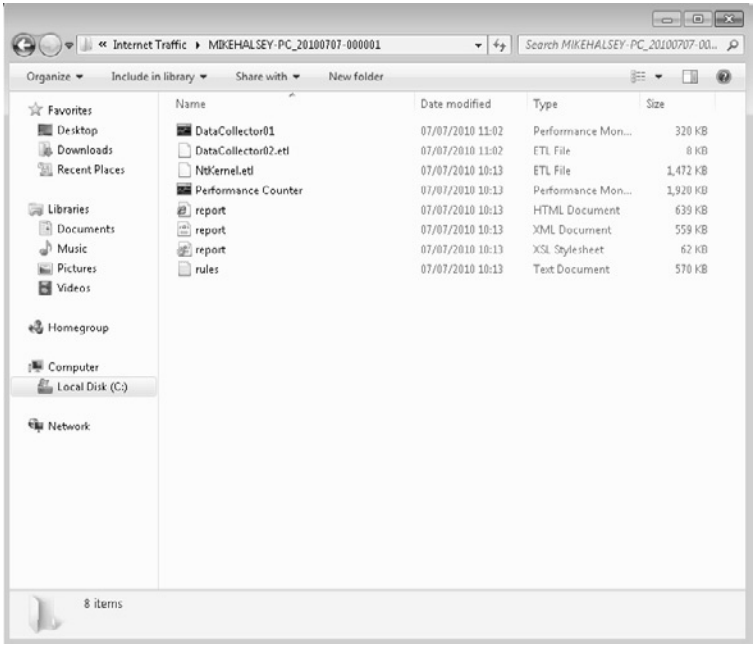


Figure 25-23 Accessing the custom Performance Logs

www.it-ebooks.info

Scheduling Data Collection

You can schedule data collection to occur at certain times and on certain days. You might, for instance, note that a particular problem tends to occur only on Mondays (when, say, the payroll is processed), so you can set the collection to run only on that day. Alternatively, if you are prone to leaving your computer on overnight, you may want to collect data only during working hours.

To do this, right-click your custom Data Collector Set, and select Properties. On the Schedule tab in the dialog box that appears, select the options for when you want data collected. This will open another dialog box (see Figure 25-24).

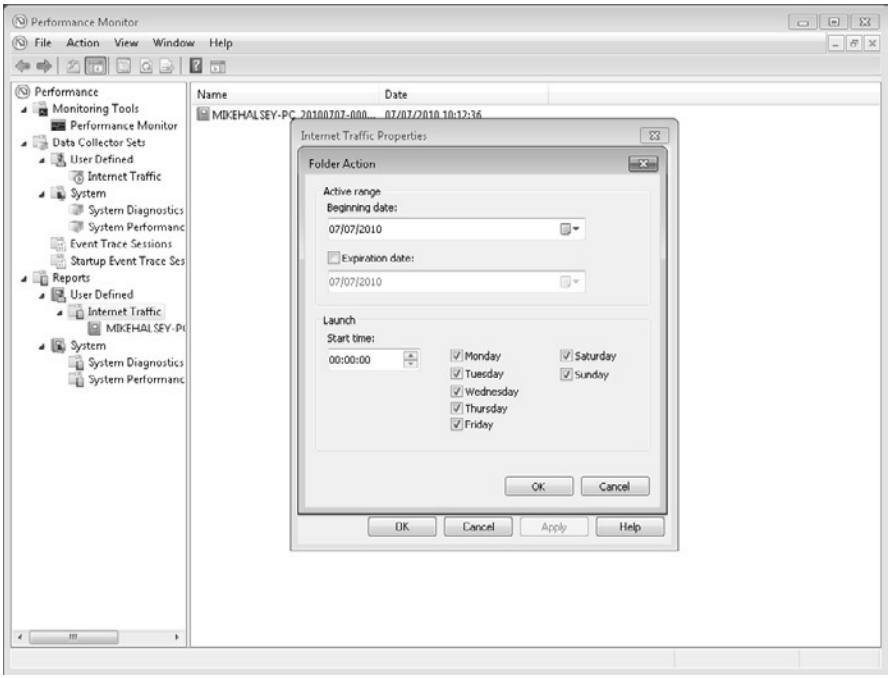


Figure 25-24 Scheduling Data Collector Sets

Resource Monitor

Resource Monitor enables you to view information about how your hardware and software are operating in real time. You can view data about specific Windows 7 processes or more general information.

www.it-ebooks.info

Across the top of Resource Monitor are five tabs: Overview, CPU, Memory, Disk, and Network (see Figure 25-25).

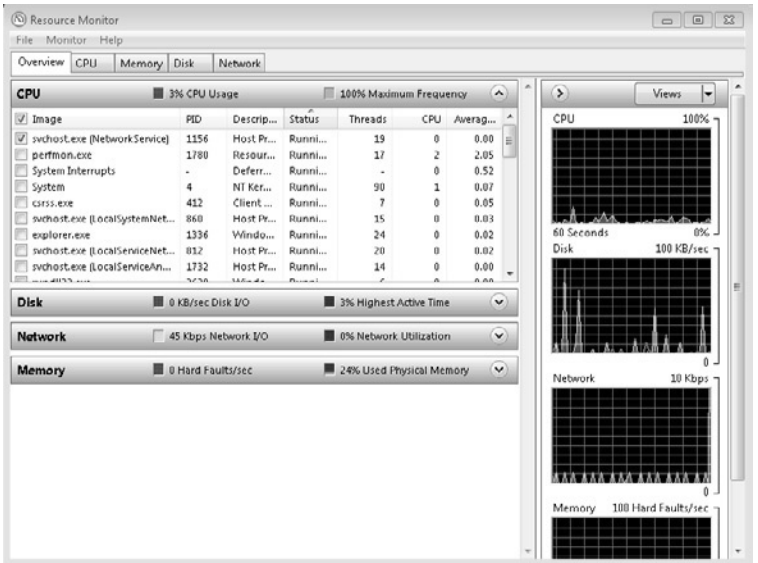


Figure 25-25 Windows 7 Resource Monitor

Each of these tabs provides general or specific information about every piece of hardware, software, or Windows component that is using a resource, complete with the details of how resource hungry it is.

Below the tabs are other collapsible panels providing more specific information in the context of the tab you have chosen.

Figure 25-26 shows an active Memory tab. You can see exactly what programs and Windows components are using the memory on the PC. The columns can be sorted and filtered by clicking them. This way, you can quickly find processes and programs that are being too greedy or consuming unnecessary resources.

www.it-ebooks.info

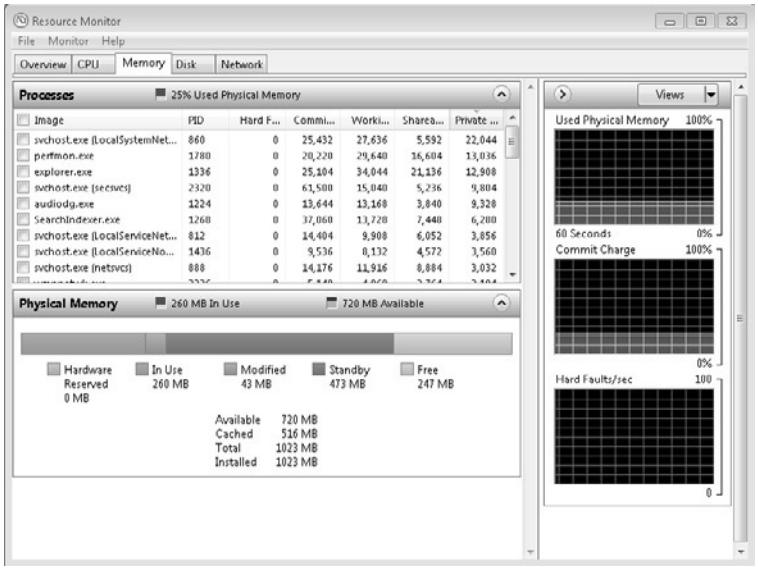


Figure 25-26 You can use Resource Monitor to find resource-hungry processes

Resource Monitor is especially useful for monitoring disk and network activity. On the Disk tab and the Memory tab, you can not only view programs and services that are using those resources, but you can see the throughput of data.

Resource Monitor offers additional functionality over Performance Monitor, because if there is a problem, you can easily see specifically what disk, program, network device, or process is causing the issue.

INSIDE OUT

Monitor specific processes and programs exclusively

In the main panel at the top of the Resource Monitor window are check boxes next to running programs and processes. If you need to monitor a specific one (or several), you can select the corresponding check boxes, and all the information in the other graphs and panels will change to show information about these selected items exclusively.

www.it-ebooks.info

Task Manager

Task Manager is not a tool I recommend using for troubleshooting. It provides a subset of the features found in Performance Monitor and Resource Monitor. However, it can be a useful and quick way to close faulty programs or processes.

System Information

The System Information panel (see Figure 25-27) provides a large amount of detailed information about your PC, your copy of Windows, and your system configuration. It can be especially useful if you suspect that something like a Windows Environment Variable (that is, the pointer to the Windows system folder) has become corrupt or has changed. You can also use it for diagnosing conflicts between hardware driver interrupt requests (IRQs).

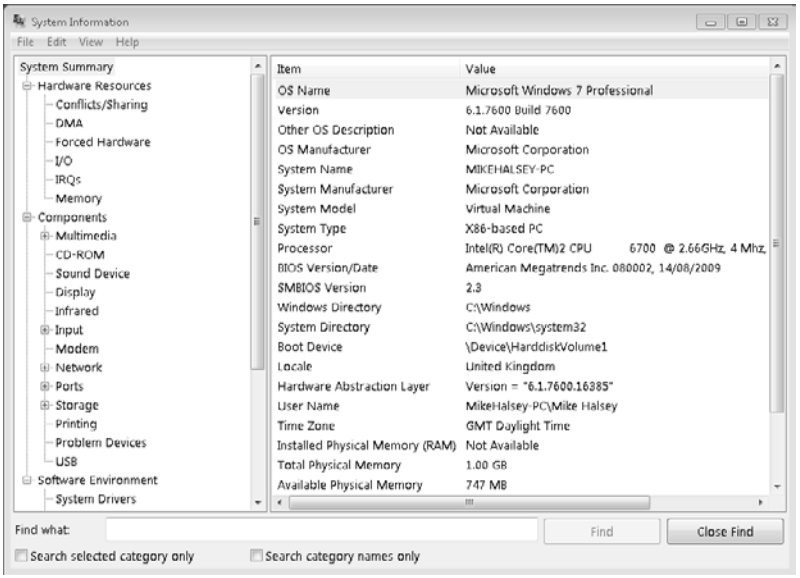


Figure 25-27 System Information

Appearance and Performance

Appearance and Performance was covered earlier in this chapter in the section entitled "Visual Effects."

Disk Defragmenter

With Disk Defragmenter, you can control and monitor the defragmenting of hard disks in your PC. Fragmentation is the splitting of files across the disk when there is not

www.it-ebooks.info

enough space to put the entire file in one place. This can slow down access to the file. Defragmenting brings all of the pieces of files back together for faster access.

Defragmenting and solid state disks

Because solid state disks (SSDs) are a random access technology based on silicon chips rather than on spinning disks, they do not need to be defragmented, and doing so will probably yield no performance benefit.

System Health Report

A system health report (see Figure 25-28), sometimes known as a system diagnostics report, brings together all of the information from Performance Information and Tools. It is described within Windows 7 as a tool that will:

Generate a report detailing the status of local hardware resources, system response times, and processes on the local computer along with system information and configuration data. This report includes suggestions for ways to maximize performance and streamline system operation.

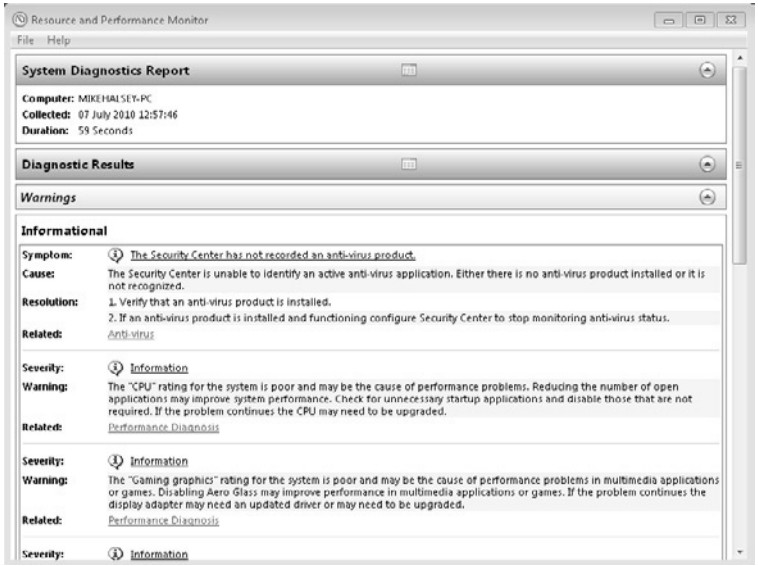


Figure 25-28 A system health report

www.it-ebooks.info

This report is long and complex, but it is broken into collapsible panel sections, each detailing a specific part of the PC's hardware or software system. This can make it very easy to find the detailed information you require.

INSIDE OUT Sending a system health report to a third party

In the File menu of the System Diagnostics Report dialog box, you can choose to either save the report as a file or to automatically send it via email if you have email client software (such as Microsoft Outlook) installed on your PC.

Control Panel Troubleshooters

Windows 7 has built-in troubleshooters that are much more useful than small help wizards to configure the odd option or two (see Figure 25-29). Access the troubleshooters by typing **troubleshooting** into the Start menu search box, by selecting Troubleshooting from the Action Center, or by selecting Troubleshooting when the Control Panel view is set to show all items (large or small icon views).

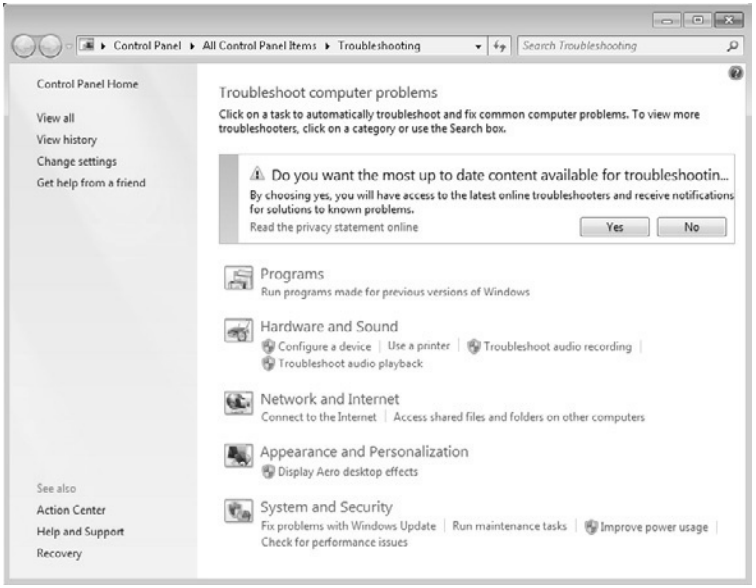


Figure 25-29 The Windows 7 Troubleshooting panel

www.it-ebooks.info

Although the Windows 7 troubleshooters can provide useful diagnostics for users, they are also extensible in two important ways.

First, as you can see in the example in Figure 25-29, they can be automatically updated over the Internet to provide new features and functionality.

Second, there is also the ability for corporate and business users to write their own trouble-shooting add-ins for this system.

The troubleshooters are organized into easy-to-use categories and are also searchable using the search box in the top right corner (see Figure 25-30 where I have searched for Internet-related troubleshooters).

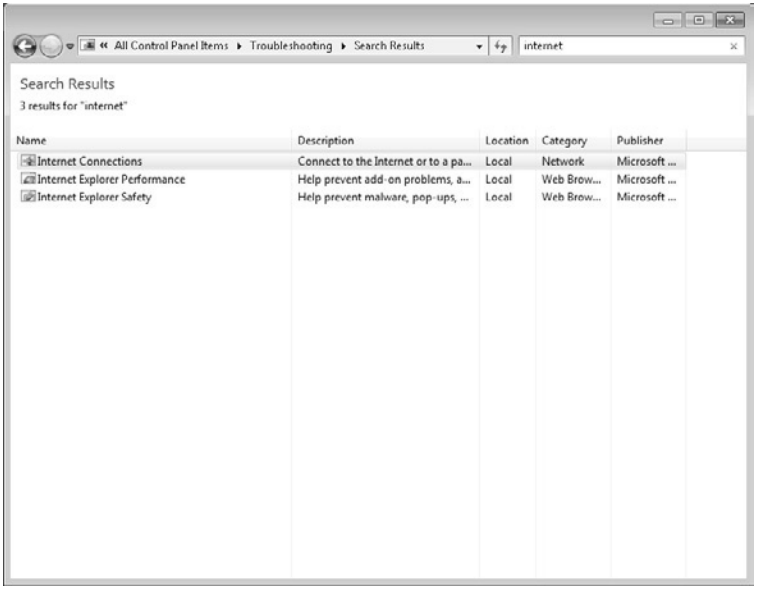


Figure 25-30 Searching for Internet-related troubleshooters

When you run a troubleshooter, you can select Advanced Options, which will appear as a check box in the bottom-left of the Troubleshooter dialog box. This will allow you to clear the option to have Windows 7 apply any repairs it deems necessary automatically, so that you can review them first. You can also optionally run the troubleshooter as an administrator.

If the troubleshooter cannot find a problem or a solution, you can click Explore Additional Options. As shown in Figure 25-31, the troubleshooter will guide you to sources of help and support online.

www.it-ebooks.info

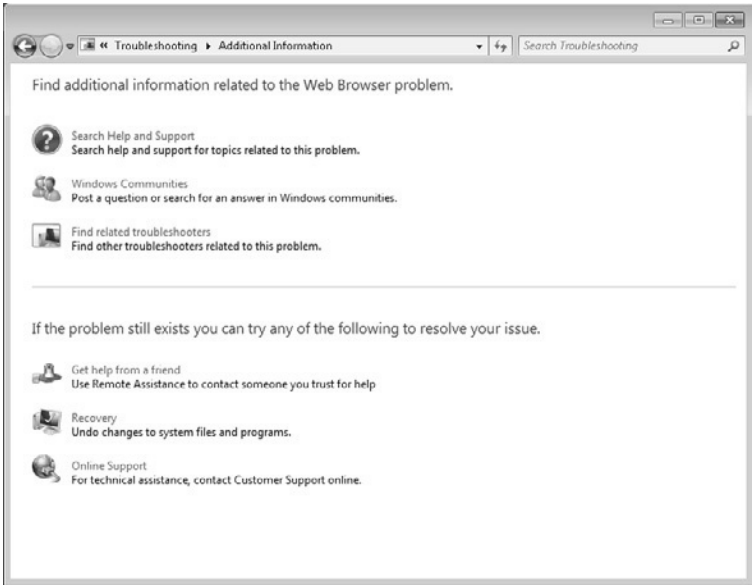


Figure 25-31 The Windows 7 troubleshooters can help you find advice elsewhere.

TROUBLESHOOTING

Not all the troubleshooters fix problems

It's worth noting that not all of the automated troubleshooters fix problems with Windows 7. Some, depending on the troubleshooter, will simply reset a Windows component to its default state.

Summary

The advanced diagnostic and troubleshooting tools in Windows 7 are innovative and, in parts, complex. All they can really do, however, is give you information on what is happening and where. You will need to rely on your own experience and intuition in most cases to interpret this information in a way that will enable you to diagnose and repair problems in Windows and with your PC.

Due to the size of the Windows ecosystem, with thousands of possible pieces of hardware and hundreds of thousands of software packages, it's simply beyond the scope of any automated system to be able to diagnose and fix everything.

www.it-ebooks.info

CHAPTER 26

Windows Firewall in Depth

Windows Firewall 401
Windows Firewall with Advanced Security. 403
Port Control for Routers 411
Summary 412

In Chapter 10, "Viruses, Malware, and Other Threats," I wrote about the online threats to a modern PC, how to identify and avoid them, and how to repair any harm done by them. In Chapter 10, I stressed that the biggest part of maintaining security on any PC is making sure that you are properly educated and informed about the threats and problems associated with carelessly clicking on links or opening files that could contain malicious software. Viruses, malware, and hackers can never gain access to a PC without user intervention. If users are careless about what they click online and which websites they visit, they may also be careless about maintaining their anti-virus and anti-malware protection, leaving it unattended and out of date. Careless users may even have no anti-virus protection at all.

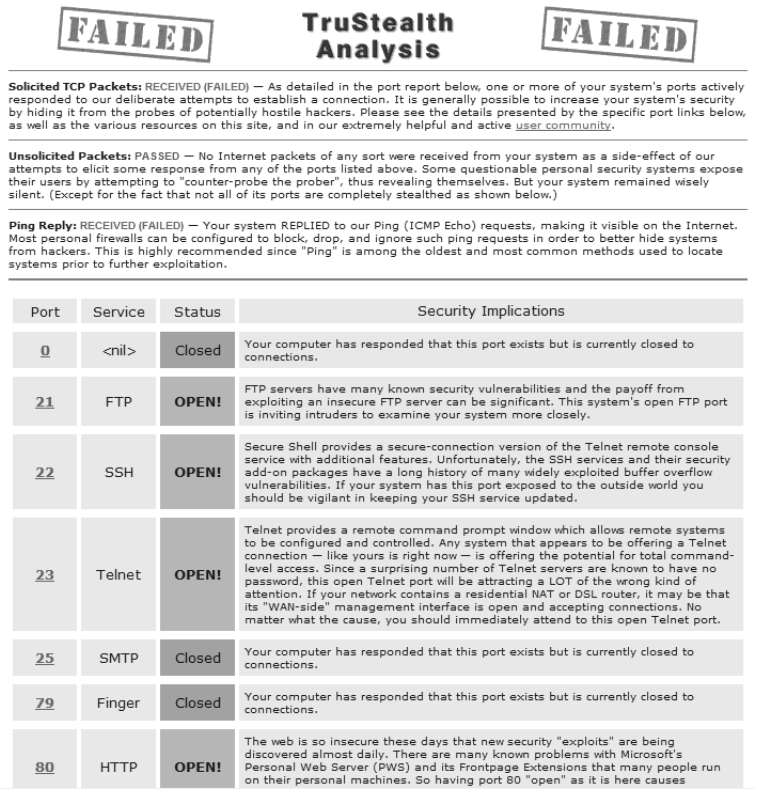
A common belief is that you *must* have third-party anti-virus, anti-malware, and firewall software with Windows. This thinking goes back to the early days of Windows XP and the first appearance of e-commerce. Originally, Windows XP didn't come with any protection at all, and, therefore, users were wide open to attack. Now things are different, especially where it concerns the firewall. Windows 7 includes a perfectly competent firewall as standard with all versions, and in this chapter I'll detail how you can use it to great effect to secure your PC.

