TWEAKGUIDES

TWEAKING COMPANION

for Windows 7

KOROUSH GHAZI

WWW.TWEAKGUIDES.COM

[Version 1.3]

TABLE OF CONTENTS

Table of Contents

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 often delicate procedures in this book. Professional translations of this 250,000 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 TweakGuides Tweaking Companion download 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 the TGTC - I truly appreciate it. The only thing which motivates me to keep writing guides is the fact that I know there are intelligent people out there who are patient enough to take the time to read them, and 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.

Special thanks to Microsoft, and in particular Nestor Portillo, for generously providing me with access to the final build of Windows 7 prior to its public release.

INTRODUCTION

After much anticipation, Windows 7 was officially released to the public on 22 October 2009. For those of you upgrading from Windows XP, many of the features and functionality in Windows 7 may be new and confusing; for those accustomed to Windows Vista, they will be much more familiar. Regardless, I've made sure that the *TweakGuides Tweaking Companion for Windows 7* caters equally to both categories of users, as well as to those completely new to Windows.

Windows 7 is an evolution of Windows Vista. This should not be considered a bad thing; Vista has been unfairly maligned. The important thing to keep in mind is that the jump from Windows XP to Vista was quite significant, introducing a range of important and necessary new technologies and features. In going from Windows Vista to Windows 7, Microsoft has successfully refined and built upon these features.

When examined closely, Windows 7 has a large number of improvements over previous versions of Windows, both above and beneath the hood. However there are also some areas where you may find the changes undesirable. The primary aim of this book is to objectively explain all the features and functionality in Windows 7 in an easy to understand manner. The book then provides details on how to customize Windows 7 to better suit your particular tastes and needs, helping you to minimize any negative impacts which may flow from the changes, and find better ways of using Windows 7.

As with my earlier *TweakGuides Tweaking Companions* for Windows XP and Windows Vista, first released in 2005 and 2007 respectively, I understand that the length of this book will no doubt frustrate people who are looking for a handful of quick tips to 'make Windows faster'. Clearly that is not the sole aim of this book. My goal is to explain how things work in simple but sufficient detail so that readers can customize and optimize their machines appropriately while learning more about them. Computers are now integral to many aspects of our lives, so it is simply not possible to pretend that it is not important to know how they work. The book is long because I make sure that whether novice or advanced, you are given enough details 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 simply told to do something without a second thought.

I promise you that if you patiently work your way through this book over the course of several days, that you will come out at the other end with not only a better performing, more stable and better customized PC, you will also be much more comfortable with using Windows 7 on a daily basis; the mystery will disappear. More importantly, you will be able to better diagnose, indeed prevent, any problems on your PC in the future. In any case, the choice as to how best to use the book is left up to you.

In closing, if you find the book useful, I ask that you consider making a donation or purchasing the enhanced Deluxe Edition of this book. The Deluxe Edition is much easier to use, and your support will allow me to continue releasing the free version of this book, and to also continue creating new works in the future.

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

BEFORE USING THIS BOOK

BASIC REQUIREMENTS

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

§ You will 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 your important data prior to undertaking any of the changes detailed in this book. See the Backup & Recovery chapter for details.

§ You should have a Windows 7 DVD. This is recommended, as you may not be able to reverse certain changes without it. However under Windows 7, PCs without a Windows 7 DVD can access a built-in System Recovery partition and/or create a System Repair Disc prior to proceeding, which is sufficient for repairing Windows. See the Backup & Recovery chapter for details.

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

DIFFERENT VERSIONS OF WINDOWS

This book is designed only for Windows 7 32-bit and 64-bit. There are separate TweakGuides Tweaking Companion books available for Windows Vista and Windows XP, to which users of those operating systems should refer. The major content differences between the various editions of Windows 7 are covered in this Microsoft Article and this Wikipedia Article, and are taken into consideration and noted throughout this book. However there are no content differences between the OEM, Academic, MSDN, TechNet, Upgrade and Retail editions of Windows 7 - 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 Activation chapter for details.

WHERE ARE THE PICTURES?

There is a distinct lack of pictures in this version of the book. The Deluxe Edition of this book does contain detailed screenshots and illustrative images, as well as other useful features which make using this book much more convenient, such as high quality text resolution for better print quality, full bookmarks for quicker chapter and section access, and the ability to copy text which is handy for purposes such as correctly assigning Windows Registry values or entering complex Command Prompt commands. If you want the book with these features, and more importantly want to show your support, please consider purchasing a Deluxe Edition from the link above, the electronic version of which is only a few dollars.

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 for 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, you can 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 which magically speed up or fix Windows 7. It is a complex inter-relationship of hardware and software settings which 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 to both those who are doing a new installation of Windows 7 and those who are using an existing installation of Windows 7. 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 procedures or details from other chapters are required, they are referenced accordingly. If you don't wish to read the book sequentially, I strongly recommend reading the Basic PC Terminology and New & Common Features chapters before reading anything else. Then I suggest becoming familiar with the contents of the Windows Explorer, Windows Drivers, PC Security and Graphics & Sound 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 which I recommend to enable you to carry out some of the procedures in the book or to provide additional functionality in Windows. If you do not feel comfortable in downloading or installing this software for whatever reason, you should ignore those procedures which rely upon it, as none of them are critical to the functioning of Windows 7. Furthermore, at no point do you have to purchase any software. I am not paid or sponsored by any software or hardware company, so I generally recommend the best free software available to do the job. In a few cases the software may require purchase, but usually the trial version of it retains enough functionality to complete the job for which I have recommended it. Of course if you do find any of the software useful I encourage you to purchase it or donate to the software's author. Not everything on the Internet is free, nor should it be.

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 PC hardware and software available. If there is anything in the book which you believe is genuinely inaccurate or misleading, or if you just want to report a broken link, please Email Me with specific details and if appropriate I will rectify it in the next version of the book. You can also email me if you wish to share any general feedback or thoughts you have about the book.

However I must stress 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, so under no circumstances will I provide personalized optimization, customization or purchasing advice/feedback, 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 the steps necessary to customize and optimize their system. As such, 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 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 completely accurate to the best of my knowledge, and that the sites and utilities linked to in the book are free from any malware or deceptive practices at the time of writing. In all respects the book is safe to use if followed correctly, with careful consideration and taking appropriate precautions. However 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 do not proceed any further - close the book immediately.

BASIC PC TERMINOLOGY

This chapter explains in layman's terms commonly used technical terminology. All of the major hardware components found in a modern PC are also covered. While advanced users may want to skip this chapter, everyone should read the Bits & Bytes section below to clarify a common point of confusion.

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 as noted, 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 however 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 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 through it 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 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, and 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 and with varying degrees of portability. Storage drives plug into one of four main types of drive controllers found on the motherboard, listed from slowest to fastest below:

§ 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 is 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 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 7 is the first version of Windows to provide full 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 this 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 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 most 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 most modern PCs now fully support the use of optical discs or USB drives for these purposes instead. In fact the only major 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 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 very 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 7, 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 the 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 still have a traditional Cathode Ray Tube (CRT) monitor as their primary display device, however most 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 pixels 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.

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 Speakers or Headphones, directly into the sound card or integrated sound device through the back of 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 the component through conduction. This heat then travels along the heatsink until cooler air and a large surface area help in accelerating the dissipation of the heat.

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 removing 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, 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 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 for example. 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 7, is a vital piece of software - 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 interact with the PC 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 & COMMON FEATURES

This chapter briefly covers the most important and most commonly used features of Windows 7, some of which have existed in one form or another in previous versions of Windows, and some of which are entirely new. Full details of all of these features are provided in the relevant chapters of this book as indicated. Do not skip this chapter - it is a crash course in the fundamental features referred to often throughout this book, so you need to be familiar with all of them before delving further into Windows 7.

WINDOWS AERO

Windows Aero is the glass-like user interface first introduced in Windows Vista. It has had some modifications and new features added to it as of Windows 7. When Aero is enabled, the Windows Desktop is no longer a simple 2D environment; it can have both 2D and 3D elements at the same time. To quickly see if you are currently running full Aero, and to demonstrate its 3D capabilities, press WINDOWS+TAB to trigger the Flip 3D task switching function.

In Windows 7 the performance of Aero and related graphics interface functionality has been improved over Windows Vista. For those who do not like Aero or do not have the graphics hardware to support running it smoothly, the Aero interface can be disabled by right-clicking on the Desktop, selecting Personalize, and then selecting the Windows 7 Basic theme. However the Aero interface in Windows 7 is desirable because aside from its aesthetic appeal, it also allows a range of useful functions, including:

Thumbnail and Full Screen Previews - Moving your mouse pointer over the icon for an active program in the Taskbar brings up live Thumbnail Preview(s) of its current contents, as it did in Vista. You can go to any active program or window by left-clicking its Thumbnail Preview, and you can also close it by clicking the red X in the Thumbnail Preview. Additionally in Windows 7, if you move your mouse pointer over a specific Thumbnail Preview, a Full Screen Preview immediately appears. Move your mouse away from the Thumbnail Preview and the Full Screen Preview disappears.

Flip & Flip 3D - Windows Flip is essentially the ALT+TAB task switching function available in previous versions of Windows. However under the Aero interface, accessing Flip by using ALT+TAB brings up a set of thumbnail previews of all open windows. Furthermore, by using WINDOWS+TAB for Flip 3D, you can switch to an animated 3D representation of all open windows.

Aero Peek - New to Windows 7, if you want to quickly glance at what is currently on your Windows Desktop, you don't need to minimize or close your open windows. Move your mouse pointer over the small glassy rectangle at the far right of the Windows Taskbar next to the clock in the Notification Area to instantly make everything in front of the Desktop transparent. Move it away to again see your windows as before. If instead you click on the rectangle, you will instantly switch to the Desktop, and clicking it again will restore all minimized windows.

Aero Snap - Windows 7 introduces native support for the use of basic mouse gestures on the Windows Desktop. The two most common categories of mouse gestures are called Aero Snap and Aero Shake. Aero Snap allows you 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, or 'snaps', 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.

Aero Shake - Based on the same principle as Aero Snap, Aero Shake allows you to quickly minimize all open windows except one. Grab and rapidly shake the window of your choice 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.

Gadgets - First available in Vista as part of the Windows Sidebar, Windows 7 has removed the Sidebar and now only has free-floating Gadgets which also use less resources. Gadgets are small graphical applications which sit on your Desktop and can provide a range of useful information and functionality at a glance.

For details of how to use and customize these and other interface features see the Graphics & Sound chapter.

TASKBAR

The Windows Taskbar is the bar which lies across the bottom of the screen. Windows 7 brings a noticeable change to the way the Taskbar is displayed and used, making it a unified location for interacting with programs in a range of ways. By default the Taskbar is now fully transparent and slightly larger, with bigger icons representing both those programs which are permanently pinned to the Taskbar, as well as any programs currently open in Windows. The icons are now freely rearrangeable on the Taskbar, whether pinned or not. Additionally, under the Aero interface the Taskbar provides extra functionality in the form of thumbnail previews. The other key features of the Taskbar include:

Jump Lists - When a Taskbar icon is right-clicked, or if the icon is dragged upwards, a context menu of various options known as a Jump List appears. Commonly the Jump List will show any recently opened files or folders for the program, allow the user to pin/unpin the program to the taskbar, and also provide the ability to open new instances of the program, as well as close any existing instances of it. Other features available on the Jump List depend on the level of support the application has for this functionality in Windows 7.

Notification Area - Also referred to as the System Tray in previous versions of Windows, the Notification Area is the small section of the Taskbar which by default shows the time and date, as well as the small Volume, Network and Action Center icons. Additional icons may appear in this area depending on how individual programs are set up to notify the user. In Windows 7 the Notification Area has had some changes, particularly with the addition of the Aero Peek item, and the fact that by default it hides most icons until otherwise customized by the user. These hidden items can be accessed by clicking the small white triangle to the left of the Notification Area. You may also notice that the Network icon is no longer animated to show Internet traffic activity.

Start Menu - The Start Menu is accessed via the circular Start button at the far left of the Taskbar. The Start Menu allows users to pin a range of shortcuts on the left side, as well as access documents and several commonly-used Windows features on the right side of it, in one easily accessible location. It also contains a Search Box at the bottom which provides easy access to the Windows Search functionality. The Start Menu has not been significantly changed since Vista, however it is notably different from that used in XP. The most noticeable change for all users is that the links to personal folders are now to the relevant Library, and not directly to the folder itself. Jump lists are now also available for displaying recently opened files for certain programs that are pinned to the Start Menu, denoted by a small black arrow to the right of the pinned item. Note that Classic View is no longer available for the Start Menu.

More details of the Taskbar and Start Menu can be found in the Graphics & Sound chapter; the Search Box is covered in the Windows Search chapter.

WINDOWS EXPLORER

Windows Explorer is the main interface used to manipulate files and folders in Windows. It can be opened via the Computer item on the Start Menu, by clicking the yellow folder icon found on the Taskbar, or by pressing WINDOWS+E. Many of the interfaces in Windows are based on Windows Explorer. While Windows Explorer should be familiar to users of previous Windows versions, the major changes and features of Windows Explorer in Windows 7 include:

Libraries - The most noticeable change in Windows Explorer, Libraries are virtual folders not to be confused with the traditional *My Documents*, *My Music*, *My Pictures*, and *My Videos* user-specific personal folders. Although the default Libraries have similar names to these user directories, Libraries are a user-defined virtual collection of content, not an actual directory or storage location in their own right. Library folders are all held under the Libraries category in Windows Explorer, whereas your personal folders are located under the *\Users\[Username]* directory by default. The key difference is that Libraries provide a unified display of the contents of various directories. For example, you can add all the various folders under which you store pictures and photographs across your drive(s) to the Pictures library, and it will then display all these files in a single view, sorted to suit your taste. Your original files and folders remain where they are, but the Library allows you to manipulate and view these files in a single location.

Libraries are tightly integrated into Windows 7. For example, the Documents, Pictures, Music and Videos items on the Start Menu all point to the Libraries of the same name, not your personal folders; when you open Windows Explorer, by default the Libraries folders are exposed, even if you link directly to a particular user directory; and some applications such as Windows Media Player incorporate the media-related Libraries for use in media display and selection.

Details Pane - The Details Pane is the small area at the bottom of Windows Explorer which, when a file is selected, instantly displays basic details about that file at a glance.

Preview Pane - The Preview Pane is a larger area to the right of Windows Explorer which, when a file is selected, allows you to preview its contents in real-time. It can be toggled on or off at any time using the 'Show/Hide the preview pane' button at the top right of the Explorer window. The Preview Pane has been improved since its implementation in Windows Vista. For example, if you highlight a video file with the Preview Pane open, you can play the video if you wish; if you highlight an audio file, you can listen to it in the Preview Pane, and so forth.

Content View - New to Windows 7, Content view is a combination of several other view types, providing 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. Content view is best suited to browsing multimedia files - for example, if it isn't already in Content view, right-click in your Music Library and select Content to see how it looks.

Live Icons - First introduced in Windows Vista, Live Icons display actual content from the files on which they're based. The most prominent example of Live Icons are picture and video thumbnails, which when viewed in Icon, Content or Tile view in windows explorer, change from generic thumbnail icons to icons with images derived from the file's content. These icons are also fully scalable, either by right-clicking in the folder and selecting a relevant icon size under the View menu, or by holding down the CTRL key and using your mousewheel to resize the icons when in Icon view.

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

SEARCH BOX

First introduced in Windows Vista and refined in Windows 7, the main Search Box can be found at the bottom of the Start Menu, however versions of it also appear throughout the Windows interface, typically at the top right of any Explorer-based windows. The aim of the Start Menu Search Box in particular is not only to find lost files, it is primarily for allowing fast access to any program, file or Windows feature - simply type the first few letters of it to bring it up for selection. As such, throughout this book I frequently refer to Start>Search Box as a place to launch programs or access Windows features. Strictly speaking it is not a command line interface like the Windows Run box which you can access by pressing WINDOWS+R or using the Run item on the Start Menu. However it is much quicker to use than going through various menus to find the relevant shortcut, or typing an exact executable or command name in the run box.

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

USER ACCOUNT CONTROL

User Account Control (UAC) was introduced in Windows Vista, and to understand the rationale behind it, you need basic understanding of User Accounts. In Windows the two main levels of User Accounts are Administrators and Standard users. When User Account Control is disabled, Administrator level users - such as the account created when you first install Windows 7 - have the greatest freedom, able to make any system change and install any software, however this also brings with it potential security and stability issues. A Standard User Account on the other hand is deliberately designed to restrict users from making certain changes which could alter system settings in undesirable ways, and also allows the convenience of having multiple users on the same PC in isolation from each other.

When enabled, UAC ensures that whether an Administrator or Standard user, your account actually runs with only Standard level privileges regardless. Then whenever you attempt to make certain system-intrusive changes, you may see an elevation prompt - known as a UAC Prompt - appear. If you're running a Standard account, the prompt will ask for an Administrator password; if you're running an Administrator account, you can simply click Yes to the prompt if you wish to proceed. Importantly, this UAC prompt contains a range of details regarding the program to be launched or installed, all of which can be used to ascertain whether you actually want to allow the program in question to make system-intrusive changes.

Note that programs or Windows options which may trigger a UAC prompt when launched are usually denoted with a small shield symbol in their shortcut icon.

UAC has been improved in Windows 7, firstly to allow Standard users to undertake several common and relatively less intrusive tasks without being prompted. The number of redundant UAC prompts has also been reduced, and by default many Windows applications will not raise a UAC prompt, making changes to common Windows settings much easier to perform. Furthermore, Windows 7 adds user-customizable UAC notification levels, accessible under the User Accounts component of the Windows Control Panel by clicking the 'Change User Account Control Settings' link.

Some older programs not designed specifically for Windows Vista or Windows 7 may not launch properly or have full functionality when UAC is enabled, because they don't ask for administrative access to the system even when it is required. In such cases, launch the program by right-clicking on its executable or launch icon and select 'Run as Administrator' to ensure that it will have correct functionality.

Don't alter your UAC settings until you have a greater understanding of both User Accounts and UAC.
More details of UAC can be found in the User Account Control section of the PC Security chapter, and more details on User Accounts can be found in the User Accounts chapter.

ADMINISTRATOR COMMAND PROMPT

One important UAC-related issue is that of the MS DOS-based Command Prompt. You will sometimes require what is known as an Administrator Command Prompt to successfully use certain command-line commands. If ever a particular command line option is not executing properly or appears to have no impact, it is most likely because you need to use it in an Administrator Command Prompt. There are several ways to launch one:

- Go to Start>Search Box, type *cmd*, then right-click on the *cmd.exe* item which appears in the Start Menu and select 'Run as Administrator'.
- Go to Start>Search Box, type *cmd*, then press CTRL+SHIFT+ENTER.
- Go to Start>Search Box, type *cmd*, then right-click on the *cmd.exe* item, and select Send To>Desktop to create a shortcut on your Desktop. Right-click on this shortcut, select Properties, click the Advanced button under the Shortcut tab and tick 'Run as Administrator'. You can now use this shortcut to launch an Administrator Command Prompt as required.

Note that when an Administrator Command Prompt is correctly launched, you will see the word *Administrator* in its title bar. You can also launch any program or Windows feature directly from an Administrator Command Prompt without requiring a re-confirmation through UAC, because it already has elevated privileges.

WINDOWS MAIL

One of the most noticeable differences between Windows 7 and previous versions of Windows is the absence of a mail program. Windows XP had Outlook Express, Windows Vista had Windows Mail, but Windows 7 has no email client whatsoever by default. It's also worth noting that Windows 7 sees the exclusion of not only Windows Mail, but Windows Movie Maker has also been removed, the Windows Photo Viewer built-in image viewing program now has no image editing capabilities, and Parental Controls no longer includes any web filtering features.

If you type *Windows Mail* or *Movie Maker* in the Start>Search Box for example, you will see that Microsoft encourages you to obtain these, and other components, from the free Windows Live Essentials suite available online. You can however install any third party version of these applications instead if you wish. This book provides appropriate links and instructions, giving you enough information to make the choice which suits you best. In particular there is a detailed chapter on how to configure Windows Live Mail to more closely match the look and behavior of previous Windows mail clients.

More details can be found in the Windows Live Mail chapter, as well as the Parental Controls section of the User Accounts chapter and the Windows Media Player chapter.

RIBBON

The Ribbon user interface came to prominence in Microsoft Office 2007, and is identified by a series of overlapping toolbars selected via tabs. Windows 7 introduces native support for the ribbon framework, and has incorporated the ribbon interface, most notably in the new versions of the Paint and Wordpad utilities. If you're not familiar with the ribbon interface, note that aside from the main options on the ribbon which are sorted under tabs, you can click the small button at the top left of the window to see a drop-down box with further options, and for easy access you can pin any ribbon options to the small toolbar in the title bar of the window by right-clicking on the relevant item and selecting 'Add to Quick Access Toolbar'.

DRIVERS

A driver is software specifically designed to let Windows communicate with your hardware. Windows 7 employs the same driver architecture as Windows Vista, which itself was a major departure from Windows XP - this means that while drivers specifically designed for Windows 7 are the best choice for optimal performance and functionality, drivers originally designed for Vista can also be used in Windows 7, though this may result in the loss of some performance and functionality. Fortunately, major hardware manufacturers such as Intel, ATI/AMD, Nvidia and Creative Labs have released fully functional Windows 7 drivers. Given the popular appeal of Windows 7, driver support will continue to improve. Fortunately for owners of older hardware who may not have access to appropriate drivers, Windows 7 improves generic support for a range of common devices, and simply connecting them in most cases will see the automatic installation of the appropriate driver. In short driver support is not a major issue in Windows 7.

32-bit vs. 64-bit Support - As with previous versions of Windows, software designed for Windows 7 32-bit should function without any issues under the 64-bit version of the OS. Windows 7 64-bit users should note that under normal circumstances you cannot run drivers which are unsigned, or which are designed for 32-bit Windows, under 64-bit Windows.

Device Stage - A new feature of Windows 7 designed as a central location for accessing the common features of your connected device(s), Device Stage opens automatically when a supported device is detected, and allows access to a range of useful functions for the device without the need to install additional software.

Devices and Printers - While Device Stage is for individual devices, Devices and Printers is another new feature of Windows 7 which provides a central location for making it easier to access and configure a range of devices on your system. It also replaces the Printers folder as the location to access print-related functions.

See the Windows Drivers chapter for more details, as well as the 32-bit vs. 64-bit section of the Windows Installation chapter; the Device Stage section of the BIOS & Hardware Management chapter; and finally the Graphics & Sound chapter for important details on graphics and sound driver-related issues.

COMPATIBILITY ISSUES

Windows 7 is based heavily on Windows Vista, and because software developers have had over three years to make their software compatible with Vista, the good news is that recent versions of most prominent software already provide support for Windows 7. Make sure to check for newer versions of your favorite software regularly and upgrade or update as necessary. For most systems, compatibility issues should be almost non-existent, especially if your system ran fine under Windows Vista. However Windows 7 provides various solutions if you experience what you believe are genuine compatibility problems, particularly with older software which is no longer being updated:

Run as Administrator - As noted in the User Account Control section above, if UAC is enabled and you are having problems with a program, manually launch it in Administrator mode to see if this resolves the issue.

Compatibility Mode - If problems persist, run the program in Compatibility Mode. This option is found by right-clicking on the file or shortcut, selecting Properties, then under the Compatibility tab ticking the 'Run this program in compatibility mode for' box and selecting the previous version of Windows best suited to the program. For more recent programs simply running a program in 'Windows Vista' compatibility mode will fix any quirks. For older programs try 'Windows XP Service Pack 2' mode instead, as it is the most common Windows OS configuration.

Compatibility Wizard - Found under the new Troubleshooting component of the Windows Control Panel, click the Programs item then select the Program Compatibility troubleshooter to start a wizard which will guide you through a process that can automatically resolve certain compatibility issues.

Windows XP Mode - For programs which only function under a true Windows XP environment, Windows 7 users can access a new feature called Windows XP Mode. Not installed by default, but available as a free download to owners of Windows 7 Professional, Ultimate, and Enterprise editions, XP Mode is a fully licensed copy of Windows XP SP3 running under the Windows Virtual PC environment in Windows 7.

See the Windows Installation, Windows Drivers and Performance Measurement & Troubleshooting chapters for details on sorting out compatibility issues; see the Virtual Hard Disk section of the Drive Optimization chapter for details of Windows XP Mode.

WINDOWS CONTROL PANEL

This book assumes that you are viewing the Windows Control Panel in either Large Icons or Small Icons view, not Category view, as either of these views provides the greatest level of detail. You can change the view using the 'View by' link at the top right of the Windows Control Panel. I recommend switching to this view now before proceeding.

KEYBOARD AND MOUSE SUBSTITUTES

If you're having problems using your keyboard or mouse, either because one or the other is broken, or you are differently abled, there are two substitute methods you can use in Windows:

Microsoft Onscreen Keyboard: This utility can be accessed by going to the Ease of Access Center in the Windows Control Panel and selecting it, or go to Start>Search Box, type *osk* and press Enter. A virtual keyboard will be displayed, allowing you to use your mouse to click on virtual keys as though you were using a keyboard. To make things easier, it always remains on top of other windows. Next, click the Options button at the bottom right of the onscreen keyboard. Here you can select the 'Hover over keys' option if you can't click the left mouse button to select keys, or just want a quicker way of selecting keys. Set the length of time needed to hover over a key before it registers as an entry, and now you can rapidly move your mouse cursor over keys on the Onscreen Keyboard and it will register as a keystroke. You can also enable text prediction via the 'Use Text Prediction' option, which can assist in increasing typing speed.

Mouse Keys: If instead of your keyboard you're having problems using the mouse, you can enable the Windows MouseKeys functionality by going to the Ease of Access Center component in the Windows Control Panel and selecting 'Make the mouse easier to use', then ticking the 'Turn on Mouse Keys' option. MouseKeys allows you to use the Numpad keys - the numerical keys on the far right of your keyboard - to move the mouse cursor around on screen. You can configure these keys further by clicking the 'Set up Mouse Keys' link.

There are a range of features designed to make using the Windows 7 interface convenient for a range of tastes - see the Graphics & Sound chapter for more details.

KEYBOARD SHORTCUTS

The standard usage for keyboard shortcuts in this book is to refer to the pressing of two or more keys simultaneously by using the '+' sign. For example, when referring to ALT+TAB, this means you should press both the ALT key and the TAB key on your keyboard. Similarly, CTRL+ALT+DEL means pressing the Control (CTRL), ALT and Delete (DEL) keys together, and so forth. Also note that any references to the WINDOWS key are to the key found on most PC keyboards between CTRL and ALT, and labeled with a Windows Logo.

On the next page is a consolidated table of the major common keyboard shortcuts you can use to quickly access useful functions in Windows 7:

Keyboard Combination	Function
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.
CTRL+ +	Force all columns to be shown in Explorer interfaces.
SHIFT + DEL	Delete highlighted item, bypassing Recycle Bin.
WINDOWS	Open Start Menu. You can also use the arrow keys to select an item and press Enter.
WINDOWS + Number	Open pinned items on Taskbar. The number used corresponds with the order of the item on the Taskbar from left to right.
WINDOWS + Spacebar	Aero Peek. Temporarily makes all open windows transparent to display the Desktop.
WINDOWS + D	Minimize/Restore all Windows.
WINDOWS + E	Open Windows Explorer.
WINDOWS + F	Open Windows Search.
WINDOWS + L	Lock Workstation.
WINDOWS + M	Minimize open windows.
WINDOWS + SHIFT + M	Restore open windows.
WINDOWS + P	Open quick select menu for multi-display output.
WINDOWS + R	Open Windows Run box.
WINDOWS + T	Cycle through all Taskbar icons, press Enter to select any one
WINDOWS + F1	Open Help & Support.
WINDOWS + TAB	Switch between active programs in 3D Flip mode. Note: CTRL + WINDOWS + TAB opens 3D Flip permanently, TAB or Arrow Keys to cycle elements, ESC to exit.
WINDOWS + Arrow Key	WINDOWS + Up Arrow - Maximizes window. WINDOWS + Down Arrow - Minimizes window. WINDOWS + Left Arrow/Right Arrow - Cycle through Aero Snap.
ALT + TAB	Switch between active programs in 2D Task Switcher. Note: CTRL + ALT + TAB opens Task Switcher permanently, TAB or Arrow Keys to cycle elements, ESC to exit
CTRL + SHIFT + ESC	Open Task Manager.
ALT + F4	Close highlighted program. Show PC Shutdown options if on Windows Desktop.
SHIFT + LEFT CLICK	Select multiple items within a range.
CTRL + LEFT CLICK	Select multiple non-sequential items individually.
TAB	Step forward through screen elements.
SHIFT + TAB	Step backward through screen elements.
F2	Rename/Enter text for item.
F5	Refresh active window.
SHIFT + RIGHT CLICK	Open Expanded Context Menu for highlighted item.

This chapter has briefly highlighted some of the more noticeable changes and the most commonly used features in Windows 7. 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, so if there are features you don't like or find annoying, 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, though I recommend becoming familiar with the contents of the Windows Explorer, Windows Drivers, PC Security and Graphics & Sound chapters as soon as possible.

SYSTEM SPECIFICATIONS

The first step in optimizing or customizing your PC is to find out precisely what 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 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 know if it can run Aero, to update its drivers, or to see whether it can run the latest games; or you may have a complex problem which 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 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 7. 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 going to Start>Search Box, typing *performance information* 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 system information, click the 'View and print detailed performance and system information' link. This will open a new screen 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, as important information such as the make and model of your motherboard are not provided for example.

WINDOWS SYSTEM INFORMATION TOOL

You can access the Windows System Information Tool by going to Start>Search Box, typing *msinfo32* and pressing Enter. The Windows System Information Tool presents a range of basic information about your system. Some of its more useful functionality includes:

§ A listing of your hardware components by type under the Components section.
§ 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 going to Start>Search Box, typing *device manager* and then 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 individual device drivers or uninstall a device altogether should you wish. The Device Manager has several important roles and is covered in more detail under the Device Manager section of the BIOS & Hardware Management chapter.

DIRECTX DIAGNOSTICS

You can access the DirectX Diagnostic Utility (DXDiag) by going to Start>Search Box, typing *dxdiag* and pressing Enter. DXDiag is another built-in Windows Diagnostic/System Information tool that is part of DirectX 11 - see the Graphics & Sound chapter for more information on DirectX 11. The main tab of DXDiag, called System, displays basic information about 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 can find more 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 - see the Performance Measurement & Troubleshooting chapter.

The most useful function for DXDiag is its ability to generate a detailed text file with all your major system information, including 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 main DXDiag screen. You will be prompted to save this report somewhere, and the default of the Windows Desktop is fine. You can now double-click this *DXDiag.txt* file to read through its contents. It can also 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.

SIW

SIW is the System Information for Windows tool which can be downloaded from the SIW Website. Once you've downloaded the standalone version of the program, you can simply run it from the file - there's no need to install anything. The interface is intuitive; click items in the left pane to see more details about them. For example, to find out more about your motherboard, click the Motherboard item under the Hardware section, and the details will be shown in the right pane. Alternatively, you can access each item by going to the Software or Hardware menus at the top of the screen. Note that SIW also has a range of other tools, but I don't recommending changing anything using them. The best use for this utility is simply for viewing system information.

SANDRA

Sandra stands for System ANalyser, Diagnostic and Reporting Assistant. You can download Sandra from the SiSoftware Website - the Lite version is free, and once installed, you will see a wide selection of information and benchmarking modules to choose from. Note that during installation of Sandra, you can disable the Remote Network Services, Price Engines and Rank Engines as they are not critical, however the Rank Engines option does allow Sandra to display a comparison of your score with others who have run the benchmarks, which can be useful. If you do enable the Rank Engine, after installation you can customize it so that your results aren't made public for example. Sandra also installs a new Service for itself called the 'SiSoftware Deployment Agent Service' which you should leave at its default of Manual.

Sandra Lite has many inactive (grayed out) modules, however the main ones we need have sufficient functionality for our purposes. For example, if you want to know more about your system, double-click the Hardware icon (or select the Hardware tab) and then double-click on the Computer Overview module. It will display a range of useful information about your system, such as the CPU speed and type, your motherboard Chipset, and your Memory Module brand and speed. If you then want to know more about your motherboard in particular for example, open the Mainboard module, and it will display more detailed information. Sandra also has several useful benchmarking and stress testing features that are covered in more detail in the Third Party Tools section of the Performance Measurement & Troubleshooting chapter.

CPU-Z

A highly recommended tool, you can download CPU-Z from the CPU-Z Website. Run the program and it will provide you with all the major information you require about your hardware. It has highly 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, although note that for information to appear under the SPD tab you must first select the slot(s) on the motherboard that your RAM stick(s) occupy. CPU-Z even provides details about your graphics card under the Graphics tab, as well as PCI-E link speeds under the Graphics Interface section of the Mainboard tab.

GPU-Z

Another highly recommended tool, you can download GPU-Z from the GPU-Z Website. Note that GPU-Z is distinct from the CPU-Z utility covered above; it relates to your GPU (Graphics Processing Unit), which is typically your graphics card. Run the *GPU-Z.exe* file, and much like CPU-Z, it will provide you with all the information you need to know about your graphics card. Under the main Graphics Card tab you will see all 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. Finally, note that the Validation tab is there only if you want to submit your specs to the GPU-Z Statistics Database, which is not essential.

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 including a list of supported features, the drive standard, firmware version, serial number, as well as the current temperature of the drive and the health of the drive. It supports both hard drives and solid state drives. It 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 which are available, some of which are not free. However a combination of the tools in this chapter should be more than enough to give you all the details you need for every aspect of the hardware that is in your PC. I strongly encourage you to make sure that you are fully aware of your hardware specifications and capabilities, as incorrect knowledge can cause major problems when you try to install drivers or make configuration changes in software or in the BIOS for example. Also make sure that you are completely familiar with the contents of the Basic PC Terminology chapter of this book.

< PROVIDING SYSTEM SPECIFICATIONS

If you ever require technical assistance for a computer-related problem, you will inevitably have to provide your system specifications. Whether to a qualified technical support person, or to computer enthusiasts on an online forum, you should provide your specifications in an appropriate format. Simply copying the entire contents of a DXDiag text file for example might be quick and easy, but few people have the patience to wade through it, so I recommend using the format shown below unless instructed otherwise.

Also bear in mind that no-one can magically solve a problem simply by looking at your system specifications, no matter how detailed. There is no real substitute for becoming extremely familiar with your own system, for a range of reasons beyond simply troubleshooting problems.

Use several of the system information tools covered above to fill in the appropriate details in the categories shown below. The more detail you can provide, the better - the bare minimum is the brand and model number of your major components, but you should add in details like whether any of the components are overclocked or physically modified in any way. I have filled in some sample information from my own system in italics:

CPU:	*Intel Core i7 920 CPU @ 2.66GHz, stock speed, stock cooling*
Motherboard:	*Asus P6T Deluxe X58*
Graphics card:	*Leadtek Nvidia GeForce GTX 285 1GB, stock speed*
Monitor:	*24" Samsung 2443BW LCD*
Sound Card:	*Onboard ADI AD2000B HD Audio Chipset*
RAM:	*6GB (3 x 2GB) G.Skill 1333MHz DDR3*
Storage Drive(s):	*Western Digital 150GB VelociRaptor SATA2* *Western Digital 74GB Raptor SATA*
Optical Drive(s):	*Pioneer DVD-RW 216BK SATA*
Power Supply:	*Seasonic 700W M12*
Operating System:	*Windows 7 Ultimate 64-bit, including latest Windows Updates*
Other Details:	*257.21 Nvidia Forceware graphics driver* *6.10.0002.6585 SoundMax HD Audio sound driver* *System not overclocked, not physically modified*

You can also provide details of your other hardware, such as the keyboard, mouse, speakers/headphones and case, however these are usually not critical to solving most PC problems, at least not in the first instance.

I must stress again that it is an extremely important element of PC optimization and customization that you have more than just a passing acquaintance with your hardware components. Becoming familiar with hardware specifications and what they mean not only allows you to discover areas of potential optimization on your system and assists with troubleshooting problems, it also gives you the ability to make better purchasing decisions when buying a new system or upgrading any hardware components in the future.

BACKUP & RECOVERY

Computers can store a great deal of valuable information. Over time your PC may 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 backing up this information, so that if your PC is stolen, damaged, or its data is corrupted or accidentally overwritten, that you do not lose all this valuable data permanently. Hence backing up 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 your important and irreplaceable data before proceeding any further with this book. If you already have a recent backup of all your important data, you can skip to the BIOS & Hardware Management chapter and return to this chapter at a later point.

< WINDOWS BACKUP AND RESTORE

Windows 7 comes with an automated Backup and Restore feature that allows you to create both backups of specific folders, and also an exact copy of an entire drive, to a location of your choice. To access Backup and Restore, open the Backup and Restore component of the Windows Control Panel, or go to Start>Search Box, type *backup* and press Enter. Unlike Windows Vista, all the major features of Backup and Restore in Windows 7 are available to owners of any edition, with the exception of saving to a network location which is only possible in the Professional, Ultimate or Enterprise editions of Windows 7.

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 Backup and Restore window, or in the relevant Action Center notification in your Notification Area. 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 7, 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. Note further that 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, \Desktop, \Downloads, \Favorites, \Links, \Saved Games,* and *\Searches* directories for every user on the system.

This typically means that every default folder under the *\Users* directory will be backed up. This is one of the reasons why you should get into the habit of storing all your data under these default Windows directories and/or in a local Library - see the Personal Folders and Libraries sections of the Windows Explorer chapter for details.

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 the data necessary to recreate your entire installation of Windows, including all installed programs and settings, and all your user 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 include their Libraries and personal data in 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. 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 in particular 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, however you can click the 'Change schedule' link to bring up a new box, allowing you to choose whether to run the backup daily, weekly or monthly, the particular time and date, and most importantly, whether you want to disable scheduled backups altogether. You can also turn off an existing schedule at any time by clicking the 'Turn Off Schedule' link in the left pane of the main Backup and Restore 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 named after your computer name, which for standard home users is typically '*[username]*-PC'. 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 Windows Restore feature to restore your data - 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 Backup function 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 the previous versions of your backed up data, see the Managing Backups section further below.

Optimal Backup Strategy: Given the wealth of choice available as to how you backup your data, and what to include in the backups, here are some important things to consider which will help you decide on the best backup strategy for you:

To begin with, the benefits of backing up individual folders in combination with a full system image need to be explained further. A system image is ideal if you experience a significant problem, such as major drive corruption or damage, or a serious malware infection, and lose the ability to boot into Windows or have massive data loss of some kind - it allows you to restore your system to exactly the way it was when the image was made, even to another drive of the same type. A system image is not ideal on the other hand if you just want to restore a single file or folder which you lost or accidentally deleted for example, because it does not allow the restoration of individual files or folders under normal circumstances - this is what the backing up of individual user folders is meant to address.

By having a combination of both a system image and all your important folders individually backed up by Windows, you are covered for any eventuality, whether it is a total rebuild of your system after catastrophic failure, or quickly restoring a copy of a single file. This is why it is strongly recommended that you choose to create both types of backups on a regular basis. If drive space is preventing you from doing both however, you should always choose to back up your important personal folders, as these are much easier to restore individually when required in a range of scenarios.

Another important consideration is the portability of the backup. If your primary concern is the ability to move your backups around, whether from system to system, or for the sake of storing in a secure location like a safe, then I recommend using a USB flash drive, or ideally a large capacity external drive for your backups. These drives are highly portable, easy to store and protect, and can be plugged into any PC via an external USB port for quick and easy access.

If you don't have the option of a large external storage or separate internal drive for this purpose, then I recommend manually selecting only your most important personal folders or Libraries for backup to rewriteable DVDs. This is the least costly method and will use the least amount of space, typically spanning only a few DVDs, and provides excellent portability and ease of access on any PC. However make sure to use good quality DVD media and remember to update the backups on a regular basis.

If you are a Windows user who experiments a great deal, often installing potentially unsafe or unstable software, or overclocking your hardware for example, then ideally you should create a system image immediately prior to commencing any hardware or software experimentation. This will ultimately save you a great deal of time and effort, because at the first sign of system corruption or infection, you can simply reformat your system drive - or swap it for a similar drive - and install the system image on it in far less time than it would take to try to undo the damage, or reinstall Windows and all your software from scratch.

Finally, I strongly recommend against simply backing up to another partition on your system drive, because whether through physical drive failure or data corruption, you may need to reformat/repartition the entire drive, or find that the drive is unusable, and you will lose both your original data and the backups. Drives can often fail or become corrupt with little or no warning, and this can affect all partitions on a drive. Partitioning may be a useful data storage strategy but it is not an appropriate data backup strategy.

MANUAL BACKUPS

The Backup and Restore functionality in Windows 7 is designed primarily so that Windows can automatically backup 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. However there are times when you may wish to manually create backups on an irregular basis. Furthermore, you may wish to create a system image which contains more than just the data on your system drive(s) for example. In such cases you can use the Create a System Image and/or Create a System Repair Disc features in Backup and Restore as covered below:

Create a System Image: By default a system image created by Windows is an exact copy of the 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 in the left pane of Backup and Restore, as with the automated backup method, you must first choose your destination drive. Then, unlike the automated system image method, here you can specify additional available drive(s) to be included in the system image if you wish. 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 Next, review your backup settings, and 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 Windows 7 installation DVD can act as a system repair disc, however by clicking the 'Create a System Repair Disc' option in the left pane of Backup and Restore, you will be prompted to enter a blank CD or DVD which Windows will then turn into another system repair disc. See the System Recovery section in this chapter for full details of how to use a system repair disc and the associated system recovery options it provides.

If you've set up an automatic backup, you can also update that backup at any time, regardless of the schedule, by going to the main Backup and Restore window and clicking the 'Back up Now' button - this will immediately initiate an incremental backup run, whereby Windows will add any new or changed files to the existing backups.

ORGANIZING DATA

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 Windows Backup method, but to also take maximum advantage of Windows 7's other features which are covered in more detail later in this book.

Libraries: Your default personal folders are found under the *\Users\[username]* directory, and much like previous versions of Windows, there are several clearly-named subfolders designed for specific content such as music or pictures. However Windows 7 has also introduced Libraries, which go beyond your default personal folders, allowing you to access and manipulate files of different types across a range of locations in a single virtual folder. Of relevance here is that the Windows Backup feature incorporates full support for the Libraries functionality. The 'Let Windows Choose' option in Windows Backup for example automatically ensures that all the data stored in your Libraries is backed up; similarly, the 'Let Me Choose' option has a single tick-box entitled '*[username]*'s Libraries', which is ticked by default, making it quick and easy to backup your important files with confidence.

The point is that - aside from any other benefits - by setting up your Libraries so that they include all your important personal folders across all your storage locations, it makes sure that all your data is backed up without having to manually find and select each and every folder on each and every drive, and thus possibly forgetting to include important folders. You can create new Library folders at any time if some of your personal files or folders don't fit into any 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 store any personal files on the destination drive selected for Windows Backup, nor on a network, because by default Windows Backup will automatically exclude any such files when backing up a Library.

The Libraries feature is covered in detail in the Libraries section of the Windows Explorer chapter.

Settings and 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 like Firefox, or settings and saves for certain games, particularly older games, which are held in a variety of folders spread throughout your Windows installation. An easy option is to manually find and add all such folders to your Libraries, but this will also add files you may not want. A better option if you want to save space and also make it easier to restore these settings in the future is to sort out only the relevant files and back them up individually to a Library. Each browser should provide the ability to import/export bookmarks, so use this feature to export a copy of your bookmarks regularly to a Library of your choice. For games, check the documentation or go to the online support forum and find the default locations for storing saved game and configuration files. You may then wish to copy and archive these files, and store this archived copy in a Library - although bear in mind that if you are having problems with a game, or change your hardware before restoring a backup, that it is not recommended that you use your saved configuration files; only backed-up saved games are fine in such circumstances.

Programs: An important note regarding installed 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 7 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 7 also purposely skips adding program files and folders as part of the Windows Backup functionality for this reason.

Usernames/Passwords: You can store all your usernames and passwords securely electronically as covered in the Backing Up & Restoring System Passwords section further below. If you have no faith in electronic storage systems then 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 7 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.

MANAGING BACKUPS

Once you've created your backups using Windows Backup, you can manage them to ensure optimal use of space on your destination drive. To do this, go to Backup and Restore, 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 (typically *[username]-PC*), 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 because Windows usually backs up on an incremental basis, it already saves space 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 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 the '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're not 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 Backup feature, then you should go to the Backup and Restore window and click the 'Restore my files' button. Alternatively, go to the drive which holds the backup, and for the relevant folder (typically *[username]-PC*), 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 Windows 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 7 doesn't 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 7 installation DVD and using the System Recovery Options covered in detail under the System Recovery section of this chapter. Alternatively you can restore a system image by going to Control Panel>Recovery and clicking the 'Advanced recovery methods' link in the Recovery window. This will allow you to select the option 'Use a system image you create earlier to recover your computer'. 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 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 must 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, and is only available to Windows 7 Ultimate or Enterprise users:

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 .VHD file can corrupt the backup.
5. The VHD file 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 Windows 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 general things to note regarding restoration of backups:

- Windows 7 is able to restore files from a backup made using the Windows Vista Backup and Restore Center.
- System images can also be used in conjunction with the System Restore feature to provide additional restore points you can use - see the System Protection section below.
- If you simply want to restore an earlier version of a file, due to recent unintended changes for example, then it is best to first try using the Previous Versions functionality as covered under the System Protection section below.

SYSTEM PROTECTION

Windows 7's System Protection features, enabled by default on your system drive, are a set of basic safeguards put in place to ensure that you don't unintentionally alter your files without some form of backup to fall back on, and that any changes to important system files and settings can be easily reversed if necessary. 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 the left pane, or go to Start>Search Box, type *systempropertiesprotection* and press Enter.

Under the main System Protection properties window you will see the individual drives on your system for which system protection is currently 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:

- Restore system settings and previous versions of files - Selecting this option enables both System Restore and Previous Versions on the drive;
- Only restore previous versions of files - This option disables System Restore and leaves Previous Version functionality enabled;
- Turn off system protection - Disables all system protection functionality and deletes all restore points and previous versions.

You can also determine the maximum amount of space allocated to potential use by system protection features here.

To understand how best to configure these options for 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 emails, pictures, documents or music; instead it creates periodic Restore Points which are a snapshot of the key Windows system-related files and programs, 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. Go to the main System Protection properties window and click 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 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: Going to Start>Search Box, typing *rstrui* and pressing Enter; going to the Windows Control Panel and selecting Recovery, then clicking the 'Open System Restore' button; and under the Backup and Restore component of the Windows Control clicking the 'Recover system settings or your computer' link and then clicking the 'Open 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 you made any system image backups using the Windows Backup feature covered earlier in this chapter, 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 or overwrite 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 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 turn off System Restore, go to the main System Protection properties window and highlight a drive of your choice. Click the Configure button and to turn off only the System Restore functionality of System Protection, select the 'Only restore previous versions of files' option. Alternatively you can select the 'Turn off system protection' option if you also wish to disable the Previous Versions function, effectively disabling System Protection altogether. Importantly, doing this removes all existing restore points and previous versions.

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 beta driver which is unstable or makes an undesirable change to the Windows Registry, 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 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 - by default System Restore is allowed to use up to 5% of your drive space. It requires at least 300MB of free space on each drive to work properly, and only works on drives larger than 1GB. Over time System Restore will delete older restore points automatically so as not to exceed its size limit. Fortunately Windows 7 has also added the ability to readily select exactly how much drive space to allocate to System Protection features - see further below for details.

Deleting Restore Points: Windows automatically deletes older restore points once System Restore hits its allocated space limit on your drive. However 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 Cleanup utility - see the Disk Cleanup section of the Cleaning Windows chapter. If you want to delete all restore points, including the latest one, open the System Protection properties window, click the Configure button, and then click the Delete button. While this will remove all restore points as well as all previous versions of files, it doesn't prevent Windows from creating new ones again in the future - that will only occur if you choose to turn off system protection altogether.

Previous Versions

Although System Restore does not restore copies of your personal files as part of a restore point, the System Protection feature ensures that Shadow Copies, also known as the Volume Shadow Copy Service (VSS), or more commonly known as Previous Versions, are automatically created for most non-system files during the creation of restore points. As long as you keep System Protection enabled on a particular drive, then shadow copies will also be made of relevant files whenever they are altered. While shadow copies are not a substitute for taking proper backups of your important files, this is an added safety feature in Windows 7 which remains much the same as when it was introduced in Vista. Its aim is to make recovery from accidental deletion or alteration of important files much easier, and is yet another reason why it is recommended that you do not disable System Protection.

Just to be clear: the main difference between System Restore and Previous Versions is that System Restore is used for restoring system-related files and settings, while Previous Versions is for restoring personal and other non-system files; Previous Versions of Windows system files, such those under the *\Windows* directory, are not kept.

To view and/or restore any existing Previous Versions of a file, do the following:

1. Open Windows Explorer and browse to the selected file, whether in its original location or in the appropriate Library.
2. Right-click on the file and select 'Restore previous versions', or alternatively right-click on the file, select Properties and click on the 'Previous Versions' tab.
3. Under the Previous Versions tab you will see all available previous versions listed in order of the date in which the file was last modified, not the date it was saved. If the file was not modified since the last restore point or Windows Backup was taken, there will be no previous versions available. If you want to restore a file which has been deleted, and thus is not available for you to select and examine its Previous Versions tab, then you can look at the Previous Versions tab of the folder in which it originally resided instead and restore a previous version of the entire folder.
4. To preview the contents of a previous version before restoring it, highlight the version you wish to restore and click the Open button.
5. Once you have found the version of the file or folder you wish to restore, you can either click the Restore button which will overwrite your existing version of that file with the previous version, or you can click the Copy button which allows you to copy the previous version to another directory. The Copy option is recommended, especially if you are restoring an entire folder, because this allows you to keep and compare both versions of the file or folder, and then discard whichever files you no longer need.

