TWEAKING COMPANION

for Windows 8

KOROUSH GHAZI
TWEAKGUIDES.COM

[Version 1.0]

TABLE OF CONTENTS

Table of Contents 2
Copyright & Credits 14
Introduction 15
Using this Book 16
Basic Requirements 16
Different Versions of Windows 16
PC vs. Mobile Devices 16
Where are the Pictures? 16
Why is the Book So Long? 17
Where Do I Start? 17
Recommended Software 17
Problems with the Book 18
Your Responsibilities 18
Basic PC Terminology 19
Bits & Bytes 19
Data 20
PC 20
CPU 20
Motherboard 20
Memory 20
Storage Drives 21
Graphics Card 22
Display Device 22
Sound Card 23
Speakers 23
Power Supply Unit 23
Cooling Devices 23
Case 24
Peripheral 24
Operating System and Software 24
New Features 25
Metro 25
Metro Apps vs. Desktop Programs 26
Local Account vs. Microsoft Account 27
Window Search 27
Desktop 27
File Explorer 28
Optimize Drives 28
Task Manager 28
Internet Explorer 29
Windows Mail 29
Windows Media Center & DVD Playback 29
Power Options 29
Administrator Command Prompt 30
Windows Control Panel & PC Settings 30
Keyboard Shortcuts 30
System Specifications 33
System Information Tools 33
Windows Experience Index 33
Task Manager 33
Windows System Information Tool 34
Device Manager 34
DirectX Diagnostics 34
Sandra 35
CPU-Z 35
GPU-Z 35
HD Tune 35

Backup & Recovery **37**
Windows File History 37
Automated Backups *37*
Restoring Backups *39*
Windows 7 File Recovery 40
Automated Backups *40*
Manual Backups *42*
Managing Backups *42*
Restoring Backups *43*
Organizing Data For Automated Backups 45
System Protection 46
System Restore *47*
Backing Up & Restoring Passwords 48
Setting Up & Restoring a Microsoft Account Password *49*
Backing Up & Restoring a Local Account Password *49*
Gaining Access Without a User Account Password *50*
Storing General Passwords *50*
Other Backup Methods 52
Third Party Drive Imaging Software *52*
Online Backup *53*
Custom Backups *54*
Data Recovery 55
Recovering Deleted Files *55*
Permanently Deleting Files *56*
Low Level Format & Zero Fill *57*
System Recovery 57
System File Checker *58*
Windows Refresh *59*
Windows Reset *60*
Windows Recovery Environment *61*
System Restore *61*
System Image Recovery *61*
Automatic Repair *62*
Command Prompt *62*
Startup Settings *62*
Hardware Management **65**
The BIOS & UEFI 65
General Hardware Management 66
Handling Hardware *66*
Thermal Compounds *67*
Surge Protectors *68*
Power Supply Unit *68*
Cooling *69*
Device Manager 72
Resource Allocation *72*
Device Power Management *74*
Problematic Devices *74*
Disabling or Removing Unused Devices *75*
DeviceS in Metro 76
Devices and Printers 77
Device Stage 78
Overclocking 78
Benefits *79*
Drawbacks *79*
Methodology *80*
Stability *81*
Power Supply Unit *81*
Cooling *81*
Comparing Overclocks *82*
Research *82*
Windows Installation **83**
Choosing a Product Edition 83
OEM vs. System Builder vs. Upgrade *84*
Prior to Installation 85

Check your Hardware and Software for Compatibility ... 85
Disable Unused Resources in the BIOS/UEFI ... 86
Scan for Malware ... 86
Prepare Backups ... 86
Deactivate/Deauthorize Software ... 87
Windows Refresh and Windows Reset ... 87
Custom or Upgrade Install ... 87
Modifying The Windows Installation Media ... 89
Preparing the Drive ... 92
Partitioning ... 92
Formatting ... 94
RAID Configuration ... 96
Storage Spaces ... 97
Dual Boot or Multiboot ... 98
32-bit vs. 64-bit ... 99
Installing Windows ... 101
Web Installation ... 101
Step 1 - Launching the Installer ... 102
Step 2 - Install Updates ... 102
Step 3 - Windows Product Key ... 102
Step 4 - Custom Install - Advanced Options ... 102
Step 5 - Personalize ... 104
Step 6 - Express Settings ... 104
Step 7 - Sign In to Your PC ... 105
Step 8 - Finishing Installation ... 105
Windows Activation ... 106
Failed Activation ... 107
Boot Configuration ... 109
Boot Files ... 109
Accessing The Boot Menu ... 110
Secure Boot ... 110
Boot Configuration Data ... 110
BCDEdit ... 111
Startup and Recovery ... 111
MSConfig ... 112
EasyBCD ... 113
Custom Boot Screen ... 114
Bootdisks ... 114
File Explorer ... 116
Basic Features ... 116
Ribbon ... 116
Search Box ... 118
Address Bar ... 118
Navigation Pane ... 119
Details & Preview Panes ... 122
Status Bar ... 123
Folder Views ... 123
Correctly Setting Folder Views ... 126
Folder Options ... 128
General ... 128
View ... 128
Search ... 130
Personal Folders ... 130
Libraries ... 132
Customizing Libraries ... 133
Disabling Libraries ... 134
Directory Junctions and Symbolic Links ... 135
Advanced Features ... 136
Set File Explorer Startup Folder ... 136
Manipulate Multiple Files ... 137
Explorer Restart substitute for Reboot ... 138
Dual Window Explorer View ... 138
Customize Folder Icons & Folder Pictures ... 138
Expanded Context Menus ... 139

Edit Context Menus ... 139
Edit 'Open With' Context Menu ... 141
Edit 'New' Context Menu ... 141
Edit 'Send To' Context Menu ... 142
Add 'Copy To' and 'Move To' Context Menu Items ... 142
Add 'Open with Notepad' Context Menu Item ... 143
Increase Menu Display Speed ... 143
Fix Changing Folder Views ... 143
God Mode ... 145

Windows Drivers ... **146**
Driver Compatibility ... 146
Finding Compatible Drivers ... 146
Driver Installation Difficulties ... 147
64-bit Compatibility ... 147
Driver Signature ... 148
Signature Warnings ... 148
Signature Verification ... 149
Driver Installation ... 150
Step 1 - Service Packs ... 150
Step 2 - DirectX ... 150
Step 3 - Windows Update ... 150
Step 4 - Motherboard Drivers ... 153
Step 5 - Graphics Drivers ... 154
Step 6 - Sound Drivers ... 155
Step 7 - Peripheral Drivers ... 156
Step 8 - Windows Update Revisited ... 156
Manually Updating or Uninstalling Drivers ... 157
Viewing Driver Details ... 157
Manually Updating Drivers ... 157
Going Back to an Earlier Driver ... 158
Selecting Another Installed Driver ... 159
Uninstalling Drivers ... 159
Removing Stored Drivers ... 160
Driver Verifier ... 162
General Driver Tips ... 163

User Accounts ... **165**
Local Account vs. Microsoft Account ... 165
Local Account ... 165
Microsoft Account ... 166
Setting Up a Microsoft Account ... 166
Microsoft Account Synchronization ... 167
User Account Privileges ... 167
Administrator ... 167
Standard ... 168
Guest ... 168
User Account Strategies ... 168
Number of Users ... 169
Synchronization ... 169
Physical Access ... 170
Data Sensitivity ... 170
Managing User Accounts ... 170
Change Your Account Name ... 171
Change Your Account Type ... 171
Create/Change the Password ... 171
Switch Between Microsoft Account and Local Account ... 172
Sign-in Options ... 172
Add a New User ... 173
Delete the Account ... 173
Change the Account Picture ... 174
Family Safety ... 174
Advanced Settings ... 176
Local & Roaming User Profiles ... 176
Correctly Renaming a User Account ... 177
Advanced User Accounts Control Panel ... 177

Hidden Administrator Account ... 179

Security ... 180

Security Threats ... 180
Viruses & Worms ... 180
Trojan Horses ... 181
Spyware ... 181
Adware ... 181
Rootkits ... 181
Social Engineering ... 181
Windows Action Center ... 182
Security Categories ... 182
Configuring Action Center ... 184
User Account Control ... 184
The UAC Process ... 185
Detecting Malware Using UAC ... 186
File System and Registry Virtualization ... 188
Customizing UAC ... 188
UAC and the Language Bar ... 191
Access Control and Permissions ... 192
Taking Ownership ... 192
Altering Permissions ... 192
Windows Defender ... 194
Configuring Windows Defender ... 195
Windows Defender Command Line Utility ... 198
Windows SmartScreen ... 198
Configuring Windows SmartScreen ... 199
Windows Firewall ... 200
Basic Configuration ... 200
Advanced Configuration ... 201
Local Security Policy ... 202
Account Policies ... 203
Local Policies ... 203
Data Execution Prevention ... 204
Address Space Load Randomization ... 205
Structured Exception Handling Overwrite Protection ... 205
EMET ... 205
Safe Unlinking ... 206
Kernel Patch Protection ... 206
Secure Boot ... 206
Encrypting File System ... 207
Backup Encryption Key ... 208
BitLocker Drive Encryption ... 208
Additional Security Software ... 210
Anti-Malware Packages ... 210
Phishing Protection ... 211
Firewalls ... 211
Important Security Tips ... 211
Secure Passwords ... 212
Account Recovery ... 214
Physical Access ... 215
General Online Tips to Avoid Scams, Spam & Malware ... 216
Balancing Security vs. Convenience ... 220

Memory Optimization ... 222

Memory Hardware ... 222
CPU Cache ... 222
Physical RAM ... 223
Video RAM ... 224
Windows Memory Management ... 224
Maximum Supported RAM ... 225
Metro Memory Management ... 225
Services ... 226
SuperFetch ... 226
Desktop Windows Manager ... 228
Fault Tolerant Heap ... 228

ReadyBoost ... 229
ReadyBoot ... 230
Resource Exhaustion Prevention and Resolution ... 231
Memory Dump ... 231
Virtual Memory ... 232
Upgrading Memory ... 236
Drive Optimization ... 238
Windows I/O Management ... 238
Hard Disk Drives ... 239
Short Stroking ... 239
Optical Drives ... 239
Solid State Drives ... 240
TRIM ... 240
Defragmentation ... 241
Pagefile ... 241
Search Index ... 242
SuperFetch & ReadyBoost ... 242
Temporary & Personal Files ... 242
Partition Alignment ... 242
Longevity ... 243
Mounting ISO Files ... 244
Virtual Hard Disk ... 244
Booting Up From A VHD ... 245
Creating a VHD or VHDX ... 245
Mounting and Detaching a VHD ... 246
Accessing a System Image Backup VHD ... 246
Hyper-V ... 247
RAM Drive ... 247
Disk Management ... 248
Disk Diagnostics ... 249
Check Disk ... 250
Drive Controllers ... 251
AutoPlay ... 253
Master File Table ... 254
Optimize Drives ... 255
Advanced Defragmentation ... 256
Windows Control Panel ... 258
Customizing Windows Control Panel ... 258
Action Center ... 259
Add Features to Windows 8 ... 260
Administrative Tools ... 260
Component Services ... 260
Computer Management ... 260
Defragment and Optimize Drives ... 260
Disk Clean-up ... 260
Event Viewer ... 261
Hyper-V Manager ... 261
iSCSI Initiator ... 261
Local Security Policy ... 261
ODBC Data Sources ... 261
Performance Monitor ... 261
Print Management ... 261
Resource Monitor ... 261
Services ... 261
System Configuration ... 261
System Information ... 262
Task Scheduler ... 262
Windows Firewall with Advanced Security ... 262
Windows Memory Diagnostic ... 262
Windows PowerShell ... 262
AutoPlay ... 262
BitLocker Drive Encryption ... 262
Color Management ... 262
Credential Manager ... 262

Date and Time ... 263
Date and Time ... *263*
Additional Clocks ... *263*
Internet Time ... *263*
Default Programs ... 263
Set Your Default Programs ... *263*
Associate a File Type or Protocol with a Program ... *264*
Change AutoPlay Settings ... *264*
Set Program Access and Computer Defaults ... *264*
Device Manager ... 265
Devices and Printers ... 265
Display ... 265
Ease of Access Center ... 265
Family Safety ... 265
File History ... 265
Folder Options ... 266
Fonts ... 266
HomeGroup ... 266
Indexing Options ... 266
Internet Options ... 266
Keyboard ... 266
Language ... 266
Location Settings ... 267
Mouse ... 267
Buttons ... *267*
Pointer Options ... *267*
Wheel ... *268*
Network and Sharing Center ... 268
Notification Area Icons ... 269
Performance Information and Tools ... 269
Personalization ... 269
Phone and Modem ... 269
Power Options ... 269
Sleep Modes & Fast Startup ... *272*
Programs and Features ... 274
Recovery ... 277
Region ... 277
Formats ... *277*
Location ... *277*
Administrative ... *277*
RemoteApp and Desktop Connections ... 277
Sound ... 277
Speech Recognition ... 278
Storage Spaces ... 278
Sync Center ... 278
System ... 278
Computer Name ... *278*
Hardware ... *279*
Advanced ... *279*
System Protection ... *279*
Remote ... *279*
Taskbar ... 280
Troubleshooting ... 280
User Accounts ... 280
Windows 7 File Recovery ... 280
Windows Defender ... 280
Windows Firewall ... 280
Windows Update ... 280
PC Settings ... 281
Personalize ... 281
Users ... 282
Notifications ... 282
Search ... 282
Share ... 282
General ... 283

Privacy 284
Devices 284
Ease of Access 285
Sync Your Settings 285
HomeGroup 285
Windows Update 285
Startup Programs 286
Finding Startup Programs 286
Microsoft System Configuration Utility 286
Task Manager 287
Registry Editor 288
Autoruns 288
Correctly Identifying and Removing Startup Programs 289
Startup Troubleshooting 290
Regular Maintenance 291
Services 292
Services Utility 292
Backing Up Services 293
Windows Services 293
Non-Microsoft Services 294
Customizing Services 294
Change Service Status via Command Line 294
Trigger Start Services 295
Permanently Deleting Services 296
Background Tasks 296
Task Scheduler 297
Force Idle Task Processing 298
Create a Task 298
Windows Registry 300
Backup and Restore the Registry 300
Backing Up the Entire Registry 300
Backing Up Portions of the Registry 301
Registry Editor 301
Registry Structure 302
Editing Registry Entries 303
Creating and Deleting Registry Entries 304
Registry Permissions 304
Maintaining the Registry 305
Group Policy 306
Local Group Policy Editor 306
Prevent Access to a Specific Windows Feature 307
Prevent Access to the Windows Store 307
Hide Specific Control Panel Items 307
Modify CTRL+ALT+DEL Screen 307
Turn off Thumbnails 307
Hide Notification Area 308
Turn Off Shake 308
Disable the Lock Screen 308
Prevent Uninstallation of Apps on Start Screen 308
Block Removable Storage Access 308
Enable Pagefile Encryption 308
Prevent Automatic Restore Point Creation 309
Prevent Windows Media DRM Access 309
Prevent Windows Media Player Codec Download 309
Handling of Attachments 309
Windows Search 310
Search Methods 310
Start Screen 310
File Explorer 311
Advanced Search Query 313
Federated Search 314
Search Configuration 315
Search Index 315

Performance Impact ... 316
Customizing the Index ... 317
Indexing and File Properties ... 318
Disabling Windows Search ... 319
Internet Explorer ... **321**
IE Desktop vs. IE Metro ... 321
Internet Explorer Desktop ... 322
General ... 322
Security ... 325
Privacy ... 326
Content ... 327
Connections ... 328
Programs ... 328
Advanced ... 329
Search ... 331
InPrivate Browsing ... 331
ActiveX Filtering ... 332
Tracking Protection ... 333
Accelerators ... 334
Internet Explorer Metro ... 334
Basic Usage ... 334
Internet Options ... 335
Other Features ... 336
Advanced Settings ... 336
Customize Internet Explorer's Appearance ... 336
Frequently Visited Sites ... 337
Internet Explorer 64-bit ... 338
Start with InPrivate Browsing Mode Enabled ... 338
FTP with Explorer-Based Windows ... 339
Increase Maximum Simultaneous Connections ... 339
DNS Cache Issues ... 339
Fix Internet Explorer ... 340
Other Internet Browsers ... 340
Windows Live Mail ... **342**
Mail Metro ... 342
Windows Live Mail ... 342
Step 1 - Email Accounts ... 343
Step 2 - Import Saved Mail ... 344
Step 3 - Folder Pane & Unified Inbox ... 344
Step 4 - Customize Menus and Toolbars ... 345
Step 5 - Add Color ... 346
Basic Settings ... 346
General ... 346
Read ... 347
Receipts ... 348
Send ... 348
Compose ... 349
Signatures ... 349
Spelling ... 349
Connection ... 350
Advanced ... 350
Safety Options ... 351
Options ... 351
Safe Senders ... 352
Blocked Senders ... 352
International ... 352
Phishing ... 353
Security ... 353
Windows Contacts ... 354
Mail Rules ... 355
Backing Up ... 355
Backing Up Emails ... 355
Backing Up Accounts ... 356
Other EMail Clients ... 356

Windows Media Player 357
Initial Settings 357
Views 358
Library View 358
Now Playing View 359
Basic Settings 361
Player 361
Rip Music 361
Devices 362
Burn 363
Performance 364
Library 365
Plug-ins 366
Privacy 366
Security 368
Network 368
Advanced Features 368
Enhancements 368
Skins 370
Taskbar Player Mode 370
Audio & Video Codecs 370
Viewing and Editing Codecs 370
Obtaining Codecs 371
DVD & Blu-Ray Playback 372
DVD Playback 372
Blu-ray Playback 372
Digital Rights Management 373
Other Media Players 374
Graphics & Sound 375
Metro 375
Start Screen 376
Tiles 377
App Bar 378
All Apps Screen 378
Semantic Zoom 379
Using Apps 379
Charms 381
Power User Tasks Menu 382
Power Options 382
Metro Customization 382
Customize the Start Screen 382
Bypass the Start Screen 383
Bring Back The Start Menu / Disable Metro 384
Edit the Power User Tasks Menu 386
Customize the All Apps Screen 386
Change Start Screen Animations 387
Aero Glass 387
Desktop Gadgets 388
Desktop 389
Personalization 390
Change the Visuals and Sound on your Computer 390
Desktop Background 391
Color 392
Sounds 393
Screen Saver 393
Saving Themes 393
Change Desktop Icons 394
Change Mouse Pointers 394
Visual Effects 394
Display Settings 395
Screen Resolution 395
Calibrate Color 397
Adjust ClearType text 397
Multiple Monitors 397
Magnifier 397

Taskbar ... 398
Taskbar Icons & Effects ... *398*
Jump Lists ... *399*
Thumbnail and Full Screen Previews ... *399*
Taskbar Customization ... *401*
Toolbars ... *401*
Additional Features ... *403*
Notification Area ... 403
Sticky Notes ... 405
Image capture and manipulation ... 406
Image Capture ... *406*
Image Viewing & Editing ... *407*
Fonts ... 408
Font Clarity ... *408*
Font Size ... *409*
Font Management ... *409*
Customize Fonts ... *409*
Icons ... 410
Remove Text from Desktop Icons ... *411*
Remove Shortcut Arrows from Icons ... *411*
Remove '- Shortcut' from New Shortcuts ... *412*
Repair Incorrectly Displayed Icons ... *412*
Save Desktop Icon Positions ... *412*
Create Custom Shutdown, Restart, Sleep or Lock Icons ... *412*
Icon Creation and Customization ... *415*
Sound ... 415
Volume Control ... *415*
Playback ... *416*
Recording ... *418*
Sounds ... *418*
Gaming ... 419
Games Explorer ... *419*
Alternatives to Games Explorer ... *422*
Old Games ... *422*
Performance Measurement & Troubleshooting ... 423
Windows Experience Index ... 423
Windows System Assessment Tool ... *424*
Reliability Monitor ... 425
Troubleshooting ... 426
Problem Steps Recorder ... *427*
Windows Action Center ... 427
Automatic Maintenance ... *428*
Windows Error Reporting ... *428*
Event Viewer ... 429
Performance Monitor ... 431
System Health Report ... 432
Resource Monitor ... 433
Task Manager ... 434
Processes ... *435*
Performance ... *435*
App History ... *437*
Start-up ... *438*
Users ... *438*
Details ... *438*
Services ... *438*
General Usage ... *438*
Processor Affinity and Priority ... *439*
Process Explorer ... *441*
Windows Memory Diagnostic ... 441
Windows Errors ... 442
Third Party Tools ... 443
3DMark ... *443*
Heaven ... *443*
FurMark ... *444*
Game Benchmarks ... *444*

PCMark *444*
Sandra *444*
Prime95 ..... *445*
Super PI *445*
HD Tune *446*
AS SSD Benchmark *446*
ATTO Disk Benchmark *446*
MemTest *446*
Cleaning Windows **448**
Recycle Bin 448
Remove Recycle Bin from Desktop *448*
Disk Clean-up 449
Advanced Disk Clean-up *450*
CCleaner 451
Manual Cleaning 452
Deleting 'In Use' Files *454*
Regular Maintenance **455**
Step 1 - Maintain Security *455*
Step 2 - Check Startup Programs & Services *455*
Step 3 - Backup *455*
Step 4 - Clean Windows *456*
Step 5 - Optimize Drives *456*
Scheduled Maintenance *456*
Conclusion **457**
Version History 457

COPYRIGHT & CREDITS

HOSTING, DISTRIBUTION AND TRANSLATIONS OF THIS BOOK

Reproducing, altering, hosting, or mass distributing this book in any way is not permitted. The latest version is always available from TweakGuides.com.

Translations of this book are not permitted, as I have absolutely no way to determine the quality and accuracy of any translations, particularly given the somewhat complex, and at times quite delicate procedures in this book. Professional translations of this 270,000 word book into the multiple languages required would cost a great deal, and amateur translations are unacceptably shoddy.

If you wish to spread the word regarding the book, please link to the main TweakGuides Tweaking Companion page.

I've invested a huge amount of time and effort into creating this book, and I also provide a free version of this book which is easily accessible so that the widest possible audience can benefit from its contents. There is no reason for anyone to publicly reproduce or distribute this book when the latest version is always available for free from my site. People who host this book or portions of it are usually doing so to generate easy traffic, income or credit for themselves using my hard work, which is not acceptable. Appropriate action will be taken against any such individuals who do not respect the concept of author rights.

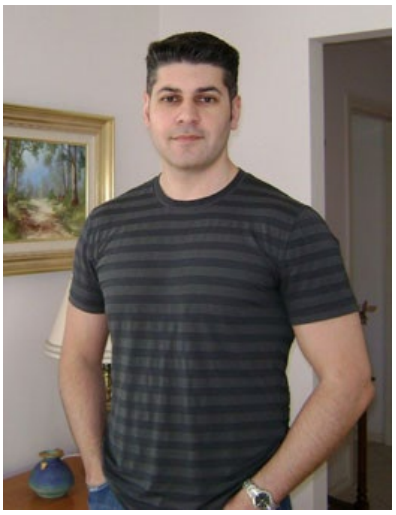
For those who do not understand the strictness of these conditions, please see the TweakGuides FAQ.

CREDITS

This book is a reference compilation borne out of a great deal of testing, research, reading and personal experience. I give full credit to any websites and authors linked in this book, as well as all the software developers whose excellent tools I recommend in this book, especially those who provide their software for free. It is amazing that they invest so much time and effort into developing and testing their software and then provide it free to all PC users. I encourage you to support their work with donations and purchases where relevant, because giving is a two way street.

Thank you to my readers who, since TweakGuides began in April 2004, have provided a great deal of support. From those who support the site by linking to it on various websites and forums, to those who take the time to write to me with thoughtful and constructive contributions, and in particular to those who donate to the site or purchase the Deluxe Edition of this book - I truly appreciate it. The only thing which motivates me to keep writing is the fact that I know there are intelligent people out there who are patient enough to take the time to use the material in the spirit in which it is intended: to learn more about their PCs, and to think for themselves and resolve their own problems.

INTRODUCTION



Windows 8 officially debuted on 26 October 2012, almost exactly three years since Windows 7 was released. Having proven to be very popular, Windows 7 is a tough act to follow. Instead of simply further optimizing Windows and tinkering around the edges, Microsoft has chosen to make a radical change with Windows 8, aimed squarely at garnering greater market share on mobile touch-centric devices, such as tablets. This has resulted in interface changes that may be confusing or annoying to you.

Further compounding the potential confusion is that you may have skipped one or more previous versions of Windows, and thus will find Windows 8 an even less familiar environment than those who are upgrading from Windows 7. Fear not, I've made sure that this book caters equally to all types of users, regardless of which version of Windows you're transitioning from, or even if you're relatively new to Windows.

I have mixed feelings regarding Windows 8. On the one hand, it takes some of the best aspects of Windows 7 and makes them even better in terms of performance. On the other hand, Microsoft's desire to unify the mobile and PC platforms by unavoidably grafting the Metro design philosophy so firmly onto Windows 8 is as much an annoyance as an innovation. Once you learn the ins and outs of the Metro UI, it is actually a relatively simple interface. Despite this, in my opinion it is still rather a large and unnecessary addition that powerful non-touch-capable desktop PCs should not be forced to use.

Fortunately, my personal opinions are largely irrelevant to this book. My aim is not to convince you that the changes in Windows 8 are either good or bad. Instead, I've kept in mind the larger goal of simply explaining all of the changes in plain English, and giving you as many options for safe customization as possible. Only you can make the choice of whether you wish to curtail any of the changes in Windows 8, or alternatively, to indulge in them, and make full use of them.

As with my earlier *TweakGuides Tweaking Companions* for Windows XP, Vista and 7, I understand that the length of this book will frustrate people who are simply looking for a handful of quick tips to "make Windows faster", or to "make Metro go away". That is not the goal of this book. Instead, I try to make sure that you are given sufficient detail to actually understand the logic behind Windows functionality, as well as any recommendations I provide, rather than being treated like a small child who is told to do something without a second thought. As a result, the book is unapologetically long. However, I promise you that if you patiently work your way through this book over the course of several days, you will come out at the other end with not only a better performing, stable, and better customized PC, you will also be much more comfortable with using Windows 8 on a daily basis.

In closing, if you find the book useful, please consider purchasing the enhanced Deluxe Edition of this book. The Deluxe Edition has several features, including pictures, text copying, and navigational aids, which make it much easier to use. Your support will also allow me to continue releasing the free version of this book.

Cheers,

Koroush Ghazi
Owner/Author
TweakGuides.com

In honor of 2,500 years of Persian Culture
Dedicated to the noble ideals of Cyrus the Great

USING THIS BOOK

This chapter contains important information that you should consider before using this book.

BASIC REQUIREMENTS

There are three key requirements you should meet to use this book successfully:

- You need access to an Administrator level user account to make many of the changes in this book. The default user account created during Windows installation is one such account. See the User Accounts chapter for details.
- You should prepare backups of all of your important data prior to undertaking any of the changes detailed in this book. See the Backup & Recovery chapter for details.
- You should have Windows 8 installation media, as you may not be able to reverse certain changes without it. However, under Windows 8, PCs without Windows 8 installation media can access a built-in System Recovery partition, or create a System Repair Disc prior to proceeding, and can also access the Windows Refresh and Windows Reset features, which should be sufficient for restoring Windows to its default state. See the Backup & Recovery chapter for details of these features.

I do not recommend applying any of the changes covered in this book unless you meet all three of the requirements above. The bare minimum requirement is that you must have Administrator level access.

DIFFERENT VERSIONS OF WINDOWS

The information in this book is applicable to 32-bit and 64-bit editions of Windows 8, Windows 8 Pro, and Windows 8 Enterprise. Some of the information may also apply to Windows RT, but it has not been tested on it. The major content differences between Windows 8, Windows 8 Pro, Windows 8 Enterprise and Windows RT are covered in this Microsoft Article, and in more detail in this Wikipedia Article. There are no content differences between the OEM, System Builder, Upgrade, MSDN or TechNet editions of Windows 8. These are all identical in terms of performance and content; the actual difference is that certain licensing and usage conditions apply to each of them. See the Windows Installation chapter for details.

PC VS. MOBILE DEVICES

This book is aimed at desktop PCs, and full-featured PC-like devices, such as laptops. A large portion of the information in this book may also be relevant to more powerful mobile devices, such as tablets that can run a full version of Windows 8. However, this book does not focus on providing instructions specific to such devices, and does not cover the feature differences of Windows RT, which is the most common version of Windows 8 installed on mobile devices. Please keep in mind that none of the procedures in this book have been tested on anything other than a standard desktop PC.

WHERE ARE THE PICTURES?

There is a distinct lack of pictures in this version of the book. The Deluxe Edition of this book contains detailed screenshots and illustrative images, as well as other useful features that make using the book much more convenient, such as high quality text resolution, full bookmarks for quicker chapter and section access, and the ability to copy text, which is handy for correctly assigning Windows Registry values, or entering complex File Explorer paths or Command Prompt commands. If you want the book with these features, and more importantly, want to show your support, please consider purchasing the Deluxe Edition from the link above. The electronic version is only a few dollars and has no intrusive DRM.

WHY IS THE BOOK SO LONG?

This book is intended primarily as an educational and reference source. It is not intended for people seeking quick fixes. I provide explanations and appropriate links for a wide range of features and procedures, aimed at a relatively broad audience, so that anyone can gain a good understanding of what they're doing, and make up their own mind, rather than just taking my word for it. I firmly believe in the old saying: *Give a man a fish and he will eat for a day; Teach a man to fish and he will eat for a lifetime*. To find information on any topic in the book at any time, use the Table of Contents, or press CTRL+F to bring up the PDF search functionality. I will not be releasing a cut-down version of this book; there are no "10 best tweaks" or a handful of changes that magically speed up or fix Windows 8. It is a complex inter-relationship of hardware and software settings that determine how fast and how stable your PC runs, and it requires understanding and thought to correctly optimize and customize a system.

WHERE DO I START?

This book has been designed to cater equally to those who are doing a new installation of Windows 8, and those using an existing installation of it. The chapters follow a roughly sequential order as to the types of things I would personally configure before and after doing a new installation. However, any chapter, or even any section, can be read in any order you wish, because where any major procedures or details from other chapters are required, they are referenced accordingly. If you don't wish to read the book sequentially, I recommend reading the Basic PC Terminology and New Features chapters first. Then I suggest becoming familiar with the contents of the Graphics & Sound, File Explorer, Windows Drivers and Security chapters as soon as possible, as these cover the most important interface, functionality and security-related topics.

RECOMMENDED SOFTWARE

Listed throughout this book is a range of software to enable you to carry out some of the procedures in the book, or to provide potentially desirable functionality in Windows. This book is not sponsored by any software or hardware company, nor do I receive any affiliate fees, or any other form of kickback, commission or perk from recommending any software to you. I simply try to recommend the best free software available to do the job. In a few cases, certain software may require purchase. I try to minimize the use of such software in this book, but sometimes it is unavoidable, as there are no decent free alternatives at the time of writing. It is left up to you to decide whether such software is worthy of purchasing.

If at any point you feel uncomfortable or uncertain about downloading or installing any third party software, for whatever reason, you should ignore those procedures that rely upon it, as none of them are critical to the proper functioning of Windows.

Importantly: You must pay close attention when downloading and installing any third party software. Websites frequently obscure the actual download link among a sea of ads that may display various unrelated download buttons. During the installation procedure you may also be automatically opted-in to the installation of various browsers, toolbars, and other non-malicious but undesirable software or setting changes, unless you explicitly untick certain boxes. Some software may also periodically nag you for donations, or launch web pages for the same purpose.

All of these aspects are unfortunately part and parcel of most free software these days. I have made every effort to ensure that at the time of writing, none of the software I recommend is malicious in any way, nor will it make any unauthorized changes, or install any undesirable software, without at least giving you the option to opt out of them during installation. Regardless, you must be vigilant at all times to avoid any problems resulting from these increasingly common and unavoidable practices.

Problems with the Book

While I have made every effort to ensure that this book is as clear and accurate as it can be, I hope you can appreciate the fact that I cannot possibly test the information and recommendations in this book on every potential combination of hardware and software available. If there is anything in the book that you believe is genuinely inaccurate or misleading, please Email Me with specific details. You can also email me if you wish to share any general feedback or thoughts you have about the book.

I must stress however that the book is provided "as is", and I cannot provide technical support of any kind. It simply isn't viable or appropriate for me to do so. Under no circumstances will I provide personalized optimization, customization or purchasing advice, or any other form of technical support related to the information in this book. The whole reason for writing this book is to give each and every reader a thorough rundown on all of the steps that I consider necessary to correctly configure and troubleshoot Windows 8. There are sufficient resources and links in this book to help anyone learn more about their system, and solve most any problem, when combined with additional research and some thought.

Your Responsibilities

The basic theme throughout this book is that as long as you read and consider the advice given carefully, and use common sense when applying any changes, you will remain problem-free. I have made every reasonable effort to ensure that the contents of this book are accurate to the best of my knowledge, and that the sites and utilities linked to in the book are free from any malicious or deceptive practices at the time of writing. In all respects the book is safe to use if followed correctly, when combined with careful consideration and taking appropriate precautions, including conducting additional research when in doubt.

For legal reasons, I cannot take any responsibility for any damage or loss incurred through the use of this book. **It is a condition of use for this book that you agree to take full responsibility for any of your actions resulting from reading this book**. If you do not wish to take full responsibility for using this book, and any resulting impacts, then please do not proceed any further.

BASIC PC TERMINOLOGY

This chapter explains commonly used technical terminology in layman's terms. All of the major hardware components found in a modern PC are covered. Advanced users may want to skip this chapter.

BITS & BYTES

You will often see the terms Bits, Bytes, Kilobytes, Megabytes and Gigabytes (or their abbreviations) being thrown around. Understanding these is very important to learning more about PC usage. To start with, a Bit (Binary Digit) is the lowest form of computer information, and can take the value 0 or 1 (i.e. Off or On). All computer functionality is derived from the behavior of bits. For the purposes of this book, the most common units of measurement are:

8 bits (b) = 1 Byte (B)
1,024 Bytes = 1 Kilobyte (KB)
1,024 Kilobytes = 1 Megabyte (MB)
1,024 Megabytes = 1 Gigabyte (GB)

Note that bits are shown as a small b, and Bytes are shown as a capital B - this is an important distinction. For example, 512kbps is 512 kilo*bits* per second, which converts to 64KB/s (Kilo*bytes* per second).

For most users, knowing the above conversion factors is sufficient for understanding the terminology used in this book and around the Internet, as well as for general PC usage. However, strictly speaking, the values shown above are not correct, as explained in this article.

The discrepancy stems from the fact that the commonly used metric prefixes Kilo, Mega, Giga and so forth are based on the decimal (base ten) system, while computers are based on the behavior of bits, which is a binary (two digit) system. Therefore, while 8 bits still equals 1 Byte under either system, the correct prefixes to use in other cases are:

1,024 Bytes = 1 *Kibi*byte (KiB)
1,024 Kibibytes = 1 *Mebi*byte (MiB)
1,024 Mebibytes = 1 *Gibi*byte (GiB)

1,000 Bytes = 1 Kilobyte (KB)
1,000 Kilobytes = 1 Megabyte (MB)
1,000 Megabytes = 1 Gigabyte (GB)

What's the difference? Well one Kilobyte (KB) actually equals 1,000 bytes, since 'kilo' is a decimal prefix meaning 'thousand'. Yet one Kilobyte as interpreted by a computer is actually 1,024 bytes, so 'kilo' is not the appropriate prefix to use, Kibibyte (KiB) is the correct term referring to multiples of 1,024 bytes. This discrepancy may seem minor at first - only 24 bytes difference between 1KB and 1KiB - but as the values grow, it becomes more significant, so it is important to understand the difference. This is particularly true because hardware and software manufacturers often use these prefixes differently, causing PC users a great deal of confusion.

The best practical example of this discrepancy is drive capacity. A drive advertised as having 150GB of storage space is a technically correct use of the term Gigabyte, because it holds 150,000,000,000 Bytes of storage. However, purchasers of the drive soon become confused when they see that Windows typically reports the drive as having only 139GB of usable space. This is because 150,000,000,000 Bytes translates to 139GiB in the binary system the computer uses, as opposed to 150GB in the decimal system, but Windows incorrectly shows GB instead of GiB. This results in many users feeling ripped off because their usable drive

space does not match the advertised storage capacity. As drive capacities grow, the discrepancy between advertised and reported space becomes much larger, causing even greater concern among consumers.

In any case, to avoid further confusion, throughout this book I will continue to refer to values based on the accepted (but technically inaccurate) common usage, i.e. the way in which hardware manufacturers report them, and the way in which Windows reports them, despite the discrepancy. Eventually, widespread adoption of the correct terms will be necessary to prevent growing consumer confusion.

DATA

In the context of PCs and technology, Data is a general term referring to any amount or type of information which is stored and used by a computer.

PC

A Personal Computer (PC), also referred to as a System, Machine, Rig or Box, is a collection of hardware (electronic components) which function as a unified system through the use of software (programmed instructions).

CPU

The Central Processing Unit (CPU), also referred to as the Processor, is the single most important component of a PC. The CPU chip is typically a small thin square chip which is seated firmly on your Motherboard, and usually covered by a large metal heatsink and fan to cool it. The CPU controls and co-ordinates the actions of the entire PC under instruction from software. It has the role of determining which hardware component does what, assigning tasks and undertaking complex calculations which are then fed through the various relevant components and back.

MOTHERBOARD

The Motherboard, also called a Mainboard or Mobo, is the large rectangular Printed Circuit Board (PCB) into which all of the electronic components are connected in a PC. The motherboard is typically firmly attached to the inside of a PC Case. The motherboard provides a network of pathways for the CPU to communicate with the various hardware components, and a range of ports for standard peripherals and other devices to plug into the PC.

MEMORY

A PC uses several different types of Computer Memory to store data, whether temporarily or permanently, for the purposes of speeding up processing performance. Memory chips are fast because unlike other forms of data storage, such as physical Hard Drives or Optical Drives, they have no moving parts. The main types of PC memory are covered below:

Random Access Memory (RAM), also called System RAM or simply just Memory, is the most common form of memory hardware used by a PC. RAM usually comes in the form of a long thin PCB stick (a DIMM) that plugs into the motherboard, and provides a place for the CPU and other components to temporarily store any data which the system needs to rapidly access. RAM only holds data while it has a source of power; if a PC is rebooted or switched off, any data in RAM is instantly lost. For this reason, this type of memory is referred to as Volatile Memory.

Read Only Memory (ROM) is a more permanent form of memory, and works similar to RAM, however unlike RAM it can only be read from, and not written to, under normal circumstances. Furthermore, it will not clear when it has no source of power; that is, when the system is rebooted or switched off, it does not lose its contents. For this reason, this type of memory is referred to as Non-Volatile Memory. ROM is primarily used to hold smaller amounts of important data, such as the Basic Input Output System (BIOS) -

the program which tells the computer how to function when it is first switched on - stored on the ROM chip in the motherboard. Certain ROMs can be written to by use of a process called Flashing, such as when the BIOS is flashed with a newer version of its programming.

The CPU and other hardware such as hard drives often have small memory chips of their own called Caches to temporarily hold specific data. This memory is typically a smaller RAM chip and is used as another point of temporary storage to further speed up data transfers.

STORAGE DRIVES

As noted under Memory above, RAM is only a temporary form of storage. While able to store data permanently in the absence of power, ROM has typically been too small to store large volumes of data, and is also not designed for being frequently written to. Therefore modern computers employ one or more of several forms of storage drives designed to permanently hold data in large quantities, with varying degrees of portability and access speed.

Storage drives plug into one of four main types of drive controllers found on the motherboard, listed below from slowest to fastest:

§ Floppy Disk Controller (FDC);
§ Integrated Drive Electronics (IDE) / Parallel Advanced Technology Attachment (PATA);
§ Serial ATA (SATA); or
§ Small Computer System Interface (SCSI), including Serial Attached SCSI (SAS).

The controller available for any particular drive to use depends on both the drive type and the motherboard type. Some storage drives can also plug into the Universal Serial Bus (USB) port of a PC, however this is a multi-purpose port and not a dedicated drive controller, so it is not listed above.

The various types of drive hardware are covered below:

A Hard Disk Drive (HDD) is a magnetic storage device that acts like Memory, except it is semi-permanent, slower and far larger in capacity. The hard drive is a rectangular metallic box inside which sits a stack of round platters and a read/write head. Whenever the PC requires data, it must first be read from the hard drive, usually into RAM, from where it is then accessed by the CPU and other devices. Data written to the hard drive will remain on the drive regardless of whether the system is rebooted or switched off. Because a hard drive has moving physical components, such as the read/write head and a spinning disk, it can never be as fast as memory chips - which have no moving parts - in providing data. As a result, a system may slow down, pause, or stutter while waiting for more data to be loaded up from or written to a hard drive. The amount of data stored on the hard drive itself usually has no significant impact on its performance, however if the data on the drive becomes fragmented, this will reduce performance.

A Solid State Drive (SSD) is a memory-based storage device which combines the advantages of the speed of computer memory with the more permanent nature and larger capacities of hard disk drives. By using a type of Non-Volatile memory called Flash Memory, which is similar to ROM as covered under the Memory section above, an SSD can store data even when the PC is rebooted or switched off. Unlike a hard drive, an SSD has no mechanical moving parts, and as such is much faster in accessing its stored data. As SSDs become cheaper, faster and more reliable, they are steadily replacing hard disk drives for consumer PC usage. Windows 8 provides full native support for SSDs.

An Optical Disc Drive is a disc-based data storage device that reads from and sometimes writes data onto CD, DVD or Blu-Ray discs via laser or other light-based methods, hence the use of the term 'optical'. These portable discs permanently hold the data until overwritten or deleted. Optical drives usually come in plastic rectangular boxes with a loading slot or extendable tray in the front. While much slower than hard drives or

SSDs due to physical limitations, the main advantage of optical drives is the portability and relatively low cost of their media, along with the fact that such media can also be played on a variety of non-PC devices, such as standalone CD, DVD or Blu-Ray players. Note that the term *disk* usually refers to magnetic media, like a floppy disk, while the term *disc* refers to optical media, such as a DVD disc.

A Floppy Disk Drive (FDD) is a magnetic storage device which reads and writes data on thin plastic 3.5" Floppy Disks. The floppy drive comes in a rectangular plastic box with a loading slot at the front and a manual ejection button. Floppy drives are extremely slow compared to any other form of drive, and also hold very little data (around 1.44MB), and hence are a legacy device no longer used on modern PCs. Some PC users retain a floppy drive for Windows recovery purposes, or to flash the BIOS, however this is no longer necessary as modern PCs now support the use of optical discs or USB flash drives for these purposes instead. In fact the only advantage of floppy drives - the relative portability of their 3.5" disk media - has been completely superseded by USB flash drives which are much smaller, faster, sturdier and more reliable, and can hold several GB of data as opposed to just 1.44MB.

A USB Flash Drive is extremely similar to an SSD, in that it also uses Non-Volatile Flash memory to permanently store data. However USB drives are typically much smaller in capacity and physical size, and offer much slower performance and reliability than an SSD. Their main advantage is that of low cost and portability due to their small size, which is why they are also known as thumb or key drives. They plug into a standard external USB port on a PC, making them much easier to use for connecting to and transferring data between different PCs, since unlike a standard drive they do not need to be connected to a motherboard drive controller found inside a PC.

Graphics Card

The Graphics Card, also called the Video Card, GPU, Graphics Adapter or VGA Adapter, is a miniature computer of its own dedicated solely to processing complex graphics-related data. It is a thin rectangular plastic PCB with a Graphics Processing Unit (GPU), also known as the Core, and Video RAM (VRAM), also known as Video Memory. The GPU and VRAM are the graphics-specific equivalents of the CPU and System RAM on a PC, and the graphics card itself has Pipelines for transferring data internally, similar to the data pathways on a motherboard. The graphics card plugs into the motherboard through one of the following interfaces, listed from slowest to fastest:

§ Peripheral Component Interconnect (PCI);
§ Accelerated Graphics Port (AGP); or
§ Peripheral Component Interconnect Express (PCI-E).

Graphics cards typically come with some form of cooling enclosure built around them, to ensure that the GPU and the VRAM remain cool enough to operate correctly.

The graphics card undertakes the majority of 2D and 3D graphics calculations under Windows 8, and also sends data directly to a Display Device. Some motherboards have built-in graphics functionality that works in much the same way as a plug-in graphics card, but is referred to as Onboard or Integrated Graphics. PCs with such graphics functionality typically process graphics-related data far less quickly than those with plug-in graphics cards.

Display Device

A Display Device, more commonly referred to as a Monitor, is the device through which the PC's data output is displayed graphically. This graphical data typically comes directly from the graphics card, and a display device must be plugged into the graphics card to facilitate this. Some computers may still have a traditional Cathode Ray Tube (CRT) monitor as their primary display device, however the majority of modern PC monitors now utilize Liquid Crystal Display (LCD) technology. Furthermore, a modern PC can

also be plugged into a television set of any type, such as CRT, LCD, Plasma, Rear or Front Projector, and other similar technology sets if the user desires, or even a combination of multiple displays at once if the graphics card supports such functionality.

Display devices have the ability to display graphics at various Display Resolutions, typically expressed in number of Pixels wide by number of Pixels high (e.g. 1920 x 1200). A Pixel is the smallest component of a digital image, thus the higher the resolution, the more pixel samples of the image are displayed on the display device, and the clearer the image. At each resolution a display device can also update the image a number of times per second, referred to as the Refresh Rate, which is expressed in hertz (Hz). Refresh rate is not to be confused with Frame Rate, which is expressed in Frames Per Second (FPS). Refresh rate is a physical limitation of a display device in refreshing the image on the screen a certain number of times per second. Frame rate on the other hand is the number of times per second that the software and graphics device can provide a whole new frame of imagery to the display.

Sound Card

The Sound Card, also called the Audio Card or Audio Device, is a thin PCB that acts as a dedicated CPU for calculation of audio data. It typically plugs into the motherboard, and usually has no form of cooling enclosure around it. Some motherboards have built-in audio functionality that works in much the same way as a sound card, but is referred to as Onboard or Integrated Sound. PCs with such audio functionality may process audio-related data less quickly, or with less additional functionality, than those using plug-in sound cards.

Speakers

A PC usually comes with some form of sound output device, typically a built-in PC speaker, to provide audible warnings in the form of beeps or tones. Users with a Sound Card or Integrated Sound can attach more functional sound output devices, such as standalone Speakers or Headphones, directly into the sound card or integrated sound device through a port on the PC. The addition of speakers or headphones allows the user to experience higher quality sound and also a potentially higher number of discrete Audio Channels which can increase the realism of sound reproduction.

Power Supply Unit

The Power Supply Unit (PSU) is a square metal box which is connected to mains power from the back of the PC, and inside the PC is cabled to several major components, as well as to the motherboard which regulates this power to the remaining components. Thus the PSU is the primary source of power which allows the PC to function; if the PSU cannot provide sufficient stable power to the hardware components of a PC, it can cause erratic behavior or even a failure to start up.

Cooling Devices

Electronic components can generate a great deal of heat, especially when under heavy load. The hardware components in a PC most susceptible to heat buildup, such as the CPU and GPU, come with cooling solutions designed to dissipate the heat into the surrounding air. The two most common types of PC Cooling solutions used are:

A Heatsink is a square or rectangular solid metal object typically with a perfectly flat surface on one side, and multiple spines, fins or rods on the other side(s). The role of a heatsink is to sit on top of the component to be cooled, and draw out the heat from that component through conduction. This heat then travels along the heatsink until cooler air and a large surface area help in accelerating its dissipation.

A Fan is designed to draw in cold air or expel hot air. Fans can either be employed on their own, such as case fans which simply suck in or blow out air from a PC case; or they can be mounted on or near heatsinks to

assist in more rapidly dissipating the heat drawn out from hardware components. The larger the fan and/or the faster it rotates, the greater the volume of air it can move, hence the greater the potential cooling it provides, at the cost of additional noise.

Other forms of cooling can be used, such as Watercooling, but are much less common due to their additional cost, risk and complexity.

Case

The PC Case is a hardened structure, usually made of thin but strong metal and/or plastic, which encloses all of the PC components, and onto which the motherboard is firmly attached. The case provides the basic framework required for holding together and protecting all the components of a modern PC. However a case also increases the potential for heat buildup around components, and can also trap dust which can cause hardware to overheat and malfunction if not cleaned out regularly.

Peripheral

Peripheral is a general term referring to any device attached or used externally to a PC, such as a mouse, keyboard or printer. The term specifically indicates that the device tends to lie on the periphery - that is, the outside - of the PC case. The only thing peripherals have in common with each other is that they provide additional input and output capabilities to a PC.

Operating System and Software

The Operating System (OS), such as Windows 8, is a vital piece of software. It is a compilation of instructions that tells all the hardware and software components in a PC how to function to achieve particular outcomes in a unified manner. An OS is a necessity on all modern PCs since without an overarching program to provide core functionality, all the computer components would not be able to function as a single machine. The OS also provides the main interface for users to be able to interact with the hardware and software.

Software is a more general term, referring to a collection of programmed instructions which, through interaction with hardware, provide various functionality on a PC. While the OS itself is part of the software on a PC, and provides a great deal of functionality, additional installed software provides further functionality to perform more specialized tasks, such as word processing or gaming.

Hopefully the information in this chapter has helped you to better understand common technical terminology used throughout this book. I encourage you to research further about any particular concept or component which may confuse or intrigue you, as it is important to have a solid grounding in the basic concepts and terms before moving on to more advanced material. The better you understand the basics, the more readily you will grasp the more complex topics covered in this book.

NEW FEATURES

This chapter summarizes the most significant feature changes between Windows 7 and Windows 8 that affect usability. You need to be familiar with all of these changes before reading any further. If you have upgraded to Windows 8 from an older version of Windows, such as XP or Vista, then there will be a larger number of noticeable changes that you will need to become familiar with, but unfortunately these cannot all be summarized in this chapter. The rest of this book covers all features, new or old, in full detail. If necessary, jump to the Graphics & Sound and File Explorer chapters after reading this chapter to become familiar with using all of the common elements of the Windows 8 interface.

METRO

Windows 8 introduces the Metro interface, characterized by large, flat multi-colored tiles against a generally non-distracting background. The Start Screen, which always appears after you log in to Windows 8, is the most prominent example of a Metro-based interface, and is the main Metro environment. The Metro design philosophy is aimed primarily at touch-capable mobile devices, such as tablets and smart phones. Microsoft has officially dropped usage of the term Metro, and now refers to it in various ways, including "Modern UI", and "Microsoft Design Language". For the sake of brevity, and to prevent confusion, in this book I use the term Metro.

The key aspects of the Metro interface are covered below.

Start Screen: Windows 8 removes the Start Button and Start Menu from the Desktop, and replaces them with the Start Screen, which is a collection of pinned applications shown as large colored tiles. The Start Screen appears after Windows startup, and can be accessed at any time in a range of ways, including by pressing the WINDOWS key, or by clicking in the bottom left corner of the screen. The Start Screen also incorporates the Search Box functionality found on the old Start Menu, by allowing users to launch a search simply by starting to type a search term while on the Start Screen. You can pin any Metro or Desktop program, file or folder to the Start Screen as a tile by right-clicking on it and selecting 'Pin to Start'.

All Apps: To see a list of all applications, not just those pinned on the main Start Screen area, right-click on an empty area of the Start Screen and select 'All Apps', or press CTRL+TAB.

Tiles: Instead of icons, Metro has Tiles. Clicking on a tile launches a program, but tiles have additional functionality. The most notable of these is the Live Tile feature, which allows a Metro app to provide updates of its current information within its tile, without having to launch the app or keep it active in the background. Tiles can also be resized to two different preset sizes, and can be moved around freely to reorganize them, or split them into Tile Groups with custom category headings.

Metro removes complex hierarchical menus, and replaces them with context-sensitive hidden menus that appear when triggered in certain ways. The most common of these are as follows:

Charms: The Charms menu will appear whenever you move your mouse to the bottom or top right corner of the screen, or press WINDOWS+C, whether in the Metro environment, or on the Desktop. When the Charms menu is opened, five icons will be shown: Search, Share, Start, Devices, and Settings. A clock and calendar overlay will also be shown while the Charms menu is open. To select an option from the Charms menu, move your mouse cursor straight up or down from the corner of the screen, and left-click on the relevant icon. The Search, Share, Devices and Settings items in the Charms menu will reveal different settings and features when selected, based on the context in which they are used. For example, different app-specific

settings will be shown when the Charms menu is opened and Settings is selected while within any Metro app. Similarly, opening the Charms menu and selecting Search will focus on general search when on the Start Screen, but will switch to a focus on searching within an app if Search is opened in a Metro app.

App Bar: The App Bar appears at the bottom of the screen when you right-click, or press WINDOWS+Z, on the Start Screen, on a tile, or within a Metro app. The options that appear in the App Bar will differ based on the context in which it is used.

Navigation Bar: A Navigation Bar may also appear at the top of the screen when right-clicking within a Metro app. The options in the Navigation Bar are used to navigate between different sections of an app, such as between pages, tabs or sections.

Power User Tasks Menu: To access the Power User Tasks Menu, right-click on the bottom left corner of the screen, or press WINDOWS+X. This menu takes a more traditional appearance, allowing access to a range of commonly-used Windows features with a single click.

App Switcher: A Metro-based task switching menu is shown when you move your mouse to the top left corner of the screen and then move it downward. A thumbnail menu of any open apps, as well as the Desktop and Start Screen, are selectable here.

Lock Screen: The Lock Screen appears by default at startup whenever a user account with a password is used to login to Windows. It displays an image, as well as the time and date, and can also display notifications from Metro apps.

METRO APPS VS. DESKTOP PROGRAMS

Metro apps function only in the Metro environment, and cannot be run under the Desktop environment. When a Metro app is launched, it will always open as a full-screen application, and the App Bar, Navigation Bar and Charms menu options will become context-sensitive. Metro apps can only be downloaded from the Windows Store, while Desktop programs can be downloaded and installed from a range of places, and run only on the Windows Desktop environment. Both Metro apps and Desktop programs can be pinned to the Start Screen and launched via Metro, but will run under their respective environments when launched.

The main differences between Metro apps and Desktop apps are covered below.

Installing Metro Apps: There are a range of apps that come pre-installed with Windows 8. To download and install additional Metro apps, you must use the Windows Store, which can be found as the Store app on the Start Screen. Some apps are free, and some require purchase. Any updates for installed Metro apps can only be obtained from the Windows Store.

Minimizing, Maximizing and Closing Apps: The minimize, maximize and close buttons have been removed on Metro apps. Metro app runs completely maximized, and the Metro environment does not allow freely resizable, floating windows like those on the Desktop. When you switch away from an open Metro app, it will remain open in the background. To completely close an open Metro app, while within the app you must either press ALT+F4, or move your mouse to the very top of the screen, left-click and drag downwards to the bottom of the screen.

App Snap: There is a way to have two Metro apps open side-by-side, or have a Metro app open alongside the Desktop environment. This is known as App Snap, and to activate it, open the app that you wish to snap to the side of the screen, then left-click at the very top of the screen and drag it to the far left or far right side as desired. Alternatively, press WINDOWS+. (i.e., the WINDOWS key plus the period key) to cycle through App Snap positions. You can now open another app - whether Metro or Desktop-based - and the newly

launched app or Desktop program will take up the rest of the screen. App Snap only works if your screen resolution is 1366x768 or above.

More details on all of the features of the Metro interface, including its customization, can be found in the Graphics & Sound chapter.

LOCAL ACCOUNT VS. MICROSOFT ACCOUNT

Windows 8 introduces two separate types of user account, known as a Microsoft Account, and a Local Account. A Local Account is similar to the user accounts in previous versions of Windows. It does not require a password, and stores all information locally on your PC. A Microsoft Account requires both a valid email address and a password, is an online-based account that can store your Windows 8 customizations on Microsoft's SkyDrive servers in encrypted form, for use in synchronization across your PCs or devices when you login with the same account. You can choose to set up a Microsoft Account or a Local Account during Windows installation, and subsequently switch your user account between these two types at any time thereafter.

More details on Local Accounts, Microsoft Accounts, and user accounts in general, can be found in the User Accounts chapter.

WINDOW SEARCH

Along with removing the Start Menu, Windows 8 removes the main Search Box found at the bottom of it. Primary access to the Windows Search functionality is now via the Start Screen. To initiate a search, simply start typing your search term while on the Start Screen, and it will switch to the search interface. Alternatively, open the Charms menu and select Search, or press WINDOWS+Q.

In Windows 8, the search screen splits any search results into four separate categories: Apps, Settings, Files, and a list of individual apps. The category you are searching within will be highlighted on the right, and displayed in large text at the top left of the main Search Results area. You can select any other category to see any relevant results listed there.

The search functionality pulls its results directly from a special Search Index, and as such, the results you see are not a comprehensive listing of all files on your system. To conduct a more thorough search, you will need to use the advanced search functionality of File Explorer. Click the Search Box at the top right of File Explorer, and a range of advanced options will appear under the Search menu in File Explorer's ribbon.

More details of the search functionality in Windows can be found in the Windows Search chapter.

DESKTOP

The traditional Desktop environment is still available in Windows 8, however it does not load up by default after Windows startup, and must be launched by clicking the Desktop tile on the Start Screen. The Desktop is largely unchanged in Windows 8, but the most prominent differences are covered below.

Start Menu: The Start Button, and the Start Menu that opened when it was clicked, have both been completely removed from the Desktop. Clicking on the area where the Start Button used to be now switches you to the Start Screen, because it is the replacement for the Start Menu.

Aero Glass: The Aero Glass transparency effects used for Desktop elements in Windows Vista and Windows 7 have been removed in Windows 8. Only the Taskbar retains a very basic level of transparency. The Desktop has been redesigned to more closely align to the Metro design philosophy, through the use of flat, monochromatic, opaque, sharp-edged tile-like windows.

Peek - Previously called Aero Peek, you can use the Peek function if you want to quickly glance at what is currently on your Windows Desktop without minimizing or close your open windows. It is disabled by default in Windows 8, so right-click on the far right of the Taskbar and select 'Peek at desktop' to enable it. Whenever you hover your mouse pointer over the same area, everything in front of the Desktop will be hidden until you move your mouse away again.

Snap - Previously called Aero Snap, you can still use the Snap function to quickly resize open windows by dragging the window in a particular direction. Drag an open window to the far left or far right edges of the screen and it resizes, to take up exactly half the screen. Drag a window to the very top of the screen and it becomes maximized. Drag a maximized window downwards and it converts to its regular windowed mode.

Shake - Previously called Aero Shake, the Shake feature also continues on in Windows 8, allowing you to quickly minimize all open windows except one. Grab and rapidly shake the window of your choice left and right, or up and down, repeatedly to minimize all other open windows at once. Doing the same thing again will restore all the windows to their previous state.

More details on all of the features of the Desktop interface, including its customization, can be found in the Graphics & Sound chapter.

FILE EXPLORER

File Explorer, the main interface used to manipulate files and folders, known as Windows Explorer in previous versions of Windows, can be opened by clicking the yellow folder icon found on the Taskbar, or by pressing WINDOWS+E. While most of File Explorer's functionality remains unchanged, the most significant difference, aside from the name change, is the incorporation of the Ribbon interface in place of the menu bar, adding a large range of options. The Ribbon is a collapsible menu system that came to prominence in Microsoft Office 2007, and is identified by a series of overlapping toolbars selected via tabs.

More details of all File Explorer-related functionality can be found in the File Explorer chapter.

OPTIMIZE DRIVES

What was previously known as the Windows Disk Defragmenter, has been converted into the Optimize Drives utility in Windows 8. It now addresses both fragmentation on hard drives, as well as TRIM cleanup on solid state drives. To access the Optimize Drives utility, go to the Start Screen, type *dfrgui* and press Enter. Optimize Drives will automatically detect your drive types, and when run, will either conduct a defragmentation on HDDs, or send TRIM commands to SSDs, as appropriate.

The Optimize Drives utility is covered in more detail under the Optimize Drives section of the Drive Optimization chapter.

TASK MANAGER

Task Manager is a Windows utility that allows you to view real-time information about which applications, processes and services are running on your system, as well as a range of performance and system information. Task Manager can be accessed in a range of ways, including by pressing CTRL+ALT+DEL and selecting 'Task Manager', or with CTRL+SHIFT+ESC. The most common use for Task Manager is terminating an application that is not responding. However, this utility has been significantly revamped in Windows 8, and is now much more useful due to an improved user-friendly interface, as well as more detailed performance data.

See the Task Manager section of the Performance Measurement & Troubleshooting chapter for details.

INTERNET EXPLORER

Windows 8 comes with Internet Explorer 10, which can be launched from the Internet Explorer tile on the Start Screen, or the blue Internet Explorer logo pinned to the Taskbar on the Desktop. The two separate launch methods correspond with the two separate versions of IE: Internet Explorer Metro, and Internet Explorer Desktop. They share the same rendering engine, and many of the same settings, the bulk of which you can adjust in Internet Options, found in the Windows Control Panel. However, in all other respects, these two browsers are quite separate from each other, and have different interfaces and capabilities. In particular, while both versions of IE now come with Flash Player built-in, Internet Explorer Metro has limited Flash capabilities, and does not support other plugins.

Both versions of Internet Explorer 10 are detailed in the Internet Explorer chapter.

WINDOWS MAIL

Windows 7 did not come with any built-in email application, but Windows 8 does, in the form of the Mail app on the Start Screen. This Metro-based app has limited functionality, and does not allow the use POP or IMAP accounts. You may need to install another Metro app or Desktop program that allows greater functionality for email. Windows Live Mail is suggested, and can be downloaded for free as part of the Windows Essentials suite.

More details on configuring all of the options in Windows Live Mail, including instructions on how to configure it to more closely match the look and behavior of previous Windows mail clients, can be found in the Windows Live Mail chapter.

WINDOWS MEDIA CENTER & DVD PLAYBACK

As of Windows 8, the ability to play back DVD movie discs by default has been removed from Windows. Furthermore, just like previous versions of Windows, you cannot play back Blu-ray movie discs by default in Windows. You will require additional software to enable DVD or Blu-ray movie disc playback functionality. Microsoft has also removed Windows Media Center, making it a standalone upgrade that can be added on through the Add Features to Windows 8 component of the Windows Control Panel.

DVD and Blu-ray playback, along with usage of the built-in Windows Media Player utility are covered in the Windows Media Player chapter; obtaining Windows Media Center is covered under the Add Features to Windows 8 section of the Windows Control Panel chapter.

POWER OPTIONS

The power options, such as shutdown, restart, and sleep, are not visible on the Start Screen and the Desktop. These have been moved, and can now be accessed in several ways:

§ Open the Charms charm and select Settings, or press WINDOWS+I, and then click the Power icon.
§ Press CTRL+ALT+DEL and then click the Power icon in the bottom right corner.
§ Press ALT+F4 while on the Windows Desktop to access a Shutdown selection menu.

ADMINISTRATOR COMMAND PROMPT

One important and frequently-used function in this book is an Administrator Command Prompt. This type of Command Prompt has elevated Administrator privileges when User Account Control (UAC) is enabled, necessary in order to successfully implement certain commands. Given the changes in Windows 8, the various methods for launching an Administrator Command Prompt have changed:

- Go to the Start Screen, type *cmd*, then right-click on the Command Prompt tile that appears, and select 'Run as Administrator' in the App Bar.
- Go to the Start Screen, type *cmd*, then press CTRL+SHIFT+ENTER.
- Right-click on the bottom left corner of the screen and select 'Command Prompt (Admin)', or simply press WINDOWS+X+A.
- To create an Administrator Command Prompt shortcut, go to the Start Screen, type *cmd*, then right-click on the Command Prompt tile, and select 'Open file location' in the App Bar. Right-click on the Command Prompt shortcut, and select Send To>Desktop to create a shortcut on your Desktop. Right-click on this new shortcut, select Properties, click the Advanced button under the Shortcut tab, and tick 'Run as Administrator', then click OK.

When an Administrator Command Prompt is correctly launched, you will see the word *Administrator: Command Prompt* in its title bar.

WINDOWS CONTROL PANEL & PC SETTINGS

The Windows Control Panel, which holds the bulk of the components used to access various features and settings in Windows 8, is not visible by default. To access it, type *control* on the Start Screen and press Enter, or right-click on the Start Screen, select 'All Apps', then look for the Control Panel tile. You can right-click on this tile and pin it to the Taskbar or Start Screen for easier access in the future.

Windows 8 also introduces a new PC Settings section, containing a range of additional Metro and Desktop-related settings. To access it, open the Charms menu, select Settings, then click 'Change PC Settings' at the bottom.

The Windows Control Panel is covered in detail in the Windows Control Panel chapter; the PC Settings are covered in the PC Settings chapter.

KEYBOARD SHORTCUTS

The changes to the interface in Windows 8 have added a number of new or changed shortcuts, as well as increasing the usefulness of keyboard shortcuts. The standard usage format for keyboard shortcuts presented in this book is to refer to the pressing of two or more keys simultaneously by using the '+' sign. For example, ALT+TAB means you should press both the ALT key and the TAB key on your keyboard. References to the WINDOWS key are to the key found between CTRL and ALT on most PC keyboards, usually labeled with the Windows logo.

On the next page is a consolidated list of the most common keyboard shortcuts to quickly access useful functions in Windows 8. A detailed list of all Windows and program-specific keyboard shortcuts is provided in this Microsoft Article.

Keys	Function

Common Functions

CTRL + C	Copy selected item(s)
CTRL + X	Cut selected item(s)
CTRL + V	Paste copied/cut item(s)
CTRL + Z	Undo last action
CTRL + Y	Redo last action
SHIFT + DEL	Delete highlighted item, bypassing Recycle Bin
F2	Rename an item
F5	Refresh active window
TAB	Step forward through screen elements
SHIFT + TAB	Step backward through screen elements
ALT + F4	Close highlighted Desktop program or Metro app Show PC Shutdown options if on Windows Desktop
ALT + TAB	Open Task Switcher to switch between any active Desktop programs or Metro apps
CTRL + ALT + TAB	Open Task Switcher permanently - TAB or Arrow Keys to cycle through open tasks, Enter to select, ESC to exit
CTRL + SHIFT + ESC	Open Task Manager
WINDOWS + E	Open File Explorer
WINDOWS + R	Open Run box
WINDOWS + X	Open the Power User Tasks Menu
WINDOWS + X + A	Open Administrator Command Prompt
WINDOWS + F1	Open Help & Support
WINDOWS + P	Open multi-display output menu
WINDOWS + L	Activate the Lock Screen
WINDOWS + PRTSCN	Take a screenshot of current screen and save it to the Pictures Library

Metro-Specific Functions

WINDOWS	Open Start Menu, or toggle between Start Menu and Desktop
WINDOWS + C	Open the Charms menu
WINDOWS + F	Open Search in the Charms menu on the Files category
WINDOWS + Q	Open Search in the Charms menu on the Apps category
WINDOWS + W	Open Search in the Charms menu on the Settings category
WINDOWS + H	Open Share in the Charms menu
WINDOWS + K	Open Devices in the Charms menu
WINDOWS + I	Open Settings in the Charms menu
WINDOWS + Z	Show the App Bar
WINDOWS + TAB	Switch between open Metro apps
WINDOWS + .	Open App Snap, and cycle through snap positions
WINDOWS + J	Switch between main app and snapped app

Desktop-Specific Functions

ALT	Open the Menu Bar in a Desktop program
WINDOWS + D	Minimize or restore all open windows on the Desktop
WINDOWS + Number	Open pinned item on Taskbar - the number corresponds with the order of the item on the Taskbar from left to right
WINDOWS + ALT + Number	Open the Jump List for the specified pinned item on the Taskbar
WINDOWS + T	Cycle through all Taskbar icons, press Enter to select one
WINDOWS + Up Arrow	Maximizes window
WINDOWS + Down Arrow	Minimizes window
WINDOWS + Left/Right Arrow	Cycle through Snap positions
SHIFT + RIGHT CLICK	Open Expanded Context Menu for highlighted item

This chapter has briefly highlighted some of the more noticeable changes in Windows 8. There are however numerous changes, some large and some small, for which you must steadily read through this entire book to learn more about. Additionally, most any Windows feature can be customized to some extent, so if there are features you don't like, the book will show you how to alter their behavior to better suit your needs. From this point onwards you can read the book sequentially, or jump to any chapter you wish. I recommend becoming familiar with the contents of the Graphics & Sound, File Explorer, Windows Drivers and Security chapters as soon as possible.

SYSTEM SPECIFICATIONS

The first step in optimizing or customizing your PC is to determine precisely which hardware components you have, and what their various capabilities are. This is known as your System Specifications, and to find out the specific details of your hardware you will require an appropriate set of tools. Information about your system specifications is vital, both for using this book, and for general PC usage and maintenance in the future. For example, you must know the exact model and chipset type of your motherboard before you can upgrade your BIOS, or install the correct motherboard drivers; you must know the full capabilities of your graphics card if you want to update its drivers, or to see whether it can run the latest games; or you may have a problem that you wish to resolve yourself, or provide details of to a technical support person.

This chapter covers the tools you need and the methods you can use to obtain all of the relevant system information.

< SYSTEM INFORMATION TOOLS

There are a range of good free system information utilities to choose from, including some comprehensive ones built into Windows 8. A combination of these programs will tell you everything you need to know about your system specifications and capabilities:

WINDOWS EXPERIENCE INDEX

Found under the Performance Information and Tools component of Windows Control Panel, or by typing *performance information* on the Start Screen, selecting Settings and pressing Enter, the Windows Experience Index (WEI) is a built-in benchmark data designed to rate the performance of your system in five separate categories. It is covered in detail under the Windows Experience Index section of the Performance Measurement & Troubleshooting chapter, and if you haven't run the WEI yet I recommend doing so now. For the purposes of displaying system information, click the 'View and print detailed performance and system information' link shown here. This will open a new window with more detailed information on your system specifications. The information provided is certainly useful as a starting point, however it is not detailed enough for our purposes. Important information, such as the make and model of your motherboard, is not provided for example.

TASK MANAGER

Task Manager can be readily accessed by right-clicking on the Taskbar and selecting Task Manager, by pressing CTRL+ALT+DEL and selecting Task Manager. The functionality in the new and improved Windows 8 version of the Task Manager is covered in full detail under the Task Manager section of the Performance Measurement & Troubleshooting chapter.

Of relevance to this chapter, if you click the 'More details' link at the bottom of the default Task Manager window, then look under the Performance tab, you will see several hardware categories listed on the left side of the window, including CPU, Memory, Disk(s) and Network connection. Click on each category, and on the right side of the window you will see more details of the relevant hardware. For example, under the CPU section of the Performance tab, your CPU model and speed is listed at the top of the graph, and beneath the graph are details such as the number of cores, hardware support for virtualization, and CPU cache sizes.

Though handy, the hardware information provided by Task Manager is not extensive and once again, important details are omitted.

WINDOWS SYSTEM INFORMATION TOOL

You can access the Windows System Information Tool by typing *msinfo32* on the Start Screen and pressing Enter. The System Information tool presents a range of information about your system. Some of its more useful functionality related to hardware includes:

§ A listing of your hardware components by type under the Components section, as well as driver and codec details.
§ All the system driver files and their current status under Software Environment>System Drivers.
§ IRQ allocations under Hardware Resources>IRQs.
§ Shared IRQs and other potential conflicts under Hardware Resources>Conflicts/Sharing.
§ Recent Windows errors are found under Software Environment>Windows Error Reporting.

In general the System Information tool is best used by medium to advanced users who can comprehend the more complex interface and its detailed information much more easily than a beginner. Its main advantage is that it is a free built-in utility that anyone can easily access.

DEVICE MANAGER

You can access Device Manager under the Windows Control Panel, or by typing *device manager* on the Start Screen, selecting Settings and pressing Enter. As a built-in Windows utility you can gain a great deal of useful information about your hardware and associated drivers from this tool. Your major devices are displayed under various categories, and you can even choose to update or downgrade individual device drivers, or uninstall a device altogether, should you wish. The Device Manager has several important roles, and is covered in detail under the Device Manager section of the Hardware Management chapter.

DIRECTX DIAGNOSTICS

You can access the DirectX Diagnostic Utility (DXDiag) by typing *dxdiag* on the Start Screen and pressing Enter. DXDiag is another built-in Windows Diagnostic/System Information tool, and is part of DirectX 11.1 - see the introduction to the Graphics & Sound chapter for more information on DirectX. When first launched, DXDiag will ask to check if your drivers are signed. It is fine to select Yes to allow it to do this, however it is not necessary, and selecting No will not cause any problems, nor will the presence of non-WHQL certified drivers be a major issue. You can alter this behavior within DXDiag at any time by ticking or unticking the 'Check for WHQL digital signatures' box under the main System tab. For more details on digital signatures and WHQL certification, see the Driver Signature section of the Windows Drivers chapter.

The main System tab of DXDiag displays a basic overview of your system, such as your Processor (CPU) type and speed, amount of Memory (physical RAM) and the Pagefile (Virtual Memory) usage among other things. Under the Display, Sound and Input tabs you will find further information about the particular hardware you are running for each of these functions. Any problems found by DXDiag indicate that there may be an issue with your hardware or drivers. In the first instance, make sure that you have installed the latest drivers for each device, as covered under the Windows Drivers chapter. If problems persist, see the Performance Measurement & Troubleshooting chapter.

The most useful function for DXDiag is its ability to generate a highly detailed text file which lists your major system information, including all of your main hardware specifications, driver files, and environmental settings. To create this text file click the 'Save All Information' button found at the bottom of the DXDiag window. You will be prompted to save this report somewhere, and the default of the Windows Desktop is fine. You can now double-click on this *DxDiag.txt* file to read through its contents. It can be attached to an email you can send to a technical support person, or its contents can be copied and pasted onto an online forum to allow others to help you with any problems you may be experiencing. It doesn't contain any sensitive information such as serial numbers or passwords, so it is safe to post publicly.

SANDRA

Sandra stands for System ANalyser, Diagnostic and Reporting Assistant. You can download Sandra from the SiSoftware Website. The Lite version is free, and retains sufficient functionality for basic needs.

Once installed, Sandra provides a selection of hardware information under the Hardware. If you want a good overview of your key hardware components, then double-click on the Computer Overview module under the Hardware tab. After a few moments it will display a range of useful information about your system, such as the CPU speed and type, your motherboard Chipset, and your individual Memory Module(s) brand, size and speed. If you then want to know more about a particular component, launch the relevant module under the Hardware tab. For example, to find out more about your motherboard, open the Mainboard module and it will display very detailed information on that specific component.

Sandra also has several useful benchmarking and stress testing features that are covered in more detail under the Third Party Tools section of the Performance Measurement & Troubleshooting chapter.

CPU-Z

A highly recommended free tool, CPU-Z provides you with all the major information you require about your hardware. It has very detailed information about your processor under the CPU and Caches tabs, such as the CPU brand, socket type, speeds and voltage, and the various cache sizes. It also provides key motherboard details under the Mainboard tab, and your RAM's complete details under the Memory and SPD tabs. Note that for information to appear under the SPD tab, you must first select the relevant slot number(s) on the motherboard that your RAM stick(s) occupy in the drop-down box at the top left. CPU-Z even provides the basic details of your graphics card under the Graphics tab, though the PCI-E link speeds are shown under the Graphics Interface section of the Mainboard tab.

GPU-Z

Another highly recommended tool, GPU-Z is distinct from the CPU-Z utility covered above; it relates to your GPU (Graphics Processing Unit), which is typically a graphics card. Launch the utility, and much like CPU-Z, it will provide you with highly detailed information on graphics card. Under the main Graphics Card tab you will see all of the specifications for your graphics hardware, including the amount and type of Video RAM, the level of Direct X support, the BIOS version and the clock speeds. Under the Sensors tab you will find your current clock speeds, temperatures, fan speed and so forth. You can even see a rough measure of your GPU's overall quality by clicking on the GPU icon above the Graphics Card tab and selecting 'Read ASIC quality'. There are additional settings that are selectable from that menu as well.

Note that the Validation tab is there only if you want to submit your specifications to the GPU-Z Statistics Database, which is not necessary.

HD TUNE

HD Tune is a tool for quickly gaining an insight into your drive details and current capabilities. The free (non-Pro) version has sufficient functionality to provide important drive details. Select the relevant drive from the drop-down box at the top of the utility, the click on the Info tab. Here you will find a list of supported features, the drive firmware version, serial number, supported and active standards. Select the Health tab to see the health status of the drive. HD Tune supports both hard drives and solid state drives, and even includes a benchmark, which is covered under the Third Party Tools section of the Performance Measurement & Troubleshooting chapter.

There are many other system information tools that are available, some of which are not free. However there is absolutely no need to load up your system with a multitude of such utilities. A combination of the free and built-in tools covered in this chapter should be more than enough to give you all of the details you will ever need for every aspect of the hardware that is currently inside your PC. You should also make sure that you are completely familiar with the concepts covered in the Basic PC Terminology chapter.

It is an extremely important element of PC optimization and customization that you have more than just a passing acquaintance with your hardware components and what they do. Becoming familiar with hardware specifications and what they mean provides a range of benefits, including: ensuring that you install the correct drivers, which is critical to system stability and performance; allowing you to discover potential areas of further optimization unique to your system configuration; improving your ability to troubleshoot problems, or to provide relevant information to those helping you to solve a problem; and importantly, giving you the knowledge to make better purchasing decisions when it comes time to buy a new system, or upgrade components in your existing system.

BACKUP & RECOVERY

Computers store a great deal of valuable information. Over time your PC will come to hold a lot of important, private, irreplaceable data such as digital photographs, home movies, financial documents, emails, bookmarks and login details. It is of critical importance that you establish an appropriate method for regularly storing up-to-date copies of this information elsewhere, so that if your PC is stolen, damaged, or its data is corrupted or accidentally overwritten, you do not lose all of this valuable data permanently. The result of undertaking such a task is referred to as a Backup, and it is a vital and unavoidable part of sensible computing.

This chapter not only covers various backup strategies and tools, it also details a range of useful data recovery methods you can use to regain valuable information which has been lost through forgetting passwords, accidental deletion of files, data corruption, or damage to your Windows installation. You should have at least one backup copy of all of your important and irreplaceable data before proceeding any further with this book.

< WINDOWS FILE HISTORY

Windows 8 comes with a new simplified built-in backup solution called File History. The File History component can be found in the Windows Control Panel, or launched by typing *file history* on the Start Screen, selecting Settings, and selecting 'File History'. It is off by default, and requires a separate connected external drive, such as another hard drive, SSD or USB flash drive, or an available location on your network. It cannot save backups to your current system drive. If a valid drive is detected, it will be displayed in the File History window.

Once enabled, File History will perform a backup of the contents of your Libraries, Favorites and Contacts folders, as well as anything stored on the Windows Desktop. It will not backup any files or folders outside of these locations, nor will it save any system files or core Windows files, or provide the capability to create an image of your entire system drive - some of those features can be found under the System Protection and Windows 7 File Recovery components, covered later in this chapter. The File History feature focuses solely on backing up your potentially irreplaceable personal files, which it assumes will be kept in one of the four locations it monitors.

File History functions via a feature unique to NTFS files known as the USN Journal, which maintains a record of changes to files. This allows File History to quickly become aware of whether there have been any changes to a file or folder in one of the locations it is monitoring. If a change is detected, File History will save a new time-stamped backup copy of that file to your chosen backup location on a set schedule, the default being every hour. Each backup of a changed file is stored as an independent copy, allowing you to access multiple versions of the same file over time.

AUTOMATED BACKUPS

To start automatically backing up your files on a regular basis, first open File History then go through each of the steps below:

Select Drive: The first step is the most critical one, as you will need to choose a drive to which your files will be backed up. When turned on, File History will automatically select an external drive if one is connected. To choose another drive, click the 'Select drive' item on the left of the File History window. Alternatively, you can connect a drive to the system and select 'Configure this drive for backup' from the AutoPlay options which appear.

The backup drive selected must be a separate drive that is currently connected to your PC, and not the drive on which your files currently reside, as this defeats the purpose of backing them up - if your source drive is also your backup drive and it fails, is damaged, or is stolen, you will lose both the originals and backup copies. You can also backup to a separate location on a connected network, but File History will not let you backup to a location on the Internet, such as SkyDrive.

For most standalone home PCs, an external USB hard drive, or a large USB flash drive, is the simplest and cheapest available solution, however a dedicated internal hard drive or SSD will provide both faster performance and greater protection, as it is always connected and thus more likely to be kept up-to-date. When the chosen backup drive is disconnected from your PC, Windows File History will continue to generate backup snapshots of changed files, but will store them in a temporary cache on the local drive - up to a specified limit of local disk space - until you next connect the backup drive. In such instances your backup files are not secure, and could be lost if your local drive fails, or if it runs out of storage space for the cache.

The amount of disk space required depends firstly on the total size of all of the files in your Libraries, Favorites, Contacts and Desktop. The bulk of the files will be in your Libraries. Right-click on each Library in File Explorer and select Properties, and check the figure shown in the 'Size of files in library' line. Add these up for all of your Libraries and you will have a good idea of how much disk space is initially required. Next you will need to take into account that File History maintains multiple complete versions of each file that is changed, and by default it will retain these versions forever. So, for example, if you frequently make changes to large documents or pictures, this can rapidly balloon the amount of backup space required, as there will be many copies of those large files stored as separate backed up versions.

Exclude Folders: The default locations from which files and folders are backed up are: Libraries, Favorites, Contacts and the Windows Desktop. Anything under these locations, aside from Windows system files and folders, will be backed up by File History. If there are any folders that you wish to exempt from being backed up, click 'Exclude Folders' on the left of the File History window, then click the Add button and browse to the relevant folder, highlight it and click the 'Select Folder' button.

Include Folders: File History doesn't allow you to directly select specific files or folders to include in your backup. However you can still add any folder to your File History backup by first adding it to an existing Library, or by creating a new Library, and then adding any folders elsewhere on your drive(s) - see the Libraries section of the File Explorer chapter for more details. For example, you can create a new Miscellaneous or Backup Library just for this purpose. Since all Libraries are automatically included in File History's backups, the next time it runs it will include your new Library and the contents of all of its included folder locations in your backup. This is one of the reasons why you should get into the habit of storing all of your data in a local Library - see the Personal Folders and Libraries sections of the File Explorer chapter for details.

Advanced Settings: Click the 'Advanced Settings' link on the left of the File History window to alter several important parameters for how File History operates:

§ Save copies of files - This setting determines the frequency with which the File History process wakes up to check for changes, and save backup copies of any changed files to your external drive or network location. The maximum frequency is every 10 minutes, the minimum is once per day. The more frequently you set it to backup, the more up-to-date your backups will be, but the larger the size of your backup, as more separate versions are saved. The default is once every hour, but you may wish to change this to something like every 12 hours to strike a better balance between having an up-to-date backed-up version available at any time, without constantly writing to your backup location and

blowing out the size of your backup. Note that you can manually force a backup run at any time by opening the File History window and clicking the 'Run now' link.

§ Size of offline cache - Whenever your backup location is unavailable - e.g. if you have disconnected an external USB drive - then Windows will still continue to regularly create backups of any changed files on its nominated schedule. These backups will be saved to a temporary location (dubbed the 'offline cache') on your local drive, until such time as you reconnect your external backup drive, at which point the offline cached backup will be transferred to your main backup location. This setting allows you to decide how much of your local drive's space you will allocate to the offline cache. The default is 5% of total disk space, and the available options are 2%, 5%, 10% and 20%. The amount you allocate needs to be based on several factors including: the size of your local drive, the size of your backup, how frequently you make changes to the files, how often you have set File History to save those changes, and how often (if ever) you disconnect your backup drive. If you do not allocate sufficient space, especially if you frequently work on large files and/or have File History set to save often and/or disconnect your backup drive for lengthy periods, then you could lose some versions of your backed up files when the local offline cache limit is reached.

§ Keep saved versions - By default Windows File History will keep each and every separate version of any file you change forever. You can alter this setting so that it removes older versions based on how long ago they were changed, such as keeping them for only 1 Month, or up to 2 Years, or only as long as there is available space on the backup drive. If your backup drive runs out of space at any time, Windows will notify you and ask you whether you wish to replace the drive or change this setting. Note that you can run a cleanup of older files at any time by clicking the 'Clean up versions' link below this setting and specifying which older versions to remove based on how long ago the backups were made.

Once you have chosen your settings, click the 'Save changes' button at the bottom of the window.

RESTORING BACKUPS

To restore your automated backups at any time, click the 'Restore personal files' link on the left of the File History window, or browse to the current version of the file or folder (if it still exists) in File Explorer, highlight it, then click the History button under the Home menu.

The interface for previewing and restoring backup files has been simplified in Windows 8, taking most of the guesswork out of finding and restoring the correct backup version. The Restore interface is very similar to File Explorer. At the very top of the window is a navigation bar which shows you where you are in the directory structure. The base directory is simply called Home, and each of your sub-directories retain the same name as their original counterparts. To go back up the directory tree, click the up arrow at the far left of the navigation box; to look at the contents of any folder or Library, double-click on it. You can also choose between thumbnails or details view as desired by clicking the relevant icon in the bottom right corner of the Restore window.

Importantly, you can scroll through each of the individual times/days at which a backup snapshot was taken by using the forward and back arrows at the bottom of the Restore window. As you scroll through each snapshot period, the current snapshot and the total number of available snapshots is shown at the top left of the window, along with the current snapshot's date and time stamp (e.g. 2 of 7, Friday, 20 July 2012 5:30pm).

Navigate to the file or folder you wish to potentially recover, then right-click on it and select Preview to see its contents within the Restore window. This allows you to determine whether this is the correct version of the file you want to restore. Once you have found the correct version, to restore it either click the large green Restore button at the bottom of the window to restore the file to its original location - keeping in mind that this may overwrite another version of the same file already there - or right-click on it and select 'Restore to' to choose a new location to restore this backup.

If for any reason you can't access the Windows 8 restore interface, the backup files on your device can still be accessed individually, such as by examining the drive in Windows Explorer on a previous version of Windows. The backup is not encrypted or otherwise secured by File History. Your files and folders will all be found under the *\FileHistory\User\[PC Name]\Data\[Drive Letter]\Users\[Username]* directory of the backup drive. Each individual file is a complete backup copy of a particular version of that file, and each has a timestamp appended to its filename to distinguish it from other versions.

Windows File History is a useful feature for automatically and regularly backing up all of your personal information, as long as you arrange all of that information to reside in your Libraries. Any version of your data can then be restored through an easy-to-use interface. Ideally you should dedicate a separate drive to this feature if you wish to use it, and ensure that the drive is either connected permanently to the system, or connected frequently to it, to maintain up-to-date backups of your key personal data.

< WINDOWS 7 FILE RECOVERY

Aside from File History, Windows 8 also comes with a version of the Backup and Restore feature found in Windows 7. This allows you to create both backups of specific folders, and also an exact copy of an entire drive, to a location of your choice. You can access Windows 7 File Recovery as a component under the Windows Control Panel, by opening the File History window and clicking the 'Windows 7 File Recovery' link at the bottom left, or by typing *windows 7 file recovery* on the Start Screen, selecting Settings and pressing Enter. The process for backing up and restoring data using this utility is covered below, both for fully automated backups and for manually initiated backups.

AUTOMATED BACKUPS

Before being able to automatically backup your data on a regular schedule, Windows needs to know the location to which your backups will be saved, the type of backup you wish to make, and the frequency with which this occurs. This is all done via the 'Set up backup' link shown in the main Windows 7 File Recovery window. Once opened, run through these series of decisions:

Backup Destination: The backup destination can be any location detected by the system, except for the logical drive containing your existing installation of Windows 8, or the logical drive used to boot up the system. You can backup to another partition on the same drive, though this is strongly discouraged. You can also backup to a USB flash drive or external drive. If the relevant drive(s) are currently not connected to your system, connect them and click the Refresh button to have them show up on the list of destination drives. Importantly, the drive must be in NTFS format for it to be available in the list of drives. This backup process does not reformat, alter or erase any of the existing data on the destination drive, although it will replace any existing system images created by Windows on that drive.

Type of Backup: Once a destination is chosen, you will have to select the type of backup Windows will be making. There are two main choices:

Let Windows Choose - If this option is selected, Windows will automatically choose the following data to backup without any input from you:

- Files in the Libraries, however this excludes any files located on the Internet, on another computer in a network, on a non-NTFS drive, or on the drive onto which the backup is being made.
- Any files on the Windows Desktop.
- All files and folders under the *\AppData, \Contacts, \Downloads, \Favorites, \Links, \Saved Games,* and *\Searches* directories for every user on the system.

This basically means that every default folder under the *\Users* directory will be backed up.

Furthermore, if there is sufficient space on your destination drive, Windows will also create a System Image, which is an exact copy of the entire contents of your system drive, which is the drive(s) required to run Windows. A system image contains all of the data necessary to recreate your entire installation of Windows, including all installed programs and settings, and all of your personal data, to the exact state it was in when the system image was created. This means it can be extremely large as a result.

Let Me Choose - If you wish to have greater control over which particular folders are backed up, select this option and you can then manually select which folders you wish to include. The 'Back up data for newly created users' is a generic option which, if ticked, ensures that for automated backups, if any new user accounts are created in the future, Windows will automatically add their Libraries and personal data to the backup. The '*[username]* Libraries' option, which is ticked by default, includes all of the default folders under the *\Users\[username]* directory, but you also can manually select any folders you wish instead of these, or in addition to these, by expanding the folder list under the Computer item and ticking the relevant directories.

Regardless of which folders you choose however, Windows will not save the following data as part of the backup:

§ Files which are default components of installed programs - this excludes saved games and things like custom setting/configuration files, which can be backed up.
§ Files that are in the Recycle Bin.
§ Temporary files on drives less than 1GB in size.
§ Files on non-NTFS drives.

If the 'Include a system image of drives' box at the bottom of the window is also ticked, Windows will include an additional full system image of your system drive(s) as part of your backup, space permitting.

Frequency of Backup: The final step before the backup is created is to review your settings, and confirm the schedule for backing up. This option appears towards the bottom of the Review your backup settings window, and can be easy to miss, although if it can't be selected, this is because your chosen destination drive does not support scheduled backups. By default the automated backup is set to run at 7:00pm every Sunday night. Click the 'Change schedule' link to bring up a new box, allowing you to choose whether to run the backup daily, weekly or monthly, at a particular time and date, and most importantly, whether you want to disable scheduled backups altogether by ticking or unticking the 'Run backup on a schedule' box. You can also turn off an existing schedule at any time by clicking the 'Turn Off Schedule' link on the side of the main Windows 7 File Recovery window.

Once done click OK, then to commence backup click the 'Save settings and exit' button and Windows will begin backing up your selected data to the destination drive. The process may take quite a while depending on the destination drive's speed and the volume of data involved. Once this process is completed, the destination drive will contain one or both of the following:

§ A *WindowsImageBackup* folder - This contains a full system image, and under normal circumstances, you cannot view or extract individual files or folders from this folder because it stores your system image in a single Virtual Hard Drive (.VHD) file. However see the Virtual Hard Disk section of the Drive Optimization chapter for details of how to manually extract individual files or folders from a system image file without overwriting your existing data.
§ A *[Computername]* folder - This contains individual files and folders not in a system image. By default this folder is given your computer name. Under this main folder there are subfolder(s) with the name(s) *Backup Set [date of backup]*, and under that a similar folder *Backup Files [date of backup]*, and ultimately, a series of .ZIP archives which collectively hold all the individual files and folders that were backed up to

that particular set. These can be manually viewed and extracted with an archiving utility if desired, but that is not the recommended method for doing so.

Both of these folder types are designed to be used by the Restore feature - see Restoring Backups further below.

Incremental Backups: When these backups are updated by Windows, whether on a scheduled basis, or if you manually initiate another backup run through the Windows 7 File Recovery window at any time, Windows will only add any new or changed data to the backup set, it won't create an entirely new backup. This applies equally to system image or individual file backup methods. This saves space and means that subsequent backup runs are not as lengthy as the first time. If you want to manage all of the previous versions of your backed up data, see the Managing Backups section further below.

MANUAL BACKUPS

The Windows 7 File Recovery functionality in Windows 8 is designed primarily so that Windows can automatically backup your selected data on a fixed schedule. This is because a backup is most useful when it is as up-to-date as possible. Unfortunately people tend to be forgetful when it comes to backing up on a regular basis, thus the automated method covered above is the most foolproof option, especially when combined with the automated File History feature. However there are times when you may just wish to manually create a backup. For example, you may wish to create a full system image of your local drive(s) just prior to making potentially risky changes to Windows which might render it unbootable. Having a system image on hand allows you to quickly and easily restore your system to exactly the way it was just prior to the change, undoing any damage.

In such cases you can use the Create a System Image and/or Create a System Repair Disc features of the Windows 7 File Recovery as covered below:

Create a System Image: By default a system image created by Windows is an exact copy of the entire contents of your system drive(s). Once created, it can be used at any time to restore your system to exactly the state it was in when the image was made. When the 'Create a System Image' option is clicked on the left side of the Windows 7 File Recovery window, as with the automated backup method covered earlier, you must first choose your destination drive. Remember that you can't include drives which aren't currently connected, or the drive onto which the backup is being made. Also keep in mind that the destination drive's existing contents will not be overwritten by the system image, so take this into account in terms of available free space. Once selected, click the 'Start Backup' button to begin the backup process. Do this as often as necessary to keep the system image up-to-date.

Create a System Repair Disc: A System Repair Disc is used in cases where you can't boot up into Windows for some reason. It can be used to boot your PC into the System Recovery Options menu, allowing you to repair Windows or restore a system image you created earlier. Your original Windows 8 installation disc can act as a system repair disc. If you don't have a Windows 8 installation disc, by clicking the 'Create a System Repair Disc' option on the left side of the Windows 7 File Recovery window, you will be prompted to enter a blank CD or DVD which Windows will then turn into a system repair disc. See the System Recovery section later in this chapter for full details of how to use a system repair disc and associated recovery options.

MANAGING BACKUPS

Once you have created your backups using Windows 7 File Recovery, you can manage them to ensure optimal use of space on your backup drive. To do this, go to the Windows 7 File Recovery window, and click the 'Manage Space' link found beneath the Location section. Alternatively, go to the drive which holds the backup, right-click on the relevant folder, and then select Restore Options>Manage Space Used by this Backup. This opens a new window, providing you with a summary of the space taken up by various backup

files. You will then be able to access separate features to manage any individual folder backups as well as any system images:

Data File Backup: When you click the 'View backups' button, you will see any data file backups that are currently available. These are backups of personal folders and/or any individual folders you selected. This does not include a system image or any part of it. You can delete any older backups if you wish, as this will help save space, but bear in mind that unlike the File History feature, these backups are incremental, so space is already saved by not duplicating the same data each time; only new or changed data is backed up. This is why the Backup Period shown will span several days for a single backup. However periodically, Windows will create an entirely new full-sized backup and hence begin a new backup period. If you have no need for older versions of files and folders, you can delete any previous backup periods shown here, which will help reclaim drive space without losing the latest copy of your backed up folders. If only one backup period is shown, deleting it will delete all of your backed up folders, so that is obviously not recommended unless you specifically want to remove your backup altogether.

System Image: If you've created a system image, you can click the 'Change settings' button here to access options which allow you to control how backups of system images are managed. When the default 'Let Windows manage the space used for backup history' option is selected, Windows keeps as many copies of system images as it can, except on network locations where only one system image can be kept. If the destination drive's free space falls below 30% of its total size, Windows will begin deleting older system images to prevent the drive running out of space. If you wish to only keep a single system image (the latest) instead, you can select 'Keep only the latest system image and minimize space used by backup', freeing up the amount of space indicated through removal of older system image(s).

Both options are really only designed to reduce the amount of space taken up by backups. If you are not overly concerned about the size of your backups, and want the convenience of having multiple backups in case you need to restore different versions of the same files for example, then the default settings are fine. However if space is limited, I recommend frequently checking and removing all but the latest backups.

RESTORING BACKUPS

If at any time you want to restore or simply view any files and folders backed up via the Windows 7 File Recovery feature, then you should go to the main Windows 7 File Recovery window and click the 'Restore my files' button. Alternatively, go to the drive which holds the backup, and for the relevant folder, either double-click on it, or right-click and select Restore Options and select one of the Restore options available. This opens a Restore Files window which allows you to browse to any particular drive which holds an appropriate backup directory and find a specific file or folder to restore.

If you have a good idea as to where the backup file or folder resides, click the 'Browse for files' or 'Browse for folders' button - depending on whether you want to restore a specific file or an entire folder - and once you've found the appropriate file or folder on the backup drive, double-click on it or highlight it and click the 'Add...' button, and it will be added to a list of files and/or folders to be restored. If you don't know where the file resides, click the Search button, and enter some or all of the filename and click the Search button to have Windows search through your backups to see if it exists. You will be presented with a list of found files which you can tick and then click OK to add to your list of files to be restored. You can repeat the above process as often as necessary until you have added all the files and/or folders you want to restore.

By default Windows will restore the latest version of the file(s) or folder(s) you've selected. To alter this, click the 'Choose a different date' link at the top of the Restore Files window and select a previous date if available.

Once you've selected the files or folders to be restored, click the Next button and you will be prompted to either have the file/folder restored to its original location in each instance, or you can specify a new location.

I strongly recommend selecting the second option and specifying an empty directory of your choice. This prevents the backup version from overwriting the existing version of the file or folder, which may be undesirable especially if the backup winds up being the wrong version or is somehow corrupt or infected. In any case fortunately Windows does not automatically overwrite existing versions even if you choose the first option - you will be prompted in the event of any conflicts and asked to choose whether to overwrite or rename the file or folder, or to cancel the transfer altogether. However restoring your backup file(s) and/or folder(s) to an empty location is best as it allows you to properly check to ensure they are the version you desire and are working correctly and remain free from malware. You can then delete your current version of the file(s) and/or folder(s) to the Recycle Bin as an added safety precaution, and move the backup to its original location manually. Note that it is fine to leave the 'Restore the files to their original subfolders' option ticked, as it will simply create the appropriate subfolders under the new directory you specify, which is useful in sorting restored files.

If you wish to restore an entire system image rather than individual files or folders, you can do so by booting up your system using a startup repair disc or the Windows 8 installation media and using the System Recovery Options covered in detail under the System Recovery section of this chapter. This will allow you to select the 'System Image Recovery' option. Because restoring a system image will overwrite all of the existing content on your system drive, if you want to retain any of the existing data on the drive, copy it to a non-system drive to ensure that it is not lost when the drive is overwritten with the system image. You can then continue, following the prompts to restore your system image.

If for some reason you want to attempt to restore individual files or folders from a system image, it is possible to do so, but requires a more complex set of steps:

1. Open Administrative Tools in the Windows Control Panel and select Computer Management.
2. In Computer Management, select the Disk Management component.
3. Under the Action menu in Disk Management select 'Attach VHD'
4. Browse to the location of the .VHD system image backup file. I recommend ticking the 'Read-only' box before clicking OK, as any changes to this file can corrupt the backup.
5. The VHD will be mounted as the type of drive the .VHD file image was originally saved as.

This drive will now appear as an identical copy of your system drive using a new drive letter, and you can browse it in File Explorer just as with any other drive. Once finished, make sure you detach the VHD drive under the Action menu in Disk Management. See the Virtual Hard Disk section of the Drive Optimization chapter for more details.

Some additional things to note regarding Windows 7 File Recovery:

§ Windows 8 is able to restore backup files created using Windows 7's Backup and Restore feature.
§ If you had an active backup schedule in Windows 7 and did an Upgrade install of Windows 8, the backup will automatically continue running in Windows 8 after the upgrade. You can turn it off or adjust its settings in Windows 7 File Recovery.
§ System images can be used in conjunction with the System Restore feature to provide additional restore points you can use - see the System Protection section further below.
§ If you simply want to restore an earlier version of a personal file, due to recent unintended changes for example, then it is best to use the File History functionality as covered earlier in this chapter.

In practice, both the File History and Windows 7 File Recovery features should play a role in any sensible automated backup plan. File History is best used to automate backup of personal data, while Windows 7 File Recovery allows you to create full system images, which make it easy to quickly restore your entire system to the exact state it was in prior to catastrophic loss. Both features will be of greatest use if the backups are kept up-to-date.

< ORGANIZING DATA FOR AUTOMATED BACKUPS

This section provides details on how best to organize the data on your drive, primarily to ensure that all your important data is backed up correctly using the File History and/or Windows 7 File Recovery features in Windows, while at the same time taking maximum advantage of Windows 8's other features which are covered in more detail later in this book.

Libraries: The key to organizing your data is to store them in Libraries. As with previous versions of Windows, your personal folders are found under the *\Users\[username]* directory, with several clearly-named subfolders designed for specific content, such as My Music or My Pictures. Windows 7 introduced Libraries, which go beyond these default personal folders, allowing you to access and manipulate files of different types across a range of locations in a single virtual folder. Windows 8 continues the integral use of the Libraries feature.

Aside from any other benefits, by setting up your Libraries so that they include all of your important personal folders, across all of your storage locations, you will ensure the successful use of automated backup. The File History functionality for example only allows backing up of personal files if stored in a Library. You can create new Library folders at any time if some of your personal files or folders aren't in an existing Library, or don't fit under an existing category. For example, create a Miscellaneous Library and then add folders for data you don't want to store in the other Libraries. Note that you should not include folders in a Library if they are on the destination drive selected for your backup, as they will usually be excluded by the Windows backup utilities. This is because it is always bad practice to backup any file to the same location as its source, since the loss of that drive will also mean the loss of any backups at the same time.

The Libraries feature is covered in detail in the Libraries section of the File Explorer chapter. Some additional considerations when organizing data in Libraries is covered below:

Emails: Depending on which email client you are using, your saved emails may be stored on your local drive in a directory which does not necessarily sit under a Library. If you are using a Microsoft Account to sign into Windows 8 along with the built-in Metro Mail app, your emails will be saved in the cloud depending upon your synchronization settings - see the Local Account vs. Microsoft Account section of the User Accounts chapter for details. If you are using a web-based email service which you view in your browser, the emails will all be stored on the mail server for the mail service, not on your drive. However, if you are using an installed local mail program, such Outlook or Windows Live Mail, then some of your emails may be stored on your drive. In Windows Live Mail, emails are stored as .EML files under the *\Users\[Username]\AppData\Local\Microsoft\Windows Live Mail* directory on your system drive. You can either add this location to a Library, or preferably, use the email client's backup features to regularly create an archive copy of your stored emails, and place this archive within a Library. See the Windows Live Mail chapter for details.

Bookmarks: Some of your important data may not be in a readily accessible form, or might be contained in a folder which also has a large number of unnecessary files you don't wish to backup. I'm referring here to things like your bookmarks for third party web browsers such as Chrome or Firefox. You can manually find and add the browser's bookmarks folder to your Libraries, but a cleaner option is to use the browser's bookmark backup feature to regularly save a snapshot of your bookmarks to a Library location. If you use Internet Explorer, simply backup the Favorites folder under your user account directory.

Programs: Don't attempt to backup an entire program directory, or all the component files of an installed program, as you cannot restore most programs or games in this manner; they will not run properly if they are copied back onto another installation of Windows 8 due to the lack of appropriate Windows Registry entries and related files spread throughout various other directories. You must use the original installation

disc/file to reinstall a program correctly. Windows 8 also purposely skips adding program-related files and folders as part of its backup functionality for this reason. For saving particular program files or folders, such as configuration files or saved games, it is strongly recommended that you locate the particular files you wish to save, create an archived copy of these files, and then store them in a Library. Bear in mind that if you are having problems with a particular program or game, or change your hardware prior to restoring the backup, it is not recommended that you use any previously saved configuration/settings files; only backed-up saved games are fine to restore in such circumstances.

Usernames/Passwords: You can store all of your usernames and passwords securely in electronic form as covered in the Backing Up & Restoring System Passwords section later in this chapter. If you have no faith in electronic storage systems, then you compile a written list or printout of the major usernames and passwords on your system. However you must then store this list safely in a physically secure place like a safe, and keep in mind that any time you write down or store your passwords in unencrypted format in any location you are facing a security risk if it falls into the wrong hands, particularly if you share your PC with other users.

In any case organizing your data correctly in Windows 8 has a range of benefits, particularly if you become accustomed to using the Libraries. While it may be unfamiliar or counter-intuitive at first, the long term advantages are numerous and worthwhile, and not just for backup purposes, as we will see later on.

< SYSTEM PROTECTION

Windows 8's System Protection features, enabled by default on your system drive, are a set of basic safeguards put in place to ensure that changes to important system files and settings can be reversed quickly and easily. System Protection does not work to automatically backup and protect your personal files; that is what the File History feature is designed to do. Instead, it allows you to undo undesirable changes to system files without affecting your personal files.

To access the main configuration options for System Protection, open the System component of the Windows Control Panel and click the 'System Protection' link in on the left side, or open the Recovery component of the Windows Control Panel and click 'Configure System Restore', or type *systempropertiesprotection* on the Start Screen and press Enter. Under the main System Protection window you will see the individual drives on your system for which system protection can be enabled. By default your main system drive will have system protection shown as being On; any additional drives will not have it enabled by default. Also note that system protection can only be enabled on NTFS drives.

To alter system protection on any drive, first select the drive from the list shown, then click the Configure button. In the window which opens, you can select the following:

§ Turn on system protection - Selecting this option enables System Restore on the drive.
§ Turn off system protection - Disables the System Restore feature on the selected drive, and deletes all restore points.

You can determine how much of the drive may be used for this feature using the slider at the bottom, and also delete all existing restore points at any time. These functions are explained in more detail further below.

Note that the Previous Versions function found in Windows Vista and 7 has been removed from Windows 8 System Protection, so it now only controls the System Restore feature. To understand how best to make use of this feature on your system, read the following.

SYSTEM RESTORE

System Restore is not a general backup and restore utility, and should not be mistaken as one - it is a system state backup and recovery tool. System Restore does not back up or maintain any copies of your personal files, such as your pictures, documents or music; instead it creates periodic Restore Points which are a snapshot of the key Windows system-related files, as well as the Windows Registry.

Creating Restore Points: Typically a restore point is automatically created before any significant changes to the system, such as when installing a program, a driver, or a Windows update. Windows also automatically creates a restore point once every seven days, if no other restore points were created within that period. You can also manually create a new restore point at any time by going to the main System Protection window and clicking the Create button. In the box which appears, enter a descriptive name for the restore point - note that Windows automatically appends the time and date to each restore point so you don't need to enter these - and then click Create again. A new restore point will be created for all the drive(s) on which you have enabled system protection.

Restoring a Restore Point: At any time if you wish to use an existing restore point to return your system state to the way it was when that point was created, follow these steps:

1. Open System Restore. This can done in a range of ways, including: typing *rstrui* on the Start Screen and pressing Enter; selecting Recovery in the Windows Control Panel, then clicking the 'Open System Restore' link; and under the System component of the Windows Control clicking the 'System Protection' link on the left side and then clicking the 'System Restore' button.
2. Click the Next button in the System Restore box which appears, and you will be able view all of the available restore points, sorted by the date they were created. Restore points are labeled clearly under both the description and type columns, making it easier to differentiate when and how each restore point was made.
3. If any system image backups made using the Windows 7 File Recovery feature covered earlier in this chapter are available, then you can tick the 'Show more restore points' box, and each system image will provide at least one additional point which can be restored. Note that even though a system image contains both system and personal files, using a system image as a restore point source will not restore personal files, only system files.
4. To restore a specific restore point, highlight that restore point. It is recommended that you then click the 'Scan for affected programs' link, and Windows will provide a list of programs, drivers or updates which will either be deleted or restored (in part or in full) as a result of the changes brought about by restoring that particular point. Click Next if you still wish to continue. On the next screen you will be able to review your choices before proceeding with the actual restoration.
5. To complete the process, click the Finish button. Your system will need to restart so that your system files can be reverted to the way they were at the time of the restore point. You will be notified if the restore was successful.
6. If you find that using the restore point was no help at all, or made things even worse, you can undo the use of that restore point by opening System Restore again, clicking 'Undo System Restore' and then clicking Next. Note that the ability to undo a restore is not available if you use System Restore in Safe Mode.

Disabling Restore Points: If you wish to completely disable System Restore on a particular drive, go to the main System Protection properties window and highlight a drive of your choice. Click the Configure button and to turn off the System Restore functionality select the 'Turn off system protection' option. This prevents any new restore points from being created, and also removes all existing restore points.

Disabling System Restore is not recommended, as it can be invaluable in recovering from unforeseeable problems which can afflict even the most advanced user. For example, if you install a driver which is unstable, and in turn prevents you from booting into Windows, this can be difficult and time consuming to

resolve manually. With System Restore enabled, you can simply boot into Safe Mode, open System Restore, select the restore point Windows automatically made just prior to the installation of the driver, reboot, and the harmful changes are instantly undone.

System Restore has no performance penalty; the only possible disadvantage to leaving it enabled is the amount of drive space it can take up. You can manually adjust how much space to allocate to the feature as covered further below.

Resizing or Deleting Restore Points: By default System Restore is allowed to use up to 5% of your drive space when needed. It requires at least 300MB of free space on each drive to work properly, and only works on drives larger than 1GB. I recommend allocating at least 2GB to the feature. Over time System Restore will automatically delete older restore points so as not to exceed its allocated size limit. You can determine the maximum amount of space allocated to retaining restore points by using the Max Usage slider at the bottom of the System Protection configuration window for each drive. The current maximum amount of drive space available for the feature is shown just beneath the slider, and the amount of space consumed by existing system restore points is shown at Current Usage above the slider.

If you want to save disk space, you can manually delete all older restore points - except the very latest one - at any time by using the Disk Clean-up utility. See the Disk Clean-up section of the Cleaning Windows chapter. This is the recommended method for periodically cleaning out older restore points, as it retains the latest restore point should you need to use it. However, if you want to delete all restore points, including the latest one, click the Delete button in the System Protection configuration window for a particular drive. While this will remove all restore points, it doesn't prevent Windows from creating new ones again in the future. To do that, you will need to select 'Disable system protection'.

Regardless of whether you enable or disable System Protection, keep in mind that it only protects system files, not personal files, and is not a replacement for backing up your personal data. System Protection is only one component of an appropriate backup strategy.

< BACKING UP & RESTORING PASSWORDS

Backing up and restoring login passwords is a unique case worth considering on its own. This is because Windows does not automatically backup usernames and passwords as part of any of its built-in backup features, nor is it generally recommended that you simply write down a list of your usernames and passwords and keep them handy, as this is a big security risk. This section provides several alternatives which allow you to make sure that your important passwords are readily accessible if you forget them, but still quite secure.

The first and most important password to consider is the login password you use for the main Administrator user account in Windows. This is typically the first user account you create during Windows installation. If this user account is password protected - and note that this is not necessary in certain scenarios as covered in the User Accounts chapter - then forgetting the password can cause major problems. With the NTFS file system it is quite difficult to access the data on your drive without the correct login password. The best thing to do is to safely backup your user account password now before anything happens, so that if necessary you can restore it without any difficulties.

In Windows 8 there are two types of accounts possible: a Microsoft Account and a Local Account. These are covered in more detail under the Local Account vs. Microsoft Account section of the User Accounts chapter. Depending on which account type you are using, there are different recommended methods of safely storing and recovering/changing your password:

SETTING UP & RESTORING A MICROSOFT ACCOUNT PASSWORD

A Microsoft Account maintains your login credentials online in the cloud (i.e. on the Internet), and hence gives you the potential to restore your password from any PC or device. When using a Microsoft Account email address, you can enter a valid Phone number, alternate email address and also establish a Secret Question, any of which enable you to reset the password to your Microsoft Account from anywhere, as long as you have Internet access. However this also allows other people to use the same methods to remotely reset your password if, for example, they know the answer to your secret question, or steal the phone with the number nominated in your account, or hijack your alternate email account.

To access and setup or alter all of the security features of your Microsoft Account, go to the Settings charm on any screen and select 'Change PC Settings', then selecting Users. To alter the email account-related security settings of your Microsoft Account, click the 'More account settings online' link.

It is strongly recommended that you ensure that your Microsoft Account recovery methods are in line with the advice provided under the Important Security Tips section of the Security chapter. This advice will help you to choose a genuinely secure password, and use the password recovery features of the email address nominated for your Microsoft Account in the safest possible manner, along with other safety tips to keep your account out of malicious hands.

In addition to the security features of your Microsoft Account's email address, there are two new user account password features in Windows 8 which can help secure your login and make it easier to remember login details: Picture Password and a PIN. These are covered under the Managing User Accounts section of the User Accounts chapter.

BACKING UP & RESTORING A LOCAL ACCOUNT PASSWORD

A Local Account maintains your login credentials only on the PC on which it was created. If your Local Account is password protected, the password is not stored anywhere online, and hence you cannot request that anyone else reset it for you, nor reset it from another PC or device. This provides greater security, as it is harder for a hacker to gain access to your account unless they have physical access to the PC on which it is used. At the same time, it leaves you open to complete loss of your account, and hence all of your personal files and settings, if you lose the password. The only real protection you have against forgetting your password is the password hint that you can add while setting up a Local Account. This hint may help you remember the correct password, but it is also a security risk, because it can also help someone else to guess your password. Furthermore, if you are using a complex password (which is recommended) then a vague hint is less likely to help you remember it.

It is strongly recommended that you ensure that your Local Account password is in line with the advice provided under the Important Security Tips section of the Security chapter. This will make it both more complex and easier to remember.

As an added safety measure, you should also create a password backup disk which is a foolproof method of storing your login credentials and recovering your account in case you forget the password. First make sure you are logged into your Local Account on your Windows 8 PC, then follow these steps:

1. Connect a USB flash drive. I strongly encourage you to purchase a new small USB flash drive just for this purpose, as after the procedure is complete it will need to be stored somewhere secure, and not left lying around for common usage.
2. Open the Windows Control Panel, select User Accounts and click the 'Create a password reset disk' link on the left side of the window; or type *forgotten* on the Start Screen, select Settings and launch 'Create a password reset disk'.
3. The Forgotten Password Wizard will open up, click Next.

4. Select the appropriate drive when prompted. Note that if you need to format the USB drive first, open File Explorer, right-click on the drive under the Computer category and select Format.
5. You will be prompted to enter the current user account password. Do so and click Next.
6. Once the password reset disk has been created, select Finish.
7. You must now store this USB drive somewhere secure, such as a locked drawer, as anyone can now use it to access your account.

If you ever need to restore your password from the backup created above, follow these steps:

1. Boot up your PC as normal, and on the Login screen, select your account if necessary.
2. Try entering your password (or just press Enter), and you will get a message saying the Username or Password is incorrect. Select the 'Reset Password' link.
3. Insert the password reset USB flash drive you created earlier.
4. Follow the Password Reset Wizard to set a new password and log back into your system.
5. Windows will update the USB drive with the new password automatically during this procedure.
6. When done, you should once again put the USB drive away in a physically secure place.

The main Administrator account on a PC can also log in at any time and change the password for other Local Accounts, in case they are forgotten. However doing so will prevent those users from accessing any existing encrypted files or folders for that account, so the best method to prevent password loss and hence potential data loss is to use the password reset disk method above.

Gaining Access Without a User Account Password

If you've completely forgotten your login password, you don't have a password reset disk, you don't have access to any of your account recovery features, and you don't have any other Administrator who can reset it for you then generally you're in a lot of trouble.

For a Microsoft Account, you can attempt to go through alternate channels for recovering your account access. This will involve contacting Microsoft and providing various forms of proof of ownership, though in practice it can be a difficult procedure to successfully complete.

For a Local Account, if you are really desperate to regain access to your data and you have the time, you can try the Offline NT Password & Registry Editor for cracking a Local Account password. There are also other utilities you can use to recover or crack passwords, such as Ophcrack. I cannot go into detail regarding these tools, as it is beyond the scope of this book. In fact the main aim of listing two of these utilities is just to demonstrate the existence of cracking tools and methods for obtaining account passwords in Windows. The presence of these types of tools should let you see that nothing is completely safe on your machine, so it is very important to always restrict physical access to your PC only to those people you trust, and always follow the tips provided in the Security chapter.

Storing General Passwords

Remembering username and passwords for various websites and software soon becomes difficult, especially if you have chosen varied and complex passwords. Most users wind up frequently using the same one or two simple passwords, such as a common word or name along with a number or two at the end of it. This is not optimal for security purposes, and while most people are now aware that it is best to have complex passwords consisting of a combination of random letters (both uppercase and lowercase), symbols and numbers, virtually no-one can memorize these types of passwords.

Advice is provided in the Important Security Tips section of the Security chapter to make it easier to create a complex password that is also memorable. Web browsers also make the process easier by allowing storage of usernames and passwords for automatic entry into relevant prompts on websites. However neither of

these methods completely addresses the problem of potentially losing your passwords. For example, if you experience drive corruption, you will lose all of the usernames and passwords stored in your browser. For this reason, it is sensible to store your usernames and passwords in a central location, and then back them up as part of your regular backup procedures. There are two main tools which allow you to do this.

Credential Manager

Credential Manager was introduced in Windows 7, based on a very similar feature found in Windows XP and Vista. It has been improved in Windows 8 to be a genuinely viable alternative in storing login/password combinations for not only Windows logins, but also for normal websites. Credential Manager is accessed via the Windows Control Panel, or by typing *credential manager* on the Start Screen, selecting Settings and pressing Enter.

The main purpose for Credential Manager is its Credential Locker feature, which securely stores login credentials for accessing websites, other computers on a network, or remote servers, in a single location. Windows stores these credentials in special secure folders on your PC, and can access them to automatically sign you into websites or other PCs as necessary. They are also available to be synched as part of your Microsoft Account, so that if you are logged in with that account on any Windows 8 PC or device, your login details will automatically be entered for you.

When you first open up Credential Manager, you will see two separate sections: Web Credentials and Windows Credentials:

§ Web Credentials - This section holds all of the website login usernames and passwords which have been saved by supported applications. For example, when entering a username and password combination in Internet Explorer while logging into a website, you will be prompted at the bottom of the IE screen with 'Do you want Internet Explorer to remember the password for *websitename*?' If you select Yes, then it will be saved in Credential Manager, allowing you to select your saved login details the next time you visit that site. Your saved website names and usernames are listed in Credential Manager, but your password is obscured by default. You can click the Show link next to the relevant website username if you wish to see its password in plain text. Click the Remove link to remove any website credentials you no longer wish to keep.
§ Windows Credentials - Windows credentials are primarily for signing into other computers and Windows-based resources; Certificate-Based credentials are for resources which require a valid certificate; and Generic credentials are for standard web-based services, including your Microsoft Account for logging into Windows 8. The resource or program requesting the username and password must be designed to interact with Credential Manager (or the previous versions of the same feature) in Windows, otherwise your entered data will not have any impact.

The Windows Credentials are stored as part of the Windows Vault, which is an encrypted file you can backup to any location and then use on other machines as required. If any data has been entered in the Windows Credentials section of Credential Manager, you will see the 'Back up Credentials' link at the top which allows you to do precisely this, and the 'Restore Credentials' link can similarly be used to restore a previously backed up vault. The backup .CRD file which is created must be password protected, and is best stored on a USB flash drive which is then kept in a secure location such as a locked drawer or safe. Note that this backup does not retain your Web Credentials.

The main benefit of Credential Manager is that it is built into Windows and works well with Internet Explorer. It is not suited to users who want a more versatile password storage option.

KeePass Password Safe

If you want a place to store all of your usernames and passwords in a relatively straightforward manner, protected by high level encryption, with the ability to securely export and store the database for backup purposes, use the free KeePass Password Safe utility. There is both a Classic Edition and a newer version available to download, both of which are free. The differences in features are spelled out in this table. I describe usage of the latest version below.

To use KeePass, install and launch the utility, and select New under the File menu. Select a location on your drive for storing the database, then enter a Master Password and/or select a Key File. These measures are used to store and secure the password database. The key file is not essential, but make sure to enter a complex master password which has a high bit-rate. This master password is a critical component - if you forget it, there is no way to unlock your password database.

Once the database is created, you can populate it. The database is sorted by groups, which are simply categories of passwords. You can right-click in the left pane and add new groups, or add sub-groups under the existing groups, or remove any group or sub-group as you wish. Highlight the group which you believe your username/password combination is best stored under, and in the right pane right-click and select 'Add Entry' to create a new entry containing your username and password combination for a particular Windows feature, general software, or a website. Do this as many times as required to populate the database with all the username and password combinations you wish to store.

You can backup this password database to any location you wish by using the Export feature under the File menu. I strongly recommend exporting the database as a KeePass Database (.KDBX) file. This database can then be backed up to wherever you wish, and its contents can only be successfully viewed by using KeePass to open the file, and entering the correct master password. Because the database is encrypted, it is virtually impossible to access the database contents without the right master password/key file.

The main drawback of a general utility like KeePass is that unlike the username/password storage features of a web browser, or those of the Windows Credential Manager, it can't automatically populate your username and password fields when you visit a particular website or use a particular program. However it is a highly configurable method for holding all of your passwords, and allows you to securely backup the database to any location.

< OTHER BACKUP METHODS

In general the built-in backup methods in Windows 8, along with the utilities covered thus far, are more than sufficient for you to come up with a reasonable strategy for protecting your data from loss. However there are several other ways you can create and maintain backups, whether because the Windows functionality is not sufficient for your needs, or simply because you want other alternatives to supplement the Windows features. This section provides such alternatives.

THIRD PARTY DRIVE IMAGING SOFTWARE

There are third party programs available which can provide features similar to the system image functionality in the Windows 7 File Recovery component of Windows 8. Two such software packages for imaging drives are the free Clonezilla utility, and Acronis TrueImage, which is not free. Neither can be covered here in any detail. The main benefit of third party imaging utilities over Windows 8's built-in system image option is that they allow a wider choice of options, but in practice they are not essential, as the Windows system image feature should meet the majority of your needs.

ONLINE BACKUP

Online backup services allow you to store copies of your data in a secure off-site location, typically a remote data center. This is often referred to as storing data in "the cloud", and ensures that your data is encrypted and stored safely. This form of backup is not absolutely necessary for the average user, but it provides additional security and peace of mind, particularly in the event of fire or theft, whereby your PC and your onsite backups may all be destroyed or stolen, leaving you with nothing to rely on for restoring your data. For the average user there are several ways of using free online services to provide added security against such data loss:

SkyDrive: Access to Microsoft's free SkyDrive service is built into Windows 8, and is available by launching the SkyDrive app on the Start Screen. The app allows you sign in with a Microsoft Account and upload files from your PC for storage in the cloud. These can then be accessed from any location by logging into your Microsoft Account on another Windows 8 PC or device, or on any system by signing in via a web browser on this site. Furthermore, you can install a separate SkyDrive Utility on your Desktop, which adds a new SkyDrive location under the Favorites category of the Navigation Pane in File Explorer. You can then drag and drop files to this location within File Explorer, and you will once again be able to access them on other systems using the same Microsoft Account details.

Dropbox: Similar to SkyDrive, Dropbox is a service that allows users to store and share their data online. There is a free version of the service, however there are restrictions, including the possibility of losing all stored data if it is unused for 90 days.

ISP Storage: Many Internet Service Providers (ISPs) provide their customers with a basic web space to which you can upload personal data. This is a relatively secure and typically free method of storing your data offsite. Check your ISP's website or contact them directly for further details. Even if a small fee is involved in obtaining such a facility, it can be worthwhile given the added protection it provides you as a remote location to store your backups.

Email Storage: Free email services such as Gmail provide extremely large amounts of storage space, in the order of several Gigabytes. While I do not recommend uploading/emailing any sensitive data to these locations, as they are not completely secure, they do serve as good holding spots for additional backups of digital photos and other important irreplaceable files. You can use a free utility such as Gmail Drive to make storage of data on a Gmail account much easier to manage.

Photo Storage: There are a range of free photo album providers that allow you to upload and keep a large library of digital photos. This can be useful in both providing a location to store irreplaceable photos in case the originals are ever lost, and also providing easy access to viewing the photos from any location or device. The most popular free photo gallery providers are Flickr, Photobucket and Picasa. Make sure to read the instructions for the gallery and enable all of the privacy features so that members of the public cannot view your gallery contents without your explicit permission. Regardless of such features, a direct link to a particular photo can often be publicly discovered, so do not upload sensitive photos to such galleries.

While the free storage options available above are useful, ultimately, if you believe your data is worth preserving against all eventualities, or you need to store it with maximum security, it is necessary to consider a professional remote data storage service. The free options do not provide sufficient security against unauthorized access or loss of data. Also keep in mind that although storing data in the cloud is becoming more common, you will still need local backups regardless. No online data storage service is infallible or unhackable, and some also have restrictive terms of service, or may even be discontinued or go out of business at any time, so they should not be relied upon as the sole form of backup for any data.

CUSTOM BACKUPS

While I recommend that you take advantage of the built-in Windows backup functionality, I also recommend that you create additional custom backups of only your personal files. By custom backup, I am referring to manual backups taken of specific data and stored separately.

There are several reasons for doing this, foremost among them being that it is always best to have several backups of the same irreplaceable data in several forms/locations. That way if your preferred up-to-date backups are lost, you at least have some other backup of your personal data that you can use, even if it might be a bit older. Secondly, reliance on any automated backup utilities means that you may backup problematic or sub-optimal settings or conditions over time. It is common for files and settings to become infected, corrupted or contain incorrect information (e.g. after a change of installed hardware). These problems may not be easily detectable or reversible, and will work their way into your backups, making them much less useful when the time comes to use them. Finally, having custom backups of only your key personal files in a portable and non-proprietary format means you can access them from any PC or device, including those running older versions of Windows.

So in addition to taking regular system image and File History-based backups, I recommend that you create a custom "clean" backup copy of all of your important files which is highly portable and stored separately to your PC. A suggested way of doing this is as follows:

1. Manually scan your entire system thoroughly for malware using the procedures covered in the Security chapter.
2. Find a good quality USB flash drive, external USB drive, or rewriteable CD, DVD or Blu-Ray discs. For the USB flash drive, make sure to format it first in FAT32 format by connecting it your PC, and under File Explorer right-click on the drive, select Format, then select FAT32 under the File System box and click Start. FAT32 is the most widely compatible file system, which is why it is recommended for a USB flash drive.
3. Open File Explorer and manually copy across every single file that you consider irreplaceable and you wish to backup. Since you are only copying across the most important personal data, there shouldn't be a large volume of data. In most cases it should all fit on an 8 or 16GB USB flash drive, a box of DVDs, or a single Blu-Ray disc.
4. Once completed, store this backup in a secure location, such as a lockable drawer or safe.

While the above procedure may seem excessive, it really does provide additional safeguards against losing your valuable data, and importantly, allows you to do a clean reformat and reinstall of any version of Windows, and simply copy your important files back across for instant use, secure in the knowledge that no problematic or infected files or settings of any kind are being restored as well. It also provides the portability necessary to make secure storage of your most important files easier, or if you wish to quickly view or restore them on another machine at any time.

In general, the File History and system image backup features in Windows 8 are an excellent method of generating and maintaining up-to-date backups of your system, and I strongly encourage you to use them. Remember that the System Protection features also provide an important level of protection against accidental deletion or modification of system files, which even advanced users should use to their advantage. In combination with custom backups, appropriate data storage practices and some common sense, you will be protected against losing your important data in virtually any scenario. It may seem extremely tedious at first, but once you get into the habit of backing up the right way, the peace of mind it offers far outweighs the inconvenience.

< DATA RECOVERY

Accidental deletion of files is one of the most common ways in which files are lost. By default Windows 8 provides protection against this with its built-in File History and System Protection features as covered earlier in the previous sections of this chapter. As an additional safeguard, you should leave the Recycle Bin enabled, and configure it appropriately to make sure that deleted files are first moved to the Recycle Bin. See the Recycle Bin section of the Cleaning Windows chapter for details.

In the end, for one reason or another, you may still wind up permanently deleting a necessary file, and have no available backups or restore points available. Fortunately, when you delete a file from your system the file is removed from view and you regain the space on your drive, but it is not actually permanently deleted from your drive. In fact, nothing on your drive is permanently removed when you delete it. Whenever you delete a file Windows simply marks it for deletion. The entire file is still sitting on your drive, but is not visible. Windows then allows other files to write over the space where it resides if required, but the file is not completely gone from your drive until it is fully overwritten at some point. This means that you can sometimes recover files that have been "permanently" deleted, but you need to act quickly, and will require third party software to do so.

RECOVERING DELETED FILES

There are several tools that you can use to potentially recover your deleted files. In each case, it is strongly recommended that you install the recovery software on a different drive to the one which contains the deleted file(s) you wish to search for. This is needed to minimize activity on the drive on which the deleted file resides. The longer you wait, and the more drive activity there is, the greater the chance that a Windows background task such as a scheduled defragmentation, or the creation of a temporary file, may overwrite the deleted file.

Recuva: To use the free Recuva utility, after installing it you can simply follow the wizard which appears. For more options, you can Cancel out of the wizard at any time. Essentially, you first specify the particular drive to scan, or all available drives if you so wish, and then specify the file type you're looking for - whether by using the drop-down list, or entering a portion of the filename (or leave the box blank for all files) - and then click the Scan button. One of the benefits of Recuva is that it provides a preview of the recovered files wherever possible, making it easier to determine which may be the suitable one to restore. Another benefit is that Recuva can find and restore deleted emails. If nothing suitable is found after a basic scan, you can opt for an in-depth scan if prompted, or click the Options button and under the Actions tab tick the 'Deep Scan' box and scan again. This will find many more hidden deleted files, but may also take quite a while.

Pandora Recovery: To use the free Pandora Recovery software, download and install it, then launch it as normal. A wizard will present itself which you can work through, or you can simply exit the wizard to access the full interface at any time. On the main screen click the Search tab, then select the drive, enter any portions of the filename, or simply leave the box empty to find all deleted files, then click the Search button. A list of found deleted files will be shown, each one color-coded to indicate its status - black for normal files which can generally be recovered, green for encrypted files which can be recovered but remain encrypted, blue for compressed files, and red for overwritten deleted files which cannot be successfully recovered. Double-click on the relevant file or right-click on it to see more details and access the recovery options.

Restoration: To use the free Restoration utility, first download the file and run it to extract the contents to an empty directory, preferably on a USB flash drive or another drive. Then right-click on the *Restoration.exe* file and select 'Run as Administrator' to launch the utility. Select the relevant drive, then enter a filename in the search box, or a file extension (e.g. JPG, DOC, TXT), or leave the box blank to find all recoverable deleted files, and click the 'Search Deleted Files' button. Restoration will scan your drive for files which can be restored and list them. You can highlight a file and click 'Restore by Copying' to recover it.

IsoBuster: Aside from hard drives and SSDs, if you also want to attempt to recover deleted or damaged files from a CD, DVD, BD, USB, SD, MMC or assorted other portable drives and disk formats, you will have to use a more specialized utility such as IsoBuster. While it can be tried for free, IsoBuster requires paid registration for full functionality. During installation you can untick the Smart Advisor function, and then select the 'Free Func. Only' button to use the free version. You can use the free version to first check to see if there is any recoverable data on your particular drive or disk. You must then pay to purchase IsoBuster if you want to attempt recovery.

Regardless of which utility you use, bear in mind that there is no guarantee that any usable data can be recovered from a disk.

PERMANENTLY DELETING FILES

As you may have noticed, it is entirely possible to recover some or all of a file after it has been deleted in Windows. If you ever want to truly permanently delete a file so that others can't recover it in any practical way, you can use the Recuva, Restoration or CCleaner programs to do this. See the CCleaner section of the Cleaning Windows chapter for details of how to obtain and set up CCleaner.

To securely permanently delete a file, first delete the file as normal in Windows. That is, highlight it in File Explorer, press Delete, then empty the Recycle Bin. The follow these instructions:

If using Recuva, do a scan for that filename (or all files) as normal, and it should show up in the list of recoverable files. Right-click on the file and select 'Secure Overwrite Highlighted'. This will overwrite all areas of that file with data such that it can't be recovered. If you want to adjust how secure the overwriting is, click the Options button and under the General tab, select the desired level of overwriting for the 'Secure overwriting' option; the more passes, the more secure it will be. A Simple Overwrite (1 Pass) is sufficiently secure.

If using Restoration, enter the name of the file (or leave blank for all files) and click 'Search Deleted Files'. When Restoration finds the file and lists it, highlight the file and go to the Others file menu and select 'Delete Completely'.

If using CCleaner, select Tools then click the 'Drive Wiper' button. Make sure the Wipe box is set to 'Free Space Only', and select the level of security you wish. A Simple Overwrite (1 Pass) is more than sufficient, but you can select more passes if you wish, though it will take longer. Finally, tick the relevant drive(s) and then click the Wipe button. This will overwrite all space marked as free on your drive, which includes any deleted files, with blank data, such that any original data in the same location becomes unrecoverable.

If you wish to securely wipe the contents of an entire hard drive, for the purposes of ensuring the removal of malware before reformatting and reinstalling Windows, or if you want to sell the drive or dispose of it, you can use the new Windows Reset feature of Windows 8 - see Windows Reset later in this chapter for details. Alternatively, you can use the free DBAN utility.

Each of the methods above will permanently delete a file so that it is effectively unrecoverable by virtually any program or method. There always remains the possibility that some data may still be recoverable by law enforcement agencies using specialized methods, but in practice nothing short of physically destroying the drive can prevent that.

LOW LEVEL FORMAT & ZERO FILL

People might suggest that you Low Level Format your drive to permanently remove data or fix a drive problem. This is not recommended unless you are experiencing severe hard drive problems, and even then it is not possible on most modern hard drives due to the complexity involved. Modern hard drives are low-level formatted at the factory to create tracks and sectors and do not need to have it done again. The correct course of action is to Zero Fill your drive, which people often confuse for a low-level format. This method overwrites the entire hard drive with blank data, ensuring that everything is deleted permanently for most intents and purposes, but it is not as intensive or potentially disk-damaging as a low-level format. A zero fill is your best bet in getting back to a "good as new" hard drive.

Aside from using the secure erasure functions of the utilities covered further above, a quick and easy way to do a basic zero fill of a hard drive and error check it at the same time is to use the built-in formatting functionality of Windows itself. A full format (not a quick format) will achieve this. See the Preparing the Drive section of the Windows Installation chapter for more details.

If however you insist on low level formatting a hard drive and/or using a custom diagnostic program to error check it and ensure that it is wiped absolutely clean, then check your hard drive make and model and consult your drive manufacturer's website for an appropriate utility.

If you are using an SSD, you will need to use a custom utility to secure erase a drive. See the Solid State Drives section of the Drive Optimization chapter for more details.

< SYSTEM RECOVERY

Windows 8 comes with a range of tools for repair and recovery, as covered in this Microsoft Article. This section covers the methods and important Windows tools which can assist you in attempting to restore your system to a usable state after experiencing major problems.

There are three main scenarios which determine the basic procedures you should follow:

1. Can't switch on PC, or the problem occurs immediately after the PC is switched on: If your problem is with a PC that won't turn on properly, or which crashes, shows screen corruption, or makes odd noises immediately after you switch the PC on, then it is almost certain that the issue is due to an incorrect BIOS/UEFI setting, unstable power supply, overclocking, overheating, or physically faulty hardware. It is not related to your Windows settings, or your installed programs, drivers, or any other software-based settings. This is particularly true if you can't even enter Safe Mode. See the Advanced Boot Options section below for details on Safe Mode; see the Hardware Management chapter for details of hardware-related factors to check for; and see the Performance Measurement & Troubleshooting chapter for tools to test specific hardware components for faults.

2. Can't boot into Windows: If your system appears to start correctly and runs without problems or visible screen corruption up to Windows startup, but you then can't boot successfully into Windows, you will have to use the Advanced Boot Options at Windows startup to attempt to fix the issue, such as running System Restore in Safe Mode, or running the automated Startup Repair function. See the Advanced Boot Options section further below.

3. Can boot into Windows: If you can boot into Windows but experience problems once in the Windows environment, the very first thing to do is to run System Restore and revert to the most recent restore point available. See the System Protection section earlier in this chapter for details. This is the simplest method for undoing harmful changes to system files without affecting your personal files. If you don't have any system image backups or restore points to use, try uninstalling any recently installed software or drivers in the Programs and Features component of the Windows Control Panel. Also refer to the Manually Updating or

Uninstalling Drivers section of the Windows Drivers chapter for ways of cleaning out badly installed drivers which do not uninstall correctly.

If these methods don't work, then you will have to use the tools and methods in the rest of this section to assist with system recovery.

System File Checker

The System File Checker is a built-in function of Windows that allows the system to go through and check all protected Windows system files to ensure that they have not been corrupted or altered in any way. This is extremely handy if you want to rule out corrupted or tampered core system files as a cause of unusual Windows behavior. To use the System File Checker follow this procedure:

1. Open an Administrator Command Prompt.
2. To scan for and automatically fix any errors type `sfc /scannow` then press Enter to start an immediate scan of your system files. Alternatively, if you just want to scan for errors/mismatches but not have Windows fix them (e.g. if you have deliberately altered certain system files), then type `sfc /verifyonly` and press Enter.
3. The System File Checker will check all of your important system files and make sure that they have not been altered in any way. If the `/scannow` option is used, where major system files are corrupted or shown to be different from the original, they will be replaced with cached originals, or from your Windows 8 installation media.
4. Reboot your PC if required, as this may be necessary to complete any repairs.

If your system is fine, you should see the message 'Windows Resource Protection did not find any integrity violations'. If you find that certain files could not be repaired, or if you used the `/verifyonly` option, you can view the details of which system files Windows has flagged as problematic by doing the following:

1. Open an Administrator Command Prompt.
2. The original SFC log data is held within the *CBS.log* file found under your *\Windows\Logs\CBS* directory, however it can't be opened directly. To filter the relevant contents and view them, you need to type the following at the Administrator Command Prompt:

   ```
   findstr /c:"[SR]" %windir%\logs\cbs\cbs.log >%userprofile%\Desktop\sfcdetails.txt
   ```

   Note that the `/c:` above needs to be changed to the drive on which you ran SFC.
3. The resulting *sfcdetails.txt* file will appear on your Windows Desktop, and can be opened with a text editor like Notepad to reveal the process SFC ran through, and any errors found or repairs needed.

You can also use System File Checker to check the integrity of individual system files if you don't wish to run a full scan. To do so, do the following:

1. Open an Administrator Command Prompt.
2. Type the following and press Enter:

   ```
   sfc /verifyfile=[filename]
   ```

   Where the *[filename]* must include the full path to the file, as well as the filename itself - e.g.:

   ```
   sfc /verifyfile=C:\Windows\System32\imageres.dll
   ```

3. If the file is unchanged, you will be told that there are no integrity violations. Otherwise if the file has been changed in some way, you will need to refer to the *CBS.log* file as covered above.

Full usage options for the System File Checker can found in this Microsoft Article. The System File Checker does not repair general system issues such as Registry corruption for example. It simply ensures that important system files are unaltered, which removes one variable from the equation when troubleshooting a Windows problem.

WINDOWS REFRESH

Windows 8 incorporates two new recovery features designed to help you quickly and easily restore Windows to its original "factory" condition, each with certain limitations as described in this Microsoft Article.

The first such feature is Windows Refresh. If you've run into trouble on your system, and think that your Windows 8 installation is too messed up to take the time to find and fix the source(s) of various problems, or if you have a severe malware infection, or can't boot into Windows at all, then a Windows Refresh might be the best option. Using this feature will essentially reinstall Windows, but will keep most of your personal data.

The following will be retained:

§ All of your personal files stored under your user folders on the same drive.
§ Some of your Windows personalized settings. This includes your user account settings such as username, password, lock screen background and Desktop wallpaper, along with BitLocker settings and drive letter assignments.
§ All Metro apps from the Windows Store.

The following will be lost:

§ All Desktop-based installed applications. A list of removed software will be saved on your Desktop once the process is complete.
§ All of your general Windows settings will be reset to their defaults. This includes Windows Firewall settings, file type associations, and display settings.

To access this feature, open the Charms menu and select settings, click on 'Change PC Settings', and under the General category, click the 'Get Started' button under 'Refresh your PC without affecting your files'. If you can't boot into Windows, you can access Windows Refresh under the Windows Recovery Environment as covered further below.

Follow the prompts, and Windows will reboot into the Recovery Environment, scan your drive for relevant personal data and settings, and store them separately on the same drive. Windows 8 will then be freshly reinstalled, and your personal data and settings will be restored to this new installation, along with your Metro apps. You will then need to check through all of your settings and change some of those which have been reset to their defaults, and also reinstall all Desktop applications. This is the quickest way to refresh your installation of Windows and remove any problematic settings without doing a clean reformat and reinstall of Windows. If problems persist after a Windows Refresh, this tends to indicate that you have hardware-related issues.

Custom Refresh Image

The standard Windows Refresh method only retains personal data and some customizations, and essentially reinstalls Windows 8 afresh with default settings in most areas. However there is a way to create your own pre-defined snapshot of your Windows 8 installation, complete with all of your custom settings and Desktop applications, and then use Refresh to go back to that state, rather than the default Windows 8. This custom

recovery image method makes use of a command line tool called `Recimg`. You can create a recovery image on any drive/partition with sufficient space, including your current system drive.

To create a new custom recovery image of your current Windows 8 installation at any time, do the following:

1. Open an Administrator Command Prompt.
2. Type the following:

   ```
   recimg /createimage C:\
   ```

3. The command shown above will create a new file called *CustomRefresh.wim* in the base directory of C: drive. You can specify a different drive/partition or folder if you wish. For more details on the available options for the recimg command, type `recimg /?`.
4. The .WIM file created by recimg is a complete mirror image of your current system drive, including all installed applications, settings, files and other customizations. Depending on how large your Windows installation is, it may take quite some time to create, and take up a fair bit of space.
5. Importantly, unlike a regular system image, creating an image in this manner registers it in Windows as the recovery image to use when you next utilize the Windows Refresh feature. In other words, if you use Windows Refresh after the steps above, it will now restore your PC to the state it was in when you took the custom snapshot, not to the default Windows 8 image.

A custom image is best created immediately after you have done a fresh install of Windows 8, installed all of your applications, and customized/optimized all of your settings. If you are certain that your system is problem-free, by using recimg to create an image at this point, you can quickly use Windows Refresh to revert your Windows back to its optimal state at any time without subsequently having to go through the tedious task of reinstalling all of your applications and customizing/optimizing all of your settings, as you would with a normal Windows Refresh.

WINDOWS RESET

If you want to quickly and completely erase your current installation of Windows, along with all personal data on it, then a Windows Reset is the correct choice. A key feature of this option is that it allows you to reinstall Windows 8 in such a way that any personal data is unrecoverable. This is ideal if you want give or sell the PC to another user for example. Once the process is completed, the result is a fresh Windows 8 installation with default settings, and no remnants of any previous files, folders, programs or settings. This is the same as if you had reformatted the drive and reinstalled Windows 8 manually.

To access this feature, open the Charms menu, select Settings, click on 'Change PC Settings', and under the General category click the 'Get Started' button under 'Remove everything and reinstall Windows'. If you can't boot into Windows, you can access Windows Reset under the Windows Recovery Environment as covered further below.

Follow the prompts, and when given the choice, you can select to either do a quick or thorough removal of personal files. Choosing either option results in the same basic outcome, which is a fresh install of Windows 8. However with the thorough option, random patterns will be written to every sector of your drive, deleting your data in such a way that is virtually unrecoverable - though it will take quite a bit longer to do this. Selecting this option is only recommended if you are selling the PC or drive, or throwing it away, and you don't want your data falling into the wrong hands. Otherwise for your own personal use, or if giving it to a trusted person, then the normal quick reset method is sufficient.

To reiterate: the key difference between a Windows Reset and a Windows Refresh is that Windows Reset does not retain any of your settings, programs, files or anything else like Windows Refresh; it merely

simplifies the process of erasing the drive and reinstalling Windows 8 afresh, while also giving you the ability to securely erase your data from the drive at the same time.

Windows Recovery Environment

If you can't boot into the Windows Desktop to access recovery tools like System Restore, System File Checker, Windows Refresh or Windows Reset, then you will need to access the special Windows Recovery Environment (Windows RE). This feature of Windows provides a range of tools designed to simplify and automate the process of recovering from any major system issues preventing you from booting up successfully into Windows. If Windows detects that it is have a problem booting up normally, or the system keeps unexpectedly shutting down, it will automatically launch an Automatic Repair, or open the Windows RE menu.

If Windows RE doesn't launch automatically, or you just want to access it manually, there are several ways to do this:

- Go to the Charms menu, select Settings, click on 'Change PC Settings', then under General category click on the 'Restart Now' button in the Advanced Startup section.
- Go to the Charms menu, select Settings, click on the Power option, then hold down the SHIFT key and click on Restart.
- Launch a Command Prompt and type `Shutdown /r /o` and press Enter.
- Boot up your PC using your Windows 8 installation DVD or USB drive, or a System Repair Disc, then select your language and keyboard layout, click Next, and click the 'Repair your computer' link at the bottom.

Once on the main Advanced Startup screen, click the Troubleshoot option. Here you can select whether you want to use the Windows Refresh feature covered earlier by clicking the 'Refresh your PC' link, or the Windows Reset feature by clicking the 'Reset your PC' link.

For further recovery options, click 'Advanced Options'. The Advanced Options screen has multiple recovery and repairs features available, and these are each covered in separate sections below.

System Restore

Covered in detail under the System Restore section earlier in this chapter, selecting this option allows you to launch the System Restore utility within the Recovery Environment, which is useful if you can't access System Restore from the Windows Desktop. Select an available restore point to undo any recent harmful changes to system files or settings.

System Image Recovery

This utility has been covered in detail under the Windows 7 File Recovery section of this chapter. If your Windows is not recoverable, this option is a last resort, allowing you to restore your system to the way it was when you last took a full system image backup. By default you will be prompted to restore the latest available system image. Look at the date and time shown - if you don't believe it is the latest image you have made, attach any other device or disc which holds a more recent system image, choose the 'Select a System Image' option, then either select from the list of system images shown, or click the Advanced button to allow you install any necessary device drivers which will allow the re-imaging utility to properly detect any unlisted attached devices. Obviously if you haven't made any system image backups then this option is not useful, as it cannot operate on partial backups of files for example. Note that restoring a system image means that it overwrites all your existing data with that contained in the backed up image of your system at the time it was taken. This is why it is important to take a full system image and regularly backup to it using the Windows Backup tool, so that it doesn't get too far out of date.

Automatic Repair

Automatic Repair attempts to diagnose and automatically fix issues which are preventing error-free bootup into Windows. Automatic Repair is one of first options which should be tried in the event of system boot failure. Click this option and allow it to scan your system for any potential problems. If it can resolve the issue, such as a damaged or missing boot file, it will do so automatically, and will provide links at the end of the process which you can click to see precisely what issue has been found and resolved. However Automatic Repair is relatively basic, and cannot fix certain issues beyond simple boot-related misconfiguration or damage. More complex problems such as faulty or misconfigured hardware, malware infection, or the system drive not being correctly detected for example are beyond its capabilities.

Command Prompt

This option allows you to open a MS DOS Command Prompt window within the Recovery Environment. This is useful if you want to access specific DOS commands for advanced repair functionality, or attempt to browse for particular files or directories on a stricken drive and try to copy them to another drive. It is also useful for partitioning and formatting a drive in preparation for installation of Windows, to prevent automatic creation of the System Reserved Partition during Windows Setup - see the Installing Windows section of the Windows Installation chapter.

Although the Windows Recovery Environment replaces the Windows XP Recovery Console, almost all of the most useful Recovery Console commands from XP can still be used in Windows 8. There is a full list of legacy XP Recovery Console Commands at the bottom of this Microsoft Article, and when combined with a list of those which have changed or no longer work, you have a range of commands you can try for advanced recovery purposes. Note that you can enter any command with the `/?` parameter to see the help description (e.g. `BOOTREC /?`).

The following commands may be useful:

- Use the `CHKDSK /R` command to do a drive check and fix any errors if possible.
- Use the `BOOTREC` command to rebuild or repair the boot-related aspects of the drive (e.g. `BOOTREC /FIXBOOT` or `BOOTREC /FIXMBR`). More details on how to use `BOOTREC` are in this Microsoft Article.
- Use the `CD` *`[directory path]`* command to go to a specific directory, then use the `COPY` *`[filename] [destination drive]`* command to copy a file to another location.

The Command Prompt method generally requires greater expertise to use, so anything beyond the basic commands covered above will require specialist knowledge. In such instances, it is safer to simply use Windows Refresh otherwise you risk losing your personal data.

Startup Settings

Selecting this option will take you to a selection screen where a range of additional options are available. In previous versions of Windows this was known as the Advanced Boot Options screen. These options allow you to boot up Windows in special modes. To select an option on this screen, press a numerical or function key matching the number of the entry on the menu. Each option is covered in more detail further below.

1. Enable debugging
2. Enable boot logging
3. Enable low resolution video
4. Enable safe mode
5. Enable safe mode with networking
6. Enable safe mode with command prompt
7. Disable Driver Signature Enforcement
8. Disable early launch anti-malware protection
9. Disabling automatic restart after failure

Enable Debugging: This option enables kernel debugging mode in Windows. This is of little use to the average PC user, as it requires specialist knowledge to interpret the debugging data output.

Enable Boot Logging: This option logs all the drivers which are loaded at startup to a file called *ntbtlog.txt* in your *\Windows* directory. This information can be useful for more advanced users in determining which files are causing problems with the Windows startup procedure.