Windows Firewall

Simply put, a firewall is a barrier between your PC and the outside world. It acts as a barrier that prevents software on your computer from communicating with the outside world, and it prevents the outside world from being able to access your computer. A good firewall protects your computer from even being detectable from the outside at all.

Figure 26-1 shows the results of a test done on my computer running only the standard Windows 7 Firewall in the standard configuration. You can see that the firewall successfully blocks some ports, but not all. The firewall in my Internet router provides an additional layer of support that hides the PC completely.

www.it-ebooks.info



FAILED

TruStealth Analysis

FAILED

Solicited TCP Packets: RECEIVED (FAILED) — As detailed in the port report below, one or more of your system's ports actively responded to our deliberate attempts to establish a connection. It is generally possible to increase your system's security by hiding it from the probes of potentially hostile hackers. Please see the details presented by the specific port links below, as well as the various resources on this site, and in our extremely helpful and active user community.

Unsolicited Packets: PASSED — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)

Ping Reply: RECEIVED (FAILED) — Your system REPLIED to our Ping (ICMP Echo) requests, making it visible on the Internet. Most personal firewalls can be configured to block, drop, and ignore such ping requests in order to better hide systems from hackers. This is highly recommended since "Ping" is among the oldest and most common methods used to locate systems prior to further exploitation.

Port	Service	Status	Security Implications
0	<nil>	Closed	Your computer has responded that this port exists but is currently closed to connections.
21	FTP	OPEN!	FTP servers have many known security vulnerabilities and the payoff from exploiting an insecure FTP server can be significant. This system's open FTP port is inviting intruders to examine your system more closely.
22	SSH	OPEN!	Secure Shell provides a secure-connection version of the Telnet remote console service with additional features. Unfortunately, the SSH services and their security add-on packages have a long history of many widely exploited buffer overflow vulnerabilities. If your system has this port exposed to the outside world you should be vigilant in keeping your SSH service updated.
23	Telnet	OPEN!	Telnet provides a remote command prompt window which allows remote systems to be configured and controlled. Any system that appears to be offering a Telnet connection — like yours is right now — is offering the potential for total command-level access. Since a surprising number of Telnet servers are known to have no password, this open Telnet port will be attracting a LOT of the wrong kind of attention. If your network contains a residential NAT or DSL router, it may be that its "WAN-side" management interface is open and accepting connections. No matter what the cause, you should immediately attend to this open Telnet port.
25	SMTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
79	Finger	Closed	Your computer has responded that this port exists but is currently closed to connections.
80	HTTP	OPEN!	The web is so insecure these days that new security "exploits" are being discovered almost daily. There are many known problems with Microsoft's Personal Web Server (PWS) and its Frontpage Extensions that many people run on their personal machines. So having port 80 "open" as it is here causes

Figure 26-1 A firewall test done at www.grc.com

This ShieldsUp! test provides an excellent assessment of your firewall, and you can find it online at *www.grc.com*, which is a site I've recommended elsewhere in this book.

You access Windows Firewall settings (see Figure 26-2) in the Security section of the Action Center or in Control Panel by clicking System And Security, and then clicking Windows Firewall.

www.it-ebooks.info

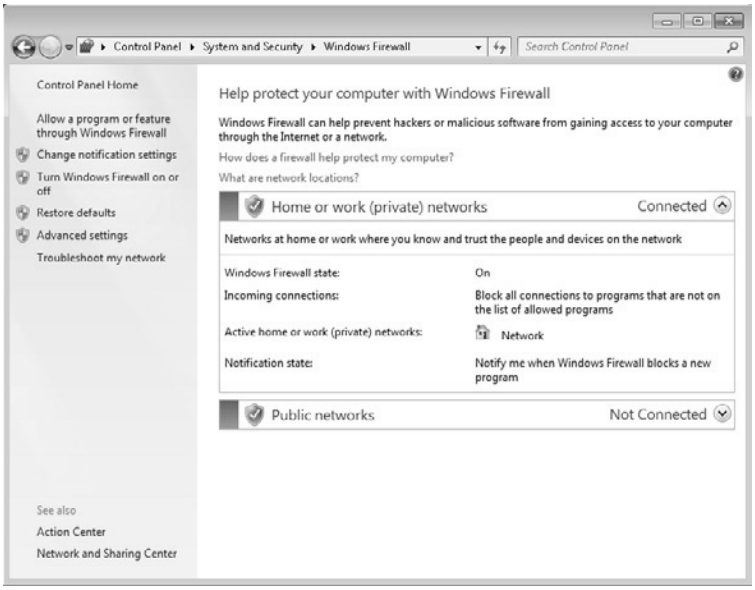


Figure 26-2 Windows Firewall

Windows Firewall with Advanced Security

The basic Windows Firewall settings include turning the firewall on and off and allowing a program through it. However, clicking Advanced Settings in the left pane opens the Windows Firewall With Advanced Security management panel (see Figure 26-3).

www.it-ebooks.info

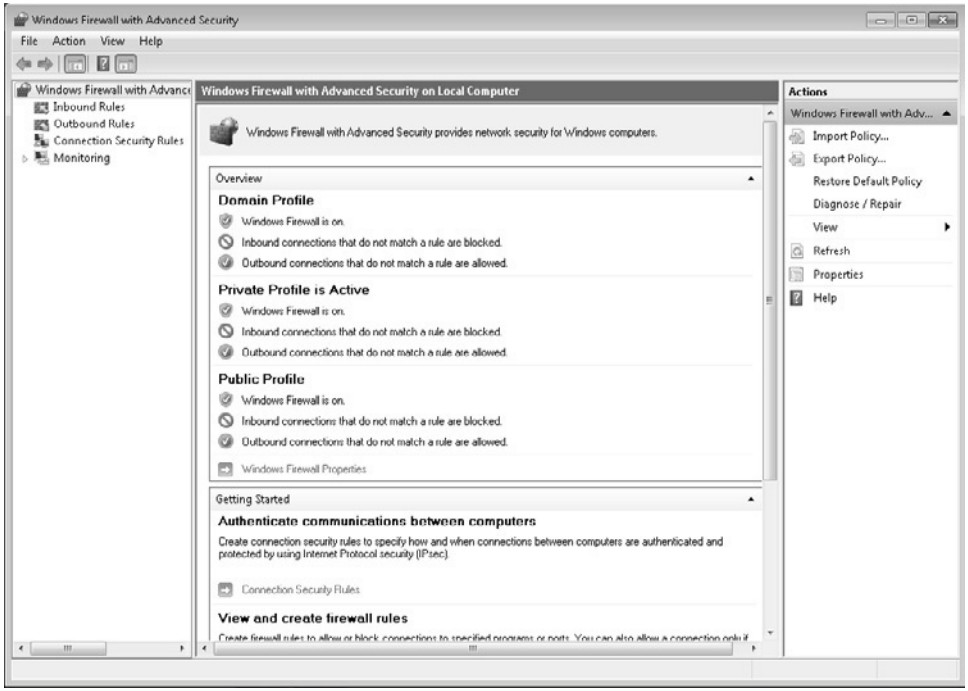


Figure 26-3 Windows Firewall with Advanced Security

By default, the main advanced firewall settings screen includes three panes of information and controls, just like any other management console in Windows 7. In the center pane is status information about the firewall, and below that are some quick links to help you set up advanced rules.

In the Actions pane on the right are links for working with advanced firewall policies once you've set them up. Here you can import and export firewall policies or reset the firewall to its default state if something has gone wrong or become corrupt. You can also use options in the Actions pane to launch the Windows 7 troubleshooters that are relevant to the Windows Firewall.

INSIDE OUT How to reset Windows Firewall

If something goes wrong with your firewall or the firewall settings become corrupt, you can reset it to the default state by clicking Restore Default Policy in the Actions pane on the right side of the Windows Firewall With Advanced Security management panel.

www.it-ebooks.info

Managing Firewall Rules

In the left pane of the Windows Firewall With Advanced Security management panel, you can manage inbound and outbound rules. Inbound rules cover connections that are made to your PC from your network or from the Internet. Outbound rules affect Windows software and your installed applications that may want to communicate with your network, the Internet, or other devices.

Clicking these links opens a list of existing rules. Quite a few of these rules deal with individual Windows components that need to communicate with the outside world, such as Windows Update.

The currently enabled rules are identified by a green check mark. If you want to turn a rule on or off, right-click it and select either Enable or Disable. To modify a rule, right-click it and select Properties (see Figure 26-4).

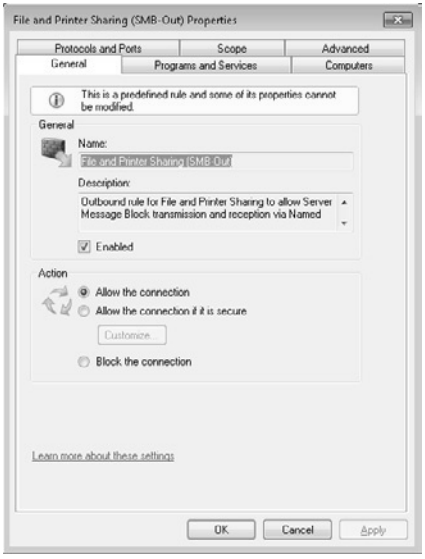


Figure 26-4 Managing the properties of a firewall rule

There are several tabs in a firewall rule Properties dialog box.

General

The General tab displays common information about the firewall rule with controls for switching it on and off or blocking the connection completely.

www.it-ebooks.info

A useful setting on this tab allows a connection only if that connection is secure. You can set the rule to allow a connection only if certain security measures are in place, such as an encrypted connection across a company network.

Program and Services

If the firewall rule applies to specific programs or Windows services, you can set and configure it on the Programs And Services tab.

Computers

The Computers tab is useful for controlling firewall connections on organization networks. Here you can limit the connection to certain computers on your network only.

Protocols and Ports

Your PC has 65,535 ports, each of which is a communications "doorway" into your PC. Some of these ports are reserved for specific functions, some are used by Internet and other communications software on your computer (some used exclusively by external hardware such as your router), and others are user-configurable.

The protocols these ports use to communicate vary, but the most common communication method is Transport Control Protocol and Internet Protocol (TCP/IP) used on the Internet.

In a business environment where your computer is connected to a server, you might want to open or block access to specific ports. Or, if you engage in online gaming or peer-to-peer file sharing, you sometimes have to open access to a specific port in Windows and/or in your router to allow communications access.

Scope

Similar to the Computers tab, the Scope tab is where you can limit access to or from specific IP addresses on your network and in the wider world.

Advanced

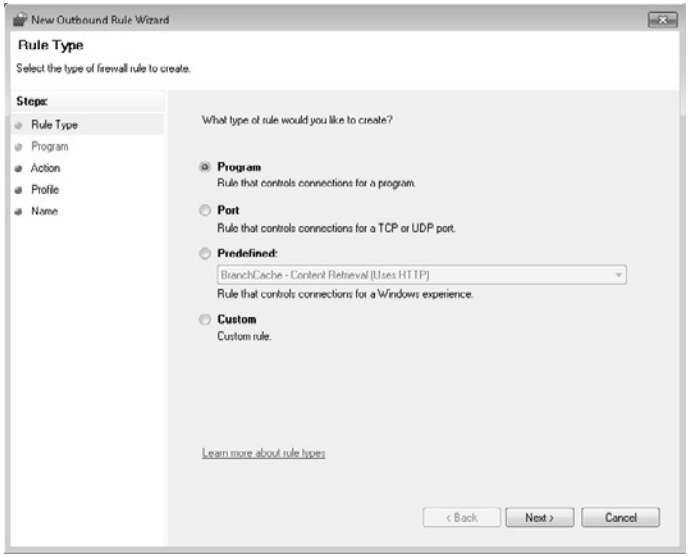
Finally, on the Advanced tab you can specify profiles to apply to a rule. For example, you can specify that a rule applies only when you are connected to a public network with a certain type of connection, such as a Wi-Fi connection.

Adding New Inbound or Outbound Firewall Rules

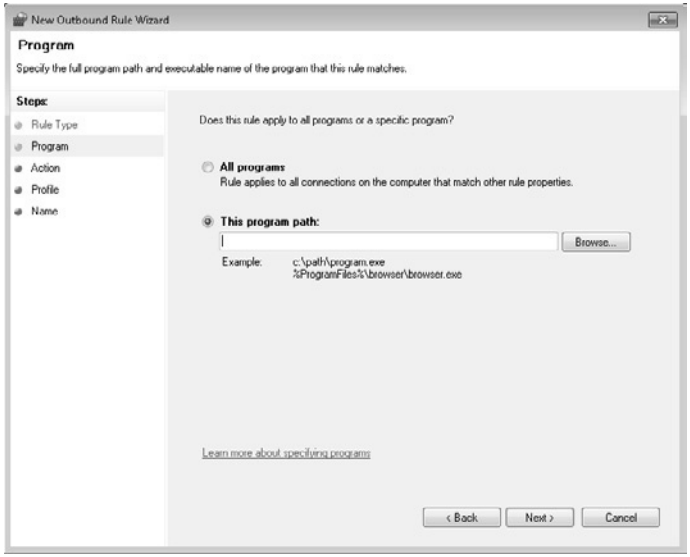
In the Inbound Rules or in the Outbound Rules section of the Windows Firewall With Advanced Security management panel, click New Rule in the Actions pane to create a new custom rule.

www.it-ebooks.info

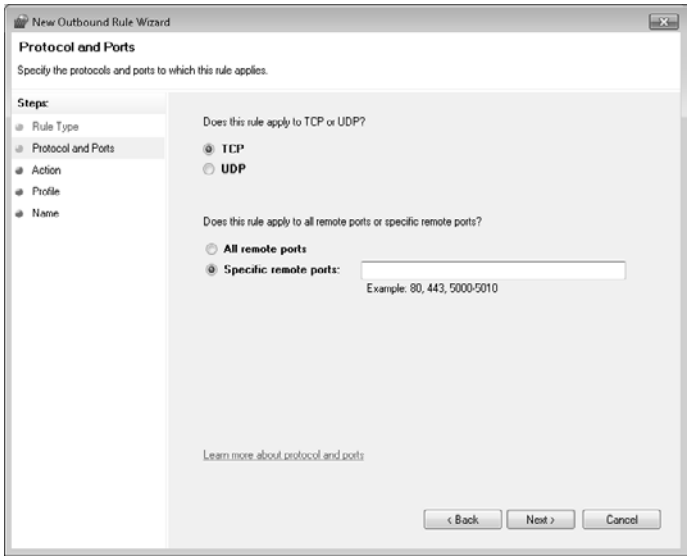
1. First, determine the type of firewall rule you want to create: a rule for a program, a port, or a Windows service.



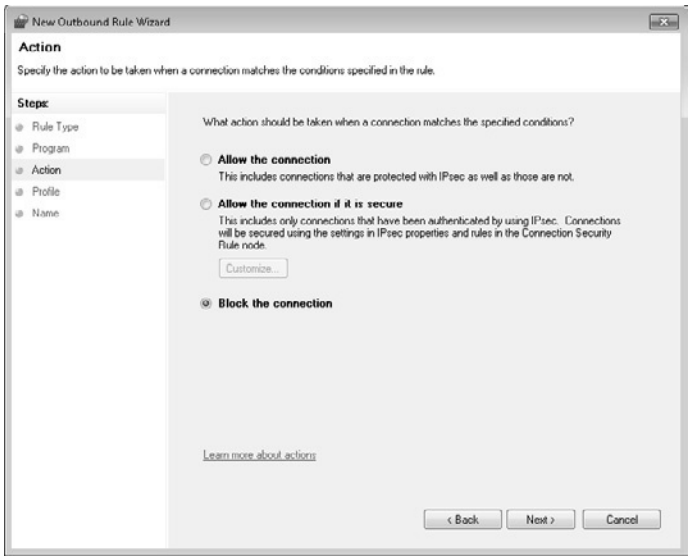
2. Next, specify the program, port, or service the rule applies to. The following two images show the options for programs and ports. These will be the most common types of rules you set.



www.it-ebooks.info

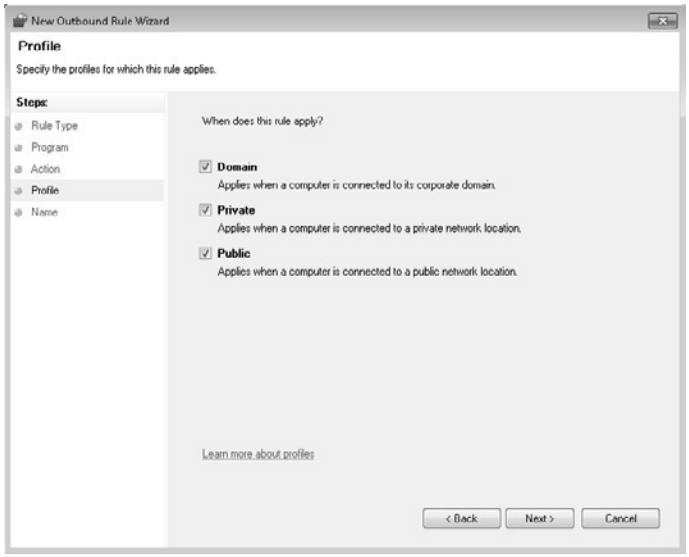


3. On the Action page, set the firewall action. Do you want to always allow this connection, allow it only if the connection is secure, or are you blocking it?

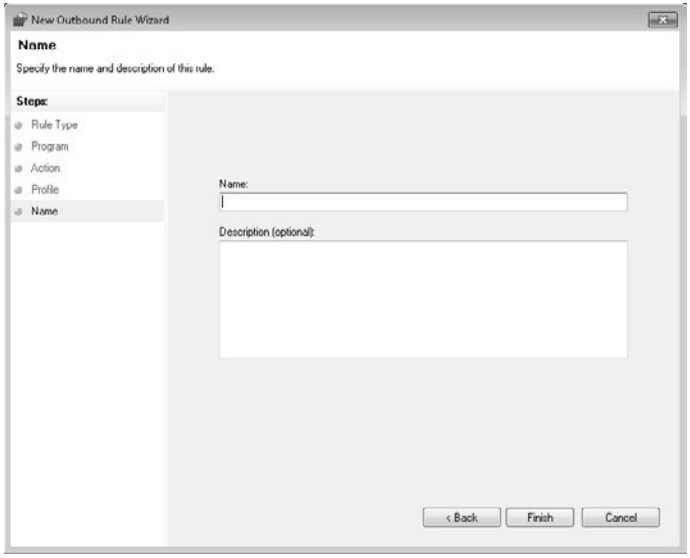


www.it-ebooks.info

4. On the Profile page, indicate what network types this connection applies to. Do you want it to apply to all network types or perhaps just the corporate network or public networks?



5. Finally, on the Name page, give the rule a name and, optionally, a description.



www.it-ebooks.info

Setting a Connection Security Rule

Below Incoming Rules and Outgoing Rules in the left pane of the Windows Firewall With Advanced Security management panel, you will find Connection Security Rules. You can use this feature to set new rules for controlling connections between your PC and other computers or servers (see Figure 26-5).

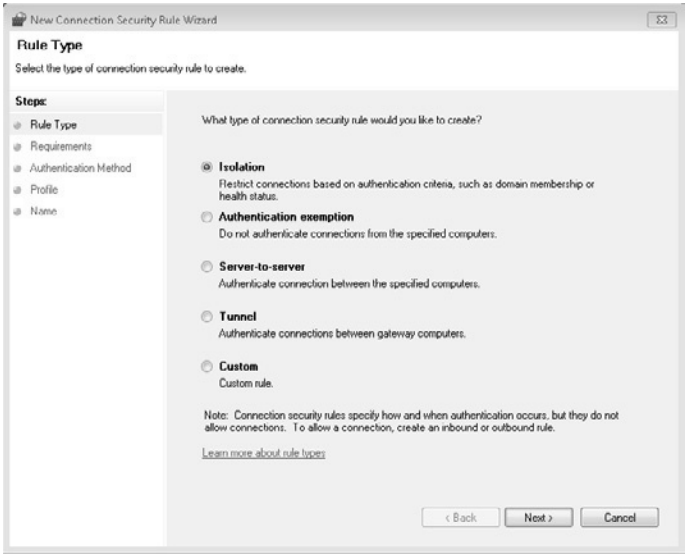


Figure 26-5 New Connection Security Rule Wizard

This feature can be very useful in any environment where security is essential. You can use it to set rules for a variety of scenarios, including office-bound PCs, PCs connected via virtual private networks (VPN), and other scenarios.

You can also use this feature to set a variety of authentication methods between two computers, including the use of root security certificates. Some options also let you select the encryption method(s) used to transmit data between computers.

Monitoring

Click Monitoring in the left pane of the Windows Firewall With Advanced Security management panel to access information on the current status of your firewall and any custom rules you have set up in it.

www.it-ebooks.info

More importantly, opening the Monitoring panel displays the results of the most recent activity of any particular firewall rule. You can check if the rule is working correctly (accessing the correct port, for example) and see what it is allowing through the firewall and what it is blocking.

Port Control for Routers

Some connection problems cannot be solved by using Windows Firewall to unblock access to specific ports if these ports are blocked by the router you use to connect to the Internet.