6. If you select the Copy option you will be prompted to choose a directory in which to place the previous version - I recommend an empty directory. If you choose the Restore option and a current version of the file or folder already exist, you will be prompted to confirm the choice and if you click Restore again, it will overwrite any existing version on your drive. Note that shadow copies as part of a restore point are stored on your main Windows drive and will be restored immediately, whereas shadow copies which are part of a Windows Backup will be stored on another drive and require that you have that particular drive connected before you can restore the file.

How recent your previous versions are depends on how frequently you use the Windows Backup and System Restore functions, so this is not a foolproof method of restoring a file to precisely the desired version, especially for files which you change very often. Also, depending on the amount of drive space you have made available to System Protection and the number of files on your system, over time you will lose older previous versions. Note also that if you access your main Windows 7 drive with a version of Windows prior to Vista, because of the differences in NTFS the older version of Windows will automatically delete all shadow copies, which means the deletion of Previous Versions as well - keep this in mind if you are dual-booting Windows 7 with Windows XP for example.

Previous Versions is a very useful function, and makes a strong case for not disabling System Protection, especially as it has no performance impact. It is certainly much quicker and easier to use Previous Versions for undoing accidental deletions and unintended changes to files than any other method. However I must stress that it is not a substitute for taking proper backups, because shadow copies are stored on your system drive, and in the event of drive corruption or complete failure, you will lose both the originals and the Previous Versions at the same time.

RESIZING SYSTEM PROTECTION'S RESERVED DRIVE SPACE

As noted under System Restore, for full functionality the System Protection features require a 1GB or larger drive, at least 300MB of free drive space, and can use up to 5% of your total drive space on your main Windows drive by default. In Windows Vista you were only able to alter these settings by using the `vssadmin` command with appropriate parameters in an Administrator Command Prompt. While you can still use this command in Windows 7, it is no longer necessary because all the relevant information and resizing capabilities are provided in a graphical user interface. Go to the main System Protection properties window, found by clicking the 'System Protection' link in the System component of the Windows Control Panel. Then highlight the relevant drive and click the Configure button. Under the Disk Space Usage section of the window you can see the amount of space currently used by System Protection. To limit the maximum amount of space available to System Protection, move the slider to the appropriate percentage of your drive space and then click the Apply button.

By reducing the maximum amount of space usable by System Protection, you may lose older restore points and previous versions, and if set too low this may make System Protection effectively useless by not being able to protect all of your files, folders and settings. I recommend that you set at least 2GB of drive space, preferably more if you have more files on the drive, particularly if they are large files. If in doubt, do not alter this setting from its default.

Remember that you can manually remove older restore points at any time to reduce disk space usage without completely losing the protection afforded by these features - see the Disk Cleanup section of the Cleaning Windows chapter. In the end if you truly resent any space being taken up by System Protection features, or just don't have the space to spare on your drive, then it may be best to simply disable System Protection for that drive altogether rather than cripple it and hence have a false sense of security.

Regardless of which option you choose, I strongly recommend that you make sure to regularly back up all your important and irreplaceable files often and to multiple locations, in case of accidental deletion, malware infection, drive failure, theft, or fire. 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 usual Backup features, nor is it generally recommended that you simply write down a list of your usernames and passwords and save them as a standard document or text file for example - this is a big security risk. This section provides several alternates which allow you to make sure your important passwords are 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 Protected Administrator account in Windows, i.e. the first User Account you create when Windows 7 is installed. 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 is a major headache. With the NTFS file system it is quite difficult to access the data on your drive without the correct login password. Clearly the best thing to do is backup your password now before anything happens, so that if necessary you can restore it without any difficulties. The recommended way to securely back it up is as follows, though note you will require a floppy disk or preferably a USB flash drive for this procedure:

BACKING UP LOGIN PASSWORD

1. Open the User Accounts component of the Windows Control Panel and click on your User Account.
2. Connect your USB flash drive or insert a floppy disk as applicable.
3. Click on 'Create a Password Reset Disk' in the left pane. 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 or floppy disk first, open Windows Explorer, right-click on the drive 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. Store this disk/stick somewhere safe, as anyone can now use it to effectively access your account.

I encourage you to purchase a small USB flash drive just for this purpose. The added security and protection against loss of your login password is well worth this tiny investment.

RESTORING LOGIN PASSWORD

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

1. Boot your PC as normal, and on the Windows Login screen select your User Name.
2. Try entering your password (or just press Enter), and if it's incorrect you'll get a message saying the Username or Password is incorrect. Click OK and then select 'Reset Password', inserting the password reset disk or USB flash drive you created earlier.
3. Follow the Password Reset Wizard to set a new password and log back into your system.

The password reset disk needs to be write-enabled so that Windows can update it with the new password automatically during this procedure. When done, you should once again put it away in a physically secure place.

The main Administrator account on a PC can log in at any time and change the password for other 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, regardless of whether you are an Administrator or a Standard user of the PC.

RECOVERING LOGIN PASSWORD

If you've completely lost your login password, you don't have a password reset disk, and you don't have any other Administrator who can reset it for you then generally you're in a lot of trouble. Usually you will have to simply reformat and reinstall Windows.

However if you are really desperate to regain access to your user account and you have the time, you can try the Offline NT Password & Registry Editor for cracking your Windows account password. I am providing this information in good faith for users who want to restore their own account, not to attempt to hack other accounts. If you are alarmed at the existence of cracking tools and methods for getting account passwords in Windows then I strongly recommend that firstly you set your user account password to something strong such as a 12 character (or more) base64 or base95 random password. For example, you can use this online Password Generator to generate one. These complex passwords are extremely difficult to crack, especially the more characters you use. Secondly and most importantly, I recommend that you restrict physical access to your machine to only those people you absolutely trust, and if in doubt, make sure to observe the use of your PC by others to ensure they don't use a tool like the one above to compromise your account's security.

STORING PASSWORDS

Remembering username and passwords for various websites and software soon becomes extremely difficult to do. Most users wind up using 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) and numbers, and even some symbols thrown in for good measure, virtually no-one can remember these passwords. Web browsers make the process easier by allowing storage of usernames and passwords for automatic entry into relevant prompts on websites, however this still doesn't solve the problem of potentially losing your passwords in the event of an emergency, such as drive corruption, or if you want to transfer the passwords to another machine, or if you simply don't wish to trust your browser to store your passwords.

Credential Manager is a new feature in Windows 7 based on a very similar feature found in Windows XP and Vista under an advanced User Account configuration screen accessed by running the *control userpasswords2* command. Credential Manager can now be accessed directly under the Control Panel, or by going to Start>Search Box, typing *credential manager* and pressing Enter.

The main purpose for Credential Manager is to store login credentials for accessing other computers, servers or sites which support this feature. You can add the relevant credential details by clicking the Add link on the right side of the three main categories: Windows Credentials, Certificate-Based Credentials, or Generic 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. However the resource 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. This means that Credential Manager is not as useful for the average PC user.

Importantly, the information you enter here is stored as part of the Windows Vault, which is an encrypted file you can backup to any location - preferably a removable source such as a USB flash drive - and then use on other machines as required. If any data has been entered in Credential Manager it will display a 'Back up vault' link at the top which allows you to do precisely this, and the 'Restore vault' link can similarly be used to restore a previously backed up vault.

If instead you simply want to hold all your usernames and passwords in a relatively straightforward central database protected by high level encryption, which also provides 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. The differences in features are spelled out in this table, but for the most part all the functionality required, in addition to portability and smaller footprint, can be found in the Classic Edition (ZIP Package) version of this software, which is the one I recommend and describe below.

To use KeePass, launch *KeePass.exe* and select New under the File menu, then enter a Master Password and/or select a Key File. These measures are used to secure the password list, and while the key file is not essential, make sure to enter a master password which has a high bit-rate by using a combination of letters both lowercase and uppercase, as well as numbers, and not just a common word or name. This master password is a critical component - if you forget it, there is no way to unlock your password list. 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, other 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 To' feature under the File menu. I strongly recommend exporting the database as a KeePass Database (.KDB) file. This database can then be stored or backed up 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 password/key file.

Recovering Other Passwords

If you haven't properly stored your passwords and you've managed to forget or lose an important password which you can't simply reset, such as your Windows login password, there are utilities you can use to recover or crack these passwords. The best free tool which works in Windows 7 is Ophcrack, though you can also try the free Cain & Abel. I cannot go into detail regarding these tools, as it is beyond the scope of this book. The presence of these types of tools should again 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 PC Security chapter.

< OTHER BACKUP METHODS

The built-in backup and system protection methods in Windows 7 are extremely useful and should not be ignored. In general they 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 Windows Backup. The two major software packages for imaging drives quickly and easily are Norton Ghost and Acronis TrueImage. However neither is free, so they will not be covered here in any detail - refer to the relevant Norton Ghost Manual or the Acronis TrueImage User Guide for more details. The main benefit of third party imaging utilities over Windows 7'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 Backup system image feature should meet the majority of your needs.

ONLINE BACKUP

Online backup services allow you to back up data to a secure location, typically a remote data center. This ensures that your data is encrypted and stored safely, but this not a free service, so it is only recommended if you genuinely need that level of protection against data loss or theft. 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 however there are several ways of using free online services to provide added security against such data loss:

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. In fact you can use a free utility such as Gmail Drive to make storage of data on a Gmail account much easier to manage, though bear in mind that Gmail and other free email providers may take steps to prevent this practice if it becomes widespread.

Photo Storage: There are a range of free photo album providers which allow you to upload and keep a large library of digital photos, which is extremely useful again as yet another place to store irreplaceable photos in case the originals are ever lost. The most popular free photo gallery providers are Flickr, Photobucket and Picasa. Make sure to read the instructions for the gallery and enable all the privacy features so that members of the public cannot view your gallery contents without your permission. Regardless of such features, a direct link to a particular photo can often be publicly discovered, so I do not recommend uploading sensitive photos to such galleries.

Ultimately, if you believe your data is worth preserving against all eventualities, or you need to store it with maximum security, it is necessary that you consider a professional remote data storage service to hold your backups. The free options while convenient do not provide sufficient security against unauthorized access. Of course most Windows users do not require this level of protection; regularly taking both system image and personal folder backups and also keeping a copy of your backups in a fireproof safe for example is sufficient protection.

CUSTOM BACKUPS

The Windows Backup functionality in Windows 7 now allows any user the ability to not only select individual folders for backup, but to also create a full system image backup as well, and do so on a schedule. As such I strongly recommend that you take advantage of this functionality. However I also recommend that you create additional custom backups of your data for one very important reason: any automated backup utility you use, whether the Windows utility or a third party one, may inevitably backup problematic or sub-optimal settings or conditions. This means that any time you restore such backups, even after a clean reformat and reinstall of Windows, you may also be restoring the problematic files or settings as well. 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 scheduled backups, making them much less useful when the time comes to use them. There's also the added issue of not being able to readily use backups made using the Windows 7 Backup utility on older versions of Windows, such as Windows XP, or on other machines.

So in addition to taking regular system image and personal folder backups using Windows Backup, I recommend that you create a custom 'clean' backup copy of all your important files which is highly portable and stored separately to your PC. The quickest way to do this is:

1. Manually scan your entire system thoroughly for malware using the malware scanners covered in the PC Security chapter.
2. Find a good quality USB flash drive or several rewriteable CD, DVD or Blu-Ray discs. For the USB drive, make sure to format it first in FAT32 format by connecting it your PC, and under Windows Explorer right-click on the drive, select Format, then select FAT32 under the File System box and click Start. FAT32 is the most compatible file system, which is why it is recommended for a USB flash drive.
3. Open Windows Explorer and manually copy across every single file and folder which you consider irreplaceable and you wish to backup. Also remember to generate a new backup of your bookmarks using the bookmark management options in your browser, copy across any saved games (but not settings) you wish to keep, and also export your stored emails to an empty folder and then store the entire exported folder(s) in an archival format like .ZIP for easier handling - see the Backing Up section of the Windows Live Mail chapter of this book for more details of how to do this. Since you are only copying across the most important personal data, there shouldn't be a large volume of data; certainly it should all fit on an 8 or 16GB USB flash drive, or at most a box of DVDs or a single Blu-Ray disc.
4. Once completed, store this backup in a secure location - at the very least in a lockable drawer of some kind.

While the above procedure may seem excessive, it really does provide both 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, Registry settings or system settings of any other 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 Windows Backup features in Windows 7 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 your personal and 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 7 provides protection against this with its built-in Backup and System Protection features as covered earlier in this chapter. You should also leave the Recycle Bin enabled and configure it appropriately to make sure that deleted files are moved to the Recycle Bin - see the Recycle Bin section of the Cleaning Windows chapter.

However in the end for one reason or another you may still wind up permanently deleting a necessary file, and have no previous backups, restore points or previous versions available. Fortunately, when you delete a file from your system the file is removed from view and you regain the space on your drive, however 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 special software to do so.

Recovering Deleted Files

There are several tools I recommend that you use to potentially recover your deleted files:

Recuva: To use Recuva, after installing it you can simply follow the wizard which appears. For more options, click the 'Switch to advanced mode' button in the main Recuva window, or disable and exit the wizard at startup. Essentially once you specify the particular drive to scan, or all available drives if you so wish, you 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 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, but bear in mind this could take quite a while.

Restoration: To use Restoration 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 run the *Restoration.exe* file as an Administrator and either 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: If you want to recover deleted or damaged files on a CD or DVD disc, you will have to use a more specialized utility such as IsoBuster. While it can be downloaded for free, IsoBuster requires paid registration for full functionality. However you can use the free version to first check to see if there is any recoverable data on your particular disc. There is no guarantee that any usable data can be recovered from a damaged or deleted disc - particularly if it has been overwritten.

Regardless of which tool you use, the more activity there is on the medium where the deleted files reside, the less chance you can fully recover them, since portions of them may have been overwritten by new data. This is why the files recovered by any tool are often not complete, so there is no guarantee you can recover a usable file this way. For this reason, if you have accidentally deleted an important file, try and minimize any further activity before running a data recovery utility. If you can't run a recovery utility straight away it is best to shut down Windows immediately to prevent a background task from commencing (e.g. a scheduled defragmentation) as these will potentially overwrite the areas where deleted file portions are sitting. Furthermore it is best to install on and run a recovery utility from another drive, again to prevent overwriting data on the drive where the deleted files reside.

Permanently Deleting Files

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

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

Next, if using Recuva, launch it and 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.

If using Restoration, then launch it and 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 you wish to securely wipe the contents of an entire hard drive, for the purposes of ensuring the removal of malware, or disposing of or reselling a drive for example, then you can use the free DBAN utility to do so.

These methods will permanently delete a file so that it is effectively unrecoverable by virtually any program or method. However there always remains the possibility that some data may still be recoverable by law enforcement agencies using specialized methods, although it is highly unlikely that anyone could recover the bulk of this data regardless of the methods used.

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.

A quick and easy way to zero fill a hard drive and error check it at the same time is to use the built-in formatting functionality of Windows itself to do a full format - 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 manufacturer's website for an appropriate utility such as: Seagate DiskWizard & SeaTools for both Seagate and Maxtor drives, Western Digital Data LifeGuard, or Hitachi Drive Fitness.

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

This section covers the main methods and important Windows tools which can assist you in attempting data recovery and/or regaining the ability to boot into Windows after experiencing major system issues.

BASIC TROUBLESHOOTING

The most likely cause of a major system problem is one or more of the following:

- Overheating and/or Overclocking - See the Overclocking and BIOS & Hardware Management chapters for details. An overheating and/or overclocked component can malfunction in unusual ways, or cause other components near it to overheat and malfunction.
- Bad shutdown - If your system suddenly reboots itself or you see a Windows Blue Screen error message, or if the power is lost to your PC while it is on, this prevents Windows from closing down properly, and can result in data corruption leading to various problems. See the Windows Errors section of the Performance Measurement & Troubleshooting section for more details.

§ Faulty software - Installation of a faulty driver or program can cause data corruption or harm to important Windows settings or file. This also includes the installation of malware as covered under the PC Security chapter.

§ Faulty hardware - If a component is physically defective or damaged, it can corrupt your Windows installation or process data incorrectly, causing a range of problems. This includes an insufficient or unstable supply of power from your PC's Power Supply Unit. See the Hardware Management section of the BIOS & Hardware Management chapter.

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

If you can't switch on your 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 or shows screen corruption immediately after you switch the PC on, or at any time prior to the Windows startup procedure, then it can be stated with absolute certainty that the issue is with your hardware configuration, not Windows or your installed programs, drivers, or software settings. This is particularly true if you can't enter Safe Mode - see the Advanced Boot Options section below. This is an indication of problems such as a bad BIOS setting, faulty or missing hardware connections, unstable power supply, overclocking, overheating, or faulty hardware - see the BIOS & Hardware Management chapter for details of things to check for.

If you 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 can't boot successfully into Windows, then 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 below, as well as the Windows System Recovery section further below for details of these procedures.

If you can boot into Windows: If you can boot into Windows but experience major problems once in the Windows environment, try these steps:

1. Run a range of malware scanners to make sure your system is free of any malware which may be the cause of the problems - see the PC Security chapter for details. You may need to run these malware scanners in Safe Mode if they don't launch under the normal Windows environment.
2. Run System Restore and revert to the most recent Restore Point available - see System Restore earlier in this chapter. This is the quickest method for undoing potentially harmful changes to system files without affecting your personal files.
3. If you don't have any recent restore points, try to restore a recent full Windows Registry backup, as corruption or bad settings in the Registry are a major source of problems. See the Backing Up and Restoring the Registry section of the Windows Registry chapter.
4. If you don't have any recent backups or restore points of any kind, try uninstalling any recently installed software and/or drivers - see the Manually Updating or Uninstalling Drivers section of the Windows Drivers chapter in particular for ways of cleaning out badly installed drivers which do not uninstall correctly.
5. Use the System File Checker as detailed below to scan for any changes to your Windows system files.

If these methods don't work, refer to the Performance Measurement & Troubleshooting chapter for more advanced tools and methods, though bear in mind that major problems can sometimes only be solved by reformatting and reinstalling Windows.

The rest of this section covers the main Windows tools used for 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 suspect that corrupted/tampered system files are leading to unusual Windows behavior. To access 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 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 7 DVD.
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 should be changed to the drive on which you ran SFC if it is not C: drive.
3. The resulting *sfcdetails.txt* file will appear on your desktop by default, and can be opened with a text editor like Notepad to reveal the process SFC ran through. Check for any errors or unrepairable files.

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, however it does ensure that important system files are unaltered, which removes one variable from the equation when troubleshooting a problem.

ADVANCED BOOT OPTIONS

To access a range of more advanced startup options for Windows 7, reboot your PC and keep pressing the F8 key during startup. You will come to a screen with the heading Advanced Boot Options, providing a range of options, including some or all of the following:

Repair your Computer
Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt
Enable Boot Logging
Enable low-resolution video
Last Known Good Configuration
Directory Services Restore Mode
Debugging Mode
Disable automatic restart on system failure
Disable Driver Signature Enforcement
Start Windows Normally

The most useful of these are covered below in more detail:

Repair your Computer: Selecting this option leads to the System Recovery Options menu - see the Windows System Recovery Options section further below for details.

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. You can read the details of the specific devices, drivers and services which are loaded up in Safe Mode in this Microsoft Article.

There are three types of Safe Mode you can launch:

- Safe Mode - This is the basic Safe Mode and usually the best option to select.
- Safe Mode with Networking - Loads up Safe Mode with network drivers, allowing Internet access. You should not select this mode to start with if your issue is potentially related to networking device drivers or a malware infestation.
- 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. Note that this is not the same as DOS mode.

When you enter Safe Mode you will see the Windows Desktop, typically shown at lower resolution, and with no graphical enhancements such as Aero or even the background wallpaper. The words 'Safe Mode' appear around the edges of the screen to inform you that you are running a cut-down version of the Windows 7 environment. The main use for Safe Mode is to determine whether your device drivers or recently installed software are the source of a problem you are currently experiencing, and allow you to uninstall them or alter your system as necessary to be able to restart normally. Because Safe Mode does not load any of your installed third party device drivers - instead using the default versions built into Windows - and because Safe Mode does not load up any startup programs or non-essential services into the background, this gives you the opportunity to determine whether your drivers or startup programs are causing problems.

If you couldn't boot into Windows normally, but you can boot into Safe Mode for example, that is a clear sign that one of your recently installed drivers or programs is the likely cause of the problem. You can choose to permanently remove/roll back or temporarily disable the relevant programs or drivers by using Device Manager or MSConfig for example. Furthermore if you made a change to a system setting or the Windows Registry that may have caused the problem, you can undo the setting in Safe Mode, or use System Restore to revert to an earlier restore point, or restore a Registry backup here.

Finally, a major use for Safe Mode is the removal of malicious software such as viruses, trojans or spyware. Many of these can load into memory areas of Windows that cannot be unloaded during normal Windows operation, preventing proper removal. However in Safe Mode there are no such protected memory areas, and no startup programs or services are loaded with Windows, so this is the best way to remove such troublesome software. Enter Safe Mode and find and delete the problematic file(s), edit your startup items or Services to remove unusual or harmful entries (See the Startup Programs and Services chapters), or run a suitable scanner in Safe Mode to find and remove any malicious software (See the PC Security chapter).

In extreme cases where you cannot resolve your problem using Safe Mode, then at the very least Safe Mode provides you with the opportunity to access and backup your important personal files before reinstalling Windows or restoring a system image for example.

Note that if you cannot boot into Safe Mode using the F8 method during bootup, another method (if you can boot into Windows) is to use the MSConfig utility to select Safe Mode - see the Boot Configuration Data section of the Boot Configuration chapter for details of how to do this. Importantly, once you have entered Safe Mode using this alternate method, you need to run MSConfig again and disable the 'Safe Boot' option under the Boot tab of MSConfig so you can reboot into the normal Windows environment again.

If you find that you cannot boot into Safe Mode, or are having similar problems in Safe Mode as you are in normal Windows - for example your graphics are garbled or show glitches - then the problem is likely hardware-based one such as overclocking, excess heat, permanent damage to a component/faulty component(s), or a bad BIOS setting or incompatibility - see the BIOS & Hardware Management chapter.

Enable low-resolution video (640×480): This option starts Windows using a low resolution of 640x480 pixels and a low refresh rate supported by all monitors. This is useful if you've selected display settings which are unsupported by your monitor and your screen goes blank for example. If this occurs, hold down your PC's power button for up to five seconds to force Windows to shut down and select this option in the Advanced Boot Options upon restart.

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 can be useful for more advanced users troubleshooting startup problems.

Last Known Good Configuration: You should select this option if trying to resolve problems with Windows not booting up or acting strangely. This mode uses the driver and Registry settings which were in effect the last time you successfully managed to boot into Windows. It will not alter or revert your personal files to an earlier state, only certain system-related files/settings and the Windows Registry.

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.

Disable Driver Signature Enforcement: This is an option referring to an important security feature of 64-bit versions of Windows which is detailed in this Microsoft Article. By default, the 64-bit version of Windows 7 - and Vista before it - only load up a Kernel-mode driver if Windows can verify the digital signature of the driver. Unsigned drivers therefore will not be loaded by 64-bit Windows - see the Driver Signature section of the Windows Drivers chapter for details. However you can press F8 during bootup and select this option 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. One alternative is to use the Sleep or Hibernate feature in Windows to close down Windows without restarting, and hence keeping this setting in effect - see the Power Options section of the Windows Control Panel chapter. The permanent solution is to use a signed driver downloaded from a trusted source, however some manufacturers will not release such drivers on a frequent basis, nor will they release such drivers for older hardware. For more details of the key differences between 32-bit and 64-bit Windows, see the 32-bit vs. 64-bit section of the Windows Installation chapter.

Start Windows Normally: This mode is the first one you should select if you encounter the Advanced Boot Options unexpectedly. Windows typically displays the Advanced Boot Options automatically after a bad shutdown of Windows, and in many cases, simply restarting Windows normally will result in booting up into Windows without any issues. If you can boot into Windows you will have to determine what caused the bad shutdown if it wasn't an obvious one-off such as loss of power.

< WINDOWS SYSTEM RECOVERY OPTIONS

The Windows Recovery Environment was introduced in Windows Vista, and while remaining much the same, has had some refinements added in Windows 7. More commonly referred to as the System Recovery Options, this feature of Windows attempts as much as possible to simplify and automate the process of recovering from any major system issues preventing you from booting up successfully into Windows. There are several ways to access the System Recovery Options menu:

Automatic Access: If Windows detects that it is having a problem booting up normally, it may automatically prompt you to launch a component of the System Recovery Options such as Startup Repair - which you should do - or automatically load up the Advanced Boot Options menu, at which you can select the 'Repair your Computer' link to launch into the System Recovery Options.

System Reserved Partition: By default Windows 7 will install a small 100MB System Reserved Partition, also known as a Recovery Partition, as part of normal Windows installation under certain circumstances. This partition contains your Windows boot files, the required tools to run System Recovery Options, and is also required for the BitLocker Driver Encryption feature. Alternatively, if you purchased your PC with Windows 7 already installed, this partition may have been created by the manufacturer. In some scenarios Windows 7 will not create this partition during its installation, or if you specify that you do not want its creation during Windows installation. In these cases, the contents of the Recovery Partition will instead be created under a hidden and protected *Recovery* directory found on your main Windows drive. More details regarding this System Reserved Partition can be found in the Installing Windows section of the Windows Installation chapter.

Regardless of where this recovery data sits, if you keep pressing F8 to enter the Advanced Boot Options screen at Windows startup - see Advanced Boot Options earlier in this chapter - then you should be able to select the 'Repair your Computer' link to launch System Recovery Options.

Booting Off the Windows 7 DVD: All Windows 7 installation DVDs come with the Windows System Recovery tools. To access these tools in case you can't access them using any other method, insert your original Windows 7 DVD and restart your PC. Your computer should boot from this DVD, but if it doesn't, go into your BIOS and set your optical drive as the first boot device then reboot, and if prompted, press any key to boot from the DVD. Once you reach the main Windows installation screen, select your language and keyboard layout, then click Next. On the next screen click the 'Repair your computer' link at the bottom left of the box.

System Repair Disc: In the event that you cannot access the built-in Windows System Recovery tools and you don't have a Windows 7 installation DVD, you can use a custom System Repair Disc to launch System Restore. This disc must first be created in advance under the Backup and Restore component of the Windows Control Panel by clicking the 'Create a system repair disc' link in the left pane and inserting a formatted DVD - see earlier in this chapter for details. Once created, you can boot up from it using the same instructions as those provided for booting off the Windows 7 DVD above.

Once you have launched the System Recovery Options using one of the methods above, you will be presented with prompts to firstly select the relevant OS, then select your keyboard input method, and to then log in to your User Account - note that if your User Account has no password, leave the Password box blank and click Next. Finally, you will see the main System Recovery Options menu, which is covered in more detail below:

Startup Repair

Startup Repair is the most important feature of Windows 7's recovery options. It is the primary tool that anyone can utilize to diagnose and automatically fix issues which are preventing error-free bootup into Windows. It is also the first option 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 system or boot file, it will do so automatically, rebooting as often as required, and will provide links at the end of the process which you can click to see precisely what issues have been found and resolved. However Startup Repair cannot fix certain issues resulting from any type of hardware failure, certain types of malware, or if your system drive is not being correctly detected for example. If Startup Repair cannot detect or repair the problem, then this tends to indicate that the problem is more complex and requires investigation of both potential hardware-based issues such as a physical fault, overclocking or overheating, or perhaps the presence of harmful software on your system.

System Restore

This utility has been covered in detail under the System Restore section earlier in this chapter. This option allows you to launch System Restore and use any available restore points in case you can't access System Restore from within Windows. Obviously this requires that a suitable restore point be present and able to be used. This is yet another reason why you should keep System Restore enabled. If using System Restore still doesn't resolve a problem, then this tends to indicate that the problem is more likely to be hardware-related.

System Image Recovery

This utility has been covered in detail under the Windows Backup and Restore 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 took a full system image backup at an earlier date. 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 System Recovery 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.

WINDOWS MEMORY DIAGNOSTIC

This option allows you to launch the Windows Memory Diagnostic tool by clicking the 'Restart now and check for problems' link, or schedule it for launch at the next restart by clicking the 'Check for problems the next time I start my computer' link. The first option is fine unless you have other things you still wish to do in the System Recovery Options first, in which case choose the second option. If the tool detects any errors with your memory it will let you know, though this doesn't automatically mean your RAM is physically faulty - other aspects of your memory subset could be at fault, including memory-related BIOS settings for example. See the Windows Memory Diagnostic section under the Performance Measurement & Troubleshooting chapter for more details.

COMMAND PROMPT

This option allows you to open a MS DOS Command Prompt window to enter a range of commands. 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 the stricken drives 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 System Recovery Options replaces the Windows XP Recovery Console, almost all of the most useful Recovery Console commands from XP can still be used in Windows 7. 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 in Windows 7, 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 /?`).

In particular, 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.

If none of the System Recovery Options help you in repairing or restoring your Windows installation, then your problem is more complex than simple Windows system file corruption, and likely a hardware-related issue of some kind. Furthermore, unless any such issues are correctly diagnosed and resolved properly, it may be a waste of time to repair or reinstall Windows, as the same issues will reappear again in due course. Read the rest of this book, particularly the BIOS & Hardware Management and Performance Measurement & Troubleshooting chapters for more details of how to ensure that your hardware is set up and functioning correctly. If necessary, seek additional technical support from your hardware manufacturer if you believe your hardware may be faulty.

Ultimately the best course of action if you can't recover Windows is to reformat your drive and either reinstall Windows 7 on it, or restore a fairly recent system image which you believe was taken when the system was stable and free from malware. Then run further diagnostics within Windows as necessary.

The most important point throughout this entire chapter is that it is absolutely critical that you become familiar with all of Windows 7's backup and recovery features, and get into the habit of regularly backing up your irreplaceable files, and doing so to a range of places, using a range of methods precisely so that in the event of any kind of issue, you have peace of mind knowing that you're not going to lose important data.

BIOS & HARDWARE MANAGEMENT

Before delving any further 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 configured 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 settings in the BIOS are correct, that the hardware is properly cooled, and that all of your devices are configured to function optimally in Windows. This chapter covers all of these topics in detail.

Note that this chapter does not provide information on how to select and purchase a PC from new, however if you are interested in that type of information, see my Hardware Confusion article for general guidance.

< THE BIOS

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 what 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.

Note that some of the latest motherboards may have a different type of BIOS-like interface called UEFI (Unified Extensible Firmware Interface). UEFI is a new form of software interface between your hardware and the Operating System. While UEFI brings with it a range of changes as covered in this Intel Article, in practice you will still need to configure all your hardware settings in much the same way as a BIOS, so the information in this chapter still applies in much the same way.

POST SCREEN

As your BIOS 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. A quick general guide to what the startup error beeps may mean is this POST Error Codes, but a more accurate description specific to your hardware is usually found in your motherboard's manual.

If you have no initial POST errors you will then see your PC's startup screen, which shows such information as your BIOS type (e.g. American Megatrends), the key to press to access your BIOS 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.

BIOS SETTINGS

To access the detailed settings in your BIOS, you typically need to press a particular key (e.g. the Delete key) repeatedly as your system is booting up - check your motherboard manual. If your BIOS also has a password then you will need to enter it first to access your BIOS settings; if you've forgotten the password, then try this BIOS Password Site. Once in your BIOS screen you will see a multitude of settings. The layout of the BIOS 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. The best reference source is this Definitive BIOS Optimization Guide - scroll down that page to find the 'Free Access' link to the guide. It covers all the common BIOS settings, and combined with your motherboard's manual and Google, you can understand what all of your BIOS settings do and thus undertake the very important task of optimizing your BIOS before doing any Windows tweaking.

I cannot stress the importance of making sure all the major settings in your BIOS are correct for your particular hardware setup, and importantly that you've disabled all unnecessary devices and options. It may take some time and some research, but it only needs to be done once and ensures maximum performance and stability. No amount of Windows customization can overcome a badly set up BIOS.

BIOS UPDATES

The BIOS is written on a rewriteable ROM chip, which means that it can be updated (or 'flashed') with new information. Motherboard manufacturers release new BIOS versions that 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. I can't list all the manufacturer websites here, as there are far too many, however if you have a look through your motherboard manual you should see a link to the appropriate website. Download the latest BIOS for your exact motherboard brand and model number and follow the instructions on the site to 'flash' (reprogram) the BIOS chip on your motherboard with this new BIOS version. A word of warning: flashing the BIOS is not to be taken lightly. If something does go wrong then your PC may not boot up and you may have to take your motherboard to a dealer to have the BIOS chip replaced or reprogrammed. While this is rare, when updating your BIOS make sure you follow the instructions provided to the letter.

Note that modern motherboards allow flashing the BIOS from a CD, DVD or USB flash drive, so installing a floppy disk drive on your PC is no longer necessary.

FIRMWARE UPDATES

Your motherboard is not the only device which has a BIOS. Many components, indeed most major electronic equipment like TVs, DVD and Blu-Ray players and mobile phones have their own inbuilt BIOS chips. The software on these chips is typically referred to as Firmware, and all firmware can be updated using the correct equipment and software. For PC components, it can be upgraded in much the same way as flashing your BIOS. You will need to check your manufacturer's website for more recent versions of the BIOS/firmware you require, and any specific instructions or software necessary. The most common firmware updates are for optical drives. If you want to find out more about these updates, check your hardware manufacturer's website, and see this Firmware Database in particular for optical drives. A firmware upgrade can help resolve problems like difficulties reading from a particular disc type, 'disc not detected' errors, and other issues. Just like BIOS flashing it involves an element of risk, so please read any instructions carefully before proceeding.

The motherboard BIOS is a critical component of the PC which is often overlooked, so I urge you to take the time to become more familiar with your own BIOS, and to configure it correctly. Of course if you are not sure what a setting in the BIOS does, do not change it from its default. If necessary check your hardware manufacturer's website for more details, or do a thorough search on Google. It might be tedious at first, but it's typically a once-only job - once you've done it, you don't need to go back and customize the BIOS settings again, you can reap the benefits of an optimal BIOS from that point onward.

< HARDWARE MANAGEMENT

It is important to properly maintain your hardware, to ensure that it remains in good operation. The information in this section will help you understand how to keep your 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 component connections, or cleaning components, you should make sure to follow these tips to prevent any permanent damage to the components 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 your PC can kill or injure you, especially the dangerous voltages contained in your Power Supply. 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 or insert any metal objects into its casing.
- Once you've 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 computer 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. Typically if you leave your Power Supply Unit 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 also purchase an anti-static wrist strap if you handle components regularly. If you are going to handle components 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. An electrostatic discharge from your body can damage or kill an electronic component, so do not take this lightly as it can actually happen.
- Do not use a vacuum cleaner to clean the inside of your computer and its components, precisely because vacuum cleaner nozzles can discharge static electricity and zap your components. Use a clean barely damp lint-free cloth or barely damp q-tips to wipe dust from most surfaces, making sure you don't scrape the Printed Circuit Board (PCB). Don't use any detergents and most certainly don't spray anything onto the components. Ideally if it is available to you, use a can of compressed air (or an air compressor) 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 appear to be matched, the pin arrangements may be slightly different or out of alignment and hence forcing a fit may actually 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 just end up breaking the pins and 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 documentation and especially the motherboard manual to ensure that all components are plugged in correctly and firmly 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 for example mounting heavy fans onto them insecurely which can pass 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 dry out the component thoroughly, such as through the use of a hair dryer.
- Do not place excessive weight on a PCB as this can crack or warp it such that it will be permanently damaged. Don't even rest a large object temporarily on the motherboard or a component for example, put them on another surface until you need to use them.

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, so the tips above should be observed if you want to maintain your PC and your electronic components in good condition.

Thermal Compounds

Thermal compounds of various types 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 to ensuring optimal mating between the two surfaces, filling in any tiny surface imperfections. If they are not used, this usually results in severe overheating or hot spots on a component which can shorten its lifespan considerably and/or cause it to malfunction or shut down within moments. While 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 instructions which come with these compounds and apply either too much or too little. Follow the instructions exactly as given, as extensive testing has shown these 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 conductivity, or too much compound which actually prevents proper conductivity and builds up heat.

Also keep in mind during the application of any thermal or adhesive compounds of any type that most 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 compounds thoroughly with a cloth or appropriate cleaner. The best way to prevent such problems is to make sure you don't use excessive amounts and that you don't place any thermal compound too close to the edge of a component, as under pressure it will spill over the edges.

Surge Protectors

Make sure you invest in a good quality Surge Protector for your PC and all your other sensitive 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 any phone lines used for DSL for example.

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 customization or optimization can overcome the problems caused by a poor quality PSU, and it also jeopardizes your other components, potentially damaging them over time. A more efficient PSU can also save you money 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 which 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 should 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 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 for an Nvidia GeForce GTX 285). You should refer to the specifications of the PSU to see if the +12V rail(s) provide that much 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, and some even consider it undesirable. 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 huge difference whether you have single or multiple 12V rails.

The problem is that beyond trying to take note of the key factors above, an accurate review is required to tell you whether a PSU is genuinely good quality or not. As this article points out, specialized measurement instruments are necessary to determine this, not just measuring voltages with a multimeter. Hence most PSU reviews are inaccurate and effectively useless. Accurate PSU reviews can be found at sites like 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 or software; 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 due to the power it consumes, and this heat needs to be dissipated somewhere. A typical computer case usually traps heat, and 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 your Windows, you must make sure your system is 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 the core 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, otherwise known as the ambient temperature. Some other hardware components such as power supply units and hard drives may also come with temperature measurement devices you can access.

To actually see the temperature readings from your components, you can check the key readings in your BIOS settings screens, 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 already come with such software, so check your motherboard manual and driver disc, or the motherboard manufacturer's website for an appropriate monitoring utility. However for the most accurate and consistent temperature readings I recommend one of the following free utilities which work on almost any system:

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 hard 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, such as playing games. However 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 are designed to run hotter than others. However you can ascertain a reasonably normal temperature range for your component by searching Google 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 states 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 50-60C is normal when under maximum sustained load.

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 noticeably reduced performance. Use a utility like CPU-Z (See the System Specifications chapter) to monitor your CPU frequencies and 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 then there is a strong likelihood that it is overheating, especially if temperature monitoring also reveals a very high temperature under full load.

GPUs - An overheating GPU will result in graphical corruption and/or crashes, whether on the Windows Desktop or within graphically intensive applications like 3D 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 game and click the 'GPU temperature' line of GPU-Z, select 'Show Highest Reading' to see what the highest temperature was. A moderately high temperature combined with signs of graphical anomalies or corruption 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. Note that SSDs are not the same as HDDs and are less likely to suffer from heat-related issues because they have no moving parts.

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

Cooling Tips: If you are experiencing problems with heat in your system, 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, such as having them pressed against a wall, blocked by dust etc. 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 do have several case fans, 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 low 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 perhaps 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 the two hottest components in most cases. Secured cabling and snug plug connections also mean you can be sure nothing becomes accidentally unplugged or short-circuited over time 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 they are not too heavy for the surface they are mounted on. 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, once again damaging the motherboard PCB beyond repair. If you feel you require such hefty cooling you should instead consider buying a larger case that has better airflow properties.
- 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 a vital 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 the component requires minimal cooling, as sometimes manufacturers skimp on putting a fan on these components, which simply means the heatsinks have to do more work, so keep them well exposed to cool air. You may even consider positioning a fan near them if you wish to aid in 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 your components to their default settings to see if this removes or reduces the severity of the problem - see the Overclocking chapter for more details.

Thermal compounds are covered in more detail earlier in this chapter, however it should be noted that a common cause for component 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 better quality thermal compound for use on your components.

The most simple of all of these tips which anyone can undertake is to provide greater access to fresh cool air for the case's contents and regularly clean the case to remove dust buildup. Dust in particular can reduce airflow significantly, so keep your case and your components dust-free using a barely damp cloth, q-tip or compressed air. Furthermore, the next time you go to upgrade your PC, consider buying a larger case with plenty of ventilation as the single best investment in cooling and hence general system stability.

< DEVICE MANAGER

Once you have configured your BIOS optimally and 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 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, however this is covered in more detail under the Devices and Printers section in this chapter.

To access Device Manager, go to the Windows Control Panel, or go to Start>Search Box, type *device manager* and press Enter. The main Device Manager window lists all your detected hardware grouped by category, and you can expand particular categories to see individual devices. Double-click on any particular device to see more details on it.

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 Windows 7 and Windows Vista you could run hardware which didn't support ACPI, or even disable ACPI if you wanted to attempt manual resource allocation. However this is no longer possible as of Windows Vista - Vista and 7 require ACPI for hardware to function. That means that you cannot disable ACPI, and older hardware which is not properly ACPI-Compliant will not run on Windows 7. Only systems based on motherboards whose BIOS is ACPI Compliant and dated 1 January 1999 or newer can be used. If you're running older hardware this means you should update to the latest available BIOS for your motherboard and also ensure that any ACPI options are enabled for Windows to install and run without problems.

Windows 7 does not fundamentally change the way resources are handled compared to previous versions of Windows. Since Windows 7 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 a major issue. However one practical aspect of ACPI 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 usually 16 - 24 main hardware 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 and under the View menu select 'Resources by Type', then expand the 'Interrupt Request (IRQ)' item. You will see all 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*. While you may see IRQs numbered up to 190 or more, all of the IRQ numbers above 24 are for legacy Industry Standard Architecture (ISA) or non-Plug and Play devices, not for your main system hardware, so the key IRQs to examine are those numbered up to 24.

For an easier method of viewing IRQs and checking for potential IRQ conflicts, use the built-in System Information tool (see the System Specifications chapter). To access it go to Start>Search Box, type *system information* and press Enter. Expand the 'Hardware Resources' item in the left pane, and click the IRQs item to see the IRQs listed in order from 0 upwards. Click the 'Conflicts/Sharing' item to see a summary of sharing conflicts. Don't panic if you see conflicts, this doesn't mean your system is unstable or configured incorrectly. In many cases some hardware will be sharing a single IRQ or resource and there's not much you can do to prevent or alter this, it is normal behavior.

Window allows several devices to share an IRQ without any major issues, and in general this should be fine. However in cases where two or more high-performance components, such as your graphics card, sound card, or Ethernet controller are sharing a single IRQ, this may be a source of potential problems. High performance hardware is best placed on its own IRQ, but unfortunately 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. The only ways to prevent or minimize the impact of IRQ sharing are:

§ Disable unused devices - Covered in more detail further below, disabling unused devices in the BIOS and in Device Manager is a way of reducing unnecessary resource usage and speeding up boot time, and also preventing IRQ sharing-related problems. This is best done in the BIOS prior to installing Windows.

§ Move Conflicting Devices - On an existing installation of Windows 7 you can attempt to reduce IRQ sharing by moving a device. Physically move one of the items to another location on your system if possible, such as shifting 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 neither of the shared devices can be physically moved then you will have to accept the situation. Remember that Windows can share IRQs without major problems in most cases.

If after the above procedures you still have difficulties or reduced performance which you feel are attributable to IRQ sharing, the final option is to reformat and reinstall Windows 7, first making sure to correctly configure your BIOS and disable all unnecessary devices. Even then there is no guarantee that major devices won't wind up being shared again. Unlike previous versions of Windows, you cannot disable ACPI to force manual IRQ allocation, as Windows 7 must have ACPI enabled to work properly.

DEVICE POWER MANAGEMENT

Aside from the global Power Options available under the Windows Control Panel and 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, click on it and you will typically see two options, one or both of which are available:

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

Allow this device to wake up the computer: If selected, this allows the device to wake the computer up from Sleep mode if it is used. It should be only enabled if you want that to occur, otherwise untick it.

In most cases both boxes should be unticked if you want to minimize problems with a device, particularly USB devices.

PROBLEMATIC DEVICES

Devices with a question mark or exclamation mark next to them in Device Manager will need further troubleshooting to correctly identify and install, as by default Windows is unable to use the Plug and Play system to identify what these devices are. 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 for example. The key to Windows detecting the device properly is the installation of an appropriate driver - see the Windows Drivers chapter for full details.

The first thing you should try is using the new Hardware and Sound Troubleshooter function found under the Troubleshooting component of the Windows Control Panel - this is covered in more detail under the Troubleshooting section of the Performance Measurement & Troubleshooting chapter.

However if after following the advice in the Windows Drivers chapter and using the Troubleshooter you still can't get your device to work, you can use the 'Add Legacy Hardware' option of Device Manager, found under the Action menu, to manually add a device. Once this option is selected, a wizard will open, guiding you through the process.

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. If this option fails, you need to select the second 'Install the hardware that I manually select from a list option'. You will be taken to a list of hardware categories, and you should then select the category which you believe is the closest for your device, then click Next. A list of several Brands and Models of that particular device category will then be shown, and you can select the one which you believe is closest in functionality and compatibility to your device. If you find none of the options is appropriate, and you have another driver 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, it will be difficult to resolve the problematic device and hence use it with full functionality.

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 before installing Windows 7. However if this is not possible, it is still useful to disable devices in the BIOS on an existing installation of Windows - see the BIOS section earlier in this chapter.

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

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

Once these have been disabled in the BIOS, boot into Windows and make sure that all your normal functionality is unaffected. You can always re-enable any device in the BIOS at any time, so this is by no means a permanent disabling of particular devices. However you should only disable devices in the BIOS that you are certain will not be used during your normal Windows usage; disabling a necessary device 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 speed up bootup time noticeably because firstly your BIOS will not spend time trying to detect and enable these functions, and secondly, Windows won't load up drivers for these devices at startup. Once you've disabled a device in the BIOS 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, as covered below.

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 generally only recommended for more 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.

Furthermore, for each device that has ever been connected to your system, Device Manager will retain a range of entries in the Windows Registry relating to the device type, and the drivers and settings it used. That way if it is ever reconnected it can be quickly recognized again. However there are times when you have permanently discontinued the use of a device, or through a change in the BIOS, the device no longer uses those 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 all the categories and start looking through all the devices. Devices in gray are usually for old/unused/disconnected devices and safe to remove by right clicking on each one and selecting 'Uninstall'. However don't uninstall a device you know you will be reconnecting to Windows soon.
4. In particular, you might find several entries under the Monitors and Display Adapters 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 should remain. You may also find grayed entries for drive controllers you no longer use, and these should be safe to remove.
5. Do not remove any Microsoft devices such as those under the 'Sound, video and game controllers', or those under 'Storage volume shadow copies'. If in doubt, do not remove an item, gray or otherwise.
6. 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 to do so.

Use this method with caution. In many cases if you accidentally uninstall a hardware device which 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 - so this method doesn't permanently remove any device such that it prevents it from being detected or used again in the future usage. In some cases however, removing important devices may prevent Windows from booting up, which is where an appropriate restore point comes in handy to undo the damage.

< DEVICES AND PRINTERS

A new component in Windows 7, Devices and Printers is designed to consolidate a range of functionality related to device management and usage in one easy-to-use location. You can access Devices and Printers from under the Windows Control Panel, or by going to Start>Search Box, typing *Devices and Printers* and pressing Enter, or typically by attaching a relevant device. Aside from listing your PC and monitor, the types of devices which are likely to appear in Devices and Printers include any portable devices which you have connected to the PC, USB devices, wireless devices, printers and any detected network-based devices.

Unlike Device Manager, Devices and Printers is not designed to be a listing of all the hardware and devices on your PC, such as your CPU, hard drive or graphics card - it is primarily aimed at providing quick access through a 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 i.e. *[username]*-PC - and select 'Device Installation Settings'. This opens the settings, allowing you to choose whether you allow Windows to automatically download drivers and realistic icons for your devices. There are essentially two different functions to which this question relates. The first is whether you allow Windows to automatically detect, download and install what it considers optimal drivers for your hardware. The second is whether Windows downloads any custom icons and device information which the hardware manufacturer has provided to Microsoft. This does not affect the device's functionality at all, but it does make the device easier to identify in the Devices and Printers window, as its icon will change to an exact image of the device you have connected rather than a generic Windows device icon.

If you select the 'Yes, do this automatically' option, 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.

For more advanced users I recommend the second option 'No, always let me choose what to do' - this gives you ability to ensure that outdated or undesirable driver versions are not automatically installed over more recent or custom drivers you have installed yourself. Then I recommend selecting 'Install driver software from Windows Update if it is not found on my computer', as this means only devices for which you have not already installed a driver will be updated. Whether you tick the 'Replace generic device icons with enhanced icons' option is up to you; as noted it does not affect functionality as such, it simply replaces the generic icons with more realistic ones and can provide more information about the device, which is generally desirable.

Now connect your device(s) to the PC and allow Windows to detect them one by one. 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. If it still does not appear, see the Troubleshooting section of the Performance Measurement & Troubleshooting chapter.

Once a device appears in Devices and Printers, 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. Typically this involves Windows finding appropriate drivers, whether on your system or on Windows Update, or both, depending on your settings. You can then apply the fix and if successful the device will be installed properly and the exclamation mark will be removed. 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 Device Manager section further above as well as the Windows Drivers chapter.