Enable low-resolution video: This option starts Windows normally, but using a low screen resolution of 800x600, and low refresh rate supported by all monitors. This mode is useful for example if you've selected display settings which are unsupported by your monitor, or you have installed a problematic display driver that does the same, and your screen goes blank. If this occurs in Windows, hold down your PC's power button for up to five seconds to force Windows to shut down, then reboot into the Windows Recovery Environment and select this option so you can boot back into Windows and uninstall the driver or change your display settings as appropriate.

Enable safe mode: Safe Mode is an important Windows mode which only loads up the bare essentials required for Windows to function. Third party drivers, graphical enhancements, startup programs, unnecessary processes etc. are all skipped and only the minimum required to display and use Windows and access your primary hardware devices is provided. Safe mode is provided precisely for troubleshooting purposes and not for general usage. The idea is that by reducing the number of software variables involved in the Windows environment, it becomes easier to identify the true cause of a problem. When you reach the Desktop in safe mode, it will be devoid of graphical enhancements, and there will be text indicators in the corners of the screen to confirm that you are in safe mode. Use this mode to uninstall problematic programs, drivers or malware, or to change settings or undo any recent changes that are causing problems with normal Windows startup. If you can't boot up into safe mode, then chances are that either you are experiencing hardware-related issues, or your Windows installation is heavily damaged.

Enable safe mode with networking: Loads up safe mode with network drivers and related services enabled, allowing Internet access. Use this mode if you need Internet access for downloading tools or drivers, or want to seek assistance. However you should avoid this mode if your issue is potentially related to malware infestation.

Enable safe mode with command prompt: Loads up safe mode with a Command Prompt interface instead of a graphical user interface. Use this if you have problems entering normal safe mode. See the Command Prompt section earlier for the types of commands that you can use in this interface.

Disable Driver Signature Enforcement: This is an option referring to an important security feature of 64-bit versions of Windows. By default, the 64-bit version of Windows 8 - and Windows 7 and Vista before it - only load up a kernel-mode driver if Windows can verify the digital signature on the driver. Unsigned drivers will not be loaded by 64-bit Windows. See the Driver Signature section of the Windows Drivers chapter for details. However you can select this option during bootup to temporarily disable driver signature enforcement by Windows, allowing you to boot into Windows and use the unsigned driver for that session

only; the next reboot will require the same procedure again. If you wish to keep on using an unsigned driver in this manner, one alternative is to use the Sleep or Hibernate modes in Windows to close down Windows without doing a full restart, and hence keep this setting in effect. See the Power Options section of the Windows Control Panel chapter for more details on the sleep modes.

Disable early launch anti-malware driver: By default, Windows loads up the Early Launch Anti-Malware (ELAM) driver at boot time, before any other drivers, so it can check to see if other drivers are safe to load at startup. This is an anti-malware measure in Windows which may cause problems with startup. If you are certain that recently installed programs are safe, try disabling ELAM and if this results in normal bootup, then you will at least confirm that this feature is the cause of the problem. You may have to uninstall any recently installed software until the issue is resolved by the developer.

Disable automatic restart on system failure: This option disables the automatic restart which occurs when Windows experiences a major error such as a Blue Screen of Death. I recommend that you permanently disable this function within Windows, as this will then allow you to have enough time to read and record the details of an error. See the Windows Errors section of the Performance Measurement & Troubleshooting chapter for details.

If none of the tools in the Windows Recovery Environment help to diagnose and resolve your problems, then the best course of action is to use the new Windows Refresh feature to put Windows 8 back to its default state, but also keep your personal data and key settings. If the same problems persist after a Refresh, then chances are that you have a hardware-related issue, which means you should refer to the Hardware Management chapter.

The most important point throughout this entire chapter is that prevention is better than cure. While Windows 8 comes with a suite of troubleshooting and recovery features, the backup features are far more important. The backup functionality in Windows allows you to protect your data in a range of simple automated ways, so that should anything and Windows becomes unbootable or corrupted, you can simply use System Restore, System Image Recovery, or Windows Refresh, and be up and running again with no discernible loss of data or time.

HARDWARE MANAGEMENT

Before delving into Windows optimization or customization, it is very important to first ensure that your hardware and connected devices are correctly configured for optimal operation. Regardless of any changes you make in Windows or your software, if your hardware is not managed properly its capabilities will not be correctly utilized, indeed serious problems such as random crashes or data corruption may occur. Whether you've built a PC or purchased a pre-built machine, you should make certain that all of the hardware-related settings are correct, and that your hardware is maintained in an optimal state.

This chapter covers all the key considerations when it comes to managing hardware, but please note that details regarding the purchasing and building of a PC are beyond the scope of this book.

< THE BIOS & UEFI

The BIOS (Basic Input/Output System) is a program held on a small ROM chip on your motherboard. It provides the instructions for what your PC should do as soon as it turns on. Your BIOS is independent of your Operating System, which means it is not directly affected by the operating system you use, or which driver version you've installed, or what your settings are in Windows for example. The BIOS supersedes all of that, and your drivers and operating system will only load after the BIOS has loaded up. The BIOS controls a range of hardware-related features and is the middle-man between your CPU and other devices.

If there is an incorrect setting in your BIOS - that is, a setting which is not optimal or correct for your hardware configuration - then you will have problems regardless of any setting you change in Windows, or which driver versions you install. Importantly, the BIOS is best configured correctly before installing Windows, as this reduces the number of unnecessary services and drivers which Windows may install, and helps reduce the potential for device conflicts.

The latest motherboards have a different type of BIOS-like implementation called UEFI (Unified Extensible Firmware Interface). UEFI is a newer form of software interface between your hardware and the Operating System, and in some cases is implemented on top of a BIOS. While UEFI brings with it a range of changes, in practice you will still need to configure all your hardware settings in much the same way as a BIOS.

As a BIOS/UEFI starts to load, the first thing it does is the Power-On Self Test (POST), a diagnostic program which quickly checks your components and makes sure everything is present and working OK. The POST sequence is usually extremely fast; you will only really notice it if it stops when encountering an error. POST error messages can be a bit obscure, but usually give you a lead as to where to look in your BIOS settings. Check your motherboard's manual for descriptions of POST error messages or error sounds.

If you have no initial POST errors you will then see your PC's startup screen, which shows such information as your BIOS/UEFI type, the key to press to access your BIOS/UEFI settings (e.g. DEL, F1 or ESC), the type of processor and its speed, RAM amount and RAM test results, drive information, and so forth. Note that if any of this information is incorrect, it may be that your hardware is extremely new and hence not recognized correctly by the current BIOS version; you've overclocked your PC too far; or you have bad hardware or incorrect BIOS settings.

On the latest UEFI systems, the entire startup procedure above may be completed in a matter of seconds with Windows 8.

To access the detailed settings in your BIOS/UEFI, you typically need to repeatedly press a particular key as your system is booting up, such as DELETE or ESC. Check your motherboard manual for specific details, as the exact procedure to enter this setup screen will differ from system to system. The layout of the BIOS or UEFI settings screen, and the names of all the settings vary greatly depending on the particular motherboard brand and model you own, so I cannot possibly cover them all here. Once again, you must refer to your motherboard manual, combined with online research, to determine what these settings do. Configuring these settings is an important step, as it ensures the correct operation of your hardware. Equally as important is disabling any unused devices or unnecessary options in the BIOS/UEFI, as this will prevent Windows from installing superfluous drivers or services.

Finally, since the BIOS/UEFI is written on a rewriteable ROM chip, it can be updated (or 'flashed') with an updated version of this Firmware. Motherboard manufacturers release new versions of this software which can improve performance, stability and compatibility, add new features, or modify existing features, and fix known bugs. These new BIOS versions are available for download on the manufacturer's website. You must make sure that you download the correct BIOS/firmware version for your motherboard, so aside from checking the motherboard manual, use the tools under the System Specifications chapter to determine your motherboard's exact model number and current BIOS/firmware version before applying any updated software to it.

Unfortunately this section has been quite vague regarding the configuration of the BIOS/UEFI, despite its critical importance to the correct and efficient operation of your hardware. This is because there is a great degree of variability between the BIOS/UEFI interface and optimal settings across various systems. The main aim of this section therefore is to alert you to the need to perform this important task. As noted repeatedly, your first port of call should be your motherboard manual, and then next you should visit your motherboard manufacturer's website, for the information and updates you need. Although it can be difficult, take the time to configure your BIOS/UEFI correctly, particularly if you are about to (re)install Windows 8.

< GENERAL HARDWARE MANAGEMENT

It is important to properly maintain your hardware, to ensure that it works efficiently and remains in good operation for many years to come. The information in this section will help you understand how to keep all of your hardware components operating smoothly.

HANDLING HARDWARE

If you have to physically handle the hardware components in your system at any time, such as removing or installing a component, checking connections, or for cleaning purposes, you should make sure to follow these tips to prevent any permanent damage to your hardware through mishandling:

- Before opening your case and/or handling any of your components, always shut down your PC and turn off the power directly at the wall socket. The electricity in a PC can kill or injure you, especially the dangerous voltages contained in your Power Supply Unit (PSU). Even when switched off at the wall, the PSU can retain a lethal charge for quite some time, so on no account should you ever open your PSU, put any liquids into it, or insert any metal objects into its casing.
- Once you have turned off your system at the wall, press and hold the PC power button for several seconds to discharge any residual charge in the motherboard's capacitors.
- While handling hardware components, make sure you regularly discharge any static electricity in your body by touching any earthed object - that is, any object that can harmlessly dissipate static electricity. An electrostatic discharge from your body can potentially damage or kill an electronic component. Typically if you leave your PSU plugged into the wall socket (but switched off), then periodically touching the side of the metal PSU case will harmlessly discharge any static electricity. You can purchase a special anti-static wrist strap if you handle computer hardware regularly. Also try to minimize how

much artificial fabrics and materials you are wearing, as these can help to build up a significant electrostatic charge in your body.

- Do not use a vacuum cleaner to clean the inside of your computer and its components, precisely because vacuum cleaner nozzles can build up and discharge static electricity. Use a clean, barely damp, lint-free cloth (e.g. a microfiber cloth or chamois), along with barely damp Q-tips to wipe dust from surfaces and crevices. Be very gentle, making sure you don't scrape the Printed Circuit Board (PCB) of any hardware component. Don't use any detergents, and most certainly don't spray anything onto the components. Ideally, if it is available to you, a can of compressed air (or an air compressor) can be used to blow dust from hard-to-reach or sensitive surfaces, as this is much safer and far more effective.
- If blowing dust from a fan, especially if using a high pressure source like compressed air, insert and hold something like a pen in the fan's spokes to prevent it from suddenly spinning rapidly, as this can damage the fan's bearings.
- Do not force any plugs, cables or components into sockets that do not appear to be accepting them. Even if the two ends seem to be matched, the pin arrangements may be slightly different, or out of alignment, and hence forcing a fit may bend or break some of the pins and permanently damage the connection. Computer hardware interfaces are designed to fit together with firm but not excessive force. This includes components like the CPU chip which fits into the appropriate socket on the motherboard. Align all the pins perfectly and press evenly, but not too hard, and they will mate safely. Force the fit and you may end up breaking the pins, making your CPU unusable.
- Most devices in your PC require a source of power, however the voltage they require is very specific. If you connect the wrong plug to the component (which is hard to do), or forget to attach a necessary power connector (which is quite common), then the component will appear to be dead or may malfunction. You will have to check your component's documentation and the motherboard manual to ensure that all components are plugged in correctly to receive sufficient power.
- Most hardware components are sensitive to physical impact and strong vibrations. Avoid situations which result in the bumping or banging of these components, or insecurely mounting heavy fans or heatsinks onto them, which can pass excessive vibrations to these components, or warp them under the weight.
- Do not handle liquids around electronic components. Any spillage can result in disastrous short-circuiting. If liquid is spilled onto a component, disconnect it from the power straight away, and ensure that they are dried out thoroughly before switching them back on for testing.
- Do not place excessive weight on a PCB as this can crack or warp it such that it will be permanently damaged.

Electronic components these days are quite hardy, and can withstand some abuse, but given how valuable they are, I suggest that you don't take any risks when handling them and in their general usage. The tips above should be observed if you want to see optimal performance and longevity from your PC hardware.

THERMAL COMPOUNDS

Thermal compounds are used to provide greater conductivity between two surfaces, such as the heat spreader on a CPU chip, and the base of a CPU heatsink. Thermal compounds are essential for ensuring optimal mating between two heat-conducting surfaces, filling in any tiny surface imperfections. If they are not used, severe overheating or hot spots on a component can result, which in turn will shorten its lifespan considerably, or cause it to malfunction or shut down within moments.

Most people who build their own PC are familiar with the use of thermal compounds, especially for the mounting of CPUs. Unfortunately many do not follow the specific instructions which come with these compounds, and apply either too much, or too little. Follow the application instructions exactly as given, as extensive testing has shown it to be the best method. Attempting to evenly spread the thermal compound manually for example is not recommended. Whether you put too little or too much compound on your component, the end result will be the same: the component will overheat, as it will either have insufficient

compound to provide optimal thermal conductivity, or too much compound, which prevents proper conductivity and builds up heat.

Also keep in mind during the application of any thermal or adhesive compounds of any type that many of these can conduct electricity, and hence cause a short-circuit. Apply them cautiously, and don't just assume that any excess will dry up and disappear; remove all excess thermal compound thoroughly with a cloth or appropriate cleaner. The best way to prevent such problems is to only use a small amount of thermal compound, and don't place any thermal compound near the edge of a component, as once under pressure, it will spill out over the edges.

Surge Protectors

Make sure that you invest in a good quality Surge Protector for your PC, and all of your other electronic devices. Aside from typically letting you plug multiple devices into one outlet, surge protectors serve an important function: they prevent spikes in voltage - which can occur for a range of reasons - from harming your components. Voltage surges needn't be sudden or catastrophic; even minor increases in voltage can reduce your component's lifespan over a period of time. Note that most surge protectors will not protect your equipment from the surge generated by a direct lightning strike on or near your house, so during heavy thunderstorms it is recommended that you turn off your PC and any other expensive electronic equipment, and disconnect their power plugs from the wall socket to provide foolproof protection against any surge. This also includes unplugging any phone lines used for DSL.

Power Supply Unit

Your Power Supply Unit (PSU) is an essential part of your system, and one that is often ignored. It is critical to system stability, and if, after reading the information below, you feel that there may be cause for doubting the quality or capability of your existing PSU to service your PC properly, you may wish to purchase a new and more adequate unit before investing too much time into optimizing your Windows installation. This is because no amount of optimization can overcome the problems caused by a poor quality PSU. It also jeopardizes your components, potentially damaging them over time. A more efficient PSU can also save you money in the long run by using less electricity.

For basic details regarding PSUs, see this PSU FAQ which covers the common output specifications for PSUs and what they mean. In particular you should consider three key factors when determining the quality and adequacy of a PSU for your system: Wattage, PSU efficiency, and total amps delivered on the +12V rail. These figures should be readily available from the PSU's specifications.

Wattage: To work out a rough estimate of the PSU Wattage that is sufficient for a particular system, use this Interactive PSU Calculator. It is fairly straightforward to use, however there are some traps you can easily fall into which will result in overestimating your power usage. Pay careful attention to the descriptions and footnotes while going through the calculator.

Efficiency: This doesn't represent how much of a PSU's power is usable; all good PSUs can provide up to their maximum rated wattage with stability if required. Furthermore, contrary to popular belief, whether a high or low wattage PSU, the PSU only provides the amount of power the system needs, so buying a larger PSU than you require won't result in extra power usage all by itself. PSU efficiency is the proportion of the power the PSU draws from your power socket that is actually relayed to your system. For example, a PSU with 80% efficiency providing 400W of power to your system will actually draw 500W from the power socket on your wall while doing so. In practice efficiency will differ at different levels of load on different PSUs, and it's an important figure to look out for. Ideally you want 80% efficiency or higher at your expected load level on the PSU. The higher the efficiency, the more money you save in electricity bills.

Amperage: The Amperage on the +12V rail is a key factor in system stability. For example, if you look at the specifications of some graphics cards, they will say that they require a current of a certain number of amps on the +12V rail (e.g. 40A on +12V). You should refer to the specifications of the PSU to see if the +12V rail(s) provide the required amperage in total. Some PSUs may have multiple 12V rails; this is technically a safety requirement to prevent potential overload on a single 12V rail, but is not a necessity. In practice as long as the amps and total wattage supplied along the 12V rail(s) are solid and sufficient for the job required, it shouldn't make a difference whether you have single or multiple 12V rails.

The problem is that beyond trying to take note of the key factors above, only an accurate review can tell you whether a PSU is genuinely good quality or not. As this article points out, specialized instruments are necessary to determine this, not just by measuring voltages with a multimeter. Hence most PSU reviews are inaccurate and effectively useless. Accurate PSU reviews can be found at sites like HardwareSecrets, SilentPCReview and JonnyGuru, so start there if you want to know more about a particular PSU.

As a final note, if you live in an area where the mains power supply is not stable, or you can suffer periodic outages, I strongly recommend investing in a good quality Uninterruptible Power Supply. This will increase the life of your components, and is important in preventing potential data loss resulting from a power outage, such as when you enable the performance features covered under the Drive Controllers section of the Drive Optimization chapter.

COOLING

One of the most common reasons for a range of problems in Windows has nothing to do with Windows itself or any installed software, nor is it caused by physically faulty hardware. It is actually the hardware-related phenomenon of overheating. Overheating hardware can cause all sorts of strange errors, crashes and problems, and is often misdiagnosed as being a software or driver problem. Most computer hardware generates heat as a byproduct of the power it consumes, and this heat needs to be dissipated somewhere. A typical computer case is a restrictive enclosure that traps heat. As this heat builds up in a PC case, it will cause components to malfunction, and even become permanently damaged over time. Overheating can occur in both stock systems and overclocked systems; it all depends on a range of factors we look at below. Before spending time optimizing Windows, you must make sure that your system is being properly cooled.

Measuring Temperatures: The first step in determining whether a component is running too hot is to measure its temperature. On modern PCs the CPU, graphics card and motherboard all have built-in diodes that measure the temperature for these components. The CPU temperature monitor is a reasonably accurate measure of the temperature at or near each of the various cores of the CPU; the graphics card temperature monitor provides an indication of the temperature near the GPU core; while the motherboard temperature monitor is a good measure of the general temperature within the PC case. Some other hardware components, such as power supply units and drives, may also come with temperature measurement devices whose output you can access.

To see the temperature readings from your components, you can check the BIOS/UEFI, typically under a Hardware Monitor section or similar. This gives you the CPU and motherboard temperatures, perhaps also the PSU temperatures as well. Clearly you need a more convenient method of checking temperatures under Windows, especially when running system intensive applications or games. Most motherboards come bundled with such software, but for the most accurate and consistent temperature readings, I recommend one of the following free utilities:

Real Temp - Primarily for measuring CPU temperatures, particularly across the individual cores of a multi-core CPU. Also provides a basic GPU temperature reading. Does not support AMD CPUs.
Core Temp - Similar to Real Temp, is designed to measure CPU temperatures, but also supports AMD CPUs.
GPU-Z - Covered under the System Specifications chapter, GPU-Z has a range of GPU temperature monitoring capabilities found under its Sensors tab. It also has basic CPU and motherboard temperature monitoring.
HWMonitor - Can monitor a range of system temperatures, as well as system voltages and fan speeds.
HD Tune - Covered under the System Specifications chapter, the free version of HD Tune provides a temperature readout showing the current temperature of the selected drive.
SpeedFan - A more general temperature monitoring utility which can provide CPU, motherboard and drive temperature readouts, as well as allowing manual fan speed adjustment.

Once you have the appropriate utilities, monitor your component temperatures both at idle and when your system is under heavy load. If particular components reach what appear to be very high temperatures when under load, then those components may malfunction while undertaking strenuous activities on your PC for a sustained period of time. Even when idle, your PC may begin to malfunction if heat steadily builds up in your PC case and is not cleared fast enough.

Safe Temperatures: Most people will want to know what the 'safe' temperature is for a particular component in their system. Unfortunately there is no easy answer; safe temperatures differ based on different hardware architectures, as some hardware is designed to run hotter than others. You can ascertain a reasonably normal temperature range for your component by conducting a web search using the specific brand and model of the component, along with the word "temperature", to see if any user feedback or reviews of your hardware state what temperature ranges are normal. As a very general rule of thumb, at the time of writing, both the current generation of CPUs and GPUs should not exceed 90-100C under 100% load; and for hard drives, no more than 50C is normal when under maximum sustained load. Heat is generally a non-issue for SSDs.

The best way to tell if your component is overheating is to watch for potential symptoms:

CPUs - An overheating CPU will usually throttle down its speed when under increasingly heavier loads, resulting in reduced performance. While using a utility like CPU-Z (See the System Specifications chapter) to monitor your CPU frequencies, run a CPU-intensive program such as Prime95 (See the Performance Measurement & Troubleshooting chapter). If under 90-100% load you find that the CPU is not reaching its full advertised frequency, or your system freezes or crashes, then there is a strong likelihood that it is overheating, especially if temperature monitoring also reveals a very high temperature.

GPUs - An overheating GPU will result in graphical corruption and/or crashes, whether while using a web browser, or within graphically intensive applications like games. Using GPU-Z, under the Sensors tab tick the 'Continue refreshing this screen while GPU-Z is in the background', then launch a modern game or stressful 3D application. See the Third Party Tools section of the Performance Measurement & Troubleshooting chapter for some free ones you can obtain. Watch for any noticeable anomalies in the graphics, such as flickering textures, dots, or strange colors, and then after a few minutes quit the application and click the 'GPU temperature' line of GPU-Z, and select 'Show Highest Reading' to see what the highest temperature was. A high temperature combined with signs of graphical anomalies, corruption or crashing, is almost always a clear sign of an overheating graphics card.

HDDs - An overheating hard drive is less common, and also harder to spot, however any strange noises from the drive, any signs of data corruption, or any problems or long delays in accessing the drive tend to indicate a problem which may be caused by overheating. SSDs are not the same as HDDs, and are unlikely to suffer from heat-related issues because they have no moving parts.

If you believe you are experiencing any heat-related issues in your system, see the tips below.

Cooling Tips: If you suspect that you are experiencing system problems due to heat, or more importantly, if you want to prevent any heat-related problems from occurring, the following basic cooling tips should be observed. This applies equally to overclocked and non-overclocked systems:

- Remove any obstructions from around your case. For example, don't obscure any of your case grills/air holes by having them pressed up against a piece of furniture or a wall, or blocked by dust or carpeting. Insufficient flow of air into and out of the case is the number one cause of heat buildup and heat-related problems. No matter how much cooling you have inside a case, if air can't easily get into and out of the case, then your system will overheat.
- If you have few or no major case fans drawing in cool air and expelling hot air, remove the sides of your case so that the fans on the CPU, graphics card and Power Supply can get a fresh supply of cooler air, and can expel hot air outside the case.
- If you have several case fans, where possible arrange them so that some are to the front and low in the case, sucking air into the case (as the air near the floor is cooler), and some are to the rear and/or the top of the case, blowing hot air out of the case (where the hot air expelled will rise away from the case). In this situation make sure to keep the sides of your case closed so that the fans have more pressure to suck/blow air through the case's contents like a wind tunnel.
- Don't position a sucking and a blowing fan too close together as they will "short circuit" each other - that is, they will pass air through the shortest line between the two, bypassing your components and hence not cooling them as efficiently. Again, fans sucking air into your case should be lower down and on the furthest side of the case from the fans that expel heat from the case.
- If one component is shedding a lot of heat, pay extra attention to providing greater cooling to the components immediately around it. Often the excess heat from one component can cause another nearby component to overheat.
- Tidy the internal components of your case. This means all ribbon cables, power cables, etc. should be clipped or twisty-tied to be as neatly arranged as possible, primarily to avoid blocking the flow of free air around components, especially near the CPU and graphics card, which are typically the two hottest components. Secured cabling and snug plug connections also mean that you can be sure nothing becomes accidentally unplugged or short-circuited over time if the case is bumped, and hence cause mysterious hardware-based errors that will confuse you in the future.
- If using additional internal cooling like larger heatsinks or fans, make sure that they are not too heavy for the surface on which they are mounted. For example, using extremely large heatsinks on a graphics card can result in the card actually bending under the weight and hence becoming permanently damaged. Even a large heatsink mounted on a motherboard can cause it to warp or crack, damaging it beyond repair. If you feel you require such hefty cooling you should instead consider buying a larger case that has better airflow properties, or look into more specialized forms of cooling.
- Make sure your drive(s) are not smothered by cabling or crammed into a stuffy area of the case with no nearby cooling or fresh air. Higher speed hard drives in particular (i.e. 10,000 RPM or faster) can heat up quite a bit. Hard drives are often overlooked in cooling, and yet they are an important system component, and as such you should make sure they aren't confined to an extremely hot section of your case.
- Make sure that any heatsinks or heatpipes on the motherboard itself are not covered or blocked by other components or cables, or covered in dust. There is a reason why these heatsinks are there: because the chips on a motherboard often require cooling, otherwise they can malfunction due to excessive heat just like any other major component. Don't assume a heatsink or heatpipe without a fan implies that the component requires minimal cooling, as sometimes manufacturers avoid putting a fan on these components to reduce noise, or to reduce costs. This simply means the heatsinks or heatpipes have to do more work, so keep them well exposed to cool air. You may even consider placing a case fan near them if you wish to aid in overall system stability.

While non-overclocked components can overheat, overclocked components heat up much faster and are a very common cause of system instability and a range of problems. If experiencing problems on your system make absolutely certain that as part of your initial troubleshooting you return all of your components to their default settings to see if this removes or reduces the severity of the problem. See the Overclocking section later in this chapter for more details.

Thermal compounds are covered in more detail earlier in this chapter, however it should be noted once again that another common cause for overheating is the incorrect application of thermal compound by the user. Too much or too little thermal compound can cause a component to overheat dramatically, so always follow the application instructions to the letter and don't improvise unless you are highly experienced. You may also wish to consider purchasing high quality thermal compound for use on your components, as the compounds which come with any component are typically of mediocre quality at best.

The most simple of all of these hardware management tips which anyone can undertake is to provide greater access to fresh cool air for the case's contents, and to regularly clean the case to remove dust buildup. Dust in particular can reduce airflow significantly, and can build up surprisingly fast, so keep your case and your components dust-free. Furthermore, the next time you upgrade your PC hardware, I recommend placing a priority on buying a larger case with plenty of ventilation. This is the single best investment in cooling, and hence general system stability.

< DEVICE MANAGER

Once you have configured your BIOS/UEFI optimally, and have made sure that your hardware is correctly connected and cooled, the Device Manager in Windows is the central location you should use for appropriate software configuration of all of the hardware on your system. You can also use the Devices and Printers component under the Windows Control Panel to access a range of hardware functionality and configuration options for connected devices, and this is covered in more detail under the Devices and Printers section later in this chapter.

To access Device Manager, open the relevant component in the Windows Control Panel, or type *device manager* on the Start Screen, select Settings and press Enter. The main Device Manager window lists all of your detected hardware, grouped by category. You can double-click on any category to see the individual devices listed beneath it. To see more details for devices, double-click on a device, or right-click on it and select Properties.

RESOURCE ALLOCATION

ACPI is the Advanced Configuration and Power Interface standard, and is an important part of the way Windows and drivers communicate with your hardware. In versions of Windows prior to Vista, you could run hardware that didn't support ACPI, or even disable ACPI if you wanted to attempt manual resource allocation. This is no longer possible, as newer versions of Windows require ACPI for hardware to function correctly. That means that you cannot disable ACPI, and older hardware which is not properly ACPI-Compliant will not run on Windows 8. Only systems based on motherboards whose BIOS is ACPI Compliant and dated 1 January 1999 or newer can be used.

Windows 8 does not fundamentally change the way resources are handled compared to Windows 7. It adds support for low-power internal buses, such as I^2C, SPI, GPIO, and High Speed UARTs. Basically, since Windows 8 only accepts ACPI-compliant systems, and because most recent hardware supports Plug and Play functionality, resource allocation is handled automatically and quite efficiently, and should not be an issue requiring user intervention. One aspect of automatic resource allocation which could cause an issue on some systems is covered below.

Interrupt Requests (IRQs) are the way in which all of your major system devices get the CPU's attention for instructions/interaction as often as necessary. There are a number of IRQs available in a modern PC, and these are typically assigned to individual components or hardware functions. To view your current IRQ allocation open Device Manager, then under the View menu select 'Resources by Type'. Expand the 'Interrupt Request (IRQ)' item and you will see all of the devices currently active on your PC with the IRQ number showing as the number in brackets, e.g. IRQ 0 is shown as *(ISA) 0x00000000 (00) System Timer*.

Ideally, your major hardware components should each be on a separate IRQ. However Window allows several devices to share an IRQ, and usually manages this without any major issues. But there are cases where a shared IRQ, also known as an IRQ conflict, can cause problems. This typically occurs when two or more high-performance components, such as your graphics card, sound card, or Ethernet controller are sharing a single IRQ.

The quickest method to check for potential IRQ conflicts is to use the built-in System Information tool, as covered in the System Specifications chapter. Open the System Information tool, expand the 'Hardware Resources' item in the left pane, and you can click the IRQs item to see the IRQs listed in numerical order. Now click the 'Conflicts/Sharing' item in the left pane to see a summary of potential sharing conflicts. Don't panic if you see several shared resources listed, as it is common for some hardware to be sharing a single IRQ or resource, depending upon your motherboard's chipset. In any case, usually you can't alter the IRQ allocations from within Windows, as they are automatically handled by ACPI. Only legacy devices will have the option to attempt manual alteration of their resources under the Resources tab of the relevant device Properties in Device Manager; most other devices do not allow the 'Use automatic settings' option to be unticked.

What you need to look for are any sharing conflicts for devices on your system which are currently displaying problems, and also whether any high-performance devices such as graphics cards, sound cards or network controllers are sharing a resource with each other. There may be a degradation of performance if two or more high-performance devices are on the same IRQ (e.g. a graphics card and an ethernet controller on the same IRQ, or a graphics card and sound card on the same IRQ).

To remedy a potentially harmful conflict, try the following methods:

§ Disable unused devices - Covered in more detail further below, disabling unused devices in the BIOS/UEFI, as well as within Device Manager, is not only a way of reducing unnecessary resource usage and speeding up boot time, it also helps prevent IRQ sharing-related problems.
§ Move conflicting devices - You can attempt to reduce IRQ sharing by physically moving a device to another location on your system if possible. For example, shift a sound card from one PCI/PCI-E slot to another, or if a USB Host Controller is sharing with a major device, avoid plugging any USB device into the specific USB hub that controller relates to.

If after disabling unused devices and attempting to move conflicting devices around you still have difficulties or reduced performance which you feel are attributable to IRQ sharing, the final option is to do a clean reinstall of Windows, first making sure to correctly configure your BIOS/UEFI and disable all unnecessary devices. There is no guarantee that major devices won't wind up being shared again in exactly the same manner as before. For the most part, IRQ sharing should not be cause for concern when using modern hardware under Windows 8.

Device Power Management

Aside from the global Power Options, covered under the Power Options section of the Windows Control Panel chapter, you can access individual device-specific power management settings in Device Manager for certain types of devices (e.g. Keyboards, Mice, HID and USB devices). To do so, open the Properties of any specific device, and if there is a Power Management tab, select it and you will typically see two options, one or both of which may be available to be ticked (on) or unticked (off):

Allow the computer to turn off this device to save power: This option lets Windows power management disable a device if it considers it to be idle. Unfortunately, USB devices in particular can have performance issues if this option is ticked, so I recommend unticking it.

Allow this device to wake the computer: This option allows the device to wake the computer up from a sleep mode. You can untick this option if you specifically don't want a particular device to be able to interrupt sleep mode, or if you don't use any sleep modes.

Problematic Devices

Devices with a question mark or exclamation mark next to them in Device Manager indicate that Windows is unable to use the Plug and Play system to accurately identify these devices. They will need further action to correctly identify and install. Until Windows can identify a device properly, it cannot be used even if it is correctly connected to your system and identified by your BIOS. In most cases, the most important step required for Windows to detect the device properly is the installation of an appropriate driver. If a suitable driver isn't available from the manufacturer's website, you may be able to find one by running Windows Update, or by using a driver for a similar device. See the Windows Drivers chapter for full details.

If the correct driver is installed, the next thing you should try is the Hardware and Sound automated troubleshooter function found under the Troubleshooting component of the Windows Control Panel. See the Troubleshooting section of the Performance Measurement & Troubleshooting chapter.

If a driver update is ineffective, and the troubleshooter has also failed, you can explore the specific error under the 'Device Status' section of the General tab of the device's Properties. A fully functional device should state 'This device is working properly'. If anything else is stated, copy the text shown and do a web search on it along with the name of your device to find what other people have done to resolve the issue. It should be noted that Windows 8 has added more descriptive error messages for USB devices as detailed in this Microsoft Article.

You can also check the information under the Events tab of the device's Properties. This lists a series of events relating to the device's installation and initialization in chronological order. Highlight each entry in the list of events to see more details in the Information box at the bottom. You can see which driver(s) have been installed for the device, and any status updates which may give you a clue as to the point at which the device malfunctioned.

If all of the steps above have not resolved the issue, you can use the 'Add Legacy Hardware' feature of Device Manager, found under the Action menu, to manually add a device. Once this option is selected, the Add Hardware wizard will open, guiding you through the process:

1. The first step is to select the 'Search for and install the hardware automatically option'. This will force Windows to attempt to redetect any newly connected hardware and install it using any existing drivers.
2. If this option fails, select the 'Install the hardware that I manually select from a list option' and click Next.

3. You will be taken to a list of general hardware categories. Select the category which you believe is the closest for your device, then click Next.
4. A list of one or more brands, models or types of that particular device category will then be shown. Select the one which you believe is closest in functionality and compatibility to your device. Click Next to install the relevant device on your system, and test to see if your problematic hardware now has any functionality.
5. If you find none of the options is appropriate, and you have found a suitable driver that you want to manually install, click the 'Have Disk' button and direct Windows to the drive/directory where the driver files are held.

Ultimately if you cannot find a working driver for the device, whether it be a driver specifically made for your device, or for one like it, it will be difficult to resolve the problem and hence use your hardware with full functionality. Windows requires a driver of some kind - whether a built-in generic Windows driver, or a third party one - in order to communicate with your hardware components.

DISABLING OR REMOVING UNUSED DEVICES

One of the best ways to reduce startup times in Windows, reduce resource usage, and prevent potential hardware conflicts, is to disable or remove unused devices. The recommended way to do this is to first disable any unused devices in the BIOS/UEFI before installing Windows 8. However if this is not possible, it is still useful to disable devices in the BIOS/UEFI on an existing installation of Windows.

Some examples of common devices that should be disabled if you're not going to use them include:

§ Unused IDE Channels
§ Unused SATA Channels
§ RAID options
§ Onboard Audio
§ Onboard Video
§ Game Port
§ Midi Port

Once these have been disabled in the BIOS/UEFI, boot into Windows and make sure that all of your normal functionality is unaffected. You can always re-enable any device in the BIOS/UEFI at any time, so this is by no means a permanent disabling of particular devices. However you should only disable devices in the BIOS/UEFI that you are certain will not be used during your normal Windows usage; disabling a necessary device, such as a required drive controller, may see you unable to boot into Windows.

Disabling unused devices not only frees up unreserved IRQs and reduces the chances of resource sharing, it speeds up bootup time noticeably, especially on older systems. This is because firstly your BIOS/UEFI will not spend time trying to detect and enable these functions, and secondly, Windows won't load up drivers or services for these unnecessary devices at startup.

Once you've disabled a device in the BIOS/UEFI and are certain that there has been no loss of functionality, you can then move on to disabling or removing relevant components in Device Manager. If you aren't using certain devices which appear in Device Manager, you can safely disable them by right-clicking on the device and selecting Disable. This is only recommended for medium to advanced users, as disabling necessary devices can cause a lot of problems. In particular I don't recommend disabling any device found under the Computer, Processors or System Devices categories as these are all needed. If in doubt, do not disable anything without first conducting extensive online research.

As a final step, you can clear out hidden entries in Device Manager for devices which are no longer connected to your PC. For each device that has ever been connected to your system, Device Manager will

retain a range of entries relating to the device type, and the drivers and hardware settings it used. That way if it is ever reconnected, it can be quickly recognized again and ready for immediate use. However there are times when you have permanently discontinued the use of a device, or through a change in the BIOS/UEFI settings, or drivers, the device no longer uses particular resources.

To view and remove unused devices in Device Manager, first use System Restore to create a restore point as a precaution, then do the following:

1. Open an Administrative Command Prompt.
2. Type the following lines, pressing Enter after each one:

```
Set devmgr_show_nonpresent_devices=1
```

```
Devmgmt.msc
```

3. In the Device Manager window that opens, go to the View menu and select 'Show Hidden Devices'. Now expand each category one by one and start looking through all the devices. Device names shown in gray are for old/unused/disconnected devices, and are usually safe to remove by right clicking on each one and selecting Uninstall. However, don't uninstall a device that you know you will be reconnecting to Windows in the near future, as this is pointless.
4. In particular, you might find several entries under the Display Adaptors or Monitors sections from previous graphics driver or graphics card installations. You should delete all of these grayed out entries, but at least one un-grayed entry must remain. You may also find grayed entries for drive controllers you no longer use, and these should be safe to remove. Various disconnected USB devices typically found under the Keyboards, Mice and other pointing devices and Universal Serial Bus controllers categories are also fine to remove if you don't foresee connecting them again, or if they are duplicates of an already connected device.
5. Once done, you can close Device Manager the usual way and the next time you open it up it will not show unused devices until you again use this method.

In many cases if you accidentally uninstall a hardware device that is currently connected to or required by your system, you can simply disconnect and reconnect the device, or reboot Windows, and it will be redetected by Windows and the appropriate drivers installed again. This method doesn't permanently remove any device such that it prevents it from being detected or used again in the future usage. But in some cases, removing important devices may prevent Windows from booting up or functioning properly, which is where an appropriate restore point comes in handy to quickly undo the damage. As a general rule, if in doubt, do not remove any item Device Manager, gray or otherwise.

< DEVICES IN METRO

Basic device management functionality can be found under the Metro environment in the form of the Devices feature. To access it, go to the Settings charm, select 'Change PC Settings', then click the Devices category; or type *devices* on the Start Screen, select Settings and press Enter. This section lists a range of connected devices, and allows you to disconnect any one of them by clicking on it and selecting the minus button which appears. You can also add a device by clicking the Add button, which allows Windows to scan for hardware changes and newly connected devices, and add them to the list.

Another new feature of Windows 8, as covered in this Microsoft Article, is that connected a new device may result in the automatic installation of a Metro-based app for that device. The installation and functionality of such an app is dependent on the device manufacturer. You can control whether any device app is installed by changing the settings under Devices and Printers, as covered in the next section.

< DEVICES AND PRINTERS

Introduced in Windows 7, and continuing in Windows 8 with much the same functionality, Devices and Printers is designed to consolidate a range of device management and usage features in a central location that is more user-friendly than Device Manager. You can access Devices and Printers as a component under the Windows Control Panel, or by attaching a supported device to your system.

Aside from listing your basic PC components, the types of devices which appear in Devices and Printers include any peripherals that you have connected to the PC, such as USB devices, wireless devices, printers and any network-based devices. Unlike Device Manager, Devices and Printers is not designed to be a detailed listing of all of the hardware components of your PC, such as your CPU or graphics card - it is primarily aimed at providing quick access through a user-friendly graphical interface to common functionality for connected peripherals, such as cameras, phones and printers.

To configure the general settings for Devices and Printers, right-click on your PC device - the device with your computer name - and select 'Device Installation Settings'. There are two possible options here:

Yes, do this automatically: Windows will connect to the Internet and automatically download any drivers it considers best for your connected device(s) from Windows Update without prompting you, and will also update your generic device icons with any custom ones which have been provided by the manufacturer. This is the best option if you are a relatively new user, and will allow you to quickly use your devices.

No, let me choose what to do: Additional options appear, giving you the ability to ensure that outdated or undesirable driver versions are not automatically installed over more recent or custom drivers that you have installed yourself. As such, selecting 'Never install driver software from Windows Update' will give you full control over the drivers installed on your system. Whether you tick the 'Automatically get the device application and information provided by your device manufacturer' option is up to you; enabling it replaces the generic device icons with more realistic ones, and also allows the automatic download of a custom Metro app for that device. These functions depending on the level of support for these features provided by the device manufacturer. The device app is a new Windows 8 feature covered under the Devices in Metro section earlier in this chapter.

All connected devices should automatically be added to Devices and Printers. If a device is not detected, click the 'Add a device' button at the top of them Devices and Printers window to force Windows to search for all attached devices and list them. Each device should appear in Devices and Printers, even if it is not identified correctly or does not have full functionality.

Once a device appears in Devices and Printers, any problematic devices will be identified with an exclamation mark. Right-click on these and select Troubleshoot to allow Windows to attempt to find the best solution. If unsuccessful, you can explore further options as prompted by Windows, but usually this simply means you will have to manually find and install relevant drivers. See the information in the Device Manager section earlier in this chapter for dealing with problematic devices.

If a device is correctly detected, you can right-click on it for a menu of available functions and settings, depending on the device. While all of these functions and settings can be accessed in various other areas of Windows, the aim of Devices and Printers is to allow quick access to them in one location. The most useful unique settings relate to printer functionality, because Devices and Printers replaces the Printers folder used in previous versions of Windows. Right-clicking on a printer in Devices and Printers brings up a range of printer-related options, letting you access printer preferences, see what's printing, and set the default printer.

Note that the icon for any device in Devices and Printers can be sent to the Desktop as a shortcut by right-clicking on it and selecting 'create shortcut'; or you can simply drag and drop the icon to the Desktop to

place a shortcut there. This special device shortcut retains all the functionality it would normally have within Devices and Printers, including the useful right-click context menu items.

< DEVICE STAGE

Device Stage is similar in intent to the Devices and Printers function. It is designed to be a central location for providing relatively straightforward access to the major functionality of a particular device in an easy-to-use graphical interface. If you connect a compatible device to your PC, Device Stage will automatically open. You can also open Device Stage by double-clicking on a supported device in Devices and Printers.

Device Stage typically displays a picture of your connected device in the Taskbar. This icon can be right-clicked to quickly access a range of functionality for the device, or you can left-click on it to open the Device Stage window. A customized screen with a large picture of your device, along with its full name and details, will appear at the top of the Device Stage window. At the bottom of the window are a range of options relevant to your particular device.

Device Stage is mainly intended for mobile phones, digital cameras, portable music players and various printers. A device's compatibility with Device Stage is determined by the support provided by the hardware manufacturer. This means that certain devices, particular older devices, may not do anything more than open the normal AutoPlay prompt when connected. Other devices may open a basic Device Stage window without much customization or specific branding. Fully supported devices open a Device Stage window with the feature-rich content and device-specific pictures and Taskbar icon as described.

Device Stage is designed for convenience. Although most of its functionality is available through a range of other Windows settings and applications, the fact that it appears automatically and provides all of the common functions in one location makes using a device much easier for both novice and advanced users. Note that when you disconnect a device, any Device Stage window and Taskbar icon for it automatically closes, which means it doesn't add to Desktop clutter.

If you wish to customize the Device Stage functionality for a particular device for any reason, you can use the Device Stage Visual Editor Tool.

< OVERCLOCKING

People who want additional performance from their PC may undertake a procedure known as Overclocking. This is the process of increasing the clock speed of a component beyond its normal specifications. The clock referred to is a specialized oscillator, pulsing with a frequency that determines the rate at which a data processor can perform instructions. The theory of overclocking is simple: increase the clock speed and you will increase the rate at which instructions are performed, leading to a faster PC. Overclocking is possible on a range of hardware components including CPUs, graphics cards, motherboards and RAM.

Another method of overclocking which doesn't involve increasing the clock rate is by altering timings. Memory-based components, such as system RAM and Video RAM, have latency timings - rest periods between operations measured in clock cycles. By decreasing the latency time, a memory component can be made to wait less between completing specific operations, and hence function faster.

So why are these methods possible? Why aren't the hardware components you buy not already performing to their peak potential? One reason for this is that hardware components are expected to work in diverse environmental conditions, and be put to vastly different tasks. Hardware manufacturers ensure safe headroom is provided so that in adverse conditions, the component can still operate safely and with stability. Overclocking takes up this slack by pushing the component beyond recommended specifications.

Of course when you push a component beyond its normal specifications the component requires ideal conditions to continue operating with stability. That usually means more cooling on the component, since any cooling device it already uses is only really designed to deal with stock operation. The component also requires stable voltage from the power supply, either directly, or as regulated through the motherboard. Often to achieve a stable overclock the component may also require additional voltage, which in turn can add to heat, and hence raise the cooling requirements even further. Furthermore, the additional heat being dissipated from one component may cause other nearby components to overheat.

As you can see overclocking is not as simple as it first appears, and there are often complex interactions involved at the hardware and software level which must be taken into account to achieve proper stability. Before going into any more detail about overclocking it is important to discuss the advantages and disadvantages of overclocking objectively, so you don't undertake it without knowing what you're getting yourself into:

BENEFITS

§ Increased performance - This is of course the primary reason why people overclock. The degree to which performance improves depends on the component(s) being overclocked, how far they are overclocked, and whether they are the hardware most relied upon by particular games and applications. The performance difference can be anywhere from negligible to quite significant.
§ Bragging rights or coolness factor - Some people gain a great deal of satisfaction and prestige in having the fastest machine, or the highest overclocked component, or the highest benchmark score. Or they may simply feel they are extracting the most out of their hardware by overclocking it. Some people also enjoy the tinkering and hobbyist aspect of overclocking and hardware modification. In short it can be quite challenging and fun.

DRAWBACKS

§ Costs in providing improved cooling - In almost all cases you will have to purchase more effective and/or additional cooling for your system in the form of more efficient heatsinks and/or fans, a case with more space or better airflow, or specialized equipment like a liquid cooling setup. Of course if you plan your system purchase carefully, you can minimize the additional costs to some extent by beginning with the right components.
§ System instability - Without a doubt, the number one cause of problems in games and applications is overclocking. People often refuse to acknowledge that their overclocking is the cause of the problem, and instead blame Windows, their drivers, or the game or application. Different programs react differently to overclocking. Some can tolerate much higher levels of overclocking on particular components, some cannot tolerate any overclocking at all; it all depends on how stressful the game or program is, and how stable or unstable the overclock actually is in your particular setup.
§ Potential data corruption - Pushing components like the CPU or RAM beyond their limits can result in instability, which in turn can lead to data corruption. Often this data corruption can occur subtly over time without any indication or warning.
§ Reduced component life span - Since an overclocked component is working beyond specification, hotter and faster than it was designed to handle, it will have a reduced life span. The reduction in the useful life of a component can sometimes be negligible, sometimes significant, depending on the extremity of the overclock, the quality of the component, and how well it is kept cool and supplied with stable voltage. A mild overclock typically has little or no practical impact on the life expectancy of a component; an extreme overclock can drastically reduce the error-free life of a component.
§ Damage to components - Since computer hardware is based on sensitive electronic equipment, if a hardware component is not kept adequately cool (and even in some cases if it is), it can be permanently damaged or destroyed through overclocking. It happens quite often, especially with graphics cards.
§ Loss of warranty - Most hardware manufacturers make it clear that overclocking beyond recommended clock speeds or timings will instantly void your warranty. This also goes for any associated physical

modifications to the hardware, such as changing its cooling. Unless explicitly stated otherwise, a warranty is only designed to cover unmodified hardware operating within factory specifications.

So far the disadvantages appear to far outweigh the advantages of overclocking. This is not strictly true, it all depends on how far you overclock a component and how much performance you can gain in return, as well as the quality of the hardware itself. It's important to point out that overclocking is not a beneficial procedure at all times. Despite everyone urging you to overclock your system, you should weigh up the options rationally and either choose to avoid overclocking due to the additional expense and the potentially modest performance gains, and/or the strong likelihood of instability/damage; or alternatively, research the topic thoroughly, and invest the time and money required to achieve a good balance of performance and stability.

The bottom line is that if you don't have much time or patience, or you can't afford to replace a vital system component should it get damaged, do not overclock. If your CPU or graphics card dies for example and you can't replace it, your entire computer becomes unusable, so it is not something to be taken lightly. Overclocking is easy, but overclocking properly and with perfect stability is actually extremely difficult.

METHODOLOGY

The precise details of how to overclock vary greatly depending upon your particular hardware configuration and available BIOS/UEFI options. That means it is impossible to provide step-by-step details here on how to overclock a particular component of your system. The information below provides a brief overview on the main overclocking possibilities and methods:

- *CPU:* The most common component to be overclocked, there are typically multiple settings in your BIOS/UEFI that allow you to indirectly or directly alter the clock speed (in MHz) of your CPU. Doing so will increase the speed with which data is processed, which can improve overall system performance in a range of activities.
- *GPU:* The graphics card is like a small computer by itself. It has a Graphics Processing Unit (GPU) which is the graphics equivalent of the CPU, and it has its own dedicated memory in the form of Video RAM (VRAM). Overclocking a graphics card involves increasing the frequency (in MHz) of the core of the GPU and/or the Video RAM. The Core generates the graphics data, while the VRAM transfers information to/from the Core. You can overclock one or both of these components, with varying results based on a number of factors, but generally resulting in an increase in graphics performance the higher you overclock each component. You will need a dedicated GPU overclocking utility to perform these changes, such as the free RivaTuner, Afterburner or Precision tools.
- *RAM:* The speed of your system RAM can be adjusted in the BIOS/UEFI. This is usually in the form of adjustments to its clock speed (in MHz), as well as its timings (latency in clock cycles). Whether increasing RAM speed or lowering latency is the better option is not clear. Generally speaking, applications which have large amounts of non-graphics information to transfer to the CPU and back will benefit more from faster RAM speed which provides more bandwidth. On the other hand, applications which primarily require very complex calculations with repeated access to information in memory, such as games, will benefit more from lower RAM latency. Obviously some applications require both, so again, there is no clear-cut answer as to which area is best to overclock.
- *Voltage Adjustment:* As components are pushed outside factory specifications with overclocking, they will do more work. Often they can accommodate this extra work within their current voltage, however sometimes to gain stability, or to push a component further, you will have to increase the voltage to it. The CPU, RAM and graphics card can all potentially benefit from voltage adjustments, but it is a risky procedure. There are typically a range of voltage settings in your BIOS/UEFI, and you can also view voltages in Windows using the free CPU-Z, HWMonitor or SpeedFan utilities.

Refer to the System Specifications chapter for utilities that will provide you with detailed information about your components. Also refer to the cooling section earlier in this chapter for utilities that will let you measure hardware temperatures within Windows.

STABILITY

Overclocking is pointless if it leads to instability or other problems. The Golden Rule for troubleshooting any problem on an overclocked system is: *Always start by assuming your overclock is the primary source of any problem*. Begin the investigation of any problem or strange behavior on your PC by suspecting your overclock as the source of that problem. Reset your entire system to its default speeds and see if the problem persists, or is as severe. If the problem goes away, or doesn't happen as often, you can be certain overclocking is contributing in some way to it, or is perhaps the sole cause of it. You will have to lower or remove your overclock, or increase your cooling, until the issue is resolved. Details on how to correctly test your system for stability are covered in the Third Party Tools section of the Performance Measurement & Troubleshooting chapter. Bear in mind that even if your system can run every artificial test and benchmark there is for hours on end without a problem, the real test is having complete stability day-in, day-out, even when running stressful games and programs during hot summer days for example. If your system starts behaving strangely, or you are having crashes and problems, don't persist in maintaining your overclock.

Electronic hardware components are highly accurate devices, and forcing them to run outside their normal operating speeds can increase the potential for small errors to creep into their operation. Manufacturers often push a particular component close to its limits by default from the factory, leaving very little safe headroom, so even a small amount of overclocking can be enough to cause problems. If you're going to overclock, don't do it at the cost of system stability. At the first sign of strange behavior, don't be quick to blame everything else; reset your system to default speeds first and foremost. Make sure you have optimized and maintained your entire system as covered in this book. Then, and only then, if the problem persists to the same degree, and if, after further online research, you still find no solution, you can consider the actual program or game to be buggy in some way. Unfortunately many people start this process the other way around.

POWER SUPPLY UNIT

See the Hardware Management section earlier in this chapter for details on how to determine if your Power Supply Unit (PSU) is appropriate, and whether you need to purchase a new one to ensure stable and optimal performance. Successful overclocking requires a stable source of power, and a poor quality PSU will mean that you will experience instability regardless of any other settings you alter. Invest in a good quality PSU before considering overclocking your system.

COOLING

You will need to know what the safe temperature range is for all of your major components. There is no simple answer, as each different component, indeed different architectures and brands of components, have different safe temperature ranges. Some components, such as the CPU and graphics card, have built-in thermal throttling which automatically reduces the speed of the hardware if it reaches a preset temperature. This can prevent the component from being damaged, but you should never let your component become hot enough that it needs to throttle in this manner. Prolonged operation at such temperatures reduces the component's lifespan and increases potential instability. See the cooling section of this chapter for more details on cooling. Just like a good PSU, if your system does not have decent cooling, then overclocking is a complete waste of time as it will simply result in system instability and eventual damage.

COMPARING OVERCLOCKS

People with similar system components will frequently compare their overclocks. In some cases, one system may be operating with relative stability at a much higher overclock than the other, and this can cause some confusion. The reasons for such discrepancies are as follows:

- No two components are exactly the same. Even if the two components being compared are an identical brand, model and speed, they may have very different tolerances to overclocking depending on quality of materials, and different revisions of the same hardware.
- No two people have the exact same conditions. Your computer room may be hotter or cooler, your case may provide better or worse cooling, your combination of components may include a different PSU or different brand or speed of RAM, your system may be clogged with more dust, etc.
- Your Windows settings and general software environment will not be identical to anyone else's. In particular, you may have different applications installed with various background programs that are causing conflicts.
- No two games or programs are identical in the way they use resources and stress components on your machine. Even if all of your other games or programs work absolutely fine at a certain level of overclock, it may well be that the latest game you are playing, or the latest program you are using, has a completely different tolerance to your overclock due to different resource usage patterns, and will crash.

RESEARCH

The importance of researching overclocking before you dive into it cannot be overstressed. As this section has shown, overclocking can be quite complex, despite the ease with which it can be conducted. Don't rush into overclocking, do it slowly and methodically, and conduct a thorough web search to find peoples' experiences with overclocking hardware that is similar to your own. More often than not you will find someone who has a similar setup and who has overclocked it with reasonable success, so look out for such information as it can save you some time in your own experimentation. You will also find a range of guides, of varying quality, that spell out the procedures relevant to your hardware for overclocking various components.

While researching the topic, be aware that people often have different definitions of "stable" when it comes to overclocking, or may even outright lie when asked if their system is stable. Furthermore, no two systems are identical so don't automatically assume that you can achieve the same results as someone else using the same hardware. Take the time to research, read and think about overclocking, and make sure that you have the right tools and knowledge to undertake it properly.

And remember - if you have doubts, or you cannot afford to replace components which may be damaged through overclocking, then don't overclock. It is not a necessary procedure and in my opinion, carries more risks than benefits, especially if you value genuine stability and data integrity.

This chapter has attempted to highlight the importance of making sure that your BIOS/UEFI is correctly configured, that your hardware is appropriately connected, maintained and cooled, and that your devices are all detected and available for use in Windows. No amount of software optimization will resolve problems in Windows if they are hardware-based. If there are any areas of doubt or confusion relating to your hardware, I strongly suggest that you clarify them now with further research, perhaps even contacting your hardware manufacturer for more information, before moving on with Windows optimization.

WINDOWS INSTALLATION

Windows 8 uses an image-based installation method, similar to Windows Vista and 7. Your Windows 8 installation media actually contains the different editions of Windows 8, with the Windows Product Key entered at the start of the installation process identifying the specific edition you will be able to install. As installation begins, instead of selectively copying across a large number of individual files, a complete compressed 'hardware neutral' image of a standard Windows 8 installation is copied across to the target drive, is uncompressed and overwrites the drive contents. As the installation continues, Windows then identifies your hardware and reconfigures itself accordingly.

Windows 8 introduces some changes to the way you can purchase and install Windows. It provides a new web-based installation option, allowing you to download and install Windows 8 in one go, or create installation media for later installation. This provides a method of quickly and cheaply upgrading any existing installation of Windows XP, Vista or 7. Windows 8 also reduces the number of product editions, and alters some of the terms of usage to simplify things further.

This chapter covers a series of important things you should consider prior to (re)installing Windows 8, including various drive preparation/configuration methods, the general steps involved during the actual installation of Windows, and anything you may need to do immediately afterwards.

< CHOOSING A PRODUCT EDITION

If you haven't already purchased a copy of Windows 8, then the very first thing you must decide is which product edition you will need. This is an important decision, as it determines which features will be available to you, and what, if any, restrictions you will face when attempting to install Windows 8.

There are four product versions available:

§ Windows 8, also known as Windows 8 Core
§ Windows 8 Pro
§ Windows 8 Enterprise
§ Windows RT

For the average PC user, only two of these are relevant: Windows 8, and Windows 8 Pro; Windows 8 Enterprise, while similar to Windows 8 Pro, is designed for businesses, while Windows RT is a stripped-down version of Windows 8 aimed at tablets and other lower-powered devices.

A basic feature comparison of Windows 8 vs. Windows 8 Pro vs. Windows RT is provided in this Microsoft Article, and a more detailed chart is available in this Microsoft Article as well as this Wikipedia Article. The choice for the average user comes down to Windows 8 vs. Windows 8 Pro, and both will perform identically. However only Windows 8 Pro will provide the following key features:

§ Group Policy Editor, allowing greater Windows customization.
§ Windows Media Center functionality via an add-on.
§ BitLocker and BitLocker To Go drive encryption.
§ Encrypting File System file encryption.
§ Hyper-V virtualization.
§ Booting from a Virtual Hard Disk.
§ Connecting to a work network.

These features are covered in various chapters, and where a feature is restricted to Windows 8 Pro, it is usually noted as such throughout this book. For the most part, there is no real reason for anyone to select Windows 8 core - Windows 8 Pro can be purchased relatively cheaply and is the recommended option.

If you already have Windows 8 Core on your PC, and want to upgrade to Windows 8 Pro for the additional features, you can use the Add Features to Windows 8 component of the Windows Control Panel to purchase the Windows 8 Pro Pack. This will allow you to upgrade your current installation of Windows 8 to Windows 8 Pro without requiring the reinstallation of Windows. See the Add Features to Windows 8 section of the Windows Control Panel for more details.

OEM vs. System Builder vs. Upgrade

An important factor to consider is which particular version to use of the particular product edition you wish to purchase. These versions do not differ in terms of content or performance, but each has its own licensing agreement terms, which in turn determines the types of usage restrictions you may face.

As of Windows 8, Microsoft has removed the Full Retail Edition of Windows, which was the most expensive and most versatile version. There are now three separate versions of any Windows 8 product: OEM, System Builder, and Upgrade. The End User License Agreement (EULA) for Windows 8 contains the terms and conditions of acceptable usage for each of these versions. Microsoft has improved the EULA, using plain English descriptions wherever possible, so I recommend that you download and read the EULA for your particular edition of Windows 8. The reason you require a license for using Windows 8 is that, as with previous versions of Windows, and indeed most modern software, you do not actually own the software outright. Microsoft gives you permission (a license) to use a copy of their software, as long as you operate it in accordance with certain terms and conditions, to which you must explicitly agree during the installation of Windows.

To make things simple, below I provide a summary of my interpretation of the key points of the license terms. For legal reasons this should not be considered a substitute for actually reading the license yourself, as your particular license terms and conditions may differ for a range of reasons.

OEM: An OEM version of Windows 8 comes pre-installed on, or accompanying, a new PC. The license is bound specifically to the first PC on which it is installed. If you substantially alter that PC's hardware, or you attempt to install the OEM copy on a different PC, you may fail activation, since you have technically breached the licensing conditions. See the Activation section later in this chapter. The OEM version is not available for general sale, and is not designed to be purchased separately by the end user.

System Builder: This version of Windows has a new Personal Use License designed for home users. As such, the System Builder version of Windows 8 replaces the previously available Full Edition. It specifically grants the right to install and run Windows 8 on any system, new or old, which has been built by a home user for personal use. Unlike an OEM version, the System Builder edition allows you to transfer your copy of Windows 8 to another PC, or change your hardware components, as many times as you like, as long as it is installed on only one system at any one time.

Upgrade: An Upgrade Edition of Windows 8 requires that you already own any valid edition of Windows XP, Windows Vista, or Windows 7. By undertaking the upgrade, you are replacing the original version of Windows you are upgrading, such that you lose the right to run that version of Windows. For the Upgrade version of Windows 8 to install and activate properly, it requires that a qualifying previous of Windows be detected. An Upgrade Edition allows you to do either an In-Place Upgrade, or a Custom (clean) install, and also allows transfer to another PC, or substantial hardware changes on an existing PC, as many times as you like, as long as it is installed on only one system at any one time. However, if you are installing Windows 8 on a completely new PC with no prior version of Windows, or if you want to run a dual boot or virtualized

setup of Windows 8, then although it is possible to use the Upgrade edition in these instances, the license terms do not allow it. This means that under such conditions, activation may fail.

The Upgrade edition is recommended if you already run Windows XP, Vista or 7. It is the cheapest version, is relatively versatile, and allows you to do a clean install of Windows 8 should you wish - see later in this chapter for details. The only time you should consider the System Builder edition is if you don't have any prior versions of Windows, or you want to run a dual boot or virtualized copy of Windows 8. The OEM version is irrelevant if you want to buy Windows 8 on its own.

In addition to the details above, below is a summary of some general conditions of use for all editions of Windows 8:

§ The OS is licensed to one specific device at any time, namely the PC on which it is currently installed. You cannot install the same copy of Windows 8 on multiple PCs or devices unless you have specifically purchased multiple licenses - one for each PC or device.
§ If the edition of Windows 8 that you buy includes both the 32-bit and 64-bit copies, you can use one or the other, but not both at the same time, whether on the same machine, or on separate machines.
§ The same product key can be used to install either the 32-bit or 64-bit version of your current edition of Windows 8. However if you run a web upgrade via the Upgrade Assistant, it will automatically upgrade a previous 32-bit version of Windows to the 32-bit version of Windows 8; and a previous 64-bit version of Windows will automatically upgrade only to a 64-bit version of Windows 8. You can only choose the platform version if you are using a boxed retail Upgrade or System Builder package which specifies that it contains 32-bit and/or 64-bit versions as relevant.
§ Except for the OEM version, you can upgrade or alter any of the hardware in the PC on which Windows 8 is installed as often as you wish.
§ Except for the OEM version, you can transfer Windows 8 from one PC to another as many times as you want, as long as it is not installed on more than one machine at any time.
§ By default, Windows 8 will automatically activate during the installation process if an Internet connection is available. OEM versions of Windows 8 typically come pre-installed and already activated. If you do not activate Windows, you will face usage restrictions until successful activation.
§ You are permitted to make one backup copy of the Windows 8 DVD, or transfer one copy to disc or other media if you purchased Windows as a digital download.

The above has been provided for information purposes only and cannot be the sole basis for any actions you take. You must carefully read the specific EULA which accompanies your particular edition of Windows to ensure that you understand all of the licensing terms and conditions as applicable to you in your country, and based on your particular circumstances.

< PRIOR TO INSTALLATION

Before installing any version of Windows 8, there are various preparations you should make and issues you should consider.

CHECK YOUR HARDWARE AND SOFTWARE FOR COMPATIBILITY

Ideally, before purchasing or attempting to install Windows 8, you should make sure that all of your hardware components and key software are compatible with Windows 8, and will run on it reasonably well. Fortunately, the Windows 8 installer incorporates several tools, which were previously available separately, to check and advise you on these matters when you initiate the installation process. So just launching the Windows installation process as normal should alert you of any major incompatibilities and what actions you can take to resolve them before Windows 8 is actually installed.

For those who want to do some research beforehand, use the following resources:

Windows 8 System Requirements - Lists the minimum hardware required to run Windows 8.
Windows 8 Compatibility Center - Lists all the hardware and software that is currently compatible with Windows 8. Enter the name of the hardware or software in the main Search box and you will see its compatibility status, and whether there is any action required to make it compatible.
Windows 8 Upgrade Assistant - Scans your PC and connected devices, as well as your installed software, and tells you if you will have any potential issues under Windows 8. After providing a compatibility report, the Upgrade Assistant utility also allows you to purchase, download and install Windows 8 if you wish to proceed. See the Web Installation section later in this chapter.

Keep in mind that Windows 8 is using the same basic architecture as Windows Vista and 7, and hence is designed to be compatible with most products supported on these earlier versions of Windows. In particular, if your system and software was able to run under Windows 7, it is highly likely to work equally as well in Windows 8.

If you haven't purchased Windows 8, and want to try it out on your hardware and software combination to see if you will run into any problems during normal usage, or to try out its features, then you can download a free 90-day Evaluation version. This provides you with a full copy of Windows 8 Enterprise, which is similar to Windows 8 Pro and contains all of the features covered in this book. Once the 90 day evaluation period expires, the trial version of Windows will go into reduced functionality mode. You cannot upgrade the evaluation license to a working version of Windows 8, so you will need to backup your data and install a purchased version of Windows.

Disable Unused Resources in the BIOS/UEFI

Prior to installing Windows 8, it is important to turn off any options and devices in the BIOS/UEFI which you will not be using, as covered in the Hardware Management chapter. This will ensure that you speed up Windows startup, minimize any shared resources or potential hardware conflicts, and prevent the installation of unnecessary drivers and services. Also see the Preparing the Drive section later in this chapter, as some other BIOS/UEFI options, such as RAID or AHCI, may need to be changed prior to Windows installation.

Scan for Malware

If you are going to transfer any data from an existing installation of Windows to your new installation of Windows 8, it is strongly recommended that you do a complete malware scan of your existing Windows installation. This ensures that you don't wind up copying across infected files which ruin your new installation of Windows. See the Security chapter of this book for full details. Importantly, if you plan to run the Windows 8 installer from within your current version of Windows, it is recommended that you disable any heuristic/real-time protection components of your anti-malware program(s). These can potentially interfere with the proper installation of Windows.

Prepare Backups

Once you are sure that your files are clear of any malware, the next step is to prepare complete backups of all of your important information. This is covered under the Backup & Recovery chapter. Regardless of which type of install you are going to undertake, even if you choose an Upgrade install for example, I still recommend having backups of your irreplaceable data on disc or another drive prior to installation of Windows, just in case anything goes wrong. It is genuinely much better to be safe than sorry.

I also recommend preparing a separate disc or USB flash drive with a copy of all of the latest appropriate Windows 8-compatible device drivers for all of your key hardware. Installing the correct drivers as soon as possible after installing Windows 8 ensures optimal stability, compatibility and performance, and can

prevent major problems. You may even need certain drivers, such as RAID or other drive or device-related drivers, for correct detection of some of your drives or attached devices during the Windows installation process. Prepare these in advance and store them on CD, DVD, USB flash drive or external drive. See the Windows Drivers chapter for more details of the different types of drivers, and where to obtain all of them.

DEACTIVATE/DEAUTHORIZE SOFTWARE

Some software is specifically linked to your current hardware and operating system via online activation or authorization. For example, the iTunes media application, or the Steam gaming platform, require that you activate and authorize them for each computer on which they are used, with a limit on the maximum number of computers or devices on which this can occur. This form of Digital Rights Management (DRM) is becoming increasingly common for a range of software.

Prior to installing Windows 8, or at any time if altering key pieces of system hardware, or if selling or destroying your PC, it is strongly recommended that you first manually deauthorize all such software on your drive to prevent any issues or the loss of activation slots. Check the software's website for more details on the steps necessary to do this correctly. Windows 8 will make an attempt to identify and prompt you to deactivate/deauthorize any such software which it detects during the installation stage as part of the built-in Upgrade Assistant functionality. However there is no guarantee that it will find all instances of such software on your system, so be sure to always undertake this step manually in advance of (re)installing Windows 8.

WINDOWS REFRESH AND WINDOWS RESET

If you are on an existing installation of Windows 8, and are experiencing severe problems to the extent that you are considering reinstalling Windows 8, then you might want to use the Windows Refresh feature in the first instance. This will allow you to keep your personal data, your user accounts, some of your key Windows settings, and all Metro apps, while resetting Windows 8 back to its default state in all other areas.

If a Windows Refresh fails, or you want to start with a completely clean slate, then you can use the Windows Reset function instead to do a full clean install of Windows 8, also ensuring that all of your previous data is securely deleted so that it cannot be recovered. This provides the quickest and cleanest way of doing a reinstall of Windows 8.

See the System Recovery section of the Backup & Recovery chapter for more details of Windows Refresh and Windows Reset.

CUSTOM OR UPGRADE INSTALL

An important decision you will have to make is how you want to install Windows, irrespective of which edition of Windows 8 you are using. This decision primarily affects whether your existing user data, programs and settings are transferred to Windows 8 as part of the installation process, and also whether you will have the option to reformat/repartition the drive during the installation process.

The two different methods for installing Windows 8 are as follows:

Custom Install

Also known as a Clean Install or Advanced Install, a Custom Install involves installing Windows 8 onto a new blank drive, or onto a drive with existing data, but not allowing Windows 8 to attempt to upgrade any previous version of Windows. A fresh new copy of Windows 8 will be installed.

A Custom install is the recommended method for ensuring that Windows 8 is installed as "cleanly" as possible, devoid of any personal files, settings, potential software conflicts, and other residue from previous

installations of Windows. However, it also means that you will have to manually backup any existing data you wish to keep before commencing installation since it will be lost, particularly if the drive is reformatted or the partition is deleted. You will then have to manually restore this data once Windows 8 is installed.

You can do a Custom (Clean) Install of Windows 8 using a System Builder or Upgrade Edition of Windows. There are two ways to initiate a Custom (Clean) Install, and each results in different options being available:

§ *Booting up from a Windows 8 DVD or USB thumb drive* - If the Windows 8 Setup media is launched at bootup, you will be able to select a Custom Install option in the installer. This provides you with the full range of options in the installation process, including the ability to choose the partition and/or the drive to which Windows will be installed, and whether you wish to (re)format and/or (re)partition the drive.
§ *Launching Windows Setup from within Windows* - If the Windows installation process is initiated by using the Web Setup method, or by launching Windows 8 Setup from within an existing version of Windows, you will only be able to select from the options available at the 'Choose what to keep' stage. If Nothing is selected, this effectively does a Custom (Clean) Install on your current drive/partition. You will not be able to choose the logical drive, or have access to the partitioning and formatting options during installation.

Note the following:

§ If custom installing Windows 8 to a partition with an existing installation of any version of Windows without first reformatting it, your personal and program files and folders may automatically be saved to a *\Windows.old* directory on that partition. This is not a substitute for taking a proper backup prior to commencing. This directory can safely be deleted after installation if you don't require any of its contents.
§ If you repartition your drive within Windows Setup, this results in the creation of a small additional System Reserved Partition which may not be desirable. See the Preparing the Drive section later in this chapter for details.

Upgrade Install

This type of installation involves either running Windows 8 at bootup and selecting the Upgrade option, or running Windows 8 Setup from an existing installation of Windows, and selecting anything other than the Nothing option at the 'Choose what to keep' stage. This method is also known as an In-Place Upgrade, and should not be confused with the Upgrade Edition of Windows.

As part of the built-in Windows Easy Transfer functionality of Windows 8 Setup, Windows 8 can keep your personal files, settings and programs instead of simply replacing everything with a fresh new Windows 8 installation. An in-place upgrade can only occur from qualifying versions and editions of Windows - details are provided in this Microsoft Article.

If you are able and willing to do an in-place upgrade, the three categories of data that can be transferred are:

§ *Windows Settings:* This includes some basic Windows settings, such as accessibility settings, Internet Explorer Favorites and History, and your Desktop background.
§ *Personal Files:* This includes anything saved under your user folder.
§ *Applications:* This includes any compatible apps or programs.

For Windows 7 users, you can do a complete in-place upgrade, copying across Windows settings, personal files and applications:

§ To Windows 8 from Windows 7 Starter, Home Basic, Home Premium.
§ To Windows 8 Pro from Windows 7 Starter, Home Basic, Home Premium, Professional and Ultimate.
§ To Windows 8 Enterprise from Windows 7 Professional and Enterprise.

For Windows XP or Vista users, the limitations are as follows:

§ For Windows Vista users, an in-place upgrade can only copy across your Windows settings and personal files.
§ For Windows XP users, an in-place upgrade can only copy across your personal files.
§ For Windows 8 Release Preview or Consumer Preview users, an in-place upgrade can only copy across your personal files.
§ For those changing languages from an existing version of Windows 8, 7 or Vista, an in-place upgrade can only copy across your personal files.
§ You cannot do an in-place upgrade to from 32-bit to 64-bit, and vice versa.
§ You cannot do an in-place upgrade from the Windows 8 Developer Preview.

The main reason for these limitations is that Microsoft cannot guarantee satisfactory performance and compatibility if older or different versions of Windows are in-place upgraded.

An Upgrade Install is only recommended for novice users, particularly those running a relatively trouble-free installation of Windows 7. This will provide the safest transition with minimal effort. For everyone else, I recommend doing a Custom (clean) Install, as this is the best way to ensure that you start with an entirely clean slate, and hence minimize the potential for conflicts or sub-optimal settings and residue being copied across to your new installation of Windows 8. Regardless of which method you choose, you should back up all of your data beforehand.

MODIFYING THE WINDOWS INSTALLATION MEDIA

As a final step prior to installation, you may want to modify the Windows 8 installation media that you will be using. Windows 8's image-based installation system allows easier creation of modified installation media. All the tools you need to do this are in the Windows Assessment and Deployment Kit (ADK). The Deployment Image Servicing and Management (DISM) tool allows you to add or remove drivers, updates and features, and generate a new customized Windows 8 installation image for any edition.

For the average user, there are some common scenarios which may require the legitimate alteration of their Windows 8 image, and we look at these below.

Adding drivers to the Windows 8 installation image: It is not recommended that you modify the Windows 8 installation image to remove features or drivers. This can cause a range of problems in the future, especially with Windows Update or Service Packs. However, you may wish to add drivers to your image, so that all of your devices will be detected and functional immediately after installing Windows. The instructions are provided in this Microsoft Article.

Changing the Product Edition or Installing Windows 8 without a Product Key: If you want to change which edition of Windows 8 is being installed, and/or install Windows 8 without having to enter a valid Product key during Windows Setup, you can use the following method.

1. You will need an ISO image of any version of Windows 8, such as the one which you can create using the 'Install by creating media' option of the Windows 8 Upgrade Assistant's web setup method.
2. Extract the ISO file contents to an empty directory, using an archival utility such as 7-Zip or WinRAR.
3. Go to the *Sources* folder of the extracted ISO contents.
4. Create a new text file by right-clicking in an empty area of the directory and selecting New>Text Document, then rename this text file to *ei.cfg*.
5. Open the ei.cfg file with a text editor such as Notepad, and add the following lines to it:

```
[EditionID]
Core
[Channel]
Retail
[VL]
0
```

6. Under `[EditionID]`, in place of `Core`, you can use `Pro` for Windows 8 Pro, or `Enterprise` for Windows 8 Enterprise. Under `[Channel]`, in place of `Retail`, you can use `OEM`. Finally, under `[VL]`, you can instead use `1` instead to indicate a Volume License version.
7. If your *ei.cfg* file only has the `[Channel]` section, then during Windows Setup you will be prompted as to which edition you wish to install, and when you reach the end, you will be prompted for a Product Key, but can choose to Skip this step and finish installation with a Default Product Key.

Once you have modified *ei.cfg* as appropriate, to successfully recreate a working Windows 8 installation image you will need to use a tool which allows you to make a bootable ISO. This is important, because if the ISO is not bootable it won't work. There are several methods for attempting this, such as using the DISM tool. But in general you should be able to use the free ImgBurn utility to create a bootable ISO relatively simply by following the instructions provided here.

The main use for the method above is if you want to test out a particular version of Windows 8, but note that if a Default Product Key is used to install Windows, it will not activate and will go into a restricted usage mode. Otherwise the method above is unnecessary, because as long as you enter a legitimate Product Key during Windows Setup using any Windows 8 media, it will automatically determine the correct product edition to install and will activate automatically during installation.

USB Flash Drive Windows 8 Installation: If you wish to make working Windows 8 installation media - whether modified or unmodified - the easiest way is to use the Windows 8 Upgrade Assistant's web installation method. This allows you to create an ISO file or USB flash drive image of Windows 8 for later use.

If you can't use the Upgrade Assistant method, but you have a Windows 8 ISO file, then you can use the free Windows USB/DVD Tool originally created for Windows 7 to make a USB flash drive version.

If you only have a Windows 8 DVD and want to create a USB flash drive version, then you can use the method below.

The first step is to make sure that the USB flash drive is bootable by following these instructions:

1. Insert your USB flash drive, and backup any existing data on it as it will all be erased in Step 4 below.
2. Open an Administrator Command Prompt and type the following, pressing Enter after each command:

   ```
   Diskpart
   list disk
   ```

3. Determine the disk number for your USB flash drive based on its size, then type the following and press Enter:

   ```
   select disk [disk number]
   ```

4. Type the following to clean the existing contents of the drive, create a single Primary partition, and select that partition and make it active. Press Enter after each command:

   ```
   clean
   create partition primary
   select partition 1
   active
   ```

5. Type the following to format the drive and press Enter. Note that either NTFS or FAT32 can be used after the `fs=` command, but FAT32 is the most widely compatible, hence is recommended, as some procedures (e.g. flashing a motherboard BIOS) require a FAT32 formatted USB flash drive to work:

   ```
   format fs=FAT32
   ```

6. Once the format procedure is complete, type the following and press Enter to automatically assign a drive letter to your USB flash drive in Windows. Note that you can change this drive letter by using the Disk Management utility as covered under the Disk Management section of the Drive Optimization chapter.

   ```
   assign
   ```

7. You can now type `Exit` to close Diskpart, and then close the Command Prompt.

At this stage, you cannot simply attach the USB device and boot into Windows or DOS mode from it. It requires a boot image of some kind to be truly bootable. To create a Windows 8 installation image to boot up from, follow the steps below:

8. Extract the contents of your Windows 8 DVD or ISO across to a temporary folder on another drive.
9. Make any modifications if desired, and then copy all of these files to the USB flash drive.
10. Set your BIOS/UEFI to boot from a Removable Device, USB drive, or similar option. Check your motherboard documentation for details.
11. Connect the USB drive and reboot, and Windows 8 setup should automatically boot from the USB drive and begin as normal.

Finally, be aware that Windows 8's image-based installation system means that you are potentially exposed to malware if you use a downloaded Windows 8 installation image that you have not created. Do not

download or use any untrusted installation images, as aside from legal issues, you could be installing undetectable malware or built-in security vulnerabilities and exploits on your system in the process.

< PREPARING THE DRIVE

Before you can install Windows, you need to think about how best to configure your target drive(s) for optimal functionality to properly meet your needs. This includes considering whether you want to (re)partition or (re)format any of the drives, whether you want to use a RAID configuration, and whether you want to dual boot Windows 8 with an earlier version of Windows or another OS. It is also much better to partition and format a drive prior to Windows installation, though it is still possible to do so after you install Windows. Make absolutely certain to read all of the following information before proceeding with Windows installation.

PARTITIONING

Before doing anything with a drive, you must first Partition it. Partitions are fenced-off portions of a drive, and there must be at least one partition on a drive before it can be formatted and used. You can create multiple partitions if you wish, effectively dividing a single drive into several smaller logical drives of varying size, each with their own drive letter. There are various advantages and disadvantages to partitioning a drive, but it is important to understand that you should never create multiple partitions under the false impression that this improves performance. On a hard drive, the first (Primary) partition is always the fastest, and subsequent partitions are not as fast. On an SSD, partitioning makes no difference to performance, as all partitions can be sought out with equal speed.

In any case, whether SSD or HDD, partitioning does not replicate the performance benefits of having multiple separate drives, such as in a RAID configuration (see further below). On a single hard drive in particular, performance is still limited by how fast the single drive head can seek (move around to read or write) information. It can't be in two places at once, whereas with two physically separate hard drives, each hard drive's head can seek information independently, such as one drive reading program information while the other concurrently reads/writes Virtual Memory information in the Pagefile. Therefore partitioning is useful as an organizational tool, not an optimization procedure.

The main reason you may wish to create multiple partitions on your drive is so that you can install Windows 8 on one partition, and use other partitions for storing personal data, or other operating systems. This way you can completely reformat one partition for example, and the others will be unaffected. Importantly though, partitioning on the same drive is not recommended as part of a valid backup strategy, because drive failure can affect all partitions on a drive - see the Backup & Recovery chapter for details.

If you're not certain of how many partitions you wish to use, it is useful to know that Windows 8 allows you to create, delete and resize partitions from within an existing installation of Windows at any time, so you are not locked into a particular partition configuration on your drive once you've installed Windows. If in doubt, start with one partition, and you can always change this within Windows later on.

Creating Partitions

Before installing Windows, you must make sure that the target drive is partitioned. You can do this during the Windows Setup procedure as covered later in this chapter, but it is recommended that you partition and format your drive prior to entering Windows Setup. The reason for this is that a drive partitioned and formatted within Windows Setup will result in the automatic creation of a separate System Reserved Partition (typically 350MB in size), necessary for the BitLocker Drive Encryption utility, and which also holds Recovery and boot data.

To prevent the creation of this extra partition, I recommend using the Diskpart command. You can use this command in the Windows Recovery Environment prior to Windows installation. Boot up your system with the Windows 8 installation media, then at the main installation screen, select your language and keyboard layout, then click Next. On the next screen click the 'Repair your computer' link at the bottom. on the Advanced Startup screen, click the Troubleshoot option, then click 'Advanced Options' and select 'Command Prompt'.

At the prompt, type the following, pressing Enter after each line:

```
Diskpart
list disk
select disk [disk no.]
```

The commands above start the Diskpart utility, list the available disks on your system, and you can then specify the particular disk you wish to partition (e.g. `select disk 0`). If there are existing partition(s) on the drive, you can delete them as follows by repeatedly running through the three commands below:

```
list partition
select partition [partition no.]
delete partition
```

The following command creates a primary partition of any size in MB (e.g. `create partition primary size=51200` to create a 50GB partition), or if you leave the size parameter out, it uses the entire drive for the primary partition. That is, just enter `create partition primary` to partition the entire drive as a single primary partition:

```
create partition primary [size=MB]
```

Once the partition has been created, you can then format it:

```
format fs=NTFS
```

The `fs` value above can be `=FAT32` if you wish rather than NTFS, though NTFS is strongly recommended. If you created more than one partition, you will need to use the following commands instead:

```
select partition [partition number]
active
format fs=NTFS
```

Once completed, you can exit the Diskpart utility and then the Command Prompt by typing:

```
exit
exit
```

Restart your PC and commence installation of Windows 8 as normal.

Altering Partitions Within Windows

You can repartition a drive on an existing installation of Windows 8 at any time using the built-in Computer Management features. To add or resize partitions in Windows follow these instructions:

1. Open the Administrative Tools component of the Windows Control Panel and launch Computer Management.
2. In Computer Management, click the 'Disk Management' item in the left pane.
3. In Disk Management, select the drive from the list at the top of the screen.
4. If there is no space marked as Unallocated available, right-click on the drive and select 'Shrink Volume'. This will allow you to reduce the size of an existing partition, freeing up space for new partition(s) to be made.
5. In the dialog box which opens, enter the amount in MB that you want to use for the new partition(s); the maximum amount available is the amount of free space left on the drive.
6. When done, click the Shrink button and the existing partition will be reduced by the amount you chose above, and a new Unallocated partition will be shown.
7. You can create new partition(s) in any Unallocated space on the drive by right-clicking on it and selecting 'New Simple Volume', then following the prompts to assign a particular amount of space and a drive letter to the new partition, and format it as well if you wish.

There are a range of other functions possible under Disk Management, but these are covered in more detail under the Disk Management section of the Drive Optimization Chapter.

GParted

If you want to undertake more complex partitioning of your drive, you can use the free GParted tool. It is not a Windows-specific tool, but it supports all Windows file systems and works with Windows 8. It is not documented here as it is quite detailed in functionality, and recommended for more advanced users. Refer to these instructions if you wish to learn more.

In general I recommend having a single primary partition for Windows and your data, as this keeps things simple and performance will be optimal. For proper data separation and genuinely improved performance I recommend using two or more physical drives instead. This may be more expensive, but it noticeably improves performance, especially during multi-tasking, and also allows the use of a much more foolproof backup and recovery strategy.

As noted, if you partition your drive within Windows Setup, Windows 8 may automatically create an additional System Reserved Partition during installation. This partition is primarily for BitLocker Drive Encryption, as well as for storing the Recovery Environment and boot files. It should not be manually deleted. For more details on this partition, see later in this chapter, as well as the System Recovery section of the Backup & Recovery chapter.

There are also several partition-related optimization procedures you can undertake on hard drives and SSDs. See the Drive Optimization chapter for more details.

FORMATTING

A drive needs to be Formatted before it can be used to store data. As covered under the Backup & Recovery chapter, hard drives in particular are low-level formatted at the factory, and this does not need to be done again. However a high-level format is usually required on any type of drive to set up a file system on it and create an appropriate boot sector, and this is most commonly what the term format refers to. Note that the format command has changed from the one used in Windows XP, as detailed in this Microsoft Article. Formatting a drive in Windows 8 automatically deletes all of the drive's contents and zero-fills it.

Furthermore, you will usually have the option of formatting the drive using a Quick format method. Choose this Quick option if you want a fast zero fill with no real error checking. Otherwise use the default full format option to both zero fill and error check the drive to ensure optimal data integrity.

There are several ways to format a drive in Windows:

§ Open File Explorer, right-click on the drive of your choice and select Format.
§ For more detailed control over formatting, partitioning, volume labels, drive letters and so on, in Windows Vista or 7 go to Start>Search Box, type *computer management* and press Enter, then in the Computer Management window select the Disk Management item in the left pane. In Windows 8, type *disk management* on the Start Screen, select Settings and press Enter. See the Disk Management section of the Drive Optimization chapter, as well as further below, for more details of this functionality.
§ From any Command Prompt, use the Format command. Type `Format /?` for help.
§ Boot up your PC from the Windows 8 installation media, begin the installation of Windows 8, select a Custom Install, then highlight a drive or partition in the selection window and click the Format option.

Whichever method you choose, I strongly recommend doing a full format of a hard drive before installing Windows. This will ensure that data is only written to error-free portions of the drive. On an SSD, a Quick Format combined with a Secure Erase is recommended instead - see the Solid State Drive section of the Drive Optimization chapter for details.

Note that if the drive is not partitioned yet, you will not be able to do a format.

File System

If you choose to format a drive, you will typically be presented with the option of choosing the File System to use:

§ *NTFS & FAT 32:* The common choice in the consumer versions of Windows 8 is either an NTFS (NT File System) or FAT (File Allocation Table) file system. The file system used on a drive determines how the drive will store and organize data, so it is an important choice. You can see a comparison of the two file systems in this Microsoft Article. Windows 8 actually uses an enhanced version of NTFS called Transactional NTFS, which allows it to perform single and multiple file operations more securely and with greater data integrity. This newer version of NTFS was introduced in Vista, and allows other changes, such as Directory Junctions and improved searching. See the File Explorer and Windows Search chapters for details. Much of the advanced functionality in Windows 8 will only work on drives formatted with NTFS.
§ *exFAT:* Windows 8 supports the exFAT (Extended FAT File System), designed for flash drives and portable devices. However because it is a more recent proprietary format, it does not have the same level of compatibility that NTFS and FAT have with versions prior to Windows 7. This may cause problems if you wish to connect your drive to systems using older versions of Windows.
§ *ReFS:* A newer and more advanced version of NTFS, known as Resilient File System (ReFS), is currently only available on Windows Server 2012.

For standard non-removable drives, I strongly recommend choosing the NTFS format. This ensures full support for all of Windows 8's features, as well as optimal performance and security. The only reason for using the FAT32 file system on a drive or partition would be for compatibility purposes, such as if you wish to install another OS on it.

For USB flash drives, I recommend using FAT32, as this ensures that you can use them for a range of tasks, such as flashing a BIOS, or transferring data between systems using various operating systems.

If you want to convert an existing FAT32 drive or partition to NTFS, it is strongly recommended that you backup the data on it and reformat the drive in NTFS for optimal performance. However if that is not possible, you can convert an existing FAT32 drive/partition to NTFS without reformatting by using the instructions in this Microsoft Article. Conversely, if for any reason you want to convert an NTFS drive/partition to FAT32, you can only do so by reformatting that drive/partition, as covered in this Microsoft Article.

RAID CONFIGURATION

RAID (Redundant Array of Independent Disks) is a common method of configuring multiple drives to perform better and/or provide protection against data loss. There are various RAID levels available, and these are demonstrated in this RAID Article. Click a number to see that type of RAID level demonstrated graphically by clicking the diagram. The most common configurations are RAID 0, RAID 1, RAID 5, RAID 10 and RAID 0+1.

To set up a RAID array, you need two or more drives of the same type, whether HDD or SSD, preferably of the same size and speed, and a motherboard with RAID support. You will then need to install the drives in your system as normal and configure the appropriate RAID options in your motherboard's BIOS/UEFI - see your motherboard manual for instructions. If your motherboard supports RAID, and most motherboards do, then there is no additional hardware required, it is all driven by the motherboard and Windows. Once configured correctly, a RAID configuration of multiple drives will always be seen as a single drive by Windows, and treated as such.

To determine which RAID configuration best suits your needs, you will need to read the articles linked above, and then consider your most common PC tasks. For the average user the most commonly used RAID array is a pair of identical drives in RAID 0 formation, which provides the best all-round performance at minimal cost. RAID 0 usually beats a single drive configuration in terms of speed, particularly for large file movements, due to there being two drives independently seeking portions of the data, in place of just one. However RAID 0 also provides absolutely no fault tolerance at all, and in fact doubles the chance for data loss. If one of the drives suffers a serious error or is damaged, you lose all of the data on both drives since the data is split evenly (striped) across them. If you require proper protection against data loss, combined with good desktop performance, you should consider a RAID 5 or RAID 10 configuration which is more costly, but far safer.

While setting up striped RAID arrays - that is, RAID arrays which split data evenly across two or more drives (such as RAID 0 or RAID 5) - you will need to determine a Stripe Size, which is the smallest unit of data allocation to be used in your RAID array. In general, if you are uncertain of the size to choose, use the Auto setting if available, or select a 64kb stripe. If you use the drives primarily for gaming, I suggest a smaller stripe size such as 16kb, even for SSDs, as this can assist in reducing/eliminating stuttering.

Once you have connected your drives and set up your RAID array using the options in the motherboard's BIOS/UEFI, you may need to have a disc or USB flash drive handy with the correct RAID drivers prior to starting the Windows 8 installation procedure. You will need to initiate a Custom Install, and on the setup screen where you select which drive to install Windows onto, if your RAID drives are not shown as a single logical drive with the correct size and volume name, you will need to click the 'Load driver' link, insert a disc or connect a device with the appropriate SATA/RAID driver, load up the relevant driver, then click Refresh on the drive selection screen. If you miss this step, the RAID drives may not be correctly detected as one large drive, and you will not be able to install Windows on them properly, or you will break the RAID array.

Once Windows is successfully installed on your RAID drives, from that point onwards there are no special considerations as such; the drives are treated as one large normal drive for all intents and purposes. Always keep in mind though that under certain RAID configurations such as RAID 0, a single faulty drive can see the loss of all of your data on any of these drives.

STORAGE SPACES

If you don't wish to use the RAID options on your motherboard as covered above, or don't have the hardware to support its use, or have already installed Windows and don't want to reformat and re-setup your system for RAID, then there is another alternative which you can use.

Windows 8 introduces a new feature called Storage Spaces, which is very similar to RAID. The main aim of Storage Spaces is much the same as RAID: to merge multiple physical drives together into a single pooled logical drive under Windows, and to provide data redundancy options so that your data is protected should any one of these physical drives fail. The main benefit of Storage Spaces as compared to hardware RAID is that you can combine a mixture of drive types, including HDDs, SSDs and USB flash drives of varying capacity and speed, and pool them together seamlessly. There's no need to worry about motherboard support for RAID, or altering any BIOS/UEFI options such as stripe size.

You can access the Storage Spaces component under the Windows Control Panel, or by typing *storage spaces* on the Start Screen, selecting Settings and pressing Enter. To create a new storage pool, you must have at least one connected drive, not including your system drive(s). Click the 'Create a new pool and storage space' link in the Storage Spaces window, and select the relevant drives you wish to use for the new pool. Note that you will lose any existing data on any drives used by storage spaces, as they must be cleared before they can be used. The drives should also be formatted in NTFS to use this feature.

Once you have selected the drives to use for storage spaces, the next step is that they are combined into a single pool with any name you wish. A pool is seen by Windows 8 as a single drive. Out of this pool, you can create multiple Spaces, which are similar to partitions, with each space having a name you can assign, along with a logical drive letter. Spaces are an organizational tool, and can also be used to assign data to different redundancy measures as covered further below. You can allocate any size you wish to a storage space, even if it is in excess of the sum of the physical storage capacity of the individual drives in the pool. This is part of the thin provisioning technique used by Storage Spaces, and allows you to add new drives to the pool at any time as required. Windows will simply prompt you to add more capacity if you run out of physical space.

An important step involves selecting a Resiliency (data redundancy) method for each space. This determines how well your data is protected against loss if one or more of the drives in your storage pool physically fails:

- None - Provides no protection against data loss. If one or more of the drives in your pool fails, you may lose some data. This setting provides maximum storage space in return for no protection, and is only recommended if the data in the pool is not important, or you have full backups of the data elsewhere.
- Two-way Mirror - This setting requires at least two separate physical drives in a pool. It provides good protection against data loss by mirroring your data across the drives. That is, at least two full copies of the data are stored on two or more separate drives in the pool. If one of the drives fails, the data is still available from the mirrored copy. Using this option means your data will consume more space as a result, but it is the recommended setting for most people using Storage Spaces as it provides good protection against data loss.
- Three-way Mirror - This is similar to the Two-way Mirror setting above, but requires at least three separate physical drives in a pool. As a result, at least three separate full copies of your data will exist across your drives. It uses even greater storage space than Two-way Mirroring for the same amount of data, but provides greater protection in case of multiple drive failure. It is only recommended if you have very valuable data.
- Parity - Enabling the Parity setting allows Windows to store some redundancy information along with the data, spreading the parity information across your drives in the storage pool. The end result is similar to mirroring as described above, but using less storage space. However Parity requires at least three drives in the pool, and has a higher random I/O overhead (i.e. a negative performance impact). It is best used for spaces which have large files that are valuable, but rarely altered, such as movies.

Windows will notify you if any drive in a Storage Space pool has health issues, or is disconnected. The redundancy option will automatically protect your data and keep it accessible while you address the problem accordingly by replacing the affected drive(s) with a healthy drive, and adding it to the pool under Storage Spaces.

You can allocate different Resiliency methods to each space, so create and organize your spaces accordingly: for example, one space with Three-way Mirror resiliency for your irreplaceable documents; one space with Two-way Mirror for assorted small to medium-sized files; and another space with None or Parity resiliency for digital backups of DVD or Blu-ray movies, to maximize storage space in the pool.

In all other respects, a Storage Space is treated the same as a physical disk in Windows 8, and can be accessed, formatted, even encrypted with BitLocker Drive Encryption if so desired. While Microsoft states that the read performance of a pool in Storage Spaces is similar to RAID 0, it is unlikely to match the read/write performance of hardware RAID options, so it is not recommended in situations where optimal performance is the key consideration. The best use for Storage Spaces is to create a large storage pool for your data and have it suitably protected against loss. It is still not a complete replacement for having other forms of backups as covered in the Backup & Recovery chapter.

DUAL BOOT OR MULTIBOOT

For those who want to consider installing Windows 8 alongside another operating system on the same machine, dual booting or multibooting allows this. For example, you may wish to have your current installation of Windows 7 and a new install of Windows 8 on the same drive, to allow you to slowly transition to Windows 8. Windows 8 will then provide a custom graphical Boot Menu to let you select which OS to boot into each time your PC starts up. Such a configuration does not provide any performance benefits, it is simply designed to allow two or more different operating systems to reside on the same machine, totally isolated from each other.

Note that technically, the Windows 8 licensing agreement specifies that if you wish to dual boot, you will need the System Builder Edition of Windows 8. The license of an Upgrade Edition does not allow for dual booting, as it is designed to just upgrade an existing older version of Windows, not run parallel with it. However, dual booting may still work with an Upgrade Edition.

Basic instructions on how to dual boot with Windows 8 and an earlier version of Windows are as follows:

1. You will need to have the older version of Windows, such as Vista or 7, already installed and on the first drive. This method will not work to multiboot with Windows XP or other operating systems.
2. You will need a separate drive, or another partition on your existing drive, as each operating system needs to reside on its own logical drive. See the Partitioning section earlier in this chapter for details of how to partition a drive.
3. Boot your PC with the Windows 8 installation media, and when prompted, select the Custom Install option.
4. Select the empty drive or new partition on which you wish to install Windows 8.
5. Be aware that when Windows 8 is installed, it will place its boot files on the active partition of the first drive. So if you have multiple drives, the boot files are installed on Drive 0 in the drive list.
6. Continue with Windows installation as normal. As part of the installation of Windows 8, it will create a boot menu which allows you to select which operating system to boot into.
7. You can customize this boot menu by typing *systempropertiesadvanced* on the Start Screen and pressing Enter, then clicking the Settings button under 'Start-up and Recovery'. Here you can select how long to display the boot selection menu (if at all) and which operating system will load up by default.

To multiboot with other operating systems, see this Dual Booting Guide. For more advanced boot menu customization, you can use the EasyBCD utility covered in the Boot Configuration chapter.

Keep in mind that if your older version of Windows is the active partition on the first boot drive, then it will be altered to include Windows 8's boot manager files. If you delete or damage these boot files, or you remove the older OS, or reformat that partition or drive, then you will need to run the Automatic Repair function of the Windows Recovery Environment to fix Windows 8's boot configuration, otherwise Windows will not bootup properly. See the System Recovery section of the Backup & Recovery chapter for details. Also see the Boot Configuration chapters for other methods of troubleshooting and fixing boot-related issues.

< 32-BIT VS. 64-BIT

The final choice to make is whether you install the 32-bit (also called x86) or 64-bit (also called x64) version of Windows 8. On a system which supports 64-bit processing, a 64-bit operating system allows the handling of larger amounts of system memory more efficiently; the computer can store more data in its temporary working area, which can potentially improve performance under certain scenarios, particularly when using data-intensive programs. While 64-bit computing is not a necessity, the move from 32-bit to 64-bit computing is inevitable as data size increases. For full details of 64-bit computing see this Wikipedia Article.

Before deciding on which version to install, consider the following points:

Your PC hardware must support 64-bit processing. Windows 8 64-bit only runs on a 64-bit capable CPU. Fortunately, all CPUs released in the last few years are 64-bit capable. See the System Specifications chapter for details of how to determine your CPU's specifications and abilities. For example, using CPU-Z and checking under the Instructions section of the main CPU tab, you should see a 64-bit related instruction set such as EM64T or AMD64 listed if your CPU supports 64-bit. The easiest way to check is to use the free SecurAble utility which does not require installation. Simply download and run the small file and you will see in the 'Maximum Bit Length' field whether your CPU supports 32 or 64 bits.

You should use 64-bit Windows if you have 4GB or more of system RAM installed. This is because a 32-bit OS cannot properly make use of 4GB or more of RAM. If for some reason you still choose to install a 32-bit OS on a system with 4GB or more of RAM, you must use the Physical Address Extension (PAE) option as covered under the Boot Configuration Data section of the Boot Configuration chapter.

If you run the Windows 8 installation process from the Windows 8 Upgrade Assistant web installer, or from installation media created by that installer, then it will automatically match the Windows 8 platform with that of your current version of Windows, without giving you the option to select 32-bit or 64-bit. For example, if you are currently running Windows 7 32-bit and upgrade via the Windows 8 Upgrade Assistant, then it will automatically download and install, or create install media for, Windows 8 32-bit without giving you a choice. So it is important that if you want to switch from 32-bit to 64-bit (or vice versa), that you use a retail Windows 8 package which explicitly contains both the 32-bit and 64-bit versions, or specifies the exact version that you require (e.g. Windows 8 Pro Upgrade 64-bit).

Windows 8 64-bit requires that all device drivers be designed specifically for 64-bit and that they be digitally signed. Windows 8 64-bit cannot use 32-bit drivers, and can only use unsigned drivers with a tedious workaround at each bootup. For most recent hardware this shouldn't be a problem, as your manufacturer will usually have a signed 64-bit driver available. However some older or less popular hardware may never receive 64-bit drivers and/or signed drivers. Check your hardware manufacturer's website to ensure that an appropriate signed 64-bit Windows driver is available for all of your major hardware components. See the Windows Drivers chapter for more details.

Finally, some general points:

§ You are only licensed to use one version of Windows 8 at a time - either 32-bit or 64-bit - not both. If you have a retail edition which has both versions, you cannot install both of them on different drives or partitions at the same time.
§ You cannot perform an in-place upgrade from 32-bit to 64-bit of any version of Windows (or vice versa). This does not mean that you cannot upgrade from 32-bit to 64-bit, it just means that you will have to do a Custom (clean) Install if you want to go from an existing Windows 32-bit installation to Windows 8 64-bit.
§ The 64-bit version of a program may provide improved performance under Windows 64-bit compared to its 32-bit counterpart.
§ Windows 8 64-bit has added security over its 32-bit counterpart. See the Security chapter for details.
§ Windows 8 64-bit does not support 16-bit programs, so if you use very old 16-bit programs you may have to opt for Windows 8 32-bit instead.
§ Windows 8 64-bit can support all 32-bit programs, usually with no problems or performance degradation, nor any need to customize anything. A few 32-bit programs may experience compatibility issues or have impaired functionality under Windows 8 64-bit, or require specific customization, but this quite rare.

It is recommended that anyone with a modern PC choose Windows 8 64-bit. Unless you have hardware for which appropriate 64-bit drivers are not available, or you use programs which you know are not supported under 64-bit, the choice of 64-bit Windows is optimal in all respects. In fact if you have more than 4GB of RAM, Windows 8 32-bit should not be installed, as doing so will result in much of the memory effectively being wasted. The level of support for 64-bit Windows has grown dramatically in the past few years, and this is primarily because of the fact that 64-bit computing is a logical evolution of 32-bit computing, and must occur as programs become increasingly more complex and data-intensive. Rapid adoption of 64-bit Windows starting with Windows Vista has ensured that driver and program support is now excellent.

If you choose to install Windows 8 64-bit, there will be few if any noticeable differences between it and the 32-bit version on the surface. Most of the differences are not obvious to users; the most prominent differences users may notice are:

§ In File Explorer you will see both a *Program Files* directory, and a *Program Files (x86)* directory. The main Program Files directory is for native 64-bit programs, while the (x86) version of the directory is for 32-bit programs. Windows will determine which directory to install a program in automatically. In fact it makes no practical difference which directory a program is installed to, it will work regardless, so if given the choice, and you're not clear on whether a program is a native 64-bit application, simply choose the *Program Files (x86)* directory.
§ In File Explorer you will see a \ *SysWOW64* directory under the *Windows* directory. WOW64 stands for Windows 32-bit on Windows 64-bit, and it handles the emulation of a 32-bit environment for non-64-bit applications. You do not need to manually install or alter anything in this directory, nor do anything for this emulation to function correctly.
§ In the Windows Registry Editor you will see an additional option to create `QWORD (64-bit)` keys. In practice it is not necessary to use this feature unless specifically instructed to do so.
§ In the Windows Control Panel you will see that some components have the (32-bit) suffix. This has no practical impact on their functionality.

For all intents and purposes Windows 8 64-bit looks and feels precisely the same as Windows 8 32-bit, so you should not be concerned about any major changes in functionality or usability if you are switching to 64-bit Windows for the first time. The most important changes are under the hood, and provide the potential for greater performance, security and stability.

< INSTALLING WINDOWS

At this point you should have sufficient knowledge to have made the appropriate choices to be ready to begin the actual installation process for Windows 8. This section details the procedures required to install Windows, but it assumes that you have read the rest of this chapter, as well as the Hardware Management chapter. If you haven't done so yet, please put some time aside to research and make the necessary changes and choices prior to installing Windows 8. There's no point rushing the installation of Windows only to find out that you have to go through it again because you overlooked something, or made a sub-optimal choice.

WEB INSTALLATION

As of Windows 8, you can purchase, download and install Windows all via the Internet. The Windows 8 Upgrade Assistant utility integrates Upgrade Advisor, Windows Easy Transfer and purchasing functionalities. The procedure is detailed in this Microsoft Article. It is the cheapest and easiest method for purchasing and installing Windows 8, and is recommended for most users currently running a previous version of Windows.

When launched, the Windows 8 Upgrade Assistant will first check to see if your system is compatible with Windows 8 and advise you of any potential problem areas that need your action, or which may result in incompatibilities or reduced features. If you wish to continue, you will then see the option to purchase Windows 8, and can follow the prompts to purchase and immediately obtain your Windows 8 Product Key.

The Windows 8 Upgrade Assistant will then allow you to choose whether you want to perform an In-Place Upgrade, carrying across personal files, Windows settings, and programs on your existing installation of Windows, just your personal files, or nothing at all - see the Prior to Installation section earlier in this chapter for details. Once you have selected what, if anything, you wish to carry across from your existing Windows installation, the utility will then download Windows 8 from the Internet, with a progress indicator.

The next step involves determining whether you wish to proceed with installation straight away; to install Windows by creating installation media; or to install later by launching the icon placed on your Desktop. I recommend selecting 'Install by creating media' so that you can create a Windows 8 installation disc or bootable USB drive for later use, especially if you want to install Windows 8 on another partition or drive. Once this option is selected, you will then be able to choose to create media for a USB flash drive, or save an ISO file on your drive which can then be burned to a DVD. This step will require around 3GB of space for the resulting Windows 8 image file.

Finally, be sure to note down your Windows 8 Product Key when shown, and store it somewhere safe.

This web-derived Upgrade Edition of Windows 8 allows you to perform a Custom (clean) Install or Upgrade Install as necessary, so there is no disadvantage to using this method compared to purchasing a boxed retail version of Windows 8. The only requirement is that the Windows 8 Upgrade Assistant must detect a valid installation of Windows XP, Vista or 7. If the Windows 8 installer cannot detect a qualifying earlier version of Windows, you may not be able to install or successfully activate your Windows 8, as mentioned in this Microsoft Article.

In practice, once you create the install media in this manner, you should be able to use it to boot up any PC, even one with a completely fresh drive, and install Windows 8 as normal. Should you run into problems, there is a workaround which will allow you to do a full Custom (clean) Install on a brand new or freshly formatted drive, without a previous version of Windows, covered in the Activation section further below.

If you only have a Windows 8 product key and no install media, you can still use a similar procedure to the one above to install Windows 8, as detailed in this Microsoft Article.

A detailed account of the Windows 8 installation procedure is provided in this Microsoft Article. The following steps highlight the key things to consider during the installation of Windows 8, along with any recommendations:

STEP 1 - LAUNCHING THE INSTALLER

There are different ways to trigger the installation of Windows 8 depending on the type of installation that you want:

- *An In-Place Upgrade* - Launch the Web Installation method, or insert and launch the Windows 8 installation media, from within the version of Windows XP, Vista or 7 that you wish to upgrade. If the installer doesn't launch, open the installation media in File Explorer and launch *Setup.exe*. Then during installation, select anything other than Nothing at the 'Choose what to keep' stage.
- *A new system or new drive/partition, or dual boot* - Boot from the Windows 8 installation media. Make sure that you change your BIOS/UEFI boot options to boot first from DVD or USB device as relevant. Select the Custom (Clean) Install option, and then choose the target drive/partition.
- *A clean install on a drive with existing data* - You can use either of the methods above. If given the choice at the 'Choose what to keep' stage, select the Nothing option. Alternatively, if given the choice, select a Custom (clean) Install.

In general, unless you want to install Windows 8 as a relatively straightforward in-place upgrade to an existing version of Windows on the same partition and drive, it is recommended that you boot from the Windows 8 installation media to initiate Windows Setup. This will allow you much greater choice, including the ability to choose the Custom Install option, which provides the ability to specify the target partition or drive, and also presents the formatting and partitioning options if necessary.

STEP 2 - INSTALL UPDATES

During Windows installation, when prompted to 'Go online to install updates now', selecting this option and clicking Next will allow the installer to check for important updates prior to installation. These include any critical updates which have been made available since Windows 8 was first released. If you are connected to the Internet at this time, it is recommended that you allow these updates.

STEP 3 - WINDOWS PRODUCT KEY

When prompted to enter your Windows Product Key (in the format `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`), keep in mind that dashes are entered automatically, and case is not important.

Unlike Windows 7, with Windows 8 you must enter a valid product key before you can continue with installation. The product key is what Windows Setup uses to identify which edition to install. As soon as a valid key is entered, it will automatically be checked and you will be shown whether it is working or not before you can proceed. Only a modified Windows 8 installation image can allow installation without entering a valid product key - see the Prior to Installation section earlier in this chapter.

Windows 8 will automatically activate your product key during the installation process. See the Activation section at the end of this chapter for details.

STEP 4 - CUSTOM INSTALL - ADVANCED OPTIONS

If you have selected a Custom (clean) Install, then you will be given the option to choose the logical drive onto which Windows 8 will be installed. You should see a list of all the detected drive(s) currently connected to your system, displayed in the format: *[Disk #] [Partition #] [volumename] [driveletter].* If the drive(s) are not correctly identified, or are unpartitioned/unformatted, then you will see something like *Disk 0 Unallocated Space* under the drive name. Also check the Total Size and Free Space columns to make sure the size is

correctly identified. Remember though that advertised drive space is different to the way Windows displays it due to a discrepancy between Gigabytes (GB) and Gibibytes (GiB) - see the Bits & Bytes section of the Basic PC Terminology chapter for more details.

On a drive which has already been partitioned and formatted, you will see the following options. On a new drive, you will first need to click the 'Drive Options (advanced)' button.

Load Driver: If multiple drives in RAID formation are not displaying as a single drive, or any drives are showing incorrect sizes, or formatted and partitioned drives are showing up as being unformatted and/or unpartitioned, then your drive(s) are not being correctly detected. You will need to click the 'Load driver' link at the bottom of this box, and then insert or attach an appropriate disc or drive containing the necessary drivers (e.g. RAID drivers) and load all the relevant controller drivers needed. Once done, click the Refresh link at the bottom of the screen and your drives should now be displayed correctly. If they still aren't then you may have to abort installation (click the red X button at the top right of the box) and either download appropriate drivers from your motherboard manufacturer's website and/or check your BIOS/UEFI to see if the drives are detected and configured correctly there. The bottom line is that if Windows 8 does not detect your drives properly at this stage, you will either be unable to install Windows, or the installation will not work as intended, especially if you are attempting to use a dual boot or RAID configuration.

Format, New, Delete, Extend: Format allows you to (re)format the selected drive. This is recommended to clean any drive with existing data. On a hard drive, a full format using the NTFS file system is recommended for ensuring optimal compatibility, performance and data integrity; on an SSD, a quick format using the NFTS file system is recommended. You can also use the New, Delete, and Extend options to (re)partition a drive if you wish, which is necessary for a new drive. See the Preparing the Drive section earlier in this chapter for full details of various considerations in relation to formatting and partitioning.

System Reserved Partition: Importantly, if installing Windows on a blank new drive, or if you manually delete all of the partitions on an existing drive and then repartition it within Windows Setup, Windows may create an additional partition for system files. It will prompt you with: 'To ensure that all Windows features work correctly, Windows might create additional partitions for system files'. This System Reserved Partition will range in size from 100MB to 350MB, and is a hidden partition with no drive letter, created specifically for the BitLocker Drive Encryption feature to hold unencrypted boot files, as well as storing System Recovery and Boot files. There is no harm in letting this partition be created, however if you don't wish to have multiple partitions on your system drive, and you are certain you will not use the BitLocker Drive Encryption feature, then it is best to prevent this System Reserved Partition from being created. This will place the boot files and Recovery Options in hidden folders in the base directory of your system drive.

The way to prevent creation of the System Reserved Partition is to cancel out of any prompts and exit Windows Setup. Then (re)partition and (re)format the drive prior to launching Windows Setup. Windows 8 will not create a System Recovery Partition on a drive with partitions which are already defined before entering Windows Setup, only on a drive where partitions are not defined (i.e. a new blank drive), or drives where the user deletes all partitions and creates new partition(s) within Windows Setup. See the Partitioning section earlier in this chapter for details of how to create a partitioned and formatted drive before entering Windows Setup.

Once your drive(s) are partitioned and formatted the way you want them and are detected correctly, highlight the relevant logical drive to which you want to install Windows 8 and click the Next button. The existing contents of the target logical drive will be lost as Windows 8 installs over it, however if installing Windows 8 over an existing installation of Windows without first formatting that partition, Windows 8 will attempt to save the programs and personal files under a *\Windows.old* directory. This is not a substitute for having prepared a proper backup, and in general I recommend that you format a partition first before installing Windows 8 precisely to prevent any residue from previous Windows installs being carried across.

STEP 5 - PERSONALIZE

During the final stages of Windows Setup, you will be given the option to personalize the color scheme for the Metro environment. This can be set now, or ignored, as it can always be changed within Windows at a later date.

You will also be able to enter a name for your PC. Note that this is not the name for your user account. The computer name is primarily used to identify this particular machine when connected to a network of computers. For the average home user, unless you are on a network, then any name will do. If connected to a network, give the PC a descriptive name. The computer name can also be changed at a later date if you wish.

STEP 6 - EXPRESS SETTINGS

You will be prompted to select whether you wish to 'Use Express Settings' or Customize them at this point. All of these settings can be adjusted within Windows at a later date. If you select 'Use express settings', all of the features listed below, with the exception of those under 'Send Information to Microsoft', will automatically be enabled. It is recommended that you customize them at this point for optimal results.

When you select Customize, the groups of settings you will be walked through are covered below:

- *Network Sharing:* You can choose between 'Yes, turn on sharing and connect to devices', which sets your network type as a Private network, suitable for connecting to trusted home or work networks; or you can select 'No, don't turn on sharing or connect to devices', which sets your network type as a Public network, suitable for connecting to less trusted networks in public locations. If you are not on a home or work network (excluding the Internet), I recommend the second option (No) to start with, as this will prevent installation of unnecessary features such as HomeGroups. See the Network & Sharing Center section of the Windows Control Panel chapter for details.
- *Windows Update:* I recommend leaving the 'Automatically install important and recommended updates' option as is, as well as leaving the 'Automatically get device drivers, apps and info for new devices' set to On here. This will safeguard you against security vulnerabilities, as well as preventing non-working devices, when you first start using Windows 8. However these settings are not my final recommendation. See the Driver Installation section of the Windows Drivers chapter, as well as the Devices and Printers section of the Hardware Management chapter for details.
- *Windows SmartScreen Filter, IE SmartScreen Filter and Do Not Track:* Both SmartScreen Filter options should remain enabled to begin with, and indeed I recommend that they always stay On during normal Windows usage for security purposes. The Do Not Track option of Internet Explorer can also remain enabled to maximize privacy, and generally should stay on from that point onward. See the Windows SmartScreen Filter section of the Security chapter, and the Internet Explorer Desktop section of the Internet Explorer chapter for details.
- *Send Information to Microsoft:* The options in this section are all designed to provide additional feedback and information to Microsoft based on your usage of Windows 8. Microsoft uses this information to improve Windows 8 and the way future versions of Windows are developed. However these options are all Off by default, and none of them need to be enabled if you have any privacy concerns.
- *Windows Error Reporting:* The Windows Error Reporting option controls whether this problem reporting and solution feature is enabled. If you have privacy concerns, disable it to begin with. See the Windows Action Center section of the Performance Measurement & Troubleshooting chapter for more details.
- *Internet Explorer Compatibility Lists:* If enabled, this option allows Internet Explorer to use an online list of websites which have been reported as having compatibility issues with Internet Explorer 10. This list allows IE to automatically switch to Compatibility View when such websites are viewed. It should be fine to leave this option enabled unless you have privacy concerns. See the Internet Explorer Desktop section of the Internet Explorer chapter for more details.

§ *Share Info With Apps:* The 'Let apps use my name and account picture' option, if enabled, allows Metro apps to use your user account name, and any associated picture for your user account, as part of their functionality, to personalize the usage experience. This can be disabled if you wish with no major impact on app functionality. See the Privacy section of the PC Settings chapter for details. The Windows Location Platform option determines whether you allow location tracking by apps. Disabling it will protect your privacy, but may make some apps less useful, as they won't be able to determine your physical location and hence can't customize their output to suit. See the Location Settings section of the Windows Control Panel chapter for details.

If you have privacy concerns about any of these settings, see this Microsoft Article.

STEP 7 - SIGN IN TO YOUR PC

This is an important step, as it involves the creation of the first and default Administrator user account. It also determines whether you use an online-based Microsoft Account for signing into Windows, or a Local Account, which is similar to the user accounts created under previous versions of Windows. The difference between these two account types is covered in detail under the Local Account vs. Microsoft Account section of the User Accounts chapter, and it is recommended that you read that section before deciding which account type to use.

It is strongly recommended that you start off by creating a Local Account. You can always switch between a Local Account and a Microsoft Account at any time in the future. To create a Local Account, instead of entering an email address, click the 'Sign in without a Microsoft Account' link at the bottom of the screen.

The username you enter for this account will be the name of your user account, and the password, if entered, will be the password required to log into the user account, so make sure that you keep a note of it. You do not need to enter a password if you do not want to password-protect your user account; a password can always be added later if you wish. If you do enter a password, the password hint will help you to remember it. For important advice on how to create a secure password, how to remember or store it safely, and how to set up your account recovery methods for maximum security, see the Important Security Tips section of the Security chapter.

STEP 8 - FINISHING INSTALLATION

A few things to keep in mind immediately after installing Windows:

§ Make sure to remove the Windows 8 DVD or disconnect any removable USB installation device before rebooting Windows.
§ Make sure to go into your BIOS/UEFI and reset your main system drive as the first boot device if you had set your optical drive or a removable device as the first boot device for Windows installation purposes.
§ Try to limit general Internet browsing or other online activities until after you've read through the Security chapter.

Windows should be automatically activated and ready to use from this point onward. You can continue reading this book sequentially, or you can skip to any chapter which takes your fancy. I recommend reading the Graphics & Sound, File Explorer, Windows Drivers and Security chapters as soon as possible to cover the key functionality, stability and security-related topics.

If you are having problems activating Windows 8, see the next section.

< WINDOWS ACTIVATION

To confirm that you are running a legitimately purchased copy of Windows 8 in accordance with the terms of the End User License Agreement (EULA), Microsoft relies on Windows Product Activation, better known simply as Activation, which verifies your Windows Product Key, Windows 8 Edition and hardware configuration online. Activation is designed to join your product key to your specific hardware specifications, making sure that your key is valid, and not in use on more systems than the licensing terms allow, which is usually only a single system at any one time for a standard license.

As of Windows 8, the activation process has changed. It now occurs automatically during the Windows installation process, and can't be skipped unless you modify your installation media as covered earlier in this chapter. When you run Windows Setup, you will be prompted to enter your Product Key, which appears as a series of 25 letters or numbers separated by dashes in the format: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX. This key can usually be found on a sticker on your computer if you purchased the PC with Windows 8 pre-installed, in the Windows 8 retail package, or will be provided by the Windows 8 Upgrade Assistant if you purchase Windows 8 online. The product key is very important because it is integral to validating and activating your copy of Windows 8. If the key is used by anyone else at the same time as you, or on another one of your PCs, this will breach your license terms and can invalidate your key for use on any PC. Make sure you keep your product key in a safe place, and do not share it with anyone else.

When activation commences, you will automatically connect to a Microsoft activation server and send several pieces of information that will be stored there as detailed in this Microsoft Article. The information includes:

§ Computer make and model.
§ BIOS/UEFI name, revision number, and revision date.
§ A unique number assigned to your computer.
§ Drive volume serial number (hashed).
§ Windows version and the version of the activation software.
§ Your Windows Product Key, as well as the product ID (hashed).
§ Your region and language settings.

The entire process should take less than a minute. If automatic activation fails, or you are not connected to the Internet, you will be given instructions on how to activate Windows, such as by contacting Microsoft over the phone. If automatic activation succeeds, you will not see any notification, but you can check on your activation status within Windows as covered further below.

You will not be required to reactivate Windows 8 again, unless:

§ You reinstall Windows.
§ You substantially alter the PC's main hardware components, or possibly if a driver or BIOS update makes your key hardware component(s) appear to be different.
§ Your product key is found to be in use by another system, or turns out to be an illegally obtained one.
§ There are signs of system tampering aimed at circumventing the Windows Activation Technologies.

To view your activation status in Windows, go to the System component of the Windows Control Panel, and look at the bottom section. You should see text indicating that 'Windows is activated'. Click the 'View details in Windows Activation' link to see more details. This will open the Windows Activation window, providing details of the activation date, the current edition of Windows that is activated, and the last 5 letters of your product key.

If you want to change your product key at any time, or if you installed Windows using modified Windows 8 installation media, or an Enterprise version, and haven't yet entered a product key, then you should be able to click the 'Activate with a new key' or 'Buy a new key' button in the Windows Activation window.

You can also open a prompt to allow for entering a new product key at any time as follows:

1. Open an Administrator Command Prompt.
2. In the Command Prompt type the following and press Enter:

   ```
   slui 3
   ```

3. Enter a valid product key in the box shown.
4. Click the Activate button.

If you have lost your product key, unfortunately all of the existing utilities to extract a Windows product key from a current install of Windows do not appear to function correctly under Windows 8; the key they display is not correct. This is because Windows 8 has changed the way in which the key is encrypted. The safest way to obtain your product key is to contact your hardware vendor or Microsoft.

For more advanced configuration of activation parameters, you can use the `slmgr` command, which has a range of options. You can see these options simply by typing `slmgr` in a Command Prompt and pressing Enter, or you can view the list in this Microsoft Article.

FAILED ACTIVATION

If you have not activated Windows successfully, you may face some restrictions in Windows 8, including being unable to:

§ Use the interface Personalization options.
§ Connect and synchronize using a Microsoft Account.
§ Download apps via the Microsoft Store.

Furthermore, you may also experience the following:

§ Regular messages reminding you to activate Windows.
§ A Desktop message indicating that Windows is non-genuine.
§ A non-genuine message appears when the Windows Control Panel is launched.
§ The Desktop Wallpaper will turn black.
§ You will not be able to receive optional updates from Windows Update.

You will need to successfully activate your copy of Windows 8 with a valid product key to remove these restrictions and get back to normal. If you were lead to believe your copy of Windows was genuine when you purchased it, contact Microsoft and report the details of where and how you purchased this copy. If you knowingly used an illegal product key or used the key in breach of licensing conditions (e.g. the same key on multiple machines), then you can still obtain a legitimate key and return Windows to normal.

For general problems with activation, see this Microsoft Article and this Microsoft Article for more details.

One of the most common scenarios which results in failed activation is when installing from an Upgrade Edition of Windows 8. As long as the Upgrade Edition was purchased and downloaded on a valid qualifying version of Windows XP, Vista or 7, or the setup process is launched from within such a version of Windows, there should be no problem if you want to reformat your drive or otherwise do a Custom (Clean) Install on it.

Under certain circumstances however, Windows 8 may not be able to detect that you qualify to use the Upgrade Edition, in which case you may have problems successfully activating Windows 8 at the end of the Windows Setup procedure. There are several workarounds to this issue:

If you can reach the Start Screen, try the following method to activate Windows 8:

1. Open Registry Editor and go to the following location:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\OOBE]
   MediaBootInstall=0
   ```

   Change the value of the DWORD above from 1 to 0.

2. Open an Administrator Command Prompt and type the following then press Enter:

   ```
   slmgr /rearm
   ```

3. Reboot your system and you should now be able to enter your Windows Product Key and activate normally via Windows Activation.
4. If you still have problems, open an Administrator Command Prompt and type the following then press Enter:

   ```
   slmgr /ato
   ```

If the method above doesn't work, insert the Windows 8 Upgrade media, launch Windows Setup from within the new install of Windows 8, then do an In-place Upgrade reinstall of Windows 8. Once reinstalled, activate Windows as normal. This is effectively the same as a clean install.

If all else fails, first do a Custom (clean) Install of an earlier version of Windows on the drive, then you will be able to do a Custom (clean) Install of Windows 8 onto it.

Bear in mind that these workaround methods for installing an Upgrade edition on a new system or a newly formatted drive are only legal if you actually own a valid version of Windows XP, Vista or 7.

If you continue to have problems with Windows installation or activation, the only correct course of action is to contact Microsoft Technical Support for your particular country.

BOOT CONFIGURATION

Windows 8, just like Windows 7 and Windows Vista, has a substantially different boot configuration than earlier versions of Windows. Instead of using a simple *Boot.ini* file as in Windows XP, Windows 8 has a special Boot Configuration Data (BCD) database to hold all of the relevant bootup parameters, and to allow compatibility with newer bootup methods.

Windows 8 takes the complexity even further by altering the boot process from that used in Windows Vista or 7, as covered in this Microsoft Article. The most noticeable change is that the Windows 8 boot menu, which appears if multi-booting, or accessing troubleshooting options, now provides a graphical interface rather than a text-based one. The biggest change however is under the hood, and involves altering the boot sequence to provide both greater security and enhanced speed on the latest systems with UEFI. The practical result is a series of changes in the way Windows looks and acts during bootup, and in the available options for interacting with the bootup sequence.

This chapter examines the Windows 8 boot process, focusing on customization and troubleshooting. The information is particularly relevant if you ever need to resolve a startup-related problem, attempt to use 4GB or more of system RAM on 32-bit Windows, or modify or repair a multiboot setup. Fortunately, for basic boot-related problems, the Automatic Repair utility in the Windows Recovery Environment is the quickest and easiest method to resolve any bootup issues, and is covered under the System Recovery section of the Backup & Recovery chapter.

< BOOT FILES

The Windows 8 boot configuration is held in a hidden *\Boot* folder, along with the *bootmgr, BOOTNXT* and *BOOTSECT.BAK* files. This folder and all the files are required for Windows 8 to boot up correctly, and they should never be manually deleted.

If your drive has a small 350MB System Reserved Partition which was created when installing Windows 8, then the boot files and folder will be located there. This partition is part of the requirement for BitLocker Drive Encryption, since the boot files cannot be encrypted if they are to be read properly at startup, so they are stored separately as unencrypted files on another partition.

The System Reserved Partition is hidden by default and is not assigned a drive letter. You can check for the presence or otherwise of the System Reserved Partition on your drive by going to the Windows Control Panel, opening the Administrative Tools component, launching the Computer Management tool and clicking the 'Disk Management' item in the left pane. It will be shown as a separate 350MB System Reserved partition with no drive letter. You can prevent its creation during installation if you wish. See the Installing Windows section of the Windows Installation chapter for more details.

If you don't use BitLocker, and have successfully prevented the System Reserved Partition from being created during installation, then the boot files and folder will be located in the base directory on the primary partition of your system (boot) drive, which is recommended. However if the System Reserved Partition has already been created on your drive, then you should not attempt to remove it, as this can render your system unbootable.

< ACCESSING THE BOOT MENU

Windows 8 has improved startup time on most PCs compared to previous versions of Windows. The greatest benefit in boot speed can be found on newer PCs which use UEFI instead of the legacy BIOS - see the Hardware Management chapter for more details on UEFI. On some UEFI-based systems, Windows 8 can go from powering up to the Lock Screen in a matter of seconds, as covered in this Microsoft Article.

The problem is that this rapid startup doesn't allow for easy access to advanced Windows bootup options using methods like pressing a particular key during startup (e.g. repeatedly pressing the F8 key). There is only a 200 millisecond (1000 milliseconds = 1 second) window during which such keystrokes can be read on some UEFI systems, so it is extremely difficult to register the right keypress at the right time.

Fortunately there are several ways to access the boot menu options in Windows 8:

§ If you are unable to boot into Windows, then you should automatically see the boot options menu appear the next time Windows attempts to boot up. In cases where you are able to boot into Windows but can't proceed any further for some reason, you should repeatedly reboot Windows. This prompts Windows 8 to determine that there is a startup problem and it will then automatically display the boot menu or run the Startup Repair Tool as appropriate.
§ On a legacy BIOS system you can access the boot menu screen by continually pressing the F8 key during Windows startup until the boot menu options appear.
§ On a UEFI system, as well as on legacy BIOS systems, you can force Windows to open the boot options menu at next startup by going to the Settings charm, selecting 'Change PC Settings', and under the General section, clicking the 'Restart Now' button under the 'Advanced Startup' section. The PC will begin to shutdown, but just before physically resetting your machine, the boot menu options will appear. You can then select an appropriate choice, and your PC will reboot with your chosen option.
§ The quickest option on any system is to open the Charms menu, select Settings charm, click on the Power option, then hold down the SHIFT key and select Restart. Note that this method also works for the Power option accessible at the bottom right of the Login screen, and in any other places as well.
§ From a Command Prompt, you can use the following command and press Enter:

```
shutdown.exe /r /o
```

Once at the boot menu, the basic features are self-explanatory, and the rest are covered in detail under the System Recovery section of the Backup & Recovery chapter.

< SECURE BOOT

This is a new feature of Windows 8 which only works on PCs with UEFI, not those with legacy BIOS. It is designed to ensure that the system remains secure against boot loader malware, which can bypass Windows security by silently gaining control of the system before Windows even has a chance to load. Secure Boot is enabled by default on PCs and devices certified for Windows 8. It does not allow any unauthorized boot loaders to run; only loaders which are verified by the UEFI as being authorized with a proper security signature, checked against an internal firmware database of allowed signatures, will be able to boot at startup. You may have the option to disable Secure Boot in the UEFI, as that is the only place where it can be adjusted. For more details, see the Secure Boot section of the Security chapter.

< BOOT CONFIGURATION DATA

The Boot Configuration Data store contains the parameters which determine which operating system will boot, as well as any other options which need to be passed onto the system at startup. There are several ways you can view and modify your Windows 8 BCD, each covered below.

BCDEdit

BCDEdit is a built-in command line tool for altering the boot configuration in Windows 8. To use it, open an Administrator Command Prompt and type `bcdedit /?` for a full list of commands. Just typing `bcdedit` by itself will provide you with a list of your system's current boot parameters.

An example of using BCDEdit, along with the `bootmenupolicy` parameter, is provided below.

If you find that the Windows 8 graphical boot menu has changed to a Windows 7 or earlier text-based menu, and Windows 8 is already set as your default OS, this can be fixed using the following BCDEdit command:

1. Boot into Windows 8.
2. Open an Administrator Command Prompt.
3. Enter the following and press Enter:

```
bcdedit /set {current} bootmenupolicy Standard
```

4. Ensure that Windows 8 is set as your default OS. You can do this by typing *systempropertiesadvanced* on the Start Screen and pressing ENTER, clicking the Settings button under 'Startup and Recovery', and choosing Windows 8 in the 'Default operating system' drop box'.
5. Reboot.

Conversely, if you want to switch back to a text-based menu, first try setting another OS as the default if multi-booting, and if that doesn't work, use the following command:

1. Boot into Windows 8.
2. Open an Administrator Command Prompt.
3. Enter the following and press Enter:

```
bcdedit /deletevalue {current} bootmenupolicy
```

4. You can set Windows 8 as the default OS if you wish as it won't affect this procedure.
5. Reboot.

Given it is a complex tool to use, BCDEdit cannot be covered in detail here. I strongly suggest using the other methods covered below to edit your boot configuration instead, at least to start with. Only turn to BCDEdit if you have no other option, and only after appropriate research. It is very risky to manually edit your boot configuration without proper knowledge.

Startup and Recovery

The easiest method to alter your basic Windows bootup-related options is to go to open the System component of Windows Control Panel and click the 'Advanced system settings' link on the left side, or type *systempropertiesadvanced* on the Start Screen and press Enter. Once in the System Properties window, click the Settings button under the 'Startup and Recovery' section of the Advanced tab.

In the Startup and Recovery window, under 'System Startup' if you want a Boot Menu to be shown when your PC first loads, tick the 'Time to display list of operating systems' box and in the box next to it choose how many seconds you want the Boot Menu to remain on screen before it automatically loads up the default OS. If you only have a single operating system listed (i.e. Windows 8), then this boot menu is unnecessary.

The 'Time to display recovery options when needed' box should always be ticked. Enter a reasonable amount of time, such as 15 or 30 seconds. The Recovery Options menu will only appear if you run into

problems with Windows, and its features are covered under the System Recovery section of the Backup & Recovery chapter.

For details about the System Failure settings, see the Windows Memory Management section of the Memory Optimization chapter.

MSCONFIG

Another relatively straightforward way to alter the boot configuration is to use the Microsoft System Configuration utility (MSConfig). Type *msconfig* on the Start Screen and press Enter. Go to the Boot tab of MSConfig and you will see under the 'Boot Options' section there are several options for altering the way your PC boots up. These are primarily used for troubleshooting purposes. Highlight the installation of Windows you wish to alter, then you can select one of these options to apply to it:

Safe Boot: If ticked, the next boot will be into Safe Mode, rather than the normal Windows environment. Default safe mode is called Minimal; 'Alternate Shell' is safe mode with command prompt instead of a GUI; 'Active Directory repair' is safe mode with GUI and active directory; Network is safe mode with GUI and networking features enabled. See the System Recovery section of the Backup & Recovery chapter for details on safe mode.

No GUI boot: If ticked, this option removes the default Windows 8 startup screen when booting up, and replaces it with a black screen until you reach the Windows welcome screen.

Boot log: If ticked, records all of the drivers which Windows did or did not successfully load up during bootup, and saves it in a logfile stored under your *\Windows* directory as *ntbtlog.txt*.

Base video: If ticked, boots up Windows using the default Windows graphics driver rather than any third party graphics driver for your graphics hardware. This is useful if a recent graphics driver installation is preventing you from booting up, or you are seeing graphical corruption as Windows loads.

OS boot information: Shows the names of all the drivers on screen as they are being loaded during bootup.

Timeout: This box is the same as the 'Time to display a list of operating systems' setting covered under the Startup and Recovery section further above. It controls how long the boot menu for operating system selection is shown, and hence is only relevant if you more than one operating system installed.

Make all boot settings permanent: By default, Windows will apply any boot changes you have made in MSConfig at next bootup, and from that point onward. If you have made any changes to your startup configuration, the 'Startup selection' type under the General tab of MSConfig will change from 'Normal startup' to 'Selective startup'. You can undo your changes simply by selecting 'Normal startup' at any time. However, if you make any changes, and tick the 'Make all boot settings permanent' box and click Apply, MSConfig will not track your changes, and hence you will not be able to easily undo them by selecting 'Normal startup' as described above. You will have to manually alter them, retick this box and click Apply to revert the changes. In other words, do not tick this box after making any changes unless you are certain that you want to keep a particular change made in MSConfig.

If you click the 'Advanced Options' button you will see more advanced bootup options which are only useful for troubleshooting purposes:

Number of processors: If you have a multi-core CPU, ticking this option allows you to manually force some or only one of the processors (cores) on the CPU to be detected and used by Windows during bootup. This is not a performance option, it is designed only for troubleshooting by artificially limiting the maximum number of cores on your CPU being used in order to determine if there is a fault with one of them. The

default setting of having this box unticked is optimal, as it allows all of your cores to be used if needed, and prevents any potential problems.

Maximum Memory: This option allows you to manually force Windows to only use a certain amount of RAM on your system, up to and including your full physical RAM amount, for troubleshooting purposes. The amount entered is in Kilobytes (KB).

PCI Lock: This option stops Windows from dynamically assigning system resources to PCI devices. The devices will use the BIOS configuration instead. Of no practical use to most users.

Debug: If ticked, this option starts Windows in debugging mode. Ticking this option also ungrays a range of additional options as to where to write the debug output, such as to an external port or USB device. Again, of no practical use to most users, as it requires specialist knowledge to interpret debugging output.

Once done selecting which bootup options you wish to apply to the boot configuration, click the Apply button at the bottom of MSConfig and these option(s) will come into effect from the next boot onwards. Remember, unless you have ticked the 'Make all boot settings permanent' option, the quickest way to undo any of your changes in MSConfig is to go to the General tab and select the 'Normal startup' option.

The other useful aspects of MSConfig are covered under the Startup Programs and Services chapters.

EASYBCD

EasyBCD is a tool you can use to make complex changes to your boot configuration in a user-friendly manner. EasyBCD is free for personal use, but requires registration before you can download it. Once EasyBCD is installed and launched, before altering anything first backup your existing Bootloader settings so they can be easily restored if required. Click the 'BCD Backup/Repair' button, then click the 'Backup Settings' button to create a backup .BCD file in the directory of your choice.

EasyBCD has a range of functions, but only the major features are covered below.

On the main 'View Settings' screen you can see a summary of the bootloader data held in the BCD. You can view this in simple (Overview) mode, or if you prefer the raw data, select the 'Detailed (Debug Mode)' option. The information here is useful for confirming the basic parameters of your boot configuration.

To alter boot menu entries, click the 'Edit Boot Menu' button. Here you can set the Default OS, and then choose either a timeout delay before the default OS is automatically loaded; or you can set the boot menu to remain shown until you manually select an OS; or simply have Windows skip the boot menu altogether and boot automatically into the default OS each time. You can also rename the OS entries which show up in the Boot Menu by selecting the relevant OS from the list and clicking the Rename button at the top of the screen. When done, click the 'Save Settings' button to save your changes.

The 'Add New Entry' button allows you to add or remove other operating systems (including non-Windows OSes) as part of a multiboot system. You can even boot up into a Virtual Hard Disk (VHD) image here, specified under the 'Disk Image' tab. The listing also allows you to rearrange the order in which the OS entries are presented if you wish. If you create any entries which you then decide to remove, go back into the 'Edit Boot Menu' section, highlight the relevant entry and click the Delete button at the top.

The 'Advanced Settings' include various features which the MSConfig utility and other Windows utilities can also accomplish. Most of these features are described elsewhere in this book and in general are best altered using the relevant Windows utilities or settings. The specific features for which EasyBCD is more convenient to use can be found under the Advanced tab:

PAE Support: This option provides control over Physical Address Extension (PAE) in Windows. This is only necessary for correct memory usage if you have 4GB or more of RAM and are running a 32-bit version of Windows 8, in which case you can select Enable here. Note that enabling PAE support does not simulate the benefits of a 64-bit environment. See the 32-bit vs. 64-bit section of the Windows Installation chapter for details.

NoExecute: This setting relates to Data Execution Prevention (DEP) which is covered in the Data Execution Prevention section of the Security chapter. You can alter its basic settings within Windows, however a larger range of options is provided here:

§ OptIn - The same as the 'Turn on DEP for essential Windows programs and services only' Windows setting.
§ OptOut - The same as the 'Turn on DEP for all programs and services except those I select' Windows setting.
§ Always On - Forces DEP to be enabled, without any exceptions.
§ Always Off - Completely disables DEP, without any exceptions.

Under the 'BCD Backup/Repair' section of EasyBCD, you can (re)install the Bootloader, allowing you to repair any problems caused by uninstalling or formatting an OS in a multiboot configuration for example, or due to some other form of problem. Select the 'Re-create/repair boot files' option and click 'Perform Action' to undertake this form of repair. In the first instance however you should attempt to restore a backed up .BCD file - specify the path to your backup .BCD file and click the 'Restore Backup' button.

EasyBCD is a very useful tool for easy BCD editing as the name suggests, but it also carries some risk, so if in doubt do not alter any settings, and if you wind up seriously damaging your BCD or any other Windows boot files, try the Automatic Repair functionality of the Windows Recovery Environment.

< CUSTOM BOOT SCREEN

This Microsoft Article explains that as of Windows 7, customization of the boot screen is not allowed. This is a deliberate decision intended to prevent any arbitrary elements being loaded into memory at boot time, because this is a critical period during which certain security checks are not yet possible. As such, I strongly recommend against using any tool that purports to provide this functionality, as it may prevent bootup or may be malicious.

Customizing the Windows Lock Screen, which appears immediately after Windows has booted up is quite simple, and is covered under the Personalize section of the PC Settings chapter. Alternatively, you can disable the Lock Screen altogether so that it is skipped after bootup, by referring to the instructions under the Disable the Lock Screen section of the Group Policy chapter.

< BOOTDISKS

A boot disk is a term traditionally used to describe media such as a special DVD which allows you to boot Windows into a recovery environment for troubleshooting and repair purposes. As of Windows Vista onwards, there is no longer a need for a separate boot disc. The Windows installation media acts as a boot disc as well, allowing you to boot into the Windows Recovery Environment to access a range of features covered under the System Recovery section of the Backup & Recovery chapter.

If you don't have Windows 8 installation media, you can create it using the instructions under the Prior to Installation section of the Windows Installation chapter. Alternatively, you can create a System Repair Disc for the same purpose, by referring to the Windows 7 File Recovery section of the Backup & Recovery chapter.

If you want to start up your PC in a very basic DOS mode, then bear in mind that the Command Prompt mode of the Windows Recovery Environment is only appropriate for certain purposes. Windows does not have a pure DOS environment, it only provides an emulated DOS-like Command Prompt interface. You can run a range of DOS commands from this prompt, but it is not the same as a true DOS environment, which some programs require for correct functionality. Therefore if you wish to boot into DOS to flash a hardware component for example, or to run certain DOS programs, you must use the instructions and tools provided at BootDisks, or use the free Ultimate Boot CD utility to create a boot disc. Alternatively, you can use the instructions provided here to make your USB flash drive bootable into DOS mode, but bear in mind that you also need to alter your BIOS/UEFI boot options to allow correct bootup from a removable device like a USB flash drive.

On balance there aren't many reasons to manually alter your boot configuration under normal circumstances, so approach the use of the tools and methods in this chapter with caution, rather than any desire to experiment. If you run into boot-related problems, always turn to the built-in tools within the Windows Recovery Environment first, particularly System Restore and Automatic Repair. If complex boot file editing is beyond your capabilities, you can also consider using the Windows Refresh feature to reinstall Windows while maintaining your personal data and key settings.

FILE EXPLORER

Windows 8 continues the use of the Explorer-based interface as the primary means for complex manipulation of files and folders in Windows. This interface is used by File Explorer - the new name given to the traditional Windows Explorer - as well as by many Desktop applications. It should be familiar to all Windows users, however there have been some notable changes in Windows 8. For those transitioning from Windows XP or Vista, the most noticeable new feature is Libraries, which was introduced as of Windows 7. Another major change which all users of previous versions of Windows will notice is that File Explorer now makes use of the Ribbon interface. Depending on which version of Windows you are upgrading from, there will be a range of other minor changes, however File Explorer's core file management functionality remains much the same as it has been over the past decade.

File Explorer can be accessed in several ways, including by typing *File Explorer* on the Start Screen and pressing Enter, by clicking the folder icon in the Taskbar on the Desktop, or by pressing WINDOWS+E at any time. This chapter covers all of the important new and existing features of File Explorer and Explorer-based interfaces in Windows 8, allowing you to make better use of this frequently-accessed tool and customize it to suit your needs.

Note that the common Windows graphical user interfaces often used in conjunction with Explorer-based interfaces, such as the Taskbar and Ribbon, are covered in more detail in the Graphics & Sound chapter.

< BASIC FEATURES

This section covers the basic features of File Explorer.

RIBBON

The Ribbon interface, first seen in the Microsoft Office 2007 suite, and then incorporated into selected built-in utilities in Windows 7 such as Paint and WordPad, is identified by a series of overlapping toolbars selected via tabs. In Windows 8, the ribbon interface replaces the standard menu in File Explorer.

In File Explorer, selecting a menu item in the ribbon now opens a separate toolbar with a range of options to select. Many of these options are context-sensitive, meaning that you first need to select a particular file or folder before they become available. Furthermore entire menu entries will not be shown until they become relevant. For example:

- The Search menu is not show in the default ribbon for Explorer until you first click in the Search Box at the top right.
- The Play menu will not appear until you select a file or folder which contains appropriate multimedia that Windows can play. If a video file/folder is selected, the 'Video Tools' highlight appears above the Play menu, and if a music file/folder is selected, the 'Music Tools' highlight appears above the Play menu, making it clear the type of media to which the play commands relate.
- The Manage menu will only appear when you select a drive or folder with additional management options, such as selecting a Library folder, or a connected USB drive.

The four menus that always appear whenever you open File Explorer are each covered in more detail below:

File: This general menu is not context-specific, and always allows you to access several higher-level functions. You can open a new copy of the current window, either as part of the existing process (which uses less resources), or as part of a new process (which uses more resources but is more stable); you can open a normal Command Prompt or an Administrator Command Prompt; open the PowerShell normally or as an Administrator; and you can also see the most frequent locations you have opened in Explorer, with the ability to pin any one of those places to the File menu by clicking the small pin icon next to its entry, or clear your entire history by clicking the 'Delete History' item.

Home: This menu contains the most commonly-used file and folder commands. You can also quickly access most of these commands by right-clicking on any file or folder, or right-clicking on an empty space within a folder. Most of the commands are self-explanatory, and have existed in all previous versions of Windows. Commands of interest here include the new 'Copy path' option which copies the current directory path shown in the Address Path; the History option, which accesses the File History feature covered in the Windows File History section of the Backup & Recovery chapter; the 'Select all', 'Select none' and 'Invert selection' options for quickly selecting all files, unselecting all highlighted files, or inverting the existing selection (i.e. selected files become unselected, while unselected files become selected); and the 'Easy Access' item which allows you to do things like pinning a selected folder to the Start Screen, or adding it to a Library or Favorites.

Share: This menu allows access to various methods of quickly sharing files with other people or devices. For example, you can highlight one or more files and select Email to open a new email message with your files already attached and ready to be sent; click the Zip button to automatically archive your selected file(s) into a compressed .zip file, which is then placed in the same directory; select 'Burn to disc' to burn a copy of the files to a recordable CD or DVD using the basic Windows disc burning wizard interface; or to share it with selected people on your network, or other people who also use your PC.

View: This menu provides various methods for customizing the way in which File Explorer presents files and folders. You can alter the view type, choose to display the Navigation, Preview and/or Details panes, and select the way in which files are sorted. Also provided is quick access to options previously only available in the Folder Options window - the ability to view or hide 'File name extensions' and 'Hidden items'.

All of the key features briefly mentioned above are covered in greater detail throughout this chapter.

If you're not familiar with the ribbon interface, there are several other important features unique to the ribbon which are worth getting to know:

§ You can't remove the ribbon altogether, but you can collapse it by clicking the small white arrow at the top right of the ribbon, next to the Help question mark icon, or by right-clicking on any item in the ribbon and selecting 'Minimize the ribbon'. This will hide the ribbon tab while keeping the menu headings available; clicking on a menu heading will then temporarily open the ribbon tab beneath it at any time. This is useful in providing maximum vertical viewing space.
§ You can pin any ribbon options as small icons to the Quick Access Toolbar in the title bar of the window. To do this, right-click on an item in the ribbon and select 'Add to Quick Access Toolbar'. This is useful in letting you access your most frequently-used commands without having to open a particular ribbon tab. You can customize the Quick Access Toolbar by clicking the small black down arrow at the end of it to see a drop-down box. For example, you can untick particular items to remove them from the Quick Access Toolbar, or you can even move the toolbar so that it is displayed below the ribbon rather than at the top of the window.
§ You can access all ribbon options in File Explorer using unique keyboard shortcuts. To see existing common keyboard shortcuts, hover your mouse over individual options - some have the standard system-wide shortcuts usable in most any Explorer-based interface. However, to see the File Explorer ribbon-specific shortcuts, press the ALT key once, and letters or numbers will appear above every menu

heading. You must then press ALT along with the appropriate menu key shown to further display a range of shortcuts for individual options within that menu. For example, press ALT+H to select the Home menu on the ribbon, and further shortcut keys will appear for every option under the Home menu. To trigger one of those options, you will need to press ALT+H plus the key sequence shown for the desired option (e.g. ALT+H+C+P to trigger the Copy Path function within the Home menu).

SEARCH BOX

The Search Box is present in all Explorer-based interfaces, including most open windows and of course File Explorer. It is shown at the top right of the window, with a small magnifying glass at the far right. This is a very useful feature which allows you to quickly refine in real-time what is displayed in the current window or folder by typing in a search term, or even partial characters. For example, to quickly show any executable files in a large folder, open that folder in File Explorer and type **.exe* in the Search Box to filter out other files and show only .EXE files.

Any filters you previously entered in the Search Box are displayed in a drop down box for quick selection as you begin typing, as well as a range of suggested filters. You can also use advanced filters based on various file properties and Windows will show common values in the drop box. For example, type *bitrate:* into the Search Box and Windows displays common values for you to select such as *Near CD Quality (over 128 Kbps)*, or you can enter your own value.

A large number of search-based options are now accessible under the Search menu in the Explorer ribbon which appears after you click in the Search Box. These options allow you to conduct specific searches using a variety of pre-defined parameters without needing to remember which search filters to enter into the Search Box. For example, click in the Search Box, then select the Search menu in Explorer, click the 'Date Modified' button and select Yesterday - this will automatically enter the *datemodified:yesterday* search filter into the Search Box and show any files in the current folder that were modified yesterday.

The Search Box and associated search functionality is covered in full detail in the Windows Search chapter.

ADDRESS BAR

At the top of each Explorer-based window is a web browser-like Address Bar which has back and forward arrows at the far left, an up arrow, a refresh button at the far right, and the path to the currently displayed directory or window in the main address box. Useful aspects of the Address Bar include:

- You can jump to any available subdirectories under each branch of the displayed path by clicking the small black arrow next to that particular directory branch.
- You can go back up the directory path one directory at a time by clicking the up arrow at the left of the Address Bar. This feature has been added back as of Windows 8, having been removed in Windows Vista and 7.
- You can view and select recently opened locations during the current session of File Explorer by clicking on the small black Recent Locations down arrow found between the right arrow and the up arrow at the left of the Address Bar.
- You can use the Back and Forward arrows at the far left of the Address Bar to go backwards or forwards through any recently opened locations.
- You can view and select previously opened locations by clicking the small Previous Locations down arrow found to the left of the Refresh button at the far right of the Address Bar.
- You can go to a specific directory or path by left-clicking on an empty space in the Address Bar and typing the full path, or just the directory name. If the location doesn't exist, Windows will launch a web search on your default browser using the search string entered.
- You can copy the full directory path shown in the Address Bar by either right-clicking within the Address Bar and selecting 'Copy address as text', or using the 'Copy path' function under the Home

menu in Explorer. You can then paste this copied path into the Address Bar at any time by first left-clicking in an empty area of the Address Bar, then right-clicking and selecting Paste.

Note that to clear the stored history under Previous Locations at any time, right-click in the Address Bar and select 'Delete History'. To clear the history stored in Recent Locations, simply close and reopen File Explorer.

NAVIGATION PANE

This is the area in the left pane of File Explorer which lists various locations, including Favorites, Libraries, folders and drives, usually shown as a directory tree. This section details the individual components of the navigation pane, and how to customize the navigation pane view.

Favorites

Shortcuts to commonly visited folders can be stored under the Favorites folder at the top of the navigation pane for quick access - by default Desktop, Downloads and Recent Places are shown. You can remove any shortcut here by right-clicking on it and selecting Remove; this removes the shortcut only, not the original directory. To add a new shortcut to Favorites, first navigate to any directory in File Explorer, then right-click on the Favorites folder and select 'Add current location to Favorites', or simply drag the directory folder and drop it on Favorites.

The Favorites folder is actually an extension of the *\Links* folder found under your user directory, so if you delete the Links folder, it will remove all of the saved shortcuts under Favorites, leaving the Favorites folder intact with no visible subdirectories. If you wish to regain full Favorites functionality you can manually create a new folder called Links under your user directory (i.e. *\Users\[username]\Links*), however adding folders to Favorites will result in the *-Shortcut* extension also being added for each folder shortcut. Instead of this, go to the *\Users\Default\Links* directory and copy that folder across to sit under your main *\Users\[username]* directory, and this will re-enable the normal Favorites functionality exactly as before.

You can remove the Favorites folder by right-clicking in an empty area of the Navigation Pane and selecting the 'Show Favorites' item so that it becomes unticked. This will remove Favorites from view, but it won't delete your saved favorite locations, so that should you wish to restore them at any time, you can follow the procedure above and retick the 'Show Favorites' item to display it again.

You can rename the Favorites folder by going to the following location in Registry Editor:

```
[HKEY_CLASSES_ROOT\CLSID\{323CA680-C24D-4099-B94D-446DD2D7249E}\ShellFolder]
```

Right-click on the key above, and if necessary change the permission to allow you to edit it - see the Windows Registry chapter for details on how to edit the Registry correctly, and see the Access Controls and Permissions section of the Security chapter for details on permissions.