To see your router's firewall settings, you can log in to your router, typically by typing the address **192.168.1.1** or **192.168.2.1** into your web browser. Figure 26-6 shows a router with firewall options in the left pane. Under the Client IP Filters link, you can see the options to set or block port access for specific computers (IP addresses).

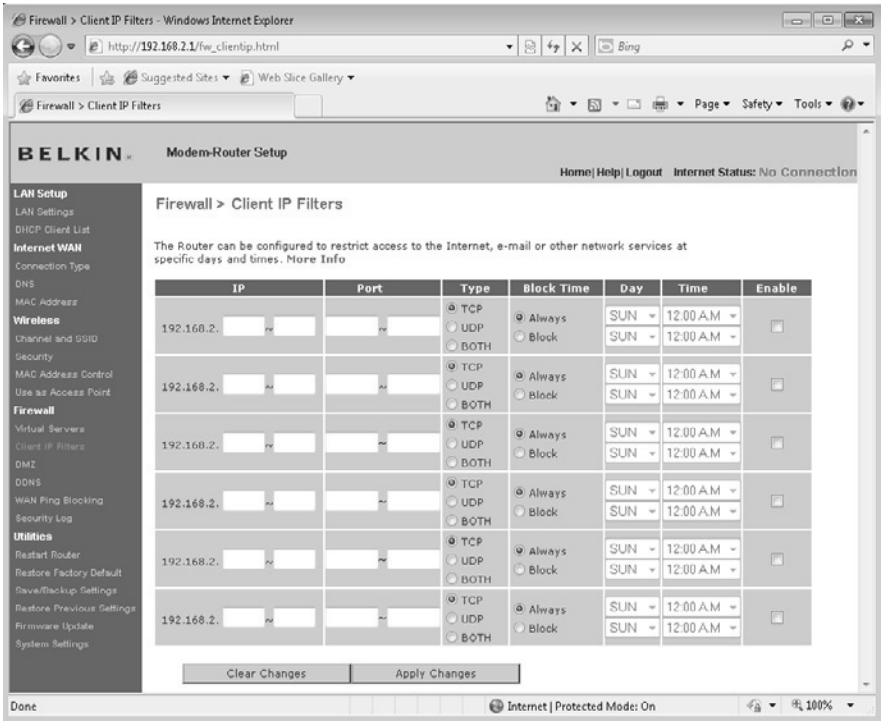


Figure 26-6 Router firewall control

www.it-ebooks.info

INSIDE OUT Troubleshooting router blocks

The router will assign your computer an IP address when it connects. This should always be the same, but sometimes the router assigns a different IP address for your computer, which can cause connection problems.

The router will have a section in its control panel where you can see the IP addresses for all the computers on your network. If you have previously set a port unblocking rule and it is not working, it is worth checking here to see if the IP address assigned to that rule still points to the correct PC.

Summary

Many people prefer to use a third-party firewall with Windows, and you might feel more comfortable doing so. However, even the most advanced Windows Firewall settings are easy to use and can provide all the control you need over your networking and Internet connection settings.

www.it-ebooks.info

CHAPTER 27

Advanced Registry Work

Registry Sections 414
Registry Keys and Settings 415
Backing Up and Restoring the Registry 416
Working with the Registry 416
Finding Information in the Windows Registry. 419
Summary 419

The registry is a database of settings and configuration options for Windows and all of your programs. In its description of the registry on the Microsoft support website, Microsoft describes the operation of the registry as follows.

The registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used.

You might occasionally need to change a setting for Windows or for a program that is contained within the registry, perhaps because an error has occurred and a program or Windows component is malfunctioning or because you are making (or undoing) a tweak to the operating system or a program to change its behavior or performance. If this is the case, you can access Registry Editor (see Figure 27-1) by typing **regedit** in the Start menu search box.

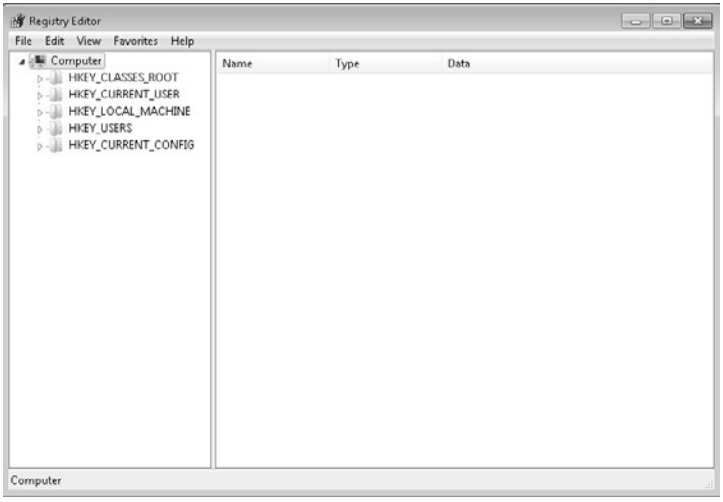


Figure 27-1 Windows Registry Editor

www.it-ebooks.info

Each user has an individual registry file called Ntuser.dat, which is a hidden file that's stored in the root of the user's C:\Users*UserName* folder.

Registry Sections

The registry is split into five different sections, two for the current user, two for the machine, and one for system startup.

HKEY_CLASSES_ROOT

HKEY_CLASSES_ROOT is a subkey of HKEY_LOCAL_MACHINE\Software. This section stores all of the information for registered applications, including file associations. This key is sometimes abbreviated as HKCR. If you write a registry key to HKEY_CLASSES_ROOT and the key already exists under HKEY_CURRENT_USER\Software\Classes, Windows will use the information stored in the HKEY_CURRENT_USER\Software\Classes as the master key instead.

HKEY_CURRENT_USER

The HKEY_CURRENT_USER section contains configuration options for the current user's profile, including the location pointers to the user's documents folders, display options, and Control Panel settings. This registry key is sometimes referred to as HKCU.

HKEY_LOCAL_MACHINE

The HKEY_LOCAL_MACHINE section of registry keys is the most commonly altered. It contains settings specific to the PC, including installed applications. It is sometime known as HKLM.

HKEY_USERS

The HKEY_USERS section in the registry contains keys that are subkeys corresponding to HKEY_CURRENT_USER. It stores information for each user profile that is actively loaded. It is sometimes known as HKU.

HKEY_CURRENT_CONFIG

HKEY_CURRENT_CONFIG includes information gathered at startup. Information and keys are stored here temporarily and are replaced when the PC is restarted.

www.it-ebooks.info

Registry Keys and Settings

There are different types of registry keys and settings. They are usually stored as binary, decimal, and hexadecimal numbers.

- **REG_BINARY** Raw binary data for storing hardware component information.
- **REG_DWORD** Data represented by a 4-**byte** number (32-bit integer). DWORDS are used as the parameters for many settings, including device drivers and software and configuration options.
- **REG_EXPAND_SZ** A variable length data string.
- **REG_MULTI_SZ** A multiple string, for example a list of multiple values in a format that people can read. These are usually separated by commas or spaces.
- **REG_SZ** A fixed-length text string.
- **REG_RESOURCE_LIST** A resource list in a series of nested arrays. These are used by device drivers.
- **REG_RESOURCE_REQUIREMENTS_LIST** An array list of hardware resources required by device drivers.
- **REG_FULL_RESOURCE_DESCRIPTOR** Nested arrays used to store resource lists for physical hardware devices.
- **REG_NONE** Data without any particular type.
- **REG_LINK** A Unicode string that names a symbolic link.
- **REG_QWORD** Data that is represented by a 64-bit integer.

> **Note**
> **In the same way that 64-bit versions of Windows 7 have two Program Files folders for 32-bit and 64-bit programs, the registry contains different sections for 64-bit registry keys. You can find these in HKEY_LOCAL_MACHINE\Software\WOW6432Node.**

www.it-ebooks.info

Backing Up and Restoring the Registry

Before you do any work in the registry, always back it up in case a change you make causes Windows 7 or one of your applications to become unstable or unresponsive. You can do this on the File menu in Registry Editor by selecting Export (see Figure 27-2).

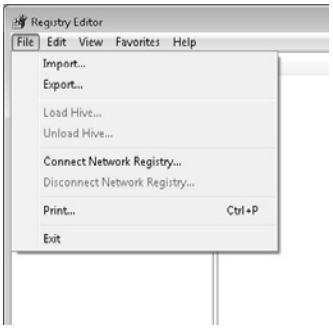


Figure 27-2 Backing up the Windows registry

You can restore the registry the same way.

> **Note**
>
> **If changes to the registry have made Windows 7 unresponsive, you might be able to boot into Safe Mode or use System Restore in the System Recovery options to restore the registry. See Chapter 11, "Easy Ways to Fix Windows 7," and Chapter 15, "Advanced Repair Methods," for more information on how to use System Restore and Safe Mode to rescue your PC.**

Working with the Registry

Using Registry Editor is just one way you can work with the registry. The following list describes some other methods.

- You can use Group Policies and Microsoft Management Console (MMC) to administer networks, your PC, services, or other operating system components.
- You can use .REG files, which contain registry keys that can be added to the registry by double-clicking to open and run them.

www.it-ebooks.info

- You can use VBScript or Jscript scripts directly with Windows Script Host.
- You can use Windows Management Instrumentation (WMI), an enterprise-based tool for managing the Windows operating system, to automate certain tasks.
- You can use the command line program Reg.exe in a command prompt window. Type **reg /?** to get a full list of supported commands. You will need to run the command window as an administrator.

Microsoft provides more information on using these methods online at *http://support.microsoft.com/kb/256986*.

Editing, Deleting, or Adding Registry Keys

Right-click any registry key to modify, rename, or delete it (see Figure 27-3).

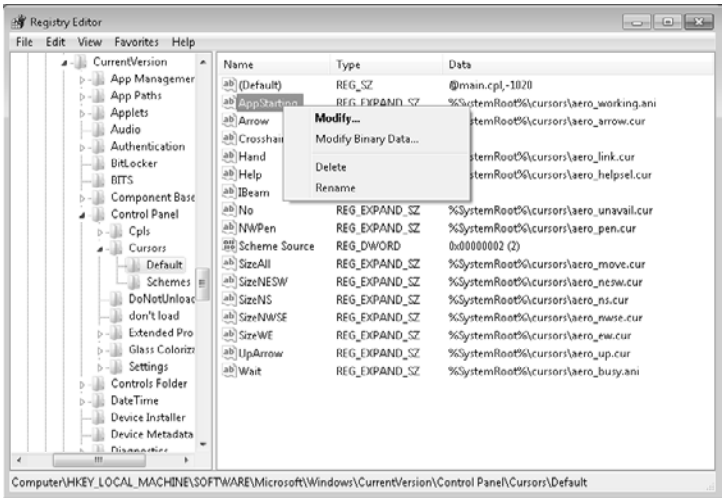


Figure 27-3 Editing or deleting a registry key

By right-clicking any blank space in the right pane of Registry Editor, you can create new registry keys of any type (see Figure 27-4).

www.it-ebooks.info

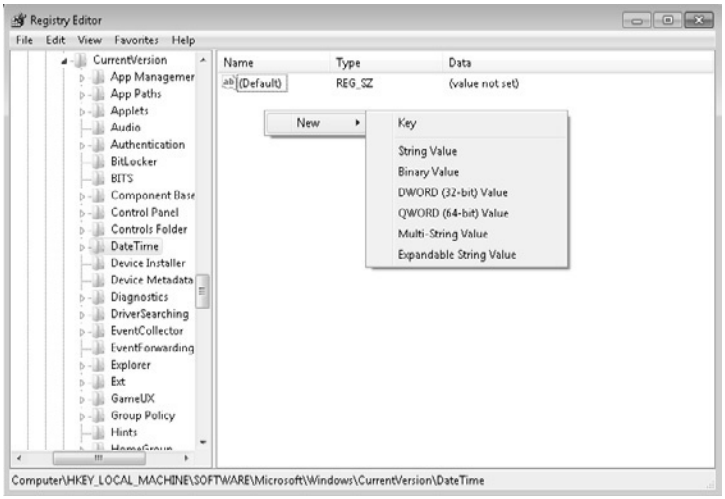


Figure 27-4 Adding a new registry key

Backing Up Specific Registry Keys

You can also back up specific registry keys, or sets of keys, in Registry Editor by right-clicking the folder in the left pane and selecting Export (see Figure 27-5). This will create a .reg file that you can later reimport to the same or to a different PC.

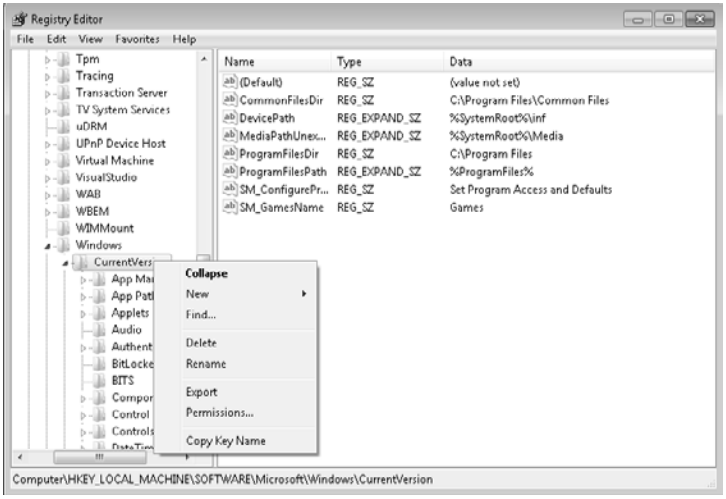


Figure 27-5 Backing up a specific registry key set

www.it-ebooks.info

Finding Information in the Windows Registry

Although the registry is large and complex, it is logically organized. You will find most of the Windows 7 settings, for instance, in the following key.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

Similarly, most of your software configuration options can be found in

HKEY_LOCAL_MACHINE\SOFTWARE

Registry keys are also sensibly named, so if you are looking for a specific setting, it is usually relatively simple to find.

CAUTION

You should always create a backup of the registry whenever you intend to work with it. Even the smallest, seemingly innocent change can cause Windows or one of your programs or hardware drivers to become unstable.

Summary

Precisely what you will want to change in the registry will depend entirely on what you are trying to do and whether it is with Windows 7, a hardware driver, or a software application. If you need more specific guidance on working with the registry, you can usually find a great deal of advice available via a quick search on the Internet. See Chapter 18, "Where to Find More Help and Support," for details about how to contact a help and support person.

www.it-ebooks.info

www.it-ebooks.info

PART 6

Appendices

APPENDIX A
Windows 7 Editions 423

APPENDIX B
Windows 7 Features by Edition 425

APPENDIX C
Windows 7 Shortcut Keys 431

APPENDIX D
BIOS Beep Codes 439

www.it-ebooks.info

www.it-ebooks.info

APPENDIX A

Windows 7 Editions

Edition	32-bit Memory Limit	64-bit Memory Limit	Availability	Notes
Windows 7 Starter	2 GB	—	System Builders Only	—
Windows 7 Home Basic	4 GB	8 GB	Emerging Markets Only	—
Windows 7 Home Premium	4 GB	16 GB	Retail/System Builders	—
Windows 7 Professional	4 GB	192 GB	Retail/System Builders	—
Windows 7 Enterprise	4 GB	192 GB	Volume Licensing	—
Windows 7 Ultimate	4 GB	192 GB	Retail/System Builders	—
Windows 7 N Editions*	4 GB	16 GB/ 192 GB*	European Union Only	As above but without Windows Media Player

*Windows N Editions include Windows 7 Home Premium N, Professional N, and Ultimate N

www.it-ebooks.info

www.it-ebooks.info

APPENDIX B

Windows 7 Features by Edition

User interface features	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
Windows Basic UI	Yes	Yes	Yes	Yes	Yes	Yes
Windows Standard UI	—	Yes	Yes	Yes	Yes	Yes
Aero Glass UI	—	—	Yes	Yes	Yes	Yes
Aero Peek	—	—	Yes	Yes	Yes	Yes
Aero Snap	Yes	Yes	Yes	Yes	Yes	Yes
Aero Shake	—	—	Yes	Yes	Yes	Yes
Live Taskbar Previews	—	Yes	Yes	Yes	Yes	Yes
Live Preview (Explorer)	—	—	Yes	Yes	Yes	Yes
Jumplists	Yes	Yes	Yes	Yes	Yes	Yes
Windows Flip	Yes	Yes	Yes	Yes	Yes	Yes
Windows Flip 3D	—	—	Yes	Yes	Yes	Yes
Windows Search	Yes	Yes	Yes	Yes	Yes	Yes

Bundled applications	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
Calculator	Yes	Yes	Yes	Yes	Yes	Yes
Games (Basic)	Yes	Yes	Yes	Hidden*	Hidden*	Yes
Games (Premium)	—	—	Yes	Hidden*	Hidden*	Yes
Microsoft Internet Explorer 8	Yes	Yes	Yes	Yes	Yes	Yes
Paint	Yes	Yes	Yes	Yes	Yes	Yes
Snipping Tool	—	—	Yes	Yes	Yes	Yes

www.it-ebooks.info

Bundled applications	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
Sticky Notes	—	—	Yes	Yes	Yes	Yes
Windows Fax and Scan	Yes	Yes	Yes	Yes	Yes	Yes
Windows Gadgets	Yes	Yes	Yes	Yes	Yes	Yes
Windows Journal	—	—	Yes	Yes	Yes	Yes
Windows PowerShell	Yes	Yes	Yes	Yes	Yes	Yes
WordPad	Yes	Yes	Yes	Yes	Yes	Yes
XPS Viewer	Yes	Yes	Yes	Yes	Yes	Yes

*Can be unhidden in Control Panel by clicking Programs and Features, and then clicking Windows Features

Digital media features	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
AAC and H.264	Yes	Yes	Yes	Yes	Yes	Yes
Device Stage	Yes	Yes	Yes	Yes	Yes	Yes
Dolby Digital	—	—	Yes	Yes	Yes	Yes
DVD Playback	Can be Added	Can be Added	Yes	Yes	Yes	Yes
MPEG-2 Decoding	—	—	Yes	Yes	Yes	Yes
Sync Center	Yes	Yes	Yes	Yes	Yes	Yes
TV Tuners Supported	—	—	4	4	4	4
Windows DVD Maker	—	—	Yes	Yes	Yes	Yes
Windows Photo Viewer	Yes	Yes	Yes	Yes	Yes	Yes
Windows Media Center	—	—	Yes	Yes	Yes	Yes
Windows Media Player 12	Yes	Yes	Yes	Yes	Yes	Yes
Windows Media Player - Remote Media Experience	—	—	Yes	Yes	Yes	Yes

www.it-ebooks.info

Security features	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
Action Center	Yes	Yes	Yes	Yes	Yes	Yes
Bitlocker	—	—	—	—	Yes	Yes
Bitlocker To Go	—	—	—	—	Yes	Yes
DEP	Yes	Yes	Yes	Yes	Yes	Yes
Encrypting File System	—	—	—	—	Yes	Yes
Fast User Switching	—	Yes	Yes	Yes	Yes	Yes
IE 8 Protected Mode	Yes	Yes	Yes	Yes	Yes	Yes
Parental Controls	Yes	Yes	Yes	Yes	Yes	Yes
UAC	Yes	Yes	Yes	Yes	Yes	Yes
Windows Defender	Yes	Yes	Yes	Yes	Yes	Yes
Windows Firewall	Yes	Yes	Yes	Yes	Yes	Yes
Windows Update	Yes	Yes	Yes	Yes	Yes	Yes

Performance features	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
64-Bit Processor Support	Yes	Yes	Yes	Yes	Yes	Yes
Maximum RAM (32-Bit)	2Gb	4Gb	4Gb	4Gb	4Gb	4Gb
Maximum RAM (64-Bit)	—	8Gb	16Gb	192Gb	192Gb	192Gb
Physical Processor Support	1	1	1	2	2	2
Processor Core Support	No Limit	No Limit	No Limit	No Limit	No Limit	No Limit
Superfetch	Yes	Yes	Yes	Yes	Yes	Yes
Windows ReadyDrive	Yes	Yes	Yes	Yes	Yes	Yes
Windows ReadyBoost	Yes	Yes	Yes	Yes	Yes	Yes

www.it-ebooks.info

Reliability features	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
Backup	Yes	Yes	Yes	Yes	Yes	Yes
Back to Network	—	—	Yes	Yes	Yes	Yes
Disk Defragmenter	Yes	Yes	Yes	Yes	Yes	Yes
Previous Versions	Yes	Yes	Yes	Yes	Yes	Yes
Problem Steps Recorder	Yes	Yes	Yes	Yes	Yes	Yes
System Image	Yes	Yes	Yes	Yes	Yes	Yes
System Rescue	Yes	Yes	Yes	Yes	Yes	Yes
System Restore	Yes	Yes	Yes	Yes	Yes	Yes

Networking features	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
Ad-Hoc Network Support	Yes	Yes	Yes	Yes	Yes	Yes
Connect to a Projector	Yes	Yes	Yes	Yes	Yes	Yes
Homegroup	Join Only	Join Only	Yes	Yes	Yes	Yes
IIS Web Server	—	—	Yes	Yes	Yes	Yes
Network Bridge	—	Yes	Yes	Yes	Yes	Yes
Network and Sharing Center	Yes	Yes	Yes	Yes	Yes	Yes
Offline Files	—	—	Yes	Yes	Yes	Yes
Remote Desktop	Yes	Yes	Yes	Yes	Yes	Yes
Remote Desktop Host	—	—	Yes	Yes	Yes	Yes
RSS Support	Yes	Yes	Yes	Yes	Yes	Yes
SMB Connections	20	20	20	20	20	20

www.it-ebooks.info

Mobility features	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
Improved Power Management	Yes	Yes	Yes	Yes	Yes	Yes
Mobility Center	—	Yes	Yes	Yes	Yes	Yes
Sync Center	Yes	Yes	Yes	Yes	Yes	Yes

Enterprise features	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
AppLocker	—	—	—	—	Yes	Yes
BranchCache	—	—	—	—	Yes	Yes
DirectAccess	—	—	—	—	Yes	Yes
Domain Join	—	—	—	Yes	Yes	Yes
Federated Search	—	—	—	—	Yes	Yes
Location-Aware Printing	—	—	—	Yes	Yes	Yes
Multi-Language Packs	—	—	—	—	Yes	Yes
Subsystem for UNIX	—	—	—	—	Yes	Yes

Other features	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
Boot from VHD	—	—	—	—	Yes	Yes
Create and Attach a VHD	Yes	Yes	Yes	Yes	Yes	Yes
Libraries	Yes	Yes	Yes	Yes	Yes	Yes
Multi-Touch Support	—	—	Yes	Yes	Yes	Yes
Tablet PC Functionality	—	—	Yes	Yes	Yes	Yes
Windows Sideshow	—	—	Yes	Yes	Yes	Yes
Windows XP Mode (via Add-In)			Yes	Yes	Yes	Yes

www.it-ebooks.info

www.it-ebooks.info

APPENDIX C

Windows 7 Shortcut Keys

Windows 7 provides many shortcut keys to help you complete tasks faster and save you time. Many applications also use the same shortcut keys. Of course, any application can include additional shortcuts to its own unique features.