Once a device is correctly installed, 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 Settings is to allow quicker access in one location. The most useful unique settings relate to printer functionality, because Devices and Printers replaces the old Printers folder which was 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 also 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 another location to place a shortcut there, such as on the Start Menu. This 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 providing relatively straightforward access to the major functions of a particular device with an easy-to-use graphical interface. If you connect a compatible device to your PC, Device Stage will automatically open, however you can also open Device Stage by double-clicking on a supported device in Devices and Printers. When opened, a large picture of your device along with its full name will appear at the top of the Device Stage window. At the bottom of the window are a range of options as relevant to your particular device. A new icon of the device will also appear in your Taskbar, and right-clicking on it will provide a range of custom tasks in the Jump List.

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 - see the AutoPlay section of the Drive Optimization chapter. Other devices may open a basic Device Stage window without much customization or specific branding. Fully supported devices open a Device Stage window with feature-rich content and device-specific pictures and Taskbar icon.

For the most part Device Stage is very convenient, and although most of its functionality is available through a range of other Windows settings and applications, the fact that it all exists in one location makes things much easier for both novice and advanced users. Minimized to your Taskbar, a particular Device Stage window is very handy for quick access. Note that when you disconnect a device, any Device Stage windows for it also automatically close, which means it doesn't unnecessarily add to Desktop clutter.

For advanced users who wish to edit the Device Stage package for a particular device for any reason, you can use the official Device Stage Visual Editor Tool.

This chapter has attempted to highlight the importance of making sure that your BIOS 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 tweaking will resolve odd problems in Windows if they are hardware-based, so if there are any areas of doubt or confusion relating to your hardware, I strongly suggest clarifying them with further research, perhaps even contacting your hardware manufacturer for more information, before moving on with Windows optimization or customization.

WINDOWS INSTALLATION

Windows 7 uses an image-based installation method which is covered in this Microsoft Article. Your Windows 7 installation DVD actually contains all the different consumer editions of Windows 7, however at the start of installation, a small configuration file on the disc identifies the specific edition you've purchased and 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 7 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. This installation method has a range of practical impacts which are discussed further below.

This chapter covers a series of important things you should consider prior to installation, as well as all the steps involved during the actual installation of Windows 7, and immediately afterwards. Even if you've already installed Windows 7, some of the information in this chapter is still applicable and worth reading.

< PRIOR TO INSTALLATION

Before we move onto the Windows installation process, we first look at the various preparations you should make and the issues you should consider prior to starting Windows 7 installation.

Check your Hardware and Software for Compatibility

Ideally before installing or even purchasing Windows 7, you should make sure that all your hardware components are compatible with Windows 7 and will run on it reasonably well. You should also check to see if your current software will run under Windows 7. Use the following resources to do both:

Windows 7 System Requirements - Lists the minimum hardware required to run Windows 7.
Windows 7 Upgrade Advisor - Scans your PC and connected devices and tells you if you will have any potential issues under Windows 7. It also tells you which Windows 7 edition you can upgrade to.
Windows 7 Compatibility Center - Lists all the software which is compatible with Windows 7. Note that there is a 32-bit and 64-bit list in each category.
Windows 7 Hardware Compatibility List - Lists all the hardware certified to be Windows 7 compatible. If your hardware is not on the list, that doesn't necessarily mean it's not Windows 7 compatible. Check your hardware manufacturer's website for Windows 7 support details.

Keep in mind that Windows 7 is using the same basic architecture as Vista, and is designed to be compatible with Windows Vista products, so if your system and software was able to run under Vista, it is highly likely to work with Windows 7.

Disable Unused Resources in the BIOS

As covered in the BIOS & Hardware Management chapter, it is important to turn off any options and devices in the BIOS which you will not be using prior to installing Windows 7. This will ensure that you speed up Windows startup, minimize any shared resources or potential conflicts in Windows, and prevent the installation of unnecessary drivers and services. Also see the Preparing the Drive section further below as some other BIOS options need to be changed prior to Windows installation for optimal performance. Don't ignore this step.

SCAN FOR MALWARE

If you are going to transfer any data or personal files from an existing installation of Windows to your new installation of Windows 7, 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 PC Security chapter of this book for full details. Importantly, if you plan to run the Windows 7 installation DVD from within your current install of Windows, make sure to completely disable any anti-malware program(s) after your scan, as they can interfere with the proper installation of Windows.

PREPARE BACKUPS

Once you're sure that your files are clear of any malware, the next step is to prepare complete backups of all your important information. This is covered under the Backup & Recovery chapter of this book. Regardless of which type of install you're 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 and you lose all the existing data on your drive. 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 the latest appropriate Windows 7 device drivers for all of your key hardware. Installing the correct drivers as soon as possible after installing Windows 7 ensures optimal stability, compatibility and performance, and can prevent major problems. You may even need certain drivers - especially SATA, RAID or other drive-related drivers - for correct detection of your drives during the Windows installation process. Prepare these in advance and store them on a CD, DVD, USB flash drive or external drive so that you can load them if necessary during the step where you choose the target drive for Windows installation. Check the Windows Drivers chapter for more details of where to obtain these drivers.

If you have any games installed, after backing up the relevant saved games and making note of any custom settings or saving any custom configuration files, uninstall your games in your current version of Windows before installing Windows 7. This is necessary for any games which are protected by online activation protection mechanisms. For such games, uninstalling the game, or in some cases using a special revoke tool, will ensure that you do not run out of valid activations when you next attempt to install or use the game. If you are unsure if your game is protected in this manner, I recommend uninstalling it anyway and then checking the game's documentation and website for more details of any additional procedures necessary in relation to its copy protection mechanism. This may also apply to certain general software protected by online activation technology.

CUSTOM OR UPGRADE INSTALL & DATA MIGRATION

An important decision you will have to make is how you want to install Windows 7. This decision primarily affects the way in which your existing user data, programs and settings are transferred to Windows 7. Depending on which version and edition of Windows you are currently using, there are two different methods for installing Windows 7:

Custom Install

This involves installing Windows 7 onto a new blank drive, or onto a drive with existing data, but not allowing Windows 7 to attempt to upgrade any previous version of Windows - a fresh new default copy of Windows 7 will be installed. This is called a Custom Install, also known as a Clean Install, and allows you to choose the partition of the drive to which Windows 7 will be installed. You can also choose to reformat the drive or repartition it in preparation for installing Windows 7, though note that if you repartition your drive in 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 further below for details.

A Custom install is the recommended method for ensuring that Windows 7 is installed as 'cleanly' as possible, devoid of any 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 7 is installed. See the Backup & Recovery chapter for appropriate backup and restoration strategies.

Note that if custom installing Windows 7 to a partition with an existing installation of a version of Windows without reformatting, files under your personal folders will automatically be saved to a *\Windows.old* directory on that partition. This is not recommended nor a substitute for taking a proper backup prior to commencing.

Upgrade Install

This involves allowing Windows 7 to install itself through an existing activated installation of Windows and selecting the Upgrade option, also known as an In-Place Upgrade. Windows 7 will attempt to keep all your files, settings and programs instead of simply replacing everything with a fresh new default Windows 7 installation. An in-place upgrade can only occur from qualifying versions and editions of Windows - details are provided in this Microsoft Article, and displayed graphically in this Microsoft Chart.

Essentially, you cannot choose to do an in-place upgrade to Windows 7 from:

§ Any versions of Windows prior to Windows Vista SP1.
§ A 32-bit version of Windows to 64-bit, and vice versa.
§ Different languages.

It is possible, but not recommended, to attempt an in-place upgrade from a pre-release version (e.g. Beta or RC) of Windows 7 if you modify the *cversion.ini* file as detailed in this Microsoft Article.

All editions of Windows Vista SP1 or SP2, excluding Enterprise, can in-place upgrade to Windows 7 Ultimate. However aside from this, Vista Home Basic and Home Premium users can only in-place upgrade to Windows 7 Home Premium; Windows Vista Business can only in-place upgrade to Windows 7 Professional or Enterprise; and Windows Vista Ultimate users can only in-place upgrade to Windows 7 Ultimate.

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

Upgrade Edition

An Upgrade Edition is a discounted version of Windows 7 which requires that a qualifying full version of Windows 2000, XP or Vista already be installed on your system. Importantly, an Upgrade Edition is not the same as an in-place upgrade; if you qualify to use an Upgrade Edition, you can always do a custom (clean) install, however whether you also qualify to undertake an in-place upgrade is another issue, as covered further above. Basically:

§ Full version Windows 2000 and Windows XP owners can purchase and use any Upgrade Edition of Windows 7. However no Windows 2000 or XP user can do an in-place upgrade; Windows will detect the presence of a legitimate Windows 2000 or XP install necessary to allow the use of an Upgrade Edition, but then only provide a Custom Install (i.e. Clean Install) option for Windows 7. There is no way around this, nor would it be recommended even if it were possible, due to the significant differences between the OS architectures.

§ Full version Windows Vista owners can purchase and use any Upgrade Edition of Windows 7, however you can only do an in-place upgrade to an equivalent or higher edition of Windows 7 as covered further above.

§ Any full version 32-bit Windows 2000, XP or Vista owner can use a 64-bit Windows 7 Upgrade Edition, but this precludes the ability to do an in-place upgrade from 32-bit to 64-bit Windows or vice versa; only a custom (clean) install is possible, again due to key underlying differences between the 32-bit and 64-bit architectures.

If you are in any doubt as to whether you qualify to use an upgrade edition of Windows 7, use the Windows 7 Upgrade Advisor covered earlier in this section to check. Also note that at any time after Windows 7 has been installed, you can use Windows Anytime Upgrade to purchase a new license and upgrade your current edition of Windows 7 to a higher version automatically - see this Microsoft Article for details.

If supported, an in-place upgrade should provide a reasonably good foundation for relatively novice Windows users moving to Windows 7 and not wanting to go through having to reinstall and reconfigure all their installed applications and risk losing user data. However this method is not advised for users who want to be sure they start with the cleanest and most optimal configuration for Windows 7 - only a Custom Install can do that.

Windows Easy Transfer

If you can't or don't want to do an in-place upgrade installation of Windows 7, but still want to migrate your user data and settings across in a relatively automated manner, use the Windows Easy Transfer utility. This allows you to transfer your user data and certain settings between previous versions of Windows (including pre-final versions of Windows 7) and Windows 7. To access Windows Easy Transfer in Windows 7, go to Start>Search Box, type *windows easy transfer* and press Enter. If you are not already using Windows 7, you can launch the Windows Easy Transfer utility under another version of Windows by inserting the Windows 7 DVD, exiting the Windows setup utility if it appears, opening Windows Explorer and going to the *\Support\Migwiz* directory of the DVD, and launching the *migsetup.exe* file there.

Once Windows Easy Transfer is launched, you will enter a migration wizard which will take you through all the steps required to carry out the migration. For full details of how best to handle the migration, see this Microsoft Article. To successfully migrate the data you will need a removable drive or USB flash drive, a special USB Easy Transfer Cable, or be connected to a network. Note that the Windows Easy Transfer utility has been improved over previous versions of Windows, such that you have a lot more options and thus greater flexibility in choosing precisely what to transfer to Windows 7. In general any type of user-based data can be transferred, but this does not include installed programs.

Unless you are a beginner, I recommend against doing an in-place upgrade install of Windows 7, or even using Windows Easy Transfer to migrate data and settings. While neither method is likely to cause you any serious problems, to ensure that you have a perfectly clean slate to begin with, I strongly recommend that you backup your data, reformat your drive and start with a full clean Custom Install of Windows 7, and then manually copy back only your personal data. Any programs or games which require configuration in Windows 7 can be done so with reference to the original configuration files you backed up, but not just by simply copying and pasting configuration or settings files into Windows 7. This may take a while longer to do, but it is most definitely worth the added effort in the long run as it provides the most trouble-free and performance-maximizing method of installing Windows 7.

MODIFYING THE WINDOWS INSTALLATION DISC

Windows 7's image-based installation system allows easier creation of a modified installation disc. All the tools you need to do this are in the Windows Automated Installation Kit (WAIK). Combined with these ImageX commands and the Deployment Image Servicing and Management (DISM) tool which allows you to add or remove drivers, updates and features, you can generate a new customized Windows 7 installation image for any edition.

However for the average user, there are simpler alternatives to using the tools above. There are three common scenarios for which a user may wish to legitimately alter or transfer their Windows 7 image, and some relatively straightforward methods of doing so:

Changing Product Editions: All consumer editions of Windows 7 - excluding Enterprise - are including on the single Windows 7 DVD. This means that even a Windows 7 Home Basic DVD has Windows 7 Ultimate on the same disc for example. This is the same as Windows Vista, however unlike Vista, the way in which Windows 7 determines the particular product edition to use during installation is not through the Product Key entered, but through the use of the data in a small *ei.cfg* file found under the *\Sources* directory of the Windows 7 DVD. This file can be opened with a text utility like Notepad, and the contents show which edition of Windows 7 the disc is designed to install. You can make a custom Windows 7 DVD for any edition of Windows 7, or indeed configure Windows so it prompts you to choose an edition from a menu during its installation.

This method requires that you either edit *ei.cfg* to change the text under the *[EditionID]* section to the desired edition, i.e. *Ultimate*, *Professional*, *HomePremium, HomeBasic* or *Starter* as required; or remove the *ei.cfg* file altogether to force Windows to present a choice of editions during install. To modify or remove *ei.cfg* and successfully create a working Windows 7 DVD containing this or any other change, you will need to use a tool which allows you to make a bootable .ISO image. This is important, because if the ISO is not bootable it won't work as a proper Windows 7 installation DVD. There are several methods for attempting this, whether you have a Windows 7 .ISO image, or only the Windows 7 DVD:

§ You can use UltraISO to edit or remove *ei.cfg* and subsequently create a new .ISO image. This is the simplest method, however UltraISO is not free.

§ If you already have a Windows 7 .ISO image, you can use the free Edition Switcher utility to alter or remove the *ei.cfg* file from the image without altering it in any other way, then burn the .ISO as normal.

§ Import the files from the Windows 7 DVD or .ISO image to a temporary directory, make the relevant changes to *ei.cfg*, then launch the free RT Se7en Lite utility (see further below) to create a bootable .ISO image from these files.

Note the following:

§ For the purposes of viewing or extracting contents from an .ISO file, you can use the free 7-Zip utility.

§ Once a bootable .ISO has been created, you can use the burn options in RT Se7en Lite to create the DVD, use the free ImgBurn utility to burn an .ISO to DVD, or use the Windows Disc Image Burner.

§ If you still can't successfully create a bootable .ISO for a working Windows 7 DVD, the alternative is to use a USB flash drive, as covered below.

Remember that altering the product edition does not mean you can activate that edition of Windows 7 unless you have a valid product key for that edition. The main use for this method would be if you have lost your Windows 7 DVD for example, and using another person's Windows 7 DVD you can create a new install DVD to suit your product version.

USB Drive Windows 7 Installation: If you wish to make a working Windows 7 installation disc - whether modified or unmodified - one of the simplest methods is to copy all the Windows 7 installation files to a USB flash drive and boot from there whenever you wish to install Windows 7. This is much more portable and typically much faster than installing from a DVD. First, I recommend making sure the USB 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 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 compatible for a USB device and hence is recommended, as some procedures (e.g. flashing a motherboard BIOS) require a FAT32 formatted USB flash drive to be correctly detected:

```
format fs=FAT32
```

6. Once the format procedure is complete, type the following and press Enter to 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. See the Boot Disks section of the Boot Configuration chapter for more details. If you just want to create a Windows 7 installation image, you can simply follow the steps below:

8. Copy the entire file contents of your Windows 7 DVD or .ISO across to a temporary folder on another drive, make any modifications if required, then copy all these files to the USB flash drive.
9. Set your BIOS to boot from a 'Removable Device', USB drive or similar, depending on the options you are presented in your BIOS. You may need to alter other BIOS settings in conjunction with this for your USB device to be bootable - check your motherboard documentation.
10. Connect the USB drive and reboot, and Windows 7 setup should automatically boot from the USB drive and begin as normal.

RT Se7en Lite: For any general alterations or customizations to your Windows 7 installation image, the easiest method is to use RT Se7en Lite. Similar to nLite and vLite before it, this is a free automated utility for creating a custom Windows 7 disc image for use in installation. It allows you to select the components you wish to remove from Windows, as well as things you might like to add, such as particular Windows Updates, the latest drivers and so on. Once you have integrated the relevant components and removed the components you don't need, the utility generates a bootable ISO file which you can burn onto CD or DVD and use as your Windows 7 installation disc.

Importantly, it has been demonstrated in the past that people who used these types of utilities or any other third party method to remove Windows components could not install new Service Packs for that OS properly. Therefore I strongly recommend against removing anything from the Windows 7 installation image simply because you think that it somehow 'speeds up' your PC or 'removes bloat'. Removing most components simply reduces disk space, it doesn't increase speed in the vast majority of cases. Don't fall into the trap of thinking that it is cool to strip out virtually every component of Windows and replace it with a third-party alternative - you are more likely to inadvertently cripple desired functionality in unforeseen ways or cause other problems for yourself down the track which only a reinstall of Windows 7 can fix.

For most users I recommend using RT Se7en Lite only to integrate useful components to the Windows 7 installation image, such as drivers and official updates, as this is a relatively safe process. Once Windows is installed, you can then safely remove or disable a range of Windows components using the 'Turn Windows features on or off' option under the Programs and Features component of Windows Control Panel - see the Programs and Features section of the Windows Control Panel chapter. Windows 7 has increased the number of integral components you can uninstall in this way, including Internet Explorer 8, Windows Search, Windows Media Player, Windows Media Center, etc. That way if you need to restore any component or turn any feature or resources back on at any time, you can simply re-enable them quickly and easily from within Windows, whereas removing something from the Windows 7 installation image can make it next to impossible to correctly fix certain issues without having to reinstall Windows 7 from scratch.

Finally, be aware that Windows 7's image-based installation system means that you are potentially exposed to malware if you use a downloaded Windows 7 installation image which 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, bypassing all Windows security features and rendering them useless.

< 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)format or (re)partition any of the drives, whether you want to use a RAID configuration, and whether you want to dual boot Windows 7 with an earlier version of Windows or another OS. It is also much better to partition and format drives 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.

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. In Windows 7 and Vista the format command has changed from that of XP, as detailed in this Microsoft Article. Formatting a drive in Windows 7 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 the 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 Windows 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 go to Start>Search Box, type *computer management* and press Enter. In the Computer Management window select the Disk Management item in the left pane. 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 7 DVD, begin the installation of Windows 7, 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 the drive before installing Windows - this will ensure that data is only written to error-free portions of the drive. However if the drive is not partitioned yet, you will not be able to do a format, so see the Partitioning section below.

File System

If you choose to format a drive, you may be presented with the option of choosing the File System to use. The common choice in Windows 7 is either the 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 7 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 Windows Explorer and Windows Search chapters for details. A range of functionality in Windows 7 will only work on drives with the NTFS format, such as Windows Backup.

Thus for your non-removable drives I strongly recommend choosing the NTFS format. This ensures full support for all of Windows 7's features and optimal performance and security. The only reason for using the FAT32 file system on a drive or partition would be for compatibility purposes if you wish to install another OS or a much older version of Windows, such as Windows 98, on that drive or partition.

Windows 7 also sees the introduction of full support for exFAT (Extended FAT File System), designed for flash drives and portable devices. However because it is a recent proprietary format, it does not have the same level of compatibility that NTFS and FAT have with previous versions of Windows, and this may cause problems if you wish to use your device on non-Windows 7 systems. For this reason I recommend formatting USB flash drives in FAT32, particularly as this ensures that you can use them for flashing the BIOS and transferring data between various systems.

If you want to convert an existing FAT32 drive or partition to NTFS, it is strongly recommended that you reformat the drive in NTFS for optimal performance. However if that is not possible, you can convert the 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.

PARTITIONING

Before formatting 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 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 most 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 7 on one partition, have your user files and folders on another partition, and use other partitions for storing other data or other operating systems. This way you can 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 still not certain of how many partitions you wish to use, it is useful to know that Windows 7 allows you to create, delete and resize partitions from within Windows at any time, so you are not locked into a particular partition configuration on your drive once you've formatted it and installed Windows. Therefore if in doubt, start with one partition and you can always change this within Windows 7 later on.

Creating Partitions

Before installing Windows, you must make sure your 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 the 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 100MB System Reserved Partition, necessary for the BitLocker Drive Encryption utility, and which also contains Recovery and boot data.

To prevent the creation of this extra partition, I recommend using the Diskpart command. Boot up your system with the Windows 7 DVD, then at the main Windows installation screen select your language and keyboard layout, then click Next. On the next screen click the 'Repair your computer' link at the bottom left. In the System Recovery Options menu, select the Command Prompt option. 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, 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:

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

The following command creates a primary partition of any size (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 this is not 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 as normal.

Altering Partitions Within Windows

You can repartition a drive on an existing installation of Windows 7 at any time using the built-in Computer Management features. To add or resize partitions in Windows 7 follow these instructions:

1. Open the Administrative Tools component of the Windows Control Panel and select Computer Management, or go to Start>Search Box, type *computer management* then press Enter.
2. In the Computer Management box, click the 'Disk Management' item in the left pane.
3. Select the drive for which you want to alter a partition from the list at the top of the screen.
4. If there is no unallocated space available, right-click on the drive and select 'Shrink Volume' - this will reduce the size of the existing partition, freeing up space for a new partition(s) to be made.
5. In the next dialog box enter the amount in MB you want to use for the new partition; 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.

You can now create a new partition in this freed up space. There are a range of other functions possible under Disk Management, but these are covered in more detail under 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 instead. It is not a Windows-specific tool, however it supports all Windows file systems and works with Windows 7. It won't be documented here as it is quite detailed in functionality, and recommended for more advanced users, however refer to these instructions if you wish to learn more.

Short Stroking

It is worth noting that there is a partitioning procedure which may improve performance on a hard drive (but not an SSD). It is referred to as Short Stroking, and essentially involves restricting the drive such that the head movements on the hard drive are kept 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 lower cost of large hard drives, and when combined in a RAID configuration (see below), you can still generate a reasonably large amount of storage using multiple short-stroked hard drives, albeit at a higher cost. Short stroking can also reduce the lifespan of the drive.

In any case, 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), which is automatically placed at the outer edge of the drive, and this 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. This is not a procedure I would recommend for most people - if you value performance over drive space, then consider purchasing an SSD instead as they will provide a range of benefits including much greater real-world performance gains than any short stroking ever could, as well as quieter operation and lower heat, at a cost that is rapidly declining.

In general I recommend having a single primary partition for Windows 7 and your data, as this keeps things simple and performance will be optimal. For proper data security 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 allows the use of a much more foolproof backup and recovery strategy. As noted, by default Windows 7 may automatically create an additional 100MB System Reserved Partition during installation of Windows primarily for BitLocker Drive Encryption, as well as for storing the Recovery Environment and boot files - for more details see later in this chapter as well as the Windows System Recovery Options section of the Backup & Recovery chapter.

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. The various RAID levels are best 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, 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 as normal and configure the appropriate RAID options in your motherboard's BIOS - 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 Windows and the motherboard. Once configured correctly, the RAID configuration of multiple drives will be seen as a single drive by Windows, and treated as such.

To determine which RAID configuration best suits your needs if any, you will need to read the articles linked above and consider your most common PC tasks. For the average user the most commonly used RAID array is a pair of similar 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 independent drives seeking data in place of 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 the data on both drives since the data is split evenly ('striped') across both drives. Therefore 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 (the smallest unit of data allocation) to be used in your RAID BIOS. In general, if you are uncertain of the size to choose, use the Auto setting if available, or a 64kb stripe. If you use the drives primarily for gaming I suggest a smaller stripe size such as 16kb, as this can assist in reducing stuttering in games.

In any case once you have connected your drives and set up your RAID array using the options in the motherboard's BIOS, you may need to have a disc or USB flash drive handy with the correct RAID drivers prior to starting the Windows 7 installation procedure. Then during Windows installation, on the 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 drivers, then click Refresh on the drive selection screen. If you miss this step, the RAID drives may not be correctly detected by Windows as one large drive, and you will not be able to install Windows on them properly, or you will break the RAID array and lose the benefits of RAID.

Once Windows 7 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, though remember that under certain RAID configurations such as RAID 0, a single faulty drive can see the loss of all your data on the RAID drives.

DUAL BOOT OR MULTIBOOTING

For those who want to consider installing Windows 7 alongside another operating system on the same machine, dual booting or multibooting allows this. A Boot Menu will 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.

Windows 7, while relatively new, already has excellent compatibility, particularly with software and drivers created for Vista, and also includes Windows XP Mode functionality for running older applications that only run correctly under Windows XP - see the Virtual Hard Disk section of the Drive Optimization chapter for details. As such, there is no real reason for the average user to dual boot Windows 7 with Windows XP or Vista.

The instructions for creating a dual boot/multiboot system in Windows 7 are in this Microsoft Article, and in more detail in this Multiboot Configuration article which applies equally to Windows 7 in conjunction with these added notes. To begin with you need to have at least two or more partitions on a drive (excluding the hidden System Reserved Partition) and/or have two or more drives. You should then boot up into your existing version of Windows and insert the Windows 7 DVD and run Windows setup from there. This ensures that Windows 7 will see your existing Windows installation and configure the boot menu properly to give you the choice of booting into either OS - see the Boot Configuration chapter. Importantly, for Windows to correctly identify all of your drives prior to installation, and correctly configure the dual boot, you may require appropriate SATA/RAID drivers on a disc or USB flash drive and insert them during the drive listing stage of Windows Setup.

I recommend having Windows 7 and any other OS on completely separate drives, as this causes the least number of problems, particularly if you want to remove an older version of Windows eventually. Performance is also improved if each OS resides on the first primary partition of different drives - except on SSDs where it makes no difference - so for optimal performance in Windows 7, do not install it on a secondary partition of any hard drive. Some important things to note about dual boot setups:

§ It is strongly recommended that you install the older version of Windows first (or it must already exist) before installing Windows 7. It is possible to install Windows 7 first and then install an older version of Windows afterwards, but this requires boot configuration editing - see the Boot Configuration chapter.

§ If your older version of Windows is the active partition on the first boot drive (the drive or partition which is first booted up by your BIOS), then it will be altered to include Windows 7's boot manager files. If you delete or damage these boot files, or you remove the older OS or reformat that partition, then you will need to boot from the Windows 7 DVD or access the System Recovery Options in another way and run Startup Repair to fix Windows 7's boot configuration, otherwise Windows will not bootup properly - see the Backup & Recovery and Boot Configuration chapters.

§ If you want to remove Windows 7 from a dual boot arrangement and return the boot record of your earlier version of Windows to its normal state, see the Boot Configuration chapter for details.

For more detailed instructions on how to manage dual booting with different versions of Windows as well as Linux, see this Dual Booting Guide.

< 32-BIT VS. 64-BIT

The final choice to make is whether you install Windows 7 32-bit (also called x86) or Windows 7 64-bit (also called x64). Every retail edition of Windows 7, except for Home Basic, comes with both 32-bit and 64-bit install DVDs, so this is a choice almost every Windows 7 user must make, and it is very important.

The first step is to understand the difference between 32-bit and 64-bit systems. 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 yet, there is no doubt that the move from 32-bit to 64-bit computing is inevitable, and adoption of 64-bit systems is growing at a rapid pace. For full details of 64-bit computing see this Wikipedia Article and also see this Microsoft Article.

Next you must determine if your PC hardware supports 64-bit processing. Windows 7 64-bit only runs on a 64-bit capable CPU. Fortunately all recent CPUs are 64-bit, but specifically all Intel Pentium D, Xeon, Core 2, Core i5, i7, i9 and Extreme Edition based CPUs or newer, and all AMD Turion, Opteron, Athlon64, X2 and Phenom or newer CPUs support 64-bit computing. 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. A quicker 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.

Thirdly, it is recommended that you 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. As such, for people with 4GB or more of RAM, you should almost always choose 64-bit Windows by default. 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.

Fourthly, keep in mind that 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 can't use the 64-bit Upgrade edition of Windows 7 if you currently have 32-bit Windows, it means you will have to do a custom (clean) install if you want to go from an existing Windows 32-bit to Windows 7 64-bit. Furthermore, even though you may have both a 32-bit and 64-bit Windows 7 DVD, you are only licensed to use one version of Windows 7 at a time - either 32-bit or 64-bit - not both separately on different drives/partitions or different systems. Your product key will work for either version.

Finally, consider the following points:

§ Windows 7 64-bit requires that all device drivers be designed specifically for 64-bit and that they be digitally signed. Windows 7 64-bit cannot use 32-bit drivers, and can only use unsigned drivers with a tedious workaround at each bootup (pressing F8 at each startup and selecting 'Disable Driver Signature Enforcement'). For most recent and popular 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 7 or Vista driver is available for all of your major hardware components - see the Windows Drivers chapter for more details.

§ Windows 7 64-bit does not support 16-bit programs, so if you use very old 16-bit programs this is worth noting.

§ Windows 7 64-bit can use almost 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 7 64-bit, or require specific customization, but this is rare and rapidly becoming a non-issue.

§ The 64-bit version of a program may provide improved performance under Windows 64-bit compared to its 32-bit counterpart.

§ Windows 7 64-bit has added security - see the PC Security chapter for details.

In general, it is recommended that anyone with a modern PC choose Windows 7 64-bit. Unless you have specific 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 fact if you have 4GB of RAM or more, there is no reason to use Windows 7 32-bit, since 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 and inevitable evolution of 32-bit computing, and must occur as programs become increasingly more complex and data-intensive, especially games. 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 7 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 will notice are:

- In Windows Explorer you will see both the *\Program Files* directory and a new *\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 7 will usually 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 Windows Explorer you will see a *\Windows\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.
- If you use the Windows Registry Editor, you will see an option to create `QWORD (64-bit)` keys. In practice it is not necessary to use this feature unless specifically instructed to.
- In the Windows Control Panel you will see that certain items have the (32-bit) suffix. This has no practical impact on the functionality of these items.

For all intents and purposes 64-bit Windows 7 looks and feels precisely the same as 32-bit Windows 7, 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. Only very old or low-end systems should use Windows 7 32-bit.

< INSTALLING WINDOWS

At this point you should have made the appropriate choices to be ready to begin the actual installation process for Windows 7. This section details the procedures required to install Windows, but it assumes you have read the rest of this chapter, as well as the BIOS & Hardware Management chapter. If you haven't done so yet, please put some time aside to research and make the necessary changes prior to installing Windows 7 - there's no point rushing the installation of Windows only to have to go through it again because you overlooked something or made the wrong choice.

The installation options are covered briefly in this Microsoft Article, and in more detail step by step below, noting the various options available and including any recommendations:

STEP 1 - LAUNCH THE INSTALLER

There are two main ways to commence Windows 7 installation depending on the type of install you want - an Upgrade Install or a Custom (Clean) Install. The differences between these two are discussed in detail earlier in this chapter. Depending on which you've chosen, follow the instructions below:

Upgrade Install or Dual Boot

An Upgrade Install or Dual Boot installation of Windows 7 requires that you first boot up into your existing version of Windows and then insert your Windows 7 DVD. This should automatically begin the Setup application, however if it doesn't, open Windows Explorer, go to the Windows 7 DVD and launch the *setup.exe* file on it. Setting up from within a valid existing version of Windows is necessary for Windows 7 to:

- Correctly identify your eligibility for using an Upgrade edition of Windows 7.
- Determine if you can perform an in-place upgrade from this version of Windows.
- Identify your existing version of Windows and set up the correct boot files for Windows 7 if you want to create a dual boot.

You can do a Custom (clean) Install of Windows 7 using an Upgrade edition, including the ability to reformat and repartition the drive if you wish. All you need to do is boot up and launch the Windows 7 installation process from within an existing qualifying install of Windows, and then select the Custom Install option to do a clean install.

However it is also possible to do a Custom (clean) Install of Windows 7 without booting up into another version of Windows first. This is particularly useful if you want to partition and format your drive outside of Windows Setup. The details are provided here and involves simply booting up from the Windows 7 Upgrade DVD and selecting the Custom (clean) Install option during installation. Once installed, you can try to Activate as normal. If this fails, you can then try the following method to Activate:

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 product key and activate normally via Windows Activation.

If this method doesn't work, insert the Windows 7 Upgrade DVD, launch Windows Setup from within this new install of Windows 7, reinstall Windows 7 by choosing the Upgrade option this time during installation, and once reinstalled, Activate Windows 7 as normal. This is effectively the same as a clean install.

Bear in mind that these workaround methods for installing an Upgrade edition on a blank or newly partitioned and/or formatted drive are only legal if you actually own a qualifying valid full previous version of Windows, though at no point does Windows 7 check to confirm this.

Custom Install

A Custom or Clean Install of Windows 7 will erase any data on the target drive/partition - it will not transfer any existing files or settings on that drive. Make sure you have backed up any data on the drive which you wish to keep. To start a Custom Install, go into your BIOS and set your optical drive as the first boot device, and make sure all your drives are correctly connected, configured and detected in the BIOS. Then insert your Windows 7 DVD and reboot your system, pressing any key when prompted on the screen to boot up via the DVD drive.

STEP 2 - INSTALL NOW

On the first Windows 7 Installation screen, if you booted from the Windows 7 DVD you will be asked to select your Language, Time & Currency Format and Keyboard method. Set these correctly and click Next.

Once you've done this, or if you started Windows 7 installation from within an existing version of Windows, the screen you will now see should have a large 'Install Now' button. Click this if you want to start installation of Windows 7.

Repair your Computer: This functionality is covered under the Backup & Recovery chapter and is only necessary if you are troubleshooting a problem.

If launching Windows 7 installation from within an existing version of Windows, you will also see the following option:

Check Compatibility Online: If you aren't certain of your hardware compatibility with Windows 7 then click the 'Check compatibility online' button and you will be taken through the Windows 7 Upgrade Advisor, which is covered earlier in this chapter.

STEP 3 - GET IMPORTANT UPDATES FOR INSTALLATION

You will be prompted to check for important updates prior to installation. These include security updates and any necessary driver updates. If you can connect to the Internet, it is recommended that you do so and select the first option to get the latest updates now, as it will make Windows 7 installation much simpler and more secure. However if you don't have an Internet connection or wish to skip this step, it is not critical and can be done later via Windows Update.

At the next screen you will see the End User License Agreement (EULA) - read this and tick the 'I accept license terms' box if you wish to continue installing Windows 7, then click Next. To download a full copy of this license and read it at your leisure, and to understand the key practical aspects of the license see the Windows Activation chapter. You may wish to read that chapter now before you agree to the license.

STEP 4 - SELECT UPGRADE OR CUSTOM (ADVANCED) INSTALL

At this point, you will get the choice to do an Upgrade install or a Custom (Advanced) install which translates to a clean installation. The Upgrade installation option should only be chosen if you want to do an in-place upgrade install; it has nothing to do with whether you are using an Upgrade Edition of Windows 7 or not. Otherwise select the Custom (Advanced) install option to begin a clean installation.

If the Upgrade install option is available and you choose it, your system will be scanned and you will be presented with a Compatibility Report indicating which of your currently installed programs and drivers may be problematic under Windows 7, as well as any other issues which need to be resolved before you can successfully continue with Windows 7 installation. You can stop installation at this point without any problems or changes to your existing Windows install if you feel there are too many issues identified. If you choose to proceed with the Upgrade installation, skip to Step 6 below, since by necessity the target drive/partition is automatically the one on which your current install of Windows is sitting.

Again, I recommend against an Upgrade install unless you are a relatively new Windows user, or you are absolutely certain that you do not have the time to reinstall and reconfigure Windows 7 from scratch.

STEP 5 - WHERE DO YOU WANT TO INSTALL WINDOWS

This screen allows you to choose the logical drive where Windows 7 will be installed. You should see a list of all the detected drive(s) currently connected to your system. They are 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 Bytes and Bits section of the Basic PC Terminology chapter for more details.

Load Drivers: 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 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 to see if the drives are detected and configured correctly there. The bottom line is that if Windows 7 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: If you booted up with the Windows 7 DVD to do a Custom install, you will also see these additional options here; if you started the setup from within Windows you will not see these options. Format allows you to (re)format the selected drive. This is recommended for any drive with existing data. A full format using the NTFS file system is recommended for ensuring optimal compatibility, performance and data integrity. 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 the partitions on an existing drive and repartition it within Windows setup, Windows will inform you that 'To ensure that all Windows features work correctly, Windows might create additional partitions for system files'. This prompt indicates the automatic creation of an additional 100MB System Reserved Partition, a hidden partition with no drive letter, created specifically for the BitLocker Drive Encryption feature to hold unencrypted boot files and also stores the System Recovery Options. 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 before launching Windows Setup. Windows 7 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 in Windows 7 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 7 and click the Next button. The existing contents of the target logical drive will be lost as Windows 7 installs over it, however if installing Windows 7 over an existing installation of Windows without first formatting that partition, Windows 7 will attempt to save user-related files and move them into a *\Windows.old* directory once Windows 7 is installed. 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 7 to prevent residue from previous Windows installs.

STEP 6 - AUTOMATED INSTALLATION

From this point on, no user interaction is required for some time as Windows 7 begins to copy across the compressed image of itself to the target drive, expands it and configures the required features and updates. Your PC will then restart several times to complete installation.

STEP 7 - SET UP WINDOWS

Windows 7 will then commence the final phase of the installation which requires your input. Note that at this point you can remove the Windows 7 DVD from your drive and put it away if you wish, as installation is now occurring from your primary system drive. Also remember to reset your primary system drive as the first boot device in your BIOS when your system next reboots.

Windows 7 will run through some additional configuration and performance checks, before arriving at the user input stage, each section of which is covered below:

Username & Computer Name: This is an important step. You will be asked to enter your preferred Username for the first User Account on this system. This first account will have Administrator-level privileges, and is called the Protected Administrator account. The User Account username will also be used to label the root directory of your personal folders under the *\Users* directory, so choose something relatively simple but descriptive, like your first name. Once you've entered a username, Windows 7 will automatically generate a Computer Name for the system - this is really only used to identify this particular machine in a network of computers. For most home users who don't connect to a network of other PCs, the Windows 7 default of *[Username]-PC* is perfectly fine, otherwise if you want to run this PC on a network then choose a descriptive name. Click Next when done.

Password: Here you will be prompted to enter a password for the User Account whose username you entered in the previous screen. If you share this PC with others, particularly if you want to have multiple User Accounts on the one PC, or if the PC is physically accessible by others you don't fully trust, or you simply want a very high level of security, then enter an appropriate password. If these scenarios do not apply to you, then for convenience's sake I recommend not entering a password - leave the Password fields blank and click Next. You can always add a password to your User Account later if you wish.

See the User Accounts chapter as well as the User Account Control section of the PC Security chapter for full details of how User Accounts work in Windows 7.

Product Key: You will be prompted to enter your Windows Product Key in the format XXXXX-XXXXX-XXXXX-XXXXX-XXXXX. Dashes are entered automatically, and case is not important. Importantly, you don't have to enter your product key if you don't wish; you can click Next to continue Windows installation without it. As noted earlier in this chapter, unlike Windows Vista, the product key is not what Windows 7 uses to identify which edition of Windows to install - that is determined by the configuration data already held on your Windows 7 installation DVD. However it is strongly recommended that you enter your product key now, because it is best to determine at this point if your product key is valid for your current edition of Windows. For example, if you skip entering the key now and at a later date within Windows you enter a perfectly valid product key but one which is incorrect for your installed edition of Windows (e.g. if you used someone else's Windows 7 DVD) then Windows will not accept the key and will not be able to activate, necessitating a reinstall of Windows 7 using the correct DVD. Microsoft does not encourage or support the 'trial' use of Windows 7 by skipping entry of the product key.

Also note that the 'Automatically activate Windows when I'm online' box, if ticked, will begin Activation shortly after you have loaded up Windows 7 for the first time and an active Internet connection is detected. I recommend unticking this option for the moment and manually activating when you are ready. See the end of this chapter for the reasons, and refer to the Windows Activation chapter for more details.

Help Protect Your Computer and Improve Windows Automatically: You will be asked how you wish to configure Windows 7's security and online update settings. Specifically, these settings relate to the following features:

- Windows Update - Automatic downloading and installation of Windows security updates and driver updates. See the Driver Installation section of the Windows Drivers chapter for details.
- Detailed Device Information - Downloads detailed information for any devices you have connected. See the Devices and Printers section of the BIOS & Hardware Management chapter for details.
- Windows Defender - Enables full Defender anti-malware functionality. See the Windows Defender section of the PC Security chapter for details.
- Windows Problem Reporting - Allows Windows to report any problems to Microsoft for better identification of potential solutions. See the Windows Action Center section of the Performance Measurement & Troubleshooting chapter for details.
- Windows Customer Experience Improvement Program - This program collects information which is not personally identifiable about your hardware and the way in which you use Windows. It sends this information to Microsoft to allow improvement of Windows functionality as detailed in this Microsoft Article. You can alter this setting at any time in Action Center - go to Start>Search Box, type *Action Center*, press Enter and in the left pane click the 'Change Action Center settings' link, then click the 'Customer Experience Improvement Program settings' link at the bottom of the box which opens.
- Windows Online Help & Support - Allows the Windows Help feature to download newer content for Help & Support functionality. You can alter this setting at any time by opening Help & Support - press F1 while on the Windows Desktop, or go to Start>Search Box, type *Help and Support* and press Enter. In the Help and Support box, click the Options button at the top left and select Settings, then tick or untick the 'Improve my search results by using online Help' box.
- Windows Help Experience Improvement Program - This program collects any words or phrases you enter into the Help and Support feature and sends it to Microsoft to allow MS to improve the Help functionality. You can alter this setting at any time by opening Help & Support - press F1 while on the Windows Desktop, or go to Start>Search Box, type *Help and Support* and press Enter. In the Help and Support box, click the Options button at the top left and select Settings, then tick or untick the 'Join the Help Experience Improvement program' box.

If you select 'Use recommended settings', all of the above features will automatically be enabled. If you select 'Install important updates only' then only the Windows Update-related settings will be enabled. If you select 'Ask me later' then none of these features will enabled unless you choose to alter them manually in Windows. If you have privacy concerns see this Microsoft Article. I recommend the 'Ask me later' option, as we will be modifying all of the relevant options above later in the book anyway.

Review Your Time and Date Settings: Set your correct time zone, time and date, and also I recommend ticking the 'Automatically adjust clock for Daylight Saving Time' box.

Select Your Computer's Current Location: This screen asks you to set your location for networking/Internet connectivity purposes. The options are Home network, Work network or Public network. Ironically, for the average standalone home PC connected to the Internet the best choice is actually 'Public Location' not Home, as this allows you to connect to the Internet with full functionality but maintains tighter security. The other options are only relevant if you are actually connected to a network of other computers (excluding the Internet), such a collection of networked PCs in your home, or when connected to your employer's network. See the Network & Sharing Center section of the Windows Control Panel chapter for more details.

STEP 8 - WINDOWS STARTUP

Windows 7 then launches into its final setup phase, which may take a while - you will see the prompt 'Preparing your desktop' and you will eventually reach the Windows 7 Desktop. From this point onward Windows installation is complete and you can begin using Windows 7 as normal, continuing with the rest of this book.

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

- Make sure to remove the Windows 7 DVD and/or any removable devices if you haven't already before rebooting Windows.
- Make sure to go into your BIOS 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.
- Limit any general Internet browsing or other online activities until after you've completed the PC Security chapter.
- Don't Activate your Windows straight away if possible. If you plan on making any major physical changes to the hardware configuration of your PC, if you will be experimenting heavily, or if you simply aren't sure if your system is functioning properly and/or you are planning on reinstalling Windows again within the next 30 days then wait until you've bedded down your configuration before activating. This is because multiple activations within a short period of time may be viewed as suspicious by Microsoft. See the Windows Activation chapter for details.

At this point, you can continue reading this book sequentially, or you can skip to any chapter which takes your fancy. I recommend reading the Windows Explorer, Windows Drivers, PC Security and Graphics & Sound chapters as soon as possible to cover the key functionality, stability and security-related topics.

BOOT CONFIGURATION

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

For the most part, editing boot configuration is for more advanced users. You should not need to edit or alter the Windows 7 boot configuration unless you're troubleshooting a more complicated bootup-related problem, attempting to use 4GB or more of system RAM on 32-bit Windows, or modifying or repairing a multiboot setup. For basic boot-related problems, the automated Startup Repair utility in the System Recovery Options is recommended, as covered under the Windows System Recovery Options section of the Backup & Recovery chapter.

< BOOT FILES

The Windows 7 boot configuration is held in a hidden *\Boot* folder, along with the *bootmgr* and *BOOTSECT.BAK* files, all required for starting up Windows. If your drive has a small 100MB System Reserved Partition which was created when installing Windows 7, then these files will be located there. This 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 must be stored as unencrypted files on a separate partition. This partition is hidden by default and is not assigned a drive letter, however you can prevent its creation - see the Installing Windows section of the Windows Installation chapter for more details.

You can view the presence or otherwise of this 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 100MB System Reserved partition with no drive letter.

If you don't use BitLocker, and have successfully prevented this 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 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, and will then require you to use the Startup Repair method to fix your boot configuration.

< BOOT CONFIGURATION DATA

There are several ways you can view and modify your Windows 7 boot configuration data, and each is covered in more detail below.

BCDEDIT

BCDEdit is a built-in command line tool for altering the boot configuration in Windows 7. To use it, open an Administrator Command Prompt and type `bcdedit /?` for a full list of commands, or refer to this Microsoft Article for a command list. One example of using BCDEdit is provided below, as it also assists in fixing common boot problems.

If you find that your Windows 7 boot screen has changed to a Windows Vista boot animation, this is due to a problem with the boot loader, and can be fixed using a simple BCDEdit command as follows:

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

```
bcdedit /set {current} locale en-US
```

3. Note that if your locale is different from English US, then enter it in place of `en-US` above.

Given it is a complex tool to use, BCDEdit cannot be covered in detail here. I strongly suggest using the EasyBCD tool below to edit your boot configuration instead, at least to start with, and only turn to BCDEdit if you have no other options, and only after appropriate research, as it is risky to 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, click the 'Advanced system settings' link, or go to Start>Search Box, type *systempropertiesadvanced* and press Enter. Then 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 with a list of all installed Operating Systems, 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 7), then this boot menu has no impact, so untick the box.

The 'Time to display recovery options when needed' box should 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 Backup & Recovery chapter.

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

MSConfig

A relatively straightforward way to alter the boot configuration is to use the Microsoft System Configuration utility (MSConfig). Go to Start>Search Box, type *msconfig* then 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 install of Windows 7 you wish to alter, then you can select one of these options to apply to it:

Safe Boot: If selected, the next boot will be into Safe Mode, as detailed under the System Recovery section of the Backup & Recovery chapter. Default Safe Mode is called Minimal; 'Alternate Shell' is Safe Mode with Command Prompt instead of GUI; 'Active Directory repair' is Safe Mode with GUI and Active Directory; Network is Safe Mode with GUI and Networking features enabled.

No GUI boot: Removes the default Windows 7 animated Windows logo startup screen when booting up, replaces it with a black screen until you reach the Windows welcome screen. See further below for more details of customizing the Windows boot and login screens.

Boot log: Records all 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 n*tbtlog.txt*.

Base video: Boots up Windows using the default Windows graphics driver rather than the specific graphics driver for your graphics hardware. Useful if a recent graphics driver installation is preventing you from booting up.

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

The Timeout value in the box on the right is the same as the 'Time to display a list of operating systems' setting covered under 'Startup and Recovery' further above - it controls how long the boot menu for operating system selection is shown and hence is irrelevant if you only have one operating system installed.

If you click the 'Advanced Options' button you will see more advanced bootup options for troubleshooting:

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 be detected and used by Windows during bootup. However, this is not a performance option, it is only related to troubleshooting by artificially limiting the number of cores on your CPU being used to determine if there is a fault with one of them. The default setting of having this box unticked is optimal and results in the best bootup time.

Maximum Memory: 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. Amount entered is in Kilobytes (KB).

PCI Lock: 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: Starts Windows in debugging mode. Ticking this option ungrays a range of additional options as to where to write the debug output. Again, of no practical use to most users.

Once done selecting which bootup options you wish to apply to the boot configuration, click the Apply button in the MSConfig Boot tab and these option(s) will come into effect on next boot. Should you wish to apply any permanently, you can tick the 'Make all boot settings permanent' box. If you wish to undo these changes at any time, the quickest way is to go to the General tab under MSConfig and select the 'Normal startup' option.

Use MSConfig only to test a boot option, or for troubleshooting purposes. Use BCDEdit below to make any desired changes to the boot configuration permanent.

EASYBCD

EasyBCD is a tool you can use to make changes to your boot configuration in a much more user-friendly manner. The most recent version of EasyBCD is not free, so I recommend and cover an older version here (2.0.2) which is much lighter and is available for free via a link at the bottom right of the official EasyBCD download page. There is another popular BCD editing utility called DualBootPro, however it is not free.

Before altering anything in EasyBCD, first backup your existing Bootloader settings so they can be easily restored if required. Click the 'BCD Backup/Repair' button and then click the 'Backup Settings' button to create the backup .BCD file. If your system is currently problem-free then I also strongly recommend also creating a full general backup of your system, as detailed in the Backup & Recovery chapter, before continuing with the use of EasyBCD or any other BCD editing utility.

EasyBCD has a range of functions, but we'll cover only the major ones here. On the main 'View Settings' screen you can see a summary of the data held in the BCD. You can view this in simple (Overview) mode, or if you prefer the raw data, select the Detailed option. The information here is useful for troubleshooting, and also gives you an idea of the kind of data held in the BCD.