```
Attributes=a0900100
```

Change the DWORD value above to `a0900130` in Hexadecimal view.

Restart Windows, or logoff and logon, and you will now be able to access new Rename and Delete options when you right-click on the Favorites category.

Libraries

The Libraries feature is covered in full detail later in this chapter. If you want to hide particular Libraries from the Navigation Pane, then select the relevant Library, right-click on it and select Properties, then untick the 'Shown in navigation pane' box and click Apply. Alternatively, simply right-click on the relevant Library and select 'Don't show in navigation pane'. That Library will no longer be shown under the Libraries category in the Navigation Pane, however it will still be shown in the right pane of Explorer when you click on the Libraries category heading. There you can restore any Library to the Navigation Pane by right-clicking on it and selecting 'Show in navigation pane'.

If instead you wish to remove the entire Libraries category from the Navigation Pane, you will need to go to the following location in the Registry:

`[HKEY_CLASSES_ROOT\CLSID\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\ShellFolder]`

Right-click on the key above, and if necessary change the permission to allow you to edit it.

`Attributes=b080010d`

Change the DWORD above to `b090010d` in Hexadecimal view.

Restart Windows, or logoff and logon, and the Libraries category will no longer be shown in File Explorer. However, the Libraries functionality has not been disabled; you can still access these libraries through supporting applications, and the original Libraries still sit under the *\Users\[Username]\AppData\Roaming\Microsoft\Windows\Libraries* directory.

To restore Libraries in the navigation pane, simply follow the steps above and change the `Attributes` value back to `b080010d`.

Homegroup

The HomeGroup feature is enabled if you turn on sharing for your network. That is, if your Network Location is set to Private, whether during Windows installation, or at a later date. Enabling HomeGroups will result in a Homegroup category being shown in the Navigation Pane of File Explorer. For users who are not part of a network of computers (excluding the Internet), and are not using network resources in any way, this is an unnecessary addition that can be safely disabled, removing this item from the Navigation Pane.

To remove the Homegroup item, do the following:

1. Right-click on the Homegroup category in File Explorer, select 'Change HomeGroup settings', or go to the HomeGroup component in Windows Control Panel.
2. To stop using the HomeGroup feature, click the 'Leave the homegroup' link, then select 'Leave the homegroup' to confirm.
3. To then completely remove the HomeGroup item from File Explorer, you will need to open the Charms menu, select the Settings Charm, and click on the Network icon at the bottom.
4. Right-click on your Network connection which appears and select 'Turn sharing on and off'.
5. When presented with the options, select 'No don't turn on sharing or connect to devices' - this will set your Network location to Public, which automatically disables HomeGroups.

You can also disable the two HomeGroup-related services which are currently running by opening the Services utility and setting both the 'HomeGroup Listener' and 'HomeGroup Provider' services to Disabled, though this isn't really necessary, as they are set to Manual by default and won't run unless required - see the Services chapter for more details.

If you do wish to use HomeGroups, then see the HomeGroup section of the Control Panel chapter for more details of this functionality.

User Folder

To see your user folder and subfolders as a separate category in the Navigation Pane, you need to go to the Folder Options component of the Windows Control Panel, and under the General tab, tick the 'Show all folders' box and click Apply. Alternatively you can right-click in an empty area of the Navigation Pane and tick the 'Show all folders' option. This will display your main user folder (labeled with your user account name), under which will be all of the standard subfolders, such as *Downloads, My Documents, My Music, My Pictures, My Videos* etc.

You may also see a range of additional folders - marked with shortcut arrows - which are actually Directory Junctions, not real folders; see the Directory Junctions and Symbolic Links section later in this chapter for more details. It is not necessary for you to see these additional items in the Navigation Pane as they are not designed to be directly accessed by users, and only end up cluttering your view in File Explorer. You can remove them from view by going to the View tab in Folder Options, ticking 'Hide protected operating system files', then clicking Apply, and closing and re-opening File Explorer.

More details regarding your user folder are under the Personal Folders section later in this chapter.

Computer

All of your connected drives will be listed under the Computer category. Note that if the 'Show all folders' box is not ticked in Folder Options, then drives which are currently empty, such as DVD or Blu-ray drives which contain no discs, will not be displayed as a separate item under the Computer category in the Navigation Pane, however they will be shown in the right pane when the Computer category is highlighted.

Network

The Network category always appears, even if you are not on a home or work network. To remove the Network item from the Navigation Pane, go to the following location in the Registry:

```
[HKEY_CLASSES_ROOT\CLSID\{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}\ShellFolder]
```

Right-click on the subfolder above, and if necessary change the permission to allow you to edit it.

```
PinToNameSpaceTree
```

Right-click on the value shown above and delete it. Restart Windows, or logoff and logon, and the Network category will no longer be visible in the Navigation Pane. To undo this change at any time, simply go to the subfolder above, right-click in the right pane, create a new STRING with no value data and name it `PinToNameSpaceTree` then restart Windows or logoff and logon.

Customizing Navigation Pane Views

If you do not like the contents of any of the main categories such as Favorites, Libraries or Computer cluttering the Navigation Pane, then aside from removing certain components as covered above, you can also customize them in a relatively simple manner from within Windows without resorting to any advanced methods, or in conjunction with the advanced methods.

To start with, you can minimize any major category by simply double-clicking on it, or clicking on the small arrow at its left, or right-clicking on it and selecting Collapse. Then to make this setting stick so that each time you open File Explorer the minimized folders remain as such, go to Folder Options in the Windows Control Panel, and under the General tab, untick the 'Automatically expand to current folder' box and click Apply. If you wish, you can also untick the 'Show all folders' option so that Windows minimizes all folders except Libraries and Favorites, and you can then choose whether to minimize Libraries and/or Favorites as well, creating an extremely compact Navigation Pane.

For example, try the following:

1. Untick the 'Show all folders' and 'Automatically expand to current folder' boxes in Folder Options as covered above.
2. Manually add all of your commonly used directories to Favorites.
3. Minimize (or remove) Libraries and Network, and minimize the Computer category, leaving only the Favorites folder maximized.
4. Now each time you open File Explorer you will have a very clean layout with quick and easy access to your commonly used folders under Favorites. Should you need to access other folders at any time, you can readily expand the Computers category and delve into the detailed directory structure from there.
5. Alternatively, if you make use of the Libraries feature, then do the same as above, however this time minimize every other folder except your Libraries, and you can now quickly access all of your personal files in that manner.
6. As yet one more alternative, if you only want your user folders showing as expanded, then under the Navigation Pane options in Folder Options leave only the 'Show all folders' box ticked, then in Explorer minimize all other folders.

Obviously you can experiment with a combination of these options to obtain the layout which suits you best. Finally, if for whatever reason you wish to disable the Navigation Pane altogether, then go the View menu in File Explorer and select 'Navigation Pane', then untick the 'Navigation pane' item. You can then access a list of the main locations by clicking the first black arrow shown inside the Address Bar.

Regardless of how you customize the Navigation Pane, by default File Explorer selects the Libraries category whenever it is opened. You can alter this default behavior by using the tips under the Advanced Features section later in this chapter.

DETAILS & PREVIEW PANES

While the Navigation Pane is shown by default, two additional types of panes can be enabled to provide further details for files and locations: the Details Pane and the Preview Pane.

Details Pane

Under the View menu you can select whether to display the Details Pane. If enabled, the Details Pane is displayed on the right side of File Explorer. In Windows 7 the Details Pane would sit at the bottom of the Explorer window, however it has been changed to the right side in Windows 8 to make better use of the

greater horizontal space on widescreen monitors, particularly as the ribbon already takes up quite a bit of vertical space when expanded.

The Details Pane will displays a range of details about any highlighted file or folder, including information from its Properties tab, as well as an icon or thumbnail preview of its contents. You can also quickly edit the properties of a file by clicking on any of the customizable fields in the Details Pane and entering new information, as long as the file is not read-only. Leaving the Details Pane enabled should have minimal performance impact when browsing files, however selecting more complex files, especially picture and video files, may be slower, especially if Windows has to generate a new live thumbnail for the file's content.

You can resize the Details Pane by dragging its divider left or right.

Preview Pane

Under the View item you can select whether to display the Preview Pane. If enabled, the Preview Pane sits at the right side of the Explorer window, and replaces the Details Pane. In other words, unlike Windows 7, you can enable either the Preview Pane, or the Details Pane, but not both together.

The Preview Pane is usually empty if no file is highlighted. Once you highlight a particular file, a preview of its contents will be displayed where possible. This preview can be in the form of text or multimedia, such as the ability to playback a song or video, or browse a Word document, from within the Preview Pane. Enabling the Preview Pane can increase file browsing time, so disable it if you don't need this functionality.

Note that if the 'Show preview handlers in preview pane' option is disabled under the View tab in Folder Options, multimedia files will not have playback capability, and many files will not show a preview of their contents - see the Folder Options section later in this chapter.

STATUS BAR

To make up for the loss of the ability to display the Details Pane at the bottom of File Explorer, there is now a small Status Bar that can be enabled there instead. The Status Bar is a one-line display at the bottom of Explorer, showing the number of items in the current folder, the shared status of the file/folder, and the file size of any selected item. There are also two 'Change your view' buttons at the far right of the Status Bar, allowing you to switch between Details and Large Icons view in each folder.

You can turn the Status Bar on or off by changing the 'Show status bar' option under the View tab of Folder Options.

FOLDER VIEWS

Every directory in File Explorer and Explorer-based interfaces can display its contents using one of a variety of pre-defined views. There are also a wide range of options for customizing the appearance of content, including the ability to sort, group, filter, and add or remove columns.

The most important step is to choose from a layout for each folder. Some of these layout types were introduced in Windows Vista, with Contents view being added as of Windows 7.

The available view layouts can be accessed in several ways:

§ Open the View menu in the File Explorer ribbon and select from the list of view types shown in the Layout box. These include: Extra large icons; Large icons; Medium-sized icons; Small icons; List; Details; Tiles and Content. You can also simply hover your mouse over each view type listed here to preview how it would look in the selected folder.
§ Right-click in an empty area of a folder, then select the View item and the desired view.
§ Click the 'Change your view' buttons at the bottom right on the Status Bar. The button on the left selects Details view, the button on the right selects Large icons view.
§ Hold down the CTRL Key and scroll the mouse wheel to actively cycle through all the available views.

The standard Windows view types are described below:

§ *Icon* - Icon view shows all files as icons, sorted by the filename by default. You can select Small icons, Medium icons, Large icons and Extra Large icons views. These icons are typically the standard Windows icons for each file type, however multimedia files such as music, picture and video files, and even document files under certain circumstances, will display as Live Icons in Icon view by default, providing a snapshot of the actual contents of the file - see Live Icons further below. The icon size can also be dynamically scaled to suit your taste by holding down your CTRL key and scrolling up or down with the mouse wheel.
§ *List* - This view is the most basic, and simply lists all the files with their filename and a small generic icon, and no other details are shown. By default the files are sorted by filename down as many columns as can fit within the pane. No Live Icons are shown in List view.
§ *Details* - This view provides much greater potential for displaying and sorting items based on a range of file properties. Files are listed by name, with additional columns such as Size, Type, Date Modified and so forth available to be added, resized or removed as desired. To add or remove a column and change sort order see the Sorting section further below. No Live Icons are shown in Details view.
§ *Tiles* - In this view, files are displayed as a range of "tiles", with each tile containing the filename, file type and file size, along with a medium-sized generic icon. Live Icons are shown in Tiles view by default.
§ *Content* - Content view is primarily used for more convenient browsing of multimedia files. Each file is listed along a single row, with a small Live Icon and a range of information such as file name, file type, file size and date modified. It also includes media-specific details such as play length for music or movies, picture or video dimensions, and other useful metadata from multimedia files, all available at a glance.

Live Icons

In Icon, Tiles or Content view, the icons for certain files will be shown as Live Icons, not generic Windows application icons. Live Icons provide a sample of the file's contents as a thumbnail image. For example, with Live Icons enabled, a .JPG image file will have a thumbnail of the image shown as its icon; an .AVI or .WMV video file will have a sample scene from the video shown as a thumbnail instead of a generic icon; and .DOCX or .PDF documents will have a page of their contents shown as the thumbnail, depending on certain factors covered below.

Icon View is enabled by default when using certain view types as covered above. You can disable it at any time by going to Folder Options in the Windows Control Panel, and under the View tab ticking the 'Always show icons, never thumbnails' box, then clicking Apply. Doing this will replace all Live Icons with generic Windows icons for that particular file type. Disabling Live Icons can speed up file browsing time, particularly when viewing a directory with multimedia files which have not yet had a Live Icon thumbnail generated by Windows. However once the icon is generated, it is stored in a Windows thumbnail database, and on a moderate to fast system it doesn't take any longer than normal to view a folder with Live Icons as

opposed to generic icons. Consideration should also be given to its usefulness in assisting in the rapid visual identification of file contents in certain folders.

If you've enabled Live Icons but they are not being displayed correctly, then you need to consider several things. Under Windows 8 64-bit, even though 32-bit applications run without any issues, when it comes to File Explorer, it runs as a 64-bit application by default, and requires that all the shell extensions (extra interface features) it uses are also compiled as native 64-bit applications for full functionality. In plain English this means that under Windows 8 64-bit, the default program/codec/plugin associated with viewing particular content needs to also be a native 64-bit application as well, or the Live Icon for that content will not be correctly generated.

This shouldn't be a problem if you associate a built-in Windows program with playback of audio and video and the viewing of pictures for example. However for file types which are being handled by 32-bit applications, you will need to install and/or associate a 64-bit application or media handler with that file type to get Live Icons. See the Codec section of Windows Media Player for further details in relation to common multimedia codecs and plugins.

One common issue with Live Icons is documents saved using 32-bit versions of Microsoft Office - Live Icons for such documents won't be shown in Windows 8 64-bit. To get around this, you can install the 64-bit version of Office 2010 or 2013 if available to you, but note that the 32-bit versions are generally recommended as they are the most compatible with add-ons. However, there is another way around this problem: when saving a document in Office 2007, or the 32-bit versions of Office 2010 or 2013, select the 'Save As' option, tick the 'Save Thumbnail' box at the bottom, then save the document. It will now be saved with the equivalent of a Live Icon thumbnail preview, which can be seen in Icon View in File Explorer.

Whether you are running Windows 8 64-bit or not, you may still find the Live Icons not displaying properly, or displaying old content for an updated file. To resolve this you will need to clear the Icon Cache and allow Windows to rebuild it again. This should restore or create all Live Icons as desired - see the Icons section of the Graphics & Sound chapter for more details of how to do this correctly.

Sorting

The contents of any folder can be sorted by a range of properties. By default the contents are automatically sorted in Ascending order by Name (file name), and the sorting is dynamic; that is, there is usually no need to refresh the Explorer window whenever new files are added to a folder, as Windows 8 should automatically resort to maintain appropriate order.

To access various sorting options, go to the View menu in the Explorer ribbon, or right-click in an empty area of the folder:

Sort By: Here you will see the common properties you can use to sort files, such as Date Modified, Type and Size, as well as being able to choose Ascending (A-Z, 1-10) or Descending (Z-A, 10-1) order. You can click the More or 'Choose columns' option and select from any one of a larger range of properties upon which to sort the current view of folder contents.

Note that to quickly toggle between Ascending and Descending sort order in any column, click the column header once. As you click on the column header, a small arrow at the top will show the current sort status of that column: upward for Ascending, and downward for Descending.

Group By: You can create subcategories within a view by selecting 'Group by', then selecting the particular property by which you wish to group the contents. This will arrange the contents under separate headings for each subcategory. Once again you can select the More or 'Choose columns' item to see additional

properties for use in grouping contents. If you wish to remove grouped view, choose the (none) item under 'Group by'.

Filter By: If you only want to view a certain subset of the contents in a folder, aside from using the Search box, you can switch to Details view, move your mouse over a column header and click on the small black arrow which appears at the right side of the header. You will then be able to select a check box to filter the contents by one or more of the specific categories displayed.

Note that the 'Stack By' sorting option available in Windows Vista was removed as of Windows 7.

Modifying Columns

For each folder type, as well as individual folders, you can add or remove the columns which are displayed. The common columns include Name, Date Modified, Type and Size. You can alter the column layout either by clicking 'Add columns' under the View menu in the Explorer ribbon, or by right-clicking on any column. You can resize any existing column by moving your mouse to the separator between column headers, and then dragging it left or right - this resizes the column to the left of the separator.

If you want to quickly resize columns so that they are wide enough to show all of the information they contain, then either select the 'Size all columns to fit' button in the Views menu of the Explorer ribbon, or right-click on a column header and select the same option. This will resize all available columns in the current folder so that each column is exactly as wide as the longest string of text displayed under it. If you only want to do this for a single column, right-click on the column header and select 'Size column to fit' instead.

CORRECTLY SETTING FOLDER VIEWS

Windows decides the default view for a particular folder based on the type of folder involved, and the types of files within a folder. Windows assigns a folder type based on five different categories:

- General Items
- Documents
- Pictures
- Music
- Videos

You can see the default views for each of these types by going to your personal folders under the *\Users\[username]* directory and selecting the *My Documents*, *My Pictures*, *My Music*, and *My Videos* folders which each take on the folder type of the same name. See a folder like *Downloads* or *\Windows* for an example of the General Items folder type.

To view a particular folder's folder type, right-click on that folder and select Properties, then under the Customize tab look at the box under 'Optimize this folder for'. If you wish to change this folder's type, you can do so here, and you can also tick the 'Also apply this template to all subfolders' box if you want all of the sub-directories under this folder to also be set to the same folder type. Click the Apply button when done to implement the change.

You can alter the view for a specific folder, or all folders of a particular type, and make this change permanent so that each time you open that folder or folder type, the view remains the same. This requires that you follow a specific set of procedures, otherwise Windows may automatically alter the folder type and/or the view type used whenever the folder's contents change, which can be quite annoying. The steps below will ensure that your view selections are made permanent until you choose to manually alter them again.

For every folder type, you will have to go to at least one folder of that type and set your desired view preferences. I recommend that you open File Explorer and go to directly your *My Documents*, *My Pictures*, *My Music*, *My Videos* and *Downloads* folders found under *\Users\[username]* (and not via Favorites or the Libraries). Then follow the procedure below for each folder type:

1. Adjust the view in the folder to suit your preferences using the methods covered earlier in this chapter. Change the view type, resize any icons shown if required, add or remove and/or resize any columns if applicable, choose your sort order for files, etc.
2. Once done, you must then click on the Options button under the View menu of the Explorer ribbon and select 'Change folder and search options'. Don't open Folder Options via Windows Control Panel or any other method, do it from the Options button under the View menu.
3. With Folder Options open, go to the View tab of Folder Options and click the 'Apply to Folders' button, and click Yes when prompted. This forces Windows to recognize that the changes you have made to the view in this particular folder apply to all folders of the same folder type. So for example, using this method, any changes you make to the view in your *My Pictures* folder will apply to all folders flagged with the Pictures folder type.
4. Click OK to close Folder Options.
5. Repeat Steps 1 - 4 above for each of the five main folder types.

Once done, close File Explorer, then open it again and check a range of folders to see if the views have stuck. For any folders which don't appear to be sticking, check and select the correct folder type and then manually alter the view to suit your taste if required, and they should also stick.

Importantly, setting the views in this manner does not apply them to your Libraries, as they need to be set separately. In fact if you try to adjust folder views within a Library, the 'Apply to Folders' button won't be available in Folder Options, and any change you make in one folder will apply to your entire Library, so be aware of the difference. Your first step should be to follow the procedures above by going directly to your user folders under the *\Users\[username]* directory. Then you can customize your Library views as necessary. Your user folders and Libraries will maintain separate view settings from each other.

Note further that some system folders will not have a Customize tab under their Properties; this is normal, and their default view should correspond to the General Items folder type.

Some folder customizations and settings are stored in a file called *Desktop.ini* in each folder. These files are hidden by default unless you disable the 'Hide protected operating system files' option under the View tab in Folder Options, which is not recommended. Do not delete or move these files, they need to remain where they are to maintain specific custom folder settings in Windows.

Despite following these procedures, you may sometimes find that Windows still changes the folder views, for a range of reasons including Registry corruption and/or the folder type setting being overridden by another application, or when Windows detects multimedia files for the first time in that folder. To resolve issues with folder views not remaining the way you want them, see the Fix Changing Folder Views tip under the Advanced Features section later in this chapter.

To correctly alter other view-related aspects of folders, you will need to refer to the Folder Options section below.

< FOLDER OPTIONS

Folder Options can be found as a separate component under the Windows Control Panel, or by pressing the Options button in the View menu of the File Explorer ribbon.

As the name suggests, Folder Options has a range of options which affect the way folders are viewed, as well as the appearance of File Explorer. It also has important Search-related options. Each tab of the Folder Options window is covered separately below.

GENERAL

Browse folders: If 'Open each folder in the same window' is chosen, then selecting an option or launching a component from a window will mean that it opens in the existing window. If 'Open each folder in its own window' is chosen, a new window will open for each component or option launched from within an existing window. I recommend the first option, as this reduces the number of open windows, which in turn reduces resource usage and Desktop clutter.

Click items as follows: The 'Double-click to open an item (single-click to select)' option is the default behavior that most Windows users are familiar with, and the one which is assumed when providing descriptions in this book. If you prefer more web-like behavior, you can select the 'Single-click to open an item (point to select)', and choose whether to have selectable items and icons underlined all the time, or only when you hover your mouse over them. In general the double-click method is most familiar, and prevents accidental launching of programs or options from wayward mouse clicks, so it is recommended.

Navigation pane: These options are covered under the Navigation Pane section earlier in this chapter. The 'Show favorites' option is new to Windows 8, and allows you to hide the Favorites category in File Explorer if the box is unticked. The 'Show all folders' option, if ticked, shows all the possible folder categories in the navigation pane, including your *[username]* folder and its main subdirectories. The 'Automatically expand to current folder' option, if ticked, expands and shows all the levels of the directory tree leading to the folder you've currently chosen, which can override any minimizations in the Navigation Pane that you wish to keep.

VIEW

Folder views: When you change the look and layout of a particular folder in File Explorer, such as the number and size of any columns, the size of icons, or the type of view that folder type has, to apply your changes to all other folders of the same folder type, click the 'Apply to Folders' button. Conversely, to undo your changes, click the 'Reset Folders' button. More details on how to correctly set folder views for various folder types is covered in the previous section of this chapter.

Advanced Settings: Most of the options in this section of Folder Options are dependent on your particular tastes in functionality and appearance. Below I briefly cover these features, noting where there may be performance or other impacts. These options all have fairly significant impacts on the way File Explorer looks and functions, so make sure you go through each one carefully:

- Always show icons, never thumbnails - If ticked, Live Icon thumbnails will be disabled and replaced with generic associated application icons; see the Live Icons section of this chapter for details.
- Always show menus - If ticked, always shows the Menu Bar which resides at the top of most windows. If unticked, the Menu Bar is hidden until you press the ALT key to bring it up temporarily. This setting does not affect windows using the ribbon interface, such as File Explorer.
- Display file icon on thumbnails - If ticked, displays a small icon at the bottom corner of Live Icons representing the default application associated with that file.
- Display file size information in folder tips - If ticked, whenever you hover your mouse cursor over a directory in the right pane of an Explorer-based interface, a small popup appears providing details on

the size of the directory and some of the files it contains. This option only works if the 'Show pop-up description for folder and desktop items' setting is also ticked (see below). This option is generally unnecessary, and may cause reduced responsiveness when moving your mouse over folders.

§ Display the full path in the title bar - If ticked, the full directory path to the currently selected folder will be shown as the title for File Explorer. For example, by default if you're in your Downloads personal folder on C: drive, only *Downloads* is shown in the title of File Explorer. With this option enabled, *C:\Users\[username]\Downloads* will be shown instead.

§ Hidden files and folders - If 'Show hidden files, folders and drives' is selected, you will see all hidden system files, folders and drives, excluding protected files and folders (see below). It is important to have this option ticked if you want to see all of the important files and folders on your system, especially when using this book. You can also quickly toggle it on or off at any time by using the 'Hidden items' box under the View menu in File Explorer.

§ Hide empty drives in the Computer folder - If ticked, any drives with removable media which are not currently holding any such media will be hidden under the Computer category in Explorer.

§ Hide extensions for known file types - If ticked, will hide the extensions (e.g. the .EXE portion of a *setup.exe* file) for all known file types. It is strongly recommended that you do not tick this option, as it will make file editing confusing. For example, if you are asked to create a blank text file and rename it to *user.cfg*, with this option enabled, you will actually be incorrectly renaming the file *user.cfg.txt*, since the .TXT part of the extension will be hidden. You need to be able to clearly see the full filename, including any extensions, for a range of customization and security reasons, so untick this option.

§ Hide folder merge conflicts - A folder merge conflict occurs when you attempt to copy or move a folder to a location where another folder has the same name. If this option is unticked, you will be prompted each time a conflict occurs, and asked whether to merge the folders or not. If this option is ticked, Windows will automatically merge the contents of both folders without raising any prompt. It is recommended that you untick this option so that you can see and decide what to do for every instance of a merge conflict.

§ Hide protected operating system files - Shows a range of additional hidden system files and folders which under normal circumstances should be not be accessed, changed or deleted, such as Directory Junctions (see below), log files, *desktop.ini* files, and the Pagefile. If unticked, you will see these files and folders, but this only adds to clutter in Explorer and also results in the temptation to (purposely or accidentally) delete important system files. Unticking this option is generally only necessary as part of advanced tweaking or troubleshooting, and is usually only a temporary measure. It should remain ticked at all other times.

§ Launch folder windows in a separate process - If ticked, this option increases stability at the cost of performance by opening each window in a separate process, in effect isolating that window and preventing a crash in one window from shutting down others. It is not recommended that this item be ticked. If you are having stability issues you should check application compatibility, undertake general system troubleshooting, and research online to find the root cause; it is not normal for a window to crash or freeze.

§ Restore previous folder windows at logon - If ticked, makes sure that Windows remembers your specific folder settings for each open folder when you last shut down Windows, and restores them to the same state the next time you boot back into Windows. This setting is essentially a session restore feature, and does not relate to permanently saving customized folder views in Explorer, which is a different process covered earlier in this chapter.

§ Show drive letters - If ticked, shows the drive letter for every drive (e.g. C:, D:, E:, etc.). Unticking this option will remove the drive letters, but still show the drive name. I don't recommend unticking this option as it is important that you know the drive letter of specific drives for a range of purposes, such as running Command Prompt commands.

§ Show encrypted or compressed NTFS files in color - If ticked, highlights files which have been encrypted or compressed in a different color. This is useful for identifying files which are compressed or encrypted that you would otherwise be unaware of. This option should be left ticked unless you find it annoying.

- Show pop-up description for folder and desktop items - If ticked, this option will raise a small pop-up box whenever you hover your mouse cursor over a file or folder in the right pane of Explorer-based windows, or on any item on the Desktop. The pop-up usually contains a description of the file, folder or Desktop item. In general this is unnecessary, and may slow down mouse movements over items if enabled.
- Show preview handlers in preview pane - If the Preview Pane is enabled, and if this option is ticked, wherever possible a preview is provided of the file's contents, and you can also select to play the content of multimedia files. If this option is unticked, multimedia playback is disabled, certain files will only demonstrate a static picture of their content, and some files will have no preview at all. This can speed up the selection of files while the Preview Pane is open, however it is not recommended that you untick this option if you use the Preview Pane, as it basically renders it useless. If you find the Preview Pane annoying or slowing things down, disable it, or try the Details Pane instead.
- Use check boxes to select items - If ticked, this option allows a check box to appear next to every file and folder in the right pane of File Explorer whenever you hover your mouse cursor over that file/folder. This can make the selection of multiple objects much easier. However, the easiest method is to simply hold down the CTRL key to select multiple individual files, or select the first file/folder, hold down SHIFT and click at the end of your selection to select a continuous range of files/folders.
- Use Sharing Wizard - If ticked, this option places a 'Share with' item in the context menu which appears whenever you right-click on a file or folder. This allows you to more easily share files and folders with other users on your PC or network. If you do not wish to share anything with anyone else, particularly if you are a single PC user on a non-networked machine, then you should untick this option.
- When typing into list view - When a folder is selected in Explorer, this option determines what happens when you begin typing. If the 'Automatically type into the Search Box' option is selected, then any text you enter will automatically be shown in the Search Box at the top right of the window. One of the drawbacks of selecting this option is that if you choose to create a new file or folder in a directory, the cursor will suddenly jump to the Search Box when you attempt to type a name for that file or folder. If the 'Select the typed item in the view' option is selected, then the text you type won't appear on screen; the file which most closely matches what you are typing will be highlighted instead.

Remember that as you tick or untick each item, you must click the Apply button if you want to implement a change and see the impact straight away. When finished, click the Apply button again to ensure that you implement all changes.

SEARCH

These settings and search-related features are all covered in detail in the Windows Search chapter.

< PERSONAL FOLDERS

Every user account has a set of Personal Folders created for that account. They can be found under the *\Users\[username]* directory, where the username matches your user account name. Each user directory contains specific subfolders including: *My Documents*, *My Pictures*, *My Music* and *My Videos*. If you have unticked the 'Hide protected operating system files' option in Folder Options, you will also see a range of legacy personal folders which used to exist under Windows XP (such as *Cookies*, *Local Settings* and *PrintHood*). These are Directory Junctions, not actual folders, and are covered in the Directory Junctions and Symbolic Links section further below.

While you may be tempted to ignore your personal folders, or even delete them and create your own custom folders instead, I strongly recommend against doing so. Aside from being quite convenient for holding various file types, these folders are linked to a range of important features in Windows, such as File History, Libraries, Search Indexing, and of course your user account. Furthermore, Windows security-related features take into account that these personal folders are owned by you, and hence give you the greatest freedom in

altering their contents without being potentially faced with UAC prompts, or needing to manually change ownership of a file or folder.

You should instead focus on making the best use of them, and customizing them to suit your needs.

Rename Personal Folders

To start with, if you don't find the names of some of your personal folders appealing, you can change them. For example, you can safely rename the *My Documents*, *My Music*, *My Pictures*, and My Videos folders to drop the "My" portion of the name (e.g. from *My Documents* to *Documents*) without affecting their functionality. Just right-click on the folder, select Rename, and edit the name as normal.

You can rename other personal folders, such as *Links* or *Desktop*, and their functionality will remain intact, however this is not necessary nor is it recommended, as aside from causing confusion when reading references to these folders (e.g. such as those in this book), it may result in application errors and other unintended consequences.

Relocate Personal Folders

You can safely move your personal folders to another location, whether on the same drive, or another drive, without affecting their link to key Windows features. However you need to do this properly, so follow the steps below:

1. Go to the relevant folder under your personal folders.
2. Right-click on it and select Properties, then go to the Location tab.
3. Click the Move button and specify a new folder and/or drive to move the current folder to. Alternatively, you can just type the new path in the Target box. Note that I don't recommend entering just a drive letter by itself as this may cause problems. That is, don't just enter *C:*, *D:* or *F:* in the location box for example - enter a full directory path and click the Apply button.
4. The folder and all of its contents will be moved to the new location.

When complete, Windows will recognize the new location as the home of this particular personal folder, and all references to it throughout Windows 8, including in your Libraries and Search Indexing, should point correctly to this new location automatically. If necessary close and reopen File Explorer to see the updated references to the new folder.

Customize Personal Folders

You can create as many subfolders under your personal folders as you wish. This is useful if you want to organize your data in various ways under the existing personal folders without affecting their functionality within Windows. In fact when combined with the ability to view all your files across various directories and locations in a unified view using the Libraries feature, there are no real drawbacks to creating multiple subfolders under the personal folders.

You can also customize the icon used to represent any of your personal folders, in fact almost any folder, by following the steps in the Customize Folder Pictures & Icons tip under the Advanced Features section later in this chapter.

As a final note, before undertaking any alterations to your personal folders, because of the elevated risk of losing personal data, I strongly recommend that you first create a fresh backup of your personal data as covered in the Backup & Recovery chapter.

< LIBRARIES

One of the major changes which users of Windows XP or Vista will notice in Windows 8 is the inclusion of the Libraries feature. Introduced in Windows 7, and tightly integrated into the way Windows now works, Libraries are not a new set of folders intended to replace the traditional personal folders such as *My Documents* and *My Pictures*. Instead, Libraries are virtual folders designed as a complementary tool to assist users in more readily accessing and managing their data across various folders and/or drives from a single location.

A Library is a container providing a single place from which you can access and manipulate all the files and folders which have been linked to that Library. At least one existing folder must be assigned to any Library. The specific folder(s) included in any Library are visible when that Library is expanded in the left pane of Explorer, or seen by right-clicking on a Library and selecting Properties. The linked folder(s) determine the content displayed in a Library, however none of these folders has moved from its original location, nor has the Library created a copy of, or shortcuts to, these files or folders.

Any file or folder on a local drive or on an external, removable, or network drive, can be linked to a Library. Removable discs such as DVDs are not included, nor are any drives or network locations which are currently disconnected from the system.

Importantly, even though a Library is a virtual folder, any changes you make to files and folders within a Library will affect the contents of those actual files and folders. If you delete or rename a file within a Library for example, the original file or folder will be deleted or renamed. Deleting an entire Library on the other hand will not delete the files or folders it contains.

If you save, copy or move a file to a Library, by default the file will actually be saved/copied/moved to the first folder location linked to the Library. Right-click on the Library and select Properties to see the default save location, indicated by a small tick next to the folder under the Library Locations box. You can change the default save location by highlighting any folder in the Library Locations box and clicking the 'Set save location' button - the tick mark should appear next to your selected folder.

Although Libraries are virtual folders, they exist as separate physical files with the filename *[libraryname].library-ms* under the *\Users\[username]\AppData\Roaming\Microsoft\Windows\Libraries* directory. Libraries are stored here as .XML definition files whose structure is explained in this Microsoft Article. You can edit these files using a text editor as covered in the Customizing Libraries section below. The original location of the Library definitions is useful to know, because aside from customization, it allows you to access them even if you hide the Libraries category in File Explorer, as covered under the Navigation Pane section earlier in this chapter.

Libraries are tied in to a range of key features to make them more useful. Libraries are integrated into the following prominent Windows features:

- File Explorer - Aside from having a separate Libraries category, File Explorer also opens in the Libraries category whenever it is launched using a default shortcut such as the one on the Taskbar. You can alter this behavior as covered in the Advanced Features section later in this chapter.
- Windows Search - Windows Search is synchronized with Libraries, automatically adding all files and folders in your Libraries to the Search Index for fast access. See the Windows Search chapter for details.
- Windows Media Player - The built-in Windows Media Player utility works closely with the Music Library, not your *My Music* personal folder. See the Windows Media Player chapter for more details.

Windows users who skipped Windows 7 may initially find Libraries to be confusing, annoying or redundant, and will want to hide or remove them. While attempting to do this is not advised given the integral nature of Libraries, methods of reducing the presence of Libraries have been covered throughout

this chapter. Before turning to such methods, I recommend that you attempt to work with the Libraries as much as possible, customizing them and adding new Libraries for various content as you desire. You should find that you become accustomed to them, and actually find them helpful, the same way you may have become accustomed to the default Windows personal folders.

CUSTOMIZING LIBRARIES

Just as with a regular folder, you can adjust the folder view and the sorting method used in Libraries to suit your needs - see the Folder Views section further above. Note that the custom views you applied to other folders and folder types do not automatically apply to Libraries, or vice versa. You will need to set the views you wish within a single folder in each Library, and it will then automatically apply to all the folders within that Library. If at any time you wish to return to the default view for a Library, go to the Manage menu which appears in the Explorer ribbon under 'Library Tools' and click the 'Restore settings' button.

By default under the main Libraries category there are four existing Libraries: Documents, Music, Pictures and Videos. The content in these corresponds to the content in your *My Documents*, *My Music*, *My Pictures* and *My Videos* folders respectively. It also includes the contents of the non-user-specific *Public Documents*, *Public Music*, *Public Pictures* and *Public Videos* folders as relevant, each found under the *\Users\Public* directory. I don't recommend deleting these Libraries, as they are linked to Windows functionality; hide any Library you don't want instead.

Fortunately, you are not confined to these Libraries or their default contents. You can modify Libraries as you wish by opening File Explorer and following the steps below.

Add or Delete Library

To add a new Library, right-click on the main Libraries category heading and select New>Library. You can name this Library whatever you wish, though obviously the content it will reference should help determine its name for the sake of clarity. Once you've created a new Library, you must then tell Windows the specific folder(s) to which this Library will be linked for gathering its content. To add or remove folders from a Library:

- Add Folders - Right-click on the new Library and select Properties, then click the Add button. Navigate to the folder you wish to include in this Library and select it, click the 'Include folder' button and then click Apply. Bear in mind that any subdirectories of that folder will also automatically be included.
- Remove Folders - This is an important step which needs to be done correctly. If you simply want to remove a folder from being referenced in a Library, do not delete it - this will delete the original folder and all of its contents. To properly remove a folder from a Library, right-click on that folder and select 'Remove location from library'. Alternatively, right-click on the Library, select Properties, highlight the folder in the list at the top, click the Remove button, then click Apply.

To delete an entire Library, right-click on a Library name under the main Libraries category and select Delete. This deletes the Library, but does not delete its contents - they are still stored in their original folders. All you have done is delete the virtual container that collectively referenced those files and folders.

Changing Library Icons

The icons used to represent your user-created Libraries can be changed either by selecting the Library and then clicking the 'Change icon' button under the Manage menu of the Explorer ribbon, or by right-clicking on the Library, selecting Properties and then selecting 'Change library icon'. A window with a list of generic Windows icons will open, and you can select one and click OK to apply it. If instead you wish to find or create a custom icon file of your own see the Icons section of the Graphics & Sound chapter for details.

However the icons for the four default Libraries cannot be changed in the manner above. You can change them if you manually edit the .XML definition file for the Library. To do so, follow these steps:

1. Navigate to the *\Users\[username]\AppData\Roaming\Microsoft\Windows\Libraries* directory.
2. In the right pane, right-click on the Library whose properties you wish to edit and select 'Open With'.
3. If either Notepad or WordPad are shown, select them here. Otherwise select 'Try an app on this PC' and select Notepad or WordPad in the available list. If these methods don't work, see the 'Add Open with Notepad Context Menu Item' tip under the Advanced Features section below, and use that method.
4. Once open in a text editor, look for the line with the `<iconReference>` tags. If this line exists, usually close to the top of the document, the text between these `<iconReference> </iconReference>` tags points to the location of the icon to be used. In most cases it will be a reference a location in a default Windows icon storage file, like *imageres.dll*. Make a note of its existing contents in case you wish to undo this change.
5. If you can't find an `<iconReference>` line, then manually insert one at the bottom of the file, one line above the last `</libraryDescription>` tag. Whether it exists or not, the line must look like the following for this to work:

   `<iconReference>`*`[path to valid .ico file]`*`</iconReference>`

   Where the path to the valid .ICO file should be a full reference to where a custom icon definition file exists, e.g.:

   `<iconReference>`*`C:\users\user1\pictures\favicon.ico`*`</iconReference>`

6. Save the file and the change will be implemented immediately. To undo this change, simply delete the `<iconReference>` line, or revert it back to the content it previously held.

Once again, refer to the Icons section of the Graphics & Sound chapter for details of how to find or create valid icon files.

DISABLING LIBRARIES

There is no proper user-based method to completely disable every element of the Libraries feature, as it is fully integrated into the Windows shell. There is a method which simply removes Libraries from view in the Navigation Pane of File Explorer, and is covered under the Navigation Pane section earlier in this chapter. It is relatively safe to use because it is easily undone, and doesn't actually attempt to disable Libraries; it simply removes them from view in File Explorer, which for most people who dislike Libraries should be sufficient. Even when hidden, the Libraries can still be found under the *\Users\[username]\AppData\Roaming\Microsoft\Windows\Libraries* directory.

If you find the default File Explorer behavior of opening at the Libraries category annoying, you can also customize this easily using the 'Set File Explorer Startup Folder' tip under the Advanced Features section later in this chapter.

There is a method which attempts to remove the integration of Libraries into Windows through a large number of Windows Registry changes. This is a very risky method, and does not take into account the impact of future updates or changes in Windows which will require the presence of such Registry entries or the Library functionality. Purely for the sake of completeness I am including this tip, however given the length and complexity of the procedure involved, particularly to undo the changes, this is one of the few instances in this book where I provide download links to pre-made Windows Registry files which you can

execute to automatically make the relevant changes to your Registry and also undo them if needed: DisableLibraries.zip.

I strongly advise against performing this change. If you do proceed, at the very least use System Restore to create a new restore point, and preferably also make a full system image backup as well - see the Backup & Recovery chapter. Note that I do not normally recommend automated changes to the Registry because they encourage people to remain ignorant about how the Windows Registry works, and given the critical importance of the Registry, it is not wise to make changes to it which you do not fully understand.

One last point regarding Libraries: whether desirable or not, Libraries are now an embedded feature of Windows after their introduction in Windows 7. You don't have to actively use them, and you can minimize their presence, but I strongly advise against mangling Windows in an attempt to completely remove this core piece of functionality.

< DIRECTORY JUNCTIONS AND SYMBOLIC LINKS

If you disable (untick) the 'Hide protected operating system files' option under the View tab in Folder Options as covered in the Folder Options section earlier, you will notice that a range of new directories become visible among your personal folders. That is, under the *\Users\[username]* directory you will see additional sub-directories such as *\Application Data*, *\Cookies*, *\Local Settings*, *\NetHood* and *\Recent*. Yet when you click on them, you will get an access error. This is because they are not actual directories and don't contain anything, they are Directory Junctions, also called Junction Points. These are redirection links which point to another directory, and this is also why they are denoted with a small shortcut arrow in their icon.

Directory Junctions exist primarily for compatibility purposes, so that when an application not originally designed for more recent versions of Windows attempts to put files or folders under a non-existent directory in your personal folders, such as the *\Application Data* directory for example, the *\Application Data* junction automatically sends that data to the correct *\AppData\Roaming* directory in Windows 8. This allows the application's requirements to be satisfied, maintaining its functionality without any errors or the need for user intervention, while placing the data in the correct location for Windows 8 to use.

To test a Directory Junction's functionality for yourself, right-click on an existing file anywhere on your system and select copy, then right-click on a Directory Junction and select Paste - a copy of the file will instantly be placed in the directory to which the Junction points to.

Under Windows 8 the junctions under your personal folders point to the following real directories:

Junction / Windows XP Directory	Corresponding Windows 8 Directory
Application Data	\AppData\Roaming
Cookies	\AppData\Roaming\Microsoft\Windows\Cookies
Local Settings	\AppData\Local
My Documents	\My Documents
My Documents\My Music	\My Music
My Documents\My Pictures	\My Pictures
My Documents\My Videos	\My Videos
NetHood	\AppData\Roaming\Microsoft\Windows\Network Shortcuts
PrintHood	\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
Recent	\AppData\Roaming\Microsoft\Windows\Recent Items
SendTo	\AppData\Roaming\Microsoft\Windows\SendTo
Start Menu	\AppData\Roaming\Microsoft\Windows\Start Menu
Templates	\AppData\Roaming\Microsoft\Windows\Templates

The table above is particularly useful for Windows XP users who may be confused as to where data previously held under the personal folders in XP now exists in Windows 8. For Windows Vista and 7 users, the personal folders remain much the same, except that the *Recent* folder has been renamed *Recent Items* between Vista and Windows 8.

A Directory Junction is actually part of a feature first introduced in Windows Vista called Symbolic Links. A Symbolic Link is like a shortcut, except a shortcut is actually a type of file (.LNK), whereas a Symbolic Link is not a file; it is a redirection which exists at the file system level in NTFS. It can point to anywhere, whether a file, a directory, or even another drive.

You can rename or delete Directory Junctions and other Symbolic Links just like any other file or folder, but to undertake advanced manipulation of them, particularly if you wish to create a Symbolic Link of your own, you must use the `MKLink` command. Open an Administrator Command Prompt and type `MKLink /?` for a full list of parameters.

Note that you can delete a Symbolic Link and it will not delete the file or folder to which it is linked.

These features are not designed for the average user, they are more an internal mechanism for Windows to automatically maintain compatibility with older applications, and generally speaking, you should not need to create or alter Directory Junctions or Symbolic Links unless troubleshooting a problem with an old program.

< ADVANCED FEATURES

The following are some features of File Explorer that go beyond its common functionality, including tips and tweaks for making Explorer easier to use.

SET FILE EXPLORER STARTUP FOLDER

If you usually open File Explorer from a shortcut, this procedure allows you to set which directory it will open in when launched from that shortcut. By default the existing shortcuts to File Explorer, such as the folder icon in the Taskbar, open File Explorer in the Libraries category. To alter this behavior do the following:

1. To customize an existing File Explorer shortcut, right-click on the shortcut and select Properties. To create a new custom shortcut to File Explorer right-click on an empty area of the Desktop and select New>Shortcut. For the existing Explorer folder icon in the Taskbar, right-click on the icon, then right-click again on the 'File Explorer' entry in the bottom section of the Jump List which opens and select Properties.
2. In the Location or Target box use the following:

   `%windir%\explorer.exe /e, path`

   In place of *path* above you should enter the actual path to the directory you want open by default, e.g.: *C:\User\User1\Downloads*. The path does not require quote marks around it, however make sure not to forget the comma and single blank space after the `/e` switch and before the path.
   For example:

   `%windir%\explorer.exe /e, C:\Users\User1\Downloads`

   If you omit the path (i.e. no text is entered after the `/e,`), this will simply open File Explorer in the Computer category instead.
3. For existing shortcuts, click the Apply button; for a new shortcut, click Next, then name the shortcut something appropriate, like File Explorer, and click Finish.

4. This shortcut can now be used to always open a File Explorer window in the directory specified.

Note that if the Taskbar folder icon is altered as above, other instances of File Explorer launched from normal shortcuts will now be shown as separate icons in the Taskbar.

If at any time you quickly want to open File Explorer at any particular folder on your system, go to the Start Screen and type either a partial or full path to the folder (without quotes), then press Enter. This will automatically open a File Explorer window on the Desktop at the specified path. In the case of your default Libraries, simply enter their name on the Start Screen and press Enter - File Explorer will open on the Desktop in that Library. Note further that instead of typing on the Start Screen, you can paste a path which has been copied onto the clipboard (e.g. by using the Copy path function in Explorer); just press CTRL+V on the Start Screen to paste the path, then press Enter to launch it in Explorer.

MANIPULATE MULTIPLE FILES

If you have a range of files you want to manipulate together - e.g. move, copy, rename, or change the properties of all of them - you can do so rapidly in File Explorer using the methods below.

Highlight the group of files you want to manipulate in one of three ways:

- Hold down the SHIFT key and left click on the first file in the group, then while still holding down SHIFT, left click on the last file in the group and everything in between will also be highlighted.
- Hold down the CTRL key and click on any individual files you want to select or deselect until all the relevant files are highlighted.
- Under the Folder Options component of the Windows Control Panel enable the 'Use check boxes to select items' option under the View tab, then select individual files using the check boxes which appear when you hover your mouse cursor over them, or select all files in a column by ticking the check box at the top of the column.

You can also combine these methods, e.g. SHIFT select a large range of files, then use CTRL or the check box method to add or remove individual files to or from the already highlighted ones.

Now, without clicking anywhere else, you can:

- Drag and drop these files to another folder or drive to move them.
- Hold down CTRL while dragging and dropping to copy them.
- Hold down ALT while dragging and dropping to create shortcut links to them.
- Right-click on the first highlighted file you want to manipulate and select Rename, Copy, Delete, Properties or any other available options.

If you choose to rename the files, all the highlighted files will be renamed with the same name you gave the first file, however they will also automatically be assigned a number in brackets at the end of their filename. For example, if you rename the first in a series of highlighted photo files *SummerHoliday.jpg*, the remaining highlighted files will automatically be renamed *SummerHoliday (1).jpg*, *SummerHoliday (2).jpg,* and so on.

One last tip: If you make a mistake and wish to undo a copy, move, delete, rename etc., then before doing anything else, immediately right-click on an empty area of a folder in File Explorer and select 'Undo *[action]*', or press CTRL+Z.

EXPLORER RESTART SUBSTITUTE FOR REBOOT

There is a method of doing a reboot of the Explorer process as a substitute for having to do a full restart of Windows under certain circumstances. This is done as follows:

1. Close all open instances of File Explorer.
2. Open Task Manager - see the Task Manager section of the Performance Measurement & Troubleshooting chapter.
3. Under the Details tab right-click on the *Explorer.exe* process and select 'End Process' - do this for every instance. Confirm the End Process prompt. Parts of the Taskbar and screen background will go blank.
4. Still in Task Manager, go to the File menu and select 'Run new task'.
5. Type *explorer* in the box which opens and press Enter. Explorer will be reloaded and the interface should return to normal.

This method can help resolve problems with the Windows interface showing glitches or being unresponsive, or if a particular file or program is not responding. Furthermore, if you've implemented a Windows Registry change, then restarting Explorer will often implement the change without having to restart Windows. However this method does not replace the need to reboot in most other circumstances, such as during the installation of certain drivers, Windows updates, or after serious errors.

DUAL WINDOW EXPLORER VIEW

If you want to undertake more complex file copying/moving between various folders/drives on your system, File Explorer can be combined with Windows 8's Snap feature - covered in detail under the Graphics & Sound chapter - to provide a more efficient method of utilizing the Explorer interface. Follow these steps:

1. First open two separate instances of File Explorer. A quick way to do this is to left-click on the folder icon in Taskbar once to open the first instance, then middle-click on the folder icon again.
2. Drag one File Explorer window to the far left of the screen until Snap automatically resizes it to fill exactly half the screen.
3. Drag the second File Explorer window to the far right of the screen until Aero Snap resizes it to fill the other half of the screen.
4. A quicker way of doing Steps 2 - 3 above is to only have the two File Explorer windows open on your Desktop, then right-click on an empty area of the Taskbar and select 'Show windows side by side'.
5. You now have two separate File Explorer windows, in effect simulating a dual-window file manager interface. You can choose the source directory in the left window, and in the right window you can select a destination directory.
6. To quickly move files between the Explorer windows, select the relevant file(s) and drag and drop between the open windows. To copy files instead of moving them, hold down the CTRL key while dragging and dropping.

When you're done, close one Explorer window, then grab and move the other one back towards the center of the screen - it will resize to its default size and location. Alternatively, you can just close both Explorer windows and the next time you launch File Explorer it will open with its default size and location intact.

CUSTOMIZE FOLDER ICONS & FOLDER PICTURES

Most folders in File Explorer use an image of an open yellow folder as their icon - this is called the Folder Icon. Often, another smaller image is also displayed within the Folder Icon, representing the type of data stored in that folder - this is called the Folder Picture. Both of these can be customized by following these steps:

1. Open File Explorer and navigate to the folder you wish to customize. Note that you must go to the folder by expanding the full path found under the Computer category in the Navigation Pane, particularly if customizing a personal folder, because the shortcuts to the personal folders found under the user account category of the Navigation Pane do not display all the customization options we need.
2. Right-click on the folder in question and select Properties.
3. Under the Customize tab, you can choose to change the Folder Picture and/or Folder Icon.
4. To change a Folder Picture - which is the picture that appears within the Folder Icon image of an open yellow folder - click the 'Choose File' button and navigate to a valid file. Most standard picture and icon formats are supported. Highlight the appropriate file and click Open to select it, then click the Apply button. To undo this change at any time, come back here and click the 'Restore Default' button, then click Apply.
5. To change the Folder Icon - which is the actual icon used to represent the entire folder (and which can override the Folder Picture) - click the 'Change Icon' button and either select another standard Windows icon, or Browse to another location with a valid icon stored in a .DLL, .EXE or .ICO file format. To undo this change at any time, come back here, click the 'Change Icon' button, then click the 'Restore Defaults' button, and click Apply.

The icon or picture you've selected should be applied immediately and visible in File Explorer. Wherever your folder is referenced with an icon, the icon should also have changed. Note that if you delete the original .ICO icon file you pointed to in Step 5 above at any time, the customization will be lost. Also, it is recommended that you use proper scalable icons so that the Folder Icon does not appear pixelated at higher resolutions and sizes. There are a range of proper scalable Windows icons you can view and use in the *Imageres.dll* and *Shell32.dll* files found under the *\Windows\System32* directory.

If the icons you've applied don't appear to be working, first close and reopen File Explorer and check again, then use the Repair Incorrectly Displayed Icons tip found under the Icons section of the Graphics & Sound chapter to rebuild the Icon cache. Also refer to that section for more details of Windows icon creation and customization.

EXPANDED CONTEXT MENUS

A context menu is the small menu which pops up when you right-click on various components, such as a file, folder or icon, whether in File Explorer or on your Desktop. If you want to view an 'expanded' context menu for a particular item, hold down the SHIFT key while right-clicking on it. You'll see additional options such as 'Copy as Path', or other options depending on the particular file, folder or desktop icon. Interestingly, the 'Send To' context menu item also has a range of additional options when using the SHIFT right-click method - typically all of your personal folders will also be shown along with the standard items in Send To.

EDIT CONTEXT MENUS

When you right-click your mouse button on any location you will see a range of context menu entries. As the name implies, the entries are dependent on the context in which the right-click was used, whether it was on a file, folder, an empty location on the Desktop, and so forth. Unfortunately some of the entries in the context menu have been unnecessarily inserted by programs you have installed, and you may wish to remove these.

The first step in getting rid of any unwanted entries involves opening the programs to which the entries relate and looking through the program's options to see if you can unselect any 'shell integration' or 'context menu' settings they have. If that doesn't work or is not possible, you can use several other methods to find and remove these entries. Before making any changes to your context menus, make sure to use System Restore to create a new restore point, as some of these changes cannot be easily undone.

Autoruns

The free Autoruns startup identification utility can be used in a relatively straightforward manner to temporarily disable or permanently remove context menu entries. For full details of how to download and use Autoruns, see the Startup Programs chapter.

For the purposes of editing context menu entries, launch Autoruns and look under the Explorer tab. The majority of the entries here will be context menu entries of one type or another. The Description, Publisher and Image Path columns should provide sufficient information to identify which Autorun entries relate to which particular context menu items. Untick any you wish to temporarily disable, then close Autoruns, reboot your system and check to see if the undesirable context menu entries are gone. To permanently remove an item, right-click on it and select Delete, though note that it may reappear if that the program or driver it relates to is updated.

ShellMenuView

The free ShellMenuView utility is an automated tool which displays all static context menu items. Download and run the *shmnview.exe* file to launch the utility - no installation is required. The interface is confusing at first, but keep in mind that most standard Windows entries are not being displayed as long as the 'Hide standard menu items' option is ticked under the Options menu, so the bulk of these entries relate to third party programs.

Each entry under the 'Menu Name' column is precisely that, the name of a menu entry in one of the context menus on your system. To determine which entries apply to which particular applications, look under the Description and 'Product Name' columns. Highlight the entries you believe you wish to remove, right-click and select 'Disable selected items', and check to see if this removes the relevant entries from your context menu. If not, you can easily undo this by highlighting the same entries, right-clicking and selecting 'Enable selected items'. If you can't disable an item properly, close the program, right-click on the *shmnview.exe* file and select 'Run as Administrator' to launch it again with full Administrator privileges.

ShellExView

Some context menu entries are not static; they enable additional functionality which makes them a shell extension. You can use the free ShellExView utility, which is similar to ShellMenuView above, to view and adjust these. Download and run the *shexview.exe* file to launch the utility - no installation is required. The interface is once again slightly confusing at first, however non-Windows shell extensions are highlighted in pink by default, as long as the 'Mark non-Microsoft extensions' option is ticked under the Options menu. Right-click on any extension you wish to disable and select 'Disable selected items'. Test to see if this disables the context menu item, however you will likely have to reboot first to see the impact of the change. If you can't disable an item properly, close the program, right-click on the *shexview.exe* file and select 'Run as Administrator' to launch it again with full Administrator privileges.

Windows Registry

The utilities above are recommended for most users as they are automated and provide safeguards to more easily undo changes. However if you wish to manually (and hence permanently) remove the context menu entries directly in the Windows Registry, look under the following locations using the Registry Editor:

```
[HKEY_CLASSES_ROOT\*\shellex\ContextMenuHandlers]
[HKEY_CLASSES_ROOT\AllFilesystemObjects\shellex\ContextMenuHandlers]
[HKEY_CLASSES_ROOT\Directory\shellex\ContextMenuHandlers]
[HKEY_CLASSES_ROOT\Directory\Background\shellex\ContextMenuHandlers]
[HKEY_CLASSES_ROOT\Drive\shell]
[HKEY_CLASSES_ROOT\Drive\shellex\ContextMenuHandlers]
[HKEY_CLASSES_ROOT\Folder\shell]
[HKEY_CLASSES_ROOT\Folder\shellex\ContextMenuHandlers]
```

The subfolders above are locations which hold most context menu entries in Windows. Under each, aside from standard Windows items such as `Sharing` or `Offline Files`, you may find keys or values which relate to particular third party programs. Right-clicking on the relevant program key and selecting Delete will remove its context menu entries. In most cases as you remove unwanted program entries, you can test the effects immediately by checking to see if the relevant entry was removed from the context menu. In some cases - mainly with shell extensions - you may need to reboot to see the effects. There is no undo function in Registry Editor, so make sure to back up the relevant branch before editing it. See the Windows Registry chapter for full Registry editing instructions.

Edit 'Open With' Context Menu

Whenever you open a particular type of file with a program, it will usually be added to the 'Open With' context menu for that file type. To edit the programs which are included in this list for a particular file extension, first open the following location in the Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts]
```

You can select the relevant file extension from the list of subfolders shown when you expand `FileExts`. Once you have found the extension for the file type that you wish to change the 'Open With' context menu entry, expand it and underneath you will typically find an `OpenWithList` and/or `OpenWithProgids` keys. In general, entries under `OpenWithProgids` can be deleted, but the default handler is typically a Windows-specific command that should not be deleted.

In most cases where there is a list of entries shown in the 'Open With' context menu, you can delete unwanted entries by going to the `OpenWithList` key for that extension. For example, to edit the 'Open With' context menu list for the .JPG image file extension, go to the `.jpg` key here, then select the `OpenWithList` key under it, and in the right pane you should see a list of STRING entries, such as the ones below:

```
a=PhotoViewer.dll
b=mspaint.exe
c=iexplore.exe
```

Each value corresponds with a particular program which is shown as an entry in the 'Open With' context menu for that particular file extension. Right-click on value(s) for the program(s) you wish to remove and select Delete, and they will be immediately removed from the relevant 'Open With' context menu.

Edit 'New' Context Menu

If right-clicking on a blank area in File Explorer, the New option appears in the context menu, and when selected, shows a range of programs for which you can create a new file. By default, certain Windows entries such as 'Text Document' appear here, which creates a new blank .TXT file if selected. However there are other entries here automatically added by various programs which may be undesirable, and which can be removed.

To remove any of these entries, first create a new file for the relevant program and look at its file extension. Then go to the [HKEY_CLASSES ROOT] folder in the Registry, expand it and look for that same file extension.

For example, the 'Microsoft Word Document' New context menu entry creates a blank new .DOCX file when selected, so in the Registry go to:

[HKEY_CLASSES_ROOT\.docx]

Then expand the .docx subfolder and keep expanding any subfolders until you find the ShellNew key (in this case, [HKEY_CLASSES_ROOT\.docx\Word.Document.12\ShellNew]). Right-click on ShellNew and delete it to remove 'Microsoft Word Document' from the list of programs shown under the New context menu. You can view the results immediately without needing to reboot, so check to see if the desired entry has been removed, and repeat the process as many times as required until all unnecessary program entries have been removed from the New context menu.

Alternatively, if you want to add a program to the New context menu, go to the [HKEY_CLASSES ROOT] folder in the Registry, right-click on the relevant file extension and select New>Key, and name this new key ShellNew. Left-click on ShellNew and in the right pane of Registry Editor, right-click in an empty area and select New>String Value, and call it NullFile - it doesn't need any value assigned to it. A new entry will now be added to your New context menu for that particular program/file extension, and when selected, it will create a blank new default file with the relevant extension.

EDIT 'SEND TO' CONTEXT MENU

When you right-click on most files or icons, you will see a 'Send To' context menu item which has further options to select. Typically you will see options like sending the file to a Compressed folder, the Desktop (as a shortcut), or to a particular Library. You can edit the list which appears in the 'Send To' context menu by going to the following folder in File Explorer:

\Users\[username]\AppData\Roaming\Microsoft\Windows\SendTo

To remove any item from the 'Send To' context menu, simply delete it from this folder, or preferably move it to another folder to keep as a backup. To add a new 'Send To' item, such as a new folder or program, simply copy its shortcut into this folder.

ADD 'COPY TO' AND 'MOVE TO' CONTEXT MENU ITEMS

Windows 8 has added the 'Copy To' and 'Move To' commands to File Explorer, found under the Home menu in the ribbon. If you want quicker access to these commands, you can add them to your context menus. Go to the following location in the Windows Registry:

[HKEY_CLASSES_ROOT\AllFileSystemObjects\shellex\ContextMenuHandlers]

```
Copy To= {C2FBB630-2971-11d1-A18C-00C04FD75D13}
Move To= {C2FBB631-2971-11d1-A18C-00C04FD75D13}
```

To add one or both of these items to your context menu, create a new key under the ContextMenuHandlers folder - that is, right-click on the ContextMenuHandlers subfolder, select New>Key, and name it Copy To or Move To as desired. Then left-click once on this new key, go to the right pane in Registry Editor and double-click on the (Default) entry and assign the appropriate value data as shown above, including the parentheses around the numbers. This will create a new context menu entry that allows you to select either 'Copy To Folder...' or 'Move To Folder...' in the context menu for a particular file

or folder, and then select the location to copy or move them to. To remove either of these entries simply delete the relevant entry you created above in Registry Editor.

ADD 'OPEN WITH NOTEPAD' CONTEXT MENU ITEM

If you want to quickly open any file using Notepad, you can add a new 'Open with Notepad' context menu item by going to the following location in the Registry:

```
[HKEY_CLASSES_ROOT\*\shell\]
```

Right-click on the subfolder above, select New>Key and call it `Open with Notepad.` Then right-click on this new key, select New>Key again to create a new key under it called `command,` with the final result looking like this:

```
[HKEY_CLASSES_ROOT\*\shell\Open with Notepad\command]
```

Select the `command` subfolder and in the right pane, double-click on the `(Default)` entry and enter the following value data exactly as shown:

```
notepad.exe %1
```

Now whenever you right-click on any file it will have a new context menu entry called 'Open with Notepad', which when selected opens that file instantly in Notepad, making text editing much easier. To remove this context menu entry simply delete the `Open with Notepad` subfolder in Registry Editor.

INCREASE MENU DISPLAY SPEED

You may wish to alter the speed with which certain menus open in Windows, such as sub-menus under context menus on the Desktop. By default Windows waits just under half a second before opening a menu, to prevent accidental opening of menus. You can adjust this delay by going to the following location in the Registry:

```
[HKEY_CURRENT_USER\Control Panel\Desktop]

MenuShowDelay=400
```

The default delay is 400 milliseconds (1000 milliseconds = 1 second). You can lower this value to increase menu responsiveness. You will need to restart Windows or logoff and logon to see the impact of this change.

Note that the speed with which many menu-like features are opened, such as Thumbnail Preview windows in the Taskbar, are based on other settings - see the Taskbar section of the Graphics & Sound chapter for a method of altering this. Also see the Personalization section of the Graphics & Sound chapter for Visual Effects settings which can disable various animation effects and thus further increase responsiveness.

FIX CHANGING FOLDER VIEWS

This is an issue which first came to prominence in Windows Vista, and can still occur in Windows 7 and 8, although it is unlikely if you set your folder views correctly as covered under the 'Correctly Setting Folder Views' section earlier in this chapter. If your folder views in Explorer-based interfaces are constantly being changed or shown incorrectly, even after you have followed the steps earlier in this chapter, then follow these instructions to fix this issue permanently. Go to the following location in the Windows Registry:

```
[HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\
Windows\Shell\Bags]

[HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\
Windows\Shell\BagMRU]
```

Right-click on the `Bags` subfolder in the left pane and select Delete, then do the same thing for `BagMRU`. This will remove most existing customizations for things like window sizes, positions and views. While still in the same place in the Registry Editor, you will need to manually recreate one of these keys with a new setting. Right-click on the following subfolder in the left pane:

```
[HKEY_CURRENT_USER\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell]
```

Create a new key called `Bags` to replace the one you just deleted. Right-click on `Bags`, select New>Key and name this new key `AllFolders`. Right-click on `AllFolders`, select New>Key and name this new key `Shell`. The end result should look like this in Registry Editor:

```
[HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\
Windows\Shell\Bags\AllFolders\Shell]
```

Now left-click on the last `Shell` key and in the right pane right-click in an empty area and select New>String Value. Name this new value `FolderType` and once created, double-click on it and in the Value Data box enter `NotSpecified`.

These steps will reset your folder views such that they can be customized again using the instructions under the 'Correctly Setting Folder Views' section of this chapter, this time without being changed once you've adjusted them.

There is one last step which can help ensure these settings remain fixed: increasing the number of customized folder views Windows can hold. To do this, go to the following location in the Registry:

```
[HKEY_CURRENT_USER\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell]
```

Left-click on the `Shell` key and in the right pane, if you can see `BagMRU Size` then there is no need to undertake this step. If it isn't there however, right-click and select New>DWORD 32-bit Value and name it `BagMRU Size`. Now set this value to 10000 in Decimal view.

The above steps should ensure that your folder views are reset, and once adjusted by you, don't change again unless you change them manually. If you still find your folder views resetting or changing every once in a while, even after following the steps above, it indicates that you may have data corruption issues (e.g. faulty or overclocked RAM or CPU), or a particular program you have installed is constantly interfering with Explorer-based views in the Windows Desktop interface.

GOD MODE

Dubbed God Mode, there is a method which allows you to create a custom link in File Explorer which when clicked displays a collective list of particular functions in Windows 8. This method uses Namespace Junctions to create a virtual folder as detailed in this Microsoft Article. Open File Explorer, right-click in an empty area in the right pane, select New>Folder and name it exactly as shown below:

```
Windows Control Panel.{ED7BA470-8E54-465E-825C-99712043E01C}
```

The folder will turn into a link which, when clicked, lists all of the individual features and settings available under the Windows Control Panel. This may be useful for some people who wish to pin a detailed list of settings to the Start Screen for example. Bear in mind though that it provides no additional functionality than that found in the actual Windows Control Panel and its components.

If you wish, there are a large number of other such links you can create for specific Windows features by renaming an empty folder in the format:

```
name.{string}
```

The name can be anything you wish, preferably an appropriate description of the component, and the relevant string (with curly brackets included) can be found in this Microsoft Article. Remember, none of these will provide any new functionality, only a different way to access existing Windows features.

File Explorer is an important component of Windows, not only because it is used so often, but also because it is the basis for managing files and folders in various built-in and third party utilities. I recommend exercising great caution when customizing or altering File Explorer beyond the details provided in this chapter. Adding a range of third party enhancements to Explorer, or installing programs which automatically do the same, can make File Explorer and Explorer-based applications use more resources, and become sluggish, or prone to crashing or freezing.

WINDOWS DRIVERS

Device drivers are the software that is necessary to give instructions to your hardware. Graphics drivers for example tell your graphics hardware what to do when displaying graphics, such as during 3D games, or when using the Desktop interface. Windows 8 comes with built-in driver support for virtually any type of common computer hardware, hence most of your hardware will operate in Windows without the need to install additional drivers. However, the built-in Windows drivers are not designed to be optimal, and do not ensure that you will get full efficient functionality out of your hardware. Thus wherever possible you need to download, install and configure the latest available Windows 8-specific device drivers for your hardware to make sure that your entire system performs optimally, with full functionality and maximum stability.

Windows 8 is based on much the same driver model used in Windows Vista and 7, which attempts to make the installation and usage of device drivers much simpler, more secure and less likely to cause critical system-wide instability. This is because much of the driver is not involved with the Kernel - the core software of Window - and thus if a device or driver malfunctions, usually the system state can be restored by restarting the driver rather than rebooting the entire system. This model also allows for better sharing of resources, making it easier to genuinely multitask without running into serious problems.

Windows 8 also improves driver compatibility, which makes finding the right drivers for your devices much easier.

There are a range of important considerations when installing and configuring drivers, and this chapter runs through these in detail.

< DRIVER COMPATIBILITY

Windows 8 provides excellent driver compatibility because it is based on the same basic driver architecture as Windows Vista and 7. This means that any hardware which ran under Windows Vista or 7 is likely to function correctly under Windows 8. If the hardware manufacturer does not provide Windows 8-specific drivers for a device, you should be able to use a driver designed for Vista or 7. For some devices, such as printers for example, you may even be able to use Windows XP drivers under Windows 8.

For a range of reasons you may still have difficulty in finding and installing compatible drivers for your devices in Windows 8. See the information below for assistance.

FINDING COMPATIBLE DRIVERS

Ideally before installing Windows 8 you should have checked your hardware's compatibility with Windows 8 as covered at the start of the Windows Installation chapter. While Windows 8 supports a wide range of hardware, certain hardware that is very old or less common may not be completely compatible. You should check your hardware manufacturer's website for the latest compatibility details. The Driver Installation section further below provides links to some of the manufacturer support sites for each of your major hardware components, but you can also find the details by checking the packaging or instruction manuals for the device, or doing a web search using the exact model name and number of your hardware.

Some manufacturers have made it clear that they will not be providing up-to-date support for older or superseded hardware, in which case you need to look for relevant Windows Vista or 7 drivers to use in Windows 8. If you still can't find a suitable driver on the web, check any discs which came with the device to see if they hold appropriate drivers that you can attempt to use.

If no appropriate driver is available for your device, then you can use Windows Update to search for any new or updated Windows 8-compatible drivers for your device. See the Windows Update section later in this chapter for details. You can also manually search for drivers using the Microsoft Update Catalog. Once at the Catalog site, install the add-on if prompted. Then you can type in your hardware's model number to see a full list of Microsoft certified drivers available for it. Note that you can sort by various columns - for example, click the 'Last Updated' column to sort the list so that the most recent drivers are shown at the top. Click the Add button to add any drivers you wish to download, then click the 'View Basket' link at the top right and click the Download button to obtain the driver for free. You can then manually install these drivers using the instructions under the Manually Updating or Uninstall Drivers section later in this chapter.

If no appropriate driver is available at all, then you can attempt to force Windows to use a generic Windows driver for a similar device, as covered under the Device Manager section of the Hardware Management chapter. If that fails, then you must simply wait for a driver to become available, whether from your manufacturer, or from Microsoft via Windows Update. Without some form of suitable driver, most devices will either not be detected, or will not function correctly. A device driver of some kind is a necessary piece of software for which there is no substitute.

Driver Installation Difficulties

If you find what you believe is an appropriate driver for the device, and it is from a trusted source, you may still have difficulties installing it. If this is the case, try the following:

- Right-click on the driver package and select 'Run as administrator' to ensure that it is properly assigned full Administrator rights for correct installation.
- Right-click on the driver package, select Properties, and at the bottom of the General tab click the Unblock button (if it exists) and click Apply to override any potential security blocks Windows has placed on the file due to it being identified as coming from an outside source.
- Right-click on the driver package, select Properties, and check under the Digital Signatures tab for more details of whether it is a signed driver. See the Driver Signature section further below for details.
- Right-click on the driver package, select Properties, and under the Compatibility tab click the 'Run compatibility troubleshooter' button to allow Windows to guide you through the detection and setting of any compatibility parameters needed to run the driver correctly.
- Right-click on the driver package, select Properties, and under the Compatibility tab tick the 'Run this program in compatibility mode for' box and set it for 'Windows 7'. You may also need to then launch the driver installation using 'Run as Administrator' to ensure proper installation in compatibility mode.

If none of these steps resolve the problem, or the drivers do not come in a standard executable driver package, then check the information in the rest of this chapter for other methods of manually installing a driver. Also check the Hardware Management and Performance Measurement & Troubleshooting chapters for details of how to troubleshoot a problematic device.

64-bit Compatibility

A critical compatibility issue for any Windows 8 user is the fact that you cannot install drivers designed for the 32-bit version of Windows 8 (or Vista or 7) on a 64-bit installation of Windows 8, or vice versa. This means that if you intend to use Windows 8 64-bit, you should check to make sure that there are appropriate 64-bit drivers for all of your key hardware components. There is no easy way to get around this requirement.

In the absence of proper 64-bit drivers for your device, you can use the built-in Windows drivers and hope that a signed 64-bit driver is released for your device via Windows Update. This may be fine as long as the device is not a key hardware component, like your graphics card for example, otherwise it may not function correctly or efficiently. Once again, be aware that in some cases the hardware manufacturer may decide to

never release 64-bit compatible drivers for old or less popular hardware, so you may need to install Windows 8 32-bit on old systems to maintain driver compatibility.

< DRIVER SIGNATURE

When a device driver is installed, it effectively becomes a part of the operating system, and has unrestricted access to much of the computer. That means you should only install drivers that come from a reputable source, typically directly from the company which manufactured the hardware for which the driver is intended. To ensure that the drivers you are installing are legitimate and have not been tampered with to include malware for example, Windows 8 prefers the installation of Signed Drivers. A signed driver has a valid digital signature which indicates that the publisher of the driver is who they claim to be, and that the contents of the driver package has not been tampered with in any way after the drivers were signed.

To check for a digital signature, right-click on the driver package, select Properties, and look under the Digital Signatures tab. Select the signature and click on the Details button for more information of when the driver was signed, and the certificate used.

Most signed drivers also carry Windows Hardware Quality Labs (WHQL) certification, meaning they have been tested by Microsoft. A Windows 8 WHQL certified driver is desirable, as it indicates that the driver has been tested to be both secure and compatible with Windows 8, and should be safe and relatively problem-free. However WHQL certification is not a guarantee of flawless operation. Furthermore, a driver does not have to be WHQL certified to be digitally signed, nor does a lack of WHQL certification indicate that the driver is problematic or insecure. It is simply preferable that a driver be WHQL certified.

SIGNATURE WARNINGS

If a driver has a valid digital signature then Windows will install it without any warnings. However if you attempt to install a driver which is unsigned, does not have a valid signature, or appears to have been altered after being signed, Windows 8 will halt installation and prompt you in one of the following ways:

Windows can't verify the publisher of this driver software: This means the driver is unsigned, or the signature cannot be verified. You should only install such drivers if you have obtained them for a completely trusted source. In most cases this should only be direct from the hardware manufacturer's site. If you are not absolutely certain of the trustworthiness of the source, do further research before installing the driver.

This driver hasn't been signed: This means the driver hasn't been digitally signed by a verified publisher, or the driver package has been altered after being signed. It could be a custom modified driver, in which case if you are aware of the risks, and downloaded it from a site you trust, you can proceed. If you downloaded it from an untrusted or unfamiliar source, such as through peer to peer or a generic file hosting site, then I recommend against installing the driver as there's a reasonable chance that it contains malware or could be problematic. If you downloaded it from a hardware manufacturer, it should be safe to install, but it is still wise to do further research and seek user feedback before installing this driver, as it could be problematic.

A digitally signed driver is required: In Windows 8 64-bit if you see this message you will not be allowed to install the driver, as it does not have a valid digital signature. This is because 64-bit versions of Windows 8 contain a feature called Kernel Patch Protection (also known as PatchGuard), first introduced in Windows Vista. PatchGuard is designed to protect the system Kernel even further. Windows 8 32-bit systems using UEFI Secure Boot now also require a digital signature. See the Kernel Patch Protection section of the Security chapter, and the Secure Boot section of the Boot Configuration chapter for more details.

There are ways in which you can use an unsigned driver and bypass these restrictions:

You can restart and enter the Windows Recovery Environment, selecting the Startup Settings feature under Troubleshooting and choosing to launch Windows with the 'Disable Driver Signature Enforcement' option. This will prevent signature checks the next time you reboot, but you will need to do this at every restart to load the unsigned driver. One workaround is to use a Sleep mode so that you don't have to reboot of your PC very often after enabling this option. See the System Recovery section of the Backup & Recovery chapter for details on the Windows Recovery Environment.

Alternatively, if you wish to disable signature checking and keep it in effect through every reboot, you can do so by using the TESTSIGNING boot option, as covered in this Microsoft Article. When this option is used, it will allow drivers that are not signed with a valid certificate to load at bootup. Windows will display a "Test Mode" watermark in the lower right corner of the Desktop when this boot option is in effect.

To alter this option, follow these steps:

1. Open an Administrator Command Prompt.
2. To disable signature checks, type the following and press Enter:

```
Bcdedit -set TESTSIGNING ON
```

3. Reboot to implement the change.
4. To re-enable normal signature checks, type the following and press Enter:

```
Bcdedit -set TESTSIGNING OFF
```

5. Reboot and Windows will once again start in normal mode.

This method may not work with completely unsigned drivers.

SIGNATURE VERIFICATION

If your system is suffering from problems and general instability, it might be a good idea to check to see precisely how many unsigned drivers you have on your system, and perhaps uninstall the ones which are the least trustworthy for troubleshooting purposes. The File Signature Verification utility is a simple built-in Windows tool for quickly checking the signature status of drivers. Go to the Start Screen and type *sigverif* then press Enter. In the dialog box which opens, click the Start button and it will scan your system and display all the unsigned drivers. You can click the Advanced button in the utility and also tell it to save the results as a log file, as well as being able to view the current log file.

You can also check the WHQL certified digital signature status of your drivers by running DirectX Diagnostics with the 'Check for WHQL digital signatures' box ticked. To run DirectX Diagnostics, type *dxdiag* on the Start Screen and press Enter. See the System Information Tools section of the System Specifications chapter for more details of DirectX Diagnostics.

Installing unsigned drivers, or using any method to circumvent the checking of signed drivers, is generally not recommended unless you are absolutely certain of the trustworthiness and reputation of the source of the software. This usually means they should be direct from the relevant hardware manufacturer's website. Some manufacturers or developers release unsigned drivers which are perfectly safe and functional, typically in the form of official Beta drivers. Some driver packages may also be modified to run on hardware they were not originally designed for, and this is not a security risk as such. But you should still try to minimize the number of unsigned drivers on your system. By installing unsigned drivers you are defeating a security feature of Windows, and potentially giving malicious or problematic software unrestricted access to your system.

< DRIVER INSTALLATION

All of your major hardware devices require the latest available Windows 8-compatible drivers and related updates to function at peak performance and with stability and full functionality. Indeed many system problems are often the result of not using the latest drivers which contain fixes or workarounds for known issues. It is important therefore to check for and install all of the latest drivers for your key hardware components as soon as possible after installing Windows, and at regular intervals afterwards.

A driver typically comes in the form of an executable (.EXE) package, which you simply need to launch by double-clicking on the file, or by extracting the contents of a .ZIP archive and running a *Setup.exe* or similar file to begin installation. Some drivers may come in a form that requires manual installation, and this is covered under the Manually Updating or Uninstalling Drivers section later in this chapter.

During the installation of a driver, if you are prompted to reboot at any time, you should do so as soon as possible to allow proper driver installation. Windows 8 has a Restart Manager which is designed to automatically attempt to close down all non-critical processes and hence allow them to be updated without a full system reboot, so the installation of some drivers may not require rebooting to complete. However some device drivers may still need a reboot in order to replace files that are currently in use by the system, so reboot as often as required, and don't do anything else on your system until driver installation is complete.

The specific key updates and drivers you should install, and their preferred order, is provided below in a series of recommended steps.

STEP 1 - SERVICE PACKS

A Service Pack is a compilation of important security, stability and performance updates for Windows. On a fresh installation of Windows, the latest Service Pack should always be installed first unless your Windows 8 installation media already has the Service Pack integrated into it, such when installing Windows via the Web Setup option.

At the moment there is no Service Pack for Windows 8.

STEP 2 - DIRECTX

Install the latest version of Microsoft DirectX. As covered under the Graphics & Sound chapter, DirectX is an important component of Windows that allows advanced multimedia functionality. Windows 8 already comes with DirectX 11.1 installed. However from time to time Microsoft releases updates for all versions of DirectX. You should always run the DirectX installer at least once after Windows installation to check for and install all of the latest components for DirectX for maximum compatibility, stability and performance in multimedia and games.

STEP 3 - WINDOWS UPDATE

Windows Update is the main tool used to obtain security patches, as well as driver and feature updates in Windows 8. It is important to configure Windows Update correctly as soon as possible after installing Windows, both so you can download and install critical security updates before doing anything else.

By default Windows Update is set to run a scheduled check of the Microsoft Update site for updates every day, and to download and install them automatically as required. The information Windows Update sends to Microsoft during any update includes:

- Computer make and model.
- Version information for the operating system, browser, and any other Microsoft software for which updates might be available.
- Plug and Play ID numbers of hardware devices.
- Region and language setting.
- Globally unique identifier (GUID).
- Product ID and product key.
- BIOS name, revision number, and revision date.
- Your Internet Protocol (IP) address.

Full details of the information collected and how it is used are in this Microsoft Article.

To customize the Windows Update settings, open Windows Update from the Windows Control Panel and click the 'Change settings' link in the left pane. Each section is covered as follows:

Important Updates: These are security and reliability-related updates that are important in keeping your system operating properly. The 'Check for updates but let me choose whether to download and install them' option is recommended. This will allow Windows Update to regularly check for updates and let you know if any are found via a prompt in the Notification Area or on the Login Screen, but it will not download or install anything without your explicit consent. This lets you download and install updates at your convenience. You can also check individual updates to ensure that nothing undesirable or unnecessary will be downloaded or installed. If you are a novice user, it is safest to select the 'Install updates automatically' option instead.

Recommended Updates: These updates address non-critical problems and provide additional features in Windows. If you have followed the recommendation for the Important Updates setting above, I recommend ticking the 'Give me recommended updates the same way I receive important updates' box so that once again Windows will regularly check for and list such updates in Windows Update, but will not download or install them unless you specifically initiate the process.

Note that driver updates are usually presented as Optional in Windows Update. Optional updates are not automatically selected in Windows Update regardless of your settings here.

Microsoft Update: If ticked, the 'Give me updates for Microsoft products and check for new optional Microsoft software when I update Windows' option allows Windows Update to also check for optional Microsoft product updates, such as Office Suite updates and add-ins, updates for any installed Windows Live programs, and so forth. This is not an essential option to enable, but is recommended if you have various Microsoft products installed. Nothing will be downloaded and installed automatically as long as the 'Important Updates' setting above is set as recommended. If you can't see this option, then you may need to click the 'Find out more' link at the bottom of the main Windows Update screen and follow the prompts to enable this functionality.

Once you have changed all of these settings, click the OK button and Windows Update will automatically begin to check for updates. If not, click the 'Check for updates' link in the left pane. If any updates are found, you will see a summary of the number and types of updates available in the main Windows Update window. Click one of the links to be taken to the 'Select updates to install' screen. Notice that there may be several tabs available at the left side of the window, showing Important and Optional updates under each tab respectively. Click each tab and untick any updates that you do not wish to install. To see more details for any update, select it and look in the right pane. If you are certain that a particular update is not necessary for your PC, right-click on it and select 'Hide update' to remove it, though note that it is not permanently removed; it can be restored at any time by clicking the 'Restore hidden updates' link in the left pane of main Windows Updates screen.

Importantly, if you've just installed Windows, at this stage you should make sure all Optional updates which appear to be related to your hardware components are unticked. You should not install any drivers from Windows Update at this point until you can first install the latest version of the relevant drivers as detailed in the following steps of this chapter.

Once done, click the Install button at the bottom, or click the 'Install updates' button on the main Windows Update screen. We will revisit the Optional updates later on in Step 8 below.

I strongly recommend allowing Windows Updates to check for updates regularly, usually done automatically on a daily basis. Do not set Windows Update to 'Never check for updates' as this opens your system to the latest security exploits and vulnerabilities, which nowadays can quickly circulate around the Internet within days or even hours. For maximum security you must always install the latest Important updates as soon as they become available. See the Security chapter for more details of the types of security threats that are possible.

If you are receiving an error when using Windows Update, check this Microsoft Article for a list of common errors and solutions. If you cannot get Windows Update to work for some reason then in the interim you must manually check the updates listed on the Windows Security Updates site. Click the 'Windows 8' link on the left side, then click the Update link below it to narrow the list down to updates for Windows 8. This site is also useful if for some reason you want to download specific updates and store them, or transfer them to another machine. I do not recommend any other method or non-Microsoft site for getting security updates for Windows, as there is no guarantee of how secure they genuinely are, or what information about your system you are providing to a third party. By letting a third party site scan your system for updates, you could be letting them know all about your unsecured vulnerabilities.

Finally, by default Windows Update creates a restore point prior to installing new updates. This provides an extra layer of protection in case an update goes wrong, and you want to put your system back to the way it was before the update. This is one more reason to leave System Restore enabled. See the System Protection section of the Backup & Recovery chapter.

There's one more step to prevent Windows from automatically installing outdated drivers for any devices you connect to your PC. Open the Devices and Printers component of the Windows Control Panel, then right-click on the icon for your PC, typically with the name *[username]*, and select 'Device Installation Settings'. Select the 'No, let me choose what to do' option and then select 'Never install driver software from Windows Update', and click the 'Save Changes' button. See the Devices and Printers section of the Hardware Management section for more details.

These measures prevent Windows 8 from automatically installing any device drivers for your hardware components and peripherals which may be out of date, since device drivers found through Windows Updates are often older than those on the manufacturer's website. It also prevents installation of other software updates which are not yet necessary. This is not a permanent set of options - Devices and Printers will be reconfigured appropriately under Step 7 below, and Windows Update in Step 8 below.

Once you are certain that all important security and stability updates have been installed on your system, rebooting as often as required to complete their installation, you can then proceed to the next step.

STEP 4 - MOTHERBOARD DRIVERS

The motherboard is the hardware foundation of your entire system. Using the latest drivers for it is extremely important, as a range of functionality, including your network adapter, drive controllers, USB ports, and onboard audio, all rely on the drivers typically contained in the motherboard driver package.

Finding all the correct motherboard drivers is not necessarily a straightforward task. You will need to know the brand, model and chipset type of your motherboard. All of these details are critical in determining the correct driver to use. A combination of the utilities covered in the System Specifications chapter, along with your motherboard manual and a web search will give you all of the information you need.

It's important to understand that the motherboard chipset type is not the same as the motherboard brand or model number. The chipset type is based on the company that manufactures the actual chipset architecture used in the motherboard. The motherboard's brand is based on the company that buys this chipset, packages it with certain features, and sells it under its own brand name with a specific model number. For example, if you have an *ASUS P8Z77-V Premium* motherboard, this brand and model information deciphers itself as follows: The motherboard is manufactured by a company called ASUS; it has the specific model number P8Z77-V Premium; and it uses the Intel Z77 chipset. These are all key pieces of information required in knowing where to go for drivers, and which drivers to select.

In the first instance, your motherboard or PC usually comes with a driver disc containing the relevant motherboard drivers. However these drivers are often well out of date. The best place to look for the latest version of these drivers is on your motherboard manufacturer's website. There are too many manufacturers to list here, so check your motherboard manual, or do a web search for a link. Once at the site, under the Support or Downloads section you may find several different types of updates for your particular motherboard model. These are broken down by the general categories below:

- *BIOS* - These are not drivers, they are firmware updates for the BIOS or UEFI on your motherboard. See the Hardware Management chapter for more details.
- *Chipset* - These are the core drivers which control your motherboard's key functionality in Windows. All systems require these for optimal performance and functionality.
- *SATA, AHCI or RAID* - These drivers are required for correct operation of your motherboard's drive controllers in Windows, and through them, your hard drives or SSDs. In certain cases you may also require drivers for correct detection of your drive configuration during the installation of Windows. See the Preparing the Drive section of the Windows Installation chapter for details.
- *Video or VGA* - If you are using your motherboard's onboard or integrated graphics capabilities, then these drivers are necessary. If you are using a separate graphics card, these are not necessary. Refer to Step 5 of this chapter.
- *Audio* - If you are using your motherboard's onboard or integrated audio capabilities, then these drivers are necessary. If you are using a separate sound card, these are not necessary. Refer to Step 6 of this chapter.
- *USB* - If you are using the USB ports on your motherboard, you may require separate USB drivers for correct functionality, although typically this feature is incorporated into the Chipset driver package.
- *LAN* - If you are using your motherboard's onboard network controller, whether for an Internet connection, or a local connection to a network of computers, then these drivers are necessary.

There may be additional drivers for other specific functionality on your motherboard, but the ones above are the most important, particularly the Chipset and SATA/RAID drivers.

If you are not using a particular function on your motherboard, I strongly recommend disabling it in your BIOS/UEFI as detailed in the Hardware Management chapter. This will prevent Windows from automatically detecting and installing built-in drivers for it as part of Step 8 further below, and in turn this reduces resource usage and speeds up Windows startup.

If there are no appropriate drivers on your motherboard manufacturer's site, or they appear to be fairly old, you must first identify your chipset type, then you can download the latest drivers directly from one of the major chipset manufacturers:

§ For **Intel** chipset motherboards, download and install the latest Intel Chipset Software.
If you also have a RAID or AHCI setup, also install the Intel Rapid Storage Technology Driver.
§ For **AMD** chipset motherboards, download and install the AMD Chipset Drivers.
§ For **Nvidia** chipset motherboards, download and install the latest nForce Drivers.
§ For **VIA** chipset motherboards, download and install the latest VIA Hyperion Drivers.

Note that some of these drivers may contain a mix of components, including chipset, SATA/RAID, USB and LAN drivers all in one package. Read the driver notes on the site for more details.

Furthermore, if you are updating an Intel chipset motherboard using the latest chipset driver on a system which has already had Intel chipset drivers installed on it in the past, as opposed to a fresh new install of Windows, you will need to follow these instructions:

1. Download the latest Intel Chipset Software.
2. Right-click on the driver package and select 'Create Shortcut'.
3. Right-click on the new shortcut and select Properties.
4. In the Target box under the Shortcut tab, go to the very end, insert one blank space and then type the following:

   ```
   -overall
   ```

   e.g., `C:\Users\User1\Downloads\INF_allOS_9.3.0.1025_PV.exe -overall`
5. Click Apply then click OK.
6. Launch from the shortcut to install the drivers.

The `-overall` switch added to the driver launch command will ensure that the chipset driver package correctly overwrites existing versions of your key Intel motherboard drivers with any newer versions if available. Note that you may then need to then reboot and (re)install the latest Intel Rapid Storage Technology driver, as the chipset driver may incorrectly detect your drive controllers.

STEP 5 - GRAPHICS DRIVERS

Install your graphics card video drivers. Just as with motherboards, graphics chipsets are developed by one company and then sold to different manufacturers who then package them together with certain features and capabilities and market them under their own brand name. The important thing to know is the manufacturer of the chipset on which your graphics card is based - for most graphics cards this will be either Nvidia or ATI. For example, an *EVGA GeForce GTX 680* graphics card uses an Nvidia GeForce 600 series chipset, packaged and sold by the company EVGA under its own brand. The chipset is the determinant of which driver to use, not the company selling the card.

Determine your graphics card's chipset and model name using the utilities in the System Specifications chapter, then download and install the relevant package:

§ For **Nvidia** graphics cards, download and install the latest Nvidia Graphics Drivers.
§ For **AMD** graphics cards, download and install the latest AMD Graphics Drivers.
§ For **Intel** graphics cards, download and install the latest Intel Graphics Drivers.
§ For motherboards with onboard graphics, check your motherboard manufacturer's website first (See Step 4) for Integrated, Onboard or HD Graphics drivers.

Note that unlike motherboards, you do not need to download graphics drivers from your hardware manufacturer's website. For Nvidia and AMD graphics cards in particular, installing the latest reference chipset drivers available directly from the relevant chipset manufacturer as shown above is the best method, as they are typically much newer.

Importantly, Windows 8 graphics functionality has improved over the way it was implemented in Windows Vista and 7, which in turn was a major change over the way it was implemented in Windows XP. The main change in Windows 8 involves the use of a new version 1.2 of the Windows Display Driver Model (WDDM) as opposed to version 1.0 used in Vista, and 1.1 in Windows 7. While you can use WDDM 1.0 or 1.1 drivers under Windows 8, to take full advantage of advanced graphics features, you will require graphics hardware with support for DirectX 11 or higher and a WDDM 1.2-compatible graphics driver. For full details see the introduction to the Graphics & Sound chapter.

STEP 6 - SOUND DRIVERS

Install your sound card audio drivers. These vary depending on the brand of the sound card you are running. Only the major brands are covered below:

§ For **Creative** sound cards, download and install the latest Creative Audio Drivers.
§ For **ASUS** sound cards, download and install the latest ASUS Audio Drivers.
§ For **Auzentech** sound cards, download and install the latest Auzentech Drivers.
§ For **Turtle Beach** sound cards, download and install the latest Turtle Beach Audio Drivers.
§ For **Hercules** sound cards, download and install the latest Hercules Audio Drivers.
§ For **AOpen** sound cards, download and install the latest AOpen Audio Drivers.
§ For motherboards with onboard audio, first check your motherboard manufacturer's website (See Step 4). Then check your onboard audio chipset manufacturer's website, such as Realtek.

Windows 8 does not significantly change the way in which audio was implemented under Windows Vista and 7, however it is a significant departure from the way audio was implemented in Windows XP. The main difference is that standalone sound cards no longer have as much importance in Windows. Windows 8 uses the Universal Audio Architecture (UAA) to provide high quality audio and a range of enhancements for almost any sound device without the need for third party drivers. A proper audio driver from the manufacturer's site as listed above is still recommended for full functionality and optimal performance. For details of audio in Windows 8 see the Sound section under the Graphics & Sound chapter.

If you are using a separate sound card, and if, after updating to the latest Windows 8 audio drivers you find that you are having strange performance issues or audio problems such as crackling, distortion or disconnected sound, then I recommend that you consider disabling or physically removing the sound card and trying out the High Definition onboard sound functionality which most recent motherboards have. Onboard audio is specifically designed for software-driven audio, which is what Windows 8 excels at, and hence it is less likely to be problematic. For all but high-end speaker setups, onboard audio will offer excellent audio quality without any significant performance impact.

STEP 7 - PERIPHERAL DRIVERS

Before installing any drivers or additional software for your peripherals and portable devices, such as a mouse, printer, or digital camera, first connect these devices to your system one by one. Windows 8 provides built-in support for peripherals and portable devices through a feature called Device Stage that handles most common tasks for supported devices without the need to install third party drivers or software. See the Device Stage and Printers and Devices sections of the Hardware Management chapter for more details of this functionality.

If your peripheral device appears to work fine, and all of the major functions you need are available, then do not install a driver for it. Peripheral drivers typically need to load in the background at Windows startup, increasing startup times, and adding to overall resource usage. Quite often they don't add anything of real value to the device's function beyond that already available in Device Stage. Furthermore, many software packages for peripherals install a range of unnecessary add-ons and programs which once again increase background resource usage, increase Windows startup times, and can cause potential conflicts, all for very little gain.

Obviously, should your device not function correctly, or a feature that you want appears to be disabled or is not working properly, then ultimately you will need to install a new driver for that device, as well as any necessary additional software. In these cases I recommend that you go to the device manufacturer's website and download the latest available drivers rather than using any drivers that come on the disc supplied with the device, as they are typically quite old.

In any case there are far too many peripheral device manufacturers to list here, but the website address is usually provided on the device's box and/or in the manual. Where possible follow the device installation instructions in the device's manual or on its website for the best method of installation.

If your device isn't being detected correctly, or you can't find an appropriate driver for it, or if you simply want to search for any newer drivers, go to the Devices and Printers component of the Windows Control Panel, right-click on your computer icon with the name *[username]*, select 'Device installation settings', then select the 'Yes, do this automatically' option to allow Windows to automatically search for and if necessary install newer drivers for your device from Windows Update. If this still fails, see the instructions at the start of this chapter, as well as those further below for more details of how to find and if necessary, manually install a device driver under Windows 8.

STEP 8 - WINDOWS UPDATE REVISITED

Now that you have installed all of the latest Windows 8-compatible drivers for your hardware, you should run Windows Update again to see if any newer drivers can be found for your devices, as well as any drivers for devices for which you could not manually find a driver.

Open Windows Update and click the 'Check for Updates' link in the left pane. If Windows Update finds any new drivers then click the link to view the list of driver updates found and tick any you wish to install. Click the Install button to install these drivers. Any drivers found using this method are completely safe to install as they've been tested and WHQL certified by Microsoft before being included in Windows Update, and will only be detected and shown if they are appropriate for your hardware, and are typically newer than the current driver version you are using. If you still have doubts, or simply don't wish to install a particular driver, untick the driver, then right-click on it and select 'Hide update'.

Once you have completed all of the steps above, Windows will be up to date, and your major devices should all have appropriate drivers to allow full functionality and optimal performance. If there are any devices which are not being detected correctly, or which have impaired or problematic functionality, then you may have to wait for updated drivers to be released by your hardware manufacturer.

As the last step after installing all your drivers, do a run of the Windows Experience Index. Open the Windows Control Panel, go to the System component and click on the Windows Experience Index link, then run (or re-run) the assessment. This allows Windows to correctly detect your hardware performance capabilities, and enable or disable certain features dependent on this. You can also compare your score to any previous score to see if the numbers have improved, or run other benchmarks to test and compare your performance with others. See the Performance Measurement & Troubleshooting chapter for more details on the Windows Experience Index and a range of performance measurement tools.

< MANUALLY UPDATING OR UNINSTALLING DRIVERS

To view the current version of a driver for a particular hardware component, or to update or uninstall a driver, you can use Device Manager. You can access Device Manager in the Windows Control Panel, or type *devmgmt.msc* on the Start Screen and press Enter. The general functionality of Device Manager is covered under the Device Manager section of the Hardware Management chapter, so in this section we only look at driver-related features.

VIEWING DRIVER DETAILS

To view the current version of the drivers installed for a particular hardware component in detail follow the steps below:

1. Open Device Manager and expand the category under which your particular hardware device is placed. For example, to view your monitor drivers, expand the Monitors category and your monitor(s) will be listed underneath.
2. Double-click on the device, or right-click on it and select Properties.
3. Under the Driver tab you will see the specific driver provider, date and version. If the device is using a default Windows driver the Driver Provider will usually be listed as Microsoft.
4. Click the 'Driver Details' button and you will see the specific driver files associated with that device, and where they reside on your drive. You can then click on each individual file shown, and the provider and version of that file will also be displayed just below it.

For a more user-friendly display of driver details for your major components, use the tools under the System Specifications chapter.

MANUALLY UPDATING DRIVERS

Normally, when you wish to update a device driver, the best course of action is to download the new driver package and run it. It should automatically detect your hardware and walk you through the steps necessary to update the device drivers. However, in some cases you may need to manually update a driver. For example, a driver may not come in an executable (.EXE) package, but rather as a set of files, perhaps within a .ZIP or similar archive. Follow the steps below to manually search for and install a new device driver:

1. Open Device Manager and expand the category under which your particular hardware device is placed, then double-click on the device or right-click on it and select Properties.
2. Under the Driver tab click the 'Update Driver' button.
3. You will have two options: you can either allow Windows to 'Search automatically for updated driver software'; or if you know where the driver files are stored, click the 'Browse my computer for driver software' option. The first option is recommended only if you do not already have the new driver files, or if you are a novice user - if you choose this option then follow Steps 4 - 5 below. If you have the relevant driver files, or if you feel you are more advanced, choose the second option and go directly to Step 6.
4. If you search automatically, Windows will determine where to search based on the device installation settings you've chosen in Devices and Printers: if you have selected 'Never install driver

software from Windows Update' in Devices and Printers, then Windows will only search your computer; if you've chosen 'Install driver software from Windows Update if it is not found on my computer' then Windows will search your computer for driver files first before checking Windows Update; on the other hand if you've chosen 'Always install the best driver software from Windows Update' under the Devices and Printers settings, Windows will always search the Windows Update driver catalog to see if a newer driver exists.

5. Once Windows has searched, it will install any newly found drivers, or tell you that your current version is the latest. Windows only detects and installs individual driver files, and does not look inside driver packages. So if the driver files are sitting inside an archive, or in a self-executing driver package on your system, Windows will not detect these as containing a newer driver. If you know there are newer driver files on your system and they are not being detected, go back to Step 3 and select 'Browse my computer for driver software' then follow Step 6 onwards.
6. Depending on where the newer driver files are held, if necessary insert the appropriate disc, USB flash drive or external drive and browse to a specific directory where you know the newer driver files are held - make sure the 'Include subfolders' option is ticked. Remember that Windows only sees individual driver files, not driver packages, so you may need to manually extract the contents of a driver package to an empty directory before continuing. Once at the correct directory, click Next and Windows should detect the newer driver files in that directory and install them.
7. If the above steps fail and you are certain you have newer driver files for the device, or you want to install an older or generic version of the drivers, then follow Steps 1 -3, selecting 'Browse my computer for driver software', but this time select 'Let me pick from a list of device drivers on my computer'. This provides a list of all the drivers which have been installed on your system to date and whose files still reside on your system.
8. In most cases you will not want to reinstall an existing driver, so click the 'Have disk' button and insert/attach or browse to the drive and directory where the newer driver files reside. If an appropriate .INF file is found, click on it and click Open. If your hardware is supported by that driver file you can select the specific driver to install.
9. If nothing else works and you wish to attempt to install a driver originally designed for a device similar to yours, then follow Steps 1 - 3 above, then Step 7. Then untick the 'Show compatible hardware' box and you will see a much wider range of drivers. Select one which you believe would be most compatible with your device, though clearly if you select a driver not meant for your specific device, you may not be allowed to install it, or it may result in a lack of correct functionality or major problems. This is a last resort option.

GOING BACK TO AN EARLIER DRIVER

If you have recently installed a driver which you believe is causing you problems, then you may wish to go back to the previous driver version you were using. To do this follow these steps:

1. Open Device Manager and expand the category under which your particular hardware device is placed, then double-click on the device, or right-click on it and select Properties.
2. Under the Driver tab click the 'Roll Back Driver' button. If it is not available then you do not have any earlier driver versions installed, or they may not be detected - see the manual instructions further below.
3. Confirm whether you want to do this, and your current drivers will be replaced with the previously installed version.

Another method is to go to the System component of Windows Control Panel, click the 'System Protection' link in the left pane, and click the 'System Restore' button. You can now follow the prompts to go back to a previous restore point, undoing any changes wrought by a recent driver install.

SELECTING ANOTHER INSTALLED DRIVER

If you wish to install a specific version of a driver, and you believe it already exists on your system (e.g. it was installed in the past and not uninstalled), you can choose to install it manually. This also allows you to revert to the built-in Windows drivers for troubleshooting purposes for example. Follow these steps:

1. Open Device Manager and expand the category under which your particular hardware device is placed, then double-click on the device or right-click on it and select Properties.
2. Under the Driver tab click the 'Update Driver' button.
3. Click the 'Browse my computer for driver software' option.
4. Select 'Let me pick from a list of device drivers on my computer'.
5. Make sure the 'Show compatible hardware' box is ticked, and you will see all the versions of compatible drivers which are available on your system for this device. It may be difficult to determine the driver versions from this list, in which case highlight the relevant driver and untick the 'Show compatible hardware' box to show you the driver's manufacturer. This will at least let you know which is a standard Microsoft driver.
6. Select the driver you want to install and click Next to install it.

If you see more than 2 or 3 installed non-Microsoft drivers under Step 5 above, then this indicates that you have not properly removed previous versions of drivers from your system. This driver residue can cause problems. If you believe a driver is the cause of any issues on your system then I recommend cleaning out your drivers and installing only the latest version, or the version which you know works best on your system - see the details below.

UNINSTALLING DRIVERS

You should not maintain multiple versions of a driver for any device on your system, as these leave various bits and pieces, known as "driver residue", on your system. This increases the potential for driver-related problems, especially if you ever go backwards in driver version. This is because different versions of various driver files and Registry entries may inadvertently be used together by Windows.

To correctly uninstall a driver package through Windows, you should first go to the Programs and Features component of the Windows Control Panel. On the main screen you will see most of the programs, updates and drivers currently installed on your system. Look for the driver manufacturer or relevant device name in the list, and if found highlight the item (or right-click on it) and select Uninstall, thus removing it. This does not guarantee that all traces of the driver have been removed from your system - see the next section.

If a driver is not listed in the Programs and Features list, you can uninstall it manually:

1. Open Device Manager and expand the category under which your particular hardware device is placed, then double-click on the device or right-click on it and select Properties.
2. Under the Driver tab click the Uninstall button.
3. Make sure to tick the 'Delete the driver software for this device' check box if available. If this option is not available, it means you are already using a default Windows driver for the device, in which case you should not continue attempting to uninstall the device unless you want the default driver to reinstall itself for some reason.
4. Click OK and the device will be uninstalled, and its currently-used driver files will also be removed from your system, which is desirable. Restart your PC as prompted to complete the process. When uninstalling certain devices, such as your graphics card or monitor, your display may go black. If after a period of time no image reappears, press the power or restart button on your PC to tell Windows to shut down or restart the PC.
5. Once your system restarts, your hardware will be automatically redetected by Windows and the next available driver, or the default Windows driver, will be installed.

REMOVING STORED DRIVERS

Whenever you upgrade your drivers or install a new driver in Windows, unless you uninstall the previous version, it may be stored by Windows, or its files and Windows Registry entries may remain on your system. Sometimes even a full uninstall of a driver or program may leave driver residue throughout your system because of a faulty uninstaller, or even as a deliberate measure by the device manufacturer. The upshot of all this is that over time, particularly for users who frequently upgrade and downgrade their drivers, various versions of driver files will come to be stored on your system. There are several methods you can use to remove the bulk of these unnecessary files and system entries.

Autoruns

You can use the free Autoruns utility, covered under the Startup Programs chapter, to identify, disable or permanently remove any driver files which are loading up with Windows. Follow these steps:

1. Uninstall any programs or drivers you do not wish to use from the Programs and Features component of the Windows Control Panel. Reboot your system when finished.
2. Launch Autoruns and under the Options menu select 'Filter Options'. Untick the 'Hide Microsoft entries' and 'Hide Windows entries' boxes, but make sure the 'Verify Code Signatures' item is ticked, and click OK.
3. Go to the Drivers tab. Most of the entries which appear here are built-in Microsoft drivers for Windows and should not be unticked or deleted. Check any entries which are color-coded, and also look at any entries under the Publisher column which are not just the standard 'Microsoft Windows'. Then check the Description column to see which application or device the driver relates to. Highlight the file and look at the details pane at the bottom of Autoruns to see the date and version number for the driver file.
4. For any drivers you wish to remove, first untick its entry in Autoruns, and when finished close Autoruns and reboot Windows. If after a period of time you believe there are no adverse impacts on your system, and required functionality is not affected, you can repeat Steps 1 - 3 above, but this time right-click on a driver and select Delete to remove it.
5. Reboot Windows and the driver file will no longer be loaded or resident on your system.

The Autoruns method only removes specific driver files, usually .SYS files, and not entire driver packages, nor a range of Registry entries which a driver may have created, so this method does not remove all driver residue, only the files which load up with Windows.

Driver Fusion

If after using the above methods you feel there is still some driver residue left on your system, you can use the free Driver Fusion utility to attempt to remove any remaining traces of the more common drivers. Once installed, follow these steps:

1. Select the driver type(s) you wish to remove from the entries on the left side, and click the Analyze button at the bottom of the screen. This will display a list of files and Registry entries that will be removed. You can manually untick any component(s) you wish to keep.
2. If you want to continue, click the Delete button at the bottom of the screen and reboot your PC to make sure all driver files and related Registry entries are removed.
3. If you find certain driver elements are still not being removed, reboot into Safe Mode and follow the steps above again. Under Safe Mode no third party drivers are in use by Windows, so none of them should be locked against deletion as long as you have Administrator access to the system. See the System Recovery section of the Backup & Recovery chapter for details of using Safe Mode.

Driver Fusion only allows the removal of the specific drivers in the list it provides. Newer versions of these drivers may install additional files and/or Registry entries which the current version of Driver Fusion cannot find. Remember that no automated method is foolproof in finding all aspects of driver residue, since drivers are constantly changing.

Windows Driver Store Repository

If you are still unable to find and remove certain drivers, or you just want to see the contents of the driver packages Window has installed, then you should note that Windows 8 holds all the driver packages it uses for standard installation under the *\Windows\System32\DriverStore\FileRepository* directory. These are not the actual driver files in use by the system, those are held under the *\Windows\System32\drivers* directory. Each separate driver package in the Driver Store is a subdirectory with the name of the .INF file for the package. For example Nvidia graphics drivers can be found in a subdirectory starting with *nv_disp.inf* and ending with a string of numbers. You can use the driver repository for three things:

§ Manually direct Windows to a particular driver package if it does not detect it automatically. Do this under Step 6 of the Manually Updating Drivers section further above.
§ Remove traces of a faulty or undesirable driver - see the method below.
§ Find and manually modify the driver package so that when Windows detects your device it uses the modified contents to install the driver - see the method below.

In each case you must first identify which folder under the *\Windows\System32\DriverStore\FileRepository* directory relates to the driver package you are seeking. The quickest way to do this is to use the pnputil command. Use the following steps:

1. Open an Administrator Command Prompt.
2. Type `pnputil /?` for a full list of commands. In this case we want to use the following command:

   ```
   pnputil -e
   ```

   This will display all the third party driver packages which are held in the driver store. Take particular note of the Published name (e.g. *oem0.inf*) as well as the driver date, version and package provider - use these to identify the driver.
3. To remove a driver package from the driver store use the following command:

   ```
   pnputil -d [Published name]
   ```

   Where *[Published name]* is the name you discovered under Step 2 above, e.g.:

   ```
   pnputil -d oem0.inf
   ```

You will find that the majority of the drivers stored under the Driver Store are default Microsoft drivers, and hence you should not attempt to manually alter or delete them. If you find an installed third party driver package that you are certain you no longer need, then you can safely delete it and hence prevent Windows from ever reinstalling it.

Alternatively, if you are an advanced user and you wish to modify a driver, you can modify the folder contents of the particular package as desired, uninstall the current drivers for your device, and Windows will then attempt to install this modified driver package when it redetects your device. Or you can simply point Windows to this folder when manually updating drivers as detailed further above.

The only foolproof method to successfully remove driver residue is to manually find and delete every single file, folder and Registry entry for a driver in Windows 8, and unfortunately this is too complex a method to

detail here as it relies on a great deal of research. Every driver and program installs its files and Registry entries in different locations, and this changes over time with newer versions of drivers. Automated utilities can only do so much precisely because they must be programmed to know where to look for every different type of driver, so they too are not foolproof. If you truly believe your system is bogged down with driver residue and hence your problems relate to this factor, it may be best to backup all of your personal files, reformat and reinstall Windows 8 afresh, then restore only your personal files and folders, and install only the latest version of each of your drivers. That is the only guaranteed way of removing faulty, mismatched or undesirable driver files. It also serves as a warning not to experiment too much with lots of different drivers, as constantly upgrading and downgrading drivers, particularly leaked or modified drivers, can quickly make a mess of your system.

See the Cleaning Windows chapter for tools which can assist further in cleaning out unnecessary files, and check the Maintaining the Registry section of the Windows Registry chapter for Registry cleaning tools.

< DRIVER VERIFIER

If you believe you are having driver-related problems, you can use an advanced tool built into Windows called the Driver Verifier. To run it, type *verifier* on the Start Screen and press Enter. It is a complex tool, so read the detailed instructions for its usage in this Microsoft Article. Its basic usage details are provided below.

1. Once Verifier starts, after a moment you will see a dialog box open. Leave the options at their default and click Next.
2. On the next screen, you can either choose to let the Verifier test only unsigned drivers; drivers built for older versions of Windows; all drivers; or select from a list. I recommend the 'Select driver names from a list' option to pick specific drivers you suspect to be problematic, and click Next.
3. Place a tick against all the driver files you believe need to be checked. To make things simpler, click the Provider column header so that the list is sorted by the providing company, that way if you want to choose your graphics drivers for example, you can tick all the boxes for the files provided by Nvidia or AMD. Note that only drivers which are currently loaded up by Windows are shown. If you want to add drivers which are not currently loaded, click the 'Add currently not loaded driver(s) to the list' button and select the additional files. Once all the relevant boxes are ticked, click Finish.
4. You will have to reboot your system, at which point during or soon after your PC starts up again you may see an error if any of the driver files you chose are potentially problematic. If Windows starts up normally and you see no error message after a while then the files have been verified as being fine.
5. If you can't find a problem with the drivers you've selected, repeat the process above, but this time at Step 2 select the 'Automatically select all drivers installed on this computer' option instead.

Importantly, you will need to disable Verifier once you've finished with it, otherwise it will continue to verify the files at each Windows startup. To do this, open Verifier again and select 'Delete existing settings' then click Finish. If you cannot access the Verifier user interface to turn it off, open an Administrator Command Prompt, or use the Command Prompt available in the Windows Recovery Environment, and type `verifier /reset` then press Enter. You can also uninstall any driver that is causing problems in Safe Mode. See the System Recovery section of the Backup & Recovery chapter.

Having an error in Driver Verifier is not indicative of a driver being the primary source of your problems. However if Driver Verifier doesn't encounter any errors, it can help rule out your drivers as the key source of a problem.

Bear in mind that the majority of system issues are the result of factors completely unrelated to drivers, such as overheating, overclocking, bad BIOS/UEFI settings, faulty hardware, one or more installed programs

causing conflicts, etc. Just because a driver file is giving an error message, or a Windows error message points to a driver, that doesn't mean the driver is the actual cause of the problem. Drivers often crash when a system is unstable for a range of reasons, and not because they are buggy or unstable themselves. In other words, a driver crash may be a symptom, not the cause of a problem. See the Performance Measurement & Troubleshooting chapter for more ways of troubleshooting a system issue.

< GENERAL DRIVER TIPS

The following is some general information and advice regarding all device drivers:

§ *Source of Drivers* - Only download and use drivers directly from your hardware manufacturer's website, Windows Update, or from a reputable and well established third-party source which you know and completely trust. This does not guarantee their stability, but it does help ensure that they do not contain malware. While many people think nothing of downloading drivers from file sharing sites, or downloading heavily modified drivers for example, you are essentially putting your trust in people who are anonymous and completely unaccountable, and who may even be infected with malware without knowing it. Then of course there are people who are deliberately malicious and will use any opportunity to spread malware. The hardware manufacturer's site should be your first (and usually only) choice for obtaining drivers.

§ *User Feedback* - Be wary of general user feedback about drivers on places like public forums and in website comments. In recent years, more and more users have turned to blaming drivers (or Windows itself) for various problems on their system, when the problems are often actually the result of general user ignorance or lack of system maintenance, such as overclocking, overheating, conflicting software, or excessive driver residue. This is particularly true for graphics and audio drivers, with any audio or graphics-related problem automatically being attributed to the drivers by the average user, when indeed many other factors can cause these issues. User feedback is useful, but should not be the sole or even the primary basis for determining which driver to install.

§ *Beta Drivers* - Beta drivers are pre-final drivers which carry the risk of causing additional system problems because they have not necessarily undergone thorough testing, thus the hardware manufacturer provides no support to users of beta drivers. Generally speaking though, beta drivers downloaded directly from a major hardware manufacturer should be relatively stable and safe to use, but best installed only if you are having problems with your current driver and/or only if the release notes and the consensus of user feedback clearly indicate that they provide some other benefit.

§ *Alpha Drivers* - Alpha drivers are even less polished than beta drivers and their use can lead to serious problems such as major instability and even data loss. They are only recommended for advanced users who wish to experiment, or for users who have absolutely no other available option for obtaining a working driver for their hardware. Make certain you prepare a full backup before installing an alpha driver.

§ *Leaked Drivers* - Leaked drivers may be alpha, beta or final versions, but they have been unofficially released to the public, often against the wishes of the hardware manufacturer. They may be modified and/or not digitally signed, which only increases the risk that they contain malware and/or may not provide stable functionality for your device and result in data loss. As with alpha drivers, I do not recommend using leaked drivers unless you have absolutely no other option, and only after making a full backup beforehand. Aside from putting your data at risk of being lost, you are also putting your security at risk.

§ *Modified ('modded') Drivers* - Modified drivers rarely provide any genuine benefit over the standard drivers from your hardware manufacturer. Don't be fooled by promises of large performance gains or magic fixes - these are almost always unfounded or exaggerated claims designed to entice people into using the driver. The only time I would recommend a modified driver is if they have been .INF modified to allow them to be installed and used on hardware they were not originally intended for. This is a simple text file modification done primarily to provide drivers for hardware that may otherwise not have frequent driver support, such as laptop graphics chipsets. Obviously .INF modification can result in unexpected behavior because the driver is being used on hardware it was not designed for, but it may

be the only option available to people with certain hardware. In all other cases I recommend against using modified drivers for safety and stability reasons. If a manufacturer has disabled a particular feature in a driver, it is usually for a good reason.

Drivers are a critical component of the way your hardware interacts with Windows, and have a significant impact on performance and stability, so it is best to make sure they are always kept up to date, and that you do not experiment unnecessarily with them. Regularly refer to the front page of TweakGuides.com for the latest news on official driver updates for popular hardware.

USER ACCOUNTS

User Accounts are a way of allowing more than one person to use the same PC in relative isolation from one another. Each user can have a different Start Screen and Desktop layout, different Windows settings, and different personal folders, all stored separately and without impact on, or access to, each other's data. User accounts are not solely designed for sharing purposes; even if there is only ever one user on a machine, you will still need to have a user account, and understand how they work for various reasons, such as security, or if you want to synchronize your settings across multiple devices.

When you first install Windows 8, a default user account with Administrator privileges must be created using the username and optional password you choose just prior to finalizing installation. Every time you start using Windows from that point onward, you are logged into this user account by default, unless you create others and switch to them.

Windows 8 continues the general user account model introduced in Windows Vista and used in Windows 7, with one important change. There are now two overarching types of user accounts: a Microsoft Account, and a Local Account. Which account type you choose, how many user accounts you wish to set up, and how you can best use them are topics covered in detail in this chapter.

< LOCAL ACCOUNT VS. MICROSOFT ACCOUNT

Windows 8 introduces two separate types of user account, known as a Microsoft Account, and a Local Account. To see which account type you are currently using, open the User Accounts component of the Windows Control Panel. You will see your current user account name shown prominently, with either 'Local Account' or an email address (Microsoft Account) displayed beneath it.

You can switch your account between a Local Account and a Microsoft Account at any time without losing your data or customizations, and you can also create a new Microsoft Account or Local Account if desired. See the Managing User Accounts section later in this chapter for details.

An overview of each account type is provided below.

LOCAL ACCOUNT

A Local Account is the name for what used to be the standard and only account category in previous versions of Windows. It is known as a Local Account because all of your account settings are stored locally, on the PC on which the account was created; nothing is stored on the Internet or shared across devices, as with a Microsoft Account.

A Local Account requires a username, but a password is entirely optional, and the account is not linked to an email address. If a Local Account has a password, when booting into Windows 8 you will first be presented with the Lock Screen, upon which you must enter the password for the account before proceeding to the Start Screen. If a Local Account has no password, after bootup Windows will reach the Start Screen with no interruption or user input required - unless you have multiple user accounts on the same PC, in which case you may need to first select the relevant account to log in to.

Note that to use the Windows Store to download and install Metro apps, you must sign in with a Microsoft Account. You can create such an account the first time you attempt to sign in to the Windows Store - see the Setting Up a Microsoft Account section further below. Importantly, you do not need to be logged in to Windows 8 with a Microsoft Account user account to use the Windows Store; you can log in using a Local

Account-based user account, then enter a Microsoft Account details when opening the Windows Store to gain access to downloading or purchasing apps.

MICROSOFT ACCOUNT

New to Windows 8, you have the ability to use a Microsoft Account, which is similar to a Local Account in most respects. The main difference is that a Microsoft account requires both a valid email address and a password, and can store a range of information regarding your Windows 8 customizations in "the cloud". That is, the data is held on Microsoft's SkyDrive servers in encrypted form, as covered in this Microsoft Article. This is a significant benefit, as it allows your customizations to be shared and synchronized with various Windows 8 PCs and devices when they are connected to the Internet and you log in to them using your Microsoft Account.

For example, if you log in to your Microsoft Account on another Windows 8 PC or device, it will carry over a range of customizations you have made on your own Windows 8 PC, such as your Start Screen configuration and apps, and Desktop wallpaper. Any changes you make to your customizations while logged in to your Microsoft Account on any PC or device will be synchronized across your other devices, so they will be up to date when next you use them with the same account.

SETTING UP A MICROSOFT ACCOUNT

When creating a Microsoft Account, the email address you enter can be an existing or new Microsoft-based one (e.g. @hotmail.com, @live.com or @outlook.com), or it can be any non-Microsoft email account that you own and currently have access to. Microsoft recommends entering the email address that you commonly use to communicate with friends and sign into your favorite websites. This is because one of the optional features of a Microsoft Account is that when using it, Windows 8 can automatically sign you into sites like Facebook or Flickr, or your Xbox Live account, as well as your email account, without prompting you for your username and password each time.

If you choose to use a non-Microsoft email address, then you will need to verify ownership of that email address before it can be used. A verification email will be sent to your non-Microsoft email address, and you must follow the steps in it to confirm your ownership of the address and enable the synchronization features of the Microsoft Account to which it is linked. Typically this involves clicking a link which takes you to a Windows Live login screen - here you must enter your Microsoft Account's email address and its password and click Login, and you should see a message stating that the account has been successfully verified.

If you don't have a suitable email address, or wish to create a new email address specifically for your Microsoft Account, then click the 'Sign up for a new email address' link at the bottom of the screen on the initial account creation page. This will take you through the steps required to set up a new Microsoft-based email account, such as Hotmail, which is then linked to your Microsoft Account.

Importantly: Regardless of which email address you choose use, you must be extremely careful while setting up a Microsoft Account. Aside from using a strong password, it is critical that you establish a foolproof and secure method of recovering the password to the account should you forget it. Make absolutely certain that you follow the Secure Password and Account Recovery guidelines covered in the Important Security Tips section of the Security chapter. Do not ignore this warning, because if you lose your password and can't successfully recover it, in the worst case scenario, you could be locked out of your account, and hence lose all of your data, especially if your PC's sole Administrator account is the Microsoft Account.

MICROSOFT ACCOUNT SYNCHRONIZATION

You can choose the particular types of settings and customizations that can be stored in the cloud and shared via a Microsoft Account. Once logged into Windows 8 using your Microsoft Account, open the Charms menu, select Settings and click on 'Change PC Settings', then select the 'Sync your settings' category. Here you can choose to enable or disable a range of categories for synchronization across your PCs and devices:

§ *Personalize* - This includes your Start Screen tiles, colors, background, Lock Screen image, and your User Account picture.
§ *Desktop personalization* - This includes your Desktop Theme and Taskbar setup, however your Desktop programs cannot be synched.
§ *Passwords* - You can store and share passwords across devices if you make your PC a trusted device by clicking the 'Trust this PC' link and following the prompts. This will then allow you to automatically sign in to certain services such as email and messenger apps without having to manually enter a username and password.
§ *Ease of Access* - This includes any usability settings you have adjusted under the Ease of Access Center in Windows Control Panel.
§ *Language Preferences* - This includes your display language and keyboard type.
§ *App Settings* - This includes certain settings and resume capabilities in supported Metro apps.
§ *Browser* - This includes History and Favorites in Internet Explorer Metro, and other supported browsers.
§ *Other Windows Settings* - This includes File Explorer customizations, mouse and keyboard settings.

When the main 'Sync your settings' option is enabled here, all of your selected settings and customizations will then be shared with any other PC or device, as long as it is connected to the Internet when you log in to it with a Microsoft Account.

If you have no use for the Synchronization feature, then it is recommended that you use a Local Account for your main user account. This is much more secure, and also does not require a password, which is more convenient if you are the sole user of a PC and it is not accessible by untrusted persons.

< USER ACCOUNT PRIVILEGES

Regardless of whether you use a Microsoft Account or a Local Account, there are different levels of privileges given to any user account. In Windows 8, as with previous versions of Windows, there are three main types of user accounts: Administrator, Standard and Guest. Each has different privilege levels as covered below.

ADMINISTRATOR

This user account type can undertake the full range of actions in Windows, from installing or uninstalling any software and making system-level changes, to viewing the files and folders of other user accounts on the system. Administrators can also create, change or delete user accounts. There must always be at least one Administrator user account on a system to be able to manage it, which is why Windows 8 forces you to create one at the end of the Windows installation process.

Furthermore, there are two different types of Administrator account:

Protected Administrator: The default Administrator account is actually known as a Protected Administrator. The key reason for this name is that User Account Control (UAC) restrictions apply to it. If UAC is enabled, then the Protected Administrator is set by default to Standard level privileges, and can only undertake Administrator level tasks by confirming UAC prompts. However, unlike a normal Standard level user, a Protected Administrator does not need to enter a password in order to confirm a UAC prompt. See the User Account Control section of the Security chapter for full details.

Full Administrator: There is another Administrator account, known formally as the Administrator Account, which is hidden and disabled by default, and is not affected by UAC settings, does not have a password, and runs with full Administrative level privileges at all times. To enable this account, see the Advanced section later in this chapter. I must stress that you should not use this account regularly as it is a major security risk, since it is not protected by a password, nor is it affected by UAC. A user logging in under this account is leaving a major security hole open. The primary use for this account is for troubleshooting purposes, such as resetting a forgotten password on the Protected Administrator account.

STANDARD

This user account type is designed for the average user. It lets any user access most of the normal functions of Windows. The main restrictions are on installing or uninstall certain types of software and hardware, changing any Windows settings which affect other users, viewing other the files and folders of other user accounts, and deleting or altering critical system files. If User Account Control is enabled, a Standard user can only bypass the restrictions above by entering the password for an Administrator level account when prompted by UAC. In practice a Protected Administrator and Standard account both run with the same type of privileges; the only difference is that the Protected Administrator does not need to enter a password to confirm a UAC prompt, whereas the Standard user does.

GUEST

This user account type is disabled by default and is only intended for temporary users, allowing very basic access to your system. Any user who logs in with a Guest level account can't install any software or hardware, can't change settings, nor set up passwords. Once they log off the Guest account, all data in their profile is also deleted. This means that there is minimum potential for them to do any harm to your system, although it is still not recommended that you grant an untrusted user even this basic level of access to your machine without some supervision. To turn the Guest account on, click the 'Manage another account' link in the main User Accounts window, then click the Guest icon and select the 'Turn On' button. It is strongly recommended that you leave the Guest account disabled, and only enable it whenever needed.

The different types of User Account privileges exist to minimize security risks, and the risk of intended or unintended harmful changes to important system settings and software, as well as preventing different users on the same machine from automatically being able to view and alter each other's files and folders. With the advent of UAC, Windows has evolved such that there is greatly reduced risk in running an Administrator level account as your normal everyday account, since by default the Administrator account only has Standard user privileges until you click a UAC prompt to escalate those privileges to full Administrator level when required.

So while many people hate UAC and its incessant prompting, the benefits of UAC - and I strongly recommend that you keep it enabled - are that you don't need to expose yourself to the security risks of running a full unprotected Administrator account on a regular basis, as has been the case in previous versions of Windows such as XP; you can now run an Administrator account as your main account for convenience, and use UAC to have tighter security as well.

To alter the privilege level of any existing account, see the Managing User Accounts section later in this chapter.

< USER ACCOUNT STRATEGIES

There is no hard and fast set of rules that allow you to determine which account types you should use. Instead, this section contains advice on how to select the user accounts type and privilege level on your system based on four important considerations:

- *Number of Users* - The number of people who will be using Windows 8 on your PC.
- *Synchronization* - Whether you will be using Windows 8 across multiple PCs or devices.
- *Physical Access* - Whether the PC is physically accessible by untrustworthy individuals.
- *Data Sensitivity* - The sensitivity of the information stored on your PC.

Each factor is covered below in more detail:

NUMBER OF USERS

The primary reason for the existence of user accounts is to allow multiple people to use a single system without interfering with each other. Hence if you are the sole user of the Windows 8 PC, then there is no need for more than one account - the default Protected Administrator created during Windows installation is sufficient. Whether this is a Microsoft Account or Local Account, and whether you password protect it, will depend on a range of considerations discussed further below.

If more than one person is likely to regularly use your Windows 8 machine, it is strongly recommended that you set up additional user accounts for each and every one of them. These should be Standard accounts, which is the default type used for new accounts. If these users are children, you can optionally enable the Family Safety feature during or after account creation to give you access to a range of monitoring and restrictive tools. See the Family Safety section further below for details.

On a system with multiple user accounts the Administrator account must be password protected. This is because the Administrator account has unrestricted access to all the other accounts on the system, as well as all system settings. It is also recommended that if there are two or more other accounts on the system, that they each be password protected as well to prevent the users from viewing or tampering with each other's accounts. You must also enable User Account Control.

You may also wish to switch one of the additional Standard User Accounts to an Administrator level account. For example, if you have a spouse who wishes to help administer child accounts, it is useful to have two separate Administrator level accounts, one for each parent. See the Managing User Accounts section later in this chapter for details of how to change an existing account's privilege level.

Some things to keep in mind when using multiple user accounts:

- The last used user account is typically the one that is shown on the Login Screen. If you have more than one user account on the machine, the user will need to go to the user account selection screen each time Windows is started to select their own account. To do this, click on the Lock Screen and if necessary click on the back arrow shown next to the current username, which will then display the full user account selection screen.
- During a Windows session you can quickly switch between accounts without restarting the machine or signing out of the current account by pressing CTRL+ALT+DEL and selecting 'Switch user', or by going to the Start Screen and clicking on the User Account picture at the top right, then selecting the particular user to switch to from the list which appears.

SYNCHRONIZATION

Whether you make an account a Microsoft Account or a Local Account depends largely on whether the account user wishes to synchronize their customizations and settings across several PCs or devices. A Local Account is more secure, as nothing is stored in the cloud. A Local Account is also easier to administrate, as the Administrator can easily reset a Local Account user's password via the User Account component of the Windows Control Panel should it be forgotten - see the Managing User Accounts section further below.

This means that unless synchronization is a real need for a particular user, you should set up additional accounts as Local Accounts. You can always switch any account between the two types without losing data or customizations should needs change over time.

PHYSICAL ACCESS

Whether your PC or device is physically accessible by any people you would consider untrustworthy is a primary consideration when determining whether to password protect a particular account. Microsoft Accounts must always be password protected, so the real issue is whether any Local Accounts you have should be password protected. As always, it comes down to a question of security vs. convenience, which we discuss in greater detail in the Security chapter.

For example, if using an Administrator level Local Account on a PC with only one account, if you don't use a password for that account, on each Windows startup you will skip the Lock Screen and go straight to the Start Screen. This is extremely convenient, and indeed, even if you have multiple user accounts, you can set any account to automatically login at Windows Startup in a similar manner, as we cover later in this chapter. However doing this for any PC or device leaves it completely open for anyone who gains physical access to it. They can go through all of your personal data, they can wreck your settings, install unwanted software, use your Internet connection for undesirable activities, and so forth. It doesn't even have to be anyone malicious like a thief, it may well be a friend or roommate causing unintentional harm.

The simple rule is that if your PC or device is currently located in an area where others have physical access to it, and you do not trust them 100%, or if your system stands any likelihood of being lost or stolen, particularly for mobile devices which you frequently carry around with you, then you should password protect any and all accounts. This won't make them impervious to intrusion, but it makes things much harder for anyone who wants to try, and reduces the potential for mindless tampering as well.

If you want to allow an untrusted person limited access to your machine at any time (e.g. letting a friend do some basic web browsing), then temporarily turn the Guest account on and log them in via that account. It is also recommended that you supervise the use of the PC by any untrusted individual, as there is still the remote possibility that anyone with physical access to your machine, when using certain tools, could crack the Administrator password and hence gain unrestricted access.

DATA SENSITIVITY

If you have personal data that you consider sensitive, and thus it would be extremely embarrassing or catastrophic if it were to fall into the wrong hands, then in addition to the recommendations above, you should look at using EFS Encryption and/or BitLocker Drive Encryption - see Encrypting File System and BitLocker Drive Encryption sections of the Security chapter. These technologies will encrypt your data in such a way that it will be next to impossible for anyone to access it without having the proper password to your account - which of course stresses the importance of having an extremely complex user account password, and highly secure password recovery processes in place. Once again, these issues are covered in detail under the Important Security Tips section of the Security chapter.

Take the time to consider your circumstances based on the factors above before deciding on the best course of action for creating and maintaining user accounts on your system.

< MANAGING USER ACCOUNTS

To create, delete or modify user accounts to suit your needs, you must first log in with an Administrator account, such as the default account you created during Windows installation. The various user account options are held in two separate locations: the User Accounts component found under the Windows Control Panel, and the Users category found by opening the Charms menu, selecting Settings and clicking on 'Change PC Settings'.

There are a range of options in these two locations which apply to your own account, or to another account if you have Administrator access, by selecting the 'Manage another account' link, and then choosing the relevant account to alter. Note that some changes will require that the user sign out and then log back in to their account before they are implemented correctly.

The common options are covered below, though note that most of them require Administrator privileges in order to be accessed.

CHANGE YOUR ACCOUNT NAME

You can change a Local Account name under the User Accounts component of the Windows Control Panel at any time, but you cannot change Microsoft Account names here. To change a Microsoft Account name, you must log in to it first, then open the Charms menu, select Settings and click 'Change PC settings', then select the Users category and click 'More account settings online'. In the account summary which is shown in your browser there should then be an option to change the user name.

Changing your account name is generally not recommended, because aside from causing confusion on the Login Screen, it also causes further confusion since the actual name of the personal folder for that user account, found at *\Users\[username],* will not be changed; it will remain as originally set. Do not manually change the name of the *\Users\[username]* folder as this will cause a range of problems, as that user account will no longer be using their personal folder if it is renamed. If you wish to rename the user's personal folder you need to follow the relevant procedure under Correctly Renaming a User Account in the Advanced Settings section later in this chapter.

CHANGE YOUR ACCOUNT TYPE

You can change the privilege level of any user account between Administrator and Standard in the User Accounts component of the Windows Control Panel. An Administrator account is always indicated as such when shown in the Manage Accounts section when you click the 'Manage another account' link. Standard accounts are the default, and will typically either say Standard beneath the account name, or have no indicator of account type, depending upon which interface the account is shown on.

Changing the account type will not alter its data or customizations, it will simply change the privilege level with which the account operates. Be certain that you wish to give Administrator access to another user, as they will then be able to make system intrusive changes, and can also make changes to your Administrator account, such as altering its password or demoting it to a Standard level account. In other words only give Administrator access to someone whom you completely trust.

CREATE/CHANGE THE PASSWORD

You can add or change a password for any Local Account under the User Accounts component of the Windows Control Panel at any time, but you cannot change Microsoft Account passwords here. To change a Microsoft Account password, you must go to the Charms menu, select Settings and click 'Change PC settings', then under the Users category click the 'Change the password' button. This will require Internet access as the password change needs to be recorded against your online Microsoft Account profile. Furthermore, a Microsoft Account must always be password protected, so you cannot remove the password from such an account.

For a Local Account, the quickest way to add or change your own account password is to press CTRL+ALT+DEL and select 'Change a password'. To add a password, leave the 'Old password' field blank and enter the new password. To remove a password, enter your current password, then leave the 'New Password' fields blank and click Next.

A user account with a password cannot have its files and folders accessed by any other user except for an Administrator. If a Standard user on your system forgets their password, an Administrator can log in and under the Manage Account section of the User Accounts component of the Windows Control Panel, can select the account and click the 'Change the password' link to set a new password, or if left blank, to remove a password from that account. Once again this option is only available for Local Accounts; Microsoft Account users must go through the online process of account recovery, as discussed above.

Importantly, if you forget the password for an Administrator account you will need another Administrator on the same machine to help reset it for you. If another Administrator doesn't exist you will be in serious trouble. See the Backup & Recovery Chapter for the recovery options of a Local Account, or use the online recovery options you set up for your Microsoft Account.

Note that for any Local Account, removing a password from the account will also meant the loss of access to any password-protected resources in that account, such as EFS encrypted files and personal certificates.

SWITCH BETWEEN MICROSOFT ACCOUNT AND LOCAL ACCOUNT

You can switch the currently logged in user account between a Microsoft Account and a Local Account at any time. Go to the Settings charm, select 'Change PC settings', and under the Users category click the 'Switch to a local account' or 'Switch to a Microsoft Account' button. The existing account will be switched to the selected account type, and your data, customizations and settings will be kept.

SIGN-IN OPTIONS

Under the Charms menu, select Settings then click on 'Change PC settings', and under the Users category you can select the login method for the currently logged in account:

§ *Password:* This includes either changing the existing password by clicking the 'Change your password' button, or adding a password to an account which previously did not have a password by clicking the 'Create a password' button. Importantly, if you password protect an account, for a Local Account you will need to enter a Password Hint; for a Microsoft Account you will need to establish a recovery method. In both cases refer to Account Recovery under the Important Security Tips section of the Security chapter for details, as these are a common security hole used by hackers to gain access to accounts if they are improperly configured.

§ *Picture Password:* This method is new to Windows 8 and best used on touchscreen PCs and devices. It will only be available if the account has a text password. The aim is to use a picture as your password prompt, and you then enter the password through a series of gestures over that image, rather than entering any text. The resulting password is unique, yet still relatively easy to remember. When creating a picture password, you must first select an image on your system. You then generate three separate gestures in a row, based on elements of the image. The gestures can be any combination of circles, straight lines and taps. However, you cannot use wavy lines, as Windows will interpret these as a straight line. Nor can you trace a complex shape like a box in a single gesture; Windows will simply interpret this as one or more straight line gestures, or a circle. Windows will prompt you for each gesture, and record the gesture and its location on the screen. Once complete, you will be prompted to enter them again before your picture password is confirmed. Once set, you will be prompted at log in time with the image you selected, and must enter the three required gestures in the right order and location to be granted access to your account.

§ *PIN:* The new Windows 8 Personal Identification Number (PIN) method will only be available if the account has a text password. It is similar to that used when accessing your bank account at an Automated Teller Machine. You must enter a four digit PIN, and once set, you can log in to your account on the Lock Screen by entering the PIN to get instant access.

Some things to note about these methods:

§ You must have a text password on an account before you can create a Picture Password or PIN. This is because it is the fallback method in case you forget, or cannot access, either of the other two methods.
§ If you have created a Picture Password or PIN, this will become your default log in method instead of a text password whenever you are prompted for a password on the Lock Screen. You can alter this behavior and/or access any other log in method by clicking the 'Sign in options' link shown on the Login Screen and selecting the relevant icon for Password, Picture or PIN, or by first clicking the 'Switch to Password' button if required.
§ You can remove a Picture Password or PIN by clicking the Remove button next to it here. This will default the password back to the text method.
§ You can remove a text password from your account by clicking the 'Change your password' button, entering your password for confirmation, and then leaving the 'New Password' field blank and clicking Next. This will also clear any PIN or Picture Password you have set up for that account.

There is also an option here which allows you to determine whether Windows will prompt for a password for a user account (if it is password protected) whenever the PC wakes up from a sleep mode. If the 'Any user who has a password must enter it when waking this PC' text is shown, the Login Screen will be shown whenever your PC or device wakes out of sleep. You can click the Change button to remove this restriction, however this means that anyone can now gain access to the currently logged in account without entering a password if the PC or device is taken out of sleep mode.

ADD A NEW USER

When you click the 'Manage another account link' in the User Accounts component of the Windows Control Panel, on the main account selection screen for Manage Accounts, you can click the 'Add a new user in PC settings' link at the bottom if you wish to create a new user account. You can also access this screen by opening the Charms menu, selecting Settings and clicking on 'Change PC settings', then selecting the Users category in the left pane.

An Administrator can create a new Microsoft Account or Local Account at any time by clicking the 'Add a user' button and following the prompts. When adding a new user, by default it will be created as a Standard user, and as a Microsoft Account if you enter an email address. If instead you want a new Local Account, don't enter an email address, and click the 'Sign in without a Microsoft Account' link at the bottom of the screen, then click the 'Local Account' button at the bottom of the next screen to continue.

Only create as many additional accounts as you actually need. Each new account you create will automatically have a full set of personal folders generated under the *\Users* directory the first time that user logs on to that account, so unused accounts will simply take up drive space for no good purpose. Note that an Administrator can view the files and folders of other users by going to the *\Users* directory in File Explorer and looking for the subfolder with that user's account name. Remember also that you can switch any new account between Standard and Administrator level privileges as covered under the Change Your Account Type section earlier in this chapter.

DELETE THE ACCOUNT

An Administrator can delete any account except their own by going to the User Accounts component of Windows Control Panel, selecting 'Manage other accounts', selecting the relevant account, and then clicking 'Delete the account'. This is obviously something that should done with caution, since deleting an account not only deletes all of that account's customizations, it can also delete all of their personal files and folders. For this reason Windows will ask you whether you wish to save the account's personal files to a new directory before deletion by selecting the 'Keep Files' button, though you will not be able to save their emails

and Windows customizations this way if it is a Local Account. Alternatively, you can permanently remove all of the files associated with the account by clicking the 'Delete Files' button.

CHANGE THE ACCOUNT PICTURE

Each User Account is represented by a small picture on the Login Screen and at the top of the Start Screen when logged in, among other places. This picture makes it easier to quickly distinguish between different accounts. To add a custom picture for your account, log in to the account and then go to the Charms menu, selecting Settings and click on 'Change PC settings', and under the Personalize category select 'Account Picture' at the top. Here you can click the Browse button to find an image from any location on your system - it must be in .BMP, .PNG, .GIF or .JPG format. Select the image and click the 'Choose Image' button to set it as your account picture. To see how the new account image will look, press CTRL+ALT+DEL and select 'Switch User' to see the image displayed on the account selection and login screens. The account image can also be seen at the top right of the Start Screen, and may also be shown within some Metro apps.

< FAMILY SAFETY

Family Safety features are built into Windows 8, similar to the Parental Controls in Windows Vista and 7, and are detailed in this Microsoft Article. These features are designed to allow an Administrator to place restrictions on any user account, as well as monitor usage by that account. One of the most common uses of user accounts is by parents who want to restrict their children from making a mess of the family computer, or accessing undesirable material on the Internet. Family Safety allows this, but it is not just for controlling children; it also allows you to lay down additional limitations on any Standard user account.

Family Safety can be accessed directly through the Windows Control Panel, or via the 'Set up Family Safety' option under the 'Manage another account' section of the User Accounts component under Windows Control Panel.

On the main Family Safety screen you will see all available user accounts on the system, including your own, though Family Safety can't be applied to an Administrator account. You can see which accounts have Family Safety enabled here, as there will be a 'Family Safety on' tag beneath the relevant account name. To customize Family Safety for a user, you must first select their user account, and importantly, your Administrator level user account must be password protected for Family Safety restrictions to be enforceable. When you select the user to which you want to apply the restrictions, you should select the 'On, enforce current settings' option at the top to enable Family Safety for this user. You can then adjust the various settings as described below:

Activity Reporting: If enabled, this option records a range of information regarding the general usage patterns of this particular user. This includes the websites they have visited most frequently, the periods in which they have used the PC and the length of usage for each session, and the most commonly used apps and games. To view the activity log at any time, open Family Safety and select the user account, then click the 'View activity reports' link on the right side.

If you are using a Microsoft Account for your Administrator user account, and you enable activity reporting for other user accounts on your system, Windows can also send you a weekly report via email which provides the details above in a user-friendly format. This makes it easier to monitor their activity while you're away from your PC, such as while at work or when travelling.

Web Filtering: This setting allows you to determine whether the user can access all websites by ticking the '*[username]* can use all websites' option, or whether you want to place any restrictions on their Internet usage by ticking the '*[username]* can only use the websites I allow'. The web filtering can either be done in a more comprehensive manner by clicking the 'Set web filtering level', with relatively straightforward descriptions provided for each option; or for a quick and easy method, click the 'Allow or block specific websites' option

and enter the address(es) of the sites you wish to allow or block. Note that the more comprehensive method also includes the ability to allow or block individual websites, so these are not mutually exclusive options.

When the user tries to browse to a web address that is specifically blocked, or is not on the allowed list - and remember, the address must be precisely the same (e.g. blocking *www.google.com* will not block *www.google.com.au*) - the user will be notified within the browser that the site is blocked, and can click a link to request access to it from you. This web filtering behavior should work on all major third party browsers, so it is not limited to Internet Explorer. If in doubt, test the browser in the account to make sure web filtering is working, and remember that UAC should prevent the user from successfully installing any other browser to try to circumvent this blocking.

Time Limits: This setting allows you to set the hours within which the selected user account can use the PC. This can be in the form of an allowance of a certain number of hours per day - to be used at any time - by clicking the 'Set time allowance' link. You can specify a general amount for each weekday and each weekend day, or by clicking the down arrow next to Weekdays or Weekend, you can specify different numbers of hours for each individual day (e.g. 2 hours on Wednesday, 3 hours on Thursday, etc.). Alternatively, you can click the 'Set curfew' link and set specific time ranges within which the user can or cannot log in and use the PC. On the schedule shown, areas shaded in blue represent hours during which use is blocked. Areas in white are allowed usage periods. For example, you can set a curfew of between midnight and 9am by shading in all the boxes from the far left up to 9AM, and the user will not be able to access their account during this period.

In either case, when the user attempts to log in after their time allowance has expired for the day, or during blocked periods, they will see a message explaining that due to time restrictions they cannot log on and should try again later, or request more time from the Administrator.

Windows Store and Game Restrictions: This setting lets you select firstly set any restrictions on games based on their ratings level. Click the 'Set game and Windows Store ratings' link, and you should see your country's rating system shown. Select the maximum rating level for games up to and including which your user is allowed to play. Some games and apps may be unrated, which does not mean they are necessarily harmful. However, you can also select whether to allow or block all unrated games at the top of the screen.