Table C-1 General keyboard shortcuts

Task	Shortcut Key(s)
Copy selected item	Ctrl+C
Cut selected item	Ctrl+X
Paste cut or copied text or item(s) to current folder	Ctrl+V
Undo the most recent action	Ctrl+Z
Delete selected icon(s) and move to Recycle Bin	Delete or Del
Delete selected icons(s) without moving to Recycle Bin	Shift+Delete
Rename selected icon(s)	F2
Extend selection through additional icons	Shift+*any arrow key*
Select all items in a document or window	Ctrl+A
Search for a file or folder	F3
Display properties for selected icon	Alt+Enter
Close program in the active window	Alt+F4
Open the shortcut menu for the active window	Alt+Spacebar
Close the active document in multiple document program	Ctrl+F4
Show Flip 3D	~WS+Tab
Switch between open programs	Alt+Tab
Cycle through open programs in the order they were opened	Alt+Esc
Cycle through screen elements on the desktop or in a window	F6
Display the shortcut menu for the selected item	Shift+F10
Open/close the Start menu	Ctrl+Esc or ~WS
Open menu option or perform menu command	Alt+underlined letter
View menu bar in active program	F10 or Alt
Move left or right in menu bar	← and →

www.it-ebooks.info

Task	Shortcut Key(s)
Move up or down in menu	↑ and ↓
Select highlighted menu command	Enter
Refresh the active window	F5
View the folder one level up in Windows Explorer	Backspace
Cancel the current task	Esc
Open Task Manager	Ctrl+Shift+Esc
Copy dragged item to destination	Ctrl+*drag*
Move dragged item to destination	Ctrl+Shift+*drag*

Table C-2 Dialog box keyboard shortcuts

Task	Shortcut Key(s)
Choose option with underlined *letter*	Alt+*letter*
Select a button if the active option is a group of option buttons	Arrow keys …
Open a folder one level up if a folder is selected in the Save As or Open dialog box	Backspace
Go to previous tab	Ctrl+Shift+Tab
Go to next tab	Ctrl+Tab
Same as clicking OK	Enter
Same as clicking Cancel	Esc
Help	F1 key
Display the items in the active list	F4 key
Move to previous option	Shift+Tab
Select or deselect the check box	Spacebar
Move to next option	Tab

Table C-3 Windows Explorer keyboard shortcuts

Task	Shortcut Key(s)
Collapse the selected folder	– on numeric keypad
Display all the subfolders under selected folder	* on numeric keypad
Select or collapse parent folder	←

www.it-ebooks.info

Task	Shortcut Key(s)
Expand current folder or move to next subfolder	↓
Display the contents of the selected folder	+ on numeric keypad
Display the bottom of the active window	End
Display the top of the active window	Home
Open selected folder in new instance	Shift+Double-Click

Table C-4 Ease of Access keyboard shortcuts

Task	Shortcut Key(s)
Open Ease of Access Center	~WS+U
Switch the MouseKeys either on or off	Left Alt+Left Shift+Num Lock
Switch High Contrast either on or off	Left Alt+Left Shift+Print Screen
Switch ToggleKeys either on or off	Num Lock for five seconds
Switch FilterKeys either on or off	Right Shift for eight seconds
Switch StickyKeys either on or off	Shift five times

Table C-5 Windows Help keyboard shortcuts

Task	Shortcut Key(s)
Open Windows Help and Support	F1 or ~WS+F1
Display the Table of Contents	Alt+C
Display the Connection Settings menu	Alt+N
Display the Options menu	F10
Move back to the previously viewed topic	Alt+←
Move forward to the next (previously viewed) topic	Alt+↓
Display the Customer Support page	Alt+A
Display the Help home page	Alt+Home
Move to the beginning of a topic	Home
Move to the end of a topic	End
Search the current topic	Ctrl+F
Print a topic	Ctrl+P
Move to the Search box	F3

www.it-ebooks.info

Table C-6 Microsoft Natural Keyboard shortcuts

Task	Shortcut Key(s)
Display or hide the Start menu	~WS
Lock the computer	~WS+L
Display the System Properties dialog box	~WS+Break
Show the desktop	~WS+D
Open Computer folder	~WS+E
Search for file or folder	~WS+F
Search for computers	Ctrl+~WS+F
Display Windows Help	~ F1
Minimize all the windows	~WS+M
Restore all minimized windows	~WS+Shift+M
Open the Run dialog box	~WS+R
Show Flip 3D	~WS+Tab
Open Ease of Access Center	~WS+U
Open Windows Mobility Center	~WS+X

Table C-7 Text navigation and editing shortcuts

Task	Shortcut Key(s)
Move cursor down one line	↓
Move cursor left one character	←
Move cursor right one character	→
Move cursor up one line	↑
Delete character to left of cursor	Backspace
Move cursor to start of next paragraph	Ctrl+↓→
Move cursor to start of previous paragraph	Ctrl+↑
Move cursor to start of previous word	Ctrl+←
Move cursor to start of next word	Ctrl+→↓
Select all	Ctrl+A
Copy to Clipboard	Ctrl+C
Copy the selected text to destination	Ctrl+*drag*
Select to end of paragraph	Ctrl+Shift+→
Select to end of word	Ctrl+Shift+Æ
Select to beginning of word	Ctrl+Shift+←

www.it-ebooks.info

Task	Shortcut Key(s)
Select to beginning of paragraph	Ctrl+Shift+↑
Select to end of document	Ctrl+Shift+End
Select to top of document	Ctrl+Shift+Home
Paste Clipboard contents to cursor position	Ctrl+V
Cut to Clipboard	Ctrl+X
Undo last action	Ctrl+Z
Delete selected text or character at cursor	Del
Cancel the current task	Esc
Select to character in line above	Shift+↑
Select to character in line below	Shift+↓→
Select character to left	Shift+←
Select character to right	Shift+→↓
Select from cursor to here	Shift+Click
Select to end of line	Shift+End
Select to beginning of line	Shift+Home
Select text down one screen	Shift+Page Down
Select text up one screen	Shift+Page Up

Table C-8 Microsoft Internet Explorer shortcuts

Task	Shortcut Key(s)
Add "www." to the beginning and ".com" to the end of text in address bar	Ctrl+Enter
Add the current page to Favorites	Ctrl+D
Click the Information bar	Spacebar
Close current tab (or the current window if tabbed browsing is disabled)	Ctrl+W
Close other tabs	Ctrl+Alt+F4
Close Print Preview	Alt+C
Close the current window (if you have only one tab open)	Ctrl+W
Copy selection to Clipboard	Ctrl+C
Display a list of addresses you've typed	F4
Display a shortcut menu for a link	Shift+F10
Display first page to be printed	Alt+Home
Display last page to be printed	Alt+End

www.it-ebooks.info

Task	Shortcut Key(s)
Display next page to be printed	Alt+↓
Display previous page to be printed	Alt+←
Display zoom percentages	Alt+Z
Find on this page	Ctrl+F
Go to home page	Alt+Home
Go to selected link	Enter
Go to the next page	Alt+↓
Go to the previous page	Alt+← or Backspace
Go to the Toolbar Search box	Ctrl+E
Help	F1
Move back through the items on a web page, the address bar, or the links bar	Shift+Tab
Move back through the list of AutoComplete matches	→
Move backward between frames (if tabbed browsing is disabled)	Ctrl+Shift+Tab
Move focus to the Information bar	Alt+N
Move forward through frames and browser elements (if tabbed browsing is disabled)	Ctrl+Tab or F6
Move forward through the items on a web page, the address bar, or the links bar	Tab
Move forward through the list of AutoComplete matches	↓
Move selected item down in the Favorites list in the Organize Favorites dialog box	Alt+↓
Move selected item up in the Favorites list in the Organize Favorites dialog box	Alt+↑
Move the cursor left to the next punctuation in the address bar	Ctrl+←
Move the cursor right to the next punctuation in the address bar	Ctrl+→
Move to the beginning of the page	Home
Move to the end of the page	End
Open a new tab in the foreground	Ctrl+T
Open a new tab in the foreground from the address bar	Alt+Enter
Open a new website or page	Ctrl+O
Open a new window	Ctrl+N
Open Favorites	Ctrl+I
Open Feeds	Ctrl+J

www.it-ebooks.info

Task	Shortcut Key(s)
Open History	Ctrl+H
Open links in a new background tab	Ctrl+Click
Open links in a new foreground tab	Ctrl+Shift+Click
Open search query in a new tab	Alt+Enter
Open the Organize Favorites	Ctrl+B
Page Setup	Alt+U
Paste Clipboard contents	Ctrl+V
Print the current page or active frame	Ctrl+P
Refresh the current web page	F5
Refresh the current web page regardless of timestamp	Ctrl+F5
Save the current page	Ctrl+S
Scroll down a line	↓
Scroll down a page	Page Down
Scroll up a line	↑
Scroll up a page	Page Up
Select all items on the current web page	Ctrl+A
Select frames to print in framed website	Alt+F
Select the text in the address bar	Alt+D
Set printing options and print the page	Alt+P
Stop downloading a page	Esc
Switch between tabs	Ctrl+Tab or Ctrl+Shift+Tab
Switch to a specific tab number	Ctrl+*n* (where *n* is a number between 1 and 8)
Switch to the last tab	Ctrl+9
Toggle between full-screen and regular views	F11
Toggle Quick Tabs on or off	Ctrl+Q
Type the number of the page you want displayed	Alt+A
Zoom in	Alt+Plus Sign
Zoom in 10 percent	Ctrl+Plus Sign
Zoom out	Alt+Minus Sign
Zoom out 10 percent	Ctrl+Minus Sign
Zoom to 100 percent	Ctrl+0

www.it-ebooks.info

www.it-ebooks.info

APPENDIX D

BIOS Beep Codes

When your computer can't start or give you a display, it can still provide you with useful troubleshooting information in the form of beeps. Depending on your motherboard's BIOS (consult your motherboard manual to determine which one you have), these can provide useful feedback to help you diagnose and fix problems with your PC.

Table D-1 Standard Original IBM Error Codes

Sound	Meaning
1 short beep	Normal–everything OK
2 short beeps	POST error (shown on screen)
Continuous beep	Power supply, system board, or keyboard problem
Repeating short beeps	Power supply or system board problem
1 long, 1 short beep	System board problem
1 long, 2 short beeps	Display adapter problem
1 long, 3 short beeps	Enhanced graphics adapter problem
3 long beeps	Keyboard card error

Table D-2 AMI BIOS Beep Codes

Sound	Meaning
1 short beep	DRAM refresh failure
2 short beeps	Parity circuit failure
3 short beeps	Base 64k RAM failure
4 short beeps	System timer failure
5 short beeps	Process failure
6 short beeps	Keyboard controller gate A20 error
7 short beeps	Video mode exception error
8 short beeps	Display memory read/write test failure
9 short beeps	ROM BIOS checksum failure
10 short beeps	CMOS shutdown read/write error
11 short beeps	Cache memory error
1 long, 3 short beeps	Memory failure
1 long, 8 short beeps	Display test failed

www.it-ebooks.info

Table D-3 Award BIOS Beep Codes

Sound	Meaning
1 long, 2 short	Video error
Any other	Memory problem

Phoenix BIOS beep codes are represented by a number of beeps followed by a pause. For example. 1-1-2 would indicate one beep, a pause, one beep, another pause and then two beeps.

Table D-4 Phoenix BIOS Beep Codes

Sound	Meaning
1-1-2	The CPU is faulty.
Low 1-1-2	The motherboard is having an undetermined fault.
1-1-3	The real-time clock/CMOS is faulty.
Low 1-1-3	The extended portion of the CMOS RAM has failed.
1-1-4	The BIOS ROM has failed.
1-2-1	The programmable interrupt timer has failed.
1-2-2	The DMA controller has failed.
1-2-3	The DMA controller has failed.
1-3-1	The RAM refresh controller has failed.
1-3-2	The test of the first 64-KB RAM has failed to start.
1-3-3	The first RAM IC has failed.
1-3-4	The first RAM control logic has failed.
1-4-1	The address line to the first 64-KB RAM has failed.
1-4-2	The first RAM IC has failed.
1-4-3	Replace the motherboard.
1-4-4	Replace the motherboard.
2-1-1	Bit 0; This data bit on the first RAM IC has failed.
2-1-2	Bit 1; This data bit on the first RAM IC has failed.
2-1-3	Bit 2; This data bit on the first RAM IC has failed.
2-1-4	Bit 3; This data bit on the first RAM IC has failed.
2-2-1	Bit 4; This data bit on the first RAM IC has failed.
2-2-2	Bit 5; This data bit on the first RAM IC has failed.
2-2-3	Bit 6; This data bit on the first RAM IC has failed.
2-2-4	Bit 7; This data bit on the first RAM IC has failed.

www.it-ebooks.info

Sound	Meaning
2-3-1	Bit 8; This data bit on the first RAM IC has failed.
2-3-2	Bit 9; This data bit on the first RAM IC has failed.
2-3-3	Bit 10; This data bit on the first RAM IC has failed.
2-3-4	Bit 11; This data bit on the first RAM IC has failed.
2-4-1	Bit 12; This data bit on the first RAM IC has failed.
2-4-2	Bit 13; This data bit on the first RAM IC has failed.
2-4-3	Bit 14; This data bit on the first RAM IC has failed.
2-4-4	Bit 15; This data bit on the first RAM IC has failed.
3-1-1	The DMA controller has failed.
3-1-2	The DMA controller had failed.
3-1-3	The interrupt controller IC has failed.
3-1-4	The interrupt controller IC has failed.
3-2-2	The BIOS was unable to load the interrupt vectors into memory.
3-2-3	Reserved
3-2-4	The keyboard controller has failed.
3-3-1	Replace the CMOS battery or CMOS RAM if possible.
3-3-2	The CMOS configuration has failed.
3-3-3	Reserved
3-3-4	There is a problem with the video memory.
3-4-1	There is a problem with the video adapter.
4-2-1	The system's timer IC has failed.
4-2-2	The CMOS has failed.
4-2-3	The keyboard controller has failed.
4-2-4	This is a CPU problem.
4-3-1	System RAM addressing circuitry is faulty.
4-3-3	The system timer IC has failed.
4-3-4	The real-time clock/CMOS has failed.
4-4-1	A error has occurred in the serial port circuitry.
4-4-2	A error has occurred in the parallel port circuitry.
4-4-3	The math co-processor has failed.
1-1-1-3	Verify Real Mode
1-1-2-1	Get CPU type
1-1-2-3	Initialize system hardware
1-1-3-1	Initialize chipset registers with initial POST values

www.it-ebooks.info

Sound	Meaning
1-1-3-2	Set in POST flag
1-1-3-3	Initialize CPU registers
1-1-4-1	Initialize cache to initial POST values
1-1-4-3	Initialize I/O
1-2-1-1	Initialize Power Management
1-2-1-2	Load alternate registers with initial POST values
1-2-1-3	Jump to UserPatch0
1-2-2-1	Initialize keyboard controller
1-2-2-3	BIOS ROM checksum
1-2-3-1	8254 timer initialization
1-2-3-3	8237 DMA controller initialization
1-2-4-1	Reset Programmable Interrupt Controller
1-3-1-1	Test DRAM refresh
1-3-1-3	Test 8742 Keyboard Controller
1-3-2-1	Set ES segment to register to 4 GB
1-3-3-1	28 Autosize DRAM
1-3-3-3	Clear 512-K base RAM
1-3-4-1	Test 512-K base address lines
1-3-4-3	Test 512-K base memory
1-4-1-3	Test CPU bus-clock frequency
1-4-2-4	Reinitialize the chipset
1-4-3-1	Shadow system BIOS ROM
1-4-3-2	Reinitialize the cache
1-4-3-3	Autosize cache
1-4-4-1	Configure advanced chipset registers
1-4-4-2	Load alternate registers with CMOS values
2-1-1-1	Set Initial CPU speed
2-1-1-3	Initialize interrupt vectors
2-1-2-1	Initialize BIOS interrupts
2-1-2-3	Check ROM copyright notice
2-1-2-4	Initialize manager for PCI Options ROMs
2-1-3-1	Check video configuration against CMOS
2-1-3-2	Initialize PCI bus and devices
2-1-3-3	Initialize all video adapters in system

www.it-ebooks.info

Sound	Meaning
2-1-4-1	Shadow video BIOS ROM
2-1-4-3	Display copyright notice
2-2-1-1	Display CPU type and speed
2-2-1-3	Test keyboard
2-2-2-1	Set key click if enabled
2-2-2-3	56 Enable keyboard
2-2-3-1	Test for unexpected interrupts
2-2-3-3	Display prompt Press F2 to enter SETUP
2-2-4-1	Test RAM between 512 and 640k
2-3-1-1	Test expanded memory
2-3-1-3	Test extended memory address lines
2-3-2-1	Jump to UserPatch1
2-3-2-3	Configure advanced cache registers
2-3-3-1	Enable external and CPU caches
2-3-3-3	Display external cache size
2-3-4-1	Display shadow message
2-3-4-3	Display nondisposable segments
2-4-1-1	Display error messages
2-4-1-3	Check for configuration errors
2-4-2-1	Test real-time clock
2-4-2-3	Check for keyboard error
2-4-4-1	Set up hardware interrupts vectors
2-4-4-3	Test coprocessor if present
3-1-1-1	Disable onboard I/O ports
3-1-1-3	Detect and install external RS232 ports
3-1-2-1	Detect and install external parallel ports
3-1-2-3	Reinitialize onboard I/O ports
3-1-3-1	Initialize BIOS Data Area
3-1-3-3	Initialize Extended BIOS Data Area
3-1-4-1	Initialize floppy controller
3-2-1-1	Initialize hard disk controller
3-2-1-2	Initialize local-bus hard disk controller
3-2-1-3	Jump to UserPatch2
3-2-2-1	Disable A20 address line

www.it-ebooks.info

Sound	Meaning
3-2-2-3	Clear huge ES segment register
3-2-3-1	Search for option ROMs
3-2-3-3	Shadow option ROMs
3-2-4-1	Set up Power Management
3-2-4-3	Enable hardware interrupts
3-3-1-1	Set time of day
3-3-1-3	Check key lock
3-3-3-1	Erase F2 prompt
3-3-3-3	Scan for F2 key stroke
3-3-4-1	Enter SETUP
3-3-4-3	Clear in-POST flag
3-4-1-1	Check for errors
3-4-1-3	POST done; prepare to boot operating system
3-4-2-1	One beep
3-4-2-3	Check password (optional)
3-4-3-1	Clear global descriptor table
3-4-4-1	Clear parity checkers
3-4-4-3	Clear screen (optional)
3-4-4-4	Check virus and backup reminders
4-1-1-1	Try to boot with INT 19
4-2-1-1	Interrupt handler error
4-2-1-3	Unknown interrupt error
4-2-2-1	Pending interrupt error
4-2-2-3	Initialize option ROM error
4-2-3-1	Shutdown error
4-2-3-3	Extended Block Move
4-2-4-1	Shutdown 10 error
4-3-1-3	Initialize the chipset
4-3-1-4	Initialize refresh counter
4-3-2-1	Check for Forced Flash
4-3-2-2	Check hardware status of ROM
4-3-2-3	BIOS ROM is OK.
4-3-2-4	Do a complete RAM test
4-3-3-1	Do OEM initialization

www.it-ebooks.info

Sound	Meaning
4-3-3-2	Initialize interrupt controller
4-3-3-3	Read in bootstrap code
4-3-3-4	Initialize all vectors
4-3-4-1	Boot the Flash program
4-3-4-2	Initialize the boot device
4-3-4-3	Boot code was read OK.

www.it-ebooks.info

www.it-ebooks.info

Glossary

32-BIT Operating systems and programs that operate with binary numbers up to a maximum of 32 digits long, giving a maximum of 65,535.

64-BIT Operating systems and programs that operate with binary numbers up to 64 characters long. These allow for addressing much larger numbers than 32-bit systems.

ACTION CENTER Indicated by the white flag on the Windows 7 taskbar. This is a feature that aggregates system messages and troubleshooting help.

ADMINISTRATOR A user account level that allows any changes to be made to an operating system or programs.

AGP Accelerated Graphics Port, a graphics card interface.

ADSL Asymmetric Digital Subscriber Line. Broadband Internet connection (3 to 200 times faster than dial-up). You need to be close to a digital telephone exchange, connected to cable, or have a satellite dish. You can remain connected permanently.

ANTI-VIRUS PROGRAM Something that can spot a virus attached to an email or on your computer and remove or quarantine it.

APPLICATION A program such as Microsoft Office Word or Microsoft Internet Explorer.

BACK UP Keeping copies of programs or data in a separate place in case of corruption of the first version. There are various methods. See floppy disk and CD/CDROM/CD-R/CDRW compact disc.

BANDWIDTH A measure of the maximum amount of data that can be transferred over the Internet or phone system at any one time.