If you want to alter these entries, click the 'Edit Boot Menu' button. Here you can set the Default OS and the timeout, though these are best altered using the normal Windows Startup and Recovery options as covered earlier in this chapter. Of use for multiboot systems, you can rename the OS entries which show up in the Boot Menu. To help prevent confusion and make things neater, click on each OS listed and tick the 'Rename selected operating system' checkbox - new options will appear allowing you to provide a new name and also change the drive letter if necessary. When done, click the 'Save Settings' button to save your changes.

The 'Add New Entry' button takes you to a screen where you can add or remove other operating systems as part of a multiboot system. You can even boot up into newly supported Windows 7 Virtual Hard Disk (VHD) images here, specified under the Virtual Disk tab. The listing also allows you to rearrange the order in which the OS entries are presented if you wish.

The 'Advanced Settings' include various advanced features which the MSConfig utility and other Windows utilities can accomplish. Most of these features are described elsewhere in this book and in general should be altered using the relevant Windows settings. The specific features which you can use EasyBCD to more easily alter are under the Advanced tab:

PAE Support: This option provides control over Physical Address Extension (PAE) in Windows. This is only necessary for correct memory detection and usage if you have 4GB or more of RAM in the 32-bit version of Windows 7, in which case you can select 'Force Enable' here. Note that this 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 of the difference between the two architectures.

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

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

Under the 'Bootloader Setup' 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 relevant option and click 'Write MBR' to complete the change. In the first instance however you should attempt repair of the boot files by going to the 'BCD Backup/Repair' section of EasyBCD and selecting 'Re-create/repair boot files' then clicking the 'Perform Action' button.

EasyBCD is a very useful tool for easy BCD editing as the name suggests, however 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 to restore the Bootloader backup from within EasyBCD, or alternatively use the Startup Repair functionality of Windows to fix the problem.

< CUSTOM BOOT AND LOGIN SCREENS

This Microsoft Article explains that unlike previous versions of Windows, Windows 7 does not allow customization of the boot screen. This is a deliberate design 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 which purports to provide this functionality, as it may cause problems and/or increase boot time at best, or is malicious at worst. At present there are no such utilities which can successfully alter the boot screen in Windows 7.

Note that if you find your boot screen has reverted back to the Vista boot logo, this is due to damage to the Bootloader - see the Boot Configuration Data section further above for a fix.

If you simply want to replace the default Windows 7 animated boot screen with a blank boot screen, you can do so using the No GUI Boot option, available under the Boot tab of the MSConfig utility, covered further above.

Customizing the Windows Login Screen - which only appears by default if you have more than one User Account, or if your User Account has a password - is much easier to do. Logon Changer is a free tool which allows you to change the background image on the Login screen. It can use any image you wish for the Login screen background, automatically resizing and compressing the image to meet the 245KB limit imposed by Windows.

< BOOTDISKS

The original Windows 7 DVD is effectively a boot disc, however you can now also create a System Repair Disc for the same purpose if you don't have an original Windows 7 DVD, or simply as a backup. If you're having problems booting up into Windows, you can then boot up using one of these discs, then use Startup Repair to automatically detect and repair any issue preventing proper Windows startup. Details of these functions are covered in 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 7 System Recovery Options 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 DOS environment, which some programs require for correct functionality.

Therefore if you wish to boot into DOS to flash a hardware component for example, you must use the instructions and tools provided at BootDisks, or use the Ultimate Boot CD utility to create a bootable floppy or CD. 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 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 Windows tools first, particularly the automated Startup Repair, before delving into more complex boot editing.

WINDOWS ACTIVATION

To confirm that you are running a legitimately purchased copy of Windows 7 in accordance with the terms of the End User License Agreement (EULA), Microsoft relies on Windows Product Activation, better known as simply Activation, which verifies your Product Key and hardware configuration online or over the phone. This is combined with Validation, a process whereby your Windows is periodically checked to ensure it is genuine. While activation and validation have been used since Windows XP, these measures have been tightened and improved in recent years. In Windows 7, Microsoft builds on the Microsoft Software Protection Platform first built into Windows Vista. Collectively, product activation and validation are now referred to as Windows Activation Technologies (WAT) in Windows 7, and are very similar to the protection methods employed as of Windows Vista Service Pack 1 (SP1).

This chapter looks at the practical aspects of how your license to use Windows works, along with examining the way in which activation and validation operate in Windows 7.

< LICENSING AGREEMENT

The End User License Agreement (EULA) for Windows 7 contains the terms and conditions of acceptable usage. This section attempts to provide the most important practical considerations which arise from the standard user license in plain English. Importantly, what follow are my interpretations of the license terms based on research, but for legal reasons this should not be considered a replacement for actually reading the license yourself, as your license terms and conditions may differ for a range of reasons.

The reason you require a license for Windows 7 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 explicitly agree during the installation of Windows. The key points are explained below.

OEM VS. UPGRADE VS. RETAIL EDITIONS

While their contents do not differ, there are some notable differences between the license conditions for OEM (Original Equipment Manufacturer) or 'System Builder' editions of Windows 7, versus the Upgrade and Retail editions:

OEM: An OEM edition of Windows 7 usually comes pre-installed on, or accompanying, a new PC or the purchase of one or more major hardware components. 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 reinstall the OEM copy on a different PC, you may fail activation since you have technically breached the licensing conditions. There are other limitations applying to OEM versions, including limited or no technical support from Microsoft. This is why OEM copies are the cheapest editions to purchase. OEM versions can only be used to do a Custom (clean) install.

Upgrade: An Upgrade Edition of Windows 7 requires that you already own a full Retail or OEM edition of a qualifying previous version of Windows. In the case of Windows 7 this means you must own and have installed a full Retail or OEM edition of Windows 2000, XP or Vista. When using an Upgrade Edition of Windows 7, you must first boot up your existing qualifying previous version of Windows, then you can choose to do either a Custom (clean) install, or an In-Place Upgrade only from Windows Vista SP1 or newer, to an equivalent or higher version of Windows 7. There is a workaround to this method covered in the Installing Windows section of the Windows Installation chapter, allowing you to install an Upgrade Edition on a brand new or freshly formatted drive, however this method is not supported by Microsoft, and is not considered legal if you do not own a full Retail or OEM edition of a qualifying previous version of Windows. In terms of upgrading your PC hardware or transferring Windows 7 to a new PC, there are no specific limitations on the number of times you can do this.

Retail: The full Retail Edition does not require the ownership or installation of any other version of Windows, and can be installed on any PC. You can choose to do either a Custom (clean) install, or an In-Place Upgrade only from Windows Vista SP1 or newer, to an equivalent or higher version of Windows 7. The Retail Edition allows unlimited upgrades or moves to another PC. It is the most flexible edition, which is why it is also the most expensive edition.

For details of eligibility for in-place upgrades, and related upgrade information, see the Prior to Installation section of the Windows Installation chapter.

General Conditions of Use

Aside from the specific licensing conditions covered above, all editions of Windows 7 must also adhere to some general conditions of use. These are spelled out below:

§ The OS is licensed to one specific device at any time, namely the PC on which it is currently installed. You can't install the same copy of Windows 7 on multiple PCs unless you have specifically purchased multiple licenses - one for each PC.

§ If the edition includes both the 32-bit and 64-bit versions of Windows 7, 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 7.

§ If you install an Upgrade Edition of Windows 7, you lose the license for the previous full version of Windows. For example, if you use an Upgrade Edition to install Windows 7 from your Retail Edition of Windows XP, you lose your XP license.

§ Except for the OEM version, you can upgrade or alter the hardware in the PC on which Windows 7 is installed as often as you wish.

§ Except for the OEM version, you can transfer Windows 7 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.

§ The OEM version can only be transferred with the original computer on which it is installed.

§ You must Activate your copy of Windows within 30 days of installation, and you must allow it to periodically connect to the Internet to validate - see further below for full details. Some OEM versions of Windows 7 come pre-installed and already activated, so manual activation is not required.

§ You are permitted to make one backup copy of the Windows 7 DVD, or transfer one copy to disc or other media if you purchased the software 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 the licensing terms and conditions as applicable to you in your country, and based on your particular circumstances. For example, if you have purchased a PC with Windows 7 pre-installed from a certain hardware manufacturer, your OEM copy of Windows 7 may have different or additional terms and conditions than those specified here or elsewhere.

< ACTIVATION

This section goes through the procedure for Windows Product Activation, simply referred to as activation, and any associated issues.

PRODUCT KEY

When you first install Windows 7, 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-XXXXXX. This key can be found on a sticker on your computer if you purchased the PC with Windows 7 pre-installed, on the installation disc holder of your Windows 7 package, or on the Windows 7 manual. The product key is very important because it is integral to validating and activating your copy of Windows 7. 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, do not share it with anyone else and if your PC or copy of Windows 7 did not come with a product key then contact your retailer or the person from whom you purchased the Windows 7 DVD or PC and ask them to give you one as it is absolutely necessary - unless you are in a corporate or business environment.

In Windows 7 you can legitimately skip the entry of the product key when prompted during Windows installation. However unlike Vista this does not allow you to choose the edition of Windows 7 you wish to use, as by default the specific edition which is installed is embedded in the particular Windows 7 DVD you use. It is recommended that you enter your product key during installation to confirm that it is correct, rather than finding out after installation that it does not match the product version you installed and hence can't be activated. Details on customizing your Windows 7 installation DVD to another edition are provided in the Prior to Installation section of the Windows Installation chapter.

If you have lost your original product key and wish to extract it from your current installation of Windows, you can use the free Magical Jelly Bean Keyfinder or ProduKey utilities. Note that some anti-malware programs flag them as suspicious, but they are perfectly safe to use. However if in doubt, the safest way to obtain your product key is to contact your hardware vendor or Microsoft. If you wish to alter your product key from within Windows 7, you can do so at any time by going to the System component of the Windows Control Pane and clicking the 'Change product key' link. Entering a new key will require you to reactivate. If you want to look at options for purchasing additional Product Key(s) online from Microsoft see here.

ACTIVATION PROCESS

Activation is designed to join your product key to your specific hardware specifications, checking to make 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 home license. Once you have installed Windows 7, you will have exactly 30 days within which to activate Windows. During this time you can use Windows 7 as normal, but you will be prompted on a daily basis to activate, culminating in prompts every four hours in the final 3 days before the deadline for activation, and every hour on the day of the deadline. To see how many days you have left before your activation grace period runs out, either click the prompt which appears in the Notification Area, or go to the System component in the Windows Control Panel and click the activation link at the bottom of the window, or go to the Start>Search Box, type *slui* and press Enter.

If you are aware that your PC may undergo some further changes shortly, such as the installation or removal of key pieces of hardware, it is recommended that you do not activate Windows right away. You have 30 days within which to bed down your final hardware configuration after Windows installation, and I suggest you use it. Activating before your hardware setup is finalized could see you having to re-activate repeatedly, including having to call Microsoft to complete activation or running into other potential complications. Microsoft generally views multiple activations of the same key in a short space of time as suspicious.

If you need longer than 30 days to bed down your hardware, there is a built-in tool you can use to extend the grace period before activation is mandatory by another 30 days each time, up to a maximum of 120 days in total, before you must activate. Follow these steps to do so:

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

```
slmgr /rearm
```

3. Reboot your PC and you should now have an additional 30 days before activation.
4. You can repeat Steps 1 - 3 above to give you a total of 120 days maximum before activation is required.

Note that the `slmgr` command has a range of other options which you can see by simply typing `slmgr` in the Command Prompt and pressing Enter.

Bear in mind that at some point you must activate your copy of Windows 7 for it to be legal, as Microsoft does not view the use of Windows without activation as a legitimate method of 'trialing' Windows 7. The 30 day grace period offered by activation is simply to allow ample leeway for people to activate Windows when it is convenient. It should not be considered a trial period. If you genuinely wish to try out Windows 7 you can download the free Windows 7 Enterprise Trial Version and run it for 90 days.

Once you are ready to activate Windows, go to Start>Search Box, type *slui* and press Enter. Click the 'Activate Windows online now' button. When activation commences, you will automatically connect to a Microsoft server and send several pieces of information specific to your system including:

- The version of the OS and the version of the activation software.
- Your language.
- Your Product Key.
- The Internet Protocol (IP) address of your PC.
- A set of non-unique hardware hashes generated based on your hardware configuration. These hashes don't have any personal information, nor can they be used to determine the make/model of your PC.

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 by contacting Microsoft over the phone. If activation succeeds you will not be required to reactivate Windows 7 again unless:

- 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 tampering with Windows to circumvent the Windows Activation Technologies.

For more details of exactly what Activation entails, and under what circumstances you may need to do it, see this Activation FAQ.

Failed Activation

If you have not activated Windows successfully within 30 days, or if you do not reactivate within 3 days after any major hardware changes, or you are found to be running a non-genuine version of Windows at any time, you will enter a reduced functionality state in which you will experience the following:

- A message from the system tray once every hour reminding you to 'Activate Windows Now'.
- A desktop message indicating that Windows is non-genuine.
- A non-genuine message that appears when the Windows Control Panel is launched.
- The Desktop Wallpaper will turn black. Even if you reset the wallpaper to something else, it will again turn black within an hour.
- You will not be able to receive optional updates from Windows Update.

You will need to successfully activate your copy of Windows 7 with a valid product key to remove these effects 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 as covered in this Microsoft Article.

< VALIDATION

Alongside product activation, Microsoft has built additional anti-piracy features into Windows 7 called Validation, previously known as Windows Genuine Advantage (WGA). While activation verifies your product key, validation is an ongoing process that periodically checks your Windows to ensure that no tampering has taken place to bypass activation, and that your product key is still legitimate and not in use in breach of licensing conditions. When validation occurs, Windows will connect to Microsoft servers to send information similar to that described under the activation procedures further above. This validation may also occur when you connect to Windows Update or download certain Microsoft updates. If validation fails, you will not be able to download updates from Microsoft, and can only download critical security updates through the Microsoft Download Center or through Windows Update if set to automatically update. You may also drop down into reduced functionality mode as described further above.

FAILED VALIDATION

If you are having problems with validation when using a legitimate product key, visit the Windows Genuine Advantage Diagnostic Site. To manually validate your Windows at any time, use the official Validate Now method. If you fail validation but still believe your product key is legitimate, check to see if the Certificate of Authenticity (COA) sticker on your PC or copy of Windows 7 is genuine using the information in this Microsoft Article. If you are hesitant to allow validation and have concerns about your privacy and the information being transmitted to Microsoft, read the Microsoft Privacy Statement Highlights for summarized details in plain English.

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

WINDOWS EXPLORER

Windows 7 uses the Explorer-based interface as the primary means for manipulating files and folders in Windows. This interface is used by Windows Explorer as well as by many applications. It should be familiar to all Windows users, however there have been some notable changes in Windows 7, building on the changes which Windows Vista introduced.

Windows Explorer can be accessed in several ways, including by going to Start>Search Box, typing *windows explorer* and pressing Enter, by using the Computer link in the Start Menu, by clicking the folder icon in the Taskbar, or by pressing WINDOWS+E. This chapter covers all of the important new and existing features of Windows Explorer and Explorer-based interfaces in Windows 7, 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 Windows Aero, the Taskbar, Start Menu, and Windows Desktop, are all covered in detail in the Graphics & Sound chapter.

< BASIC FEATURES

This section covers the basic features of Windows Explorer in detail.

SEARCH BOX

The Search box is present in all Explorer-based interfaces, including Windows Explorer and most open windows, shown at the top right of the window. This is a very useful feature which allows you to quickly refine 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 Windows Explorer, type **.exe* in the Search Box to filter out other files and show only .EXE files.

In Windows 7 any filters you previously entered are now displayed in a drop down box for quick selection, 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.

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, a refresh button at the far right, and the path to the currently displayed directory or window in the 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 to a specific directory or path by left-clicking on an empty space in the navigation pane and entering the full path or the directory name. If the directory doesn't exist, Windows will launch a web search on your default browser using the search string entered.

§ You can view and select recently opened directories by clicking on the small Recent Pages down arrow found between the Address Bar and the right arrow on the left side of the window.

- § 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 copy the current directory path, or a portion of it, by right-clicking on the appropriate directory and selecting 'Copy address as text'.

Note that to clear the stored history of recently viewed and previously opened locations at any time, right-click in the Address Bar and select 'Delete History'. Then close and reopen Windows Explorer and you will see that the Recent Pages arrow is grayed out, and the Previous Locations drop-down box is empty.

NAVIGATION PANE

This is the area in the left pane of Windows Explorer which lists various folders. 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 Windows 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 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]*), 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't delete the Favorites folder, however if you wish to rename it you can do so 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 PC 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 Rename and Delete options when you right-click on the Favorites category. While deleting Favorites will not work permanently, you can rename it if you wish.

Libraries

The Libraries feature is covered in full detail later in this chapter. However if you simply wish to remove the Libraries category from the Navigation Pane, 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 Windows 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

If you have enabled the HomeGroup feature, typically by setting your Network Location to Home during Windows installation or at a later date, then you will see this category in the Navigation Pane. 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 feature which can be safely disabled, removing this item in the Navigation Pane.

To remove the HomeGroup item, right-click on the Homegroup category, select 'Change HomeGroup settings', or go to the HomeGroup component in Windows Control Panel. Click the 'Leave the homegroup' link, then select 'Leave the homegroup' to confirm. You may also have to disable the two HomeGroup-related services which are currently running by opening the Services utility and setting both 'HomeGroup Listener' and 'HomeGroup Provider' services to Disabled - see the Services chapter for more details of how to do this.

See the HomeGroup section of the Control Panel chapter for more details of this functionality.

User Folder

Depending on the options you've enabled under Folder Options (See Folder Options further below), a category which may appear on the navigation pane is your user folder which has your *[username]* as its title. To see your user folder and subfolders as a separate category on its own, you need to go to Folder Options in 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 along with the standard subfolders such as *My Documents, Downloads, 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 below 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 Windows 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 Windows Explorer.

More details regarding your user folder are under the Personal Folders section later in this chapter.

Computer

All 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 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 appears in all versions of Windows 7, 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 Navigation Pane folders 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 the folder, or right-clicking on it and selecting Collapse to close the folder, reducing its presence. Then to make this setting stick so that each time you open Windows 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' item 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, untick both the boxes under the Navigation Pane options in Folder Options as covered above, manually add all your commonly used directories to Favorites, then minimize Libraries, Computer and Network, leaving only the Favorites folder maximized. Now each time you open Windows Explorer you will have a very clean layout with quick and easy access to your commonly used folders under Favorites.

Alternatively, if you make use of the Libraries feature, then do the same as above, however minimize every other folder except your Libraries, and you can now quickly access all your files in that manner.

Finally, 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 except your user folder.

Obviously you can experiment with a combination of these options to obtain the layout which suits you best. Note that regardless of how you customize the Navigation Pane, by default Windows Explorer selects the Libraries category whenever Explorer is opened. You can alter this default behavior by using the tips under the Advanced Features section later in this chapter.

COMMAND BAR

Beneath the Address Bar and the Menu Bar (if showing) at the top of Windows Explorer and some Explorer-based windows is the Command Bar which contains a range of buttons. These buttons are context-sensitive and will instantly change depending on the folder or file type you are viewing or have highlighted. For example, if you highlight an .MP3 music file, the command bar will change to display a Play button. Other buttons you may see include but are not limited to: Open, Include in Library, Share With, Burn, New Folder, E-mail, New Contact, Print, and Slide show.

You will always see the Organize button on the command bar; this allows you to access a range of useful functions that let you customize the Explorer interface. Under this button, aside from common tasks such as Copy, Paste, Rename and Properties are the following useful features:

Menu Bar

Under the Layout item you can select whether to display the Menu bar at the top of the screen - if selected the Menu Bar will be enabled permanently in Explorer and Explorer-based interfaces, which includes most normal windows. If you don't wish for it to be permanently displayed, untick the option here. Alternatively, you can choose to enable or disable the Menu Bar's permanent display by using the 'Always show menus' option in Folder Options - see the Folder Options section later in this chapter.

Even if the Menu Bar is not displayed in a window, you can toggle it on or off temporarily at any time by pressing the ALT key while in an Explorer-based window.

Details Pane

Under the Layout item you can select whether to display the Details Pane. If enabled, the Details Pane sits at the bottom of the Explorer window and displays relevant 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 right-clicking in an empty area in the Details Pane and selecting Small, Medium or Large from the Size menu.

Preview Pane

Under the Layout 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 is usually empty if no file is highlighted. Once you highlight a particular file, a preview of the contents will be displayed where possible. This preview can be in the form of text or multimedia. This can increase file browsing time, so disable it if you don't need this functionality.

The Preview Pane can be toggled on or off at any time using the separate Preview Pane button found at the far right of the Command Bar, next to the circular Help and Support button. This means you can quickly enable or disable this functionality as desired. However if the 'Show preview handlers in preview pane' option is disabled in Folder Options, multimedia files will not have playback capability, and many files will not even show a preview of their contents - see the Folder Options section further below.

Navigation Pane

Under the Layout item you can select whether to display the Navigation Pane. The Navigation Pane is covered in more detail earlier in this chapter. Unticking this option removes the whole Navigation Pane, leaving Windows Explorer in a single pane view, which is generally not recommended.

Folder and Search Options

Selecting this item opens up Folder Options, which is also accessible from the Windows Control Panel. Folder Options is an important component and is covered in more detail in its own section later in this chapter.

Views

This functionality is covered in more detail in the Folder Views section just below.

FOLDER VIEWS

Every directory in Windows Explorer and Explorer-based interfaces can display its contents using one of a variety of pre-defined views. The available views can be accessed in three main ways:

§ Click the 'Change your view' button at the right side of the Command Bar. Either click the button until a view you like appears, or click the small down arrow next to the button to select the desired view.
§ Right-click in an empty area of a folder, then select the View item and the desired view.
§ Hold down the CTRL Key and scroll the mousewheel to actively cycle through all the available views.

The standard Windows view types are described below:

§ *Icon* - You can select Small Icons, Medium Icons, Large Icons and Extra Large Icons views. Icon view shows all files as icons, sorted by the filename by default. These icons are typically the standard Windows icons for each file type, however multimedia files such as music, pictures and video files, and even document files, 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 mousewheel.
§ *List* - This view is the most basic, and simply lists all the files with their filename and a small generic icon, with no other details 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 icon. Live Icons are shown in Tiles view by default.
§ *Content* - New to Windows 7, 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 size and date modified. It also includes 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

When in Icon view, but also when using Content or Tiles 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 that 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 covered above and in combination with an Aero-enabled desktop - see the Graphics & Sound chapter for more details. However 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 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 then takes not much longer than normal to view a folder with Live Icons as opposed to generic icons, and consideration should 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 7 64-bit, even though 32-bit applications can run without any issues, when it comes to Windows 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 7 64-bit the default program/codec/plugin associated with viewing particular content needs to also be a native 64-bit application, or the Live Icon 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 need to install and/or associate a 64-bit application or media handler with that file type. See the Codec section of Windows Media Player for further details in relation to common multimedia codecs and plugins.

In the case of documents saved using Microsoft Office 2007, it is a 32-bit-only application, so Live Icons for documents won't be shown in 64-bit Windows 7. However there is a way around this: when saving a document in Office 2007, or the 32-bit version of Office 2010, select the 'Save As' option, tick the 'Save Thumbnail' box, 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 Windows Explorer for example.

Whether you are running Windows 7 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, which 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, as Windows 7 should automatically resort to maintain appropriate order.

Sort By: To sort by something other than file name, right-click on a blank spot in the folder and select 'Sort By', and you will see the common properties such as Date Modified, Type and Size on which you can sort the contents, either in Ascending or Descending order. You can click the More option and select any one of a larger range of properties upon which to sort the current view of folder contents.

Group By: You can create sorting subcategories within a view by right-clicking on an empty area in a folder and selecting 'Group By', then selecting the particular property by which you wish to group the contents. This will arrange the contents under headings for each subcategory. Once again you can select the More item to see additional properties for use in grouping contents. If you wish to remove grouped view, right-click, select 'Group By' then choose the (none) item.

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. If a category you wish to use for filtering isn't available, you can add more column types by right-clicking on a column header, selecting the More item and selecting which additional columns to add.

Note that the 'Stack By' sorting option available in Windows Vista has been removed in Windows 7.

Changing Folder Views

Windows decides the default view for a particular folder based on the type of folder involved and/or the types of files within a folder. Windows 7 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 under 'Optimize this folder for'. If you wish to change this folder's type, you can do so here, and you should 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. However 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. Follow the steps below to ensure your view selections are made permanent until you choose to manually alter them again:

To begin with, 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 Windows Explorer and go to your *My Documents*, *My*

Pictures, *My Music*, *My Videos* and *Downloads* folders found under *\Users\[username]* and then do the following for each:

1. Adjust the view to suit your preferences using the methods covered earlier. Add or remove and/or resize any columns if applicable, change the view type and resize any icons shown if required, and choose your sort order for files.
2. Once done, then you must click on the Organize button in the Command Bar and select 'Folder and search options' to open Folder Options - don't open Folder Options via Windows Control Panel or any other method, do it from the Organize button.
3. With Folder Options open, go to the View tab and click the 'Apply to Folders' option, and click Yes when prompted. This forces Windows to recognize that the changes you have made to the view in this folder apply to all folders of the same folder type. So for example, using this method, the changes you make to the view in your *\Users\[username]\My Pictures* folder will apply to all folders currently 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 Windows 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.

Note that setting the views in this manner does not apply them to your Libraries, as they need to be set separately - see the Libraries section later in this chapter. Note further that some system folders will not have a Customize tab; 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 7.

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 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, under the Tools menu in the Menu Bar, or by pressing the Organize button in the Command Bar of Windows Explorer and selecting 'Folder and search options'. As the name suggests, Folder Options has a range of options which affect the way folders are viewed, as well as the appearance of Windows Explorer. It also has important Search-related options. Each tab of the Folder Options box is covered separately below:

GENERAL

Browse folders: If 'Open each folder in the same window' is chosen, then launching a Windows option or utility 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 utility 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 a more web-like behavior, you can select the 'Single-click to open an item (point to select)', and further 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 using practical examples under the Navigation Pane section further above. 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 you wish to keep.

VIEW

Folder views: When you change the look and layout of a particular folder in Windows 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 further above.

Advanced Settings: Most of the options in this section of Folder Options are dependent on your own particular tastes in functionality and appearance. Below I briefly cover all of these features, noting where there may be performance or other impacts. These options all have fairly significant impacts on the way Windows 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 above.
- 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.
- 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 hovering over folders in the right pane.
- Display the full path in the title bar - If ticked, and only when using the Windows Classic theme, the full directory path to the currently selected folder will be shown as the title for Windows Explorer. For example, by default in Windows Classic theme, if you're in your Downloads personal folder on C: drive, only *Downloads* is shown in the title. With this option enabled, *C:\Users\[username]\Downloads* will be shown instead. Has no impact on Aero or Windows 7 Basic Themes and hence can usually be disabled.
- Hidden files and folders - If ticked, shows 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 the important files and folders on your system, especially when using this book, but also for any future tweaking.
- Hide empty drives in the Computer folder - If ticked, will hide any drives with removable media which are not currently holding any such media.
- 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 and tweaking difficult and confusing. For example, if you are asked to create a blank text file and rename it to *ei.cfg*, with this option enabled, you will actually be incorrectly renaming

the file *ei.cfg.txt* since the .TXT extension will be hidden. You need to be able to clearly see the full filename, including any extensions, so untick this option.

§ Hide protected operating system files - Shows a range of additional hidden system files and folders which under normal circumstances should be not be 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 adds to clutter 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.

§ 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 a session restore feature and does not relate to saving different folder views in Explorer, which is covered further above.

§ Show drive letters - If ticked, shows the drive letter for every drive (e.g. C:, D:, E:, etc.). While the drive name will still be displayed, 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 certain 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. If annoying, can be disabled with no negative impact.

§ 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 Explorer-based windows, or on any item on the desktop. The pop-up usually contains a description of the file, folder or desktop item, and in general this is unnecessary and may slow down browsing 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 as it cripples the Preview Pane's functionality. Instead if you find the Preview Pane annoying or slowing things down, simply toggle it on or off as required using the button at the top right of the Command Bar.

§ 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 Windows Explorer whenever you hover your mouse cursor over that file/folder. This can make the selection of multiple objects much easier, but in general 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. See the HomeGroups section in the Windows Control Panel chapter for more details.

§ When typing into list view - When a folder is selected, 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 in the Search Box at the top right of the window. However 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 to implement all changes.

SEARCH

These settings and 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 already being quite convenient for holding various file types, these folders are linked to a range of important features in Windows, such as 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.

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 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 to do so properly, you need to 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 *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 files will be moved to the new location.

When you're done, Windows will now recognize the new location as the home of this particular personal folder, and all references to it throughout Windows 7, including in your Libraries and Search Indexing, should point correctly to this new location automatically. If necessary close and reopen Windows 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 new Libraries feature in Windows 7, there are no real drawbacks to creating multiple subfolders under the personal folders if you wish to do so.

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 creating a fresh backup of your personal data - see the Backup & Recovery chapter.

< LIBRARIES

One of the most prominent changes in Windows 7 that users of previous versions of Windows will notice are Libraries. Tightly integrated into Windows 7, 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 location 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 a Library are visible when that Library is expanded in the left pane, or by right-clicking on a Library and selecting Properties. These folder(s) determine the content displayed in a Library, however none of them has moved from its original location, nor has the Library created a copy of, or a shortcut 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. However 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.

Since a Library is a virtual folder, when saving, copying or moving a file to a Library, by default the file will actually be saved/copied/moved to the first folder 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.

Even though 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 - see 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 disable Libraries from being shown in Windows Explorer, as covered under the Navigation Pane section earlier in this chapter.

Windows 7 ensures that Libraries are tied in to a range of key features, both to encourage their use, and to make Libraries more useful. Libraries are integrated into the following prominent Windows features:

- Start Menu - The Documents, Pictures, Music and Videos components on the Start Menu all link to the default Windows Libraries of the same name, not directly to the personal folders which hold this content. See the Start Menu section of the Graphics & Sound chapter for more details.
- Windows Explorer - Aside from having a separate Libraries category which cannot be removed using normal methods, Windows Explorer also opens in the Libraries whenever it is launched using a default shortcut such as the one on the Taskbar. Both of these features can be customized - see the Disabling Libraries section below, as well as the Advanced Features section 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 12 utility works closely with the Music Library, not your *My Music* personal folder. See the Windows Media Player chapter for more details.

Many users will initially find Libraries to be confusing, annoying or redundant, and will want to remove them or disable their integration into Windows. While attempting to do this is not advised given the integral nature of Libraries, methods of reducing the presence of Libraries is covered further below. I strongly recommend that you attempt to work with the Libraries, customizing them and adding new Libraries for various content as you desire. After a while 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 to suit your needs - see the Folder Views section further above. Note that the 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 each Library, and then at any time if you wish to return to the default view for a Library, left-click on the 'Arrange by' link at the top right and select 'Clear changes'.

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 Start Menu items of the same name - for example, deleting the Documents Library will make the Documents component in the Start Menu inoperative.

Fortunately you are not confined to these Libraries or their default contents. You can modify Libraries as you wish by opening Windows Explorer and following these steps:

Add or Delete Library

To add a 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 folders which this Library will reference for gathering its content. To add or remove folders from a Library:

§ Add Folders - Select the new Library and either right-click on it and select Properties then click the 'Include a folder' button, or click the 'Include a folder' button in the right pane. 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 all the 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 at the top of the box and 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 which collectively references those files and folders.

Changing Library Icons

The icons used to represent various Libraries can't be changed by default. However you can change them if you manually edit the .XML definition file for a 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 available, select them here. Otherwise select 'Choose default program' and/or click the Browse button and select Notepad or Wordpad in the available list. If none of these methods 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, 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.

To find or create a valid icon file see the Icons section of the Graphics & Sound chapter for details.

DISABLING LIBRARIES

In actuality there is no proper user-based method to completely disable every element of Libraries as they are fully integrated into the Windows shell. However there is a method which simply removes Libraries from view in the Navigation Pane of Windows Explorer, and is covered under the Navigation Pane section earlier in this chapter. While not recommended, 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 Windows Explorer, which for most people who dislike Libraries should be sufficient. They can still be accessed from the relevant Start Menu items and also be found under the *\Users\[username]\AppData\Roaming\Microsoft\Windows\Libraries* directory.

If you find the default Windows Explorer behavior of opening at the Libraries category annoying, you can also customize this easily using the Set Windows Explorer Startup Folder tip under the Advanced Features section below.

There is however 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, Microsoft has made it clear that it wants to promote the use of Libraries by users and software developers alike. This means that many future applications designed for Windows 7 are likely to link to the Libraries functionality in some way, such as by saving files to the relevant Library by default instead of to a specific user folder. As such, it is best to learn to live with Libraries and take advantage of them. You don't have to actively use them however, and you can minimize their presence, but I strongly advise against mangling Windows in an attempt to remove this core piece of Windows 7 functionality, at the very least because of future compatibility implications.

< 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, 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 Windows 7 attempts to put files or folders under a non-existent directory under 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 7. 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 7. 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 7 the junctions under your personal folders point to the following real directories:

Junction / Windows XP Directory	Corresponding Windows 7 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 7. For Vista users, the personal folders remain much the same, except that the *Recent* folder has been renamed *Recent Items* in Windows 7.

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 the NTFS file system. 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.

For example to create a link simply called *ReadMe* in your current directory linking to the file *Text.doc* under *C:\Users\User1\Downloads\*, open an Administrator Command Prompt and use the following command:

```
MKLink ReadMe C:\Users\User1\Downloads\Text.doc
```

The Symbolic Link *ReadMe* will be created under the current directory in which the Command Prompt is sitting, and is denoted with a shortcut icon when viewed in Windows Explorer. If you want to see where this link points to, right-click on it, select Properties and under the Shortcut tab click the 'Open folder location' button. You can also use the `/J` switch for the `MKLink` command to create a Directory Junction to link to a directory instead of a file, e.g.:

```
MKLink Downloads C:\Users\User1\Downloads\ /J
```

Note that you can delete a Symbolic Link and it will not delete the file or folder it is linked to.

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 games, and generally speaking you should not need to create or alter Directory Junctions or Symbolic Links unless troubleshooting a related problem.

< ADVANCED FEATURES

The following are some slightly more advanced features of Windows Explorer which go beyond its common functionality, including tips and tweaks for making Explorer easier to use.

SET WINDOWS EXPLORER STARTUP FOLDER

If you usually open Windows 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 Windows Explorer, such as the folder icon in the Taskbar, open Windows Explorer in the Libraries category. To alter this behavior for Windows Explorer, do the following:

1. To customize any existing Windows Explorer shortcut, right-click on the shortcut and select Properties. For the folder icon in the Taskbar, right-click on the icon, then right-click again on the Windows Explorer item in the bottom section of the Jump List which opens and select Properties.
2. To create a new custom shortcut to Windows Explorer right-click on an empty area of the Desktop and select New>Shortcut.
3. In either case, 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. E.g.:

   ```
   %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 Windows Explorer in the Computer category instead.
4. For existing shortcuts, click the Apply button; for a new shortcut, click Next, then name the shortcut something appropriate, like Windows Explorer, and click Finish.
5. This shortcut can now be used to always open a Windows Explorer window in the directory specified.

Note that if the Taskbar folder icon is altered as above, other instances of Windows Explorer launched from normal shortcuts will be shown separately in the Taskbar.

If at any time you quickly want to open Windows Explorer at any particular folder on your system, go to Start>Search Box and type (or paste) either a partial or full path to the folder (without quotes), then select it from the list shown in the Start Menu. In the case of your default Libraries, simply enter their name in Start>Search Box and press Enter - Windows Explorer will open in that Library.

MANIPULATE MULTIPLE FILES

If you have a range of files you want to manipulate together - e.g. move, copy, rename, change the properties of all of them - you can do so rapidly in Windows 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 click on the first file in the group, then while still holding down SHIFT, 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 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.

Without clicking anywhere else, you can now:

- Drag and drop these files 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 be automatically 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.

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 Windows Explorer.
2. Open Task Manager - see the Task Manager section of the Performance Measurement & Troubleshooting chapter.
3. Under the Processes 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 will go blank.
4. Still in Task Manager, go to the File menu and select 'New Task (Run...)'.
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 reboot or logoff and logon again. However this method does not replace the need to reboot in most other circumstances such as during the installation of drivers, or after serious errors. Furthermore if your interface is constantly showing glitches, this is a sign of a problem that you should properly resolve, as it is not normal.

DUAL WINDOW EXPLORER VIEW

If you want to undertake more complex file copying/moving between various folders/drives on your system, Windows Explorer can be combined with Windows 7's Aero 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 Windows 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. Now drag one Windows Explorer window to the far left of the screen until Aero Snap automatically resizes it to fill exactly half the screen.
3. Drag the second Windows 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 Windows 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 Windows 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 flick 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 Windows Explorer it will open with its default size and location intact.

CUSTOMIZE FOLDER ICONS & FOLDER PICTURES

Most folders in Windows 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 Windows Explorer and navigate to the folder you wish to customize. Go to 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 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 Windows Explorer. If the folder is also linked to the Start Menu, your new Folder Icon will also appear at the top of the Start Menu when the relevant Start Menu item is highlighted - for example, if you change the Folder Icon for the *\My Documents* personal folder, then it will appear whenever you select Documents from the Start Menu. Indeed wherever your folder is referenced with an icon, the icon should have changed. Note that if you delete the original .ICO icon file you pointed to in Step 5 above, 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 - for example there are a range of proper 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 Windows 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.

For full details of Windows icon creation and customization, see the Icons section of the Graphics & Sound chapter.

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 Windows 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 'Pin to Start Menu' and '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 your personal folders will 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 our purposes look under the Explorer tab of Autoruns - the majority of the entries 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 and check to see if the undesirable context menu entries are gone. To permanently remove an item, right-click on it and select Delete. For full details of how to use Autoruns, see the Startup Programs chapter.

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, expand the columns and look under the 'File Type' column - the associated applications for each menu entry are shown. 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, 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 item, however you will likely have to reboot to see the impact of the changes. 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 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]
```