The second option is to click the 'Allow or block specific games' link and you should be presented with a list of games currently installed on the system. Here you can explicitly allow or block them, or allow the game's restrictions to be dictated by the ratings scheme you selected earlier.

App Restrictions: This setting allows you to block all Metro apps and Desktop programs for the user, except those which you specifically allow. Remember that UAC and the SmartScreen Filter in Windows will prevent Standard users from successfully installing system intrusive or malware programs - see the Security chapter for more details. These restrictions in Family Safety are more to prevent other types of potentially harmful apps, such as those involving online gambling or in-game purchases. Here you will see a full list of firstly Windows Store apps, then as you scroll down, Desktop programs, that have been installed on the system. Remember that if the '*[username]* can only use the apps I allow' option is ticked, the user will be blocked from using all other apps and programs except those which you explicitly allow by ticking them on the list here. This means it is usually best to click the 'Check all' button to allow all existing apps and programs, and then manually find and untick only those apps or programs you wish to block.

If you can't find the relevant program, click the Browse button and find the main executable (.EXE file) for that program to add to the list. You can determine the location of the correct executable to block by going to the program's launch icon, right-clicking on it and selecting Properties, then looking at the Target box under the Shortcut tab.

If the user is blocked from an app or program, attempting to run it will simply result in failure to launch followed by a notification. The user can then click this notification to request permission to run the app or program, and if you are supervising, you can grant permission at that time.

In fact in all cases, setting up a Family Safety restriction on an account will present the user with a Toast Notification in the top right of the screen, or displayed prominently in the center of the screen, explaining why they have been blocked from a certain activity. In some instances they will have the option to send a request to you to extend or remove the restriction, but they will have no available option to override the restriction on their own.

For most purposes the built-in Family Safety features are more than sufficient to maintain safe PC use, when combined with regular supervision, and good communication. Family Safety is certainly much-improved over the Parental Controls feature in Windows 7, which means that a third party program is not necessary. However Family Safety is not foolproof, and indeed there is no easy way to simply turn off all Internet access for a particular user account. Nor is there any guarantee that a suitably motivated child can't find some loophole to view objectionable material, or launch undesirable programs, regardless of the restrictions placed on them. But it is much more difficult to do so with Family Safety enabled. You should also make the user aware that with activity logging enabled, you will quickly become aware if they are somehow bypassing any of your restrictions.

< ADVANCED SETTINGS

This section covers more advanced ways of accessing and manipulating user account-related settings.

LOCAL & ROAMING USER PROFILES

Your User Profile is the sum of all the information in your user account, including all the data you keep under your personal folders - that is, all the files and folders under your *\Users\[Username]* directory - as well as your user-specific Windows Registry settings - that is, those in the `[HKEY_CURRENT_USER]` hive - stored in the *ntuser.dat* system file under the root directory of your personal folders.

Each user account on your computer has a user profile stored. You can access a list of these and change them by clicking the 'Configure Advanced User Profile Properties' link on the left side of the main User Accounts window in the Windows Control Panel. However this only gives you access to your own User Profile. To access all user profiles, open the System component of the Windows Control Panel and click the 'Advanced System Settings' link in the left pane, then under the Advanced tab click the Settings button under 'User Profiles'.

There should be a Default Profile here, as well as at least one user profile with your username, and one for every other user account. You can Delete or Copy other profiles if you wish, though deleting a user account is best done first through the normal user account management interface covered earlier in this chapter.

Of greatest use here is the ability to click the 'Change Type' button, letting you switch a user profile between a Roaming and Local profile if you are on a network. A Roaming profile allows the user to maintain a single user account on the network's central server which can be accessed on any machine on that network, and which remains up to date; a Local profile on the other hand is simply a locally stored copy of your user account and associated user profile data, any changes to which are not accessible on other machines in a network. For standalone home PC users this functionality is irrelevant as all profiles are locally stored, and to synchronize across machines you will need to use a Microsoft Account.

One of the changes, introduced in Windows 7, is the ability to undertake periodic background uploading of the *ntuser.dat* file to the network server to ensure that this data doesn't become outdated in case of a problem. The setting which controls this periodic updating is the 'Background upload of a roaming user profile's

Registry file while user is logged on' setting available in Group Policy Editor. See this Microsoft Article for more details, as network-related functionality is not covered in detail in this book.

Correctly Renaming a User Account

Renaming a user account is covered in the Managing User Accounts section earlier in this chapter. As noted there, if you simply rename a user account, it will not rename the associated personal folders, which can cause confusion. To correctly rename the user account and the personal folder to which that account is linked, follow these steps:

1. You must be logged in as an Administrator.
2. Make sure the user account you are about to change is logged off completely. To check this, go to the Start Screen and click on the user account image at the top right. Any user accounts, apart from the current one, which have 'Signed in' beneath them must be logged in to and signed out.
3. Rename the user account by following the instructions under Change Your Account Name in the Managing User Accounts section earlier in this chapter.
4. Open File Explorer, go to the *\Users* directory and rename the particular personal folder you wish to change. It is recommended that you match the folder name with the name for the user account you renamed in Step 3.
5. Go to the following location in Registry Editor:

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

This location holds all the separate user profiles. One of the subfolders here contains the user profile data for the account you wish to change. Find it by clicking on each one and looking at the `ProfileImagePath` value in the right pane until you find the one which matches the name of the User Profile you're changing.

```
ProfileImagePath=C:\Users\[username]
```

Once found, edit the path to point to the folder you recently renamed, then close Registry Editor. When that user next logs in, they will be correctly using the newly renamed personal folder. Renaming a personal folder by itself will link it to a renamed user account. The method above is required to fully associated a changed user account name with its renamed personal folder.

Advanced User Accounts Control Panel

To access a second, more advanced User Accounts Control Panel, go to the Start Screen and type *netplwiz* then press Enter, or you can type *control userpasswords2* in an Administrator Command Prompt and press Enter. The options provided here are similar to those available in the User Accounts section of the Windows Control Panel, but are consolidated and presented in an interface more suitable for power users, with a few additional options as well. Most of the settings here are the same as those covered earlier in this chapter, so below are descriptions for the unique features available here:

Automatic Login: If your system is only using one account - the default one created during Windows installation - and you have not set a password, then in effect you won't see the Lock Screen or Login Screen, and won't have to enter a password at any time. However, if you have set a password for your account, and/or it is a Microsoft Account, and/or you have multiple user accounts on the system, then you will always see the Lock Screen and Login Screen after Windows bootup.

If you wish, you can use the option here to select a particular user account to automatically log in to Windows at each startup without being prompted to select a user or enter a password. Follow these steps:

1. Left-click to highlight the relevant account from the list show in the 'Users for this computer' box.
2. Untick the 'Users must enter a name and password to use this computer' box at the top, and click the Apply button.
3. In the dialog box which appears, confirm that the user account is the correct one by checking the name at the top. Then enter the account's password twice and click OK.
4. This account will now automatically log in each time you start Windows, skipping the Lock Screen and Login Screen.
5. To undo this change at any time, select the account here and tick the 'Users must enter a name and password to use this computer' box and click Apply.

This method is most useful if you have a Microsoft Account, which always requires a password, but wish to avoid seeing the Lock Screen and Login Screen at each bootup by automatically signing into the account in this manner. This is obviously a security risk, and is not recommended unless you are the sole user of the PC, and the PC is located in a physically secure environment.

Advanced Privilege Levels: Under the 'Users for this computer' area, highlight an account and click Properties. Under the 'Group Membership' tab not only can you select whether to set this as an Administrator or Standard account as normal, you can click Other and select one of the other more specialized groups which have specific privileges. For example, you can select the 'Backup Operators' group for a user, which allows them to perform a range of backup and restore-related tasks that a regular Standard user would not be able to do. You will need to understand what each of the groups can do, so refer to this Microsoft Article for more details. You can also use the Local Users and Groups Manager to see descriptions for each group - see below for details. For the most part groups are designed for network administrators, not home users, and so are best left alone. If you wish to experiment with group privilege levels, do so on a secondary user account, and not your own Administrator account.

The following unique options are found under the Advanced tab:

Advanced user management: Clicking the Advanced button opens the Local Users and Groups manager window. You can also access the Local Users and Groups manager directly at any time by going to the Start Screen and typing *lusrmgr.msc* then pressing Enter. Here you can see and administer individual users in detail by clicking the Users item in the left pane, and then double-clicking on the particular user you wish to view/alter. See the Hidden Administrator Account section below for one useful function of this utility. Another useful feature can be found if you click the Groups item in the left pane to view all the available groups to which a user account can be assigned. There are descriptions of the privilege levels for each group. Additional features here include the ability to disallow password changes for particular users, or temporarily disable an account without deleting it.

Secure Logon: If you wish to have added security, you can tick the 'Require users to press Ctrl+Alt+Delete' box here. This means that whenever anyone tries to log in on this PC, they first have to press the CTRL, ALT and DEL keys together to bring up the Login Screen; it will not display automatically. This increases security because it places the Login Screen in Secure Desktop mode - as covered in the User Account Control section of the Security Chapter - meaning the screen cannot be faked or otherwise manipulated by malware to capture your login details. This level of security is generally not necessary for the average home PC user, and is best used only on publicly accessible machines.

HIDDEN ADMINISTRATOR ACCOUNT

Windows has a hidden built-in Administrator account which is disabled by default. The user account you create when you first install Windows is an Administrator level account, however it is called a Protected Administrator because it is bound by the limits imposed by User Account Control. The hidden Administrator account on the other hand has the highest level of privileges in Windows, and is not bound by UAC in any way. It is also an Owner of all the files and folders on the system, so it does not require additional permission to alter or delete any such files and folders - see the Access Control and Permissions section of the Security chapter. This makes it an extremely powerful account, but also a dangerous one.

To view this Administrator account, open the Local Users and Groups manager as covered in the section above. Then click the Users item in the left pane, and you will see an account with the name Administrator. This is not your regular Administrator account, it is the Hidden Administrator account. Double-click on this account and under its properties you can see that the 'Account is disabled' box is ticked, which is why it is not normally accessible. If you wish to make this account accessible, untick this box and click Apply. Then go to the User Accounts component of the Windows Control Panel and click the 'Manage another account' link, and you can now see the Administrator account showing. If you go to the Start Screen and click the user account at the top right, or press CTRL+ALT+DEL and select 'Switch User', this account will be now shown as Administrator, and can be logged in to just like any other account.

The Hidden Administrator account is designed primarily for troubleshooting purposes, and for very advanced users who have need of the unrestricted functionality to perform a range of system-intrusive tasks without being repeatedly prompted by UAC, or having to constantly alter file permissions for example. It is definitely not designed for daily use by the average home PC user as it is incredibly powerful and does not have protection against abuse. For example, if your computer is infiltrated by malware while you are using this account, the hacker will have complete unrestricted access to everything on your PC. Even if your system is totally secure, you can unintentionally make harmful changes to your system by accidentally deleting or altering critical system files and settings, because no prompts will appear to warn you.

For all of these reasons, you should not enable this account permanently. The main reason you should be aware of its existence is as noted, for temporary use during complex system configuration, or for troubleshooting purposes where you need the highest level of unrestricted access to your system.

Understanding user accounts is now more important than ever, because of the introduction of the Microsoft Account/Local Account dichotomy in Windows 8. In general you should limit the number of user accounts on the system to those you absolutely need, and delete or disable inactive accounts. You should use the main Administrator account and avoid the hidden Administrator account, and encourage any other users on your system to use strong passwords on their accounts. Finally, if you continually experience issues with a particular user account and nothing else works, the best solution is to manually backup the important data from that account, delete the account completely along with all of its files, then create an entirely new account and copy back the data into the new personal folders for the account.

SECURITY

Security has become a major issue of concern as the average person moves more and more of their personal data and transactions onto the Internet. Accordingly, Windows Vista saw a marked improvement in security features over Windows XP, to which Windows 7 added refinements, and Windows 8 in turn further strengthens, as covered in this Microsoft Article. You may find some of these security features annoying or confusing, especially if you are upgrading from Windows XP. However I strongly advise you not to take the topic of security lightly, or to simply disable these features without understanding what it is that they do. It is extremely important that you become acquainted with both the types of security threats, as well as how you can effectively counter them.

It is incorrect to suggest that only the very careless or novice user will succumb to a security-related problem. Even if you consider yourself a more advanced user, you need to bear in mind that security threats these days are becoming increasingly complex and dangerous. In the past a Malware (malicious software) infestation would usually result in little to no real harm; you'd have to delete a few files, or at worst reinstall Windows. Now however, malware development and distribution, as well as other techniques to violate your security, are often coordinated by organized crime groups for financial gain. So even a single breach can result in the loss of money, software serial numbers, email accounts, and other sensitive personal information. Having a carefree "can't happen to me" attitude towards security is a thing of the past.

Yet despite the increasing danger, I do not advocate bogging your system down with lots of security software that runs in the background, causing performance issues and triggering software conflicts or crashes. Instead, this chapter explains the various types of threats to your security, the features in Windows 8 which work to counter them, as well as a range of important general tips on how to stay safe. Education and awareness are truly the best defense against security breaches.

< SECURITY THREATS

There are a wide range of security threats which computer users face, particularly from various types of malicious software. Malware can enter your system and cause problems ranging from the very minor to the very serious. Malware can remain hidden for long periods and have subtle effects, or its impact can be immediate and blatant. However, it is important to understand that malware does not damage your computer hardware directly, nor does it actually physically "infect" the hardware. Malware is software-based, and its threat is to the integrity of your data, your privacy and your finances.

The major categories of malware and security threats are covered below.

VIRUSES & WORMS

Viruses are small programs that load onto your computer without your permission or knowledge of their real function. They are called viruses because just like a human virus they are designed to self-replicate, attaching themselves to normal programs and files and spreading to other computers through exchange of these infected files, where they repeat the same process on the new computer. Viruses range from the mischievous to the truly harmful, and can potentially destroy valuable information through data corruption, or cause a range of strange system behaviors.

Worms are similar to viruses, but they generally do not attach to other files, and can spread independently.

TROJAN HORSES

A Trojan, short for Trojan Horse, is a malicious program that is typically installed on your system under the guise of being another, often useful-looking, program. Trojans differ from viruses in that they are used to provide an outside attacker with unauthorized access to your system. This may be for the purposes of stealing valuable information, installing other forms of malware, or using your system as part of an illegal network such as a botnet.

SPYWARE

Spyware is similar to a Trojan, in that it is software that is usually installed on your system purporting to have different functionality, or as a component of a useful program. Spyware does not allow an outside attacker to take control of your system, but it does transmit information about you and your system, such as your passwords, keystrokes, or Internet usage behavior, to the creator of the software.

ADWARE

Adware is similar to spyware, but is not necessarily malicious, as it is mainly used to target online advertising, create popup ads, or forcibly redirect your browser to view pages with advertising. It is usually installed without your full knowledge or permission. Despite its relatively less malicious nature, this software is still undesirable as it breaches your privacy and uses your system's resources and bandwidth without benefit to you.

ROOTKITS

A Rootkit is a form of malware deliberately designed to mask the fact that your machine has been compromised and is now open to unauthorized access by an outside attacker. The rootkit will prevent traces of itself or any associated malicious activity from being detected by usual detection methods, such as running an anti-virus program, or examining the Windows Task Manager for unusual processes. A remote attacker can take advantage of the rootkit to access your machine for malicious purposes.

SOCIAL ENGINEERING

While not a form of malicious software, Social Engineering is fast becoming a common and significant security threat. It goes by many new names, such as Phishing, but essentially it is nothing more complex than what has traditionally been referred to as a con or scam. Social engineering in the Internet age typically involves fooling unsuspecting users into revealing important personal information, such as credit card or login details. For example, a phishing attempt may involve sending you a phony email purporting to be from your bank. In that email there may be a login link that looks genuine, but when clicked, actually takes you to an imitation of your bank login page. Entering your login details on the fake page will give the perpetrator all the information they need to then log in to your real bank account and steal your money. Or it can be as simple as someone calling by phone, claiming to be from a major company, and asking you for your personal details to "confirm" your account.

The categories above are in no way all-encompassing. There are many variants of the above security threats, and more are emerging every day. The people behind the creation of security threats are making large sums of money from doing this, so they have the resources and the incentive to constantly adapt to existing defenses, and innovate new and ever-more-intrusive forms of malware and online scams. But at their core, most security threats share a similar entry point into your system: an uneducated and unsuspecting user. In the majority of cases, a breach of security occurs due to the lack of some basic precautions and common sense on the part of the average user, and not on some incredibly complex new technique.

Protecting yourself against security threats is not as simple as installing lots of malware scanners and turning them all on. There is no black box set-and-forget method of staying safe. Aside from draining performance, and causing software conflicts or other system issues, even the best anti-malware software

often lags behind in the detection of new security vulnerabilities and exploits. The best defense against a breach of security is a combination of correctly configuring the built-in Windows 8 security features, along with being educated and vigilant, and understanding your own system.

The rest of this chapter contains the tools and techniques you can use to counter a wide range of security threats, starting with all of the security features built into Windows 8.

< WINDOWS ACTION CENTER

The Windows Action Center was introduced in Windows 7 as the replacement for the Windows Security Center in Windows XP and Vista, and remains much the same in Windows 8. Action Center is designed to be a central location for Windows to provide a range of alerts, and for users to quickly access several security-related Windows features. However, unlike the Security Center in previous versions of Windows, Action Center is not restricted to security-related features; warnings on a range of general system maintenance issues are also provided. Action Center is covered in this chapter because its most important function for the average user is still to provide security-related alerts.

Action Center can be opened through its component in the Windows Control Panel; by typing *action center* on the Start Screen, selecting Settings and pressing Enter; or by clicking the Action Center flag icon which appears in the Notification Area and selecting the 'Open Action Center' link. Once opened, Action Center can display two major categories of issues: Security and Maintenance. The Maintenance category is covered under the Windows Action Center section of the Performance Measurement & Troubleshooting chapter.

Action Center monitors a range of security features and settings in Windows. To see a full list of these, click the small down arrow at the right of the Security category heading. The status of each of these features is displayed here, e.g. On, Off, or OK. Where Windows considers any of your settings for these features to be less secure than it recommends, specific warnings will be shown in large boxes at the top of the Action Center. Red warnings are urgent and should be addressed immediately; Yellow warnings are less critical, and in some cases, require no action.

SECURITY CATEGORIES

The Action Center security categories are each covered in more detail below:

Network Firewall: This category monitors whether a software firewall is installed and enabled. I strongly advise against running Windows without an active software firewall of some kind. Since Windows 8 already comes with the built-in Windows Firewall, as long as that is enabled then you will not receive any warning here, and indeed for security purposes, the Windows Firewall is perfectly adequate - see the Windows Firewall section later in this chapter for details. If you have installed and configured a trusted third party firewall package, but it is not being detected by Windows, you can turn off the warning here. In any case, do not enable a third party software firewall in conjunction with the Windows Firewall; only have a single software firewall running at any time.

Windows Update: This category monitors the built-in Windows Updates feature of Windows. As noted under the Windows Updates section of the Windows Drivers chapter, I recommend against automatic updating for important updates, and instead advise the selection of the 'Check for updates but let me choose whether to download and install them' option to give you maximum control over what is downloaded and installed on your system, and when. Unfortunately, Action Center considers anything other than full automatic updating by Windows Update to be an issue. You can safely disable this warning by clicking the 'Turn off messages about Windows Update' link in the yellow warning box. Just make sure that you don't completely disable Windows Update at any point.

Virus Protection: Windows uses the term Virus in a general sense to refer to a range of malware. Therefore virus protection generally means having any of the recognized major anti-malware packages installed on your system. Windows 8 introduces a full built-in anti-malware program in the form of Windows Defender, which now incorporates the anti-malware features of the Microsoft Security Essentials package. Windows Defender is covered later in this chapter, and using it will satisfy this category's requirements. However, if Windows Defender is not set to the maximum possible level of protection, then a red warning will appear here, claiming that your system is unprotected. As long as you follow the advice in this chapter, if this warning still appears, you can disable it by clicking the 'Turn off messages about virus protection' link in the red box.

Spyware and unwanted software protection: This category is similar in nature to the Virus Protection category above, however it relates to less malicious, but still undesirable, software such as spyware. The key difference is that there are software packages specifically designed only to detect spyware and the like, and the installation of such a recognized package will prevent this category from flagging any problems. Of course the built-in Windows Defender once again satisfies this criteria as well, but again, may flag a warning if it is not set to the maximum possible protection level.

Note that if you don't wish to use Windows Defender, then I provide a range of other anti-malware packages you can use later in this chapter, or you can click the 'Find an app online to help protect my PC' link beneath the two categories above to get recommendations from Microsoft.

Internet Security Settings: This category monitors Internet Explorer's security settings, such as Protected Mode, the IE SmartScreen Filter, and its general Security Level. If these are not at recommended levels, Windows will warn you and allow you to reset them to secure levels again - see the Internet Explorer chapter for details of these features.

User Account Control: This category monitors the built-in User Account Control (UAC) feature in Windows. UAC is covered in full detail in the next section of this chapter. I strongly advise against disabling UAC for a range of reasons. Clicking the 'Change settings' link here, or clicking the 'Change User Account Control settings' link on the left side of the Windows Action Center window, will take you directly to the UAC settings window.

Windows SmartScreen: This is a new system-wide security feature in Windows 8, previously only available when using Internet Explorer. SmartScreen is designed to protect you against downloading and launching malicious software, and is covered in more detail in the SmartScreen section later in this chapter. If SmartScreen is disabled, then a warning will be shown here. I recommend against completely disabling SmartScreen. Clicking the 'Change settings' link here, or clicking the 'Change Windows SmartScreen settings' link on the left side of the Windows Action Center window, will take you directly to the SmartScreen settings window.

Network Access Protection: This category relates to Network Access Protection (NAP), which is a feature Network Administrators can use to make sure that any computer connected to a network of computers meets the minimum security requirements for that network. It serves no purpose for the average home user and should be disabled, which it usually is by default.

Windows Activation: This section shows your Activation status. Your copy of Windows 8 should be activated automatically during the installation of Windows, otherwise you may face a range of restrictions. Click the 'View activation details' link to see more details. See the Windows Activation section of the Windows Installation chapter for more details.

CONFIGURING ACTION CENTER

Action Center can be useful as an initial reminder to install and configure various security-related settings or software soon after installing Windows. Over time, once you have bedded down your software configuration and are comfortable with the level of security you have chosen, for the most part the prompting behavior of Action Center can become quite annoying and pointless. You can disable individual prompts from within the Action Center, all the way to removing the Action Center from the Notification Area altogether if you so wish.

To configure Action Center, click the 'Change Action Center settings' link on the left side of the Action Center window. Here you can untick the specific categories for which you do not want Action Center to alert you, then click OK. There is a danger in disabling categories in this manner, because there may be new, completely legitimate, security warnings related to a particular security component that will now not appear.

A better method of controlling the way in which Action Center prompts appear is to open the Notifications Area Icons component of the Windows Control Panel, or click on the small white arrow at the left of the Notification Area and select Customize. Under the Icons column, look for the Action Center, and under the Behaviors column you can select from the following options:

- Show icon and notification - Allows Action Center to both notify you of any alerts, and constantly shows the Action Center's flag icon in the Notification Area.
- Hide icon and notifications - Removes the Action Center flag icon from the Notification Area and also prevents any alerts from popping up. You can still access the Action Center icon by clicking the small white triangle in the Notification Area, or through the Windows Control Panel.
- Only show notifications - This hides the Action Center flag icon, however alerts will still pop up in the Notification Area periodically.

So instead of removing Action Center warnings for entire security categories, you can select 'Only show notifications' above, and hence Action Center will remain hidden most of the time in the Notification Area, but you will still be briefly prompted periodically if a security issue is detected, and you can still open Action Center directly and browse the warnings and security status of each category.

If you wish to completely disable all Action Center security prompts, then select 'Hide icon and notifications' above. You can also prevent Action Center from actively monitoring security-related settings by disabling the 'Security Center' Service - see the Services chapter for details. This is only recommended if you are frequently being annoyed by Action Center and you are an advanced user who has sufficient knowledge and tight control over system security. Otherwise it is best to leave Action Center hidden but able to prompt you should a potential issue arise.

< USER ACCOUNT CONTROL

A fundamental change in security for Windows, first introduced in Vista, is the restriction of Administrator privileges for any user account. Windows 8 continues with this concept, known as User Account Control (UAC).

The reason Administrator access to a system may need to be restricted is that a user logged in with an Administrator user account can do pretty much anything to the system, from altering or deleting system files to installing any software to creating or deleting other user accounts. This provides a user with the greatest power and flexibility, and hence is the preferred choice for most users, as opposed to a Standard user account - see the User Accounts chapter for more details.

The problem is that malware capitalizes on the fact that most people run Administrator level user accounts for the sake of convenience. Malware uses this loophole in various ways to get itself installed, often quietly in the background, and hence gains unrestricted access to your system. Furthermore, running as an Administrator means that a user may inadvertently make undesirable system changes without being aware of their potentially disruptive nature to the system, or to other users. Thus running an unrestricted Administrator user account as your day-to-day account has a great deal of risk attached to it, both in terms of security and system integrity.

In an attempt to balance these risks with user convenience, Windows manages user account access privileges with UAC, which is enabled by default. It turns an Administrator account into what is known as a Protected Administrator account; basically, an Administrator account runs with Standard user account privileges most of the time. See the User Account Privileges section of the User Accounts chapter for more details.

THE UAC PROCESS

A simple walkthrough of the User Account Control process at the default UAC settings in Windows 8 is provided below, and in more detail in this Microsoft Article. If you alter your UAC settings you may not see some of the steps below:

Step 1 - Regardless of whether you're logged in with a Standard or Administrator user account, you are restricted to only making changes to the files and folders you own, installing non-intrusive software and other basic functionality. Essentially you have Standard user privileges even if logged in as an Administrator.

Step 2 - As soon as you try to make a system-intrusive change such as installing a driver, editing the Windows Registry, or altering or deleting another user's files, Windows will require Administrator level privileges. Since even Administrator user accounts run with only Standard user account privileges by default, user account privileges must be elevated to full Administrator level before proceeding with any such changes. To allow this, a UAC Elevation Prompt will appear. Note that programs which trigger a UAC prompt are usually denoted with a blue and gold shield icon on their icon in the Desktop environment.

Step 3 - When a UAC prompt is displayed, the important aspects of the prompt you should pay close attention to are:

- *Secure Desktop Mode* - Your Windows background may dim slightly as you are placed in a sort of "limbo", whereby no other program can execute itself except for important system processes. This Secure Desktop is an important layer of protection, and can help prevent malware from doing things like faking the file details on a UAC prompt, or automatically accepting a UAC prompt.
- *UAC Prompt Color* - The UAC prompt will have a background color corresponding to the potential level of risk involved: Blue (safe), Yellow (warning) or Red (blocked).
- *Administrator Password box* - If you are not currently logged in as an Administrator, you will be prompted to enter the password for an Administrator user account on the system before you can continue. If you are already logged in with an Administrator-level user account, you can simply press Yes to continue without needing to enter a password.
- *Yes and No Buttons* - You can't just press Enter to continue as soon as a UAC prompt appears, because by default the UAC prompt's focus is on the No button. This helps ensure that you don't get into the habit of quickly pressing Enter whenever you see a UAC prompt without paying attention.
- *Program Details* - Details of the program to be launched are displayed, with the program or filename, publisher, and the location from which it was launched all shown clearly in the prompt. In some cases the publisher may be unknown or untrusted. To find out more, click the 'Show details' down arrow and you can then see the path to the program file being launched, and click a link to get more details about the publisher.

Step 4 - If you have any doubts about the program being launched, click No. If you click Yes to continue and have the appropriate credentials - that is, you are logged in as an Administrator, or a Standard user who enters a correct Administrator password - the program will then install or launch as normal with full system access and full functionality. Programs which do not get Administrator level access may still install or launch, however they may have reduced functionality - see the File System and Registry Virtualization section further below for details.

DETECTING MALWARE USING UAC

Microsoft has made it clear that although UAC can be used to prevent certain security vulnerabilities, it is not designed as a foolproof protection method against malware. This is because there are known ways of exploiting UAC prompts, or bypassing UAC, which even the most advanced user cannot detect. Despite this, the presence of UAC has already been shown to have increased resilience to malware in Windows Vista and 7. Obviously less advanced users are still likely to disable UAC, or click Yes to any and every UAC prompt (indeed any type of prompt) which appears before them. However, more advanced can utilize UAC to their advantage, and educate less advanced users to do the same.

When combined with appropriate user vigilance, and a range of built-in Windows security features such as Data Execution Prevention (DEP) and Address Space Load Randomization (ASLR) - both covered later in this chapter - UAC is yet one more security barrier, and can still be quite effective against many types of malware and exploits, if used properly. Below are some tips on how to use UAC correctly:

A UAC Prompt Appears - This in itself is confirmation that a program you are about to launch, or a file or document you are about to open, requires access to restricted areas of the system. For a document, this is almost always a warning sign, as opening a standard .DOCX or .PDF file for example should not require Administrator privileges. For a program, there should be no need for relatively straightforward or purportedly non-intrusive functionality to require unrestricted access to your system. This does not mean that a program or file which does is malicious, but it is certainly a warning sign of a potential issue, or an indication of poor programming, both of which warrant further investigation before installation. This is also true of any situation in which you did not expect a UAC prompt and one suddenly appears. Don't just accept every UAC prompt you see.

Even if a program or file has no malicious intentions whatsoever, you are still giving it unrestricted access to your system should you accept the UAC prompt. This means the program may make system-intrusive alterations that can destabilize your system, or make undesirable and irreversible changes to it. Consider whether you really need to install or launch that program, as the more of these types of programs you have on your system, the greater the potential for problems regardless of any security concerns.

The UAC Prompt Color: Look at the UAC prompt's color. If the UAC elevation prompt is:

- Blue - A blue background combined with a blue and gold shield icon at the top left indicates that the program is digitally signed and recognized as a default Windows application, and can be trusted. A blue background, combined with a blue question mark shield icon, means the program is a non-Windows application but the publisher is known and can be trusted. In both cases this is not a guarantee of security, as some malicious software can find ways to attach itself to a trusted program, but it is certainly a good sign.
- Yellow - A yellow background shows that the publisher is not known. Some caution needs to be taken in determining whether this is a safe application. In practice, in most cases it will be safe, it is simply a case of the lack of a verified digital signature on the application. But it still bears further research if you have any doubts at all.
- Red - The program is from a known untrusted publisher and is blocked. It cannot and should not be run on your system.

The general rule is that a standard blue background on a UAC prompt, especially when using what you would expect to be a safe and trusted application, such as a built-in Windows utility, is sufficient reassurance that the application is highly likely to be precisely what it says it is. A yellow background which appears on a newly downloaded application is cause for undertaking further research and ensuring that (a) you have downloaded a genuine copy of the application or file from a trusted source, and (b) that you scan the download with a malware scanner. You should never see a red background when launching an application or file; this is a major warning sign, and the program is best deleted immediately, followed by a full system malware scan.

The Program Details: The UAC prompt clearly shows the program or filename, publisher and location of the program/file. These should be quickly looked at, and if anything out of place is noted, the UAC prompt should be cancelled and more research done before launching with full Administrative rights. More important is the 'Show Details' button, which takes you to the exact filename and full path for the program. If you have any doubts about the program, e.g. the UAC prompt has a yellow background, then examine the path very closely. One trick malware can use in a UAC prompt to fool even advanced users is to show a path similar to a real location on your drive, but actually different. For example, look closely at these two paths:

C:\Program Files\Recuva\Recuva64.exe

C:\ProgramFiles\Recuva\Recuva64.exe

At first glance they may appear identical and completely legitimate, especially if seen in isolation. But when examined closely, it soon becomes apparent that the second path is referring to a non-system location which doesn't exist by default, i.e. *C:\ProgramFiles*. The correct and genuine protected system location is *C:\Program Files* - note the space between the two words. So if in doubt, click the 'Show Details' button, note the exact path as shown, then investigate further. For example, do a full system search on the filename (see the Windows Search chapter), and where you find duplicates of the exact same file, check to see where and why this is the case, combined with some web research. A program never has multiple primary executables with identical names, especially if one has a verified digital certificate and the other doesn't, and/or one usually resides in a secure directory location and the other doesn't.

Digital Signature: Digital signatures are covered under the Driver Signature section of the Windows Drivers chapter. A verified digital signature validates that the publisher of a file is who they say they are. A trusted certificate testifies to this fact, and is available to be viewed when you click the 'Show Details' button in the UAC prompt and click the 'Show information about this publisher's certificate' link. However a lack of a verified digital signature is not necessarily cause for alarm, as not all publishers go to the trouble and expense of getting one. Still, it is a feature of a reputable program that it is signed, and the publisher is known and properly verified, and therefore trusted by Windows. If you see a yellow UAC prompt, the publisher cannot be confirmed, and you should investigate further. If you see a red UAC prompt the publisher is untrusted and the program should not be installed or executed. In all cases, if in doubt, run a malware scan over the file or your entire system, and do further online research before installing it.

UAC is not a replacement for common sense and it is not a fully automated barrier against malware. Many of the tools and tips covered later in this chapter must be used in conjunction with UAC for it to be effective. Contrary to popular belief, while UAC can help beginners in preventing some malware, it is actually best used by advanced users to not only flag potentially suspicious software or behavior for further investigation, but to also warn you that what you are about to do, even if not malicious in nature, will be system-intrusive. This will allow you to pause and reconsider launching the application, or backup your system and use System Restore to create a restore point before proceeding for example. There should be no reason for any user, no matter how advanced they believe themselves to be, to disable UAC. However, you can customize UAC as covered further below.

File System and Registry Virtualization

In order to provide compatibility with older applications not built with UAC in mind, UAC incorporates File System and Registry Virtualization. When UAC is enabled, this virtualization comes into effect if a program requires, but does not request and/or is not given, full Administrator privileges while attempting to install itself, or make changes to the following protected system folders/sub-folders and system-wide Registry locations:

§ *Program Files*
§ *Program Files (x86)*\
§ *Windows*
§ `[HKEY_LOCAL_MACHINE\SOFTWARE\]`

Any files, folders or Windows Registry changes the program needs to make are automatically redirected to local copies which are stored under the current user's profile locations:

§ *Users**[Username]**AppData**Local**VirtualStore*\
§ `[HKEY_CURRENT_USER\Software\Classes\VirtualStore]`

This prevents Standard user accounts on your system with insufficient privileges from potentially harming the system, but still allows them to install and use many types of software.

This is not a foolproof solution. Some programs can only function if they have full Administrator access, but may not ask Windows for such privileges, and hence there will be no UAC prompt to escalate their privileges during installation, or at launch time. Virtualization may allow them to install or run, but they will fail to launch or function properly once installed.

The best way to address the issue of certain trusted applications failing to install or launch properly when UAC is enabled is to go to the main setup executable or launch icon for the program, right click on it and select 'Run as Administrator'. This will launch the program and automatically raise a UAC prompt to elevate privileges, which you will need to successfully accept to continue. The program will then run or install as normal, having been given full Administrator access. To set this behavior permanently, right-click on the main executable or launch icon, select Properties and under the Compatibility tab tick the 'Run this program as an administrator' box at the bottom and click OK. Alternatively, if that option is not available, go to the Shortcut tab for the program's launch icon properties and click the Advanced button, then place a tick in the 'Run as Administrator' box. Only do this if you completely trust the application, having obtained it from a reputable and trusted source.

Importantly, because of File System and Registry Virtualization, if you install an application under a Standard user account, or don't accept an elevation prompt from UAC, your settings for particular applications may be stored under your local profile. If you then switch to another user account, or run that same application with full Administrator privileges later on, your settings may appear to have been lost or reset to the defaults as the program switches to using another set of folders or another area of the Registry for its saved settings. In simple terms this means that it is not wise to enable or disable UAC constantly. For common solutions to virtualization issues, see this Microsoft Article.

Customizing UAC

In Windows Vista, the only User Account Control options presented to all users was whether to disable or enable UAC. From Windows 7 onwards, all users have the ability to easily customize UAC to better suit their needs through a graphical user interface. It should be understood though that changing UAC settings can also reduce the protection provided by this feature. In fact disabling certain UAC settings is in some ways worse than just turning it off, because it can give you a false sense of security.

To customize UAC settings, go to the User Accounts component of the Windows Control Panel and click the 'Change User Account Control settings' link, or when a UAC prompt appears, click the 'Change when these notifications appear' link at the bottom of the prompt. There are four preset levels for UAC, and each is covered in more detail below:

Always Notify Me - This setting is the maximum possible level for UAC. It means that UAC will prompt you whenever any software attempts to make system-intrusive changes, as well as whenever you attempt to change most Windows settings. This provides the best security but can be annoying, especially when you first install Windows 8 and have to make a lot of changes to Windows settings.

Notify Me Only (Default) - This is similar to the 'Always Notify Me' setting, with the important exception that you will not be prompted whenever changing common Windows settings. This is because most built-in Windows software is digitally signed and verified in such a way that Windows recognizes it as a trusted and secure native Windows application, and automatically provides it with full Administrative access. This introduces slightly increased risk, because malware may attach itself to, or launch under cover of, trusted Windows applications, but in practice the risk is low. As long as you use the tools and practice the tips provided throughout this chapter, the difference in security between the 'Always Notify Me' level and this level of UAC is relatively minor, and is outweighed by the convenience of being able to carry out common Windows tasks without constantly being prompted. This acceptable compromise is confirmed by the fact that it is the default level for UAC in Windows 8.

Notify Me Only (Do not dim my desktop) - This setting is identical to the Default setting above, with the exception that you will not enter Secure Desktop mode whenever a UAC prompt appears. That is, the screen background will not dim when a UAC Elevation Prompt is shown. As discussed earlier, the Secure Desktop feature is an important barrier against having a UAC prompt faked or manipulated in such a way as to deceive you into accidentally launching a potentially harmful program. This UAC setting should only be used if your system has major problems with entering Secure Desktop mode, such as long delays, or graphical glitches. Selecting this option reduces your security further, and given the relatively infrequent appearance of the UAC prompt, even a slight delay in showing the Secure Desktop is hardly a major inconvenience.

Never Notify - This option effectively disables UAC. If you are using an Administrator level account, any system-intrusive changes you make, or programs you install, will be done without prompts, and all programs will have unrestricted access to your system. For Standard user accounts, any apps or features which would normally raise a UAC prompt will automatically be denied. Further, disabling UAC completely will effectively disable Protected Mode in Internet Explorer. This option is the least secure, and it is strongly recommended that no user - whether novice or advanced - select it.

I recommend the default option for UAC in Windows 8 as a good balance of security and convenience. However it must be used in conjunction with a range of other security measures as covered in this chapter. On its own UAC is not and does not purport to be an invulnerable barrier to malware, especially because much of the defense provided by UAC relies on user vigilance and education. It is definitely not designed to be a set-and-forget anti-malware feature.

Local Security Policy

In addition to the standard UAC options available to all users, Administrators using the Pro or Enterprise editions of Windows 8 have access to the UAC-related Local Security Policy settings, which allow further customization of UAC. To change these settings, you can use the Local Security Policy Editor. To access the Local Security Policy Editor open the Administrative Tools component of the Windows Control Panel and select it from there, or go to the Start Screen, type *secpol.msc* and press Enter. The options we want to

examine reside under the Local Policies>Security Options folder in the left pane. When that folder is selected, the following options are shown in the right pane, all of them begin with the words 'User Account Control':

Admin Approval Mode for the Built-in Administrator account: This setting determines whether the built-in Administrator account in Windows is affected by UAC - by default it is not. This account is not the same as the Administrator account you create when installing Windows, this setting refers to a hidden built-in Administrator account as covered under the Advanced Settings section of the User Accounts chapter.

Allow UIAccess applications to prompt for elevation without using the secure desktop: This setting determines whether User Interface Accessibility (UIAccess) programs, such as Windows Remote Assistance, can automatically disable the Secure Desktop feature when providing UAC elevation prompts. Disabled is fine for most people, unless you are in an environment where you're likely to need remote assistance and are using a Standard user account.

Behavior of the elevation prompt for administrators in Admin Approval mode: By default the UAC prompt will ask Administrators to simply click Yes to proceed for non-Windows programs. This is equivalent to the 'Prompt for consent for non-Windows binaries' option and is recommended. You can however select:

§ Elevate without prompting - Removes prompts altogether for Administrator accounts.
§ Prompt for credentials on the secure desktop - Prompts for full Administrator credentials, including a Password, using the Secure Desktop.
§ Prompt for consent on the secure desktop - Same as above, except does not prompt for the Password.
§ Prompt for credentials - Prompts for a Password without using Secure Desktop.
§ Prompt for consent - Simply asks Yes or No to proceed without using Secure Desktop.

Behavior of the elevation prompt for standard users: This option is similar to the one above, however it controls the behavior of UAC for Standard users not Administrators. The options are 'Prompt for Credentials', which asks the user to enter an Administrator password, but you can increase this to 'Prompt for credentials on the secure desktop' to do the same thing using Secure Desktop mode as well, or you can select 'Automatically deny elevation requests' if you want tight security, so that Standard users won't see a UAC prompt and won't be able to undertake any task that triggers a UAC prompt.

Detect application installations and prompt for elevation: If Enabled, Windows will attempt to detect a program installation and UAC will kick in to ensure the application gets Administrative access if it requests it; if Disabled, any program can be installed without a UAC prompt, but this is not wise for a home user as programs which need Administrator access but don't request it won't get it, and won't install properly.

Only elevate executables that are signed and validated: If Enabled, forces Public Key Infrastructure (PKI) certificate validation before an executable can be run. In other words, only signed, validated, and therefore trusted executables can be given full Administrator access to the system. Disabled is recommended for home users unless you require absolute maximum security, as some legitimate programs will fail this test.

Only elevate UIAccess applications that are installed in secure locations: If Enabled only UIAccess applications which reside in a secure location, namely under the *\Program Files*, *\Program Files (x86)* or *\Windows\System32* directories, will run with UIAccess level integrity; if Disabled any UIAccess program can run with UIAccess integrity from any location. There is no reason to Disable this as it provides an extra layer of security against malware.

Run all administrators in Admin Approval Mode: This option provides the core functionality of UAC. If Enabled all Administrator user accounts will operate as described earlier in this section. If Disabled then UAC is effectively disabled for Administrator user accounts, so it is not recommended unless you explicitly want to

disable UAC for Administrators and leave it functional for Standard users, and understand the risks involved in doing so.

Switch to the secure desktop when prompting for elevation: Secure Desktop mode has been described further above and is a critical component of UAC. It prevents tampering or execution of programs in the background when UAC is running. You can Disable it here but it is not recommended, especially as it can be disabled via the standard UAC settings.

Virtualize file and registry write failures to per-user locations: As discussed under the File System and Registry Virtualization section above, when Enabled (by default), this option ensures that Standard user accounts can still install applications that require traditional full Administrator access; the system locations usually written to by the program will be "virtualized" by redirecting them to locations within the Standard user's personal folders.

You should ensure that you do not change any of the above options unless you have good reason to do so. Most of the default settings above are necessary for UAC to work effectively, and other options are provided mainly for Network Administrators operating under corporate environments where UAC may hinder specific functionality.

If your version of Windows has no Local Security Policy Editor, you will instead need to access the Windows Registry if you want to customize the UAC settings covered above. See the introduction to the Group Policy chapter for a link to a spreadsheet that contains the various Group Policy-based settings and their Registry locations.

UAC AND THE LANGUAGE BAR

In some instances, when a UAC prompt appears, the Language Bar will also appear at the top of the Desktop. If you do not need to switch languages, this is an unnecessary addition, and can be disabled by going to the following location in the Windows Registry:

```
[HKEY_USERS\.DEFAULT\Software\Microsoft\CTF\LangBar]
```

```
ShowStatus=3
```

The `LangBar` key and/or `ShowStatus` entry may not exist, so right-click on the `CTF` key shown above and select New>Key then name it `LangBar`. Left-click on `LangBar` and in the right pane create a new DWORD called `ShowStatus` and set it to a value of 3 to prevent the language bar from appearing whenever a UAC prompt appears. If you want to reverse this, set the above entry to a value of 0.

Some final thoughts on User Account Control:

- § UAC has no performance impact, compared to the performance impact that background malware scanners have in slowing down reads and writes to your drive.
- § UAC tries to provide a compromise between the convenience of running an Administrator user account all the time and the security of running a Standard user account.
- § UAC gives both novice and advanced users notification that a program is about to make system-intrusive changes.
- § UAC is highly useful when there are multiple user accounts on the same PC. By setting these accounts as Standard users and enabling UAC, the users cannot install harmful software or change key system settings, but can still use most non-intrusive software normally, and without impact on other users.
- § The default UAC setting in Windows 8 allows a range of basic Windows settings to be altered without an Administrator or Standard user experiencing a UAC prompt.

Make sure to also read the User Accounts chapter for relevant details regarding privilege levels and setting up multiple user accounts before considering any changes to UAC settings.

On balance there is no reason for anyone, especially advanced users, to disable UAC.

< ACCESS CONTROL AND PERMISSIONS

Windows assigns every item on the system a security descriptor which specifies which users or groups are allowed access to them, and what that level of access is. This is designed to prevent unauthorized access or harmful changes by users with insufficient privileges. To view these Permissions for any file or folder, right-click on it and select Properties, then under the Security tab you can see the groups or usernames currently assigned to that object. Left-click on a particular group or username and you will see in the box below it the types of things they are allowed to do.

All of the files and folders under your personal folders belong to you, and you are permitted to alter them as you wish. Furthermore, any files or folders you create are automatically assigned to you as the owner. However, if you wish to alter certain system files or folders, or some areas of the Windows Registry, you may need to first take ownership of them, and this in turn allows you to change the permissions for what a particular user or group can do to them. There are essentially two aspects to the process:

TAKING OWNERSHIP

If you are an Administrator you can take ownership of any file, folder or Registry key as follows:

1. In File Explorer, right-click on the file or folder and select Properties; in Registry Editor, right-click on the key and select Permissions.
2. Under the Security tab, click the Advanced button.
3. In the Owner section at the top of the Advanced Security Settings window click the Change link.
4. Enter the user account name you wish to assign as the new owner in the 'Enter the object name to select' box, then click the 'Check Names' button and it should be correctly identified. Click OK.
5. Back in the Advanced Security Settings window, tick the 'Replace owner on subcontainers and objects' box if you also wish to take ownership of any subfolders and objects within a folder, then click the Apply button to change ownership and click OK.

To then make any changes to the file, folder or Registry key, you will need to alter its permissions.

ALTERING PERMISSIONS

Once you have ownership, you can view and alter permissions for all the users of that file, folder or Registry key. To do so, follow these steps:

1. In File Explorer, right-click on the file or folder and select Properties; in Registry Editor, right-click on a key and select Permissions.
2. Under the Security tab, in the top pane you can select particular users or groups, and in the bottom box you will see tick marks corresponding to the various permissions granted or denied to that user or group.
3. To alter a permission, for example to give yourself full permission to alter a file as you wish, you must first be the owner - see the section above. Once you are the owner, click the Edit button for a file or folder, or skip to the next step for a Registry entry.
4. In the Permissions window which appears, you can highlight any group or user, and if you are the owner, you can tick or untick particular permission categories.
5. To give yourself complete control over a file, folder or Registry entry, highlight your user name, tick the 'Full Control' box under the Allow column, then click the Apply button. Click Yes to the prompt that appears, and click OK.

You now have full control over the file, folder or Registry entry as though you created it yourself, and can modify or delete it as you wish. Obviously this brings with it a range of risks, which is precisely why you were restricted from easily accessing it in the first place, and had to go through the steps above just to gain full access.

Given the system has to check permissions for every file and folder, it is better for system performance purposes to assign permissions to particular groups, rather than specific users, wherever possible. Furthermore, for security purposes, do not give yourself ownership and full permission over general system folders such as *\Windows* and all of its subdirectories, and definitely not on a system-wide basis.

Instead of using the above method, you can use the `Takeown` command to claim ownership of an item. Open an Administrator Command Prompt, type `Takeown /?` and press Enter for details of how to use the command. This command also allows advanced users to write more complex scripts which can take ownership of a range of files, rather than having to do it individually.

There is a way to integrate the `Takeown` command into the Windows shell, so that you can right-click on any file or folder and select a 'Take Ownership' context menu item to do the above automatically. This should be used with caution, and is only recommended for advanced users who know the consequences and potential security risks of taking ownership of a file or folder.

This procedure is relatively complex. Start by going to the following locations in the Registry Editor:

```
[HKEY_CLASSES_ROOT\*\shell]
```

```
[HKEY_CLASSES_ROOT\Directory\shell]
```

Right-click on each of the subfolders above, select New>Key and create a key called `runas` then right-click each of these new keys, select New>Key again and create a key called `Command` - the end result should look like this:

```
[HKEY_CLASSES_ROOT\*\shell\runas\command]
```

```
[HKEY_CLASSES_ROOT\Directory\shell\runas\command]
```

Now go back up to the following subfolders and left-click on each one:

```
[HKEY_CLASSES_ROOT\*\shell\runas]
```

```
[HKEY_CLASSES_ROOT\Directory\shell\runas]
```

In each case, in the right pane, double-click on the `Default` value and enter the following value data:

```
Take Ownership
```

Right-click in the right pane, select New>String and create the following string with no value data:

```
NoWorkingDirectory
```

Once done, go to the following key:

```
[HKEY_CLASSES_ROOT\*\shell\runas\command]
```

Left-click on the above key, and in the right pane double-click on the `Default` value and enter the following data, exactly as shown, including all quotes and symbols:

```
cmd.exe /c takeown /f "%1" && icacls "%1" /grant administrators:F
```

While still in the right pane, right-click and select New>String, call it `IsolatedCommand` and enter the following value data, which is the same as the data entered above:

```
cmd.exe /c takeown /f "%1" && icacls "%1" /grant administrators:F
```

Once done, go to the following key:

```
[HKEY_CLASSES_ROOT\Directory\shell\runas\command]
```

Left-click on the above key, and in the right pane double-click on the `Default` value and enter the following data, exactly as shown, including all quotes and symbols. Note that it is not the same as the value data used further above:

```
cmd.exe /c takeown /f "%1" /r /d y && icacls "%1" /grant administrators:F /t
```

While still in the right pane, right-click and select New>String, call it `IsolatedCommand` and enter the following value data, which is the same as the data entered above:

```
cmd.exe /c takeown /f "%1" /r /d y && icacls "%1" /grant administrators:F /t
```

When complete, you can now right-click on any file or folder, and a 'Take Ownership' context menu option will appear, allowing you to easily take ownership of a file or folder. To undo this feature at any time, delete the following keys - that is, go to each key, right-click on it and select Delete:

```
[HKEY_CLASSES_ROOT\*\shell\runas]
[HKEY_CLASSES_ROOT\Directory\shell\runas]
```

While taking ownership and changing permissions may be necessary for making certain changes in Windows, if you absolutely must operate without any restrictions for making a large number of changes, rather than taking ownership of a large number of files, folders and Registry settings with your regular Administrator account - which is a security risk - you should consider temporarily using the unrestricted hidden Administrator account instead. See the Advanced Settings section of the User Account chapter.

< WINDOWS DEFENDER

A key security feature included in Windows 8 is Windows Defender. In Windows Vista and 7, the primary aim of Windows Defender was to provide a basic level of protection against spyware, as this is one of the most common types of malware found on the average PC. However this cut-down version of Windows Defender was not designed to provide effective protection against a large range of other forms of malware - for that, a standalone anti-malware package was necessary.

This has changed in Windows 8. Windows Defender now has the same functionality as the full version of the Microsoft Security Essentials (MSE) anti-malware software package. This means that you now have a very effective anti-malware package built-in and running in the background immediately after you have installed Windows. Furthermore, if Windows 8 detects that you have installed another acceptable anti-malware package, it will automatically disable Windows Defender. If the third party anti-malware package ever becomes out of date, Windows will then prompt you to update it in the Action Center, and after 15 days you will also be given the choice to re-enable Windows Defender from a list of possible alternatives.

For the most part I now recommend running Windows Defender as your sole anti-malware package. This may sound like dubious advice at first, but it is part of a balanced approach. Third party anti-malware packages are known to cause a range of problems and conflicts, particularly when running side-by-side. This includes slowing down performance, causing issues with software installation or usage, unusual behavior such as crashes or freezes, and falsely identifying legitimate software or websites as being harmful. These packages are becoming increasingly more intrusive in an effort to proactively detect and block various types of malware and social engineering attempts on your system. Unfortunately, the end result is that any marginal amount of increased security which these packages provide is usually outweighed by the much greater potential for problems that they cause.

Windows has reached the point where it has a combination of powerful anti-malware features built-in, as we will examine in various sections later in this chapter. These have already proven themselves to be highly effective against most forms of intrusion, without any significant impact on performance or stability. Since Windows Defender is now basically the same as Microsoft Security Essentials, which has also shown itself to be quite successful at detecting malware, yet is also one of the least performance-intensive or problematic of all anti-malware packages, there is no pressing need to install any third party solutions.

There is a common misconception that running one or more third party anti-malware packages, or finding and using the "best" anti-malware package - and each security expert will have a different opinion of which package is the best - will somehow automatically protect you against security breaches. This is patently false. As in several other areas of Windows usage, there is no set-and-forget method of remaining secure. If there was, everyone would be using such software, and malware would be on the decline. The reality is that most security breaches these days use relatively simple social engineering techniques against which no automated software can provide any true barrier.

Basically, a combination of Windows Defender, the other defenses built into Windows 8, and most critical of all, user education and vigilance, are the best form of protecting yourself against any security breach while also keeping your system problem-free and performing optimally. If you still wish to use a third party anti-malware package, then see the Additional Security Software section later in this chapter for some suggestions. Note that since Windows Defender is much the same as Microsoft Security Essentials, you will not be able to install MSE on Windows 8, and there is no point in trying.

CONFIGURING WINDOWS DEFENDER

Windows Defender allows users to configure precisely how intrusive it will be in scanning for malware on your system. For novice users, there is no need to configure Windows Defender, as by default it is set for the maximum level of protection, while still being light on system resources. For medium to advanced users, it is recommended that Windows Defender be modified to be slightly less intrusive if you want maximum performance from your system with a minimum of potential conflicts or issues.

To access the full user interface for Windows Defender, go to the Windows Defender component of the Windows Control Panel, or type *defender* on the Start Screen and press Enter. The elements of the Defender interface are covered below in detail.

Home: This tab displays your current security status:

§ Green - Everything is fine, and Windows Defender is using its recommended (default) settings.
§ Yellow - There may be a problem which requires attention. Most commonly this is due to an outdated definition file, so you should go to the Update tab and click the Update button to allow Defender to update over the Internet.
§ Red - A potential security threat has been detected. Alternatively, if you have disabled what Defender considers one of its key setting, it will also flag this as a security risk.

Seeing a red status indicator simply because you have disabled the real-time protection component for example can be misleading, since this does not mean you are at any significant risk, as long as you follow the rest of the advice in this chapter. Look closely though, because if the red status indicator is accompanied by details of a potential threat being found, and the red button on the home page says 'Clean computer', then potential malware has been detected. Click the 'Clean computer' button and either have Windows Defender undertake the default action for that risk type (see Default Actions below), or select another action for each detected file.

Also available under the Home tab are the manual scan options on the right side. You can select from a Quick, Full scan or Custom scan. The Quick scan is the fastest, going through your most important system files, folders and the Windows Registry to look for prominent traces of malware, and usually takes only a few minutes. A Full scan is much more thorough, going through every file, folder and system area on your PC looking for malware, and hence takes much longer, but provides much greater security. A Custom Scan allows you to select the specific drive(s) and/or folder(s) you wish to scan when you select it and click the 'Scan now' button.

In general I recommend running a Full scan at least once a week, and a Custom Scan whenever you download a potentially risky file from the Internet. For example, download the file to your *\Downloads* folder, then select only that folder in the Custom scan interface. Keep in mind that Windows SmartScreen, if enabled, also does a basic security check of any downloaded file before it can be launched.

Update: This tab shows the current version and date for the definition files. These definition files are extremely important, as they are the means by which Windows Defender can accurately detect new malware. You can keep Windows Defender up to date by regularly clicking the Update button here, or by checking Windows Update for new definition files. Defender will update itself with these files automatically, and the Action Center will periodically prompt you to update in case the definitions become out of date. I also recommend manually updating the definitions prior to launching any manual scan. Keep in mind that some forms of malware can prevent you from accessing the Internet, so do not let your definitions become more than a few days out of date, as you may then not be able to update them once infected.

History: This tab shows any malware detected by Defender. I recommend selecting 'All detected items' to see all malware detected on the PC so far. Note that if the 'Allow all users to view the full History results' is not ticked in the Advanced section of the Settings tab, each non-administrative user will not be able to see results from other users, which can help protect privacy on a shared PC. Administrators can just click the 'View Details' button to see more details. If a particular file has been quarantined, and you have done sufficient research to genuinely determine whether it is safe or harmful, then you can select the 'Quarantined Items' option here, then highlight that file and either click the Remove button to permanently delete it, or click Restore to put the file back into its original location. By default Windows Defender will delete quarantined files 3 months after being detected, though you can change this setting under the Advanced section of the Settings tab.

Settings: Defender comes with a good default configuration, so novice users in particular do not need to alter anything here. Below I provide recommendations for more advanced users to consider:

§ Real-time Protection - This option, which is enabled by default, allows Windows Defender to constantly monitor application and system behavior in the background to prevent malware from installing or executing on your system. The performance impact of having real-time protection enabled is minimal, and hence for most users this option should be left enabled for maximum security. However, performance-minded users may consider turning off real-time protection. This is because real-time protection has the potential to reduce performance, cause software conflicts and/or raise false positives. Ultimately, your choice should be based on a range of factors including: how risky your browsing and file downloading activities are; your level of PC knowledge; who else uses your machine; and your other Windows security-related settings, such as UAC. The more lax your system security or knowledge, and the more risky your online behavior, the greater the need to keep real-time protection enabled. You should also consider temporarily disabling real-time protection if troubleshooting any performance issues on your system. Note that if the real-time protection option is disabled, the Windows Defender status will go to red ('at risk'), and will also raise an alert in the Alert Center.

§ Excluded Files and Locations/Excluded File Types/Excluded processes - These three sections allow you to specify particular files or folders, entire file types, or processes that you don't want Windows Defender to include as part of its scans. It is not recommended that you exclude anything from Defender's scans, as this can allow malware to slip past undetected. However, if you know for certain that a particular file, folder, file type or process is going to be constantly picked up as a false positive, when you are certain that it is legitimate and harmless, then you can include it here.

§ Advanced - There several options here to further customize Defender's behavior. 'Scan archive files' if ticked allows scanning inside archives such as .ZIP, .CAB and .RAR files - I recommend ticking this, as malware can easily hide inside such files. 'Scan removable drives' if ticked scans any removable drives, such as USB flash drives, when they are attached to the system - an extra form of protection which is recommended, but may cause additional delays when you attach such drives. 'Create a system restore point' if ticked does precisely what it says: creates a new restore point for System Restore (if enabled) before taking any action against detected malware - I recommend ticking this option because it allows you to easily undo any potentially undesirable system changes Defender may make. 'Allow all users to view the full History results' if ticked allows non-administrator users the ability to see any detected malware from any other user on the same PC - this can have privacy implications because it may highlight sensitive filenames if enabled. 'Remove quarantined files after' if ticked automatically removes any detected malware which is quarantined after a certain period - generally you should research and either delete or restore any quarantined file shortly after detection, but this option, if enabled, ensures such files don't build up on your system over time due to inattention, as most are malicious and undesirable. The default of 3 months is fine for this setting.

§ MAPS - The Microsoft Active Protection Service (MAPS) reports information regarding malware found on your system by Defender back to Microsoft in order to improve Windows Defender's malware detection technology. Here you can select whether to opt out of MAPS, which is not recommended as it undermines the power of Windows Defender as a malware scanner; or you can select Basic or Advanced Membership. Basic is recommended. If you have concerns, see the Privacy Statement for more details. It is precisely because of the information gathered from a large user base that Windows Defender can provide such powerful malware detection functionality without resorting to the more intrusive measures that other scanners do. An example of the type of information collected, and how it is used, can be found in this Microsoft Article. Microsoft has proven in the past that it takes the protection of user information very seriously, so the risk to users is not great, especially at the Basic Membership level. If you still have privacy concerns, then you may wish to use another anti-malware package altogether, though most of these also require some form of user telemetry in order to improve their detection rates.

§ Administrator - This option allows you to enable or disable Windows Defender. Unticking this box and clicking 'Save changes' will automatically disable Defender and its associated service. If you want to re-enable Defender, you will need to go to the Action Center and click the 'Turn on virus protection' link.

Note that Defender will automatically disable itself if it detects another supported anti-malware package on your system.

Click the 'Save changes' button when finished adjusting the settings for Windows Defender.

Windows Defender uses a service called 'Antimalware Service Executable' (Windows Defender Service), with the associated file being *MsMpEng.exe.* The Windows Defender Service is set to Automatic by default, and needs to remain that way for Defender to work properly. Once running, unlike Microsoft Security Essentials, Windows Defender does not place an icon in your Notification Area.

WINDOWS DEFENDER COMMAND LINE UTILITY

If for some reason you cannot access the Windows Defender graphical interface, such as only being able to load up Windows in Safe Mode (with Command Prompt), you can access Defender using the Windows Defender Command Line utility. The utility (*MpCmdRun.exe*) can be found under the *\Program Files\Windows Defender* directory. To launch it and see all of the available options, follow the steps below:

1. Open an Administrator Command Prompt.
2. Type the following command exactly as shown (including the quotes) and press Enter:

   ```
   "%programfiles%\Windows Defender\MpCmdRun.exe"
   ```

3. For example, to run a Full system scan from the command line, enter the following command and press Enter:

   ```
   "%programfiles%\Windows Defender\MpCmdRun.exe" -Scan -ScanType 2
   ```

4. To stop a scan at any time press CTRL+C.

Windows Defender provides a good balance between security and convenience, and integrates seamlessly into Windows 8. In the past I have recommended combining Windows Defender/Microsoft Security Essentials with other anti-malware packages on your system. I no longer recommend this for a range of reasons outlined earlier in this section. You can still use other packages if you wish, but I believe this only provides a false sense of security and more potential problems, and is no substitute for user education and vigilance.

< WINDOWS SMARTSCREEN

Internet Explorer 7 introduced a built-in Phishing Filter that warned you if a particular site seemed to be deceptive, or was a known phishing perpetrator. From Internet Explorer 8 onwards, the name of this option was changed to the SmartScreen Filter, with features to detect and block potential malware downloads made through IE. It continues on in Internet Explorer 10, as covered in the Internet Explorer chapter.

A major change in Windows 8 is that it takes this Internet Explorer malware filtering concept, and applies it to the entire operating system. Windows SmartScreen is an important new security feature, and is one of the reasons why, along with the much more robust Windows Defender, there is now virtually no need for third party security software in Windows 8.

The SmartScreen concept is covered in this Microsoft Article, and its Application Reputation technique, first introduced in Internet Explorer 9, is covered in this Microsoft Article. Essentially, whenever you try to launch a program that has been downloaded from the Internet, SmartScreen will first check the file's status against an online reputation list. If the program has an established positive reputation, then no warning is shown and it will launch as normal - this occurs in the majority of cases. If the application has an established

negative reputation, typically the case for known malware, then you will be warned and should not run it. In some instances an application will have an unknown reputation, in which case a warning will be shown to make you aware that it could be potentially harmful - you can click the 'More Info' link to see details and to access the ability to run the program anyway.

If you see a SmartScreen warning prompt at any time, it is important to take heed and do further research before considering launching the downloaded application. Since the Application Reputation list is maintained by Microsoft online, it is always up to date, so it should be fairly accurate at all times. However the two key issues to consider are that firstly, you need to be connected to the Internet to use it, otherwise launching any downloaded application can raise a SmartScreen warning simply because you don't have Internet access to the latest version of the list. Secondly, an unrecognized application does not mean it is harmful in any way; it has simply not yet been properly identified in the Application Reputation list as to whether it is safe or harmful. Some applications are too new, or not well known, and hence can falsely be flagged as suspicious.

CONFIGURING WINDOWS SMARTSCREEN

To adjust the way in which SmartScreen works in Windows, you will need to either go to the Start Screen, type *smartscreen* and select Settings, or go directly to the Action Center component of the Windows Control Panel. Then you should click the 'Change Windows SmartScreen settings' link on the left side of the Action Center window, and the Windows SmartScreen window will appear. The available options are covered below:

- *Get administrator approval before running an unrecognized app from the Internet* - This is the maximum level of protection, and the default setting for Windows SmartScreen. It means that full Administrator privileges are required before a user can successfully launch an application which SmartScreen has initially blocked. This prevents any Standard user accounts on your system from launching potentially harmful applications, so it is generally recommended that you leave SmartScreen at this setting.
- *Warn before running an unrecognized app, but don't require administrator approval* - Similar to the setting above, a SmartScreen prompt appears under the circumstances described earlier in this section. However, any Standard user account can launch the application if they wish to ignore the warning. You should only select this if you completely trust the judgment of other users on your system, in that they will conduct sufficient research before launching a potentially harmful application.
- *Don't do anything (turn off Windows SmartScreen)* - This setting completely disables Windows SmartScreen, turning off its detection and prompting capabilities. This is not recommended.

Windows SmartScreen is not a foolproof method of detecting and preventing malware installation, but then again, no anti-malware software of any kind can make that claim. SmartScreen is however an important built-in extra layer of defense, not only in blocking known malware, but also in flagging any suspicious downloads for further investigation before you commit to running them on your system. In other words, if SmartScreen is enabled and you don't see a SmartScreen warning when attempted to run a downloaded program, you can be fairly certain it is actually safe.

The only reason you may wish to disable SmartScreen is if you frequently encounter false warnings for downloaded applications which you are certain are safe to run, or if you have serious concerns about privacy. By virtue of checking against an online Application Reputation list, Windows SmartScreen will send basic information about the programs you are download and installing to Microsoft. It is highly unlikely that Microsoft will store or use this information for anything other than making improvements to SmartScreen, however if this is still a major concern of yours, then you might wish to disable SmartScreen.

It is strongly recommended that you keep Windows SmartScreen enabled at its maximum setting to provide you and all users on your system with strong protection against launching harmful software that has been inadvertently downloaded from the Internet.

< WINDOWS FIREWALL

To help protect your system against intrusion through your network connection - typically via the Internet - Windows 8 provides a built-in Windows Firewall. The major role for a firewall is to prevent unauthorized network traffic from coming into or out of your system. For example, if a Trojan installs on your system, it needs to send your data back to its originator to fulfill its purpose. A firewall can block this type of unauthorized data transfer, thwarting the main aim of the malware which is to steal your sensitive information. Hackers also run automated programs looking all over the Internet for entry points (called Ports) into unprotected PCs, and this type of unauthorized entry can again be blocked through the use of a firewall. At the same time, the firewall is designed to allow your normal network traffic through without any problems.

There are actually two forms of firewall: software and hardware. Windows Firewall, and other third party firewalls you can install in Windows, are software-based. If you are using Cable/DSL router hardware, it often has its own built-in hardware-based firewall solution. You should enable both hardware and software firewalls together for maximum protection. The hardware firewall in your networking hardware will be enabled by default, but you must check its documentation to find out more about accessing the feature.

To access the Windows Firewall, go to the Windows Firewall component of the Windows Control Panel, or go to the Start Screen, type *windows firewall* and select Settings. Configuring the Windows Firewall, indeed any firewall, can be quite complex depending on your particular needs, especially if you are on a network of computers. The information below relates primarily to configuring the Windows Firewall options to suit an average home user connected to the Internet.

BASIC CONFIGURATION

On the main Windows Firewall screen you will see the status of the firewall. The first thing to note is that there are at least two network location categories shown: 'Private networks' and 'Guest or public networks'. These network locations relate to the choice of location you made when first installing Windows 8, and subsequently any changes you've made in the Network and Sharing Center, which is covered in more detail in the Network and Sharing Center section of the Windows Control Panel chapter.

Regardless of which location you are currently using, the Windows Firewall allows different active firewall configurations, one for each separate location. For example, you can be connected to a private home network and use one set of Windows Firewall settings for that network connection, while using another location and set of Firewall rules for browsing the web in a public location. Your currently connected location is always show in the category headers in the main Windows Firewall window, denoted as "Connected" or "Not Connected".

Full details of the relevant settings are covered below:

Windows Firewall state: Windows Firewall is on by default, but you can switch it on or off at any time by clicking the 'Turn Windows Firewall on or off' link on the left side, which takes you to the 'Customize Settings' screen for Windows Firewall. Here you can selecting the 'Turn off Windows Firewall' or 'Turn on Windows Firewall' option under your network location as relevant and click OK. It is strongly recommended that you do not disable Windows Firewall for either network location unless you have another reputable third party software firewall installed and active - in which case it is recommended that you only keep one software firewall enabled at any time, because two software firewalls will cause problems.

The status of the Windows Firewall can be seen at a glance, by looking at the color of the category heading for your network location, as well as any icons shown. If the color is green, along with a green shield with a

tick in it, the Windows Firewall is enabled. Red, along with a red shield with a cross in it, means the Windows Firewall is disabled. Choosing to customize the firewall to block connections beyond the default settings will also display an appropriate "blocked" icon.

Incoming Connections: Click the 'Change notification settings' link on the left side of the main Windows Firewall window, and under the 'Customize Settings' screen you can also choose to 'Block all incoming connections, including those in the list of allowed programs'. This is not recommended unless you want maximum security, because it brings with it the potential for impaired functionality. To see the list of allowed programs, also known as Exceptions, click the 'Allow an app or feature through Windows Firewall' link in the left pane of the main Windows Firewall window. This provides a full list of the default Windows apps, programs and features allowed to communicate freely through the Windows Firewall, as well as any third party programs which you have installed or allowed to be added to the list. Many programs automatically add an exception for themselves in this list, as it is necessary for their normal functionality (e.g. online games). However at any time you can select any Metro app, Desktop program or Windows feature here and untick the relevant box under your network location column to prevent it gaining automatic access through the Windows Firewall. By default, if a program is not provided access through the firewall when it needs it, Windows will raise a prompt asking whether you wish to 'Keep Blocking' it, or Unblock that program - if in doubt, select 'Keep Blocking' and investigate further. Furthermore, if you already see suspicious or undesirable programs on this list, temporarily disable them and do some research. Highlight the program, click Details to check the filename and path, then research it on the Internet. You can permanently remove any program by highlighting it and clicking the Remove button.

The more programs you allow through the Windows Firewall, the greater the security risk you face, so make sure to first untick and then eventually remove all unnecessary programs from the list. Fortunately, the programs on this list only open a hole (Port) through the Windows Firewall whenever they need to use it; they do not permanently open a Port, which would create much greater risk of unauthorized access.

Notification State: Under the 'Customize Settings' screen, accessible when you click the 'Change notification settings' link in the left pane of the main Windows Firewall window, the 'Notify me when Windows Firewall blocks a new program' box if ticked will enable the behavior described above. That is, Windows will prompt you if a program attempts to communicate over the network and is blocked, and you will be given the option to Unblock it or 'Keep Blocking'. If this box isn't ticked, you will receive no warning that a new program you are attempting to run is being automatically blocked by the Firewall and hence it may not function properly. Make sure you leave this box ticked unless you want to deny all firewall access requests.

ADVANCED CONFIGURATION

For most users the main Windows Firewall window provides all the settings they need to access. For more advanced users who have need of greater control over the firewall, you can access the Windows Firewall with Advanced Security interface by clicking the 'Advanced Settings' link on the left side of the main Windows Firewall window. A separate window will open, allowing much greater customization and monitoring of the Windows Firewall, including the ability to configure the blocking of outgoing network traffic, something that was not available in the Windows XP firewall.

Covering all of the functionality of the Advanced Windows Firewall settings is beyond the scope of this book, as it is quite detailed - for full details see this Microsoft Article. Below we will only look at how to enable the blocking of outbound network traffic, which is not usually required, but might be desirable for home users who want tight security. Remember that inbound traffic is already automatically blocked by the Firewall, unless an exception is made for particular programs, as described earlier in this section.

In the main Overview pane, you will see three profiles: Domain Profile, Private Profile and Public Profile. These profile types correspond with network locations, and are covered in more detail under the Network & Sharing Center section of the Windows Control Panel chapter. The network location you are currently using

will determine which of these three profiles is in effect - the words 'is Active' will be shown after the relevant profile type. You will see the Windows Firewall status, as well as the status of Inbound and Outbound connections. The default settings are that all outbound connections are allowed, even if they do not match any rules, while inbound connections that do not match a rule (i.e. are not made by allowed programs) are blocked.

For basic configuration of the Advanced Windows Firewall, click the 'Windows Firewall Properties' link in the main Overview pane. A new window will open with four tabs: one for each type of profile, and the last for IPsec Settings. Go to the tab for your active profile, and there are two settings of particular interest to us which are not available in the normal Windows Firewall settings:

Outbound Connections: The Windows Firewall blocks inbound connections by default, only allowing programs on the Exceptions list to go through. However all outbound connections are allowed by default to minimize the potential for problems. Here you can select to block all outbound connections which do not have a rule (see further below) by selecting Block from the drop down list and clicking the Apply button. I don't recommend doing this unless you are aware of the consequences, and have already set up relevant rules, because it can prevent you from accessing the Internet for example.

Logging: By default the Windows Firewall does not keep a log of successful or denied connection attempts. If you wish to enable logging, for example to troubleshoot a problem, or to see if there is any suspicious network activity on your system, then click the Customize button next to the Logging option and set the details of where and what to record in the log. The location of the log is available for you to see and customize, so that you can easily find and read the log file once it has compiled some data.

In the left pane of the Windows Firewall with Advanced Settings window you can select the 'Inbound Rules' or 'Outbound Rules' component and view all the existing rules for each of these. The rules under Inbound Rules are simply the list of all the allowed programs (Exceptions) discussed earlier. You can select any item under either Inbound Rules or Outbound Rules and in the right pane select from a list of available actions. You can also create a New Rule for a program, particular port, a predefined component, or even a custom rule.

The settings in the Windows Firewall with Advanced Security utility can be configured in such a way that, for example, you can block all outbound connections from your PC except those coming from your browser and email client. This provides you with normal Internet access, while at the same time preventing any other applications on your machine from communicating with the outside world. Generally speaking it is not necessary to go to these lengths for the average user, and rules-based determinations of ingoing and outgoing connections through the Windows Firewall can become quite tedious for most home users, especially as new programs are installed. This is why Windows does not have outbound connection blocking on by default. I only recommend altering the settings here once you have done appropriate research and feel you have the need for it. The default Windows Firewall settings are more than sufficient to provide adequate defense against unauthorized network activity on your system, when combined with the advice in this chapter, without also impairing normal functionality.

< LOCAL SECURITY POLICY

One of the Administrative Tools provided to further customize Windows security settings is the Local Security Policy tool. This can be accessed by going to the Administrative Tools component of Windows Control Panel, or go to the Start Screen, type *secpol.msc* and press Enter. This tool is only available on the Pro and Enterprise editions of Windows 8, because it is a tool primarily designed to allow Network Administrators to be able to impose certain limitations on the users of a network. Many of the settings are not relevant to the average home PC user, and won't be covered here. Furthermore, some of the useful options have already been covered - namely the Advanced Firewall settings and the User Account Control-related settings - under the relevant sections earlier in this chapter.

For our purposes, the Account Policies and Local Policies categories in Local Security Policy contain several additional settings which are useful in customizing the level of security on your system. To access and change a setting, click on the relevant category in the left pane, then find the setting in the right pane and double-click on it to alter it, or to see a more detailed explanation. Below are a range of useful settings you can alter, but please exercise caution and do not change anything if in doubt. To see the default option for each setting, click the Explain tab.

ACCOUNT POLICIES

Password Policy settings: These settings allow you to force passwords for user accounts to be a certain length, age and complexity. In general you should not alter these settings unless you want tighter security at the expense of convenience, as they will create extra requirements for user account passwords. For example, by enabling the 'Passwords must meet complexity requirements' option, you will force all user passwords to meet the requirements detailed under the Explain tab whenever they change or create a password. This can cause problems with users remembering their own passwords, often forcing them to write these passwords down, which can create a bigger security risk. Importantly, you should not enable the 'Store passwords using reversible encryption' as it makes passwords easy to find since they will not be encrypted.

Account Lockout Policy settings: This group of settings control what happens when a user is locked out of their account for failing to enter a correct password. By default they can't be locked out, but if you wish you can set the number of times a user can try to login and fail before being locked out for a certain duration. This provides tighter security against other users attempting to crack a particular account through repeated login attempts. These settings should only be changed if you are in a less physically secure environment, or suspect someone is constantly trying to guess an account password. Remember that an account lockout can be extremely inconvenient, as the user will not be able to legitimately access their own account until either the lockout period expires, or the Administrator resets the account.

LOCAL POLICIES

Audit Policy settings: These settings allow you to enable a range of options for logging various events, viewable under Event Viewer - see the Event Viewer section of the Performance Measurement & Troubleshooting chapter. For example, you can log the number of successful and failed logon attempts. These are useful for both troubleshooting purposes, and also if you suspect any unauthorized or unusual activity on your system.

User Rights Assignment settings: These settings determine the default user privileges required for a wide range of system tasks, such as creating a Pagefile, changing the system time, or backing up files and directories. These should not be altered unless you have an explicit need, as in every case there is a reason why particular users are allowed to, or restricted from, conducting these tasks - namely to provide a balance between sufficient functionality, security and system integrity.

Security Options settings: These settings are the most useful in customizing Windows security for the average home user. We've already looked at all of the User Account Control-related settings in the User Account Control section earlier in this chapter, so below we look at some of the other useful settings for the average home PC user:

§ *Accounts: Administrator account status:* If Enabled, this option turns on the built-in Administrator account in Windows. This is the unrestricted global Administrator account with the username 'Administrator' which is not obstructed by UAC, and is not the same as the (Protected) Administrator user account you created when first installing Windows. For more details see the Advanced Settings section of the User Accounts chapter.

- *Accounts: Guest account status:* Allows you to enable or disable the Guest account. For security reasons the Guest account should be kept disabled unless explicitly needed - see the User Account Types section of the User Accounts chapter.
- *Interactive Logon: Do not require CTRL+ALT+DEL:* If you disable this option it will require that a user press CTRL+ALT+DEL before being able to logon. This can increase security because it will mean users are entering their password in Secure Desktop mode, where it is much more difficult for malware to interfere or log keystrokes.
- *Shutdown: Clear virtual memory pagefile:* If enabled, this option clears the Pagefile, which is the storage location for Virtual Memory, each and every time you shut down the PC. While this can increase security, since the Pagefile may contain fragments of private information from the latest sessions, it also slows down shutdown time and is generally not recommended unless you require a high level of security, such as on a publicly accessible machine. See the Windows Memory Management section of the Memory Optimization chapter.

As noted, be very careful in what you change here, as the defaults are perfectly fine for the average home user, and some of the settings can cause unintended problems if changed. As always, think carefully about the balance of security vs. convenience before enabling or disabling a setting.

< DATA EXECUTION PREVENTION

Data Execution Prevention (DEP) is a Windows security feature that uses software, and where supported, hardware methods to detect programs that try to access and run code from designated non-executable memory areas. In practice DEP protects against malware that has become resident on the system and which then tries to run malicious code from such memory areas. When DEP detects an attempt to launch an executable from a non-executable memory area, it will shut the program down and provide a notification that it has done so.

You can access the DEP settings by going to the System component of the Windows Control Panel and clicking the 'Advanced system settings' link in the left pane, or by going to the Start Screen, typing *systempropertiesadvanced* and pressing Enter. Under the Advanced tab, click the Settings button under the Performance section, and go to the 'Data Execution Prevention' tab.

When 'Turn on DEP for essential Windows programs and services only' is selected, DEP protection is only enabled for programs that choose to work with DEP, along with Windows system files. This is the default and minimum form of DEP protection, and the one I recommend. For greater protection, you can choose to extend DEP to all programs by selecting 'Turn on DEP for all programs and services except those I select' and then if necessary, choose which programs to manually exclude from DEP by using the Add or Remove buttons.

On some systems, hardware-enforced DEP is also enabled and will be indicated at the bottom of the DEP window. Your CPU must support hardware-based DEP for this to be possible, and typically you must also be running Windows 8 64-bit.

DEP is a valuable form of additional protection against malware, and the default setting provides a balance of good security and compatibility. You may wish to try the more secure form of DEP by extending it to all programs. Then if you find certain programs not functioning correctly with DEP enabled, and you are absolutely certain they are not infected with malware, you can add them to the exceptions list in the DEP window.

If for some reason you wish to completely disable DEP, such as to temporarily troubleshoot a problem to see if it is DEP-related, you can force DEP off in your boot options by using the BCDEdit command as follows:

1. Open an Administrator Command Prompt.
2. Type the following and press Enter:

```
bcdedit /set {current} nx AlwaysOff
```

3. You should see a confirmation that the operation was successful.
4. Reboot your system to implement the change.

Alternatively, you can use the EasyBCD utility to configure DEP or turn it off - see the EasyBCD section of the Boot Configuration chapter for more details. You can also adjust DEP using the EMET utility as discussed in the SEHOP section further below.

It is strongly recommended that you do not permanently disable DEP.

< ADDRESS SPACE LOAD RANDOMIZATION

Address Space Load Randomization (ASLR) is an important built-in security feature, and is covered here for the sake of informing you of its role. First introduced in Windows Vista, ASLR essentially randomizes the location in which a Windows system program sits in memory each time it is loaded up.

ASLR is normally enabled only for core Windows programs, however third party developers can also take advantage of ASLR to randomize the location of their key program files. The end result is that due to this randomization, it is much more difficult for malware to find the correct location to exploit a system interface for accessing Windows features and data on your system. This security feature was enhanced in Windows 7, and has been improved again in Windows 8, with a wider range of random load locations, as well as increased randomization. ASLR is also further enhanced on 64-bit systems. It is always enabled, defeating some malware and slowing or crippling the functionality of others, while having no discernible performance impact on the system.

You can adjust ASLR using the EMET utility as discussed in the next section.

< STRUCTURED EXCEPTION HANDLING OVERWRITE PROTECTION

Structured Exception Handling Overwrite Protection (SEHOP) is a feature first introduced in Windows Vista SP1, and similar to ASLR, is designed to protect applications from being exposed to memory-based exploits. However similar to DEP, by default this feature is only enabled for programs which choose to use it. This is because it can cause potential incompatibilities with software that is based on Cygwin, Armadillo, or Skype.

SEHOP is now also automatically enabled in Internet Explorer under Windows 8 to provide additional protection.

EMET

To configure SEHOP in a more comprehensive manner, you can use the free Microsoft Enhanced Mitigation Experience Toolkit (EMET) utility. Download and install EMET, and note that the utility requires .NET Framework 2.0 to install and function. Although Windows 8 already has .NET Framework 4.5 built-in, if prompted to install .NET Framework 2.0, click Yes, then download and install .NET Framework 3.5, as it contains backward compatibility for .NET 2.0.

Once installed, launch EMET and you will see a graphical interface which shows your current System Status with regards to not only SEHOP, but also the DEP and ASLR features discussed earlier in this chapter. By clicking the 'Configure System' button you can adjust the settings for DEP, SEHOP and ASLR as follows:

§ DEP - You can turn off DEP by selecting Disabled, or forcibly turn it on for all programs by selecting 'Always On'. You can select 'Application Opt In' which is the default and optimal choice, so that aside from core Windows files, only applications which choose to run DEP can do so. Alternatively, you can select 'Application Opt Out', which means applications must explicitly opt out of using DEP otherwise it will be enforced on them. See the Data Execution Prevention section earlier in this chapter for details.
§ SEHOP - You can turn off SEHOP completely by selecting Disabled, which is not recommended. You can forcibly turn on SEHOP for all programs by selecting 'Always On', but this may cause compatibility issues with some programs. The default and optimal choice is 'Application Opt In', which means that aside from core Windows files, only applications which choose to run with SEHOP will do so. Or you can select 'Application Opt Out', which means applications must explicitly opt out of using SEHOP otherwise it will be enforced on them, once again raising the potential for compatibility issues.
§ ASLR - You can switch off ASLR by selecting Disabled, which is not recommended given the significant security benefits it provides. The default of 'Application Opt In' is optimal in allowing core Windows files and only those programs which work with ASLR to use it. See the Address Space Load Randomization section earlier in this chapter for details.

In practice, given all three of these security features are already configured optimally by default in Windows 8, there is no need to use EMET to adjust them, unless you either wish to boost your security at the expense of potential compatibility issues, or you are troubleshooting an issue and want to temporarily disable a feature to see if it is a possible cause.

< SAFE UNLINKING

Safe Unlinking is a security feature that is enabled by default, and is not designed to be customized by the user. Once again it is designed to prevent memory-based exploits, by running a series of checks during memory allocation. This does not provide foolproof protection, but it can defeat a range of common exploits used by malware, and should be taken into consideration as part of a suite of security features and techniques used to prevent malware from causing harm to your system in Windows 8.

< KERNEL PATCH PROTECTION

Kernel Patch Protection, also known as PatchGuard, is a feature unique to 64-bit versions of Windows. This feature protects the system Kernel - the core of the operating system - such that only Microsoft-certified changes can directly be made to memory locations holding the Kernel. This provides excellent protection against malware or legitimate software making unauthorized changes to the Kernel which can destabilize or compromise Windows.

You cannot disable PatchGuard, however you can manually override one of its key components: the check for digitally signed drivers during Windows bootup. Methods to temporarily disable this check are covered under the Driver Signature section of the Windows Drivers chapter.

< SECURE BOOT

A hardware-based feature new to Windows 8, Secure Boot only works on PCs with UEFI. It is designed to ensure that the system remains secure against boot loader malware (such as a Bootkit), which can bypass Windows security by silently gaining control of the system before Windows even has a chance to load. Secure Boot, which is enabled by default on PCs and devices certified for Windows 8, does not allow any unauthorized boot loaders to run. Only loaders which are verified by the UEFI as being authorized with a

proper security signature, checked against an internal firmware database of allowed signatures, will be able to boot at startup.

Secure Boot provides much greater security, but it can also cause problems, particularly in multi-boot environments with operating systems that do not support UEFI and/or are not signed. For example, if you connect a drive which contains an existing copy of Windows XP originally installed on a non-UEFI system, it may not be allowed to run. Similarly, non-commercial yet legitimate distributions of Linux which are not signed may not be allowed to boot with Secure Boot enabled. The only way that the UEFI can tell if an OS boot loader is legitimate is if it has a valid embedded certificate; you cannot force the firmware to boot any unrecognized OS boot loaders in any other way when Secure Boot is enabled.

For this reason, the ability to disable Secure Boot is available in the UEFI options of most PCs, though it is not possible to disable it on some devices. One workaround is to run the other operating system in a virtualized environment within Windows 8.

Secure Boot is actually a function of UEFI, and not Windows 8. As such, the ability to enable or disable Secure Boot, or to add new certificates, will ultimately come down to decisions made by different hardware manufacturers. If you require full control over this feature, you must research this aspect of any system or device prior to purchasing it, to determine if it can be disabled in the UEFI. For most Windows 8 users, Secure Boot should be enabled to provide enhanced system security from the moment you bootup your PC or device.

< ENCRYPTING FILE SYSTEM

The Encrypting File System (EFS) is a built-in file encryption protection method for Windows. It allows you to encrypt a file or folder such that it cannot be opened by anyone else unless they have the appropriate encryption key. To encrypt an entire drive, see the BitLocker Drive Encryption section further below.

To enable EFS encryption on a particular file or folder, follow these steps:

1. Open File Explorer and go to the file or folder you wish to encrypt.
2. Right-click on it and select Properties, and under the General tab click the Advanced button.
3. Tick the 'Encrypt contents to secure data' box and click OK, then click Apply.
4. You will be prompted firstly whether you want to apply the encryption to the file itself, or to its parent folder. It is best to encrypt an entire folder, so if necessary move all the files you wish to encrypt to a new folder and encrypt both the files and folders; otherwise just encrypt the file if you don't wish to move it.
5. The file will be shown in green text by default in Explorer to indicate that it is encrypted. You can alter whether Windows shows encrypted files in a different color under Folder Options - see the Folder Options section of the File Explorer chapter.
6. You can remove encryption for your own files at any time by following the steps above and unticking the 'Encrypt contents to secure data' box instead, then clicking OK and Apply.

Now whenever you aren't using the file, it will automatically be encrypted, and thus its contents are secure against unauthorized access.

Full EFS functionality is only supported on Windows 8 Pro and Enterprise editions. On the regular edition of Windows 8 you can modify or copy encrypted files, but only if you have the encryption key for the file or folder. You can also decrypt an encrypted file, again only if you already have the encryption key, and only through the use of the `Cipher` command; type `Cipher /?` in a Command Prompt to see more details.

BACKUP ENCRYPTION KEY

Once you encrypt a file, Windows will prompt you to back up your encryption key, as this is the only way in which you can decrypt the file if you move the file to another system, upgrade Windows, or your current Windows installation becomes corrupted for example. Losing your encryption key can effectively make your encrypted files inaccessible in the future, so this is an important step you should not ignore. Back up the key to a secure location as soon as possible by clicking the relevant prompt in the Notification Area. If you choose not to do so, you will be prompted to back up the key each and every time you log on, until you either choose to permanently ignore the request, or actually back up your key.

To view details of the encryption, or allow other users to use the file/folder, or to backup the encryption key for this file/folder, follow Steps 1 - 2 further above, then click the Details button.

To access the EFS Key Wizard which makes the process of managing and backing up an EFS encryption key much easier, go to the Start Screen, type *rekeywiz* and press Enter, then follow the prompts.

You can also view your EFS certificate in the following manner:

1. Go to the Start Screen, type *certmgr.msc* and press Enter.
2. In the left pane, go to Personal>Certificates.
3. Your EFS certificate should be listed in the right pane. Check the Intended Purposes column to ensure it has 'Encrypted File System' listed for that certificate.
4. You can right-click on the certificate and select All Tasks>Export to trigger the EFS Key Wizard.

Note that if you lose your user account password, and it has to be reset by the Administrator, you may lose automatic access to all of your encrypted files and folders.

EFS encryption is not a foolproof security method. If someone gains access to your user account for example, they can then access all encrypted material normally, so it is only one extra layer of protection. You can combine EFS file or folder encryption with BitLocker whole-of-drive encryption to provide even greater security from unauthorized access.

< BITLOCKER DRIVE ENCRYPTION

BitLocker is a whole-of-drive encryption feature first introduced in Windows Vista as part of the Ultimate Extras for Windows Vista Ultimate. It is now a standard feature of Windows 8 Pro and Enterprise. As of Windows 7, BitLocker's functionality was extended by allowing removable drives to be encrypted, now referred to as BitLocker To Go.

The changes to BitLocker in Windows 8 are detailed in this Microsoft Article, and include the choice of Used Disk Space Only or Full Volume encryption. The Used Disk Space Only method allows for much quicker encryption of a full drive, as it doesn't encrypt free space areas, while Full Volume encryption is the traditional encryption method used in previous versions of BitLocker, encrypting the entire drive.

BitLocker Drive Encryption technology is designed to secure a drive (or logical drive) against unauthorized access, as opposed to the Encrypting File System which is designed for specific files and folders, and only works on a per-user basis. BitLocker can be used in conjunction with EFS, so the two are not mutually exclusive. To access BitLocker, go to the BitLocker Drive Encryption component of the Windows Control Panel, or go to the Start Screen, type *bitlocker,* select Settings and press Enter. Only an Administrator can enable BitLocker on a drive; it is not a per-user feature like EFS.

On the main BitLocker window you can select to turn on BitLocker for any of your detected drives. If you have a removable drive, such as a USB flash drive or hard drive, insert it and it will also be displayed here,

and the option to enable BitLocker will be provided. You can also enable BitLocker on any drive by opening File Explorer, going to the Computer category, right-clicking on the relevant drive and selecting 'Turn on BitLocker'.

Importantly, for BitLocker Drive Encryption to work on system drives, you must have at least two NTFS partitions. One of these is your normal Windows 8 partition which is to be encrypted, and the other is a smaller partition designed to hold your boot files in unencrypted format so that the system can start normally. This is one of the reasons why by default Windows 8 creates a System Reserved Partition during installation, as covered under the Installing Windows section of the Windows Installation chapter. This System Reserved Partition is not essential, even if you wish to use BitLocker, because BitLocker will create a separate partition for its purposes when you begin the encryption process. Ideally, if you know that you are going to use BitLocker when installing Windows, you should simply let Windows create the System Reserved Partition during Windows installation. You can ensure that this happens by deleting any existing partitions, then partitioning and formatting your drive within Windows Setup.

The other key requirement for BitLocker is a BIOS/UEFI which is compatible with the Trusted Platform Module (TPM) standard, version 1.2 or newer. To check for TPM hardware compatibility, open the BitLocker component of the Windows Control Panel and at the bottom of the left side click the 'TPM Administration' link. If your system does not have hardware TPM support, then you will need to use a dedicated USB flash drive to hold the BitLocker startup key required whenever you start your PC.

Once your drive has been encrypted, BitLocker protection on a drive can be (re)configured by going to the BitLocker component of the Windows Control Panel and clicking the 'Manage BitLocker' link for a drive, or by right-clicking on that drive in File Explorer and selecting 'Manage BitLocker'. For the sake of convenience, you can choose to have a drive automatically unlock on a particular computer, which saves having to enter a password each time you use it. However, this obviously makes the drive less secure, so it is recommended that you only do this if you have a password-protected user account and the PC or device is not in a location that would leave it open to theft.

You can use a BitLocker protected drive on an old version of Windows, such as Windows XP, however you need to use the BitLocker To Go Reader. This application is stored as *bitlockertogo.exe* in the root directory of your BitLocker encrypted drive, and you will either be prompted to install it, or need to run it manually, before you can access your drive on another system. Importantly, a BitLocker encrypted removable drive must be formatted using the FAT file system for it to be able to be used on Vista or XP.

BitLocker is aimed primarily at providing protection in an environment where the PC or device is not physically secure from unauthorized access. A BitLocker encrypted removable drive is particularly useful if you store sensitive data on a USB drive which you carry around with you for example, or you can encrypt a laptop drive with BitLocker to protect against unauthorized access in the event of accidental loss or theft. For the average home desktop PC user, I do not believe it is necessary to enable BitLocker. Protecting individual files and folders using EFS encryption should be sufficient if you just wish to prevent other users on your system from examining their contents. Only if your PC is in a location where it is physically accessible or susceptible to theft by untrusted people should you consider also using BitLocker for added protection.

The use of BitLocker will result in the degradation of performance. It is best used only on drives where security outweighs performance considerations, such as on portable devices like laptops which can easily be stolen.

If your version of Windows 8 doesn't allow you to access BitLocker, then you might consider using TrueCrypt, which is a free utility with similar features.

< ADDITIONAL SECURITY SOFTWARE

Having examined the major Windows security features, it should be obvious that these features are constantly evolving and improving. As of Windows 8, the built-in security features, especially the enhanced Windows Defender, and Windows SmartScreen, are sufficient to protect you against most types of malware and intrusions. However these features do not pretend to protect you against every possible form of security breach, especially since - as we will discuss at length in the Important Security Tips section later in this chapter - the most critical form of protection is knowledge and vigilance.

Some people will require more protection, either due to the fact that they regularly undertake very risky behavior on their system, such as downloading pirated software or modified drivers, or frequently trying out new software of dubious repute. Or it may simply be because they store highly sensitive material, such as extremely valuable commercial-in-confidence data, on their system and can't afford to take even the slightest chance. In such cases, it may be desirable to have additional layers of different types of protection so that even if several defenses are defeated, other layers exist to prevent or detect the malware before it does any serious harm. That's where the use of selected third party anti-malware software may warrant the potential problems that they bring with them.

This section provides a small selection of different types of anti-malware software you can use instead of Windows Defender. Some of this software is not free, and I have not found any conclusive way to determine which is any better than the rest. Aside from varying opinions from security experts, popular anti-malware comparison tests are entirely synthetic, and typically place a heavy emphasis on security at the expense of performance, stability or convenience. The bottom line is that there is no automated solution to the problem of malware, otherwise it would have been largely defeated by now.

ANTI-MALWARE PACKAGES

There are several reputable anti-malware packages which are compatible with Windows 8. Note that these packages are often referred to as anti-virus products, when in fact they scan for a wide range of malware, hence my use of the more general term "anti-malware ". Only some of them are free, and in most cases, only for a trial period.

It bears repeating that the prominent free anti-malware package, Microsoft Security Essentials (MSE), is already built into Windows 8 as Windows Defender, and can't be installed separately. If you want a portable stand-alone version of MSE, the free Malicious Software Removal Tool is ideal, as it is lightweight, scans for the most prevalent forms of malware, and is also released every month through Windows Update as part of Microsoft's monthly security patch cycle.

For a comprehensive anti-malware package, look to the following suites:

AVG
McAfee
Nortons
Avast
Kaspersky
NOD32
Trend Micro
Emsisoft Anti-Malware

PHISHING PROTECTION

Phishing is a form of deception that does not necessarily rely on any malicious software. Simply by tricking unsuspecting users into entering personal information into fake websites and falsified login screens, the originators of this form of online fraud obtain exactly the information they need to steal your money or your personal information without having to go through any of the defenses built into Windows. Phishing is the age-old method of conning people taken to a new level through the use of technology. The main method for combating phishing is user vigilance. Fortunately there is some assistance, as the most popular Internet browsers - Internet Explorer, Firefox, Chrome and Opera - all have some form of phishing protection built into them, detecting reported phishing sites, and warning users of the potential dangers of visiting them.

In Internet Explorer the Phishing Filter is enabled by default and will warn you if it suspects that a site you are about to visit is fraudulent. I do not recommend disabling it - see the Internet Explorer chapter for more details. The Phishing Protection feature in Firefox is covered in more detail in the Firefox Tweak Guide, and once again it is strongly recommended that you do not disable this functionality. Chrome's Safe Browsing features are detailed in Chrome Help, and protect against phishing and malware, thus should be kept enabled. More details of Opera's Fraud Protection features are in this Opera FAQ and is best kept enabled.

Even the most advanced user can fall prey to phishing, either due to laziness, or simply because some fraudulent sites and techniques can appear so authentic, they can fool almost anyone. For various ways to prevent falling victim to phishing and malware see the Important Security Tips section at the end of this chapter.

FIREWALLS

The built-in Windows Firewall is completely sufficient in protecting against network intrusion. By default it prevents external intruders from accessing your system, as long as you do not manually open lots of Ports and/or have lots of program Exceptions. It can also be configured further if required, but this functionality is best suited to more advanced users. In short the Windows Firewall provides a good balance of security and convenience, while still providing full customization options for advanced purposes should they be needed.

However you do have other options if you want even more security or customization potential. There are several commercial firewall packages you can turn to. Two free alternatives, ZoneAlarm and Comodo, provide firewalls for those who want to use a third party package. Your network device, such as a router or modem, may also come with a hardware firewall which you can configure - see your manufacturer's site or your product's packaging for documentation. A combination of a software firewall like Windows Firewall, and the hardware firewall capabilities of most networking hardware, is totally sufficient to prevent the majority of unauthorized intrusions into your system, without also crippling normal functionality.

< IMPORTANT SECURITY TIPS

All of Windows 8's built-in security features, and all the malware scanners and phishing protection in the world, are no substitute for learning how to identify and prevent a security breach. Prevention is indeed much better than the cure in the case of security, because once your system is infected, or once your online account(s) have been breached, and once your credit card details, login passwords, software serial numbers, personal documents and so forth have been compromised or lost, then it is usually too late. At times a malware infection may quietly spread to your backups as well, rendering them useless, so a simple reformat and reinstall of Windows may not rid you of the malware. Furthermore, certain malware and exploits are so new that no malware scanner or known method can successfully detect or block them, at least for a period of time. Finally, anti-malware packages frequently throw up false positives, flagging harmless software as potentially harmful. This can wind up desensitizing some users to such warnings, to the point where a person may still run a harmful package under the notion that it has been falsely flagged.

So it is imperative that you learn various techniques for preventing the entry of malware into your system, detecting their possible presence, and seeing through all the various forms of online scams. The tips I provide below are lengthy, but can be just as valuable as any anti-malware feature or software. This advice has stood me in good stead for many years, steering me clear of malware infection and the loss of personal data or money, while at the same time allowing me to enjoy all the features of my PC, and full use of the Internet, without impeding my system performance or general convenience in any way.

SECURE PASSWORDS

A strong password is the first layer of defense against unauthorized access to an account. It is important to understand however that it is not the only way in which your account can be compromised, and hence even the strongest possible password is not necessarily going to make you completely secure. But as a starting point, you will need a secure password. To understand how to make a password secure, you must understand the basic ways in which passwords can be cracked:

- The simplest method to crack a password is to guess it. This is reasonably straightforward for anyone to attempt, but is actually much harder than it sounds. What will make it easier is if the password box indicates the number of characters in the password, provides a hint, or if the person guessing knows the account holder's password for another account, and hence can try variations of it.
- The next method is a Dictionary Attack. This involves using a program to run through all the words found in a dictionary, perhaps with some commonly used names or phrases as well, and sometimes with common numbers at the end of the words (e.g. jesus1 or lion88).
- Another method is a Brute Force Attack. This method depends on pure computational power to try every valid variation of code to crack an encrypted password. The lengthier the password, and the more complex the encryption, the longer such an attack will take, and the more computational power is required.
- Yet another method is to use Rainbow Tables. These pre-computed tables speed up the process of cracking a password. The only real defense against this form of attack is out of the user's hands, as it depends on whether the encrypted password is Salted by the people maintaining the database which stores the password.

From the four basic methods above, we can come up with some simple rules as to how to create a secure password:

1. Make the password as random as possible, avoiding the use of common words, phrases, or names. This provides the best defense against the password being guessed or dictionary attacked.
2. Make the password as long as you possibly can. Eight characters is the bare minimum, but 12 or 16 characters is much better, and much harder to crack. This provides the best defense against brute force attacks.
3. Do not use the same password, or slight variations of it, for various accounts. This provides the best defense if your password is obtained in one location, such as via an insecure database. Try to have a unique password for every major account, so that one breach in the weakest location doesn't compromise all of your accounts.
4. Try to periodically change your passwords, but not simply by adding a number to the end of them, then incrementing it by 1 every once in a while.

Most people will agree that the advice above is intuitively sound, and you have probably seen variations of this advice around the Internet. The biggest problem is how to implement this advice in a practical manner. For example, security experts may suggest that you create lengthy, random passwords and frequently change them. But such passwords are next to impossible for the average person to remember, so they will inevitably either write the password down and keep it near their PC or device, or choose something that's easy to remember and then vary it only slightly each time. In both cases, this defeats much of the purpose of having a secure password.

I provide some better alternatives which you can try. To start with, if you want to create a genuinely random and long password, you can use this online Password Generator, or the random password generator in the Keepass Password Safe utility - see the Backing Up & Restoring Passwords section of the Backup & Recovery chapter. Try to make the password at least 12 characters long, preferably longer. Once you have generated a range of these passwords for different purposes, you can store them securely in the Keepass utility, and secure it by using a single complex but easy-to-remember Master Password, as covered below. Keep in mind that your browser also has the facility to remember store and automatically fill in passwords, though once again, it is recommended that a very strong Master Password be used to secure the browser's password repository.

To generate a complex, but relatively easy-to-remember password, you can make up a "manipulation rule" to apply to any common word, phrase or name. I'll provide an example of one such rule:

1. Start with a common phrase. For this example, I will use *cheesepizza*.
2. Reverse the phrase. So in this case, it now becomes *azzipeseehc*.
3. Insert a pair of numbers, such as your birth year, or graduation year, in the approximate middle. In this example I'll insert 71 in between azzip and eseehc, the result being *azzip71eseehc*.
4. For increased complexity, add a symbol to the start or the end, such as an exclamation mark, comma or period. In this example, I'll add a period at the start, so the result is *.azzip71eseehc*.

As you can see, through four simple repeatable rules, we've transformed *cheesepizza* into *.azzip71eseehc*, which is a fairly complex 14 character password. It is impossible to guess, quite secure against a dictionary attack, and because of its length, is also reasonably secure against all but the most determined and knowledgeable brute force attacker. The chances that anyone will be able to put together your starting phrase, the full manipulation rule, the pair of numbers you use, and the symbol and location of that symbol are extremely slim.

As long as you remember the original phrase and memorize (or write down) the rule involved, you can usually reproduce it when necessary. To make it even easier to remember, use a memorable common word or name, such as the name of the website on which the password is to be entered, and manipulate it using your unique rule so that it still winds up being fairly complex. For example, the site name TweakGuides turns into *.sediug71kaewt* using the method above.

You can come up with any sort of manipulation rule for generating a password. For example, you might take the first two letters of the first line of the chorus of your favorite song. Let's use "We Are The Champions" by Queen: *We are the champions, my friend*. This results in *wearthchmyfr*. Already a reasonably complex 12 character password, but you can add a number and symbol to the start or end to really make it unique, e.g. by adding an exclamation mark and the number 7 to the start: *!7wearthchmyfr*. There is no way anyone will ever guess that, no chance of a dictionary attack working, and once again, it is safe from all but the most sophisticated and determined hackers due to its length. Yet it is still possible for you to remember, as long as you keep in mind the starting name, phrase, song or whatever, along with the manipulation rule you have created for yourself.

Ultimately, a secure password is only a starting point. It will definitely help protect your various accounts from being hacked, but is not a foolproof defense. As we will see shortly, there are other, much easier methods of bypassing even the strongest password ever created.

ACCOUNT RECOVERY

It is quite common for people to forget their passwords, particularly given the proliferation of online accounts that are becoming necessary for individuals to maintain. This is exacerbated by the fact that security experts will encourage (or force) people to frequently change passwords, and use different passwords for each account. Using a secure password repository, such as the one in the Keepass utility, or your browser's password storage facility, as covered in the section above, is one solution to this dilemma. But since these methods rely on using a strong Master Password to keep the repository secure, this means that there is still at least one password which you will need to remember. The temptation is to write it down, and this is one possibility which I will discuss further in the Physical Access section further below.

In addition to the possibility of forgetting your password, there is also the potential for your account to be hijacked by a hacker, and thus the need for you to reset the password so you can regain control of your account.

To address both instances, whether because the account owner has legitimately forgotten their password, or because the account has been hijacked, most online account providers will provide an account recovery mechanism. For example, if you forget the password for your Microsoft Account in Windows, then you will have to go through an online account recovery process, such as the one in Hotmail. This is typically an automated process, which prompts you with previously determined account recovery questions, such as "Mother's birthplace", or sending the account recovery details to a set phone number or alternate email address. Once the account recovery details are received, they can be used to reset the password to the account, and this in turn allows you to enter a new password and log into the account using it.

It should be immediately apparent that this account recovery process is incredibly risky. It is frequently used as a backdoor method of gaining unauthorized access to an account, because most people do not pay sufficient heed to securing this channel of access, and instead use very simple recovery options. For example, if indeed your account recovery question is "Mother's birthplace", or some other simple question, then there's no question that with sufficient tries, it can eventually be guessed, even by a total stranger. Therefore, regardless of just how complex and secure your password is, it can be bypassed in a moment by someone with little expertise, just by entering the correct answer to your account recovery question.

Some online accounts have now strengthened this channel of entry by using what is known as Two-Factor Authentication. This greatly reduces the possibility of unauthorized entry via account recovery, as it requires two separate types of authentication, such as a security question combined with a code sent to a predetermined phone number. The chances of an attacker having access to both methods at once is extremely slim.

In any case, it is of vital importance that you secure your account recovery process for every online account that you hold, especially your Windows 8 Microsoft Account, if you use one. The following tips are designed to help you determine how to do this:

- Make sure you set up at least two different account recovery methods. If two-factor authentication is available, such as gmail's 2-step verification, then enable it.
- It is strongly recommended that your primary account recovery method be a phone number to which a code can be sent. Ideally, this should be a land-line (fixed home) phone number, as mobile phones can be stolen. If you are renting, and expect to move relatively frequently, then it is risky to specify a land-line number, as you may forget to change it in the future. In that case, use a mobile number, but be certain to keep the phone secure, and change the number as soon as possible if the phone is stolen.
- If you use a security question, make absolutely certain that the answer can never be guessed by anyone, no matter how many times they try. Names of pets, mother's birthplaces, grandfather's occupations, favorite colors or numbers etc. are quite simple to guess, especially for people who know you, and thus completely insecure. Even if someone has no clue as to who you are, through a simple process of

elimination, they can eventually guess the answer to these (E.g. for mother's birthplace, they can enter every major country or city, and eventually hit upon the right answer). If the option is provided, create your own security question, a question to which only you will ever know the answer, and which cannot be randomly guessed. A better method is to choose one of the simple questions, such as "Mother's birthplace", then use the manipulation rule we discussed in the password section above to create a seemingly random answer. For example, if your mother is born in Sydney, using my earlier manipulation rule, you would wind up with *.yen71dys* as the answer to the security question. This is completely unguessable unless the person guessing knows both the original answer and your manipulation rule, and indeed is even aware that the answer has undergone any manipulation.

§ If using an alternate email for account recovery, make absolutely certain that each and every account linked in this way is secured using the advice above. For example, you may have an important online account which is completely secure both in terms of password, and recovery options. But if one of those recovery options includes sending a password reset email to a less secured email account, then a hacker can simply get into the less secure account, reset your secure account's password that way, and gain access. In other words, don't just create a weakly secured "disposable account" for the purpose of being an alternate email address for account recovery.

§ In some cases, certain aspects of the security of the account recovery process is out of the user's hands. Account recovery policies vary depending on the provider. At the time of writing for example, Microsoft still does not have 2-factor authentication available for their accounts. A recent example of a high-profile hacking involving Amazon.com and Apple's relatively lax account recovery procedures is demonstrated in this article. This means you should be extremely careful as to which accounts you link together, and how much information you enter in such accounts. Hackers will typically enter via the weakest link in the account recovery chain.

The main point is that account recovery is an extremely dangerous, yet frequently overlooked, method for hackers to get into online accounts. By virtue of the fact that most users are not technically competent, and don't want to jump through too many hoops to regain access, many account recovery processes have far too much leeway for abuse in order to maintain ease of use. As long as you follow the tips above to secure your account recovery process for each and every online account you have, then you should be relatively safe from this method of attack.

PHYSICAL ACCESS

Another method for a hacker to get into your online accounts, or the files stored on your system, is by gaining physical access to your home, or to the PC or device. Burglars frequently target electronic equipment during break-ins, and portable electronic devices such as phones, tablets and laptops are also susceptible to being grabbed out of purses, taken out of motor vehicles, or stolen while unattended at virtually any other location. Furthermore, you may have family members, friends or visitors who seize the opportunity to browse through your PC or device, or install undesirable software onto it. This can bypass any password or account recovery security you set up.

Let's look at one example. Someone gains access to your PC, and unbeknownst to you, they install Keylogging software from a small USB flash drive that they're carrying. This software will now record all of the keystrokes you make on your keyboard, including the text of any emails you write, and any usernames and passwords you enter, along with other details. If this information gets back to the person who installed the keylogger, they can use it to access most of your accounts, depending on whether the accounts have additional security checks. This method may also be detected by a malware scanner, but it may be too late to prevent an account hijacking.

Another example would be if you write down one or more of your passwords, and you have a roommate or partner who finds this password list and logs in using your machine. This method is virtually undetectable, unless you suspect it is occurring and start looking at various system logs to see unusual login times.

As covered under the Backup & Recovery chapter, there are even hacking tools available that are specifically designed to crack locally stored passwords. So given physical access, enough time, and the right tools, a hacker could crack your user account password and login to your machine.

There are of course many other scenarios where people can log in to or steal your PC or device and access sensitive photos or documents on it, or use the information to log in to your online accounts and cause all sorts of mayhem. To prevent this, read the following tips to secure your PC or device against unauthorized physical access:

§ It is vital that you restrict physical access to your PC or device to only those people whom you completely trust.
§ If you must let someone who you do not completely trust use the machine, let them only use the Guest Account as covered under the User Accounts chapter, and supervise them as much as possible.
§ If you live in a high-crime area, or must share your system with untrusted users, or you have a portable Windows 8 device, then aside from having a user account with a strong password, you should individually encrypt sensitive files, and also use BitLocker drive encryption to encrypt the entire drive - see the Encrypting File System and BitLocker Drive Encryption sections earlier in this chapter. This means that if the PC or device is stolen, the data stored on it will be securely encrypted and extremely difficult to access without the appropriate password.
§ If you must keep passwords written down in any form, store them in a lockable drawer and carry the key with you, or store the passwords in a safe and memorize the combination. It is recommended instead that you store your passwords in digitally encrypted form, such as through the use of the Keepass Password Safe utility.

It isn't necessary to be extremely paranoid about physical access, as in general your friends and relatives should be trustworthy enough without requiring constant suspicion and supervision. However, even when surrounded only by trusted people, it is still best to remove the temptation of an easy opportunity, and hence keep honest people honest.

General Online Tips to Avoid Scams, Spam & Malware

The tips provided thus far should be sufficient to keep your system and your online accounts secure. There is one more avenue of attack which can be used to breach your security, and that is through what is generally called Social Engineering, described in more detail under the Security Threats section at the start of this chapter. Basically, social engineering involves tricking a user into revealing sensitive information or voluntarily providing access to their system. In other words, it is a con, or a scam.

As part of social engineering, people may gain unauthorized access to your system not so much to directly steal from you, but to facilitate the spread of what is known as Spam - unsolicited emails sent out from your machine. The contents of these emails range from annoying but harmless advertising, to deceptive links designed to defraud the receiver of the email, or download malware. Even if your system is not sending out spam, you will undoubtedly receive some in your email account(s) at some point.

To help you understand and protect yourself against these practices, below are a range of general rules. Of course I could write a thousand rules, and still not cover every single type of circumstance. But the rules below do provide a strong basis for warding off the bulk of scams, spam and associated malware.

Social Networking: The rise of social networking sites, such as Facebook, Google+ and Twitter, have made the job of hacking into accounts much easier. This is because people will often unwittingly make a great deal of personal information about themselves available to others via social networking. This information can be used maliciously in various ways, such as hacking into your accounts via the account recovery method discussed earlier, or to undertake Identity Fraud, by setting up a false account and pretending to be you. At the very least you must make sure you go through all of the privacy options in your social networking

account to secure your personal information against access by the general public. More generally, I would recommend against ever entering any sensitive information, such as physical addresses, dates of birth, medical histories, credit card numbers and the like in such accounts.

Once It's on the Internet, It's Out of Your Hands: To go hand-in-hand with the social networking advice above, a general warning regarding putting any personal or sensitive information anywhere on the Internet: once information is stored online, it's out of your hands. There is no way to know precisely how far the information will spread, and it's impossible to destroy every copy of it. Information on the Internet is routinely stored in multiple locations, such as the cached copies held in search engines like Google, copies found on backup servers, and of course people who download the information may make it widely available by other means. The basic rule is that you should never upload anything onto any part of the Internet - and this includes via private email - if you wouldn't want anyone else to see it or know about it. Once any data leaves your machine, it's out of your control.

Address Book/Contacts: If you are infected with malware, or have your email account breached by a spammer, one of the first methods used to redistribute the malware or initiate spam is through the use of your contacts list. This is because an email that comes from a known person is more likely to be opened and the contents read, and any links clicked, than if it came from a stranger. One method of negating this form of attack is to not maintain an address book or contacts list. Instead, save at least one email you have received from people you wish to contact regularly in a separate mail folder. Then whenever you want to email that person, open this folder, search for their name, and reply to their last email, clearing the existing contents and subject line before entering your text. The lack of a consolidated and categorized list of contacts makes it much harder for anyone else who accesses your account to quickly spam all of your contacts, or to work out the relationships between you and various people on the list.

Stay Up to Date: Regularly keep your system up-to-date in terms of Windows patches and security updates, definition files for malware scanners, and the latest versions of your installed programs. These updates often contain fixes for known security exploits and vulnerabilities, and are a simple but effective way to prevent infection. Don't wait until you suspect infection before updating your system, as by then it may be too late, since some malware deliberately blocks the use of certain updating features.

Attachments and Downloads: A common method for spreading malware is through infected email attachments and file downloads. Different file types can hold or trigger malware on your system depending on your settings. Any email attachment or download link should be viewed as a potential source of malware, even if it is from a known source, because even if the sender/host is not deliberately malicious, they could be infected themselves and hence accidentally spreading infected files. Only save attachments or obtain downloads from trusted sources. Keep Windows SmartScreen enabled, as it will immediately warn you, before you can launch a downloaded file, whether it is potentially risky or infected with malware. Also scan the downloaded file using Windows Defender or another anti-malware package.

Patches & Security Updates: In addition to the advice above, if you receive an email with an update or security patch for a software package or Windows, do not use it. Whether attached to the email itself, or linked to in the body of the email, most of these updates or patches are fraudulent. No reputable software company publicly distributes updates or patches via email, they are always hosted on the company's site, or downloaded automatically by the software itself. If you are unsure, use a bookmark or manually type the legitimate company's web address into your browser, and check for any updates or patches on their site.

Unknown Sender: If you receive an email or message from someone you don't know, this is instant cause for suspicion. The vast majority of message from unknown individuals are spam, malicious and/or fraudulent.

Too Good to be True: If you receive a message or see an online offer of any kind which seems too good to be true, then almost without exception, it is likely to be a scam or a form of malware. It may not be malicious, it might simply be a hoax or a chain letter, but in virtually every case, it is worth deleting.

Spelling and Grammar Oddities: A dead giveaway that something is potentially malicious, spam or a scam is the presence of bad spelling and grammar. This is not necessarily due to the author being foreign; the use of misspellings of common words, or symbols and other characters in place of standard letters, is a tactic designed to circumvent certain keywords used by spam filters to block such emails. This is why, for example, the brand name Viagra is spelled V1agra, or ViaGr@, or any number of variations.

Address Check: If a particular email or website appears suspicious, check the address closely. Often times the address of an apparently well-known site can be easily spotted as false if you pay attention. For example, the addresses http://www.amazon.shop.com and http://webstore.us/amazon.com/ have nothing to do with the reputable online store http://www.amazon.com. Similarly, the address http://www.facebook.users.org has no relationship with the social networking site http://www.facebook.com. A domain name is always read from right to left before the first single slash (/) mark. The first component of an address when read from right to left is the Top Level Domain (TLD) found in the main site name, such as .com, .net, .co.uk and so forth. The real site name always appears just after the first incidence of a TLD when read from right to left. So in the example http://www.amazon.shop.com, the amazon portion of the address is just a sub-location of the website Shop.com. Scammers and advertisers are very inventive, and create all sorts of variations on legitimate site names, sometimes with only a letter or two out of place, so in reality the only true way to be completely sure you are going to the correct site is to open a new tab or window in your browser and manually enter a known and trusted site address, or use your bookmarks.

Link Check: Even if a link on a web page or email appears completely legitimate and correct, spoofing links is extremely easy. For example, this link: http://www.google.com/ actually goes to my website www.tweakguides.com when clicked, not Google. The only way to safely tell where a link really goes to, whether it is provided in an email or on a website, is to right-click on the link and select 'Copy shortcut' (or similar), and then paste it somewhere harmless (i.e. not in your browser address bar). For example, you can paste it into the search box of a search engine like Google. Then look closely at the link to (a) see if it matches the original address displayed by the link - if it doesn't this tends to indicate that the link was attempting to be deceptive and hence is untrustworthy; and (b) to see the actual address it links to, which you can research further as discussed under the Address Check tip above. It has become fashionable for people to use short link services to generate URLs which are completely non-descriptive and hence potentially unsafe. For example, this link http://bit.ly/dxdpT should point to www.tweakguides.com, but there is no possible way to determine that using any of the methods above. The only way to check such links is to use a URL expanding service, such as LongURL or KnowURL, which allow you to paste in a short link and see the original link.

Browser Security Check: For any secure transaction, the link which appears in your address bar must contain *https://* at the start, not just *http://* - note the addition of the "s" in the first link, which indicates it is a secure web link. Do not enter any financial information on a site which doesn't start with https://. However the level of security provided by a secure https:// link can vary, so by itself this is not a guarantee that your transaction is completely secure. Your browser will usually give you some indication or warning about the level of security, and this should be combined with research on the site in question.

IP Addresses: Any link starting with a series of numbers instead of a domain name should be viewed with extreme suspicion. For example, http://74.125.45.100/ tells you absolutely nothing about the site; in this case it's actually Google. In most cases an IP address is used instead of a domain name precisely to hide the true nature of the site.

Domain Check: If you believe a particular website may be untrustworthy, you can check to see who owns it and where they are located. A Google search on the site name is a start, but for more details, enter the

domain name in a WHOIS lookup box at a domain registrar, such as the one provided here. In most cases this will provide sufficient details or leads regarding the owner of the domain to help determine whether it is reputable or possibly malicious. Any site where the owner or administrator details are hidden or deliberately obscured, and do not logically correspond with the information on the site itself, tends to significantly reduce its trustworthiness.

Replying or Unsubscribing: There is a large online market for email lists used by spammers and malware distributors. These people place a particularly high value on email addresses where the recipient is known to still check their email, as opposed to a false or long-dead email account. One way they verify an email address is with a phony 'Click here to unsubscribe' or similar link. Clicking such a link will not unsubscribe you, it will simply set you up for more spam in the future. Worse still, some of these links take you to a phishing site, or download malware when clicked. For similar reasons, never reply to any such emails. Spammers know full-well that they cause annoyance, so abusing them is pointless; replying simply lets them know your account is active, increasing the amount of spam you will receive.

Backups: The need for regular backups has been covered in detail in the Backup & Recovery chapter. Malware provides another important aspect to consider: you should always do a full malware scan of your system before creating any backups, and never backup if you suspect you are infected, otherwise you may wind up infecting your backups and rendering them useless.

File Sharing: One of the biggest sources of malware infestation in recent times is file sharing, such as via torrents, usenet, FTP, IRC, or web-based file sharing services. Many shared files are fakes containing malware, but equally, genuine files can also contain malware, especially in any 'key generators' or associated utilities or links allegedly designed to unlock the shared files. Legality aside, file sharing is very risky and one of the easiest ways of being infected with malware. Malware distributors are increasingly innovating in this area due to the surging popularity of file sharing.

Financial Statement Check: If malware perpetrators gain access to your finances, they can sometimes be very cautious not to trigger any preset alarm points. Instead of withdrawing large sums of money which can arouse suspicion on both your part and the bank's, they can instead withdraw smaller irregular sums, or purchase normal goods and services online in an unpredictable, and thus seemingly normal manner. The only way to detect this is if you regularly check your financial statements closely, making sure you can account for every transaction.

Browser Tools: If an untrusted website prompts you to install a particular plugin, program or toolbar to view or download their content, chances are this is malicious, or at the very least unnecessary and undesirable. The first step is to cancel all such installation attempts and do some research. The most common software you require for full Internet multimedia functionality are the Flash Player, SilverLight, ShockWave Player and Java plugins. Only if a completely trusted and reputable website, such as Microsoft.com for example, asks you to install a browser plugin or download manager should you consider accepting, and if you are still in any doubt as to its necessity, once again cancel any installation attempts and research further.

Block Internet Access: If you strongly suspect a malware infection on your system, disable your Internet connection as soon as possible. If necessary update your malware scanner definition files first and run Windows Update before doing this. The quickest and most foolproof way to disable your Internet access is to turn off your router/modem, or unplug your cable or DSL line. The main reasons to do this is (a) to prevent the malware from spreading; (b) to prevent it from sending out any of your personal information to the creator/distributor of the malware; and (c) to prevent any hacker from accessing your system using any newly opened exploits or vulnerabilities. You can then scan your system for malware, and conduct further research on another machine, track down the malware and remove it, and once you're confident your system is malware-free, you can reconnect to the Internet.

Common Sense: The simple application of common sense can provide an excellent method for detecting the validity of many forms of fraud or malware. For example, if you receive an offer from a foreign king to place $18m into your bank account, but he needs your details first, or a nominal fee, then common sense would tell you it is ridiculous and highly risky to follow through on this. Similarly, a beautiful woman you don't know contacts you out of the blue to become friends with you. Or a close friend sends you an odd email with an uncharacteristic request or a suspiciously named attachment. All of these threats can be easily countered with the application of common sense, as none of them remotely pass even a simple sanity check. Yet every year, thousands of people fall victim to these scams. Don't allow your curiosity or base desires to overwhelm your common sense. Exercise some patience and caution, and do some research first. At the same time, you cannot live in a constant state of complete paranoia - there are reputable sites and individuals whom you know you can trust, and cases where a quick rudimentary check is sufficient. Still, the adage *If there is doubt, there is no doubt* rings true: if you have even the slightest bit of suspicion, act on it by conducting further checks; don't take silly risks.

Intimate System Knowledge: One of the many benefits of becoming closely acquainted with your PC and the workings of Windows 8 is that it allows you to spot odd behavior and unusual files and processes which most other users would not see, or dismiss as normal. When properly configured and maintained, contrary to popular belief, Windows does not behave in an unpredictable manner, and your programs will not randomly crash or glitch. Therefore, when strange things do begin to happen, such as unexpected program crashes or changes, your browser behaving in odd ways, the system slowing down at times, or other unusual activity, you can spot it and investigate. Using a range of tools, such as those covered in the Startup Programs and Performance Measurement & Troubleshooting chapters, you can then determine which processes and files are not normal for your system, and hence detect malware which may otherwise elude less knowledgeable users. It takes time and patience to gain such knowledge, but there are many rewards for being familiar with the fundamentals of Windows and PCs.

Research, Research, Research: This is the Golden Rule. You are not the only person in the world using the Internet, thus it is highly likely that you are not the first person to encounter a particular form of malware, fraud or related problem. This means that somewhere, someone is quite likely to have posted about having the same type of problem, or similar symptoms, and furthermore, detailed sources of knowledge may already exist to help you determine the best course of action in an almost limitless range of scenarios. Everything from researching whether a particular website is potentially malicious, or a certain online offer is too good to be true, to the purpose of strange files on your system, to working out if a particular browser plugin is safe and actually necessary for certain functionality - the information is already there, you simply to make use of it. Without fail, I have always found sufficient information to determine virtually anything I need to know simply by using a search engine. Knowledge is power.

BALANCING SECURITY VS. CONVENIENCE

In many ways, the advice in the sections above is just the tip of the iceberg. I've tried to cover the fundamentals, particularly the creation of a secure but easy-to-remember password, establishing a robust account recovery method, and maintaining physical security of your PC or devices. But I cannot even begin to cover all the variations and additional tips required to keep someone secure online in today's world. The information provided is aimed primarily at showing you the underlying logic behind ways of keeping safe.

In reality, nothing is 100% secure. Anything that is built by humans can eventually be bypassed by other humans, if they are determined and knowledgeable enough. If you do find yourself the target of a skilled and persistent hacker, there is little you can do. Even if your own security practices are impeccable, it is still possible that the companies that hold your data will fall victim to security exploits. Some of the biggest companies in the world today, including ironically some security firms, have been hacked in high-profile cases, resulting in the loss of income, as well as commercial and personal data. It's a never-ending battle between hackers and security software developers.

In such an environment, it's important to keep things in perspective. You can't live in a climate of complete paranoia, and place your system and all of your information in total lockdown. Nor is it wise to cripple your system with numerous security software packages and rigorous security procedures. There has to be a balance between security and convenience.

In the past the balancing act between adequate security and convenience tended more towards convenience, since security threats were not as prominent, and even if you caught a virus, it was often just a harmless prank or at worst it ruined a few of your files. Unfortunately, in recent times there has been a significant rise in genuinely malicious software; namely software designed solely to do harm to your system, or compromise your personal information and steal your money. This coincides with the rise in the number of people who are using the Internet to pay bills, do their banking, go online shopping and share personal information.

The stakes are much higher now, so no matter how advanced a user you believe yourself to be, it is important to pay attention to the security of your PC, and it will continue to become even more important in years to come as the malware creators and online fraudsters find increasingly more complex and intrusive ways of getting into your system. They make millions of dollars from undertaking this sort of activity, so they have every incentive to innovate. This is why Windows 8's enhanced security features, such as User Account Control and Windows SmartScreen, which at first appear to be annoying, are actually very necessary, and should not be disabled without careful consideration.

The balancing act between security and convenience has now swung more towards security than purely convenience, so you must make some effort to keep your system secure, even if this can be a bit of a pain at times; it's simply unavoidable. In this chapter I've provided what I believe is a healthy balance, especially for performance-minded users. Rather than simply suggesting the use of multiple malware scanners which can hurt performance, I have recommended a combination of Windows 8's built-in features used in minimalist but effective manner, combined with sensible secure computing practices, to create an excellent layer of defense with no real performance impact. Of course the most important theme throughout this entire chapter has been the need for user education and research, which as I've repeatedly stated, is the only genuine defense against malware and online fraud.

MEMORY OPTIMIZATION

Windows 8 adds some new memory management enhancements. To start with, the Windows Desktop will only load up if launched by the user, saving some memory if you only work in Metro. Furthermore, Metro apps, unless explicitly closed, are designed to remain running in the background (are "suspended") after being minimized. This means they are much quicker to respond when opened again. Should your system run low on physical memory resources, it can be almost wholly reclaimed from suspended Metro apps without needing to shut the apps down. Memory usage by Services has been improved further, with many services now only launched when needed, and terminating once their task is complete. Virtual Memory has also been streamlined to provide efficiencies in terms of sharing paged data and optimizing the general layout of data in Windows.

This chapter looks at the configuration and optimization of memory-related functionality on your system. Although most Windows Memory Management functionality is automated, it is still important to understand the basics of how Windows 8 uses the various forms of memory on your system. Memory-related hardware and software settings have a significant impact on your system's responsiveness and stability, not to mention your data integrity. A system with poorly configured memory-related settings risks slowing down, stuttering, becoming unstable, experiencing errors and sudden reboots, and ultimately corrupts your data.

< MEMORY HARDWARE

The following are the common forms of memory hardware used on modern PCs:

CPU CACHE

The CPU Caches are small fast memory chips that cache (buffer) information for faster usage by the CPU, since the CPU is the central component of your system. They assist in temporarily storing the information in anticipation of reading/writing by the CPU, preventing any bottlenecks or slowdowns. There are usually several levels of CPU caches: Level 1 (L1), Level 2 (L2), Level 3 (L3) and so forth. The cache chips themselves vary in storage capacity depending on your CPU, but essentially they are physical chips that you should not have to worry about. Windows and your associated hardware are designed to automatically detect the size of these caches and use them optimally, as long as you have them enabled in your BIOS/UEFI. That is, if options relating to the use of CPU L1/L2/L3 Cache(s) are present in your BIOS/UEFI, never disable them unless you are troubleshooting. There is a `SecondLevelDataCache` Registry setting found under the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management` key. Some people encourage changing this entry in an attempt to manually adjusting the CPU's L2 Cache. However, as with previous versions of Windows, this setting is not necessary, as the default value of 0 allows Windows 8 to automatically identify and use the correct L2 Cache size. This setting is only for very old CPUs, such as pre-Pentium II models, that use direct-mapped L2 caches.

Since the user has no control over the CPU's caches, aside from ensuring that they are enabled in the BIOS/UEFI, this is one area of the memory subset you should not worry about unless you are troubleshooting a memory-related problem. For example, a CPU with a faulty cache may exhibit strange behavior, such as constantly returning data errors. In such cases you can temporarily disable the caches in the BIOS/UEFI to see if this reduces or resolves errors; if it does then the CPU is likely to have a hardware fault.

PHYSICAL RAM

This is the most well-known, and most important form of memory. RAM (Random Access Memory) is a temporary data storage area, as covered under the Memory section of the Basic PC Terminology chapter. The primary advantage of RAM over other forms of data storage, such as a hard drive, is that it is much, much faster for the system to access data when held in RAM.

There are three key factors affecting RAM performance: RAM size, RAM speed and RAM timings, each covered below:

RAM Size: This is the actual storage capacity of the RAM in Megabytes (MB) or Gigabytes (GB). The primary impact of having more RAM is that, when combined with appropriate Windows Memory Management settings, your system will perform more smoothly. This is because data has to be loaded less often from your drive, as more of it is stored in RAM, making it easier to access rapidly by your CPU and the rest of your system when required. RAM size is important in Windows because of the way it can utilize physical memory to speed up your system. However, various improvements in Windows 8 have reduced the memory requirements for smooth operation such that it can still perform quite well on systems with lower amounts of memory. The formal memory requirement for Windows 8 32-bit is a minimum of 1GB of RAM, and 2GB of RAM for Windows 8 64-bit. If you are into heavy multi-tasking or play complex games, I recommend more than 2GB of RAM to allow smooth performance without stuttering or frequent loading pauses. There are no RAM size tweaks; if you have a low amount of RAM then the best solution is to install more of it in your system if possible - see the Upgrading Memory section at the end of this chapter. Bear in mind that the 32-bit version of Windows 8 cannot efficiently utilize more than 4GB of RAM; only the 64-bit version can do that.

RAM Speed: This is the frequency at which RAM operates (in MHz), much like the speed at which a CPU operates. The higher the RAM's speed, the faster it can undertake the read and write operations it needs to perform. Each stick of RAM has a speed rating, which is the speed up to which a stick of RAM is certified to safely operate. However the actual speed a RAM module is currently running at on a particular system varies depending on how fast it is set to operate in the BIOS/UEFI. It is possible to adjust your BIOS/UEFI such that the RAM can operate at a higher or lower speed. The bottom line is, the faster the RAM's actual speed in MHz, the faster it reads and writes information and the better your performance. But the more the RAM's actual speed surpasses its advertised speed rating, the greater the chance for instability, so ideally you should always keep the RAM at or below its rated speed for maximum stability and data integrity.

RAM Timings: These are composed of several variables, set in your BIOS/UEFI, which determine not the frequency of the RAM module (i.e. the RAM speed), but the Latency of the RAM - that is, the amount of time it waits between updating various signals. For example, the RAS (Row Access Strobe) and CAS (Column Access Strobe) latency settings measure in clock cycles the delay in sending signals which specify firstly the row in which a particular memory cell is located, and then the column. The lower the RAM timings, the less time the RAM rests between these operations, and hence the faster it performs, but the greater the chance for errors and instability. Just like speed ratings, RAM modules come with recommended timings already encoded in their Serial Presence Detect (SPD) on a special chip. These SPD settings are used by default on your system unless manually changed in the BIOS/UEFI, and when used with the recommended RAM speed rating (see above), ensure maximum stability.

To view basic details of your RAM, check the Memory section under the Performance tab of the Task Manager - see the Task Manager section of the Performance Measurement & Troubleshooting chapter. For full details of your RAM, use a utility like CPU-Z and check under its Memory and SPD tabs - see the System Specifications chapter for details. Also see the Overclocking section of the Hardware Management chapter for more details on adjusting RAM speed and/or timings and the impacts this has. If you want to test your RAM for stability, see the Windows Memory Diagnostic section of the Performance Measurement & Troubleshooting chapter.

VIDEO RAM

Video RAM (VRAM) is the physical memory built into a graphics card, and the size of this is usually quoted in MB or GB as part of the graphics card's specifications (e.g. GeForce GTX 680 2GB). This RAM acts as a temporary storage location specifically for holding graphics data for faster access by your graphics card, much the same as system RAM does for general data. For this reason, the VRAM is also called the Frame Buffer, in that it holds (buffers) individual graphics frames, ready to send to your monitor one by one. Just like system RAM, VRAM has a speed in MHz, and latency in clock cycles, with the higher the speed and the lower the latency the better the graphics performance. Unlike system RAM, altering the latency of your VRAM is tricky and not recommended, though still possible. The speed (in MHz) on the other hand can be easily altered up or down using an overclocking utility, with the faster the speed, the higher the overall performance, but once again the greater the chance of graphical glitches and freezes. See the Overclocking section of the Hardware Management chapter for more details.

If you're interested in a plain English step-by-step overview of how the memory features of your system are utilized for a system-intensive task like gaming, read the Graphics Process section of the Gamer's Graphics & Display Settings Guide for details.

< WINDOWS MEMORY MANAGEMENT

Windows 8 builds on the memory management improvements of Windows 7, which in turn was an enhancement of that used in Vista. All three of these operating systems have significantly improved memory management efficiency over Windows XP, and hence require much less tweaking to optimize.

This section examines the general Windows memory management features, which can be summarized as follows:

- Metro memory management, which is designed to keep suspended Metro apps running in the background for greater responsiveness, without hogging memory resources.
- Metro usage allows Windows to avoid loading into memory Windows Desktop components until they are actually needed by the user.
- Service improvements, through greater use of Trigger Start Services which only run when required, and removal of unnecessary services.
- Virtual Memory improvements, including Memory Combining to allow for greater sharing of paged data, along with optimizing the general layout of Windows data structures.
- SuperFetch, which analyzes common usage patterns on a system and attempts to anticipate and preload (cache) key information for quicker access.
- ReadyBoost which uses connected USB flash drive(s) to provide additional memory resources to potentially speed up system access on low memory devices.
- Desktop Windows Manager (DWM) graphics improvements which greatly reduce the memory footprint of Windows.
- Fault Tolerant Heap to resolve many common memory management issues.
- Potentially improved performance on 64-bit systems and those using multi-core CPUs.
- Increased security to maintain data integrity and prevent memory exploits - see the Data Execution Prevention (DEP), Address Space Load Randomization (ASLR), Structured Exception Handling Overwrite Protection (SEHOP) and Safe Unlinking sections of the Security chapter.
- General performance improvements through optimizations in the way the memory management algorithms work to prioritize and allocate memory resources.

Let's look at the most important aspects of Windows 8's Memory Management system in more detail.

MAXIMUM SUPPORTED RAM

There are key differences in the way memory is utilized between the 32-bit and 64-bit versions of Windows 8. This is covered in greater depth under the 32-bit vs. 64-bit section of the Windows Installation chapter, but of relevance here is the fact that under Windows 8 32-bit, a PC can normally only use a maximum of 4GB of RAM - any higher won't be detected or used by default. Furthermore, even with 4GB of RAM, you may only see around 3GB of that available in Windows 8 32-bit, sometimes even less, because some of the memory address space will be reserved by the system for certain hardware requirements, which in turn limits how much system RAM can be used at any time by a particular process. The 4GB memory barrier is a normal limitation of the 32-bit architecture, which is a major reason why the 64-bit architecture was invented, and is fast becoming standard as more people expand beyond 4GB of RAM on their desktop systems.

To allow Windows 8 32-bit to access 4GB or more of RAM, you need to enable a feature called Physical Address Extension (PAE), which can be done by opening an Administrator Command Prompt and typing the following, then pressing Enter:

```
BCDEdit /set PAE ForceEnable
```

Alternatively, you can enable PAE using a utility like EasyBCD. See the Boot Configuration Data section of the Boot Configuration chapter for more details. There are other benefits to enabling PAE, including enabling support for hardware-enabled DEP. See the Data Execution Prevention section of the Security chapter.

Regardless, under the 32-bit platform there is not much to be gained by having more than 4GB of RAM, as it cannot be used efficiently. Any single application or process under a 32-bit environment can't address more than 3GB, so for gaming purposes for example, more than 4GB is effectively a waste. If you currently use, or will eventually require, larger amounts of RAM, then the correct course of action is to install the 64-bit version of Windows 8.

The official physical memory limits for Windows 8 are listed in this Microsoft Article, and are summarized below:

- *Windows 8:* 4GB (32-bit), 128GB (64-bit)
- *Windows 8 Pro:* 4GB (32-bit), 512GB (64-bit)
- *Windows 8 Enterprise:* 4GB (32-bit), 512GB (64-bit)

METRO MEMORY MANAGEMENT

Metro apps are designed for lower memory devices, such as tablets, so their general memory usage is not excessive. You can track the current memory usage for any open Metro app by looking under the Apps section of the Processes tab in Task Manager - see the Task Manager section of the Performance Measurement & Troubleshooting chapter for more details.

Unlike Desktop programs, Metro apps by default will continue to run in the background when they are minimized, such as when switching back to the Start Screen, or opening another Metro app or Desktop program. Unless you explicitly close a Metro app, it will remain resident in memory, marked as Suspended. This means that over the course of a session, you may have a large number of Metro apps open in the background, which can potentially use up a sizeable portion of memory.

In practice however, it is actually more efficient to allow an suspended app to keep its allocated memory. The solution to running out of memory resources, as covered in this Microsoft Article, is that Windows will reclaim memory from apps, but only if your system comes under "memory pressure". That is, if other apps or programs have greater need of the resources, they will be stripped from the suspended background Metro

apps. This is all done automatically, and without the need to completely shut down the suspended apps, unless memory resources become critically low. The benefit of this method is that the next time you access a suspended app, it will reopen where you left it rather than launching afresh, with possibly only a second or two of extra delay, depending on the speed of your drive.

In general, if you know you are not going to access a Metro app again during a session, or at least not for quite a while, it is still best to completely shut down the app rather than allowing it to minimize. The method to fully shut down a Metro app is covered under the Metro section of the Graphics & Sound chapter.

Another positive aspect of Metro is that if you only work within the Metro environment during a session, there is no need for Windows to load up the components associated with the Desktop. It means that unless and until you trigger the Windows Desktop, it will not use any additional resources while you are in Metro. This is typically of greatest benefit on lower memory devices such as tablets, where it is entirely possibly to remain in Metro throughout a session.

SERVICES

Services are customizable programs that run in the background and support specific system-wide functionality. Windows uses a range of services to provide important features in Windows, such as the Windows Update service which allows Windows to periodically check for a range of software updates. There are a large number of services, both those installed by Windows itself, and those installed by third party applications, which can quickly use up a lot of memory resources if left running in the background.

Windows 8 refines memory usage by firstly removing a range of Windows services that were not required. As with Windows 7, many Windows services are now set to Manual in Windows 8, which means they only launch when necessary. Furthermore, a range of services are now Trigger Start Services, which are similar to Manual services, starting up only when actually required, and importantly, terminating after making sure they are no longer needed.

These changes mean that the bulk of service optimization potential in Windows 8 comes from reconfiguring third party services. Services are covered in more detail in the Services chapter.

SUPERFETCH

SuperFetch was introduced in Windows Vista, and used with some modification in Windows 7, and now in Windows 8. It is similar to, but much more efficient and more useful than, the Windows XP prefetching feature. SuperFetch uses an intelligent prioritization scheme which, over time, analyzes your system usage patterns, and places portions of your most commonly used programs into memory in advance. This can make the system feel more responsive, and allows applications to load up more quickly. In effect this turns your otherwise idle RAM into a Windows cache designed to improve speed and responsiveness.

SuperFetch can cause some confusion to users, as it can make Windows appear to be using large amounts of memory for no apparent reason. This is completely false - the concept behind SuperFetch is that if your RAM is sitting idle and unfilled, it is serving absolutely no useful purpose whatsoever; free RAM is wasted RAM. SuperFetch can make productive use of the memory by caching lots of data that it anticipates you will use at some point. At the same time, given the speed of RAM, cached memory can be almost instantly freed up when needed by any other program.

Unfortunately, in Windows Vista the implementation of SuperFetch was somewhat aggressive. Almost immediately after reaching the Windows Desktop, it would begin to rapidly cache large amounts of data from the drive in an attempt to fill as much available free memory as possible. The end result was a lengthy period of noticeable drive churn at the beginning of a user session, and this annoyed many people.

SuperFetch has since been refined and toned down in several important ways. The SuperFetch service is still not set on a delayed start, and hence begins immediately after bootup. However, initially the caching is done at a very leisurely pace and is difficult to detect. After a few minutes, SuperFetch starts to increase the rate at which data is cached. Furthermore, SuperFetch does not automatically try to fill all available RAM in a short space of time; it only caches the most important data based on your usage history, and this often equates to a few hundred MB of cached data to begin with. Part of this reduced caching is also due to the fact that Windows 8 uses less resources by way of background services and desktop memory usage for example, and hence there is less data needed to be cached. Typically, at the normal rate at which SuperFetch caches data, in less than a minute of subdued drive usage the cache is sufficiently full. Over time the cache will then continue to grow very slowly as necessary, usually loading up during idle periods. Windows will try to retain high priority information in the cache as long as possible, but any time your system requires the use of the memory space occupied by the cache, it is almost instantaneously given up as free RAM for system usage, so there is no real drawback to this process.

You can see how much RAM is being used as a cache by SuperFetch at any time by opening Task Manager, and under the Performance tab clicking the Memory item on the left side. Under the Memory category you can see the total amount of RAM installed on your system at the top right, the memory used primarily by SuperFetch under the Cached heading, and the Available memory, which is Cached memory plus Free Memory. See the Task Manager section of the Performance Measurement & Troubleshooting chapter for more details of how to interpret the memory data.

SuperFetch can noticeably improve application launch times, and as such, I strongly recommend against disabling it. It needs time to analyze your usage patterns and prioritize data accordingly, so system performance will continue to improve over time as SuperFetch refines its analysis. Leave SuperFetch enabled for at least two weeks of daily usage before judging its impact.

Importantly, on faster drives which score 6.5 or above in the Primary Hard Disk component of the Windows Experience Index (WEI), Windows automatically disables SuperFetch, as well as boot and application launch prefetching. Typically only faster SSD drives can obtain such a score - see the Windows Experience Index section of the Performance Measurement & Troubleshooting chapter for details. The reason SuperFetch is disabled on SSDs is because on balance they are considered fast enough in terms of their random read performance to make SuperFetch unnecessary. If you have an SSD and want to make sure SuperFetch is disabled, see the information further below on how to manually disable SuperFetch.