BETA A program that is being tested, which is given out to users to find any problems.

BIOS The Basic Input Output System for the computer's motherboard.

BITLOCKER A full disk and partition security encryption system.

BITMAP A graphic image made up of many tiny dots.

BLUE SCREEN OF DEATH Known to the trade as BSOD, the screen that comes up in Windows when your computer can't cope with something. It suggests you press a key to continue. Called the Blue Screen of Death because pressing a key doesn't help at all! Restart the computer.

BLUETOOTH Using radio transmission from your PC to control everything from printers to lights to the washing machine. See also WI-FI.

BOOT To start a PC.

BROADBAND High-speed Internet connections such as cable or ADSL for faster connections.

BROWSER Program for browsing the Internet such as Microsoft Internet Explorer, Firefox, Safari, and Chrome.

BYTE A piece of data made up of eight bits (or digits) per character.

CAB FILE A compressed file. In Windows CAB files contain all the files necessary to create the Windows operating system.

www.it-ebooks.info

CABLE MODEM Required to receive a broadband Internet connection from a cable communications company. An alternative method to ADSL.

COOKIE A small text file that is downloaded to your computer by a website. Used to remember your login details and record your activities for future reference. Can be deleted by using Windows Explorer or blocked by Internet Explorer security.

CD/CDROM/CD-R/CDRW COMPACT DISC Physical media that hold programs and data. Some are read-only because the tracks are burned in and cannot be changed. The RW type can be rewritten many times.

CHIP Silicon chip. The silicon base used to mount the millions of components that make up a computer processor.

CLOUD Programs or services hosted on and run from Internet servers.

COMPATIBILITY MODE A special mode in Windows that allows programs to be run in an emulated mode mimicking an earlier version of Windows.

COMPUTER MANAGEMENT CONSOLE An interface in Windows for managing programs, services, and components.

CONTROL PANEL An important set of icons that enable you to configure the basic functions of your computer.

CONTROL KEY Marked Ctrl on the keyboard. Like Alt and Function keys, its use varies from program to program.

DATA EXECUTION PREVENTION A Windows service that can make it harder for viruses and malware to cause memory overflows.

DEFRAGMENT Reducing the fragmentation (scattering) of files across a hard disk so that they can be read more quickly.

DESKTOP The screen first displayed when a user logs in to a computer.

DEVICE DRIVER A service in Windows that handles communications between the operating system and a hardware device.

DIGITAL The method of storing or transmitting things as a series of numbers. These numbers never get past 1; they are made up of 0s (zeros) and 1s (ones). The speed and accuracy with which these can be stored has enabled most information to be stored in this way—including television, photography, all computing, and the Internet.

DIRECTORY An organized search facility on the web**.**

DIRECTX A free, downloadable Windows program that ensures that graphics programs work with all the different types of graphics hardware.

DOWNLOAD The process of transferring files from the web to a machine's hard disk. You can download pictures, text, and programs.

DPI Dots per inch. Used in connection with printers, scanners, and monitors.

DRAG AND DROP The facility in most programs to select text or a file and drag it to another position.

DRIVE LETTER An alphabetical letter from A to Z that Windows assigns to a fixed or removable disk.

DUAL BOOT Having more than one operating system installed on a PC and being able to choose, at startup, which one to use.

DUAL CORE A processor with two physical cores.

DVD-ROM Digital Versatile Disk Read Only Memory. A disc capable of holding much more data than a CD. Used for music, films, and large programs.

DVD-RW A rewriteable DVD.

DVD Player Special disc player for DVD discs. Capable of playing CDs as well.

EMAIL Messages sent to people over the Internet. Email addresses always contain the @ symbol.

www.it-ebooks.info

EMAIL CLIENT Program you use to send and receive emails such as Windows Live Mail, Mozilla Thunderbird, and Microsoft Outlook.

ENCRYPTION Using a cryptography technique to make data unreadable with a method for unlocking it.

EVENT LOG Records kept by Windows of events and errors.

FAT, FAT32 File Allocation Table. This is the file system used on a disk. It is a form of index that is constantly updated to keep track of everything on the disk. FAT is limited to 4 GB per partition. FAT32 is almost unlimited but cannot cope with files larger than 4 GB.

FAVORITES Also known as bookmarks. All web browsers enable you to add favorite sites to a list for easy retrieval.

FIREWALL A program that ensures that a PC has no open ports that allow hackers to access it.

FIREWIRE A socket on some PCs that enables much faster transfer of data than via serial, parallel, and USB ports. Needed if you are transferring large amounts of data, for example from a digital video camera for editing purposes.

FIRMWARE Software on a chip for a device such as a BIOS or SSD that can sometimes be updated.

FLASH DRIVE A removable and portable USB storage device.

FLOPPY DISK An outdated form of storage on a small, 3.5-inch disk.

FONT A collection of characters of a predefined style such as Times or Arial.

FREEWARE Computer programs that are distributed free of charge.

FUNCTION KEYS Programmable keys F1 to F12, which may vary in their use.

GIGABYTE 1,073,741,824 bytes.

GIGAHERTZ A thousand megahertz.

GRAPHICS The general term used for pictures and drawings.

GRAPHICS CARD The part of the PC that sends signals to the monitor or display.

GROUP POLICY Rules that can be set in Windows for managing permissions and allowed activities for groups of users.

HACKER A person who delights in changing software programs to give them more features. Criminal hackers use their knowledge to write destructive programs.

HARD DISK A set of spinning disks coated with recording material. Can retain details of programs and data indefinitely.

HARDWARE Any piece of equipment such as a computer or a printer.

HOMEGROUP A networking feature that allows Windows 7 PCs to share files and printers.

HOTMAIL A web-based email service owned by Microsoft.

HYPERLINK A link on a web page that takes you to another web page. Hyperlinks are often colored and underlined, although images and maps can also act as links. The mouse pointer changes to a hand graphic when hovering over a link. See surfing.

HYPERTEXT LINKS Addresses of other sites or pages, which might be on the same site or on the other side of the world. They are often colored and occasionally underlined. When a mouse pointer hovers over a hyperlink, it changes shape. Mostly you will see hypertext when connected to the Internet, but you may also find it in things like encyclopedia CDs. When a hypertext is clicked, your computer may connect to the Internet to access the site.

ICON A graphic representation of something such as a shortcut to a program.

www.it-ebooks.info

INTERNET A conglomeration of linked computers that can be accessed by people who are connected to the web.

INTERNET EXPLORER The most common web browser, issued for free by Microsoft. Other browsers include Firefox and Chrome.

ISP Internet Service Provider. A company that provides access to the Internet.

JAVA and JAVASCRIPT A programming language used on some web pages.

KILOBYTE (Kb) 1,024 bytes.

LAN Local Area Network. Computers connected "locally," for example within a company or home, so they can communicate and share programs and data.

LASER PRINTER A printer that uses a laser to create an image on a light sensitive drum, which then loads toner powder onto paper. Faster and more economical than inkjet printers when a large amount of printing is needed.

LINUX An operating system, like Windows, but is often free. It requires software written especially for it.

MALWARE Unwanted and malicious software.

MACRO A small program within another program that, at the touch of a couple of keys, performs an action or a series of actions.

MEGABYTE (Mb) 1,048,576 bytes. See also byte, kilobyte, and gigabyte.

MEGAHERTZ A measure of how fast your PC processor works. Basically, a million cycles per second. One instruction takes place each vibration.

MEMORY Hardware in a PC that Windows uses to store files it is working with and needs to operate.

MONITOR The computer screen. Also called a visual display unit (VDU).

MOTHERBOARD The main circuit board of a computer to which other components are attached.

MP3 A highly compressed form of music, which can be downloaded from the Internet and played on a computer or a portable MP3 player. It stands for Music Program Expert Group Audio Layer 3 (or MPEG3).

MSCONFIG A Windows feature for controlling startup and diagnostic startup options.

NET A term used loosely to mean the Internet.

NETWORK General term for connected computers. See also LAN.

OFFLINE Not connected to the Internet. Some things, like writing emails, can be done before going online.

ONLINE Connected to the Internet.

OPERATING SYSTEM A software interface for a computer in which you can run programs and control devices.

PARALLEL PORT Almost always a 25-pin "female" socket on the back of a computer that is used for printing and also to attach devices like scanners and other external equipment. See also USB.

PARENTAL CONTROLS A Windows feature for controlling permissions for children.

PARTITION A physical hard disk can be separated using software into several logical sections, each appearing as its own disk in Windows.

PATH The location of a file or program on a disk. for example C:\Users\Public.

PCI SLOT Peripheral Component Interface. A type of connector—usually white—that enables you to add components to your PC.

PCI-EXPRESS A more recent version of the PCI standard.

www.it-ebooks.info

PCMCIA Originally stood for Peripheral Component MicroChannel Interconnect Architecture. Difficulty with the acronym led to the simpler term "PC Card" for the version 2 specification. It was originally for memory expansion, but the existence of a usable general standard for notebook peripherals led to all manner of devices being made available in this form. Typical devices include network cards, modems, and hard disks.

PDF Portable Document Format. A file format from Adobe for creating documents that can be read across different devices.

PERFORMANCE MONITOR A Windows feature that allows the user to track the performance of the operating system and installed programs.

PHISHING The name given to a scam where you get an email supposedly from your bank, requesting that you confirm your password. If you give out a password like this, you can expect your account to be robbed shortly afterwards!

PROBLEM STEPS RECORDER A Windows program that allows you to create annotated screenshots of a problem and send them in a file to a support person.

PLUG AND PLAY Modern machines and hardware (printers, sound cards, CD players and so on) are able to recognize when they are connected, enabling easy installation or use.

PORT Either a socket on your computer, such as USB, parallel (printer), or serial (communications), or part of the system that allows communication with your computer (the latter being numbered, as in Port 110).

PROCESSOR A physical silicon chip on a motherboard that is the brains of a computer.

PS/2 A small socket used for modern keyboard and mouse connections.

QUAD CORE A processor with four physical cores.

RAID Redundant Array of Independent Disks. A hardware-managed system for linking hard disks together to create larger logical disks or automatic backups.

RAM Random Access Memory. The temporary storage facility on a computer.

READYBOOST A Windows feature that allows the use of USB flash drives as an extra memory cache.

REGISTRY A file (one per user on a computer) containing a database of settings for Windows, user preferences, and installed software and hardware.

REMOTE ASSISTANCE A feature that allows a person to remotely control a PC over a network or the Internet.

REMOTE DESKTOP A feature that allows the remote control of another computer on a network.

RESOURCE MONITOR A Windows feature for viewing in real time the usage of computer resources.

SAFE MODE Starting Windows in its most basic form with no background programs in operation. Used to address various problems including virus and defragmentation difficulties.

SCANNER A piece of equipment capable of converting a printed picture or text into a digital file.

S-VIDEO A high-quality video connection. It carries brightness and color information separately.

SEARCH ENGINE A program, usually accessed through the Internet, that enables you to search for information by entering text.

SERIAL PORT A socket on the back of a computer used to attach a mouse, a modem, or a printer. Referred to as a COM (communication) port. Serial ports fell out of use when USB was introduced.

SHADOW COPIES Automatic backups of previous versions of files.

SHAREWARE Free computer programs or software. Contributions toward the costs of shareware are encouraged and welcomed.

SHELL FOLDER A pointer toward a physical folder on a disk.

www.it-ebooks.info

SLIPSTREAMING The process of integrating a Windows service pack into the operating system installation disc.

SOFTWARE Programs of all kinds that make the computer act in a particular way.

SPAM Unsolicited advertising that usually arrives as email.

SPYWARE Software that is installed on a computer without the user's knowledge, used to monitor and report back what the user does.

SSD Solid State Disk. A hard disk that uses nonvolatile memory chips for storage instead of the traditional spinning disk.

STARTUP REPAIR A Windows feature for automatically repairing a Windows installation that will not start.

STREAMING Receiving sound or pictures continuously over the Internet (rather than downloading first).

STYLE SHEET A document that defines specific type styles, weights, and sizes.

SURFING Using hypertext links to move from one website or page to another.

SYSTEM FILE CHECKER A Windows feature that compares all the currently installed operating system files against the originals on the installation disc to find and replace corrupt files.

SYSTEM HEALTH REPORT A Windows tool for generating a text-file report of the current status of Windows, drivers, and programs.

SYSTEM IMAGE A backup of the installed copy of Windows, stored in a single file.

SYSTEM RESCUE DISC A bootable CD or DVD that can be used to launch Startup Repair.

SYSTEM RESTORE A Windows feature that makes copies of critical system settings and files before changes are made; can be restored later if required.

TAB KEY The key on the left of a QWERTY keyboard that allows you to jump certain fixed distances across the page when using a word processor.

TASKBAR The bar containing the Start menu and program icons that normally appears at the bottom of a computer screen.

TEMPORARY FILES Files stored on your computer that contain information or data to be used for a short-term purpose. These files can sometimes be left undeleted after use.

TFT Thin film transistor. The technology used to create flat screen monitors.

TOOLBAR A set of icons often found at the top of a program's user interface.

TROJAN A virus program that is disguised as something else. It invades a PC and can be accessed by a hacker.

UAC User Account Control. A security system in Windows that helps prevent unauthorized changes from being made to an operating system.

UI User Interface. A way of displaying the controls for a computer in a friendly, graphical way.

USER FOLDER A folder containing a user's files, documents, and settings.

URL Universal Resource Locator or web address. Always starts with http:// and, usually, www.

USB Universal Serial Bus. A versatile communication port, which can transfer data faster.

USB 2.0 At 480 MB/s, this is even faster than USB. Looks the same as USB, and slower devices can also be attached to it.

USB 3.0 At this writing, the fast standard for USB, dubbed Super Speed, with speeds of up to 4.8 GB/s. Is backward compatible with earlier USB standards and will run older USB devices at their native speeds.

VHD Virtual Hard Disk. A file containing an operating system and files that can appear as a physical disk.

www.it-ebooks.info

VIRTUALIZATION The process of running multiple operating systems simultaneously on the same computer.

VIRTUAL MEMORY Otherwise known as a Swap of Page File, a reserved space on a hard disk that Windows uses as a memory cache.

VIRUS A malicious program that can harm a computer. It is spread through programs, either from disks or from the Internet. May also be called Trojan or worm.

WEB BROWSER A program to help you navigate the Internet, for example Microsoft Internet Explorer or Firefox.

WEBCAM A small camera that is attached to a computer.

WEP (WIRED EQUIVALENT PRIVACY) An encryption method for wireless networks.

WI-FI A wireless interface, using radio to link computers and other devices. A snappier name than the 802.11n standard. See also Bluetooth.

WINDOWS 7 The very latest edition of the Windows operating system, on which this book is based.

WINDOWS XP Released in 2001, Windows XP was still commonly in use on computers when Windows 7 was launched eight years later.

WINDOWS UPDATE A feature in Windows for automatically updating the operating system with the latest updates.

WIZARD A program that helps step a user through a process such as installing new software or hardware.

WORM A virus program that spreads by sending itself to people in a user's email address book.

WPA An encryption method for wireless networks.

WWW World Wide Web.

XP MODE A special copy of Windows XP Professional that runs in a virtual machine in Windows 7.

ZIP FILE Compressed file that ends in .zip. To see their contents, they must be viewed using a special program such as Winzip or Enzip.

www.it-ebooks.info

www.it-ebooks.info

Index

Symbols and Numbers

32-bit registry keys, 415

64-bit registry keys, 415

256-bit encryption
- zPOD, 339

- (minus) sign
- Internet searches, 273, 274

+ (plus) sign
- Internet searches, 273, 274

A

accessing
- BitLocker, 362
- Computer Management console, 227, 227–229, 369
- Device Manager, 182
- Disk Defragmenter, 70
- Indexing Options, 129
- MSConfig, 11, 76, 241
- Performance Information and Tools, 217, 217–218
- Previous Versions, 163
- Problem Steps Recorder, 285
- Registry Editor, 246, 413
- Services panel, 244
- System File Checker, 239
- System Recovery Options, 250
- Windows drive in Ubuntu, 327
- Windows Remote Assistance, 282–286
- Windows Remote Desktop, 278
- Windows Task Manager, 224

accounts
- confirmation links, 146
- guest, 83
- user, 80–86
  - administrator passwords, 81–83
  - guest accounts, 83
  - parental controls, 84–87

Acronis Disk Director, 292

Acronis True Image, 291, 313

Action Center, 17–20
- Check For Solutions option, 18
- logs, 18
- Maintenance section, 18
- Network Access Protection, 19
- notifications, 19
- panel, 18, 19
- program compatibility notifications
  - notifications, 173–175
- Reliability History
  - viewing, 19
- repelling attacks, 137–138
- Security section, 402
- settings, 19
- System and Security section, 21
- troubleshooters, 194–195
- User Account Control, 19

Actions tab (Task Scheduler), 371

activating
- Windows 7, 8

ActiveX
- files, 258–259

add-ons
- Internet Explorer
  - disabling, 231–232
  - managing in Control Panel, 234–235
  - running without, 233–234

www.it-ebooks.info

address bars
online security, 49
Adjust Visual Effects link, 380–382
Administrative Events pane (Event Log), 220
administrator mode
Program Compatibility Assistant, 30
administrator passwords
user accounts, 81–83
Advanced Attributes dialog box, 348
advanced diagnostic tools
Computer Management console, 227–229
Event Log, 219–221
Performance Monitor, 222–223
Resource Monitor, 223–224
System Health Report, 226–228
System Information tool, 224–225
Windows Task Manager, 224
Advanced EFS Data Recovery, 360
Advanced Encryption Standard (AES)
BitLocker, 43–47
Advanced Encryption Standard (AES) key, 361
advanced options
system repair disc, 250
Advanced Options dialog box, 383
Advanced security settings
Windows Firewall, 403–411
Inbound rules, 406–409
managing firewall rules, 405–406
Outbound rules, 406–409
setting Connection Security Rules, 410
advanced settings
Windows Firewall, 24–25
Advanced Settings panel, 384
Advanced System Settings link, 279
Advanced tab (System Properties dialog box), 10
Advanced tab (Windows Firewall With Advanced Security management panel), 406
Advanced Tools (Performance Information and Tools), 385–398
Disk Defragmenter, 396–397
Event Log, 386
Performance Monitor, 386–393
Resource Monitor, 393–395
System Information panel, 396
Task Manager, 396
AES (Advanced Encryption Standard)
BitLocker, 43–47
AES (Advanced Encryption Standard) key, 361
alerts
User Account Control (UAC), 40–41
all-in-one PCs, 301–303
cleaning, 99
Amazon S3, 62
AMI
beep codes, 439
and, using in Internet searches, 274
annotating screenshots (Problem Steps Recorder), 286
anti-malware
Microsoft Security Essentials, 38
Windows Defender, 26–27
anti-malware software, 38–40, 140–144
malicious, 150–151
Malwarebytes, 39, 143
Microsoft Windows Malicious Software Removal Tool, 142–143
repairing attack damage, 153
SpyBot Search & Destroy, 39
Spyware Blaster, 144
Spyware Terminator, 39, 76, 143
Windows Defender, 39, 141–142
anti-spyware
Windows Defender, 26–27
anti-spyware software, 48
Antivirus 2010, 150

www.it-ebooks.info

anti-virus software, 27–28, 38–40. *See also* viruses
AVG Anti-Virus/AVG Security Suite, 140
installing after Windows 7 installation, 7
Malwarebytes, 39
Microsoft Security Essentials, 28, 38, 139
Microsoft Windows Malicious Software Removal Tool, 39
Norton Internet Security/Norton 360, 28, 39, 140
repelling attacks, 138–140
updates, 47
Windows Virtual PC, 117
Windows XP Mode, 117
AppData folder, 259, 260
Application Control Policies (Local Policy Editor), 89
applications, 259
compared to processes and services, 208
Computer Management console, 378–379
definition, 208
dupliware, 211
exiting
system tray, 206–207
extensions, 259
shutting down
End Process Tree option, 207
Safe Mode, 208–209
Windows Task Manager, 207–208
Ashampoo WinOptimizer, 74, 344
associations (files)
troubleshooting, 125–126
ATI support website, 293
attaching
virtual hard disks (VHD), 110
attachments (email)
viruses, 48
attacks
identifying, 144–152
browser plug-ins, 148–149
malicious anti-malware software, 150–151
malicious websites, 149–150
padlock icon, 144–145
phishing, 146–147
spam, 146–147
toolbars, 147–148
repairing damage, 153–162
anti-malware software, 153
BIOS viruses, 159–161
McAfee Stinger, 154–155
online virus scanners, 153
removing viruses, 157–158
restoring Windows 7 from backups, 159
Safe Mode, 155–156
viruses hiding, 161–162
repelling, 137–144
Action Center, 137–138
anti-malware software, 140–144
anti-virus software, 138–140
Attrib command, 253
audio devices
setting, 136
Audit Mode, 269
authentication
BitLocker, 361
Automatically Manage Paging File Size For All Drives option, 10
automatic restarts
disabling, 215
auto-running software, 76
AVG Anti-Virus/AVG Security Suite, 140
Award BIOS beep codes, 440