Here you can select the relevant file extension from the list of subfolders shown. For example to edit the .AVI video file extension, go to the `.avi` key here, then select the `OpenWithList` key under it, and in the right pane you will see a list of STRING entries such as the ones below:

```
a=wmplayer.exe
b=VirtualDub.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 values 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 Windows Explorer, the New option appears in the context menu, and when selected, shows a range of programs for which you can open a new document/file type. 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. 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 will create a blank new file with the relevant extension when selected.

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 the Desktop (as a shortcut), or to a Compressed folder, or to a Library. You can edit the options which appear in the 'Send To' context menu by going to the following folder:

\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

If you want to add two useful commands to your context menus - namely 'Copy To' and 'Move To' - then 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 specify the location to copy or move them to. To remove either of these entries simply delete the relevant subfolder 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, or the All Programs item on the Start Menu. 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. Finally, also refer to the Windows Aero section of the Graphics & Sound chapter for details of how to customize the Aero Peek responsiveness speed.

FIX CHANGING FOLDER VIEWS

This is an issue which first came to prominence in Windows Vista, but can still occur in Windows 7, although it is unlikely to occur if you set your folder views correctly as covered under the 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 instructions in the Folder Views section of this book, 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 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 don't change again without you changing them manually. However 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 interface.

GOD MODE

Dubbed God Mode, there is a method which allows you to create a custom link in Windows Explorer which when clicked displays a collective list of particular functions in Windows 7. This method uses Namespace Junctions to create a virtual folder as detailed in this Microsoft Article. Open Windows 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 the features available in the Windows Control Panel. This may be useful for some people, but bear in mind it provides no additional functionality than that found in the actual Windows Control Panel which you can access normally within Windows.

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.

Windows 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 Windows 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 Windows Explorer and Explorer-based applications use more resources and become 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 in various situations, such as during 3D games or when displaying the Windows Desktop. Windows 7 comes with built-in driver support for virtually any type of common computer hardware, and hence most of your hardware will operate in Windows without the need to install additional drivers. However the built-in Windows drivers are not optimal and do not guarantee 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 7-specific device drivers for your hardware to make sure your entire system performs optimally, with full functionality and maximum stability.

Windows 7 is based on much the same driver model used in Windows Vista, 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 then 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 7 also improves driver compatibility, which makes finding the right drivers for your devices much easier. However there are a range of important considerations when installing and configuring drivers, and this chapter runs through these in detail.

< DRIVER COMPATIBILITY

Windows 7 provides improved driver compatibility because it is based on the same driver architecture as Windows Vista. This means that any hardware which ran under Windows Vista is extremely likely to function correctly under Windows 7. Even if the hardware manufacturer does not provide Windows 7 drivers for a device, you can use a driver designed for Vista under Windows 7. For some devices, such as printers for example, you may even be able to use Windows XP drivers under Windows 7.

For a range of reasons you may have difficulty in finding and installing compatible drivers for your devices in Windows 7. See the information below for assistance.

FINDING COMPATIBLE DRIVERS

Ideally before installing Windows 7 you should have checked your hardware's compatibility with Windows 7 - see the start of the Windows Installation chapter for links to appropriate resources to do so. While Windows 7 supports a wide range of hardware, certain hardware that is older or less common may not be completely compatible with Windows 7. You should also 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 your device manufacturer's site by checking the packaging or instruction manuals for the device, or searching Google using the model name and number. Check to see if there are any Windows 7 drivers for your device, or if the manufacturer has made any announcements regarding providing support for Windows 7. 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 drivers to use in Windows 7. If you still can't find a suitable driver there, check any discs which came with the device to see if they hold appropriate Windows 7 or Vista drivers you can attempt to use.

If no Vista or Windows 7 driver is available for your device, then you can use Windows Update to search for any new or updated Windows 7-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, you can type in part or all of your hardware's brand and 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 first. Add any drivers you wish to download, then click the 'View Basket' link at the top right and then click the Download button to obtain the driver for free.

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 BIOS & Hardware Management chapter. If that fails, then you must simply wait for one to become available, whether from your manufacturer, or from Microsoft via Windows Update. Without a suitable driver, most devices simply will not function correctly - it 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 due to general compatibility issues. If this is the case, try all of the following:

§ Right-click on the driver package and select 'Run as administrator' to ensure it is properly assigned full Administrator rights.

§ 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 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 tick the 'Run this program in compatibility mode for' box and set it for 'Windows Vista' - this is particularly useful for attempting to install Vista drivers on 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, check the information in the rest of this chapter for other methods of manually installing a driver. Also check the BIOS & Hardware Management as well as the Performance Measurement & Troubleshooting chapters for details of how to troubleshoot a problematic device.

64-bit Compatibility

A critical compatibility issue for any Windows 7 user is the fact that you cannot install drivers designed for the 32-bit version of Windows 7 or Vista on a 64-bit installation of Windows 7, or vice versa. This means that if you intend to use Windows 7 64-bit, then you should check to make sure that there are appropriate 64-bit drivers for all of your key hardware components. There is no 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. Be aware that in some cases the hardware manufacturer may decide to never release 64-bit compatible drivers for older, superseded or less popular hardware, so I strongly recommend checking the availability of 64-bit drivers for your hardware using the procedures further above before deciding to use Windows 7 64-bit.

< 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. This means you should only install drivers that you are familiar with, and which are from a reputable source, such as 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 7 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 altered in any way after the drivers were signed.

Most signed drivers carry Windows Hardware Quality Labs (WHQL) certification, meaning they have been tested and digitally signed by Microsoft. A Windows 7 WHQL certified driver is desirable, as it indicates that the driver has been tested to be both secure and compatible with Windows 7, and should be relatively problem-free. However WHQL certification does not necessarily guarantee 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 or appears to have been altered after being signed, Windows 7 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 trusted source. In most cases this should be direct from the hardware manufacturer's site. If you are not completely sure 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 are downloading 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.

Windows requires a digitally signed driver: In Windows 7 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 7 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 - see the Kernel Patch Protection section of the PC Security chapter for details. However there is a way around this limitation if you absolutely must install an unsigned driver. Detailed in this Microsoft Article, it involves restarting your PC and during bootup continually pressing the F8 key until you come to the Advanced Boot Options screen, where you can select the 'Disable Driver Signature Enforcement' option to prevent signature checks throughout the current session. You will need to do this at every restart though, otherwise any unsigned driver(s) will not load up with Windows. Note that Microsoft consistently patches Windows to disable or prevent other methods of circumventing this signature check on 64-bit Windows, because they are considered security holes.

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 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 Start>Search Box, type *sigverif* and 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, go to Start>Search Box, type *dxdiag* and press Enter. See the System Information Tools section of the System Specifications chapter for more details of DirectX Diagnostics.

Again, installing unsigned drivers is generally not recommended unless you are absolutely certain of the trustworthiness and reputation of the source of the drivers. This usually means they should be direct from the relevant hardware manufacturer's website. Some hardware manufacturers release unsigned drivers which are perfectly safe and functional, typically in the form of official Beta drivers, but you should still try to minimize the number of unsigned drivers on your system. Just because a driver package appears to be the same as one your hardware manufacturer, doesn't mean it hasn't been modified by someone else afterwards, so by installing unsigned drivers you are defeating a security feature of Windows, and potentially giving malicious or problematic software direct access to your system.

< DRIVER INSTALLATION

All of your major hardware devices require the latest available Windows 7-compatible drivers and related updates to function at peak performance and with stability and full functionality. Indeed many problems in applications and games often result from not using the latest drivers. It is important therefore to check for and install all the latest relevant 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 *Setup.exe* or similar file. Some drivers may come in a form which requires manual installation, or other procedures, 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 to allow proper driver installation. Windows 7 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. However some device drivers may still need a reboot in order to replace files which are currently in use, so reboot as often as required and don't do anything else on your system until driver installation is complete.

The specific updates and drivers you should install, and their preferred order, is provided below in a series of recommended steps you should follow:

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 7 installation disc already has the Service Pack integrated into it.

Service Pack 1 (SP1) has been released for Windows 7, and is a compilation of all the major updates released on Windows Update prior to SP1's release, along with a range of miscellaneous hotfixes. The full list of updates and changes included in SP1 can be found in this Microsoft Article, however there are no notable feature changes relevant to the average home PC user as a result of SP1. Once you have installed SP1, you can safely remove the unnecessary backup files and the redundant previous versions of system files left over from the service pack process - see the Service Pack Cleanup section in the Cleaning Windows chapter for details.

STEP 2 - DIRECTX

Install the latest version of Microsoft DirectX. As covered under the Graphics & Sound chapter, DirectX is an important component of Windows which allows advanced multimedia functionality. Windows 7 already comes with DirectX 11 installed, which is the latest version of DirectX, however from time to time Microsoft releases updates for all versions of DirectX, and the latest of these should be installed to ensure the best performance, compatibility and stability.

STEP 3 - WINDOWS UPDATE

Windows Update is the main tool used to obtain security patches, as well as driver and feature updates in Windows 7. It is covered at this stage because it is very important to configure Windows Update correctly as soon as possible after installing Windows 7, both so you can download and install relevant security updates before doing anything else, and also to prevent Windows Update from installing any outdated device drivers until you first get the chance to manually update all the important devices as per the following steps. In Step 8 you will revisit Windows Update to then change the settings such that any newer or missing drivers can also be found and installed.

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 is as follows:

- 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 updates are security and reliability-related updates which 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, as it will allow Windows Update to regularly check for updates and let you know if any are found via a prompt in the Notification Area, but it will not download or install anything without your explicit consent. This lets you download and install updates at your convenience, and also check the individual updates to ensure that nothing undesirable or unnecessary will be downloaded or installed.

Recommended Updates: These updates address non-critical problems and provide additional features. 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.

Who Can Install Updates: This determines whether Standard level User Accounts can install updates or not. If the box is ticked, all such accounts can install updates via Windows Update; if unticked, only Administrator level User Accounts can install from Windows Updates.

The following options only become available if you click the 'Find out more' link next to the 'Get updates for other Microsoft products' section on the main Windows Update screen. You will be taken to the Microsoft Updates website where you will have to agree to the Terms of Use for this service before being able to access this service. Tick the box, click Next, and select 'Use current settings' and click Install to enable these options:

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 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.

Software Notifications: If the 'Show me detailed notifications when new Microsoft software is available' option is ticked, you may receive regular notifications when new Microsoft products are released. This is not a necessary option unless you like to be informed of new Microsoft products. If you untick this option, a 'Find out more about free software from Microsoft Update' box will be shown at the bottom of the main Windows Update screen, which you can ignore.

Once you have changed all the settings, click the OK button and Windows Update will automatically 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 the updates you want to install screen'. You should notice that there may be 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 you do not wish to install. To see more details for any update, highlight it and check the right pane. If you are certain the update is not necessary for your PC, right-click on it and select Hide to remove it, though note it is not permanently removed; it can be restored at any time by clicking the 'Restore hidden updates' link in the left pane of Windows Updates, ticking the relevant updates and clicking the Restore button.

Importantly, if you've just installed Windows, at this stage you should make sure all Optional updates which appear to be related to drivers are unticked. You should not install any drivers 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 OK and then click the 'Install updates' button on the main Windows Update window. We will revisit these Optional updates in Step 8 below.

I strongly recommend allowing Windows Updates to check for updates regularly. Do not set Windows Update to 'Never check for updates' as this opens your system up to recent 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 PC Security chapter for more details.

If you are receiving an error when using Windows Update, check this Microsoft Article for a list of 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 7 item on the left side, then click the Security Patch item below it to narrow the list down to security updates for Windows 7. This site is also useful if for some reason you want to download specific updates and store or transfer them to another machine. I do not recommend any other method of 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 - e.g. letting a third party know all about your unsecured vulnerabilities.

Finally, by default Windows Update creates a restore point prior to installing new updates, which 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 it. I recommend leaving System Restore enabled to allow this to happen - 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 image of your PC - typically with the name *[username]-PC*, 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 BIOS & Hardware Management section for more details.

These measures prevent Windows 7 from automatically installing any device drivers for your hardware components and peripherals which may be out of date, since device drivers found through on 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 can be reconfigured appropriately under Step 7 below, and Windows Update in Step 8 below.

Note that if for some reason you skipped Steps 1 and 2 in this chapter, Windows Update will also identify and provide the option for installation of any available Service Pack(s) and DirectX updates. Installing these separately as detailed in Steps 1 and 2 is best, particularly as they can sometimes take a while to appear on Windows Update. However they can also be installed via Windows Update without any problems if that is your preferred method.

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, so using the latest drivers for it is important in achieving optimal, trouble-free performance for your entire system, as well as providing additional motherboard-specific functionality such as onboard audio, onboard network adapter, RAID, etc.

Finding all the correct motherboard drivers is not necessarily a straightforward task. To start with, 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, an *ASUS P6T Deluxe* motherboard is manufactured by a company called ASUS, it uses an Intel X58 Express chipset and it has the specific model name P6T Deluxe. All of these details are important when determining the correct driver to use. A combination of the utilities covered in the System Specifications chapter, along with your motherboard manual and Google will give you all the required details about your motherboard.

Your motherboard usually comes with a driver disc which contains the relevant drivers, however these are often well out of date. The first place you should look for the latest version of these drivers is on your motherboard manufacturer's website - there are too many to list here, so check your motherboard manual 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 category below:

BIOS - These are not drivers, they are BIOS updates for which you should refer to the BIOS & Hardware Management chapter for more details.
Chipset - These are the core drivers which control your motherboard's key functionality. All systems require these for optimal performance and functionality.
IDE, SATA, RAID - These drivers are required for correct operation of your motherboard's drive controllers. You may also require these drivers for correct detection of your drives during the installation of Windows - see the Preparing the Drive section of the Windows Installation chapter.
Video - 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 below.
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 below.
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 already incorporated into the Chipset driver package.
LAN - If you are using your motherboard's onboard network/Ethernet controller, whether for an Internet connection or a 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 IDE/SATA/RAID drivers.

If you're not using a particular function on your motherboard, I strongly recommend disabling it in your BIOS as detailed in the BIOS & Hardware Management chapter. This will prevent Windows from automatically detecting them and installing drivers for them 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 can download the latest drivers directly from one of the major chipset manufacturers:

- For **Intel** motherboards, download and install the latest Intel Chipset Software.
  If you also have a RAID or AHCI setup install the Intel Rapid Storage Technology Driver.
- For **Nvidia** motherboards, download and install the latest nForce Drivers.
- For **VIA** motherboards, download and install the latest VIA Hyperion Drivers.

Note that some of these drivers may contain a mix of driver components, including chipset, SATA/RAID and LAN drivers all in one package. Read the driver notes on the site for more details.

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 285* graphics card uses an Nvidia GeForce 200 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 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 Forceware Graphics Drivers.
  For details on how to install and set these up correctly read the Nvidia Forceware Tweak Guide.
- For **ATI** graphics cards, download and install the latest ATI Catalyst Drivers.
  For details on how to install and set these up correctly read the ATI Catalyst Tweak Guide.
- For **Intel** graphics cards, download and install the latest Intel Graphics Drivers.
- For **SiS** graphics cards, download and install the latest SiS Graphics Drivers.
- For motherboards with onboard graphics, check your motherboard manufacturer's website first (See Step 4), then check one of the sites above for Integrated or Onboard Graphics drivers.

Note that unlike motherboards, you do not need to download your graphics drivers from your hardware manufacturer's website. Installing the latest 'reference' chipset drivers available directly from the chipset manufacturer as shown above is the best method as they are typically much newer.

Importantly, under Windows 7 graphics functionality has improved over the way it was implemented in Windows Vista, which in turn was a major change over the way it was implemented in Windows XP. The main change in Windows 7 involves the use of a new version 1.1 of the Windows Display Driver Model (WDDM) as opposed to version 1.0 used in Vista. In version 1.0 a large number of improvements and changes were introduced, such as allowing the Desktop Window Manager (DWM) to use both 2D and 3D effects as part of the Aero interface. The revised WDDM 1.1 brings with it additional improvements that increase the efficiency of desktop rendering, use less memory and provide hardware-accelerated 2D graphics. To take advantage of these enhanced graphics features in Windows 7, you require graphics hardware with support for DirectX 10 or higher and a WDDM 1.1-compatible graphics driver. You can still use older Vista graphics drivers, as well as older graphics cards, but this will not provide the full benefits of the graphics improvements in Windows 7. For full details see the start of 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, check your motherboard manufacturer's website first (See Step 4), then check your onboard audio chipset manufacturer's website such as Realtek.

Windows 7 does not significantly change the way in which audio was implemented under Windows Vista, however Windows Vista was a significant departure from the way audio was implemented in Windows XP. The main difference is that sound cards no longer have as much importance in Windows. Windows 7 uses the new Universal Audio Architecture (UAA) to provide good quality audio and a range of enhancements for almost any sound device without the need for third party drivers. However a proper audio driver from the manufacturer's site as listed above is still recommended for full functionality and optimal performance. For full details of audio in Windows 7 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 7 audio drivers you find you are having strange performance issues or audio problems such as crackling, distortion or disconnected sound, then I recommend that pending newer drivers for your sound card, 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 7 excels at, and hence it is less likely to be problematic, and for all but high-end speaker setups, will offer excellent audio quality without any significant performance difference.

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 7 provides improved built-in support for peripherals and portable devices through a new feature called Device Stage that handles most common tasks for supported devices without the need to install third party drivers or software. If your device appears to work fine and all the major functions you need are available then do not install a driver for them. See the Device Stage and Printers and Devices sections of the BIOS & Hardware Management chapter for more details of this functionality.

Peripheral drivers typically need to load in the background at Windows startup and usually add to overall resource usage, increase startup times, and quite often 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.

Obviously should your device not function correctly, or a feature that you want appears to be disabled, 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 you first go to the device manufacturer's website and download the latest available drivers rather than using any drivers that come on the disc with the device, as they are typically older.

In any case there are far too many device manufacturers to list here, but the website address is usually listed 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]-PC*, 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 7.

STEP 8 - WINDOWS UPDATE REVISITED

Now that you've installed all the latest Windows 7-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 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 OK and then click the 'Install updates' button to install these drivers. Any drivers found using this method should be 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 newer than the current driver versions you are using. If you have any doubts or don't wish to install a particular driver, untick the driver, right-click on it and Hide it in Windows Update so it doesn't appear again.

Once you've completed all 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 go to Start>Search Box, type *devmgmt.msc* and press Enter. The general functionality of Device Manager is covered under the Device Manager section of the BIOS & 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 version, date and provider. 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. 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 detail 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 execute and walk you through the steps necessary to update the device. However in some cases you may need to manually update a driver - for example if a driver does 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 see 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. However Windows only detects and installs individual driver files, and does not look inside driver packages. So if the driver files are archived or in a self-executing driver package on your system, Windows will not detect these as containing a newer driver even if they do. 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, then follow Steps 1 - 3, selecting 'Browse my computer for driver software', then 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 set which you believe is causing you problems, then you may wish to go back to the previous drivers 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.

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 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 versions, since different versions of various driver files and Registry entries may inadvertently be used together by Windows and cause potential problems.

To correctly uninstall a driver package through Windows you should first go to the Programs and Features component of the Windows Control Panel and 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.

However 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 from your system, 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 device 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 and/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 deliberately measure by the device manufacturer. The upshot of all this is that over time, particularly for users who frequently update 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.

Driver Sweeper

If after using the above methods you feel there is still some driver residue left on your system, you can use the free Driver Sweeper utility to attempt to remove any remaining traces of the more common drivers. Note that during installation of Driver Sweeper, you may be prompted to install adware which is undesirable. Make sure to proceed through installation carefully and untick all such prompts.

Once installed, launch Driver Sweeper with Administrative privileges and follow these steps:

1. Tick the driver(s) you wish to remove from the list provided, and click the Analyse button at the bottom of the screen first to see precisely which files and Registry entries will be removed. You can manually untick any component(s) you wish to keep.
2. If you want to continue, click the Clean 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 Sweeper only allows the removal of the specific drivers in the list it provides. Furthermore newer versions of these drivers may install additional files and/or Registry entries which the current version of Driver Sweeper cannot find, so check for updates to Driver Sweeper and remember that no automated method is foolproof in finding all aspects of driver residue, since drivers are constantly changing.

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 go to the Drivers tab. Under the Options menu, untick 'Hide Microsoft and Windows Entries' and 'Hide Windows Entries', but make sure the 'Verify Code Signatures' item is ticked. Press F5 or select Refresh under the File menu.
3. In the list which appears, most of the entries are built-in Microsoft drivers for Windows and should not be unticked or deleted. However under the Publisher column you should check every entry for which the provider is not 'Microsoft Corporation', as most of these are third party drivers installed on your system - though note that some are still built-in Windows drivers provided by other companies. 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 entry in Autoruns, and when finished close Autoruns and reboot Windows. After a period of time if 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. See the Cleaning Windows chapter for tools which can assist in cleaning out unnecessary files, and check the Maintaining the Registry section of the Windows Registry chapter for a Registry cleaning tool.

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 similar to Vista, Windows 7 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 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. However if you find an installed 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 7, and unfortunately this is too complex a method to detail here as it relies on a great deal of research. Furthermore 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. 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 your personal files, reformat and reinstall Windows 7 afresh, then restore only your personal files and folders, and install 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 installing various driver versions, particularly leaked or modified drivers, can quickly make a mess of your system.

< DRIVER VERIFIER

If you believe you're having driver-related problems, you can use an advanced tool which comes with Windows called the Driver Verifier. To run it, go to Start>Search Box, type *verifier* 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 ATI. Note that only drivers which are currently loaded up by Windows are shown. If for some reason

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 a Blue Screen of Death (BSOD) error if the driver files you chose are potentially problematic. If Windows starts up normally and you see no BSOD 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 System Recovery Options Command Prompt and type `verifier /reset` and press Enter. You can also uninstall any driver which 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 as 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 settings, faulty hardware, one or more installed programs causing conflicts, etc. Just because an error message points to a driver file, that doesn't mean the file itself is the 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 the problem. See the Performance Measurement & Troubleshooting chapter for more ways of troubleshooting a system issue, including the use of Event Viewer to see specific error logs.

< 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 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 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 through drivers. The hardware manufacturer's site should always be your first choice for obtaining drivers.

User Feedback - Be wary of general user feedback on drivers on places like public forums and in blog 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 your 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 significant 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 proper backups 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 which 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 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 a wide range of 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. These users can each have a different Desktop layout and background wallpaper, different settings, and different personal folders all stored separately and without impact on or access to each other. However User Accounts are not solely designed for sharing purposes; even if there is only ever one user of the machine, you will still need to know about User Accounts for security reasons.

When you first install Windows 7, a default User Account with Administrator privileges is created using the username and optional password you choose just prior to finalizing installation - see the Windows Installation chapter. 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. This first User Account is actually called the Protected Administrator, and to understand the significance of this and other aspects of User Accounts, you need to read this chapter.

< USER ACCOUNT TYPES

There are different levels of privileges given to User Accounts, depending on their type. In Windows 7 there are three main types of User Accounts: Guest, Standard and Administrator. Each has different privileges:

Administrator: This User Account type can undertake the full range of actions in Windows, from installing or uninstalling any software or hardware, making system-level changes, to viewing the files and folders of other User Accounts on the system (if they are not password-protected accounts). Administrators can also create, change or delete new or existing 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 forces you to create one during the Windows Installation process.

Protected Administrator: The default Administrator level account is actually known as a Protected Administrator (PA), and the key reason for this name is because User Account Control (UAC) restrictions apply to the PA. If UAC is enabled, then the PA is set by default to Standard level privileges, and can only undertake Administrator level tasks by confirming UAC prompts - see the User Account Control section of the PC Security chapter for full details.

Full Administrator: While UAC can be disabled, there is actually a Full Administrator account, known as the Administrator Account, which is hidden and disabled by default, and is not affected by UAC settings, does not have a password, and has 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 default Administrator account is leaving a major security hole open. The primary use for this account would be for troubleshooting purposes, such as resetting a forgotten password on the Protected Administrator account.

Standard: This User Account type lets the 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 User Account files and folders, and deleting or altering critical system files. If User Account Control is enabled, a Standard user can remove these restrictions at any time by entering the password for an Administrator level account when prompted by UAC. In practice a normal 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 allowing very basic and temporary access to your machine. 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 logoff the Guest account, all data in the profile is also deleted. This means that there is minimum potential for them to do any harm to your system, although it is not recommended that you grant an untrusted user even this 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. Unless you are going to actively use this account type, it is strongly recommended that you leave the Guest account disabled.

The reason there are different types of User Accounts is 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 others' 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 account (i.e. the Protected Administrator), since by default you only have Standard user privileges until you click a UAC prompt to escalate those privileges to 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 major 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.

< USER ACCOUNT SCENARIOS

This section contains my advice on how to set up User Accounts on your system based on four common scenarios. When you are setting up User Accounts in Windows, you must first decide on how many people you want to provide access to your machine, and also consider whether the PC is readily accessible by others or is relatively isolated from physical access. The number of users is an obvious factor, but the second variable has to do with the fact that a PC which can be physically accessed by other people you don't necessarily trust requires much tighter security than one which is physically isolated. Below are my recommendations for the main general scenarios which are possible and the best way to configure one or more User Accounts to suit:

Single user, isolated machine: If the PC only has one main user and is not physically accessible by untrusted individuals then the default Protected Administrator User Account created by Windows during installation is sufficient. For maximum convenience you may also wish to leave this Administrator level account without a password, which provides the fastest startup into Windows as you won't see a login screen.

Single user, accessible machine: If the PC has only one main user but other people who are not necessarily trustworthy can physically access it, or you are worried about sensitive information and potential theft, then the default User Account created by Windows is still sufficient, but you must assign a strong password to the account - see the Backing Up & Restoring Passwords section of the Backup & Recovery Chapter for details of how to generate a strong password and back it up safely to prevent loss. This password will need to be entered at the login screen each time you start up Windows, and as long as the password is quite strong, will prevent anyone else from gaining access to your machine. However there are ways of cracking such passwords if a person has physical access to the machine, so you may also wish to also use EFS Encryption and/or BitLocker Drive Encryption if the data is very valuable and/or the threat of physical access or theft is quite high - see Encrypting File System and BitLocker Drive Encryption sections of the PC Security chapter.

Multiple users, isolated machine: If the PC has more than one user but is only physically accessed by trusted people such as close family members then I recommend creating a Standard User Account for each of the additional people who will be using the machine, and keeping the default Protected Administrator account for yourself to use. However importantly you must now use a password for your Administrator account and you must also enable UAC. Aside from malware risks, a password and UAC are required to prevent the other User Accounts from making system-wide changes which may destabilize or harm the PC, and it also allows you to use the Parental Control features detailed further below. The Standard accounts themselves don't have to have passwords, but it is recommended that they do in case one user accidentally or purposely logs in under another user's account and accesses sensitive data or makes undesired changes. Furthermore Standard accounts which don't have passwords can have the contents of their personal folders viewed by Administrators; if password protected, personal folders cannot be viewed by anyone else. By virtue of having more than one User Account on the machine, you will see a login page each time you start Windows, allowing anyone to choose which user to login as, as long as they enter the appropriate password if required.

Multiple users, accessible machine: If the PC has more than one user, and is also physically accessible by a range of people some of whom you may not completely trust, or there is greater risk of theft, then I recommend the same procedures as the scenario above, however the Administrator password must be made very strong, and the Standard account passwords should also be made quite strong. Individual users may also wish to use EFS encryption for their sensitive files or folders. In addition, if you want to allow an untrusted person limited access to your machine (e.g. for basic web browsing), then turn the Guest account on as well and ask them to use that. UAC must be enabled at all times in this scenario for maximum protection against unauthorized changes and to prevent malware. It is also recommended that you supervise the use of the PC by any untrusted individual(s), as there is still a possibility that using certain tools they can crack the Administrator password and hence have unrestricted access to your machine.

Note that on a PC with multiple user accounts, you can quickly switch between accounts without restarting the machine by pressing CTRL+ALT+DEL and selecting 'Switch user', or by clicking the Start button, clicking the small arrow next to the Shutdown option and selecting 'Switch user'. You can also go back to the main logon screen by selecting 'Log off' instead of rebooting.

For more details of how UAC works, and for details of additional ways to customize UAC to suit your specific needs, see the User Account Control and Local Security Policy sections of the PC Security chapter. I also urge you to check the Backing Up and Restoring Passwords section of the Backup & Recovery chapter for details of how to create, backup and protect against password loss or theft. There are a range of techniques which people can use to crack your system if they have physical access to it, so the single most important thing you can do to prevent a breach of your security and privacy is to restrict physical access to your PC only to trusted individuals, and supervise untrusted individuals closely. On the other hand, the use of separate User Accounts and enabling UAC for scenarios where only trusted family members have physical access to the PC is more than sufficient to ensure security and privacy if all accounts are password protected.

< MANAGING USER ACCOUNTS

Once you've decided on the best strategy, you will need to create, delete or modify existing User Accounts to suit your needs. This is done by first logging in as the default Protected Administrator account, then going to the main User Accounts screen. Here you can either edit your own account, or by clicking the 'Manage another account' link you can edit the details of any other accounts on the system. Below are the typical range of options shown when managing another account:

Create a new account: This allows an Administrator to create a new account, assigning it a name and an account type. Only create as many additional Standard 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 purpose. Note that an Administrator can view the files and folders of other users who don't use a password by going to the *\Users* directory in Windows Explorer and looking for the subfolder with that User's account name. Remember also that the more Administrator level accounts you have, the more likelihood there is that a user can cause unintended harm to the system, or breach another user's privacy, or inadvertently allow malware onto the system. For that reason it is best not to have more than one active Administrator account on the system - the Protected Administrator account. Be sure to also disable the Guest account until you actually need it.

Change the account name: You can change an account name at any time if you are an Administrator, including your own. However aside from causing confusion at login time, it also causes further confusion because the actual name of the personal folder for the user 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 additional problems, since 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 the Advanced Settings section later in this chapter.

Delete the account: You can delete any account except your own by highlighting it and selecting 'Delete the account'. This is obviously something that should done with caution, since deleting an account not only deletes all that account's saved preferences, it can also delete all 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, but note that you will not be able to save their emails and personal settings this way. You should delete all unused User Accounts on your system if you are sure they will not be needed again.

Create a password: If an account doesn't have a password and you need to create one then select the account, click this link, and enter an appropriate password. Any User Account with a password cannot have its files and folders accessed by other users. Importantly, if you lose or forget the password for an Administrator account you will need another Administrator on the same machine to help you; if another Administrator doesn't exist you will be in serious trouble - see the Backup & Recovery Chapter for recovery options. If a Standard user forgets their password, an Administrator can click the 'Change the password' or 'Remove the password' links as appropriate to fix this. However removing a password also removes access to any password-protected resources for that account, such as EFS encrypted files. To change your own account password at any time press CTRL+ALT+DEL and select 'Change a password'.

Change the picture: Each User Account is represented by a small picture on the login screen and at the top of the Start Menu among other places. This picture makes it easier to quickly distinguish between different accounts. Select one from the list shown, or to use your own custom picture click the 'Browse for more pictures' link at the bottom of the images and find an appropriate image on your drive(s) to use - it must be in .BMP, .PNG, .GIF or .JPG format. Note that you can quickly open the User Account properties window by going to the Start Menu and clicking this picture.

Change the account type: An account can be changed from Administrator to Standard user and vice versa, though this is obviously something which should be done with some consideration. In particular I don't recommend changing the first default Protected Administrator account created under Windows to a Standard user.

< PARENTAL CONTROLS

Parental Controls can be accessed directly through the Windows Control Panel, or via the 'Set up Parental Controls' option under the 'Manage another account' section of User Accounts. 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. Parental Controls was introduced in Vista and continues to be a handy tool in Windows 7 for addressing these situations. However Parental Controls is not just for controlling children; it allows you to lay down additional limitations on any Standard User.

On the main Parental Controls screen you will see all available User Accounts on the system including your own. To customize Parental Controls for a user, you must first select their User Account, and importantly, your Administrator level User Account must have a password for Parental Control 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 to enable Parental Controls for this user. Then adjust the various settings as described below:

Time Limits: Allows you to set the hours within which the selected User Account can 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. To apply any time restrictions select any periods you wish to block and click OK. When the user attempts to log in during these periods they will see a message explaining that due to time restrictions they cannot log on and should try again later.

Games: This area lets you select firstly whether the user can play any games at all, and then you can block games with particular ratings - these should be set to match your local region's rating scheme. You can also choose either to allow or block unrated games, since some (mainly older) games may be unrated regardless of their content type. Furthermore you can manually specify which of the existing games installed on the system you wish to block or allow.

If enabled, the user's activity will be logged. You can view these logs here by clicking the 'View activity reports' link at the right of the screen. You can see more details by browsing the log categories in the left pane.

Allow and block specific programs: If you wish to block the user from being able to run particular programs, click the '*[user]* can only use the programs I allow' option and then select from the list of all installed programs shown. If a program file is missing from the list, click Browse and go to its directory then select it.

WINDOWS LIVE FAMILY SAFETY

Microsoft has removed the web filtering and activity reports features of Parental Controls, previously available under Windows Vista. You must install additional software to enable this functionality as detailed in this Microsoft Article. I recommend Microsoft's free Windows Live Family Safety software which provides web filtering and detailed activity reports functionality. However unlike Windows Live Mail or other Windows Live software recommended in this book, Windows Live Family Safety requires that you log in with a valid Windows Live ID before you can use the software, because it is an online-oriented tool. If you do not have such an account, you can create one for free here.

To install Windows Live Family Safety, download from the link provided above and run the installer. In the window which appears select only the 'Family Safety' component and click Install. Once completed, untick the boxes at the end of installation to prevent your default search provider or homepage from being changed, then click Continue. If you are prompted to Sign Up with a Windows Live ID and you already have a Live ID, you can skip this step and click Close; otherwise sign up for one as it is necessary.

To open and use Windows Live Family Safety go to Parental Controls and click 'Select a Provider' box and make sure 'Windows Live Family Safety' is chosen. When you then select a user in Parental Controls, you will be prompted to login to Windows Live Family Safety. Enter your Windows Live ID details to continue, or if you don't wish to use the additional features, click the red X at the top right of the login window to access the normal Parental Controls options. You can also access Windows Live Family Safety directly at any time by going to Start>Search Box, typing *Family Safety* and pressing Enter.

Follow these steps to configure the additional settings enabled by Windows Live Family Safety:

1. There is only one account required to login to Family Safety, and this account is considered to be the Parent. Other Windows Live IDs may be required, for example to manage your children's email access through the Contact Management setting.
2. Once you log in, you will be prompted to select which accounts are being monitored. Select all relevant accounts by placing a tick in the 'Monitor account' box next to them. I don't recommend ticking your own Administrator account.
3. Click Save when done.
4. To configure the actual settings for the account(s) being monitored, you will need to click the link shown under 'Customize settings for your family' section. This will open a browser window and automatically log you into the Family Safety online settings area of the Windows Live Family Settings site.
5. Click the 'Edit Settings' link next to the User Account(s) you are monitoring, and for each one you can configure Web Filtering, Activity Reporting and Contact Management - all of which are covered further below.
6. If you wish to remove a user from being monitored, click the Remove link at the bottom of this screen.

Web Filtering: If enabled, there are two preset levels of Internet filtering available here - Basic and Strict. Strict is intended for very young children as only a small number of kids-only sites are allowed. Basic is more appropriate for older children. Alternatively you can select Custom and determine the categories of web content you wish to allow or block. Regardless of which option you choose, you can also manually enter web addresses for particular sites you wish to allow or block, and this list always overrides any other filtering measures currently being applied. You can also tick or untick the 'Allow *[user]* to download files online' to control whether file downloads are allowed from any site. Click the Save button when done to save and apply these settings for this user.

Activity Reporting: If enabled, Activity Reporting allows you to record and display the online and offline activity for this user. The categories of activity recorded are: Web activity, which is browser-based activity; Other Internet activity which covers other types of web access, such as via the built-in updating utilities of a program; and Computer Activity, which records general activity on the current computer, such as the launching of any games or programs.

Contact Management: If enabled, this setting determines the people (Contacts) with which the child can exchange emails or have chat sessions. Your child will need to use a Windows Live Hotmail account for email, and Windows Live Messenger for chat, for these features to be supported.

Requests: The Requests section allows your children to make requests for particular content they want to view, or contacts they wish to add, which are currently being blocked. You can approve or deny the queued requests listed here and they will automatically be blocked or allowed as appropriate.

Once you have completed setting up and saving all relevant settings, you can close the browser window. To access Windows Live Family Safety in the future, you can click the 'Windows Live Family Safety' link which appears in the Parental Controls options when a user is selected, or the relevant Action Center notification which appears in the Notification Area.

When a child attempts to undertake any restricted activity, they will be presented with a blocked message, giving them the option to Email you with a request which will appear under your Requests section in Family Safety, or select the 'Ask in person' option which raises a Parent Approval prompt. To instantly allow access to the blocked resource, the Parent must then enter their Windows Live ID password and click the Approve button, or they can simply click Deny to continue blocking the requested resource.

It is unfortunate that the web filtering and activity reporting features have been removed from Windows and replaced with web-based components. While not a major concern in terms of privacy and safety, given Microsoft has always shown a strong commitment to maintaining both of these aspects for all users, the web interface and need for Windows Live ID and Windows Live-based applications to support all of these features is annoying. You can turn to a third party solution to provide you with web filtering and activity reporting functionality, however the best of these are not free, and certainly don't provide any better privacy guarantees. I suggest you examine the following Windows 7-compatible software packages if you don't wish to use Windows Live Family Safety:

Net Nanny
Safe Eyes

There is no other way of easily restricting or completely disabling Internet access on a per-user basis in Windows 7, particularly as many methods can be bypassed with the appropriate knowledge. You must use one of the software packages in this section if you wish to properly restrict Internet access to a particular User Account.

The built-in Parental Controls are useful not just for children but to also prevent certain users from running specific programs for example if you know that such programs may potentially be harmful or intrusive. Keep in mind that as long as UAC is enabled at its default setting, even if you don't specifically block harmful or intrusive programs, Standard users cannot successfully run any programs which make intrusive changes.

< ADVANCED SETTINGS

This section covers more advanced ways of accessing and manipulating User Account-related settings.

USER PROFILES

Your User Profile is the sum of everything for 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, and you can access a list of these and change them by clicking the 'Configure Advanced User Profile Properties' link in the left pane of the main User Accounts window. 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, 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. 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.

One of the changes 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.

If you wish to change or rename the personal folder to which a particular User Profile is linked, which can be useful if you have changed your account's username for example, you can do so by following 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.
3. Open Windows Explorer, go to the \Users directory and rename the personal folder you wish to change.
4. 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 each one and looking at the `ProfileImagePath` value 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 above to point to the folder you recently renamed. When that user next logs in they will be using this personal folder. Note that renaming the personal folder does not change the name of the User Account and vice versa - see earlier in this chapter for the correct way to rename a User Account.

Advanced User Accounts Control Panel

To access a second, more advanced User Accounts Control Panel, go to Start>Run, type *netplwiz* and press Enter. The options provided here require caution and are for more advanced users - if in doubt do not alter anything. Below are the descriptions for these settings:

Users must enter a user name and password to use this computer: 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 a 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 have two or more User Accounts, you will see a login screen at Windows bootup, and you may also be prompted for a password. To override this default behavior simply select the account you wish to have automatically logging in to Windows from the list shown, untick the 'Users must enter a name and password to use this computer' box, click Apply, and enter any password if applicable. This account will then automatically login each time you start Windows. This is a major security risk and is not recommended unless you are the sole user of the machine and the machine is in a physically secure environment.

Users for this computer: This area lists all the User Accounts on this PC. You can add or remove accounts here, though it is not recommended; you should use the normal User Accounts window instead wherever possible. Highlight an account and click Properties; aside from letting you change the name and description of the account, under the 'Group Membership' tab not only can you select whether to set this as an Administrator or Standard account, you can also select one of the other more specialized groups which have specific limitations. 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 which a Standard user would not otherwise be able to do. However you will need to understand what each of the groups can do - see this Microsoft Article for more details. You can also use the Local Users and Groups Manager to see descriptions for each group - see the Advanced User Management section below for more details. For the most part groups are designed for network administrators not home users.

Reset Password: Allows you to set a new password for the highlighted User Account (if it has one). This is useful if that user has forgotten their password. To change your own password at any time press CTRL+ALT+DEL and select 'Change a password'.

The following options are under the Advanced tab:

Manage Passwords: This option allows you store and backup various passwords in the Credential Manager - see the Backing Up and Restoring Passwords section of the Backup & Recovery chapter for more details.

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 Start>Run, typing *lusrmgr.msc* and pressing Enter. Here you can see and administer individual users on this PC by clicking the Users item in the left pane, and then double-clicking on the particular user you wish to view/alter. Importantly, see the Hidden Administrator Account section below for one useful function of this utility. Similarly, you can 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. Again, this functionality is primarily intended for network administrators. For home users, even those running a home network, the normal Standard and Administrator level accounts are sufficient, given a Standard level account can now perform a range of additional non-intrusive tasks under Windows 7.

Secure Logon: If you wish to have added security, you can tick the 'Require users to press Ctrl+Alt+Delete' box, and thus whenever anyone tries to logon on this PC, they first have to press the CTRL, ALT and DEL keys together to bring up the logon screen; it will not display automatically. This increases security because it places the logon screen in Secure Desktop mode - as covered in the User Account Control section of the PC Security Chapter - meaning the logon screen cannot be faked by malware to capture your login details for example. This level of security is generally not necessary for the average home PC user.

HIDDEN ADMINISTRATOR ACCOUNT

Windows 7 has a hidden built-in Administrator account which is disabled by default. The User Account you create when you first install Windows 7 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 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 PC Security chapter. This makes it an extremely powerful account, but also an extremely 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. 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. If you go to the main User Accounts window under the Windows Control Panel and click the 'Manage another account' link, you can now see the Administrator account showing. When next you start up Windows, if you logoff your current session, or go to the Start button, click the arrow next to the Shutdown button, and click the 'Switch User' option, this account will appear on the login screen and can be logged into just like any other account.

This account is designed for troubleshooting purposes, and for very advanced users who have need of this 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 not designed for daily use by the average home PC user as it is incredibly powerful and does not have much protection against abuse. 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 these reasons you should not enable this account permanently, and most definitely should not use it as your daily account. The main reason you should be aware of its existence is as noted, for temporary use during system configuration or for troubleshooting purposes where you need the highest level of unrestricted access to your system.

Limit the number of User Accounts you make to those you absolutely need, have only one main Protected Administrator account on your system - do not use the hidden Administrator account - and encourage any other users on your system to use passwords to protect their accounts and prevent accidental deletion. If you continually experience issues with a particular User Account and nothing else works, the best solution is to backup the important data from that account, delete the User Account and create an entirely new one and copy back the data into the new personal folders for the account.

PC SECURITY

PC security has become a major issue of concern due to the increase in the number of ways in which the security of the average home PC user can be compromised. Accordingly, Windows Vista saw a marked improvement in security features over Windows XP, and Windows 7 builds on and refines these features as covered in this Microsoft Article. You may find some of these features annoying or confusing, however I strongly advise you not to take the topic of PC security lightly or ignore it. It is extremely important that you become acquainted with both the types of threats to the integrity and privacy of your PC, as well as how the Windows security-related features actually work to counter them.

It is incorrect to suggest that only the very careless or novice user will succumb to a security-related problem or Malware (malicious software) infestation. Even if you consider yourself an advanced user, you need to bear in mind that malware threats these days are becoming increasingly complex and dangerous. In the past a malware infestation would usually result in little to no real harm; you'd have to delete a few files or at worst reinstall Windows or restore a backup. Now however, malware development and distribution is often coordinated by organized crime groups for financial gain, so even a single incidence of malware infestation can potentially result in the loss of money, software serial numbers, email account details, and other sensitive personal information. Having a carefree attitude towards PC security is a thing of the past.

However I do not advocate bogging your system down with security software that runs in the background, slowing things down, triggering software conflicts and crashes. Instead, this chapter explains the various types of threats to PC security and provides a range of important tips for maintaining a secure PC, because education and awareness are the best defense against malware. We examine the built-in tools and features in Windows 7 which deal with these threats, and I also recommend a set of third party software to supplement Windows security measures in a non-intrusive manner with virtually no performance impact.

< SECURITY THREATS

There are a wide range of security threats which Windows 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.

There are different types of malware and security threats, and the major categories of these are covered below:

Viruses & Worms

Viruses are small programs that load onto your computer without your permission and without your 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 once on the new computer. Viruses range from the mischievous to the truly harmful, destroying valuable information through data corruption and causing a range of strange system behaviors.

Worms are similar to viruses, however they generally do not attach to other files, they 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, program. Trojans differ from viruses in that they are used to provide an outside attacker with 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 distributor of the spyware.

ADWARE

Adware is similar to spyware, but is not necessarily malicious, as it is mainly used to target online advertising or create popup ads or redirect/force your browser to view pages with advertising. However again it is usually installed without your full knowledge or permission. Despite it's relatively less malicious nature, this software is still undesirable as it breaches your privacy and uses system resources and bandwidth for no genuinely useful purpose.

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 usage 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. At the same time, a remote attacker can take advantage of the rootkit to access your machine for malicious purposes.

PHISHING

While not a form of malicious software, Phishing is fast becoming a common and significant security threat. Typically it involves fooling unsuspecting users into revealing important personal information such as credit card numbers or passwords. For example a phishing attempt may involve getting you to click a login link in a fake email that appears to be from your bank, which then takes you to an imitation of the bank login page. Entering your login details on the fake page will give the perpetrator all the information they need to then login to your real bank account and rob it. Phishing is not malware as such, since it does not usually involve software infection, it uses social engineering techniques instead to trick and defraud its targets.

The categories above are in no way conclusive or all-encompassing. There are many variants and combinations of the above security threat categories, and more are emerging every day. Over the past few years these types of threats have become ever-more sophisticated, intrusive and malicious. Even relatively tech-savvy users face the risk of picking up a serious piece of malware or even accidentally falling prey to phishing. It may not happen often, but it only takes one serious security breach to result in financial loss or data loss and the subsequent major hassles of having to obtain new credit cards, proving your case to a bank or financial institution, changing all your passwords, contacting software manufacturers for new serial numbers, and so forth. The people behind the creation of these security threats are making large sums of money from doing this, so they have the resources and the incentive to constantly adapt to existing malware defenses and innovate new and ever-more-intrusive forms of malware and online scams.

Protecting yourself against these security threats is not as simple as installing lots of malware scanners and turning them all on. Aside from draining performance, causing software conflicts and other system issues, malware scanners often lag behind in the detection of new security vulnerabilities and exploits. The best defense against malware is a combination of correctly configuring built-in Windows security features, using appropriate third party security software, and most importantly, being educated and vigilant, and understanding your own system. This is one of the reasons I urge users to learn about how Windows and their PC works, because people who gain an intuitive understanding of the fundamentals stand a much greater chance of avoiding a security breach.

The rest of this chapter contains the tools and methods you can use to counter a wide range of security threats, starting with the security features built into Windows 7.

< WINDOWS ACTION CENTER

The Windows Action Center is the replacement for the Windows Security Center in Windows XP and Vista. Action Center is a central location for Windows to provide a range of alerts, and for users to quickly access several Windows features. 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; the other types of alerts are not as important if not acted upon and can be accessed in other ways.

Action Center can be opened through the Windows Control Panel, by going to Start>Search Box, typing *action center* 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, and you will see the specific features being monitored. These include: Windows Firewall, Windows Update, Windows Defender, Internet Explorer security settings, User Account Control and Network Access Protection - these Windows features are all covered in detail under relevant sections throughout this book. The status of each of these features is displayed here, e.g. On, Off, OK or Not Found. Where Windows considers any of your settings for these features to be less secure than it recommends, specific warnings will be shown in large yellow or red boxes at the top of the section. This is not necessarily cause for alarm.

SECURITY CATEGORIES

Aside from Windows Update, which is a specific Windows feature, the other categories Action Center monitors are broader than may first appear:

Network Firewall: This category monitors whether a software firewall is installed and enabled. I strongly advise against running without an active software firewall in Windows. Since Windows 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, turn one of them off.

Windows Update: This category monitors only 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 automatic updating by Windows Update to be less than ideal, and will raise a warning here. You can safely disable this warning by clicking the 'Turn off messages about Windows Update', as long as you don't completely disable Windows Update at any point, which is definitely not recommended.

Virus Protection: Windows uses the term Virus in a general sense, as people have come to know the term to not only apply to actual viruses, but similar types of malware such as worms or trojans. So virus protection generally means any of the recognized major anti-malware scanners, which can usually detect a range of malware, not just viruses. Windows does not have a built-in antivirus program, and unfortunately, even if you install the Microsoft Security Essentials anti-malware scanner as covered later in this chapter, if it is not set to the maximum possible settings then a warning will appear here. If you've followed the advice in this chapter and installed the appropriate anti-malware software, configuring it as recommended, and this warning still appears, you can disable it by clicking the 'Turn off messages about virus protection' link.

Spyware and Unwanted Software Protection: This category monitors any general anti-spyware package that is installed and enabled. This includes any major anti-malware packages which also contain this functionality. However because Windows has the built-in Windows Defender anti-spyware software, as long as you enable its real-time protection feature, Windows will consider you adequately protected against spyware and similar unwanted software. Windows Defender is covered in detail later on in this chapter, and there I recommend disabling the real-time protection feature. If you follow the recommendation in this chapter and install Microsoft Security Essentials, it will replace Windows Defender and will still adequately protect you against spyware. In either case, you can safely disable this warning by clicking the 'Turn off messages about spyware and related protection'.

Internet Security Settings: This category monitors Internet Explorer's security settings, such as Protected Mode, the Phishing Filter and general Security Level. If these are not at recommended levels, Windows 7 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 below, and I strongly advise against disabling UAC.

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 standard home user and should be disabled, which it usually is by default.

DISABLING ACTION CENTER

Action Center can be useful as an initial reminder to check various security-related settings and install relevant software soon after installing Windows 7. However over time, once you have bedded down your software configuration and are comfortable with the level of security you have chosen, then for the most part you can disable the prompting behavior of Action Center as it can become quite annoying. You can disable individual prompts from within the Action Center, all the way to removing the Action Center from the Notification Area altogether.

The quickest way to disable the categories for which you don't wish Action Center to alert you is to open Action Center and in the left pane click the 'Change Action Center Settings' link. Here you can untick the specific categories for which you do not want Action Center to alert you, then click OK. There are also maintenance and troubleshooting message settings you can alter, and these relate to the Windows Backup feature which is covered in the Backup & Recovery chapter, as well as the Troubleshooting feature covered under the Troubleshooting section of the Performance Measurement & Troubleshooting chapter.

To control the way in which Action Center prompts appear in the Notification Area, go to the Windows Control Panel and select the Notification Area Icons component. 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 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 Control Panel.
- Only show notifications - This hides the Action Center flag icon, however alerts will still pop up in the Notification Area periodically.

To effectively disable the Action Center prompting behavior completely, select 'Hide icon and notifications' above. You can also prevent it from actively monitoring security-related settings by disabling the 'Security Center' Service - see the Services chapter for details. This is only recommended if other methods of disabling Action Center notifications don't work and you are an advanced user.

< 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 7 continues with this concept, known as User Account Control (UAC), and now provides greater control over the way in which it is implemented.

The reason Administrator access to a system may need to be restricted is that a user logged in with a full 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 User Accounts. It uses various tricks to get itself installed, often quietly in the background, and hence gains unrestricted access to your system. Malware aside, running as an Administrator also means that you may inadvertently make various undesirable system changes without being aware of their potentially disruptive nature. 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 a Protected Administrator account.

THE UAC PROCESS

A simple walkthrough of the User Account Control process at the default UAC settings in Windows 7 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 - see Customizing UAC further below for details.:

Step 1 - To begin with, 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 may require that Administrator credentials be provided before proceeding. If this is the case, a UAC Elevation Prompt will appear.

Step 3 - When a UAC prompt is displayed, the important aspects of the prompt you should note 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.

§ *Prompt Background Color:* The UAC prompt will have a background color corresponding to the potential level of risk involved, whether 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 account on the system before you can continue. If you are already logged in with an Administrator-level 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 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:* The details of the program to be launched is 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 - i.e. 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 altered or 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 which existed prior to its implementation, UAC by itself is not 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. However the presence of UAC has been shown to have increased security and resilience to malware in Windows Vista, and continues to do so in Windows 7 as well. 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 barrier against malware, and can still be quite effective against many types of malware and exploits if used properly. Below are some tips for determining whether software is potentially risky by examining the UAC prompt more closely:

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 something relatively simple or purportedly non-intrusive to require unrestricted access to your system. This does not mean that a program or file which does is malicious, but it is certainly the first 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.

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 which can destabilize your system or make undesirable changes to it. Consider whether you really need to install or launch the program, as the more of these types of programs you have on your system, the greater the potential for problems regardless of 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 7 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, however 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's simply a case of the lack of a verified digital signature on the application, but it still bears investigating 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.

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 or existing application is cause for undertaking further research and ensuring that (a) you have downloaded the application or file from a trusted source, and (b) that you scan the download with at least one of the malware scanners covered later in this chapter. You should never see a red background when launching an application or file; this is a major warning sign and the program and its files are best deleted, 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 a glance they may appear identical, 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 Google research. A program should not have duplicate primary executables with identical names, especially if one has a verified digital certificate and the other doesn't, or one exists in a secure directory location and the other doesn't.

Digital Signature: Digital signatures are covered in detail 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 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 research.

UAC is not a replacement for common sense and it is not an 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 and thus maybe you should reconsider, 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 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 and system-wide Registry locations:

§ *\Program Files*
§ *\Program Files (x86)*
§ *\Windows*
§ *\Windows\System32*
§ `[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 users with insufficient privileges from potentially harming the system, but still allows them to install and use many types of software.

However this is not a foolproof solution. Some older applications and games 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, but they will not install properly and/or will fail to launch or function properly.

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 and click OK. Alternatively if that option is not available, go to the main Shortcut tab for the program's launch icon and click the Advanced button, then place a tick in the 'Run as Administrator' box. Only do this if you know and 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 and/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 be 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. There were advanced methods of customizing UAC beyond this, however they required editing the Windows Registry or having access to the Local Security Policy utility which only existed in the more expensive editions of Windows Vista. In Windows 7, all users now have the ability to easily customize UAC to better suit their needs through a graphical user interface. However it should be understood 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. There are four preset levels for UAC, and each is covered in more detail below from the top of the slider to the bottom:

Always Notify Me - This setting is the maximum possible, and equates with the default UAC setting in Windows Vista when UAC was enabled; namely UAC will prompt you whenever any software attempts to make system-intrusive changes, as well as whenever you attempt to change certain Windows settings. This provides the best security but can be annoying, especially when you first install Windows 7 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 certain 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 some 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 7.

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 actually another important barrier against having a UAC prompt faked or manipulated in such a way as to deceive you into willingly 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 some other type of glitch. Selecting this option reduces your security further, and given the relatively infrequent appearances of the UAC prompt when the Default option is chosen, even a slight delay in showing the Secure Desktop is hardly a major inconvenience.

Never Notify - This option effectively disables UAC. It also automatically disables additional Windows protection features related to UAC, such as Internet Explorer's Protected Mode, which results in a major reduction in security for Internet Explorer users. UAC prompts will not appear under any circumstances; all programs will have unrestricted access to your system. It is the least secure option and it is strongly recommended that no user - whether novice or advanced - select this option.

I recommend the default option for UAC in Windows 7 as a good balance of security and convenience. However it must be used in conjunction with a range of other PC 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 Professional, Ultimate or Enterprise editions of Windows 7 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 Start>Search Box, type *secpol.msc* and press Enter. The options we want to examine reside under the Local Policies>Security Options folder. These are shown in the right pane, all of them begin with the words 'User Account Control', and are detailed below:

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 - see the Advanced Settings section of the User Accounts chapter for details.

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 the 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 which triggers a UAC prompt.

Detect application installations and prompt for elevation: If Enabled, Windows will attempt to detect an application 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 don'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 which 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 options above are necessary for UAC to work effectively, and are designed for Network Administrators operating under various environments where UAC may hinder specific functionality.

If you run Windows 7 Starter, Home Basic or Home Premium, there is no Local Security Policy Editor or Local Group Policy Editor, so you will instead need to access the Windows Registry directly if you want to customize UAC as covered above. Remember that this is not necessary, since under Windows 7 the main UAC settings are available for everyone to change, but details are provided here for completeness. All the main UAC settings are held under the following location when using Registry Editor:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
```

The following settings may not exist, so you will have to create each of them as a new DWORD as required. The names of the settings described further above are reproduced below along with the relevant Registry entries and the valid values that can be assigned to them. Note that entering the value using Hexadecimal or Decimal view makes no difference as all the possible values are below 10:

Admin Approval Mode for the Built-in Administrator account:

```
FilterAdministratorToken=0
```

Set to 1 to enable, 0 to disable.

Allow UIAccess applications to prompt for elevation without using the secure desktop:

```
EnableUIADesktopToggle=0
```

Set to 1 to enable, 0 to disable.

Behavior of the elevation prompt for administrators in Admin Approval mode:

```
ConsentPromptBehaviorAdmin=5
```

Set to 0 to elevate without prompting, 1 to prompt for credentials on secure desktop, 2 to prompt for consent on secure desktop, 3 to prompt for credentials, 4 to prompt for consent, and 5 to prompt for consent for non-Windows binaries.

Behavior of the elevation prompt for standard users:

```
ConsentPromptBehaviorUser=3
```

Set to 0 to automatically deny elevation requests, 1 to prompt for credentials on secure desktop, and 3 to prompt for credentials.

Detect application installations and prompt for elevation:

```
EnableInstallerDetection=1
```

Set to 1 to enable, 0 to disable.

Only elevate executables that are signed and validated:

```
ValidateAdminCodeSignatures=0
```

Set to 1 to enable, 0 to disable.

Only elevate UIAccess applications that are installed in secure locations:

```
EnableSecureUIAPaths=1
```

Set to 1 to enable, 0 to disable.

Run all administrators in Admin Approval Mode:

```
EnableLUA=1
```

Set to 1 to enable, 0 to disable.

Switch to the secure desktop when prompting for elevation:

```
PromptOnSecureDesktop=1
```

Set to 1 to enable, 0 to disable.

Virtualize file and registry write failures to per-user locations:

```
EnableVirtualization=1
```

Set to 1 to enable, 0 to disable.

UAC and the Language Bar

In some instances when a UAC prompt appears, the Language Bar will also appear at the top of the screen. 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 for any reason 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 account all the time and the security of running a Standard Account.
- UAC is perfect for people wanting to have multiple accounts on the same PC. By setting these accounts as Standard Users and enabling UAC, they cannot install harmful software or change system settings, but due to Virtualization can still install and use most non-intrusive software normally and without impact on the other users. In fact the default UAC setting in Windows 7 now allows a wider range of Windows settings to be altered without an Administrator or Standard user experiencing a UAC prompt.

On balance there is no reason for anyone, especially advanced users, to disable UAC. The default UAC setting in Windows 7 has reduced the annoyance of UAC while still maintaining its ability to provide some extra protection from malware, and importantly, prompt you to consider whether the software you are about to install or run may be suspicious or unduly system intrusive and worth investigating further.

Make sure to also read the User Accounts chapter for relevant details before considering any changes to UAC settings.

< 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 the files and folders under your personal folders should belong to you, and are free for you to alter 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. Right-click on the file or folder and select Properties; in the Registry Editor, right-click on the key and select Permissions.
2. Under the Security tab, click the Advanced button.
3. Under the Owner tab of the Advanced Security Settings box click the Edit button if available; if not skip to the next step.
4. Check to see if your User Account, usually denoted by *[Username]*-PC, is listed and can be selected - if so, skip to Step 6; if not see the next step.
5. Click the 'Other users or groups' button and enter your username in the box shown, and click the 'Check Names' button to provide the correct username format, then click Ok.
6. Highlight your User Account, and tick the 'Replace owner on subcontainers and objects' box if you wish to also take ownership of any subfolders and objects within a folder, then click the Apply button to change ownership and click OK.

To then make 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. Right-click on the file or folder and select Properties; in the Registry Editor, right-click on a key and select Permissions.
2. Under the Security tab, in the top box you can highlight individual users or groups and in the bottom box you will see tick marks corresponding to the various permissions granted 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 box 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 access to read, write and execute a file, highlight your username, tick the 'Full Control' box under the Allow column, click the Apply button and click OK.

You now have full control over the file, folder or Registry key as though you created it yourself, and can alter or delete it as you wish, though obviously this brings with it a range of risks, which is precisely why you were restricted from easily accessing it in the first place.

Given the system has to check permissions for every file and folder, it is better for system performance purposes to assign permissions to groups rather than specific users wherever possible, and for security purposes, do not give yourself ownership and full permission over general system folders such as *Windows* and 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 manually.

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 they don't originally own. 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 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 - this is the same as the value 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 more 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 hidden unrestricted Administrator account as covered in the Advanced Settings section of the User Account chapter.

< WINDOWS DEFENDER

Another layer of protection included in Windows is Windows Defender. The primary aim of this program is to provide basic protection against spyware, as this is one of the most common types of malware found on the average PC, and can compromise important personal information such as online banking login passwords and credit card numbers. Windows Defender can also find other common forms of malware including adware and rootkits, but it is not completely effective in finding all types of malware so it should definitely not be relied upon as the sole anti-malware scanner on your system.