Modifying SuperFetch

If you want to customize SuperFetch's behavior you can do so in the following location in the Windows Registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\
Memory Management\PrefetchParameters]

EnablePrefetcher=3
EnableSuperfetch=3
```

These DWORD value can be changed to a value of 0 to disable; 1 to only prefetch application processes; 2 to only prefetch boot files; and 3 for boot and application processes. The default of 3 is recommended and generally should not be changed, but if you wish to experiment, change them both to the desired value, move the existing contents of your *\Windows\Prefetch* folder to a backup location, and see if after a period of several days you prefer the new settings. If not, reset them both to the defaults, delete the existing contents of the Prefetch folder and move back your backed up Prefetch folder contents.

Disabling SuperFetch

If you want to completely disable SuperFetch and prefetching activity in Windows, do the following:

1. Open the Task Manager by going to the Start Screen, typing *task manager* and pressing Enter.
2. Go to the Services tab of Task Manager.
3. Find the SysMain service, which has SuperFetch in its description. Right-click on it and select Stop.
4. Open the Services Utility by going to the Start Screen, typing *services.msc* and pressing Enter.
5. Find the SuperFetch service and set it to Disabled and click Apply.
6. You can also delete the files under the *\Windows\Prefetch* directory.
7. After a reboot SuperFetch will no longer be in use.

Disabling SuperFetch is not recommended for any system unless either Windows automatically disables it for you, or you have an SSD and need to disable it manually. Keep in mind that disabling SuperFetch also disables ReadyBoost.

If you do disable SuperFetch, and then re-enable it again in the future, remember that it will take SuperFetch a while to get back up to speed in analyzing your usage patterns. Importantly, if SuperFetch is active, don't clean out the *\Windows\Prefetch* folder at any time, as this reduces SuperFetch and prefetching performance. Windows maintains the folder automatically by regularly removing lower priority items.

DESKTOP WINDOWS MANAGER

The Desktop Window Manager (DWM) is covered in more detail in the Graphics & Sound chapter, as it relates primarily to graphics functionality in Windows. It is discussed briefly here because one of the major improvements, introduced in Windows 7, is the way in which the DWM was redesigned to reduce the memory utilization of Desktop rendering. In Windows Vista, for every window that was opened on the Desktop, DWM would allocate two copies of the data to memory: one to the system RAM for fast access by the CPU, and the other to the Video RAM for fast access by the graphics card. In later versions of Windows this has been refined so that only one copy of the data is held in Video RAM. Through the use of hardware acceleration, the performance impact of the lack of a copy in system RAM for the CPU to access is minimized.

The end result is that in Windows Vista, the amount of system memory consumed would scale upwards in direct proportion to the number of windows open, as well as the screen resolution, while from Windows 7 onwards, system memory usage remains consistently low regardless of the number of open windows and/or resolution, since these are all stored in Video RAM. The benefits include a reduction in drive activity through reduced paging and SuperFetch caching, and increased system responsiveness, particularly during Desktop multi-tasking.

To take advantage of this improvement in memory management, you must use a WDDM 1.1 (Windows 7) or WDDM 1.2 (Windows 8) graphics driver; WDDM 1.0 drivers (designed for Vista), while supported, do not provide these benefits. See the Windows Drivers and Graphics & Sound chapters for relevant details.

FAULT TOLERANT HEAP

Windows uses dynamic memory allocation to provide memory resources to processes when they launch. This is also known as heap-based memory allocation. There are times when corruption of the data in heap can occur due to one program overwriting the memory location allocated to another program, and in turn eventually causing a crash when that location is accessed. The Fault Tolerant Heap feature, introduced in Windows 7, and used in Windows 8, attempts to identify, analyze and mitigate against such memory management issues in the event of a crash. The aim is for Windows to automatically detect and rectify crashes that are caused by heap corruption, without the need for the user to get involved. This does not

mean that programs will no longer crash; it simply reduces the potential for crashes related to this particular issue, increasing overall Windows stability.

READYBOOST

ReadyBoost was introduced in Windows Vista, and involves the use of external memory devices to speed up your system through caching data in conjunction with SuperFetch. You will require a USB flash drive or similarly fast removable media, such as a flash memory card, ideally with at least 1GB of free space or more. Any data already on the ReadyBoost device will not be deleted, but the device cannot be used for normal file storage purposes while being used for ReadyBoost. Windows 7 improved ReadyBoost by allowing devices larger than 4GB to be used, as well as being able to use multiple devices at once - up to eight separate devices for a maximum of 256GB of memory.

Connecting a ReadyBoost-compatible device to your system will bring up a 'Speed up my system' prompt. The prompt will not come up if you've disabled AutoPlay for this type of device - see AutoPlay under the Windows Control Panel chapter. You can also access the ReadyBoost settings by going to File Explorer, right-clicking on the device, selecting Properties and then clicking the ReadyBoost tab. If ReadyBoost is enabled, the device will be configured for use by SuperFetch to hold information which would otherwise be cached out to your system drive. By placing it on an attached flash memory-based drive instead, your system can access it faster than if it were on a slower hard drive, thus potentially improving system performance. The less RAM you have, the more you will see a benefit from ReadyBoost. However, ReadyBoost is not a direct replacement for RAM, and any improvements may not be significant.

In the ReadyBoost window you can configure ReadyBoost. If you select 'Dedicate this device to ReadyBoost', Windows will automatically use all available free space for ReadyBoost; if you select 'Use this device', you can manually set the amount of the device's storage space ReadyBoost uses under the 'Space to reserve for system speed' - Windows will provide a recommendation of how much you should use as a minimum, and around twice your system RAM is optimal. Any data stored temporarily on the ReadyBoost device is compressed and encrypted using 128-bit AES encryption, so if you misplace the device or it is stolen, others will not be able to readily access your data.

If you don't wish to use the device for ReadyBoost at any time, select 'Do not use this device' in the ReadyBoost window. Furthermore, if you disable SuperFetch, then ReadyBoost will have no impact.

If you are using a fast SSD as your main drive, Windows will not allow you to use ReadyBoost. You will see the message 'ReadyBoost is not enabled on this computer because the system disk is fast enough that ReadyBoost is unlikely to provide any additional benefit'. There is not much point to using ReadyBoost on a system which already has an SSD, as it will be faster for Windows to directly cache data onto your SSD rather than to attempt to cache it on a slower attached flash memory device.

In general ReadyBoost is only of any real use if you have a low amount of system RAM on your PC or device, such as 1GB or less, and are unable to upgrade the RAM for some reason. Otherwise the performance benefits of ReadyBoost may be marginal at best, although it does no harm to experiment. If you have enabled ReadyBoost and are unsure of how the system is using it, you can monitor the performance of ReadyBoost using the Performance Monitor utility, covered in the Performance Monitor section of the Performance Measurement & Troubleshooting chapter. There is a specific 'ReadyBoost Cache' monitoring category in Performance Monitor that can show you how well ReadyBoost is utilized on your system.

One final note: if you are going to purchase a USB flash drive specifically for ReadyBoost purposes, make sure to research its random read and write speeds in various reviews. A cheap USB flash drive may either be rejected by Windows as too slow for ReadyBoost, or will provide poor performance, making ReadyBoost pointless. Ultimately it may be best to simply invest the money into buying more RAM, or upgrading to a faster main drive, rather than buying a quality USB flash drive.

Disabling ReadyBoost

The ReadyBoost feature cannot be readily disabled on its own, because there is no ReadyBoost service in Windows 8, only the *rdyboost.sys* driver. It is strongly recommended that you do not attempt to disable this driver from loading, as the ReadyBoot feature also relies on it (see below), and disabling it may also prevent Windows from starting up. There is no reason to disable ReadyBoost in any case, as it does not function unless you specifically attach a ReadyBoost-enabled flash drive to your system.

If you still wish to attempt disable ReadyBoost, the safest method is to disable SuperFetch as covered in the previous section. To disable ReadyBoost on its own, you can use Autoruns to disable the ReadyBoost driver by itself as follows:

1. Launch Autoruns - see the Startup Programs chapter for more details on Autoruns.
2. Under the Options menu select 'Filter Options', then untick the 'Hide Microsoft Entries' and 'Hide Windows Entries' items.
3. Select the Drivers tab and if necessary, click the refresh button or press F5.
4. Untick the *rdyboost* component, close Autoruns, and restart Windows.

Again, this is not recommended. There is nothing to gain by doing this, and it will quite likely prevent Windows from booting up.

READYBOOT

Not to be confused with ReadyBoost, although related to it, ReadyBoot is another feature designed to use memory to optimize the boot process. However ReadyBoot can use normal system RAM to do this, as well as any external device. After every bootup, ReadyBoot calculates a caching plan for the next boot and stores part of this information under the *\Windows\Prefetch\ReadyBoot* folder, and part in the Windows Registry. The end result is that each time you boot up Windows, ReadyBoot can improve boot times through use of this cache. After bootup the memory used for caching is automatically freed up after 90 seconds, or sooner if required.

If you are finding that your bootup times have significantly increased over time, then it may indicate a problem with ReadyBoot. It can be a useful troubleshooting step to rename the *\Windows\Prefetch\ReadyBoot* folder to something else, which will force Windows to recreate it upon next startup and recommence the optimization procedure for ReadyBoot.

Disabling ReadyBoot

It is strongly recommended that you do not disable ReadyBoot, but if you wish to do so, then follow these steps:

1. Open Performance Monitor by going to the Start Screen and typing *perfmon*, then pressing Enter.
2. In Performance Monitor, double-click on the 'Data Collector Sets' item in the left pane.
3. Left-click on the 'Startup Event Trace Sessions'.
4. Double-click on the ReadyBoot item in the right pane, and under the 'Trace Session' tab untick the Enabled box, then click Apply and OK.
5. Go to the *\Windows\Prefetch* folder and delete, or preferably rename, the *ReadyBoot* folder.
6. You should then disable SuperFetch - see the SuperFetch section earlier for details.
7. Reboot your system and ReadyBoot should no longer perform its analysis and caching routines.

This will almost certainly noticeable degrade boot performance on most systems. However, whether for troubleshooting purposes, or if you have an SSD as your primary drive which you believe is fast enough not

to require boot caching, then you might wish to experiment and see if disabling ReadyBoot can improve your boot time, and in particular your post-bootup responsiveness.

Resource Exhaustion Prevention and Resolution

Windows automatically detects if any particular process is consuming most of your memory resources through the Resource Exhaustion Detection and Resolution (RADAR) feature. As memory resources, such as Virtual Memory, come close to being depleted, Windows may present a warning indicating that a particular program is using too much memory, and provide you with an option to close the program to prevent data loss through abnormal termination of processes.

The prompt usually appears when a program has a memory leak - that is, it is using ever-increasing amounts of memory resources as part of a fault within the program. Microsoft uses the information provided by RADAR to fix bugs in Windows code, and may potentially inform third party software developers of such bugs so that they too can fix any issues relating to their software. As such, you should check for an update to the problematic program in question which may fix this bug. Furthermore, you should also consider increasing your Virtual Memory limits if you have manually altered them, as they may be set too low. See the Virtual Memory section later in this chapter for details.

Memory Dump

When Windows experiences a major crash due to a fault with the core of the operating system, known as the Kernel, then the contents of the memory are dumped into a file for use in debugging the cause of the problem. A Blue Screen of Death (BSOD) error is one such crash which generates a memory dump - see the Windows Errors section of the Performance Measurement & Troubleshooting chapter for more details.

Windows 8 creates a Memory Dump file after a major crash, and by default it is stored under the %systemroot% (i.e. *\Windows*) directory in the file *MEMORY.DMP*. This file can be quite large, typically around 200MB or more. The main use for these dump files is for technical support personnel to attempt to resolve a fault. They are not designed for the average home user, as they require specialized techniques to debug.

You can configure both the type of memory dump file that gets made after a crash, and how Windows stores these dump files, using the options below. Importantly, this choice also impacts on the size of the Pagefile you will need to set, covered in the next section. To view and alter the memory dump behavior, go to the System component of the Windows Control Panel and click the 'Advanced system settings' link. Alternatively, go to the Start Screen and type *systempropertiesadvanced*, then press Enter. Under the Advanced tab, click the Settings button under the 'Startup and Recovery' section at the bottom of the window. The memory dump details are contained at the bottom of this window, under the 'System failure' section.

I recommend ticking the 'Write an event to the system log' box to assist in troubleshooting in the event of a crash or error. However you should untick the 'Automatically restart' box, as this option forces Windows to restart each time a major crash or error occurs, such as a Blue Screen of Death (BSOD). The problem with this is that this may not allow you enough time to read the actual error message or make a note of it, so by disabling this option you can note the error and then manually reboot when ready. The other settings here are covered in more detail under the Boot Configuration Data section of the Boot Configuration chapter.

As discussed later in this section, the Pagefile and the memory dump size are linked together. Depending on which type of memory dump you use, this will impact on the minimum size possible for a system-managed Pagefile. Go to the 'Write debugging information' area of the Startup and Recovery window where you can select the following:

- *Automatic Memory Dump* - This is a new option in Windows 8, and is the recommended setting. It allows Windows to create a full Kernel Memory Dump after each crash, as long as the Pagefile is large enough to contain it. If the Pagefile is too small for a Kernel Memory Dump, a Small Memory Dump will be created instead.
- *Complete Memory Dump* - Allows Windows to create a memory dump containing the entire contents of your system RAM at the time of the crash. Hence the dump file is the same size as your system RAM.
- *Kernel Memory Dump* - Allows Windows to create a full Kernel Memory Dump after each crash at the specified location.
- *Small Memory Dump* - Forces Windows to only store a small memory dump file of up to 256KB in size (the maximum for 64-bit systems) which has the most important information. This dump file is stored under the *\Windows\Minidump* subdirectory by default.
- *None* - Does not allow Windows to save any memory dump files after a crash.

If the 'Overwrite any existing file' option is ticked, Windows will automatically overwrite any existing dump file at the stored location, which is recommended to prevent excessive drive space being wasted through storage of multiple old dump files. Even without this option being ticked, if free space on the specified drive is below 25GB, Windows will automatically prevent the saving of the dump file to the drive, so that the drive doesn't fill up with lots of dump files. If dump files are critical to your needs, ensure that there is much more than 25GB of free space on the specified drive location.

Note that depending on the memory dump option you choose, this can affect the recommended minimum Pagefile size, as covered in more detail in the next section. In short:

- For the new Automatic Memory Dump option, there is no minimum Pagefile size, as Windows will automatically select the correct dump size to fit into the existing Pagefile.
- For the Complete Memory Dump option you require a Pagefile which is at least the same size as your system RAM + 1MB.
- If you have enabled Kernel Memory Dump, you will require a minimum Pagefile size of 150MB - 2GB depending on your RAM size.
- For the Small Memory Dump option, a 2MB Pagefile is required as minimum.
- If you choose to have no memory dump file, there is no set minimum Pagefile, though keep in mind that a zero Pagefile is not recommended, so 1MB is the suggested minimum.

For most home users the default Automatic Memory Dump option is suitable, as is ticking the 'Overwrite any existing file' option. Note that under certain circumstances, such as serious errors, Windows may not be able to generate a crash dump file in time, thus none may be available regardless of your settings.

VIRTUAL MEMORY

Virtual Memory refers to a memory management technique used in several generations of Windows. During normal operation, system RAM is the best place to store information for fast access by your CPU and other components, since it has no moving parts, and information in it can be accessed at many times the speed of any drive. So ideally Windows likes to keep a portion of all of your most commonly used programs in RAM, as well as most of your currently used application(s). There are also other memory requirements for the hardware and software on your system which all use some portion of memory resources.

When RAM starts to run low, or if Windows determines that a particular application is no longer a high enough priority, it breaks up some of the portions of data in memory into 4KB units known as "pages", and temporarily swaps them out from your RAM to your drive. This "swap file" where the memory pages are held on your drive is *pagefile.sys*, and resides in the base directory of your drive. That's why you will often see the terms Virtual Memory, Pagefile and Swapfile being used interchangeably to refer to the same thing. You can only see *pagefile.sys* if the 'Hide Protected Operating System Files' option is unticked under Folder Options - see the Folder Options section of the File Explorer chapter.

Windows 8 continues the use of Virtual Memory management, but with a few improvements as detailed in this Microsoft Article. These include a new Memory Combining technique to allow Windows to assess the contents of system RAM and locate duplicate content, reducing redundancy and thus freeing up memory resources. The structure of the underlying Windows code has also been optimized, better prioritizing the code that needs to be running in memory and again freeing up more memory resources that would otherwise be used less efficiently.

Windows 8 now also creates a new *swapfile.sys* file, in the same location as *pagefile.sys*. This *swapfile.sys* file is linked to Virtual Memory, but is a custom system-controlled Pagefile used to improve the efficiency of paging operations, including the handling of Metro apps. It is typically 256MB in size, and is not user-customizable, but will also be disabled if you manually disable the main Pagefile.

Although Windows tries to minimize reliance on your physical drive, since using it can cause small delays, a Pagefile is still very important to Windows Memory Management. Even on a system with a great deal of RAM, the Pagefile is not something you should disable or consider redundant, as paging portions of processes to it is a necessary part of efficient memory management and program prioritization in Windows. In the absence of this aspect of Virtual Memory, your system may actually use more system RAM than is necessary.

To access your Virtual Memory settings, go to the System component of the Windows Control Panel and click the 'Advanced system settings' link, or go to the Start Screen, type *systempropertiesadvanced* and press Enter. Under the Advanced tab click the Settings button under Performance, and select the Advanced tab in the Performance Options window that opens. Under the 'Virtual Memory' section here you can see the amount of drive space currently allocated to the Pagefile. For most users, letting Windows automatically manage the Pagefile is perfectly fine and will prevent your system from running out of memory resources, since the Pagefile will automatically be resized as required. However more advanced users can manually adjust the Pagefile size, after taking into account appropriate considerations.

Adjusting the Pagefile

To alter the Pagefile settings, access the settings as covered above, then click the Change button. Untick the 'Automatically manage paging file size for all drives' box, and you can now alter the physical location and size limits for the Pagefile. Read all of the advice below before making any changes.

Clearing the Pagefile: Before setting a new Pagefile size or location, you should first clear your existing Pagefile. To do this select your system drive(s), choose the 'No paging file' option and click the Set button, then reboot your system. This step does two things: firstly, it clears and resets the Pagefile, fixing any potential Pagefile corruption which can occur after a bad shutdown; and secondly, it ensures that any new Pagefile you create will start off as a single unfragmented contiguous block on your drive for optimal performance, and should remain unfragmented in the future. Note that if you have any problems booting back up into Windows due to a lack of a Pagefile during this step, enter Windows in Safe Mode and continue the setup procedures for Virtual Memory from there - see the System Recovery section of the Backup & Recovery chapter for details of Safe Mode.

Location of the Pagefile: Highlight the logical drive where you want the Pagefile to be placed in the Drive box. The drive(s) or partition(s) the Pagefile should be located on is based loosely on the following scenarios:

- 1 Drive (1 Partition) - The Pagefile can only be located on the first primary partition of your drive, which provides optimal performance. Do not create a new partition for the Pagefile, as there is no performance benefit from doing so.
- 1 Drive (2 Partitions or more) - Make sure the Pagefile is placed on the first primary partition as this is the fastest partition on hard drives; on SSDs it makes no difference which partition is chosen. Placing the Pagefile on another partition of the same drive does not provide any performance benefits.
- 2 Drives or more (similar speeds) - If all of your drives are similar in terms of their rated speed, you should put the main portion of the Pagefile on the drive that doesn't contain your Windows installation and applications, e.g. put it on a general data drive. If you've already separated your Windows installation from your applications/games, then place the Pagefile on the drive which doesn't contain your applications, even if this is the Windows drive. Alternatively, you can experiment with splitting the Pagefile evenly by creating multiple smaller Pagefiles, one on each drive - up to a limit of 16 - and this may improve overall performance.
- 2 Drives or more (different speeds) - If one drive is notably faster than the others (e.g. an SSD), you should put the main Pagefile on that drive, regardless of whether it is the system drive or not. This is particularly important if you have relatively low system RAM, since the Pagefile will be accessed more often, and thus needs to be on the fastest drive. Note that for the purposes of creating a memory dump, you may need to retain a small Pagefile on your system drive regardless of where the main Pagefile is located.
- RAID Configuration - For striped RAID configurations, such as RAID 0 or RAID 5, or for drives in a Storage Pool, Windows sees these as a single large drive, hence you cannot actually choose which drive to place the Pagefile on; it will be split evenly across the drives, which is optimal. If you have a separate faster drive outside the RAID or Pooled configuration, such as an SSD vs. a pair of RAID hard drives, you may choose to shift the Pagefile to the faster drive.

Microsoft does not recommend disabling the Pagefile if you have an SSD. Indeed, it is recommended that if you have the choice, you should place the Pagefile on an SSD if available and it has sufficient storage space. Pagefile access primarily consists of reads, which will not have a significant detrimental impact on SSD lifespan. In any case the rules to determining the Pagefile size as covered below apply equally to HDDs and SSDs.

Pagefile Size: After selecting the location for the Pagefile, you can then determine its total size in MB. To do this, in the Virtual Memory settings window select the 'Custom size' option. Although there are many differing opinions as to how big the Pagefile should be, it is important not to disable your Pagefile regardless of how much RAM you have. Windows need a Pagefile in order to operate correctly and efficiently. Setting the Pagefile to zero results in less efficient use of system RAM, and it also restricts the amount of memory resources your system can allocate should a program require more memory than you have in the form of available RAM. It also prevents memory dumps being created for debugging purposes after a crash.

According to this Microsoft Article, by default Windows 8 sets your Pagefile with a minimum size of equal to your system RAM, and the maximum equal to three times your RAM. In practice however, Windows 8 actually seems to set much lower limits. Regardless, there is scope to refine the Pagefile size. The "correct" size of the Pagefile is frequently and hotly debated, and there are many conflicting accounts of the optimal size. I take my recommendations from a person best positioned on this topic, with both practical and theoretical experience on the matter: Microsoft technical guru Mark Russinovich, as covered in this Microsoft Article.

The correct method to determine the optimal Pagefile size for your particular system is to examine the maximum Commit Charge value for the combination of programs you frequently run at the same time. The Commit Charge is the amount of Virtual Memory reserved for a particular process. Compare this value to the current Commit Limit on your system, which is the sum of your system RAM + Pagefile. If the sum of Commit Charge for all of your common processes attempts to exceed the Commit Limit at any time, then there will be memory allocation problems, potentially leading to crashes and system failure. So the aim is to ensure that the peak value achieved for Commit Charge never exceeds the Commit Limit, which in turn tells us how big the Pagefile must be.

The way to determine your Peak Commit Charge is as follows:

1. Download and launch the free Process Explorer utility, and keep it running in the background.
2. Use your system normally for a lengthy period, including loading up any and all programs you would normally use in a session, as well as any additional data. For example, load up your most strenuous games one by one and play them for a while. Or load up your largest applications and load any data you may be working on within those applications. The aim is to see the maximum amount of memory resources you might potentially use in any typical session in the future. Don't artificially load up a dozen applications at once if that's not what you would normally do.
3. Without restarting your system, after a period of time go to the View menu in Process Explorer and select System Information - a new window will open.
4. In the System Information window, go to the Memory tab and examine the Commit Charge section. The Peak Commit Charge is shown, as well as the Commit Charge Limit. The Peak/Limit section also shows you how large a proportion of the Commit Limit the Peak Commit Charge came to being.

Using this data, you should then set the minimum Pagefile size according to this formula:

Pagefile Minimum Size = Peak Commit Charge - Total System RAM

That is, subtract your Total System RAM amount from the Peak Commit Charge amount. If the result is negative (i.e. you have more RAM than the Peak Commit Charge), this does not mean you should set a 0 Pagefile minimum size. Remember that at the very least you require a minimum Pagefile size corresponding to your memory dump settings, covered in the Memory Dump section earlier in this chapter. For the default 'Automatic Memory Dump' setting in Windows 8, this means at least 2MB. If you've completely disabled the memory dump, then 1MB is fine.

The maximum Pagefile size is then calculated as:

Pagefile Maximum Size = Up to 2 x Pagefile Minimum Size

Since your Commit Limit has already been set to meet your most strenuous requirements as per the Pagefile minimum formula further above, you should be fine to set your Pagefile Maximum Size to equal that of the Pagefile Minimum Size. However I recommend being safe and setting the maximum up to twice the minimum, or 1GB, whichever is higher, to provide a bit of extra headroom. This provides some padding in the case of unforeseen usage patterns, and to future-proof against upcoming applications and games which may use a bit more memory. Note that there is a 4GB limit for maximum Pagefile size if running a 32-bit version of Windows 8. You need to enable Physical Address Extension to remove this limit - see the Maximum Supported RAM section earlier in this chapter.

If you've decided to spread the Pagefile over multiple drives, ensure that the sum of the Pagefile sizes equals the values above.

Once you've adjusted your Virtual Memory size settings click the Set button and reboot if required.

If you still insist on setting a zero (disabled) Pagefile, at least make sure you have your Memory Dump set to the None option to ensure there isn't a problem if the system tries to save a memory dump after a crash. Also keep in mind that in some circumstances, having no Pagefile may mean that you will lose any unsaved work if Windows suddenly runs out of memory and does not have access to sufficient Virtual Memory resources. It can also lead to inefficiencies in the way in which Windows handles memory allocation. Basically, aside from saving some disk space, there will be no noticeable performance benefit from disabling the pagefile.

If you want to monitor the usage of your memory and the Pagefile, there are several methods to do so. These include the use of the Task Manager, the Process Explorer utility, and the Performance Monitor - all covered in detail under the Task Manager section of Performance Measurement & Troubleshooting section, where the various memory-related settings are explained in more detail. In particular, a common point of confusion regarding Pagefile usage is the Paged pool and Non-paged pool memory items under the Memory section of the Performance tab of the Task Manager. These do not monitor Pagefile usage, they monitor areas of core Windows memory usage that can be paged if necessary, or must remain unpaged. This is not the same as actual data in the Pagefile, and once again the Task Manager section covers this in more detail.

The method for determining the Pagefile size in this section may seem tedious or confusing at first, in which case I strongly advise that you use the default 'System managed size' option until you have the time to get a better understanding of it. Keep in mind that the recommendation in this section hinge solely on analysis of your Peak Commit Charge at a single point in time. If over time you install and launch new programs which use much greater amounts of memory, or you multitask with more programs than you originally envisioned, or load up increasingly large datasets within your programs, then there is greater likelihood that your Peak Commit Charge will rise, and you must therefore revisit your Pagefile size and go through the steps above again with more recent data. This is also why it is important to build some headroom into your maximum Pagefile size, as suggested above.

If at any time the Resource Exhaustion Detection prompt comes up, you should consider increasing your maximum Pagefile size. Having a larger maximum Pagefile size does not hurt performance as such; it can only takes up additional drive space, so if in doubt play it safe, or just revert back to the System Managed setting.

You can set the Pagefile to be automatically erased each time you shutdown Windows, if you have security concerns regarding the fragments of user information which may be stored there. This is an unnecessary measure for most users as it can significantly slow down shutdown times. If you require this level of security, see the Local Security Policy section of the Security chapter for details.

< UPGRADING MEMORY

There is no real substitute for having a decent amount of physical RAM installed on your system. All of the advanced memory management features in Windows 8 ultimately can't truly compensate for having too little RAM for the programs you choose to run. This is particularly true for gamers, as complex 3D games sometimes require large amounts of RAM to operate smoothly. Fortunately, RAM is relatively cheap. A combination of purchasing more RAM and using the 64-bit version of Windows 8 provides the simplest method of attaining smooth and responsive performance on your system. With excellent support from developers for 64-bit Windows, with SuperFetch having been tamed, and the various other Windows Memory Management features all having been refined to reduce the potential for memory-related errors, the RAM will be used efficiently to improve your Windows experience noticeably.

In Windows 8, even though the minimum requirement is 1GB, I suggest a more practical minimum of 2GB if you want greater responsiveness, and 4GB of RAM or more is optimal for genuinely smooth performance. If however you are restricted in how much RAM you can upgrade to, such as being on a mobile device with non-upgradeable memory, then consider either upgrading your drive to a faster SSD, or utilizing one or more fast USB flash device(s) as part of the ReadyBoost feature.

DRIVE OPTIMIZATION

Windows Memory Management is intimately related to the way your drives are used in Windows. The drive is traditionally one of the slowest components of a system, particularly when using a Hard Disk Drive (HDD). To remedy this, Windows attempts to hold as much of the information as possible in RAM. That way, whenever one of your other components, such as the CPU or graphics card, needs information, it can access it much faster from memory, without the stuttering or slowdowns commonly associated with directly accessing a drive for data.

Regardless of how much RAM you have, or how efficient Windows is with memory management, at the end of the day RAM is only a temporary form of storage which is cleared each time your PC shuts down. It is a physical drive on which all of your information is permanently stored, and which your system must regularly access to load up data. To a large extent, the advent of the memory-based Solid State Drive (SSD) has removed this weak link from the equation, replacing slower mechanic hard drives.

This chapter looks at how the drives are used in Windows, and then provides tips on how to make sure that this usage is optimal for your particular hardware configuration, whether HDD or SSD.

< WINDOWS I/O MANAGEMENT

To deal with the potential bottleneck that the drive can represent on a modern systems, especially in light of the rapidly expanding processing speeds of CPUs and other key system components, as well as user desires to undertake greater multi-tasking, a markedly improved Input/Output (I/O) System was introduced as of Windows Vista. Windows 8 continues the use of this system.

Windows prioritizes the allocation of drive read and write tasks by your various programs. Multiple applications running at the same time can put great demands on drives, some of which may struggle to smoothly supply all the data required. For example, you may be using Windows Media Player to listen to music or watch a movie while a malware scanner is doing a full scan; or you may be playing a game while a disk defragmenter attempts to run a scheduled job in the background; or you may be downloading a file from the Internet while your system is encoding a large video file. If multiple tasks like these are not handled properly by Windows, the end result is significant stuttering or freezes, and even data errors.

When you run multiple applications at once - called multitasking - Windows first prioritizes applications based on how much CPU time they need. This is not disk I/O prioritization, this is the management of separate process threads which are competing to get access to the CPU so they can complete their tasks. Windows then prioritizes these threads such that the important ones receive more overall CPU time if they require it. The six broad priority categories for CPU Priority from highest to lowest are: Real Time, High, Above Normal, Normal, Below Normal and Low. They can be viewed and manually altered using Task Manager - see the Task Manager section of the Performance Measurement & Troubleshooting chapter for details. Multitasking is where having a multi-core CPU is of most benefit, as any time you run multiple programs at once, the separate threads can be automatically split across your CPU cores, run concurrently, and thus complete much faster.

Having allocated a priority for CPU time, Windows then determines the relative priority of applications for drive time, or in other words disk I/O prioritization. Windows bases I/O Priority on four broad categories: Critical, High, Normal and Low. You cannot manually alter these, as they are determined by the application itself combined with Windows. and how you are currently using the system. The bottom line is that certain tasks will run at reduced speed, or will even cease altogether, if the I/O resources are required by more

important tasks; this is particularly important for gamers, since games require almost total control of I/O resources for smooth performance.

The practical impacts of this I/O prioritization scheme are that firstly, less critical background tasks, such as SuperFetch prefetching, will not cause the system to become unresponsive. In fact Windows will suspend certain background tasks altogether if a more important task is being undertaken, like running a system-intensive program. Windows also reserves drive bandwidth for certain tasks that specifically need a consistent flow of data, especially multimedia applications, so that these are not disrupted. Thus it is possible to run a drive-intensive task while also listening to music on Windows Media Player without frequent audio glitches occurring for example.

The actual impact of multiple tasks running at once on your system will vary depending on a range of factors, particularly your drive speed and the amount of RAM you have. The slower your drive, and/or the less RAM you have, and/or the more applications you try to run at once, the greater the likelihood that no matter how hard Windows tries, it won't be able to prevent some slowdown or stuttering. In that case clearly you should try to reduce the number of things you are doing at once. Windows I/O prioritization cannot work miracles, so to minimize stuttering issues when running system-intensive programs, I recommend that you close down all other open programs, including shutting down minimized Metro apps.

< HARD DISK DRIVES

A major reason why Windows requires a range of complex I/O management features is primarily because of the relatively slow nature of traditional Hard Disk Drives (HDD). The problem with hard drives is that even the fastest hard drive is still slowed down by the mechanical nature of its operation: a spinning platter and a moving drive head are used to seek out pieces of data, and these mechanisms can only move so fast. A hard drive is typically the slowest component in any system.

Hard drives still serve a useful purpose, and will continue to do so for a while yet, as they are quite reliable, and provide tremendous amounts of storage space at a low price. Many Windows 8 users are likely to still be using a hard drive, and this is both taken into account by Microsoft when they developed Windows 8, and is also a primary consideration in this book - the optimization tips throughout this book all apply to hard drives. There is specific a partitioning procedure which may improve performance on a hard drive, and it is covered below.

SHORT STROKING

Short Stroking essentially involves partitioning the hard drive such that the head movements on the drive are restricted only to the outer sectors of each platter, which are the quickest to access. The problem with short stroking is that it significantly reduces the usable storage capacity of the hard drive, although given the low cost of large hard drives, and especially when combined in a RAID configuration, you can still generate a reasonably large amount of storage using multiple short-stroked hard drives relatively cheaply.

The easiest way to achieve the short stroke effect on a hard drive is to create only a single small partition (i.e. around 10% of the total drive capacity or less in size). This is automatically placed at the outer edge of the drive, and may improve performance for the drive. The real-world performance benefits of short stroking are somewhat dubious, because the benefits are mostly seen in synthetic benchmarks.

< OPTICAL DRIVES

Optical drives such as CD, DVD and Blu-Ray drives, are even slower than hard drives, again due to inherent physical constraints, so they have never been considered as a viable replacement for primary data storage on desktop systems. Since they only serve as secondary storage, primarily due to the portability of optical media, the speed of optical drives is not critical to Windows performance.

Windows 8 goes a long way towards alleviating one of the major annoyances in earlier versions of Windows, whereby inserting a disc into an optical drive could see certain system functions freeze until the disc was correctly detected. This could take 10 seconds or more depending on the optical drive and the media involved. In Windows 8, while you obviously cannot access the contents of the optical drive itself while it is busy spinning up a disc, you can usually undertake normal functionality in File Explorer on other drives without interruption. Refer to the AutoPlay section later in this chapter to configure how Windows behaves when you insert different types of optical media.

< SOLID STATE DRIVES

A Solid State Drive (SSD) is a flash memory-based storage drive that has no physical moving parts. The key benefits of SSDs is their very fast read speeds, with a random read speed roughly a hundred times faster than a hard drive, and sequential read and write speeds which can vary depending on the quality of the drive, but which usually exceed those of the fastest hard drives, often by a large margin. There are still various potential drawbacks to using an SSD aside from its price, however these are steadily being ironed out with newer and higher quality versions of these drives. If you are considering upgrading your current system drive, or adding a new drive to your system, it is strongly recommended that you consider purchasing an SSD. SSDs provide greatly improved overall system performance by removing the significant bottleneck which mechanical hard drives have placed on systems.

Windows 8 natively support SSDs through a range of built-in optimizations and features. This means that there is little need for any specific optimization procedures by the average user, as an SSD will be detected and various relevant features will be correctly configured automatically by Windows. Throughout this book, SSD users are given special notes where a procedure should be different for an SSD when compared to an HDD. Below is some additional information on Windows 8's SSD-specific features.

TRIM

TRIM is a command that ensures that deleted blocks on an SSD are securely erased, and that the drive is aware of which blocks have been deleted. This helps maintain optimal performance and a longer lifespan on an SSD. Windows 8 automatically enables support for the TRIM command under NTFS. TRIM support can be confirmed by opening an Administrator Command Prompt and typing the following:

```
fsutil behavior query DisableDeleteNotify
```

If the result is shown as `DisableDeleteNotify=0` then TRIM is enabled. This is the default setting for Windows 8 on all systems. To change this setting for any reason, use the following command:

```
fsutil behavior set DisableDeleteNotify 1
```

A value of 1 for the command above disables TRIM, and a value of 0 enables it.

Even when TRIM is enabled in Windows, whether TRIM is actually being used by your SSD, and how it is used, is determined by its firmware and the motherboard storage controller drivers being used. Check your SSD manufacturer's site for details of the TRIM support on your drive. The only reason to manually disable TRIM support in Windows is if the drive manufacturer specifically recommends this to prevent problems on certain drives.

TRIM hints given by Windows 8 to the drive may be used immediately by the drive to perform a cleanup, or the drive may reschedule or even discard TRIM hints under certain circumstances. This is all handled by the drive. However you can force the drive to undertake full optimization by running the new Optimize Drives utility, formerly known as Windows Disk Defragmenter - see the Optimize Drives section later in this chapter for details.

In short, for most SSD owners, there is no action required, as TRIM will automatically be enabled and used by your SSD when using an NTFS-formatted drive under Windows 8. If your SSD does not allow proper TRIM support, its performance may noticeably decline over time. This can only be rectified by using the Optimize Drives utility in the first instance.

If your SSD performance continues to degrade, you will need to use a custom erase command to reset it to its correct speed, as a regular format will have no impact on this issue. You should check your SSD manufacturer's website for a utility which triggers this built-in command, or use this free Secure Erase utility to do so. Download and extract the *HDDErase.exe* file, and read the .txt file that comes with it for usage instructions. The HDD Erase utility is designed for both HDD and SSD, however it is an older utility which may not be compatible with the latest SSDs. You can instead use the free Parted Magic utility. Go to the System Tools menu in Parted Magic and select the 'Erase Disk' command, then select the 'Internal: Secure Erase command' option.

It is recommended that you backup your data and then do a full secure erase of your SSD if you notice that your drive's performance has been significantly degraded over time. You can also do a secure erase prior to reformatting the drive for a new Windows installation to ensure optimal performance.

DEFRAGMENTATION

Defragmentation involves finding fragments of files which are spread throughout the drive and putting them back together again to prevent a degradation in performance. SSDs don't need to read files sequentially, and are not affected by file fragmentation, hence they don't benefit from defragmentation. Furthermore, defragmenting an SSD has a negative impact on the potential reduction in SSD lifespan.

Under Windows 7, scheduled defragmentation via the built-in Windows Disk Defragmenter was automatically disabled on any detected drives which exceed random read speeds of 8MB/s, which basically means all SSDs.

Under Windows 8, the Windows Disk Defragmenter has been renamed the Optimize Drives utility, and a scheduled run of this utility is now active for SSDs. This is because under Windows 8, the Optimize Drives utility takes different actions depending on whether it is used on an HDD or SSD. When running on an SSD, Optimize Drives will not do a traditional defragmentation, rather it will send TRIM commands to the SSD, giving it the opportunity to clean up and optimize the entire drive in one go. This is beneficial, and should be kept enabled.

See the Optimize Drives section at the end of this chapter for more details.

PAGEFILE

Microsoft does not recommend disabling the Pagefile on a system with an SSD as the primary drive. Pagefile access primarily consists of reads, which will not have a significant detrimental impact on SSD lifespan. Furthermore, if the Pagefile is going to be used by Windows at any time, it is best placed on the fastest possible drive to prevent stuttering or slowdowns. The same rules to determining the Pagefile size and location as those for traditional hard drives apply.

See the Windows Memory Management section of the Memory Optimization chapter for more details.

SEARCH INDEX

You should not disable the Search Indexer if you have an SSD, since Indexing still makes a noticeable difference to the speed and comprehensiveness of search results on all types of drives. This is why Windows 8 does not automatically disable the Search Index when an SSD is detected, and it is not recommended that you do so either. One thing you can do however is to refine your Search Index to reduce its overall size and scope, and hence reduce the frequency with which it is altered to no real benefit.

See the Windows Search chapter for more details.

SUPERFETCH & READYBOOST

Windows 8 will automatically disable SuperFetch and ReadyBoost on drives with sufficiently fast random read, random write and flush performance. This occurs on any drive which scores 6.5 or above in the drive performance category of the Windows Experience Index. If Windows has not disabled SuperFetch, you can manually disable it if you feel your SSD is fast enough.

See the Windows Memory Management section of the Memory Optimization chapter for more details.

TEMPORARY & PERSONAL FILES

Personal files, such as movies, photos and documents, can be moved off an SSD both to create extra space, and to reduce the amount of write activity on the SSD. This should have little detrimental impact on performance. For example, you can relocate your Personal Folders to a spare HDD, and do so without breaking Windows 8's link to these folders. See the Personal Folders section of the File Explorer chapter for details of how to do this correctly.

Temporary folders used by programs, such as caches, on the other hand are generally best left on the SSD. This is based on the same principle as keeping the Pagefile on an SSD. The entire reason for purchasing an SSD is to speed up data access. If you move important data that Windows or a program needs to regularly access to a slower drive, then you defeat some of the performance benefits of having an SSD.

PARTITION ALIGNMENT

You may need to manually realign your drive partitions periodically on an SSD, depending on a range of circumstances. Disk Partition Alignment is required when the physical sectors of a drive are not in complete alignment with the logical partition sectors/pages. Under Windows XP and versions prior to it, a 31.5KB offset is used at the start and between each partition, while under Windows Vista, Windows 7, and now Windows 8, 1024KB-sized offsets are used. If the incorrect offset is used, the resulting misalignment will cause a noticeable degradation of performance. It can affect hard drives, but has the greatest impact on modern SSDs due to the fact that their page system differs from the sector logic of hard drives.

If you have only ever used the built-in Windows Vista, 7 or 8 partitioning and formatting tools on your drive, then your partitions should be aligned correctly. Furthermore, if you want to migrate a hard drive's contents to an SSD, you can ensure correct partition alignment by using the system image functionality in Windows 7 File Recovery, as covered in the Windows 7 File Recovery section of the Backup & Recovery chapter. Create a full system image backup of your hard drive to a temporary location, then restore that image to the new SSD, and it should correctly migrate your data while retaining proper alignment.

If on the other hand you have used Windows XP or third party tools to create or manipulate your partitions, then they may not be correctly aligned. It is wise to check all of your partitions now and fix this if necessary, as it can provide a significant increase in drive performance on SSDs.

The first step involves determining whether any of your existing partitions are misaligned. The quickest way to do this is to with built-in Windows tools as follows:

1. Type *msinfo32* on the Start Screen and press Enter.
2. In the System Information tool window that opens, expand the Components section in the left pane, then expand Storage, and select Disks.
3. Alternatively, open a Command Prompt, and type the following then press Enter:

```
wmic partition get name,startingoffset,size
```

4. For either method, for each drive there is a listing of partitions (e.g. Disk #1, Partition #0), and for each partition, a 'Partition Starting Offset' or StartingOffset item.
5. Typically a value of 1,048,576 bytes is shown, which is the correct value. For any other value, use a calculator and enter the starting offset figure shown in bytes, then divide it by 4,096. If the result is a whole number, the offset is correct and the partition is aligned; if the result shows any decimals, the partition is misaligned.

If any of your partitions are incorrectly aligned, the next step is to rectify this in one of several ways:

§ Delete the misaligned partition(s), then reinstall Windows, making sure to partition and format the drive fully through the Windows installer to ensure correct alignment.
§ Delete the misaligned partition(s), then use the manual `Diskpart` command method to partition your drive as covered under the Preparing the Drive section of the Windows Installation chapter. At the step where you create a partition, add the `align=1024` command to be certain that the partition uses the correct 1,024KB offset. For example:

```
create partition primary align=1024
```

§ Use the free GParted utility along with this tutorial to attempt to align an existing partition without deleting it.
§ Use a non-free utility, such as Aomei Partition Assistant or Paragon Alignment Tool, which have custom partition alignment features to align your partition without deleting it.
§ Check your drive manufacturer's website for a custom partition management/alignment tool.

While partition alignment isn't really necessary for modern hard drives from Windows Vista onwards, ensuring that an SSD is aligned can make a real difference to performance. Check your partition alignment after any partition management activities, especially when using third party utilities.

LONGEVITY

There are many online tutorials and optimization guides that recommend disabling a wide range of features in Windows when running on an SSD. This appears to be a misguided attempt to prolong the life span of an SSD. Everything from forcibly disabling all of the features covered above, to disabling critical features like anti-malware scanners and System Restore, following these tips can actually do much more harm than good.

It is true that consumer flash memory-based solid state drives have a set lifespan. The flash memory chips used in such drives eventually wear out, having only a limited number of erase and write cycles. Different SSD technologies will have different maximum erase/write cycles. All SSDs manage this issue by ensuring that data is evenly distributed in the drive, so that all the cells are worn out at the same rate. But the key thing to consider is that any modern SSD, when used normally just like an HDD, will take many years before the drive becomes unusable. It's much more likely that the drive will die of some other cause, or simply become obsolete, before it uses up all of its erase/write cycles.

So essentially the question of SSD longevity should be a non-issue for most users. Crippling Windows functionality, or constantly moving files to hard drives, defeats the primary purpose for which the SSD was created: to speed up all data access on your system. Use the drive as you would any normal HDD. If you want to determine how many years of life are left in your SSD, you can use a utility like SSD Life to get an estimate by analyzing your usage patterns and extracting information from SMART. The utility isn't free, but it is sufficiently functional for a trial period. Check your SSD manufacturer's website for a similar utility.

In all other respects, SSD users should follow the same advice provided for traditional hard drive owners in this book, as they apply equally to SSDs. If there are any special considerations for SSDs, they are noted where relevant. An SSD is a fast drive to be sure, but flash-based SSDs are still not as fast as system RAM, hence many Windows Memory Management features are beneficial on systems using SSDs.

< MOUNTING ISO FILES

One of the new features of Windows 8 is native support for ISO Image files. These files are typically an exact duplicate of an optical disc, such as a CD or DVD. The benefit of an ISO file is that aside from containing a precise copy of the data on the disc, it retains the format of the disc as well. This means the ISO file can be burned to a disc of the same type, and function in the same manner as the original disc.

Windows 8 provides the ability to mount ISO files as though they are a separate (virtual) optical drive on your system. To use this feature, double-click on a valid ISO file in File Explorer, or right-click on it and select Mount.

When an ISO file is successfully mounted, it will appear as a separate new drive under the Computer category in File Explorer. Its contents can be viewed or launched like a physical disc in an optical drive. Note that playback of movie DVDs is not possible by default in Windows 8 unless a third party application with appropriate support, or the Windows Media Center add-on, is installed. See the DVD & Blu-ray Playback section of the Windows Media Player chapter for details.

You can also burn an ISO file to disc by right-clicking on it in File Explorer and selecting 'Burn disc image', which will open the Windows Disc Image Burner utility. Insert the appropriate type of blank disc and the image will be burned.

To detach a mounted ISO image, right-click on its virtual drive and select Eject.

< VIRTUAL HARD DISK

Windows 7 introduced native support for the Virtual Hard Disk (VHD) format, which Windows 8 continues. As the name implies, a VHD file is designed to be identical in structure to a physical hard disk, and is generally treated as a physical drive by Windows. Note that this function is only available on Windows 8 Pro or Enterprise editions.

Windows 8 adds the VHDX format which, as described in this Microsoft Article, provides improvements, including up to 64 Terabytes of space, support for TRIM commands on SSDs, and data corruption protection during power failures.

VHD/VHDX files have a range of useful purposes in Windows, many of which are really only relevant to Network Administrators, software developers and testers. However we look at the most useful of these features for home PC users.

BOOTING UP FROM A VHD

Windows 8 supports natively booting up from a VHD/VHDX file. This allows you to run multiple copies of Windows 8 on a single PC for example without the need for separate partitions or drives devoted to each one, because each separate OS environment can be stored as a VHD/VHDX file, and selected from the Windows boot menu. It will launch without requiring another operating system to work in. The main benefit for a home user of doing this would be to allow you to test software or drivers on an identical VHD/VHDX copy of your Windows 8 install, without worrying about any harm being done to your original installation of Windows 8.

To boot up a Windows 8 VHD/VHDX, the first thing you require is a Windows 8 .VHD or .VHDX file. To create one from an existing install of Windows 8 or from a Windows 8 DVD, you can use the Microsoft Convert-WindowsImage or the free Disk2VHD utility. The procedure for booting up a Windows 8 .VHD/.VHDX is detailed in this Microsoft Article, however the easiest method is to use an automated boot configuration tool such as EasyBCD, which is covered in the Boot Configuration Data section of the Boot Configuration chapter. Follow these steps:

1. Open EasyBCD, then click the 'Add New Entry' button.
2. Select the 'Disk Image' tab at the bottom.
3. Select 'Microsoft VHD' in the Type box.
4. Click the '...' button next to the Path box and browse to the location of your VHD file and select it.
5. In the Name box, give it a descriptive name (e.g. Windows 8 Virtual).
6. Click the 'Add Entry' button at the bottom to add it as an entry to your Windows 8 boot menu. This will let you to select whether to boot into the real Windows 8 or the Virtual Windows 8 at each startup.
7. Reboot, and the Virtual Windows 8 should now be available in the boot menu.

Be aware that in this virtual VHD/VHDX version of Windows 8, certain features may not function correctly, such as BitLocker, Hibernation and the Windows Experience Index. Also keep in mind that depending on how you took the Windows 8 .VHD or .VHDX image, it may be hardware-dependent; that is, it captured the hardware state of your system, and hence it may not be bootable or operative when mounted on a physically different PC.

CREATING A VHD OR VHDX

To create an empty VHD/VHDX for use as a new virtual drive or partition, do the following:

1. Open Administrative Tools in the Windows Control Panel and select Computer Management.
2. In Computer Management, select the Disk Management component in the left pane.
3. Go to the Action menu in Disk Management and select 'Create VHD'. You can create a basic .VHD file, or the more advanced .VHDX file. It is recommended that SSD users select .VHDX, but if you want to use the file on a Windows 7 system as well, select .VHD for compatibility purposes.
4. You will then be asked where to place the .VHD/.VHDX file and what to call it, the total size to allocate to this new 'drive', and whether it is Fixed or Dynamically Expanding - Fixed is recommended for .VHD, Dynamic for .VHDX.
5. Once created you will see a new unformatted drive appear in the bottom pane of Disk Management.
6. You must prepare this new virtual disk for use by right-clicking on the name of the disk in the bottom pane of Disk Management (e.g. right-click on 'Disk 2') and selecting 'Initialize Disk'.
7. You can now partition and format the disk and assign a drive letter as normal by right-clicking on the disk space (showing size and Unallocated) and selecting 'New Simple Volume' and following the prompts.

This new .VHD or .VHDX file is seen as a separate drive on your system for most intents and purposes, with its own drive letter and file format. It can be reformatted as desired, and can store files and folders like a normal drive or partition. However if you look at the location where you set up the VHD/VHDX, you can see that it is a separate file with the extension .VHD or .VHDX. This means that unlike a partition, it is portable, and can also be easily duplicated and distributed for other computers to mount as a virtual drive. However make sure that you detach a VHD before performing any copy or move operations on it - see further below for details.

To create a new VHD image of an existing drive, use the Disk2VHD utility mentioned earlier. To create a VHD from an existing file in the Virtual Machine Disk (VMDK) format use the free V2V Converter.

While computers running Windows 7 and 8 have native support for the .VHD format, and only Windows 8 natively supports .VHDX, PCs running Windows XP or Vista can use the Microsoft Virtual PC software to mount these .VHD files.

MOUNTING AND DETACHING A VHD

If you use the steps above to create a new .VHD or .VHDX file, it will automatically be mounted, which means it is automatically detected as a connected drive by Windows. To simulate the removal of this physical drive from your system, you must detach it. This is done as follows:

1. Open Administrative Tools in the Windows Control Panel and select Computer Management.
2. In Computer Management, select the Disk Management component.
3. Right-click on the name of the disk in the bottom pane of Disk Management (e.g. right-click on 'Disk 2') and select 'Detach VHD'.
4. Confirm the location of the file and click OK to detach the .VHD file as a drive on your system.

Detaching a .VHD or .VHDX file will not delete it, it will simply tell Windows that the file is no longer "connected" as a physical drive, hence it won't be shown in the Drive Management window or in File Explorer. You should always detach a .VHD or .VHDX file before moving it to another location.

To reattach or mount an existing .VHD or .VHDX file at any time, do the following:

1. Open Administrative Tools in the Windows Control Panel and select Computer Management.
2. In Computer Management, select the Disk Management component.
3. Under the Action menu in Disk Management select 'Attach VHD'.
4. Browse to the location of the .VHD or .VHDX file and click OK.
5. The .VHD or .VHDX file will be mounted as the type of drive the file image was originally saved as, and will already be ready to use with its existing data, so there is no need to initialize, format or partition it again.

ACCESSING A SYSTEM IMAGE BACKUP VHD

One of the most useful ways to utilize the VHD support in Windows 8 is to mount a full system image backup created using Windows 7 File Recovery. As covered in the Backup & Recovery chapter, normally when a system image backup of your entire drive is created, it cannot be accessed to restore individual files or folders; it must be restored in its entirety on a physical drive, overwriting all existing information on that drive. However the system image backup is actually created as a .VHD file, so it can be mounted as a separate drive using the steps covered earlier, allowing you to access the contents of your system image and browse and copy individual files and folders using File Explorer without deleting the existing contents of your drive.

Mount the system image backup using the same procedures to mount a VHD as covered further above. This time, I strongly recommend that under Step 4 of the process, you tick the 'Read-only' box before mounting your system image backup, because any modification to this system image can prevent you from using it in the future as part of the Windows backup feature. Also, when you are finished using the system image VHD, make sure to right-click on the disk and detach it without deleting the file as covered further above.

< HYPER-V

Windows 8 introduces built-in support for Hyper-V, which is a virtualization platform that allows users to run other operating system(s) as guest OSes in a virtual environment within Windows 8. This is mainly for use by network administrators or software developers, however it can be useful for home users, especially given Windows 8 removes support for Windows XP Mode. This means that you can instead use Hyper-V to run a virtual installation of Windows XP for example, as long as you have a fully licensed copy of Windows XP available to install in this manner.

To run Hyper-V you will need to have a 64-bit capable system and 64-bit Windows 8 Pro or Enterprise, along with a PC that has support for Intel VT or AMD-V hardware virtualization features. Hyper-V is disabled by default in Windows 8, so to enable it you must follow these steps:

1. Open the Programs and Features component of the Windows Control Panel.
2. Select 'Turn Windows features on or off' on the left side.
3. In the window that opens, tick the Hyper-V box in the list shown and click OK.
4. You will need to reboot your system at least once to install the required components.

Once enabled, the Hyper-V Manager can be accessed by typing *hyper-v* on the Start Screen and pressing Enter, or clicking the new Hyper-V Manager icon that appears on the Start Screen. When Hyper-V Manager opens, you must create a new virtual PC (Virtual Machine) on which to install and run your desired OS. Do this by left-clicking on your username in the left pane, then selecting 'New>Virtual Machine' under the Actions menu. From this point onward, the New Virtual Machine Wizard should provide sufficient guidance.

In practice, the average home PC user does not need to enable Hyper-V or create a Virtual Machine, particularly as it will be slower than running an OS on a physical PC given the virtualization overheads. Its primary use is for corporate users or software developers who need to test software out in a range of different environments, or are running old software that does not run properly in compatibility mode under Windows 8, and hence requires a fully virtualized copy of the original OS on which to operate.

< RAM DRIVE

A RAM Drive is a not a physical drive, it is a portion of your system RAM which has been converted into a virtual disk drive. The primary benefit of a RAM drive is that it is as fast as your system memory in terms of data access, which is faster than any normal hard drive or flash-based SSD. The down side is that a RAM drive can only function when the system is on; when it is off, the contents of the RAM drive will either be lost, or must be saved to your drive before or during shutdown, and reloaded at startup, which can slow down startup and shutdown times.

To set up a RAM drive on your system, you will need use a program designed to perform this task, such as RAMDisk. Once installed, run the RAMDisk Configuration Utility and under the Settings tab you can select how much RAM to allocate to the RAM drive - note that the free version of RAMDisk only allows up to 4GB (4096MB) of memory to be used in this manner. Remember that the amount you set aside for the RAM drive cannot be used by your system for other purposes while the RAM drive is in operation, so don't assign a large portion of your RAM unless you have plenty to spare. For the formatting of the drive, select Unformatted as it will need to be formatted in NTFS as covered further below.

Under the Load/Save tab you can make the data stored in the RAM drive permanent by ticking the 'Load Disk Image at Startup' box, as well as the 'Save Disk Image at Shutdown' box. These are necessary if you are going to install a program to the RAM drive, or save any non-temporary data onto it, but this will increase shutdown and startup times depending on the size of your RAM drive. The actual image file(s) saved during shutdown and loaded at startup are shown in the boxes below these options - change their names and locations if you wish.

If you only want a RAM drive for use as a temporary cache by other programs in each Windows session on the other hand, untick the Load and Save boxes above and instead tick the 'Create Temp directory' box. Anything stored on such a RAM drive configuration will be lost each time you shut down your PC, which is fine for temporary files as they typically need to be purged at shutdown anyway.

When ready, click the 'Start RAMDisk' button, accept the prompt to install the device driver necessary for this functionality, and either the image files or a temporary RAM drive will be created depending on your options. The RAM drive is not ready to be used yet, it needs to be mounted and formatted in Windows. Close the RAMDisk Configuration Utility, and follow these steps:

1. Open Administrative Tools in the Windows Control Panel and select Computer Management.
2. In Computer Management, select the Disk Management component.
3. You will find a new disk here which is equivalent in size to the amount of memory you allocated to the RAM disk.
4. Right-click on its name (e.g. right-click on Disk 2) and select 'Initialize Disk' then click OK.
5. Right-click on the disk space (showing size and Unallocated) and select 'New Simple Volume', then follow the prompts.
6. Format the drive in NTFS with a Default allocation size, give it an appropriate label (e.g. RAM Drive), and tick the 'Perform a quick format' box, then click Next.
7. Click Finish to commence the format.

When complete, Windows will detect a new drive with the volume name and letter you have assigned it, and it can now be used like a normal physical drive. You will see it under the Computer category in the Navigation Pane in File Explorer, and depending on whether it is a temporary or permanent RAM drive, you can use it accordingly. Anything stored here will be extremely fast to load.

To remove this RAM drive at any time, open the RAMDisk Configuration Utility and click the 'Stop RAMDisk' button. The drive will disappear from Windows. Uninstall RAMDisk if you want to remove the driver it has installed, and manually delete any .IMG files you created to permanently remove the RAM drive contents from your system.

While the RAMDisk utility is easy to use, it is only free for RAM sizes up to 4GB. ImDisk is a completely free RAM Drive alternative, but is much more complex to set up.

< DISK MANAGEMENT

Disk Management is a sub-component of the Computer Management component of the Administrative Tools, which can be accessed in the Windows Control Panel. You can also directly access Disk Management by typing *diskmgmt.msc* on the Start Screen and pressing Enter.

Once open, you will see all of your connected and detected logical drive(s) listed in the top pane of Disk Management, with more details on each available drive listed in the bottom pane. Some common tasks you can do with Disk Management include:

Changing Drive Letters: If you want to change any of the drive letters on your system - for example if you want to alter your DVD ROM drive from being called D: to F: or if you wish to change a hard drive letter from C: to J: you can do so here by right-clicking on the drive letter in the top pane and selecting 'Change Drive Letter and Paths'. Highlight the drive letter that appears, click the Change button, and select a new drive letter in the drop-down box. Note that you cannot the drive letter of the system drive under certain circumstances.

Partitioning: A Partition is a logical subdivision of your drive. To create a new partition on any drive, you will first need to have some Unallocated Space, which is not the same as free drive space. In most cases there will not be any unallocated space since your existing partition(s) will be taking up all available space. You can create unallocated space by using the Shrink function, which reduces one of your partitions and in return creates an equal amount of unallocated space. Right-click on the drive and select 'Shrink Volume' if you wish to do this, then enter the amount of unallocated space you wish to create. Once you have some unallocated space, you can right-click on it in the bottom pane and select 'New Simple Volume' to create a new partition, and follow the Wizard to choose a size for it. You can also format an existing partition, which destroys all data currently on it and prepares it for use. If you want to create more than three partitions, you will have to create an Extended partition within an existing partition. For more details on partitions see the Partitioning section under the Windows Installation chapter.

System Reserved Partition: If you see a 350MB System Reserved partition in Disk Management, this is a hidden partition with no assigned drive letter created automatically during Windows installation. I do not recommend attempting to remove or alter this partition, as aside from being required for BitLocker and System Recovery features, it also contains all of your boot files, and removing it can make Windows 8 unbootable. It does no harm if it has already been created. See the Installing Windows section of the Windows Installation chapter for more details.

Basic and Dynamic Disks: All of your drives are formatted as a Basic disk with partition(s) as necessary. However if you wish, you can format them as a Dynamic Disk by right-clicking on the relevant drive name in the bottom pane and selecting 'Convert to Dynamic Disk'. Dynamic disks can emulate a RAID array - that is they can span multiple drives as though they are one large drive, and they do not use partitions. The features of Dynamic Disks are discussed in this Microsoft Article. It is not recommended that the average home PC user convert a disk from Basic to Dynamic, particularly as you cannot reverse the process without losing all of your data, so it is not worth experimenting with. The new Storage Spaces feature in Windows 8 is more appropriate if you want to merge multiple drives into a single drive - see the Preparing the Drive section of the Windows Installation chapter. You should only use the Dynamic Disk option if you have specific needs which you know will require this function, such as holding very large databases. Furthermore, you should only do so if you are an advanced user. Note that this function is only available on Windows 8 Pro or Enterprise editions.

Virtual Hard Disk: There are a range of features for VHDs available in the Disk Management component - see the Virtual Hard Disk section earlier in this chapter for details.

< DISK DIAGNOSTICS

By hourly checking data from a drive's Self Monitoring, Analysis, Reporting Technology (SMART) feature, the built-in Windows Disk Diagnostics feature can detect if there are going to be potential drive errors or a drive failure in the near future, and either take steps to rectify it, or warn the user in advance, also providing a prompt to begin backup of your data before it is potentially lost. For this feature to work, SMART must be enabled in your BIOS/UEFI and supported by your drive. Note that certain drive setups such as RAID configurations or USB connected drives may not allow SMART functionality.

If you want to manually check the SMART information yourself at any time to see your drive's health, use one of the methods below:

HD Tune: The free version of the HD Tune utility has a Health tab under which you can see whether your drive(s) have any problems as reported by SMART.

PassMark: The free PassMark Disk Checkup utility shows SMART information for a drive by selecting that drive under the Physical Devices list at the top of the DiskCheckup window, then looking under the SMART Info tab and looking at the Status column.

If you wish to disable the Disk Diagnostics functionality, you will need to access it through the Local Group Policy Editor if it is available to you - see the Group Policy chapter for details. This feature is found under the Computer Configuration>Administrative Templates>System>Troubleshooting and Diagnostics section. Select the Disk Diagnostic component in the left pane and in the right pane double-click on the 'Disk Diagnostic: Configure Execution Level' item. By default it is set to Not Configured, which enables this functionality. You can set it to Disabled which will remove the prompting behavior and only log detected errors. It is not recommended that you disable or alter this functionality.

Although this feature is extremely useful, you may not get sufficient warning before drive failure occurs, and any initial failure may be catastrophic enough to render some or all of your data unreadable. Some drives, such as SSDs, can fail in such a manner as to suddenly become completely unusable without any warning. Disk Diagnostics is not a replacement for making regular backups as covered in the Backup & Recovery chapter.

CHECK DISK

One important area related to drive health is the health of the file system. In Windows 8, improvements have been made to the NTFS health model as detailed in this Microsoft Article. These changes mean that if Windows detects any file system corruption, as before, it will automatically initiate self-healing of the issue without any user action. If the problem persists, a spot verification of the issue, then a scan during idle periods to identify and log it, will occur. Then, only if problems still continue to be detected, the user will be prompted to 'Scan drive for errors', or 'Restart to repair drive errors', which will run the Check Disk utility to correct them.

The changes mean that there is no need to manually initiate a Check Disk unless you are experiencing major system issues. You can still run the Check Disk utility at any time to manually scan for errors, but the utility has changed from previous versions of Windows.

To check your drive for general errors such as bad sectors or corrupted indexes, you can access Windows Check Disk utility as follows:

1. Go to the Computer category in File Explorer, or open on the Computer item in Start Menu.
2. Right-click on your drive name and select Properties.
3. Under the Tools tab, click the Check button to launch Windows Check Disk.
4. Click the 'Scan drive' option - this conducts a scan of your drive within Windows, without requiring a reboot.
5. If the scan does not encounter any problems, you will be informed that it was completed without any errors.
6. If the scan does find problems, or if you are accessing Check Disk due to prompts regarding drive errors, you will be able to select the 'Repair drive' option instead, which will attempt to fix the issues, and may need to restart your system to complete repairs.

To run a version of Check Disk that is similar in output to that found in earlier versions of Windows, and in particular, allows you to force a repair, do the following:

1. Open an Administrator Command Prompt.
2. Type the following and press Enter:

   ```
   chkdsk [drive letter]
   ```

   e.g. chkdsk C:
3. This will run a full check disk on the selected drive, reporting the progress and any problems found in particular areas in more detail.
4. You can force a detailed scan followed by an automatic repair attempt by typing the following and pressing Enter:

   ```
   chkdsk [drive letter] /F
   ```

   e.g. chkdsk C: /F
5. If running a full scan and repair in this manner on the current system drive, you will be prompted to schedule the disk check for the next reboot. Type Y and press Enter, then reboot to allow this full scan and repair attempt to run properly and correct the errors.

If there are errors on the drive, and a full Check Disk repair still does not appear to fix them, then in the first instance you should attempt to backup all of your data to a separate source, then do a full reformat of the drive. If problems continue, then the drive may be physically faulty, and will need to be replaced.

< DRIVE CONTROLLERS

One of the key determinants of your drive performance is the type of drive controller it is using. The most common drive controllers are for the IDE and SATA interfaces - see the Storage Drives section of the Basic PC Terminology chapter for more details. To ensure that your controllers are set up correctly and configured for optimal performance in Windows, follow the steps below.

First, make sure that you have installed the latest drivers for your particular motherboard, as the drive controllers on your motherboard require these drivers for optimal operation, as well as for special functions like AHCI or RAID. See the Driver Installation section of the Windows Drivers chapter for more details. Open Device Manager in the Windows Control Panel, and expand the Disk Drives section. Your drive(s) should all be listed here and correctly identified. If they are not, check your BIOS/UEFI to ensure that you have enabled the relevant controllers and that the drives are all being correctly detected there - see the Hardware Management chapter.

Now right-click on each drive in Device Manager and select Properties. Under the Policies tab, you will see some or all of the following options:

Quick Removal or Better Performance: The 'Better performance' option should be selected for maximum performance, unless you actually need to remove this drive frequently. If the 'Better Performance' option is selected, you will need to click the 'Safely Remove Hardware' icon in your Notification Area before disconnecting the drive to ensure that you don't experience any data corruption or loss. As such, if the drive is a removable one, such as an external USB drive that you frequently connect to the PC, then select 'Quick Removal' instead so that you can quickly and easily remove it when desired without any additional steps or risks to the data it contains.

Enable Write Caching on the Device: Write caching uses the drive's cache memory to temporarily store writes to your drive before they are actually written permanently to the drive. This allows the drive to write faster, since writing to the cache is quicker than writing directly to the drive. However if there is a power failure,

any data in the cache may be lost before being committed to the drive. The risks are quite low, so this option should be ticked for maximum performance.

Turn Off Windows Write-Cache Buffer Flushing On the Device: By default Windows flushes (empties) the write cache buffer periodically. If this option is ticked, that feature is disabled, which can further increase performance. Again, the risk is that if any there is any sudden interruption to the power supply to your drive, or any other hardware issues, you may lose or corrupt any data that was held in the Write Cache but not yet written to the drive.

I recommend ticking both of the above options to ensure maximum performance from your drive. If you have an unreliable supply of power in your area, or you don't want to risk potential data loss under any circumstances, untick these options at the cost of some performance. A better alternative is to keep these options enabled and invest in an Uninterruptible Power Supply (UPS), as covered in the Hardware Management chapter. A UPS will maintain power to your PC during a power outage, giving you sufficient time to save your work and exit Windows properly without any risk of sudden data loss.

Next, go to the 'IDE ATA/ATAPI Controllers' or 'SCSI and RAID Controllers' section in Device Manager and expand it. Right-click on any sub-controllers listed, select Properties for each and see the relevant section below as applicable. The information below covers the most common options, however what you see on your system may vary depending on your motherboard drivers and hardware configuration - in some cases some of the options below may not be available:

IDE Channel / ATA Channel: This controller affects all PATA drives which use the IDE interface - typically this is older hard drives, or SATA drives specifically configured to run in legacy IDE mode in the BIOS/UEFI. You may also see this section if you have SATA drive(s) configured for AHCI, but have not installed the appropriate drivers for your motherboard - e.g. Intel Rapid Storage Technology drivers for AHCI drives on Intel motherboards. See the Windows Drivers chapter to determine the full range of drivers you need for your motherboard features to work correctly.

Go to the 'Advanced Settings' tab and at the bottom make sure 'Enable DMA' is ticked for optimal performance. In the Devices box you will also see what mode any attached IDE drive(s) are running under. The maximum speeds shown here are typically Ultra DMA Mode 4 for optical drives, and Ultra DMA Mode 6 for IDE drives. Use a tool like HD Tune to check your actual drive mode. Look under the Info tab at the bottom to see the active UDMA mode for each drive.

You cannot alter the drive speed under the controller section here, but if it is below the maximum then it may be due to one or more of the following factors which you should troubleshoot:

- Check your motherboard manual for the various drive configuration details, and also make sure that you have installed the correct drivers for this motherboard - see the Windows Drivers chapter.
- Your BIOS/UEFI is not configured correctly to enable the highest speed - see the Hardware Management chapter.
- You are sharing a hard drive/SSD with an optical drive on the same channel - move any optical drive(s) to a separate channel of their own where possible.
- Your hardware doesn't physically support the highest transfer mode available. This should only be the case if the motherboard and/or the drive are very old.
- No drive should be running in PIO or Multi-word DMA mode as these provide poor performance, so if this is the case, check your BIOS/UEFI settings and also any physical switches on the back of the drive(s).

Standard SATA Controller: This affects all drives connected to the SATA controllers on your motherboard. Right-click on this controller, select Properties, then go to the 'Primary Channel' and 'Secondary Channel' (or 'Port 0' and 'Port 1') tabs if they are available.

Selecting AHCI mode under the drive configuration in your BIOS/UEFI is generally the best choice for most users, as it is native to SATA drives, and is covered below:

AHCI Mode: If you run a SATA-based drive, you can enable Advanced Host Controller Interface (AHCI) mode on your SATA controller in your BIOS/UEFI. This mode has a range of benefits, especially on SATA II or newer hard drives and SSDs with NCQ support - this includes quieter operation on hard drives, and better multi-tasking capabilities. However it may or may not result in a speed boost. Furthermore it requires appropriate drivers from your motherboard manufacturer to function properly. Most importantly, if you do not enable this mode in your BIOS/UEFI prior to installing Windows, you may experience an error and may not be able to boot back into Windows if you switch to AHCI from IDE mode or vice versa. If you switch an existing installation of Windows from IDE to AHCI mode, follow these steps:

1. Check to make sure that AHCI mode is selectable for your drive in the BIOS/UEFI, but do not change to AHCI mode just yet.
2. Open the Registry Editor, and go to the following location:

   ```
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\storahci]
   Start=0
   ```

3. Change the above value to 0, and close Registry Editor.
4. Reboot your system and go directly into your BIOS/UEFI.
5. Enable AHCI mode for your drives.
6. Reboot into Windows.

You can also usually select a RAID mode in the BIOS/UEFI, but this is only necessary if you actually have a RAID drive configuration; that is, two or more drives set up to operate in RAID mode. See the Preparing the Drive section of the Windows Installation chapter for more details on RAID.

To test your drive's actual speeds at any time, you can run a drive benchmark, or even the built-in Windows Experience Index. Drive benchmarks are artificial and not necessarily indicative of real-world performance. They are best used only as an indication of relative performance, such as whether your performance has significantly improved or degraded after making a change, or to compare with other users of the same drive. See the Performance Measurement & Troubleshooting chapter for details on drive benchmarking programs.

< AUTOPLAY

Related to drives, whenever you insert a particular type of media such as an audio CD or a movie DVD, or connect a device such as a USB flash drive, Windows detects the type of device or media and can automatically undertake a specific action, such as opening a multimedia file in Windows Media Player. Alternatively, Windows can simply prompt you as to the types of actions you can undertake with the media or device. This functionality is called AutoPlay.

Note that when certain devices such as portable music players, cameras and phones are connected, instead of AutoPlay, Windows will automatically open Device Stage, which provides greater functionality. See the Device Stage section of the Hardware Management chapter for more details.

There is also an associated feature in Windows called AutoRun (not to be confused with the Autoruns utility) which only relates to the automatic launching of programs on inserted or attached media. The key difference is that AutoRun presents a potential security risk, since the automatic launching of any malware programs contained on an external storage device for example is obviously not desirable. For this reason, as of Windows 7, the AutoPlay behavior was changed such that AutoRun will not work for non-optical

removable media. For example, if you attach a USB flash drive, it will provide you with an AutoPlay prompt as normal asking whether you want to browse files and folders, or use the device for ReadyBoost, but it will not automatically launch any program which is on that drive, nor will there be any option to launch a program on that device from the AutoPlay prompt.

If you insert a CD or DVD, Windows will open AutoPlay as normal, but in the case of discs designed to install a program, you will see a notification prompt requesting the launching of a program. If you are using a legitimately purchased retail disc, or a disc you created from a trusted downloaded image, then the risk of malware should be minimal. If you did not expect to be installing a program from the disc, then cancel any such prompts and research further.

In any case, you can customize all AutoPlay and AutoRun behavior by going to the AutoPlay component of the Windows Control Panel and setting Windows 8's default behavior for each and every type of media or device that can be attached to your system. For example, you can set the 'Software and games' component to 'Open folder to view files (File Explorer)', providing greater protection against automatically installing malware. Then when a software DVD is inserted, Windows will simply open File Explorer with a focus on the optical drive where the software disc resides without prompting you, and you can then manually find and launch the setup executable. This is recommended for more advanced users who desire greater security.

Go through and set your desired AutoPlay action for each and every type of file, media, or device, and if in doubt, select the 'Take no action' setting to prevent an AutoPlay or AutoRun prompt from appearing. If you wish to disable AutoPlay functionality altogether, untick the 'Use AutoPlay for all media and devices' box at the top of the AutoPlay window and click Save.

Even if you have disabled AutoPlay for a particular media or device type, you can still manually trigger the AutoPlay notification window at any time by opening File Explorer, right-clicking on the drive with the inserted media under the Computer category, then selecting 'Open AutoPlay'.

< MASTER FILE TABLE

The Master File Table (MFT) is a system area of Windows that NTFS uses to hold an entry for every file and directory on your drive. The information held in the MFT includes data on file size, attributes, permissions, timestamps and so forth. It is like a table of contents for your drive, and as such serves a very important function. Windows automatically manages the MFT, increasing its size as necessary. It initially reserves a 200MB zone of drive space for the MFT to prevent fragmentation, and this allocation grows as new files are added to the drive. If your drive becomes full, Windows allows your data to overwrite any reserved MFT space which is not actually being used by the MFT, so the space is not wasted.

To examine MFT information in more detail, you can use the free NTFSInfo utility:

1. Download and extract the *ntfsinfo.exe* file.
2. Copy the file to your *\Windows\System32* directory
3. Open an Administrator Command Prompt.
4. At the prompt, type the following:

   ```
   ntfsinfo [drive letter]
   ```

   e.g. ntfsinfo C:
5. Look under the MFT Information section of the displayed information to see current MFT size, and the MFT zone size.

If you wish to display the location of the MFT in graphical form, you can use the free Defraggler utility. Install the utility and launch it, then select the 'Drive Map' tab. Click the Analyze button to refresh the drive

map display, and then click the 'Reserved MFT Space' item under the Color box to highlight the location and size of the reserved MFT zone on your selected drive.

It is possible to manually control the amount of space Windows reserves for the MFT as it grows. You can do so by going to the following location in the Registry:

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]

NtfsMftZoneReservation=0
```

The DWORD above is set to 0 by default, which means it is being automatically managed by Windows and will increase as required - this is strongly recommended. However you can change the value above to be between 1 and 4 inclusive, which implements a multiplier for the MFT reservation, with 1=200MB, 2=400MB, 3=600MB, and 4=800MB. For example, if the above value is set to 4, the MFT reserved zone will rise in 800MB increments whenever required.

As of Windows Vista onwards the MFT is automatically managed and does not need any user input or adjustment. However, it is important to regularly defragment hard drives to ensure that the MFT doesn't become fragmented over time and thus degrade drive performance.

< OPTIMIZE DRIVES

As data is written to and deleted from your hard drive, portions of individual files will become fragmented and physically spread out all over the drive. This happens because as Windows starts writing the data for a new or updated file onto the drive, when it reaches an occupied portion of the drive it jumps to the next available empty spot and continues writing from there. So a single large file may actually be in many separate chunks, in various locations on your drive. The more the files on your system are fragmented, and in particular, the smaller the fragments, the more time your drive takes to find all of these fragments and access all the information it needs at any time. It's like trying to read a book with the pages out of order. This can clearly reduce hard drive performance and increase the potential for stuttering and loading pauses when accessing data.

Sold state drives are not affected by fragmentation, as they do not read files in the same sequential manner that a physically spinning hard drive does. As such, so long as Windows gives the TRIM command and the SSD's own firmware-based wear management is operating correctly, files will be allocated optimally throughout the SSD without any need for defragmentation. Indeed defragmenting an SSD will simply cause unnecessary use of write cycles for no real benefit. If any defragmentation utility reports that an SSD is fragmented, it can be safely ignored.

To address fragmentation on hard drives, in the past Windows incorporated the Windows Disk Defragmenter utility, also known as Defrag. However, in recognition of the fact that SSDs are now in wide usage, and that there is a fundamental difference between hard drives and SSDs, Windows 8 has renamed and retasked the Defrag utility, calling it Optimize Drives.

To access the Optimize Drives utility, open File Explorer, go the Computer category, right-click on the relevant drive and select Properties, then look under the Tools tab and click the Optimize button. Alternatively, go to the Start Screen, type *dfrgui* and press Enter.

The Optimize Drives utility works on both hard drives and SSDs, but in different ways:

Hard Disk Drives: Selecting a hard drive and clicking the Optimize button will conduct a defragmentation, which includes defragmenting system files like the Master File Table and NTFS metadata, and consolidating free space.

Solid State Drives: Selecting an SSD and clicking the Optimize button will send TRIM commands to the SSD. In practice an SSD will be already be utilizing TRIM hints on the fly during normal usage, given Windows 8 has native TRIM support. However, under certain circumstances the drive may not have the opportunity to implement these TRIM operations, and may reschedule or even discard them. Running Optimize Drives gives the SSD the opportunity to optimize the entire drive using TRIM in one go, doing a full cleanup which it may not otherwise be able to do during normal usage.

The Optimize Drives utility will detect the type of drive(s) you are using and automatically utilize the appropriate method on each, as they are incompatible with each other. You can also select multiple drives at the same time and click Optimize All to allow the utility to optimize them all as required.

As with the Defrag utility in Windows 7 and Vista, there is no graphical representation of the drive map, or any visual representation of how the drive optimization is occurring in Optimize Drives. Instead, you are provided with two indicators: the first shows the percentage of fragmentation or the requirement for optimization on each drive, which you can refresh by highlighting the drive and clicking the Analyze button. The second is a Progress indicator which shows the proportion of the current pass the defragmentation is currently on, or the percentage of the drive which has been trimmed. For hard drive defragmentation, depending on the amount and type of fragmentation, Disk Defragmenter will typically do multiple passes, and some may take quite a while to complete.

Regardless of whether you have a hard drive or SSD, by default Optimize Drives is scheduled for a weekly run. You can edit this schedule by clicking the 'Change Settings' button at the bottom of Optimize Drives, and altering the frequency and/or the drives on which the optimization will run. While a scheduled run can be left enabled for those who are forgetful, in practice running a drive optimization should not be done on any fixed basis. On both an HDD and an SSD, the frequency of optimization required actually has more to do with the number and size of file changes to the drive. As such, I recommend running manual optimization of your drive(s) immediately after any of the following events:

- Installation of any major program, especially drive-intensive applications such as games or benchmarks.
- Installation of any drivers.
- Patching any program or running Windows Update.
- Adding or deleting very large, or numerous, file(s) or folder(s).

Defragmentation is particularly necessary for gamers using hard drives, since games are already quite prone to stuttering and longer loading times due to their data-intensive nature. By defragmenting your hard drive after a game installation or after patching a game, you can significantly reduce any in-game stuttering.

ADVANCED DEFRAGMENTATION

If you want greater control and feedback from the Windows Disk Defragmenter, you can use the `Defrag` command line option. Start an Administrator Command Prompt and then type `Defrag /?` for a list of commands.

For example, to run a defragmentation on two available hard drives C: and D: simultaneously at normal priority and with free space consolidation, open an Administrator Command Prompt and type:

```
Defrag C: D: /M /X /H
```

If you have specialized needs, or if you desire a graphical representation of fragmentation as part of your defragmentation utility, then there are several advanced defragmentation utilities you can use. For utilities that are free, I recommend one of the following:

Defraggler
Auslogics Disk Defrag

There are several commercial defragmentation packages which all have a free trial version you can use for a limited period, but ultimately require eventual purchase. Of these, I recommend:

Diskeeper
PerfectDisk
O&O Defrag

In general I don't see a pressing need to use a third party defragmentation tool of any kind in Windows 8. The third party defragmentation packages above may or may not provide marginally improved drive performance as a result of more advanced defragmentation or additional features, but this has to be balanced with the fact that the built-in Optimize Drives utility is free and easy to use, and gives you the most significant benefits of defragmentation/TRIM optimization with no background resource usage.

Regardless of whether you use the built-in utility or a third party one, make sure to defragment your hard drives and TRIM optimize your SSDs regularly, as it is essential to maintaining smooth performance.

WINDOWS CONTROL PANEL

This section runs through all of the general options available under the Windows Control Panel, which is an important central location for accessing most of the settings in Windows. Under Windows 8 some additional settings are now separately contained under the Settings section of the Charms menu, and these are covered in the PC Settings chapter.

The Windows Control Panel can be accessed in several ways: by typing *control panel* on the Start Screen and pressing Enter; by right-clicking in an empty area of the Start Screen, selecting 'All Apps', and clicking the 'Control Panel' icon under the 'Windows System' category; by opening the Charms menu, selecting settings and then clicking on 'Control Panel'; or by right-clicking in the lower left corner of the Desktop and selecting 'Control Panel'.

Most of the important Windows settings relevant to the average home PC user can be accessed through the Windows Control Panel, but the vast majority of these settings and features are already covered in detail in the various chapters throughout this book, so this chapter primarily contains references to other chapters. There are a few features and settings which do not fit neatly into any other chapter, and hence are covered here in more detail. By making sure that you systematically go through all of the components of Windows Control Panel one by one, along with those under the PC Settings chapter, you will in effect have configured all of the important Windows settings.

Importantly, it is assumed throughout this book that Windows Control Panel is being viewed using one of the Icons view options, as this provides direct access to all of the individual components available. To switch to this view if you haven't already, open Windows Control Panel and in the top right corner select either 'Large icons' or 'Small icons'. Only the default Windows Control Panel components are covered in this chapter, not those installed by third parties. Further, some features may be unavailable in the Windows 8 core edition as opposed to Windows 8 Pro or Enterprise.

< CUSTOMIZING WINDOWS CONTROL PANEL

Third party applications can install Control Panel components that may be undesirable, particularly as they can add clutter to the Windows Control Panel. This section provides methods for finding and removing any such components from the Control Panel interface. These methods do not uninstall or otherwise harm the functionality associated with the components, they simply prevent them from being displayed in Windows Control Panel.

The easiest method to hide any Windows Control Panel item, whether a default Windows component, or one installed by a third party program, is to use the Local Group Policy Editor. See the Hide Specific Control Panel Items tip in the Group Policy chapter.

If you do not have access to the Group Policy Editor, or want a simpler method, there are other ways of removing Windows Control Panel items. Many third party applications install their components as .CPL files, which are small applications designed to run within the Windows Control Panel. Removing the relevant .CPL file will remove that component's icon from Windows Control Panel. You can find these .CPL files typically stored under the *\Windows\System32* or *\Windows\SysWOW64* folders on your drive, or in the program's own directories. If you can't readily find the relevant .CPL file, initiate a system-wide search for all .CPL files - see the Windows Search chapter for details. Also refer to the list of common third party .CPL files in this Wikipedia Article.

Once the relevant .CPL file is found, close the Windows Control Panel, temporarily delete the suspected .CPL file to the Recycle Bin, re-open Windows Control Panel and if you removed the correct file, the component should no longer be visible.

You can also check the Windows Registry for Windows Control Panel components. Go to the following locations in the Registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\Cpls]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace]
```

The keys and values located beneath these subfolders contain entries relating to Windows Control Panel components, both third party and default Windows components. Remember that deleting a Registry entry cannot be undone, so make sure you create a backup of the relevant branch of the Registry as covered in the Windows Registry chapter before deleting anything. You may have to restart Windows, or logoff and logon, to see the changes reflected in the Windows Control Panel.

Finally, given Windows Control Panel is a component that is frequently used, you may wish to create a Desktop shortcut, a Start Screen shortcut, or pin it to the Taskbar for quicker access.

To create a Desktop shortcut to Windows Control Panel, do the following:

1. Right-click on an empty area of the Windows Desktop.
2. Select New>Shortcut.
3. In the location box, enter the following:

   ```
   C:\Windows\System32\control.exe
   ```

   Note: substitute your drive letter in place of C: above if it is different.
4. Click Next, and enter a suitable name such as Control Panel, then click Finish

To create a pinned Start Screen or Taskbar icon for the Windows Control Panel, do the following:

1. Type *control panel* on the Start Screen.
2. Right-click on the 'Control Panel' item which appears.
3. Select 'Pin to Start' if you want a 'Control Panel' shortcut pinned to your Start Screen.
4. Select 'Pin to Taskbar' if you want a 'Control Panel' icon pinned to the Taskbar on your Desktop.

Remember that it is also available for easy access under the Power User Tasks Menu, found by right-clicking in the lower left corner of the screen in either the Metro or Desktop environments.

The remainder of this chapter covers the individual Windows Control Panel components.

< ACTION CENTER

The Windows Action Center is a central location for Windows to provide a range of alerts, and for users to quickly access a range of important security and maintenance features. The Security section of the Action Center is covered in the Windows Action Center section of the Security chapter, and the Maintenance section of Action Center is covered in the Windows Action Center section of the Performance Measurement & Troubleshooting chapter.

< ADD FEATURES TO WINDOWS 8

Add Features to Windows 8 is the Windows 8 replacement for the Windows Anytime Upgrade feature in previous versions of Windows. It is covered in this Microsoft Article. This feature lets you change your version of Windows 8 or add features in-place without needing to do a reinstall.

You can obtain additional features for your installation of Windows 8, either by purchasing a product key for an upgrade pack, or by entering a product key you have obtained elsewhere to unlock an upgrade. To see the features available to be purchased and installed on your current edition of Windows, click the 'I want to buy a product key online' option. The two most common feature packs available are:

§ The Windows 8 Pro Pack allows Windows 8 core users to purchase an upgrade to Windows 8 Pro, which provides a range of additional features that are covered in more detail under the Choosing a Product Edition section of the Windows Installation chapter. The Pro pack also contains Windows Media Center.
§ The Windows 8 Media Center Pack, initially available as a free download until the end of January 2013, and subsequently must be purchased, requires Windows 8 Pro before becoming available. It adds the Windows Media Center feature, which also contains DVD playback support. See the DVD and Blu-ray Playback section of the Windows Media Player chapter for more details.

Alternatively, if you have purchased a product key from another source, or already have one from a previous installation of Windows 8, then click the 'I already have a product key' option and enter the key on the next screen.

< ADMINISTRATIVE TOOLS

The Administrative Tools are a range of utilities for access to the advanced configuration and monitoring features of Windows. They are primarily designed for System Administrators, so some of the utilities and functions are not of any use to the average home PC user. However I provide details of the main Administrative Tools and point out their most useful aspects below:

COMPONENT SERVICES

This utility allows you to configure and administer Component Object Model (COM) components. The tool is designed for software developers and network administrators, and is not covered in this book.

COMPUTER MANAGEMENT

This utility provides access to several highly useful system management tools including Disk Management, Event Viewer, Task Scheduler, Device Manager, Performance Monitor and Services - see the relevant sections throughout this book for more details on each of these.

DEFRAGMENT AND OPTIMIZE DRIVES

This opens the Optimize Drives utility, which is covered in detail under the Optimize Drives section of the Drive Optimization chapter.

DISK CLEAN-UP

This opens the Disk Clean-up utility, which is covered in detail under the Disk Clean-up section of the Cleaning Windows chapter.

EVENT VIEWER

This opens the Event Viewer utility, which is covered in detail under the Event Viewer section of the Performance Measurement & Troubleshooting chapter.

HYPER-V MANAGER

If the Hyper-V feature is enabled, this opens the Hyper-V Manager, which is covered in more detail under the Hyper-V section of the Drive Optimization chapter.

ISCSI INITIATOR

The iSCSI Initiator is a management interface for iSCSI devices. These devices can be disks, tapes or other storage components which are connected to a network. The iSCSI Initiator manages the connection and control of these target devices. It is mainly used for remote storage over a network, and is not covered in more detail in this book.

LOCAL SECURITY POLICY

This opens the Local Security Policy tool, which is covered in more detail under the Local Security Policy section of the Security chapter.

ODBC DATA SOURCES

This tool lets you add and configure drivers for managing access to data on various database management systems. Unless you use databases extensively on your machine, you can ignore this tool as it is not relevant to the average home PC user, and is not covered in more detail in this book.

PERFORMANCE MONITOR

This opens the Performance Monitor tool, which is covered in more detail under the Performance Monitor section of the Performance Measurement & Troubleshooting chapter.

PRINT MANAGEMENT

This tool allows you to manager print servers and printers connected to the PC. Details of its usage are in this Microsoft Article. The interface is not designed for the average user, so instead see the Devices and Printers section of the Hardware Management chapter for more details of a user-friendly way to access and manage your printers.

RESOURCE MONITOR

This opens the Resource Monitor tool, which is covered in more detail under the Resource Monitor section of the Performance Measurement and Troubleshooting chapter.

SERVICES

This opens the Services utility, which is covered in more detail in the Services chapter.

SYSTEM CONFIGURATION

This opens the Microsoft System Configuration tool, also known as MSConfig, which is covered in more detail under relevant sections of the Boot Configuration, Startup Programs and Services chapters.

SYSTEM INFORMATION

This opens the Windows System Information utility, which is covered in more detail under the System Information Tools section of the System Specifications chapter.

TASK SCHEDULER

This opens the Task Scheduler utility, which is covered in more detail under the Background Tasks section of the Services chapter.

WINDOWS FIREWALL WITH ADVANCED SECURITY

This opens the Windows Firewall with Advanced Security tool, which is covered in more detail under the Windows Firewall section of the Security chapter.

WINDOWS MEMORY DIAGNOSTIC

This opens the Windows Memory Diagnostic tool, which is covered in more detail under the Windows Memory Diagnostic section of the Performance Measurement & Troubleshooting chapter.

WINDOWS POWERSHELL

The Windows PowerShell is a command line interface combined with a powerful scripting language, and is designed for use by system administrators and very advanced home users. Refer to this Microsoft Article for a general overview of using PowerShell, with links to additional resources. PowerShell is beyond the scope of this book and is not covered in more detail.

< AUTOPLAY

AutoPlay functionality is covered under the AutoPlay section of the Drive Optimization chapter.

< BITLOCKER DRIVE ENCRYPTION

BitLocker Drive Encryption is a drive security feature available only in Windows 8 Pro and Enterprise. It is covered in more detail under the BitLocker Drive Encryption section of the Security chapter.

< COLOR MANAGEMENT

Windows Color Management is a tool that allows you to ensure that the colors displayed on your screen are accurate, and reproduce images faithfully across a range of devices. For accurate color reproduction it is important that your monitor have proper drivers loaded in Windows. These should be available from your monitor manufacturer's site - see the Windows Driver chapter for details of how to check and update device drivers as necessary.

Once the appropriate driver has been loaded, the average home PC user should not change the settings here as they require knowledge of color standards. However, you can calibrate your display color using the built-in Display Color Calibration utility, found under the Advanced tab by clicking the 'Calibrate display' button. This is covered in more detail under the Display Settings section of the Graphics & Sound chapter.

< CREDENTIAL MANAGER

Credential Manager is a central location for holding usernames and passwords for quicker access to protected resources. It is covered in more detail under the Backing Up & Restoring Passwords section of the Backup & Recovery chapter.

< DATE AND TIME

It is important that you have the correct system date and time. Some software will not function properly unless these are set and maintained correctly. There are also additional features you may wish to configure here to customize the display of date and time on your system.

DATE AND TIME

Make sure the date and time are set correctly under this tab. Click the 'Change date and time' button if necessary and set the current date and time. Clicking the 'Change calendar settings' link takes you to a Customize Format window which is covered in more detail under the Region section later in this chapter.

Make sure to set the correct Time Zone for your region by clicking the 'Change time zone' button, as this will affect the way changes like Daylight Savings will impact on your system. I recommend ticking the 'Automatically adjust clock for Daylight Savings Time' so that your clock is automatically adjusted back or forward when Daylight Savings occurs in your area. If necessary also tick the 'Notify me when the clock changes' box so that Windows can provide advance notification regarding any upcoming changes due to Daylight Savings.

ADDITIONAL CLOCKS

You can display up to two additional clocks alongside the main clock. Click the 'Show this clock' box above each of the clocks you wish to show, set the time zone for the clock(s), and give the clock(s) suitable names, such as the name of a city, or the time zone you have chosen. The clock name(s) and the time for each clock will then appear whenever you hover your mouse over, or click on, the time display in the Notification Area on the Taskbar.

INTERNET TIME

By default Windows updates your system clock over the Internet once a week to maintain its accuracy. If you wish to disable this option, or manually update your clock at any time, click the 'Change settings' button. To update manually, click the 'Update now' button. To disable the automatic update functionality, untick the 'Synchronize with an Internet time server' option. If for some reason the system time is not updating, or is inaccurate, click the drop down box and select another time server for Windows to connect to for this purpose. I recommend allowing Windows to update the clock automatically, as it has no performance impact and helps prevent the clock from slowly becoming more and more inaccurate over time.

< DEFAULT PROGRAMS

This component allows you to set the default programs and file associations Windows uses. These determine which program opens a particular type of file by default when you attempt to launch it. Each of the sub-options is covered in more detail below.

SET YOUR DEFAULT PROGRAMS

This option provides a list of Desktop programs and Metro apps which are the default handlers for the common Windows file associations, such as image files, multimedia files, emails and web pages. Select a listed program or app, and in the right pane you will see that you can either 'Set this program as default' which basically sets the program as the default one for all the file types it can open; or you can manually choose which file types it can open by clicking the 'Choose defaults for this program'.

I recommend that you do not alter these settings unless you have specific strong preferences, or you know a certain program is problematic with certain file types. For example, by default Windows 8 associates all common video file formats with the Video app, even if they are launched from the Desktop. You may wish

instead to associate these formats to Windows Media Player. To do this, select Windows Media Player from the list, then click the 'Set this program as default' option.

If you just want to manually assign a default program to a particular file type, it is quicker and more thorough to use the 'Associate a file type or protocol with a program' option below. Changing the file association using that method will also add the program to the Programs list here.

ASSOCIATE A FILE TYPE OR PROTOCOL WITH A PROGRAM

This option allows you to manually view and set the default program to be used when opening a file with a particular type of extension. For example, you can choose the program or app that will open all .MP3 audio files, or all .PDF document files on your system by default. It doesn't prevent other programs from opening these file types, it simply chooses the program that Windows will automatically use when a file of that type is launched. Note, if you can't see the file extensions for your files in File Explorer, make sure the 'Hide extensions for known file types' option is unticked in Folder Options - see the Folder Options section of the File Explorer chapter.

When you first open this tool, it may take a moment for it to populate the list of all file types on your system and their associated default programs. You can then scroll down the list to view the associations, and note that where 'Unknown application' is listed, that means there is currently no default program for that file type. To change the association for a particular file extension, highlight it and click the 'Change program' button at the top right of the window. If it already has a default program, it will be shown and recommended with the words 'Keep using *[program name]*'. You can either select one of the other programs shown, or to view additional programs which can handle this file type, click the 'More Options' link. If you still can't see your desired program, scroll down to the bottom of the list and click the 'Look for another app on this PC' link, then browse to the location of the program's main executable and select it. If you can't find a program which will work with the file type, then you should conduct a web search on that file type to see the programs that are capable of running it.

If you have problems with an association constantly changing back to an undesirable program after having set it here, remember that when installing certain programs, they may automatically make themselves the default program for particular file types, often without asking your permission. Some programs also re-associate themselves with their file types each time you launch them. You should therefore go into the options for the particular program which is currently associated with a file and check for any settings or file associations there, and alter or disable them first before coming here and changing file associations manually, otherwise the program may override the association again.

You can also associate common protocols such as HTTP (web pages) and MAILTO (email) with a particular program here at the bottom of the list under the Protocols category. For example, if you change the MAILTO protocol handler, this will affect the default program used when you launch email links in web pages. Windows also allows you to change the SEARCH protocol, letting you associate some of the built-in Windows Search functionality with a third-party search provider - see the Windows Search chapter.

CHANGE AUTOPLAY SETTINGS

The AutoPlay settings are covered in more detail under the AutoPlay section of the Drive Optimization chapter.

SET PROGRAM ACCESS AND COMPUTER DEFAULTS

This section allows you to set the defaults for key functions in Windows: Internet browsing, Email, Media playback, Instant messaging, and Java virtual machine. Importantly, it also allows you to block particular built-in Windows programs, effectively disabling them. The main reason for the presence of these options is that Microsoft was charged with monopolistic behavior, and as part of the terms of settlement of a case

against them, they are now required to provide users with the option to disable certain built-in programs, such as Internet Explorer and Windows Media Player, which cannot otherwise be uninstalled.

I recommend that you select the Custom option, which will expand to allow you to customize programs under several categories. Choose your default programs, and I strongly recommend that you do not untick the 'Enable access to this program' option for Internet Explorer or Windows Media Player, as both of these may be required to view certain web pages, or play certain media sources. If you wish to safely remove certain built-in Windows features, such as Internet Explorer or Windows Media Player, see the Programs and Features section later in this chapter.

< DEVICE MANAGER

The Device Manager utility is covered in more detail in the System Specifications, Hardware Management and Drive Optimization chapters.

< DEVICES AND PRINTERS

The Devices and Printers feature is covered in more detail under the Devices and Printers section of the Hardware Management chapter.

< DISPLAY

The Display functions are covered in more detail under the Display Settings section of the Graphics & Sound chapter.

< EASE OF ACCESS CENTER

There are a range of features here that can be used to accommodate different keyboard usage styles, make Windows easier to see on screen, or provide audible notification of events for example. The settings you choose will depend on your individual requirements. If you want to find out more about these options go to the Windows Accessibility Page. The majority of users will not need to enable or use these settings, and should leave them at their defaults.

Some functionality found here may be desirable for any user, so if in doubt, go through all the settings and experiment to see if something suits you. For example, you can select the 'Make the mouse easier to use' option and then change both the color and size of the mouse pointer. Alternatively, you may wish to disable the Aero Snap feature by ticking the 'Prevent windows from being automatically arranged when moved to the edge of the screen' option. See the Graphics & Sound chapter for coverage of general features in this area which potentially relate to all users.

< FAMILY SAFETY

The Family Safety feature is covered in more detail under the Family Safety section of the User Accounts chapter.

< FILE HISTORY

The File History feature is covered in more detail under the Windows File History section of the Backup & Recovery chapter.

< FOLDER OPTIONS

This Folder Options feature is covered in more detail under the Folder Options section of the File Explorer chapter.

< FONTS

The Fonts feature is covered in more detail in the Fonts section of the Graphics & Sound chapter.

< HOMEGROUP

HomeGroup is a feature designed to make the sharing of files and printers much easier on a home network. To create or join a HomeGroup, your network location type must be set to Private - see the Network and Sharing Center section later in this chapter for more details. When this network location is chosen - whether during Windows installation, or at any point afterwards - Windows will automatically enable the HomeGroup feature, the most obvious component of which is a new category called HomeGroup visible in the Navigation Pane of File Explorer.

To create a HomeGroup, click the 'Create a homegroup' button in the main HomeGroup window and follow the prompts. When you enable the HomeGroup feature, you can then select a new HomeGroup option under the 'Share with' context menu when right-clicking on files or folders, or from the Share ribbon menu in File Explorer. Thus you can share content with others on your home network in a simple manner.

If you do not wish to use the HomeGroup feature, to disable it and remove the HomeGroup category in the Navigation Pane of File Explorer, see the Basic Features section of the File Explorer chapter.

< INDEXING OPTIONS

The Indexing Options are covered in more detail under the Search Index section of the Windows Search chapter.

< INTERNET OPTIONS

This component brings up the 'Internet Properties' box for the Desktop version of Internet Explorer, regardless of your default browser. See the Internet Explorer chapter for full details of how to configure these options.

< KEYBOARD

This component provides access to basic keyboard-related settings in Windows. Under the Speed tab, I recommend that you set the 'Repeat delay' slider to the far right (Short), and also set the 'Repeat rate' slider to the far right (Fast). This will provide maximum responsiveness for your keyboard, with the least delay between keystrokes. You can test these settings by clicking in the small test box provided, then holding down a key. There may also be keyboard-related options in your BIOS/UEFI that affect the speed with which the keyboard responds, so check there if you find that your keyboard still feels sluggish. You should also adjust the 'Cursor blink rate' to your taste, as it controls how fast any text cursor blinks within Windows.

< LANGUAGE

The basic language options should have already been set during the Windows installation process, however here you can change these settings. The main Language screen shows your current language. You can add, remove or re-prioritize languages in Windows by using the links at the top of the screen. For example, click 'Add a language' to select another language, then select it and click the Add button to add it to the main list. Any language which is shown at the top of your list is the default primary language for Windows, so select a language from the list and use the 'Move up' or 'Move down' links at the top to rearrange the list order as

required. Click the Options link at the far right of each language to access additional options, such as viewing the keyboard layout for the language by clicking the Preview link.

To view even more options for Language, click the 'Advanced Settings' link in the left pane. Here you can override the language list on the main screen by explicitly selecting a particular display language for Windows. If you wish to enable the Language Bar, which is handy for quickly changing languages, then tick the 'Use the desktop language bar when it's available', otherwise leave it disabled. If you've enabled the Language Bar, then click the 'Change language bar hot keys' link to open more settings to customize the appearance and access methods for the Language Bar.

To quickly change display languages in Windows, either click the language icon which appears in your Notification Area (e.g. displayed as 'ENG' for English), or open the Charms menu, select Settings and click the Keyboard icon in the lower right corner.

You can also adjust the date, time and number formats for your language by clicking the 'Change date, time or number formats' link in the left pane. You can also access these options by opening the Region component of the Windows Control Panel.

< LOCATION SETTINGS

Installed apps can adapt their behavior based on detected geographical location. For example, using your IP Address, Wi-Fi triangulation, Cell phone triangulation or onboard GPS, an app can determine your geographical location and use that for giving directions on a map.

If you have privacy concerns regarding this functionality, the Locations Settings component gives you the ability to turn off the Windows Location platform. You can also control this functionality on a per-app basis in most cases, or you can disable app access to your location data under the Privacy section of the PC Settings - see the PC Settings chapter for more details.

< MOUSE

This component allows you to configure your mouse-related settings. If you've installed a third party mouse driver, you may see different settings available under this screen, however the basic settings described below should still be available on most systems. Any options not covered can be set to suit your taste as they have no impact on performance.

BUTTONS

Adjust the double-click speed to the rate which suits your usage patterns, and test it on the folder image provided. I recommend setting a slower double-click speed so that you can open files and folders more comfortably.

POINTER OPTIONS

Adjust the mouse cursor movement speed using the Motion slider. I recommend ticking the 'Enhance pointer precision' option before you adjust your pointer speed. This option enhances the acceleration/deceleration of your mouse to allow for larger movements when you move the mouse fast, and finer movements when you move the mouse more slowly, giving you greater precision when needed while also providing faster coverage of your Desktop.

WHEEL

You can increase or decrease the responsiveness of your mouse's scroll wheel by altering the number of lines it will scroll on each turn of the wheel under the Vertical Scrolling option. For example, an increase from the default of 3 to 4 will make a subtle but noticeable difference if you previously found the mouse wheel relatively unresponsive. The same goes for Horizontal Scrolling, which determines how fast the screen scrolls left or right when you use a tilt wheel on a supported mouse.

< NETWORK AND SHARING CENTER

The Network and Sharing Center provides a visual representation of your current network setup and allows you to further customize and troubleshoot your connection settings. Detailed network setting configuration advice is beyond the scope of this book, as it is a very complex topic which varies greatly based on the type of connection and hardware involved. Furthermore Windows detects and sets up your network/Internet connection automatically and does a good job of it, as long as you have correct device drivers for your hardware. So there is nothing to be gained by altering these settings beyond the functionality covered below:

Network Location: When you first install Windows 8 you can set your network type, as covered under the Installing Windows section of the Windows Installation chapter. The two main types are Private network or Public network. Your current network location is shown here under the Network heading at the top.

The network locations are described in this Microsoft Article. For the average home user with a standalone PC and a connection to the Internet, I recommend a Public network to begin with, as this is the most private and secure setting, since it is designed to be used in public areas, and also prevents the installation of unnecessary features like HomeGroup. A Private network is suitable if you're connected to a trusted network of other home or work PCs, and wish to more easily share files between them.

To change your network location at any time, open the Charms menu, select Settings, then click on the Network icon. Alternatively, simply click on the Network icon in the Notification Area. This will open the Networks panel, showing all available network connections, and whether you are currently connected to any of them. Right-click on the relevant connection shown here, and select 'Turn sharing on or off'. In the next panel, select No if you want a Public network location, or select Yes if you want a Private network location for your connection.

The network location you choose affects whether the HomeGroup setting is enabled - see the HomeGroup section earlier in this chapter. Furthermore, the network location also affects the profile used in the Windows Firewall, so see the Windows Firewall section of the Security chapter to ensure that the settings for your currently chosen profile are appropriate if you have recently switched locations.

Connections: The connections area at the top right shows the types of connection(s) currently enabled on your system. This is usually set automatically based on the type of network device you have on your PC. Click the connection name to see more details in a new window. Click the Details button in this window to see even more details. If you're having problems with your connection, click the Diagnose button and follow the prompts. If no problem is found but your device is still not working correctly, go to the main Network and Sharing Center window and select the 'Troubleshoot problems' link. This provides access to tools for troubleshooting any network-related issues, covered further in the Troubleshooting section of the Performance Measurement & Troubleshooting chapter.

If at any time you want to terminate the connection, click the Disable button in the connection status window. However, the most foolproof way to terminate a connection, if you suspect that your PC is infected with malware, or there are other concerns, is to turn off your router/modem and pull out your DSL/cable line from the wall. This ensures that nothing can possibly get to or from your machine via the Internet.

For advanced configuration of your network device, click the connection name on the main Network and Sharing Center window, then click the Properties button in the status window. Here you can see the various clients, services and protocols that this connection uses. These should not be altered unless you have specific needs - refer to your device's documentation for detailed instructions. In general there is little to gain from unticking any of the items here.

Finally, to benchmark and compare your Internet speed, use the free Speedtest online service.

Once again, I strongly suggest leaving the settings here at their defaults if you are not certain of what to change. Unless explicitly instructed, there is far more potential to do harm than good by changing these settings, especially if you wind up disconnecting yourself from the Internet for example and hence have no easy way to seek outside assistance and information to rectify the problem. The default Windows settings are already optimal and don't need any adjustment in the majority of cases. If you are having any connection problems, it is usually due to third party firewall software, or even an actual physical fault in your line.

< NOTIFICATION AREA ICONS

The Notification Area Icons feature is covered in more detail under the Notification Area section of the Graphics & Sound chapter.

< PERFORMANCE INFORMATION AND TOOLS

This component takes you to a range of tools that are useful in measuring and adjusting performance-related features on your system. Full details of all of these tools can be found in various chapters, including Performance Measurement & Troubleshooting, Windows Search, Graphics & Sound, and Cleaning Windows.

< PERSONALIZATION

The Personalization component is covered in more detail under the Personalization section of the Graphics & Sound chapter.

< PHONE AND MODEM

This option lets you configure any connected phone or modem devices. This is a legacy option and is not covered in detail in this book.

< POWER OPTIONS

The Power Options component allows you to apply or change a power plan. The plans controls the power consumption and idle behavior of Windows, and importantly, can also have an impact on performance.

There are three preset levels of power plans available: Power Saver, Balanced and High Performance. These are described further in this Microsoft Article. I recommend that instead of using a preset level, you should create an entirely new power plan and individually customize each of the settings, since none of the presets is exactly right for any system. To customize your own settings, follow these steps:

1. Click the 'Create a power plan' link on the left side of the main Power Options window.
2. Choose 'High Performance' as the starting point for your changes.
3. In the Plan Name box, give the new power plan a descriptive name.
4. I recommend turning off the display after a set period of system inactivity, as this has no performance impact and does no harm to the monitor, but prevents energy waste and potential image retention on LCD or Plasma displays. A delay of 15 minutes is reasonable.

5. I recommend disabling the Sleep functionality (select Never) to start with. See further below for details.
6. Click the Create button to create the new power plan.
7. In the main Power Options window, you must then click the 'Change plan settings' link next to the name of the new plan you have created.
8. Click the 'Change advanced power setting' link, and a new 'Advanced settings' window will open with a range of detailed settings you can adjust.
9. Click the small plus sign next to each and every setting to fully expand them one by one, changing them individually as covered below. You should also click the 'Change settings that are currently unavailable' link at the top of the window to ensure that all possible settings are shown.

Each of the advanced power settings are explained below. Note that you can quickly access the Power Options at any time on a mobile device by clicking the power plug/battery icon in the Notification Area. In any case, my recommendations below relate primarily to a standard desktop home PC - you may see additional battery-related power options on your device which are not covered below:

Require a password on wakeup: If set to Yes, this option forces you to reenter the password (if one exists) for the current user account to unlock the PC when waking up from a sleep mode. Set to suit your security needs.

Hard Disk - Turn off hard disk after: Set this to the number of minutes of inactivity before your hard drive(s) are turned off. I recommend selecting Never to maintain maximum responsiveness and longevity for your main system drive; hard drives should not be constantly switched on and off. However, on a system with multiple drives, where some of the drives are often left unused for long periods, you can leave this option enabled and set for something moderate like 20 minutes so that those drives are turned off. Your main system drive should remain on, since even when idle, Windows will be frequently running background tasks which will keep the system drive live.

Internet Explorer - JavaScript Timer Frequency: This option determines how the JavaScript engine in Internet Explorer works. When set to Maximum Performance, JavaScript on web pages in IE will be executed more quickly, and when set to Maximum Power Savings, JavaScript performance may be slower in return for less system resource usage, and hence lower power consumption. This should be set to Maximum Performance on a desktop PC.

Desktop background settings - Slide show: Determines whether the Slide Show feature for Desktop Backgrounds is Available, or is Paused by default. Set to suit your taste, and has no impact if you haven't enabled the Slide Show (i.e. you have only selected a single Desktop wallpaper). See the Personalization section of the Graphics & Sound chapter for more details.

Wireless Adapter Settings - Power Saving Mode: If you have a wireless network adapter connected to your system, select a power saving mode. For maximum responsiveness select 'Maximum Performance'.

Sleep: This section of the Power Options requires more comprehensive coverage in the separate Sleep Modes & Fast Startup section further below.

USB settings - USB selective suspend setting: This option controls whether the system will selectively suspend individual USB devices that do not require power. This should generally be set to Disabled to prevent USB devices becoming non-functional during a session, unless you run a mobile device where power savings are important.

Power buttons and lid - Power button action: This is an important setting as it determines what happens when you press the Power button on your PC. I recommend setting this to 'Shut Down' which is the normal behavior for a power button. If you've enabled one of the sleep-related modes and don't have a dedicated sleep button on your PC, you may want to change this option to Sleep.

Power buttons and lid - Sleep button action: This setting determines what happens when you press the Sleep button - if one exists - on your PC or device. Set to suit your other options. For example, if you've enabled Hibernation, then you can set the Sleep button to Hibernate instead of Sleep.

PCI Express - Link state power management: This setting will allow an idle PCI-E connection to reduce power consumption depending on the option chosen here. Since PCI-E is most commonly used for plug-in graphics cards which are high performance devices, I recommend against anything other than Off for this setting to prevent slowdowns or problems.

Processor power management - Minimum processor state: This setting controls the minimum percentage of CPU performance Windows will throttle the CPU down to in order to save power. If you don't want any throttling, set this to 100%. Typically a CPU can't throttle down beyond a certain point - usually no less than 50% of its speed - regardless of how low this setting is. I recommend setting this option to 50% to allow your CPU to throttle as far as it can when it is not in use; this will reduce power usage and more importantly, will keep the CPU cooler when its full power is not needed, but anytime an application requires it, the CPU will throttle back up to full power instantly.

Processor power management - System cooling policy: This setting determines how the CPU is controlled when its temperature rises. The Active setting will attempt to raise the fan speed before throttling down CPU speed, while the Passive setting will do the reverse, reducing CPU speed to maintain temperatures. In either case your CPU, fan and motherboard must support this feature for it to take effect. I recommend the Active setting so that your system first attempts to increase cooling to the CPU before reducing its speed. In practice this setting should not need to kick in if you keep your CPU properly cooled. See the Hardware Management chapter for more details on cooling hardware.

Processor power management - Maximum processor state: This setting controls the maximum percentage of CPU performance Windows will allow when CPU resources are in demand. There should be no reason for a desktop PC to set this below 100%, as otherwise your CPU may have lower performance precisely when you need the most processing power.

Display - Turn off display after: This setting lets you select the amount of inactivity before your monitor is switched off, and is already covered at the start of this section. It is recommended that you enable this option and set it to around 15 minutes of inactivity.

Display - Enable adaptive brightness: This setting, if set to On, allows any system or monitor that has an ambient light sensor to change the display brightness according to the brightness of the surrounding environment. An ambient light sensor is most commonly found on mobile devices such as tablets. Without the appropriate sensor, this setting has no impact, and can be left Off.

Multimedia settings - When sharing media: Determines your PC's behavior when it is sharing or playing back media via a connected device, or to other computer(s). I recommend selecting 'Prevent idling to sleep' so that your PC doesn't enter Sleep mode, disrupting the media stream, unless you manually select to put it to Sleep.

Multimedia settings - When playing video: This setting allows Windows Media Player to determine whether to optimize for quality or power savings when playing a video. Unless you need to save power on a portable device, on a desktop PC this should be set to 'Optimize video quality' for the best video playback quality.

There may be additional settings to those listed above. This depends on your actual device and its capabilities. Once done with these settings click the Apply button and then click OK, and your scheme will now be configured and put into effect. You can see this under the main Power Options screen - your custom power plan will be selected.

SLEEP MODES & FAST STARTUP

The sleep modes under the Power Options, and a new feature of Windows 8 known as Fast Startup which utilizes similar functionality, are covered in more detail below.

Sleep - Sleep after: This option lets you choose the period of inactivity required before your system goes to Sleep. Sleep is a power-saving mode designed as a compromise between switching off your PC and leaving it running at full functionality. To activate Sleep mode, you need to select Sleep from the shutdown options, or press the sleep button on your PC. In Sleep mode your PC turns off most of its components except RAM, and saves your open documents, programs and system state to RAM. This uses minimal power (less than 3W), and your system will appear to be inactive, but it can be "woken up" almost instantly by pressing the Power or sleep button, opening the lid, or using a peripheral. The main problem with Sleep mode is that because your data is stored in RAM, it is susceptible to loss through sudden loss of power, or faulty RAM.

Sleep - Allow Hybrid Sleep: This option lets you choose whether to enable Hybrid Sleep mode or not. Hybrid Sleep mode is similar to the regular Sleep mode covered above, but instead of saving your system state to RAM, it saves them to a *Hiberfil.sys* file in your drive's base directory, providing added security against potential data loss. This file is exactly the same size as the amount of system RAM currently being used, and the act of writing to it when entering Hybrid Sleep and reading from it when waking up may briefly make the system less responsive. Selecting the Sleep option from the shutdown menu when Hybrid Sleep is enabled will put your system into Hybrid Sleep not normal Sleep.

Sleep - Hibernate after: This option allows you to configure Hibernation, which will write your open documents, programs and system state to a *Hiberfil.sys* file on your system drive after a period of inactivity as specified here. However unlike any Sleep mode, rather than putting your system into a power-saving state, it turns off the entire PC and leaves it that way for as long as you like. You can then turn the system back on at any time in the future to find your previous session restored as you left it. It both saves power and protects against data loss, but takes slightly longer to get back to your Desktop compared to regular Sleep mode. Note that Hibernation performance has been improved in Windows 8 as part of optimizing the startup process.

Sleep - Allow wake timers: If you have enabled a Sleep mode, you can enable wake timers, which allow the PC or device to be automatically woken up from Sleep by scheduled tasks and events, and then return to its sleeping state once they are completed. For example, you can schedule a full malware scan using Windows Defender at 1:00am every Wednesday - see the Background Tasks section of the Services chapter for more details of how to configure a range of tasks in this manner. This task will then wake up your sleeping PC, run until completed, then return the PC or device back to sleep mode upon completion. If on the other hand you don't want any task or event to wake up your PC under any circumstances, set this option to Disable.

Define Power Buttons: There is one other area of the Power Options which is relevant to sleep modes. To access it, on the main Power Options screen in Windows Control Panel, click the 'Choose what the power buttons do' link in the left pane. Here you can define what the main power button your PC or device does, as well as the sleep button if you have one. If you find that some of the options on this screen are grayed out and can't be changed, click the 'Change settings that are currently unavailable' link at the top of the screen.

Importantly, at the bottom of this section, you can further adjust your shutdown and sleep options:

There are four shutdown settings here, with Fast Startup covered in more detail below. Of the other three options available here, the Sleep and Hibernate options relate to whether those items are displayed in the Shutdown menu, which you can access by opening the Settings charm, and clicking the Power icon. For example, if you don't use the Sleep or Hibernate modes, then untick both options here, and click the 'Save Changes' button. They won't be displayed the next time you open the power menu. The Lock option here relates to the Lock item which appears in the selection menu when you click on your user account picture at the top right of the Start Screen. Once again, if you don't lock your system, then you can untick this option here and click 'Save Changes', and the Lock item will be removed from that menu when next you access it.

Turn on Fast Startup: A new feature of Windows 8, Fast Startup, also called Hybrid Boot, has some similarities to Hibernation mode, but does the job much more efficiently. It is enabled by default, but can be turned on or off here at any time. If you can't see the Fast Startup option displayed here, see further below for instructions on how to regain it by re-enabling the Hibernation file which it requires.

With Fast Startup enabled, whenever you perform a shutdown, critical parts of the system state known as the kernel session are first saved to your drive, as part of the *Hiberfil.sys* file. When next you boot up Windows, this saved information is accessed and helps speed up startup time, as the data does not have to be recreated from scratch. Your previous user session won't be saved however, so as you boot into Windows it will appear to be an entirely fresh session. Note that Fast Startup does not apply after restarts, only shutdowns.

If you leave Fast Startup enabled, but want to force a full shutdown at any time without having your kernel session saved, such as after driver installation or a hardware change, then open a Command Prompt and type the following when you're ready to shut down:

```
shutdown /s /f /t 0
```

Fast Startup already attempts as much as possible to initialize the system like a fresh session each time you bootup, so it shouldn't require a forced shutdown, and won't adversely affect system stability. It is recommended that you leave Fast Startup enabled, and only disable it for troubleshooting purposes.

If you have disabled Fast Startup and the Hibernate feature, you can also delete the *Hiberfil.sys* file in the base directory of your system drive. It is usually quite large, typically equal in size to 75% of your system RAM. Note that you cannot see this file unless you disable the 'Hide protected operating system files' option under Folder Options - see the Folder Options section of the File Explorer chapter.

You can't manually delete *Hiberfil.sys*. To remove it, you must open an Administrator Command Prompt, then type:

```
Powercfg -h off
```

This will remove *Hiberfil.sys* from your drive, but it will also disable the Hibernate and Fast Startup features, and remove their options from your Power Options screen as well.

The Hibernation file, and its associated Hibernate and Fast Startup options, can be restored at any time by using the following command in an Administrator Command Prompt:

```
Powercfg -h on
```

Given the Fast Startup feature is generally beneficial on almost all systems and relies on *Hiberfil.sys*, it is not recommended that you remove the Hibernation file. A better option is to resize *Hiberfil.sys* to make it smaller, but still functional for Fast Startup, by typing the following command at an Administrator Command Prompt:

```
Powercfg -h size [percentage of system RAM]
```

Where the /size parameter is a percentage between 0 and 100 for the size of *Hiberfil.sys* in relation to your system RAM. Microsoft recommends that for Fast Startup usage, *Hiberfil.sys* be at least 10-15% of your system RAM size. However the command cannot force the file to fall below 50% of system RAM, so for the smallest Hibernation file size, type the following command in an Administrator Command Prompt:

```
Powercfg -h size 50
```

This will reduce the size of *Hiberfil.sys*, and remember that the default for the Hibernation file is 75% of system RAM in case you want to reset it for troubleshooting purposes (i.e., substitute 75 in place of 50 in the command above to reset it to default).

A final piece of advice regarding the Sleep, Hibernation and Fast Startup features. For a mobile device, these are all viable options depending on your power needs. However aside from Fast Startup, I recommend against using any of the Sleep-related modes on a desktop PC if you value system stability and performance. A fresh restart every day or so uses more power and requires more time at startup, but provides the most stable and optimal Windows environment by cleaning out the contents of your system RAM and video memory, resetting all program states, and deleting and recreating all temporary files. If you do choose to use a Sleep mode of any kind, or leave your PC on for long periods at a time, at the very least make sure to do a restart at least once a week, as recommended under the Restart Regularly section of this Microsoft Article.

While there are valid concerns about Global Warming and the wasteful use of energy and resources, I believe it is false economy to enable too many power saving features on a desktop PC as you may reduce the functionality of your PC, decrease its stability, and potentially experience data loss if you go overboard. Certainly for gamers and other high-performance users I don't recommend that power saving options be used aside from those recommended above. For users of mobile and low-power devices on the other hand, as well as casual PC users who primarily browse the Internet, the options require some thought based on individual usage patterns and the desire to save power or battery life. Regardless, if you experience any system instability or strange system behavior, I recommend temporarily selecting the standard 'High performance' preset for troubleshooting purposes to see if power-based settings are the cause of your problems.

< PROGRAMS AND FEATURES

Programs and Features is the primary component used to view, modify or uninstall the Desktop programs and system drivers currently installed on your PC. It also allows you to add or remove a range of Windows features.

The main Programs and Features window provides useful details, such as the date a program was installed under the 'Installed On' column, the total size of the program on disk under the Size column, and even the version number in the Version column. If you select a particular item from the list, you may see additional resources such as links to the software manufacturer's support site in the Details Pane at the bottom of the window.

Some programs and drivers installed on your system will not appear in this list because they are standalone programs that don't require installation, they have problematic installers, or they are manually installed

drivers which did not come in an installation package. See the Windows Drivers chapter for information on how to manually find and remove installed drivers that don't appear on this list. You can also use the Uninstall function of the CCleaner utility to remove any unnecessary entries in Programs and Features. Open CCleaner, click the Tools button, then select the Uninstall option. In the list of Programs to Remove, you can highlight an entry and click the 'Run Uninstaller' button to attempt to uninstall it as normal. If this fails, you can attempt to manually delete its files as covered under the Cleaning Windows chapter. Once you are sure the program has been removed from your system, you can select its entry from the list and click the 'Delete Entry' button to remove it. See the CCleaner section of the Cleaning Windows chapter for more details.

The main functionality for Programs and Features is covered below:

Uninstalling Programs: Highlight the program or driver you wish to uninstall, right-click on it and select Uninstall to commence removal. If the program allows you to alter its installed components, a Change and/or Repair option will also be available, or you may see a combined Uninstall/Change option. In all cases, selecting one of these options should initiate a series of prompts, or an automated wizard that will take you through the process.

Turn Windows Features On or Off: This option is shown on the left side of the window, and when selected, opens a new windows displaying a list of all the built-in Windows features that you can choose to install or uninstall. This allows you to only have the features you need in Windows, saving you disk space and disabling associated drivers and services. Importantly, it also allows you to quickly and easily re-enable any such features in the future should you want them again. For this reason, this is preferred over other methods which permanently remove a feature from your Windows installation media, such as those covered under the Prior to Installation section of the Windows Installation chapter.

You will need to take your time going through these features and carefully decide if you need to access them at some point in the future. If in doubt, do not disable or alter a feature, as it is not a major performance-enhancing step, and could provide more problems than any perceived benefits. On the next page are brief descriptions and recommendations, intended for the average home PC connected to the Internet but not to a network of other PCs. Certain editions of Windows 8 may not contain all of these features, and the default options and features may also vary depending on your system and edition of Windows. Note that you can purchase and add certain features to Windows by using the Add Features to Windows 8 component of the Windows Control Panel, and once successfully enabled, they will be added to this list on your system.

Feature	Default	Recommend	Details
.NET Framework 3.5	Main box Ticked, Components Unticked	As Default	Required for applications programmed using .NET. The two Windows Communication Foundation components are unnecessary and can be unticked.
.NET Framework 4.5 Advanced Services	Main box ticked, TCP Port Sharing ticked	As Default	Required for applications programmed using .NET, including Metro apps. Should remain ticked, but the ASP.NET 4.5 and all of the WCF Services components (except TCP Port Sharing) can be left disabled.
Active Directory Lightweight Directory Services	Unticked	As Default	This is a service used by Windows Server, and hence not of use to home PC users.
Hyper-V	Unticked	Optional	Hyper-V functionality is covered in more detail under the Hyper-V section of the Drive Optimization chapter. It is not necessary for most home users.
Internet Explorer 10	Ticked	As Default	Allows you to disable Internet Explorer 10. Keep it enabled in case it's required by a certain site or program.
Internet Information Services, Internet Information Services Hostable Web Core	Unticked	As Default	These services are all designed for running a Web or FTP server, and are unnecessary for an average home PC.
Media Features	All Ticked	As Default / Optional	Install/uninstall Windows media-related programs. Keep Windows Media Player ticked. You can also add Windows Media Center as covered under the Add Features to Windows 8 section earlier in this chapter.
Microsoft Message Queue (MSMQ) Server	Unticked	As Default	Unnecessary unless you specifically run an MSMQ server.
Network Projection	Unticked	As Default	Relates to the use of a video projector over a network, which is unnecessary for home users.
Print and Document Services	Main box Ticked, Internet Printing Client, Windows Fax & Scan Ticked	Optional	Internet Printing Client, LPD Print Service, LPR Port Monitor and Scan Management items are all network-related and unnecessary for the average home PC. Windows Fax and Scan can be ticked or unticked depending on whether you need fax and scanning functionality.
RAS Connection Manager Administration Kit (CMAK)	Unticked	As Default	Used for remote network access via dial-up or VPN, and not needed for the average home PC user.
Remote Differential Compression API Support	Ticked	Untick	Allows more efficient file synchronization over a network. Not needed if you are not on a network of PCs.
RIP Listener	Unticked	As Default	Only tick if on a network which uses the RIPv1 protocol.
Simple Network Management Protocol (SNMP)	Unticked	As Default	Protocol for managing network-based devices, and not used by the average home PC.
Simple TCPIP Services	Unticked	As Default	Not required, installs unnecessary services.
Telnet Client	Unticked	As Default	Untick unless you use Telnet features to connect to a server.
Telnet Server	Unticked	As Default	Lets others connect to your machine via Telnet, which is a security risk unless you need this functionality.
TFTP Client	Unticked	As Default	Only tick if you want to use Trivial File Transfer Protocol to connect to a TFTP server. Unnecessary for average home PC.
Windows Identity Foundation 3.5	Unticked	As Default	Provides developers with tools to add identity management to their software. Unnecessary for the average home PC user.
Windows Location Provider	Ticked	Optional	Provides geographical location data to apps based on Wi-Fi triangulation and IP address data. Disable if you don't use apps which rely on this feature, or consider it a privacy risk.
Windows PowerShell 2.0	Ticked	Untick	Runs the older PowerShell 2.0 engine. If you don't use any PowerShell scripts you can disable it.
Windows Process Activation Service	Unticked	As Default	Not related to Product Activation, this is required for certain applications to transfer information. Not normally needed.
Windows Search	Ticked	As Default	Enables the Window Search functionality. Do not untick - if you want to disable Windows Search then set the Windows Search service to Disabled instead.
Windows TIFF IFilter	Unticked	Optional	Allows Windows Search to index the contents of .TIFF files. Can be ticked if you have any TIFF files you wish to index, otherwise best left unticked.
XPS Services	Ticked	Optional	Allows you to create documents in the Windows XPS format.
XPS Viewer	Ticked	Optional	Allows you to view documents in the Windows XP format. Best left ticked in case you need to view an XPS document.

After changing any of these settings and clicking OK, you may need to reboot and insert your Windows 8 media if required. If you experience any odd behavior, reduced functionality or other problems, then come back here and reset the features back to their defaults. This is one of the key benefits of disabling Windows features in this manner - it allows you to easily undo the change, as opposed to more permanent methods like removing the component from the Windows 8 installation image, or other intrusive techniques.

< RECOVERY

The Recovery window is simply a central location for accessing several troubleshooting and system recovery features in Windows. These features are each covered in more detail in the Backup & Recovery chapter.

< REGION

The basic region options should have already been set during the Windows installation process, however here you can change or refine these settings.

FORMATS

Select the language format that suits your particular region of the world, and it will automatically customize the date and time formats for you. Your format should match the language you set under the Language component of the Windows Control Panel - in which case the 'Match Windows display language' option should be selected. If for some reason you want to have another format for your date and time, either select another language from the drop-down box, or manually go through each of the options in this section and adjust them to suit your taste. For more detailed adjustment of numerical, time, date and currency formats click the 'Additional settings' button at the bottom of the Region window.

LOCATION

Select your current geographical location from the list.

ADMINISTRATIVE

Welcome screen and new user accounts: You have the option of copying your Region and Language settings to the default template used to create new user accounts in the future. To do this, click the 'Copy setting' button and tick the 'New user accounts' box. If you also want to make them the default for the system (aside from existing user accounts), then tick the 'Welcome screen and system accounts' option. Click OK, and then click Apply to implement the change.

Language for non-Unicode programs: The Unicode system allows modern programs to adapt their menus and dialogs to your system's default language, so this setting only applies to older non-Unicode programs. For any older (non-Unicode) programs, you can set the locale which they will use in case the program's text is not being displayed correctly. In most cases the system locale and non-Unicode locale should be the same.

< REMOTEAPP AND DESKTOP CONNECTIONS

RemoteApp and Desktop Connections is a feature designed to allow users to access remote programs and desktops on a network of machines, as though they were located on your own PC. This is a network-related feature of little value to the average home user, is only available in Windows 8 Pro and Enterprise editions> it is not covered in detail in this book.

< SOUND

The Windows audio-related features are covered in more detail in the Sound section of the Graphics & Sound chapter.

< SPEECH RECOGNITION

This component allows you to configure the Speech Recognition functionality of Windows, which lets you control the computer using voice commands. To use speech recognition, you will require a microphone connected to your system, preferably a good quality one. The Speech Recognition feature is quite specialized, so it won't be detailed here. Sufficient resources are provided to help you configure and learn more about this functionality in the Speech Recognition window. Click the 'Take Speech Tutorial' link to learn more. Most problems experienced with Speech Recognition are due to using a poor quality microphone, or being in a noisy environment.

If you don't use the Speech Recognition functionality, click the 'Advanced speech options' link on the left side of the window and make sure the 'Run Speech Recognition at startup' box is unticked to prevent unnecessary resource usage.

< STORAGE SPACES

Storage Spaces is covered in more detail under the Preparing the Drive section of the Windows Installation chapter.

< SYNC CENTER

The Sync Center is a feature for people working on two or more copies of the same file across different devices or on a network. Note that synchronizing across network folders is only possible under Windows 8 Pro or Enterprise Editions. When a compatible device is detected, Windows will show it under the list of available Sync Partnerships you can use in the Sync Center. Then when a file is stored on both your PC and the device with which you have a partnership, if one version of the file is changed, Sync Center allows you to synchronize the files, such that the newest version is always maintained in both locations. If there is any doubt - for example if both file locations show a changed version - then Windows will ask you which version to keep. For simple syncing between your PC and a portable device, it is best to use the functionality in Device Stage, as covered in the Device Stage section of the Hardware Management chapter. You can also synchronize your user account across various PCs and devices by using a Microsoft Account, as covered in the Local Account vs. Microsoft Account section of the User Accounts chapter.

< SYSTEM

The System component of the Windows Control Panel provides central access to a range of system configuration functionality, as well as displaying an overview of your system specifications and performance. The actual functions found here are covered in full detail in several other chapters. In particular see the Device Manager section of the Hardware Management chapter; the System Protection section of the Backup & Recovery chapter; the Windows Activation section of the Windows Installation chapter; and the Windows Experience Index section of the Performance Measurement & Troubleshooting chapter for more details.

The primary unique functionality for the System component is the Advanced System Settings which contain a range of important options. You can access these options by clicking the 'Advanced system settings' link on the left side of the System component in Windows Control Panel, or by typing *systempropertiesadvanced* on the Start Screen and pressing Enter. Below are details of each tab of this window.

COMPUTER NAME

The Computer Name tab is primarily used for identifying PCs connected to a network. For the average home PC user you can skip this tab; do not alter any of these details. The computer name you entered during Windows installation is perfectly fine. If for some reason you wish to change it, click the Change button. If your PC is part of a network of computers, click the 'Network ID' button and follow the prompts.

HARDWARE

You can access Device Manager here, as well as the Device Installation Settings. Both of these features are covered in detail respectively under the Device Manager and Devices and Printers sections of the Hardware Management chapter.

ADVANCED

This tab has four main sections, covered below:

Performance Settings: Clicking this button takes you to a separate window containing three tabs. Visual Effects is covered under the Personalization section of the Graphics & Sound chapter; the Processor Scheduling component of the Advanced tab is covered under the Task Manager section of the Performance Measurement & Troubleshooting chapter; the Virtual Memory component of the Advanced tab is covered under the Windows Memory Management section of the Memory Optimization chapter; and the Data Execution Prevention tab is covered under the Data Execution Prevention section of the Security chapter.

User Profiles Settings: This area allows you to view, and if necessary change, User Profiles. These profiles hold all of the user account-related settings for each user. See the Advanced Settings section of the User Accounts chapter for more details.

Start-up and Recovery Settings: The settings under the System Startup section are covered under the Boot Configuration Data section of the Boot Configuration chapter, and the System Failure functionality is covered under the Windows Memory Management section of the Memory Optimization chapter.

Environment Variables: This button displays a set of variables and paths which are all configured by Windows 8 when it first installs, and should not be altered here. For example, if you change the windir variable to a different (and incorrect) path, your system will not function correctly, as Windows will not be able to find the correct files to launch itself properly.

Many of these variables can be safely changed using the MSConfig utility. See the Boot Configuration Data section of the Boot Configuration chapter for more details on MSConfig.

SYSTEM PROTECTION

The features under this tab are covered in more detail under the System Protection section of the Backup & Recovery chapter.

REMOTE

This tab allows you to configure how a remote (outside) connection to your PC is controlled. The main purpose for remote connections is when someone in another location on the same network wants to control your PC, for the purpose of troubleshooting a problem you're having for example, or to access resources on your machine directly as though they were sitting in front of your machine. This can be an extremely useful feature when you're on a trusted network, such as a work network, but it is a security risk for the average home PC user. I recommend that you untick the 'Allow Remote Assistance connections to this computer' box, and only enable it if prompted by a 100% trusted technical support person. I also recommend setting the Remote Desktop option to 'Don't allow connections to this computer', and only manually configure this to allow particular users - click the 'Select Users' button - if once again you are dealing with someone who you know for certain is a trusted individual.

Leaving these features enabled is a security risk, especially as many phone scammers will utilize this remote access functionality to compromise your machine under the guise of providing you with technical support

or removing "detected viruses" from your machine. Disable these features here, and there are also related services you may wish to disable - see the Services chapter.

< TASKBAR

The settings under the Taskbar component are covered in detail under the Taskbar section of the Graphics & Sound chapter.

< TROUBLESHOOTING

The Troubleshooting window is a central location to access Windows troubleshooting resources. There are a range of wizards here that automate the process of troubleshooting common problems. This is covered in detail in the Troubleshooting section of the Performance Measurement & Troubleshooting chapter.

< USER ACCOUNTS

The User Accounts component is covered in detail in the User Accounts chapter.

< WINDOWS 7 FILE RECOVERY

The Windows 7 File Recovery features are covered in more detail under the Windows 7 File Recovery section of the Backup & Recovery chapter.

< WINDOWS DEFENDER

Windows Defender is covered in detail in the Windows Defender section of the Security chapter.

< WINDOWS FIREWALL

The Windows Firewall is covered in detail in the Windows Firewall section of the Security chapter.

< WINDOWS UPDATE

Windows Update is covered in more detail in the Driver Installation section of the Windows Drivers chapter.

As mentioned in the introduction to this chapter, while the chapter is primarily a set of references to other areas in this book, it is still useful to run through all of the sections listed here to ensure that you haven't missed any particular Windows setting or feature.

Also make sure to go through all of the additional Metro-based PC settings which are found under the Charms menu, as covered in the next chapter.

PC SETTINGS

As covered in the previous chapter, the Windows Control Panel is the central location for accessing the majority of important Windows settings. With the introduction of the Metro interface in Windows 8 however, a second area has been added which contains a range of additional settings, some of which are Metro-specific. This area is referred to as PC Settings throughout this book, and is found by opening the Charms menu, selecting Settings, then clicking 'Change PC Settings' at the bottom. When the PC Settings app opens, you will see various categories on the left side, each containing a range of settings when selected. We run through all of these in this chapter, however as with the Windows Control Panel chapter, some functionality is already detailed in other chapters, so there are only references to those other chapters here.

< PERSONALIZE

There are three key areas of the Metro interface you can alter here: the Lock Screen, the Start Screen and your Account Picture - these are selectable at the top of the section, and described below:

Lock Screen: This is the screen that appears when you first boot up Windows 8, prior to selecting an account or entering a password. The Lock Screen also appears if you have set your system to require a password when waking up from a Sleep mode or resuming from a Screen Saver. Finally, you can trigger the Lock Screen at any time by clicking on your user account picture at the top right of the Start Screen and selecting Lock.

Your current Lock Screen image is shown in the large pane, and you can quickly select another image from the sample images shown below it. To select from a wider range of images, click the Browse button, and images from your Pictures Library will be available to select. If you have an image outside the Pictures Library that you wish to use, click the Files link at the top and select another location or device to browse and select images from. When a suitable image is displayed, click on it and then click the 'Choose Picture' button at the bottom to set it as your Lock Screen background.

Under the 'Lock Screen Apps' section of the Lock Screen options, you can add or remove Metro apps which can run in the background even while the Lock Screen is active, providing you with updates and notifications. This is useful if you want to quickly see at a glance whether you have new emails, or any upcoming appointments or notes, or an update on the weather for example, without having to log back in to your account. There may already be several apps in the list shown here, including the Messaging, Mail and Calendar apps. Click on the app icon and you can either select another app in its place, or click the 'Don't show quick status here' link if you don't want that app to run in the background and provide updates on the Lock Screen. To add an app, click on of the '+' buttons and select from the list of supported apps shown. You can also select one of these apps to provide more detailed status information on the Lock Screen, by clicking the app icon or '+' button under the 'Choose an app to display detailed status' text at the bottom, and selecting the relevant app. This app's status will now also be shown next to the clock on the Lock Screen.

Note that if you want to avoid seeing the Lock Screen at bootup, then follow the instructions under the User Accounts chapter to either use a Local Account with no password, or automatically login any particular user account at startup. To prevent your system from locking in general, see the 'Require a password on wakeup' setting under the Power Options section of the Windows Control Panel chapter. Also make sure the 'On resume, display logon screen' option is unticked if you have enabled a Screen Saver, as covered in the Graphics and Sound chapter. To disable the Lock Screen altogether, see the Disable the Lock Screen tip under the Group Policy chapter.

Start Screen: The main screen in the Metro interface, the Start Screen can be customized here. The main changes you can make are the overall color scheme of the Start Screen and related Metro elements, such as highlights and text colors. This is selectable via the palette at the bottom. You can also alter the background pattern, limited to the selection shown beneath the large preview image. To set a custom image of your own for the Start Screen background, you will need to use a third party utility, as covered in the Metro Customization section of the Graphics & Sound chapter.

Account Picture: This feature is covered in more detail under the Managing User Accounts section of the User Accounts chapter.

< USERS

The configuration of user accounts is covered in more detail in the User Accounts chapter.

< NOTIFICATIONS

Notifications, also known as App Notifications or Toast Notifications, are a new feature of Windows 8. They appear as a Metro-based panel that pops up in the top right hand corner, in both the Metro interface, as well as on the Desktop. They are typically used to make you aware of a background app event, such as arrival of a new email or text message, or a reminder of an upcoming calendar appointment. These notifications are separate from the normal popups which appear in the Notification Area at the bottom right of the screen, or general Windows information or warning dialog boxes.

The notification functionality can be customized in this section as follows:

Show app notifications: This option provides overall control of notifications. If set to off, no app notifications will be shown.

Show app notifications on the Lock Screen: This option determines whether app notifications appear on the Lock Screen. See the Personalize section earlier in this chapter for details of how to select apps which can provide notifications on the Lock Screen.

Play notification sounds: If enabled, this option plays a sound when an app notification appears.

Show notification from these apps: This section lets you customize which particular installed apps are allowed to provide app notifications. This is useful if you want to leave app notifications enabled globally, but then want to disable certain apps from providing nuisance updates.

< SEARCH

The Search functionality is covered in more detail in the Windows Search chapter.

< SHARE

Sharing content has been made easier in Windows 8 via the Share option available on the Charms menu. When you select the Share charm in the Metro interface, a list of apps which you can use to share the currently viewed content will be shown. In the Share section of the PC Settings, you customize the list of apps that can appear in Share:

Show apps I use most often at the top of the apps list: If enabled, this setting arranges the list of sharing apps with those apps which you most frequently use in Windows being at the top.

Show a list of how I share most often: If enabled, this lists your common share methods, with the number of items listed controlled by the 'Items in the list' box.

Use these apps to share: You can control the individual apps to which shared content can be sent. Disable any apps to which you know you will not be sending shared content, and they will not appear in the app list when the Share charm is opened.

< GENERAL

This section contains a range of general system settings, many of which are adjustable elsewhere in Windows.

Time: These options are covered in more detail under the Date and Time section of the Windows Control Panel chapter.

App Switching: To quickly switch between recently opened Metro apps, you can move your mouse to the top left corner of the screen and click to switch to the next open app, or the Windows Desktop if it is open. Alternatively, you can move your mouse to the top left corner of the screen then move downward to show a list of recently opened apps from which to choose. If you don't like this functionality, set the 'Allow switching between recent apps' option to Off. This will also prevent switching to open Metro apps via other task switching methods as well, such as ALT+TAB.

Spelling: The options here control whether spell checking and correction occur for text that you type in Metro apps, such as the Mail app. If the 'Highlight misspelled words' option is On, any words which the built-in dictionary considers to be incorrect for your chosen display language will be underlined in red. If the 'Autocorrect misspelled words' option is On, words detected as misspelled will be autocorrected where possible to the closest correct spelling.

Language: The Language options are covered in more detail under the Language section of the Windows Control Panel chapter. Clicking the 'Language Preferences' link here will simply take you to the Language component of the Windows Control Panel.

Available Storage: This section shows you how much free space you have left on your drive. It is aimed primarily at devices with lower storage capacities. Clicking the 'View app sizes' button will display all installed Metro apps, and how much storage space each one is currently consuming.

Refresh your PC Without Affecting your Files: This feature will initiate a reinstall of Windows, but will keep your personal data. It is covered in more detail under the System Recovery section of the Backup & Recovery chapter.

Remove Everything and Reinstall Windows: This feature will initiate a reinstall of Windows without retaining any of your data. It simplifies the process of erasing the drive and reinstalling Windows 8 afresh, while also giving you the ability to securely erase your data from the drive. It is covered in more detail under the System Recovery section of the Backup & Recovery chapter.

Advanced Startup: Clicking the 'Restart Now' button will restart Windows into the Advanced Startup screen, which is covered in more detail under the System Recovery section of the Backup & Recovery chapter.

< PRIVACY

This section controls several features which may have privacy implications. These settings are as follows:

Let apps use my location: Some apps, such as mapping apps, will try to use data regarding your actual geographical location as determined by Windows via IP address, Wi-Fi triangulation or GPS, so that they can provide you with better service or appropriate functionality. If you don't wish Metro apps to know your location, turn this setting off.

If you have privacy concerns regarding location-based services, you may also wish to:

§ Enable the 'Never allow websites to request your physical location' option in Internet Explorer, as covered in the Internet Explorer chapter.
§ Turn off the Windows Location platform, as covered under the Location Settings section of the Windows Control Panel chapter.
§ Completely disable this functionality in Windows by removing the Windows Location Provider service, as covered under the Programs and Features section of the Windows Control Panel chapter.

Let apps use my name and account picture: When this setting is On, apps may use your account name and your user account image in the context of personalizing the app experience. If you sign in with a domain account, apps can also get your domain account info, which includes your domain name and domain user name. Once the app has this information, it is up to each app provider's privacy policy, not Microsoft's, as to how they handle and transmit it. If you don't want apps to have this information, then set this option to Off. Disabling this feature should have no real impact on the functionality of most apps.

Help improve Windows Store by sending URLs for the web content that apps use: If enabled, information on the web content which you are seeing in apps will be sent to Microsoft. This information is only used to help detect apps that might be interacting with unsafe web content, such as harmful web addresses or scripts. Addresses of web content can unintentionally contain personal information, but Microsoft says that this information isn't used to identify, contact, or target advertising to the user. Disabling this option will not affect app functionality in any way.

If you continue to have concerns regarding privacy in Windows 8, click the 'Privacy Statement' link at the bottom of this section to see the official Windows 8 Privacy Statement from Microsoft. It provides much more detail regarding how your information is used in Windows 8.

< DEVICES

This section of PC Settings lists a range of connected and detected devices. It is not as comprehensive as the Device Manager. The main use for this location is to readily add or remove plug-in peripherals to a mobile device or PC. In general it is recommended that for correct and more thorough device installation and usage on a desktop PC, you use Device Manager or the Device Stage functionality. See the Hardware Management chapter for more details.

The 'Download over metered connections' option at the bottom relates to whether you permit Windows to download drivers for newly detected devices when using a mobile device that has a metered data plan. Disabling this option is recommended in such cases, but has no real application to most desktop PC users.

< EASE OF ACCESS

This section of PC settings allows configuration of accessibility options. Also see the Ease of Access Center section of the Windows Control Panel chapter. Neither are covered in more detail in this book.

< SYNC YOUR SETTINGS

The settings in this section only apply if you are signed in to Windows 8 using a Microsoft Account as your user account type. They have no impact if you are using a Local Account. These settings and the Microsoft Account are covered in more detail under the Local Account vs. Microsoft Account section of the User Accounts chapter.

< HOMEGROUP

The HomeGroup functionality allows sharing the content of Libraries with other computers in a trusted network. It is only available if your network location is set to Private, as covered under the Network and Sharing Center section of the Windows Control Panel chapter. The HomeGroup functionality itself is covered under the HomeGroup section of the Windows Control Panel chapter.

< WINDOWS UPDATE

Windows Update is covered in more detail under the Windows Update section of the Windows Drivers chapter.

Note that individual Metro app updates are not handled by Windows Update, and are obtained via the Windows Store when signed in. Any updates for your installed apps will be shown on the Store app's tile on the Start Screen. Launching the store app will provide the ability to view the particular apps that need updating by clicking the Updates link at the top right. Select the app to update and click the Install button.

Although mainly designed to control Metro-related settings, confusingly the PC Settings area also contains settings which are necessary for both Metro and Desktop configuration, and of course there is also significant overlap of settings here with those in other areas of Windows, particularly the Windows Control Panel. In any case, by running through all of the settings under PC Settings, once again you are making sure that you have covered all the key settings in Windows.

STARTUP PROGRAMS

Windows needs to load a range of data into memory during its startup procedure. This includes drivers, applications and services required to provide the main functionality in Windows. Windows 8 improves startup time through new features such as the Fast Startup hybrid boot process, as well as incorporating the improvements which Windows 7 brought to features that load at startup, such as SuperFetch and Services. The end result is that on modern systems, it can now take literally only seconds to reach the Lock Screen.

Regardless of the improvements in Windows 8's boot time, removing unnecessary startup programs, services and tasks is still strongly recommended. Not only does it help to reduce excessive loading, both during and immediately after Windows startup, more importantly, it reduces unnecessary background resource usage, which in turn improves overall responsiveness, reduces stuttering, and prevents program conflicts and crashes.

Details on Windows 8's Fast Startup feature are under the Power Options section of the Windows Control Panel chapter, and information on general startup-related optimizations in Windows can be found in the Memory Optimization, Drive Optimization and Services chapters.

In this chapter we look at the correct way to find, identify and properly remove unnecessary startup programs. As of Windows 7, this area of Windows optimization provides potentially the single greatest benefit in terms of stability and performance.

< FINDING STARTUP PROGRAMS

The first step in the process is to find the names of all of the programs and files which are running at startup on your system. To do this you will need to use one or more of the tools covered below.

MICROSOFT SYSTEM CONFIGURATION UTILITY

The Microsoft System Configuration Utility (MSConfig) is a valuable built-in Windows utility for identifying startup programs. To access it, type *msconfig* on the Start Screen and press Enter. Its main use is to provide a brief snapshot of key system variables, and provide a means for troubleshooting Windows boot and startup problems. The options under the Boot tab of MSConfig are covered in more detail in the Boot Configuration chapter; the options under the Services tab are covered in more detail in the Services chapter; and the options under the Tools tab are merely shortcuts to other features and utilities in Windows covered throughout this book. So below we examine the General and Startup tabs of this utility, part of the functionality of which has been transferred to the new Task Manager in Windows 8.

General: By default MSConfig will display the 'Normal startup' option as being selected under this tab. This means that no programs, drivers or features have been disabled by MSConfig, and that Windows is booting up as normal. If you wish to boot up into Safe Mode instead you can select the 'Diagnostic startup' item - see the System Recovery section of the Backup & Recovery chapter. Of particular relevance to this chapter, to perform a quick temporary check to see the impact on functionality and performance of all of your startup items, you can enable the 'Selective Startup' option and untick the 'Load startup items' box then click Apply. When you next reboot your system, Windows will start up without loading any of the additional programs it would usually load at startup. You will then be able to observe firstly how much of an impact your startup programs are having on startup time, post-startup drive usage and general performance. However you will soon be able to see the types of functionality which is no longer available as a result of these startup items being disabled. This can range from not being able to open certain programs, to not being able to use certain features of various programs, or some of your hardware or devices not working correctly.

Make sure to run MSConfig again and reset it back to 'Normal startup' under the General tab, then examine the details below to see how to correctly identify and remove individual unnecessary startup items using MSConfig.

Startup: In previous versions of Windows, the Startup tab under MSConfig showed all the current programs which load into memory at Windows startup. This functionality has been transferred to the Start-up tab under the new Task Manager in Windows 8. Clicking the 'Open Task Manager' link here will open the start-up tab of Task Manager.

TASK MANAGER

Task Manager can be accessed by typing *Task Manager* on the Start Screen and pressing Enter, or by pressing CTRL+ALT+DEL and selecting 'Task Manager', or by right-clicking on the Taskbar and selecting 'Task Manager'. For more details of its functionality, see the Task Manager section of the Performance Measurement & Troubleshooting chapter. Below we examine its startup-related features.

Start-up: Under the Start-up tab of Task Manager, you will see several entries. All of these are for third party programs that have been installed; they are not core files or programs which are part of Windows 8. You should note the details under the Name and Publisher columns, as this information will help you determine the program or feature to which this startup item relates. You can right-click on any startup item listed here and select 'Open file location' if you wish to see the actual file that is being loaded at startup.

Windows 8 adds several ways to correctly determine the impact of a startup item, as detailed in this Microsoft Article. The 'Start-up Impact' column in the Start-up tab of Task Manager shows the overall impact of any startup program as follows:

- *High:* Apps or programs that use more than 1 second of CPU time, or more than 3MB of disk I/O at startup.
- *Medium:* Apps or programs that use 300-1,000 milliseconds (where 1,000 milliseconds = 1 second) of CPU time, or 300KB - 3MB of disk I/O at startup.
- *Low:* Apps or programs that use less than 300 milliseconds of CPU time, and less than 300 KB of disk I/O at startup.
- *None:* Apps or programs which would normally load at startup, but which are currently disabled from starting up, and hence have no impact.

If you have a lot of startup entries, click on the 'Start-up Impact' column to sort the apps from highest to lowest impact, then focus initially on those with a High or Medium impact rating.

To see just how much CPU time and disk I/O time a particular program is actually taking up at startup, right-click on one of the column headers and select 'Disk I/O at start-up' and 'CPU at start-up'. This will add two new columns to the Start-up tab of Task Manager which display this data. Once again, you can sort by these columns and focus on the entries that are taking up the most disk time and/or CPU time at startup.

Finally, to disable a startup entry, right-click on it and select Disable. This will change its status from Enabled to Disabled under the Status column, indicating that it will not load up the next time you boot up your system. This is the recommended way to initially disable a startup item, as it is easily reversible by coming back to this area of Task Manager, right-clicking on the entry and selecting Enable at any time.

To correctly identify which startup programs you can safely disable, see the Identifying Startup Programs section later in this chapter. Once you have determined with certainty that a startup item is not necessary for normal functionality, instead of just disabling it in Task Manager, you can permanently disable or remove it, as covered below.

REGISTRY EDITOR

The Registry Editor is a Windows tool detailed under the Windows Registry chapter. To launch the Registry Editor, type *regedit* on the Start Screen and press Enter. Below is a brief run-down of the primary locations where startup items are commonly held in the Registry, and how to permanently remove such entries.

The Windows Registry holds a record of the programs to launch at startup in five separate areas:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run]
```

If you find any items listed under any of these subfolders, it means they are set to run at Windows startup, with those under the `Run` keys being permanent items that run at every startup, and those under `RunOnce` being temporary items which only run for the next bootup. These items should already be listed under the Start-up tab of the Task Manager, as covered earlier. However some items will not appear there, such as malware-based entries.