B

Backup and Restore, 57–60
Backup And Restore window, 61–62
backups, 4, 49, 57–63, 313
Backup and Restore, 57–60
BitLocker, 45
cloud storage, 62
copies, 315–317
corporate image, 65
determining number of, 66–67

www.it-ebooks.info

backups *(continued)*
image, 314
Windows System Image Backup, 314–316
incremental, 66
Linux ISOs, 333
Nero, 62
networks, 16, 59
NTI Shadow, 62
partitions
size, 7
Previous Versions, 165, 166
RAID (Redundant Array of Independent Disks), 318
registry, 249, 416–417
registry keys, 418
reinstalling Windows 7, 77
removable optical discs, 66
restoring files/data from, 61–62
restoring Windows
custom installs, 315–317
restoring Windows 7 from, 159
restoring Windows from, 313–315
splitting data across desktops, 5
starting Windows 7, 179
storage locations, 66–67
storing, 314
version control, 63
viruses, 161
Windows 7, 14–16, 63–66
Basic Input Output System (BIOS), 94–96
resetting, 307–309
BCD (boot configuration data) file
creating, 266
BCDEdit, 252
beep codes (BIOS), 94, 439–445
BIOS (Basic Input Output System), 94–96
corruption, 213
resetting, 307–309
viruses, 159–161
warning beep codes, 94, 439–445
BitLocker, 43–47, 361–364
accessing, 362
authentication, 361
backups, 45
encrypting drives, 363
encrypting hard disks, 364
non-Windows computers, 45–46
reading encrypted hard disks, 362
reasons to use, 47
BitLocker Drive Encryption window, 362
BitLocker To Go, 361–364
Windows XP, 362
BitLocker To Go Reader, 45–46, 362
blocking
CDs, 90–91
DVDs, 90–91
external hard disks, 90–91
Flash drives, 90–91
blocks
routers
troubleshooting, 412
Blue Screen of Death (BSOD), 214–215, 320
bookmarks
resetting Internet Explorer, 236
Boot Camp, 104
boot configuration data (BCD) file
creating, 266
boot discs
Linux, 326
Boot folder, 258, 259, 262
booting
dual booting
compared to virtualization, 104
from virtual hard disks (VHD), 110–115
minimal hardware boots, 306–307
boot log, 241–243
finding, 242

www.it-ebooks.info

Boot menu
BCDEdit, 252
repairing with bootrec.exe, 251–252
Boot Order setting, 64
Bootrec.exe, 251
repairing Boot menu, 251–252
Browser Ballot Screen
Internet Explorer alternatives, 238–239
browsers
clearing temporary files, 72–73
Google Chrome, 239
Internet Explorer. ***See*** Internet Explorer
Mozilla Firefox, 239
plug-ins
identifying attacks, 148–149
security, 48
BSOD (Blue Screen of Death), 214–215, 320
burning
ISO files (Linux), 335–336
burning CDs/DVDs
Linux, 333–334

C

cases, 98
desktops, 295–296
CCleaner, 73
Cd command, 253
CDs
blocking, 90–91
burning
Linux, 333–334
burning ISO files to
Linux, 335–336
manuals, 50
Certificate Export Wizard, 349
certificates
EFS (Encrypted File System), 354–356, 356–359
File Encryption Certificate Manager, 359
certification
hardware, 75
Change Action Center Settings option, 174
Change Advanced Power Settings, 134
Check For Solutions option (Action Center), 18
chkdsk /? command, 251
Cipher.exe, 360
cleaning
all-in-one PCs, 99
desktops, 99
keyboards, 100–101, 301
laptops, 99
mice, 100–101, 301
PCs, 98
clean installs, 4–6
Clean Up System Files option, 72
Clear CMOS jumper, 308
clearing
temporary files, 72–73
cloud storage
backups, 62
SkyDrive, 46
cmd (Command Prompt)
accessing System File Checker, 239
code
legacy, 35
security, 35
legacy code
updates, 21
command-line switches
/FixBoot, 252
/FixMbr, 252
/ScanOS, 252
Command Prompt (cmd)
accessing System File Cheker, 239
Command Prompt window
cutting/pasting in, 114

www.it-ebooks.info

commands
Attrib, 253
Cd, 253
chkdsk /?, 251
Copy, 253
Del, 253
Devices By Connection, 377
Devices By Type, 377
Dir, 253
Diskpart, 253
/F, 250
Mkdir, 253
More, 253
Move, 253
/R, 250
Rd, 253
Ren, 253
Resources By Connection, 377
Resources By Type, 377
Show Hidden Devices, 377
Type, 253
/X, 250
Xcopy, 253
compatibility, 28–33
hardware
Microsoft list, 171
Program Compatibility Assistant, 29–30
Program Compatibility troubleshooter, 172–173
software
Microsoft list, 171
notifications, 173–175
troubleshooting, 170–171
manually setting, 170–172
Windows XP Mode, 31–33, 175
Complete PC Backup, 313–315
Components (System Information tool), 225
Computer Configuration section (Group Policy Editor), 87
Computer Management console, 89–90, 227–229, 369–379
accessing, 227, 369
applications, 378–379
Device Manager, 377
Local Users and Groups option, 376
reattaching virtual hard disks (VHDs), 110
services, 378–379
Shared Folders option, 376
system tools, 370–377
Event Viewer, 373–376
Task Scheduler, 370–372
Task Scheduler, 90–91
Windows Management Instrumentation (WMI), 379
Computer Management Console
Event Viewer, 90
Shared Folders, 90
computers
policies
restoring folders, 263
restarting
after software crashes, 214
disabling automatic restarts, 215
restoring data, 321–324
Computers tab (Windows Firewall With Advanced Security management panel), 406
Computing.net, 292
Conditions tab (Task Scheduler), 371
configurations
system preferences, 7–12
System Restore, 167–168
Windows
minimum configuration, 206–208
Windows Remote Desktop, 279
confirmation links, 146
connections
Internet
Linux, 330–331
Windows Remote Assistance, 282–286
Windows Remote Desktop, 279

www.it-ebooks.info

Connection Security Rules
setting, 410
connectors
jump-starting PCs, 309
power supplies, 305
control
users
UAC (User Account Control), 79–80
controllers, 183
Control Panel
Indexing Options, 129
logs, 261
System and Security panel, 9
troubleshooters, 398–400
Control Panel Item. *See* cpl files
controls
Parental Controls, 84–87
Copy command, 253
copying
encrypted data, 364
registry files, 321
Copype.cmd script, 265
cores
running multiple operating systems, 37
corporate environments
Windows Remote Assistance, 281–285
Windows Remote Desktop, 278–280
corporate image backups, 65
corruption
BIOS, 213
counters
adding to Performance Monitor, 387
cpl files, 259
craplets, 211
crashes
software
rebooting, 214
Create a System Image dialog box, 15
Create a System Repair Disc option, 63–64
Create A System Rescue Disc option, 63–64
Create Basic Task option, 372
cryptography
BitLocker, 43–47
Custom (Advanced) option, 316–318
Custom Install option, 5
custom installs
restoring data, 315–317
restoring Windows, 315–317
cutting
in Command Prompt window, 114

D

data
copying encrypted data, 364
recovering
Advanced EFS Data Recovery, 360
Cipher.exe, 360
registry settings, 415
rescuing
Ashampoo WinOptimizer, 344
O&O Disk Recovery, 344
restoring
custom installs, 315–317
from backups, 313–315
recovery specialists, 344
with Linux distributions, 325–330
with other PCs, 321–324
restoring from backups, 61–62
splitting across desktops for backups, 5
splitting across partitions for backups, 5
data backups, 49
Data Collector Sets
adding event logs, 390
Performance Monitor, 388–393
scheduling, 393
viewing, 392
Data Execution Prevention (DEP), 382

www.it-ebooks.info

data loss
reinstalling/restoring, 4
DDOS (distributed denial of service) attacks, 140
Debian, 335
debug folder, 261
decryption
Cipher.exe, 360
Default setting (UAC), 42
defragmenting hard disks, 69–71
Del command, 253
Delete Browsing History dialog box, 72, 73
deleting
files
Disk Cleanup, 71–72
fragmentation, 69–74
temporary files, 262
registry keys, 417–418
registry settings, 248–249
DEP (Data Execution Prevention), 382
desktops
cases, 295–296
cleaning, 99
Device Driver folder, 259
device drivers, 180–194
common problems, 180–181
common Windows problems, 213
Device Manager, 182–187
installing, 187–190
reinstalling, 190–191
removing, 190–191
rolling back, 193–194
updating, 192–194
Device Manager, 182–187, 377
accessing, 182
hidden devices, 185–187
installing device drivers, 187–190
reinstalling device drivers, 190–191
removing device drivers, 190–191
rolling back device drivers, 193–194
updating device drivers, 192–194
warning triangles, 184
devices
common problems, 180–181
controllers, 183
Device Manager, 377
diagnosing problems, 205
displaying, 377
hidden devices
Device Manager, 185–187
human interface, 183
IRQ (interrupt requests) conflicts, 209–210
troubleshooting, 101
USB3
troubleshooting, 135
Devices By Connection command, 377
Devices By Type command, 377
Diagnose/Repair feature (Windows Firewall), 26–27
diagnosing
common problems, 213
domino effect, 213
hardware problems
System Monitor for Linux, 331–332
reasons problems occur, 211–213
step-by-step approach, 205–210
minimum Windows configuration, 206–208
unplugging hardware, 209–210
Diagnostic Results panel (System Health Report), 226–227
diagnostics folder, 261
diagnostic startups
MSConfig, 241–243
diagnostic tools
Computer Management console, 227–229
Event Log, 219–221
Performance Monitor, 222–223
Resource Monitor, 223–224
System Health Report, 226–228

www.it-ebooks.info

System Information tool, 224–225
Windows Task Manager, 224
dialog boxes
Advanced Attributes, 348
Advanced Options, 383
Create a System Image, 15
Delete Browsing History, 72, 73
Indexing Options, 383
Internet options, 237
Power Options, 384, 385
Properties, 170–171, 245, 379
Resources tab, 209
Remote Desktop Connection, 279
System Configuration, 243
System Properties
Advanced tab, 10
User Account Control, 80
Windows 7 Disk Defragmenter, 70
Dir command, 253
DirectX Diagnostic Tool
identifying problems, 126–128
disabling. *See* turning off
automatic restarts, 215
EFS (Encrypted File System), 354
Internet Explorer add-ons, 231–232
discarding PCs, 50
Disk Cleanup, 71–72, 385
Disk Cleanup Wizard, 53–54
Disk Defragmenter, 70–71, 396–397
disk images
Linux, 333
Disk Management console, 228–229
Diskpart command, 253
disks. *See* hard disks
custom installs, 317, 317–318
monitoring, 395
displaying
hidden devices, 377
tasks (Task Scheduler), 372
distributed denial of service (DDOS) attacks, 140
distributions
Linux, 325, 334–335
DLLs
(Dynamic Link Library), 259
domino effect, 213
Doyle, Sir Arthur Conan, 205
drivers
CDs
manuals, 50
diagnosing with boot log, 241–243
Drivers folder, 259
DriverStore folder, 259
drives. *See also* hard drives
accessing Windows drive in Ubuntu, 327
encryption with BitLocker, 363
IDE (Integrated Drive Electronics) drives, 298
managing in Ubuntu, 328
optical, 300
RAID (Redundant Array of Independent Disks)
backups, 318
drv files, 259
dual booting
compared to virtualization, 104
dual-boot systems
Windows Vista, 6
Windows XP, 6
dupliware, 211
DVDs
blocking, 90–91
burning
Linux, 333–334
burning ISO files to
Linux, 335–336
install
Startup Repair, 178–179
installation
restoring Windows 7 from, 314

www.it-ebooks.info

DVDs *(continued)*
installation DVD
System File Checker, 239–240
slipstreamed installation DVDs
creating, 263–272
Dynamic Link Library files. *See* DLLs

E

Easy Connect, 283
ECC (Elliptic-Curve Cryptographic) algorithm cipher, 360
editing
registry keys, 417–418
editions
Windows 7, 423
features, 425–429
EFS (Encrypted File System), 347–360
certificates, 354–356, 356–359
EnCase Forensic, 360
keys
restoring, 352–354
reading Windows files in Linux, 328
recovering EFS files, 359
setup, 348–351
smart cards, 356–359
turning off, 354
electricity
laptops, 304
static electricity, 93
memory cards, 97
safety, 304
Elliptic-Curve Cryptographic (ECC) algorithm cipher, 360
email
attachments
viruses, 48
phishing, 48, 146–147
spam, 48, 146–147
EnCase Forensic, 360
Encrypt Contents To Secure Data check box, 348
Encrypted File System. *See* EFS
encryption
256-bit
zPOD, 339
BitLocker, 43–47, 361–364
encrypting drives, 363
encrypting hard disks, 364
non-Windows computers, 45–46
reasons to use, 47
BitLocker To Go, 361–364
Cipher.exe, 360
copying encrypted data, 364
EFS (Encrypted File System), 347–360
certificates, 354–356, 356–359
EnCase Forensic, 360
reading Windows files in Linux, 328
recovering files, 359
restoring EFS keys, 352–354
setup, 348–351
smart cards, 356–359
turning off, 354
File Encryption Certificate Manager, 359
files, 350–351
folders, 350–351
PGP (Pretty Good Privacy), 347
TrueCrypt, 46
End Process Tree option, 207
engines
scanning
Norton Internet Security/Norton 360, 39
erasing PCs, 50
errors
administrative, 220
partitions
SpinRite, 343
Event Log, 219–221, 386
reading, 221
event logs
adding to Data Collector Sets, 390
filtering, 374–375

www.it-ebooks.info

events
attaching to tasks to, 374–375
Event Viewer, 219, 373–376
attaching tasks to events, 374–375
creating custom views, 375–376
event log filtering, 374–375
Event Viewer (Computer Management Console), 90
exiting
programs
system tray, 206–207
expandable VHD files, 112
expansion cards, 97, 301
Explore Additional Options, 399
exporting
tasks (Task Scheduler), 372
extending
partitions, 55–57
extensions
applications, 259
extensions (file)
viewing, 257
external hard disks
blocking, 90–91
encrypting with BitLocker, 43

F

factory resetting
Internet Explorer, 235–237
failures
common problems, 213
fans, 301
faults
minimal hardware boots, 306–307
favorites
resetting Internet Explorer, 236
/F command, 250
Fedora, 335
File Encryption Certificate Manager, 359
files
ActiveX, 258–259
associations
troubleshooting, 125–126
Backup and Restore, 57–60
BCD (boot configuration data)
creating, 266
cpl, 259
deleting
Disk Cleanup, 71–72
fragmentation, 69–74
temporary files, 262
DLLs
(Dynamic Link Library), 259
drv, 259
encrypting, 350–351
encryption
File Encryption Certificate Manager, 359
hidden, 201
viewing, 257
inf, 258
moving away from Windows 7, 12–13, 53–57
Disk Cleanup Wizard, 53–54
Shell user folders, 57–58
shrinking/extending/creating partitions, 55–57
ntuser.dat, 321
ocx, 259
operating system, 257–260
operatng system
System Restore, 166–170
program files, 200
reading Windows files in Linux
EFS (Encrypted File System), 328
recovering
EFS (Encrypted File System), 359
registry
copying, 321

www.it-ebooks.info

files *(continued)*
restoring, 262
previous versions, 163–166
System File Checker, 239–240
restoring from backups, 61–62
restoring Windows, 320–321
Search
troubleshooting, 129–130
structure, 199–202
System File Checker, 239–240
temporary, 262
clearing, 72–73
vbs, 259
viruses (hidden), 161
writing to disks
troubleshooting permission issues, 121–125
filter
event logs, 374
filters
phishing, 48
spam, 48
finding
boot log, 242
files
troubleshooting Search, 129–130
hard disks in My Computer, 322
registry information, 419
firewalls, 47
ShieldsUp! test, 402
troubleshooting WI-FI networks, 125
updates, 47
Windows Firewall, 23–26, 401–403
Advanced security settings, 403–411
port control for routers, 411–412
resetting, 404
troubleshooters, 404
Windows Remote Desktop, 280
Windows Remote Desktop, 278, 280
firmware, 95
/FixBoot switch, 252
fixed VHD files, 112
/FixMbr switch, 252
Flash drives
blocking, 90–91
encrypting with BitLocker, 43
folders
AppData, 259, 260
Backup and Restore, 57–60
Boot, 258, 259, 262
debug, 261
Device Driver, 259
diagnostics, 261
Drivers, 259
DriverStore, 259
encrypting, 350–351
Globalization, 202, 261
Help, 258
hidden, 201
INF, 262
LiveKernelReports, 262
logs, 261
Logs, 262
Media, 261
ModemLogs, 262
NTUSER.DAT, 260–261
operating system, 257–260
personalization, 261
Public, 200
Resources, 202, 261
Root, 200
Security, 260
ServiceProfiles, 260
Shared Folders (Computer Management Console), 90
Shell user
moving, 57–58
structure, 199–202
System32, 202, 262
Users, 200, 324

www.it-ebooks.info

Web, 261
Windows, 200, 201
Windows.old, 317, 317–318
winsxs, 259
WinSxS, 262
X:\Users\AppData, 259
X:\Windows\Boot, 258
X:\Windows\debug, 261
X:\Windows\diagnostics, 261
X:\Windows\Downloaded Program Files, 262
X:\Windows\Globalization, 261
X:\Windows\Help, 258
X:\Windows\inf, 258
X:\Windows\LiveKernelReports, 262
X:\Windows\Logs, 262
X:\Windows\Media, 261
X:\Windows\ModemLogs, 262
X:\Windows\Prefetch, 262
X:\Windows\Resources, 261
X:\Windows\Security, 260
X:\Windows\ServiceProfiles, 260
X:\Windows\SoftwareDistribution, 262
X:\Windows\System32, 258
X:\Windows\Temp, 262
X:\Windows\Web, 261
X:\Windows\winsxs, 259

fragmentation, 69–74
Disk Defragmenter, 396–397

freeware, 75

G

game controllers, 183

General tab (Task Scheduler), 371

General tab (Windows Firewall With Advanced Security management panel), 405–406

Gibson Research, 293

Gibson Research Corporation, 51

Gibson, Steve, 51, 291, 293

Glary Utilities, 73

Globalization folder, 202, 261

Google Chrome, 239

GoToAssist, 290

gpedit.msc, 87–88

graphics
troubleshooting, 126–128

graphics cards, 97, 300
resolution, 306
screen resolution, 306

graphics drivers
common problems, 181–182

GRC SpinRite, 341–343

green bar
shopping online, 49

grounding PCs, 93

group policies, 87–91

Group Policies
registry, 416

Group Policy
Windows Update, 22–23

Group Policy Editor, 87–91
blocking access to removable storage, 90–91

guest accounts, 83

Guest Mode, 50

H

hard disk drives
SMART (Self-Monitoring, Analysis, and Reporting Technology). ***See*** SMART

hard disks, 298–299
backups, 4
BitLocker, 362
defragmenting, 69–71
encrypting with BitLocker, 43–45, 364
external disks, 43
external
blocking, 90–91
finding in My Computer, 322
fragmentation
Disk Defragmenter, 396–397
GRC SpinRite, 341–343

www.it-ebooks.info

hard disks *(continued)*
moving files away from Windows, 12–13
restoring, 4
Ashampoo WinOptimizer, 344
O&O Disk Recovery, 344
restoring data plugging into other PCs, 321–324
size, 7
SpinRite
Surface Analysis Monitor, 342
SSDs (Solid State Disks)
SpinRite, 343
writing files to
troubleshooting permission issues, 121–125
hard drives, 97
IDE (Integrated Drive Electronics) drives, 298
hardware
all-in-one PCs, 301–303
BIOS
viruses, 159–161
BIOS (Basic Input Output System), 94–96
resetting, 307–309
cases, 98
compatibility
Microsoft list, 171
desktop PC cases, 295
devices
diagnosing problems, 205
displaying, 377
encrypting with BitLocker, 43–45
expansion cards, 97, 301
fans, 301
graphics cards, 300
screen resolution, 306
hard disks, 298–299
hard drives
restoring data, 321–324
IRQs (interrupt requests) conflicts, 209
keyboards, 301
laptops, 301–303
electricity, 304
memory, 97, 298
mice, 301
minimal hardware boots, 306–307
monitors, 101
troubleshooting, 135
motherboards, 94–95, 296–297
Basic Input Output System (BIOS), 94–96
Clear CMOS jumper, 308
Northbridge and Southbridge chipset, 96
sockets, 94
netbooks, 301–303
optical drives, 300
partitions
restoring data, 321–324
peripherals, 100–101
power supplies, 98, 102, 295–296
connectors, 305
jump-starting PCs, 309
laptops, 304
processors, 96, 297–298
Performance Monitor, 387
riser cards, 97
searching for in Device Manager, 185–187
sockets, 94
static electricity
safety, 304
surge protectors, 102
System Monitor
Ubuntu Linux, 331–332
unplugging, 209–210
utilities, 211
Windows 7 certification, 75
Hardware Resources (System Information tool), 225
headphones
troubleshooting, 136
help
Internet solutions, 273–277

www.it-ebooks.info

Microsoft Answers, 276–277
Microsoft Support website, 274–276
Microsoft TechNet, 276–277
Microsoft Windows 7 Solution Center, 274–275
Problem Steps Recorder, 285–287
Remote Desktop
Ubuntu Linux, 330–331
third-party software
Acronis Disk Director, 292
Acronis True Image, 291, 313
GoToAssist, 290
Norton Ghost, 291, 313
Paragon Partition Manager, 291
Sisoftware Sandra, 289–290
SpinRite, 291
Windows Memory Diagnostic, 291
Windows Sysinternals, 290
Zinstall zPOD, 290
third-party websites
Annoyances, 293
ATI support, 293
Computing.net, 292
Gibson Research, 293
How-To Geek, 292
Long Climb, The, 294
MSDN, 293
NVidia, 293
Tech PC Forums, 292
Tom's Hardware, 292
Within Windows, 293
Windows Help, 289
Windows Remote Assistance, 281–285
Windows Remote Desktop, 278–280
Help folder, 258
hibernate mode, 133–134
hidden devices
Device Manager, 185–187
displaying, 377
hidden extensions (file)
viewing, 257
hidden files, 201
viewing, 257
hidden folders, 201
hidden viruses, 161–162
History tab (Task Scheduler), 371
HKEY_CLASSES_ROOT, 414
HKEY_CLASSES_ROOT (registry), 247
HKEY_CURRENT_CONFIG, 414
HKEY_CURRENT_CONFIG (registry), 247
HKEY_CURRENT_USER, 414
HKEY_CURRENT_USER (registry), 247
HKEY_LOCAL_MACHINE, 414
HKEY_LOCAL_MACHINE (registry), 247
HKEY_USERS, 414
HKEY_USERS (registry), 247
Holmes, Sherlock (Sign of Four), 205
home users
Windows Remote Assistance, 281–285
How-To Geek, 292
human interface devices, 183