Windows Defender is on and running in the background by default in Windows 7, but to access its full user interface, go to the Windows Defender component of the Windows Control Panel. I recommend that you leave Windows Defender enabled, but configure it to be less intrusive as detailed below.

Note that if you are going to install Microsoft Security Essentials as recommended later in this chapter, then you can skip the entire Windows Defender section because Windows Defender is automatically disabled and replaced by Microsoft Security Essentials. Only follow the instructions below if you wish to leave Defender enabled alongside other third party malware scanners:

Configuring Windows Defender

Below are details on the range of options and features in Windows Defender, including relevant recommendations:

Home: Takes you to the main Windows Defender screen where you can see the current status of your machine, whether any scan is running, whether Real-time protection is enabled, and when the last and next scans are scheduled to be undertaken. The Antispyware definition version is important - do not allow the Windows Defender definition file to be too old, regularly update the definition file through Windows Update.

Scan: When clicked, this option starts a Quick Scan of your system by default, going through your important system files, folders and the Windows Registry to look for traces of spyware. By clicking the small down arrow next to the Scan button, you can manually choose to do a Quick Scan, Full Scan or Custom Scan. As noted, a Quick Scan focuses on your system files and folders, taking the least amount of time to complete, but also providing the least security. A Full Scan goes through your entire PC to look for traces of malware, which is more secure but can take quite a bit longer. A Custom Scan allows you to select the specific drive(s) and/or folder(s) you wish to scan. You should run a Full Scan of Windows Defender in conjunction with other scanners every week or so, and also if you suspect you've actually been infected. A custom scan of any downloaded files is also recommended as required.

History: This section displays a history of any recent actions you've taken in response to Windows Defender notifications. Click the View button to see the list, and click on any item displayed to see more details of the exact file(s) involved.

Tools: This section contains several important settings and tools:

§ *Options:* Allows you to configure how Windows Defender works, and contains a range of sections:

Automatic Scanning - I recommend disabling Defender's automatic scans of your PC. If you wish to leave this enabled, a Quick Scan should be sufficient as this usually only takes a few minutes at most and is useful if you forget to manually run any malware scanners often. If you wish to leave automatic scanning enabled, then I recommend ticking the 'Check for updated definitions before scanning' so that it uses the latest definition file, as without the latest definition file it's pointless to scan your system regularly; I also recommend ticking the 'Run a scan only when the system is idle' box to ensure that Defender doesn't begin a scheduled scan while you're undertaking another task.

Default Actions - The default actions listed allow you to specify what you want Windows Defender to do when it finds potentially malicious software in various categories of risk. There are four categories of risk: Severe, High, Medium and Low. A Severe or High risk is for malware which may collect your personal information and/or damage your Windows installation; a Medium risk is for programs which generally breach your privacy and may alter your Windows settings; a Low risk is for potentially unwanted software which may be harmful but is a low-level threat. The default action for each of these categories is 'Recommended action based on definitions' which means that if found, Windows will recommend a particular action based on the information in its definition file. For Severe or High risk malware, Windows recommends its immediate removal; for Medium or Low risk malware, Windows will give you the option to remove or block it. This default is fine to use, because Defender will not do anything without first getting your consent. However if you tick the 'Apply recommended actions' box, Windows Defender will automatically apply its recommended actions to your software - I recommend against ticking this box to avoid seeing your software removed without your consent.

Real-time Protection - These options allow you to determine which types of activities and areas Windows Defender constantly monitors in the background to prevent spyware from installing or executing on your system. The performance impact of having real-time protection is minimal, and hence all these options are best left enabled for novice users. Intermediate and advanced users can choose to enable real-time protection but untick the 'Scan programs that run on my computer' box, leaving the 'Scan downloaded files and attachments' box ticked. This should have virtually no performance impact, since Defender will only scan a file or attachment which is downloaded, and not constantly scan in the background during normal system usage, which could have an adverse performance impact.

Excluded Files and Folders, Excluded File Types - These two sections allow you to specify particular files, folders or file types which 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 may allow malware to slip past Defender. However if you know for certain that a particular file, folder or file type is going to be picked up as a false positive (i.e. falsely detected as malware when it is not), then you can include it here.

Advanced - There several options here to further customize Defender's behavior. 'Scan archive files' if ticked allows Defender to scan inside archived files such as .ZIP, .CAB and .RAR archives. I recommend ticking this option as malware can easily hide inside such files. 'Scan e-mail' if ticked scans for any attachments to emails which may be malicious. I recommend ticking this option as this is a common form of distribution for malware. 'Scan removable drives', if ticked, scans any removable drives such as USB flash drives when they are attached to the system. This is an extra form of protection, however ticking this may cause additional delays when you attach such drives, so untick it if this bothers you. 'Use heuristics' if ticked attempts to use additional but less precise methods to attempt to detect malware which may not otherwise be detected using the Defender definitions file. I recommend ticking this option to improve the chance of catching new malware, but bear in mind that it can also result in more false positives. 'Create 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 strongly recommend ticking this option to provide added protection against unintended system changes by Defender.

Administrator - If you are using an Administrator User Account, you can choose to completely turn off Windows Defender by unticking the 'Use this program' box. This will prevent all Windows Defender functionality from running, it will also set the 'Windows Defender' service to Manual and stop it (the default is Automatic (Delayed Start)) - see the Services chapter for more details. The only time I would recommend disabling Defender is if you know it is causing a conflict with your other software and you also have at least one other anti-spyware scanner installed. Also as noted at the start of this section, Windows Defender is automatically disabled if you install Microsoft Security Essentials, which is fine. You can display the History, Allowed and Quarantined items for all users under the History section of Defender if you tick the 'Display items from all users of this computer' box. Click the Save button when finished here, and you will be taken back to the main Tools and Settings screen for Defender.

§ *Quarantined Items:* Shows any items which have been caught as suspected spyware and allows you to determine what to do with them.
§ *Allowed Items:* Lists the items which have been flagged by Windows Defender as potential malware but which you have manually chosen to allow to keep on your system.

The remaining items provide links to Microsoft services and resources related Windows Defender and malware in general. Note that the Software Explorer function which used to exist within Windows Defender in Windows Vista has been removed in Windows 7, and is not available here nor anywhere else. See the Startup Programs chapter for alternative tools you can use for the same functionality.

WINDOWS DEFENDER CACHE

The first time Windows Defender is updated with definition files and runs itself after installation of Windows, it will perform a scan of your system to identify system files that don't require scanning in the future. It creates a system file cache called *MpSfc.bin* under the *C:\ProgramData\Microsoft\Windows Defender\Scans\History\CacheManager* directory. This cache is necessary for Windows Defender to perform optimally. If the cache doesn't exist for some reason do the following:

1. Open an Administrator Command Prompt.
2. Type the following command exactly as shown and press Enter:

```
"%programfiles%\Windows Defender\MpCmdRun.exe” –BuildSFC
```

In general you should not need to manually create or access the Defender cache.

DISABLING WINDOWS DEFENDER

If you are absolutely certain that you do not want Windows Defender running on your system, you can disable it as follows:

1. Open Windows Defender as an Administrator.
2. Click the Tools button, click the Options link, and click the Administrator item.
3. Untick the 'Use this program' link and click Save - this will close down the Windows Defender interface, stop the Windows Defender service, and set the service to Manual so it doesn't launch again at next reboot.
4. Go to the Services component and set the Windows Defender service to Disabled if you want to make absolutely sure it doesn't enable itself in the future. See the Services chapter for more details of how to change a service.

If at any time you want to re-enable Windows Defender, set the Windows Defender service to 'Automatic (Delayed Start)', then go to the Windows Defender component in the Windows Control Panel and click the 'click here to turn it on' link.

Once again, if you install Microsoft Security Essentials as recommended later in this chapter, it automatically disables Windows Defender. In this case it is absolutely fine to leave Defender disabled, since Defender's functionality is incorporated into Microsoft Security Essentials.

Windows Defender must be viewed in the context of being a built-in tool designed to provide basic protection against the most common form of malware with a substantial risk of causing harm to the user through invasion of privacy, loss of personal data, and undesirable system behavior. Many Windows users will never be fully aware of the danger of malware nor use appropriate precautions, so having Windows Defender built into Windows 7 and enabled by default provides a good level of basic protection with no discernable performance impact. For advanced users I recommend leaving Defender enabled if you don't install Microsoft Security Essentials, but scale back its presence as covered further above, relegate its background functionality to scanning only when it detects that you have downloaded a file or email attachment, as well as using it for manual scans of your system if you suspect it may be infected with malware. Of course this must be supplemented by all the other measures covered in this chapter, as Defender by itself is completely insufficient as the only form of defense against malware.

< WINDOWS FIREWALL

To help protect your system against intrusion through your network connection - typically via the Internet - Windows 7 provides a built-in Windows Firewall. The major role for a firewall is to prevent unauthorized or malicious network traffic into or out of your system. For example if spyware or 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. However 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 can check its documentation to find out more about this feature.

To access the Windows Firewall go to the Windows Firewall component of the Windows Control Panel, or go to Start>Search Box, type *windows firewall* and you can either choose the basic Windows Firewall or the Windows Firewall with Advanced Security. 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: 'Home or work (private) networks' and 'Public networks'. These network locations relate to the choice of location you made when first installing Windows 7, 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 using, the Windows Firewall in Windows 7 now allows multiple active firewall configurations, one for each separate location. For example you can be connected to a home network and use one set of Windows Firewall settings for that network connection, while browsing the web from your machine using another set of firewall rules for the Internet connection. For most home users who are not on more than one location at any time, the network location you are currently using will be the one for which the Windows Firewall will show the full details, 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 in the left pane 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 unless you have a 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, not both at the same 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 for your network location, as well as any icons shown. If the color is green, the Windows Firewall is enabled, while red means the Windows Firewall is disabled. Choosing to block connections beyond the default settings will also display an appropriate 'blocked' icon.

Incoming Connections: Click the 'Change notification settings' link in the left pane 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 a program or feature through Windows Firewall' link in the main Windows Firewall window. This provides a full list of the default Windows programs and features allowed to communicate freely through the Windows Firewall, as well as any programs which you have 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. However at any time you can select a program or 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 Google. 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, the 'Notify me when Windows Firewall blocks a new program' box if ticked will enable the behavior described above - namely 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 blocked by the Firewall and hence it may not function properly, so make sure you leave this box ticked.

ADVANCED CONFIGURATION

For most users the main Windows Firewall window provides all the settings they need to access. However for more advanced users who have need of greater control over the firewall, you can access the Windows Firewall with Advanced Security interface in one of two ways: go to Start>Search Box, type *windows firewall* and select the 'Windows Firewall with Advanced Security' item; or in the normal Windows Firewall window click the 'Advanced Settings' link in the left pane. A new window will open which allows much greater customization and monitoring of the Windows Firewall, including allowing you to configure the blocking of outgoing network traffic, something that was not available in the Windows XP firewall.

Covering all 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.

In the main Overview box, 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. 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. 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. Here you can select to also 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, as by default 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 through the firewall. 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.

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 existing 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, 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 Internet access while at the same time preventing any suspicious applications on your machine from communicating with the outside world. However 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 Start>Search Box, type *secpol.msc* and press Enter. However this tool is only available on the Professional, Ultimate and Enterprise editions of Windows 7. This is because it is a tool primarily designed to allow Network Administrators to be able to impose certain limitations on the users of a network, so many of the settings are not relevant to the average home PC user and won't be covered here. Furthermore some 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 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, 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 creates a bigger security risk for example. 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: These settings control what happens when a user is locked out of their User 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 from using the account. This provides tighter security against other users attempting to crack a User Account through repeated login attempts, and these settings should only be changed if you are in a less physically secure environment and/or suspect someone is constantly trying to guess an account password.

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 rights 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 the User Account Control-related settings in the User Account Control section earlier in this chapter, so we will look at the rest of the more useful settings below:

- *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 Administrator level 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 with or log your 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 information from the latest sessions, it also slows down shutdown time and is generally not recommended unless you require such a high level of security. 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 problems for users of the system if changed. 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 running malicious code from such memory areas. When it 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 Start>Search Box, typing *systempropertiesadvanced* and pressing Enter. Then 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.

DEP is a highly valuable form of additional protection against malware, and the default setting provides a balance of good security and compatibility. However 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, then you can add them to the exceptions list in DEP.

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.

It is strongly recommended that you do not disable DEP.

< ADDRESS SPACE LOAD RANDOMIZATION

Address Space Load Randomization (ASLR) is not a user-customizable feature of Windows 7, however it is an important built-in security feature and is covered here for the sake of informing you of its role. First introduced in Vista, ASLR essentially randomizes the location in which a Windows system program sits in memory each time it is loaded up. 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 has been enhanced in Windows 7 with an increased number of random load locations, and is further enhanced on 64-bit systems. It is always enabled, defeating some malware and slowing or crippling the functionality of others, while having no discernable performance impact on the system.

< 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 by default this feature is disabled, because it can cause potential incompatibilities with software that is based on Cygwin, Armadillo, or Skype - though in practice it won't cause any problems on most systems.

If you wish to enable SEHOP for enhanced security, go to the following location in the Registry Editor:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel]
```

```
DisableExceptionChainValidation=0
```

The DWORD above controls whether this feature is enabled or not. If it doesn't exist, create it and set it =0 to enable SEHOP. If at any time you want to disable SEHOP again, you can set this value to =1.

Enabling SEHOP should have a negligible impact on performance. However if you believe you are having a conflict between SEHOP and any software on your system, disable SEHOP, reboot and check your application again to confirm whether SEHOP is the cause.

Windows 7 provides an additional use for SEHOP: enabling it to provide additional protection in Internet Explorer, as detailed in this Microsoft Article. Go to the following location in the Windows Registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\iexplore.exe]
```

If the `iexplore.exe` key above doesn't exist, right-click on the `Image File Execution Options` key, select New>Key and name it `iexplore.exe`

```
DisableExceptionChainValidation=0
```

Left-click on the `iexplore.exe` key and in the right pane, create a new DWORD as shown above and set it =0 to enable SEHOP just for Internet Explorer. To disable it at any time, set it to =1.

< SAFE UNLINKING

A security feature new to Windows 7 is Safe Unlinking. Enabled by default and 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 7.

< KERNEL PATCH PROTECTION

Kernel Patch Protection, also known as PatchGuard, is a feature unique to 64-bit versions of Windows, including Windows 7 64-bit. 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. A method to temporarily disable this check is covered under the Driver Signature section of the Windows Drivers chapter, but there is no permanent way to disable it, as that would be a security hole and Microsoft frequently patches Windows to prevent any applications from doing so.

< 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 Windows 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 Windows 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 much more secure against unauthorized access.

Full EFS functionality is not supported on the Starter, Home Basic or Home Premium editions of Windows 7. In these editions 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 have the encryption key, and only through the use of the `Cipher` command - type `Cipher /?` in a Command Prompt to see more details of this command.

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. 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, and/or allow other users to use the file/folder, and/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 Start>Search Box, type *rekeywiz* and press Enter, then follow the prompts.

You can also view your EFS certificate in the following manner:

1. Go to Start>Run, type *certmgr.msc* and press Enter.
2. In the left pane, go to Personal>Certificates.
3. Your EFS certificate should be listed in the middle of the Window - 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 Export to trigger the EFS Key Wizard.

Note that if you lose your account password and it has to be reset, you can lose access to all 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 however combine EFS file or folder encryption with BitLocker whole-of-drive encryption to provide 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 built-in feature of Windows 7 Ultimate and Enterprise, but is not available for other Windows 7 editions. Windows 7 extends BitLocker's functionality by also allowing removable drives to be encrypted, referred to as BitLocker To Go.

BitLocker Drive Encryption technology secures an entire 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. However BitLocker can be used in conjunction with EFS, so the two are not mutually exclusive. To access BitLocker, go to the BitLocker component of the Windows Control Panel, or go Start>Run, type *bitlocker* and press Enter. Here 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, 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 Windows Explorer, going to the Computer category, right-clicking on the relevant drive and selecting 'Turn on BitLocker'.

Importantly, for BitLocker Drive Encryption to work, you must have at least two NTFS partitions. One of these is your normal Windows 7 partition which will 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 7 attempts to create a System Reserved Partition during installation -

covered under the Installing Windows section of the Windows Installation chapter. In practice this System Reserved Partition is not essential even if you wish to use BitLocker, because BitLocker will create a separate partition if needed for its purposes. However if you know you wish to use BitLocker, you should let Windows create the System Reserved Partition during Windows installation. You can ensure that this happens by deleting any existing partitions and then partitioning and formatting your drive all within Windows Setup.

The other requirement for BitLocker is a BIOS compatible with the Trusted Platform Module (TPM) standard, or supports a USB flash drive if you don't have TPM hardware compatibility. To check for TPM hardware compatibility, open the BitLocker component of the Windows Control Panel and in the left pane click the 'TPM Administration' link. If your system does not have hardware TPM support, then you will need a 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 Windows 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 is not prone to theft.

You can use a BitLocker protected drive on an older version of Windows such as Vista or 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 is not physically secure from unauthorized access. A BitLocker encrypted removable drive is particularly useful if you store sensitive data on a USB flash 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 this feature. 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 and/or susceptible to theft by untrusted people should you consider also using BitLocker for added protection.

If your version of Windows 7 doesn't allow you to access BitLocker, then you might consider using TrueCrypt which is a free utility with similar features.

< ESSENTIAL ADDITIONAL SECURITY

Having examined the major Windows security features, it should be obvious that security is very important in Windows 7. However these built-in security features are not sufficient on their own to protect you against all malware, nor do they pretend to be. They are important layers of defense against most of the common security threats, and provide the average user with a good starting point in preventing harm to their system. Yet there is more that needs to be done to provide genuinely good security. It is important 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 is absolutely critical in ensuring that your system is clean of malware and remains so, but I urge you to use them in conjunction with Windows security features, not instead of them, or vice versa.

The programs below are designed for all systems, and the ones I specifically recommend are fully tested and compatible with Windows 7. In this section I provide detailed configuration advice for the recommended malware scanners which I personally use on my system. This will help give you a balance between security and convenience, with minimal performance impact. You may notice that I recommend disabling certain real-time protection and/or background functionality - this may seem risky at first glance, however there are two very important reasons for this:

§ Background functionality typically involves constantly scanning your data in an attempt to detect patterns which may indicate the presence of malware. This not only uses system resources such as CPU and memory, of greater significance is the fact that it can induce stuttering and reduce performance in a range of scenarios, particularly during gaming or when running drive-intensive applications.

§ Having background scanning/real-time protection functionality active on malware scanners can cause software conflicts which can result in the incorrect installation of software, as well as general system instability and crashes while running software. This is a known issue which many software developers specifically warn against in the documentation for their programs.

I strongly believe that there is no reason to slow down a system with intrusive malware scanning features when the best protection comes from a combination of a range of built-in Windows security features, user vigilance, and regular manual scans of your system. See the advice throughout this chapter, and the tips at the end of this chapter for more details.

If you disagree with my security philosophy, particularly if you are a user who feels that the trade-off between security and performance should favor security in your own circumstances, then ignore my advice and use the default settings for each of these software packages. Just keep in mind that installing and enabling any malware scanning package on your system does not automatically mean that you are protected against malware. There is no simple automated fix to the problem of malware, otherwise it would have been defeated by now; instead malware is a bigger problem than ever. This is because prevention is always better than any potential cure, and that comes from user education and awareness, not a reliance on a range of automated tools. Unfortunately user education requires user effort, whereas the relatively ignorance of total reliance on automated tools requires minimal user effort, so obviously most users opt for the easy way out. I encourage you not to be such a user if you genuinely value your security.

Below is the essential free security software I recommend that you install and use in conjunction with the Windows features and advice covered in this chapter:

MALICIOUS SOFTWARE REMOVAL TOOL

To start with, regularly download and use the Malicious Software Removal Tool. This is a free Microsoft tool provided monthly through Windows Update, so as long as you keep up to date with Windows Update, it will automatically install and run itself when a new version is available. You can also download it from the link above and run it manually at any time, if you suspect an infection for example. Once it is downloaded and installed you can choose to do a Quick Scan or a Full Scan of your system for the most common viruses - a Quick Scan is sufficient if you also use other malware scanners. The Malicious Software Removal Tool does not install itself permanently on your system and does not stay resident on your system, it simply runs a single scan each time it is downloaded from Windows Update, or if you manually download it and use it.

The tool is designed to detect the most common malware threats, but as the tool itself recommends, you will need dedicated anti-malware scanning software which can perform regular full scans of your system for a wider range of viruses, worms and other types of malware.

MICROSOFT SECURITY ESSENTIALS

I use and recommend Microsoft Security Essentials (MSE) as a dedicated all-purpose anti-malware scanner. It is a free and lightweight malware scanner which is similar to Windows Defender, however it contains a much more powerful engine designed to scan for viruses, worms, trojans, adware and spyware, as well as other types of common security threats. One of the benefits of MSE is that it integrates neatly into Windows 7 and upon installation, Windows Defender will automatically be disabled, so there is no duplication of functionality involved. There are four main tabs under the main MSE window, and each is covered below:

Home: Displays your current security status:

§ Green - Everything is fine, and MSE is using its recommended 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 allow MSE to update over the Internet.
§ Red - A potential threat has been detected, or you have disabled one or more of the real-time protection components - read all text prompts closely to determine the actual issue.

Seeing a red status indicator simply because you have disabled one of the real-time protection components 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. However look closely, 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 MSE undertake the default action for that risk type (see Default Actions below), or select another action for each detected file.

Also available here are the manual scanning options. You can select from a Quick scan, a Full scan, or a Custom scan. The Quick scan is the fastest, going through your 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 goes through all the files, folders and system areas 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 - I recommend running a Custom scan on any particular file(s) you download or consider suspicious at any time. I also recommend running a Full scan at least once a week - whether scheduled or not is up to you - to ensure your system remains free from malware.

Update: Shows the current version and date for definition files. These definition files allow MSE to more accurately detect new malware, so you must keep MSE up to date by regularly clicking the Update button here, by checking Windows Update for updates to MSE, or by simply allowing MSE to periodically update its definitions in the background as it will usually do. However I recommend manually updating the definitions prior to launching any manual scan.

History: Shows any malware detected by MSE, as well as any programs or file types you have excluded from scanning in MSE, depending on the option chosen. I recommend selecting 'All detected items' by default to see all malware detected on the PC so far. You can delete this history of detected malware at any time by clicking the 'Delete history' button at the bottom of the screen. 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.

Settings: MSE comes with a good default configuration, so beginner users in particular do not need to alter anything here. However I provide my recommendations for more advanced users below:

§ Scheduled Scan - The default is a Quick scan at 2:00am every day. This is fine for most purposes, but should be supplemented (or substituted) with a manually launched Full Scan once a week. If you wish to leave the scheduled scan enabled, then tick the three boxes at the bottom of the screen as well, as this ensures MSE uses the latest definition files before commencing a scheduled scan, and also limits the disruption it causes to your other activities. The 'Limit CPU usage during scan to' option is fine when set to the default of 50%, but if you find MSE is slowing your system down, reduce the percentage, though this also increases the scan time.

§ Default Actions - The default actions listed are essentially identical to those listed for Windows Defender earlier in this chapter. The 'Recommended Action' option is fine for each of these items. However if the 'Apply recommended actions' box is ticked, MSE will automatically apply its recommended actions after any threat is detected. I recommend against ticking this box to avoid seeing your software or files accidentally removed. For example, should a false positive occur (i.e. a file falsely detected as malware when it is not) and it is rated as a Severe risk, MSE will automatically delete the particular file(s), even though it may actually be completely free of malware. Alternatively, you can leave this box ticked, but for the Severe and High alert levels, you can change the default action to Quarantine to ensure that there is no automatic file deletion. Then after any threat has been detected you can choose what action to take on a case-by-case basis, based on additional research.

§ Real-time Protection - The options here allow you to determine which types of activities and areas MSE constantly monitors in the background to prevent malware from installing or executing on your system. The performance impact of having all real-time protection options enabled in MSE is minimal, and hence for most users all these options can be left enabled for maximum security. However for more advanced or performance-minded users I recommend leaving the main 'Turn on real-time protection' option enabled, but unticking some of the other options as follows. The 'Scan all downloads' option relates to files downloaded via browser and email, and can be enabled without a major performance impact. The 'Monitor file and program activity on your computer' option allows: the scanning of files copied to or created on your drive (incoming files); or existing files being read or copied from the drive (outgoing files); or both (all files). This option is best left unticked for maximum drive performance, but if left enabled, I recommend setting it to 'monitor only incoming files' to prevent constant scanning of existing files. The 'Enable behavior monitoring' option controls heuristics, which along with the 'Enable Network Inspection System' option, are designed to catch any suspected malware or vulnerabilities before Microsoft issues an official security patch or MSE definition update. These options have the potential to cause software conflicts and/or raise false positives, so I personally disable them to ensure optimal stability and performance. Ultimately your choices for the various real-time protection options 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. Note that if any of the real-time protection options are disabled, the MSE status will go to red ('at risk'), and will also raise an alert in the Alert Center - both are no cause for alarm.

§ Excluded Files and Locations/Excluded File Types - These two sections allow you to specify particular files, folders or even entire file types which you don't want MSE to include as part of its scans. It is not recommended that you exclude anything from MSE's scans, as this can allow malware to slip past undetected. However if you know for certain that a particular file, folder or file type is going to be picked up as a false positive, then you can include it here.

§ Advanced - There several options here to further customize MSE's behavior. 'Scan archive files' if ticked allows MSE to scan 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, however 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 MSE makes. 'Allow all users to view the full History results' if ticked allows non-administrator users the ability to see any detected malware from any user on the same PC - this can have privacy implications because it may highlight sensitive filenames or hint at certain browsing patterns 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 ensures such files don't build up on your system over time due to inattention, as most are malicious and undesirable.

§ Microsoft SpyNet - MSE uses anonymous information collected from your machine as part of the Basic Membership status for Microsoft SpyNet. If you have concerns, see the Privacy Statement for more details. It is precisely because of this information gathered from such a large user base that MSE 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. If you wish to provide more advanced information, including some potentially personally identifiable information, select the 'Advanced Membership'. I don't recommend ticking the 'I do not want to join SpyNet' option, as ultimately it undermines the power of MSE as a malware scanner for everyone. 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.

Click the 'Save changes' button when finished here.

MSE installs two new services called 'Microsoft Antimalware Service' (*MsMpEng.exe*) which is set to Automatic, and needs to remain that way for MSE to work properly, as well as the 'Microsoft Network Inspection Service' (*NisSrv.exe*) which is related to the Network Inspection System setting, and is enabled or disabled at startup according to the choice for that setting. MSE also installs a new startup program 'Microsoft Security Essentials Interface' (*msseces.exe*) which triggers the launch of MSE at startup. You can disable this item however it will disable all real-time protection features until you manually launch MSE in a session, so it is best left to load at startup. Once running, MSE also places an icon in your Notification Area, though you will need to click the small white triangle to see it as it is set to 'Only show notifications' by default and hence is hidden.

MSE System Files Cache: To speed up scans of system files, similar to Windows Defender, MSE creates a cache on these files, stored in a .BIN file under the *\ProgramData\Microsoft\Microsoft Antimalware\Scans\History\CacheManager* directory. Do not alter or delete this file as it is necessary for MSE to perform optimally. However if the cache does not exist for some reason, it can be created by doing the following:

1. Open an Administrator Command Prompt.
2. Type the following command exactly as shown and press Enter:

```
"%programfiles%\Microsoft Security Essentials\MpCmdRun.exe” –BuildSFC
```

In general you do not need to manually create or delete the MSE cache unless it is for troubleshooting purposes.

Microsoft Security Essentials is a powerful anti-malware package which detects a range of malware, not just viruses. It provides a good balance between security and convenience, and integrates seamlessly into Windows 7. It is extremely tempting to allow MSE to replace all the other anti-malware packages on your system. However this is not recommended for a single reason: should MSE not detect a piece of malware, or provide what might be a suspected false positive, the only way you can be certain is to run a scan using one or more other anti-malware package(s). For this reason, I recommend installing at least one other dedicated malware scanner, and perhaps even a dedicated spyware scanner on your system, though the background functionality of neither should be enabled. This is not an essential step, as MSE and Windows' own security features have been proven to defeat the bulk of malware if set up correctly, but it is a wise precaution. See further below for details.

In any case MSE is not the only decent all-round anti-malware package. There is no consensus of opinion among security experts as to which particular package is the absolute best in all respects, but there are several other reputable scanners which are compatible with Windows 7 which you can use instead, though some of them are only free for a trial period, or may take quite a bit of work in reining in their intrusiveness:

AVG
Avast
Kaspersky
NOD32
Trend Micro AV

EMSISOFT ANTI-MALWARE

Microsoft Security Essentials provides strong defense against malware, especially when combined with the security features of Windows 7 and the various sensible computing tips spread throughout this book and particularly those at the end of this chapter. However having another malware scanner can provide valuable insurance, particularly in giving a second opinion when checking suspicious files. For that reason, you may wish to install the free Emsisoft Anti-Malware (EAM) package, formerly known as A-Squared Free. The following is information on how to set up EAM to minimize its background functionality and allow it to be used only as a standalone malware scanner for manual scans.

During the initial configuration of EAM, I recommend selecting the 'Freeware mode' option and clicking Next. This will automatically configure EAM to provide access to the scanning features we need while preventing any of the unnecessary background aspects. On the next screen, you can select all options except 'Use Beta updates' - which is not recommended. Click Next and allow EAM to update itself with the latest anti-malware definitions. Once completed, select 'Quick Scan' at the next prompt and allow it to complete the scan. Unless any high risk malware is found - which you should research further - click Next when complete and select 'Close setup wizard'.

As long as you're running EAM under an Administrator account, you can set the new 'Emsisoft Anti-Malware Service' to Manual, so that it only runs when you launch EAM - see the Services chapter. You can also disable the *a2guard.exe* background guard startup item if it exists - see the Startup Programs chapter for methods.

On the main Security Status screen of Emsisoft Anti-Malware, select the Configuration item and go through the various options under each tab - the default configuration is fine for our purposes, but you can change anything based on personal taste, though some features are disabled in the free version of EAM. To initiate a manual scan using EAM at any time, select the 'Scan PC' item on the main menu and then choose from 'Quick Scan', 'Smart Scan', 'Deep Scan' and 'Custom Scan'. I recommend selecting the 'Custom Scan' option as it provides the most control over how a scan is run. On the next screen, aside from selecting any particular drive(s) or folder(s) to include/exclude, I recommend ticking all available options except 'Alert Riskware that is often used by Malware' - since legitimate programs which aren't malware are often flagged as Riskware. You should also untick the 'Use file extension filter' as it is not wise to exclude certain file extensions from a malware scan. Click Next to initiate this Custom Scan, which may take quite a while.

Emsisoft Anti-Malware is best used as follows:

§ To run a full scan of your all your drives once a week.
§ To run a full scan of a particular folder whenever you download a file or save an email attachment.
§ To run a full scan if your primary malware scanner (such as MSE) shows possible infection - this helps provide a valuable second opinion.

The use of EAM in its minimal form as a manual malware scanner can be quite helpful in picking up new types of malware which other scanners might miss.

SPYBOT SEARCH & DESTROY

A spyware/adware scanner will find and remove this common type of malware from your system. Windows Defender is the basic built-in Windows spyware scanner, and it will protect you against most forms of common spyware. If you've installed Microsoft Security Essentials, that takes over the role of Windows Defender to a greater extent and does a better job. However if you have risky browsing habits or install lots of third party software, you can use a dedicated spyware/adware scanner. There are two main alternatives: Ad-Aware and Spybot Search & Destroy. Both are powerful, and both are nominally free. However Spybot is completely free and does not contain any prompts to upgrade to a paid version. Furthermore while both require some modification to reduce their intrusiveness, Spybot is easier to configure to remove its intrusive aspects, so on balance I recommend Spybot. The following are my recommended settings for Spybot:

The most important configuration options for Spybot actually occur during the installation process. During installation of Spybot, you will be given the option to select the components it installs. I recommend unticking everything that is available. If you wish to customize Spybot's appearance, the 'Skins to change appearance' option can be ticked, and if you require multiple languages, the 'Additional languages' option should also be ticked. Otherwise everything else is unnecessary to the core functionality of Spybot, and will only increase its resource usage if selected.

Furthermore, a few steps later in the installation procedure you will be asked to select common tasks for Spybot. Under the 'permanent protection' section I recommend unticking the 'Use Internet Explorer protection (SDHelper)' option, which is a form of additional protection Spybot integrates into Internet Explorer and hence a level of undesirable intrusiveness and a background process which is unnecessary. Similarly, the 'Use system settings protection (Tea Timer)' option is real-time protection functionality which always runs in the background if enabled, and as discussed earlier, is not desirable.

As long as you follow the instructions above, Spybot will not install any additional services or startup items.

Once Spybot commences, you will be given a message regarding advertisement robots. This is simply a warning that if you use Spybot to remove certain advertising-based features from specific programs, the programs may not function correctly. You will then be prompted to backup your Registry. You can do this if you wish, but it is not necessary and best done later as covered in the Windows Registry chapter. Click the green next arrow to skip this step, and click the 'Start using this program' button.

To start with, click the Update button, select an update server closest to you, then I recommend making sure that you deselect any updates relating to disabled functionality, like the TeaTimer. Click Download and

Spybot will update its definitions, then Exit the update box when done. Make sure to update Spybot before every manual scan.

To run a full manual scan, click the 'Search & Destroy' button in the left pane, and in the right pane select the 'Check for problems' button. If necessary click the 'Hide permanently' button to remove the tips box, allowing you to see the list of potential problems found. If problem(s) are found and listed, you can highlight a particular item and select the 'Fix selected problem' button. Red entries are relatively important spyware issues that should be fixed, while green problems are less harmful, although they can be fixed if desired. Check the additional information and/or search Google if you aren't certain. If anything is removed and later you wish to undo the change, you can click the Recovery item in the left pane.

To access the advanced and more detailed settings in Spybot, under the Mode menu select 'Advanced mode', however there are too many settings to cover here, and for most users there is no need to alter them unless you have specific requirements. Furthermore, I do not recommend the Immunize function, which attempts to block certain sites using your Hosts file. This function has caused conflicts and false positives in the past, and is unnecessary.

Spybot is best used as follows:

§ To run a full scan of your system at least once a week.

§ To run a full system scan if another malware scanner shows possible infection - this helps provide a valuable second opinion.

§ Conversely, make sure to run another malware scanner if Spybot detects a problem, because spyware and adware detection programs often exaggerate or misreport the level of potential threat.

Importantly there are a wide range of spyware, adware and general malware scanners which purport to remove malicious software, but ironically contain malware themselves, or are bad knock-offs of good scanners. Conduct a thorough Google search to read user feedback and as many reviews as you can find on your chosen anti-malware package, as there are far too many new packages coming onto the market which are not just useless and intrusive, but deliberately malicious or designed to hold your system hostage with dubious reports of malware infection and then constantly prompt you to purchase the paid version to remove such non-existent infections. In other words a great deal of alleged anti-malware software is now being created with exactly the same aims as malware itself: for financial gain through malicious or fraudulent means. Generally speaking, any malware scanner which prompts you to purchase the paid version before offering you the ability to clean the infection is highly suspicious at the very least and should not be used in any case.

PHISHING PROTECTION

Phishing is a form of deception which 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 such sites.

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 anti-Phishing 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 it too 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 that 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. There are several commercial firewall packages you can turn to. For free alternatives, ZoneAlarm and Comodo provide two popular software 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 7's built-in security features, and all the malware scanners and phishing protection in the world are no substitute for learning how to prevent malware infestation, and how to detect and avoid phishing and other forms of online fraud. Prevention is indeed much better than the cure, especially in the case of malware, because once your system is infected, and once your credit card details, login passwords, software serial numbers, personal documents and so forth have been compromised, then it is usually too late. Often times the 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 detect or block them, at least for a period of time, so you must learn other ways of preventing their entry into your system, and detecting their possible presence.

This is why it is so important that you read and understand the information in this chapter, and throughout this book. In particular, 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 reducing my system performance in any way.

MALWARE AVOIDANCE METHODS

Below are a range of general rules for helping you avoid becoming victim to malware and online fraud. Of course I could write a thousand rules, and none of them could cover every single type of circumstance. But the rules below do provide a strong basis for warding off the bulk of malware, and set you on the right course for coming to intuitively understand how malware works:

Address Book/Contacts: Don't keep any contacts in your email address book/contacts list. If you are infected with malware, this is one of the first methods it will use to distribute itself to all of your contacts, and since the email comes from someone they know, they are more likely to click a link or open an infected attachment. Instead save at least one email you receive from people you wish to contact regularly in a separate mail folder. Then whenever you want to email someone, open this folder and reply to their last email, clearing the existing contents and subject line before entering your text.

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 from trusted people, and always scan any saved attachments with malware scanners.

Patches & Security Updates: If you receive an email with an update or security patch for a software package or Windows attached, do not use it. Furthermore any links to such updates or patches are likely also fraudulent. No reputable software company publicly distributes updates or patches via email, they are always hosted on the company's site. If unsure, use a bookmark or manually type the legitimate company's web address into your browser and check for any updates or patches that way.

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 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 or spam/scam is the presence of bad spelling/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 keywords in spam filters.

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. 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.

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 (actually it's Google). In most cases the IP address is used instead of a domain name precisely to hide the true nature of the site.

Backups: The need for regular backups has been covered in detail in the Backup & Recovery chapter. However malware also 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.

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.com.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 a correct site is to open a new tab or window in your browser and manually enter a known and trusted site address. You can also use your bookmarks, but always check the address of the site which opens if you want to be sure you're on the correct site.

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.

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, 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 a plain text document, or the search box of a search engine like Google. Then look closely at the link to (a) see if it matches the original displayed text for the link - if it doesn't this indicates that the link was attempting to be deceptive and hence is untrustworthy; and (b) to see the actual site it links to, which you can research further as covered below. With the rise of services such as Twitter, it has become fashionable for people to use short link services to generate URLs which are short but 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 service such as LongURL which allows you to paste in a short link and see where it goes.

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 and/or administrator details are hidden or deliberately obscured tends to significantly reduce its trustworthiness.

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 undesirable. Cancel all such attempts. The most common software you require for full Internet multimedia functionality are the Flash, Shockwave and Silverlight players, as well as Java. You can install these safely by downloading the latest versions directly from their respective websites: ShockWave Player, Flash Player, SilverLight and Java. 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 in any doubt, cancel and research further.

Intimate System Knowledge: One of the many benefits of becoming closely acquainted with your PC and the workings of Windows 7 is that it allows you to spot odd behavior and unusual files and processes which most other users dismiss as normal. When properly configured and maintained, contrary to popular belief, Windows does not behave in an unpredictable manner, and your programs and games will not randomly crash. Therefore when strange things do begin to happen, such as unexpected program crashes or changes, your browser redirecting in odd ways, the system slowing down at times, or other unusual activity, you can spot it almost straight away 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. Unfortunately there is no simple way to gain such knowledge, it takes time and patience, but there are many rewards for being familiar with the fundamentals of Windows and PCs.

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. To disable your Internet connection, go to the Network and Sharing Center in the Windows Control Panel, click the 'Change adapter settings' link in the left pane, then right-click on your active network adapter and select Disable. The quickest and most foolproof way is to turn off your router/modem and/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; and (c) to prevent any hacker from accessing your system using any newly opened exploits or vulnerabilities. You can then use the Scan and Research methods below to track down the malware and remove it, and once you're confident your system is malware-free, reconnect to the Internet.

Scan for Malware: This is a somewhat obvious but necessary step. If you suspect a downloaded file or attachment of containing malware, or you believe your system is already infected with malware, then you must run a full manual scan using the scanners recommended earlier in this chapter. This is one of the reasons why I recommend several separate scanners, as running each one, one after the other, greatly increases your chances of successfully finding a variety of different malware types. Importantly, if you find your malware scanners are not launching or behaving oddly, or can't remove detected malware, then this is a sure sign that malware is resident on your system and blocking attempts to remove it. Reboot your system into Safe Mode and run your scans from there - see the System Recovery section of the Backup & Recovery chapter for details.

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, then common sense would tell you it is ridiculous and highly risky. 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 and/or a suspicious 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. 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.

Research, Research, Research: This is the Golden Rule. You are not the only person in the world using the Internet or receiving emails, 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 the same 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, to the true nature and 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 Google. Remember that knowledge is power.

BALANCING SECURITY VS. 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 the past few years there has been a significant rise in genuinely malicious software; namely software designed solely to do harm to your system and/or compromise your personal information. This coincides with the rise in the number of people who are using the Internet to pay bills, do their banking and go online shopping.

The stakes are much higher now, so no matter how advanced a user you believe yourself to be, it is incredibly 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 7's enhanced security features, which at first appear to be annoying - especially User Account Control - are actually very necessary and should not be disabled without careful consideration. You will most definitely need to do more than just install and enable a few anti-malware packages on your system to keep it secure.

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 now. In this chapter I've provided what I believe is a good balance, especially for more performance-minded users. Rather than just suggest the use of background malware scanners which can hurt performance, I have recommended a combination of Windows own built-in features and several trusted free third party tools used in minimalist but effective manner 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

This chapter looks at the configuration and optimization of memory-related functionality on your system. It is very important to understand the basics of how your computer uses the various forms of memory on your system, including the way the Windows Memory Management system works. 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 corrupting 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. That is, if options relating to the use of CPU L1/L2/L3 Cache(s) are present in your BIOS, never disable them unless troubleshooting. Aside from BIOS settings, there is a `SecondLevelDataCache` Registry setting for attempting to manually adjusting your CPU's L2 Cache setting. However as with Windows XP and Vista, altering this setting is not necessary, as the default value of 0 already allows Windows 7 to automatically identify and use the correct L2 Cache size from the Hardware Abstraction Layer (HAL). This setting is only for old CPUs, such as pre-Pentium II models, which use direct-mapped L2 caches.

In general since the user has no control over the CPU's caches aside from ensuring that they are enabled in the BIOS, 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 and CRC errors. In these cases you can try temporarily disabling the caches in the BIOS to see if this reduces or resolves errors.

Physical RAM

This is probably the most well-known and most important form of memory. RAM (Random Access Memory) is a temporary data storage area covered under the Memory section of the Basic PC Terminology chapter. The primary advantage of RAM over other forms of storage such as your hard drive is that it is much, much faster to access, so optimal RAM usage means smoother performance for your system. There are three main 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 main 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 7 have actually reduced the memory requirements for smooth operation such that it can still perform quite well on systems with lower amounts of memory. Windows 7 32-bit has a minimum requirement of 1GB of RAM, and Windows 7 64-bit has a minimum requirement of 2GB of RAM. If you are into heavy multi-tasking or play games, I strongly recommend more than 2GB of RAM to allow reasonably smooth performance without stuttering or frequent loading pauses. There are no RAM size tweaks; if you have a low level of RAM then it is strongly recommended that you consider buying and installing more RAM in your system - see the Upgrading Memory section at the end of this chapter. Bear in mind however that Windows 7 32-bit cannot practically use more than 4GB of RAM; only the 64-bit version can do that, so any more than 4GB of RAM is effectively wasted in Windows 7 32-bit.

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 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. It is possible to adjust your BIOS such that the RAM can operate at a higher or lower speed in practice. 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. Remember though that the more the RAM's actual speed surpasses its advertised speed rating, the greater the chance for instability, so ideally you should 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, 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 by your system unless manually changed in the BIOS, and when used with the recommended RAM speed rating (see above) ensure maximum stability.

To view all the details of your RAM, including current and maximum rated speeds and timings, 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 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 285 1GB). This RAM acts as a temporary storage location to hold 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 physical 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 physical RAM, altering the latency of your VRAM is tricky and not recommended, though still possible. The speed in MHz can be easily altered up or down using an overclocking utility, with the faster the speed the higher the performance, but once again the greater the chance of graphical glitches and freezes. See the Overclocking 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 7 has implemented a slightly improved form of the memory management system used in Windows Vista, which in turn is notably improved over that used in Windows XP. We have already examined the memory-related security features in the PC Security chapter, so this section examines other Windows memory management features relating to general system usage. These can be summarized as follows:

§ 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.
§ 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 and 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 in the PC Security chapter.
§ General performance improvements through optimizations in the way the memory management algorithms work depending on various circumstances.

Below we look at the most important aspects of Windows 7'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 7. This is covered in more detail under the 32-bit vs. 64-bit section of the Windows Installation chapter, but of relevance here is the fact that under Windows 7 32-bit, a PC can normally only use a maximum of 4GB of RAM - any higher won't be detected or used by default. Even with 4GB of RAM you may only see around 3GB of that available, 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 the major reason why the 64-bit architecture is required and will soon become standard as more people expand beyond 4GB of RAM on their PCs.

To allow Windows 7 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:

```
BCDEdit /set PAE ForceEnable
```

Alternatively you can enable PAE using a utility like EasyBCD - see the EasyBCD section of the Boot Configuration chapter. There are other benefits to enabling PAE, including enabling support for hardware-enabled DEP - see the Data Execution Prevention section of the PC Security chapter.

However 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 a waste. If you use or require larger amounts of RAM then the correct course of action is to install the 64-bit version of Windows 7.

The official physical memory limitations for Windows 7 are listed in this Microsoft Article, and are summarized below:

§ Windows 7 Starter - 2GB (both 32-bit and 64-bit)
§ Windows 7 Home Basic - 4GB (32-bit), 8GB (64-bit)
§ Windows 7 Home Premium - 4GB (32-bit), 16GB (64-bit)
§ Windows 7 Professional, Ultimate and Enterprise - 4GB (32-bit), 192GB (64-bit)

Windows 7 Home Premium 64-bit or above provides you with a suitable degree of future-proofing should you decide to install more RAM in your system at a later date.

SUPERFETCH

SuperFetch is a feature first introduced in Windows Vista, and used with some modification in Windows 7. It is similar to, but much more efficient and useful than, the Windows XP prefetching implementation. 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, making the system feel more responsive and allowing applications to load up more quickly. In effect this turns your otherwise idle RAM into a Windows cache designed to improve speed and responsiveness.

There was a mistaken belief regarding Vista's SuperFetch that using RAM as a cache meant Windows was 'hogging memory'. This is completely false - cached memory can be almost instantly freed up when needed by any program. On the other hand, if your RAM is sitting idle and unfilled, it is serving absolutely no useful purpose whatsoever; free RAM is wasted RAM. Unfortunately in Windows Vista the implementation of SuperFetch was somewhat aggressive. Almost immediately after reaching the Windows Desktop, it would begin to 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 users.

Windows 7 refines and tones down the use of SuperFetch in several important ways. Even though the SuperFetch service is not set on a delayed start and hence begins immediately during bootup, the caching functionality of SuperFetch only begins approximately 6 minutes after system start, and at a more leisurely pace of around 10MB/s. Furthermore SuperFetch does not automatically try to fill all available free RAM, it only caches the most important data based on usage history, and this often equates to around 500 - 800MB of cached data on an average system to begin with. Part of this reduced caching is also due to the fact that Windows 7 uses less resources by way of background Services and desktop memory usage for example, and hence there is less data to cache. Typically at the normal rate at which SuperFetch caches data in Windows 7, in less than a minute of subdued drive usage the cache is sufficiently full. Over time the cache may then continue to grow as necessary, as Windows tries to retain high priority information in the cache as long as possible. However any time your system requires the use of the cache RAM, 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 looking under the Physical Memory section. There you can see the Total amount of RAM installed on your system, the Cached memory used primarily by SuperFetch, and the Available memory which is roughly the sum of Free memory plus Cached Memory. See the Task Manager section under the Performance Measurement & Troubleshooting chapter for more details.

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 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 such drives is because on balance they are considered fast enough in terms of their random read performance to make SuperFetch unnecessary. As long as the SSD is not a model which has relatively slow random write performance - as many early generation and budget SSDs do - then SuperFetch can remain disabled. If your SSD scores well above 6.5 in the WEI, and you feel your drive is fast enough to do without SuperFetch, then see the information below on how to manually disable SuperFetch if it is not automatically disabled by Windows.

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 on any drive, open the Services utility, double-click on the SuperFetch service and select Disabled - see the Services chapter for more details. You should also set both Registry entries above to 0. Then you should delete the files under the *\Windows\Prefetch* directory. 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 a score of 6.5 and above in the disk component of the Windows Experience Index. If you do disable SuperFetch, and then want to re-enable it, remember that it will take SuperFetch a while to get back up to speed in analyzing your usage patterns.

Importantly, don't regularly clean out the *\Windows\Prefetch* folder as this reduces SuperFetch and prefetching performance. Windows maintains the folder automatically by regularly removing lower priority and less-used items.

Desktop Windows Manager

The Desktop Window Manager (DWM) is covered in detail under the Graphics & Sound chapter, as it relates primarily to graphics functionality in Windows 7. However it is discussed briefly here because one of the major improvements in Windows 7 memory management results from the way in which DWM has been redesigned to reduce the memory utilization of Desktop rendering. In Windows Vista, for every window that is 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 Windows 7, this has been refined so that only one copy of the data is held in Video RAM. Then 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 under Windows 7 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.