You cannot temporarily disable a startup item using the Registry Editor. However, if you have determined with certainty that a particular startup item is not necessary, you can permanently delete it here by right-clicking on the correct value in the right pane and selecting Delete. Since there is no undo functionality in Registry Editor, you should consider doing a backup of the section of the Registry as covered in the Windows Registry chapter, before deleting any items.

AUTORUNS

Autoruns is an advanced and highly useful free startup file identification and removal utility with unique features not available in most other utilities. It also serves a range of other purposes covered throughout this book, so it is a highly recommended program.

To install Autoruns, download it, extract its contents to an empty folder, and run the *Autoruns.exe* file. Under the Everything tab you will see a large number of items which are loaded up with Windows - far more than most other utilities will ever show, and this is what makes Autoruns so valuable for a range of purposes. Many of the entries shown are required for various programs to run, and the majority are Microsoft items that Windows 8 absolutely needs in order to function correctly.

Correctly identifying and removing the truly unnecessary items using Autoruns is more complex precisely because it shows so much detail. To narrow down the list by removing the core Windows items, go to the Options menu and select 'Filter Options'. In the dialog box which opens, tick the 'Hide Windows Entries' item, and the 'Verify Code Signatures' items, then click OK. The list under the Everything tab should automatically refresh, but if it doesn't, click the Refresh icon or press F5 to update the list. The items shown will be reduced, with only those entries primarily relating to third party programs being displayed, making it easier to spot unnecessary items.

One of the key benefits of Autoruns is that it provides an easy method to either temporarily disable or permanently remove any item. This means that similar to the Start-up tab of the Task Manager, you can temporarily disable specific items to see what impact this has on the functionality for that particular program, as well as on Windows in general. Remember however that Autoruns is listing various components related to a range of programs, including shell extensions, filters, drivers, and services. Click on each suspicious item and look in the Details Pane at the bottom for more information. You can also right-click on an entry, select Properties and look under the Details tab for even more details. If still unclear, right-

click on the item and select 'Search Online' to initiate a Google search on the item's name in your default browser.

A combination of the displayed information, plus any additional information resulting from a web search should allow you to accurately identify the functionality that a component relates to. To temporarily disable an unnecessary item, simply untick its entry and Autoruns will prevent that item from loading up each time Windows starts up. Reboot and test to see the impacts of disabling such items. To permanently remove an item, right-click on the entry and select Delete. If in doubt, do not delete an entry.

< CORRECTLY IDENTIFYING AND REMOVING STARTUP PROGRAMS

So far in this chapter we have covered several tools with which you can view and either temporarily disable, or permanently remove, startup items. This section covers the correct procedure to run through in conjunction with the tools above.

The first step is to make absolutely sure that you have correctly identified the functionality of a startup item, to determine whether it is truly necessary, and if any desirable functionality will be impaired by disabling or removing it. Follow the steps below to try to correctly identify all of your startup programs:

1. Some filenames will tell you quite clearly what the startup program relates to. If in doubt, also check the directory path of the file and see if there are any other indications as to which program it relates to. It's important to know the actual program the file is for, firstly so you can tell what functionality may be affected for testing purposes, and secondly for the purpose covered in the next step.
2. Launch the program which the file relates to and look through its options for settings with names such as:

   Load with Windows
   Load at Startup
   Enable System Tray
   Enable Shell Integration

   In some cases you will be given the option to disable such settings, and you may also see text or a warning which explains whether doing so will affect the program's functionality in any way. Once you've undertaken this step, reboot and check to see which startup items have been removed or disabled in your startup, using both Task Manager and Autoruns.
3. If the filename still isn't clear, and you can't determine from its directory path which program it relates to (e.g. it resides in a general directory such as *\Windows\System32*) then you will have to do some online research to find out more details. Start by searching one of the following online resources using the exact filename:

   Windows Startup List Database
   ProcessLibrary
   Security Task Manager List

   And of course, search for the filename using a general web search engine. You should find some mention of the file, or discussion of it by others, which will help you both identify what program it relates to, and what functionality it affects if disabled. Note that some of the more obscure or new Windows 8 system files may not be listed in the sources above, or typically have ambiguous or even false information regarding potential malware, so make sure you read through a large number of web search results to find the truth.

4. If your research strongly indicates that the file may be malware, run Windows Defender in the first instance, then consider using a third party malware scanner if you are still in doubt - see the Security chapter. This will help ensure that the startup file in question is not malicious.
5. Use Task Manager or Autoruns to temporarily disable the startup item(s) in question - that is, Disable them under the Start-up tab of Task Manager, or untick them in Autoruns - then reboot Windows and test to see, over a period of several days, whether any of your regular program or Windows functionality is impaired. If still in doubt, leave the item temporarily disabled for an even longer period, and you should be able to categorically determine after a few weeks whether it is truly necessary.
6. Once you've followed all of the steps above, and you're confident that you've found a truly unnecessary startup item, you can permanently remove it using Autoruns or the Registry Editor. This isn't absolutely necessary, as an item which is disabled in Task Manager or Autoruns will remain disabled and hence have no system impact. Permanent removal is only for more advanced users who want to keep a tidy system and are sure that what they are removing is truly unnecessary.

Having disabled or removed unnecessary startup programs, make sure to run through the Services chapter and disable any unnecessary third party services as well.

< STARTUP TROUBLESHOOTING

Windows 8 is designed to prioritize boot programs, services and drivers such that the system reaches the Start Screen as quickly as possible, and if necessary continues loading programs as required in the background. In fact the Desktop will not be loaded up in Windows 8 until you actually launch it; only the Start Screen's Metro environment will be loaded by default to save resources and startup time.

The startup improvements in Windows 8 mean that the removal of startup programs may not improve system startup time to a highly noticeable degree. To get a completely objective measure of your startup time, and more importantly, to get accurate details with which you can troubleshoot startup-related problems, you should rely on the data found in Event Viewer.

To view your startup and shutdown statistics, and any associated problems, follow these steps:

1. On the Start Screen type *event viewer*, go to Settings, then press Enter to open Event Viewer.
2. In the left pane go to Applications and Services Logs>Microsoft>Windows>Diagnostics-Performance.
3. Double-click on the Operational log item shown in the middle pane, and you will see a range of events.
4. Look at the 'Task Category' column and select events with the names 'Boot Performance Monitoring' or 'Shutdown Performance Monitoring' (Event IDs of 100, 200 or similar).
5. Double-click on the more recent of these to open a window with details.
6. The precise startup time (Boot Duration) or shutdown time (Shutdown Duration) is shown in milliseconds (ms), which you can divide by 1,000 to get seconds. You can also see if any particular program or driver may be slowing down performance, as it will be noted here.

To quickly determine if the removal or disabling of any startup items is causing any errors, you can use the Reliability Monitor, which provides a user-friendly display of Event Viewer output. Follow these steps:

1. On the Start Screen type *reliability,* go to Settings, then press Enter to open the Reliability Monitor.
2. In the main chart look for any yellow exclamation marks or red crosses, as these indicate warnings and errors respectively.
3. Click on any particular warning or error icon and more details will appear in the bottom pane.
4. Double-click on the events shown at the bottom, or right-click and select 'View technical details'. This will display more details.
5. Check to see if a particular error references a file you have disabled.
6. Do additional research in the case of each error (red cross). In some cases, the warning or error can be safely ignored, as a program may be requesting a file and automatically generating an error code when it can't find it, but the startup file is not actually necessary for normal functionality.

For more details on Event Viewer and Reliability Monitor usage see the Event Viewer and Reliability Monitor sections of the Performance Measurement & Troubleshooting chapter.

< REGULAR MAINTENANCE

Removing startup items is far more important than most people believe. It is not a case of simply boosting your startup time, which is already quite fast in Windows 8. It is actually a critical step in ensuring overall system responsiveness, preventing stuttering and slowdowns, and also preventing potential crashes and conflicts which can otherwise be very difficult to resolve, and are often incorrectly blamed on Windows or third party drivers.

It is perfectly normal for almost all systems to have several startup items which need to be kept enabled and serve a useful purpose. However, any system that shows a long list of startup items is at risk of experiencing performance and stability issues. Remember that the software you use on your system may not have been tested in combination with all the various other background programs you are currently using, so the results can be unexpected. People using system-intensive applications and games will be the first to trigger any potential conflicts or performance issues in such scenarios. Make absolutely sure that you follow the procedures in this chapter, as well as the Services chapter, to remove all unnecessary startup items and minimize what runs at startup, and subsequently stays in the background during normal Windows usage.

Importantly, in the future as you install new programs, you should continue to regularly examine and identify any new startup items which are being added to your system and remove those which are not needed. I strongly recommend that after each installation of any new program you quickly open Task Manager and look under the Startup tab, and open MSConfig and check under the Services tab (with the 'Hide all Microsoft services' option ticked) to see whether any new third party items have been added. Take the time to determine whether these are really needed or not. Though tedious, this is an essential part of regular maintenance on a PC.

SERVICES

Services are customizable programs that run in the background and support specific system-wide functionality. They can be initiated by Windows itself, or they can be installed and initiated by third party programs. They may start automatically during or immediately after Windows startup, they may be triggered to start or stop at any time during Windows usage by the launching of certain programs, the use of particular functionality or under certain circumstances, or they can be blocked from running altogether.

Windows 8 contains several changes to the way in which services are handled from previous versions of Windows. It continues the ability, introduced in Vista and carried on in Windows 7, to set a service to 'Automatic (Delayed Start)', which means that it will only load after the Windows startup process has completed. It expands the use of Trigger Start services, first introduced in Windows 7. These services will begin or end only when a certain event is triggered or particular functionality is required, further reducing background resource usage. Windows 8 also carries over previous security and stability enhancements to isolate services such that they cannot be as easily compromised by outside attackers, nor can they be as easily destabilized by running programs. The end result is that core services in Windows 8 are already quite optimized, and thus do not require any user customization.

The primary focus of this chapter is on identifying and reconfiguring potentially unnecessary third party services inserted by installed programs, as similar to the startup programs covered in the previous chapter, these can have a noticeable impact on stability and performance in Windows.

< SERVICES UTILITY

The built-in Services utility gives you the ability to view and edit your Service configuration. To access this utility, you can either find it under the Administrative Tools component of the Windows Control Panel, or type *services.msc* on the Start Screen and press Enter. The Services utility displays all installed services, showing you whether they are currently running or not under the Status column, their Startup Type, and a brief description of their function. To see more details and configure a service, either double-click on the service, or right-click on it and select Properties. Here you can see the location of the actual file for the service under the 'Path to executable' item, and you can also manually Start, Stop or Pause/Resume a service. Importantly, you can change its startup type here.

The startup type of a service is defined as follows:

- *Automatic* - This service is loaded up during the Windows boot process and automatically started as soon as Windows starts.
- *Automatic (Delayed Start)* - This service begins loading automatically approximately 2 minutes after Windows has reached the Desktop.
- *Manual* - This service must be started manually by the user, or typically as requested by a program or feature when needed.
- *Manual (Trigger Start)* - The service can be started with a specific trigger event. It does not reside in memory nor load at startup otherwise. Once started and used, the service will then shut itself down after a set idle period.
- *Disabled* - This service is blocked from running and does not load up at any point, even if a program requires it. It can only be started by manually setting it to one of the above startup types first, then clicking the Start button.

BACKING UP SERVICES

Before we move on to examining service customization, it is important to backup your current service configuration in Windows in case you have any problems and need to return any of your services to their initial state. Services may be configured differently on various machines based on the particular features and programs you are using, as well as your specific hardware configuration.

To save a snapshot of your current service configuration before altering it, open the Services utility, then right-click on the 'Services (Local)' item in the left pane and select 'Export List'. In the box which opens, enter a name for the list and save it as the default 'Text (tab delimited) (*.txt)' option. This file will then save with all the details of your services as they currently stand, and can then be viewed with a text editor, or with correct formatting in a program like Microsoft Excel.

WINDOWS SERVICES

The Windows 8 Service Controller has already been refined to configure your services such that you have full functionality for all the features you use in Windows without unnecessary resource usage. For our purposes, the main reason we would want to change the service settings is to:

§ Help speed up Windows startup time, especially on older systems with slower hard drives.
§ Help reduce post-startup drive activity, since Windows relegates some services and programs to loading in the background well after startup.
§ Reduce RAM and CPU usage by preventing unwanted services from running in the background.
§ Prevent program conflicts, instability, and even security risks, by removing unwanted services.

Fortunately, the majority of the default Windows 8 services are configured as Manual or Manual (Trigger Start), and hence do not load at startup or run in the background unless actually required. This means that the bulk of the benefits previously inferred through service customization in earlier versions of Windows, such as XP or Vista, are already evident in Windows 8 by default.

Altering Windows services should no longer be considered a significant performance tweak, if it ever was. You should not set any service to Disabled unless part of a specific step to deliberately disable an unnecessary function in Windows, as covered in various chapters throughout this book. There is no other benefit to disabling a service; a service set to Manual or Manual (Trigger Start) takes up no resources, yet provides a safeguard, because if it is truly needed, it can usually be restarted by Windows or a program.

For example, the Bluetooth Support Service is set to Manual (Trigger Start) by default, and only starts running if a Bluetooth device is connected to your PC. Setting it to Disabled if you don't have any Bluetooth devices provides no benefit. Only disable a service if you are absolutely certain that its functionality is undesirable on your system, and more importantly, if it would otherwise start running in the background even when set to Manual. In practice there are few Windows services that do this, and again, where they do, I have provided more details on which services you can disable under the relevant features in this book.

Furthermore, some Windows services can be very misleading as to the impact any changes to their configuration might have. Disabling one can break functionality in another, seemingly unrelated, area due to complex dependencies. I stress again that you should not consider the disabling of core Windows services as some sort of major performance tweak. Focus on adjusting any services installed by third party programs, as covered in the next section.

< NON-MICROSOFT SERVICES

Particular software, such as graphics drivers, malware scanners and system utilities, can install their own unique services. These services are not part of Windows by default, but may be required for some of the specialized functionality of the programs you have installed. Due to poor programming practices, the software developer may also set a service such that it is always running in the background, even when not required. As such, in many cases third party services can be set to Manual, or even Disabled, to speed up startup time, reduce background resource usage and prevent conflicts, without affecting the program's core functionality in any significant way.

The quickest and easiest method of displaying all third party services on your system is to run MSConfig by typing *msconfig* on the Start Screen and pressing Enter. Go to the Services tab and tick the 'Hide All Microsoft Services' box at the bottom. The only services which will then be shown are those that have been installed by third party software. To determine which of these are truly unnecessary, you will have to work out which software package has installed the service. In most cases it is fairly obvious because of the service name, however some services are not clear, or may even be part of malware and hence difficult to identify.

To correctly identify which program a service relates to, and in particular which file is launching it, follow these steps:

1. Write down the exact name of each non-Microsoft service.
2. Open the Services utility and find the same service name in the listing.
3. Double-click on the service and under the General tab for that service, look under the 'Path to executable' item, noting both the filename and its directory path.
4. If the step above doesn't help you identify the program launching the service, and if the service is currently running, launch Task Manager and under the Services tab see if you can find the service. Typically the service name you found under Step 1 above will correspond with the Description of it here. You can then right-click on it and select 'Go to details' or 'Search online' to find out more about it.
5. Conduct a web search, or check one of the databases linked under the Startup Programs chapter for this particular service filename or description. This should give you an indication of what its functionality is related to.
6. You can temporarily Stop the service, or set it to Disabled and reboot, to see what functionality it impacts on.

Many third party services can safety be set to Manual, or even Disabled, reducing unnecessary background resource usage and preventing potential software conflicts. In a few cases particular programs will not function correctly unless their service is left at Automatic.

Finding and preventing unnecessary third party services from launching is a tedious but important step in maintaining optimal performance on your system, so take the time to do it properly, and make sure to keep doing it every time you install a new program.

< CUSTOMIZING SERVICES

Aside from the Services utility, there are several other ways in which you can customize services, and these are covered in this section.

CHANGE SERVICE STATUS VIA COMMAND LINE

If you wish to change the status of a service without opening the Services utility, you can do so by using a Command Prompt. This is useful for example if you have changed a critical service such that you cannot

successfully boot back into Windows, or if you want to compile a batch file to start or stop a range of services at any time.

To alter a service via the command line you will need to know the name of the service, either its short name or full name. For example, the full name for the Windows Defender service is 'Windows Defender Service', while its short name is WinDefend. You can find these details in the Services utility by double-clicking on a service and looking at the 'Service Name' field at the top, or by looking at the subfolders under the following key in the Windows Registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]
```

To start or stop a service via command line, open an Administrator Command Prompt and use the form:

```
Net [Start/Stop] "servicename"
```

Note, if using the short name for a service, quotes are not necessary, but if using the service's full name, quotes must be used. For example, to start the Application Layer Gateway Service, you can use either command shown below to achieve the same result:

```
Net start alg
Net start "application layer gateway service"
```

You will receive a confirmation that a service has been started or stopped if successful.

TRIGGER START SERVICES

Service Trigger Events were introduced in Windows 7, and are one of the optimizations which help reduce the number of active services actually running at any time in Windows 8. Instead of constantly needing to run in the background to be ready for usage, trigger-start services only start or stop when a specific event occurs. The specific events that can trigger such services are:

- Device interface arrival - When a device is connected or removed from the system.
- Domain join or leave - When a person joins or leaves a particular domain in a network.
- Firewall port opened or closed - When a particular port is opened or closed in the Firewall.
- Group policy updates - When a particular Group Policy condition occurs.
- IP address - When an IP address is acquired or lost; typically upon accessing the Internet.
- Custom ETW event - When a custom Event Tracing for Windows (ETW) event occurs.

This means that a service which looks for the connection of a particular device for example will not constantly run in the background waiting for the connection; it will only start up when that type of device is connected, and will stop a short while after the device is disconnected. Services need to be written to take advantage of this feature, so many third party programs are unlikely to use them, hence the recommendation to find and disable unnecessary third party services still stands.

You can see which services are set to 'Manual (Trigger Start)' in the Services utility, but you cannot view the detailed aspects of trigger-start services there. You will need to use the Command Line method and the `SC` command to view and alter triggers. Type `SC /?` in a Command Prompt to see a full list of options for this command. To view the trigger conditions on any service, do the following:

1. Open an Administrative Command Prompt.
2. Determine the correct name of the service for which you wish to see a trigger event - see the previous section above for instructions on how to do this.
3. Type the following:

   ```
   sc qtriggerinfo servicename
   ```

   e.g.:

   ```
   sc qtriggerinfo bthserv
   ```

   This will show that the Bluetooth Support Service, which is set to Manual (Trigger Start) by default, is actually set to start for the trigger event Device Interface Arrival, meaning it is triggered by the connection of a Bluetooth-capable device.

To attempt to add a trigger to a particular service, use the `SC triggerinfo` command to see a list of possible options. For most purposes there is no need or use in attempting to do this as it is quite specialized. Services are best left to be configured correctly by the software developer to be trigger-aware.

PERMANENTLY DELETING SERVICES

There are times when a particular third party program or malware installs a custom service, and then does not completely remove it upon being uninstalled or forcibly removed. If you wish to delete a service from your system - and obviously this must only be done if you are certain that the service is completely unnecessary - then follow the steps below:

1. Open an Administrative Command Prompt.
2. Determine the correct name of the service which you wish to remove - see earlier sections above for instructions on how to do this.
3. Type the following:

   ```
   sc delete servicename
   ```

4. You will see a message indicating that the process is successful, and you will no longer see that service displayed in the Services utility.

If you do not feel comfortable using the command line method, then you can use the free Total Service and Driver Control (TSDC) utility. Run TSDC, let it enumerate your drivers and services, then click OK. Select the service you wish to delete from the list and click Remove, then reboot.

Use extreme caution when permanently deleting a service. Deleting a necessary service can cause major problems and will usually require the reinstallation of the program to get it back. The situation will be made even worse if you manage to delete a core Windows service, so only attempt deletion of known third party services that are left after uninstallation of a program.

< BACKGROUND TASKS

There is one more type of background program similar to a service, in that it involves the running of background processes: scheduled tasks. These tasks are scheduled to run in the background, typically when Windows is idle, or at particular times of the day, and is one of the reasons why you may see drive activity when your system is not being used. Just like core Windows services, these tasks are not meant to be directly altered by the user, and in most cases should only be configured through the normal Windows interface for various utilities. For example, you can use the Automatic Maintenance feature added in Windows 8 to

determine when a range of automated background maintenance tasks are run - see the Windows Action Center section of the Performance Measurement & Troubleshooting chapter.

This section looks at ways in which background tasks can be created or customized in greater detail.

TASK SCHEDULER

A task will only begin running when a particular trigger event occurs, and even then, only under certain conditions. These can be viewed and altered within Task Scheduler, the main utility for managing tasks in Windows. You can access the Task Scheduler at any time by going to the Start Screen, typing *taskschd.msc* and pressing Enter.

In the left pane of Task Scheduler is a library of tasks, which you can expand to see in more detail. Under the Task Scheduler Library>Microsoft>Windows folder are a series of subfolders relating to a wide range of features in Windows. Each of these sub-folders can contain one or more tasks relevant to that feature. For example, under the Defrag subfolder is the ScheduledDefrag task, as shown in the middle pane. This relates to the scheduling functionality in the Optimize Drives feature, covered under the Optimize Drives section of the Drive Optimization chapter.

Importantly, the current status of a task is shown next to its name in the middle pane:

§ *Ready:* The task is ready to be run, but no instances of it are queued or running.
§ *Queued:* One or more instances of the task are queued to be run.
§ *Running:* One or more instances of the task are currently running.
§ *Disabled:* No instances of the task are queued or running, and the task cannot be run until enabled.

You can view more details on the task, as well as customize its parameters, by double-clicking on it, or right-clicking on it and selecting Properties, to open a new window for this purpose. Each tab of the Task Properties window is covered below:

General: Describes the task, and allows an Administrator to configure the privilege level, select the user account under which the task will initiate, and whether the user needs to be logged on or not for the task to run.

Triggers: This window contains the trigger event that launches the task. This can be on a schedule, at log on, at Windows startup, on idle, on connection/disconnection to a user, or workstation lock or unlock for example. Click the Edit button to open the Edit Trigger window, and select the event type from the 'Begin the task' drop down box. Under 'Advanced Settings' you can adjust additional parameters, such as stopping a task if it runs longer than a certain length of time. Note that you can add multiple trigger events to a single task. Bear in mind however that the task will only successfully run in conjunction with the parameters under the Conditions tab.

Actions: This window contains the action which is initiated when the task runs. This can be the launching of a program or script, the sending of an email, or the display of a particular message.

Conditions: If the trigger event occurs, then the Task Scheduler will check for any conditions which prevent a task from running, as determined by the options in this window. For example, if the 'Start the task only if the computer is idle for' box is ticked, then the task will wait until the computer has been idle for the length of time specified before actually commencing. These conditions ensure that certain tasks don't simply launch regardless of current system conditions, such as running a drive optimization during the use of a system-intensive program.

Settings: The settings under this tab allow additional control over the way in which the task runs, especially if it fails, takes too long and/or hits another running instance of itself.

History: This tab lists a history of the task, however this feature may be disabled. To enable task history, click the 'Enable all task history' link in the right pane of the main Task Scheduler window.

To view all currently running tasks, first go to the View option in the right pane, click it and make sure 'Show Hidden Tasks' is ticked. Then click the 'Display all running tasks' link in the right pane, and a window will open with the tasks listed - you can manually force any of these to end if you wish, though this is not recommended unless you are troubleshooting.

You can manually change any task's status by selecting the task in the middle pane, then clicking on the Run, End or Disable links in the right pane.

FORCE IDLE TASK PROCESSING

To force all tasks currently scheduled to run at idle to run immediately, do the following:

1. Open an Administrator Command Prompt.
2. Type the following and press Enter:

   ```
   Cmd.exe /c start /wait Rundll32.exe advapi32.dll,ProcessIdleTasks
   ```

3. Do not do anything on your system, including moving the mouse, until the prompt appears again, indicating the successful completion of all idle tasks. This may take a while.

This method can be useful both to test a task you have customized to run at idle, and also if you want to ensure an idle task doesn't attempt to run in the background during a critical period, such as during a firmware update in Windows.

CREATE A TASK

Task Scheduler not only allows you to edit existing tasks, it also lets you add your own tasks. To add a custom task, click the 'Create Basic Task' link in the right pane, and you will be presented with an automated Wizard which will step you through the process. For example, if you leave your computer on at home all day long while you are at work, you can create a custom task which emails you if your system experiences a particular error. This would be done as follows:

1. Highlight a category in the left pane in which to locate the new task, or create an entirely new category for it by selecting the 'Task Scheduler Library' category and then clicking the 'New Folder' link in the right pane.
2. Select the newly created folder in the left pane.
3. Start the Create Basic Task wizard from the right pane.
4. Enter an appropriate name for the task, e.g. Email Alert, then click Next.
5. On the Trigger page, under 'When do you want the task to start', select 'When a specific event is logged' and click Next.
6. The options here tie in with the Event Viewer, which is covered under the Event Viewer section of the Performance Measurement & Troubleshooting chapter. This means that you have to select a particular Log category and Source from the Event Viewer logs, and enter a specific Event ID. Then when this Event ID is recorded by Windows, it will trigger your task to commence. Click Next.
7. Under the 'What action do you want the task to perform', select 'Send an e-mail' and click Next.
8. Enter your email details and the subject and body of the message, plus any attachments you wish to send.

9. Click Finish to implement the task.

Alternatively, instead of Steps 1 - 5 above, you can open Event Viewer, right-click on a particular event and select 'Attach Task to this Event' - see the Event Viewer section of the Performance Measurement & Troubleshooting chapter.

Having been created, the custom task is now in Ready state, and will run when it hits the appropriate trigger, sending you an email. This allows you to monitor your PC's state from anywhere at any time. Once created, you can edit the task further just like any other task, for example setting it to run only when you are logged off but the machine is still on.

The primary use for Task Scheduler is for more advanced users to either remove unnecessary tasks inserted by third party programs, to add new tasks, or customize an existing Windows task more thoroughly to allow it to run under a particular set of conditions which better meet your needs. You should not disable normal Windows diagnostic and maintenance tasks, as this can make Windows less secure and less stable.

Task Scheduler can be turned off altogether by forcing the 'Task Scheduler' service in the Services utility to Disabled. This is not recommended at all, as Task Scheduler is an important component and disabling it prevents any scheduled tasks from running, some of which have important system maintenance functions.

Service editing used to be an area of ongoing debate, with some people suggest that altering services from their default was completely pointless and unnecessary, and should not be done due to the potential problems it can cause; while others argued that many services can be disabled to increase performance. With the coming of Windows 7, the debate was all but settled, and Windows 8 reinforces the point: there is now not much of a case to be made in altering the core Windows services. Windows 8 has already been optimized in this regard by Microsoft, and any changes are more likely to result in unforeseen problems rather than any real benefits. In a select few cases, there may be legitimate need to disable a particular service as part of forcing certain functionality to be disabled in Windows, such as disabling the HomeGroup-related services on a non-networked PC, or disabling SuperFetch on an SSD if Windows does not do it automatically for some reason.

However, just as we removed unnecessary startup items under the Startup Programs chapter, there is still a genuine need for all users to identify and alter the configuration of unnecessary services installed by third party programs. Due to lazy, and sometimes deliberately deceptive, programming practices these services often launch when they are not required, and sit in the background, adding to startup time and background resource usage, increasing the security risk and greatly increasing the potential for system instability or conflicts on your system. Remember that not all software developers are particularly concerned about instigating inconvenience or additional resource usage on your system as long as it serves the purpose required by their own software. This is why editing services is still essential - but only for removing unnecessary third party impositions.

WINDOWS REGISTRY

The Windows Registry is a central database for holding a range of important system and program-related data. Whenever you change certain Windows settings, install new programs or apps, or even resize open windows for example, the Registry will be updated with key pieces of information recording these changes.

In Windows 8 the Registry remains much the same as it has been in previous versions of Windows. As of Windows Vista, some improvements were made to decrease the possibility of Registry corruption. Virtualization support was also added to the Registry as part of the User Account Control feature, allowing the redirection and successful installation of applications which otherwise require full Administrator access to write to protected portions of the Registry. As of Windows 7, Registry Reflection was removed for 64-bit operating systems.

This chapter examines the Windows Registry in detail, both in terms of its structure and how it operates, as well instructions on how users can change Registry settings to implement a range of customizations in Windows. Knowledge of the Windows Registry is essential for fine tuning system performance and functionality, as well as troubleshooting and system recovery.

< BACKUP AND RESTORE THE REGISTRY

The Windows Registry is a critically important component of Windows. By default, any changes made to the Registry can't be easily reversed, so it is vital to back up both the entire Registry, and selected portions of it in one or more of several ways, before considering making any changes to it.

BACKING UP THE ENTIRE REGISTRY

If your Registry becomes damaged or corrupted, whether through data corruption from overclocking or hardware failure, or through malware infestation or user-initiated changes via the Registry Editor for example, you will experience serious problems in Windows 8 which ultimately only the reinstallation of Windows can resolve. To avoid this, you should regularly back up the Registry before making any changes.

Windows has a built-in tool for periodically taking a snapshot of the Registry and other important system files and settings: the System Restore feature, as covered under the System Protection section of the Backup & Recovery chapter. I strongly recommend that you leave System Restore enabled, and manually create a restore point before editing the Registry, or undertaking any other potentially risky procedures. This will supplement the restore points which Windows automatically creates whenever you install drivers or install updates via Windows Update for example. Then if you experience what you believe is a Registry-related problem, you can use System Restore to easily undo any recent changes made to the Registry, without any impact on your personal files or folders, or your other program settings.

You can also use the built-in Export functionality of the Registry Editor to make a Registry backup. To open the Registry Editor, type *regedit* on the Start Screen and press Enter. Then go to the File menu, select Export, and at the bottom of the Export window, select All for 'Export Range'. Give it a suitable name and save this Registry backup somewhere safe. There are two problems with this method however: it does not save all parts of the Registry; and when restoring this backup (by double-clicking on it), it will simply merge the backup version with your existing Registry - this means it will not remove any new Registry entries made since the backup. Therefore this method should only be used to undo a change, rather than restore your Registry to its original state.

If you cannot boot into Windows after a change to the Registry, you will need to turn to the options available in the Windows Recovery Environment, covered under the System Recovery section of the Backup & Recovery chapter.

BACKING UP PORTIONS OF THE REGISTRY

Restoring a Registry backup by using System Restore can be overkill if you simply want to undo a single small change to the Registry. Since most users typically make minor individual changes to the Registry, a more practical precaution is to make a backup of the particular branch of the Registry you are about to edit, especially if you don't feel confident about making the change, or aren't sure how the change will impact on your system. That way if anything goes wrong, you don't have to go through a Registry recovery process which may also undo other changes you wish to keep - you can simply restore the individual branch that you have changed quickly and easily.

The steps to backing up a specific Registry branch or key are as follows:

1. Open the Registry Editor.
2. In the left pane of the Registry Editor window, right-click on the name of the particular sub-key that holds the settings you wish to edit.
3. Select the Export option, and choose a suitably descriptive name and appropriate location for the file. Make sure that the 'Selected Branch' option is ticked at the very bottom of the box, so that only that particular branch and all its sub-components are saved. Click the Save button and the file will be saved with a .REG extension.
4. Once the relevant section of the Registry has been saved, you can go ahead and make the desired changes to this branch of the Registry.

If you experience any undesirable behavior after your Registry changes - and remember that some Registry changes require a reboot, or logoff and logon, before their effects can be seen - then you can restore this backup of your Registry by going to the place where you saved the .REG file and double-clicking on it to upload it to your Registry. This will overwrite the existing sections of the Registry with the backed up version, effectively undoing your changes. Reboot, or logoff and logon again, to implement the change.

< REGISTRY EDITOR

The Registry Editor is the primary built-in tool used to view and edit the Windows Registry. To access it type *regedit* on the Start Screen then press Enter. The structure of the Registry is explained further below, but essentially the Registry Editor displays a File Explorer-like view of the database as a range of folders and subfolders that can be navigated just like any other Explorer-based interface.

The main reason for editing the Registry is to alter settings and features that cannot otherwise be changed using the normal Windows interface. Learning to use the Registry Editor is important because it is the most direct method of altering the Registry. Using it ensures that you are aware of precisely what has been changed, and where in the Registry it resides, should you need to change it back. For this reason, wherever possible I recommend against using third party tools that purport to automatically optimize or make changes to the Registry, and in particular I discourage the use of pre-made .REG Registry scripts which you can download. While very convenient, the use of these methods, aside from being a security risk, can result in a range of problems that you will not be able to easily resolve. If you feel you are not advanced enough to use the Registry Editor, then by the same token you are not advanced enough to deal with any potential problems third party tools or .REG files may wreak on your system, and you should steer clear of them until you learn more about the Registry Editor.

REGISTRY STRUCTURE

When you first open the Registry Editor, you will see that the Windows Registry is broken down into a five main folders, also known as Hives or Root Keys:

```
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
```

Each of these is described in more detail below:

`HKEY_CLASSES_ROOT` - This section of the Registry holds information related to the functionality of installed applications, such as file associations. The data here is actually a combination of that held under the `HKEY_CURRENT_USER\SOFTWARE\Classes` and `HKEY_LOCAL_MACHINE\SOFTWARE\Classes` keys - in other words it contains relevant user-specific settings, as well as system-wide settings respectively. If there are any duplicated values, those stored in `HKEY_CURRENT_USER\SOFTAWRE\Classes` are used.

`HKEY_CURRENT_USER` - This section of the Registry holds information for the user who is currently logged on. This folder is actually a sub-key of `HKEY_USERS`. The current user's key Windows settings are stored here, and saved in the *ntuser.dat* system file found under the root directory of the user's *\Users\[username]* directory.

`HKEY_LOCAL_MACHINE` - This section of the Registry stores settings that are specific to the entire computer and affect any user. This includes data on system drivers, hardware devices, services, various software, and Windows settings that apply to the entire PC and not just an individual user account.

`HKEY_USERS` - This section of the Registry holds all of the actively loaded user profiles on the PC. Each user profile folder has a unique Security Identifier. You can match the folders to particular user profiles by going to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList` clicking on each of the sub-keys there, and looking at the value for `ProfileImagePath`.

`HKEY_CURRENT_CONFIG` - This section of the Registry holds information about the hardware profile that is used by the computer at system startup. The data here is not permanently stored on disk, it is regenerated at boot time and is linked to `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current`.

Aside from `HKEY_CURRENT_USER` whose data is saved locally under the root directory of the current user's personal folders as noted above, the remaining Registry locations have a range of data saved under the *\Windows\System32\config* directory.

The way in which particular locations in the Registry are referenced throughout this book typically involves the following format:

```
[Hive Name\Key Name\Sub-Key 1\Sub-Key 2 (etc.)\]

Value Name = Value Data
```

In other words, under the five main `HKEY_` hives, the subfolders are usually referred to interchangeably as keys, sub-keys or subfolders. When you left-click on any one of those keys, the items displayed in the right pane are called values. Square brackets are often used to contain the full path to the desired subfolder, preventing confusion as to where a key name ends and a value name begins.

Each value has a name, type and some data:

Value Name - A value can have any name, as these are assigned by the software developer. The names are usually descriptive in some way, but at other times they may just be a string of numbers and/or letters.

Value Type - A value entry is always one of the following general types:

- STRING - A String value is any combination of letters and numbers, such as common words, directory paths, etc. This includes MULTI-STRING VALUE and EXPANDABLE STRING VALUE which are string variants.
- BINARY - A Binary value is raw data displayed as a table in hexadecimal view. Note that the hexadecimal system view uses the normal numbers 0 - 9, but for 10 - 15 it uses the letters a - f (i.e. a = 10, b = 11, c = 12, d = 13, e = 14, f = 15). This allows the display of various byte values in binary code as single characters.
- DWORD - A Dword value is a series of whole numbers which can be displayed in either hexadecimal or decimal view.
- QWORD - A Qword value is similar to a Dword, however it can be longer because it is a 64-bit integer as opposed to a Dword which is a 32-bit integer. It can be displayed in either hexadecimal or decimal view.

Value Data - The value data will differ depending on the value type. It can be letters, numbers, or a combination of both. The restrictions of each value type determine what can be entered as data for a value, plus of course the actual use that particular value has. For example, if a value is designed to tell a program the path to a particular executable file, then entering a string of numbers is meaningless, because a properly formatted and valid directory path is required.

In summary, if the Registry Editor is viewed as being similar to File Explorer, then we can consider the root keys or hives to be like parent folders in a directory tree; each sub-key under them is a subfolder; and the values stored under them are like files containing specific data. Just like the File Explorer interface, you can also edit, create or delete Registry entries.

The best way to understand all of the above information is to go through an example, as provided below.

EDITING REGISTRY ENTRIES

To edit an existing Registry entry, follow the example below to see the correct procedure:

```
[HKEY_CURRENT_USER\Control Panel\Desktop]

CursorBlinkRate=200
```

The two lines of text above indicate that to make this Registry change, you should open Registry Editor and then:

1. Double-click on the `HKEY_CURRENT_USER` root key, or click the small white arrow next to it in the left pane of the Registry Editor window. This will show every subfolder sitting directly under it.
2. Next, you must double-click on the `Control Panel` sub-key.
3. Left-click once on the `Desktop` sub-key to select it.
4. In the right pane of the Registry Editor window, look for a value called `CursorBlinkRate`.
5. Double-click on this item, and in the box that opens, click in the Value Data box - note its original value.
6. You can edit this value data by entering a new value if you wish, such as `200`.
7. As soon as you click OK, the change is automatically saved to the Registry.
8. You can close Registry Editor if you wish.
9. You may need to restart Windows, or logoff and logon, for the change to be implemented.

In the example above, I did not provide any explanation as to what impact editing this value would have. However, even without instructions you can deduce the likely impact, because the location points to the HKEY_CURRENT_USER hive, which as discussed earlier, relates to user-specific settings. Furthermore, the sub-keys Control Panel and Desktop hint at the fact that this setting is likely normally set in the Windows Control Panel and affects the Windows Desktop. Finally, the value name CursorBlinkRate points quite clearly to the likelihood that altering this value controls the rate at which the cursor blinks when displayed in normal Desktop interfaces. Of course, in this case editing this value via the Registry is a bit pointless, since we can easily change it through the Keyboard component of the Windows Control Panel.

Many Registry settings are not so simple to deduce, or more importantly, do not have the intended impact if changed. While you can experiment to find out what a setting does, most commonly you need to have specific instructions which explain what a setting does, the valid values for it, and the actual impact of changing these values, plus whether you need to reboot, or logoff and logon, for the impact of the change to come into effect. Still, as the example above demonstrates, by understanding the basics of how the Registry structure works, you will be better equipped to edit the Registry on your own and deduce what various entries mean.

This chapter does not contain any specific Registry customizations you can use. A range of the most useful of such tweaks are spread throughout this book in relevant chapters.

Creating and Deleting Registry Entries

At various times you may need to create a new key or value if it does not exist by default in your Registry. To create a new entry from scratch correctly, follow this procedure:

1. Go to the particular subfolder under which you need to create a new key.
2. Right-click on the relevant sub-key and select New>Key to create a new subfolder beneath it; alternatively, select New> and the correct value type to create a new value entry in the right pane.
3. Enter the name for the new key or value and press Enter.
4. To confirm that the new key or value is in the correct location, left-click on it and look at the bottom of Registry Editor to see if the full path matches that which you desire.

The Registry Editor does not give any indication that you've entered a valid key or value, so there is no way to know if what you have created is correct, aside from carefully checking the instructions you were following, and then testing to see if it has the intended impact. Remember, you may need to reboot, or logoff and logon again, to correctly implement a Registry change.

To delete a key or value, simply go to the particular key or value you wish to remove, right-click on it and select Delete. Take all possible care to make sure that what you're deleting is the correct key or value, and that you trust the source which has instructed you to do so, otherwise you may be doing irreparable damage to the Registry. Create a backup of that portion of the Registry before deleting it just in case.

Registry Permissions

In certain cases if you attempt to edit an entry in the Registry, you may see an error, or will be told that you do not have permission to do so. This is normal, as some locations in the Registry are protected against changes by anyone who is not an owner. See the Access Control and Permissions section of the Security chapter for ways of taking ownership and thus giving yourself full permission to make changes to these areas.

Finally, as noted earlier, you may need to reboot for the impact of any edited, created or deleted Registry entries to come into effect. However you can simply logoff - even if you only have one user account - by going to the Start Screen, clicking your user account picture in the top right corner, and selecting 'Sign Out'. Once logged off, click your account name to log back in again, and the Registry change will be loaded. You can also try restarting the *explorer.exe* process instead, as covered under the Advanced Settings section of the File Explorer chapter. Rebooting Windows is the best way to ensure that a Registry change comes into effect.

< MAINTAINING THE REGISTRY

The Windows Registry has thousands of entries, and just like any large database, over time some of these entries can become obsolete due to changes in hardware and software, and some entries can even become corrupted due to bad shutdowns, overclocking, or faulty software or hardware for example. For the most part the Windows Registry is self-maintaining, and on balance I recommend against running any utilities which attempt to "optimize" the Registry by cleaning it. There are more risks involved, and more likelihood of unintended consequences, than any marginal benefits.

For the sake of completeness, and also for more advanced users who feel ready to accept the risks, and want to use a Registry cleaner to assist in removing debris left over from bad driver or program uninstalls, then this section briefly covers the topic of Registry cleaning.

The program you can use for this functionality is the free CCleaner utility, which has a relatively trustworthy Registry cleaning capability, as described below:

1. Open CCleaner and click the Options button on the left side.
2. Click the Advanced button and make sure there is a tick against the 'Show prompt to backup registry issues' box.
3. Click the Registry button on the left side.
4. I recommend ticking everything under the Registry Integrity section except 'Unused File Extensions', 'Start Menu Ordering' and 'MUI Cache'.
5. Click the 'Scan for Issues' button and wait for the scan to complete - nothing will be altered.
6. Examine the list carefully, focusing on any entries related to programs or drivers which are no longer installed on your system, and leave a tick next to these entries. Untick any others unless you are absolutely sure they are safe to remove.
7. Click the 'Fix selected issues' button to commence removal of the ticked Registry entries.
8. When prompted, click Yes to backup Registry changes and save the backup to an appropriate location.
9. Click the 'Fix All Selected Issues' button then click OK to remove all ticked items from the Registry.

Over a period of several days, if Windows features or any of your programs start acting strangely, you can undo the changes resulting from this Registry cleaning by double-clicking on the backed-up .REG file you saved in Step 8 above and rebooting. See the CCleaner section of the Cleaning Windows chapter for more details on using this utility.

For general users I recommend against using any Registry cleaning or optimization tools due to the substantial risks compared with the marginal benefits which come from using these utilities in Windows 8. Any form of automated change to the Registry is dangerous.

The Windows Registry is a vitally important component of Windows, a central database holding a range of critical information. If it is damaged, or if parts of it are altered or removed without adequate knowledge, you may run into major problems, which in the worst case scenario could require the full reinstallation of Windows. For this reason I urge you to become familiar with the Registry as covered in this chapter. It is also strongly recommended that if you have doubts about altering the Registry in any way, it is best to leave it alone for now. None of the Registry changes listed throughout this book are absolutely necessary.

GROUP POLICY

Group Policy is designed primarily for Administrators to manage the way in which Windows behaves for different user groups on a network. When a Group Policy is in place, it tells Windows to override its normal settings and use those specified by the policy. Group Policy remains much the same in previous versions of Windows, however there are a range of new settings and some interface changes. Because Group Policy is actually designed for network administrators, and also because of its complexity, it won't be covered in great detail in this book. This chapter is mainly about Group Policy-related features which the average home PC user may find handy.

You can also use the Windows PowerShell or the Windows Registry to change many of these settings. Aside from being covered briefly under the Administrative Tools section of the Windows Control Panel chapter, detailing PowerShell usage instructions is beyond the scope of this book. Editing the Registry to change Group Policy items similarly requires lengthy and detailed descriptions, as almost all of the Group Policy settings do not exist in the Windows Registry by default and need to be created, and their various values documented. If you wish to attempt to implement these settings using the Registry method, see the Windows Registry chapter along with this Microsoft Article containing a spreadsheet listing the relevant Registry keys and values.

< LOCAL GROUP POLICY EDITOR

Configuring Group Policy for the average home user is done via the Local Group Policy Editor, which is only available in Windows 8 Pro and Enterprise editions. If the Local Group Policy Editor is not available to you, try the Registry method mentioned in the introduction above to change these settings.

To access the Local Group Policy Editor, type *gpedit.msc* on the Start Screen and press Enter. The Local Group Policy Editor has two main branches: 'Computer Configuration' and 'User Configuration'. Changes made under the 'User Configuration' sections affect a particular user regardless of which machine they are on; changes made under the 'Computer Configuration' section apply only to the current machine, and hence affect all users on that machine. The Security Settings found under the Computer Configuration branch are the same as those covered in detail under the Local Security Policy section of the Security chapter, and won't be covered again here.

The Local Group Policy Editor can be useful in letting you change particular settings and features beyond the ability provided within the normal Windows interface. For example, if you wish to prevent users on your system from accessing specific features, a change via Group Policy allows you to easily remove access to virtually any component of Windows for other users on your PC or home network.

To change a setting, go to a specified subfolder and double-click on the setting in the right pane, then choose Enabled, Disabled or 'Not Configured' as required and click Apply. The default for each setting is usually 'Not Configured' unless otherwise noted, which means the normal Windows settings apply because the Group Policy is not configured to override them. Before changing a setting, make sure to read the Help text provided. If in doubt, do not alter a setting; none of the changes provided below are necessarily recommended.

PREVENT ACCESS TO A SPECIFIC WINDOWS FEATURE

Folder: User Configuration\Administrative Templates
Setting: Various

Under this branch of the Local Group Policy Editor you can find many subfolders with a range of Windows features and functions to disable. Some of these are covered below, otherwise you should browse through all of the subfolders and settings here to see if any of them suit your purposes.

PREVENT ACCESS TO THE WINDOWS STORE

Folder: User Configuration\Administrative Templates\Windows Components\Store
Setting: Turn off the Store application

If Enabled, this setting will prevent access to the Windows Store Metro app on the Start Screen. This can be useful in preventing other users from making unauthorized purchases in the Store, or downloading and installing a large number of mostly useless free apps. Note that access to the Windows Store is required if you wish to update existing installed apps.

HIDE SPECIFIC CONTROL PANEL ITEMS

Folder: User Configuration\Administrative Templates\Control Panel
Setting: Hide specified Control Panel items

If Enabled, allows you to choose which components of the Windows Control Panel you wish to hide. Click the Show button, then click the Add button in the box which opens. You will have to manually type in the full correct name of the Windows Control Panel component. For example, to hide the Phone and Modem component in Windows Control Panel, click the Show button, type *Phone and Modem* in the Value box, and click OK. When finished adding components to the list, click OK and then click Apply, and when you next open the Windows Control Panel the relevant component(s) will be missing. Set this policy to Disabled or Not Configured, or delete the item(s) from the list under Show, to restore the relevant hidden item(s) in Windows Control Panel.

MODIFY CTRL+ALT+DEL SCREEN

Folder: User Configuration\Administrative Templates\System\CTRL+ALT+Del Options
Setting: Remove...

Here you can specify which components to remove from the screen that appears when you press CTRL+ALT+Delete. Change the setting for the specific component you want to remove to Enabled.

TURN OFF THUMBNAILS

Folder: User Configuration\Administrative Templates\Windows Components\File Explorer\
Setting: Turn off the display of thumbnails and only display icons

If Enabled prevents any folder from displaying Thumbnail view, replacing them with standard icons. This setting requires a Windows restart, or logging off and logging back on to implement.

HIDE NOTIFICATION AREA

Folder: User Configuration \ Administrative Templates \ Start Menu and Taskbar
Setting: Hide the notification area

If Enabled removes the entire Notification Area, leaving only the system clock showing. You can then also disable the Clock by right-clicking on it, selecting Properties and setting it to Off. This setting requires a Windows restart, or logging off and logging back on to implement.

TURN OFF SHAKE

Folder: User Configuration \ Administrative Templates \ Desktop
Setting: Turn off Aero Shake window minimizing mouse gesture

If Enabled, disables the Shake feature on the Desktop, but does not affect Snap functionality.

DISABLE THE LOCK SCREEN

Folder: Computer Configuration \ Administrative Templates \ Control Panel \ Personalization
Setting: Do not display the lock screen

If Enabled, the Lock Screen will not be displayed when booting into Windows. Instead you will see the Login Screen. Similarly, if you select the Lock option under the user account image on the Start Screen, you will see the Login Screen displayed instead.

PREVENT UNINSTALLATION OF APPS ON START SCREEN

Folder: User Configuration \ Administrative Templates \ Start Menu and Taskbar
Setting: Prevent users from uninstalling applications from Start

If Enabled, this policy will prevent any users from uninstalling Metro apps on the Start Screen.

BLOCK REMOVABLE STORAGE ACCESS

Folder: User Configuration \ Administrative Templates \ System \ Removable Storage Access
Setting: Various

If Enabled, the relevant settings under this folder can be used to prevent a user from reading and/or writing to removable storage devices such as CDs, DVDs and external drives. This can prevent a user from attaching such a device and transferring undesirable software, such as malware, to the system for example.

ENABLE PAGEFILE ENCRYPTION

Folder: Computer Configuration \ Administrative Templates \ System \ Filesystem \ NTFS
Setting: Enable NTFS pagefile encryption

If Enabled, the Pagefile (Virtual Memory) on disk will be encrypted, making it difficult for anyone else to read its contents. This provides greater security, particularly in shared environments, but adds to filesystem overhead and will reduce performance.

PREVENT AUTOMATIC RESTORE POINT CREATION

Folder: Computer Configuration\Administrative Templates\System\Device Installation
Setting: Prevent creation of a system restore point during device activity that would normally prompt creation of a restore point

If Enabled, prevents Windows from automatically creating a restore point for the System Restore feature during various activities which would normally result in this, such as installation of new drivers. This can speed up driver installation for example, but provides less protection against potential problems.

PREVENT WINDOWS MEDIA DRM ACCESS

Folder: Computer Configuration\Administrative Templates\Windows Components\Windows Media Digital Rights Management
Setting: Prevent Windows Media DRM Internet Access

If Enabled, prevents Windows Media-related Digital Rights Management (DRM) features from accessing the Internet for license acquisition and security upgrades. This is useful if you have privacy concerns, but may cause problems with DRM-protected media.

PREVENT WINDOWS MEDIA PLAYER CODEC DOWNLOAD

Folder: User Configuration\Administrative Templates\Windows Components\Windows Media Player\Playback
Setting: Prevent Codec Download

If Enabled, prevents Windows Media Player from automatically downloading any codecs it requires.

HANDLING OF ATTACHMENTS

Folder: User Configuration\Administrative Templates\Windows Components\Attachment Manager
Setting: Inclusion list for ...

Here you can specify precisely what file types - entered as a list of extensions, such as .EXE - the email Attachment Manager determines to be high, moderate and low risk attachments. By moving certain file types into the moderate or low risk category you can access them more easily in programs such as Windows Live Mail. However, this can also create a major security risk.

There are a large number of settings and features you can configure using Group Policy, and you can browse through the Local Group Policy Editor to see all of these at your leisure. Bear in mind that many of the most useful changes made using Local Group Policy Editor are already possible using the normal Windows settings. It is not wise to change things via Group Policy if you can change them in Windows normally, especially those under the 'Computer Configuration' branch, because in the future if you or another user forgets about the changes you made here, it will cause confusion when you find you can't use certain functionality. Group Policy overrides the ability to adjust the features within the normal Windows interface, so use it only when there is no other option.

WINDOWS SEARCH

Windows Search is a feature that underwent a dramatic change as of Windows Vista, and has once again been changed significantly in Windows 8. The aim of the search engine in Windows as of Vista onwards is to allow you to quickly find specific programs, settings or files. Searching is no longer just about "finding lost files", or knowing specific details like the exact filename, creation date or location. By entering a partial or whole word or sentence, the Windows search engine can display the most likely targets almost instantly.

The major change in Windows 8 is that of removing the Search Box along with the Start Menu on the Desktop, and instead making Windows Search a component of the Start Screen. The search functionality is now triggered simply by starting to type on the Start Screen. Searching speeds up access to all Metro apps, Desktop programs, Windows features and files. For example, to open a particular picture or song quickly, instead of navigating to its location in File Explorer, simply type part of its name on the Start Screen, and it will be instantly displayed under the Files section of the search interface, ready for launching.

In this chapter we examine the various ways in which searching is possible in Windows 8, and how to optimize and customize this behavior.

< SEARCH METHODS

Windows allows you to search for files, folders and programs from a range of locations, depending on your needs. While you can always put links to your most commonly-accessed files and programs as icons on the Desktop, or pin them to the Start Screen for example, there are still many more files and programs or features on your system which you might want to access as quickly as possible, and the search functionality can help in that regard.

START SCREEN

The primary search location in Windows 8 is the Start Screen. By opening the Start Screen and starting to type, you will trigger the search functionality which previously existed in the form of a dedicated Search Box on the Start Menu in Windows Vista and 7. You can also open the search function directly by opening the Charms bar and selecting Search; by using the WINDOWS+Q keyboard shortcut; or by right-clicking in the lower left corner of the Taskbar and selecting Search.

Extensive use of this Start Screen search functionality is already made throughout this book to quickly find and launch particular Windows programs. Some examples of how this search functionality can be used are as follows:

- Typing *services.msc* on the Start Screen and pressing Enter to launch the Services Utility will typically take less time than it would take to open the Windows Control Panel, click on the Administrative Tools component then double-click on the Services item.
- Typing *calc* on the Start Screen and pressing Enter to launch the Calculator utility will typically take less time than it would take to right-click on the Start Screen, select 'All Apps', and find Calculator under the 'Windows Accessories' category.
- Typing a search on the Start Screen starting with http:// and pressing Enter will automatically launch that web link in your default browser, or Internet Explorer Metro. This is usually faster than manually opening a web browser and typing the address in the Address Bar and pressing Enter.

There are many aspects to the Start Screen search functionality, and we examine the most important of these below.

When you conduct any search on the Start Screen, the results of the search are displayed under four separate categories: Apps, Settings, Files, and a list of individual apps. These categories are each described below:

§ *Apps:* Lists any search results that match installed Metro apps or Desktop programs on your system, including built-in Windows programs.
§ *Settings:* Lists any search results that match any Windows settings, including Windows Control Panel and PC Settings components, as well as various wizards and troubleshooters.
§ *Files:* Lists any search results that match files or folders in any of your indexed locations.
§ *Apps List:* Provides a list of installed Metro apps that support search. Once an app is selected, you can search within it by using the search box. For example, selecting the Mail app then entering a search term in the box will search through the emails in the Mail app.

The category you are searching within will be displayed in large text at the top left of the main Search Results area to the left side of the screen. If you simply start typing on the Start Screen, by default the top matches from the Apps category are displayed. You can see the number of results for each category shown next to the category's name on the right. To quickly switch between categories after typing a search result, you can use the arrow keys. For example, type a search term on the Start Screen, then press the Down or Up Arrow key to select the appropriate category on the right and press Enter, and its results will be shown in the main Search Results area. You can also use the TAB key to switch between the Search Results area and the Search Box and categories.

By default Windows will immediately begin to search for matches to any letters or partially entered words on the Start Screen, instantly showing the results. This means you can literally conduct a search letter by letter, examining the results each time you type a new letter. This allows you to dynamically refine your search results by adjusting your search term on the fly to see if it finds what you're after.

When searching the Files category, you will sometimes have sub-categories to choose from at the top of the Search Results section if the files found fall into different categories. These include: All, Documents, Videos, Music and Other. Selecting the relevant sub-category will further refine the file results accordingly.

This search functionality pulls its results directly from your search index, configuration of which is covered in the Search Index section later in this chapter. As such, the results you see are not a comprehensive listing of all files on your system. To conduct a more thorough search, you will need to use the advanced search functionality of File Explorer.

FILE EXPLORER

A Search Box can be found at the top right of most Explorer-based windows, such as in File Explorer itself, or the Windows Control Panel window. By default, any searches launched from these locations only focus on the contents of the particular window you are searching in. For example, if you initiate a search from the Search Box at the top right of a File Explorer window, it will only show results from the currently open folder and any subfolders, not across all indexed or non-indexed locations on your PC. This can be useful for quickly finding a file in a large directory.

However, there are a range of advanced search options available in File Explorer, found under the Search menu in the Ribbon, which appears whenever you click in the Search Box. These are covered below:

- *Computer:* If selected, a search is automatically launched across the entire PC for the current search term. This may take a while since the search is extended to non-indexed locations of your drive(s).
- *Search Again In:* The following three options are found by clicking the 'Search again in' button, which is only accessible after you've tried an initial search:

    - *Libraries:* If selected, a search is automatically launched within your Libraries for the current search term. Since all files linked to Libraries are automatically indexed, the search should be extremely fast.
    - *Internet:* If selected, a search is automatically launched in your default web browser using your default browser search engine on the current search term.
    - *File History:* If selected, a search is launched within any backups made by the File History feature, which is covered in more detail under the Windows File History section of the Backup & Recovery chapter.

- *Date Modified, Kind, Size, Other Properties:* These options allow you to specify various aspects of the file's properties, such as the date it was last modified, the file type, or file size. By default, this only refines the search results in the current folder, so you will have to select a location if you want to search more widely for all files on your system corresponding to the properties you've selected. For example, select E-mail under the Kind option, then click on Computer to do a global search for all stored emails.
- *Recent Searches:* This contains a list of recent search terms you have used.
- *Advanced Options:* This option allows you to customize search behavior. It contains several important options which affect how thorough your search results will be, though note that some of these options are also available under the Search tab of the Folder Options component under Windows Control Panel, as covered later in this chapter:

    - *Partial Matches* - If ticked, this allows Windows to return search results that only partially, and not exactly, match your search term. This means for example that you can enter only part of a filename and it should be found by Windows Search. This is recommended, as it makes searching easier.
    - *File Contents* - If ticked, Windows will also search within the actual contents of relevant files - such as text documents and spreadsheets - in the search location, attempting to match your search terms. This may take a long time to complete if the search is conducted outside of indexed locations.
    - *System Files* - If ticked, core Windows system files will be included in searches.
    - *Zipped (Compressed) Folders* - If ticked, your search will also extend to any files held within zipped (or similarly compressed) folders. This can increase search time, especially in non-indexed locations containing large compressed folders.

- *Save Search:* This option allows you to save your current search in case you need to use it again. The search will be saved as a .SEARCH-MS file in the location of your choice. Double-clicking on this file will automatically launch your saved search.

You can see the progress for a search in an Explorer-based window by examining the green progress bar shown in the Address Bar at the top of the window. Any found items will be displayed as they are discovered in the main window. You can stop a search at any time by clicking the red X at the far right of the Address Bar.

By default, search results in Explorer-based windows are presented in Content view type, which is covered in more detail in the Basic Features section of the File Explorer chapter. Content view provides a range of information, and a Live Icon preview of the file as well if available, allowing you to better determine its contents at a glance. You can change the view to one which may suit you better by right-clicking and choosing another option from the View menu. Content view is recommended, particularly as in this view

Windows automatically highlights relevant file details or contents matching your search terms in yellow. In terms of the order in which search results appear, Windows uses a special algorithm to weigh up a range of file details that may be relevant to your search, including filename, metadata, content, etc. Windows assigns each search result a score between 0 and 1,000, with 1,000 indicating an exact match. It then displays the results ranked by this score, from highest to lowest.

Advanced Search Query

A vital consideration for getting the most out of the Search functionality in Windows is how you form your search queries. This is particularly important when using the more advanced search functionality available via the Search Box in File Explorer. The advanced functionality in Windows Search can be fully harnessed by using Advanced Query Syntax (AQS). This type of search filtering allows you to develop very precise searches that find what you are looking for much faster. The full list of AQS search query filters is provided in the link above, but the table below contains common filter terms you can use in any Windows Search Box:

Filter	Description	Example
NOT	Finds only incidences where the first search term appears without the second search term after the NOT. Note: NOT must be in all uppercase letters.	*help NOT me* Finds only incidences where the word *help* appears without the word *me*.
OR	Finds any incidences of either or all of the terms specified. Note: OR must be in all uppercase letters.	*help OR me* Finds any incidences where either the word *help* or the word *me* appear, or both.
AND	Finds only incidences where all of the search terms appear together and not in isolation. Note: AND must be in all uppercase letters.	*help AND me* Finds only incidences where both the words *help* and *me* appear together.
" "	Finds the exact search terms surrounded by the quotes, and no other variations of them.	*"help me"* Finds only incidences of the specific phrase *help me*, not any other variations based on the words *help* and *me*.
( )	Finds the search terms surrounded by the parenthesis in any order	*(help me)* Finds any incidences of the phrases *help me* or *me help*.
+	Operates the same way as the AND filter above.	*help + me*
-	Operates the same way as the NOT filter above.	*help - me*
> < >= <=	Greater than or Less than signs. Greater than or equal to, Less than or equal to.	*size:>=50KB* Finds any file with a size greater than or equal to 50KB.
Author:	Finds any file with the specified text in its Author property.	*author:brian*
After:	Finds any file with its primary date after the specified date.	*After:10/10/07* Finds any file created after 10 October 2007.
Before:	Similar to After above, except the primary date must be before the specified date.	*Before:10/10/07* Finds any file created before 10 October 2007.
Date:	Allows you to search for a file created on a specific date, or within a particular date range.	*Date:>10/10/07<10/10/08* Finds any file created between 10 October 2007 and 10 October 2008.
Size:	Finds a file with the specified size.	*size:>100MB<200MB* Finds any file larger than 100MB in size but smaller than 200MB.
Kind:	Finds a file of a particular type, with common types being: contacts, email, docs, music, pictures, videos, folders	*kind:video* Finds only video files which contain the specified search term.
Ext:	Finds a file with the specified file extension. Can be entered without the . before the extension name.	*ext:EXE* Finds any file of the type .EXE.
To:	Finds a file with the search term contained in the To property.	*to:brian* Finds only files (typically emails) with a To: field indicating the intended recipient is *brian*.
From:	Similar to the To: filter above, except looks for the search term in any From: fields for the file.	*from:brian* Finds only files (typically emails) with a From: field indicating it is from *brian*.
Bitrate:	Finds a song with the specified data bitrate in the file properties.	*bitrate:>260kbps* Finds any music with 260kbps or higher bitrate.
Tag:	Finds any file with the specified text in a custom tag for the file.	*tag:amazing* Finds any file tagged with the word *amazing*.

For example, to initiate a search for any PDF file created, modified or accessed sometime after 1 January 2012, type the following in the Search Box File Explorer:

after:>1/1/12 ext:PDF

Many of the AQS filters will also work when typed on the Start Screen. However, you will only see a menu of preset options for certain filters presented if you type them in an Explorer-based Search Box. For example, if you type *Bitrate:* on the Start Screen, you won't see any presets displayed, but if you type the same term in the Search Box of File Explorer, a selection of bitrate choices will be shown in a drop down box.

Search filters are extremely powerful, and there are a range of ways you can use the available filters. I encourage you to experiment with them to discover the most useful way to utilize them in your searches. Remember that if you develop a complex search filter, you can use the 'Save Search' button in the Search menu of the File Explorer ribbon to save it for ease of repeated use.

FEDERATED SEARCH

Introduced in Windows 7, Federated Search provides support for the OpenSearch protocol, which is an open source format for sharing search results. In effect this means that Windows allows you to search a range of resources outside your PC - typically on the Internet - via File Explorer. This functionality is facilitated by the use of Search Connectors, which are similar to plugins. Windows Federated Search connects to servers that receive OpenSearch queries, and returns results in either the RSS or Atom XML format. Look for the availability of a Search Connector on your favorite site, or try some of the ones for more popular sites as provided in this Microsoft Article.

Download the relevant .OSDX file, and once installed, open File Explorer and check under the Favorites category in the Navigation Pane for a link to that connector. Select the connector, then enter a term in the Search Box at the top right of Explorer to initiate an online search within that particular site. You can also find any installed Search Connector by clicking the 'Search again in' button under the Search section of the Explorer ribbon.

You can create a basic Search Connector for any site yourself. All you need to do is create an XML document coded to run the correct query via Bing. To make things simple, I have prepared a template which provides you with the basic code to do this, but it requires some customization:

1. Download the following template: SearchConnector.zip.
2. Extract the .TXT file and open it with a text editor like Windows Notepad.
3. Fill in the correct details where prompted throughout the file. Enter the site name where prompted for SITE NAME (e.g. Google), and enter the web address in place of the SITENAME incidences (e.g. Google.com).
4. Rename the file with the name of the site for which you are customizing, and give it an extension of .OSDX so that Windows can recognize it as a Search Connector (e.g. *Google.osdx* not *Google.osdx.txt*).
5. Double-click on this file to install it, and click the Add button when prompted.
6. When installed, Windows will automatically open a File Explorer window with your Search Connector highlighted in the Favorites category.
7. Enter a search term in the Search Box at the top right, and a search of the site will be initiated, with results shown in Explorer just like any other Windows search.
8. Double-click on any result to launch it in your default web browser.
9. To remove a Connector at any time, right-click on it in File Explorer and select Remove.

This is a handy, but lesser used, feature, hence many sites will not have a proper full-featured Search Connector you can download and install.

SEARCH CONFIGURATION

You can customize Windows Search behavior by going to the Search tab under the Folder Options component of the Windows Control Panel. Here you can adjust the following settings:

Find partial matches: If ticked, will look for your search term anywhere within a word. For example, entering the term *an* will also result in matches where the word *and* is used, because it contains the word *an* in it. I recommend leaving this enabled and only disabling it if you find it regularly contributes to providing too many unwanted results.

Don't use the index when searching in file folders for system files: If ticked, this option forces Windows to ignore the search index and do a full search when searching for files within a folder. Provides the most thorough but the slowest results, and is generally unnecessary.

Include system directories: If ticked, this option includes all system directories as part of any search you initiate outside indexed locations. This should not be necessary unless you often look for files which you believe reside in system folders. Remember that system directories are protected by UAC in Windows, hence normal personal files or downloads can't accidentally be saved there.

Include compressed files: If ticked, Windows will also search within compressed files, such as .ZIP, .CAB and .RAR archive formats, when searching in non-indexed locations. This is recommended if you have a multitude of files stored in archives, but it will slow down searching.

Always search file names and contents: This option is the most thorough, searching for your entered terms in filenames as well as all relevant file contents, across all non-indexed locations on the drive. This can take quite a while, particularly if you have large text documents that are not indexed.

There is one additional area where you can customize your search configuration. This can be accessed by opening the Charms menu, selecting settings, then clicking on 'Change PC Settings'. Once there, click on the Search category on the left side. Here you can alter the following Metro-related settings:

Show the apps that I search for most often at the top: If enabled, this will reorder the list of apps at the right side of the Search Results window based on those which you search in the most often. For example, if you frequently select the Internet Explorer Metro app and then type a search term to search within IE Metro, then the Internet Explorer app will be shown at the top of the app list.

Let Windows save my searches as future search suggestions: If enabled, any search terms you enter will be saved and presented at the top of the list of suggested search terms when searching within an app. Click the 'Delete history' button if you want to delete your search history at any time.

Use these apps to search: The list of apps displayed at the bottom right of the Search Results window can be refined here. By default, any installed app that supports the search function will be listed, but you can turn particular apps off here to remove them from the list shown on the Search Results window.

< SEARCH INDEX

The key to the Windows Search functionality's performance and usefulness is the Search Index. This index is a pre-built list similar to the index of a book, and it stores a range of details about files on your system, updated regularly by Windows whenever a file changes. When you launch a search in Windows, by default it will look at the index first rather than searching across your entire drive(s), with the result being a more thorough search done almost instantaneously.

The search indexer does not index your entire drive, nor all the details or contents of all of your files as this would take a long time to regularly update, and noticeably reduce drive performance. By default the indexer only indexes the following information:

§ All folders in your Libraries, including any custom Libraries you create.
§ The Start Screen.
§ Offline Files.
§ Windows File History backups.
§ Internet Explorer History.
§ Commonly-used file types have their properties indexed, but some content-rich file types have both their properties and their contents indexed. For example, .DOCX and .PDF files have their properties and contents indexed; .EXE and .BIN files only have their properties indexed.
§ For privacy reasons, only your own user account files are added to the index your account uses. Windows will not show search results from the data that other user accounts store on the PC.

The actual index file which holds all of this information is stored under the *\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex* directory, which is usually hidden. Index files don't take up a great deal of drive space, and you should not delete them manually. Furthermore, for indexed searching to work properly, the Windows Search service must be running, and indexing must be fully enabled under your drive properties. That is, go to File Explorer, right-click on your drive and select Properties - the 'Allow files on this drive to have contents indexed in addition to file properties' box must be ticked.

Certain folders are automatically excluded from having their file contents indexed to ensure that searches do not get bogged down with a great deal of irrelevant content. For example, program and system file folders are excluded.

If you wish to customize indexing behavior, see further below for details.

PERFORMANCE IMPACT

Windows Search is a very useful feature given the significant integration of search functionality in Windows 8. It provides extremely fast search results, and allows you to access commonly used files and folders much more quickly than having to fill your Start Screen or Desktop with dozens of tiles or icons. Furthermore, Windows Search works seamlessly with the Libraries feature, meaning you don't have to worry about manually adding or removing any content to the search index as long as it is stored in a Library; the index is automatically updated as soon as you change Library contents.

Windows Search really only works well if the Search Index is kept up to date, otherwise your searches may exclude more recently added files/content, or show results for files/content which has since been deleted or altered. By default Windows detects changes in indexed locations, and runs the search indexer in the background as a low priority process whenever it needs to update itself. This means that only during periods when your system is relatively idle does the indexer actually operate, and the impact is all but unnoticeable on most systems. The indexer also does not start functioning immediately after Windows startup; it usually waits a few minutes before it comes into effect, so it does not contribute to post-startup drive activity. You can see this for yourself by the fact that the 'Windows Search' service is set to 'Automatic (Delayed Start)' - see the Services chapter for details. If at any time you start using your system with even moderate intensity while the indexer is running, it will throttle itself back, or stop completely, to provide the necessary responsiveness in your primary task.

To see the progress of the indexer when it is running, go to the Indexing Options component of the Windows Control Panel and at the top of the main window you will see how many files it has indexed so far. You may see something like 'Indexing speed is reduced due to user activity', which means the index is currently being

updated, but taking a back seat to some other task, even if it's something as simple as you opening a Windows Control Panel component. Again, the indexer is not going to impact on system responsiveness in any noticeable way. For this reason, and given how useful the Windows Search feature can be, I strongly recommend against disabling Windows Search, even if you have an SSD. If you still wish to disable Search, see the end of this chapter for details.

CUSTOMIZING THE INDEX

To improve the speed and accuracy of your search results and streamline the indexer's resource usage, you can customize precisely what Windows includes in the Search Index. Go to the Windows Control Panel and select the Indexing Options component. Here you can see an overview of all the currently indexed locations, and at the top of the window you can see how many actual items are currently in the index. To add or remove indexed locations, click the Modify button, then click the 'Show all locations' button. Expand the directory listing for the drive(s) you wish to index. By default Windows already indexes a range of specific folders, including most of the contents of the *\Users* folders and subfolders.

To optimize the index, unselect any subfolders whose contents you are certain do not contain files which you would normally search for. Conversely, add any subfolders whose contents you wish to include in search results. Remember that Windows automatically includes any folder linked to a Library in the indexer, so ideally, instead of manually adding indexed folders here, it would be best to modify your relevant Libraries to include all of your desired folder locations, and they will be automatically included in the index as well.

Importantly, you should not expand the index to cover most of the files and folders on your drive(s), as this defeats the purpose of indexing. Indexing most of your drive contents will simply slow down searches and also potentially provide more irrelevant results. The search index should be lean and focused, primarily containing your important personal files.

When you are finished adjusting the index, click OK and Windows will update the index accordingly.

To further customize the search index, click the Advanced button. There are some important functions here, and these are covered below:

Index encrypted files: If this option is ticked, EFS encrypted files will be included in the index. However this can be a security risk, because your index could potentially hold text from encrypted files which can be read by anyone who gains access to the index files. Hence this option is best left unticked; only enable it if you have a lot of encrypted files, and only if you use BitLocker Drive Encryption to protect the entire drive on which the index resides. See the Encrypting File System and BitLocker Drive Encryption sections of the Security chapter for more details. Note that the entire index will rebuild itself if you select this option, and this can take quite some time.

Treat similar words with diacritics as different words: Diacritics are accent marks used in different languages and for certain words in English, such as *touché* vs. *touche*. Ticking this option tells the indexer to treat the words as different if there is a difference in accent marks. This is best left unticked unless you specifically remember to include diacritics when forming search queries.

Delete and rebuild index: You can delete and rebuild your entire Search Index at any time by clicking the Rebuild button. The process can be quite lengthy, especially if you have a lot of files and folders indexed, however this may be necessary if you experience problems with search results not finding indexed files. The speed with which the indexer rebuilds the file depends on whether the system is idle or not.

Index location: The actual files for the index are held in a particular location by default, usually under *\ProgramData\Microsoft* on your primary system drive. If you wish to move the index files to another directory or drive, you can do so by clicking the 'Select new' button and browsing to the new location. Make

sure to select a non-removable drive which uses the NTFS file system. The main reason you would want to change this is if you wish to move the index contents to a faster drive for example, as this helps speed up both use of the index in searches, and more importantly allows faster updating/rebuilding of the index by Windows. In practice this isn't really necessary as having the index on the default drive usually doesn't impact noticeably on performance, and the index doesn't take up much space. It also doesn't help to move the index from an SSD to a slower drive, since the index is better placed on the fastest drive, and has an inconsequential impact on SSD lifespan.

File Types: Under the 'File Types' tab of the Advanced Indexing Options you can see the types of files the indexer can currently include in the index, listed by file extension. Any extensions which are ticked are included in the search index, and you can tick or untick any of these extensions as you wish. By default all the major, and indeed many less common file extensions are already indexed, so you should not need to change the indexed file types. If you wish to add a particular file extension that is not listed, you can do so by clicking in the text area at the bottom left of the window, typing the extension, and pressing the 'Add new extension' button which will become ungrayed once an extension is entered.

You can also change whether a particular file type only has the contents of its Properties tab indexed ('Index Properties Only') - which is the default for most extensions listed here - or whether all of that file's contents are also indexed ('Index Properties and File Contents'). For example, highlight the .TXT extension and you will see that the option highlighted is 'Index Properties and File Contents', meaning that for any plain text file, the contents of its Properties tab, as well as the contents of the actual text document itself, will be included in the Search Index. This means that if you enter a word or phrase in a Search Box, if it exists within one of your indexed text files, the document will be included in the search results shown. It is generally pointless to index the contents of files that only have computer code as their content, so for many file types, such as .EXE or .JPG files, the contents are not indexed and should not be; they don't have any useful English text in them.

Certain types of files need to have their contents translated into something intelligible by Windows Search with the use of special IFilters. Most if not all relevant IFilters are installed along with the application for that file type, and can be seen listed under the 'Filter Description' field. However, certain content, such as .TIFF image files, will not have such filters installed by default. To install a content filter for .TIFF files, you must go to the Programs and Features component of the Windows Control Panel and click the 'Turn Windows features on or off' link in the left pane, then tick the 'Windows TIFF IFilter' feature to enable it - see the Programs and Features section of the Windows Control Panel chapter. The reason this feature is optional is because .TIFF files are usually pictures, but can also contain text from scanned documents. Enabling this feature can reduce search speed if you have lots of scanned TIFF documents, so only enable it if you actually require this functionality.

Whether a file type only has its properties indexed, or both properties and content indexed, can have a noticeable impact on the index. The more files with complex contents are indexed, the more work the indexer has to do to maintain the index if these contents change regularly, and the longer search results may take to display. I recommend only indexing the contents of file types for which you regularly initiate a content search using Windows Search.

If you've changed any of the index settings, I strongly recommend that when finished you click the Rebuild button to do a total rebuild of the index data immediately using the latest settings. This may take quite some time to complete, but it will ensure that all of your search results will be completely up-to-date and accurate.

INDEXING AND FILE PROPERTIES

The search indexer will index most files by what is in their Properties, as well as their content in some instances. So one of the ways in which you can further improve search indexing is by appropriately configuring the Properties of a file. Open File Explorer, right-click on any file, select Properties, and look

under the Details tab - you will notice there are a range of fields here that are either empty, or already filled in with certain details about the file, such as its Size, Date Created, Title, and so forth. This is referred to as Metadata, and provides additional information that the indexer can use to identify the file. If you want to make it easier to find or access a particular file in the future, it is wise to add some relevant metadata to it. For example, you may wish to tag all of your Jazz songs with the word *Jazz* in the Genre field under the Details tab. Then when you type the word Jazz in the Search Box in Explorer, or type Genre:Jazz on the Start Screen and select the Files category, all of these tagged songs will be instantly listed for you to choose from.

To edit a file's details, first right-click on it in File Explorer and select Properties. Make sure it is not write protected - if it is, untick the 'Read Only' box, click Apply then re-open the file - and it is not currently in use by another program. Then click the Details tab and move your mouse cursor over the fields under that tab, and you will see that many of these fields can be edited. Edit the fields appropriately, and when you click OK, that information is saved along with the file. You can now search for that file using any one of the pieces of metadata entered into the Details tab of the file's properties. This is especially effective if you use that property in an AQS filter-based search - see the Search Methods section earlier in this chapter.

There is another useful function you can perform when in the file properties. Right-click on a file, select Properties and under the General tab, and click the Advanced button. In the box which opens you can tick or untick the 'Allow this file to have contents indexed in addition to properties' box, and this determines whether this particular file will have its contents indexed. In this way you can add or remove an individual file's contents from the indexer without having to add or remove an entire file type.

In any case, if you make sure that your files are maintained with as much descriptive metadata has possible, you will be able to access relevant files in a variety of ways much more quickly when needed, without having to remember any specific details such as filenames, dates of creation, etc.

DISABLING WINDOWS SEARCH

The search indexer does not have a noticeable performance impact because it uses idle resources that would otherwise go wasted, and does not load immediately at startup. The benefits of Windows Search are numerous, as it is an integral part of the way Windows now operates. Indeed, given the changes which Windows 8 has made to the Start Screen, search is necessary to quickly access certain features and functions that would otherwise be harder to find. The search index is useful even if you have a fast SSD, which is why Windows doesn't automatically disable the Indexer when it detects an SSD.

If, after reading this chapter, you still feel that you want to disable indexing, or remove Windows Search altogether, see the information below.

To disable Search Index-related functionality, then follow these steps:

1. Open the Services utility and set the 'Windows Search' service to Disabled, then Stop the service. See the Services chapter for details of how to do this.
2. This will not remove Search Boxes, and it will not prevent existing programs and features or Windows Control Panel items from appearing in search results. The Search Indexer will be disabled, and won't attempt to update the index. This can be confirmed by going to the Windows Control Panel and opening the Indexing Options component: it will say 'Indexing is not running' at the top of the window.
3. Go to the Folder Options component of the Windows Control Panel, and under the Search tab, select the 'Don't use the index when searching in file folders for system files' and 'Always search file names and contents' options. This ensures that Windows doesn't attempt to use the index when searching, and will instead do a normal non-indexed search in all locations.

These steps will result in slower searches, but the Search Index and related processes will not run at any time in the background.

If you wish to go further by disabling and effectively removing all Windows Search-related functionality from Windows 8, do the following:

1. Go to the Indexing Options component of the Windows Control Panel and manually remove all indexed folders from the indexer.
2. Disable the Windows Search service as covered further above.
3. Go to File Explorer, right-click on each of your drive(s), select Properties and untick the 'Allow files on this drive to have contents indexed in addition to file properties' box, then click Apply. Choose to apply this to the drive and all subfolders, and click 'Ignore all' to ignore any errors for system files which can't have their properties changed.
4. Go to the Programs and Features component under the Windows Control Panel and click the 'Turn Windows features on or off' link in the left pane.
5. Untick the 'Windows Search' box and click OK.
6. Restart your PC.

This will remove all integrated Search Boxes from Windows, and clear and disable the Search Index. You can enable indexing again by reversing the steps above. Neither of the procedures above is recommended.

If you install any third party Desktop search software, it will replace the Windows Search functionality with its own, so if you don't like Windows Search but find an alternative that suits you, it will not clash with the Windows Search functionality.

The search functionality introduced in Windows Vista was quite advanced, and Windows 7 made refinements to improve its functionality and performance. Windows 8 has changed the way searching is incorporated into the interface, but most of the functionality remains the same as that under Windows 7. The primary consideration is that Windows Search is not really about searching for lost files, it's about making access to your files and programs much quicker and easier, regardless of where you store them, or what you name them. By using a range of metadata, Windows Search can find and display any commonly used item almost instantly, ready to be launched with one click. There is no real benefit to disabling Window Search, but there is substantial benefit to learning to use it properly.

INTERNET EXPLORER

Internet Explorer (IE) is the most-used Internet browser in the world, and many Windows users are comfortable and familiar with it. While I recommend that you trial alternative browsers to see if they can provide you with additional functionality you may like, Internet Explorer is a fast and functional, and has a range of security benefits in Windows. You should not feel you have to use another browser if you are happy with IE.

Windows 8 introduces Internet Explorer 10, which comes built-in and ready to use. However, perhaps confusingly, there are two versions of IE 10 in Windows 8: a version that only runs under the Metro interface, found as an Internet Explorer app on the Start Screen; and a regular version which can be launched via the Internet Explorer icon on the Taskbar, and runs only under the Desktop environment. The desktop version of IE 10 is full-featured, and is extremely similar to Internet Explorer 9 in most respects. The Metro version of IE 10 has a redesigned interface, and slightly different, scaled-back features.

This chapter looks at both versions, focusing on the full-featured Desktop version first, and then covering the Metro version. First we examine the differences between these two versions of IE.

< IE DESKTOP VS. IE METRO

As detailed in this Microsoft Article, if Internet Explorer is set as your default browser, then both a Metro version of IE, and the Desktop version of IE will be available. If you have another web browser set as your default, then only the Desktop version of Internet Explorer will be available; the Internet Explorer tile on the Start Screen will open the Desktop version of IE. You can set your default web browser using the Default Programs component of the Windows Control Panel, as covered under the Default Programs section of the Windows Control Panel chapter.

The Desktop and Metro versions of IE share the same rendering engine and many of the same settings, the bulk of which you can adjust in Internet Options, found in the Windows Control Panel, or under the Tools menu of IE Desktop. For example, your Metro IE homepage is the same as the homepage you specify for your Desktop IE. Similarly, your history settings and history of viewed pages are shared between the two browsers.

However, these two browsers are actually quite separate from each other in most other respects. When you open a site in one version of IE, if you then open the other version of IE, you will not find the same site shown. The Metro version of IE does not support plugins, except for a native version of the Flash Player which is not really a plugin as it is built into Internet Explorer 10. The Flash Player functionality in IE Metro is also limited compared to the full Flash functionality available in IE Desktop.

Importantly, you can control which version of Internet Explorer is used by default when you click on a web link. The relevant setting is found under the Internet Options component of the Windows Control Panel, or by clicking the Tools button in the Desktop version of Internet Explorer and selecting 'Internet Options'. Under the Programs tab of Internet Options, there is a drop-down box for 'Choose how you open links' that determines which version of Internet Explorer - whether the Metro version, or the Desktop version - is launched whenever you click on a web link in another location. These settings are detailed below:

§ Let Internet Explorer decide - The default option, this allows IE to launch the Metro or Desktop version as relevant to match your current environment. That is, if you're currently on the Desktop, then launching a link will open the Desktop version of IE; if you're currently in the Metro interface, the Metro version of IE will be used.
§ Always in Internet Explorer - The Metro version of IE will always be used.
§ Always in Internet Explorer on the desktop - The Desktop version of IE will always be used.

Furthermore, there is an option entitled 'Open Internet Explorer tiles on the desktop', which overrides the settings above when the Internet Explorer tile, or a pinned website tile, is launched on the Start Screen. If this option is ticked, clicking such tiles will always open the Desktop version of IE, even though you are in the Metro environment.

So basically, if you want to completely avoid using the Metro version of IE, set the options above to 'Always in Internet Explorer on the desktop', and tick the 'Open Internet Explorer tiles on the desktop' box as well. Alternatively, if you want to completely avoid the Desktop version of IE, set the options above to 'Always in Internet Explorer', and untick the 'Open Internet Explorer tiles on the desktop' box. Otherwise, for most users selecting the 'Let Internet Explorer decide' and unticking the 'Open Internet Explorer tiles on the desktop' box will provide a more consistent experience, with IE Metro opening in the Metro environment, and IE Desktop opening in the Desktop environment.

You will need to configure and learn the features of each version of the browser separately. The sections below detail the features and settings for each version of IE, starting with the Desktop version.

< INTERNET EXPLORER DESKTOP

To configure the Desktop version of Internet Explorer, go the Desktop and open IE via the Internet Explorer icon on the Taskbar, then click the Tools button (the cog icon) at the top right of the browser and select 'Internet Options'. You can also press the ALT key in IE, then under the Tools menu which appears select 'Internet Options'. Alternatively, go to the Windows Control Panel and open the Internet Options component. Below are the descriptions and my recommendations for the important settings under each tab of Internet Options:

GENERAL

Home Page: Here you can enter the address of the web page you wish to open by default whenever you start Internet Explorer. If you want to set the website you are currently viewing as your homepage, click the 'Use current' button; clicking 'Use default' will restore IE's default homepage, which is typically a Microsoft-owned site such as MSN; If you are using tabbed browsing (see further below), you can enter multiple website addresses in the box, one on each line, then whenever you open IE, all of these pages will open at the same time as separate tabs; if you select the 'Use new tab' option, your homepage will be a screen which shows your most frequently opened websites as thumbnails. Finally, if you don't want any homepage to load when IE is opened, enter *about:blank* as the address in the box and click Apply.

Startup: This option allows you to determine whether IE opens with your designated home page(s), or whether it starts up with any tabs you had open in your previous session. If you select the 'Start with tabs from the last session', each time you open IE it will essentially continue on from the last time you closed it.

Tabs: Tabbed browsing means that new web pages launched from links will be opened as tabbed pages within the current browser window by default, rather than opening an entirely new browser window for each link. This helps reduce resource usage, and it is also much easier to manage multiple open pages this way. To configure tabbed browsing, click the Tabs button. In the box which opens you can select whether to enable or disable tabbed browsing altogether, and set the behavior of it if enabled. The following settings require some explanation:

- *Show previews for individual tabs in the taskbar* - This option allows every open tab in IE to be displayed as a separate box in the Thumbnail Preview(s) which appears when you hover your mouse over the IE icon in your Taskbar. This allows quicker access to individual pages directly from the Taskbar.
- *Enable Quick Tabs* - Quick Tabs places a small box at the far left of your tabs when you have multiple open tabs. Clicking it opens a page which contains previews of the content of every open tab.
- *Enable Tab Groups* - Tab Groups allows IE to group together tabs which are related. Tabs originating from the same source page are grouped next to each other and use the same color.
- *When a new tab is opened, open* - You can select the default action when you open a new blank tab in IE (e.g. by clicking the New Tab button at the end of the tab bar, or by pressing CTRL+T) - 'The new tab page' opens a custom page which lists your most popular sites - see the Your Most Popular Sites section later in this chapter; 'A blank page' opens an entirely blank new page; 'Your first home page' opens up the first address listed in your Home Page setting. This setting does not impact on new tabs opened when clicking on links.
- *When a pop-up is encountered* - This setting allows you to choose what happens when a popup window attempts to open - whether it opens as a new tab, or an entirely new IE window. Popups are often used for advertising purposes, but there are some sites which use popups for legitimate purposes. In either case, I recommend selecting the 'Always open pop-ups in a new tab' to minimize resource usage, and to also help prevent pop-ups from slyly opening up as a separate minimized window.
- *Open links from other programs in* - When a program launches a web page for any reason, this option lets you choose where that new page appears: either in a new IE window; a new tab in the current IE window (recommended); or in place of the current contents of your existing IE window or tab.

Some tips you can use to make tabbed browsing easier in IE include:

- Clicking on any hyperlink with the middle mouse button opens that link in a new tab.
- Clicking on any tab with the middle mouse button closes that tab.
- Holding down SHIFT and left-clicking on any link forces it to open in a new IE window.
- Holding down CTRL and left-clicking on any link forces it to open in a new tab.
- Use CTRL+TAB to quickly cycle through all open tabs.
- You can reopen a recently closed tab by pressing CTRL+SHIFT+T.
- Left-click and hold on any tab and you can then drag and drop it to rearrange tab order.
- Right-click on any tab to bring up a tab-specific context menu.
- If you want to save a set of tabs as a single bookmark folder, click the Favorites icon (the star icon at the top right), then click the drop-down arrow next to the 'Add to Favorites' button and select 'Add Current Tabs to Favorites'.
- To open the contents of an entire Favorites folder in a series of tabs, right-click on the folder under Favorites and select 'Open in Tab Group'.
- To manage Tab Groups, right-click on a tab within the group and you can close the entire group for example by selecting 'Close This Group'.
- To automatically switch the current tab to a new website using any copied web address, right-click anywhere on the page and select 'Go to copied address' (or press CTRL+SHIFT+L); or select 'Search using copied text' if the copied text is not detected as a valid website address.

Importantly, by default each tab will open on the same line as the Address Bar. While the Address Bar will remain a constant size, each tab will become progressively smaller as more tabs are opened. If you wish to place tabs on a separate row and/or change the size of the Address Bar, see the Customize Internet Explorer's Appearance section later in this chapter.

Browsing History: As you browse the Internet, certain files and customized settings from websites are stored (cached) on your drive by IE to make your browsing faster in the future. Click the Settings button here and you can select how IE uses this cache to speed up your browsing. The individual settings in this section are as follows:

Check for newer versions of stored pages: Here you can tell IE how often to check to see if a web page has been updated. Any parts of a site which don't appear to have been updated since you last visited will be loaded from your cache rather than the site, and this can decrease page load times, especially for sites which have a lot of unchanged items to load up, such as large decorative images. I recommend selecting 'Automatically' here as this allows IE to detect updated content and load from the site only what it believes is necessary. However, if you want to be absolutely certain that you see the very latest version of every page you visit select 'Every time I visit the webpage', though this may increase page loading times. Note that you can manually ensure any web page shows the latest contents at any time by pressing CTRL+F5 when on that page - this forces IE to re-download the entire page from the site rather than loading anything from the local cache on your drive. Importantly, do not select the Never option here as that will mean IE may not show updated content from web pages you commonly view; it will always rely on the cached version, which may result in out-of-date content being shown.

Disk space to use: You can specify the maximum amount of space IE uses for its Temporary Internet Files cache in Megabytes in the box provided. If the cache is too small, it will generally result in longer page loading times; if the cache is too large, then depending on your Internet connection speed and your drive speed, you may still get longer page loading times, as IE has to search through the many files in its cache to find the components of a web page to load, when it may actually be faster just to load them from the original site. Therefore I recommend 300MB of disk space for the cache as a balance of size and speed. If you have a faster drive, and/or a slower Internet connection, and/or frequently view complex sites with lots of large images or scripts, you may wish to increase this cache to around 500MB. The maximum possible cache size is 1024MB (1GB).

Current Location: Internet Explorer lists the current location of its primary Temporary Internet Files cache. This is where all of IE's local web content is actually stored on your drive. You can view the files already there by clicking the 'View files' button, and you can view any downloaded programs or configuration files necessary for certain sites to run by clicking the 'View objects' button. If you wish to move this cache - to a faster drive for example - click the 'Move folder' button. To correctly delete the temporary file contents, it is recommended that you follow the instructions further below, rather than manually deleting any of the files.

History: Internet Explorer can keep a record of the addresses of all the websites you have viewed for a certain number of days. Here you can select how many days' worth of recently viewed websites IE keeps. If you don't want a history of visited sites to be kept at all enter 0 in the box. Alternatively, see the InPrivate Browsing section later in this chapter if you just want to temporarily disable the storage of browsing history at particular times. Having a saved history can be useful, particularly if you want to revisit a site you didn't add to your Favorites, and have a hard time remembering its name.

Caches and databases: This section allows you to control the way in which certain websites and apps store data on your system. As part of application of the IndexedDB specification in IE, covered in this Microsoft Article, some sites can store sufficient data on your machine to allow their functionality to work even without an active Internet connection. Here you can specify whether this functionality is allowed, and the warning level (in MB) at which you will be notified if greater storage is being used. This functionality can remain enabled to start with, and you can adjust or disable it if you find it is being abused by sites you frequently visit.

Delete Browsing History: Back under the main General tab, by clicking the Delete button under the Browsing History section, you will open a new box which contains a range of options. These options list the individual components of your stored browsing history, giving you greater control over the specific elements you can

delete. Note that if you don't wish to leave any trace of your browsing for a particular session, it is much easier to use the InPrivate Browsing feature of IE, which is covered later in this chapter.

It is completely safe to tick all of these boxes and click the Delete button to remove all traces of browsing, but this can decrease the efficiency of your browsing, especially since you will also lose any customizations you may have for particular sites, such as saved login details. For this reason, there is an option entitled 'Preserve Favorites website data' which, if ticked (recommended), will keep your customized data for any sites you have bookmarked in your Favorites. This maintains convenience and speed when accessing your favorite sites, while also allowing you to regularly clean out any data from all other sites you have visited. If you still want to remove all stored content then untick this box as well. In any case once you have selected which components you want to remove, click the Delete button at the bottom and they'll be removed immediately. If you want to have IE automatically delete your browsing history every time you exit IE, then tick the 'Delete browsing history on exit' box under the General tab as well.

Appearance: These options allow you to change the appearance of web pages, customizing colors, fonts and even forcing particular style sheets. You shouldn't alter these options unless you have specific needs, as it can result in some sites displaying incorrectly.

SECURITY

There are four zones, shown as icon here, for which you can set individual security levels. These are:

- *Internet:* The general world wide web, where the bulk (often all) browsing is done.
- *Local intranet:* For any computers connected to your machine within a local network.
- *Trusted Sites:* Specific websites you completely trust, and which you need to manually specify by clicking the Sites button.
- *Restricted Sites:* The opposite of Trusted Sites, which again requires that you specify the address of the individual site(s) you do not trust.

The aim of these zones is to allow IE to apply a different security level depending on the level of risk involved. For most users it is perfectly fine to just choose a security level on the slider for the default Internet zone. The main security level slider ranges from Medium to Medium-High, to High, and I recommend the default Medium-High level of security as it is designed to allow most normal Internet functionality without being overly restrictive nor too relaxed. For advanced users, click the 'Custom level' button and manually select the options for each security-related function - this is far too complex to detail here; the standard preset levels are fine for the average home PC user.

For users who frequently browse new, unfamiliar or risky sites, and want greater security, I recommend selecting the High security level for the Internet Zone. Then for the times you have problems with reputable trusted websites whose functionality has become crippled due to the High security for the general Internet zone, select the 'Trusted Sites' zone, click the Sites button and add the addresses of the sites you are certain are trustworthy. This zone is generally designed for websites which provide a verified secure connection (https://), such as banking and commerce websites, but if you are absolutely certain that a normal site is reputable and secure, untick the 'Require server verification...' box at the bottom, and you can then add any normal web address to the list. Now set the security slider for the Trusted Sites zone to something lower than High; typically Medium-High or Medium is sufficient for allowing normal functionality.

Alternatively, if you don't browse unfamiliar or risky sites often, you can select Medium or Medium-High for the general Internet Zone to ensure full functionality, and then click the Restricted Sites zone - which has a fixed High security level - and click the Sites button, then add specific websites you visit which you know are relatively untrustworthy to the list. This allows your general Internet browsing to be relatively unhindered, but for the times when you visit sites that are less trustworthy, you will have greater protection.

Both of the above methods carry certain risks. No website is truly 100% trustworthy, as any site can be compromised without the site owner's consent or knowledge, despite even the most stringent server security. On balance however, simply using the Medium-High security level for the Internet zone, when combined with Protected Mode (see below), is a sufficient compromise of security and functionality for normal browsing.

Enable Protected Mode: One of the most important security features in Internet Explorer is Protected Mode. This feature works for browsing much like User Account Control does for general system usage: it restricts websites and online programs from accessing system areas and launching or installing malicious or undesirable software. While it is not foolproof, it is an important level of automated protection and I strongly recommend that it be left enabled. Note that in Internet Explorer 10, unlike earlier versions of IE, there is no visible indicator on the Status Bar (if the Status Bar is enabled) at the bottom of the screen that Protected Mode is on. But if Protected Mode is disabled, a prompt will appear at the bottom of the IE window requesting that you re-enable it.

PRIVACY

The main slider here controls the level of privacy in IE, which for the most part pertains to Cookies - small files stored on your machine designed to hold your preferences for individual websites. Cookies are not usually malicious or dangerous, as they cannot read or delete data on your computer, and can be very useful. Some cookies may attempt to track your online behavior for advertising purposes, and for this reason, the 'Medium High' level is recommended, as it should not prevent legitimate cookies from being placed on your machine, while still protecting your privacy. To be even more selective, you can click the Advanced button and tick 'Override automatic cookie handling'. Third-party Cookies can usually be Blocked without any major issues, as these are mainly from advertisers. First-party Cookies on the other hand are often useful (e.g. for holding your login details for forums, or recording display preferences for particular sites), and blocking them can impair a site's functionality.

If you do decide to block all first party cookies, or if you select a higher Privacy setting on the slider, click the Sites button and you can manually allow or block cookies for specific website. I recommend adding your trusted favorite sites to this list and allowing them, preventing any problems with functionality. For example, if you set a High or Very High privacy setting, this will block almost all cookies, making some sites non-functional, but you can still allow specific site cookies by making sure they're in the list of allowed sites. For broader blocking of undesirable third party content see the Tracking Protection section later in this chapter.

Location: This setting relates to the geolocation feature in Internet Explorer. Microsoft's Location Services determines your actual physical location (latitude and longitude) based on your IP address or closest Wi-Fi access point, and then passes this information onto a requesting website. Social networking, shopping or map-related sites most frequently use this service, as do applications for mobile phones. However, there is a risk involved in broadcasting your physical location in this manner, particularly on social networking sites. By ticking the 'Never allow websites to request your physical location' box, you can prevent any website from successfully requesting and obtaining your physical location via the Windows Location Services feature. If this box is unticked, you will be prompted whenever a site makes a location request, and can choose to either 'Allow once' if you just want to test how the functionality is used on that particular site, or 'Always allow' if you want to permanently allow that site to determine your physical location each time you open it. Most PC users can safely tick this box to disable this feature, as the majority of websites do not require it.

Pop-up Blocker: A 'popup' is a new window or tab that opens when you visit particular sites, or click on particular links or areas of a site. They are most commonly used for unsolicited advertising, hence this option exists to block them. I recommend ticking the 'Turn on Pop-up Blocker' box, but you should also click the Settings button and manually add the names of websites you trust which may have legitimate popups

that would otherwise be blocked. For example, you may wish to add your Internet banking site to the list, or Microsoft.com, as these are trusted sites which may launch legitimate popups that would otherwise be blocked. By default when a popup is blocked by IE, a small warning bar will appear at the bottom of the page to inform you of this, and you may also hear a sound. If you want to disable either or both of these visual warnings, untick the relevant boxes here. This means that you will not be aware if a legitimate site tries to open a necessary popup box, and thus you may run into problems on some sites. I recommend leaving the 'Show Notification bar when a pop-up is blocked' box ticked, so that when you run into a pop-up while browsing, you are prompted with the pop-up notification bar and can choose to 'Allow once' if you just want to see what the particular pop-up is, or 'Always allow' if the pop-up is legitimate and/or it is a trusted website, and you can thus automatically add the website to the pop-up blocker's trusted sites list.

Finally, you can choose the blocking level as either Low, Medium or High. The default of Medium is recommended as it captures most annoying popups without blocking legitimate ones. If you choose High to block all popups then I strongly recommend manually adding trusted sites to the allowed list, as otherwise legitimate popups will also be blocked.

Note that some popups are launched when you click on a particular field, image or area of a web page, and are actually script-based events specifically designed to circumvent popup blocking. Internet Explorer may not be able to block these under certain circumstances. The only guaranteed way of blocking such popups is to disable the script-related functionality in Internet Explorer, which is done under the Security section of Internet Options by setting a High security level on the slider. However, this also prevents potentially necessary script-based features from working on many sites. Enabling the ActiveX Filtering feature, covered later in this chapter, can help alleviate this problem to a certain extent.

InPrivate: InPrivate Browsing is a feature that allows you to surf the web without leaving any trace of your activities on the PC. It is covered in more detail in the InPrivate Browsing section later in this chapter. Ticking the 'Disable toolbars and extensions when InPrivate Browsing starts' box will disable all installed toolbars and extensions when using InPrivate Browsing mode to prevent them from capturing any private data during an InPrivate session. This is recommended for maximum privacy. If you absolutely require their functionality during InPrivate Browsing then untick this box, but make sure to research your installed add-ons to ensure that they do not breach your privacy, as otherwise it will defeat much of the purpose of using InPrivate Browsing. As a general rule I recommend against installing toolbars and extensions wherever possible, for security, stability and performance reasons, regardless of whether you use InPrivate Browsing or not.

CONTENT

Family Safety: Clicking the 'Family Safety' button opens the Family Safety component of the Windows Control Panel, allowing you to set specific parameters for Internet surfing for particular accounts. This functionality is covered in detail under the Family Safety section of the User Accounts chapter.

Certificates: Certificates are a form of electronic authentication method to verify that a particular website or individual is what or who they claim to be. Certificates are described in more detail in this Microsoft Article, and are beyond the scope of this book in detailing their functions. Don't alter any of the settings in this section unless you are acting on sound knowledge. If a particular site displays a certificate error or warning, I recommend pursuing this further with the site owner, or doing web research before conducting any financial transactions or entering personal information on the site, as advised in this Microsoft Article.

AutoComplete: The AutoComplete feature can save any website address you have typed into the Address Bar (or have already stored in your History), any text you've entered into online forms, and any usernames and passwords you've entered on a web page. The aim is that next time you start to type a URL, or visit a site, AutoComplete will automatically complete or restore your typed text, speeding up logging in or filling out details, or typing URLs into the Address Bar. Click the Settings button to configure which particular aspects

of a web page AutoComplete will store. For security purposes I don't recommend enabling any of these options unless you have strong password protection on your user account, or the PC is physically isolated from others.

Note that having the 'Use Windows Search for better results' box ticked will mean that an item called 'Internet Explorer History' will be added to the Search Index used by Windows Search. This item can be removed from within the Indexing Options - see the Search Index section of the Windows Search chapter for details. However you can also disable it here by unticking this option and clicking OK.

Feeds and Web Slices: If a website you're viewing has RSS or Web Slice capability, you will see the orange RSS icon or the green Web Slice icon. You can then click the relevant icon to view the feed, or preview relevant slice information. Clicking the Settings button here allows you to configure how often such feeds and slices are updated, how they're read, and how IE warns you about Feed or Slice-capable websites. If you don't use these features, I recommend unticking all the boxes on this page, as it will help to speed up browsing.

CONNECTIONS

This section is essentially redundant for most home PC users. You should instead set up and customize the details of your Internet connection in the Network and Sharing Center. See the Network and Sharing Center section under the Windows Control Panel chapter.

PROGRAMS

Opening Internet Explorer: This option determines which version of Internet Explorer - whether the Metro version, or the Desktop version of IE - is opened whenever you click on a web link in another location. It is covered in more detail under the IE Desktop vs. IE Metro section at the start of this chapter

Manage Add-ons: Clicking this button allows you to configure Add-ons in IE. Any small program installed for the purpose of extending or altering the functionality of Internet Explorer is an add-on, also known as a plugin or extension, and you will typically be aware that a site wishes to install an add-on through prompts. You can view all of your add-ons here by selecting the relevant category and making sure that the Show drop down box under the Toolbars and Extensions category says 'All add-ons'.

Some add-ons are perfectly legitimate, such as allowing you to view PDF documents within Internet Explorer, or playing YouTube videos for example. The most commonly required add-ons are Flash Player and Java, and Internet Explorer 10 already comes with Flash player as a built-in add-on. You can download a range of Other Add-Ons which provide useful additional functionality for Internet Explorer. Most of these add-ons are free and operate similar to Extensions for Firefox or Chrome, making Internet Explorer more functional and customizable.

The problem is that some sites try to install add-ons which are unnecessary at best, or contain potentially harmful or intrusive scripts designed to be annoying or malicious at worst. If you are prompted to install an add-on by a website, then I strongly recommend not doing so unless the site is completely trustworthy, such as Microsoft.com, and after you have conducted some research to see if the add-on is absolutely necessary.

Furthermore, some free software will attempt to install third party browser toolbars as part of their installation process. These can take up a portion of screen space, collect data on your browsing behavior, and add to resource usage unnecessarily. Make sure you pay close attention during the installation of any third party software, and opt out of any prompts to install such unnecessary add-ons.

The less add-ons that are installed and enabled in IE the better, both for security and performance purposes, as well as for general stability. Even legitimate add-ons can potentially slow down the launching and browsing speeds of Internet Explorer, or destabilize it and cause it to frequently crash. Regularly check your

list of add-ons in the Manage Add-ons window, and right-click on and disable those that you don't frequently use. Do a web search if the add-on name does not seem familiar.

The Search Providers category in the Manage Add-ons box is covered under the General section earlier in this chapter; the Accelerators category is covered later in this chapter, as is the Tracking Protection category.

HTML Editing: Here you can select the program IE uses for editing the HTML code of web pages when you choose the 'Edit with *[program name]*' option under the File menu.

Internet Programs: Clicking the 'Set Programs' button here simply opens the Default Programs component of the Windows Control Panel, covered in full detail under the Default Programs section of the Windows Control Panel chapter.

File Associations: Clicking the 'Set associations' button here opens the Set Program Associations section of the Default Programs component of the Windows Control Panel, once again covered in full detail under the Default Programs section of the Windows Control Panel chapter. The only benefit of clicking the button here is that it automatically narrows down the list of files to those which can be opened by IE.

ADVANCED

This section contains important settings for Internet Explorer's functionality, security and general behavior. There are too many settings to be able to describe each one of them in full detail here, so I will discuss a few of the most important options and advanced features in more detail:

Accelerated Graphics - Use software rendering instead of GPU rendering: By default Internet Explorer is designed to use your Graphics Processing Unit (GPU, also known as the graphics card) to accelerate the display of any graphics-related features on websites. This is the optimal configuration which provides the best performance on most systems. However, on some older or low-end systems, GPU rendering is either not supported, or does not work properly. In these cases, this check box should be ticked, or is already ticked by default and grayed out. In all other cases, you should untick this box, and you should also make sure that you have installed the latest graphics drivers as covered under Step 5 in the Windows Drivers chapter, to ensure optimal performance in IE.

Accessibility - Zoom-related options: Different web pages have different sized text and pictures. Internet Explorer allows you to zoom in/out of any page at any time simply by selecting the zoom level in the Zoom box in the Status Bar (if enabled), or by clicking the Tools button and selecting the Zoom category. A quicker method is to hold down the CTRL key and scroll up or down with your mouse wheel. Alternatively, you can use CTRL + (plus key) or CTRL - (minus key) to progressively zoom in and out respectively. To reset a page to its default size, press CTRL 0 (zero). Here you can alter how this behavior works. If you tick the 'Reset zoom level for new windows and tabs', regardless of how zoomed in or out you are on your current tab, opening a new tab will mean the page will open at the default zoom level; if unticked, the new tab will open at the same zoom level as your current page. You can also experiment with the 'Reset text size to medium while zooming' option to see if it suits your tastes.

Browsing - Automatically Recover from Page Layout Errors With Compatibility View: Internet Explorer has a Compatibility View that helps correctly render web pages which use code designed for older browsers. You can switch to Compatibility View at any time by clicking the small Compatibility View (broken page) icon in the Address Bar. This will change the icon from white to a solid color, meaning that IE 10 will behave like an older version of IE for the purposes of correctly rendering the current site. You should only use this option if you believe a web page is being shown incorrectly, typically when elements on the page are out of alignment, obscured by other elements, or there are missing objects/text. Here there is an option entitled 'Automatically recover from page layout errors with Compatibility View'. If ticked, as the option name

implies, any page layout rendering errors will result in the page being automatically reloaded and shown in Compatibility View, which is recommended.

Browsing - Enable flip ahead: This option controls the new Flip Ahead feature of Internet Explorer. When it is enabled, it will allow Internet Explorer to attempt to determine what the next page of a multi-page web article is likely to be, and give you the ability to proceed to the next page by pressing the forward arrow next to the Address Bar. It only works on certain sites, and note that as part of the flip ahead feature, your browsing history will be sent to Microsoft to improve how flip ahead works. Unless you have major privacy concerns, this feature is best left enabled.

Browsing - Notify When Downloads Are Complete: By default, when you click on a link to initiate a download from a website, IE will bring up a prompt with more details. Depending on the type of file being downloaded, you may see a dialog box open with Open, Save, and 'Save As' options, or you may see a yellow bar shown at the bottom of the screen with Run and Save buttons, along with a 'Save As' option if you click the black arrow next to the Save button. In any event, if you click the Save button, the file will immediately start downloading to your *\Users\[username]\Downloads* directory by default; you will need to use the 'Save as' option if you wish to specify another directory. Although the progress of the download is shown in the bar at the bottom of the screen, once the download is completed, the bar will disappear and you will see no other prompt. You must tick the 'Notify when downloads are complete' box here if you wish Internet Explorer to present an explicit prompt telling you that the download is complete. This is recommended so that if you initiate a download in IE and start doing other things, you will be visually prompted to remind you of its completion.

To configure downloading options more thoroughly, click the Tools icon and select 'View Downloads' to open the download manager. Here you can see a list of all files downloaded to date, and can open each file by clicking the Open button. Click 'Clear List' to delete the entire list of downloads without deleting the actual files. Click the Options link at the bottom of the View Downloads screen, and you will be able to change the default directory used when you click the Save button for any file download, as well as also adjusting the notification option.

Security - Always send Do Not Track header: This option is enabled by default, and controls whether Internet Explorer sends a Do Not Track (DNT) request to each website you visit. This is similar to the Tracking Protection List (TPL) feature covered in the Tracking Protection section later on, however the DNT header is simply a request to websites asking that your activity not be tracked, while the TPL is a block list that actually prevents third party content from loading, and hence is more stringent. Both features are designed to protect information about your browsing habits from being used primarily by advertisers. This option is best left enabled.

Security - Enable Enhanced Protected Mode: A new feature of Internet Explorer 10, Enhanced Protected Mode (EPM) provides greater protection from a range of browser security exploits. This feature is not enabled by default, because it can conflict with certain plugins and toolbars. If you do enable Enhanced Protected Mode - which is recommended - then you will be prompted to temporarily disable EPM if it conflicts with certain add-ons, allowing you to browse trusted sites without EPM, automatically re-enabling it for the rest of your web browsing. Note that when EPM is enabled, on 64-bit systems Internet Explorer Desktop will run as a 64-bit application. Furthermore, Internet Explorer Metro already has EPM enabled by default and runs as a 64-bit app.

Security - Enable SmartScreen Filter: The concept behind SmartScreen is covered under the Windows SmartScreen section of the Security chapter. It is a new whole-of-system Windows 8 feature designed to prevent your PC against launching downloaded malware. However, it was originally an Internet Explorer-based feature, known as the Phishing Filter, that warned you if a particular site seemed to be deceptive, or a known phishing perpetrator. From Internet Explorer 8 onwards, the name of this option was changed to the

SmartScreen Filter. In IE 10, the filter has features to detect and block potential malware downloads, and it is strongly recommended that you leave the 'Enable SmartScreen Filter' box ticked under the Security section here. If you attempt to visit a potentially unsafe site, you will receive a bright red warning screen. At this point, nothing from the offending website has been loaded up, so you can simply click the 'Go to my home page instead' link to leave. For a list of options, click the 'More Information' link at the bottom of the warning screen. There you will see details of the threat, and if you are absolutely certain that the site is completely safe, you can either report it as safe, and/or click 'Disregard and continue' to ignore the warning and visit the site. This is not recommended unless you are absolutely certain the report is false. Remember that even trusted websites can unintentionally host malware without their owner's knowledge.

To manually check a particular site using the SmartScreen Filter, first browse to that site, then click the Tools icon, go to the Safety menu and select the 'Check this Website' item. To report a website as being unsafe, go to the same menu and this time select 'Report Unsafe Website'. This doesn't automatically add the site to the list of unsafe websites, it only reports it for further examination by Microsoft. Finally, you can also disable SmartScreen Filter in IE by selecting the 'Turn Off SmartScreen Filter' option here, but this is not recommended.

A combination of the Windows SmartScreen feature and IE's SmartScreen Filter will make it very difficult for malware to slip into your system, or launch successfully even if it gets in, so I strongly recommend leaving both of these features enabled.

For the rest of the more important Advanced settings in IE, I recommend that you start by leaving them at their defaults. If you've altered these settings, you can restore the defaults by clicking the 'Restore Advanced Settings' button. Once you've reverted to the defaults, adjust the specific settings described in more detail further above, then restart IE to make sure all changes are implemented.

SEARCH

The separate Search Box found in previous versions of IE has been removed. The Address Bar is now also a search box, and hence is named the OneBox. Aside from entering web addresses in the Address Bar, searches can also be initiated by typing the search term directly into the same box, and the suggested results will be shown in a drop-down box under different categories: your browsing history, your favorites, and the default search engine's suggestions. You can select the 'Turn on/off search suggestions' link at the bottom of the suggested links box to enable or disable this feature.

The default search provider is Bing, however by selecting another search provider at the bottom of the search suggestions box, or clicking the Add button, or by going to the 'Search Providers' section of the Manage Add-Ons window, you can add other search providers as you wish. Click the 'Find more search providers' link at the bottom of the screen to be presented with a list of search add-ons available for installation in IE. If you don't want sites or programs to suggest changes to your default search provider, then tick the relevant box at the bottom of the window as well. If you don't wish to have the Address Bar act as a search box, you can disable the search provider(s) in the Manage Add-Ons window by: right-clicking on the provider(s) and selecting 'Disable'; highlighting the provider and unticking the 'Search in the address bar' box at the bottom of the window; or highlighting the provider and clicking the Remove button to uninstall it. Note that you must have at least one search provider installed and set as the default - you can't uninstall the default provider.

INPRIVATE BROWSING

InPrivate Browsing is designed to allow you to surf the Internet without leaving any trace of your browsing activity on the PC you are using. To access it, click the Tools icon and select the 'InPrivate Browsing' option under the Safety menu, or press CTRL+SHIFT+P. A new browser window will open, clearly marked as "InPrivate". Any browsing done using this InPrivate session window will not store data on your drive. This

is ideal for people who browse the Internet using publicly shared machines, or if you simply want to ensure that there is no potentially embarrassing history or cached files stored on your PC from a particular browsing session.

While using an InPrivate session, IE will generate and store several temporary pieces of information, such as cookies, mainly to ensure that normal web functionality is maintained. But as soon as you close the InPrivate browser window, these are all automatically removed. Importantly, there are a range of caveats to keep in mind when using InPrivate Browsing:

§ If you add any Favorites, RSS Feeds or Web Slices while using InPrivate, or you install any software, or add a new home page, then such changes will be saved and kept permanently even after you close the InPrivate session.
§ If you don't close the InPrivate window then others may be able to view your browsing history and temporary files on the same PC.
§ InPrivate functionality does not extend to protecting your anonymity when surfing. Your IP address for example will still be visible and recorded on various sites as you browse the Internet.
§ An InPrivate session does not offer any greater security than using the standard IE mode. Do not mistake InPrivate as a form of protection against malware or phishing for example.
§ If you have installed any third party toolbars or extensions in IE, then unless you tick the 'Disable toolbars and extensions when InPrivate Browsing starts' box as covered under the Privacy section earlier in this chapter, these toolbars and extensions may be transmitting data about your browsing behavior regardless.

While InPrivate Browsing is a useful feature, especially for those using shared machines, it is not a substitute for correctly configuring all of IE's options as per this chapter, and also exercising common sense as to general browsing. InPrivate does not guarantee that others will not find out about your browsing habits through other techniques, so minimize the extent to which you undertake potentially embarrassing on shared PCs for example.

If you wish, you can configure Internet Explorer to always open in InPrivate Browsing mode by default - see the Advanced Settings section later in this chapter.

ACTIVEX FILTERING

ActiveX controls are small programs used by websites to enhance Internet browsing functionality, such as enabling animated menus or web videos. The most common ActiveX control is Flash Player, which is built into Internet Explorer 10 on Windows 8. Just like any program, certain implementations of ActiveX-based software can incorporate security risks due to malicious intent, or even when non-malicious, can impact on performance or functionality in undesirable ways.

Internet Explorer has a feature called ActiveX Filtering that allows you to quickly toggle ActiveX controls on or off on a per-site basis, without having to alter your main security settings or completely disable ActiveX. To globally enable ActiveX Filtering, click the Tools icon and under the Safety menu select 'ActiveX Filtering'. ActiveX Filtering will prevent any site with ActiveX controls from loading such programs. To the site in question, it will be as though you don't have the required software to run the programs.

ActiveX Filtering can then be enabled or disabled on a per-site basis by using the ActiveX Filtering icon - the small blue circle with the slash through it - which appears in the Address Bar. This icon will be dark blue when filtering is enabled, and gray when filtering is not in effect. By turning off ActiveX using the icon, you are disabling ActiveX Filtering only for the current site. Explorer will automatically reload a page whenever ActiveX Filtering is toggled on a site to implement the change without the need to restart IE, but if you don't see the ActiveX Filtering icon after enabling ActiveX Filtering, manually refresh the page.

Note that if your main security setting - covered under the Security section earlier in this chapter - is set to High, then no ActiveX controls can be run, regardless of your ActiveX Filtering setting. You may wish to lower your IE security to Medium-High and enable ActiveX Filtering instead as a better compromise. This combination will let you run signed ActiveX controls on trusted websites that you have manually chosen to allow, without having them run at any other time.

TRACKING PROTECTION

Previously called InPrivate Filtering, Tracking Protection is a feature that goes hand-in-hand with InPrivate Browsing and the Do Not Track header. InPrivate Browsing is designed to remove traces of your activity from the PC, but it does not protect your privacy when online. The Do Not Track header is a request to websites to help protect your privacy, but it can be complied with or ignored. Tracking Protection on the other hand attempts, to a reasonable extent, to preventing your private data from being broadcast unnecessarily to third party sites (such as advertisers) which are displaying some of the content on the page you are viewing.

Tracking Protection is disabled by default, but can be turned on by clicking the Tools button, going to the Safety menu and selecting 'Tracking Protection'. This takes you to the Tracking Protection section of the Manage Add-ons window. This feature works on the basis of a Tracking Protection List (TPL), which contains addresses that can be blocked or allowed, so you will need to enable the 'Your Personalized List' item and click the Settings button to open it for further configuration. For most users the default 'Automatically block' option is recommended, as it allows Tracking Protection to progressively detect third party content which is found across a range of sites, and eventually block those it considers to be unnecessary to the main functionality of the site. More advanced users can manually choose to block or allow content if you're not satisfied with the way in which IE is automatically blocking certain content - select the 'Choose content to block or allow' option, highlight the desired item to block or allow, and click the Allow or Block button accordingly for each item. At the bottom of the Settings window there is a small box which allows you to change how many websites need to be visited with the same third party content before it appears on the list of Content Providers in the Settings screen. The default is 10, but you can lower it to 3 or raise it to 30; the lower the number the more third party content will be blocked, and hence also appear for you to choose to block or allow in the list.

The most useful feature for the average user however is the ability to import pre-made Tracking Protection Lists. These lists can found on the Microsoft TPL page, and by clicking 'Add TPL' next to the relevant list(s) you wish to use, you will be prompted to download and install them in IE. Once installed, the list is added to any existing lists you already have under the Tracking Protection section of the Manage Add-ons window. These third party TPLs are usually updated frequently, and automatically updated on your machine by IE on a regular basis. Using a third party TPL is the best method for most users to ensure that the correct content is being blocked, rather than attempting to manage your own personalized list.

Tracking Protection is not specifically designed as an ad blocker; it is a general tool to limit the amount of data you send to third party providers. Enabling Tracking Protection may result in some sites not displaying correctly, or possibly missing important functionality, particularly if you use certain third party TPLs. Also keep in mind that using Tracking Protection to block advertising can and will affect the viability of many sites on the Internet which rely on third party advertising income to remain free to view. If you choose to employ Tracking Protection to block the ads on sites you enjoy, consider donating to them directly if you wish to see them remain open and free to use.

ACCELERATORS

Accelerators are browser-based tools that provide additional functionality for a site. You can access an Accelerator by highlighting a portion of text on a site and clicking the blue Accelerators button which appears. To access a list of Accelerators currently installed on your IE, right-click the blue button and select 'All Accelerators', or click the Tools button in IE, select 'Manage Add-Ons' and then select the Accelerators category. There are additional free Accelerators you can download. You can view the full list by right-clicking on the Accelerators button and selecting 'All Accelerators'>'Find More Accelerators', or by clicking the 'Find More Accelerators' link in the 'Manage Add-Ons' screen. While they may provide useful functionality, I recommend exercising constraint in how many you add to IE.

If you find the Accelerators functionality unnecessary or annoying, then disable all of the available Accelerators in the 'Manage Add-Ons' window, then disable the blue Accelerators button by unticking the 'Display Accelerator Button on selection' option under the Advanced section of Internet Options - see earlier in this chapter for details.

< INTERNET EXPLORER METRO

The Metro version of Internet Explorer can be accessed via the Internet Explorer tile on the Start Screen. The interface in this version of IE is entirely different to the Desktop version of Internet Explorer 10. This section will cover the key features of the IE Metro interface.

BASIC USAGE

Address Bar: The Address Bar is found at the bottom of the IE Metro window, and is initially displayed, but becomes hidden after a short period of time to allow maximum viewable browsing space. To bring up the Address Bar at any time, right-click on a page. Web addresses can be entered normally in the Address Bar, and can then be launched by pressing Enter, or clicking the Go arrow button which appears at the far right of the Bar.

Frequently Visited & Pinned Sites: When you click in the Address Bar, a list of frequently opened sites will also be shown as tiles above the Address Bar area, as well as any sites that you have pinned to the Start Screen. Clicking any tile will launch the relevant site, and right-clicking on it will allow you to choose whether to open the site in a new tab, or remove it from the Frequent list or Start Screen. You can also access this Frequent list in IE Desktop, and customize it as well - see the Frequently Visited Sites tip under the Advanced Settings section of this chapter.

Tab Bar: To access a list of open tabs, right-click on the page and open tabs will be shown as individual page thumbnails at the top of the IE Metro window. You can click on any thumbnail to switch to that tab, or click the small 'x' at the top right of it to close that tab. You can add a blank new tab by clicking the small '+' button at the top right of the Tab Bar, or you can close all tabs by clicking on the '...' button and selecting 'close tabs'.

InPrivate Browsing: To open an InPrivate Browsing session in IE Metro, open the Tab Bar, click the '...' button at the right, and select 'New InPrivate tab'. You will be notified that the new tab is using an InPrivate session.

Pin to Start: There is a dedicated 'Pin to Start' (pin) button in the Address Bar, which if clicked, provides you with the ability to pin any website to the Start Screen as a separate tile. When that tile is clicked, depending on your settings, it will launch that site in IE Metro or IE Desktop.

Page Tools: The 'Page Tools' (wrench) button on the Address Bar provides access to three separate features when clicked: the 'Get app for this site' option will allow you to download a dedicated app (if available) for that site from the Windows Store; the 'Find on Page' option opens a small search box at the bottom left,

which allows you to conduct text searches on the current page; and the 'View on Desktop' option will open the current site in the Desktop version of Internet Explorer

Forward/Back/Refresh: To navigate forward or backwards through your browsing history in the current session, you can use the forward and back arrows shown at the far left and right of the Address Bar. Alternatively, move your mouse to the far left or far right of the screen, and gray left or right arrows will appear as relevant, and these can be clicked in the same manner to move you through your history of viewed pages. To refresh a page, click the circular Refresh button in the Address Bar. You can also force a complete reload of the site by pressing CTRL+F5.

Scroll Bars: Any scrolls bars are hidden until you move your mouse to the far right or bottom of the screen, then they will appear as gray bars which can be used as normal.

Zoom: To zoom into or out of content, you can hold down the CTRL key and scroll up or down with your mouse wheel. Alternatively you can use CTRL + (plus key) or CTRL - (minus key) to progressively zoom in and out respectively. To reset a page to its default size, press CTRL 0 (zero).

Context Menus: Right-clicking on a web page will generally open the Address Bar and Tab Bar. However if you right-click on certain areas of a website, such as a link or an image, you will instead get a small pop-up box with relevant context menu options, such as 'Copy Link' or 'Save to Picture Library'.

INTERNET OPTIONS

As covered in the IE Desktop vs. IE Metro section at the start of this chapter, many of the options which you set for the Desktop version of Internet Explorer will apply to the Metro version of Internet Explorer. This means you should go to the Internet Options component of the Windows Control Panel, or look for 'Internet Options' under the Tools menu of IE Desktop, and first adjust all the settings there as covered under the Internet Explorer Desktop section earlier in this chapter.

There are several options which you can control separately for IE Metro. To configure the options specific to the Metro version of Internet Explorer, go the Start Screen and open the Internet Explorer tile. Then open the Charms menu, select Settings, then click the 'Internet Options' item. The settings are covered below:

Delete Browsing History: Clicking the Delete button here deletes your browsing history, similar to pressing the Delete button under the Delete section of the General tab of the Internet Options in IE Desktop. In IE Metro, all history is deleted, as there are no option to choose what to keep as with the Desktop version of IE.

Permissions: If the 'Ask for location' slider is set to On, websites can request your location data from Windows. If set to Off, location tracking by websites will not be allowed. To clear all existing tracking permissions, click the Clear button.

Zoom: The Zoom slider here lets you adjust the screen zoom, from 50% to 400%.

Flip Ahead: The Flip Ahead function is covered under the 'Browsing - Enable flip ahead' setting of the Internet Explorer Desktop section of this chapter. Here you can choose to enable or disable it specifically for IE Metro.

Encoding: The options here allow you to change website encoding, in case text is not displaying properly. If you experience problems you believe are related to encoding, first set the 'Set encoding automatically' option to On, and if that doesn't work, manually select from the options available.

OTHER FEATURES

Most of the other features of IE Metro will function much like IE Desktop. For example, both InPrivate Browsing and Tracking Protection will work in IE Metro. Enhanced Protected Mode is also enabled by default in IE Metro.

Some features will not work in IE Metro. ActiveX Filtering doesn't work, because IE Metro does not support ActiveX controls or any other form of add-ons, and the built-in Flash functionality in IE Metro is limited. This means that if you run into sites which require certain add-ons or full Flash features, you should click the 'Page Tools' (wrench) button in IE Metro and select 'View on Desktop' to continue your session on Internet Explorer Desktop, which has full functionality.

You cannot access the History Manager, Downloads Manager or Favorites in IE Metro.

Search in IE Metro is also different. You can conduct basic searches in the Address Bar, giving you results which come from your browsing history, Favorites and pinned sites, along with suggested top results from your search provider. To conduct a full search, open IE Metro, then open the Charms menu and select Search, then enter your search term in the Search Box.

Finally, remember that as a Metro app, IE Metro becomes suspended and thus retains the page you were viewing in your current session when you switch away from it. To close an IE Metro session you will need to do a full app close.

< ADVANCED SETTINGS

This section contains IE customizations, ranging from moderately simple to more advanced techniques.

CUSTOMIZE INTERNET EXPLORER'S APPEARANCE

Internet Explorer 10 allows customization of its interface, but only in the Desktop version, and even then there isn't a great deal of scope for changing the way it looks. By default the IE 10 interface is already quite streamlined. However you can customize the interface very easily in a range of ways:

Menu, Favorites, Command and Status Bars: By right-clicking on an empty area of the main IE toolbar (e.g. in the blank area to the right of any open tabs), you can access the main interface customization options. In the context menu which appears, you can choose to display a Menu Bar, Favorites Bar, Command Bar, and Status Bar - all of which will take up additional vertical web viewing space in return for easier access to IE's primary functions. Note that a valid alternative to having the Menu Bar permanently showing is to open it temporarily at any time by pressing the ALT key. You can also choose to have tabs displayed on their own row, rather than next to the Address Bar, by selecting the 'Show tabs on a separate row' item.

Favorites, History, Feeds Sidebar: Under the View menu of the Menu Bar, select the 'Explorer Bars' item and you will see three further options: Favorites, History and Feeds. Selecting any of these opens up a sidebar in IE which contains three tabs corresponding to the display of your History, RSS Feeds and Favorites. This is identical in function to pressing the Favorites (star) icon at the top right of IE.

Move Stop and Refresh Buttons: If you wish to move the Refresh (circular arrow icon)/Stop (x icon) button from the right side of the Address Bar to the left, right-click on the icon and select 'Show Stop and Refresh before Address bar'.

Resize Address Bar: If you have the Address Bar and tabs on the same row, you can resize the Address Bar by hovering your mouse in the small gap between the Address Bar and the first tab next to it, then when the cursor turns to a double-ended arrow, left-click and drag the Address Bar to your desired size.

Full Screen Mode: If you want the web pages you are viewing to take up the entire screen, devoid of any of IE's interface elements, press F11 at any time, or click the Tools icon and under the File menu select 'Full Screen'. You can toggle Full Screen mode on and off using the F11 key. In Full Screen mode, only the Status Bar (if enabled) and the right scroll bar will appear - the main IE interface elements will slide out of view after a moment, and even the Windows Taskbar will be removed. If you move your mouse to the top of the screen, the main IE interface will temporarily reappear. This is very similar to the IE Metro interface.

You can navigate in Full Screen mode using a range of keyboard commands:

Back: ALT+Left Arrow
Forward: ALT+Right Arrow
Refresh: F5
Stop: ESC
Home: ALT+Home
Favorites: ALT+C
Tools: ALT+X

If you get used to Full Screen mode, and want to have Internet Explorer Desktop start up in it every time it launches, close all instances of Internet Explorer, then go to the following location in the Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
Fullscreen=yes
```

Change the STRING value from `no` to `yes`, and now each time you launch Internet Explorer Desktop it will automatically open in Full Screen mode. You can still toggle IE back to normal mode at any time using the F11 key, but doing so will reset this Registry value back to its default of `no` and hence IE will start normally the next time you launch it.

FREQUENTLY VISITED SITES

Both versions of Internet Explorer provide the ability to display a list of the sites you most frequently visit, as long as you haven't disabled or cleared your History. The Frequent tab lists thumbnails of your ten most popular pages/sites, ranked by how often you visit them. You can access this list of frequent sites at any time in several ways:

- By right-clicking in IE Metro and clicking in the Address Bar, a set of Frequent tiles will be shown.
- By clicking the 'Use new tab' button under the General tab of Internet Options to set *about:tabs* as your home page address. Clicking the Home Page button on IE Desktop will now open the Frequent page.
- By going to Internet Options, clicking the Tabs button under the General section, and adjusting the 'When a new tab is opened' option to 'The new tab page'. Clicking the New Tab button at the far right of your tab bar in IE Desktop will open the Frequent page.

Note that secure sites whose addresses start with *https://* will not be displayed in this list if you have ticked the 'Do not save encrypted pages to disk' option under the Security section of the Advanced tab of Internet Options.

By default, this display of popular sites is 2 rows of 5 thumbnails each, totaling 10 favorite pages. You can alter the default number of rows by going to the Registry and doing the following:

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\TabbedBrowsing\NewTabPage]

NumRows=2
```


In the NewTabPage sub-folder create a new DWORD called NumRows and set it to the number of rows you wish to display in the Your Most Popular Sites page. The default is 2, however you can set up to 5 rows (each row containing 5 thumbnails). To revert back to the default display of 2 rows, either set the value to 2, or delete the NumRows key altogether.

You can also get suggestions for sites you might like to visit by clicking the 'Discover other sites you might like' link on the Frequent page, and following the instructions to enable Site Suggestions. This feature will then provide you with a list of sites similar to those you have been browsing which may be of interest to you.

You can remove any page from the frequent list by right-clicking on it and selecting 'Remove this page'. You can also click the 'Hide Sites' link at the bottom right to hide all the site thumbnails from the page, or you can disable your History to prevent IE from compiling this list.

INTERNET EXPLORER 64-BIT

If you are running Windows 8 64-bit, by default whenever you launch Internet Explorer Metro, it will launch as a 64-bit app. The Desktop version of Internet Explorer on the other hand runs as a mixture of 32-bit and 64-bit processes. To make IE Desktop launch as a pure 64-bit application, you will need to enable Enhanced Protected Mode, found under the Security section of the Advanced settings in Internet Options. This setting is covered in more detail earlier in this chapter.

The main issue is that while Internet Explorer 64-bit can be more stable and secure, and may be faster, it also has compatibility issues with 32-bit add-ons. This is not a major concern for Internet Explorer 10, as the most common add-on - Flash Player - comes built into IE, and can run in 64-bit mode. However, if you frequently use other 32-bit-only add-ons, then you may need to disable Enhanced Protection Mode for IE Desktop.

START WITH INPRIVATE BROWSING MODE ENABLED

By default the InPrivate Browsing mode in Internet Explorer Desktop requires that you start up IE normally, then select the 'InPrivate Browsing' option under the Tools>Safety menu, or press CTRL+SHIFT+P, to open a new browser window which specifically uses InPrivate Browsing. To avoid all of this, you can create a shortcut which opens IE Desktop already in InPrivate Browsing mode, ready to go at the start of every session. To do so, follow these instructions:

1. Right-click on the Desktop and select New>Shortcut.
2. In the Location box, use the following path:

   ```
   "C:\Program Files\Internet Explorer\iexplore.exe" -private
   ```

   Note: Change the drive letter shown above to match the drive letter for your system drive.
3. Click Next, and give it an appropriate name.
4. Click Finish to close the box.

Now whenever IE Desktop is launched from this icon, it will automatically open with InPrivate Browsing mode already activated.

FTP with Explorer-Based Windows

Internet Explorer allows you to access files stored on web servers using FTP, a protocol designed specifically for file transfers over the Internet. Click a valid FTP:// address on a web page, or enter the address in IE's Address Bar, and the server's contents can be viewed directly in Internet Explorer. If the FTP server requires login authentication, you will be prompted accordingly. This feature is already possible on most web browsers, so it is nothing new or exciting.

An interesting added feature of Internet Explorer is the ability to subsequently open the FTP server in File Explorer, allowing you to manage file transfers to and from the FTP server more easily. To do this, while at an FTP address in IE, open the View menu on the Menu Bar (ALT+V) and select 'Open FTP Site in File Explorer'. A File Explorer window will open, and you may be prompted to re-enter your login details for the FTP site. Once logged in, you can now transfer files back and forth to the FTP server from your drive just like any normal folder in File Explorer. You can also use the Dual Window Explorer View tip under the Advanced Features section of the File Explorer chapter to open two File Explorer windows and position them side by side for easier file transfer operations.

If you want a much more advanced FTP manager, I recommend the free Filezilla FTP utility which provides a range of features with a convenient and customizable interface.

Increase Maximum Simultaneous Connections

By default Internet Explorer only allows six items in total to be downloaded at any one time from a server. This can be slow for sites which have multiple items that need to be downloaded before the page can be displayed, or for downloading multiple files. You can increase the number of maximum http connections in IE by going to the following location in the Registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_MAXCONNECTIONSPER1_0SERVER]

iexplore.exe=10
```

The `iexplore.exe` value above doesn't exist, so create it as a new DWORD and in Decimal view assign the maximum number of connections you wish to have, e.g. 10 as shown above. You should also change the value at the key below:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_MAXCONNECTIONSPERSERVER]

iexplore.exe=10
```

The value above doesn't exist, so create it as a new DWORD and in Decimal view assign the maximum number of connections you wish to have.

Restart Windows, or logoff and logon, to implement this change. You can experiment with higher values if you wish, but note that increasing the maximum number of simultaneous connections to a very high value may technically be a breach of Internet Standards, and could result in your connection being refused, so if you experience any problems lower the values, or simply delete them altogether to reset it back to default.

DNS Cache Issues

Whenever your browser tries to load up a page on the Internet, it has to access a Domain Name System (DNS) server to resolve or translate the text address you use (e.g. www.google.com) into the actual IP address for the website (e.g.: 74.125.67.100). Since your browser needs to check DNS addresses each time it loads any web pages, the browser speeds up this process by locally storing the DNS addresses you use for a period of time so that the next time you try to go to the same address it uses the IP address it has cached

rather than looking it up again on a DNS Server. Unfortunately if a site is down temporarily, or has recently moved to a new IP address, then your DNS cache may store the site as being inaccessible for a while even if it comes back online shortly afterwards, and therefore every time you try to connect to it for a while you will get an error.

To resolve any DNS problems with web pages not loading up at all or loading up with outdated information, open an Administrator Command Prompt and type `ipconfig /flushdns` and press Enter. This will clear your DNS cache.

For more advanced users who want to make sure that the browser never stores a negative DNS cache entry - that is, one which says a site is inaccessible when it may be accessible - then go to the following location in the Registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters]
MaxNegativeCacheTtl=0
```

If the value above doesn't exist, create it as a new DWORD and assign it a value data of 0 so that no negative DNS entries can be kept in the DNS cache. You can also set the length of time in Time To Live (TTL) for a positive (or working) DNS cache entry to remain active before being updated. To do this, add the following DWORD in the same location:

```
MaxCacheTtl=10800
```

Assign it a value which measures (in seconds) the total Time To Live for the positive cache entry. Make sure to enter the amount of seconds in Decimal view. Do not set this value too low, as your DNS cache will effectively become useless, and browsing will take longer. A value of between 3 and 6 hours (10800 - 21600 seconds) should be fine.

FIX INTERNET EXPLORER

If you are having problems with Internet Explorer, you can browse through this Internet Explorer 10 Support Site. To attempt to automatically diagnose and repair an Internet Explorer issue, you can run through this Microsoft Interactive Support Wizard. You can also reset all of Internet Explorer's settings to their defaults by opening Internet Options - via the Windows Control Panel if you can't access it from within Internet Explorer itself - then under the Advanced tab, click the Reset button and follow the prompts.

The most common problems in Internet Explorer, and indeed in most other browsers, stem from add-ons. These add-ons can be installed without your knowledge by third party programs, and can destabilize IE, increase its resource usage, and cause other problems depending on the type and number of add-ons installed. Internet Explorer itself analyses add-ons to a certain degree to see if they are causing an increase in startup time for example, and will warn you if this is the case. See the Manage Add-ons section earlier in this chapter for details of how to check for, and if necessary, disable or remove unnecessary add-ons in IE. This is important not only for stability and performance, but also for privacy and security purposes.

< OTHER INTERNET BROWSERS

You may have heard of other browsers, and indeed if you are not completely happy with Internet Explorer, you can trial alternatives to see if they better suit your needs. There are at least three other major free browsers which are a viable and secure alternative to IE: Mozilla Firefox, Google Chrome and Opera.

My personal preference is for Firefox. It is an excellent browser which is free and well-supported and runs without any problems alongside Internet Explorer, giving you the opportunity to try it out to see if you prefer it, or to use it for more specialized/advanced tasks for which IE is not suited. The main advantage of Firefox over Internet Explorer, and many other browsers, is that Firefox is extremely customizable, both in its interface and functionality, through a truly massive range of free Extensions and Themes. To find out more about Firefox, read the Firefox Tweak Guide which covers all aspects from basic to the advanced.

All of the major browsers, including Internet Explorer, have the essential features required for fast, secure browsing. It all depends on which browser best suits your tastes, as there is no outright "best" browser.

WINDOWS LIVE MAIL

Windows 7 was the first version of Windows not to provide a built-in email application. Windows 8 reverses this situation by provides a default email client in the form of the Metro-based Mail app, available on the Start Screen. However the Mail app is completely different from that which Windows XP or Vista users have become accustomed to. While it has a range of benefits, including live updates on the Start Screen, and notifications on the Lock Screen, it is extremely sparse in terms of features and customization opportunities, as well as the types of email accounts which you can use with it. For most PC users, it will be necessary to install a full-featured desktop mail application.

The free Windows Live Mail does a very capable job of providing Windows 8 users with the required desktop mail application. For the most part, Windows Live Mail functions much the same as Vista's Windows Mail. However, it does require a bit of customization if you want to get it to look and function like the Windows mail clients in Windows XP and Vista, which is precisely what we cover in this chapter.

First, we'll examine the Metro Mail app and cover its key features, for those who wish to use the app.

< MAIL METRO

The built-in mail application in Windows 8 is accessible by clicking the Mail tile on the Start Screen. This app will only run under the Metro environment, and not on the Desktop. The main settings for the Mail app can be found by opening Mail, then going to the Charms menu and selecting Settings. The Accounts option will show your current mail account(s), which you can click to edit. I strongly recommend editing each account to give them a unique name in the 'Account Name' box, as this is how you will be able to differentiate them on the main Mail app screen.

You can also click the 'Add an account' link to add a new email account to Mail. At present the types of email accounts you can add are restricted to Hotmail, Google or Outlook-based accounts. You cannot add IMAP or general POP accounts. Once an account is added, it will be shown in the left side of the Mail app, with multiple accounts stacked on top of each other, and their full folder structure becoming available when you click on the account name.

To create a new email, select an account and then click the large '+' button at the top right. To see a range of options, right-click on a specific email message in the second column of the Mail app. As noted, the functionality in the Mail app is very limited, but may improve with updates to the app. For details on the Mail apps current capabilities, see this Microsoft Article.

< WINDOWS LIVE MAIL

Download the Windows Essentials Installer, launch it, and during the installation process make sure that you choose the programs to install - only the Mail component is ticked for now. You can rerun the installer and select other Windows Essentials components at any other time.

Once installed, the default appearance and functionality of Windows Live Mail may be confusing and undesirable to users of previous versions of Windows Mail. Below we examine how to customize it to bring it more in line with earlier versions of Windows mail clients. If you don't wish to undertake any of these customizations, you can skip to the Basic Settings section later in this chapter.

Sign In: After installing Windows Live Mail, you will be prompted to Sign In, and there is also a 'Sign In' button at the top right of the Windows Live Mail window. You do not need to sign in or synchronize with anything. Signing in in this manner is only necessary if you have a Windows Live ID and you wish to synchronize your contacts across Live-enabled Hotmail or Messenger accounts for example. If you wish, you can simply ignore the Sign In prompts. If you're not signed in, the Sync button becomes a 'Send/Receive' button, and when clicked, checks for any new mail, and sends any outstanding mail for your mail accounts.

The instructions that follow are primarily aimed at bringing Windows Live Mail's look and functionality as close as possible to that under previous Windows mail clients, such as Windows Mail and Outlook Express. Note that on a system with multiple Windows user accounts, each user will have to configure Windows Live Mail, as customizations and accounts for Windows Live Mail are stored separately for each user account.

STEP 1 - EMAIL ACCOUNTS

After installing Windows Live Mail, open it and you will first need to recreate or import all of your email accounts. On a multi-user PC, each user should add or create their account while logged in under their own user account, as this provides proper separation and privacy for each account.

Importing Email Accounts

1. To import any email accounts saved as .IAF files, click the File button at the top left of the window, select Options, then select 'Email accounts'.
2. Click the Import button and browse to the directory where your .IAF files reside.
3. Select the accounts and import them one by one; each account will be added as a separate category in the left pane of Windows Live Mail.
4. If you wish to change any of the account details, right-click on the account name and select Properties, then edit the details as appropriate.
5. Right-click on the email account you wish to use as your primary account and select 'Set as Default'.

Creating Email Accounts

If you don't have any saved .IAF files, go to the Accounts menu and select Email. Follow the prompts to add a new email account.

An important note about email accounts in Windows Live Mail: click the File button at the top left, select Options, then select 'Email accounts'. Now for every email account, it is recommended that you click the Properties button, and under the Advanced tab, untick the 'Leave a copy of message on server' box. If this box remains ticked, it means every email you receive and download will also be stored on your email server, increasing the potential for your mail server to eventually run out of room, and hence reject all incoming emails. Once an email has been received in Windows Live Mail, you can save it to any folder you wish (except Deleted Items) and it will be stored on your computer. There is no need for a copy of it to also be stored on your mail server unless you are using a portable device with limited storage.

STEP 2 - IMPORT SAVED MAIL

The next step is to restore any saved emails you may have exported from other versions of Windows Mail, or from Windows Live Mail itself.

Importing Saved Emails

1. Click the File button at the top left and select 'Import Messages'.
2. If importing messages saved in Windows XP, select 'Microsoft Outlook Express 6'; if importing messages saved in Windows Vista select 'Windows Mail'; otherwise select Windows Live Mail.
3. Browse to the location where your saved emails are stored, select the file(s) or folder(s) and follow the prompts.
4. Your emails should be restored in an 'Imported Folder' under the 'Storage Folders' category in the left pane, and you can manually move these folders to a new location if you wish. For example, drag one of your folders from underneath the 'Imported Folders' category to the 'Storage Folders' heading to make it a subfolder alongside the other main folders. If you can't see any 'Storage Folders' category, then go to the View menu and click the 'Storage folders' button to enable it.
5. To create any new folder(s) for storing saved emails, right-click on the 'Storage Folders' category and select 'New folder', then enter the folder name and the location where you wish to place it.
6. You can delete any custom folder by right-clicking on it and selecting Delete, except for the default Inbox, Drafts, Sent Items, Deleted Items and Outbox folders which can't be deleted.

STEP 3 - FOLDER PANE & UNIFIED INBOX

By default Windows Live Mail provides a central location for displaying new emails from all of your email accounts in the form of the 'Unread email' subfolder of the 'Quick Views' category. However, this location displays all unread emails from all of your email accounts, which means even old unread emails will be displayed here (excluding any unread emails in the Deleted Items or Junk Mail folders). That means it's not really a unified Inbox for all of your email accounts.

To customize the folders which appear under Quick Views, right-click on the Quick Views category header and select 'Select Quick Views'. In the window which opens, you can add or remove relevant folders by ticking or unticking the desired boxes. For example, you can tick the 'All Inbox' category to add it to Quick Views. This will display all the emails from each inbox of every account in a single location.

If you have Quick Views enabled and have set up the subfolders appropriately so that you can see both new and saved emails in the relevant subfolders of Quick Views, you can remove the 'Storage Folders' category if you wish by going to the View menu and clicking the 'Storage folders' button. You can also minimize your individual email accounts by clicking on the small arrow next to each account heading, further reducing clutter in the Folder Pane. This provides a very streamlined view.

Some users may prefer a unified Inbox, and a folder structure in the Folder Pane similar to Windows Mail or Outlook Express, rather than the Quick Views category. Especially as Quick Views and its subfolders can't be renamed, and you can't add custom folders to it. Follow these steps:

1. Go to the View menu.
2. Under the Layout section, click the 'Quick views' button so that it is not highlighted - this removes the Quick Views category altogether. Also click the 'Compact shortcuts' button so that it is highlighted - this reduces the Mail, Calendar, Contacts, Feeds and Newsgroups items shown at the bottom of the Folder Pane to just a row of icons with no text. Make sure the 'Storage folders' button is highlighted, as this category will become the main folder structure we will use in the Folder Pane.
3. Go to each of your individual email account category headings in the Folder Pane, and click the small arrow next to them to collapse all of the subfolders underneath them.

The next set of steps create a unified Inbox for all of your accounts, similar to that in previous versions of Windows mail clients:

4. Right-click on the 'Storage Folders' category heading and select 'New Folder', and name this folder Inbox.
5. Go to the Folders menu and click the 'Message Rules' button.
6. In the window that appears, in the first pane scroll down and tick the 'For all messages' option, and tick 'Move it to the specified folder' in the second pane beneath it.
7. Click the blue underlined specified link, scroll down the list and select the Inbox folder you recently created under the 'Storage Folders' category, then click OK.
8. Call this new rule 'Inbox Rule' in the name box, and click the 'Save rule' button.
9. Make sure this rule always stays at the top of the rule list. Highlight it and use the 'Move up' or 'Move down' buttons as necessary to make sure it is always at the top.