I

IBM
error codes, 439
icons
padlock
identifying attacks, 144–145
IDE (Integrated Drive Electronics) drives, 298
identifying
attacks, 144–152
browser plug-ins, 148–149
malicious anti-malware software, 150–151
malicious websites, 149–150
padlock icon, 144–145
phishing, 146–147
spam, 146–147
toolbars, 147–148

www.it-ebooks.info

identity theft, 49, 50
image backups, 314
Windows System Image Backup, 314–316
image files
creating for slipstreamed installation DVD creation, 270
images
Windows
restoring on other PCs, 319–321
inbound rules
Windows Firewall, 25
Inbound rules
adding, 406–409
Inbound Rules section (Windows Firewall With Advanced Security management panel), 406–407
incremental backups, 66
indexing options
Performance Information and Tools, 383
Indexing Options
accessing, 129
Indexing Options dialog box, 383
inf files, 258
INF folder, 258, 262
installation disc
Linux, creating, 335–336
installation DVD
restoring Windows 7 from, 314
slipstreamed. ***See*** slipstreamed installation DVDs
System File Checker, 239–240
Windows 7
creating slipstreamed installation DVDs, 270–272
install disc
restoring Windows 7 from, 64–65
Startup Repair, 178–179
installing
compared to upgrading, 4–6
device drivers, 187–190
reinstalling, 190–191
Internet Explorer
reinstalling, 237–238
operating systems in Windows Virtual PC, 116–117
software
media player software, 212
software categories, 211
stability, 75
Windows functionalities, 212
Windows
custom installs, 315–317
Windows 7
annual reinstallation, 77
clean installs, 4–6
for slipstreamed installation DVD creation, 267–270
on VHDs (virtual hard disks), 111–112
preventing problems, 4
system preferences, 7–12
Integrated Drive Electronics (IDE) drives, 298
integrity of files
System File Checker, 239–240
Interner browsers
security, 48
Internet
connections
Linux, 330–331
privacy, 152–153
searches
processes, 208
searching for help, 273–277
security, 49
Internet browsers
clearing temporary files, 72–73
Google Chrome, 239
Internet Explorer. ***See*** Internet Explorer
Mozilla Firefox, 239
plug-ins
identifying attacks, 148–149
Internet Explorer
add-ons
disabling, 231–232
managing in Control Panel, 234–235

www.it-ebooks.info

running without, 233–234
Browser Ballot Screen alternatives, 238–239
factory resetting, 235–237
installing
reinstalling, 237–238
security, 35
starting
resetting when IE doesn't start, 237
turning off, 237
updates, 238
Internet options dialog box, 237
interrupt requests. *See* IRQs (interrupt requests)
invitations
Windows Remote Assistance, 283
IRQs (interrupt requests)
conflicts, 209–210
ISO files
burning
Linux, 335–336

J

Jscript
registry, 417
jumpers
Clear CMOS, 308
jump-starting PCs, 309

K

Karp, David A., 293
keyboards, 100–101, 301
cleaning, 301
troubleshooting, 126–128
keyboard shortcuts, 431–437
keys
AES (Advanced Encryption Standard), 361
EFS (Encrypted File System)
restoring, 352–354
registry, 415
adding, 417–418
backups, 418
deleting, 417–418
editing, 417–418
names, 419
Knoppix, 335

L

laptops, 301–303
cleaning, 99
electricity, 304
Last Known Good Configuration, 176–177
legacy code, 35
security, 35
updates, 21
legacy programs
compatibility, 28–33
Program Compatibility Assistant, 29–30
legacy support
processors, 37
updates, 36
Windows 8, 203
Windows vNext, 37–38
Windows XP Mode, 36–37
Let Me Choose option, 58
Let Windows Choose option, 58
licensing
booting Windows 7 from VHDs, 111
Linux
backup ISOs, 333
boot discs, 326
burning CDs/DVDs, 333–334
creating installation disc, 335–336
creating pen drives, 335–336
Debian, 335
distributions, 325, 334–335
Fedora, 335
Internet connectivity, 330–331
Knoppix, 335
printing douments, 329
restoring systems/data, 325–330

www.it-ebooks.info

Linux *(continued)*
software, 330–332
SuSe, 335
System Monitor, 331–332
system testers, 332–333
Ubuntu. ***See*** Ubuntu Linux
Linux disc ISO, 326
LiveKernelReports folder, 262
loading screen, 182
troubleshooting, 135
Local Group Policy Editor window, 22
local policies, 89–90
Local Security Policy Editor, 89–90
Local Security Policy window, 88, 355
Local Users and Groups option, 376
locations
PCs, 98
logs, 261
Action Center, 18
event logs
filtering, 374–375
SpinRite, 341
Logs folder, 262
Long Climb website, 294

M

Magic Card, 51
maintenance. *See also* performance
PCs, 50
Windows 7
annual reinstallation, 77
Ashampoo Winoptimizer, 74
auto-running software, 76
CCleaner, 73
clearing temporary files, 72–73
defragmenting hard disks, 69–71
Disk Cleanup, 71–72
Glary Utilities, 73
installing software, 75
PC Tune-Up, 74
Windows Update, 76
Maintenance section
Action Center, 18
malicious anti-malware software, 150–151
malicious toollbars, 148
malicious websites
attacks, 149–150
malware. *See* anti-malware software
anti-malware
Windows Defender, 26–27
Malwarebytes, 39, 143
malware software
installing after Windows 7 installation, 7
Manage Add-ons window, 232
management, computer
Computer Management console, 369–379
accessing, 369
applications, 378–379
Device Manager, 377
Local Users and Groups option, 376
services, 378–379
Shared Folders option, 376
system tools, 370–377
Windows Management Instrumentation (WMI), 379
managing
Internet Explorer add-ons in Control Panel, 234–235
services, 244–246
user accounts, 80–86
administrator passwords, 81–83
guest accounts, 83
Parental Controls, 84–87
manually setting compatibility, 170–172
manuals
CDs, 50
McAfee Stinger, 154–155
Media folder, 261
media player software, 212

www.it-ebooks.info

memory, 97, 298
static electricity
safety, 304
virtual
settings, 381
virtual memory
changing size, 9–10
Windows 7 editions, 423
Windows Memory Diagnostic option, 253–254
Memory tab (Resource Monitor), 223–224, 394, 395
menus
Boot
BCDEdit, 252
repairing with bootrec.exe, 251–252
messages
Windows
Action Center, 18
mice, 100–101
cleaning, 301
microphones
troubleshooting, 136
Microsoft Answers, 276–277
Microsoft Fix it Center, 195
Microsoft Internet Explorer. *See* Internet Explorer
Microsoft Knowledge Base
website, 206
Microsoft Live Essentials Suite, 212
Microsoft Management Console (MMC)
logs, 261
registry, 416
Microsoft Security Essentials, 28, 38, 139
Microsoft SkyDrive, 62
Microsoft Support website, 274–276
Microsoft TechNet, 276–277
Microsoft Windows 7 Solution Center, 274–275
Microsoft Windows Malicious Software Removal Tool, 39, 142–143
minimal hardware boots, 306–307
minus (-) sign
Internet searches, 273, 274
Mkdir command, 253
MMC (Microsoft Management Console)
programs, 259
registry, 416
ModemLogs folder, 262
Monitoring
Windows Firewall With Advanced Security management panel, 410–411
monitors, 101
troubleshooting, 135
More command, 253
motherboards, 94–95, 296–297
Basic Input Output System (BIOS), 94–96
blue screen of death (BSOD), 320
Clear CMOS jumper, 308
graphics cards, 300
Northbridge and Southbridge chipset, 96
sockets, 94
static electricity
safety, 304
mouse drivers
troubleshooting, 126–128
Move command, 253
moving
files away from Windows 7, 12–13, 53–57
Disk Cleanup Wizard, 53–54
Shell user folders, 57–58
shrinking/extending/creating partitions, 55–57
Shell user folders, 57–58
Mozilla Firefox, 239
Mozy, 62
MSConfig, 11–12, 76
accessing, 76, 241
diagnostic startups, 241–243
troubleshooting Windows startup, 131–132
MSDN website, 293

www.it-ebooks.info

My Computer
finding hard disks, 322

N

names
registry keys, 419
virtual hard disks (VHD), 109
NAS (network attached storage), 66
Nero, 62
netbooks, 301–303
Network Access Protection, 19
network attached storage (NAS), 66
networks
backups, 16, 59
monitoring, 395
WI-FI
troubleshooting, 125
Never Notify setting (UAC), 42
New Connection Security Rule Wizard, 410
New Technology File System (NTFS), 109
New Technology (NT) versions, 199
No Operating System Found, 135
Northbridge and Southbridge chipset, 96
Norton Ghost, 291, 313
Norton Internet Security/Norton 360, 28, 39, 140
notebooks
cleaning, 99
notification area
Action Center, 17
notifications
Action Center, 19
program compatibility, 173–175
User Account Control (UAC), 40
not, using in Internet searches, 274
ntblog.txt, 241–243
NTFS (New Technology File System), 109
removable drives, 347
NTI Shadow, 62, 76
NT (New Technology)
versions, 199
ntuser.dat, 246–249, 321
NTUSER.DAT folder, 260–261
nVidia, 293

O

ocx files, 259
online
devices, 135
online accounts
confirmation links, 146
online shopping
security, 49
online virus scanners
repairing damage from attacks, 153–154
O&O Disk Recovery, 344
opening
ports
Windows Firewall, 25–26
OpenOffice, 327
operating system files, 257–260
operating systems. *See also* Windows; Windows 7
compared to Windows 7, 202–203
installing in Windows Virtual PC, 116–117
Linux
burning CDs/DVDs, 333–334
creating installation disc, 335–336
distributions, 334–335
software, 330–332
system/data restores, 325–330
managing services, 244–246
No Operating System Found, 135
running multiple OSes on different cores, 37
UNIX, 203
virtualization, 103
compared to dual booting, 104
Windows 7. ***See*** Windows 7
optical drives, 300

www.it-ebooks.info

optical hard drives, 97
optimizers, 74
or, using in Internet searches, 274
outbound rules
Windows Firewall, 25
Outbound rules
adding, 406–409
Outbound Rules section (Windows Firewall With Advanced Security management panel), 406–407

P

padlock icon
identifying attacks, 144–145
shopping online, 49
panels
Action Center, 18, 19
Services, 244–246
System and Security, 9
Windows Firewall With Advanced Security management, 403–410
Paragon Partition Manager, 291
Parental Controls, 84–87
partitions
backups, 4
size, 7
creating, 55–57
custom installs, 317–318
defragmenting, 71
encrypting with BitLocker, 43–45
errors
SpinRite, 343
extending, 55–57
managing in Ubuntu, 329
moving files away from Windows, 12–13
restoring data, 321–324
shriking, 55–57
size, 7
splitting data across for backups, 5
virtual hard disks (VHD), 108
Passware Kit Forensic, 364
passwords, 147–148
administrator
user accounts, 81–83
cracking with EnCase Forensic, 360
pasting
in Command Prompt window, 114
PCs
all-in-one, 301–303
BIOS (Basic Input Output System), 94–96
resetting, 307–309
cases, 98, 295–296
cleaning, 98
discarding, 50
erasing, 50
expansion cards, 97, 301
fans, 301
graphics cards, 300
screen resolution, 306
grounding, 93
hard disks, 298–299
jump-starting, 309
laptops, 301–303
electricity, 304
locations, 98
maintenance, 50
manuals, 50
memory, 97, 298
minimal hardware boots, 306–307
motherboards, 94–95, 296–297
Basic Input Output System (BIOS), 94–96
Northbridge and Southbridge chipset, 96
sockets, 94
netbooks, 301–303
optical drives, 300
performance tools, 229–230
power supplies, 98, 102, 295–296
processors, 96, 297–298
removing viruses using, 158–159

www.it-ebooks.info

PCs *(continued)*
repairing
system repair disc, 250–254
restoring data, 321–324
restoring Windows images, 319–321
riser cards, 97
security, 51
sleeping options, 133–134
sockets, 94
static electricity, 93
safety, 304
surge protectors, 102
PC Tune-Up, 74
PEBCAK (Problem Exists Between Chair And Keyboard), 79
pen drives
Linux, creating, 335–336
performance. *See also* maintenance
defragmenting hard disks, 69–71
Performance Information and Tools, 217–218, 380–398
accessing, 217
Advanced Tools, 385–398
Disk Defragmenter, 396–397
Event Log, 386
Performance Monitor, 386–393
Resource Monitor, 393–395
System Information panel, 396
Task Manager, 396
Computer Management console, 227–229
Disk Cleanup, 385
Event Log, 219–221
indexing options, 383
Performance Monitor, 222–223
power settings, 383
Resource Monitor, 223–224
System Health Report, 226–228
System Information tool, 224–225
Visual Effects, 380–382
Windows Task Manager, 224
Performance Information and Tools window, 218
Performance Monitor, 222–223, 386–393
adding counters to, 387
Data Collector Sets, 388–393
performance tools, 229–230
peripherals, 100–101
permissions
Windows Firewall, 24–25
writing files to disk
troubleshooting, 121–125
personal information, 144
personalization folders, 261
PGP (Pretty Good Privacy) encryption, 347
phishing, 146–147
email, 48
filters, 48
Phoenix BIOS beep codes, 440–445
plug-ins
browsers
identifying attacks, 148–149
plus (+) sign
Internet searches, 273, 274
policies
Application Control Policies, 89–90
group policies, 87–91
local, 89–90
restoring folders, 263
ports
managing firewall rules, 406
router control, 411–412
Windows Firewall
rules, 25–26
power cables
monitors, 101
Power Options dialog box, 384, 385
Power Options panel, 383
Power Options section, 133–134
power settings, 383

www.it-ebooks.info

power supplies, 98, 102, 295–296
connectors, 305
jump-starting PCs, 309
laptops
electricity, 304
spikes, 102
Pretty Good Privacy (PGP) encryption, 347
Previous Versions
accessing, 163
backups, 165, 166
restoring previous versions of files, 163–166
settings, 164
printing
in Linux, 329
privacy, 49, 144
Internet, 152–153
Problem Exists Between Chair And Keyboard (PEBCAK), 79
Problem Steps Recorder, 285–287
accessing, 285
auto-launching, 379
process
monitoring, 393–395
processes
compared to applications and services, 208
definition, 208
Internet searches, 208
Processes tab (Windows Task Manager), 207
processors, 96, 297–298
graphics cards, 300
legacy support, 37
Performance Monitor, 387
static electricity
safety, 304
product keys, 8
program compatibility
Microsoft list, 171
notifications, 173–175
Program Compatibility troubleshooter, 172–173
troubleshooting, 170–171
manually setting, 170–172
Windows XP Mode, 175
Program Compatibility Assistant, 29–30
Program Compatibility troubleshooter, 172–173
program files, 200
programs
compared to processes and services, 208
compatibility
Program Compatibility Assistant, 29–30
Windows XP Mode, 31–33
dupliware, 211
exiting
system tray, 206–207
Microsoft Management Console, 259
shutting down
End Process Tree option, 207
Safe Mode, 208–209
Windows Task Manager, 207–208
Programs And Services tab (Windows Firewall With Advanced Security management panel), 406
Programs Only setting (UAC), 42
Properties dialog box, 170–171, 245, 379
Resources tab, 209
protocols
managing firewall rules, 406
TCP/IP (Transport Control Protocol and Internet Protocol), 406
Public folder, 200
Public Key Policies section, 355

Q

quotes
Internet searches, 273

R

RAID (Redundant Array of Independent Disks). *See* RAID
/R command, 250
Rd command, 253

www.it-ebooks.info

reading
BitLocker encrypted hard disks, 362
Event Log, 221
Windows files in Linux
EFS (Encrypted File System), 328
reattaching
virtual hard disks (VHD), 110
rebooting, 214
recording problems (Problem Steps Recorder), 286
recovering
data
Advanced EFS Data Recovery, 360
Cipher.exe, 360
EFS (Encrypted File System) files, 359
Recovery tab (Properties dialog box), 379
Redundant Array of Independent Disks. *See* RAID
.REG files
registry, 416
REG_BINARY, 415
REG_DWORD, 415
REG_EXPAND_SZ, 415
REG_FULL_RESOURCE_DESCRIPTOR, 415
regional settings, 11
registry, 246–249, 260–261
backups, 249, 416–417
copying files, 321
finding information, 419
Group Policies, 416
Jscript, 417
keys
adding, 417–418
backups, 418
deleting, 417–418
editing, 417–418
names, 419
MMC (Microsoft Management Console), 416
optimizers, 74
.REG files, 416
Registry Editor
accessing, 413
restoring, 416–417
sections, 414
settings, 247, 413, 415
removing, 248–249
VBScript, 417
WMI (Windows Management Instrumentation), 417
Registry Editor, 246
accessing, 246, 413
REG_LINK, 415
REG_MULTI_SZ, 415
REG_NONE, 415
REG_QWORD, 415
REG_RESOURCE_LIST, 415
REG_RESOURCE_REQUIREMENTS_LIST, 415
REG_SZ, 415
reinstalling
data loss, 4
Reliability History
viewing, 19
Remote Assistance, 281–285
connections, 282–286
Easy Connect, 283
invitations, 283
remote computers
firewalls, 278
Windows Remote Desktop, 280
Remote Desktop
Ubuntu Linux, 330–331
Windows Remote Assistance, 281–285
Windows Remote Desktop, 278–280
Remote Desktop, 278–280
Remote Desktop Connection dialog box, 279
Remote Desktop in Ubuntu, 330–331
removable drives
EFS (Encrypted File System), 347–360
NTFS (New Technology File System), 347

www.it-ebooks.info

removable optical discs
backups, 66
removable storage
blocking access to, 90–91
removing
device drivers, 190–191
registry settings, 248–249
viruses
manually, 157–158
Ren command, 253
repair disc. *See* system repair disc
repairing
Boot menu with bootrec.exe, 251–252
damage from attacks, 153–162
anti-malware software, 153
BIOS viruses, 159–161
McAfee Stinger, 154–155
onlne virus scanners, 153
removing viruses, 157–158
restoring Windows 7 from backups, 159
Safe Mode, 155–156
viruses hiding, 161–162
PCs
system repair disc, 250–254
repelling attacks, 137–144
Action Center, 137–138
anti-malware software, 140–144
anti-virus software, 138–140
reports
SpinRite, 341
system health reports, 397
rescue tools
Ashampoo WinOptimizer, 344
GRC SpinRite, 341–343
O&O Disk Recovery, 344
Zinstall, 337
zPOD, 320, 337–340
Reset Internet Explorer Settings section, 235–237
resolution
graphics cards, 306
Resource Monitor, 223–224, 393–395
Resources By Connection command, 377
Resources By Type command, 377
Resources folder, 202, 261
Resources tab (Properties dialog box), 209
restarting
computers
after software crashes, 214
disabling automatic restarts, 215
restore points
creating, 168
Restore section (Backup And Restore window), 61–62
restoring
Backup and Restore, 57–60
data
with Linux distributions, 325–330
with other PCs, 321–324
data rom backups, 61–62
EFS (Encrypted File System) keys, 352–354
files, 262
previous versions, 163–166
System File Checker, 239–240
files from backups, 61–62
hard disks, 4
Internet Explorer
factory resetting, 235–237
registry, 416–417
Windows
custom installs, 315–317
file by file, 320–321
from backups, 313–315
images on other PCs, 319–321
Windows 7
from backups, 159
from system image, 63–64
repair disc, 249–254
zPOD, 338–340

www.it-ebooks.info

restoring *(continued)*
Windows 7 from system repair disc, 64–65
Windows 7 with System Restore, 168–169
riser cards, 97
Rivera, Rafael, 293
Rogev
Magic Card, 51
Roll Back Driver, 193–194
rolling back
device drivers, 193–194
Root folder, 200
routers
blocks
troubleshooting, 412
port control, 411–412
rules
Windows Firewall, 25–26
managing, 405–406
setting Connection Security Rules, 410
running
Internet Explorer without add-ons, 233–234