The steps above effectively force every new email that arrives in any of the inboxes for your various email accounts to be automatically moved to the single Inbox folder under 'Storage Folders'. This means you can leave all of your individual email account categories collapsed, taking up minimal space, while the 'Storage Folders' category can be left expanded to show your new emails arriving in the Inbox. If you right-click on the 'Storage Folders' heading, you can also choose to move it up or down the list of categories in the Folder Pane.

The key benefit of this step is a reduction in clutter, and also the ability to move these inbox emails to as many individual custom folders as you wish, all of which are stored under a single 'Storage Folders' category. None of this is possible with Quick Views.

STEP 4 - CUSTOMIZE MENUS AND TOOLBARS

Windows Live Mail utilizes the Ribbon interface. This interface is quite intuitive once you get used to it, but the buttons and menus displayed on the main ribbon can't be altered. However you can still customize/streamline the interface if you wish. The simplest form of streamlining is to double-click on one of the main menu headings, such as Home or Folders, or click the small white arrow at the far right of the menu bar. This will collapse the entire ribbon to only show the menu headings. You can then access each of the menu sub-options by clicking once on its heading, and the full ribbon will open temporarily to allow access to them. Double-click on a heading to restore the ribbon permanently. You can do this to every ribbon menu shown in Windows Live Mail, including the ones shown at the top of individual emails.

There is a smaller Quick Access toolbar that is also available, and which can be displayed just above or just below the ribbon. Click the small black down arrow next to it to see a range of commands which you can enable/disable on the quick access toolbar. You can also right-click on any option in the ribbon and select 'Add to Quick Access toolbar'. Right-click on any existing quick access toolbar item, and you can select 'Remove from Quick Access toolbar' to remove it.

By placing your commonly used commands on the quick access toolbar, and collapsing the large ribbon, you can streamline Windows Live Mail's appearance quite a bit without affecting its key functionality.

Finally, to alter the amount of detail displayed for emails in the main window, first select a folder in the Folder Pane which contains one or more emails, then go to the View menu. Here you can choose to disable the Calendar Pane which is shown at the far right by clicking the 'Calendar Pane' button to unselect it. You can also disable the Reading Pane shown to the right of the email listing by clicking the 'Reading Pane' button, and selecting Off. You can then select which columns to show for the email list by right-clicking on any of the column headers and selecting Columns. Finally, you can resize each column by hovering your mouse over the area between each column header, and then dragging it left or right.

STEP 5 - ADD COLOR

As a final touch, you can change the color used for the name of each of your email accounts in the Folder Pane. Highlight the relevant account name in the Folder Pane, then go to the View menu and click the 'Account color' option and select the color you desire. This will only apply the selected color to the account name heading, not to its sub-folders.

If you undertake all of the changes suggested thus far, you will see that Windows Live Mail can be made to look relatively clean and uncluttered, with a more compact interface that still presents you with all of the major pieces of information, and one which is more in line with older Windows email clients. Of course these changes are entirely subjective, and it is up to you as to what you customize.

Some final things to note:

§ Windows Live Mail opens up on the folder last open when it was closed; it does not automatically go to your Inbox when opened. You may wish to get into the habit of closing Windows Live Mail with your Inbox open.
§ When sending and receiving emails, Windows Live Mail does not automatically show the detailed progress indicator available in previous mail versions. All you can see are the notifications given in the status bar, if the status bar is visible. To see a detailed progress indicator, you must double-click on the Send/Receive button.
§ By default Windows Live Mail also updates your Calendar, RSS Feeds and any Newsgroups each time it syncs. I recommend that you go through these features one by one and remove unnecessary accounts or entries to prevent Windows Live Mail updating any features that you don't use. To do this, click the Calendar, Contacts, Feeds and Newsgroup icons at the bottom of the Folder Pane. In particular, untick the Primary Calendar if not using it (it can't be deleted); under the RSS Feeds, expand the 'Your Feeds' category and delete any or all of the 'Microsoft Feeds' folders, subfolders or individual feeds that you don't want; finally, click the File button at the top left of the Mail window, select Options and then 'Email accounts', and in the Accounts window highlight and click the Remove button to delete every type of account you don't need.

Bear in mind that Windows Live Mail will continue to change over time as Microsoft periodically releases new versions of Windows Essentials products. As such, some or all of the instructions above may become redundant in the future if you update to the latest version.

The next section looks at the actual settings which control Windows Live Mail's core functionality.

< BASIC SETTINGS

In this section we examine all of Windows Live Mail's main settings. These are very similar to those contained in Windows Mail under Windows Vista, because Windows Mail and Windows Live Mail share similar underpinnings. To configure Windows Live Mail, click the File button at the top left of the Mail window and select Options, then select Mail. Each tab under the Options window is covered below, with descriptions and recommendations for the most significant options provided:

GENERAL

Notify me if there are any new newsgroups: If ticked, Windows will prompt you when new newsgroups are discovered. If you do not use newsgroups, or don't wish to be notified, untick this box.

Automatically log on to Windows Live Messenger: If ticked, this option allows Windows Messenger to automatically open when Windows Live Mail is started. If you don't wish this to occur, or don't use Windows Messenger, untick this option.

Help us improve Windows Live programs...: Allows Microsoft to collect information on your usage of Windows Live Mail as part of the Customer Experience Improvement Program. Whether you participate in this or not is up to you, but it is not necessary.

Play sound when new messages arrive: Whenever new email is received, Windows will play a short sound. If you don't like this occurring, untick this box. If you want to change the sound, go to the Sound component of the Windows Control Panel, and under the Sounds tab, scroll down to the 'New Mail Notification' item and select a new sound in the drop down box at the bottom of the window and click Apply. See the Sound section of the Graphics & Sound chapter for more details.

Send and receive messages at startup: If ticked, forces Windows Live Mail to send and receive messages (Sync) each time it is opened. This is generally desirable, as it allows you to see new messages more quickly when you launch Windows Live Mail.

Check for new messages every X minutes: If this option is ticked, as long as Windows Live Mail is open, it will automatically check all of your email accounts for new messages at the set interval which you specify in minutes here.

If you wish to exclude any account from being automatically checked via either of the two options above, or whenever you click the Send/Receive button, go to the Options menu, select 'Email accounts', select the relevant account and click the Properties button, then under the General tab untick the 'Include this account when receiving mail or synchronizing' box.

Default Messaging Programs: This area tells you if Windows Live Mail is your default mail or newsgroups handler. Click the 'Make Default' button to make Windows Live Mail the default handler. Note even if you set Windows Live Mail as your default email handler, you may still be prompted by Windows as to whether to use the Metro Mail app or Windows Live Mail when you click an email link. To properly set Windows Live Mail as your default email handler, or if you want to set another application to handle your mail, see the Default Programs section of the Windows Control Panel chapter for details.

READ

Mark messages read after displaying for X seconds: If ticked, whenever an email is highlighted in the Reading Pane, it will be marked as read within the time determined by this setting. If an email is opened normally this setting has no impact; it is automatically marked as read as soon as you open it. You can manually mark any read email as unread again at any time by right-clicking on it and selecting 'Mark as unread'.

Automatically expand grouped messages: If you have the Conversations option enabled under the View menu, emails will be organized into conversation threads, with the original email as the thread category and all subsequent emails listed underneath. If this option is ticked, all such conversation threads will automatically be expanded to show every email underneath the thread, otherwise you will have to manually expand each thread by clicking the small arrow next to it.

Automatically download message when viewing in the Preview Pane: If ticked, Windows Live Mail will automatically download and show the entire contents of the currently selected email in the Reading Pane. If the Reading Pane is disabled, this option is irrelevant.

Read all messages in plain text: If ticked, all emails will be opened in plain text format regardless of their original format. This will prevent font formatting and images from appearing in any email. If unticked, emails will appear in the format in which they were originally sent. Note that you can further adjust whether the images in HTML formatted emails are shown as covered under the Safety Options section later in this chapter.

Get X headers at a time: If ticked, determines how many headers to download from an open newsgroup at any time. If you don't use newsgroups then this setting is irrelevant and can be unticked.

Mark all messages read when exiting a newsgroup: If ticked, marks all messages as read in a newsgroup when you exit that newsgroup. If you don't use newsgroups then this setting is irrelevant and can be unticked.

Fonts: The options here allow you to change the fonts used to display email content by default. You can increase the standard font size from Medium to Large for example, and all emails you open will automatically display in a larger sized font.

RECEIPTS

Requesting read receipts: Read receipts tell the sender of a message if and when their message has been opened by the recipient. If you want to use them for all emails you send, tick the 'Request a read receipt for all sent messages' box, however keep in mind that most people find them annoying, as each time such an email is opened by the recipient, an automated email is sent back to you from the recipient simply stating that the email was opened, or the reader is prompted to send such an email, depending on their settings.

Returning Read Receipts: For the reasons covered above, I recommend selecting 'Notify me for each read receipt request'. That way you know when someone has sent an email to you with a receipt request, and you can choose whether to accept or deny the request to send a receipt when you open the email - you may not wish them to know if or when you have read that email. If you frequently get emails with read receipts, you may want to tick one of the two other options here instead, as otherwise you will face a large number of prompts as you go through your emails.

Secure Receipts: Secure receipts are useful if you are sending a very important message, and you want to make sure that the message arrived at the other end unaltered. Otherwise the same recommendations as those for Read Receipts above apply here when you click the 'Secure Receipts' button.

SEND

Save copy of sent messages in the Sent Items folder: If ticked, a copy of every email you send will be stored in your 'Sent Items' folder. Ticking this option is up to each individual, but it can greatly increase the storage space required for Windows Live Mail on your PC. A better option is to click the 'Show Cc & Bcc' link at the right of the subject line when composing a new message or reply, and put your own email address in the Bcc box. Do this for any important sent emails that you want to keep a copy of, and a blind copy of the email will also be sent to your email address for your records.

Send messages immediately: If ticked, emails you send will be sent out immediately after you click the Send button on the email. If unticked, the email will sit in your Outbox after you click Send, and will only be sent when Synchronization of your account is initiated.

Automatically put people I reply to in my address book after the third reply: If ticked, after your third reply to a particular email address, that address will be saved as a Contact. I recommend unticking this option for potential security reasons, as covered under the Important Security Tips section of the Security chapter.

Include message in reply: If ticked, when you reply to an email, the original message will also be shown in the email, usually at the bottom. This is part of normally accepted email etiquette, as it allows the recipient to see and recall exactly what they originally said to you.

Reply to messages using the format in which they were sent: If ticked, the format of your email reply will be determined by the format of the email you receive. If the email you receive is in plain text with no formatting

or pictures, your reply will automatically be in plain text as well. Similarly, HTML formatted email will initiate an HTML formatted reply from you. Generally speaking it is good etiquette to reply to people in the same format they used to send a message to you, particularly if they send you a plain text message.

COMPOSE

Here you can customize the appearance of your emails, by changing the font format and background stationery used. However, these effect of these settings will only be visible to readers of the email if they are viewing the email in HTML format, and don't have the 'Read all messages in plain text' setting enabled as covered further above. You can also adjust the format of messages you post in newsgroups by changing the News-related entries.

Convert special key strokes to emoticons: If ticked, this option automatically converts certain key combinations commonly used to denote emotions, such as :) (smiley face) or ;) (wink) into a graphical emoticons. Keep in mind that graphical emoticons may be removed if the recipient views the email in plain text, or if using another email client.

Convert messages to photo emails when adding photos: If ticked, this option converts a standard email into a special Photo Email format when attaching photos. This format uploads the photos to the SkyDrive cloud service, which may have privacy implications. It is typically safer not to use this option.

SIGNATURES

A signature is the text appended to the bottom of each email you send out. If you tick the 'Add signatures to all outgoing messages' option, you can automatically insert a signature to all sent emails. If the 'Don't add signatures to Replies and Forwards' box is also ticked, then a new signature will not be appended when you reply to or forward an existing email. To create a signature, click the New button, and in the box at the bottom of the window, enter your signature text, and if necessary, click the Advanced button to associate that signature with a particular email account.

SPELLING

Always check spelling before sending: If ticked, when you click the Send button on an email, Windows Live Mail will first pause and prompt you to correct all the potential spelling mistakes it has found in the email. Once you have completed this process, the email will be sent out as normal.

Automatically correct common capitalizations and spelling mistakes: If ticked, Windows Live Mail will attempt to automatically fix common mistakes, such as capitalizing the first two letters of a word, or misspelling common words.

Check my spelling as I type: If ticked, any potential spelling mistakes in your email will be highlighted with a wavy red underline while you type. You can right-click on red underlined words to see the suggested alternate spelling, and select from a list to correct the word.

Check spelling in current input language: If ticked, this setting allows Windows Live Mail to automatically change the input language it uses for spell checking to match your Windows input language, which is useful if you often change the Windows input language.

When checking spelling, always ignore: The three options here allow you to let Windows Live Mail know that it shouldn't check the spelling of words written in all uppercase letters; words that contains numbers in them; and the original text to which you are replying or forwarding. All three should be ticked.

Custom dictionary: Click the Edit button and you can add or remove any custom words from the dictionary used for spell checking. You can also add any word to the custom dictionary from within an email at any time by right-clicking on the wavy red underline and selecting 'Add to dictionary'.

Languages: Lets you install or change the current input languages available in Windows Live Mail, as well as setting which default language is used.

CONNECTION

When you click the Change button it will open the Internet Explorer Connections tab, as covered in the Internet Explorer chapter. The 'Sign in' button at the bottom of the window is related to signing in with a Windows Live ID, and as discussed at the beginning of this chapter, is only necessary if you wish to synchronize any other Windows Live services with Windows Live Mail.

ADVANCED

Use the 'Deleted Items' folder for IMAP accounts: If this option is ticked, when using an IMAP-based email account, if you delete a message it also removes the message from your message list at the same time. Most email accounts use the POP protocol, however if you know you are using IMAP then decide whether you want this option ticked or not.

Mark Message Threads I start as Watched: If the 'View by conversation' option under the Views menu is enabled, and if this option is ticked, any message threads which you start will automatically be marked as watched and hence be in a different color.

Reply on the bottom of a message: If ticked, when you reply to a message, your reply will begin at the bottom of the original message text, as opposed to the default and generally accepted method of the top.

Signature on the bottom of a message: If ticked this option automatically inserts the default signature you have created under the Signature tab at the very bottom of every email, beneath any original text you may be replying to or forwarding. This can create some confusion, as the signature may appear to be part of the original message to which you are replying, or may simply be overlooked.

When you click the Maintenance button you will see additional options. The most significant of these are:

Empty messages from the 'Deleted Items' folder on exit: If ticked, all messages in the Deleted Items folders will be permanently deleted when you close Windows Live Mail. This is generally recommended as it reduces storage space used by removing unwanted emails.

Purge deleted messages when leaving IMAP folders: This option is similar to the option above, but only affects IMAP-based email accounts.

Purge newsgroup messages in the background: If ticked, you can select how often to clear stored newsgroup messages. If you don't use newsgroups then these settings are irrelevant and can be unticked.

Compact the database on shutdown every: If ticked, this option reduces unnecessary storage space by compacting the mail database every X shutdowns of Windows Live Mail. The entire process usually adds only a few seconds to the shutdown time of Windows Live Mail, and only after the specified number of times you shutdown Windows Live Mail. At all other times, Windows Live Mail will shutdown normally.

Clean Up Now: Clicking this button takes you to a new window which lets you either Remove Messages for locally stored newsgroup message bodies, or Delete all locally stored newsgroup messages. The Reset button

does the same as Delete, but will re-download all messages when you reconnect to the newsgroup. These options have no impact on regular email, they are only related to newsgroups.

Store Folder: Clicking this button shows you where your emails are stored on your drive. By default it is under the *\Users\[username]\AppData\Local/Microsoft\Windows Live Mail* directory, however you can change the location if you wish. If you're after a method of exporting or backing up your messages instead of just moving the stored location of them, see later in this chapter for details.

Troubleshooting: This section allows a range of logs to be kept in case of any problems. If troubleshooting a mail-related problem, to begin with you should tick all the available log types, and they will be saved under your main Windows Live Mail store folder location - see above.

Once you've changed all the settings you wish to change in the Mail Options, click the Apply button and then click OK. You may need to close and reopen Windows Live Mail for some of the settings to come into effect.

< SAFETY OPTIONS

Security is an important consideration in Windows Mail, since a great many malware and phishing attacks are initiated via email. As such, you can access a separate range of security-related settings by clicking the File button at the top left and selecting Options, then selecting 'Safety Options'. These are described below:

OPTIONS

Choose the level of junk email protection you want: This option determines the way in which the automatic junk email filter works. Junk email is unsolicited email that is annoying or malicious. The Low option provides basic protection against the most obvious junk email, but can let others through. The High option provides more aggressive protection against junk email, but legitimate emails may also get caught up in the filtering. 'Safe List Only' only allows emails through from senders who are on your Safe Senders list - see below. With 'No Automatic Filtering', no emails will be blocked as junk emails, unless the sender is on the Blocked Senders list - see below. On balance I recommend the Low option for most people, as it has the least risk of diverting legitimate emails to your Junk Emails folder, while still catching the bulk of obvious junk emails. If you are absolutely certain that you do not want to receive emails from anyone other than people you know, then select the Safe Senders list option and make sure to add all of your friends and contacts to the Safe Senders list. Regardless of which option you choose, regularly check the Junk Email folders to ensure that no legitimate emails are being trapped there.

You can also flag individual emails as junk email, or unblock/unmark legitimate mail, by right-clicking on a message and selecting the 'Junk email' item, then choosing the appropriate option.

Note that Windows Live Mail applies the Junk Email filter to your emails before any custom rules can be implemented. This means that if an email is flagged as junk email, it will be moved to the junk mail folder (or deleted) before any of your message rules have a chance of being applied to it. Keep this in mind when creating custom rules.

Permanently delete suspected junk email instead of moving it to the Junk Email folder: If this box is ticked, suspected junk emails will be deleted instead of being moved to the Junk Email folder. I strongly recommend against this option, as there is the very real possibility that some legitimate emails sent to you will be flagged as junk emails and subsequently deleted before you see them. By allowing them to be diverted to the Junk Emails folder first, you at least have a chance to routinely inspect and determine whether any such emails are being caught this way, and perhaps adjust your junk email protection settings accordingly.

Report junk email to Microsoft and its partners: If ticked, allows Microsoft and its partners to gain insight into the types of junk email users are receiving and hence release regular updates to the junk email filter which better filter out junk mail while leaving legitimate email untouched. Such updates are usually released on a monthly basis via Windows Update.

SAFE SENDERS

This section allows you to enter the addresses of individuals from whom all emails will be considered legitimate, regardless of your junk email settings. This helps prevent important emails from accidentally being tagged as junk email, and potentially deleted before you see or read them. It is wise to add the addresses of people whom you trust to this list. You can add individual email addresses (e.g. *user1@tweakguides.com*) or entire domains (e.g. *tweakguides.com*) as necessary.

Also trust email from my Contacts: If ticked, any people listed in your Contacts are automatically part of the Safe Senders list, and hence their emails to you won't be flagged as junk.

Automatically add people I email to the Safe Senders list: If ticked, any address you send emails to will automatically be added to the Safe Senders list. This is recommended as it helps prevent reply emails from people you have emailed from being caught in the Junk Email folder.

BLOCKED SENDERS

This section works in the exact opposite way to the Safe Senders list. Any emails from the addresses or domains added here are automatically flagged as junk email, regardless of your junk email settings. Only add addresses here from people whose emails you do not wish to read, and more importantly, remember that spammers who send out junk emails usually do not use legitimate email accounts, or use disposable accounts. Blocking addresses in this manner will not have a discernible impact on spam in the long run, so this option is primarily for blocking annoying emails from regular individuals, not professional spammers.

The two options below only have an impact if you click the 'Delete and Block' button which appears in some emails:

Bounce the blocked message back to the sender: If ticked, this option sends the email back to the sender with message indicating that the email was undeliverable. This is not particularly effective for the reasons noted above, and is not recommended, as it simply uses more resources on your mail server to send back the email to what is most likely the wrong email address anyway. I strongly recommend unticking this option, unless you want a particular individual to know that you are blocking their emails.

If the email is a newsletter, Unsubscribe me from the mailing list: If ticked, this option attempts to unsubscribe you from a newsletter you have received. Similar to the options above, in practice this is not a particularly useful feature. Most unsolicited newsletters will continue being sent regardless of any unsubscribe messages sent back. Indeed, sending back an unsubscribe message may actually result in you receiving more spam, as the spammers have now verified that your email address is not a dead account.

INTERNATIONAL

One of the ways in which you can block spam and malware emails is to block entire country domains which are known to send out large amounts of spam. For example, the Russian Federation (.RU) and People's Republic of China (.CN) are known sources of a great many spam and malicious emails. If you are absolutely certain that you are not going to receive any legitimate emails from particular countries, you can click the 'Blocked Top Level Domain List' button and tick all of the country extensions that you wish to have blocked. However, as noted earlier, many spammers do not use legitimate email accounts, or can use hijacked accounts which are from a range of countries, so this method may not necessarily be effective against spam. The method below has a much greater chance of success.

If you click the 'Blocked Encoding List' button, you can block certain types of character sets known to be used in spam emails. This is a more effective anti-spam and anti-malware method, because many unsolicited emails have Russian or Chinese characters, and in most western countries, people would not be receiving legitimate emails containing such character sets. So you can tick virtually all of the boxes here except 'Western European' for example, and rid yourself of a large proportion of generic spam.

Make sure that you check your Junk Email folder regularly to see what types of emails are being caught because of these two rules, and adjust them if you find legitimate emails being trapped.

PHISHING

Protect my inbox from messages with potential Phishing links: If ticked, this option allows Windows Live Mail to block the contents of, and highlight, particular emails that it considers to have phishing links and content. You should enable this setting as an added layer of protection, particularly if you are less familiar with the appearance of phishing emails. But just because an email gets through this filter, doesn't mean that it is safe to click the links in it; conversely, just because an email is flagged as suspicious, doesn't necessarily mean that it is a phishing email. See the Security chapter for more details on phishing, and how to detect it.

Move Phishing email to the Junk Email folder: If ticked, any emails detected as having phishing content are automatically moved to the Junk Email folder. This option should be safe to enable. As always, regularly check your Junk Email folder and do not delete its contents before making sure that no legitimate emails have been caught up in there.

SECURITY

Virus Protection: Here you can select either the 'Internet zone' or 'Restricted sites zone' for your default email behavior. When in 'Internet zone' mode, HTML-based emails with active content will display their content just like a web page in Internet Explorer. In fact the security settings you choose for the Internet zone under the Security tab in Internet Explorer' Internet Options also apply here. When in 'Restricted sites zone' mode on the other hand, Windows Live Mail will disable active content from HTML-based emails, which is much more secure, but may reduce email functionality for HTML formatted emails. I recommend running in 'Restricted sites zone' mode, as many HTML-based emails are spam or malicious, and most active content is either annoying or malicious. For the most part legitimate emails usually come with plain text or regular HTML formatting, so this should have little visible impact on everyday email usage for most people.

Warn me when other applications try to send email as me: Ticking this option provides a warning when an application initiates an email with your email address as the sender. This helps prevent any unauthorized emails going out under your name, though this setting does not stop malware or hackers who send out emails from your account, as that works differently.

Do not allow attachments to be saved or opened that could potentially be a virus: This option will attempt to protect you from malware in email attachments. When this option is enabled, Windows Live Mail's Attachment Manager will analyze the attachment and the email it is part of to determine whether the attachment is likely to contain malware. By default if this option is ticked you will not be able to download email attachments which are flagged as malware. However just because an attachment is not blocked, doesn't mean that it is safe to open. If an attachment you trust is blocked, untick this option temporarily, view the email again, save the attachment, then retick this option. Regardless of whether you trust the sender of an email or not, I strongly recommend scanning any attachments you receive just in case the person sending it to you is unknowingly infected with malware themselves. See the Security chapter for details. To adjust the Attachment Manager's behavior, see the Handling of Attachments tip in the Group Policy chapter.

Block images and other external content in HTML email: If ticked, this option blocks certain images and content in HTML email which may be exploited by malware. I recommend ticking this option, as generally speaking most legitimate emails do not contain any significant images within them, and if they do, you can choose to allow the image on a case by case basis by clicking the relevant button presented within the email.

Show images and external content sent from email addresses in my Safe Senders list: If ticked, this option will display images in HTML formatted emails from any email addresses which are in your Safe Senders list. Ticking this option should be fine, as long as you only add trusted individuals to your Safe Senders list.

Secure Mail: The options in this section relate to digital identification, which ensures that all emails sent from your account are encrypted such that they can be verified to be from you. Similarly, when you receive a digitally signed message, you can be quite certain it is from the person it is supposed to be. These features require that you be issued with a valid Digital ID - click the 'Get Digital ID' button to find out more. Most people do not use Digital IDs, and cannot obtain one easily, hence they will have problems responding to your emails if they are digitally signed and encrypted.

Once you've changed all the settings you wish to change here, click the Apply button and then click OK. You may need to close and reopen Windows Live Mail for some of the settings to come into effect.

< WINDOWS CONTACTS

Windows Contacts is the replacement for the Address Book in Windows XP. This feature is not just restricted to Windows Live Mail, you can access your stored Contacts at any time by going to the Start Screen, typing *contacts* and pressing Enter. You can access a more detailed Windows Live Contacts manager interface by clicking the Contacts icon at the bottom of the Folder Pane in Windows Live Mail. Contacts are .XML files that can store the names, addresses, personal details and photo of an individual. To add a contact to your list, you can do so in four main ways:

- If you ticked the 'Automatically put people I reply to in my address book after the third reply' option under the Send section of Windows Live Mail options, then the third time you reply to an email from someone, they will automatically be added to your Contacts.
- You can right-click on any email address in any email message and select 'Add to contacts'; you can click the 'Add to contacts' link which appears in the email header; or alternatively you can just right-click on an email message and select 'Add sender to contacts'
- You can click the 'New Contact' button in Contacts to create a new contact.
- You can click the Import button in Contacts to import an existing file with contact details, such as your Outlook Express Windows Address Book.

In any case, once a Contact is added to the list, they are stored under your *\Users\[username]\Contacts* directory, and you can view and edit their details by double-clicking on their Contact item. This allows you to enter a range of personal and/or professional details as necessary. You can even add photos of these people to be the default display picture for each Contact, making them easier to identify. You can export Contacts to any application which supports the .CONTACT file format.

While this is a handy utility, particularly for corporate users on a network, for the average home PC user I consider it a risk to hold detailed information about yourself or other people in this form. To start with, if your PC becomes infected with malware, it may attempt to use the Contacts list to automatically send itself out to everyone you know, proliferating the malware and causing you embarrassment. Worse, if someone compromises your user account, they will be able to see the personal details of not only you, but all of your friends and acquaintances as well, and this can be very useful in successfully undertaking identity theft.

Instead I recommend keeping at least one email from all the people you wish to regularly contact under a custom storage folder in Windows Live Mail. That way if you want to contact someone, you can simply use

the search function in Windows Live Mail to find their email, and hence their contact details. Malware cannot use these stored emails to send itself out, and if someone compromises your machine it will take them much greater effort to work out all the personal details and the relationship between you and the senders of these stored emails.

< MAIL RULES

An important feature of Windows Live Mail is the ability to apply a range of rules to incoming or existing emails, filtering them to suit your needs. Note that these mail rules only apply to POP email accounts, not IMAP or web-based HTTP email accounts.

To configure mail filtering, go to the Folders menu in Windows Live Mail and click the 'Message rules' button. In the window that opens, do the following:

1. Click the New button.
2. Select a condition in the first pane, e.g. 'Where the message has an attachment'.
3. Select an action to apply to this type of message in the second pane, e.g. 'Do not download it from the server'.
4. If your condition or action requires further parameters, such as a word or phrase, or a particular folder, click the blue underlined link in the description box at the bottom and set the parameter.
5. Enter a descriptive name for the rule, e.g. 'Attachment blocker'.
6. Click the 'Save rule' button.

Repeat the steps above as many times as you like, since the rules are cascading. That means once the first rule in the list has completed its actions, the second rule in the list will then apply, and so forth. This allows you to create complex rule combinations which can sift through your mail. You should use the 'Move up' and 'Move down' buttons to rearrange your rules accordingly, as the rule order is important. If you click the 'Apply now' button, your rules will be applied to all folders, not just your Inbox, so be aware that any saved emails you have will get caught in the filtering. If you wish to temporarily disable a rule, untick the box next to and it will no longer be applied.

Importantly, be aware that Windows Live Mail will apply its junk email filtering - covered under the Safety Options section earlier in this chapter - before any custom mail rules are applied.

< BACKING UP

This section contains important details on how to backup your stored emails and email accounts, which I recommend doing on a regular basis.

BACKING UP EMAILS

If you want to back up the emails you've saved in Windows Live Mail, follow these procedures:

1. Click the File button at the top left and select 'Export email', then select 'Email messages'.
2. Select the format for the emails to be saved in. Microsoft Windows Live Mail is recommended. Click Next.
3. Click Browse and specify the folder location to export these emails. The folder must be empty, so if necessary create an empty folder in File Explorer before proceeding, select it here, and click Next.
4. Choose the specific email folder(s) you wish to export. Select All Folders if in doubt. Click Next.
5. Your messages will be saved to your specified location as a series of folders that contain all of the individual email messages as .EML files.
6. I recommend using an archival utility such as WinZip, WinRAR or 7-Zip to store these folders in a single archived file for easier handling.

To restore these emails in Windows Live Mail at any point, click the File button at the top left and select 'Import messages', then select 'Windows Live Mail' and follow the prompts.

BACKING UP ACCOUNTS

To back up your individual email accounts, follow these steps:

1. Click the File button at the top left and select 'Export email', then select Account.
2. Highlight the account you wish to export and click the Export button.
3. Choose a location for the .IAF file and click Save.
4. The account and all of its relevant details will be saved with your account email address as the filename. Store this file safely as it is a security risk to allow anyone else to access it.

To restore an email account, click the File button at the top left, select Options then 'Email accounts', click the Import button, navigate to the .IAF file, select it and click OK.

< OTHER EMAIL CLIENTS

Windows Live Mail should be more than adequate for the average PC user. It does require some customization to make it more familiar for Windows Mail or Outlook Express users, however after some initial tweaks to the interface, it performs in much the same way as previous Windows email clients. If you have any problems, see the Windows Essentials Mail Support.

If you're not satisfied with Windows Live Mail for any reason, there are a range of viable alternatives. The most comprehensive of these is Microsoft Outlook, which is included with the Microsoft Office Suite. It provides the greatest range of features to cover virtually any need, but is not free.

If you want a free email client, you can try Mozilla Thunderbird. For a range of other options see this Wikipedia Article which lists and compares a range of email clients, providing feature details and relevant download links. Or you can simply skip a local email client, and instead use an online web client, such as Yahoo, Hotmail or GMail. These not only provide free email accounts and comprehensive web-based interfaces, they also provide plenty of storage space. Obviously they cannot be accessed in offline mode, and I don't recommend relying solely on an online mail client, because if your email account is hijacked for example, you can permanently lose access to both your account and any stored emails.

WINDOWS MEDIA PLAYER

Windows 8 has two Metro apps that control the playback of media by default: the Video and Music apps. While their usage is fairly intuitive, they are very basic programs with limited capabilities. For full-featured multimedia functionality, you can use the built-in Windows Media Player (WMP). This is a Desktop utility that has many useful features, but is often mistakenly dismissed as being bloated. If configured correctly, WMP provides excellent audio and video quality, and all of the functionality that the average user requires for playing movies and music.

Windows 8 continues the usage of Windows Media Player 12, introduced in Windows 7. This version of WMP has been redesigned compared to earlier versions. As part of the integration of Libraries into Windows, WMP 12 has the Library view as its primary media management area. The alternate view is the 'Now Playing' view, which has a minimalist appearance. WMP 12 also adds built-in support for some of the most popular media formats currently in use, including DivX, Xvid, H.264 and AAC. In most other respects, the core functionality of Windows Media Player is much the same as before.

This chapter contains configuration advice and details on all of WMP's features. If you don't like Windows Media Player, alternative free media players are covered at the end of this chapter, as well as a discussion of a range of general media-related issues relevant to all media players in Windows, including DVD and Blu-ray disc playback, Codecs and DRM. Note that Windows Media Center is not included in Windows 8 by default, and is not covered in this book. It can be downloaded as an add-on as covered under the Add Features to Windows 8 section of the Windows Control Panel chapter.

< INITIAL SETTINGS

To access Windows Media Player, go to the Start Screen, type *wmp* and press Enter.

The first time you launch Windows Media Player, you will be prompted to configure a range of settings. I recommend that you select 'Custom settings' in the first prompt shown, then take into consideration the following information regarding each page that follows:

Privacy Options: These settings are covered in detail under the Privacy section later in this chapter. If you are concerned about privacy you can untick them all now, and consider whether to re-enable any of them later after you read the rest of this chapter.

Select the Default Music and Video Player: Here you can select whether to automatically allow Windows Media Player to become the default player for all non-proprietary types of music and video files on your system, or to select the second option, which allows you to specify the file types associated with Windows Media Player. At this stage the first option is recommended. You can change whether WMP is your default player, and its file associations, at any time in the future, as covered under the Default Programs section of the Windows Control Panel chapter.

All of the above settings can be configured properly within Windows Media Player at any point, so don't be overly concerned about what you choose for the initial settings.

< VIEWS

There are two main views possible in Windows Media Player: Library view and Now Playing view. Library view is used primarily for multimedia sorting and selection within WMP, while Now Playing is the main playback view. To switch between the two views, in Library view click the button at the lower right corner to switch to Now Playing view, and in Now Playing view click the similar button shown at the top right corner, or click the 'Go to Library' link in the middle of the screen. These views, and a range of related features, are covered in more detail below.

LIBRARY VIEW

Explorer-Based Interface: The Library view is very similar to the standard File Explorer interface in most respects. There is a Navigation Pane to the left, which has various categories of media, all of which are linked to your default media-related Libraries in Windows; there is a Details Pane in the middle which displays files in the currently highlighted folder/category; and there is an Address Bar-like section at the top, containing back and forward arrows and your current location within the Library structure. You can also access a Menu Bar by pressing the ALT key, or right-clicking on an empty area in the Address Bar.

Media files in the Details Pane can be displayed in Icons, Tiles or Details view. You can alter the view in most cases by clicking the Views button immediately to the left of the Search Box. In some categories, certain views are unavailable - for example, if you click the main Music category in the Navigation Pane, you can't switch to Icon View. You can customize the columns shown in the Details Pane by clicking the Organize button, selecting Layout then clicking 'Choose columns'. Similarly, you can choose which items to display in the Navigation Pane by right-clicking on one of the items in the Navigation Pane and selecting 'Customize Navigation Pane', then unselecting undesirable items. You can sort by any column simply by clicking its header, and you can search for any file using the Search Box.

Managing Libraries: By default, WMP includes all of your main media-related Libraries in the Navigation Pane: Music, Videos and Pictures. If you add or remove any files in these Libraries, Windows Media Player will automatically update the information stored in its Library view, which is one of the many benefits of Library integration. See the Libraries section of the File Explorer chapter for more details.

While you can manage a Library within File Explorer, you can also manage it here by clicking the Organize button, selecting 'Manage Libraries', then selecting the relevant Library to manage. You can then choose whether to add or remove any folders from this Library, but importantly, this change affects the Library for all purposes, not just within WMP.

To remove a file from the WMP Library, right-click on that file in WMP's Details Pane and select Delete - you will be prompted as to whether you wish to 'Delete from library only', which removes that file from the WMP-specific Library but doesn't remove it from your normal Library nor from your drive; or you can select 'Delete from library and my computer', which deletes the file permanently from the Library and from your drive.

If you wish to re-add a file to your WMP-specific Library, or rebuild the WMP-specific Libraries, go to the Tools menu and select Advanced. Here you can choose whether to 'Restore media Library', which rebuilds your entire WMP-specific Library based on the current contents of your media-related Libraries in Windows. This will restore any deleted items, however if you simply wish to restore a few deleted files to the WMP-specific Library listing without rebuilding the full list, select the 'Restore deleted library items' option instead, which only adds files that exist in your Windows media-related Libraries, but which are not present in the WMP-specific listing of these Libraries.

If you wish to control whether any media files you play are automatically added to the relevant Library, see the 'Add local media files to library when played' and 'Add remove media files to library when played' options under the Basic Settings section below.

Playlists: The Library categories allow you to access any files stored in your relevant Libraries, and you can also sort the view using preset categories such as Artist, Album and Genre. Whenever you play back a file in one of the categories, when it reaches the end, the next file in the list automatically starts playing, depending on how you've sorted the current category. In most cases you will want to arrange your files in groups corresponding to your moods, or certain genres, or even by period. To do this, you can create a Playlist.

To create a new Playlist, click the 'Create Playlist' button and give the Playlist an appropriate name - it will now be displayed under the Playlists category in the Navigation Pane. You can now add media to the Playlist by dragging it from a Library category and dropping it on the list. These Playlists are static, and their content will not change to reflect changes to your Libraries or the files on your drive.

A much quicker way to create a Playlist is to use the Auto Playlist feature. Click the small arrow to the right of the 'Create playlist' button, and select 'Create auto playlist'. A new window will open, allowing you to enter a title for this Playlist, then create a set of filters which will allow Windows to go through your Libraries and automatically add all relevant media to the list. For example, click the first green plus symbol, and select 'Album Artist', then click the 'Contains' and 'Click to set' links which appear to determine precisely what text to use for finding music by the relevant artist(s). You can then click the next green plus symbol to determine which Libraries to search, and then click the final green plus symbol to set the applicable restrictions to the Playlist, to prevent it becoming too large for example. An Auto Playlist is dynamic, and automatically updates itself depending on changes to your Libraries, so for example if you add or remove a file in your Library, it will also be reflected in the relevant Auto Playlist based on the filter conditions.

Any Playlist created is saved as a .WPL file under the *\Users\[username]\Music* folder, and also added to your Windows Music Library by default. To delete a Playlist permanently you need to right-click on it and select 'Delete from library and my computer' - this will not delete the media files within a Playlist.

List Pane: To make it more convenient to create a Playlist, you can enable the List Pane. To do this, click the Organize button, select Layout then select the 'Show list' options; you can also close the List Pane by doing the same thing. With the List Pane open, you can now drag and drop items from the Details Pane into the List Pane to create a new Playlist, and then save this list by clicking the 'Save list' button at the top of the List Pane, entering a name for the Playlist, and pressing Enter.

You can also select different types of lists in the List Pane by clicking the Play, Burn or Sync buttons. The Play button is for Playlists, as covered further above. The Burn button allows you to create a list for burning to a CD or DVD, simply by dragging the relevant media files into the Burn List, then clicking the 'Start Burn' button when ready to commence burning. The Sync button allows you to create a list of media files for syncing with a connected device which supports the uploading of such media, such as a portable music player, and then clicking the 'Start Sync' button to commence syncing of files to the device.

NOW PLAYING VIEW

The Now Playing view is the default view used when playing back a video or image file in Windows Media Player. You can also switch to Now Playing view when listening to audio by clicking the 'Switch to Now Playing' button at the bottom right of Library view. Now Playing view has a relatively simple layout, with the media information shown at the top left of WMP, a 'Switch to Library' button at the top right, and a set of player controls at the bottom. Depending on the size of the WMP window, you may also see a 'View full screen' button at the bottom right. The center of the view displays the video or image chosen for playback, or

the album art (if available) for any audio file. To access a range of features in Now Playing view, right-click anywhere in the view. These are covered separately below:

Show list/Hide list: The List functionality covered in the Library View section above is also accessible here, and depending on the size of the WMP window, may take up part or all of the view.

Full Screen: This option is the same as clicking the 'View full screen' button - it expands WMP to fill the entire screen, and is available for video and image files. In full screen mode, WMP displays only the main image or video with a set of playback controls at the bottom. You can configure whether these controls are hidden by referring to the 'Allow autohide of playback controls' setting covered in the next section. Note that there is a difference between proper full screen mode and simply maximizing WMP - when maximized, WMP still displays the Taskbar and Title Bar; in full screen mode these are hidden as well.

Shuffle, Repeat: These options allow you to either Shuffle items to be played in random order, or Repeat the currently playing file over and over. You can also toggle these functions by clicking the crossed arrows symbol in the playback controls for Shuffle, or the circular arrow symbol next to it for Repeat.

Visualizations: This menu allows you to determine the graphics displayed during the playback of audio files. The 'No Visualizations' option shows no graphics in the background. If you want any available album cover art to be shown for the audio file being played, select 'Album art'. If you want a random visualization, select it from the sub-categories of visualizations available. Note that some visualizations may add to CPU load, and this can reduce performance on lower-end PCs. You can also select an 'Info Center view', which will display additional information on the currently playing audio file, however this will only work if you right-click and select 'More options', then under the Privacy tab tick the 'Display media information from the Internet' box. See the next section for more details.

Video: If a video file is loaded, you can choose whether to allow WMP to automatically resize the video to match the size of the current WMP playback window by selecting the 'Fit video to Player on resize option'; or you can choose to have the WMP playback window automatically resize to match the video's size when launched by selecting 'Fit Player to video'. In either case you can still freely resize the WMP window after the video has started playing and the video will also change size to match. You can also select the default video playback size of either 50% (half original size), 100% (original size) or 200% (double original size).

Enhancements: This allows you to open a separate window that provides access to a range of more advanced features. These features are covered in more detail under the Advanced Features section later in this chapter.

Lyrics, Captions and Subtitles: This option allows you to enable the display of any song lyrics, video or audio file captions, or movie subtitles where relevant, and if available.

Always show Now Playing on top: If selected, when in Now Playing view, Windows Media Player will always display itself in front of any other open windows. This can be useful in preventing other applications or prompts from obscuring video playback for example.

More Options: This takes you to the full range of WMP options, as covered in the Basic Settings section below.

< BASIC SETTINGS

To configure Windows Media Player as covered below, go to the Tools menu and select Options, or click the Organize button and select Options. Each tab of the Options is covered in detail below.

PLAYER

Automatic Updates: WMP will automatically check for available updates to itself at set intervals. The only information sent out during such update checks is your current Windows Media Player version number. Since WMP is not updated very often, the 'Once a month' option should be fine; don't select 'Once a day' as this is excessive.

Keep Now Playing on top of other windows: If ticked, this option forces WMP to remain in front of all other open windows when in Now Playing view.

Allow screen saver during playback: If ticked, any screen savers you have set will be allowed to come into effect as normal when WMP is open; if unticked, no screen saver will start when WMP is open, even if it is minimized to the Taskbar.

Add local media files to library when played: If ticked, this option automatically adds any media files you play to your WMP-specific Library. This only applies to media files on local storage devices, excluding removable devices such as CD or DVD media.

Add remote media files to library when played: If ticked, this option behaves the same as the setting above, however it only relates to media files stored in remote locations outside of your PC, such as over a network.

Connect to the Internet: This option determines if Windows Media Player is allowed to connect to the Internet to update various information. If selected, it can override your other Internet-related settings as covered further below, so I recommend unticking it and manually configuring each individual option separately, then only coming back and ticking this option should you need to ensure Internet connectivity for a particular online-based feature that is otherwise not working properly.

Stop playback when switching to a different user: If ticked, this option stops playback when you go switch to another user account, otherwise WMP will continue playing. It is recommended that this be ticked.

Allow autohide of playback controls: If ticked, whenever you are playing back a media file in Now Playing view, after a moment the playback controls at the bottom will fade out of view. If you move your mouse over the WMP window at any time they will reappear. This is recommended as it provides a less cluttered interface in the Now Playing window.

Save recently used to the Jumplist instead of frequently used: If ticked, this option will only save your recently used media files to be displayed in the Jump List for Windows Media Player on the Taskbar. If unticked, your frequently used media files will be displayed instead. See the Taskbar section of the Graphics & Sound chapter for more details on Jump Lists.

RIP MUSIC

Rip music to this location: Ripping music is the process of copying and converting music from an audio CD to a media file on your computer. Click the Change button and select the directory where any ripped music or media is placed; by default it will be placed under the *\Users\[username]\My Music* folder. Click the 'File Name' button to specify the particular attributes of the CD which will be used to compose a ripped music track's filename. You can also change the name for any ripped music in the future automatically by changing the settings here and then ticking the 'Rename music files using rip music settings' option under the Library

tab of the options, as covered further below. Check the preview at the bottom of the box to see an example of how your filename configuration will look.

Rip Settings: Here you can select the output format for ripped audio files, including .WMA, .MP3 and .WAV. MP3 provides a good compromise between quality and size, and you can adjust the bitrate (quality) of the MP3 file using the slider further below. If you want an exact copy of the audio file select .WAV, however this will result in a very large file. If you select one of the Windows Media Audio (.WMA) formats, then I strongly recommend that you untick the 'Copy protect music' option if available, otherwise each track you rip will become DRM protected and this cannot be changed - see the DRM section later in this chapter. I don't recommend ticking the 'Rip CD automatically' box, as it will automatically initiate a rip on any inserted audio CD, which may not be desirable.

On the Audio quality slider, choose the audio quality you prefer for ripped music. A bitrate of 192 Kbps or above is recommended for good quality audio in the .MP3 or .WMA formats. The lossless formats, such as .WAV and .WMA lossless, don't allow for quality change, because they record at 100% of the quality available. The higher the quality, the larger the size of the resulting ripped file.

To use WMP to rip any audio tracks you want from an Audio CD at any time, do the following:

1. Insert the Audio CD in your optical drive.
2. Depending on your AutoPlay settings, Windows Media Player may open automatically with the Rip list showing; if not, open WMP manually and select the disc in the Navigation Pane.
3. Place a tick mark next to the tracks you wish to rip, and untick those you don't want.
4. If you want WMP to automatically download media information for the ripped file(s), such as relevant artist details and album art, you will need to be connected to the Internet and have the 'Update music files by retrieving media info from the Internet' setting ticked under the Privacy tab of WMP options - see further below for details. You can apply this information to the file at a later date instead if you wish.
5. You can alter the rip parameters at any time by clicking the 'Rip settings' button - these options are all the same as those covered further above.
6. Click the 'Rip CD' button which now appears at the top of the WMP window.
7. I strongly recommend selecting the 'Do not add copy protection to your music' option which appears, and tick the 'I understand...' box underneath, then click OK. If you add copy protection to your rips, then you will have to update the DRM rights regularly, and will also have a migration limit imposed on the files, preventing you from moving them to new machines or devices after a certain number of migrations, which is not desirable. See the Privacy and DRM sections later in this chapter for more information.
8. WMP will rip music from your CD to the directory specified in your settings earlier. By default this is a folder within your Music Library.

There are various third party ripping tools available, however Windows Media Player is free, quick and easy to use, and the audio tracks it produces will be of good quality, and not contain any copy protection, as long as you use the relevant options covered above, so it is well worth using.

DEVICES

The devices listed under this tab are those capable of media playback, whether video or audio or both. Select each playback device and click the Properties button. Adjust settings as appropriate, and if in doubt leave at their defaults which are fine for most purposes. Note that for your Display properties, you can alter the aspect ratio for video playback if it appears to be too wide or too narrow; the circle shown should be perfectly round on your screen. If it is not, first check your settings as covered under the Display Settings section of the Graphics & Sound chapter, then return here and move the slider to make the appropriate changes.

When deleting playlists from devices, also remove their contents: If ticked, this option forces the deletion of the original files stored on a device contained in a deleted Playlist.

Click the Advanced button to alter the settings for audio and video file conversions when being transferred to/from multimedia devices, and set to suit your tastes.

BURN

Windows Media Player allows you to also burn music or media files to a CD or DVD by selecting the Burn tab in Library view. Files can be dragged and dropped into the list under the Burn tab, ready to be burned to disc once the 'Start burn' button is pressed. Music will be burned as an audio CD, but other media can only be burned to CD or DVD as data files. If you want to burn pictures or movies to DVD for playback as a proper DVD movie disc, you need to use a custom DVD making program instead, which is covered further below.

Burn Speed: Select the burning speed, keeping in mind that if you are continually having errors with burnt discs, you should reduce the speed to Medium or even Low to ensure accurate burning. If you want the disc automatically ejected after the burn is complete, tick the relevant box.

Apply volume leveling across tracks on the CD: If burning an audio CD, you can tick this option to have WMP set a common volume level for all audio tracks. This can help prevent some tracks from being overly loud or soft relative to the others.

Burn CD without gaps between tracks: If ticked, this option burns an audio CD without the enforced 2 second gaps between each track. Your optical drive needs to support gapless burning for this option to work.

Add a list of burned files to the disc in this format: If ticked, this option burns a Playlist of the files on a data disc along with the files themselves. If you then insert this disc into a device that supports .WPL or .M3U Playlists, the device will play the files back in the order in which they appear in the Playlist.

Use media information to arrange files in folders on the disk: If you are burning a data disc and this option is ticked, WMP will sort your media into separate folders, such as *\Music\Artist\Album*, *\TV*, *\Video*, and *\Picture*. If unticked, WMP will burn all tracks to the base directory of the disc without any sorting.

Remember that you can also burn any disc using the built-in Burn features of File Explorer. Insert a blank/rewritable DVD or CD into your drive, then drag any file or folder to your optical drive in File Explorer, and it will be added to a list of files to burn to disc. When ready, right-click on the drive and select 'Burn to disc' and the files will be burned. This only creates data discs.

If you want to create a DVD movie disc that can be used in a standalone DVD or Blu-Ray player for example, then you need to use a custom app or program for that purpose. The Windows DVD Maker utility available in Windows 7 is no longer available in Windows 8.

To create proper video discs, you must first have prepared the data in the appropriate format before burning to disc. For example, to create a DVD movie disc you must have the data in correct *\AUDIO_TS* and *\VIDEO_TS* folders, with the necessary .VOB, .IFO and .BUP files, so that even if burned as a data disc by File Explorer it can be played back on a DVD or Blu-ray player. Various conversion utilities exist to allow you to convert .AVI, .MP4 and other video file formats into the appropriate files and structures for standalone DVD or Blu-Ray playback. The free Avidemux, VirtualDub, Handbrake and Avi2DVD utilities allow you to edit and convert a range of video files, and convert them into the appropriate DVD or Blu-ray format for burning onto disc and result in proper playback on standalone players.

If you're after a disc burning program for advanced purposes, there are a range of full-featured third party burning programs available. Prominent among these is Nero Burning ROM, which requires purchase, but can be trialed for free. The free ImgBurn is a reasonable, but less comprehensive, alternative.

Windows Movie Maker: On a related note, if you wish to make and edit your own movies, be aware that Windows Movie Maker was removed from Windows as of Windows 7. If you require this functionality, you can install the old standalone Windows Movie Maker 2.6, or the more recent Windows Movie Maker.

PERFORMANCE

Connection Speed: This setting controls the speed with which Windows Media Player can download streaming media. I recommend the 'Detect connection speed' option, however if WMP consistently has problems detecting your connection speed and it seems to be too low, then set it manually here.

Network Buffering: This setting controls the amount of data to be buffered (stored in advance of playing), to help prevent stuttering and skipping in streaming media playback. The 'Use default buffering' option is usually fine, but if you find streaming videos are constantly disjointed, then experiment with increasing the buffer size.

Video playback: These options affect playback of video files, and can be used to help resolve issues with particular videos. If your video goes out of sync, tick the 'Drop frames to keep audio and video synchronized' option. Tick the 'Use video smoothing' option if playing back choppy video with a low framerate, and WMP will try to interpolate frames (fill in the blanks) to provide the appearance of smoother video playback.

If the 'Display full-screen controls' option is ticked, when playing fullscreen video the playback controls will be shown at the bottom of the screen; they may become autohidden after a short period, depending on whether you ticked the 'Allow autohide of playback controls' option covered above. However, if you want these playback controls removed completely in fullscreen mode, untick this box. You can then control playback using your mouse and keyboard:

- Play or Pause - Left-click on the video.
- Change Volume - Use the mouse wheel to increase or decrease volume.
- Mute Volume - Press the middle mouse button.
- Fast Forward/Rewind - Press and hold the front and back mouse thumb buttons (if any) for Fast Forward/Rewind.
- Skip Forward/Back - Click the front or back mouse thumb buttons to Skip Forward/Skip Back.
- Command Menu - Right-click on the video.
- Return to Full Mode - Press ESC.

If you have a plug-in graphics card, tick the 'Turn on DirectX Video Acceleration for WMV Files' option to allow your graphics hardware to provide better video playback performance for .WMV videos. Windows provides support for the DXVA-HD hardware-accelerated HD video processing API.

Finally, for videos which don't fill the entire screen due to their aspect ratio being different to your monitor shape - such as video files in the old 4:3 TV format - you can set the color used to display the surrounding area. For example, for playback on a Plasma TV, to prevent burn-in or uneven phosphor aging, you can set a white or gray background by clicking the Change button.

LIBRARY

Add video files found in the Pictures Library: If ticked, adds any video files resident in your Pictures Library. However they will be added under the Videos library in WMP, not Pictures.

Add volume leveling information values for new files: If ticked, data for use with the Auto Volume Leveling enhancement feature of WMP will be added to each new file. This is only recommended if you have specific need for this feature. See the Advanced Features section later in this chapter for details of Auto Volume Leveling.

Delete files from computer when deleted from library: If ticked, this option makes the 'Delete from library and my computer' option the default selection when you right-click on a file and select Delete - see the Views section earlier in this chapter for more details. This is not recommended.

Automatically preview songs on track title hover: If ticked, whenever you hover your mouse cursor over a particular track title in WMP, an automatic preview of the song will begin, and end the moment you move your mouse away. If unticked, when you hover your mouse over a track title, the Preview box will appear and you will need to click the Preview link within it to commence a preview of the song.

Retrieve additional information from the Internet: If you want WMP to retrieve information about the particular media you are playing, such as the name of the album or artist for a track, then tick the 'Retrieve additional information from the Internet box'; you can then choose to have it fill in the gaps, or overwrite all existing information for the media. Be aware that choosing 'Overwrite all media information' can replace any customizations you've made to the tags on your media files. You can also manually force Windows Media Player to fill in missing information for specific files at any time by right-clicking on a particular track in Library view and selecting the 'Find Album Info' option. A new box will open which loads up the possible matches for this track and you can select the appropriate one, then click Next. You can then click the Edit button to enter or alter the information manually. Click Finish when done to apply this information to the file. Note that if you tick this option, it will also automatically enable the 'Update music files by retrieving media info from the Internet' option under the Privacy tab, as covered further below.

If you have privacy concerns, see the Privacy section further below for more information. By adding album information, you can make the Windows Search functionality much more useful, since the more metadata there is for a particular file, the more ways there are for you to search for and categorize that file - see the Windows Search chapter. You can also improve your ability to find music in the WMP Library and in File Explorer, because in Content or Icon view the presence of album art makes song identification at a glance much easier. So on balance enabling this option is recommended.

Rename music files using rip music settings: If this option is ticked, all music files you have ripped will be renamed using the settings you've specified in 'File Name' under in the Rip section of the player options.

Rearrange music in rip music folder, using rip music settings: Similar to the option above, if ticked this option changes the arrangement of music in ripped folders based on any changes you've made under the Rip section of the player options.

Changes resulting from enabling either of the two settings above will only be implemented the next time media information is updated for ripped files.

Maintain my star ratings as global ratings in files: If this option is ticked, your star ratings for media files will be stored as part of the media files. This prevents other user accounts from overwriting your ratings, as long as other users also don't have this option ticked in Windows Media Player under their own account. Other users will still be able to rate files, but those ratings will be stored in their WMP-specific Library and only viewable by and applicable to their own user account.

PLUG-INS

Plug-ins are various modules that add functionality to Windows Media Player, such as Visualizations or Digital Signal Processing (DSP) effects. These can be added, removed or configured here. You can also download new plugins and visualizations by clicking the relevant links at the bottom of the window. You can remove any added plugin by highlighting it and selecting the Remove button, and you can configure any settings they may have by selecting the Properties button. Bear in mind that the more plugins you use in WMP, the more resources the player may take up, and also the greater the chance for potential problems, so only install plugins that you feel are genuinely necessary.

PRIVACY

This is an important aspect of Windows Media Player which causes users a lot of concern. There is a fear that by using Windows Media Player, Microsoft is spying on your media usage behaviors for underhanded purposes. To clarify precisely what WMP reports back to Microsoft, click the 'Read the privacy statement online' link at the top of this tab in WMP. Essentially, the following basic computer information will typically be sent by WMP to Microsoft along with information requests:

§ IP address.
§ Operating system and version.
§ Internet browser and version.
§ Region and language settings.
§ Hardware ID.
§ Cookies for Microsoft's WindowsMedia.com site, which is the primary location WMP contacts for obtaining media information.

Depending on the particular options and features you enable, additional information may be transmitted to Microsoft. This is covered under the relevant settings below:

Display media information from the Internet: If this option is ticked, any CDs or DVDs you play or rip with Windows Media Player will send a request to WindowsMedia.com to provide any missing media information. This request includes the basic computer information above, along with an identifier for the CD or DVD, and the information received will be stored by WMP in your Library. This feature is particularly useful when ripping CDs, as it adds a lot of useful information and album art to the ripped tracks without requiring manual input. For this reason I recommend that it be ticked. Note that you can clear the stored information on your CDs or DVDs at any time by clicking the 'Clear Caches' button at the bottom of the Privacy tab.

Update music files by retrieving media info from the Internet: If ticked, this option allows WMP to download additional information and album art for your music files. This will occur when you use your Library after opening WMP for the first time, or whenever you add files to your Library, or add new locations to the Library. You can also force it to occur at any time by going to the Tools menu, selecting Advanced and then selecting the 'Restore media library' option. WMP will transmit the basic computer information further above to WindowsMedia.com, along with a full range of data on the music files, including any data you have manually entered for them, for the purposes of identifying the tracks. If information is found, it will be downloaded and stored in your Library. This is a useful feature, because as discussed earlier, it makes searching for and identifying music at a glance much easier. For this reason I recommend that it be ticked.

You can control whether to download only missing information for a file, or replace all existing information with new information, based on your choice for the 'Retrieve additional information from the Internet' setting under the Library tab, covered earlier. If you replace all information, bear in mind that under Windows Media Player 12, the Advanced Tag Editor feature has been removed, so you may have to

manually edit the file properties for each media file to alter any tags. You can do this within Library view by right-clicking on any tag and selecting Edit. You can also use the free MP3Tag utility instead.

Download usage rights automatically when I play or sync a file: As part of the Digital Rights Management (DRM)-related features of Windows Media Player, if this option is ticked, it will automatically check and update the rights status of any DRM-protected files you wish to play or sync via WMP. It will automatically connect to the appropriate rights server to obtain the relevant updates and rights as required. It will transmit your basic computer information, an ID for the media file, the type of action you wish to perform on the file (e.g. play or burn it), and the DRM components on your computer. You can untick this option, however if you have DRM protected content and it is not playing back properly, then you may have to enable it to allow you to continue to use those media files. This option doesn't affect media files which are not protected with DRM. You can check to see if any media file is protected by DRM by right-clicking on it within WMP, selecting Properties and looking under the Media Usage Rights tab.

Automatically check if protected files need to be refreshed: If this option is ticked, WMP will regularly scan your Library for the status of DRM-protected files, and if they have expired rights or require a software upgrade, such as a new version of Windows Media Player, then these will be installed as required. The same type of information as in the option above is transmitted to Microsoft servers for the purpose of ensuring that DRM-protected media can be played back properly. This option does not apply to unprotected media files.

Untick the 'Connect to the Internet' option under the Player tab, as covered earlier in this chapter, and see the Prevent Windows Media DRM Access section under the Group Policy chapter and enable it if you want to prevent WMP from accessing the Internet in any way to check or update any DRM-related features. See the Digital Rights Management section later in this chapter for more details.

Set clock on devices automatically: As part of DRM protection, some portable media devices have an internal clock used to validate media usage rights. If this option is ticked, WMP can automatically set the clock on the portable media device whenever it is synced. This is recommended to ensure proper playback capabilities for DRM-protected content on your device, otherwise the device may have its rights revoked and you won't be able to play new DRM protected content on it.

Send unique Player ID to content providers: If ticked, this option provides online media content providers the ability to identify your particular connection to their service over time. This provides you with no benefit whatsoever, so this option should remain unticked.

Windows Media Player Customer Experience Improvement Program: If ticked, this option collects a range of information, including your basic computer information, hardware information, errors, performance issues and how you use Windows Media Player and related services. This is sent to Microsoft to help them improve the development of future versions of Windows Media Player among other things. It is not necessary for you to tick this option if you don't wish to be involved in the Customer Experience Improvement Program.

History: This section allows you to select the specific categories for which WMP will maintain a history. One of the benefits of this history is that it provides WMP with the ability to display frequently or recently played files in its Jump List on the Taskbar, as well as usage-based Playlists. If you don't wish to keep this history, untick these boxes, then click the 'Clear History' button.

Clear Caches: WMP maintains a cache of the media information it has downloaded from the Internet, so that it doesn't have to re-download this information each time. It also keeps a cache of the relationships it has with synchronized devices, improving its ability to quickly sync with such devices. You can clear this information at any time by clicking the 'Clear caches' button.

Ultimately, while Windows Media Player may send a wide range of information to Microsoft regarding your media files and usage patterns, there are no real privacy risks; Microsoft is not trying to "spy" on you. For example, Microsoft may use the data to determine the rate and type of music piracy around the world, but in practice it would be extremely detrimental to Microsoft's reputation and customer trust if it were to use this information to take action against individuals for any such detected piracy. See the Digital Rights Management section further below for more discussion on this issue.

SECURITY

Run script commands when present: If ticked, this option allows WMP to play any script commands associated with media files. This is not recommended as scripts are a common method used to initiate malicious activity on your PC.

Run script commands and rich media streams when the Player is in a web page: If ticked, this option allows scripts and rich media, such as movies or slide shows, to play in incidences of WMP which are embedded into web pages. I recommend unticking this option, and then only ticking it if a trusted site with embedded media content requires it for normal playback.

Play enhanced content that uses Web pages without prompting: If ticked, if you visit any web page which has enhanced content, it will be played without any warning. I recommend unticking this and only playing back enhanced content when prompted on trusted websites.

Show local captions when present: If ticked, this option allows Synchronized Accessible Media Interchange captions to be displayed during media playback. I recommend unticking this option until you run trusted content which requires it.

Security Zone: Your Internet Explorer security settings will be used when Windows Media Player is browsing any web content, so see the Internet Explorer chapter for details. Note that if you choose too high a setting, it may prevent you from downloading additional media information or codecs under certain circumstances.

NETWORK

Configure this section according to your needs. The defaults should be fine unless you have specific requirements, such as streaming media which does not appear to be working correctly.

When done with the WMP options, click the Apply button and click OK to exit them.

< ADVANCED FEATURES

There are a range of more advanced features in Windows Media Player. These can help you improve the audio and video quality of WMP, as well as its usability.

ENHANCEMENTS

To access the enhanced features of Windows Media Player, switch to Now Playing view then right-click on the player and select Enhancements. The available options are:

Crossfading and Auto Volume Leveling: These are actually two separate features, and can be enabled or disabled separately. Crossfading provides the ability to slowly fade out one song while the next song is overlapped and slowly faded in at the same time. Click the 'Turn on Crossfading' link, then use the slider to determine how many seconds of overlap there will be during which the first song fades away and the second song fades in. Auto Volume Leveling can be enabled by clicking the 'Turn on Auto Volume Leveling' link in the same window, and if enabled, attempts to normalize the volume level across various songs so that they do not vary greatly in overall volume. However, Auto Volume Leveling only works for .WMA or .MP3

files that have volume leveling data added to them. You can add such data to any newly added files by ticking the 'Add volume leveling information values for new files' option as covered under the Library section earlier in this chapter.

Graphic Equalizer: Windows Media Player comes with a graphic equalizer that can noticeably enhance audio quality if set up correctly. To enable the graphic equalizer, click the 'Turn on' link at the top left of the window. To fine tune your settings, play back some music while adjusting the equalizer and the changes will be applied in real-time. You can use a range of presets for the equalizer by clicking the Default link at the top right of the window, however I recommend adjusting the equalizer bars yourself for the best results. To start with select the individual slider movement option - the first of the options at the far left just below the 'Turn off' link - as this allows you to move each slider on the equalizer without changing the other sliders. Then slowly customize the equalizer using your favorite piece of music. Keep in mind that moving from left to right, the sliders progressively go from low to high frequencies, i.e. from Bass to mid-range to Treble. Settings will vary from system to system based on the quality of your sound hardware, and importantly, any adjustments you may have made to the Windows Sound settings for your playback device - see the Sound section of the Graphics & Sound chapter.

Play Speed Settings: This option allows you to slow down or speed up the playback of media. Any values below 1.0 on the slider will slow down playback, while values above 1.0 will speed it up. You can use the Slow, Normal or Fast preset links at the top of the window for quick adjustment if you wish. There is also the capability to view a video frame by frame by using the arrow buttons at the bottom of this window.

Quiet Mode: If enabled by clicking the 'Turn on' link, this feature allows you to reduce the difference between loud and quiet portions within an audio or video file. You can choose the level of difference using the options presented, with 'Little difference' evening out audio much more than 'Medium difference'. This is not the same as the Auto Volume Leveling feature, as that equalizes volume across audio tracks, whereas this option attempts to equalize the range of volume within a track.

SRS WOW Effects: If turned on, this option enables SRS WOW effects that effectively increase the perceived size of the audio. First, select the type of audio output you have on your system by repeatedly clicking the 'Normal Speakers' link at the top left to cycle through the available options. Next, you can adjust the TruBass slider to increase the bass response, which can help weaker speakers sound fuller and more powerful. The WOW Effect slider affects mid-range and higher frequencies, altering the sharpness and positioning of the audio. In practice these effects may or may not improve your audio depending on your tastes, so experiment with them while playing back your favorite music, as the effects are applied in real-time.

Video Settings: These enhancements affect the appearance of any videos played back through WMP. You can adjust the Brightness, which controls how light or dark the overall picture is; the Contrast, which determines the level of difference between light and dark areas; the Hue, which affects the overall color tone of the image; and the Saturation, which sets the richness of colors. You must test these in real-time by running a video while you adjust them, and you can reset them to default values by clicking the Reset link at any time. Clicking the 'Select video zoom settings' link accesses the same settings available under the Video menu when you right-click in the Now Playing window, and is covered in more detail under the Views section at the start of this chapter.

Note that you can adjust any slider in these Enhancement features with greater precision by clicking once on the slider, then using your arrow keys for incremental changes. You can see the exact numerical value for any slider by hovering your mouse over it, which is useful if you wish to record the settings for future reference. Finally, you can close the Enhancements box at any time by clicking the small red 'x' at the top right of the window.

SKINS

While the default Windows Media Player 12 window can be resized, and you can turn on or hide various elements through the options covered in this chapter, for the most part that's about as far as you can go in terms of changing how WMP looks. To truly customize Windows Media Player's appearance, you can use Skins. There are two skins which already come with the player, and you can view them by opening Windows Media Player in Library view, and under the View menu selecting 'Skin Chooser' (ALT+V+S). Here you can select a skin in the left pane to see a preview of it, and then click the 'Apply Skin' button to implement it in WMP. To switch back to the default WMP appearance, go to the View menu and select Library, or find a 'Switch to Library' or 'Switch to Full Mode' button or similar and click it.

To get more free skins for use with WMP, click the 'More Skins' button, or go to a site such as The Skins Factory and download the skin of your choice. Some skins will install automatically when you double-click on them, but if that doesn't work, put the .WMZ file in your *\Program Files (x86)\Windows Media Player\Skins* directory. Using more complex and elaborate skins can take up more memory and CPU resources when you run Windows Media Player, so if you want to ensure the fastest performance and least resource usage, simply use the default WMP appearance. That is, under the View Menu select 'Full Mode'. To remove a skin from Windows Media Player, highlight it in Skin Chooser and click the red X button.

TASKBAR PLAYER MODE

One of the neat features of previous versions of Windows Media Player was the ability to shrink it down into a Mini Player interface which sat in the Windows Taskbar. Unfortunately this feature has been removed in Windows Media Player 12, replaced by a Taskbar preview mode which only contains back, forward, and pause/play buttons. Hover your mouse over the WMP icon in your Taskbar to see this mode when a media file is open. The only other option is to switch to Now Playing mode, and left-click and drag one of the corners of the WMP window such that the window becomes as small as possible. Make sure the 'Allow autohide of playback controls' option is ticked, as covered under the Basic Settings section above. This provides the smallest and most minimal interface for WMP, while still giving you full functionality when you hover or right-click your mouse over the open WMP window.

Finally, if you are having problems running Windows Media Player, check the Windows Media Player Solution Center for help in resolving it.

< AUDIO & VIDEO CODECS

A Codec (Compressor Decompressor) is a program that allows audio or video to be compressed and decompressed to or from its original format. Compressed files use special algorithms to achieve size reductions, and it is the codec that can encode/decode these algorithms. A Codec is not the same as a file format; a file format is simply a container type, while a Codec relates to the actual encoding of the media held in the container. For the most part you don't need to worry about this, because if you can play or record audio/video in a particular format, you have a Codec for that format already installed on your system. More details about Codecs in WMP can be found in this Microsoft Article.

VIEWING AND EDITING CODECS

To view the Codecs already installed on your system, do the following:

1. Open Windows Media Player and switch to Library view.
2. Go to the Help menu (ALT+H) and select 'About Windows Media Player'.
3. Click the 'Technical Support Information' link at the bottom of the dialog box.
4. A new browser window will open. Towards the bottom is a list of all the audio and video Codecs installed on your system, the files that relate to these Codecs, and their version numbers.

To view Codec information for any file or your system in more detail, and to also attempt to adjust the priorities Windows assigns to individual Codecs - for example to force Windows to use one codec of the same type over another - you can use the free GSpot utility. Install GSpot and launch it, then under the System menu select the 'List Codecs and Other Filters' option. In the box which appears, you can sort Codecs by general type, name, driver filename, etc. I recommend sorting by the first Type column to start with. Double-click on any particular codec for more information. To set the priority for a Codec, right-click on the relevant Codec and select 'Set Filter Merit'. Raising the slider will give this Codec higher priority over other Codecs of its type; lowering the slider will lessen the possibility that it will be used. Use this feature with great care, and be sure to note the original merit value for any codec you change in case you wish to restore it.

If you want to uninstall a non-standard or problematic Codec, the best way to remove it is to go to the Programs and Features component of the Windows Control Panel and look for the Codec name in the list shown. If it's not listed there, then you can use GSpot to manually remove it. Follow the instructions above to get to the complete list of Codecs on your system, and then right-click on the relevant codec and select 'Un-Register Filter', then you can try to manually delete the relevant file(s) by right-clicking on it, selecting Details, and looking for the file location.

Obtaining Codecs

Windows Media Player 12 can play the following file formats by default: MP4, AVI, MOV, 3GP, AVCHD, ADTS, M4A, DVR-MS, MPEG-2 TS, and WTV. It has built-in support for the following Codecs: H.264, MPEG4-SP, MPEG-2, MPEG-1, DIVX, XVID, 3IVX, MJPEG, DV, AAC-LC, AAC-HE, MP3, MS ADPC, Dolby Digital, and LPCM. This means that you will be able to play back all common audio and video files.

If you need to download a new Codec because a particular media file is not playing back correctly, first determine what Codec(s) a particular file uses. Use GSpot to load the file, and the relevant Codec information will be displayed on the main page. If you then want to manually find the required Codec, search the web for the Codec name to find the original author's site. The most common third party Codec required to play back video found on the web is DivX, however WMP 12 already has basic built-in support for DivX. You can also download FFDShow which is a filter that decodes most common video and audio formats, including DivX, XviD, AC3, FLAC and OGG. If you just want FLAC and OGG support, install the Xiph Directshow Filters. For FLAC only, install the FLAC Codec.

There are also certain types of media which may not play back on Windows Media Player or other media players due to proprietary issues. The RealPlayer .RM format for example is one such format which requires a special Codec, and is usually only viewable by installing the RealPlayer media player. However, you can install Real Alternative to allow WMP 12 to play back RealPlayer format files.

In other cases there may not be an appropriate free Codec available to allow you to play a particular format, in which case you may need to install the proprietary player for that format.

Note that under Windows 8, Windows Media Player will no longer play back DVD movie discs by default as it did in previous version of Windows. It also cannot play back Blu-ray discs by default. See the DVD & Blu-ray Playback section for details and alternatives.

Codec Packs: I strongly advise against installing any general Codec Packs. These packs are tempting, as they typically advertise themselves as containing all the Codecs you'll ever need in one package. However, they are known to cause conflicts which can result in a range of problems, from reduced performance, glitches and crashes in games and multimedia playback, to the complete loss of audio in certain applications. Even Microsoft warns against the installation of Codec Packs, so this is not a warning to be taken lightly. In some cases only a full reinstall of Windows can completely undo the damage caused by a Codec Pack.

64-bit Codecs: Under Windows 8 64-bit, normal 32-bit Codecs will work, however some native 64-bit software and some Windows features may exhibit minor issues. For example, videos may not correctly display a content thumbnail in Icon view in File Explorer. You can resolve this by installing the 64-bit version of the Codec instead. This shouldn't be necessary given Windows Media Player 12 runs as a native 64-bit application and supports a wide range of audio and video Codecs.

Some 64-bit applications may not detect 32-bit Codecs; for example the 64-bit version of the free video editing software VirtualDub works perfectly well on Windows 8 64-bit, but it may require a 64-bit Codec like Lame64 for full MP3 encoding support. You will have to check and resolve these issues for any third party media players and encoders. This is one of the reasons why Windows Media Player 12 is recommended as the default media player, because it is designed to be the most compatible with Windows 8, both 32-bit and 64-bit versions.

If you are going to experiment with Codecs, I strongly recommend creating a full system image backup just prior to commencing, because as noted earlier, the uninstallation and cleanup required after using problematic Codecs can be extremely difficult. The quickest solution can sometimes be to restore from a system image - see the Backup & Recovery chapter. Codecs are one of the biggest culprits of problematic behavior for media playback and in game. Don't install more Codecs than absolutely required, and do not install any Codec Packs, no matter how tempting they seem.

< DVD & BLU-RAY PLAYBACK

As of Windows 8, the ability to play back DVD movie discs by default has been removed from Windows. Furthermore, just like previous versions of Windows, you cannot play back Blu-ray movie discs by default in Windows. In both cases, Microsoft has done this to avoid the costs of licensing the proprietary decoders for these media formats. You will require additional software to enable DVD or Blu-ray disc playback functionality on Windows 8.

DVD PLAYBACK

To enable DVD video disc playback, you can do one of the following:

§ Install Windows Media Center, as covered in the Add Features to Windows 8 section of the Windows Control Panel chapter. Windows 8 Pro users can use this method to purchase the Windows 8 Media Center Pack, while Windows 8 non-Pro users can purchase the Windows 8 Pro Pack to upgrade to Windows 8 Pro along with Windows Media Center. Adding Windows Media Center to Windows 8 will enable DVD playback.
§ Download a third party media player with built-in DVD playback support. The most popular of these is the free VLC Media Player, which has a range of other useful features. Another good free alternative is Media Player Classic Home Cinema.

BLU-RAY PLAYBACK

The Blu-Ray video disc format allows high resolution video playback, typically at a resolution of 1080p, whereas standard DVD is 480p (NTSC) or 576p (PAL).

To play back Blu-ray movies from Blu-ray discs, you will need to purchase a third party media player that specifically supports Blu-Ray playback. The most popular of these are the latest versions of PowerDVD or WinDVD. There are no free media players that can play back Blu-ray movie discs, though some may purport to do this. You must also have a Blu-Ray drive on your PC, and your hardware setup will also need to meet the Windows DRM requirements to play back HD movies properly, as covered in the next section.

For general information about home theater-related topics, see A Guide to HDTVs.

< DIGITAL RIGHTS MANAGEMENT

A major issue of concern for people playing back media in Windows is Digital Rights Management (DRM). This is a form of protection, applied to media content to prevent it from being copied, or used beyond the scope of its original licensing terms.

To see if a media file is protected by DRM, add it to your Library, then open Windows Media Player in Library view, right-click on the Title of the media file and select Properties. Under the 'Media Usage Rights' tab you will see if the file has any protection, and what conditions if any there are to its usage, such as number of times you can move it to another machine or device, or when the file usage rights expire. You cannot legally remove or alter DRM, so it will not be covered here. If you have a file protected by DRM, comply with the terms it requires, which may include upgrading Windows Media Player 12 to the latest version, and enabling a range of DRM-related options as covered earlier in this chapter.

An additional form of DRM was integrated into Windows as of Vista. It is designed to provide protection for High Definition (HD) video content, such as that found on the Blu-ray movie disc format. To ensure that content from a protected HD format is not being copied, altered, or coming from an unauthorized copy, Windows requires that all of the following conditions be satisfied:

§ The TV or monitor is connected via a pure digital DVI or HDMI cable.
§ The TV or monitor supports the High-bandwidth Digital Content Protection (HDCP) format.
§ An original Blu-Ray disc is being used.
§ An activated copy of Windows 8 is being used.
§ A signed WDDM graphics driver is being used.

Windows will check at startup to ensure that your hardware and system drivers support the conditions above, and if satisfied will enter Protected Environment such that you can play back any Blu-Ray disc without any problems. Note that any standalone Blu-Ray player requires the first three conditions above to be met as well for the playback of commercial content, so this is not a Windows-specific requirement. More details of the specific requirements and impacts are in this Microsoft Article.

If you don't meet any of the requirements above, and thus don't enter the Protected Environment, the content provider, that is the company which produced the actual HD material you are trying to view, can implement a degradation in the quality of the video to that of a regular 480p DVD, or prevent playback altogether. This is left up to the provider to decide; Windows has no involvement in determining this, it simply tells the media whether it is or isn't running on a Protected Media Path.

The Protected User Mode Audio function was introduced in Windows Vista, providing the ability to protect audio content from being unlawfully copied, similar to the protection provided to HD video content.

None of the above information applies to HD content or audio that is not DRM protected. Furthermore, even DRM protected content may not enforce any or all of the possible restrictions; this is left up to each content provider to determine. So in practice, for the average user, the DRM present in Windows 8 has no noticeable impact, since it is all being handled behind the scenes without any need for user input, similar to a standalone DVD or Blu-ray player.

If you want to minimize the impact of DRM protection on your system, I recommend purchasing your media and games on physical CDs, DVDs and Blu-Ray discs, rather than through digital channels. This may sound like a backward step in the digital age, but the physical versions of this media have the following benefits:

- Fewer restrictions - You can rip an audio CD as often as you like for example, and to any particular quality you prefer, whereas digital copies are locked at a particular bitrate, and may have transfer restrictions.
- Higher quality - In some cases, such as with streaming movies, the equivalent physical Blu-ray copy will often be of higher quality. This is because streaming providers usually limit bitrate to save bandwidth.
- Greater security against accidental deletion - If you accidentally delete a digital copy, you may not be able to simply redownload it from the online store where you purchased it. A physical copy is generally more secure against accidental loss, and rarely needs to be repurchased.
- Potential resale value - In most cases, digital copies of music, movies and games cannot be legally resold; legitimate physical copies can be resold without such restrictions.
- Protection against DRM changes - Some DRM protection systems on digital files may be phased out, or altered in such a way as to cause problems with existing protected content, even locking you out of such content. Physical copies are effectively immune from changes in DRM, since they don't require updates to continue working, and most standalone players and software are backward compatible.

While somewhat old-fashioned, legitimate physical copies provide a reasonable balance of cost, convenience, quality, protection, and the ability to transfer the media between machines and devices, as well as rewarding the creators of the content. Digital downloads or streaming options may be cheaper and more convenient, but they carry more restrictions and risks.

< OTHER MEDIA PLAYERS

Although Windows Media Player is extremely convenient and quite versatile, if you don't wish to use it to view multimedia content, there are a range of free alternatives, including:

VLC
Media Player Classic Home Cinema
WinAmp
QuickTime Player

I can't go into detail about each of these players in this chapter, however their usage will depending upon your personal preference and specific needs. For the most part, installing VLC alongside WMP will allow you to handle virtually any video format or situation that arises.

GRAPHICS & SOUND

Some of the biggest changes in Windows 8 come in the form of alterations to the Windows interface. The interface commonly referred to as Metro is the most prominent of these changes. Aside from the more obvious differences, there are a range of changes beneath the hood that make Windows 8 more efficient in its handling of resources when providing graphics and audio functionality, especially when compared to Windows XP and Vista. A basic understanding of the technical changes in Windows 8 is required, and is covered in this introduction, before we go any further in this chapter.

Windows 8's graphics capabilities are powered by the Windows Display Driver Model (WDDM), which began with Version 1.0 in Vista, then Version 1.1 in Windows 7, until it has now been upgraded to Version 1.2 in Windows 8. Each iteration of WDDM has brought improvements. Under WDDM 1.0, the Desktop Windows Manager (DWM) was introduced, allowing a combination of 2D and 3D effects on the Desktop, such as the transparent Aero interface. In Windows 7, WDDM 1.1 added Graphics Device Interface (GDI) hardware acceleration for 2D graphics, which in turn allowed the DWM to use video memory as opposed to system memory for rendering the Desktop, increasing overall performance and resulting in much less system memory usage. in Windows 8, WDDM 1.2 adds Screen Rotation support, Stereoscopic 3D support, DirectX 11 Video playback improvements, and further GPU usage refinements to improve desktop responsiveness, Video RAM usage, and crash prevention and recovery, as detailed in this Microsoft Article.

You will frequently see references to DirectX when Windows graphics and audio capabilities are discussed. DirectX is the Application Programming Interface (API) built into Windows for handling multimedia. It has various components, including Direct3D for 3D graphics, DirectSound3D for 3D audio, and more recently, Direct2D for 2D graphics. Windows XP only supported versions of DirectX up to DirectX 9. Windows Vista introduced a major revision of DirectX called DirectX 10, which was subsequently updated to DirectX 10.1 when Vista Service Pack 1 was released. Windows 7 introduced built-in support for DirectX 11, which added a range of important new features, as detailed in this Microsoft Article. Windows 8 upgrades DirectX to version 11.1, adding new functionality that developers can take advantage of, as detailed in this Microsoft Article.

To enable all of the benefits described above, you need to use Windows 8-specific WDDM 1.2 graphics drivers - see the Windows Drivers chapter. However, WDDM 1.0 and 1.1 graphics drivers - essentially Vista and Windows 7 drivers - will still work under Windows 8. Similarly, programs which use earlier versions of DirectX prior to 11.1 will work under Windows 8, but a program that supports DirectX 11 or 11.1 has the potential for improved performance and functionality under Windows 8.

In Windows 8, there are essentially two separate interfaces: the more traditional Windows Desktop interface, similar to that found in previous versions of Windows; and the new Metro interface, as seen on the Start Screen. This chapter begins by covering the features of the Metro interface.

< METRO

First introduced for Windows Phone and Xbox 360, the interface design initially codenamed "Metro" is now fully incorporated into Windows 8. Due to potential legal issues, Microsoft has dropped official usage of the term Metro. The design language is now referred to in various ways, including "Modern UI", and "Microsoft Design Language", and Metro apps are also referred to as Windows 8 Store Apps. For the sake of brevity and to prevent confusion, in this book I have retained the more commonly-used Metro name to refer to this design philosophy and the apps based on it.

In Windows 8, the Metro interface is characterized by large, flat multi-colored tiles against a generally non-distracting background. The Start Screen, which appears after you sign in to Windows 8, is the most prominent example of a Metro-based interface, and is the main Metro environment. The Metro design philosophy is aimed primarily at touch-capable mobile devices, such as tablets and smart phones. This is why it features a larger interface to make touch selection easier on smaller screens; the removal of fancy graphical effects to reduce processing load, and hence increase both responsiveness and battery life on mobile devices; and the replacement of complex hierarchical menus, such as those found on right-click context menus, with simpler icon-based menus typically hidden by default and activated via certain hotspots on the screen, again to cater to touch devices. Details of the rationale behind the Metro design for Windows 8 are in this Microsoft Article.

Since the Metro interface is specifically designed for lower-powered devices, it will run on any system that meets the basic system requirements for Windows 8, noted under the Prior to Installation section of the Windows Installation chapter. Metro is also designed to be scalable, and will make use of greater screen space when available. However, the Metro UI will not appear if you are running a PC or device with a screen resolution lower than 1024x768, and some Metro UI functionality will not be available if your resolution is below 1366x768. More details are in this Microsoft Article.

The traditional Windows Desktop is still available in Windows 8, and can be accessed by clicking the Desktop tile on the Start Screen. The desktop-related features are covered in full detail in the Desktop section later in this chapter.

There is a distinction between native Metro applications, which are typically referred to as Metro apps, or just apps, and general Windows applications, usually referred to as Desktop applications, or simply programs. The key difference is that Metro apps can only be downloaded from the Windows Store, can only run in the Metro environment, and are generally designed to be full screen and touch-centric. Programs on the other hand can be downloaded or installed from a range of places, and run only on the Windows Desktop environment, although they can be pinned to the Start Screen and launched via Metro.

Metro has a range of unique features which are covered further below.

START SCREEN

A replacement for the Start Button and Start Menu found at the bottom left of the screen in previous versions of Windows, the Start Screen is a collection of pinned applications shown as large colored tiles. The Start Screen always appears at startup right after your account login, and cannot be skipped or disabled by default.

The Start Screen can be accessed from the Desktop at any time by:

- Pressing the WINDOWS key.
- Moving your mouse to the bottom left corner of the Desktop and clicking the Start thumbnail that appears.
- Activating the Charms menu by moving your mouse to the right top or bottom corner of the screen and then clicking the Window Pane (Start) icon.
- Moving your mouse to the top left corner of the Desktop and then moving downward and selecting Start. This only works if a Metro app is open in the background.

The Start Screen is designed to be the central point for accessing frequently used applications, similar to the programs listed on the Start Menu in previous versions of Windows. When a Metro app is launched, it will be launched within the Metro environment. When a Desktop app is launched from the Start Screen, you will immediately be switched to the Desktop environment.

The Start Screen also consolidates the Search Box functionality found on the old Start Menu, by allowing users to launch a search simply by starting to type a search term while on the Start Screen, or by selecting Search on the Charms menu. See the Windows Search chapter for full details of this feature.

To customize the basic appearance of the Start Screen, you will need to go to the Charms menu, select Settings, then click on 'Change PC Settings'. Select the Personalize category on the left, and click the 'Start Screen' item at the top on the right, and you can then adjust the background image for the Start Screen, as well as the color scheme used for Metro UI elements. See the Personalize section of the PC Settings chapter for more details. More advanced customization is covered under the Metro Customization section later in this chapter.

TILES

Similar to Desktop icons, Metro has Tiles. These tiles are shown on the Start Screen, and allow for functionality beyond those of static icons. The basic function of a tile is to launch a Metro app or Desktop program. Native Metro apps usually have a larger Metro-style icon within the tile, while Desktop apps will typically have a smaller Desktop-style icon within the tile. There are various things you can do with tiles:

Pinning and Unpinning Tiles: When you install any Metro app from the Windows Store, it will automatically be added as a pinned tile on your Start Screen. When you install a standard Desktop-based program, pinned tile(s) for it may also be automatically added to the Start Screen, but you can prevent this if, during installation, you can untick any 'add Start Menu shortcuts' or similar options.

You can pin any application as a tile to the Start Screen by right-clicking on that application's Desktop icon and selecting 'Pin to Start'; or by right-clicking on an empty area of the Start Screen, selecting 'All Apps' in the App Bar, finding the relevant program or link, right-clicking on it and selecting 'Pin to Start'. If you still can't find the application, utility or setting you wish to pin, then launch a search on the Start Screen by typing its name.

You can also pin individual files, folders or locations to the Start Screen. Open File Explorer, go to the relevant file or folder, right-click on it and select 'Pin to Start'. All locations and folders, including Libraries and drives, can be pinned, but only certain file types, such as .EXE, .ZIP or .CAB, can be pinned. Clicking on a pinned folder or location will open it in File Explorer, while clicking on a pinned file will execute it.

You can even pin individual website pages as tiles to the Start Screen, by browsing to the relevant page and selecting the 'Pin Site' icon in Internet Explorer Metro, or selecting 'Add Site to Start Screen' under the Tools menu in Internet Explorer Desktop - see the Internet Explorer chapter for details.

You can unpin any pinned Start Screen tile by right-clicking on it and selecting 'Unpin from Start' in the App Bar.

Navigating Tiles: To navigate across a multi-screen collection of tiles, you can use the arrow keys, or use your Mouse Wheel to scroll across. To go up and down the hierarchy for a collection of tiles, you will need to click on a tile to go down the hierarchy, or use the Semantic Zoom function, covered in the Semantic Zoom section later in this chapter, to zoom out.

Live Tiles: If supported by a Metro app, this feature allows for a notification of current information/images from the app to be shown in real time within the app's tile on the Start Screen. It does not require that the app be launched, or be active in the background. For example, the built-in Weather app will provide the latest updates on weather conditions for your chosen location if its live tile function is enabled.

The first time a supporting Metro app is launched, the live tile functionality is enabled by default for that app. You can toggle live tiles on or off by right-clicking on the relevant app tile on the Start Screen and selecting either 'Turn live tile on' or 'Turn live tile off' as relevant in the App Bar.

Resize Tiles: The tiles on the Start Screen come in two different sizes. To see if a tile can be resized, right-click on a single tile only and select Larger or Smaller if available from the App Bar. A large tile is twice the width of a small tile, and the main reason to use a larger tile is either to make it more prominent on the Start Screen, or to provide more information and larger imagery via the Live Tiles functionality.

Organize Tiles: Tiles on the Start Screen can be rearranged at any time simply by left-clicking on and then dragging them around. You can also organize tiles into groups, by dragging a tile to the left or right until a gray column appears - this indicates that the tile will be separated slightly from the others in a new group. You can create as many tile groups as you wish.

To give a tile group a name, you need to use the Semantic Zoom feature. Zoom out on the Start Screen using CTRL+Mouse Wheel, or the small Zoom Out icon at the bottom right corner. Now right-click on any tile group and select 'Name Group' from the App Bar. The name you enter will be shown as that group's heading on the Start Screen. To remove a tile group name, follow the same procedure above, but this time leave the name box blank and click Name.

APP BAR

In previous versions of Windows, right-clicking on an item or an area would typically reveal a Context Menu with a range of different options. While context menus are still available on the Desktop in Windows 8, they take a different form in the Metro UI. Note that there is one special exception, namely the Power User Tasks Menu on the Start Screen which retains the traditional context menu interface - see the Power User Tasks Menu section later in this chapter.

The most common context menu in Metro is known as the App Bar, and can be accessed by right-clicking (or pressing WINDOWS+Z) while on the Start Screen, or within an app. The App Bar typically appears at the bottom of the screen, listing a range of options or settings that can be selected. As with traditional context menus, the available App Bar options change depending on the context in which they are used.

For example, if you right-click on a tile on the Start Screen, the App Bar will show tile customization options. If you right-click while in the Mail app, you will see options such as Sync, to synchronize (send and receive) mail. If you right-click while in the Weather app, you will see options to change settings, such as Location, or the choice to switch between Fahrenheit and Celsius.

There is also a Navigation Bar that can accompany the App Bar, as it is also triggered by right-clicking within an app. The Navigation Bar usually appears at the top of the screen, as opposed to the bottom which is reserved for the App Bar. As the name suggests, the Navigation Bar is used to navigate between different sections within an app, such as between pages, tabs or sections.

ALL APPS SCREEN

The Start Screen only shows pinned apps, so to view all installed applications you need to access the All Apps Screen by right-clicking in an empty area of the Start Screen and selecting All Apps in the App Bar, or by pressing CTRL+TAB on the Start Screen. The All Apps Screen is similar to the All Programs menu found on the Start Menu in previous versions of Windows. It lists all installed Metro apps, and any pinned Start Screen apps in alphabetical order and sorted by category. A range of your installed Desktop applications will also be shown here, however you can prevent them from being added here if, during the program's installation, you can untick any 'add Start Menu shortcuts' or 'add Start Menu folder' or similar options.

Unlike the Start Screen, you cannot move the tiles under the All Apps Screen, nor can you add, remove, rename or recategorize them. Aside from the default Windows Accessories, Windows Ease of Access and Windows System categories which list a range of built-in Windows utilities, the remaining categories will be named by the program's installer. In some cases, certain programs allow you to enter a name for the 'Start Menu Folder' during installation, in which case the name you enter will be used as the category name in the All Apps Screen. To make changes to the contents of the All Apps Screen, see the Metro Customization section later in this chapter.

SEMANTIC ZOOM

A unique feature of Metro, Semantic Zoom attempts to provide logical sorting of data by levels, so that on supported apps, zooming in doesn't simply make objects larger as with the traditional optical zoom, it actually shows sub-categories of a larger dataset.

For example, open the Store app on the Start Screen, then zoom out by using CTRL+Mouse Wheel to see an overview of all of the major categories. Use the mouse wheel by itself to scroll left or right across these categories. You can zoom back in using CTRL+Mouse Wheel, or click on a particular category. In some cases, you can go back up the hierarchy by clicking a back arrow icon that is displayed.

Note that on the Start Screen and in supported apps there is also a dedicated Zoom Out button at the bottom right corner.

USING APPS

Native Metro apps, also known as Windows 8 Store apps, function only in the Metro environment, and cannot be run under the Desktop environment. When a Metro app is launched, it will always open as a full-screen application, and the App Bar, Navigation Bar and Charms menu options will become context-sensitive, revealing any settings or options specific to that particular app.

There are some key differences between Metro apps and Desktop apps:

Installing and Uninstalling Apps: You cannot download Metro apps from anywhere but the Windows Store, which can be found as the Store app on the Start Screen. Installed Metro apps will not appear under the Programs and Features section of the Windows Control Panel, hence they cannot be uninstalled from there.

There are a range of apps that come pre-installed with Windows 8. If you want to install more, you can select from a large range by opening the Windows Store app. There are three important considerations when using the Windows Store:

- You must sign in with a Microsoft Account to download and install any app, free or not. However, you do not have to be currently logged in to Windows with a Microsoft Account. You can login to Windows with a Local Account, and then enter (or create) Microsoft Account details when prompted by the Windows Store. See the Local Account vs. Microsoft Account section of the User Accounts chapter for more details.
- Some apps are free, and some cost money. The price of an app will be shown in its description. When on an app download screen, if the app is free, you can simply click an Install button to install it; if the app requires payment, you must click on a Buy button to purchase and install it.
- App updates can only be obtained via the Windows Store. Any available updates for your installed apps are shown as a number on the Store tile on your Start Screen. They will be accessible at the top right of the Store app when it is opened, as long as you are signed in. Clicking on the Updates notice in the Store app will give you further details of the specific updates available, and allow you to select which ones to download.

§ All Metro apps must meet Certification Guidelines before they will be listed in the Windows Store. This should ensure that no app is malicious or harmful. Developers can still incorporate advertising into an app, and can also limit functionality in the free version, so there is no guarantee that an app will be useful or free from annoyances.

You can uninstall any Metro app by right-clicking on it and selecting Uninstall on the Start Screen. This includes all of the built-in apps that come with Windows 8, with the exception of the Windows Store app, and the Desktop tile.

Minimizing, Maximizing and Closing Apps: The minimize, maximize and close buttons have been removed on open apps in Metro. By default a Metro app runs completely maximized, taking up the entire screen. You cannot arbitrarily resize an open app, as Metro does not allow floating windows like those on the Desktop. You can effectively minimize an app in Metro by switching away from it, and the app will remain open in the background. You can confirm this by opening the Task Manager on the Desktop and looking under the Processes tab; the app will be listed under the Apps category as an active process if it is still open. See the Task Manager section of the Performance Measurement & Troubleshooting chapter.

To completely close an open app, while within the app you can either press ALT+F4, or move your mouse to the very top of the screen, and the cursor will turn into a hand shape. You can now left-click and drag downwards to the bottom of the screen to close the app.

Switching Apps: There are several ways to switch between open apps, the Start Screen, and the Desktop:

§ The quickest way is to press the WINDOWS key, or left-click in the bottom left corner of the screen. This switches back and forth between the last open application and the Start Screen.
§ Move your mouse to the top left corner and click the thumbnail that appears. This switches to the next open app, including the Desktop if available. Continue clicking to cycle through all open apps.
§ To select from a menu of open apps, move your mouse to the top left corner of the screen and then move it downwards to view a thumbnail menu on the side of the screen. Alternatively, press WINDOWS+TAB once or repeatedly to view and cycle through the entries in this menu.
§ To switch between all open Metro apps, as well as each individual open Desktop app, use ALT+TAB to bring up the traditional application switcher.

Note that you can disable the ability to switch to Metro apps, thereby removing any open Metro apps from the various task switching displays. The setting which controls this feature is 'Allow switching between recent apps', found by opening the Charms menu, selecting Settings, selecting 'Change PC Settings', and choosing the General category. See the PC Settings chapter for more details.

App Snap: Open apps usually take up the entire screen under Metro. But there is a way to have two Metro apps open side-by-side, or have a Metro app open alongside the Desktop environment. This is known as App Snap, and it allows one app or program to remain open in a third (or less) of the screen, while another app or program takes up the remainder of the screen.

To activate App Snap, open the app that you wish to snap to the side of the screen, then left-click at the very top of the screen and drag it to the far left or far right side as desired. Alternatively, press WINDOWS+. (i.e., the WINDOWS key plus the period key) to cycle through App Snap positions. You can now open another app - whether Metro or Desktop-based - by first going back to the Start Screen, and launching it from there. The newly launched app or Desktop program will take up the rest of the screen, while the snapped app will remain in its position.

You can return a snapped app back to full size by dragging the bar on its side out to the full width of the screen. Alternatively, you can close the snapped app as normal by dragging from the top of the screen down to the bottom. App Snap only works if your screen resolution is 1366x768 or above.

CHARMS

A new hidden menu system, known as Charms, will appear whenever you move your mouse to the bottom or top right corner of the screen, or press WINDOWS+C, whether in the Metro environment, or on the Desktop. When the Charms menu is opened, five icons will be shown: Search, Share, Start, Devices, and Settings. A clock and calendar overlay will also be shown on the left side of the screen when the Charms menu is open.

To select an option from the Charms menu, move your mouse cursor straight up or down from the corner of the screen, and left-click on the relevant icon. Alternatively, you can directly access each section of the Charms menu via keyboard shortcut:

- Search - WINDOWS+Q to search within Apps, WINDOWS+W for Settings, and WINDOWS+F for Files
- Share - WINDOWS+H
- Start - WINDOWS
- Devices - WINDOWS+K
- Settings - WINDOWS+I

Each charm is briefly covered below:

- *Search:* When selected, the Search charm takes you to the main Apps Screen, alongside which a Search bar is shown. Depending on where you trigger the Search charm from, by default any search results will initially be shown from within the Apps category, or from the individual app which is currently open. See the Windows Search chapter for more details of this functionality.
- *Share:* When in a supported app, you can select an item and click the Share charm to be presented with a range of ways in which you can share it with friends. For example, in the Photos app you can select a particular image, then click the Share charm and choose Mail to email that picture without leaving the Photos app, or having to search and find the actual picture file on your drive in order to manually attach it to an email. You cannot share from the Desktop, or from the Start Screen, if nothing is selected.
- *Start:* Selecting this charm toggles between the last open app/Desktop and the Start Screen.
- *Devices:* Whether in an app or on the Desktop, you can select an item and click the Devices charm to be presented with a list of devices to which that item or output can be sent. The range of options depends on the app and which devices you have connected to your PC. For example, when viewing a PDF file in the built-in Reader app, you can send the file to a connected printer, or to a connected second screen, by selecting the relevant device under the Devices charm.
- *Settings:* This charm opens a separate Settings bar that provides access to a range of settings for the Start Screen, Desktop or a particular app, depending upon which you are in when the Settings charm is opened. The context for the settings is denoted in gray text directly under the Settings charm heading (i.e. it will say Desktop, Start Screen, or the app's name). For example, open the Internet Explorer app from the Start Screen, and access the Settings charm. You can now select the Internet Options item to change IE Metro's settings. The bottom portion of the Settings charm is the same within all environments, and provides global Network, Volume, Screen Brightness, Notifications, Power and Keyboard Language settings. Click the 'Change PC Settings' item to access more detailed global settings, as covered in the PC Settings chapter.

If you open the Charms menu but don't wish to select anything, press ESC, or just move your mouse away from it, and it will become hidden again. To disable the Charms menu, see the Metro Customization section further below.

POWER USER TASKS MENU

Traditional context menus have been removed in the Metro environment, replaced with context sensitive interfaces such as the App Bar and Charms menu. There is one significant traditional context menu that remains under Metro, and is also available in the Desktop environment: the Power User Tasks Menu. Despite its name, it isn't just for power users; it provides quick access to a range of useful tools.

To access the Power User Tasks Menu, right-click on the bottom left corner of the screen, or press WINDOWS+X. The menu that appears lets you open a range of commonly-used Windows features with a single click, though none of the features are unique to this menu. See the relevant sections and chapters throughout this book for descriptions of these features.

POWER OPTIONS

As a final note on the Metro interface, many new Windows 8 users will quickly become aware that the power options (shutdown, restart, sleep) are absent from the Start Screen and Desktop. These have been moved, and can now be accessed in a range of ways:

§ Open the Charms charm and select Settings, or press WINDOWS+I, and then click the Power icon.
§ Press CTRL+ALT+DEL and then click the Power icon in the bottom right corner.
§ Press ALT+F4 while on the Windows Desktop to access a Shutdown selection menu.

To make access to these options much quicker, you can create custom icons to initiate shutdown, restart, sleep or lock, and pin them to the Desktop, Start Screen or Taskbar. See the Icons section later in this chapter for details.

< METRO CUSTOMIZATION

While you can change various aspects of the Metro interface using the settings covered in the previous section, as well as in the PC Settings chapter, more advanced customization is possible. This section examines such techniques.

CUSTOMIZE THE START SCREEN

By default, you are restricted to a range of pre-made patterns for the background image shown on the Start Screen. These can be selected by opening the Charms menu, going to Settings, selecting 'Change PC Settings', then selecting the Personalize category and clicking the 'Start Screen' link at the top. See the Personalize section of the PC Settings chapter for details.

If you wish to change the Start Screen background to an image of your own choosing, then you will need to use one of the following third party utilities:

ModernBack Changer

The free ModernBack Changer utility allows you customize both the background image on the Start Screen, as well as the accent colors used through Metro menus and interfaces. It is a risky procedure though, as the utility needs to patch a core Windows file, and as such it is strongly recommended that you conduct a full system backup before proceeding. Launch the utility, and for full instructions, click the 'Help+Tips' button, or on the main menu screen click the '...' link next to About and select 'Help and Tips'. Make sure to follow the instructions provided carefully.

Decor8

The Decor8 utility is only free for a trial period before requiring purchase. It allows much greater control over Start Screen customization, and is much safer and easier to use than other third party utilities. With Decor8 you can perform a range of changes, including setting a custom background image, assigning custom colors for various parts of the Metro interface, as well as controlling the number of rows of tiles available on the Start Screen. The utility is straightforward to use.

If you want to customize your Start Screen, I recommend the use of Decor8, even though it's not free. It is safer and much more customizable than other third party methods.

BYPASS THE START SCREEN

The Start Screen is shown each time you start Windows, and there are no available options to allow you to boot directly into the Desktop environment. However, there are ways to automatically bypass the Start Screen, and quickly get to the Desktop each time you start Windows or log back in.

The simplest method involves using the session restore feature built into Windows, to return to your Desktop the next time you start up. To enable this feature, do the following:

1. Open the Folder Options component of the Windows Control Panel, or click the Options button under the View menu in File Explorer.
2. Under the View tab of Folder Options, tick the 'Restore previous folder windows at log-on' box, then click Apply and OK.
3. Before shutting down at any time, leave an Explorer-based window, such as File Explorer, open.
4. Shutdown as normal, and the next time Windows starts up again, it will go to your open folder on the Desktop.

A more complex method, but one more likely to work in case the method above is patched out, involves using a script along with Task Scheduler. The first step is to create the special script that will run at startup to switch to the Desktop, as follows:

1. Create a new text document by right-clicking in an empty area of a folder in File Explorer, and selecting New>Text Document.
2. Open the document with Notepad and enter the following text:

```
[Shell]
Command=2
IconFile=Explorer.exe,3

[Taskbar]
Command=ToggleDesktop
```

3. Save and exit the document, then rename it to *desktop.scf*
4. If performed correctly, the .scf portion of the extension will become hidden, and the script will have a custom Desktop icon.

Now, to automatically launch this script each time you log into Windows, we need to use the Task Scheduler functionality, as covered in the Background Tasks section of the Services chapter. Follow these steps:

5. Open Task Scheduler by going to the Start Screen, typing *taskschd.msc* and pressing Enter.
6. In the left pane, select the main 'Task Scheduler Library' folder, and in the right pane, click on 'Create Task'.
7. In the Name box, enter something suitable, like Metro Bypass.
8. Under the Triggers tab, and click the New button.
9. Select 'At log on' from the 'Begin the task' drop-down box.

10. Under the Actions tab, click the New button.
11. Click the Browse button, then go to the directory where you have stored *desktop.scf*, select it, and click Open, then click OK.
12. Under the Conditions tab, untick the Start the task only if the computer is on AC power' if you are using a battery-powered system, such as a laptop.
13. Exit Task Scheduler, as the task is now set up and active.

Restart Windows, or log on and log off, to see the task perform. After a brief moment on the Start Screen, you will automatically be taken to the Desktop.

These methods are not a perfect solution to booting into the Desktop environment. For more thorough methods of bypassing the Start Screen, and also disabling certain other Metro elements, see the utilities in the next section.

BRING BACK THE START MENU / DISABLE METRO

The most significant change in Windows 8 is the removal of the Start button and Start Menu on the Desktop, and its replacement with the full screen Start Screen Metro environment. While the Start Screen is very similar to the Start Menu in most respects, it may not be to your taste. Furthermore, some features present in the old Start Menu are not available on the Start Screen, such as a list of most recently used, or recently installed, programs.

There are also several new Metro-based features, such as the hidden menus triggered via hotspots (e.g. the Charms menu), and the fact that the Start Screen always loads up first at bootup, which may not suit individual tastes.

For users who wish to regain the Start button, and the Start Menu associated with it, and for those who want to minimize their exposure to the Metro environment in general, there are several options available:

StartMenu8

The free StartMenu8 utility provides a quick and easy method of returning the Start Menu to Windows 8. Once the utility is installed, it first provides an overview of its settings.

The Start button and Start Menu that this utility provides looks and acts very similar to that of Windows 7. To change StartMenu8's settings, right-click on the Start button. Here you can choose whether to have it run at startup, skip the Metro Start Screen at startup, disable Metro-based menus on the Desktop, and you can click the 'Customize user interface' button to access more settings.

StartMenu8 is a simple but handy tool, providing a good-looking Start Menu and Start button interface, at no cost. Its only drawback is that it is not highly customizable.

Classic Shell

The free Classic Shell utility is a more comprehensive tool that has been around for several years, initially designed to return the classic Start Menu back into earlier versions of Windows. It can now be used to both regain the Start Menu in Windows 8, and also perform a range of other interface changes.

Download the utility, and during installation pay attention to the options available during the custom setup. I recommend only allowing the Classic Start Menu option to install, and clicking on and selecting 'Entire feature will be unavailable' for the other options, as the rest are unnecessary.

Once the utility is installed, a custom Start button will now appear in your Taskbar on the Desktop. Click on it to access the settings menus. Select the 'All settings' item at the bottom, and then go through each tab, choosing the appearance and functionality of this new Start Menu to suit your taste. To access these settings again at any time in the future, just right-click on the Start button and select Settings. Note that by default, the Metro Start Screen is disabled once Classic Shell is installed, as are the usual methods of accessing it, such as pressing the WINDOWS key. To access the Start Screen, open the Charms menu and select Start.

There is tremendous scope for customization in the utility, including the ability to use a custom image for the Start button under the 'Start Button' tab, and the ability to skip the Metro Start Screen, and disable the "active corners" that trigger the Metro-based Charms and App Switcher menus, under the 'Windows 8 Settings' tab.

Two key points of difference between the real Start Menu and the Classic Shell version is that the Search functionality looks a bit different, and is not as comprehensive as the one on the Start Screen; and the programs listing is separated into Programs for Desktop programs, and Apps, for Metro apps. For the most part, Classic Shell provides a good approximation of the Start Menu from whichever previous version of Windows that you prefer, is highly customizable, safe and free to use.

Start8

The Start8 utility is another Start Menu replacement utility, but is only free for a trial period before requiring purchase.

Upon installing Start8, you will be presented with a configuration window that gives you a range of customization options. While there are not as many options as in Classic Shell, there should still be sufficient choices to make the Start Menu and Start button look and act the way you want it. You can return to these options at any time by right-clicking on the Start button and selecting 'Configure Start8'.

The key difference between Classic Shell and Start8 is that Start8 will almost exactly emulate the Start Menu in Windows 7. Every aspect of the previous Start Menu's appearance and functionality is virtually identical. Even the Search Box interface and resulting search output is more functional than other Start Menu alternatives, providing a duplicate of the one in Windows 7.

Additional features include options to go straight to the Desktop upon Windows startup, disabling the hotspots that trigger hidden menus, control over Taskbar translucency, and how Metro apps transition to the Desktop.

Start8 is very safe, easy to use, and contains a wide range of features. The only real drawback is that it is not free, although at the time of writing, the purchase price is quite low.

It should be noted that there are a large number of Start Menu replacement/Metro interface disabling utilities flooding the Internet. Some are free, some require payment. I've only provided three utilities above, as they appear to be the best of the bunch, and should cover all of your needs. If necessary, try each one out to see which you prefer, as none of them will leave a mess on your system upon being uninstalled.

I recommend Classic Shell as the best compromise, given it has the largest amount of customization potential and is free. On the other hand, if you want a perfect fuss-free simulation of the Windows 7 Start Menu in Windows 8, and don't have the time to undertake extensive customization, then Start8 is well worth the purchase price.

EDIT THE POWER USER TASKS MENU

The Power User Tasks Menu, also known as the Win+X menu because it can be triggered by pressing WINDOWS+X, appears when you right-click on the bottom left corner of the screen in either the Desktop or Metro environments. By default it contains a range of links to utilities and Windows features that more advanced users would commonly access.

You can edit the contents of this menu by going to the following directory:

\Users\[username]\AppData\Local\Microsoft\Windows\WinX

Under this directory, you will find three separate folders, named *Group1*, *Group2* and *Group3*. Each folder contains a set of shortcuts that appear as links in the Power User Tasks Menu. You can delete shortcuts here, then restart Windows, or logon and logoff, to see that the option has been removed from the menu. However you cannot add shortcuts here in the normal manner, as they will not appear in the menu.

The free WinX Menu Editor utility provides a quick and easy method for successfully editing the Power User Tasks Menu. Download the utility, extract the contents and launch the *WinXEditor.exe* file under the *x86* folder for 32-bit systems, or the one under the *x64* folder for 64-bit systems. The editor window that opens allows you to add, remove, rearrange or rename the entries in this menu. Once done, click the 'Restart Explorer' button to see the changes reflected in the menu.

CUSTOMIZE THE ALL APPS SCREEN

The All Apps Screen is shown when you right-click on the Start Screen and select the 'All Apps' button in the App Bar at the bottom of the screen. This takes you to a screen that displays all of your installed Metro apps and Desktop programs. It is similar to the All Programs function of the Start Menu in previous versions of Windows, but does not provide the same capability to customize what is shown.

To customize the All Apps screen, go to the following folder in File Explorer:

\ProgramData\Microsoft\Windows\Start Menu\Programs

Here you will see the bulk of your installed programs, sorted by folders which correspond to the category headers on the All Apps screen. You can delete the shortcut for any programs that you do not wish to show on the All Apps screen, and it should be removed from All Apps. Similarly, you can add program shortcuts here and they will appear in All Apps. You can edit category headers as well if you wish, by editing the name of the relevant folder here.

In some cases, certain programs or categories may not be found here. Look in the relevant user folder instead:

\Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs

Furthermore, to properly see any changes reflected on the All Apps screen, you will need to delete the icon cache. Go to the *\Users\[username]\AppData\Local* directory under your personal folders and delete the *IconCache.db* file. Then restart Windows, or logon and logoff, and the changes should be reflected properly on the All Apps Screen when next you open it.

CHANGE START SCREEN ANIMATIONS

The Start Screen displays a pronounced animation effect when it first loads up after Windows startup. Subsequently, whenever you switch to it, it shows a smaller animation. If you want to control how the animation effect is used on the Start Screen, go to the following location in the Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ImmersiveShell\Grid
]

Launcher_SessionLoginAnimation_OnShow=0
```

The DWORD above does not exist by default. If it is created and set to =1, the Start Screen will always use the more pronounced startup animation effect whenever it is switched to during a Windows session.

You can also control individual animation effects for the Start Screen by creating the following additional new DWORDS under the key above:

```
Launcher_SessionLogin_Icon_Offset=3000
```

The value above determines from how far the user account image at the top right will slide across the screen. Higher values mean the image will start further away and slide all the way to its resting place on the right.

```
Launcher_SessionLogin_IconText_Offset=100
```

The value above determines from how far the user account name at the top right, next to the account image, will slide across the screen. Higher values mean the user name will start further away and slide all the way to its resting place on the right.

```
Launcher_SessionLogin_Tower_Offset=500
Launcher_SessionLogin_IndividualTower_Offset=3000
```

The value above control how the tiles are spread across the screen. Higher values for the first and lower for the second will mean the tiles travel from right to left, and the opposite if the values are switched.

Experiment with the variables above to achieve the effect you are after. Note that you must have the `Launcher_SessionLoginAnimation_OnShow=1` for any of the additional animation variables to work when switching to the Start Screen. Furthermore, all values must be assigned in Decimal view, not Hexadecimal view. To undo the changes, delete all of these newly created DWORDS to revert back to normal animation for the Start Screen.

AERO GLASS

The full Windows Aero interface with its glass-like transparencies, used in Windows Vista and Windows 7, is no longer available in Windows 8. There is no workaround to re-enabling it at the moment. There are several utilities and methods that purport to reinstate Aero, but fail to do so in any meaningful way. Given changes that Microsoft has made to the Desktop Windows Manager in the retail version of Windows 8, the source code required for the Aero Glass effects is missing from Windows. The best that can be achieved at the time of writing is a very buggy form of basic transparency that is not particularly pleasant or useful.

DESKTOP GADGETS

Gadgets are small programs that display a range of useful information at a glance on the Desktop. They can also provide easier access to various features. Windows 8 has removed Desktop Gadgets, and the closest replacement for this functionality is the Live Tiles feature on the Start Screen. Microsoft has also issued a Security Warning that the Gadgets platform in Windows Vista and Windows 7 is open to abuse from malicious Gadgets, which has further hastened their demise.

For those who have trusted Gadgets they wish to install, there is a way to restore this functionality in Windows 8. It requires the use of a third party utility, as covered below:

Windows 8 Desktop Gadgets

The free Windows 8 Desktop Gadgets utility is relatively straightforward to use. Launch the utility, follow the prompts, and upon completion, right-click on your Desktop and select the new Gadgets menu item. This will launch the Gadgets window, letting you choose from several built-in Gadgets which used to be provided with earlier versions of Windows. Double-click on the relevant Gadget you wish to use, and it will be added to your Desktop. Right-click on each Desktop Gadget for configuration options.

8GadgetPack

The free 8GadgetPack utility recreates the ability to run Gadgets in Windows 8's Desktop environment, similar to the utility above. However, 8GadgetPack comes with a wider selection of custom gadgets, many of which were never originally included with Windows. After installation, right-click on the Desktop and select Gadgets. Note that the Gadget window which opens has two pages of Gadgets, so click the button on the top left to scroll to the second page. Select each Gadget and click the 'Show details' link at the bottom if you want to see more information about it.

Additional Gadgets

You can download additional Gadgets, which come in the form of .GADGET files. To install a .GADGET file, first open the Gadget window using one of the utilities above, then double-click on the .GADGET file to install it. It should be added to your Desktop, but it will also be added to your Gadgets window, from where you can right-click on it and select Add to add it to your Desktop if needed. To remove a Gadget from the Desktop, hover your mouse cursor over the Gadget and click the X which appears at the top right of the Gadget. To uninstall a Gadget, right-click on it in the Gadgets window and select Uninstall.

The links below are to a third party Gadget site that should be safe to use. To be sure, first download any Gadget and scan it with a malware scanner before installing it. Some of the Gadgets I recommend that you try include:

- iStat CPU - This CPU meter shows the CPU usage for every core of your CPU, up to 16 cores, in a clean and simple interface. Alternatively you can try this mCPU Meter which also provides a memory usage bar along with CPU usage.
- iStat Wireless - Displays the signal strength for wireless connections. You can also use this NoteBook Info Gadget which provides similar functionality, but also has other features such as battery charge.
- NASA TV - Provides a feed from NASA TV on your Desktop. Also see Full Sun and Full Moon for interesting space-related Gadgets.
- BarCode Clock - This Gadget is one of the many variations of the clock-based Gadgets available, along with other interesting clocks such as Sonar Clock.

You can also download and use the free Amnesty Generator to allow you to make custom Gadgets out of a range of existing small programs called widgets from around the web.

Bear in mind that not all Gadgets may be useful, efficient or safe to install. Download the Gadget and scan it with a malware scanner before installing. Also use Task Manager to briefly check your CPU and Memory usage, as some user-made Gadgets might be resource intensive, outweighing their usefulness. If in any doubt, do not install a Gadget.

< DESKTOP

The Windows Desktop refers to the traditional interface which has been around since the early days of Windows. It features a large open "desktop" area, containing various icons, upon which windows of differing sizes can be opened and moved around, along with a long bar at the bottom of the screen.

The Windows Desktop in Windows 8 does not load by default at startup, and will only load up when triggered from the Start Screen by launching a Desktop-based application, by clicking the Desktop tile, or by pressing WINDOWS+D. The Desktop in Windows 8 remains similar to previous versions of Windows, but elements of its interface have been changed to more closely align with Metro design principles. These changes include:

§ Removal of the Start Button and Start Menu from the Taskbar, replaced by the Start Screen thumbnail icon that appears when the mouse is hovered over the bottom left corner.
§ The Windows Aero Glass transparent glass-like interface elements used in Windows Vista and 7 have also been removed, replaced with flat, monochromatic, opaque, sharp-edged tile-like windows. Note however that the Taskbar does retain basic transparency.
§ Most Windows Aero-related 2D/3D features, such as Flip 3D and Aero Peek, have also been removed.
§ Desktop Gadgets have been removed.
§ The Ribbon interface is implemented more widely, most prominently in File Explorer.

In most other respects, the Desktop retains the same functionality it had in Windows 7, and much of the functionality of earlier Windows versions.

First we cover a few of the general Desktop features that have been altered slightly due to the removal of Aero Glass:

Task Switcher: The ALT+TAB task switching function available in previous versions of Windows is still available, and retains the thumbnail preview aspect. The Flip 3D task switcher has been removed, and in its place, pressing WINDOWS+TAB will now open a Metro-based task switching panel on the left side of the screen.

Thumbnail Previews: This feature provides a small thumbnail image of the current contents of an open application when you hover over its icon on the Taskbar, or when using ALT+TAB or WINDOWS+TAB task switching. While the backgrounds to thumbnail previews are no longer transparent, it retains most of its useful functionality as detailed in the Taskbar section later in this chapter.

Snap: Known as Aero Snap in Windows 7, this feature allows you to quickly resize an open window to a preset size by dragging the window in a particular direction. Drag an open window to the far left or far right edge of the screen and it automatically resizes to take up exactly half the screen. Drag an open window to the very top of the screen and it instantly becomes maximized. Drag a maximized window downwards and it converts to its regular windowed mode. This can be very useful in particular if you want to have two windows arranged exactly side by side on a widescreen monitor, because you can drag one window to the far right, and the other to the far left, and they will be resized to sit next to each other. You can achieve the same functionality for open windows by right-clicking on an empty area of the Taskbar and selecting the 'Show windows side by side'.

If you wish to disable Snap, go to the Windows Control Panel, select Ease of Access Center, then select 'Make the mouse easier to use'. Tick the 'Prevent windows from being automatically arranged when moved to the edge of the screen' box, then click the Apply button.

Shake: Formerly known as Aero Shake, this feature is based on the same basic principle as Snap. It allows you to quickly minimize all open windows except one using mouse gestures. Left click on the title bar of the window of your choice, and without letting go of the mouse button, rapidly shake it left and right, and/or up and down repeatedly, to minimize all other open windows at once. Doing the same thing again will restore all the windows to their previous state.

If you wish to disable Shake, you can do so by going to the following location in the Windows Registry:

```
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows]
```

Right-click on the subfolder above and create a New>Key called `Explorer` - it should look like this:

```
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer]

NoWindowMinimizingShortcuts=1
```

Create the DWORD above under the new location, and set it =1 to disable Shake. Restart Windows for the change to take effect. If you want to undo this change, simply delete the value above and restart Windows.

Peek: Normally, you can minimize all open windows at once by left-clicking on the far right area of the Taskbar. This will instantly hide everything except for the Desktop itself. Clicking on the same button will maximize all hidden windows. Formerly known as Aero Peek, there is also a feature that allows you to temporarily view the Desktop, devoid of any open windows, only for as long as you hover your mouse over the same area at the far right of the Taskbar. Due to the demise of Aero Glass, and the fact that it occupies the same space as one of the trigger points for the Charms menu, Peek is disabled by default in Windows 8. To activate it, right-click on the far right of the Taskbar, to the right of the clock, and tick the 'Peek at desktop' option. Alternatively, you can go to the Windows Control Panel, select the Taskbar component, and under the Taskbar tab, tick the 'Use Peek to preview the desktop...' box, then click Apply. Once activated, moving your mouse over the far right area of the Taskbar will let you momentarily take a "peek" at the Desktop without being obscured by any open windows.

The following sections look at each of the different components of the Desktop in more detail.

< PERSONALIZATION

This component is the central location for customizing a range of graphics and sound features which have a noticeable impact on the general appearance of the Windows Desktop. To access it, either go to the Windows Control Panel and select Personalization, or right-click on an empty area of the Desktop and select Personalize. Below are the various settings for this feature.

CHANGE THE VISUALS AND SOUND ON YOUR COMPUTER

Here you can select a particular theme for the Windows Desktop, which includes a combination of four individual components: Desktop Background, Color, Sounds and Screen Saver. There are several preset themes displayed in the main pane of Personalization, under Windows Default Themes and High Contrast Themes. Aero Glass Themes, as mentioned earlier, are no longer available.

You are not restricted to the preset themes displayed here, as you can download an additional range of free official Windows 8 themes by clicking the 'Get more themes online' link shown here, or by checking the user-made themes and wallpapers available at sites such as Deviantart. Most Windows 8 themes come in the form of a new .DESKTHEMEPACK file format, which you can simply double-click on to automatically install and apply. The key difference between the previous .THEMEPACK format used in Windows 7 and the new .DESKTHEMEPACK format is that you can still install .THEMEPACK files on Windows 8, but you can't install .DESKTHEMEPACK files on Windows 7. Furthermore, .DESKTHEMEPACK files now typically come with panoramic wallpapers (approx. 3840x1200) to support multi-monitor display setups.

Anytime you customize a theme, or install a custom theme, it will appear under the 'My Themes' category at the top of the Themes pane. You can switch to any theme at any time simply by selecting it, and the appropriate changes will be implemented on the Desktop straight away.

You don't need to use preset themes or downloaded theme packs if you want to customize your Desktop. You can alter each of the four basic components of a theme by clicking the relevant links at the bottom of the Personalization window. These are covered in separate sections below.

DESKTOP BACKGROUND

You can set an image for your Desktop background by going to the Windows Control Panel, opening Personalization and clicking the 'Desktop Background' link. By default you will see a range of Windows backgrounds, also known as Wallpapers, which come with all versions of Windows 8. These are stored under the *\Windows\Web\Wallpaper* directory under various theme-based categories. You can choose a new location from which to select a Wallpaper by clicking the Picture Location box, and selecting a location such as your Pictures Library. You can also choose the 'Solid Colors' category here if you wish to set a plain solid color Desktop background. Click the Browse button if you want to go to a specific directory which holds an image file you wish to set as a background. Note that you can change the size of the wallpaper thumbnail icons displayed here the same as in Icon view in File Explorer - by holding down the CTRL key and scrolling the Mouse Wheel up or down.

The common image formats can all be used for Desktop backgrounds, including .BMP, .PNG, .GIF and .JPG. However, depending on the method you use to apply a wallpaper, Windows may automatically convert other formats to .JPG before using the image as a wallpaper. This is because the image actually being used by Windows as the current wallpaper is only a copy of the image you have selected. It can be found under the *\Users\[username]\AppData\Roaming\Microsoft\Windows\Themes* directory with the name *Transcodedwallpaper*. If you select an image format other than .JPG to set as a wallpaper, Windows will pause momentarily as it converts it to .JPG for use. This may result in a degradation of quality if you select a high quality image in a lossless format such as .PNG. You can circumvent this automatic reformatting by using the Web Browser method of applying a wallpaper, as covered further below.

You can select one or multiple wallpapers by ticking the box(es) at the top left of the wallpaper images in the main pane. If you select more than one wallpaper, Windows will automatically begin the Desktop Slideshow feature, which cycles your selected wallpapers one at a time based on the time interval you enter under the 'Change picture every' box at the bottom. If you only select a single wallpaper, this feature is not available. Importantly, under the 'Picture position' section, you can select how to scale a wallpaper to fit onto your screen. Some of these options will change the image's aspect ratio - that is, the ratio of its height to its width, which can make the image seem distorted. The available options for Picture position are:

- Fill - Alters the image size to fill the entire screen without changing the image's aspect ratio. Portions of the image may be cut off depending upon its original size.
- Fit - Alters the image size so that the entire image fits within the screen without changing the image's aspect ratio. No portions of the image will be cut off, but there may be portions of the screen with no image. Click the 'Change background color' link which becomes available to set the color for these empty portions.
- Stretch - Alters the image size so that the image fills the entire screen, with no empty areas visible. The image's aspect ratio may be altered, resulting in a potentially noticeable distortion of the image.
- Tile - Maintains the image's size and aspect ratio, and repeats the same image in a tile pattern to fill the entire screen. If the original image is larger than the screen size, this has the same effect as the Fill option.
- Center - Maintains the image's size and aspect ratio, and displays only one copy of the image in the center of the screen. Click the 'Change background color' link which becomes available to set the color for any otherwise empty portions of the screen.

For images that precisely match your monitor's current resolution, all of the options above will have no impact; the image will be displayed without changing its size or aspect ratio. Click the 'Save changes' button when done to save your Desktop background preferences to your theme.

There are several additional ways to instantly apply a Desktop background of your choice:

File Explorer: Any image file can be right-clicked on in File Explorer and most Explorer-based interfaces and the option to 'Set as desktop background' can be selected to instantly apply that image as the current wallpaper.

Windows Photo Viewer/Gallery: While looking at any image with the built-in Windows Photo Viewer, you can right-click anywhere on the image and select 'Set as desktop background', and it will instantly become the current Desktop wallpaper.

Web Browser: When viewing an image in your web browser, such as Internet Explorer, right-click on the image and select 'Set as background' (or similar). Importantly, this method also allows the image to remain in its original format, without being automatically converted to .JPG format by Windows. This means it retains maximum quality if it is in a lossless format such as .PNG.

In terms of resource usage and performance, given the improvements in Desktop graphics resource management in Windows 8, and the removal of Aero Glass, you should not be overly concerned about the type or size of wallpaper you choose on a PC. Base the decision on what you find most pleasing.

If you wish to find a new Desktop background image, you can download a wide range of free user-made wallpapers in a selection of resolutions at InterfaceLift. Another method to find wallpapers of a specific size and type is to use Google Image Search. Enter a search term for your generally desired wallpaper image, then follow the search term with one blank space and the parameter *exactly:* with your required screen resolution, and press Enter. For example, type *sky exactly:1920x1080* and press Enter to show all images that are named, or contain as part of the image, the sky, and measure exactly 1920x1080 pixels in resolution.

COLOR

This area allows you to configure the general color of the Windows Desktop components. Any changes are reflected in real-time, so select various colors and judge their visual impact on your current Desktop. The Automatic option will determine the color scheme to use based on your wallpaper, matching its general color. If you select a specific color, you can use the 'Color intensity' slider to make that color more or less saturated. If you wish to set a custom color scheme, select a color, then click the 'Show color mixer' button and a set of additional options will be displayed. The Hue slider controls the overall color tint used, as

indicated by the colors shown on the slider itself. The Saturation slider controls the richness of color, and the Brightness slider controls how light or dark the color appears.

For the High Contrast Themes, the options under the Color section change. Instead of choosing a single color, you will see options for individual customization of all of the common Windows display elements.

Note that any changes made here are only part of your current theme, and can be undone at any time by selecting another theme.

SOUNDS

Here you can customize the sounds played during various Windows events. These options are covered in detail under the Sound section later in this chapter.

SCREEN SAVER

Here you can set whether a screen saver is used. A screen saver is an animated screen that comes into effect after a period of inactivity, and is designed to prevent the screen from having any static images imprinted on it due to displaying the same image for a lengthy period of time. It's not absolutely necessary for modern LCD displays, especially as your Power Options should be set to turn off your display after a set period of inactivity - see the Power Options section under the Windows Control Panel chapter for details, and note that you can also access those options here by clicking the 'Change power settings' link at the bottom of the window.

In practice it can be useful to set a screen saver that kicks in after a period of perhaps 5 minutes of inactivity, to further safeguard against temporary image retention on LCD or Plasma displays. It can also assist in improving security by preventing others from seeing what is on your screen when you are away from the PC, and prevent attempts to access your machine in your absence.

Go through and Preview the available screen savers, then select one. I recommend the Blank screen saver, as this will use less energy, provide the most security and privacy, and prevent any potential image retention. Some screen savers can be configured further by clicking the Settings button; e.g. the Photos screensaver requires you to tell it where your desired photos are stored. Choose how long a period of inactivity is required before the screensaver commences by entering an amount in minutes in the Wait box. I recommend a short idle period of 5 minutes. Note that the screen saver will not launch itself while idle during gaming and other full-screen 3D applications, and you can also prevent the screen saver from starting when playing back media in Windows Media Player by unticking its 'Allow screen saver during playback' option, as covered in the Basic Settings section of the Windows Media Player chapter.

If you want greater security, tick the 'On resume, display logon screen' box. If ticked, whenever you move your mouse or press a key to come out of screen saver mode, you will see the logon screen. This only works to secure your system if your user account has a password. It is strongly recommended that you enable this setting if you work in an environment where the PC is accessible by other people, as it allows you to leave your machine for extended periods without manually logging out or switching off, secure in the knowledge that someone else can't access your account, or see what is on your screen, while you are away from it.

SAVING THEMES

Once you have customized the four theme elements covered in the sections above, your new theme will be in effect and will be shown with the title 'Unsaved theme' in the My Themes section of the Personalization window. To give the theme a name, and to save it and hence prevent your customizations for this theme being lost, click the 'Save theme' link. Each user's themes are saved to their *\Users\[username]\AppData\Local\Microsoft\Windows\Themes* directory, as a file with the extension

.THEME. Any installed .THEMEPACK or .DESKTHEMEPACK files may create separate directories under this folder to hold relevant resources, such as multiple custom wallpapers, sounds and logos.

If you wish to save your theme in .DESKTHEMEPACK format for backing up purposes, or to share it with other Windows 8 users, right-click on your theme in the My Theme section of Personalization and select 'Save theme for sharing', then select a name and a suitable location to save this theme. To delete any of your themes, and hence remove them from My Themes, you can right-click on it and select Delete - though you can't delete your currently used theme, so switch away from it first if you want to delete it.

CHANGE DESKTOP ICONS

When the 'Change desktop icons' link is clicked in the left pane of Personalization, a new window opens allowing you to select which common system icons appear on the Windows Desktop. By default only the Recycle Bin will appear on your Desktop, however you can remove this if you wish - though this is not recommended - by unticking the 'Recycle Bin' box and clicking the Apply button. You can also add or remove a Control Panel icon which opens the Windows Control Panel; a Computer icon which opens File Explorer at the Computer category; a User's Files icon which opens File Explorer at the current user's *\Users\[username]* folder; and a Network icon which opens File Explorer at the Network category.

You can change the appearance of any of these icons, including the Recycle Bin, by selecting the relevant icon in the main pane, then clicking the 'Change icon' button and either selecting a new icon from the list shown, or clicking the Browse button to select a custom .ICO file. See the Icons section later in this chapter for details of how to create a custom icon file.

If the 'Allow themes to change desktop icons' box is ticked, any .THEMEPACK or .DESKTHEMEPACK files you install may alter the appearance of these Desktop icons, such as a custom Recycle Bin. This should be fine, as any customizations by themes are usually done to maintain a consistent appearance, and as always you can easily undo a theme simply by selecting another one, or customizing it.

CHANGE MOUSE POINTERS

When the 'Change mouse pointers' link is clicked in the left pane of Personalization, the Mouse options window will open at the Pointers tab. These options are covered in more detail under the Mouse section of the Windows Control Panel chapter. This section allows you to either select a preset mouse pointer theme from the Scheme box, or you can highlight the individual aspects of mouse pointer appearance in the Customize pane, click the Browse button, and apply a new appearance for that particular action. When done, you can click the 'Save As' button to save your new mouse pointer theme as a custom Scheme.

You can also choose to enable or disable a shadow displayed under the mouse cursor by ticking or unticking the 'Enable pointer shadow' box.

VISUAL EFFECTS

You can adjust a range of additional settings that help to personalize your Windows Desktop by going to the Windows Control Panel, selecting the System component, clicking the 'Advanced system settings' link on the left, and under the Advanced tab of the window that opens, clicking the Settings button under the Performance section. These settings are found here, rather than under Personalization, because they have some impact on the overall performance and responsiveness of the Windows interface. Of relevance to this chapter is the contents of the Visual Effects tab; the Advanced tab is covered under the Windows Memory Management section of the Memory Optimization chapter, while the Data Execution Prevention tab is covered under the Data Execution Prevention section of the Security chapter.

Under the Visual Effects tab you can select a range of graphical effects to enable or disable for the Windows Desktop. Many of these can already be adjusted under different sections of Windows, such as 'Show

shadows under mouse pointer' which is available under the Mouse Options in the Windows Control Panel, or 'Enable Peek' which is available under the Taskbar component of Windows Control Panel. This is why you may find some of these options are already ticked or unticked, because you may have adjusted them elsewhere. However there are a range of unique items here, such as 'Animations in the taskbar', which if unticked, removes all animated effects from the Taskbar. For example, with this option unticked, Taskbar Thumbnail Previews and Jump Lists may feel more responsive because there is no animated popup or transition effect applied to their display.

Adjust these settings to suit your taste, and if you are running a slower system, you may wish to disable a range of these features to increase responsiveness. On most desktop PCs, most if not all of these effects can be kept enabled with minimal performance impact because of the resource usage improvements in Windows Desktop rendering implemented as of Windows 7, as well as the removal of Aero Glass in Windows 8.

< DISPLAY SETTINGS

This section allows you to configure the settings related to the way in which Windows displays its output on your monitor, including resolution, orientation, color, text size and clarity. To access these settings, go to the Windows Control Panel and select the Display component.

On the main Display window, you can select the overall size of the Windows interface. The default is 100%, however you can choose Medium (125% of original size), or Larger (150% of original size), which will make the interface - including text and images - larger. To set a custom percentage, click the 'Custom sizing options' link. In the window that opens, you can adjust the scaling to a different size. Select a new percentage from the drop down box shown, or grab the ruler displayed and drag it to the right. The text at the bottom of the window will change to reflect the impact of your selection, and when you are comfortable with the new text size, click OK. The 'Use Windows XP style Scaling' box can be ticked if you want to prevent old programs, which were not originally designed to work with Windows 8's scaling method, from showing blurry fonts. Once done, click OK then click Apply. Your custom selection will be shown and selected in the main Display window, and you will need to logoff and logon, or restart Windows for the changes to come into effect.

This method is recommended over reducing your screen resolution if you wish to increase the size of the Windows interface, because for maximum clarity you should always be running at your monitor's native resolution, as covered further below. If you only wish to temporarily increase the size of particular portions of the screen, see the Magnifier section later in this chapter.

If you don't wish to alter the size of the entire interface, and only want to change the text size of particular elements of Windows, then you can use the new options under the 'Change the text size only' section here to do just that. For example, if you want to increase the size of the text shown under icons, then select Icons here, and in the box next to it, choose a font size in points. You can also make the text element stronger by ticking the Bold box.

SCREEN RESOLUTION

If you click the 'Adjust resolution' link on the left side of the main Display window, you will be shown Screen Resolution settings that affect the way the image is displayed on your monitor. You can also access this screen directly at any time by right-clicking on an empty area of the Desktop and selecting 'Screen resolution'.

Display: The Display drop down box should automatically show your current monitor. If the display is not detected properly, or the other settings in this section appear incorrect for your display type, then you will need to ensure that the display is connected firmly to your PC, preferably using the highest quality cable type, typically DVI or HDMI.

If your monitor is not being detected correctly, then click the Detect button again to force detection. Your primary monitor should be shown with a '1' in the middle of it in the graphic display, and numbered 1 under the Display drop-down box. Clicking the 'Identify Monitors' button will briefly display a large white numeral on the screen to show which is the primary monitor (denoted by the number 1) and which is the secondary (number 2), and so forth. The main reason for problematic detection of monitors is due to a lack of appropriate drivers, or incorrect driver settings - refer to the Windows Drivers chapter.

Resolution: Resolution is the level of image detail shown on the screen, based on the number of image samples taken as pixels in the format *Width x Height* (e.g. 1920 pixels x 1200 pixels). The resolution selected here impacts on the Windows Desktop and Metro environments. It affects any applications that run as windows on the Desktop, as well as fullscreen Metro apps. It does not apply to Desktop programs that run in separate full screen mode and have their own resolution settings, such as games. When selecting your Resolution, if you are using a fixed-pixel display, such as an LCD or Plasma monitor, then try to match the Desktop resolution with the monitor's native resolution. This is usually the maximum possible resolution on the slider, and is tagged as 'Recommended' by Windows. Selecting a resolution below your native resolution can result in blurry graphics and text, or large black bars around the edges of the image. Only the native resolution provides the sharpest and most accurate display output while filling the entire screen. More details can be found under the Resolution section of the Gamer's Graphics & Display Settings guide. If you find the native resolution results in an interface or text that is too small, you can adjust this, as covered further above, by clicking the 'Make text and other items larger or smaller' link.

Orientation: This option determines the direction in which the screen image is displayed. Landscape is the default for most monitors, where the width of the image is greater than its height. Portrait turns the image 90 degrees anti-clockwise, so that its height is greater than its width. Landscape (flipped) and Portrait (flipped) are the same as their normal counterparts, except the image is the reverse of how it would normally appear, i.e. in Landscape (flipped), text runs backwards from right to left, and the image is upside down. The primary use for these options is to provide the appropriate output for projectors and monitors that can be rotated appropriately.

If you click the 'Advanced settings' link, a new window opens containing a range of additional settings. Some of these will differ from system to system based on your graphics hardware. The common elements are covered below:

Adapter: Provides more detailed information about your graphics hardware, typically a graphics card, including its name, chipset type, and available memory. See the System Specifications chapter for utilities that can provide much greater information than listed here.

Monitor: This tab provides details of your monitor, and has an important monitor-specific setting: Screen refresh rate. The Refresh Rate is the number of times per second (measured in Hertz) that your monitor refreshes the currently displayed image. It is a complex setting requiring detailed knowledge before adjustment, so read the link above for more details, and also make sure to keep the 'Hide modes that this monitor cannot display' box ticked. Choosing a refresh rate that is not supported by your monitor can result in a blank image.

Color Management: These settings are covered under the Color Management section in the Windows Control Panel chapter, but you should refer to the Calibrate Color section below for a user-friendly method of configuring color output on your system.

If you have made any changes in this window, click Apply then click OK to close it, and do the same in the main Screen Resolution window as well.

CALIBRATE COLOR

When you click the 'Calibrate Color' link in the left pane of the Display window, you will open the Display Color Calibration feature, introduced in Windows 7. You can access this feature directly at any time by going to the Start Screen, typing *dccw* and pressing Enter. This feature is designed to ensure that your monitor displays content as closely as possible to the way content creators intended it to be seen. When launched, it opens a wizard that runs through a series of steps, with full instructions provided, allowing you to adjust various settings on your monitor, such as contrast and brightness, which determine image accuracy. When the calibration process is completed, the utility allows you to quickly compare your previous settings with your new ones to see the difference. If you don't wish to keep the new settings, you can simply Cancel out of the calibration at any time, even at the end, and the settings will not be saved or applied. It is recommended that you run through this calibration routine, as aside from improving image and color reproduction quality, it can also prevent damage to your eyes through overly bright display settings.

ADJUST CLEARTYPE TEXT

Clicking the 'Adjust ClearType text' link on the left side of the main Display window will open the ClearType Text Tuner utility, an automated utility for adjusting the legibility of fonts on LCD monitors. This wizard is fairly straightforward, and ClearType is covered in more detail under the Fonts section later in this chapter.

MULTIPLE MONITORS

Multiple monitor usage is not covered in detail in this book. This section has a brief look at multi-monitor support under Windows 8, which has been further improved since Windows 7. If you run a dual or multiple monitor configuration in Windows 8, it should now be correctly configured automatically, without requiring user input. New features include:

- Better edge detection on each separate display, as long as you hover your mouse cursor right near the edge and hold it there for a few seconds.
  Configuration of the Taskbar on a per-screen basis, by right-clicking on the Taskbar, selecting properties and choosing from the options under the 'Show taskbar buttons on' section.
- The addition of keyboard shortcuts for managing Metro apps on multi-monitor setups: WINDOWS+Arrow Keys to control the App Snap feature; WINDOWS+Page Up or WINDOWS+Page Down to move fullscreen Metro apps from one display to another.
- When setting a Desktop wallpaper under the Desktop Background section of the Personalization screen, you can right-click on any wallpaper thumbnail shown and select whether to set it as a background for all monitors, or choose a different background for each individual screen.

When temporarily or permanently connecting a second display to your system, you can also press WINDOWS+P to open a quick menu for selecting which display(s) to send the output to at any time. That is, whether you want to only display the image on one of the screens, duplicate the image on both screens, or extend the Desktop/Start Screen across both displays.

There are a range of additional multi-monitor features that you can access using the UltraMon utility. The tool is free for a trial period if you wish to see if it provides any features you need. For the most part, the built-in features of Windows 8 now cater to most multi-monitor needs.

MAGNIFIER

Instead of increasing your interface size or lowering your resolution, if you simply want to zoom in on particular portions of the screen from time to time, a quick solution is to use the Magnifier utility. To open this utility, go to the Start Screen, type *magnifier* and press Enter, or press WINDOWS + + (the plus key twice)

to initiate Magnifier at any time. There are three modes for the Magnifier tool which can be selected under the Views menu of the utility:

§ Full screen mode - This mode makes the entire screen larger or smaller by using the + and - buttons on the utility, or by pressing the WINDOWS key and either the + or - key at the same time. Move your mouse around to the edges of the screen to move the Magnifier's focus.
§ Lens mode - In this mode a set lens area is provided, and pressing the same keys as in Full screen mode above facilitates showing a zoomed portion of the screen only in the lens area.
§ Docked mode - In this mode a small window opens at the top of the screen, and will display the zoomed contents of the area around your mouse cursor.

The Magnifier works on both the Desktop and Metro environments.

< TASKBAR

The Taskbar is the long bar that sits at the bottom of the screen on the Windows Desktop. Its functionality was substantially altered as of Windows 7, merging the Quick Launch functionality of the Taskbar in previous Windows versions with task switching, thumbnail previews and program status information, all in one location. The Taskbar is also larger than in Windows XP or Vista to increase the visibility of the icons held there, and to allow easier selection on touch-capable devices. The Taskbar allows for a wide range of useful features, as detailed below.

TASKBAR ICONS & EFFECTS

The icons in the Taskbar have a range of features and effects. You can pin a program permanently to the Taskbar, but if you open any program, it will also be temporarily added to the Taskbar as an icon, not a tab. Multiple instances or multiple windows of the same program can also be represented by a single Taskbar icon. The way Windows prevents confusion is by using various effects to differentiate the status of all of the icons in the Taskbar:

§ An open program's icon will appear in the Taskbar with a transparent pane surrounding it. If a program has multiple instances of itself, or multiple windows within one instance, open, then there will be multiple layers of glass panes shown on that program's Taskbar icon.
§ The currently active program or window will have a highlighted pane surrounding its icon in the Taskbar. If you hover your mouse over an active Taskbar icon, it will also show a color-tinted highlight, matching the dominant color of the icon within the pane. Inactive programs, such as pinned items that are not open, will have no pane surrounding them, and no highlight, but if you move your mouse over them, a slight highlight appears under them.
§ When a program or window needs attention, rather than in previous Windows versions where the Taskbar tab would flash several times, the Taskbar icon now pulses gently in a soft color, requesting that the focus be shifted to it.
§ When a program is active and running a process that displays a standard progress bar, Windows will overlay a green fill effect on that program's Taskbar icon pane. For example, if you perform a lengthy file copy in File Explorer, even if the Explorer window is not visible, or is minimized, a green progress bar-like fill effect will start moving across the File Explorer folder icon pane in the Taskbar, indicating the actual progress of the task. This allows you to monitor the progress of lengthier tasks on the Taskbar, without having to keep the application window visible.

Program icons can be placed permanently on the Taskbar, just as they could in the previous Quick Launch Bar. By default Internet Explorer and File Explorer come already pinned to the Taskbar. You can pin any program, except native Metro apps, to the Taskbar by right-clicking on its Desktop or Taskbar icon or Metro tile and selecting 'Pin to Taskbar', or 'Pin this program to taskbar', depending on where the icon currently resides. Or you can simply drag and drop its icon into the Taskbar area. You can unpin any program by

right-clicking on the Taskbar icon to open its Jump List - covered below - and selecting 'Unpin this program from taskbar'. If you attempt to drag a pinned item off the Taskbar, you will only open its Jump List. You can however freely move both pinned and unpinned icons around in the Taskbar, rearranging their order at any time - this does not require you to unlock the Taskbar.

JUMP LISTS

Jump Lists are a feature of Taskbar icons introduced in Windows 7. A Jump List for any icon in the Taskbar can be opened by right-clicking on that icon, or by dragging the icon upwards. Depending on a program's level of support for this feature, a Jump List can provide several categories of options. The most basic of these are supported by all programs, and shown in the bottom area of the Jump List: the 'Close window' item to close any open windows for that program; the 'Pin this program to taskbar' or 'Unpin this program from taskbar' item, covered further above; and an item with the name of the program, designed to allow you to launch a new instance of that program. This last item requires some explanation: if a program is already open, clicking its icon in the Taskbar doesn't launch that program again, it simply switches you to its existing open window. So if you want to open another entirely new instance of that program, you can use this item in the Jump List to do so. Alternatively, you can simply click your middle mouse button on an open Taskbar icon to launch a new instance of it.

The real benefit of Jump Lists comes from additional categories that can appear in the Jump List, such as Recent, or Frequent, which show any recently/frequently opened files, folders or locations. If you want to permanently keep a particular Recent or Frequent item in a Jump List, right-click on it and select 'Pin to this list', preventing it from being bumped down and eventually moved off the list. Conversely, right-click on an item here and select 'Remove from this list' to remove it immediately from the Jump List for that program.

The number of items shown in Recent can be altered by right-clicking on an empty area of the Taskbar and selecting Properties. Under the Jump Lists tab, if the 'Store and display recently opened items in Jump Lists' box is ticked, then the Recent or Frequent category will appear in Jump Lists where relevant. If you want to disable the Recent or Frequent feature, untick the box and click Apply. If you want to temporarily clear all of your Recent or Frequent data across all Jump Lists without disabling this feature permanently, untick the box, click Apply, then tick it again and click Apply once more. You can set the maximum number of items that appear in the Recent or Frequent category for Jump Lists by altering the 'Number of recent items to display in Jump Lists' option here accordingly.

Programs that provide full support for Jump Lists have other available options and categories depending on the program. All native Windows 8 programs have full Jump List support, including Windows Media Player, Internet Explorer, and File Explorer. For example, right-click on the Internet Explorer icon in the Taskbar, and its Jump List has a link to 'Start InPrivate Browsing', or 'Reopen last session'. File Explorer allows multiple pinned instances of itself to be shown as a single icon on the Taskbar, and each location is then shown under the Pinned category for File Explorer's Jump List. See the Advanced Features section of the File Explorer chapter for ways in which you can customize the File Explorer Taskbar icon.

THUMBNAIL AND FULL SCREEN PREVIEWS

Introduced in Windows Vista, Thumbnail Previews allow you to see a real-time thumbnail-sized preview of the actual contents of an open window when you hover your mouse over that program's Taskbar icon. When a Thumbnail Preview is clicked, it will take you to that window. You can also see a full screen preview of any window by holding your mouse over its thumbnail preview - similar to Peek, it hides all other open windows to temporarily show the currently highlighted window in its actual size. You can close any open window by clicking the red 'X' at the top right of its thumbnail preview, or right-clicking on the thumbnail preview and selecting Close.

There are other subtle aspects to thumbnail previews. For example, quickly moving your focus between various thumbnail previews sees a smooth transition animation between the preview window contents. Furthermore, programs can display multiple thumbnail preview windows under a single icon in the Taskbar. This depends on appropriate program support, but one example can be seen if you open multiple tabs in Internet Explorer, then go to the Internet Explorer icon in the Taskbar - each tab will have its own thumbnail preview, allowing you to quickly switch to the appropriate tab based on selection of its preview.

Thumbnail previews are also "live" in the sense that in most cases they reflect the current contents of a window, not just a snapshot at a particular point in time. To see an example of this, play a YouTube video in your browser, then hide the browser window behind another window (don't minimize it). When you view the thumbnail preview for your browser in the Taskbar, the video will be shown as playing. Whether the thumbnail preview continues to remain live when a window is minimized depends upon the program - most minimized programs will only display the state of the window when it was last maximized, not its current state. Windows Media Player on the other hand will continue to play a video in its thumbnail preview, even when it is minimized. In fact Windows Media Player also provides a set of play/pause, back and forward controls in its thumbnail preview, as covered in the Advanced Features section of the Windows Media Player chapter. This demonstrates that a thumbnail preview can be programmed to provide a range of interactive features.

If you find that the thumbnail preview comes up too slowly or too quickly, or you don't like the animation effect, or you want to prevent the preview from being displayed altogether, you can customize it.

To disable the thumbnail preview animation/transition effects, which can help make thumbnail previews feel more responsive, go to the Windows Control Panel, select System, click the 'Advanced system settings' link on the left side, then under the Advanced tab click the Settings button under Performance. Under the Visual Effects tab untick the 'Animations in the taskbar' and click Apply to disable all animations used on the Taskbar. There is also a setting here called 'Save taskbar thumbnail previews', which appears to have no visible or functional impact on thumbnail previews. It corresponds with the `AlwaysHibernateThumbnails=1` entry in the Windows Registry, likely relating to the caching of Thumbnail Previews. When Visual Effects are set to 'best performance', this option is disabled, and when set to 'Best appearance' this option is enabled, so tick or untick it accordingly.

To increase or decrease the speed with which thumbnail previews appear when hovering your mouse over a Taskbar icon, you must alter your mouse hover time. Go to the following location in the Windows Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
ExtendedUIHoverTime=400
```

The DWORD value above must be created, and the value data (in Decimal view) determines the number of milliseconds (1,000 milliseconds = 1 second) which the mouse cursor must be hovered over an item before it triggers any relevant actions - the default is just under half a second (400 milliseconds). Assign a higher value to make it longer before a thumbnail preview appears when hovering over a Taskbar icon, and a lower value to make the thumbnail preview appear faster. To remove this customization you can delete the value above. You will need to restart Windows, or logoff and logon, for this setting to take effect.

Finally, there is no straightforward method to disable thumbnail previews altogether. The best method for preventing thumbnail previews from appearing in the Taskbar is to create the `ExtendedUIHoverTime` Registry value as covered above, and give it very high value data (e.g. =60000 which is equivalent to 1 minute), so that unless you hold your mouse over a Taskbar icon for an extended period, Taskbar thumbnail previews will effectively never be seen during normal usage.

TASKBAR CUSTOMIZATION

There are several ways to further customize the appearance and functionality of the Taskbar. In particular, if you prefer to return your Taskbar to something similar to that available in previous versions of Windows, this is possible to a certain extent. To access the Taskbar customization options, right-click in an empty area of the Taskbar and select Properties. Under the Taskbar tab there are several options relevant to customizing the Taskbar's appearance and functions:

Lock the taskbar: If ticked, this option prevents accidental movement or resizing of the Taskbar. If unticked, you can drag the Taskbar to any corner of the screen to relocate it permanently - see the Taskbar location setting further below. Furthermore, if unticked, this option allows you to increase the height of the Taskbar by dragging the top edge of the Taskbar outward. Note that locking or unlocking the Taskbar has no impact on allowing you to reorganize pinned and unpinned Taskbar icons on the Taskbar.

Auto-hide the taskbar: If this option is ticked, the Taskbar will automatically hide until you move your mouse cursor over the area where the Taskbar normally resides, whereupon it will temporarily reappear. This can increase the amount of viewable space on the Desktop, and provide a cleaner look, but can slightly reduce the speed with which you can access Taskbar icons.

Use small icons: If ticked, this option forces the Taskbar to go back to a more traditional size, reducing the size of program icons on the Taskbar, as well as cutting off the date portion of the clock in the Notification Area.

Taskbar location on screen: The Taskbar can be located on any edge of the screen, whether the default of the Bottom edge, or the Left, Right or Top edges of the screen. Select the appropriate location from the drop box here, or simply right-click on the Taskbar and make sure the 'Lock the Taskbar' item is unticked, then drag it to the desired location, then right-click on the Taskbar again and select 'Lock the Taskbar' to lock it in place.

Taskbar buttons: There are three available settings for this option. The default is 'Always combine, hide labels' which makes each program have a single Taskbar icon regardless of how many open windows it has, and no text is displayed in or beneath the icon. By selecting 'Combine when taskbar is full' or 'Never combine', this provides a similar appearance to that under previous versions of Windows: individual instances of open programs will each display a separate tab in the Taskbar, complete with a small icon and descriptive text within each tab. The difference between these last two settings is that when 'Combine when taskbar is full' is selected, multiple tabs for the same program will merge into an individual tab for that program if the Taskbar becomes full, whereas selecting the 'Never combine' setting means that as displayed tabs increase, each tab shrinks in size. Regardless of this setting, pinned programs on the Taskbar will remain as icons.

Basically, if you want the Taskbar to look more like Windows XP, tick the 'Use small icons' box here, then select 'Never combine' for the Taskbar buttons option, and you will have much the same appearance.

TOOLBARS

Aside from displaying program icons, you can also insert additional items onto the Taskbar in the form of Toolbars. To view the currently available Toolbars, right-click on an empty area of the Taskbar and select Toolbars. There are several choices:

Address: If selected, this places an Internet address box on the Taskbar, and any text you enter will be launched as a URL in your default web browser.

Links: This item places a Links box on the Taskbar if ticked, allowing you to select any custom Internet links placed there. These correspond with the links shown in the Favorites Bar of Internet Explorer. You can drag and drop any website link from your bookmarks onto the Links Toolbar to add it to the list, and you can

right-click on and select Delete to remove any link here. Any links you select will be launched in your default web browser.

Touch Keyboard: Selecting this item places a keyboard icon on the Taskbar. When clicked, it pops up a touch keyboard, allowing input of text via mouse or touch. The keyboard can be moved and positioned anywhere on the screen.

Desktop: If selected, this item places a Desktop toolbar on the Taskbar. When the double arrows are clicked, it opens a list of categories that you can select from, corresponding to the main categories in the Navigation Pane of File Explorer, along with all of your Desktop program icons. This can be used as a quick substitute for the Start Menu, allowing you to launch frequently used programs or access files or folders from the Taskbar.

New Toolbar: If selected, you will be prompted to choose a folder, Library or location. Your selection will be added as a Toolbar to the Taskbar. When clicked, it will open that folder, Library or location in a menu, allowing you to navigate to any file or folder beneath it. Once again, this allows quick access to files and folders directly from the Taskbar.

Quick Launch: This toolbar is not available by default, because the unified Taskbar icons can be pinned to perform the same function. There is also a way to have something similar to the traditional Taskbar arrangement, including a Quick Launch-like area, as covered further above. However if you still wish to enable an actual Quick Launch toolbar, then follow these instructions:

1. Right-click on the Taskbar and select Toolbars>New Toolbar.
2. In the prompt which follows, navigate to the following directory:

   \Users\[username]\AppData\Roaming\Microsoft\Internet Explorer

3. Select the 'Quick Launch' folder found here, and click the 'Select Folder' button.

This will add the Quick Launch Toolbar to the Taskbar, however it is not in its original location or format. To move it back to its standard location next to the Start button on the Taskbar, follow on with these steps:

4. Right-click on any pinned icons on the Taskbar and select 'Unpin this program from taskbar' to remove them all.
5. Right-click on an empty area of the Taskbar and select 'Lock the taskbar' to unlock it.
6. Drag the new Quick Launch Toolbar to the far left of the Taskbar.
7. To remove the text labels from the Quick Launch icon, right-click on the words 'Quick Launch' and select both the 'Show Text' and 'Show Title' options to remove the titles from the icons and the 'Quick Launch' text itself.
8. You can now drag any program icon or link from File Explorer, the Desktop, or the Start Menu into the Quick Launch area and it will be added to the list of items shown.
9. When you have completed customizing the new Quick Launch Toolbar, and moved it into place, right-click on an empty area of the Taskbar and select 'Lock the taskbar' to lock it again.

Note that steps 5 - 9 above also apply to the Links, Desktop and Custom Toolbars as well. However, unlike previous versions of Windows, you cannot drag Toolbars off the Taskbar and position them freely on the Desktop.

ADDITIONAL FEATURES

The Taskbar provides several additional miscellaneous features that some users will value. One of the most useful of these is the ability to launch or switch to any program on the Taskbar by using the WINDOWS key, combined with a number corresponding with the order in which the icons are presented. For example, to launch File Explorer, which is the second item from the left by default on the Taskbar, press WINDOWS+2. If a program being selected in this manner is already open, this method will switch to that program window instead. Repeatedly pressing the same key combination will maximize or minimize the open window.

There are additional features to try. Right-click on an empty area of the Taskbar to access the following:

Cascade windows: Clicking this immediately forces all open windows to be rearranged in a cascade, with the first window aligned to the top left of the screen, the second window overlapping it, slightly below it on the diagonal axis, and so forth.

Show windows stacked: Clicking this option forces all open windows to be resized into rectangular windows which are stacked one on top of each other, filling the entire screen with no overlap.

Show windows side by side: Clicking this option forces all open windows to be resized into rectangular windows and arranged next to each other, filling the entire screen with no overlap. If there are only two windows open, this results in a similar arrangement to using the Snap feature to arrange two windows next to each other.

Show the desktop: Clicking this option automatically closes all open windows and shows the Desktop. Right-click on the Taskbar again and the option to 'Show open windows' will be displayed instead, allowing you to instantly restore all minimized windows. This is similar to using the Peek button on the end of the Taskbar.

Task Manager: This option allows you to quickly open the Task Manager utility. See the Task Manager section of the Performance Measurement & Troubleshooting chapter for details.

Finally, if you are not completely happy with the Taskbar, there are software alternatives that can provide a different interface and additional functions. RocketDock and ObjectDock are the two most popular Taskbar-like utilities for Windows. Both are free, however RocketDock is older, and ObjectDock requires purchase for access to more advanced features.

< NOTIFICATION AREA

The Notification Area, previously known as the System Tray in Windows XP, is the area on the far right of the Taskbar by default. It is technically a part of the Taskbar and can't be separated, however it is covered in a separate section from the Taskbar in this book because its functions and customization are different to that of the rest of the Taskbar.

The Notification Area contains several key components, including the Clock, Volume, Network, Power and Action Center icons. Additional program icons may appear in the Notification Area, or can be accessed by clicking the small white arrow to the left of the Notification Area. As the name implies, the Notification Area provides various notifications, such as when Windows installs new drivers, or discovers new Windows Updates. These prompts can provide valuable information, but may also be annoying, so fortunately the Notification Area can be customized to better meet your needs. To configure the Notification Area, right-click on the Clock and select Properties:

Turn system icons on or off: This section allows you to individually enable (On) or disable (Off) the five main system icons displayed in the Notification Area. These have been changed slightly from previous versions of Windows, and are covered individually below:

- Clock - The system clock displays the current time and date when enabled. Hovering your mouse over the Clock area shows more details, including any additional clocks you have enabled - see the Date and Time section of the Windows Control Panel chapter. Clicking on the clock area will open the larger Date and Time display, and note that by clicking the month header you can make the calendar show only months rather than days; then by clicking the year header the calendar will display only years; and then by clicking the decade header, the calendar will display groups of decades.
- Volume - The Volume icon allows access to the master volume slider, a mute function when the 'Mute speakers' icon is clicked underneath the slider, and has links to the Volume Mixer and Speaker Properties windows by clicking the Mixer link at the bottom, or the Speaker icon at the top, respectively. These functions are covered in more detail in the Sound section later in this chapter.
- Network - When clicked, the Network icon displays the current status of the network connection. It also allows you to change your network location by right-clicking on the listed network and selecting 'Turn sharing on or off' - see the Network and Sharing Center section of the Windows Control Panel chapter for more details. Unlike Windows XP or Vista, the Network icon does not provide an animated display of incoming/outgoing traffic on your network connection. To get information on the level of Network activity, open Task Manager, go to the Performance tab and click the network item. To have a Network icon that behaves similar to the one in Windows XP, install this free Network Activity Indicator utility.
- Power - This option appears if you are using a device that can be battery powered. Clicking the Power icon provides the current power level, and a link to the current power plan in effect - see the Power Options section of the Windows Control Panel chapter for more details. This icon is not available for desktop PCs using regular AC power.
- Action Center - This icon links to the Action Center, and is covered in detail under the Windows Action Center section of the Security chapter, as well as the Windows Action Center section of the Performance Measurement & Troubleshooting chapter.
- Input Indicator - This icon usually appears if you have set up more than one input language/method under the Language component of the Windows Control Panel. It allows you to more easily switch input methods by hovering your mouse over the language currently shown, and selecting another one from the list that appears. See the Language section of the Windows Control Panel chapter for details.

You can configure additional Notification Area options by clicking the 'Customize notification icons' link here, or by going to Windows Control Panel and selecting the Notification Area Icons component.

In the Notification Area Icons window, you are presented with a list of all program icons that are currently, or have previously been, open in the Notification Area. For each program you have three options:

Show icon and notifications: This setting allows the program to both display an icon in the Notification Area, and show any program notifications as popup balloons or icons.

Hide icon and notifications: This setting removes the program icon from the Notification Area, and prevents any notifications being shown.

Only show notifications: This setting removes the program's icon from the Notification Area, but allows notifications to be shown if necessary, including various icons that can alert you about the status of a program.

For most programs the 'Only show notifications' option is recommended, as this hides the icon and prevents the Notification Area from expanding and thus cluttering your Taskbar, but still allows programs to prompt you if there is anything worth noting. However, simply hiding Notification Area icons is not a substitute for going through and removing all unnecessary startup programs from being loaded on your system. For many programs you can safely disable startup functionality, which both removes the icon from the Notification

Area, and more importantly, reduces background resource usage and prevents conflicts and crashes. See the Startup Programs chapter for more details.

If you always want to show all icons and notifications in the Notification Area, then tick the 'Always show all icons and notifications on the taskbar' box. This prevents programs from automatically hiding themselves in your Notification Area, helping you to detect any program that surreptitiously adds itself to your Windows startup, and runs in the background for no good reason.

By default a white arrow will be added to the left side of the Notification Area as you install new programs, or if you select either the 'Hide icon and notifications' or 'Only show notifications' options for a program. When clicked, this arrow opens a small Notification Area Overflow box containing any hidden icons or notifications, and these can be clicked to access the relevant program or notification. You can also drag and drop icons from the Notification Area into this Notification Area Overflow box, or vice versa. This box is designed to reduce clutter in the main Notification Area, but again, is not a substitute for actively removing unnecessary startup programs and configuring relevant options in your various programs to prevent them from loading at startup, or providing unnecessary prompts.

The programs listed in the Notification Area Icons customization window can include inactive or uninstalled programs. To reduce clutter, or to fix a faulty tray entry, you may wish to manually remove the Notification Area entries for programs which are no longer installed. To do so, go to the following location in the Registry:

```
[HKEY_CURRENT_USER\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\TrayNotify]

IconStreams

PastIconsStream
```

Delete both DWORDs above, then restart Windows, or logoff and logon again. This will remove all stored Notification Area icon entries, and they will be regenerated as various programs are launched. There is also an automated free Notification Area Cleaner utility that does the same thing.

If you wish to completely remove the Notification Area from the Taskbar, which is not recommended, you can do so by using the 'Hide Notification Area' policy in Local Group Policy Editor - see the Group Policy chapter. In practice this is unnecessary, as simply by turning off all system icons under the Notification Area options, as covered under the 'Turn system icons on or off' setting further above, you can remove almost every trace of the Notification Area. All that will remain is a small white arrow which, when clicked, opens up the Notification Area Overflow box.

< STICKY NOTES

Sticky Notes is a feature that allows you to place small 'sticky' notes anywhere on your Desktop, similar to a physical Post-It note. To access it, go to the Start Screen, type *sticky* and press Enter. A single Sticky Note will appear on your Desktop. Click on the note and you can now type a reminder or important message, and it will remain on display on your Desktop, even after restarting Windows. You can edit it anytime you wish, and you can click the small 'x' at the top right of the note to delete it.

You can freely drag a Sticky Note around your Desktop to position it wherever you wish, and by default it will remain visible on top of any icons, ensuring that it gets your attention. To create additional notes, click the small '+' sign at the top left of the note, and a new Sticky Note will appear next to it. Alternatively, you can right-click on the Sticky Note icon in the Taskbar - which remains open as long as a Sticky Note is shown on your Desktop - and select 'New Note'. This Taskbar icon also brings all Sticky Notes to the forefront of any open windows when clicked.

A Sticky Note is customizable. You can resize it by clicking on the small gray triangle in the bottom right corner and dragging it to the desired shape and size. To alter the color of the Sticky Note, right-click on it and select from the sample shown. If you want to format the text in the Sticky Note, the simplest method is to copy and paste text that is already formatted in a word processing application like Word, or even the built-in WordPad application. Text copied and pasted into a Sticky Note in this manner will retain its original font style and formatting.

There is also a basic method of formatting text within a Sticky Note by highlighting the relevant text and using the following keyboard shortcuts:

Bold: CTRL+B
Italic: CTRL+I
Underlined: CTRL+U
Strikethrough: CTRL+T
Left Align: CTRL+L
Right Align: CTRL+R
Center: CTRL+E
Bulleted/Numbered List: CTRL+SHIFT+L - press repeatedly to cycle through available types
Increase/Decrease Text Size: CTRL + Mouse Wheel up/down

Sticky Notes take up minimal system resources, regardless of how many you have open, or how much text is displayed, so use as many as you wish.

< IMAGE CAPTURE AND MANIPULATION

Windows 8 comes with several basic tools for capturing, viewing and editing images. These are covered in this section, along with several tools that can do a more comprehensive job than the built-in utilities.

IMAGE CAPTURE

If you wish to capture an image, whether from a game or on the Desktop, you can use press the PRINT SCREEN (PRTSCN) key to place a snapshot of the current screen into memory. You can then open an image editing utility as covered below, and paste this image for editing or saving. To capture only a portion of the screen, such as an open window or dialog box, and not the entire Desktop, make sure the component is selected, then press ALT+PRTSCN.

Windows 8 adds a new feature, allowing you to do both take and save an image at the same time. By pressing WINDOWS+PRTSCN, a screenshot will be taken and stored as a .PNG image under a new *Screenshots* folder in your Pictures Library. The first screenshot will be labeled as *Screenshot (1).png*, with each subsequent shot incrementing the number in brackets.

Note that the screenshot counter in Windows 8 will keep incrementing from the previous number used each time you create a new screenshot, even if you delete previous screenshots. To reset or adjust the automatic number appended to these screenshots, go to the following location in the Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer]

ScreenshotIndex=7
```

Edit the value above in Decimal view to match the number that you want to be appended to the next screenshot taken with WINDOWS+PRTSCN.

A more comprehensive way to capture and save a screenshot of any portion of the screen is to use the Windows Snipping Tool. Go to the Start Screen, type *Snipping* and press Enter - the Snipping Tool will open. To take a screenshot of any portion of the screen, first select a snip type by clicking on the small down arrow next to the New button. Here you can choose from the following:

§ Free-Form Snip - Allows you to draw a freehand line around any area, and its contents will be saved as a screenshot.
§ Rectangular Snip - Allows you to capture a screenshot by drawing a rectangle of any size.
§ Window Snip - Allows you to specify a particular open window or screen element to capture.
§ Full-Screen Snip - Takes a screenshot of the entire screen.

Once you have selected the snip type, clicking the New button will let you take your screenshot. Once taken, the Snipping tool will show the captured screenshot in a new window. In this new window you can either edit the picture using the pen, highlighter or eraser tool, send it or copy it, or click the disk icon to save the snipped portion in lossless .PNG, or .GIF, .JPG or .MHT formats. You can then click the New button to initiate a new snip if you wish.

If you want to capture a screenshot during a game or 3D application, you can typically press the PRTSCN key to put a snapshot of the current frame into memory, however only a single frame can be kept this way until you exit the game or 3D application and paste it somewhere. Instead, you can use the FRAPS utility capture multiple screenshots during a game in different formats. It also allows for high quality video capture, and has a benchmarking function as well, although these require purchase for more advanced functionality.

Image Viewing & Editing

To view any image, double-click on it and it will open in the Photos app by default. You can switch to the more detailed Windows Photo Viewer by right-clicking on the image and selecting 'Open With', then selecting 'Windows Photo Viewer'. To set Windows Photo Viewer as the default, select 'Choose default program' instead, then select 'Windows Photo Viewer', or another image viewing program if you prefer, as your default for the image type - see the Default Programs section of the Windows Control Panel chapter for details.

The Windows Photo Viewer is fairly straightforward to use, as it allows you to browse photos and pictures in various formats, and initiate a slideshow, print, burn or open the picture in another utility such as Windows Paint. There is a free enhanced version of Windows Photo Viewer called Windows Photo Gallery. This version provides similar functionality to Windows Photo Viewer, with additional features such as the ability to edit an image in a range of ways. You can also install a range of free add-ons called Plugins for Windows Photo Gallery, which will enhance its functionality.

If you want to edit an image in more detail, you can open it with the built-in Windows Paint utility, accessed either by going to the Start Screen, typing *Paint* and pressing Enter, or by right-clicking on an image and selecting Open With>Paint. Windows Paint allows you to use a variety of tools to alter the image, add text to it, resize it and so forth. You can also save the image in a range of formats including .BMP, .PNG, .JPG, .GIF, and .TIFF.

If you require more advanced forms of image editing tools, then Adobe Photoshop is the recognized leader in this field, but is extremely expensive, although Photoshop Elements is an inexpensive and more basic version. Viable free alternatives to Photoshop, which can also read Photoshop format files, include GIMP, as well as Paint.NET when used with the Photoshop Plugin. All of these programs are quite advanced, and are only recommended for people who need to undertake more complex image manipulation or creation. For the average home user the Windows tools above are perfectly adequate.

< FONTS

Fonts are sets of characters in a particular style, and form the basis of all computer text. Windows Vista introduced several new fonts including Segoe UI, Constantia, Cambria, Corbel, Candara, Calibri, and Consolas. Windows 7 expanded this font collection with several additional fonts including Gabriola, Segoe UI Light, Segoe UI Semibold, and Segoe UI Symbol. Windows 8 makes some minor changes to the Segoe UI font. Windows 7 also introduced the DirectWrite API for improved text display, and Windows 8 further improves DirectWrite. A range of parameters relating to the display of fonts in Windows can be adjusted and are covered in this section.

FONT CLARITY

The most important aspect of font display is its clarity on your screen. Introduced as an option in Windows XP, and then the default rendering mode from Vista onwards, ClearType is the technology used to make fonts look smoother and clearer on LCD displays. It is enabled by default in Windows 8, but you can customize ClearType to better suit your needs, or disable all font smoothing if you wish.

To access the ClearType tuner, open the Display component under the Windows Control Panel, then click the 'Adjust ClearType text' link in the left pane. To start with, make sure the 'Turn on ClearType' box is ticked, then click the Next button and follow the prompts to customize how ClearType is applied. If you don't like the way ClearType looks, you can reopen this utility and untick the box to disable ClearType.

If you find that font smoothing of any type is annoying you, as it can make some fonts appear slightly more blurry to some people, then you can disable all font smoothing. Go to the Windows Control Panel, open the System component, and click the 'Advanced system settings' link in the left pane, or alternatively, type *systempropertiesadvanced* on the Start Screen and press Enter. Click the Settings button under Performance, and under the Visual Effects tab, untick the 'Smooth edges of screen fonts' box and click Apply to see the change. This will automatically disable ClearType as well. You may need to refresh the screen to see all of the text elements lose their smoothing, but the difference should be noticeable.

If, instead of using the ClearType utility, you want to manually fine-tune ClearType text appearance, then go to the following location in the Windows Registry:

```
[HKEY_CURRENT_USER\Control Panel\Desktop]

FontSmoothingGamma=0
FontSmoothingOrientation=1
```

The first DWORD above determines how bright or dark the text will be. The value is normally set through the ClearType utility, but you can manually adjust it in Decimal View up to a maximum of 2200; the higher the value, the lighter and thinner text will be. The second DWORD value above determines the type of display used, with 0 = CRT, 1 = Standard fixed-pixel RGB display, and 2 = fixed pixel display using non-standard BGR arrangement. The default of 1 should be used for most LCD panels.

If you prefer a more Mac OSX-like rendering system for Windows fonts, you can attempt to use gdipp, which replaces the Windows text render. A more user-friendly method is to download this Gditray.zip file, extract the contents to a new folder such as *\Program Files\GDI*, then launch the *gditray.exe* file. Right-click on the new G icon in your Notification Area and select Enable, then select 'Redraw desktop' to see the impact. Note that using these GDI methods can increase system resource usage and cause instability, since they replace a core Windows file, so it is generally not recommended unless you truly feel you cannot stand the default Windows text rendering, and have tried to adjust it using ClearType and the other methods in this section to no avail.

Some applications, such as Adobe Reader, also have their own text rendering options, which may override or enhance the general Windows display settings for fonts. In Adobe Reader for example, go to the Edit menu, select Preferences, and under the Page Display category, there is a Rendering section with options to control the way text is displayed for PDF documents viewed within Adobe Reader.

Furthermore, in some cases, even if you disable ClearType, Windows will retain ClearType for certain fonts such as Segoe UI - which is the primary font used for much of Window 8's interface - to ensure that all prompts, dialog boxes, warnings and so forth display text precisely as intended, with no cut-off words.

Font Size

If you find that the Windows screen fonts are generally too small, especially at higher resolutions, then you can go to the Display component under Windows Control Panel and select an interface size larger than 100%. However this increases both text and images, making everything look bigger. If you just want to alter the text size used in the interface, use the options under the 'Change the text size only' section beneath it.

Font Management

Accessible under Windows Control Panel, the Font component allows you to manage all the fonts currently installed in Windows. These fonts are stored in the *\Windows\Fonts* folder, which when clicked also opens this Font management interface. You can preview any installed font by double-clicking on its icon in the Fonts component.

You can install a new font in Windows simply by dragging its .FON or .TTF file into the Fonts folder; by double-clicking the file for a preview and then clicking the Install button at the top of the window; or by right-clicking on the file and selecting Install. Note that .TTF denotes a TrueType font, a technology that ensures good scaling, so that what is displayed on your screen is what you get. Other types of fonts may look slightly different in various applications, or when printed, or when using different sizes. To find out more about fonts, go to the Microsoft Typography Website. If you wish to download and install additional free fonts, go to Simply The Best Fonts.

Click the 'Font settings' link on the left side of the Fonts window for general font-related settings. Here you can tick the 'Hide fonts based on language settings' box to hide any fonts not designed for your default input language. You can also tick the 'Allow fonts to be installed using a shortcut' box, which will install a shortcut to the original font file in the *\Windows\Fonts* folder, rather than copying the file there. This can cause problems if the original font file is deleted from its existing location in Windows, so it is not recommended.

Customize Fonts

To create your own custom fonts, Windows has a built-in font editing utility called Private Character Editor, which you can access by going to the Start Screen, typing *eudcedit* and pressing Enter. It allows you to create custom fonts that you can then insert into documents using the Character Map utility, which can be opened by going to the Start Screen, typing *charmap* and pressing Enter.

If you wish to change the actual fonts used for particular Windows interface elements, unfortunately this option has been removed in Windows 8. The only way to change interface fonts is to remap existing Windows font families stored under the following location in the Registry:

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

Segoe UI (TrueType)=arial.ttf
Segoe UI Bold (TrueType)=ariblk.ttf
Segoe UI Bold Italic (TrueType)=arialbi.ttf
Segoe UI Italic (TrueType)=ariali.ttf
Segoe UI Light (TrueType)=arial.ttf
Segoe UI Light Italic (TrueType)=ariali.ttf
Segoe UI Semibold (TrueType)=arialbd.ttf
Segoe UI Semibold Italic (TrueType)=ariali.ttf
Segoe UI Semilight (TrueType)=arial.ttf
Segoe UI Semilight Italic (TrueType)=ariali.ttf
```


The example above tells Windows to use the Arial font family in all places where various forms of Segoe UI, which is the primary interface font in Windows 8, would normally be used. Restart Windows, or logoff and logon, for the change to be implemented. You can substitute any font in place of the Arial example used above, but make sure to use the correct font file for every entry of that font family (e.g. *arial.ttf* for regular, *ariali.ttf* for italic, *ariblk.ttf* for bold, *arialbd.ttf* for semibold, and *arialbi.ttf* for bold italic). All the font filenames can be found under the Fonts component in the Windows Control Panel - right click on a font there, select Properties and you will see its real filename. Make sure to set a Restore Point first before making these changes. Note that this change applies to all users on a machine, not just one user account.

Once you have chosen your preferred font, remember that you can then adjust font sizes for various Windows elements under the Display component of the Windows Control Panel.

< ICONS

Icons are the images used to represent programs, files and folders on the Windows Desktop. Windows 8 continues the icon system introduced in Windows Vista, designed to allow scalable icons. As a result, all system icons in Windows 8 can be smoothly resized from very small to very large, without losing any significant amount of quality. To demonstrate this, in File Explorer go to any directory with a range of files, right-click and select View>Extra Large Icons. Now hold down the CTRL key and use your Mouse Wheel to resize the icons, and notice that they scale up and down smoothly. Furthermore, certain content will display as Live Icons - thumbnails of the actual contents of a file - and these content thumbnails will also scale smoothly. Only older icons created prior to the new icon rendering engine will exhibit signs of quality degradation as they are scaled up or down. See the Basic Features section of the File Explorer chapter for more details on view-related features.

Icons on the Windows Desktop can be adjusted in much the same way as those in File Explorer, able to be resized by right-clicking on an empty area of the Desktop and using the View menu, or using the CTRL+Mouse Wheel method. Under the View menu you can also select whether to let Windows 'Auto Arrange icons', or 'Align icons to Grid' to place an invisible grid on the Desktop that icons will "snap" to when moved. You can even hide Desktop icons altogether at any time by unticking the 'Show desktop icons' option.

There is much more that can be done to customize icons in Windows, and these are covered in this section.

Remove Text from Desktop Icons

To remove the text beneath any icon on your Desktop, follow these steps:

1. Right-click on the icon whose title you want to remove and select Rename.
2. Instead of entering any characters in the text box, hold down the ALT key and type 255 (ALT + 2 + 5 + 5). You need to use the NUMPAD number keys for this to work, that is the numbers to the right of your arrow keys, not the ones at the top of the keyboard.
3. When you release the ALT key the title will be blank, and you can press Enter to accept this. Blank titles are usually denied under Windows, but not when done this way, as it inserts a special blank character.
4. For every icon whose title you wish to remove, do the same as above. However, since no two icons can have the same name, for each subsequent icon you'll have to use an additional ALT 255 to the end of the string you enter. E.g. to blank a second icon name you'll need to hold down ALT and type 255, release, then hold ALT and type 255 again, then release and press Enter. For a third, you'll have to type ALT 255, ALT 255, ALT 255, Enter, and so on.

If you want to regain these blank icon names, you will have to manually edit each icon's name as there is no undo function.

Remove Shortcut Arrows from Icons

By default Windows adds a small arrow to the bottom left of any icon that represents a Shortcut link rather than a normal file, folder or program. This is to differentiate icons that are purely links - which are usually safe to delete or move - from actual files or programs. If you want to remove this Shortcut arrow, you can add an entry in the Windows Registry to make this change. Go to the following location in the Registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer]
```

Right-click on the Explorer subfolder and select New>Key, and name this `Shell Icons` - it should look like this:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell
Icons]
```

Now select the `Shell Icons` key and in the right pane, create the following new STRING with the value data exactly as shown:

```
29=%SystemRoot%\System32\blank.ico
```

The value name show above is the number 29, and the value data shown after the = sign is the path to a valid blank icon file. To obtain this file and place it in the right location, download BlankIcon.zip, extract the *blank.ico* file from the archive, and move it to your *\Windows\System32* directory. Restart Windows, or logoff and logon, and all Shortcut arrows will be removed. You can undo this change by deleting the above value in the Registry and restarting Windows, or logging off then back on.

REMOVE '- SHORTCUT' FROM NEW SHORTCUTS

Whenever you create a Shortcut, the word - *Shortcut* appears at the end of the Shortcut's name. To remove this default suffix for new Shortcuts, go to the following location in the Windows Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer]
Link=1E 00 00 00
```

Change the BINARY value above to 00 00 00 00 - that is, double-click the 1E part of the value and type a pair of zeroes, then press Enter. This will prevent the '- Shortcut' portion being appended to the name of new Shortcuts. Restart Windows, or logoff and logon, to implement the change.

REPAIR INCORRECTLY DISPLAYED ICONS

By default Windows stores a range of commonly used icons in a cache to speed up their display on the Desktop and in File Explorer. If you are experiencing problems with your icons displaying incorrectly, go to the *\Users\[username]\AppData\Local* directory and delete the *IconCache.db* file. Reboot Windows and this file will be recreated, refreshing any out of date or incorrectly displayed icons.

SAVE DESKTOP ICON POSITIONS

This tweak allows you to save the current positions of your Desktop icons so that if the icons are accidentally rearranged, you can quickly restore them back to their original positions at any time. To give you this added functionality, do the following:

1. Install the free DesktopOK utility.
2. If the utility displays German text, click on the flag in the bottom left corner and select your desired language.
3. Arrange your Desktop icons as desired, then click the Save button in DesktopOK.
4. To restore your Desktop icon positions back to this saved state at any time, launch the utility and click the Restore button in DesktopOK.
5. The utility does not need to run at Windows startup or remain active in the background to maintain your saved state; it holds the position data in its *DesktopOK.ini* file.

CREATE CUSTOM SHUTDOWN, RESTART, SLEEP OR LOCK ICONS

For quick access to the Shutdown, Restart, Sleep or Lock options, you can create icons that automatically perform these functions with just a double-click. These icons can then be placed on the Desktop, or pinned to the Taskbar or Start Screen for quick access. Follow these instructions:

Shutdown Icon:

1. Right click on an empty area of your Desktop.
2. Select New>Shortcut.
3. In the first box of the Create Shortcut Wizard, type the following and click Next:

   ```
   shutdown /s /t 00
   ```

4. Call the shortcut *Shutdown* and click Finish. Alternatively, you can remove its name altogether using the Remove Text from Desktop Icons tip further above.
5. Right click on this new icon, select Properties, click the Change Icon button and select an appropriate icon, then click Apply.

Restart Icon:

To create a Restart icon that reboots your PC when selected, follow the same steps as above, but substitute the following steps in place of the corresponding ones above:

3. In the first box of the Create Shortcut Wizard, type the following and click Next:

   ```
   shutdown /r /t 00
   ```

4. Call the shortcut *Restart* and click Finish.

Lock Icon:

To create an icon that automatically brings up the Lock Screen until you log back in, follow the same steps for the Shutdown Icon above, but substitute the following steps in place of the corresponding ones further above:

3. In the first box of the Create Shortcut Wizard, type the following and click Next:

   ```
   rundll32.exe User32.dll,LockWorkStation
   ```

4. Call the shortcut *Lock* and click Finish.

Sleep Icon:

To create a Sleep icon that automatically puts the PC into your chosen Sleep mode, follow the same steps for the Shutdown Icon above, but substitute the following steps in place of the corresponding ones further above:

3. In the first box of the Create Shortcut Wizard, type the following and click Next:

   ```
   rundll32.exe powrprof.dll,SetSuspendState 0,1,0
   ```

4. Call the shortcut *Sleep* and click Finish.

Note that by default this sends the computer into hibernation, unless you disable the hibernation feature as covered under the Power Options section of the Windows Control Panel chapter.

Double-clicking any of these icons will commence shutdown, restart, lock or sleep as relevant straight away without any warning. If you want a countdown before shutdown or restart, substitute an amount of time in seconds in place of the '00' entries in the shortcut properties above (e.g. `shutdown /s /t 10` gives 10 seconds warning before shutting down). If you want more command line switches that can be used with the shutdown command, open a Command Prompt, type `shutdown /?` and press Enter.

To create the shortcut icons above in a different manner, such that they are actually options on the context menu that appears when you right-click on the Desktop, you will need to use the Registry Editor to make the following entries as relevant.

Shutdown Context Menu Entry:

```
[HKEY_CLASSES_ROOT\DesktopBackground\Shell]
```

Go to the location above in Registry Editor, right-click on the `Shell` key in the left pane, and create a new key called `Shutdown Computer`, or if you prefer, just `Shutdown` - this will be the name of the entry that appears on the context menu, so you can customize it if you wish. It will look like this:

```
[HKEY_CLASSES_ROOT\DesktopBackground\Shell\Shutdown Computer]
```

Select this new key in the left pane, and in the right pane create two new STRING entries, as shown below:

```
icon=shell32.dll,-329
Position=Bottom
```

Then, select the `Shutdown Computer` key in the left pane again, and create a new key under it called `Command`, so that it looks like this:

```
[HKEY_CLASSES_ROOT\DesktopBackground\Shell\Shutdown Computer\Command]
```

Select this new `Command` key in the left pane, and in the right pane, create the following new STRING entry:

```
@=shutdown.exe -s -t 00 -f
```

The name of the new STRING is the @ symbol.

The change will come into effect immediately, so right-click on an empty area of your Desktop, and the new entry will be shown at the bottom of the menu that appears. To also create Restart, Sleep and Lock context menu entries, use the details below, in the same manner as the instructions provided above.

Restart Context Menu Entry:

```
[HKEY_CLASSES_ROOT\DesktopBackground\Shell\Restart Computer]
icon=shell32.dll,-221
Position=Bottom

[HKEY_CLASSES_ROOT\DesktopBackground\Shell\Restart Computer\command]
@=shutdown.exe -r -t 00 -f
```

Sleep Context Menu Entry:

```
[HKEY_CLASSES_ROOT\DesktopBackground\Shell\Sleep Computer]
icon=shell32.dll,-331
Position=Bottom

[HKEY_CLASSES_ROOT\DesktopBackground\Shell\Sleep Computer\command]
@=rundll32.exe powrprof.dll,SetSuspendState 0,1,0
```

Lock Context Menu Entry:

```
[HKEY_CLASSES_ROOT\DesktopBackground\Shell\Lock Computer]
icon=shell32.dll,-325
Position=Bottom

[HKEY_CLASSES_ROOT\DesktopBackground\Shell\Lock Computer\command]
@=Rundll32 User32.dll,LockWorkStation
```

ICON CREATION AND CUSTOMIZATION

Windows 8 uses scalable icons that can be up to 256x256 pixels in size, and these higher resolution icons are stored in compressed .PNG format to maintain their quality at a reduced file size. Windows 8 icons are fully compatible with Windows Vista and 7, and vice versa. They are backward compatible with Windows XP, but only lower resolution versions of the icon (16x16, 32x32 and 48x48) will be shown in XP.

If you wish to create or edit Windows 8 scalable icons, you can use the free Paint.NET program covered under the Image Capture and Manipulation section of this chapter, combined with this free Icon/Cursor Plugin. Alternatively you can use the RealWorld Icon Editor, though it is only free for a trial period. Using original .PNG images for best results, you will be able to create a high quality .ICO file for use as a replacement for any program or folder icon.

To change any program file icon, simply right-click on it, select Properties, click the 'Change icon' button and browse to your custom .ICO file and select it, then click Apply. Or you can browse to the *Imageres.dll* or *Shell32.dll* files, both found under the *\Windows\System32* directory, to view a range of built-in Windows icons. For folder icon customization see the Advanced Features section of the File Explorer chapter.

< SOUND

One of the major changes that occurred as of Windows Vista is the way in which the Windows audio system works. It was a significant change over the way audio had been handled in Windows XP, and Windows 8 continues with the use of this audio model, with some technical refinements.

The Windows audio stack was completely re-written as of Vista, based on the Universal Audio Architecture (UAA), to provide faster and more accurate audio rendering, and higher quality digital signal processing. The audio stack no longer entangles itself with the Kernel - the core of the operating system - which results in much greater stability. Furthermore, the entire audio system is now designed such that third party audio drivers are not absolutely necessary for an audio device to work, and also allows the use of a range of enhanced features without the need for a third party control panel. Despite these improvements, the latest audio drivers for your device are still recommended for full functionality and optimal performance, as covered under the Windows Drivers chapter.

One of the most noticeable changes due to this audio stack is that the DirectSound3D API, used extensively prior to Windows Vista for providing enhanced hardware-accelerated 3D audio effects, such as through the use of EAX in games, is emulated in software under Windows 8, and thus it cannot access these hardware-accelerated effects. This is not a major issue, as it primarily affects older games and applications that used DirectSound to provide advanced audio effects. More recent games use the OpenAL API, or their own custom audio solutions designed for the Windows audio stack, and hence are not affected.

Windows 8 adds several refinements to the audio model, as covered in this Microsoft Article, designed to improve the quality and smooth flow of streaming audio.

The quickest way to access audio-related functionality in Windows is to click on the Volume icon in the Notification Area. This is discussed in more detail below.

VOLUME CONTROL

Shown as a small speaker icon in the Notification Area at the bottom right corner of the screen by default, the Volume Control window that opens when it is clicked allows you to adjust the master volume level for the current sound output device, which is usually your speakers or headphones. When you hover your mouse over the Notification Area speaker icon, it will show the name of the current sound output device, and the current master volume level as a percentage. If you click once on it, you can adjust the master volume level for the device using the slider. If you want to mute or unmute all sound, click the small blue

speaker icon at the bottom of the slider. To access your output device's settings, click the icon above the slider - these options are covered further below.

It is possible to set volume levels independently for each active application, as well as for normal Windows sounds. To do this, click the Mixer link in the Volume Control window, or you can simply right-click on the Volume icon and select 'Open Volume Mixer', and the full Volume Mixer will open. The Volume Mixer allows you to set the volume level for each open application, and to mute/unmute each specific application's sounds. Importantly, there is a 'System Sounds' slider here that controls the level for general Windows system sounds. Note that Windows remembers the volume level you set in the Mixer for a particular application, even if it is not currently shown in the Volume Mixer window.

You can also access a separate option that affects the display of volume sliders. Make sure the Volume Mixer is not open, then right-click on the Volume icon in the Notification Area and select 'Volume control options'. The Volume Control Options window allows you to display individual Device volume sliders for each separate audio device (not program) being used for audio output. For example, if you are using the Speakers device as well as the S/PDIF sound device, ticking both devices under the 'Sound device' box in the Volume Control Options window will display two volume sliders when the Volume icon is clicked, one for each device.

To access the full audio configuration options in Windows 8, go to the Windows Control Panel and open the Sound component, or right-click on the Volume icon in the Notification Area and select 'Playback devices'. These options are covered below.

PLAYBACK

This tab lists all of the available sound playback devices on your system. This includes devices such as speakers and headphones, and the various output channels supported by your sound device, such as S/PDIF and HDMI. To select which will be the default playback device - denoted by a small green tick next to its icon - highlight the device and click the 'Set Default' button. You can also choose to set a separate 'Default Communication Device', which is the device used for VOIP and the like. For example, you can set external speakers as the default device for normal audio, and set headphones as the default communications device.

I recommend right-clicking on audio playback devices that you are certain you will not use, and selecting Disable. This removes clutter, and also prevents accidentally selecting an unused output in any application, or having it show up in the Volume Control sliders for example. You can right-click in the Playback window and select or unselect the 'Show disabled devices' and 'Show disconnected devices' items to further refine the display of relevant items in this window at any time.

Certain devices allow additional configuration, so highlight the device and if the Configure button is available, click it and follow the Wizard to correctly configure the device. Most commonly this involves configuring the Speakers device for the correct number and type of speakers used, and testing the output.

Each sound playback device can also have a range of additional options. Highlight the device and click the Properties button, or simply double-click on the device. While I can't detail every feature for all types of playback devices, below are the common features for the Speakers device. Importantly, the presence or absence of features in this area depends on the type of hardware and drivers you are using, but below are the most common ones:

General: This tab provides details about your audio hardware and available connections. You can also rename the device and change its icon if you wish - the name and icon appear at the top of the master volume slider in the Notification Area, among other places.

Levels: The sliders under this section allow you to adjust the volume levels for each of your various audio output and input types, such as CD Player, microphone, Line In, etc. I recommend muting (clicking on the blue speaker icon) each input/output type that you don't use, as this helps reduce any potential background noise. You can also click the Balance button, where you can set the relative volume level for every individual channel possible on that output type.

Enhancements: This is an important set of default Windows features designed to allow almost all types of sound hardware to access enhanced audio playback features, covered in detail in this Microsoft Article. Note that this tab may have been removed or altered if you have installed third party drivers for your audio device. The full set of basic enhancements are summarized below:

- Bass Boost - Boosts the Bass response on smaller speakers such as mobile PC speakers. Click the Settings button to configure the boost characteristics.
- Virtual Surround - Converts multi-channel sound to two-channel, and back again if required.
- Room Correction - Through the use of a microphone, Windows can automatically calibrate a multi-channel home theater setup. Click the Settings button to start the process.
- Loudness Equalization - Attempts to maintain a more constant sound level across a range of sources. Click the Settings button to configure Release Time, which is the amount of time before equalization of sound is induced at any time.
- Bass Management - Controls Bass for home theater particularly when a subwoofer is missing.
- Speaker Phantoming - When using a multi-channel source, fills in any gaps in an incomplete multi-channel speaker setup.
- Speaker Fill - The reverse of Speaker Phantoming, takes a two-channel source and spreads it over more channels.
- Headphone Virtualization - Creates a 3D sound environment for headphones.

If you are experiencing audio-related problems, you can tick the 'Disable all enhancements' box to disable these effects for troubleshooting purposes.

The availability of these Enhancement options is dependent on the sound hardware and drivers you are using, as well as the playback device chosen. If your audio device has replaced this tab with a custom tab, or has a custom utility of its own for adjusting various enhancements, then that should provide better quality enhancements, as it is tailored to your sound device's capabilities. If you wish to experiment with the above built-in Windows audio enhancements and they are unavailable to you, uninstall your sound device's drivers. Regardless of whether you use these enhancements, or those that come with your audio driver, adjusting these types of settings properly is an important part of getting optimal audio quality from your hardware.

Advanced: The 'Default Format' option shown here is the number of channels, the sample rate and the bit depth generally used to play back all audio in Shared Mode, which is the normal mode used in Windows. This mode allows playback of audio from multiple applications at the same time. All audio output in Shared Mode is remixed by Windows to match the quality chosen in this drop-down box. I recommend that you select at least the 16-bit 48,000Hz option, as this is equivalent to DVD audio, and means playing back CDs and DVDs should result in no noticeable quality loss. You can set it even higher if you wish, and this may be beneficial in some circumstances, but it will not make audio sound better than its original encoded quality.

The 'Allow applications to take exclusive control of this device' and 'Give exclusive mode applications priority' relate to Exclusive Mode, the mode in which Windows allows an application to take control of audio processing, blocking all other audio sources, and preventing audio from being resampled by the Windows mixer. Exclusive Mode is only possible if supported by an application. Ticking both these boxes allows applications that support Exclusive Mode to gain access to this mode, which is recommended. If you experience audio problems then you might want to untick the first option for troubleshooting purposes.

RECORDING

This tab lists all the available sound recording/input devices on your system. The descriptions for options in this section are much the same as those under the Playback tab above. You can also listen to a portable music player plugged in through the port for a recording device; this functionality is available under the Listen tab for the relevant input device.

SOUNDS

You can assign different sounds to particular system and application events in this section. Each sound event is listed under the main 'Program Events' box, and to hear the current sound assigned to an event (if it has a speaker icon next to it), highlight the item and click the Test button. To assign another sound to an event, highlight the event, choose from the list available under the Sounds box, or click the Browse button and find a sound file in .WAV format to use, then click the Apply button.

While system sounds are important in warning you about various occurrences, they take up memory because they are loaded into RAM at Windows startup and stay there most of the time. This is not a major issue given the audio files are typically small, and modern systems have relatively large amounts of RAM. I still recommend disabling unnecessary sounds where possible as they serve no purpose. Highlight relevant events and select None under the Sounds list, then click Apply when done. Unnecessary sounds can include sound prompts for features you don't have or don't use, such as the Battery-related, Fax-related or Windows Speech Recognition-related events on PCs which don't use these features. Of course, if resources are not a concern, then you can add various new sounds to any event to customize your system.

As you install new programs or features, they may add new system events and sounds, so make sure to go through this list every once in a while to refine it and remove unnecessary sounds.

Once you've set up the Windows sounds the way you like them, click the 'Save As' button at the top of the window and save your new sound scheme under a suitable name; any changes you make in the future will be saved automatically to this scheme. If you just want to quickly disable all system event sounds, select the 'No Sounds' option under the sound scheme area; this doesn't turn off all sound on your system, it simply removes sound effects from all the system events.

Finally, there may be additional audio configuration options available for your sound hardware in Windows, particularly after you install the latest drivers for it. These can usually be found as new components in the Windows Control Panel, or by typing *audio*, or the name of your sound hardware, on the Start Screen. These additional configuration options can vary greatly, and are not covered in this chapter. They are very important as they can have a major impact on audio performance and quality in Windows. See your sound device manufacturer's website for more information on how to configure them correctly.

As a final note, if you are using a plugin sound card, and are having audio-related difficulties, then consider removing the sound card and reverting to onboard sound functionality, especially if you have a recent motherboard. Recent onboard audio chipsets, particularly those on high-end motherboards, provide high quality high definition audio, and are actually more likely to work without any problems with the Windows audio stack, since this is precisely the type of hardware it was designed for. As long as you find relatively recent Windows 8 or Windows 7 drivers for your onboard audio chipset, using onboard audio can be the best solution in terms of performance and stability, even for gaming.

< GAMING

This book has already been written with gamers in mind, so there are no specific performance tips in this section for gamers. Follow the recommendations throughout this book to get improved performance in both games and general Windows usage. Instead, in this section I look at game-related features in Windows 8.

In general terms, gaming on Windows 8 is very similar to gaming under previous versions of Windows. The key change is that when you click on the Games tile on the Start Screen, it takes you to Xbox Live, not Games Explorer. This is because gaming in the Metro environment is generally focused on casual games that you can download from the Windows Store. If you don't want to download Metro-based games, you can still install any regular PC game on Windows 8, and run it under the Desktop environment.

By default Windows 8 no longer contains any pre-installed Windows games, such as Solitaire or Minesweeper. To download and play these games, you will need to open the Games app on the Start Screen. Login or create a new Xbox Live account, then select the 'Windows Games Store' category, and you will see a range of basic games, including the free Microsoft Solitaire and Microsoft Minesweeper, which you can install and play.

Games Explorer still exists in Windows 8, but it is hidden. It's not a necessity for installing and running games, as they can be launched from a Desktop icon or a Metro tile as appropriate, but if you prefer to use Games Explorer, it can be accessed and customized relatively easily.

GAMES EXPLORER

Games Explorer was first introduced in Windows Vista, and is designed as a central area for launching installed games, replacing the need to have multiple game icons spread throughout your Desktop or Taskbar for various games.

Games Explorer is usually hidden in Windows 8. To open it, right-click on the Start Screen tile for an installed game and select 'Open file location'. Alternatively, you can either type the following on the Start Screen, or copy and paste it into the File Explorer's Address Bar, and press Enter:

```
%SystemRoot%\explorer.exe /E,::{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}
```

To create a permanent icon for launching Games Explorer, right-click on an empty area of your Desktop, select New>Shortcut, enter the text above, then name it *Games Explorer* and click Finish. You can also pin this icon to the Taskbar or Start Screen if you wish.

The Games Explorer interface is based on File Explorer, and as such most of the basic features in the Games Explorer window are the same as those covered in more detail in the File Explorer chapter. This includes the ability to change the way in which individual games are displayed by altering the View settings; a Details Pane which appears at the bottom of the window when a game is selected, providing additional information on the game; and a Preview Pane on the right which contains box cover art, content rating and performance information for the selected game. For more details on the performance information aspect, see the Windows Experience Index section of the Performance Measurement & Troubleshooting chapter.

Installing any non-Metro game on your system should add an icon for that game in Games Explorer. This will depend on how recent the game is, and where it attempts to install itself, or whether you are using a separate game platform like Steam. If a game icon is missing from Games Explorer, you can drag and drop its launch icon from the Desktop, or from the game's main directory, into the Games Explorer window.

To configure general Games Explorer options, click the Options button in the Command Bar area. These options are covered below:

Game updates and news: This option determines whether Windows will send game identification numbers and game version details to Microsoft in order to check for updates and news related to any games you currently have installed, and provide you with an indication that these updates are available. You can then choose to download and install them directly through Games Explorer. The information sent is not used by Microsoft to identify or contact you. However if you don't wish for Windows to check for updates, you can select the 'Never check online for updates or news; I'll do this manually option'. You can then check for updates for individual games by right-clicking on a game and selecting 'Check online for updates'; by checking for game patches and updates from the game manufacturer's website, the link to which is usually shown at the bottom of the Games Explorer window when the game is selected; or by searching on the Internet for yourself. The current game version number is also shown in the Details Pane at the bottom - this can help you determine whether you have the latest version installed. Installing the latest update for a game can resolve bugs, enable additional features, and even remove DRM protection, so it is always important to keep your games updated using one of these methods. Note that I provide daily updates on newly released game patches on the front page of TweakGuides.com.

Games folder options: There are two options here. The first is 'Download art and information about installed games', which if ticked, attempts to download box cover art and any additional information for games you have installed. By default it will check the game itself for an Internet address which it can use to obtain more information about the game. This is useful in allowing your installed games to have the correct icon and detailed information available. The second option is 'Collect most recently played game information', which collects information about how recently you have played each game. This information is not sent from your machine, it is stored locally and used for features such as sorting games based on how recently you have played them - right-click in an empty area of Games Explorer and select Sort By>Last Played. You can clear the stored recently played information at any time by clicking the 'Clear information' button.

Unhide All Items: This button will become available if you have chosen to hide any games. You can hide any game in Games Explorer by right-clicking on its icon and selecting 'Hide this game'. The game will only be removed from view in Games Explorer, it will not be uninstalled or hidden from other areas of Windows, such as the Start Screen search functionality.

In addition to these options, there are other features and customization options worth noting in Games Explorer:

Tools and Family Safety Buttons: In the Command Bar area of Games Explorer you can click on the Tools button and you will see shortcuts to games-related functionality in Windows. These are all covered throughout various chapters in this book, and there are no new options here. The same goes for the Family Safety button, which takes you to the Family Safety screen, covered in more detail under the Family Safety section of the User Accounts chapter.

Layout: If you want to adjust the appearance of Games Explorer, click the Organize button, select Layout and choose to enable/disable the Menu Bar just above the Organize button, the Details Pane at the bottom of the Games Explorer, or the Preview Pane at the right.

Pin to Taskbar: If a game is right-clicked, this option can be selected to pin a specific game icon to your Taskbar, allowing you to launch that game directly from the Taskbar without having to open Games Explorer. You can also do the same thing by dragging and dropping games from Games Explorer onto the Taskbar or the Desktop.

To customize Games Explorer even further, follow the tips below:

Adding Missing Games: If an installed game on your system is missing from Games Explorer, such as for very old games, or for games purchased and installed via Steam, you can still add them to Games Explorer. Drag and drop the game's Desktop icon or main game .EXE file into the Games Explorer window, or in Steam, under the Library section right-click on the game and select 'Create Desktop Shortcut', then drag and drop this new shortcut into Games Explorer. However this doesn't necessarily create the full details Games Explorer needs to define things like box art, support links and so forth.

Customize Games: For any game in Games Explorer, you edit basic game details, except for ratings information, by going to the following location in the Registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\GameUX\Games]
```

Under this location are a range of subfolders with a string of numbers and letters - each relates to a different game shown in Games Explorer. Left-click on each folder and in the right pane the `Title` value will have the name of the game to which the folder relates. You can edit this value if you wish to change the name displayed for the game in Games Explorer. You can delete subfolders for games that have been uninstalled and/or whose icons are not functioning correctly in the Games Explorer window, removing those icons from Games Explorer. The other parameters in this area of the Registry are not designed to be edited by the end user, and previous methods to edit games, such as the Games Explorer Editor or Steam Assistance utilities do not work on Windows 8.

You can also customize a game shortcut in Games Explorer in two ways. The first method involves finding a game's existing Desktop icon, or opening File Explorer, navigating to the game's directory, finding the main game executable, right-clicking on it and selecting Send To>Desktop to create one. Right-click on this Desktop shortcut, select Properties and under the Shortcut tab edit the Target box accordingly, click Apply and OK to finish. Drag and drop this Desktop shortcut into the Games Explorer window, and use it to launch the game with your customizations. If there is already an icon for that game in Games Explorer, you can right-click on it and select 'Hide this game' to remove it.

The second method is more comprehensive, and involves going to the location where all the Games Explorer shortcuts are physically stored in Windows. This is in one or both of the following directories:

\ProgramData\Microsoft\Windows\GameExplorer
\Users\[Username]\AppData\Local\Microsoft\Windows\GameExplorer

The first folder above is system-wide, the second is user-specific - a game may be in one or both depending on whether it is accessible by all users, or only a particular user. Each installed game will have a subfolder with a string of numbers. To identify each game, open each *\PlayTasks\0* subfolder in File Explorer and the game icon will be shown in the right pane, identifying the game. Right-click on the relevant icon and select Properties, then edit the Target box as required, click Apply and OK to finish. If necessary, find the game icon in both of the directory locations above and apply the change to both to ensure your customizations work for that game. The next time you launch that game from Games Explorer, it should launch with your customizations.

ALTERNATIVES TO GAMES EXPLORER

Windows 8 has clearly sidelined Games Explorer, in favor of the Xbox Live service incorporated into the Metro environment. This means that although you can still use Games Explorer as a central location to hold your games collection, it is difficult to customize, and newer games may not fully support its functionality.

As the Steam gaming platform, and to a lesser extent, other platforms such as Origin, continue to grow in popularity, one alternative is to add all of your games to these platforms. To add a non-Steam game to the Steam platform, launch Steam, and under the Games menu, select 'Add a Non-Steam Game to My Library'. To add a non-Origin game to Origin, select 'Add Game' then choose 'Add Games Manually'. Then create a single Desktop icon or Start Screen tile to Steam and/or Origin, allowing you to quickly access all of your games in a single location.

Another method is to pin all of your games individually to the Start Screen, then create a new tile group, give it an appropriate heading like Games, and use that as a central point for accessing your games collection. See the Metro section of this chapter for details on how to create tile groups.

OLD GAMES

If you are having problems running older games under Windows 8, try the following:

- If UAC is enabled, make sure the game is being run in Administrator mode. Old games made prior to Windows Vista may not request Administrator level privileges even if they require it, and hence will not install or run properly. Right-click on the game's launch icon and select 'Run as Administrator', or right-click on the game's executable, select Properties and under the Compatibility tab select 'Run this program as an administrator', or click Advanced under the Shortcut tab and tick the 'Run as Administrator' box. See the User Account Control section under the Security chapter for details.
- Right-click on the game's Desktop shortcut or the original game executable, select Properties, and under the Compatibility tab tick the 'Run this program in compatibility mode for' box and select first 'Windows 7'. If that doesn't work try selecting 'Windows XP (Service Pack 3)', as this is the most common Windows configuration.
- If the game was made prior to 2006, and you are running a multi-core CPU, then this may affect the smoothness or running speed of the game, since it was only in mid-2005 that desktop multi-core CPUs became available to average PC users. In that case you can manually adjust the affinity for a game so that it only runs on one core of the CPU. See the Task Manager section of the Performance Measurement & Troubleshooting chapter for instructions on how to do this.
- For DOS-based games, you will require a DOS PC emulator such as the free DOSBox. Running DOS games from a Windows Command Prompt will usually not work, as modern versions of Windows do not contain a true DOS environment.

For general problems with any game, old or new, see the Performance Measurement & Troubleshooting chapter. The vast majority of gaming problems are due to system issues such as overheating hardware, overclocking, incorrect BIOS/UEFI settings, outdated or badly installed drivers, conflicting background programs, and misconfiguration of game and graphics control panel settings to name just a few causes. PC gaming is not as straightforward as console gaming, because there are a large number of variables involved. No operating system can overcome this, so it is up to the user to understand the fundamentals of how their system works and thus optimize and troubleshoot it properly - which is precisely what this book is about.

PERFORMANCE MEASUREMENT & TROUBLESHOOTING

Whenever you change various settings on your PC, or install and use particular programs, or alter your hardware in some way, it is difficult to tell whether your overall performance or system stability has improved or decreased. While you can get a general feel for whether things have improved or not, it is often best to gauge performance and stability changes objectively by using a range of tools. By the same token, you may be trying to resolve a problem that is showing up in the form of poor performance, strange behavior or an unintelligible error message. Through the use of appropriate diagnostic tools and troubleshooting methodology, you can resolve a problem more efficiently.

Windows 8 comes with a range of built-in tools designed to provide you with performance information, and assist you in diagnosing a variety of common problems. The central location for many of the Windows performance and diagnostic tools are the Performance Information and Tools and Troubleshooting components of the Windows Control Panel.

In this chapter we look at the various tools and methods for measuring performance and troubleshooting system problems. In addition to the built-in Windows tools, I also provide details on a range of third party programs that will further help you in benchmarking your performance, as well as tracking down the cause of any problems.

< WINDOWS EXPERIENCE INDEX

One of the first things Windows 8 does after you have installed it is to examine your system with the Windows System Assessment Tool (WinSAT), running a series of tests to calculate the Windows Experience Index (WEI) score for your system. This is an important process, allowing Windows to measure your system's performance.

The WEI is shown as a series of five sub-scores, culminating in a single base score displayed as the large number at the right of the sub-scores. The base score is determined by the lowest of your five individual sub-scores; it is not an average or cumulative score. You can access your WEI score, and rerun the tests at any time, by going to the System component of the Windows Control Panel and clicking the 'Windows Experience Index' link, or the 'System rating is not available' link if WEI has not yet been run.

Windows 8 continues with the WEI model used in Windows Vista and 7, but the score ranges vary. In Windows Vista, WEI went from a minimum of 1 to a maximum of 5.9; in Windows 7 the maximum was increased to 7.9; and in Windows 8, the maximum is 9.9. This has been done to take account of new hardware, such as multi-core CPUs, faster SSDs and the latest graphics cards. WEI scores are not strictly comparable across different versions of Windows, precisely because of the changes in the scale. For example, your WEI score in Windows 8 may be lower or higher than it was in Windows 7 on exactly the same hardware.

Windows uses the base score and sub-scores to determine a range of things, such as whether to disable SuperFetch for example, so the score is important, and you should investigate further into areas where you score relatively lowly.

Below is a summary of how WinSAT calculates your Windows Experience Index number for each sub-score:

Processor: The results of this score are calculated as a weighted average of various file compression and decompression tests, as well as tests involving encryption/decryption, computing hashes and encoding video.

Memory (RAM): The results of this score are calculated based on the amount of bandwidth (in MB/s) that the system memory can move within a certain period. The highest score attainable is constrained by the actual amount of system RAM (minus any memory reserved for graphics).

Graphics: This score is mainly used to determine how your system will run Desktop graphics and play back Windows Media Video. It measures video memory bandwidth (in MB/s), and note that the maximum DirectX version your graphics card supports will also determine its maximum possible WEI score.

Gaming Graphics: This score is calculated based on how many Frames Per Second (FPS) your graphics card can display for various D3D tests, in various DirectX modes. Your maximum possible WEI score for this component will vary depending on your graphics card's support for different DirectX versions, as well as the WDDM version of the graphics driver you are using.

Primary Hard Disk: This score is calculated based on your primary drive's bandwidth measured in MB/s, as well as random read, random write, and flush assessments. Traditional hard drives are restricted in their maximum score, as the higher WEI score ranges are reserved for fast Solid State Drives.

The Windows Experience Index is not the ultimate test of what a machine is capable of, as clearly different applications and games will rely more on different components. Nor is it a highly accurate benchmark of performance. However, because of the way the base score is shown not as an average - which would be misleading - but as the lowest of your individual sub-scores, it is very useful for gauging the general performance level of a PC. The WEI base score highlights the weakest link of the main hardware components of a system, and there is good reason for this: your system is only as fast as its weakest link.

For instance, on a PC that scores a 8.0 on its Gaming Graphics sub-score, you would expect excellent gaming performance, but this is not necessarily so. If the same system scores lowly on other areas, then it is likely it will run into problems with gaming. For example, if the Memory or Primary Hard Disk scores of the same machine are below 3.0, this means that while the graphics card can easily handle intensive 3D rendering for a game, the hard drive and/or memory may simply not be fast enough to continually supply the graphics card with the information it needs, and the end result will be major stuttering, or frequent loading pauses, or indeed certain games may not be able to run at all due to insufficient RAM. To achieve a balanced machine, ideally all the sub-scores should be similar to each other.

If you are looking to upgrade your system, then it would be wise to pay attention to which component(s) are scoring lowly, and address those first and foremost. If you're buying a pre-built system then make sure it has a good base score, and don't accept any dismissive statements that the Windows Experience Index is "not important". WEI should never be the only factor you use in making a purchasing decision, nor is it a precise indicator of performance. Nevertheless, a low WEI is a clear indication of potentially poor performance.

WINDOWS SYSTEM ASSESSMENT TOOL

Windows uses the performance information it obtains from the Windows System Assessment Tool (WinSAT), used to calculate the Windows Experience Index, quite seriously. For example, Windows uses WinSAT to determine your drive's speed and capabilities, and hence whether it should disable certain features if it determines that you have SSD. Games can also use WinSAT's performance information to automatically customize or disable certain game settings based on your score, although note that your score should never prevent you from playing any game, even if you don't meet the WEI requirements.

You should make sure that you keep the WEI up to date. Whenever you change your hardware, update your drivers, alter performance-related settings, or overclock your system, you may need to update the WEI, and I strongly recommend that you do so as soon as possible. You can manually update the WEI at any time by going to the Performance Information and Tools component of the Windows Control Panel and clicking the 'Re-run the assessment' link at the bottom right on the main window. For best results, make sure that you do not use your system, or have any programs currently active, while your score is being updated.

To update the individual score for a particular component, and to also see more details of the actual tests being undertaken and the detailed results, you can access WinSAT directly through a command line interface:

1. Open an Administrator Command Prompt.
2. Type the following and press Enter to get a rundown of your system information:

   ```
   WinSAT features
   ```

3. To do a full test and update your scores, type the following and press Enter:

   ```
   WinSAT formal
   ```

4. To run specific tests on individual components, with the results being shown in more detail, see this WinSAT Command List or type `WinSAT /?` for a full list of commands. For example, you can type `WinSAT CPU` to run the Processor test, or `WinSAT MEM` to run the memory test.

Each time a full WEI test is run, the results are stored in the *\Windows\Performance\WinSAT\DataStore* directory as .XML files, which you can open to see more details of individual test results, though it is hard to read due to the formatting. If you are having problems with WEI or WinSAT, you can delete or move these files to another location to clear the results, and then rerun the WEI tests. This is not recommended; the best method to clear WEI and re-run the tests is to click the 'Advanced tools' link in the left pane of Performance Information and Tools, then click 'Clear all Windows Experience Index scores and re-rate the system'.

< RELIABILITY MONITOR

Reliability Monitor is a tool that provides a user-friendly overview of your system's stability and problem history. You can launch it by typing *reliability* on the Start Screen, selecting Settings and pressing Enter, or by opening the Action Center from the Notification Area, clicking the Maintenance heading to expand it, then clicking the 'View reliability history' link.

The main feature of the Reliability Monitor is a System Stability chart that provides a graphical representation of your system stability over time. The closer you are to 10 on the System Stability Index scale of 1 - 10, the more stable your system is deemed to be. Reliability Monitor begins graphing your system in the first 24 hours after you install Windows, and continues to do so on a daily basis. Use the arrow bars on either side to scroll across the full length of the graph.

Each column on the graph is an individual day, and at the bottom of the graph you can see several rows that may contain Errors (red X), Warning events (yellow exclamation) or Information events (blue i) in the five categories of: Application failures, Windows failures, Miscellaneous failures, Warnings and Information. Click on a particular day (column) to see the details of the events on that day, along with details for each event, at the bottom of the screen. These events are all linked to the Event Viewer functionality, covered later in this chapter, however Reliability Monitor provides a more convenient and user-friendly way of viewing important system events than Event Viewer, which is why it is recommended for most users in the initial

identification of problems. It is particularly useful in seeing how frequently certain problems are occurring on your system.

To investigate any individual event in the Source pane at the bottom of Reliability Monitor, click the 'View technical details' link next to it, or double-click it and a description of the problem is provided. To view additional information on the problem, click the 'View all problem reports' link at the very bottom of the Reliability Monitor, which opens the Action Center Problem Reports window and displays all queued problem reports - see further below for more details on Action Center. For more advanced users, you can investigate the error logs in Event Viewer to find more details of any problems - see the Event Viewer section later in this chapter.

Reliability Monitor helps provide you with an overview of how many errors and problems your system is experiencing, and a general indicator of your system stability. A stable Windows installation should have very few errors or warnings, and hence should always be close to the 10 index score.

< TROUBLESHOOTING

Whether you are having an immediate problem with a particular device, program or Windows feature, or if you want to troubleshoot a potential performance issue identified by the Windows Experience Index, the simplest method of doing so is to start by using the built-in Troubleshooters. These are collectively held in the Troubleshooting component under the Windows Control Panel, and there are a range of categories for which you can launch a troubleshooting utility, including: Programs, Hardware and Sound, Network and Internet, and System and Security.

You can alter the settings for the troubleshooter functionality by clicking the 'Change settings' link on the left side of the Troubleshooting window:

Computer Maintenance: If Windows detects the presence of broken shortcuts, unused files and unused Desktop icons, and a range of other general issues, it may prompt you to resolve them by running the System Maintenance troubleshooter. If you don't wish to be prompted in this way, select the Off option here. You can manually run System Maintenance at any time by clicking the 'Run maintenance tasks' link under the System and Security category in the main Troubleshooting window.

Allow troubleshooting to begin immediately when started: If ticked, allows a troubleshooting wizard to begin immediate detection of issues when launched. Not recommended unless you are an extremely novice user. It is better to be able to select from the options presented whenever you first open a troubleshooting wizard, before proceeding.

To initiate troubleshooting, click one of the four main category headings in the Troubleshooting window, and you will be taken to a separate window containing a range of relevant tasks, which each run specific troubleshooting wizards designed to resolve a particular problem. Select the one that best suits your particular issue.

When launched, the relevant troubleshooting wizard is automated by default and will apply a series of tests to detect the problem, and then change various settings as relevant to resolve it, however you can change this behavior. Click the Advanced link on the first page of a troubleshooter, and you can untick the 'Apply repairs automatically' if you don't want automated repair. Once the troubleshooting wizard has completed its scan, you can also click the 'View detailed information' link which appears. This must be done for every troubleshooter separately, and these steps will ensure that the troubleshooting wizard provides you with details on the actual tests that it ran, the types of issues that were detected, and a list of suggested repairs that you can choose from if you wish to continue with the troubleshooter - this is strongly recommended for more advanced users, as it gives you greater information and control over any changes being made to your system.

There are additional resources available in the main Troubleshooting window to assist beginners, such as the 'Get help from a friend' link on the left side, which allows you to invite a friend to fix your problem via the Remote Assistance feature. You should only use this feature to connect to a completely trusted individual, as otherwise it is a security risk. Under the Remote Assistance window there is also a link to the Steps Recorder, which is covered further below.

The Troubleshooting utilities are of greatest benefit to novice users who have relatively simple problems that Windows can readily detect and resolve. Because of the automated nature of these tools, and the fact that they will not resolve moderately complex problems, it is strongly advised that you become familiar with the rest of the tools in this chapter, as well as the information throughout this book, for the purposes of learning how to correctly troubleshoot and resolve issues on your own.

PROBLEM STEPS RECORDER

The Problem Steps Recorder, now simply called the Steps Recorder in Windows 8, can be found under the 'Get help from a friend' link in the Troubleshooting window, or by typing *psr* on the Start Screen and pressing Enter. It is an offline tool which, when you click the 'Start Record' button, will record every keystroke and mouse movement you make, along with individual screenshots at every stage. This is not done as full motion video, it is a text and screenshot image record of your session, and you can also add comments at any stage by clicking the 'Add comment' button and entering descriptive text. When you click the 'Stop record' button, you will be prompted to save the output file in a .ZIP archive to a particular location. This archive contains an .MHT file that can be viewed in Internet Explorer, and can be sent to a tech support person who can then view precisely what steps you undertook, and what you saw on the screen when experiencing the problem.

To alter the settings for Problem Steps Recorder, click the small arrow at the right side of the utility, and select Settings. Here you can choose the default location for saving the output file, whether to enable screen captures, and the total number of screen captures which the file can hold.

Problem Steps Recorder can be very useful in sharing what you see and do on your PC with a trusted person, such as a more technically experienced and trusted family member, or a genuine Microsoft tech support person. However, make sure that you do not have any embarrassing or private information visible on screen when you launch the utility, and if your problem involves entering secure information, then consider other troubleshooting methods first.

If you prefer a utility that records your steps as full motion video, then use the Screenrecorder utility instead. It can record a particular window or the entire screen, and captures everything you do as a .WMV video file.

< WINDOWS ACTION CENTER

The Action Center's security-related functionality is covered under the Windows Action Center section of the Security chapter. In this section we examine the other half of the Action Center: the Maintenance category. Open Action Center from the Windows Control Panel, or by clicking on the Action Center icon in the Notification Area and selecting 'Open Action Center'. Click the Maintenance category heading to expand that section of the Action Center. Most of the settings and links in this area of the Action Center area are covered in various other chapters throughout this book. The features under Maintenance that are not covered elsewhere are described below.

AUTOMATIC MAINTENANCE

Windows 8 consolidates a range of daily background maintenance and updating tasks into a single Automatic Maintenance feature, as described in this Microsoft Article. These tasks include checking Windows Updates, any scheduled malware scans or drive optimization runs, basic system diagnostic routines, and any supported third party software update checking. Automatic Maintenance gives users greater control over when the background tasks are run, as well as being able to launch them immediately if desired.

You can access this feature under the main Action Center window, by expanding the Maintenance category, and clicking the 'Change maintenance settings' link. This will open the Automatic Maintenance window, and allows you to set a particular time for daily maintenance tasks to be launched in the background. By default, this is 3:00am every morning, or whenever your computer is first idle after that time. If the 'Allow scheduled maintenance to wake up my computer at the scheduled time' box is ticked, if your computer is in a Sleep mode at the appointed time, it will wake up and perform the maintenance tasks, before returning back to sleep.

You can also immediately launch the full range of daily maintenance and updating tasks at any time. To do this, expand the Maintenance category in Action Center and click the 'Start maintenance' link. You can then click the 'Stop maintenance' link that appears if you want to cease the run before it completes.

Since Automatic Maintenance is fully automated, there is no need to adjust these settings or manually run the maintenance tasks. Windows will initiate them on a daily basis in the background whenever your system is idle.

WINDOWS ERROR REPORTING

As part of Windows Error Reporting functionality, Windows will record any problems you experience with any applications, or with Windows itself. These problem reports can also be sent to Microsoft to check for available solutions.

To see all existing problem reports, launch the Reliability Monitor and click the 'View all problem reports' link at the bottom of it; or go to the Start Screen and type *view all problem*, select Settings then press Enter. For each problem listed, you will see whether a report has been sent or not under the Status column. To see full details of the problem, double-click on the relevant problem. In particular, note the specific file or feature that has triggered the problem report, then use the tools in this chapter, as well as online research, to attempt to resolve any recurring problems.

To assist you in resolving a problem, as well as to make Microsoft aware of it, you can send the problem report to Microsoft by clicking the 'Check for solutions' link under the Maintenance category of the Action Center. When sending a problem report, the information sent to Microsoft involves the following details:

- A randomly generated Globally Unique Identifier (GUID) to identify your machine.
- Where the problem happened in the software or hardware.
- The type or severity of the problem.
- Files that help describe the problem.
- Basic software and hardware information.
- Possible software performance and compatibility problems.

If an error report potentially contains personal information, you will be prompted for confirmation before sending this information, though Microsoft will not use this information to identify or contact you. If Microsoft requires more information regarding a problem you reported, you will be prompted to send additional information. Additional information may include personally identifiable information you can

choose to enter, such as your phone number or email address. You can review the problem reports for which Microsoft requires more information before choosing to send the additional information or not, and you can deny any such requests, as this is not compulsory for any problem report.

To customize the problem reporting behavior, click the Settings link under the 'Check for solutions to problem reports' area of the Maintenance section of Action Center. Here you can select whether to allow Windows to automatically check for solutions each time a problem report is generated, including whether to automatically submit additional data if required; have Windows ask you each time before checking for a solution to a problem; or disable the problem reporting feature altogether. I recommend the 'Each time a problem occurs, ask me before checking for a solution' to provide you with maximum control over the process. You can also specify particular programs to exclude from reporting a problem by clicking the 'Select programs to exclude from reporting' link and manually adding the main executable file for the relevant program to the list box.

If you are certain you will never use this functionality, you can completely disable it by selecting 'Never check for solutions'. This automated method of checking for and resolving problems is by no means ideal, but it does provide a relatively easy to understand interface for viewing and attempting to resolve application and Windows-related problems in the first instance, particularly for novice users. Most of the time you will have to do further investigation on your own to work out the source of a problem. But even if this feature provides you with no useful solution, by reporting a problem at least you will be making Microsoft aware of it, and if it is due to a genuine software bug for example, they can work to resolve it in a Windows update, or inform the relevant developer of the issue.

< EVENT VIEWER

In the Performance Information and Tools component of Windows Control Panel, click the 'Advanced tools' link in the left pane, then click the 'View performance details in Event log'. This will open the Event Viewer, though it can also be accessed directly by typing *eventvwr* on the Start Screen and pressing Enter. Event Viewer is the central location for holding various Windows event logs. Each event is categorized as either an Error, Warning or Informational. An Error is a significant problem; a Warning isn't necessarily major, but may cause problems in the future; an Informational event simply describes a successful operation, such as a driver installation.

Event Viewer is a tool best suited to intermediate and advanced users. Learning to use it can greatly improve your chances of finding out about the cause of problems or performance issues. For a more user-friendly display of the important events recorded in Event Viewer, see the Reliability Monitor section earlier in this chapter.

If you are trying to improve performance, then to access the performance-specific logs in Event Viewer go to the Performance Information and Tools component of the Windows Control Panel, click the 'Advanced tools' link in the left pane, then click 'View performance details in Event log'. This will take you to the Operational log under the Applications and Services Logs>Microsoft>Windows>Diagnostics-Performance folder of Event Viewer. Here you can see the individual events that describe potential performance issues, as identified by the Windows Diagnostic Infrastructure, which automatically monitors a range of events, including Windows startup, shutdown, Desktop performance and a range of other system events. For example, if you have a 'Boot Performance Monitoring' warning here, it is because Windows thinks your boot time may be too long. Highlight the relevant event and you can see details such as how many seconds boot time is taking in milliseconds (1,000ms = 1 second). Go through these warnings or errors, and where specific devices or programs are named as being responsible, investigate those particular aspects further.

Windows also reports the most significant of these performance issues in more intelligible form. When you open the Advanced Tools area of the Performance Information and Tools window, you may see listed at the very top of the window under 'Performance issues' one or more links, which are the results of Window's

diagnostic analysis. For example, you may see a 'Performance can be improved by changing visual settings' link which, when clicked, provides more information, in some cases even specifying a file or setting you should investigate. Unfortunately it is not as simple as removing or disabling the component(s) Windows thinks is the problem, as some of them may be necessary. Furthermore, Windows may identify something as a potential problem when in fact it is not particularly significant. Regardless, this form of automated diagnostic provides information that is easier to understand than raw Event Viewer logs, and should not be ignored.

For general troubleshooting purposes, click the 'Event Viewer (Local)' link at the very top of the left pane of Event Viewer. This brings up the Overview and Summary screen in the middle pane, showing the major events and warnings summarized and ranked, from Critical events, Errors, Warnings, and Information, down to Audit Success and Audit Failure. Each category can be expanded to show the specific event log items for that category of error or warning, as the example below demonstrates:

1. Click on the '+' sign next to Error under Summary of Administrative Events.
2. You will see all Errors listed in order of Event ID number, with the number of errors in the last hour, 24 hours, 7 days and Total shown in the columns to the right.
3. Double-click on the Event ID that has had the most number of errors in the last 24 hours. You will see a listing of all the individual event logs, sorted from newest to oldest.
4. Look at the bottom of the middle pane under the General tab. You will see a general description of the error. The information under the Details tab is usually not easy to comprehend, but you can view that also if you wish.
5. Under the General tab, click the 'Event Log Online Help' link and click Yes. A new browser window will open and you may be able to see additional information on the error.

Be aware that if you undertake Step 5 above, for errors with Windows programs and features, details regarding the error will be sent to Microsoft, but will not be used to identify or contact you. However, if you report an error for a third party program, such reports are sent to the developer or manufacturer of the third party software, and they may be used for various purposes based on that company's privacy policies.

Often times you won't be able to find much helpful advice about a particular Event ID, so try searching the official Microsoft Error Message Center, or conduct a web search for more details.

If instead of viewing the logs by type, you wish to view all logs for a specific category or component of Windows, go to the left pane of Event Viewer and browse the available folders. For example, to view all User Account Control-related logs, go to Applications and Services Logs>Microsoft>Windows>UAC and click the log file(s) under it to see the details.

Some important things to note about event logs:

§ To troubleshoot a problem, focus on any Critical events to start with, followed by Errors in the Overview and Summary pane. Warning and Information events are useful mainly for performance optimization, rather than troubleshooting an immediate problem. See further below for a method of filtering log files to only see those you want to examine.
§ Look at how recent the event was. It may be that it occurred a while ago and is no longer occurring, so it could be a one-off, or it has been resolved through some other action, such as uninstalling the problematic program, or patching it with an update. Focus on issues that occur often and more recently.
§ Remember that a log showing many events may just be the same issue that has occurred repeatedly, such as every time you start your PC. In other words, seeing 100 Errors events may just mean that you had the same type of error twice a day over the past 50 days, not 100 different errors. Sort events by the Event ID column to see how many unique events there are.

If you want to filter the type of event logs that are presented to you in Event Viewer, click the 'Create a custom view' link in the right pane, then specify the types of event levels to be shown and the time period over which they have been logged among other things. You can then examine this new filtered view by selecting it under the 'Custom Views' folder in the left pane.

You can even configure Windows to alert you immediately for a specific event by right-clicking on it and selecting 'Attach Task to this Event'. This opens the Create a Basic Task wizard for Task Scheduler, which is covered in the Background Tasks section of the Services chapter.

The Event Viewer has a wealth of information that can help you detect where a problem is occurring if you take some time to go through it. Windows also provides the most important events in easier to understand formats, through tools such as the Reliability Monitor, as well as at the top of the Advanced Tools window of the Performance Information and Tools component.

< PERFORMANCE MONITOR

The Performance Monitor can be accessed in a number of ways, either under the 'Advanced Tools' link in the Performance Information and Tools component of Windows Control Panel by clicking the 'Open Performance Monitor' link, or by typing *perfmon* on the Start Screen and pressing Enter. The Performance Monitor is an important tool for monitoring system performance and resource usage in Windows.

One of the ways to figure out how to improve your performance is to monitor your system resources and determine firstly if any programs are using too many resources when they shouldn't be; and secondly, to observe and see just what type of resources your more resource-hungry applications need - this can help identify any bottlenecks.

To begin monitoring resource usage, open the Performance Monitor, and in the System Summary pane you can see a snapshot of various system parameters in real-time. This type of information is also covered further under the Resource Monitor and Task Manager sections later in this chapter.

Select the 'Performance Monitor' item in the left pane, and you will see a graph which immediately commences charting your CPU usage. You can add components to graph over time by clicking the green '+' button at the top, or right-clicking on the window and selecting 'Add Counters'. For example, to add a counter measuring drive usage, double-click on the Physical Disk item in the list, then select a specific variable you wish to measure (e.g. Disk Write Bytes/Sec) and click the Add button. You can add as many components as you like, though obviously it is wise to limit this to make the graph readable. Click OK when done.

The series you add may be difficult to distinguish, or may not update frequently enough. Furthermore, since the Y (vertical) axis scale is fixed, some components will not display in any meaningful way when using a common scale. You can change the way the graphed data is displayed in two ways:

- The simple method involves clicking the 'Change graph type' button at the top of the chart, and selecting either Histogram, or Report view in particular which may be much more meaningful for some series.
- The more detailed method involves right-clicking on the graph and selecting Properties. Then under the Graph tab you can adjust the vertical scale manually by entering a maximum and minimum, and under the View section you can select Histogram or Report view from the dropdown box instead of Line. Under the Data tab, you can choose a different color and/or line style for each series to better differentiate them. Under the Appearance and General tabs you can also further customize the display appearance, sample rate and duration for the graph. The default sample rate is once every second, and the normal visible span of the graph is 100 seconds.

Data Collector Sets can be created to allow you to schedule performance monitoring. To begin this process, right-click on the 'Performance Monitor' item in the left pane and select New>Data Collector Set. This will open the Create New Data Collector Set Wizard. Follow the prompts to define where the set will be held - typically under the *\PerfLogs* directory. You can start the collection straight away, and to stop it, right-click on the name of the new Collector Set you've created in the left pane and select Stop. To view the results at any time, go to where the log is stored and double-click on it to open it in the Performance Monitor, or find it under the Reports>User Defined area in the left pane of Performance Monitor. To schedule performance monitoring using a Data Collector Set, right-click on it and select Properties. Then under the Schedule tab click the Add button and you can set the time and day the task will begin, and over what period of time it will run.

These functions are primarily for more advanced users. When set to track key performance-related system variables over time, you can conduct normal activity on your system, such as using a range of applications and games, and then come back and read through the logs to determine which resources seem to be in greatest demand on your system, and hence may be potentially bottlenecking your performance. Alternatively, you can log performance during idle periods and see if any malicious programs are quietly running in the background, communicating with the Internet for example. There are a range of uses, but as noted, this is best suited to someone with a bit of patience and appropriate knowledge of the various parameters involved.

< SYSTEM HEALTH REPORT

A useful Windows built-in diagnostic routine is the System Health Report, which is actually a preset Data Collector Set that runs using Performance Monitor, and provides its output in a user-friendly interface. To access the System Health Report, go to Performance Information and Tools under the Windows Control Panel, click the 'Advanced Tools' link in the left pane and then select the 'Generate a system health report' link. Alternatively, type *perfmon /report* on the Start Screen and press Enter.

As soon as it launches, the System Health Report starts gathering information for 60 seconds. When complete, the report highlights any Errors, Warnings or Critical issues at the top of the report, with details of possible methods for rectifying them. Note that some errors and warnings are completely normal; for example, if you have purposely disabled a hardware device on your system, or knowingly disabled certain Windows security features, the report may highlight these.

Ideally you should run several System Health Reports, the first under normal (relatively idle) conditions, and then subsequently if you wish to troubleshoot a particular application, start the report then launch the relevant program and exit it after a minute to see what the System Health Report says.

Under the Basic System Checks section of the report, you can see the areas in which there may be potential issues. The Resource Overview section under the Performance category shows the status of system resources during the 60-second period the report was run. This is why it's useful to run a System Health Report under various system conditions, so you can better see what type of constraints your system may be facing in particular circumstances.

You can see detailed information under the various categories at the bottom of the report by clicking on the relevant category heading and sub-headings to expand them, or you can jump directly to specific areas of each category report by left-clicking once on the report icon in the middle of any of the category header, then choosing the sub-category link to investigate.

You can save any report by going to the File menu and selecting 'Save As', and the report will be saved in .HTML format, viewable in your browser. You can also email the report by selecting the 'Send To' link under the File menu.

< RESOURCE MONITOR

Resource Monitor is a utility designed to provide a real-time display of various key system resources, including CPU, Memory, Disk and Network-related data. You can access Resource Monitor by clicking the 'Open Resource Monitor' link under the 'Advanced Tools' link in the Performance Information and Tools component of Windows Control Panel, or by clicking the 'Open Resource Monitor' link at the bottom of the Performance tab of Task Manager, or by typing *resmon* on the Start Screen and pressing Enter.

Under the main Overview tab of Resource Monitor, you can see the four categories: CPU, Disk, Network and Memory. Clicking on any one of these categories expands that section, showing its components. Even without expanding each category, you can see a summary of the current resource usage courtesy of two small graphs embedded in each category header. Under the separate CPU, Memory, Disk and Network tabs of Resource Monitor are further details for each resource type.

In the right pane you can see various graphs - the number and type of these graphs changes depending on which tab of the Resource Monitor window you are viewing. You can also alter the size of these graphs by clicking the Views button just above them and selecting Large, Medium or Small, or you can close the graphs altogether by clicking the small arrow to the left of the Views button.

Throughout Resource Monitor you will see a listing of some or all of the following items in tables:

- *Image* - This is the name of an executable image file running as part of a process.
- *PID* - This is a Process Identifier number, it uniquely identifies a process.
- *File* - The full path and filename of the actual file being used by a particular process.
- *Description* - A general description for the process.
- *Status* - The current status of the process, whether it is running or stopped for example.
- *Threads* - The number of active threads for a process; more threads can be beneficial on multi-core CPUs.
- *CPU* - The current percentage of total CPU resources being used by a process.
- *Average CPU* - The average amount of total CPU resources used by a process in the last minute.
- *Read* - The average number of Bytes per second read by the process in the last minute.
- *Write* - The average number of Bytes per second written by the process in the last minute.
- *Total* - The average combination of read and writes in Bytes per second for a process in the last minute.
- *I/O Priority* - The priority of the Input/Output requests for a process; determines which request gets a higher priority. Normal is the default but it can also be Very Low, Low, High and Critical.
- *Response Time* - The disk response time in milliseconds. The higher the value the longer a disk action takes.
- *Hard Faults* - The average number of hard page faults per second for this process in the last minute. A hard page fault occurs when Windows seeks data and finds it is not in memory, and needs to load it from disk.
- *Commit* - The proportion of the virtual memory in Kilobytes reserved by Windows for the process.
- *Working Set* - The amount of physical memory in Kilobytes currently in use by the process.
- *Shareable* - The amount of physical memory in Kilobytes currently in use by the process which can be shared with other processes.
- *Private* - The amount of physical memory in Kilobytes currently in use by the process which can't be shared with other processes.

Many of the above items are covered in more detail in the Task Manager and Process Explorer sections later in this chapter.

To monitor resources, go to the relevant tab, and click on one of the columns to sort by that column. You can right-click on any column and select Hide to remove it, and choose 'Select columns' to restore it again. Once configured the way you want it, you can save your Resource Monitor configuration by going to the File menu and selecting 'Save settings as'.

You can refine the tracking of resource usage by filtering the display for particular processes. Tick the box(es) next to specific process(es) you wish to track, and the graphs to the right will display a new orange line tracking your selection. Expanding the sub-categories under any tab will also show only your selected processes, with an orange prompt at the top of the table indicating this.

If any particular process name is not clear to you, right-click on it and select 'Search online' to launch an online search on its name. You can also right-click and select 'Analyze Wait Chain' - this opens a window displaying Wait Chain Traversal information, which in simple terms allows you to see if a particular unresponsive process is waiting for another process. This lets you select and end the process blocking completion of a task. Note that stuck processes are highlighted in red under the Overview and CPU tabs, making it easier to find them in Resource Monitor.

Resource Monitor is extremely useful, because it allows you to see precisely what is occurring under the hood in Windows at any time. Aside from letting you see which particular programs are using the most resources, if you have suspicions about the behavior of a particular program - whether it is communicating with the Internet when it shouldn't be, or not utilizing CPU, memory or disk resources efficiently for example - then running that program with Resource Monitor open lets you analyze the program's behavior in detail in real-time. Similar to Task Manager, you can also start, stop, unfreeze or research any process within Resource Monitor as well. It is clearly for more advanced users, but if you learn to use it, it can be extremely powerful for both troubleshooting and performance measurement purposes.

< TASK MANAGER

The Task Manager is a key Windows utility that allows you to view real-time information about which applications, processes and services are running on your system, as well as a range of performance and system information. It is designed for both novice and advanced users, and all users need to have knowledge of its functionality, because it is sometimes required for essential purposes, such as closing frozen programs.

There are several ways of accessing Task Manager:

§ Press CTRL+ALT+DEL and select 'Task Manager'.
§ Go to the Start Screen, type *taskmgr* and press Enter.
§ Right-click on the Taskbar and select the 'Task Manager' item.
§ Right-click in the bottom left corner of the Desktop and select the 'Task Manager' item.
§ Press CTRL+SHIFT+ESC.

Task Manager has been significantly revamped in Windows 8 to make it more detailed and easier to use, as covered in this Microsoft Article. To start with, the Task Manager's default view now only shows a basic list of running Metro apps and Desktop programs for your particular user account. This replaces the Applications tab that appeared in previous versions of Task Manager. To see a range of options for each application listed here, right-click on it. The most common function here is terminating an application that is not responding, by right-clicking on it and selecting 'End Task', or selecting it and clicking the 'End Task' button. Double-clicking on any application listed here also allows you to quickly switch to it.

Click the 'More details' link at the bottom of the basic interface, and the Task Manager window will expand to provide a much more detailed interface. Task Manager has a wide range of uses, and we look at the most important of these in this section. Each tab is covered in its own section below.

PROCESSES

This tab of Task Manager contains a list of all running processes. By default this list is sorted by the Name column, which allows Task Manager to list each process alphabetically using their full descriptive names, and into different categories depending on the type of process. You should see an Apps category for any currently running Desktop programs and Metro apps; a Background Processes category for third party drivers and non-essential services; and a Windows Processes category for core Windows processes. This allows you to determine which processes are safe to terminate; typically only those found under the Apps and Background Processes categories. You can toggle this grouped display on or off by going to the View menu in Task Manager and selecting the 'Group by type' option.

Multiple instances of processes are now also grouped together under a single user-friendly title. For example, if you have several instances of Internet Explorer open, you will find all of these instances grouped under one 'Internet Explorer' item under the Apps category. Expanding it will show each separate instance underneath, allowing you to attempt to terminate a single non-responding instance of a process, rather having to close all instances of it.

You can view the actual file associated with a process by right-clicking the process and selecting Properties, or selecting 'Open File Location' to go to that file in File Explorer. Right-clicking and selecting 'Go to Details' will take you to the Details tab, which gives you greater control over the process, such as setting its Priority or Affinity - see the Details section further below.

The performance data shown under the Processes tab is color-coded, in what is known as a "heat map" style display. The more resources a particular process is using, the warmer the color used for its data in the columns on the right. For example, if a process is using over 90% of CPU resources, it will appear with a red background; if it using minimal resources, it will appear with a pale yellow background. This makes it easier to spot processes with high resource consumption. You can also click on a column header to sort by that column, allowing you to arrange processes from highest to lowest resource usage (or vice versa) for any column.

You can determine which columns are displayed here by right-clicking on a column header and ticking the appropriate columns you wish to show. The full list of column items is covered in more detail in this Microsoft Article.

PERFORMANCE

This tab is similar to the Resource Monitor utility, and indeed an 'Open Resource Monitor' button is available at the bottom of this window for more advanced users. However, this tab provides a much easier-to-understand way to undertake basic monitoring of resource usage, as long as you understand the data being displayed. The display has also changed from previous versions of Task Manager, so it will all be clarified in detail.

There are four categories of performance data available here: CPU, Memory, Disks, and Network Connection. When you select the relevant category on the left side, more details and a full graph are shown for that category on the right side. Note that if you double-click on the graph display, it will maximize to only show the graph, hiding all other Task Manager features and data - this is known as 'Graph Summary View'. Double-click on the graph, or right-click on it and untick 'Graph Summary View', to revert back to the full Task Manager view.

You can alter how quickly each graph updates its data by going to the View menu and selecting 'Update Speed'. The default is Normal, which updates the data shown once a second. You can instead choose Low to slow down the updating to once every 4 seconds, or Fast, which updates twice a second. You can also pause updating altogether.

The main components of the Performance tab are described below:

CPU: The main graph in this section shows a time series of the total proportion of all available CPU resources used. If you have a multi-core CPU, the percentage shown here is an average across all cores, not the sum. For example, on a dual core CPU, if one core is at 100% utilization, and the other is at 0%, the graph shows a total CPU usage of 50%. The readout on this graph corresponds with the Utilization percentage shown beneath it. You can alter the CPU graph to display the utilization on each individual core by right-clicking on the graph and selecting Change graph to>Logical Processors. Note that the number of cores on a CPU may not be the same as the number of logical processors if HyperThreading is enabled.

Beneath the CPU graph you will find useful details of your CPU hardware, including its maximum and current speed - the current speed may be much lower than the maximum speed, as the CPU may be throttling down to conserve power. It also shows the number of sockets (typically only 1 on a home PC), the number of cores and logical processors, whether there is hardware support for virtualization, and your various CPU cache sizes.

The additional components related to the CPU section are described below:

§ Processes - The total number of individual processes running on your system, as individually listed under the Processes tab.
§ Threads - The total number of threads being run by all active processes on the system.
§ Handles - The total number of unique objects in use by all processes, such as files and Registry keys.
§ Up Time - The length of time since the PC was last booted up, in days : hours : minutes : seconds format.

For more details of processes and threads, see this Microsoft Article; for more details of handles, see this Microsoft Article.

Memory: The main 'Memory usage' graph shows the amount of physical RAM currently in use, as a percentage of total installed physical RAM. The smaller 'Memory composition' graph beneath it shows a breakdown of the how your physical RAM is being used. Beneath the graphs, there is more detailed memory information, including the RAM speed and number of RAM slots.

The important memory components displayed here are explained in more detail below:

§ Total Memory - Shown at the top right of the Memory section, this is the actual amount of physical RAM you have installed on your system.
§ Hardware reserved - This is the portion of physical RAM reserved for hardware, such as video cards, and hence is not available for Windows to use. On 64-bit systems it is usually quite small; but on 32-bit systems it can reach up to 1GB, which is why a 32-bit system with 4GB of RAM will only show around 3GB of accessible memory.
§ In Use - This is the total amount of memory used by running processes, drivers, and other Windows components, excluding the Cache.
§ Available - This is the amount of memory available for use by any process if required. It is the sum of any free (unused) RAM along with Cached memory.
§ Committed - This is displayed in the form Current Commit Charge / Commit Limit. The Commit Charge shows in Gigabytes the memory currently required by all running processes - that is, committed memory, both physical and virtual. The Commit Limit is also in Gigabytes, and is approximately the sum of physical RAM plus your Pagefile. This is the maximum amount of memory the system can commit to processes if needed. The Commit Charge can never exceed the Commit Limit, and should always be much lower than the limit. If it gets close to the limit, Windows will increase the Pagefile size if it's not fixed; if it hits the limit you will run out of memory resources and may experience data loss or

other problems. See the Windows Memory Management section of the Memory Optimization chapter for details of how to correctly set the Pagefile size, and hence have an appropriate Commit Limit.

§ Cached - Also known as Standby memory, this is the amount of memory currently used by the system for holding a range of commonly used data in RAM for quick access. This is associated with the SuperFetch feature - see the Windows Memory Management section of the Memory Optimization chapter for details.

§ Paged Pool - Shows the portion of data used by the core of Windows held in memory which can be safely paged out to disk at any time. Not to be confused with the Pagefile.

§ Non-paged Pool - Shows the portion of the core Windows data which can't be paged out to disk, as this might cause problems under certain circumstances, hence it is always stored in RAM. Again, not to be confused with the Pagefile.

For more details of physical memory usage in Windows, see this Microsoft Article; for more details of Paged and Non- paged Pool memory, see this Microsoft Article; and for more details of committed memory, see this Microsoft Article.

Disk: This section shows the drives you currently have connected to the system. There will be one item for each drive, and clicking on that drive in the left pane will show a separate graph for that drive on the right. The main graph shows the Active Time for the drive as a percentage, which equates to how much of its time the drive is actively processing read and/or write requests. The smaller graph beneath shows the actual Disk Transfer Rate for reads (solid line) and writes (dotted line), in hundreds of KB/s.

You can see precise readouts of the Active Time percentage, and the separate Read and Write speeds in KB/s underneath the graphs. The Average Response Time shows the amount of time in milliseconds (1,000ms = 1 second) for the drive to currently respond to a read or write request. This area also shows you the drive's capacity, whether it is a System disk (i.e. holds core Windows files), and whether it holds the Pagefile.

Network: This section is typically labeled with the adapter name of your network/Internet connection, such as Ethernet. The main graph shows the Send and Receive activity on the connection in hundreds of Kbps. The solid line on the graph is Receive activity, while the dotted line is Send activity.

For a more detailed display of network information, right-click on the graph and select 'View network details'. This will show additional data such as total Bytes sent and received during the current session, broken down into Bytes sent and Bytes received.

The Performance tab of Task Manager can be extremely useful in quickly and easily monitoring your system's key components. The left section of the Performance tab in particular shows the most important data from each category at a glance, so most of the time you only need to open Task Manager and look at this section to get a good overview of system performance. For more detailed system monitoring, consider using the Resource Monitor instead, as covered in an earlier section of this chapter.

APP HISTORY

This tab provides an overview of the resource usage history for Metro apps on the current user account. The history display dates back to when you first installed Windows 8. Similar to the Processes tab, this area shows the data in a "heat map" display, with apps that use more resources having progressively warmer colored backgrounds. This allows you to quickly see which apps have been using the most CPU or Network resources for example. You can also sort by any column, or right-click on any column header to add new columns, such as Downloads or Uploads.

START-UP

The functionality of the Start-up tab of Task Manager is covered in detail under the Finding Startup Programs section of the Startup Programs chapter.

USERS

Displays all user accounts that can access the system in the current session. It allows you to view a range of details on their resource usage and running processes, as well as being able to logoff or disconnect any user if required.

DETAILS

This tab is similar to the Processes tab under previous versions of Task Manager. In Windows 8 it contains full details of all processes currently running on your PC for all users. The processes are shown by filename, rather than their user-friendly name, and multiple instances of any process are shown separately, rather than being grouped together.

You can view a range of real-time details about each process by right-clicking on any column header, choosing the 'Select Columns' item, and then ticking the appropriate column(s) to display. The column items are covered in more detail in this Microsoft Article. You can click on a column header to sort by that column, allowing you to sort all processes by those using the most CPU resources for example.

You can view the actual file associated with a process by right-clicking the process and selecting Properties, or selecting 'Open File Location' to go to that file in File Explorer. You can also right-click and select 'End Process' to close it, or 'End Process Tree' to close the process and all associated processes. Right-clicking and selecting 'Go to Service(s)' will take you to the Services tab, highlighting the particular Services associated with the process, if any. The 'Set Priority' and 'Set Affinity' options control the allocation of CPU resources, and are covered in more detail later in this section. The 'Analyze Wait Chain' option is covered in more detail under the Resource Monitor section earlier in this chapter.

SERVICES

This tab lists all of the services on the system, and whether they are currently running or not. You can right-click on any Service and select 'Go to details' (if available) to go to the running process under the Details tab associated with that service. In many cases it will be the general *svchost.exe* (Service Host) Windows process, of which there are multiple instances. You can also start or stop a service here by right-clicking on it. See the Services chapter for more details.

GENERAL USAGE

The most common use for Task Manager is to allow you to close a problematic program that is unresponsive, or has frozen the system in some way. Whenever a program stops responding, Windows should automatically prompt you to close the non-responsive program after a short period. In some cases this does not occur because the program hasn't technically stopped responding, it simply isn't allowing you to see its output or let you interact with it directly. In these cases pressing CTRL+ALT+DEL should return sufficient responsiveness to the system to allow you to open Task Manager, and either under the Applications list, or under the Processes tab, select the relevant program and choose 'End Task'. Windows 8 does a good job of isolating the core of Windows and thus maintaining some level of system responsiveness, so this method tends to work most of the time. If you can't access Task Manager, and if after a period of waiting you do not gain responsiveness, you can force a system shutdown by holding down the power button on your PC for 5 seconds.

Another common use for Task Manager is to detect whether a particular program is using unnecessarily high levels of system resources. Open Task Manager while the suspected program is active, and go to the

Processes tab. With the new "heat map" style of display, you should instantly see any process that is using up large portions of CPU or memory, as it will have a warmer color.

In some cases a program can become caught in a loop, or have some other kind of error that causes it to use up all available CPU or Memory resources for no apparent reason, or out of all proportion to the task it is undertaking. Manually end the process, restart the program and see if it happens again - if so then it may well be a bug, such as a memory leak.

Yet another common use for Task Manager is to detect background processes or services that a recently installed program may be running without your knowledge. An examination of all running processes under the Details tab may allow you to spot an unfamiliar process, which you can either right-click on and select 'Open File Location' to see where it resides on your system, or right-click and select 'Search Online' to find out more about it. Similarly, any new services under the Services tab bear investigation, by right-clicking on them and selecting 'Go to Process'. This is also one way of detecting potential malware on your system, as most malware can't hide from the full list of running processes in the Details tab of Task Manager. Once you have found a potentially unnecessary new process or service, you can investigate and remove it as covered in the Startup Programs, Services or Security chapters as relevant.

If you can't easily resolve a process-related issue, then you can create a special file that contains debugging information for use by yourself or a trusted technical support person. Right-click on the relevant process you believe to be problematic or suspicious and select 'Create Dump File'. A .DMP file with the name of the process will be created under your *\Users\[username]\AppData\Local\Temp* directory. The file may be quite large, and you can't open or view its contents normally. You, or someone with relevant expertise, must use the Windows Debugging Tools to view and troubleshoot the contents.

PROCESSOR AFFINITY AND PRIORITY

Task Manager allows you to manually set the priority and affinity for each process. These functions require more detailed explanation.

Set Priority: Right-click on a process under the Details tab, and you can select 'Set Priority' to determine the priority with which the threads for a process are run. The default is Normal, but the available options are Low, Below Normal, Normal, Above Normal, High and Realtime. Altering the priority can change the order in which threads are processed by your CPU, making a particular process more responsive for example if it is given a higher priority. However this can also destabilize the system, and in practice, Windows 8 already has an excellent prioritization system. If you're running a program in the foreground and it needs more resources, it will get them - see the Processor Scheduling setting below. Furthermore, if you disable unnecessary background programs as recommended in this book, then your primary program will be the major focus of processing regardless. As such, it is not recommended that you alter priority for any process in this way, unless it is specifically recommended by a developer as a fix for a known problem, or unless you frequently multi-task and want to ensure a particular program always gets more resources.

If priority for a process is set in Task Manager in this manner, this new priority level only lasts as long as the process is running in the current session, so if you experiment with this option, the effect is not permanent. If however you wish to permanently implement a priority change for a particular program, you can do so by going to the program's launch icon, right-clicking on it and selecting Properties. In the Target box enter the text below exactly as shown, positioning it in front of the text already in the Target box. Make sure there is one blank space between the end of the text below and the start of the existing text in the Target box:

```
%windir%\system32\cmd.exe /c start "" /high
```

Substitute any other priority level you wish to use in place of the `/high` switch, e.g. `/realtime`.

Processor Scheduling: There is an additional setting in Windows that affects processor scheduling. Go to the Windows Control Panel, open the System component, click the 'Advanced system settings' link on the left side, and click the Settings button under the Performance section of the Advanced tab. In the window that opens, under the Advanced tab you can choose the way in which Windows allocates processor resources in the Processor Scheduling area. The Programs option allocates more resources to the program running in the foreground, and is strongly recommended. The 'Background services' option allocates CPU resources more evenly across all running processes, and is designed for systems running multiple and equally important tasks at the same time, such as web servers. Selecting 'Background services' here can result in decreased performance when using system-intensive applications and games, which is why it is not recommended.

Set Affinity: Processor affinity is a property that makes a particular thread or process run on a particular core of a multi-core CPU. This can result in improved performance or stability for some programs, but has to be weighed against the fact that it can also work to reduce load balancing across all the cores of a CPU. You can manually alter the affinity for a particular process by right-clicking on it under the Details tab of Task Manager and selecting Set Affinity. A window will open allowing you to selecting which core(s) of your CPU are allowed to run this particular process. For the most part, there is no reason to alter affinity manually.

One valid reason for manually altering the affinity for any process is for troubleshooting purposes, such as in the case of an old program not designed for multi-core CPUs. By restricting such a program to a single core of your CPU, you can emulate a single-core CPU environment for that particular program, and thus resolve potential problems. However setting affinity in the Task Manager is temporary, as it lasts only for the current session. To permanently set affinity for any program, you can use the following instructions:

1. Download ImageCFG.zip, extract the *imagecfg.exe* file and place it into your *\Windows\System32* directory. The file was originally a Windows NT system file.
2. Identify the problematic program's main executable. To do this go to the program's launch icon, right-click on it, select Properties and highlight and copy the text in the Target box.
3. Make a backup copy of this program executable first and put it somewhere safe, because ImageCFG permanently alters the executable to which it is applied.
4. Open an Administrator Command Prompt.
5. In the command prompt window type `ImageCFG /?` for a list of valid commands. For example, to set the affinity for a program to Core 1 on your CPU, type the following and press Enter:

   `ImageCFG -a 0x1 "program path/filename"`

   Obtain the *program path/filename* from Step 2 above, and note that the path and filename must be contained in quotes, e.g.:

   `ImageCFG -a 0x1 "C:\Program Files\RegCleaner\RegCleanr.exe"`

6. Whenever this modified executable file is launched from now on, Windows will only allow that program to use the specified CPU core. Restore your backed-up executable to undo this change, and importantly, never attempt to alter affinity on a Windows system file in this manner.

Once again, altering affinity is not recommended unless there is no other method of getting a program to function correctly on a multi-core CPU.

As you can see, the new Task Manager has a range of useful functions for all levels of users.

PROCESS EXPLORER

Similar to the Resource Monitor utility covered earlier, and also like Task Manager in many ways, Process Explorer is a free utility that provides far greater ability to analyze system resource usage in depth. It is too comprehensive to be covered here in detail, however several features are worth noting.

If you right-click on a particular process and select the Properties item, it opens a window with a range of tabs providing detailed information, such as the individual performance, security and thread data for this process. Under the main Image tab of the properties, you can click the Verify button to determine whether the file has a verified signature.

In the main Process Explorer window, under the View menu you can select 'System Information' to open a new window with a data display similar to that under the Performance tab of Task Manager. However here you can see a range of additional data, such as GPU (graphics card) usage, and a great deal of extra information on memory-related parameters under the Memory tab.

Importantly, you can also see actual Pagefile behavior here under the Paging section. Page Fault Delta for example displays drive usage when Windows can't find the required information in memory, while the Paging File Write Delta shows how much is being written to the Pagefile at the moment. These are real-time displays, so to actually track these values over time and get an indication of how much is being written to the Pagefile and how often, you would need to use Performance Monitor to log these types of variables over time - add the 'Paging File Usage %' item to the counters in Performance Monitor for example.

Process Explorer is a very useful tool to have on your system, though it is targeted towards advanced users.

< WINDOWS MEMORY DIAGNOSTIC

Windows Memory Diagnostic is a built-in troubleshooting utility that is usually automatically triggered when Windows detects that a problem may be caused by your physical memory subset: the system RAM and CPU caches. You can opt to manually run the tool at any time if you suspect memory-related problems with your system RAM or CPU memory caches, by opening the Windows Control Panel, selecting the Administrative Tools component, then selecting Windows Memory Diagnostic, or by typing *memory diagnostic* on the Start Screen, selecting Settings and pressing Enter.

The tool must be run at the next reboot. It needs to run prior to Windows startup, because that is the optimal time when RAM is free of any operating system or other software components residing in it. Accordingly, you can choose to 'Restart now and check for problems' to launch it immediately, or you can schedule it to run the next time you restart by selecting 'Check for problems the next time I start my computer'. If Windows has raised this prompt, or you suspect memory problems, it is strongly recommended that you run the test as soon as possible to prevent any data corruption or data loss due to faulty or unstable memory.

Windows Memory Diagnostic conducts a series of tests to determine whether your memory subset is faulty. You can choose which tests it runs by pressing F1 as soon as the tool starts, and selecting from the following options, pressing TAB to move between option categories:

- Test mix - Select the type of test you want to run, whether Basic, Standard or Extended. Standard is recommended to begin with, and Extended is recommended if you want to do a more strenuous test of your RAM, but is very lengthy.
- Cache - Select whether to have the CPU caches On or Off, or the Default, which adjusts the cache depending on the test. I recommend Default to begin with, and then rerun the test with it Off if you wish to isolate your RAM, and hence determine whether it is a RAM-related error, or a CPU cache-related error.

§ Pass count - The number of times you want to repeat the test, with 0 being infinite. I recommend 2 passes to start with, more if you really want to stress test your memory.

Press F10 to confirm your choices and start the test. Progress will be shown both for each test and the overall progress for all tests. This may take some time to complete depending on the options you've chosen. If you suspect a memory-related problem, the longer and more strenuous the testing, the better (e.g. 2 hours of testing). This will bring out any latent instability in your RAM or CPU caches. You will be told if an error is found, and what it may be related to, but if your memory subset is clear of problems then no issues should be identified.

If errors are found you can try the following:

§ Reduce or remove any overclocking on your motherboard, RAM or CPU, including any RAM timing changes, then rerun the tests. If no problems occur then clearly the issue is with your components being pushed too far by overclocking, or you have reduced the RAM latencies too much. See the Overclocking section of the Hardware Management chapter.
§ Rerun the tests with only one stick of RAM installed at a time. Windows may even tell you which particular memory stick is faulty, so remove it and rerun the tests to confirm.
§ Increase cooling in your case and make sure to remove any clutter or dust around the CPU and RAM in particular, and anything blocking the free flow of air into and out of the case. If running in a hotter environment, such as during Summer, you may need additional case cooling. See the Hardware Management section under the Hardware Management chapter for more details.

The Windows Memory Diagnostic tool, while thorough, can only detect hardware-related memory errors, so see the other tools in this chapter for detecting errors related to your Windows or software configuration. Keep in mind that if the Memory Diagnostic tool does detect a problem it is very likely that your RAM is physically faulty or misconfigured in your BIOS/UEFI, and if ignored, will lead to further problems and potentially serious data corruption, or data loss.

< WINDOWS ERRORS

Regardless of how many troubleshooting utilities and built-in self diagnostic routines Windows contains, you may still experience a range of error messages or problems that cannot easily be resolved. Some problems are caused by faulty hardware or adverse conditions (e.g. overheating), or by incompatible third party software or problematic drivers, and these are virtually impossible for Windows to self-diagnose. You must investigate these issues further yourself to work out what the problem may be related to.

For major errors you will receive what is commonly known as a Blue Screen of Death (BSOD) error, or simply a Blue Screen error, more formally known as Bug Check. In previous versions of Windows, this error screen with a blue background listed a detailed error message and provided error codes. As of Windows 8, the BSOD has been redesigned. It now simply shows a sad face, along with: "Your PC ran into a problem and needs to restart". A technical error code is provided, following the phrase "If you'd like to know more, you can search online later for this error:".

By default Windows is set to automatically reboot when it experiences a serious error. To prevent this from happening, open Windows Control Panel, select the System component and click the 'Advanced System Settings' link in the left pane, or type *systempropertiesadvanced* on the Start Screen and press Enter. Then under the Advanced tab, click the Settings button under the 'Startup and Recovery' section, and untick the 'Automatically restart' box. Now when a major error occurs your system will freeze, and I recommend making a note of the exact error message provided. You can then manually restart or shutdown your PC.

In other instances, you will see a Windows dialog box pop up with an error message, or with specific error codes. Once again, note down the exact message and any error codes associated with it.

If the problem you're experiencing doesn't have a specific error message or number, such as a sudden reboot of your system, or an unexpected crash from a program to the Desktop, then note down the application or procedure involved when you triggered the error, or use Problem Steps Recorder to record this information - see earlier in this chapter.

To assist in resolving any type of Windows error, you can search through the following official Microsoft resources:

Blue Screen Error Codes
Microsoft Solution Center
Microsoft Knowledgebase
Microsoft TechNet
Microsoft Events & Errors Message Center

If nothing is found in the resources above, conduct a thorough web search using the error number or exact error phrase, the name of any specific file(s) involved in the error, or keywords from a layman's description of the error. This often provides excellent leads for finding out more information from others with the same problem, and what they've attempted to do to resolve it, at the very least saving you time and effort in otherwise trying false solutions.

Most any problem can be resolved if researched using the links above, as well as by using the tools in this chapter. It may not be quick or easy, but often it is the only way.

< THIRD PARTY TOOLS

Although Windows contains a range of performance measurement and troubleshooting tools, there are several third party tools that can be just as valuable in helping you to measure the performance of various aspects of your PC, and also assist you further in troubleshooting problems. These are covered in this section.

3DMARK

3DMark is a 3D graphics benchmarking utility that primarily utilizes your graphics card, and to a lesser extent the CPU and memory. 3DMark provides you with a good indication of advanced 3D gaming performance on your machine. It also allows you to compare your system's gaming performance with other systems, and broadly speaking the system with a higher 3DMark score is generally better for gaming purposes. There are several versions of 3DMark dating back to 1999. The latest version is recommended if your graphics hardware supports DirectX 11.

Once you have launched a benchmark run in 3DMark, the resulting score can be compared with other people who have run the same benchmark at the same settings, and this will tell you whether your system is relatively faster or slower. If compared with others who have very similar system specifications, it will also tell you whether you have room to improve performance on your particular system. Note that some systems which 3DMark considers similar to yours may be heavily overclocked just to get a high 3DMark score, and are not particularly stable for day-to-day use.

HEAVEN

Heaven is a free DirectX 11 graphics benchmark that also supports DirectX 9, DirectX 10 and OpenGL. To run the benchmark, launch Heaven and adjust the settings as desired, then click the Run button. The Heaven demo will begin, and you can see an FPS counter at the top right, and can access a range of options by pressing the ESC key. To commence an actual benchmark run you will need to press the F9 key. Once completed you will see a result in both FPS and numerical Score - compare this with others who have run

Heaven with exactly the same settings as you to gauge your relative performance. Note that there are also the older Tropics and Sanctuary GPU benchmarks available from the same site, and both support DirectX 10 and DirectX 9 as well as OpenGL.

FurMark

FurMark is an intensive OpenGL-based graphics benchmark that also doubles as a stress tester. After installing the program, you can either run a Burn-in test to stress test your GPU; run a Burn-in benchmark that stress tests and benchmarks your system; or run a custom Benchmark. You can upload and compare any benchmark results with other FurMark users. If you experience any graphical glitches or problems while running FurMark, this is a sign that your graphics card is not being cooled sufficiently or is overclocked too far. Do not run the burn-in test if your system is already extremely unstable, or if you suspect faulty hardware components, as this could accelerate their demise.

Game Benchmarks

While graphical benchmarking utilities are useful, they are entirely synthetic. The most realistic form of graphical benchmarking and stress testing is through the use of recent high-end 3D games. Modern PC games are the most practical and system intensive benchmarks you can use, because they stress almost all areas of your system: the CPU, the graphics card, your memory and your drive(s), as well as general Windows stability.

If you can't find a built-in benchmarking feature for a game, simply select the most strenuous game you have - that is, the one with the most graphical detail, best artificial intelligence and physics - and use the FRAPS utility to measure performance over a set period of time. You can assign a key to start and stop the benchmarking process in FRAPS, or you can tell FRAPS to stop benchmarking automatically after a period of time. You can specify the benchmarking stats to save, such as minimum, maximum and average frames per second. These results can then be compared with others to give you a general idea of your overall performance.

To use any strenuous game as a stress tester, simply play it continuously for a sustained period of time, such as two or three hours, at the highest settings your system will support. If the game crashes at any point, then this is usually a good indication that your system is not completely stable. Contrary to popular belief, it is not normal for games to crash regularly, and you should not fall into the trap of blaming everything but your own system and its configuration for any problems. The vast majority of game-related problems are due to individual system configuration or hardware issues, not the game.

PCMark

PCMark is a general benchmarking utility from the makers of 3DMark. It runs a series of tests based on such activities as file encoding, disk reads/writes and basic graphics display. To use PCMark run the program and click the 'Run PCMark' button on the main screen. After several tests it arrives at a score you can compare with others. Note that PCMark results are not comparable to 3DMark results, or with earlier versions of PCMark.

Sandra

Sandra is discussed under the System Specifications chapter, however in this chapter we look at the modules designed to test certain components of your system, such as the CPU, RAM, or drives. The free Lite version of Sandra is limited in the particular modules you can access, and hence the tests you can run, however it has sufficient benchmarking capabilities for our purposes.

Click the Benchmarks tab and you will see a range of modules such as Processor Arithmetic, Physical Disks and Cache and Memory Latency. To run a benchmark, open the appropriate module and press F5 or click

the blue arrow (Refresh) icon at the bottom of the module. This will begin a benchmarking run, after which you will eventually see the results displayed in the bottom pane of the module. You can put the benchmarking results in context by looking at the results for other reference systems also provided. You can also change the reference data to reflect a variety of hardware to compare against, by clicking the relevant boxes in the left pane.

Sandra also has a role as a diagnostic tool. To use it as a stress tester of specific components on your system, use the relevant modules under the Benchmarking tab. However, instead of simply running it once, if you want to stress test a component, you can run the benchmark several times in a row by refreshing it whenever it completes To automate the process, Sandra has a Burn-in module under the Tools tab which will undertake more thorough stress testing of your machine. Start the wizard, tick the components you want to continually stress test, set the number of times for them to loop, or the period over which you want to perform these test, make sure the 'Monitor your computer's health' and 'Terminate on overheat/failure' boxes are ticked to be safe, and then commence the stress testing.

PRIME95

Prime95 is a small mathematics program that will effectively stress test only your CPU and memory. Once you've downloaded the application, run *Prime95.exe* and click the 'Just Stress Testing' button. You should automatically be prompted to select a test, but if not, under the Options menu select 'Torture Test' to start stress testing. Select the test type based on the particular components you want to focus on testing:

§ Small FFTs - Select if you want to primarily test your CPU and its caches.
§ In-place Large FFTs - Select if you want to test your CPU, and to a lesser extent your RAM, for stability under high heat and voltage usage.
§ Blend - Select if you want a more 'real word' test which tests both the CPU and RAM.

Once you click OK the testing will begin and Prime95 will open multiple threads to ensure all of your logical CPU cores are being fully utilized. If at any point you want to stop the test, go to the Test menu and select Stop. If the program aborts with an error at any time, this indicates system instability. In general if your PC can run the test for over one or two continuous hours, it shows that the CPU and memory subset are quite stable. However, Prime95 is still just a synthetic test that only artificially stresses your CPU and RAM, and regardless of how long you can run it without errors, it is not indicative of a completely stable system. Only running real-world applications and games without problems can truly confirm this.

SUPER PI

Super PI is a small utility similar to Prime95, in that it stress tests your CPU and memory by calculating the mathematical number PI to a certain number of places. Download it and run the *super_pi_mod.exe* file. Click the Calculate menu item at the top, and select the number of places to calculate PI to, ranking from 16 thousand (16k) to 32 million (32M) places - the larger the number of places, the longer it will take.

For a speed test of your CPU, select the 1M option and once the calculation is done, note the precise time taken before clicking OK. You can then compare this figure to other people to see how fast your CPU is in raw calculation power relative to theirs. If you want to stress test your CPU, run the full 32M calculation which will take longer, and hence is a better stress test of your CPU. Once again you can compare the time taken to complete this with other users.

HD TUNE

HD Tune is a drive information and benchmarking utility that has been covered elsewhere in this book, including in the System Specifications and Drive Optimization chapters. It can be used on both hard drives and SSDs. You can run a drive benchmark in HD Tune by clicking the Start button on the main Benchmark tab. The test will provide a real-time mapping of drive performance, and the final results will be displayed for use in online comparisons.

AS SSD BENCHMARK

The AS SSD Benchmark is specifically designed for Solid State Drives, but also works on hard drives. Download and install the utility, then launch it. Make sure that the drive you wish to benchmark is selected from the drop-down box at the top left, then click the Start button to commence benchmarking. The benchmark will eventually show your drive's Read and Write speeds for three types of tests, as well as Access Time and an overall score. You can then compare these with other SSD users to determine your SSD's performance.

ATTO DISK BENCHMARK

ATTO Disk Benchmark is another utility commonly used for both SSD and hard drive benchmarking. Launch the *Bench32.exe* file, select the drive you wish to benchmark at the top left, then click the Start button to commence benchmarking. A series of Read and Write results will be shown in the chart at the bottom. Compare these with other users to see where your drive's performance sits in relative terms.

MEMTEST

MemTest is a simple Windows-based memory testing utility that will help in stress testing your Windows memory configuration to detect any potential problems. The key difference between MemTest and Windows Memory Diagnostic is that the latter is designed to only test your memory hardware, while MemTest is useful in simulating a heavy memory load within Windows, which tests the software environment as well as the memory hardware.

To use MemTest simply launch the program, and I recommend manually entering the amount of RAM (in MB) that you wish to test. For example, enter 512 to test 512MB of RAM, 1024 for 1GB, or 2048 to test 2GB of RAM. You may need to run multiple instances of MemTest to use up all of your system RAM. Click the 'Start Testing' button to begin RAM testing and allow the test to run until it has reached 100%. Ideally you should run the test for at least an hour if testing for Windows stability.

If running the test triggers any errors, Windows-related warnings or prompts, then you have potentially faulty Windows settings, or your RAM is faulty, or the memory-related settings in your BIOS/UEFI are mis-configured. To test specifically for faulty RAM hardware, run the Windows Memory Diagnostic as covered earlier in this chapter. If that results in no errors, then it will narrow down the cause to your Windows settings and any installed programs that may be causing conflicts.

That covers the main performance measurement and troubleshooting tools you can use to solve problems and optimize your system. There are many other programs that can be used for this purpose, but the ones in this chapter should be the most reliable and the easiest free tools to use under Windows 8.

Importantly, despite any promises you may read to the contrary, there are no tools that can automatically diagnose and fix all of your problems. Many tools are advertised as being able to do this, but I can assure you that no such tools actually exist. The causes of PC problems are often very complex and inter-related, and can be a combination of hardware problems along with incorrect settings or driver problems. Furthermore, every system is unique in terms of the hardware it contains, the software installed on it, the configuration of that software and the interactions between the various software, and even the physical environment in which it sits. All of these variables can individually or collectively have a tangible impact on system stability and performance.

The best way to diagnose any issue and optimize your system correctly is to gain an intuitive understanding of how your system works, combined with research and thought. If there really was an automated way to resolve most problems, everyone would be using it by now, and similarly, Microsoft would have purchased the rights to it and incorporated it into Windows, rather than providing so many different diagnostic and performance measurement tools and options in Windows 8.

CLEANING WINDOWS

As you use your system in day-to-day activities, a range of temporary, backup and log files are created on your drive. Many of these files are automatically deleted whenever you close an application, or whenever you shut down Windows. Unfortunately, some of them will remain on your system, and over time they can build up, taking up disk space and cluttering your directories. This chapter looks at the tools and methods required to safely clean out unnecessary files from Windows.

< RECYCLE BIN

The Recycle Bin provides a storage area for deleted files and acts as an additional layer of protection against accidentally deleting desirable files on your system. It exists as a hidden folder called *\$Recycle.bin* in the base directory of every drive of your system. Any time you highlight a file or folder and press the Delete key, or right-click on and select Delete, it will be moved to the Recycle Bin first by default. If the file or folder is then permanently deleted from the Recycle Bin, it is not actually deleted at all - the file is simply removed from view, and the area it resides in on the drive is marked as available space. You can still recover these deleted files in some cases, as covered under the Data Recovery section of the Backup & Recovery chapter.

To access the configuration options for the Recycle Bin, right-click on it on the Desktop and select Properties. If you can't see the Recycle Bin on the Desktop, see further below.

Custom Size: This option sets the maximum amount of drive space that can be used by the Recycle Bin should it need it. Highlight the drive you wish to set the space for, and then enter an amount in Megabytes (MB), with the minimum amount being 1MB. I strongly recommend allocating a decent amount of space here, at least as large as the largest files you are likely to delete from the selected drive, otherwise if the Recycle Bin is not large enough, your only available option will be to permanently delete files instead. On drives where this is not important, you can set the Recycle Bin to its minimum size of 1MB, but on the primary system drive I recommend a reasonably large Recycle Bin to prevent accidental permanent deletion of desirable files.

Don't move files to the Recycle Bin. Remove files immediately when deleted: If this option is ticked, any file or folder that is deleted in Windows will bypass the Recycle Bin and be deleted permanently. I strongly recommend against ticking this option, as the Recycle Bin provides an important layer of protection against accidental deletion of important files or folders. If you wish to permanently delete individual files on a case by case basis instead, hold down the SHIFT button at the same time as pressing the Delete key to temporarily bypass the Recycle Bin.

Display delete confirmation dialog: If ticked, every time you choose to delete a file, you will be asked if you wish to continue. As long as you have the Recycle Bin enabled, then I recommend unticking this option, unless you want to be prompted each time you delete a file.

REMOVE RECYCLE BIN FROM DESKTOP

If you wish to remove the Recycle Bin from your Desktop, go to the Windows Control Panel, select the Personalization component, then click the 'Change desktop icons' link on the left side. Here you can tick or untick the 'Recycle Bin' item to show or hide this component on the Desktop. You can also change the icon used for the Recycle Bin if you wish - highlight the Recycle Bin (full) or Recycle Bin (empty) icon displayed here, click the 'Change icon' button, then select a new icon to use, or click Browse to find and select additional icons.

If you wish to have a Desktop completely clear of icons, but still wish to retain the Recycle Bin, you can pin it to your Taskbar, or to the Start Screen. To pin it to your Start Screen, right-click on the Recycle Bin and select 'Pin to Start'. If pinned to the Start Menu, it will act just like the Desktop Recycle Bin, including indicating whether it is full or empty with the appropriate icon.

However, because the Recycle Bin is an Explorer-based interface, if pinned to the Taskbar through normal means, it will become a pinned location under the File Explorer icon. To create a separate Recycle Bin Taskbar icon, do the following:

1. Right-click on an empty area of the Desktop and select New>Shortcut.
2. Type the following in the location box and click Next:

   ```
   %SystemRoot%\explorer.exe shell:RecycleBinFolder
   ```

3. Name the shortcut *Recycle Bin* and click Finish.
4. Right-click on this new shortcut, select Properties.
5. Click the 'Change icon' button under the shortcut tab, browse to the following file and click Open:

   \Windows\system32\imageres.dll

6. Select the Recycle Bin icon from the list presented and click Apply.
7. Right-click on this shortcut and select 'Pin to Taskbar'.

If pinned to the Taskbar, the Recycle Bin will not display a dynamic full or empty icon to indicate whether it is holding any deleted files like it normally would.

< DISK CLEAN-UP

The built-in Disk Clean-up utility provides the ability to automatically find and safely remove a range of unnecessary files. To access the Disk Clean-up utility, open File Explorer, right-click on the drive you wish to clean, select Properties and under the General tab click the 'Disk Clean-up' button; alternatively, you can type *cleanmgr* on the Start Screen and press Enter. To access all the cleaning options of the utility, click the 'Clean up system files' button at the bottom of the Disk Clean-up window.

There are two main tabs in the Disk Clean-up window, though the 'More Options' tab is only visible if you have clicked the 'Clean up system files' button. The contents of these tabs are covered in detail below:

Disk Clean-up: There are a range of components you can choose to clean out, and these are listed here. Highlight each one and a description will appear in the box below the list. All of these categories are safe to remove, as none are necessary for Windows to function correctly. Highlight a category and click the 'View files' button if available to see precisely which files and folders will be deleted.

Keep in mind the following when selecting components to clean out:

§ Downloaded Program Files - Deleting these may simply mean you have to redownload them the next time you visit your favorite websites, slowing down browsing, so only clean them out periodically.
§ Temporary Internet Files - If you use Internet Explorer, deleting these cached files can slow down browsing speed. See the Basic Settings section of the Internet Explorer chapter.
§ Thumbnails - These are stored thumbnails for any files you have viewed in Icon or Content view in File Explorer. Deleting these files means they will have to be recreated the next time you view such folders in the same view, which can slow down browsing. See the Basic Features section of the File Explorer chapter.

§ Windows Error Reports - These components store your Windows error reports, as covered under the Windows Action Center section of the Performance Measurement & Troubleshooting chapter. Don't delete these if you want to send any error reports to Microsoft.

Once the relevant components have been selected, click OK to remove the files.

More options: Under this tab you will be able to access the Programs and Features area of Windows by clicking the 'Clean up' button under the Programs and Features area. See the Programs and Features section of the Windows Control Panel chapter for more details.

The second option here is more important, as clicking the 'Clean up' button under the 'System Restore and Shadow Copies' area will bring up a prompt asking you if you wish to delete all of your System Restore points except for the most recent. This feature is covered in more detail under the System Protection section of the Backup & Recovery chapter. If your system is performing without any problems, then it is usually fine to click this option, as older Restore Points can take up a substantial amount of disk space.

ADVANCED DISK CLEAN-UP

There is a more advanced form of the Disk Clean-up utility that provides additional options you can select for cleanup, along with the original options covered above. To activate it, you must type the following in a Command Prompt, or on the Start Screen:

```
Cleanmgr /sageset:1
```

The number after the `/sageset` switch can be anything from 0 to 65535, it just specifies the place in the Registry that your options will be saved. You cannot specify a particular drive using this method, as it applies to all drives and partitions, so use this method cautiously if you have other users and/or drives on the machine. Make sure to click the 'Clean up system files' button to see all of the possible categories here. All categories have descriptions provided when highlighted, but it is important to note the following:

§ Previous Windows installation(s) - If Windows 8 found a previous installation of Windows on the drive to which it was installed, it will typically save previous files and folders under a *\Windows.old* directory. You can view the contents of this directory in File Explorer to see if there's anything you want to keep, otherwise it is best deleted, as it can take up a very large amount of space.
§ User file history - If you have enabled the Windows File History feature, some backups may be stored temporarily on your drive until they can be transferred to your backup location. Deleting these will result in the loss of some of your backup data in File History. See the File History section of the Backup & Recovery chapter.
§ Windows ESD installation files - These files are necessary for the Windows Reset or Windows Refresh features to work correctly, and should not be deleted unless you are an advanced user and extremely short on drive space. See the System Recovery section of the Backup & Recovery chapter for details of these features.

Once you have selected the relevant options, click OK. However, nothing will be deleted yet - your settings have only been saved.

To actually run an advanced Disk Clean-up with the saved settings, type the following in a Command Prompt, or on the Start Screen:

```
Cleanmgr /sagerun:1
```

Press Enter and the cleanup process will begin immediately. The number after `/sagerun` must match the number used in the `/sageset` switch further above for the same options to execute.

In general this advanced method need not be used very often; once after you have installed Windows, and then infrequently after that is sufficient. The regular Disk Clean-up method is safer and more configurable, especially as you can specify the drive to which it applies, preventing unintended impacts on other drives or other users on your system.

< CCLEANER

CCleaner is a free utility that can find and remove a wide variety of potentially useless files on your system. CCleaner automates a task that is much more complicated to do manually. If used with caution, it is quite safe in removing only genuinely unnecessary files.

To configure CCleaner, run the program and click the Options button, then adjust the following settings:

1. Under the Settings section, all available boxes can be unticked if desired, as none are vital to running CCleaner correctly. Selecting the 'Normal file deletion' option is recommended, as secure deletion can make it virtually impossible to recover accidentally deleted files.
2. Under the Cookies section, in the left pane are a list of cookies that CCleaner will automatically delete if the Cookies option(s) are ticked under the main Cleaner portion of the program. If you have ticked any of the Cookies boxes in the Cleaner portion, select any cookies you would like to keep from the list in the left pane, and use the arrow to move them to the list in the right pane.
3. Under the Include and Exclude sections you can manually add particular files or folders that you would specifically like CCleaner to scan for deletion, or exclude from deletion, as relevant. This is only recommended if you know for certain that the contents of these files or folders are safe to delete or keep.
4. Under the Advanced section I recommend ticking the 'Show prompt to backup registry issues' box as a safety mechanism if you use the Registry cleaning functionality; and the 'Only delete files in Windows Temp folders older than 24 hours' to prevent deletion of temporary files that are required for the current session. The other settings can be set to suit your taste.

To start the cleaning process, first close all open applications to prevent any conflicts if CCleaner tries to delete actively used files. Then launch CCleaner and under the Windows tab of the Cleaner function, take the time to go through and select or unselect particular options. As a general balance between safety and removing unnecessary files, I recommend the following configuration for each category:

§ Internet Explorer - If you don't use Internet Explorer as your main browser, all options here can be ticked. If you do use Internet Explorer, I don't recommend ticking any options here as it can reduce performance and functionality in IE. Proper configuration of IE as covered under the Internet Explorer chapter will ensure that relevant files are kept or removed by IE itself during normal operation.
§ File Explorer - All options can be ticked, however you may want to untick the 'Thumbnail Cache' option as it means any folders in which you use Icon views will need to recreate their thumbnails, slowing down browsing of those folders. You may also want to untick the 'Taskbar Jump Lists' functions if you use the Recent functionality of Jump Lists. See the Taskbar section of the Graphics & Sound chapter for details. The 'Network passwords' option should also be unticked if you want to keep any such passwords.
§ System - The default options here are fine. Note that ticking items like 'Windows Log Files', 'Memory Dumps' and 'Windows Error Reporting' can make troubleshooting much more difficult, so only select these if you are not having problems on your system - see the Performance Measurement & Troubleshooting chapter for details. I also don't recommend ticking the 'Empty Recycle Bin' option here for the reason covered at the end of this chapter.
§ Advanced - I recommend against ticking any of the options here, as most of these options will result in deletion of files which are self-maintained by Windows. For example, deleting 'Old Prefetch data' is unnecessary, as Windows automatically purges the Prefetch folder periodically to maintain a list of the

most commonly used programs based on its analysis. Various caches are also necessary to speed up normal Windows functionality, so regularly deleting them simply works against this.

Under the Applications tab I recommend unticking all available options. This is because in the vast majority of cases, removing application-specific files in this manner can remove desirable functionality from such applications, and introduce unexpected behavior. Be aware that CCleaner may automatically add and enable new entries here when you install new applications, so check under this tab regularly.

Once you have ticked all of the relevant options, click the Analyze button and after a while CCleaner will come up with a list of files it wants to delete. Nothing has been deleted yet. By default the results are shown in summary form, which can make it difficult to determine precisely which files will be deleted. Right-click in an empty area of the analysis window and select 'View detailed results' if you wish to see a full list of the individual files that are going to be deleted.

When you are satisfied that the files to be deleted are unnecessary, click the 'Run Cleaner' button and the files will all be permanently deleted.

There are several other useful functions of CCleaner:

Registry: The Registry function in CCleaner attempts to find redundant Registry entries, and is relatively safe to use if configured correctly. This functionality is covered under the Maintaining the Registry section of the Windows Registry chapter.

Uninstall: The Uninstall function found under the Tools section of CCleaner can be used to remove faulty entries from the Programs and Features list. This functionality is covered under the Programs and Features section of the Windows Control Panel chapter.

Startup: The Startup function found under the Tools section of CCleaner allows you to view, disable and delete startup items. This is not the preferred method for handling startup items. See the Startup Programs chapter for details of recommended tools and methods.

System Restore: The System Restore function is found under the Tools section of CCleaner, and is handy for deleting individual Restore Points on your system. The very latest Restore Point cannot, and should not, be deleted, but older ones are usually safe to delete if your system is problem-free.

Drive Wiper: The Drive Wiper functionality can be found under the Tools section of CCleaner. It allows for secure deletion of data, and is detailed under the Data Recovery section of the Backup & Recovery chapter.

CCleaner is a very useful tool in removing a range of unnecessary files, but caution is required, as Windows is already quite good at maintaining itself, and thus does not really need to have a range of files deleted by this or any other utility. Many files will simply recreate themselves the next time you start Windows or use a program, so in many ways all you are doing by deleting them is actually slowing down Windows, and undermining normal application functionality. The recommendations in this section try to limit CCleaner to deletion of genuinely unnecessary files.

< MANUAL CLEANING

Below is a basic method for manually finding and removing the more obvious redundant files on your system. If you don't trust an automated third party cleaning tool, or just want to do a more thorough job, read the following. This method is not recommended for novice users as it requires a reasonable level of system knowledge in determining which files to delete and which to keep.

Before manually cleaning out any files, first close all open applications, as some of these may have created temporary files that cannot be deleted because they are in use. Then restart your system, as Windows will remove many temporary files upon shutdown. Now make sure that the option to move files to the Recycle Bin is enabled, and that your Recycle Bin is of an adequate size, as this will provide protection against accidentally deleting a necessary file or folder.

To begin with, it is safe to delete the contents of the *\Users\[username]\AppData\Local\Temp* directory. These are temporary files specific to your user account.

Next, go to the Programs and Features component under the Windows Control Panel and uninstall any programs you do not wish to keep. Then go to the following folders and manually delete any subfolders for programs or drivers you are certain that you have uninstalled from your system:

\Program Files
\Program Files\Common Files
\Program Files (x86)
\Program Files (x86)\Common Files
\ProgramData
\Users\[username]\AppData\Local
\Users\[username]\AppData\LocalLow
\Users\[username]\AppData\Roaming

In some cases the folders may be named after the company that has created the software, rather than the software itself. A quick web search should help you determine which programs the folders relate to if in doubt. Certain programs may have files that are "in use"' and can't be deleted - see further below for details.

Next, if you have no major issues on your system, and you are not trying to troubleshoot a problem or recover any files, it is possible to delete a range of files with particular extensions identifying them as potentially redundant. You will need to access the advanced Windows Search functionality by opening File Explorer, typing the following, and selecting Computer each time from the Search ribbon menu:

ext:dmp - .DMP files are Dump Files created by Windows after crashes and errors.
ext:old - .OLD files are generally backup copies of files.
ext:bak - .BAK files are generally backup copies of files.
ext:log - .LOG files are files containing logged activity or error data.
ext:wer - .WER is for files related to the Windows Error Reporting function.
ext:lnk - .LNK is for shortcut files, including links to recently opened files in programs.

Do not simply delete all the results you discover for each of the system-wide searches above. You must exercise your judgment in most cases. For example, the *ext:lnk* search will discover a large number of valid and necessary shortcuts and links. You must only remove links to programs or files that you know no longer exist on your system.

Furthermore, as noted in the CCleaner section, do not regularly clean out the contents of certain Windows directories such as *\Windows\Prefetch*. These cache directories are self-maintaining, and there is greater potential for reducing performance or harming functionality in removing these files, than any benefits.

The key thing to understand is that there are usually no performance or functionality benefits to be had by deleting unnecessary files. This type of cleaning is only done to reduce clutter and free up disk space. If in doubt, do not delete a file or folder until you have done plenty of research on its purpose.

DELETING 'IN USE' FILES

During the attempted removal of a file or folder you may find that Windows prevents you from deleting it because it is "in use" by another person or program. This means that Windows needs this program for some reason. There are several legitimate reasons for this:

§ The most common reason is that the file is actually being used by an active program. Close all open programs, reboot your system and try again. If the problem persists, then it is likely that a background program or driver is using this file, loading it into memory at Windows startup. See the Startup Programs and Services chapters to identify all your background programs, and you can temporarily prevent a particular file from being loaded into memory by disabling the related program in the Start-up tab of Task Manager, or in the Autoruns utility, then rebooting and trying again.
§ Certain files can't be deleted because you need to be the owner of the file - see the Access Control and Permissions section of the Security chapter. Be very careful deleting such files, as they are often core Windows system files, and should not be deleted or modified.
§ If a file continues to be problematic in removing, you should attempt to remove it in Safe Mode - see the System Recovery section of the Backup & Recovery chapter. You should also run a full malware scan of your system as covered in the Security chapter, as it is often malware-related files that require such measures to remove.

Ultimately however, some files will refuse to be deleted no matter what you try, in which case you should try the free Unlocker utility. To use the program, install it then right-click on the relevant file or folder and select Unlocker for options.

After deleting all the files you consider unnecessary via any of the methods above, you should not empty your Recycle Bin. Reboot your system and use it normally for a few days just to be sure that the files you have deleted are genuinely no longer needed. In general a combination of the Disk Clean-up utility and CCleaner are the safest methods for conducting regular and relatively thorough cleaning of your system. Manual cleaning is also necessary at times, particularly after uninstalling a program or driver that does not correctly remove all portions of itself from your system. In any case, cleaning Windows in this manner is not a performance boosting method, it is primarily for reducing clutter and freeing up disk space.

REGULAR MAINTENANCE

Keeping Windows and your PC in optimal working order requires regular system maintenance. Any operating system will degrade over time if not properly maintained, particularly as you install and uninstall a range of programs and drivers. Even though Windows 8 has improved its self-maintenance procedures, and by default schedules a range of these tasks to automatically run on a daily basis, this is not a replacement for proper maintenance.

The best method of conducting system maintenance is to get into a routine, so that it becomes a matter of habit. This prevents you from forgetting to conduct system maintenance. However, it cannot be done on a completely rigid schedule; certain maintenance tasks should only be done under certain circumstances, their frequency dependent on how you use your PC.

For the reasons above, I can't provide an all-encompassing maintenance schedule that everyone should follow. This entire book contains a wealth of information and recommendations designed to help you understand how best to maintain your own PC. By having appropriate knowledge of the various features in Windows, you will come to know how to configure Windows 8's automated maintenance tools, and when to manually intervene as necessary. For the purposes of providing some basic guidelines however, I outline a list of maintenance tasks I regularly perform on my own PC to maintain it in peak condition. This is only an example, and should not be followed blindly.

STEP 1 - MAINTAIN SECURITY

Action: Check Windows Update, then update Windows Defender and run a full manual scan of all drives.
Frequency: Once a week, and also scan individual downloaded files before use with Windows Defender.

See the Security chapter for details.

STEP 2 - CHECK STARTUP PROGRAMS & SERVICES

Action: Check under the Start-up tab of Task Manager, and the Services tab of MSConfig, for any newly installed startup programs or non-Microsoft services. Identify any new or unfamiliar entries and disable unnecessary ones as required. Run Autoruns to see if any unnecessary extensions or other types of entries have been added.
Frequency: After every new program or driver install.

See the Startup Programs and Services chapters for details.

STEP 3 - BACKUP

Action: Create a new restore point using System Restore, and then run Windows 7 File Recovery to update a full system image backup stored on a separate drive. Also make a separate manual "clean" backup of important personal files to rewriteable DVDs for secure and portable storage.
Frequency: Once a week.

See the Backup & Recovery chapter.

STEP 4 - CLEAN WINDOWS

Action: Run CCleaner, then the Disk Clean-up utility. Do a manual clean out of remaining unnecessary files.
Frequency: Once a week, and also after major updates, program installs and uninstalls.

See the Cleaning Windows chapter for details.

STEP 5 - OPTIMIZE DRIVES

Action: Use the Optimize Drives utility to run a full drive optimization on all drives.
Frequency: Once a week. For hard drives, defragment after every major program install or uninstall, any program updates, any Windows Updates, and any driver installations.

See the Drive Optimization chapter for details.

The steps above may seem somewhat tedious to run through on a frequent basis, but in practice it is precisely what has ensured that my system always remains problem-free. Proper maintenance is important in keeping your data secure, and your system as responsive as when you first installed Windows.

SCHEDULED MAINTENANCE

Windows runs a series of general maintenance and diagnostic tasks on a daily basis, when your system is idle. The Automatic Maintenance feature gives you control over exactly when these automated Windows maintenance tasks are run, as well as letting you initiate them immediately if you wish. See the Windows Action Center section of the Performance Measurement & Troubleshooting chapter for details.

The Task Scheduler also allows you to create and customize a range of automated tasks for maintaining your PC. This means that more arduous tasks can be set to run at a time when you are not actively using the PC. For example, if you leave your machine on overnight, you can schedule certain utilities to run at that time. See the Background Tasks section of the Services chapter for details of how to do this.

A critical part of proper maintenance is prevention, and this involves making sure that you do not constantly install a range of unnecessary programs on your system. Codec packs, various dubious tweaking utilities, constant upgrades and downgrades of leaked drivers, etc. are one of the major reasons why many systems are so unstable and insecure, beyond Windows 8's capabilities to manage the mess of program conflicts and detritus that such systems have accumulated. Treat your PC as a complex and finely-tuned electronic machine, not a dumping ground for everything you find on the Internet, and it will remain stable and perform well for a very long time.

CONCLUSION

That brings *The TweakGuides Tweaking Companion for Windows 8* to a close. I hope you've found the information in this book useful.

Cheers,
Koroush

< VERSION HISTORY

The table below shows any major revisions made to this book since first released.

Version	Release Date	Pages Revised
1.0	9 December 2012	Nil - First Release.