S

Safe Boot checkbox, 241–243
Safe Mode, 176–177, 241–243, 243, 254
repairing damage from attacks, 155–156
shutting down programs, 208–209
safety
static electricity, 304
SATA (Serial ATA) connectors, 298–299
scanners
virus
repairing damage from attacks, 153–154
scanning engines
Norton Internet Security/Norton 360, 39
/ScanOS switch, 252
scheduling
Data Collector Sets, 393
Scope tab (Windows Firewall With Advanced Security management panel), 406
screen resolution
graphics cards, 306
screenshots, annotating (Problem Steps Recorder), 286
scripts
Copype.cmd, 265
Visual Basic VBScript, 259
Search
troubleshooting, 129–130
search engines
Internet searches, 273
searches
Internet
processes, 208
troubleshooters, 399
searches (Internet), 273–277
secpol (Security Policies)
EFS certificates, 355
sections
registry, 414
security
anti-malware software. ***See*** anti-maleware software
anti-spyware software, 48
anti-virus software. ***See*** anti-virus software
BitLocker, 43–47
browsers, 48
common Windows problems, 213
email attachments, 48
encryption
EFS (Encrypted File System), 347–360
File Encryption Certificate Manager, 359
PGP (Pretty Good Privacy), 347
firewalls, 47
ShieldsUp! test, 402
updates, 47
Windows Firewall, 401–403
Windows Remote Desktop, 278, 280
Internet, 49
Internet Explorer, 35
legacy code, 35

www.it-ebooks.info

PCs, 51
personal information, 144
phishing filters, 48
restoring folders, 263
shopping online, 49
spam filters, 48
User Account Control (UAC), 40–43
settings, 41–42
user errors to avoid, 47–50
Windows, 35
Windows Firewall, 23–26
Windows Update, 48
Windows XP Mode, 32
Security folder, 260
Security section (Action Center), 402
Self-Monitoring, Analysis, and Reporting Technology. *See* SMART
Serial ATA (SATA), 298–299
Service Pack
troubleshooting, 130–131
service packs
slipstreaming, 272
System File Checker, 240
ServiceProfiles folder, 260
services
compared to applications and processes, 208
Computer Management console, 378–379
definition, 208
diagnosing with boot log, 241–243
managing, 244–246
recovery specialists, 344
shutting down, 208
turning off, 245
Services panel, 244–246, 378–379
accessing, 244
settings
Action Center, 19
BIOS, 95–97
Boot Order, 64
Change Advanced Power Settings, 134
Computer Configuration (Group Policy Editor), 87–88
DEP (Data Execution Prevention), 382
Group Policy Editor, 87
Previous Versions, 164
Program Compatibility Assistant, 30
registry, 247, 413, 415
removing, 248–249
User Account Control (UAC), 41–42
User Configuration (Group Policy Editor), 87–88
virtual memory, 381
Wait To Kill Service Timeout, 132–133
Windows 7 installation
changing, 8–11
Windows Firewall, 24–25
Windows Firewall Advanced security, 403–411
Windows Remote Desktop, 279
Settings tab (Task Scheduler), 371
setup
EFS (Encrypted File System), 348–351
Shared Folders (Computer Management Console), 90
Shared Folders option, 376
shareware, 7, 75
Shell user folders
moving, 57–58
ShieldsUp! test, 402
shopping online
security, 49
shortcut keys, 431–437
Show Hidden Devices command, 377
Show Hidden Devices option, 185
shrinking
partitions, 55–57
shutting down
programs
End Process Tree option, 207
Safe Mode, 208–209
Windows Task Manager, 207–208
services, 208

www.it-ebooks.info

shutting down *(continued)*
software to diagnose problems, 205
Windows
troubleshooting, 132–133
Sign of Four, 205
Sisoftware Sandra, 289–290
size
hard disks, 7
virtual hard disks (VHD), 108
SkyDrive, 46, 62
sleeping options, 133–134
slipstreamed installation DVDs
creating, 263–272
new image file creation, 270
requirements, 264
Windows 7 fresh install, 267–270
Windows 7 installation DVD, 270–272
WinPE (Windows Pre-Installation Environment), 264–267
slipstreaming
definition, 263
service packs, 272
SMART
(Self-Monitoring, Analysis, and Reporting Technology), 100
smart cards
EFS (Encypted File System), 356–359
sockets, 94
software
Advanced EFS Data Recovery, 360
anti-malware, 38–40, 140–144
malicious, 150–151
Malwarebytes, 39, 143
Microsoft Security Essentials, 38
Microsoft Windows Malicious Software Removal Tool, 142–143
repairing attack damage, 153
SpyBot Search & Destroy, 39
Spyware Blaster, 144
Spyware Terminator, 39, 76, 143
Windows Defender, 39, 141–142
anti-spyware, 48
anti-virus, 27–28, 38–40
AVG Anti-Virus/AVG Security Suite, 140
installing after Windows 7 installation, 7
Malwarebytes, 39
Microsoft Security Essentials, 38, 139
Microsoft Windows Malicious Software Removal Tool, 39
Norton Internet Security/Norton 360, 39, 140
repelling attacks, 138–140
updates, 47
Windows Virtual PC, 117
Windows XP Mode, 117
Ashampoo WinOptimizer, 344
auto-running, 76
backups
Backup and Restore, 61–62
Nero, 62
NTI Shadow, 62
common Windows problems, 213
compatibility, 28–33
Microsoft list, 171
notifications, 173–175
Program Compatibility Assistant, 29–30
Program Compatibility troubleshooter, 172–173
troubleshooting, 170–171
Windows XP Mode, 175
craplets, 211
crashes
rebooting, 214
dupliware, 211
EnCase Forensic, 360
GRC SpinRite, 341–343
installing
media player software, 212
software categories, 211
stability, 75
Windows functionalities, 212
Linux, 330–332

www.it-ebooks.info

malware
installing after Windows 7 installation, 7
O&O Disk Recovery, 344
OpenOffice, 327
Passware Kit Forensic, 364
product keys, 8
shareware, 7
shutting down to diagnose problems, 205
third-party
slipstreaming, 272
third-party help software
Acronis Disk Director, 292
Acronis True Image, 291, 313
GoToAssist, 290
Norton Ghost, 291, 313
Paragon Partition Manager, 291
Sisoftware Sandra, 289–290
SpinRite, 291
Windows Memory Diagnostic, 291
Windows Sysinternals, 290
Zinstall zPOD, 290
third-party rescue tools. ***See*** rescue tools
trial version, 7
trialware, 211
updates, 48
after installing new software, 8
legacy support, 36
zPOD, 320, 337–340
Software Environment (System Information tool), 225
Solid State Disks (SSDs)
SpinRite, 343
sound controllers, 183
sound drivers
troubleshooting, 126–128
spam, 146–147
filters, 48
spikes, 102
SpinRite, 291
Surface Analysis Monitor, 342
SpyBot Search & Destroy, 39
spyware
anti-spyware
Windows Defender, 26–27
Spyware Blaster, 144
Spyware Terminator, 39, 76, 143
SSDs (Solid State Disks)
SpinRite, 343
Ssytem Recovery Options
Windows Memory Diagnostic option, 253–254
starting
Internet Explorer
resetting when IE doesn't start, 237
Windows 7
backups, 179
diagnostic startups, 241–243
Last Known Good Configuration, 176–177
Safe Mode, 155–156, 176–177, 254
Startup Repair, 178–179
troubleshooting, 131–132, 175–179
Windows Startup Repair, 177–178
Startup Repair
install DVDs, 178–179
restoring Windows 7, 314
system repair disc, 178–179
startups
dual-boot systems, 6
static electricity, 93
memory cards, 97
safety, 304
step-by-step approach
diagnosing problems, 205–210
unplugging hardware, 209–210
minimum Windows configuration, 206–208
storage
backups, 66–67
storing
backups, 314
strong passwords, 147–148

www.it-ebooks.info

subscriptions
Microsoft TechNet, 277–279
support
legacy, 35–36
processors, 37
updates, 36
Windows 8, 203
Windows XP Mode, 36–37
third-party software
Acronis Disk Director, 292
Acronis True Image, 291, 313
GoToAssist, 290
Norton Ghost, 291, 313
Paragon Partition Manager, 291
Sisoftware Sandra, 289–290
SpinRite, 291
Windows Memory Diagnostic, 291
Windows Sysinternals, 290
Zinstall zPOD, 290
third-party websites
Annoyances, 293
ATI support, 293
Computing.net, 292
Gibson Research, 293
How-To Geek, 292
Long Climb, The, 294
MSDN, 293
NVidia, 293
Tech PC Forums, 292
Tom's Hardware, 292
Within Windows, 293
Windows Help, 289
Windows Remote Assistance, 281–285
supports
legacy
Windows vNext, 37–38
Surface Analysis Monitor, 342
surge protectors, 102
SuSe, 335
switches
/FixBoot, 252
/FixMbr, 252
/ScanOS, 252
System32 folder, 202, 258, 262
System and Security panel, 9
System and Security section (Action Center), 21
System Configuration dialog box, 243
System File Checker, 239–240, 263
accessing, 239
creating slipstreamed installation DVDs, 263–272
new image file creation, 270
requirements, 264
Windows 7 fresh install, 267–270
Windows 7 installation DVD, 270–272
WinPE (Windows Pre-Installation Environment), 264–267
resetting Internet Explorer, 237
service packs, 240
System Health Report, 226–228
system health reports, 397
system image
restoring Windows 7 from, 63–64
System Image Recovery, 179–180
System Information panel, 396
System Information tool, 224–225
System Monitor
Linux, 331–332
system preferences
installing Windows 7, 7–12
changing settings, 8–11
MSConfig, 11–12
System Preparation Tool window, 268, 269
System Properties dialog box
Advanced tab, 10
System Recovery Options
accessing, 250

www.it-ebooks.info

system repair disc, 249–254
advanced options, 250
restoring Windows 7 from, 64–65
Startup Repair, 178–179
system rescue disc
creating, 63–64
System Restore, 166–170
configuring, 167–168
creating restore points, 168
Previous Versions, 163–166
restoring Windows 7, 168–169
undoing changes, 169–170
viruses, 161
system restores
Linux distributions, 325–330
system testers
Linux, 332–333
system tools, 370–377
Event Viewer, 373–376
attaching tasks to events, 374–375
creating custom views, 375–376
event log filtering, 374–375
Task Scheduler, 370–372
system tray
exiting programs, 206–207

T

Task Manager, 396
shutting down programs, 207–208
tasks
attaching to events, 374–375
Task Scheduler, 370–372
Task Scheduler (Computer Management console), 90–91
tasks (Task Scheduler)
adding, 372
displaying, 372
exporting, 372
TCP/IP (Transport Control Protocol and Internet Protocol), 406
Tech PC Forums, 292
temporary files
clearing, 72–73
temproary files, 262
tests
ShieldsUp!, 402
third parties
slipstreaming Windows service packs, 272
Tom's Hardware, 292
toolbars
identifying attacks, 147–148
toollbars
malicious, 148
TPM Administration link, 362
Transparent Operation mode, 361
Transport Control Protocol and Internet Protocol (TCP/IP), 406
trial version software, 7
trialware, 75, 211
Triggers tab (Task Scheduler), 371
Trojans, 150
Antivirus 2010, 150
troubleshooters, 398–400, 404
Action Center, 194–195
searching, 399
troubleshooting
devices, 101
Troubleshooting panel, 398
TrueCrypt, 46
turning off. *See* disabling
computers after software crashes, 214
EFS (Encrypted File System), 354
Internet Explorer, 237
services, 245
Type command, 253

U

UAC (User Account Control), 30, 40–43, 79–80
settings, 41–42
System Restore, 166

www.it-ebooks.info

Ubuntu Linux, 334
accessing Windows drive, 327
managing drives, 328
managing partitions, 329
Remote Desktop, 330–331
restoring Windows 7, 325–330
System Monitor, 331–332
system testers, 332–333
undoing
System Restore changes, 169–170
uninstalled programs
removing registry settings, 248–249
uninterruptable power supplies (UPS), 102
UNIX, 203
unplugging
devices
to diagnose problems, 205
hardware, 209–210
Update Install
troubleshooting, 130–131
updates
anti-virus software, 47
device drivers, 192–194
firewalls, 47
installed software, 8
Internet Explorer, 238
legacy code, 21
legacy support, 36
Microsoft Windows Malicious Software Removal Tool, 39, 142–143
security, 21
software, 48
User Account Control (UAC), 40
Windows Defender, 39, 142
Windows Update, 20–23, 48, 76
Internet Explorer, 238
running after Windows 7 installation, 8
troubleshooting, 129
Windows Defender, 26, 142
upgarding
compared to installing, 4–6
UPSes (uninterruptable power supplies), 102
USB3 devices
troubleshooting, 135
USB Flash drives
encrypting with BitLocker, 43
USB Key mode, 361
User Account Control, 19
User Account Control dialog box, 80
User Account Control (UAC), 30, 40–43, 79–80
settings, 41–42
System Restore, 166
user accounts
Guest Mode, 50
managing, 80–86
administrator passwords, 81–83
guest accounts, 83
Parental Controls, 84–87
user acounts
AT Service Account Configuration link, 372
User Authentication mode, 361
User Configuration section (Group Policy Editor), 87
user errors
security, 47–50
users
UAC (User Account Control), 79–80
Users folder, 200, 324
utilities. *See* individual names of
hardware, 211

V

vacuuming PCs, 98
VBScript
registry, 417
vbs files, 259

www.it-ebooks.info

versions
consumer, 199
control
backup programs, 63
New Technology (NT), 199
VHDs (virtual hard disks), 105–115
booting from, 110–115
creating, 105–109
installing Windows 7 on, 111–112
names, 109
reattaching, 110
size, 108
VHDs (virtualization hard disks). *See also* virtualization
video cables
monitors, 101
video controllers, 183
viewing
Data Collector Sets, 392
devices
IRQs (interrupt requests), 209
extensions (file), 257
hidden files, 257
Reliability History, 19
views
custom views
creating, 375–376
virtual hard disks (VHD), 105–115
booting from, 110–115
creating, 105–109
installing Windows 7 on, 111–112
names, 109
partitions, 108
reattaching, 110
size, 108
virtualization, 103. *See also* virtualization hard disks (VHD)
benefits, 105–106
compared to dual booting, 104
Windows Virtual PC, 111
Windows Virtual PCs, 115–117
Windows XP Mode, 36–37, 111, 115–117
virtualization hard disks (VHD). *See also* virtualization
virtual machines, 103, 104
virtual machines (VM)
Zinstall, 337
zPod, 337
zPOD, 320
virtual memory
changing size, 9–10
settings, 381
Virtual PC Management console, 117
viruses. *See also* anti-virus software
anti-virus software, 138–140
backups, 161
BIOS, 159–161
email, 161
email attachments, 48
hidden viruses, 161–162
removing
manually, 157–158
using other PCs, 158–159
System Restore, 161
virus scanners
repairing damage from attacks, 153–154
Visual Basic VBScript scripts, 259
Visual Effects, 380–382
VMs (virtual machines), 103, 104
Zinstall, 337
zPod, 320, 337
vNext, 37

W

Wait To Kill ServiceTimeout setting, 132–133
warning beep codes (BIOS), 94, 439–445
warning triangles (Device Manager), 184
Watson, Doctor (Sign of Four), 205

www.it-ebooks.info

web browsers
clearing temporary files, 72–73
Google Chrome, 239
Internet Explorer. ***See*** Internet Explorer
Mozilla Firefox, 239
plug-ins
identifying attacks, 148–149
security, 48
Web folder, 261
web sites
Acronis Disk Director, 292
Acronis True Image, 291
Advanced EFS Data Recovery, 360
Annoyances, 293
Ashampoo Winoptimizer, 74
ATI support, 293
AVG Anti-Virus/AVG Security Suite, 140
CCleaner, 73
Computing.net, 292
EnCase Forensic, 360
Gibson Research, 293
Gibson Research Corporation, 51
Glary Utilities, 73
GoToAssist, 290
How-To Geek, 292
Long Climb, 294
malicious
attacks, 149–150
Microsoft Answers, 276–277
Microsoft Fix it Center, 195
Microsoft Security Essentials, 139
Microsoft Support, 274–275
Microsoft TechNet, 276–277
Microsoft Windows 7 Solution Center, 274–275
MSDN, 293
Norton Ghost, 291
Norton Internet Security/Norton 360, 140
NTI Shadow, 62
NVidia, 293
Paragon Partition Manager, 291
PC Tune-Up, 74
privacy, 152–153
security, 49
Sisoftware Sandra, 289
SkyDrive, 46
SpinRite, 291
Tech PC Forums, 292
Tom's Hardware, 292
TrueCrypt, 46
Windows Memory Diagnostic, 291
Windows Sysinternals, 290
Windows XP Mode, 33
Within Windows, 293
Zinstall, 337
Zinstall zPOD, 290
websites
Microsoft Knowledge Base, 206
WI-FI networks
troubleshooting, 125
Wi-Fi USB dongles, 101
windows
Backup And Restore, 61–62
BitLocker Drive Encryption, 362
Command Prompt
cutting/pasting in, 114
Local Group Policy Editor, 22
Local Security Policy, 88, 355
Manage Add-ons, 232
Performance Information and Tools, 218
System Preparation Tool, 268, 269
Windows Firewall With Advanced Security, 25–26
Windows
Blue Screen of Death (BSOD), 214–215
configuration
minimum configuration, 206–208
images
restoring on other PCs, 319–321
maintenance, 50

www.it-ebooks.info

messages
Actoin Center, 18
restoring
custom installs, 315–317
file by file, 320–321
from backups, 313–315
security, 35
Windows 1.0, 199
Windows 2.0, 199
Windows 3.1, 199
Windows 7
activating, 8
backups, 14–16, 63–66
common problems, 213
compared to other operating systems, 202–203
editions, 423
features, 425–429
files
System Restore, 166–170
files associations
troubleshooting, 125–126
installation DVD
creating slipstreamed installation DVDs, 270–272
installing
annual reinstallation, 77
clean installs versus upgrades, 4–6
for slipstreamed installation DVD creation, 267–270
on VHDs (virtual hard disks), 111–112
preventing problems, 4
system preferences, 7–12
loading screen, 182
troubleshooting, 135
maintenance
annual reinstallation, 77
Ashampoo Winoptimizer, 74
auto-running software, 76
CCleaner, 73
clearing temporary files, 72–73
defragmenting hard disks, 69–71
Disk Cleanup, 71–72
Glary Utilities, 73
installing software, 75
PC Tune-Up, 74
Windows Update, 76
moving files away from, 12–13, 53–57
Shell user folders, 57–58
shrinking/extending/creating partitions, 55–57
moving files away from Windows 7
Disk Cleanup Wizard, 53–54
partitions
size, 7
restoring
from backups, 159
from system image, 63–64
repair disc, 249–254
zPOD, 338–340
restoring from system repair disc, 64–65
shutting down
troubleshooting, 132–133
starting
backups, 179
diagnostic startups, 241–243
Last Known Good Configuration, 176–177
Safe Mode, 155–156, 176–177, 254
Startup Repair, 178–179
troubleshooting, 131–132, 175–179
Windows Startup Repair, 177–178
troubleshooting when not genuine, 128
versions, 199
WI-FI networks
troubleshooting, 125
writing files to disks
troubleshooting permission issues, 121–125
Windows 7 certification
hardware, 75
Windows 7 Control Panel
System and Security panel, 9
Windows 7 Disk Defragmenter dialog box, 70

www.it-ebooks.info

Windows 8
legacy support, 203
Windows 95, 199
Windows 98, 199
Windows Backup and Restore. *See* Backup and Restore
Windows Defender, 26–27, 39, 141–142
updates, 142
Windows Update, 26
Windows Encrypted File System. *See* EFS
Windows Experience Index, 218
Windows Firewall, 23–26, 401–403
Advanced security settings, 403–411
adding Inbound rules, 406–409
adding Outbound rules, 406–409
managing firewall rules, 405–406
setting Connection Security Rules, 410
advanced settings, 24–25
Diagnose/Repair feature, 26–27
port control for routers, 411–412
resetting, 404
rules, 25–26
settings, 24–25
troubleshooters, 404
Windows Remote Desktop, 280
Windows Firewall with Advanced Security (Local Security Policy Editor), 89
Windows Firewall With Advanced Security management panel, 403
Connection Security Rules, 410
managing firewall rules, 405–406
Monitoring option, 410–411
Windows Firewall With Advanced Security window, 25–26
Windows folder, 200, 201
Windows Help, 289
Windows Management Instrumentation (WMI), 379
registry, 417
Windows Me, 199
Windows Memory Diagnostic, 291
Windows Memory Diagnostic option, 253–254
Windows NT, 199
Windows NT 3.1, 199
Windows NT 4.0, 199
Windows.old folder, 317, 317–318
Windows Pre-Installation Environment (WinPE).
creating, 264–267
Windows registry. *See* registry
Windows Remote Assistance, 281–285
connections, 282–286
Easy Connect, 283
invitations, 283
Windows Remote Desktop, 278–280
firewalls, 278
Windows services
Computer Management console, 378–379
Windows Startup Repair, 177–178
Windows Sysinternals, 290
Windows System Image Backup, 314–316
Windows Task Manager, 224
accessing, 224
shutting down programs, 207–208
Windows Troubleshooting Platform (WTP), 293
Windows Update, 20–23, 48, 76
Group Policy, 22–23
Internet Explorer, 238
running after Windows 7 installation, 8
troubleshooting, 129
Windows Defender, 26, 142
Windows Virtual PC, 111–112, 115–117
anti-virus software, 117
Windows Vista, 199
dual-boot systems, 6
Windows vNext, 37
Windows XP, 199
BitLocker to Go, 362
dual-boot systems, 6
Windows XP Mode, 31–33, 115–117, 175
anti-virus software, 117
security, 32

www.it-ebooks.info

virtualization, 36–37
web site, 33
Windows XP More, 111–112
WinPE (Windows Pre-Installation Environment)
creating, 264–267
winsxs folder, 259
WinSxS folder, 262
wizards
Certificate Export Wizard, 349
Disk Cleanup, 53–54
New Connection Security Rule, 410
WMI (Windows Management Instrumentation), 379
registry, 417
writing
files to disk
troubleshooting permission issues, 121–125
WTP (Windows Troubleshooting Platform), 293

X

/X command, 250
Xcopy command, 253

Z

Zinstall, 337
compared to zPOD, 340
zPOD, 320, 337–340
Zinstall zPOD, 290
zPOD, 320, 337–340
256-bit encryption, 339
compared to Zinstall, 340

www.it-ebooks.info

www.it-ebooks.info

About the Author

Mike Halsey is a technical beta-tester for Microsoft, technology blogger, and teacher of English, Maths, and ICT. He was born on the borders of Surrey, Hampshire, and Berkshire (UK), and now proudly lives in an eco-home in Sheffield with his rescue border collie Jed, whom he dotes on constantly.

He has had a variety of jobs on the way to working in ICT, including spending a few years touring the UK as a club singer and having two photographic exhibitions. His first book, the self-published *Windows 7 Power Users Guide*, went on sale in 2009.

Mike also writes for a variety of technology websites, including *windows7news.com*, *windows8news.com*, *ghacks.net*, *connectedinternet.co.uk*, and his own website *thelongclimb.com*.

Contacting the Author

Mike can be contacted through his website, *www.thelongclimb.com*, and is also on Facebook (*mike.halsey*) and Twitter (*@mike_halsey*).

www.it-ebooks.info

www.it-ebooks.info

www.it-ebooks.info

www.it-ebooks.info

www.it-ebooks.info

www.it-ebooks.info

www.it-ebooks.info

www.it-ebooks.info

www.it-ebooks.info

www.it-ebooks.info

www.it-ebooks.info

What do you think of this book?

We want to hear from you!

To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Tell us how well this book meets your needs—what works effectively, and what we can do better. Your feedback will help us continually improve our books and learning resources for you.

Thank you in advance for your input!

Microsoft Press

Stay in touch!

To subscribe to the *Microsoft Press® Book Connection Newsletter*—for news on upcoming books, events, and special offers—please visit:

microsoft.com/learning/books/newsletter

www.it-ebooks.info