However to take advantage of this improvement in Windows 7 memory management, you must use a Windows 7-specific WDDM 1.1 graphics driver; WDDM 1.0 drivers, 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 allocate 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 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 which are caused by heap corruption, without the need for the user to get involved. Of course 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 PC 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 it cannot be used for normal file storage purposes while being used for ReadyBoost. Windows 7 brings two improvements to ReadyBoost: you can now use devices larger than 4GB with ReadyBoost, and you can also 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 prompt asking if you want to 'Speed up my system'. Note that the prompt will not come up if you've disabled AutoPlay for this type of device - see AutoPlay under the Windows Control Panel chapter. If you select this option, the device will now be configured for use by SuperFetch to hold information which would otherwise be cached out to your hard drive; by placing it on a flash memory-based drive, your system can access it faster, 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 dialog box which opens - or which can be accessed by going to Windows Explorer, right-clicking on the device, selecting Properties and then clicking the ReadyBoost tab - 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 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 box. Furthermore if you disable SuperFetch then ReadyBoost will automatically have no impact.

If you are using a sufficiently fast SSD as your main drive, Windows will not allow you to use ReadyBoost. Instead 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 a fast SSD, as it will be faster for Windows to directly access your SSD drive for data than to use the cached data on a slower attached flash memory device.

The ReadyBoost feature cannot be readily disabled because unlike Windows Vista, there is no ReadyBoost service in Windows 7, 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. If you still wish to do this, you can use Autoruns to do so. Launch Autoruns, under the Options menu untick the 'Hide Windows Entries' item, select the Drivers tab, click the refresh button or press F5, then untick the *rdyboost* component and restart Windows - see the Startup Programs chapter for more details on Autoruns.

In general ReadyBoost is mainly useful if you have a low amount of system RAM and are unable to upgrade it for some reason and/or if you are running a relatively slow hard drive. Otherwise the performance benefits of ReadyBoost may be marginal at best, although it does no harm to experiment. If you are unsure of whether you should use ReadyBoost or not, 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 which can show you how well ReadyBoost is utilized on your system.

One final note: if you are going to purchase a USB flash drive for ReadyBoost purposes, make sure to research its random read and write speeds in various reviews. A very 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 in more RAM or a faster main drive rather than a quality USB flash drive.

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.

Though it is not recommended that you do so, if you wish to disable ReadyBoot (e.g. on a system with a fast SSD as the primary drive), then follow these steps:

1. Open Performance Monitor by going to Start>Search Box, typing *perfmon* and 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\* and delete the *ReadyBoot* folder.
6. You should then disable the ReadyBoost driver - see ReadyBoost above for details.
7. Reboot your system and ReadyBoot should no longer perform its analysis and caching routines.

This is not recommended, however if you have an SSD which you believe is fast enough 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 processes are 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 to the user indicating the particular program that is using too much memory, and provide the user 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 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 further below 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 7 creates a Memory Dump file after a major crash, and by default it is a Kernel Memory Dump 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. Fortunately you can configure both the type of memory dump file which 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.

If you wish to change the memory dump behavior, go to the System component of the Windows Control Panel and click the 'Advanced system settings' link. Alternatively go to Start>Search Box, type *systempropertiesadvanced* and press Enter. Under the Advanced tab, click the Settings button under the 'Startup and Recovery' section at the bottom of the window.

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 it doesn't 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.

Of particular relevance to this topic is the 'Write debugging information' setting where you can select the following:

§ *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. On systems with more than 2GB of memory this option is not available, but you can enable it through the Registry - see further below.
§ *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 you tick the 'Overwrite any existing file' option, Windows will automatically overwrite any existing dump file already at the stored location, which is recommended to prevent excessive drive space being wasted through storage of old dump files. However even without this option being ticked, if free space on the specified drive is below 25GB, Windows 7 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 most users don't need. If dump files are critical to your needs, ensure that there is much more than 25GB of free space on the specified drive location, or see the settings below. For most home users the Kernel Memory Dump option is suitable, as is ticking the 'Overwrite any existing file' option.

For advanced configuration of these options, go to the following location in the Registry Editor:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]
```

```
CrashDumpEnabled=1
```

The DWORD above corresponds with the 'Write debugging information' option available within Windows. The valid data for this value are: 0 = None; 1 = Complete Memory Dump; 2 = Kernel Memory Dump; and 3 = Small Memory Dump. You can set the desired option using the normal Windows interface covered above, however because Windows does not allow a Complete Memory Dump for systems with more than 2GB of RAM, you can force enable this option here by setting this value to =1, though note that it won't show up as being selected in the regular Windows interface for this option.

```
AlwaysKeepMemoryDump=1
```

The DWORD above does not exist by default, so create it and set it =1 if you want Windows to ignore space limits and always save a memory dump file to disk. This is only recommended for advanced users who must ensure that each and every dump file is saved, even on a drive with less than 25GB of free space.

```
MinidumpsCount=50
```

The DWORD above determines the number of previous small memory dump files kept. The default value is 50 such files (in Decimal view), because they are relatively small in size. However you can alter this value to reduce or increase the maximum number stored.

Depending on the memory dump option you choose in Windows, this will affect the recommended minimum Pagefile size, as covered in more detail in the next section. In short:

- For the Complete Memory Dump option you require a Pagefile which is at least the same size as your system RAM + 1MB.
- For the Small Memory Dump option, a 2MB Pagefile is required as minimum.
- If you have enabled Kernel Memory Dump, you will require a minimum Pagefile size of 150MB - 2GB depending on your RAM size.
- 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 absolute minimum.

See this Microsoft Article for details of the exact size required for the different memory dump options.

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 require 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 (called 'pages') and temporarily swaps them out from your RAM to your drive. The 'swap file' where the memory pages are held on your drive is called *pagefile.sys*, and resides in the base directory on 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 the *pagefile.sys* file if the 'Hide Protected Operating System Files' option is unticked under Folder Options - see the Folder Options section in the Windows Explorer chapter.

Under Windows 7, the improved Disk and Memory Management techniques try to minimize reliance on your physical drive, since using it can cause stuttering or small delays and hence reduce responsiveness. However a Pagefile is still very important to Windows Memory Management and even with a great deal of RAM, is not something you should disable or consider redundant, as paging portions of processes to Virtual Memory is a necessary part of normal memory management. In the absence 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 Start>Search Box, type *systempropertiesadvanced* and press Enter. Under the Advanced tab click the Settings button under Performance, and select the Advanced tab in the new box which opens. Here you can see the amount of drive space allocation to the Pagefile at the bottom of the window. For less advanced users, a System Managed Pagefile is perfectly fine and will prevent your system from running out of memory resources, since Windows will automatically resize the Pagefile 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 untick the 'Automatically manage paging file size for all drives' 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 need to first clear your existing Pagefile. To do this select each relevant drive, choose the 'No paging file' option and click the Set button, then you need to reboot your system. This step does two things: first it clears 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 under the Drive window. Which drive(s) or partition(s) the pagefile should be located on is based loosely on the following scenarios:

§ 1 Drive with 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.

§ 1 Drive with 2 or more Partitions - 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 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/games, 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/games, 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 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, 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 configuration, such as an SSD vs. a pair of RAID hard drives, you may choose to shift the Pagefile there.

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. Pagefile access primarily consists of reads, which will not have a significant detrimental impact on SSD lifespan, and the same rules to determining the Pagefile size as covered below apply to SSDs.

Pagefile Size: After selecting the location for the Pagefile, you can then determine its total size in MB. In the Virtual Memory settings screen 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.

By default Windows 7 sets your Pagefile with a minimum size equal to your system RAM, and the maximum size at 3 times your system RAM. So if you have 2GB of RAM for example, Windows will set a dynamic Pagefile which starts off at 2GB and can go up to a maximum of 6GB. This default Pagefile size is reasonable but not optimal. The correct size of the Pagefile is often debated, and there are many conflicting accounts of the optimal size. In the past I have provided what I have personally tested and found to be completely safe recommendations for the Pagefile size. However to remove all doubt and provide a concrete recommendation for this important system file, I now rely on the advice of the 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.

Essentially, 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 your processes attempts to exceed the Commit Limit, then there will be memory allocation problems, potentially leading to crashes and even 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 and also see the Commit Limit 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 custom 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 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, 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 pagefile minimum size according to this formula:

Pagefile Minimum Size = Peak Commit Charge - Total System RAM

If the value for this 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 you require a Pagefile of a particular size as a minimum due to your Memory Dump settings, covered in the relevant section above. For the default 'Kernel Memory Dump' setting in Windows 7, this means anywhere from 50MB - 800MB or more based on your system RAM size. As such, as a safe value for the Pagefile Minimum Size I recommend at least 1GB or the result of the formula above, whichever is higher.

The pagefile maximum size is then calculated as:

Pagefile Maximum Size = Up to 2 x Pagefile Minimum Size

Given your Commit Limit has already been set such that it meets your most strenuous requirements as per the Pagefile minimum, you should already have plenty of headroom even if you 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 to provide even greater headroom, especially in case of unforeseen usage patterns, and to future-proof against upcoming applications and games which may use more memory. Note that there is a 4GB limit for maximum Pagefile size if running a 32-bit version of Windows 7. You need to enable

Physical Address Extension to remove this limit - see the Maximum Supported RAM section earlier in this chapter.

If you've spread the Pagefile over multiple drives, ensure that the sum of the Pagefile sizes equals the values above, or that the main Pagefile follows the above rules, and the other Pagefiles are all very small.

Once you've adjusted your Virtual Memory size settings click the Set button and reboot if required.

If you still insist on setting an extremely small or zero Pagefile, at least make sure you set your Memory Dump settings to either the None or 'Small Memory Dump' 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 you may lose any unsaved work if Windows runs out of memory and does not have access to sufficient Virtual Memory.

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 particular, a common point of confusion regarding Pagefile usage is the Paged and Nonpaged memory items in the Kernel Memory section under the Performance tab of the Task Manager. These do not monitor Pagefile usage, they monitor areas of core Windows memory usage which 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 referred to above 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 'System managed size' option until you have the time to get a better understanding of it by reading the associated articles. As noted, the recommendation is fairly broad but it is based on advice from one of the most reputable Microsoft experts available, so any other recommendations you find are unlikely to be as accurate. However keep in mind that the recommendation hinges solely on proper analysis of your Peak Commit Charge at a point in time. If over time you install and launch new programs and games which use much greater amounts of memory, or you multitask with more programs than you originally envisioned, or load up increasingly large datasets for your programs, then obviously 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.

If at any time the Resource Exhaustion Detection prompt comes up, you should consider increasing your maximum Pagefile size. Having a larger Pagefile size does not hurt performance as such; it mainly 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 slow down shutdown times noticeably, but if you require this level of security, see the Local Security Policy section of the PC Security chapter for details.

< UPGRADING MEMORY

There is no real substitute for having a decent amount of physical RAM installed on your system. All the advanced memory management features in Windows 7 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 switching to using the 64-bit version of Windows 7 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 7, even though the minimum requirement is 1GB, I suggest a more practical minimum of 2GB if you want reduced stuttering, 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, consider either upgrading your drive to a fast 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 drive(s) are used in Windows. Your drive is one of the relatively slower components of your system - even the fastest Hard Disk Drive (HDD) or Solid State Drive (SDD) cannot access, read or write data as quickly as RAM. So when one of your components such as the CPU or graphics card needs information, to prevent pauses, stuttering or slowdowns, Windows attempts to hold as much of the information as possible in RAM for fast access. However 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. Therefore it is the physical drive(s) where all your information is permanently stored, and your system must regularly access the drive for data. This chapter looks at how the drives are used in Windows, including the new Virtual Hard Disk feature in Windows 7. It also examines how you can make sure that this usage is optimal for your particular hardware configuration.

< WINDOWS I/O MANAGEMENT

To deal with the potential bottleneck that the drive represents on 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, Windows Vista introduced a markedly improved Input/Output (I/O) System. Windows 7 continues the use of this system, along with a range of refinements.

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 your drive, 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, long pauses or freezes and even data errors.

In Windows 7, 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 completed 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 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 gaming.

The practical impacts of this I/O prioritization scheme are that firstly less critical tasks such as scheduled Windows Defender scans, the Windows Disk Defragmenter or SuperFetch will not cause the system to become unresponsive. In fact Windows will suspend certain tasks altogether if a more important task is being undertaken, like running a system-intensive program. Windows also reserves drive bandwidth for certain tasks which specifically need a consistent flow of data, especially multimedia applications, so that these are not visibly disrupted. Thus it is possible to run a drive-intensive task while also listening to music on Windows Media Player without audio glitches occurring for example.

However 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 slowdowns 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 such as games, I recommend that you close down all other open applications.

< 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 modern 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. The 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 relatively low price. The vast majority of Windows 7 users are likely to be using a hard drive, and this is both taken into account by Microsoft when they developed Windows 7, and is also a primary consideration in this book. Ultimately however, the hard drive is a technology which is slowly dying out, to be steadily replaced by storage based on memory chips such as Solid State Drives.

< 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 the hard drive on desktop systems. Since they only serve as secondary storage media, and given the portability of optical media, the speed of optical drives is not critical to Windows performance.

Fortunately, Windows 7 alleviates one of the major annoyances in previous 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 7 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 Windows Explorer on other drives without interruption. Refer to the AutoPlay section later in this chapter to configure how Windows 7 behaves when you insert different types of optical media.

< SOLID STATE DRIVES

A Solid State Drive (SSD) is a flash memory-based storage drive which has no physical moving parts. SSD technology has been around for a while, but it has only been relatively recently that they have risen in storage capacity and fallen in price sufficiently, while also attaining good all-round performance, to become a good alternative to traditional hard disk drives. 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 can usually exceed those of a fast hard drive, 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. This means that for those who do not own an SSD yet, there is no hurry to purchase one as they will continue to improve in terms of performance, storage space and price. There is no doubt however that SSDs will become the mainstream form of storage in coming years, providing greatly improved overall system performance as a result by removing the significant bottleneck which mechanical hard drives have placed on systems.

Windows 7 is the first version of Windows to be built with SSDs in mind, and to natively support SSDs through a range of built-in optimizations and features. The key features of Windows 7 which SSD owners should consider are covered below:

Trim Support: Windows 7 automatically enables support for the Trim command in NTFS to ensure that deleted blocks are erased and that the SSD is aware of which blocks have been deleted. This helps maintain better performance and a longer lifespan. This 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 7 on all drives, SSD or otherwise. To change this setting for any reason, use the following command:

```
fsutil behavior set DisableDeleteNotify 1
```

Where a value of 1 disables Trim, and a value of 0 enables it.

There may be reasons to disable Trim, for example if the manufacturer recommends this to prevent problems on certain drives. The primary issue however is that whether Trim is actually being used by your SSD is determined by its firmware and the particular motherboard storage controller drivers being used. Until your SSD manufacturer updates the firmware to enable full Trim support - if it isn't already listed as being supported in the drive specifications - and until the controller drivers are also suitably updated, it may be best to disable Trim. Check your SSD manufacturer's support site for updates and more details.

Without proper Trim support your SSD performance may noticeably decline over time. This can only be rectified by using a custom erase utility, as a regular format will have no impact. You should check your SSD manufacturer's website for such a utility, or use this free Secure Erase utility to do a full erase of your SSD if you feel your performance has been significantly degraded over time. Refer to this Secure Erase Guide for more details of how to use this utility. It is not critical to do this regularly, but it is best to do so whenever you are ready to (re)install Windows 7 on your SSD, even if your drive supports Trim. Note that you will likely have to set your SSD's controller to IDE/legacy/compatibility mode in your BIOS first, and then boot up into a Command Prompt or boot up using a USB flash drive to run such a utility. Once the process is completed, reset your drive controller to its original mode in the BIOS, reboot and install Windows 7 as normal.

For Intel SSD owners there is a specific Intel SSD Toolbox utility to help maintain drive integrity and performance. Other SSD manufacturers may provide similar tools, so check your manufacturer's site.

Defragmentation: Windows 7 will automatically disable scheduled defragmentation via the Windows Disk Defragmenter on any detected drives which exceed random read speeds of 8MB/s - basically for all SSDs. Fast drives like SSDs don't benefit sufficiently from defragmentation, certainly not enough to offset the negative impacts of the additional writing involved in defragmentation and hence the potential reduction in

SSD lifespan. You should avoid manually defragmenting SSDs by any means, and if you already have a third party defragmentation utility installed on your system before installing an SSD, make sure to disable it for the SSD. If you find Windows has not disabled Windows Disk Defragmenter on your system despite using an SSD as your primary drive, you should manually disable it from running on a schedule - see the Windows Disk Defragmenter section later in this chapter.

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, and the same rules to determining the Pagefile size as those for traditional hard drives apply. See the Windows Memory Management section of the Memory Optimization chapter for more details.

Search Indexing: 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 7 does not automatically disable the Search Index when an SSD is detected, and it is not recommended that you do so either. You should however refine your Search Index as covered in the Windows Search chapter to reduce its overall size and hence reduce the frequency with which it is written to - the rest of the time, the Index is primarily used for reading data.

SuperFetch and ReadyBoost: Windows 7 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. This means your SSD must perform sufficiently well in all respects to warrant Windows disabling these features. Many older or cheaper SSDs do not perform well enough in some areas, and this is reflected in a Windows Experience Index which may not be above 6.5. The entire 6.0 - 7.9 score range in the drive component of the WEI was created for SSDs - see the Windows Experience Index section of the Performance Measurement & Troubleshooting chapter for more details. If you have a high disk score and still find these feature enabled, you can manually disable them as covered under the Windows Memory Management section of the Memory Optimization chapter.

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 not as fast as system RAM and hence some aspects of Windows Memory Management are still beneficial on systems using SSDs.

< VIRTUAL HARD DISK

A feature new to Windows 7 is native support for the Virtual Hard Disk (VHD) format. As the name implies, a VHD file is designed to be identical in structure to a physical drive, and is generally treated as a physical drive by Windows. Note that this function is only available on Ultimate or Enterprise editions of Windows 7. For more details of VHD functionality in Windows 7, see this Microsoft Article.

VHD 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 the VHD features for home PC users:

MULTIBOOTING WINDOWS 7

Windows 7 supports natively booting up from a VHD file. This allows you to run multiple copies of Windows 7 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 file and selected via the Windows boot menu. The main benefits for a home user of doing something like this would be to allow you to test software or drivers on an identical .VHD copy of your Windows 7 without worrying about any harm being done to your original installation of Windows 7. You cannot boot up from VHDs of other operating systems, but if you wish to use Windows XP in a virtual environment within Windows 7, see Windows XP Mode at the end of this section.

To multiboot Windows 7, the first thing you require is a Windows 7 .VHD file. To create one from an existing install of Windows 7 or from a Windows 7 DVD, you can use the Microsoft WIM2VHD Converter or the free Disk2VHD utility. The procedure for booting up a Windows 7 .VHD 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 EasyBCD section of the Boot Configuration chapter. Follow these steps:

1. Open EasyBCD, click the 'Add/Remove Entries' button, then select the 'Virtual Disk' tab.
2. Click the '...' button to browse to the location of your VHD file and select it.
3. Give it a relevant name (e.g. Windows 7 Virtual) and click the 'Add Entry' button to add it as an entry to the Windows 7 boot menu. This allows you to select whether to boot into the real Windows 7 or the virtual Windows 7 at each startup.
4. You can tick the 'Force boot device' box to make Windows automatically boot up into the virtual Windows 7 at each startup.
5. Reboot and the Virtual Windows 7 should be available in the boot menu with the name you gave it.

Be aware that in the VHD version of Windows 7, 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 7 .VHD image, it may be hardware-dependent; that is, it captured the hardware state of your system and hence this .VHD may not be bootable or operative when mounted on a physically different PC.

Creating a VHD

You can create an empty VHD for use as a new virtual drive or partition by doing 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. Go to the Action menu in Disk Management and select 'Create VHD'.
4. You will then be asked where to place the .VHD 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 optimal performance and safety.
5. Once created you will see a new unformatted drive appear in the bottom pane of Disk Management.
6. You can prepare this new virtual disk for use by right-clicking on it and selecting 'Initialize Disk'.
7. You can partition and format the disk and assign a drive letter as normal by right-clicking on the disk and selecting 'New Simple Volume' and following the prompts.

This new VHD is now 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, you can see that it is a separate file with the extension .VHD. 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 you detach a VHD before performing any copy or move operations on it - see further below.

To create a new VHD image of an existing drive, use the Disk2VHD utility mentioned above. To create a VHD from the Virtual Machine Disk (VMDK) format use the free V2V Converter. While computers running Windows 7 have native support for the .VHD format, PCs running Windows XP or Vista can use the Microsoft Virtual PC software to mount .VHD files.

MOUNTING AND DETACHING A VHD

If you use the steps above to create a new .VHD file, it will automatically be mounted, which means it is automatically detected as a connected drive by Windows. You can however detach it at any time, simulating the removal of the drive from the system, by right-clicking on the disk and selecting 'Detach VHD' then following the prompts. Just as with the removal of a physical drive, it will no longer be detected by Windows, however unless you chose the 'Delete the virtual hard disk file after removing the disk' box, the .VHD file itself will remain where it was created, ready to be backed up, moved to another location or reattached at any time.

To reattach or 'mount' an existing .VHD file, 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 file and click OK.
5. The .VHD file will be mounted as the type of drive the .VHD file image was originally saved as.

ACCESSING A SYSTEM IMAGE BACKUP VHD

One of the most useful ways to utilize the VHD support in Windows 7 is to mount a full system image backup created using the Windows Backup utility. 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 above, allowing you to access the contents of your system image and browse and copy individual files and folders using Windows 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. However 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.

WINDOWS XP MODE

Windows XP Mode is a virtual installation of a fully licensed copy of Windows XP SP3. The main purpose of Windows XP Mode is to allow users who have applications which can only operate properly under a true Windows XP environment to run such an environment on their Windows 7 desktop, without the need for a dual boot scenario. It is available as a free download, but only for Windows 7 Professional, Enterprise and Ultimate edition owners. To run Windows XP Mode, your PC needs to have Intel VT or AMD-V hardware virtualization features available and enabled in the BIOS.

In practice, the average home PC user does not require Windows XP Mode, because Windows 7 already provides excellent support for applications and games which ran under Windows XP. In most cases an application works without any need for user intervention. In some cases you may need to manually assign Administrator privileges to the software, whether during installation and/or launch, and you might also need to set the compatibility mode for the software to 'Windows XP' - these procedures are covered under the Compatibility Issues section of the New & Common Features chapter, as well as the User Account Control section of the PC Security chapter.

Windows XP Mode is targeted towards corporate users who have custom applications which have only been tested to work under Windows XP. Thus using Windows XP Mode provides substantial convenience and reduces costs for these businesses as it guarantees 100% compatibility with Windows XP-based applications in every scenario without the need to retest. Windows XP Mode won't be covered in any further detail here because as noted, it is not required nor recommended for most desktop PC users, and all relevant instructions are provided in the link above.

< RAM DISK

A RAM Disk 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 disk 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 disk can only function when the system is on; when it is off, the contents of the RAM disk will either be lost, or must be saved to your drive before shutdown and reloaded at startup, which can slow down startup and shutdown times noticeably.

To set up a RAM disk on your system, use a program designed to perform this task, such as the free DataRAM RAMDisk. Once installed, run the RAMDisk Configuration Utility and under the Settings tab you can select how much RAM to allocate to the RAM disk. Remember that the amount you set aside for the RAM disk cannot be used by your system for other purposes while the RAM disk is in operation, so don't assign a large portion of your RAM. For the formatting of the disk, select Unformatted as it will need to be formatted in NTFS as covered further below.

Under the Load and Save tab you can make the data stored in the RAM disk 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 disk or save data onto it, however this will increase shutdown and startup times accordingly, especially if there is a large amount of data to be saved. The actual image files saved during shutdown and startup are shown in the boxes below these options - change their names and/or locations if you wish.

If you only want a RAM disk for using as a temporary cache by other programs in each Windows session on the other hand, untick the Load and Save options above and instead tick the 'Create Temp directory' box. Anything stored on such a RAM disk configuration will be lost each time you shutdown your PC.

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 disk will be created depending on your options. However the RAM disk 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. Right-click on it and select 'New simple volume', then click Next in the wizard.
4. Make sure the 'Assign the following drive letter' option is chosen, and change the drive letter if desired, then click Next.
5. Format the drive in NTFS with a Default allocation size, give it an appropriate label (e.g. RAM Disk), and tick the 'Perform a quick format' box, then click Next.
6. 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 Windows Explorer, and depending on whether it is a temporary or permanent RAM disk, you can use it accordingly. Anything stored here will be extremely fast to load.

To remove this RAM disk at any time, open the RAMDisk Configuration Utility and click the 'Stop RAMDisk' button. The drive will disappear from Windows. Uninstall the RAMDisk and manually delete any .IMG files you created to permanently remove the RAM disk contents from your system.

< 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. However you can directly access Disk Management by going to Start>Search Box, typing *diskmgmt.msc* and pressing Enter.

Once open, you will see all 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 bottom right pane and selecting 'Change Drive Letter and Paths', then highlight the drive letter which appears, click the Change button and assign a new drive letter. Note that you cannot change system drive letters 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) are likely taking up all available space, which is normal. You can however 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. Once you have some unallocated space, you can right-click on it 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 100MB System Reserved partition here, 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 your boot files, and removing it can make Windows 7 unbootable, necessitating the use of the Startup Repair feature. It does no harm to leave it be if it has already been created. See the Installing Windows section of the Windows Installation chapter for more details.

Basic and Dynamic Disks: All 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 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 your data, so it is not worth experimenting with. You should only use this option if you have specific needs which you know will require a Dynamic Disk, such as for holding very large databases. Furthermore you should only do so if you are an advanced user. Note that this function is only available on Ultimate or Enterprise editions of Windows 7.

Virtual Hard Disk: There are a range of features for VHDs now available in the Disk Management component - see the Virtual Hard Disk section above for details.

< DISK DIAGNOSTICS

By hourly checking data from a drive's Self Monitoring, Analysis, Reporting Technology (SMART) feature, the Windows built-in Disk Diagnostics 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 and supported by your drive, otherwise Windows won't be able to automatically check for drive problems in this manner. 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 HD Tune has a Health tab under which you can see whether your drive has any problems.

PassMark: The free PassMark Disk Checkup utility shows SMART information for a drive by selecting that drive under the Physical Devices list in the tool, then checking under the SMART Info tab and looking at the Status column where everything should read OK.

If you wish to disable this 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, which is not recommended.

This feature is extremely useful, however you may not get sufficient warning of drive failure, and the failure may be catastrophic enough to render some of your data unreadable when it first occurs, so Disk Diagnostics is not a replacement for making regular backups as covered in the Backup & Recovery chapter.

CHECK DISK

To check your drive for general errors such as bad sectors or corrupted indexes, you can run the Windows Check Disk utility. To access it follow these steps:

1. Go to the Computer category in Windows 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 Now' button to launch Windows Check Disk.
4. To run a quick and basic error scan within Windows, untick both boxes and click the Start button.
5. To run a longer scan of the drive to find any bad sectors within Windows, tick only the 'Scan for and attempt recovery of bad sectors' box and click Start. This can take a while.
6. To run a quick error scan which automatically repairs any detected problems, but which requires restarting Windows to commence the scan at next bootup, tick only the 'Automatically fix file system errors' box and click Start. Click the 'Schedule disk check' button and the next time you reboot Check Disk will run at startup. If it finds any problems it will try to fix them automatically.
7. To run a lengthy thorough check and automatic repair procedure which requires restarting Windows, tick both boxes and click Start. Click the 'Schedule disk check' button and the next time you reboot Check Disk will run at startup. If it finds any problems it will try to fix them automatically.

Do a basic check whenever you suspect drive-related problems as per Step 4. However even if you don't suspect any major problems, a periodic run of Check Disk using the method in Step 6 is relatively quick and detects and fixes any small errors before they develop into anything more serious. If there are known errors on the drive, then run the full scan and fix procedure as per Step 7 - it will take quite a while but is the most thorough method of detecting and repairing drive errors.

< 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, including the newer SATA II standard - 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:

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 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 to ensure that you have enabled the relevant controllers and that the drives are being detected in the BIOS - see the BIOS & 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:

Removal Policy: The 'Better performance' option should be selected for maximum performance, unless you actually need to remove this drive frequently. However 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 you don't experience any data corruption or loss. If the drive is a removable device such as a USB flash drive which you frequently connect to the PC then select 'Quick Removal' so 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 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 interruption to the power supply to your drive, or any other hardware issues, you may lose or corrupt your data.

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. Alternatively, invest in an Uninterruptible Power Supply (UPS), as covered in the Hardware Management section of the BIOS & Hardware Management chapter.

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 and optical drives, or SATA drives specifically configured to run in legacy IDE emulation mode in the BIOS. 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 which can be shown here are Ultra DMA Mode 4 for optical drives, and Ultra DMA Mode 6 for IDE drives. However your actual speeds may be even higher due to newer technology, so use a tool like HD Tune to check your actual drive mode under its Info tab.

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 you have installed the correct drivers for this motherboard - see the Windows Drivers chapter.
§ Your BIOS is not configured correctly to enable the highest speed - see the BIOS & Hardware Management chapter.
§ You are sharing a hard drive or SSD with an optical drive on the same channel - move any optical drive(s) to a separate channel of their own.
§ 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 quite 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 and any switches on the back of the drive(s).

Serial ATA 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 a drive is connected to these channels, the 'Transfer Mode' should show the correct maximum speed for the drive: 1.5GB/s for SATA I, or 3.0GB/s for SATA II. Alternatively click the 'Speed Test' button to do a quick benchmark of the drive's speed and see the speed rating. The 'Let BIOS select transfer mode' box should be ticked unless you are troubleshooting or you see 'PIO Mode' for your drive, which is sub-optimal; in that case untick the box and manually attempt to switch to 'DMA Mode'.

Selecting IDE mode under the drive configuration in your BIOS is generally the best choice for most users, as it is the most compatible mode for SATA hard drives and SSDs while also providing excellent performance. However AHCI mode is native to SATA drives, and is covered below:

AHCI Mode: If you run a SATA-based drive, you can try enabling Advanced Host Controller Interface (AHCI) mode on your SATA controller in your BIOS. This mode has a range of benefits, especially on SATA II hard drives with NCQ support - this includes quieter operation 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 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 - see this Microsoft Article for details.

Some SSDs may not properly support AHCI, and indeed some SSD manufacturers do not recommend using AHCI mode due to potential performance issues, since NCQ is designed for drives with a physical drive head, not SSDs which are memory-based. However some users report increased speeds with AHCI enabled on their SSD, so it can still provide performance benefits if you are willing to experiment.

You can also select RAID mode in the BIOS, but this is only necessary if you have a RAID drive configuration - see the Preparing the Drive section under 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 such as HD Tune, or the drive benchmarking component of Sandra, or simply the built-in Windows Experience Index. Drive benchmarks can be quite artificial and not necessarily indicative of real-world performance, so they are best used to determine if your performance has improved or degraded, or to compare with other users of the same drive to check if your performance is significantly lower and hence indicative of a potential problem. See the Performance Measurement & Troubleshooting chapter for more details.

< AUTOPLAY

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. This functionality is called AutoPlay, and while it can be very handy in some instances, it can also be a nuisance at times.

When certain devices such as portable music players, cameras and phones are connected, instead of AutoPlay, Windows will open Device Stage, which provides greater functionality - see the Device Stage section of the BIOS & 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, Windows 7 has changed the AutoPlay behavior such that AutoRun will not work for non-optical removable media. This means 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 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, and in the case of discs designed to install a program, you will see a prompt requesting the launching of a program. However Windows 7 provides text above this option stating that the program is being run from your media, indicating that the software could potentially be malicious. If you are using a legitimately purchased manufactured disc, or a disc you created from a trusted image, then the risk of malware should be minimal.

In any case, you can customize all AutoPlay and AutoRun behavior by going to the AutoPlay component of the Windows Control Panel and adjusting Windows 7's default behavior for each and every type of media or device which can be attached to your system. For example, you can set the 'Software and games' component to 'Open folder to view files using Windows Explorer', providing greater protection against automatically installing malware. Then when a software DVD is inserted, Windows will simply open Windows 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.

I recommend going through and setting 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 in that instance. 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.

< MASTER FILE TABLE

The Master File Table is a system area of Windows which contains an entry for every file and directory on your drive with information on its size, attributes, permissions, timestamps and so forth. In a way, 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 around 200 MB in drive space for the MFT to prevent fragmentation, and this allocation grows as required. If your drive is 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.

If you want 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 automatically managed and will increase as required - this is 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 as required.

In Windows 7 and Windows Vista the MFT is automatically managed and never needs any user input or adjustment. However it is important to regularly defragment hard drives (not SSDs) to ensure the MFT doesn't become fragmented over time and thus degrade drive performance.

< WINDOWS DISK DEFRAGMENTER

As data is written to or deleted from your 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 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 several 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 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 drive performance and increase the potential for stuttering and loading pauses on hard drives.

Windows Disk Defragmenter (Defrag) is a built-in utility that performs a very important function: it finds all of these file fragments and attempts to put as many of them back together again as is necessary to prevent the degradation of your drive's performance. To access the Disk Defragmenter utility, open Windows Explorer, go the Computer category, right-click on the relevant hard drive and select Properties, then look under the Tools tab. Alternatively, go to the Start>Search Box, type *dfrgui* and press Enter.

In Windows 7 the Disk Defragmenter has changed in both function and appearance from its previous counterparts in Vista and XP. It expands on the types of files which can be defragmented over those possible in Vista, and much more than what is capable in XP, defragmenting system files like the Master File Table and NTFS metadata, and consolidating free space much better than any previous version. In Windows 7 you can now also defragment multiple drives at the same time, and can cancel defragmentation at any time without causing any problems. As with Vista's Defrag, there is no graphical progress indicator to provide you with a visual representation of how fragmented your drive is or how long the process may take. Instead you are provided with two indicators: the first shows the percentage of fragmentation on each drive, which you can refresh by highlighting the drive and clicking the 'Analyze disk' button. The second is a new Progress indicator which shows the pass the defragmenter is currently on, and the proportion of that pass completed. Depending on the amount and type of fragmentation, Disk Defragmenter may do up to 11 passes, and some may take quite a while to complete, so in practice it doesn't tell you a great deal about the relative progress of defragmentation.

Importantly, if Windows detects that you are using an SSD, it disables Disk Defragmenter, since SSD random read times are extremely fast, counteracting any performance decreases due to fragmentation, not to mention that the act of defragmenting an SSD can reduce the lifespan of the drive. Do not run a scheduled or manual defrag of any type on an SSD, and if necessary, manually check and disable scheduled defragmentation in case it is not automatically disabled by Windows. You can also disable the Disk Defragmenter service if desired, though this is not necessary - see the Services chapter for details.

Windows Disk Defragmenter is designed primarily to be automated and by default runs on a weekly schedule at 1:00am every Wednesday morning, defragmenting your drive in the background at a low priority when idle hence causing minimal disruption to system responsiveness. If you wish to change the scheduled time or frequency with which the automatic defragmentation occurs, or to turn off scheduled scanning altogether, open Defrag and click the 'Configure schedule' button. You can specify how often, on which particular day and at what time the process is initiated, and also choose which drive(s) to run it on - remember that Defrag can now defragment multiple drives at the same time. If you wish to disable this scheduled defragmentation altogether then untick the 'Run on a schedule' box. In general I suggest leaving the automated defragmentation schedule to run once a week, at a time when you know the PC will be on but you will not be doing anything with it.

In practice however, defragmentation is best done immediately after you make major file changes to the drive, so I strongly recommend that you also do a manual defrag immediately after any of the following events:

§ Installation of any program, especially games or any drive-intensive applications such as benchmarks.
§ Patching any program or running Windows Update.
§ Installation of any drivers.
§ Adding or deleting large file(s) or folder(s) of any type.

Defragmentation is particularly necessary for gamers, since games are already quite prone to stuttering and longer loading times due to their data-intensive nature, so by defragmenting your drive after a game installation or after patching a game, you can significantly reduce any stuttering while playing the game.

To initiate a manual disk defragmentation at any time, open Defrag, highlight the desired drive(s) and click the 'Defragment now' button for every drive you want to defragment. Once defragmentation starts, you will see the pass on which it is currently operating, and as noted earlier, it may do as many as 11 passes, each of varying times, with the time taken for each pass depending on how fragmented your drive is, how large the fragments are, and whether you are doing anything else at the same time. If you run any other program during this process, Windows will further reduce the priority given to Defrag, which in turn can increase the time taken for process to complete, so while there is no danger to your data, try not to do anything too drive intensive while Defrag is running. Note that for the defragmentation process to work, you must have a reasonable amount of free space on the drive, preferably 15% or more.

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. Windows 7 adds several new commands to the Defrag command, including the `/M` switch to run the operation on each volume in parallel; the `/X` switch to perform free space consolidation; the `/H` switch to force normal priority instead of the default low priority; and the `/U` switch to provide details of the progress.

For example, to run a defragmentation on two available 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
```

Windows Disk Defragmenter provides a comprehensive tool for addressing file fragmentation on your system. However 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 in Windows 7. For utilities which are free, I recommend the following:

MyDefrag
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 purchase for use beyond this period. 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 in Windows 7. The third party defragmentation packages above may 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 Windows 7 Disk Defragmenter is free, fully integrated into Windows, and gives you the majority of the benefits of defragmentation, including a range of advanced features not available in previous versions of Windows Disk Defragmenter.

Furthermore, as traditional hard drives are being phased out in favor of much faster solutions like SSDs which don't require the use of a defragmentation utility, I don't believe it is a wise investment to purchase a third party defragmentation tool now. The money is better put towards eventually upgrading to an SSD instead.

Regardless of whether you use the built-in defragmenter or a third party utility, make sure to defragment your hard drives regularly as it is essential to smooth performance.

WINDOWS CONTROL PANEL

This section runs through all the general options available under the default Windows 7 Control Panel, which is an important central location for accessing most of the Windows settings on your system. The Windows Control Panel can be accessed by clicking the Control Panel item in the Start Menu, or by going to Start>Search Box, typing *control panel* and pressing Enter.

All the important settings which are 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 however a range of features and settings which do not neatly fit into any other chapter, and hence are covered here. By making sure that you systematically go through all the components of Windows Control Panel one by one you will in effect have configured all the important Windows settings.

Importantly, it is assumed throughout this book that Windows Control Panel is being viewed using the Icons view option, 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' in the 'View by' list. Only the default Windows 7 Control Panel components are covered in this chapter, though some editions of Windows 7 may not have all the Control Panel items because particular features are not available in certain editions, and this is noted where relevant throughout this book.

< CUSTOMIZING WINDOWS CONTROL PANEL

Third party applications can install Windows Control Panel items which may be undesirable, particularly as they can add clutter to the Windows Control Panel. This section provides methods for finding and removing these components. These methods do not uninstall or otherwise harm the functionality associated with the components, they simply prevent the relevant components 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.

However Local Group Policy Editor is only available in the Ultimate and Enterprise editions of Windows 7, so if you do not have access to it, there are other methods for removing Windows Control Panel items. Many third party applications install .CPL files which are small applications designed to run in the Windows Control Panel. Removing the relevant .CPL file will remove that component from Windows Control Panel. You can see a list of common third party .CPL files in this Wikipedia Article. You can find these .CPL files typically stored under the *\Windows\System32* folder, or in the program's own directories, or you can initiate a system-wide search for all .CPL files. Once the file is found, close the Windows Control Panel, temporarily delete the suspected .CPL file to the Recycle Bin, reopen 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\ControlPa
nel\NameSpace]
```

The keys and values located beneath the subfolders above contain entries which relate to Windows Control Panel components, both third party and default Windows components. However remember that deleting a Registry entry cannot be undone, so make sure you create a backup of the relevant branch and/or the entire 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 made in the Registry in the Windows Control Panel.

The remainder of this chapter covers the individual default 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 features. The Security section of the Action Center is covered in the PC Security chapter, and the Maintenance section of Action Center is covered in the Performance Measurement & Troubleshooting chapter.

< 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 useful to the average home PC user. However I provide details of the main Administrative Tools and point out their most useful aspects for the average user 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 a combination of several administrative and system 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.

Data Sources (ODBC)

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 won't be covered in this book.

Event Viewer

The Event Viewer is a useful troubleshooting tool which shows a log of system events. These events are recorded by Windows over time, and reflect information alerts, warnings and errors that have occurred to date. See the Event Viewer section of the Performance Measurement & Troubleshooting 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 won't be covered in this book.

Local Security Policy

This tool allows you to establish and alter security-related settings. The main purpose is to allow an Administrator to limit or control the usage rights of other user accounts on the system or a network. For more details see the Local Security Policy section of the PC Security chapter.

Performance Monitor

This tool allows you to monitor the usage of major system resources. It is covered in 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.

Services

This tool is extremely useful in configuring service usage under Windows. See the Services chapter for full details of this tool.

System Configuration

The Microsoft System Configuration tool, also known as MSConfig, is covered in detail under relevant sections of the Boot Configuration, Startup Programs and Services chapters.

Task Scheduler

Task Scheduler functionality is covered under the Background Tasks section of the Services chapter.

Windows Firewall with Advanced Security

This feature is covered in the Windows Firewall section of the PC Security chapter.

Windows Memory Diagnostic

The Windows Memory Diagnostic tool is a system memory (RAM) troubleshooting utility. Its functionality is covered in detail under the Windows Memory Diagnostic section of the Performance Measurement & Troubleshooting chapter.

Windows PowerShell Modules

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 who want to write scripts for automating particular tasks in Windows. PowerShell is beyond the scope of this book, however you can refer to this Microsoft Article for a general overview of using PowerShell, this Microsoft Article for changes in PowerShell under Windows 7, this Microsoft Article for more details of scripting with PowerShell, as well as the PowerShell Pack for additional scripts to download.

< AUTOPLAY

AutoPlay functionality is covered under the AutoPlay section of the Drive Optimization chapter.

< BACKUP AND RESTORE

Backup and Restore provides access to functionality covered in full detail in the Backup & Recovery chapter.

< BITLOCKER DRIVE ENCRYPTION

BitLocker Drive Encryption is a security feature available only in Windows 7 Ultimate and Enterprise. It is covered in more detail under the BitLocker Drive Encryption section of the PC Security chapter.

< COLOR MANAGEMENT

Windows Color Management is a tool which allows you to ensure that the colors displayed on your screen are accurate and will be reproduced faithfully across a range of devices. For accurate color reproduction it is very important that your monitor have proper drivers loaded in Windows - these should be available from your monitor manufacturer's site. Also see the Windows Driver chapter for details of how to check and update device drivers as necessary.

Note that there is a known bug whereby installing a monitor driver will make the background of Windows Photo Gallery take on a yellow tinge instead of being white. To fix this issue, remove the new color profile from Color Management and use the default Windows profile as covered in this Microsoft Article.

The average home PC user should not change these settings as they require specialist knowledge. However you can calibrate your display color more easily using the built-in Display Color Calibration utility, which is covered 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 here. 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 screen which is covered in more detail under the Region and Language 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 strongly 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 on the main screen so that Windows can provide information in advance regarding any scheduled time changes such as Daylight Savings.

ADDITIONAL CLOCKS

Under Windows 7 you can show up to two additional clocks in different time zones from your main system 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 cursor over 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 ensure 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 immediately, 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 for a variety of reasons.

< 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. Each of the sub-options is covered in more detail below:

SET YOUR DEFAULT PROGRAMS

This option provides a list of programs 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, 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'. For example, if you select Windows Media Player, you can either let it automatically become the default for all the relevant media types it can support, or see details of the specific file types and choose from them manually.

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. If you do 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 settings using the more thorough file association method will also add your programs 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 which 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 files, it simply chooses the program which Windows will automatically use when a file of that type is launched. Note, if you can't see the file extensions for your files, make sure the 'Hide extensions for known file types' option is unticked in Folder Options - see the Folder Options section of the Windows 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 no default 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. To view additional programs which can handle this file type, click the small down arrow to expand the 'Other Programs' category. To add a new program to the list, click the Browse button and go to the main executable for the specific program you wish to add.

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 reassociate 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 even 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, allowing you to 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 here are already covered in full detail under the AutoPlay section of the Drive Optimization chapter.

SET PROGRAM ACCESS AND COMPUTER DEFAULTS

This section allows you to quickly 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 has been charged with monopolistic behavior, and as part of the terms of settlement of a case against them, they are 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. This is also part of the reason why there is no longer a built-in email client like Windows Mail, as covered in the Windows Live Mail chapter.

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 altogether, such as Internet Explorer or Windows Media Player, see the Programs and Features section later in this chapter.

< DESKTOP GADGETS

Desktop Gadgets can display a range of useful information on the Windows Desktop. This functionality is covered in more detail under the Gadgets section of the Graphics & Sound chapter.

< DEVICE MANAGER

The Device Manager is an important hardware management tool whose functionality is covered in detail under the System Specifications, BIOS & Hardware Management and Drive Optimization chapters.

< DEVICES AND PRINTERS

Devices and Printers is a new Windows 7 feature covered in detail under the Devices and Printers section of the BIOS & Hardware Management chapter.

< DISPLAY

The Display functions are all covered in 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 7 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.

< FOLDER OPTIONS

This feature is covered in full detail under the Folder Options section of the Windows Explorer chapter.

< FONTS

This feature is covered in full detail, along with other font-related functionality, in the Fonts section of the Graphics & Sound chapter.

< GETTING STARTED

This feature simply provides a range of links to common Windows features which Microsoft believes users would wish to visit shortly after installing Windows 7. All of the functions linked to here are covered in their respective chapters throughout this book, and by itself this is not a particularly useful component of the Windows Control Panel.

< HOMEGROUP

HomeGroup is a new Windows 7 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 'Home Network' - 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 automatically enables the HomeGroup feature, the most obvious component of which is a new category called HomeGroup visible in the Navigation Pane of Windows 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, a new option called 'Share with' also appears in the Command Bar in Windows Explorer. This allows you to select a particular file, folder or Library, click the 'Share with' button and choose how to share it with others on the home network.

If you do not wish to use the HomeGroup feature, to disable it and remove the HomeGroup category in the Navigation Pane of Windows Explorer, click the 'Leave the homegroup' link in the main HomeGroup window, then select 'Leave the homegroup' again in the prompt. Finally, set the 'HomeGroup Listener' and 'HomeGroup Provider' services to disabled if you wish to prevent this feature from restarting - see the Services chapter for more details.

< INDEXING OPTIONS

This tool controls the indexing of files and folders as part of the Windows Search functionality. This function is covered in more detail under the Search Index section of the Windows Search chapter.

< INTERNET OPTIONS

This component brings up the Internet Explorer 'Internet Properties' box. There is no difference between accessing it here and accessing it from within Internet Explorer, so see the Internet Explorer chapter for full details of how to configure these options. If you are using another browser as the system default browser then clicking this item will still bring up the Internet Explorer 'Internet Properties' box - this is normal and cannot be changed.

< KEYBOARD

This component provides access to 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 typing or holding down a key in the small test box provided. There may also be keyboard-related options in your BIOS that affect the speed with which the keyboard responds, so check there if you find that your keyboard still feels sluggish. You can also adjust the 'Cursor Blink Rate' to your taste, and then click OK to apply.

< LOCATION AND OTHER SENSORS

New to Windows 7, Locations and Other Sensors allows your PC and its programs to adapt their behavior based on detected geographical location and environmental changes. For example, if equipped with a light sensor, the PC can automatically dim or brighten the display depending on the level of ambient light around the PC. Similarly, with a GPS device the PC can determine your geographical location and automatically customize localization and provide information that is more relevant to your circumstances. When you open this component, any appropriate sensors installed on your PC will be shown. Without relevant sensors, this functionality is not possible. Any sensor can be enabled or disabled as desired, and notifications regarding sensor usage are show in the Notification Area.

Since this feature is dependent on appropriate hardware being installed on a PC, and since many PCs do not currently have such hardware, it won't be covered in detail in this book.

< 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 image of the folder 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.

For people who don't want any mouse acceleration applied within games use this Mouse Acceleration Fix.

Wheel

If your mouse has a mousewheel, you can increase or decrease the wheel's responsiveness by altering the number of lines it will scroll on each turn of the wheel under the Vertical Scrolling option. For example, even an increase from the default of 3 to 4 will make a subtle but noticeable difference if you previously found the mousewheel 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 7 you are prompted to choose your current location which in turn determines your network type. The available choices for network location are Home Network, Work Network and Public Network. You can view your current network location at any time by clicking the network icon in your Notification Area, and you can change it by clicking the current network location link under the 'View your active networks' section of Network and Sharing Center.

The difference between the network locations is described in this Microsoft Article. For the average home user with a standalone PC and a connection to the Internet, I strongly recommend Public Network, as this is the most private and secure setting. Choose the Work Network option only if you're connected to a trusted network of other work PCs. Choose the Home Network location if you are connected to a network of trusted and secure PCs within your own home.

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 PC Security chapter to ensure that the settings for your currently chosen profile are appropriate.

Connections: The connections section 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 connected or installed on your PC. Click the connection link to see more details on the device, and click the Details button 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 at the bottom. This provides access to tools for troubleshooting any network-related issues, covered further in the Troubleshooting section of the Performance Measurement & Troubleshooting chapter.

For advanced configuration of your network device, click the connection link on the main Network and Sharing Center window, then click the Properties button. Here you can see the various clients, services and protocols this connection uses, which again should not be altered unless you know what you are doing - refer to your device documentation or detailed instructions. Below are my recommendations for a standard Internet connection via a modem or router on a home PC not connected to a network of other PCs:

You can safely untick the following items:

§ Client for Microsoft Networks
§ QoS Packet Scheduler
§ File and Printer Sharing for Microsoft Networks

The above features are intended primarily for PCs connected to a network of other PCs, and hence are not needed by the average non-networked home PC for normal Internet access. They are completely safe to disable, however if at any point you experience reduced functionality or problems, re-enable them all again.

If you are concerned or curious about the newer IPv6 protocol enabled by default in Windows 7 and Vista before it, see this Microsoft Article for more details. I do not recommend disabling IPv6 as there is no real performance benefit, and indeed certain Windows features such as HomeGroup are wholly reliant on IPv6 and will not function correctly without it. Unless you are an advanced user with detailed experience in this area, do not alter any settings here.

Sharing: Click the 'Change advanced sharing settings' link in the left pane to access file and folder sharing options for each type of network location profile. Your currently used profile will be denoted by '(current profile)' at the top, so configure it first and foremost. For standalone home PC users, you can turn off network discovery, file and printer sharing, and Public folder sharing. Conversely, you should turn on password protected sharing for greater security, even though there is nothing to be shared, as the alternative is to have unprotected sharing. If you are on a home or work network, then you will have to go through these options more carefully and only enable the features which suit your needs.

Finally, to test your Internet speed and compare it with others, use the free Speedtest online service.

Once again, I strongly suggest leaving the settings here at their defaults if you are not sure of what to change. 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 here are already quite optimal and don't need any tweaking in most circumstances to provide excellent performance and stability. Individual devices may have specific problems which can be resolved by checking your hardware manufacturer's website.

< NOTIFICATION AREA ICONS

The Notification Area is at the far right of the Taskbar, and is covered in more detail in the Notification Area section of the Graphics & Sound chapter.

< PARENTAL CONTROLS

The Parental Controls feature is designed to let an Administrator set particular limitations on specific User Accounts. See the Parental Controls section of the User Accounts chapter for more details.

< PERFORMANCE INFORMATION AND TOOLS

This component takes you to a range of tools which 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 the Performance Measurement & Troubleshooting, Graphics & Sound and Cleaning Windows chapters.

< PERSONALIZATION

This component provides a range of features designed to allow you to alter the appearance and sound of Windows 7. They are covered in more detail in the Personalization section of the Graphics & Sound chapter.

< PHONE AND MODEM

This option lets you configure any connected phone or modem devices. This is generally a legacy option and won't be covered in detail in this book.

< POWER OPTIONS

The Power Options allow you to apply or change a power plan. These impact on 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: Balanced, Power Saver and High Performance. These are described further in this Microsoft Article. I recommend that rather than using a preset level, you create an entirely new custom 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 in the left pane.
2. I suggest choosing 'High Performance' as the basis for your changes, as the other schemes can result in reduced performance.
3. You can give the plan a descriptive name, or use the default which is fine.
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. The default of 20 minutes is reasonable.
5. I don't recommend enabling the Sleep functionality (select Never) - 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.
9. A new 'Advanced settings' window will open with a range of detailed settings.
10. 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 settings are available to you.

The advanced power settings are explained individually below. Note that if you have a mobile PC, you can access the Power Options by clicking your battery icon in the Notification Area. You may also see additional options relating to battery use here - my recommendations below are for a standard desktop home PC:

Require a password on wakeup: When waking up from sleep mode, if set to Yes this option forces you to reenter the password (if one exists) for the current User Account to unlock the PC. 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 is turned off. I recommend selecting Never to maintain maximum responsiveness and longevity; hard drives should not be constantly switched on and off.

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.

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'.

The following sections allow you to use Sleep, Hybrid Sleep and Hibernate modes which replace the Standby mode in Windows XP. These modes are covered in more detail below, as well as in this Microsoft Article.

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. It is primarily intended for mobile PC users who need to conserve power but also maintain responsiveness. In Sleep mode your PC turns off most of its components and saves your documents 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 button or opening the lid. The problem is that while data is stored in RAM, it is susceptible to loss through sudden loss of power for example - Hybrid Sleep mitigates against this risk.

Sleep - Allow Hybrid Sleep: In this section you can choose whether to enable Hybrid Sleep mode or not. Hybrid Sleep mode is similar to the Sleep mode covered above, however instead of saving your open documents, programs and 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 your used system RAM 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 is the same as Hybrid Sleep in that it will write your open documents, programs and system state to the *Hiberfil.sys* file after a period of inactivity as specified here. However unlike Sleep or Hybrid Sleep, rather than putting your system into a power-saving mode, it allows you to turn off the entire PC and leave it that way for as long as you like. You can then turn the system back on 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.

For a mobile PC, these are all viable options depending on your power needs. However I recommend against using any of the Sleep-related modes on a desktop PC if you value system stability and performance. A fresh reboot every day or two 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 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 full shutdown and restart once a week, as recommended in this Microsoft Article.

Importantly, whether for Hybrid Sleep or Hibernate, if you have disabled these options and do not plan on using them, you should also delete the *Hiberfil.sys* file if it exists as it can be quite large. However you can't just delete it in Windows Explorer. You must open an Administrator Command Prompt, then type:

```
Powercfg -h off
```

This will remove *Hiberfil.sys*, but will also remove the Hibernate and Hybrid Sleep options from your Power Options as well. These options can be restored at any time by using the following command in an Administrator Command Prompt:

```
Powercfg -h on
```

Sleep - Allow wake timers: If you have enabled any of the Sleep-related options above, you can enable wake timers, which allows the PC to be automatically woken up from Sleep by scheduled tasks and events, and then return to its sleeping state once completed. For example you can set the Windows Disk Defragmenter to wake up your PC and run a full defrag 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. If you don't want any task or event to wake up your PC under any circumstances, set this option to disabled.

USB settings - USB selective suspend setting: This option controls whether the system will selectively suspend individual USB devices which do not require power. This should be left at Disabled to prevent USB devices becoming non-functional during a session, unless you run a mobile PC where power savings are important.

Power buttons and lid - Power button action: This is actually quite 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. However if you've enabled one of the sleep-related modes and don't have a dedicated Sleep button on your PC, you can 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. Set to suit your taste.

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.

Search and Indexing - Power savings mode: If search indexing is enabled (See the Search Index section of the Windows Search chapter), this option determines whether to allow background disk indexing to use more or less power by updating the index more or less frequently. For the average home PC user there is no reason to attempt to save a small amount of power by setting this option to anything other than 'High Performance'. Any power savings you might make by lowering this setting will mean that your index will be less up to date and hence less useful in return.

The following settings control any power management features supported by your CPU. This allows Windows to direct your CPU to throttle down its speed when it is not required to reduce power consumption, however when greater processing speed is required the CPU can instantly jump back to its rated speed to perform the desired task. These settings work in conjunction with your BIOS and hardware's power management settings, so check your motherboard manual and the BIOS & Hardware Management chapter for more details.

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, keep the CPU cooler when its full power is not needed, but anytime an application or game 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. 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 section of the BIOS & Hardware Management chapter.

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 processing power.

Display - Turn off display after: This setting lets you select the amount of inactivity before your monitor is switched off. It will instantly switch on again as soon as you press a key or move the mouse. Since displays use quite a bit of power, and since LCD and Plasma displays can suffer from image retention when displaying a static image for too long, it is wise to enable this option and set it to something like the default 20 minutes of inactivity. That way when you're away from your PC for longer periods your monitor goes into standby mode, protecting the display, reducing your power usage, and having no impact on your hardware's performance or stability since monitors are designed to turn off and on frequently.

Multimedia settings - When sharing media: Determines your PC's behavior when your PC 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 quality.

There may be additional settings compared to those listed above. This depends on your actual hardware and its capabilities. Once done with these settings click the Apply button and then 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.

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 stability and also potentially experience data loss if you go overboard. For gamers and other high-performance users I certainly don't recommend that power saving options be used aside from those recommended above. For mobile PC and casual desktop PC users however 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 primarily tool used to view, modify or uninstall the programs and drivers currently installed on your system. It also allows you to add or remove a range of installed 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 some cases in the Version column. If you select a particular item you may see additional resources such as links to the software manufacturer's support site in the Details Pane at the bottom.

Unfortunately some programs and drivers installed on your system will not appear in this list because they are standalone programs which 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 which don't appear on this list.

Conversely, if you uninstall a program or driver and its entry remains in this list, you can use the Uninstall function of the CCleaner utility to remove all such unnecessary entries. Open CCleaner, click the Tools button, then select the Uninstall option. In the list of Programs to Remove, you can highlight a faulty entry and click the 'Delete Entry' button to remove it, though make sure that you have already uninstalled the relevant program from your system beforehand - click the 'Run Uninstaller' button first if in doubt. 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 this process should initiate a series of prompts or an automated wizard which will take you through the process.

Turn Windows Features On or Off: This option is shown in the left pane, 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. However importantly, it also allows you to quickly and easily re-enable any such features in the future. For this reason, this is preferred over other methods which permanently remove a feature from your Windows installation disk, 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 remove 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 my 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 7 may not contain all of these features. Note also that the defaults provided are for a standalone non-networked PC using Windows 7 Ultimate 64-bit - other systems may vary.

Feature	Default	Recommend	Details
Games	All Ticked	Tick/Untick	Uninstall any built-in Windows games you're certain you won't play. You can untick 'More Games' here to remove the 'More Games from Microsoft' icon in Games Explorer.
Indexing Service	Unticked	Untick	This is not the same as the Windows Search indexing service; it's for legacy applications and may cause issues if enabled.
Internet Explorer 8	Ticked	Tick	Allows you to disable Internet Explorer 8. I recommend keeping it enabled just in case it's required by a certain site.
Internet Information Services, Internet Information Services Hostable Core	All Unticked	Untick	These services are all designed for running a Web or FTP server, and are unnecessary for an average home PC.
Media Features	All Ticked	Tick	Allows you to uninstall Windows media-related programs. I recommend keeping at least Windows Media Player.
Microsoft .NET Framework 3.5.1	Main box Ticked, Components Unticked	Tick	Required for applications programmed using .NET. The Windows Communication Foundation components are unnecessary.
Microsoft Message Queue (MSMQ) Server	Unticked	Untick	Unnecessary unless you specifically run an MSMQ server.
Print and Document Services	Main box Ticked, Internet Printing Client, Windows Fax & Scan Ticked	Tick/Untick	Internet Printing Client, LPD Print Service, LPR Port Monitor and Scan Management items are all network-related and unnecessary for the average home PC.
Remote Differential Compression	Ticked	Untick	Only tick if connected to a network at any time.
RIP Listener	Unticked	Untick	Only tick if on a network which uses the RIPv1 protocol.
Services for NFS	All Unticked	Untick	Not required, NFS Protocol is for networks.
Simple Network Management Protocol (SNMP)	All Unticked	Untick	Protocol only for network-based devices.
Simple TCPIP Services	Unticked	Untick	Not required, installs unnecessary services.
Subsystem for UNIX-based Applications	Unticked	Untick	Only tick if running Unix-based applications; not applicable to the average home PC.
Tablet PC Optional Components	Ticked	Untick	This component is not required for access to the Snipping Tool covered in the Graphics & Sound chapter. Only tick if you have a Tablet PC.
Telnet Client	Unticked	Untick	Only tick if you plan to use Telnet features to connect to a server.
Telnet Server	Unticked	Untick	Lets others connect to your machine via Telnet, which is a security risk unless you need this functionality.
TFTP Client	Unticked	Untick	Only tick if you want to use Trivial File Transfer Protocol to connect to a TFTP server. Unnecessary for average home PC.
Windows Gadget Platform	Ticked	Tick	Necessary for display of Windows Gadgets on the Desktop.
Windows Process Activation Service	All Unticked	Untick	Not related to Product Activation, this is required for certain applications to transfer information. Not normally needed.
Windows Search	Ticked	Tick	Enables the Window Search functionality covered in the Windows Search chapter. Do not untick; if you want to disable Windows Search then set the Windows Search service to Disabled instead.
Windows TIFF IFilter	Unticked	Untick/Tick	Allows Windows Search to index the contents of .TIFF files. Can be ticked if you have any TIFF files you wish to index.
XPS Services	Ticked	Tick	Allows you to create documents in the Windows XPS format.
XPS Viewer	Ticked	Tick	Allows you to view documents in the Windows XP format. Best left ticked in case you need to view an XPS document.

After changing these settings and clicking OK you may need to reboot and/or insert your Windows 7 DVD 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. That is one of the key benefits of removing Windows features from within Windows 7 in this manner - it allows you to easily undo the change, as opposed to more permanent methods like removing the component from the Windows 7 installation image.

< RECOVERY

The Recovery window is simply a central location for accessing troubleshooting, system recovery and program uninstallation features in Windows. These features are covered in more detail in the Backup & Recovery and Performance Measurement & Troubleshooting chapters, as well as in the Programs and Features section just above.

< REGION AND LANGUAGE

The basic region and language options should have already been set during the Windows installation process, however here you can change or refine these settings. It's important to select your correct geographical location in particular, as this determines things like daylight savings adjustments to the system clock.

FORMATS

Select the language format that suits your particular region of the world. This is important for making sure that tools such as spell checkers can operate correctly, and that your currency and time are appropriately displayed. You can also manually alter the date and time display format. For more detailed adjustments of numerical, time, date and currency formats click the 'Additional settings' button.

LOCATION

Select your current physical location from the list.

KEYBOARDS AND LANGUAGES

Click the 'Change keyboards' button to access the advanced settings here. Each tab is covered below:

General: The default input language used for your keyboard should be chosen correctly based on your location and hardware. In many countries that use the western alphabet the keyboard is a standard QWERTY US keyboard. However if you have a different type of keyboard and/or you want to set a different language from the location you are in, click the Add button, select the language you wish to use, then tick the box for the actual keyboard hardware you're using. To see a graphical representation of the keyboard layout, highlight the keyboard type and click the Preview button. On the other hand, if you are not going to use a particular location or keyboard layout, then highlight it on the main list and click Remove. If your keyboard hardware is not being detected correctly you may have to install specific drivers for it.

Language Bar: The Language Bar is a small icon or floating bar which only appears if you have two or more keyboard languages installed. It is used to provide easy access for switching between languages. To alter where the Language Bar is shown, select whether to have it as a floating rectangular box on the desktop or whether it will sit in the Taskbar at the bottom of the screen. If you want to get rid of the Language Bar then select Hidden and also make sure you delete all additional languages from under the General tab above. To alter the appearance of the language bar use the three checkboxes on this page to suit your tastes. To stop the Language Bar appearing when a UAC prompt is shown, see the User Account Control section of the PC Security chapter.

Advanced Key Settings: Here you can set the keyboard shortcut method to switch between languages. The default for switching between input languages is Left ALT+SHIFT to switch language, and CTRL+SHIFT to switch keyboard layouts. You can change this sequence by highlighting the 'Between input languages' item and clicking the 'Change key sequence' button, and you can also assign a key shortcut combination to switch directly to a specific language by highlighting the language in the list and once again clicking the 'Change key sequence' button.

ADMINISTRATIVE

Welcome screen and new user accounts: You have the option of copying your Regional 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 most 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 only available in Windows 7 Professional, Enterprise and Ultimate editions, and is not covered in detail in this book.

< SOUND

All Windows audio-related features are covered 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 and not used by the average home PC user, so it won't be detailed here. Fortunately Microsoft has provided sufficient resources 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 and/or being in a noisy environment.

If you don't use the Speech Recognition functionality, click the 'Advanced speech options' link in the left pane and make sure the 'Run Speech Recognition at startup' box is unticked to prevent unnecessary resource usage.

< 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 7 Ultimate 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. I won't go into a more detailed description of the Sync Center functionality here as it is primarily network-related. For simple syncing between your PC and a portable device, it is best to use the functionality in Device Stage - see the Device Stage section of the BIOS & Hardware Management 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 under other chapters. In particular see the Device Manager section of the BIOS & Hardware Management chapter, the System Protection section of the Backup & Recovery chapter, the Windows Activation chapter, and the Windows Experience Index section of the Performance Measurement & Troubleshooting chapter for more details.

The main unique functionality for System is the Advanced System Settings component which contains a range of important options. You can access these options by clicking the 'Advanced system settings' link in the left pane of the System component in Windows Control Panel, or by going to Start>Search Box, typing *systempropertiesadvanced* 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 default computer name of *[username]*-PC is perfectly fine. If for some reason you wish to change this, 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 BIOS & Hardware Management chapter.

ADVANCED

This section has four main sub-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 Virtual Memory component of the Advanced tab is covered under the Windows Memory Management section of the Memory Optimization chapter; the Processor Scheduling component is covered under the Task Manager section of the Performance Measurement & Troubleshooting chapter; and the Data Execution Prevention tab is covered under the Data Execution Prevention section of the PC Security chapter.

User Profiles Settings: This area allows you to view and if necessary change User Profiles, i.e. the profiles which hold all the Windows Desktop and User Account-related settings for each user. See the Advanced Settings section of the User Accounts chapter for more details.

Startup 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 which are all configured by Windows 7 when it first installs, and for the most part are always set appropriately. You should not change these unless you have specific knowledge of what it is you are about to change, as most of them are necessary for Windows and various programs to function correctly. Many of them can be 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 here are covered 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. While this is an extremely useful feature when you're on a trusted network (e.g. your work network), it is a security risk for the average home PC user, or when you are on an untrusted network. I recommend that you disable (untick) the 'Allow Remote Assistance connections to this computer' box and only enable it if prompted by a 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 a trusted individual. Leaving these features enabled when you don't use them is a security risk, so disable them whenever they're not in use. There are also relevant services you may wish to disable - see the Services chapter.

< TASKBAR AND START MENU

This component accesses Taskbar and Start Menu-related settings which are all covered in the Taskbar and Start Menu sections 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 which automate the process of troubleshooting common problems. This functionality is covered in detail in the Troubleshooting section of the Performance Measurement & Troubleshooting chapter.

< USER ACCOUNTS

User Accounts are covered in detail in the User Accounts chapter.

< WINDOWS CARDSPACE

Windows CardSpace is form of digital identity verification card which you can use online rather than a username and password combination. You can create a Personal Card or a Managed Card, with Personal Cards being for personal use, but less reliable and less likely to be accepted for important transactions since they rely on you to enter and store all the details on your own PC (though the data is encrypted); Managed Cards are designed primarily for business use and are created by a third-party provider who manages the card for you, thus independently verifying who you are. Whether you use CardSpace is up to you. You should have no need to set this system up until you run into a site which uses it. You can then decide whether to proceed, and whether to only use a Personal Card or set up a Managed Card as well.

< WINDOWS DEFENDER

Windows Defender is a security feature of Windows covered in detail in the Windows Defender section of the PC Security chapter.

< WINDOWS FIREWALL

The Windows Firewall is a security feature which is covered in detail in the Windows Firewall section of the PC 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, while this chapter is primarily a set of references to other chapters in this book, it is still useful for running through to ensure you haven't missed any particular Windows setting or feature. Also make sure to keep an eye on your Windows Control Panel and remove any unnecessary components installed there by third party software on a regular basis.

STARTUP PROGRAMS

Windows needs to load a range of programs into memory during its startup procedure, including drivers, applications and services required to provide the main functionality in Windows. Windows 7 has noticeably improved the time it takes to get to the Windows Desktop by refining technologies designed to speed up boot time introduced in Windows Vista. Improvements to ReadyBoot and SuperFetch, as well as loading certain programs, scripts and services in the background with a lower priority and/or loading them after the Windows Desktop has appeared all contribute to Windows 7's decreased boot time.

Regardless of the improvements in Windows 7's boot time, removing unnecessary startup programs, services and tasks is still strongly recommended, as it helps to further reduce excessive loading both during and immediately after Windows startup, and more importantly, will reduce unnecessary background resource usage, which in turn improves overall responsiveness, reduces stuttering, and prevents program conflicts and crashes.

In this chapter we look at the correct way to find, identify and properly remove unnecessary startup programs. Details of how Windows 7's startup behavior is optimized, as well as information on post-startup processes, are provided in the Memory Optimization, Drive Optimization and Services chapters.

< FINDING STARTUP PROGRAMS

The first step in the process is to find the names of all 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 Software Explorer utility provided in Windows Vista has been removed in Windows 7, but another valuable built-in Windows utility for identifying startup programs is the Microsoft System Configuration Utility (MSConfig). To access it, go to Start>Search Box, type *msconfig* 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.

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; these can be seen under the Startup tab. You will then be able to observe firstly how much of an impact your startup programs are having on startup time and on post-startup drive usage. Then you can try to use all your common programs and features, and 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 in the next section to see how to correctly identify the individual startup items using MSConfig.

Startup: This tab under MSConfig shows all the current programs which load into memory at Windows startup. A few of these may relate to Windows functionality, such as Desktop Gadgets. Most of them are for third party programs, whether from Microsoft or other manufacturers. You should note the details under the Manufacturer column, as well as the file path and filename shown under the Command column, as this information will help you determine the program or feature to which this startup item relates. The Location column shows where in the Windows Registry the command to run this particular file resides, which is useful for permanent removal. Any item here can be temporarily disabled by unticking the box next to its name, which is a good way of testing to see which startup items relate to which functionality before deciding to permanently disable or remove them. However MSConfig is not the correct place to permanently disable or remove a startup program - see the methods below for that purpose.

REGISTRY EDITOR

The Registry Editor is a Windows tool detailed under the Windows Registry chapter. To launch the Registry Editor go to Start>Search Box, type *regedit* and press Enter. Below is a brief run-down of the primary locations where startup items are held in the Registry, and how to permanently remove them. The Windows Registry holds a record of the programs to launch at startup in four 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]
```

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 which run at every startup, and those under `RunOnce` being temporary items which only run for the next bootup. You cannot temporarily disable a startup item here, 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 Registry in part or in full, as detailed under the Backup & Restore the Registry section of 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. 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; this is what makes Autoruns so valuable for a range of purposes. Most of the entries shown are required for various programs to run, and the vast majority are Microsoft items which Windows 7 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 to remove core Windows items, go to the Options menu and tick the 'Hide Windows Entries' item, and also make sure there is a tick against the 'Verify Code Signatures' item. Then click the Refresh icon on the taskbar or press F5 to update the list under the Everything tab. The list of items shown will be reduced, with only items primarily relating to third party programs showing, making it easier to spot unnecessary items.

One of the key benefits of Autoruns is that it allows you to temporarily disable any item, as well as choosing to permanently remove it. This means that similar to MSConfig, 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 not only startup programs, but also various components related to a range of programs, including context menu entries, Services, and third party Gadgets. Click on each suspicious item and look in the Details Pane at the bottom of the program for more information, then right-click on it and select Properties and look under the Details tab for yet 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 on the Internet should allow you to accurately identify the functionality that component relates to.

You can then disable any suspected unnecessary item temporarily by unticking 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.

< IDENTIFYING STARTUP PROGRAMS

Once you have noted the names of all the startup programs and files using one or more of the utilities above, and you have a reasonable suspicion as to which are unnecessary, the next step is to make sure you correctly identify their functionality and determine whether they are truly necessary. Some features require that a program or certain component(s) load into memory at Windows startup otherwise they may not function correctly or at all. Other times a startup component is not necessary for a program to function properly, or provides optional functionality for particular features you may not use. Some startup items may even be part of malware or other undesirable software and hence must be removed.

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 like 'Load with Windows', 'Load at startup', 'Enable System Tray', 'Enable Shell Integration', and so on. In many cases you will be given the option to disable any such settings, and you may also see text or a warning which explains whether doing so will affect the program's functionality in any major way. Typically disabling a program component from loading at startup means it won't be running in the background after Windows loads - you will have to manually open it yourself. For some programs this is not an issue, and in fact is desirable; for others it can prevent them from working automatically in the background or even from being able to be launched. The aim is to minimize the number of programs and components running in the background at all times, but not damage functionality for necessary programs.
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 the *\Windows\System32* directory) 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:

   Google
   Windows Startup List Database
   ProcessLibrary
   Security Task Manager List

   Some of the more obscure or new Windows 7 system files may not be listed in the sources above, or typically have ambiguous or even false information regarding potential malware, so reading through a large number of Google search results is the best method for finding the truth.
4. Run the malware scanners recommended in the PC Security chapter to ensure that none of the startup files relate to malicious software. If any such files are flagged as malware by your scanner, you can usually click on their names or a provided link to find out more details from the scanner's own database.

5. Use MSConfig or Autoruns to temporarily disable the startup item(s) in question - that is, untick it in Autoruns or MSConfig - 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.

< REMOVING STARTUP PROGRAMS

Once you've followed all the steps above, and you're confident that you've found a truly unnecessary startup item, the final step involves permanent removal. You can do this in several ways:

§ Go to the program in question and make sure there are no options to disable it from running at Windows startup. As noted earlier, if any options such as 'Load with Windows', 'Load at startup' or similar exist, disable them otherwise if you just manually delete the item it may simply be recreated each time you boot into Windows or start that program.
§ Go to Autoruns, right-click on the item and select Delete.
§ Go to the Registry Editor, find the item under the relevant startup key, highlight it in the right pane and select Delete. Registry Editor does not have any undo capabilities, so it is best used as a last resort, or only if you are completely certain.

Once the item is removed from your startup, you should reboot Windows and re-check to see if it is indeed gone. In a worst case scenario, if at any point any of your programs start to behave strangely or do not function at all, then uninstall and reinstall that particular program and its relevant startup items will be recreated. It's not wise to permanently remove any Microsoft startup programs unless you are completely certain that you will never use such functionality.

Having removed unnecessary startup programs make sure to run through the Services chapter and disable any unnecessary services as well, particularly third party services.

< STARTUP PROBLEMS

Windows 7 is designed to prioritize boot programs, services and drivers such that the system reaches the Desktop as quickly as possible, and if necessary continues loading programs as required. This means that the removal of startup programs may not noticeably improve system startup time. The best way to measure bootup time is not to use some arbitrary point of reference, but to either time it from the moment you press the power button to the precise moment your desktop appears, or better yet, for a completely objective measure of your startup time, or to troubleshoot startup problems, view specific startup statistics in Event Viewer.

To view your startup and shutdown statistics and any associated problems follow these steps:

1. Go to Start>Search Box, type *event viewer* then press Enter to open Event Viewer.
2. In the left pane go to Applications and Services Logs>Microsoft>Windows>Diagnostics-Performance.
3. Click on the Operational log item shown, and in the middle pane you will see a range of events.
4. Typically there will be items with the Task Category 'Boot Performance Monitoring' or 'Shutdown Performance Monitoring' (Event IDs of 100, 200 or similar). Click on the more recent of these to see details - you can click the 'Date and Time' column to sort by date if necessary.
5. In the bottom pane 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 double-click on any event to get more details, and to see if any particular program or driver may be slowing down performance.

To quickly determine if the removal or disabling of any startup items is causing an error, you can use the Reliability Monitor as follows:

1. Go to Start>Search Box, type *reliability* and 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 and more details will appear in the bottom pane. Double-click on the details shown to see the crash report, noting the file which is involved - if it is a file you disabled it may be necessary, but by the same token it may be unnecessary and simply throwing up a warning each time the program looks for it, so this is not a definitive sign that you need to re-enable it.
4. Do additional research in the case of each error (red cross).

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, though it can help to do that. 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, drivers or the program which is crashing.

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 which has 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, so if you belong in this category, then make absolutely sure you follow the procedures in this chapter and remove all unnecessary startup items and minimize what runs at startup.

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 recommend that after each installation of any new program you open MSConfig and quickly look under the Startup and Services tabs to see whether new item(s) have been added, and 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 7 contains several changes to the way in which services are handled from previous versions of Windows. It continues the ability, introduced in Vista, to set a service to 'Automatic (Delayed Start)' which means that it will only load after the Windows startup process has completed. However Windows 7 adds to that the ability to Trigger Start or Stop a service, meaning such services will begin or end only when a certain event is triggered, further reducing background resource usage. Windows 7 also carries over Vista's 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 services in Windows 7 are already quite optimized and this is one of the main contributors to Windows 7's improved startup time and reduced resource usage.

Services are user-configurable under Windows 7, just as they were in Windows Vista and XP. As such there is scope to improve system resource usage and startup time by changing your services configuration. However in Windows 7 most unnecessary core Windows services have already been set as Manual, which means they will not run in the background nor use any resources if they are not required. Therefore the primary focus of this chapter is on identifying and reconfiguring third party services inserted by installed programs, as these can have a noticeable impact on the stability and performance of Windows.

< SERVICES UTILITY

The built-in Services utility gives you the ability to view and edit your Service configuration. To access the Services Utility, you can either find it under the Administrative Tools component of the Windows Control Panel, or go to Start>Search Box, type *services.msc* and press Enter. This opens the Services utility, displaying all installed services by name, showing you whether they are currently running or not under the Status column, whether they are set for Automatic, Automatic (Delayed Start), Manual or Disabled under the 'Startup type' column, along with a brief description. You can see the details of each service by left-clicking on it and the default Extended view will show the description to the left of the service. 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 where the actual program file resides for the service under the 'Path to executable' item, and you can also manually Start, Stop or Pause/Resume a service as applicable. 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. In Windows 7 it can also be started with a specific trigger event. It does not reside in memory nor load at startup otherwise.

§ *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 7 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, so the best thing to do is save a snapshot of your current service configuration. To do this, 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.

For convenience sake, I have also listed my default Windows 7 Ultimate service configuration in the table later in this chapter under the column labeled 'Startup Type (Default)', but again, remember that these can vary from system to system, so as a precaution take the steps above before altering your own services.

CUSTOMIZING SERVICES

The Windows 7 Service Controller has already been refined to configure your services such that you have full functionality for all the features you use in Windows 7, while also disabling those which are unnecessary. For our purposes, the main reason we would want to change the service settings is to:

§ Help speed up Windows startup time especially on 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 7 services are configured as Manual, 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 other versions of Windows are already evident in Windows 7 by default. Services configuration should no longer be considered a significant performance tweak. In fact I warn against setting any service to Disabled unless part of a specific step to deliberately disable an unnecessary function in Windows. There is no other benefit to disabling a service - a service set to Manual usually takes up no resources, yet provides a safeguard because if it is truly needed it can usually be automatically restarted by Windows or a program. For example the Bluetooth Support Service is set to Manual and only starts running if a Bluetooth device is connected to your PC, so setting it to Disabled provides no benefit whatsoever. Only disable a service if you are absolutely certain that its functionality is not needed or 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 which do this.

Furthermore, some services can be very misleading as to the impact any changes to their configuration might have. For example, disabling the Server service results in the disabling of the display of Previous Versions for files and folders, despite no indication that it will do so from its name or description. I stress again that you should not consider the disabling of services as some sort of major performance tweak. In particular, if you change several services at once, it can sometimes be extremely difficult to track back your problems to a particular service change. Indeed if you are not an advanced user, I recommend leaving all of the Windows services at their defaults, and focusing on only adjusting any services installed by third party programs, as covered in the Non-Microsoft Services section of this chapter.

With all of the above in mind, what follows is a list of the services in Windows 7, the defaults as found on my Windows 7 Ultimate 64-bit system, and suggestions for potential service changes on a home PC.

Service Name	Startup Type (Default)	Potential Change	Notes
ActiveX Installer (AxInstSV)	Manual		
Adaptive Brightness	Manual		
Application Experience	Manual		
Application Identity	Manual		
Application Information	Manual		
Application Layer Gateway Service	Manual		
Application Management	Manual		
Background Intelligent Transfer Service	Automatic (Delayed Start)		
Base Filtering Engine	Automatic		
BitLocker Drive Encryption Service	Manual		
Block Level Backup Engine Service	Manual		
Bluetooth Support Service	Manual		
BranchCache	Manual		
Certificate Propagation	Manual		
CNG Key Isolation	Manual		
COM+ Event System	Automatic		
COM+ System Application	Manual		
Computer Browser	Manual		
Credential Manager	Manual		
Cryptographic Services	Automatic		
DCOM Server Process Launcher	Automatic		
Desktop Window Manager Session Manager	Automatic		
DHCP Client	Automatic		
Diagnostic Policy Service	Automatic		
Diagnostic Service Host	Manual		
Diagnostic System Host	Manual		
Disk Defragmenter	Manual	Disabled	Can be disabled on systems where only SSDs are used.
Distributed Link Tracking Client	Automatic		
Distributed Transaction Coordinator	Manual		
DNS Client	Automatic		
Encrypting File System (EFS)	Automatic		
Extensible Authentication Protocol	Manual		
Fax	Manual		
Function Discovery Provider Host	Manual		
Function Discovery Resource Publication	Automatic		
Group Policy Client	Automatic		
Health Key and Certificate Management	Manual		
HomeGroup Listener	Manual		
HomeGroup Provider	Manual		
Human Interface Device Access	Manual		
IKE and AuthIP IPsec Keying Modules	Manual		
Interactive Services Detection	Manual		
Internet Connection Sharing (ICS)	Disabled		
IP Helper	Automatic		
IPsec Policy Agent	Manual		
KtmRm for Distributed Transaction Coordinator	Manual		
Link-Layer Topology Discovery Mapper	Manual		
Media Center Extender Service	Disabled		
Microsoft .NET Framework NGEN v2.0.50727_X64	Manual		
Microsoft .NET Framework NGEN v2.0.50727_X86	Manual		
Microsoft iSCSI Initiator Service	Manual		
Microsoft Software Shadow Copy Provider	Manual		

Service Name	Startup Type (Default)	Potential Change	Notes
Continued...			
Multimedia Class Scheduler	Automatic		
Net.Tcp Port Sharing Service	Disabled		
Netlogon	Manual		
Network Access Protection Agent	Manual		
Network Connections	Manual		
Network List Service	Manual		
Network Location Awareness	Automatic		
Network Store Interface Service	Automatic		
Offline Files	Automatic	Manual	Not useful for PCs which do not synchronize with other computers.
Parental Controls	Manual		
Peer Name Resolution Protocol	Manual		
Peer Networking Grouping	Manual		
Peer Networking Identity Manager	Manual		
Performance Counter DLL Host	Manual		
Performance Logs & Alerts	Manual		
Plug and Play	Automatic		
PnP-X IP Bus Enumerator	Manual		
PNRP Machine Name Publication Service	Manual		
Portable Device Enumerator Service	Manual		
Power	Automatic		
Print Spooler	Automatic	Manual	Not useful for PCs which don't use a printer or virtual printer (e.g. PDF makers).
Problem Reports and Solutions Control Panel Support	Manual		
Program Compatibility Assistant Service	Automatic		
Protected Storage	Manual		
Quality Windows Audio Video Experience	Manual		
Remote Access Auto Connection Manager	Manual		
Remote Access Connection Manager	Manual		
Remote Desktop Configuration	Manual		
Remote Desktop Services	Manual		
Remote Desktop Services UserMode Port Redirector	Manual		
Remote Procedure Call (RPC)	Automatic		
Remote Procedure Call (RPC) Locator	Manual		
Remote Registry	Manual	Disabled	Poses a security risk - only enable if requested by a trusted tech support person.
Routing and Remote Access	Disabled		
RPC Endpoint Mapper	Automatic		
Secondary Logon	Manual		
Secure Socket Tunneling Protocol Service	Manual		
Security Accounts Manager	Automatic		
Security Center	Automatic (Delayed Start)	Disabled	Can be disabled if you want to completely disable Action Center.
Server	Automatic		
Shell Hardware Detection	Automatic		
Smart Card	Manual		
Smart Card Removal Policy	Manual		
SNMP Trap	Manual		
Software Protection	Automatic (Delayed Start)		

Service Name	Startup Type (Default)	Potential Change	Notes

Continued...

SSDP Discovery	Manual		
Superfetch	Automatic	Disabled	Can be disabled on systems using an SSD as primary drive.
System Event Notification Service	Automatic		
Tablet PC Input Service	Manual		
Task Scheduler	Automatic		
TCP/IP NetBIOS Helper	Automatic		
Telephony	Manual		
Themes	Automatic		
Thread Ordering Server	Manual		
TPM Base Services	Manual		
UPnP Device Host	Manual		
User Profile Service	Automatic		
Virtual Disk	Manual		
Volume Shadow Copy	Manual		
WebClient	Manual		
Windows Audio	Automatic		
Windows Audio Endpoint Builder	Automatic		
Windows Backup	Manual		
Windows Biometric Service	Manual		
Windows CardSpace	Manual		
Windows Color System	Manual		
Windows Connect Now - Config Registrar	Manual		
Windows Defender	Automatic (Delayed Start)	Manual	Can be set to Manual if using Microsoft Security Essentials.
Windows Driver Foundation - User-mode Driver Framework	Automatic		
Windows Error Reporting Service	Manual		
Windows Event Collector	Manual		
Windows Event Log	Automatic		
Windows Firewall	Automatic		
Windows Font Cache Service	Manual		
Windows Image Acquisition (WIA)	Automatic		
Windows Installer	Manual		
Windows Management Instrumentation	Manual		
Windows Media Center Receiver Service	Manual		
Windows Media Center Scheduler Service	Manual		
Windows Media Player Network Sharing Service	Manual		
Windows Modules Installer	Manual		
Windows Presentation Foundation Font Cache 3.0.0.0	Manual		
Windows Remote Management (WS-Management)	Manual		
Windows Search	Automatic (Delayed Start)	Disabled	Can be disabled if you want to disable all Windows Search functionality.
Windows Time	Manual		
Windows Update	Automatic (Delayed Start)		
WinHTTP Web Proxy Auto-Discovery Service	Manual		
Wired AutoConfig	Manual		
WLAN AutoConfig	Manual		
WMI Performance Adapter	Manual		
Workstation	Automatic		
WWAN AutoConfig	Manual		

NON-MICROSOFT SERVICES

You may notice that your services list has several additional services that are not in the list above. This is because particular programs and drivers, 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. However, due to poor programming practices, the software developer may set a service to run automatically at launch and hence always be running in the background, when this is neither required nor desirable. As such, in many cases these 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 functionality in any significant way.

The quickest and easiest method of displaying all third party services is to run MSConfig (See the Startup Programs chapter), 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. In MSConfig, having ticked the 'Hide All Microsoft Services' box, 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 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, press CTRL+ALT+Delete and select 'Start Task Manager', click the 'Show Processes from all users' button, then under the Services tab see if you can find the filename for the service you're examining. Right-click on this filename and select 'Go to Process'. This may show you the program which is running it, though often it's just the generic Service Host process *svchost.exe*.
5. Search Google or one of the databases shown under the Startup Programs chapter for this particular filename. This should give you an indication of what its functionality is related to. If necessary you can temporarily Stop the service, or set it to Disabled and reboot to see what functionality it impacts on.

With appropriate research and testing you should be able to either set to Manual, or if all else fails, set to Disabled a range of these third-party services. In a few cases particular programs will not function correctly unless their service is left at Automatic. If in doubt, leave them at their default settings.

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 if you have changed a critical service such that you cannot successfully boot back into Windows to change it back, 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', 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, 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 around the name. For example, to start the Application Layer Gateway Service, you can use either command 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 are new to Windows 7, and are one of the optimizations which help reduce the number of active services actually running at any time. 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 which 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 when the device is disconnected. Services need to be written to take advantage of these new features, so many third party programs will be unlikely to use them and hence the recommendation to disable unnecessary third party services still stands.

You cannot view the detailed aspects of trigger-start services in the normal Services utility in Windows. 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 tabletinputservice
   ```

   This will show that the Tablet PC Input Service which is set to Manual by default is set to start for the trigger event Device Interface Arrival, meaning it is triggered by the connection of a tablet PC device.

Most services are not configured for triggers, as they are called by particular programs or features and hence are triggered in that manner. Furthermore a service that has its own dependent services running can't be stopped in response to a trigger event, so this is not suitable for services with dependencies. However if you want to attempt to add a trigger to a particular service, then 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 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 unnecessary and not related to default Windows functionality - 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.

Once again, use caution 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 default Windows service, so only attempt deletion of known third party services.

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; others argued that many services should be disabled to increase performance. With the coming of Windows 7, the debate has all but been settled: there is now not much of a case to be made in disabling the core Windows services, as Windows 7 has already been optimized in this regard by Microsoft, and any changes are more likely to see problems rather than benefits ensuing. 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 required for SSD users, but only under certain circumstances, and mainly for advanced users to consider.

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 if necessary alter the configuration of unnecessary services installed by third party programs. Due to poor 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 interested in fast Windows performance, nor do they care about instigating inconvenience or additional resource usage on your system as long as it serves the purpose required by their software. This is why editing services is still essential - for removing these unnecessary third party impositions.

< BACKGROUND TASKS

There is one more type of background program which is similar to a service, in that it involves the running of background processes: scheduled tasks. These tasks are scheduled to run in the background 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 otherwise idle for example. However 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. This section looks at the cases where manual intervention may be required for background tasks.

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 the main utility for managing tasks in Windows: Task Scheduler. You can access the Task Scheduler at any time by going to Start>Search Box, 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. Importantly, the current status of the 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, in the section at the bottom of the middle pane when a task is highlighted. Or you can double-click on it, or right-click on it and select Properties to open a new window for this purpose. Each tab of the Task Properties 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 which runs 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 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 defragmentation during the use of a system-intensive program or game.

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 is disabled by default. To enable task history, click the 'Enable all task history' link in the right pane of Task Scheduler.

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 box 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 in the command prompt 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 for example.

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. Start the Create Basic Task wizard.
3. Enter an appropriate name for the task, e.g. Email Alert.
4. On the Trigger page, under 'When do you want the task to start', select 'When a specific event is logged' and click Next.
5. 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.
6. Under the 'What action do you want the task to perform', select 'Send an e-mail' and click Next.

7. Enter your email details and the subject and body of the message, plus any attachments you wish to send.
8. Click Finish to implement the task.

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 should be 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 tasks, as this can make Windows less secure and unable to diagnose and maintain itself properly.

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 diagnostic or system maintenance functions.

As this chapter has explained, configuring any service or background task must be done with thought and research. These are not major performance optimization steps, the main purpose of editing services and background tasks is to either remove the unnecessary intrusions of third party programs, or fine tune certain features if you are an advanced users. If you are not confident in what you are doing, or don't have the time or patience to do proper research and sort out your own needs, then do not alter your services or tasks in any way. And most importantly, do not consider the disabling of a range of Windows services to be some sort of optimization procedure - they are already highly optimized by default in Windows 7.

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 even resize open windows for example, the Registry will be updated with key pieces of information recording these changes.

The Windows Registry remains much the same in Windows 7 as it has been in previous versions of Windows. As of Windows Vista, some improvements were made to decrease the possibility of Registry corruption. Furthermore Virtualization support was 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 - see the User Account Control section of the PC Security chapter for more details.

The most significant change to the Windows Registry in Windows 7 is the removal of Registry Reflection for 64-bit operating systems. In previous versions of Windows 64-bit, the Windows 32-bit on Windows 64-bit (WOW64) emulation provided a special alternate view of the Registry for 32-bit applications, and Registry reflection copied keys for 32-bit and 64-bit applications back and forward between these two views to keep them synchronized. This feature caused some inconsistencies and has been removed in Windows 7 64-bit, as detailed in this Microsoft Article. In practice there is no real impact on users from this change.

This chapter examines the Windows Registry in detail, both in terms of its structure and how it operates, as well as the way in which users can change Registry settings to implement a range of customizations in Windows 7. Knowledge of the Windows Registry is essential in troubleshooting and system recovery, along with fine tuning system performance and functionality.

< BACKUP AND RESTORE THE REGISTRY

The Windows Registry is a critically important component of Windows 7. By default, any changes made to the Registry can't be easily reversed, so it is vital to regularly 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 7 which ultimately only the reinstallation of Windows can resolve. To avoid this, you should regularly back up the entire Registry.

Fortunately Windows has a built-in tool for quickly taking a snapshot of the Registry and other important system files and settings: the System Restore feature - see the System Protection section of the Backup & Recovery chapter for details. I strongly recommend that you leave System Restore enabled, and manually create a restore point before editing the Registry or undertaking any other 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 quickly and easily undo any changes made to the Registry without any impact on your personal files or folders or your other program settings.

If you experience problems booting into Windows after a change to the Registry, you can also attempt to use the 'Last known good configuration' option available in the Advanced Boot Options menu, accessible by repeatedly pressing F8 during Windows startup - see the System Recovery section of the Backup & Recovery chapter.

If you experiment quite frequently with the Windows Registry and want to take a full independent backup of your entire Registry, you can use the free ERUNT tool to make such a backup. Download this program and install it by right-clicking on it and selecting 'Run as Administrator' (or with UAC disabled). Note that during the installation of Erunt you should answer 'No' if asked whether you want Erunt to be placed in the startup folder, as this is unnecessary. To make a backup of the Windows Registry using Erunt, launch the program by right-clicking on it and selecting 'Run as Administrator'. You will be prompted to backup your Registry to a folder, which you should accept by clicking OK until the backup has been made. If you want to restore this backup at any point, simply go to the directory where the backup was made, typically *\Windows\ERDNT\[Date of backup]*, and launch the *ERDNT.exe* file there to restore that backup. On systems with a separate System Reserved Partition - as covered under the Installing Windows section of the Windows Installation chapter - you may receive an error when running this tool. This is normal and can be safely ignored. For most users Erunt is unnecessary, as long as System Restore is enabled and restore points are taken regularly.

BACKING UP PORTIONS OF THE REGISTRY

Restoring a full Registry backup or using a previous restore point can be overkill if you simply want to undo a single change to the Registry. Since most users typically make a range of 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 lengthy 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, not the entire Registry. 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 quickly and easily. Reboot or logoff and logon again if necessary to implement the change.

While you can use the Export function of the Registry Editor to take a full snapshot of the entire Windows Registry by selecting the All option when prompted, any Registry backup made in this manner cannot be restored properly and is not a substitute for taking full Registry backups as covered further above.

< REGISTRY EDITOR

The Windows Registry Editor is the primary built-in Windows tool used to view and edit the Windows Registry. To access it go to Start>Search Box, type *regedit* then press Enter. The structure of the Registry is explained further below, but essentially the Registry Editor displays a Windows Explorer-like view of the database as a range of folders and subfolders which 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 a powerful tool, and is the most direct method of altering the Registry. Using Registry Editor 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 I recommend against using any third party tool which automatically 'optimizes' or makes changes to the Registry, and in particular I discourage the use of pre-made .REG Registry scripts which you can download. While very convenient, in both cases the use of these methods, aside from being a security risk, can result in a range of problems which you will not be able to resolve. If you feel you are not advanced enough to learn about 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 how to use the Registry Editor.

REGISTRY STRUCTURE

When you first open the Registry Editor, you can 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 folder, display settings and Control Panel settings are stored here, and saved in the *ntuser.dat* system file found under the root directory of each 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 which apply to the entire PC and not just an individual User Account.

`HKEY_USERS` - This section of the Registry holds all 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 hold 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.

§ 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, etc.). This then 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 words, 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 Windows 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 Windows Explorer interface, you can also edit, create or delete Registry entries.

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=530
```

The text above indicates 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 that it says 600.
6. You can edit this value data by entering a new value if you wish, such as 530.
7. As soon as you click OK the change is automatically saved to the Registry.
8. You can close Registry Editor if you wish.

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 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 tends to point quite clearly to the likelihood that altering this value controls the rate at which the cursor blinks when displayed in normal Desktop interfaces.

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 explore the Registry on your own and deduce what various entries mean.

This chapter does not contain any specific Registry customizations you can use, however a wide range of such tweaks are spread throughout this book in their relevant chapters.

I strongly suggest using one or more of the backup methods covered earlier in this chapter to make an appropriate backup of the entire Registry and/or the branch you are editing before making any change to the Registry. The Registry Editor does not have an undo function of any kind.

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 to see if the full path matches that which you desire.

The Registry Editor does not give any confirmation or sign 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 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 implement the 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 if in doubt.

REGISTRY PERMISSIONS

In certain cases if you attempt to edit an entry in the Registry, you may see an error or 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 PC Security chapter for ways of taking ownership and thus giving yourself full permission to make changes to these areas.

As a final note, 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 clicking the Start button, then clicking the arrow next to the Shutdown button and selecting 'Log off'. 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 Windows Explorer chapter.

< 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 given the improvements to the Registry in Windows 7, on balance I recommend that you do not run 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.

However 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 this topic.

The programs you can use for this functionality are the free CCleaner utility, which has a Registry cleaning ability, or the JV16 PowerTools utility which requires purchase after a trial period. I recommend and cover the CCleaner Registry-related functionality below, as it is more than sufficient for our purposes:

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 - leave a tick next to these entries.

7. Untick any others unless you are absolutely sure they are safe to remove.
8. Click the 'Fix selected issues' button to commence removal of the ticked Registry entries.
9. When prompted, click Yes to backup Registry changes and save the backup to an appropriate location.
10. 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 caused by Registry cleaning by double-clicking the backed-up .REG file you saved in Step 9 above and rebooting. Note that CCleaner's primary functionality is covered under the CCleaner section of the Cleaning Windows chapter.

The NTRegOpt utility, by the same author as the Erunt utility covered earlier in this chapter, does not clean or alter the Registry, but instead can compress it to take up less space. Similar to Erunt, it requires that you install and launch it with full Administrator privileges, or disable UAC, for it to work properly. Furthermore it will show an error if you have a System Reserved Partition on your drive, which can be ignored. Registry compression is not of major importance anymore, given the risks involved and the fact that saving a few Megabytes of memory is relatively insignificant compared to the total installed RAM on most systems.

Once again, 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 7. Any form of automated change to the Registry can result in a range of problems and unusual behavior in Windows.

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, and importantly, check the Backup & Recovery chapter both to read details of how to protect yourself against, and if necessary recover from, any catastrophic changes to the Registry.

Finally, it is 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 can be considered absolutely necessary, and if you don't feel comfortable editing the Registry at the moment, skip all Registry-related steps, and come back to them when you feel more confident and have more knowledge about the Registry.

GROUP POLICY

Group Policy is designed primarily for Administrators to alter the way in which Windows behaves for different user groups on a network or on a particular machine. When a Group Policy is in place, it tells Windows to override the normal settings and use those specified by the policy. Group Policy remains much the same in Windows 7 as it was 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. However aside from being covered briefly under the Administrative Tools section of the Windows Control Panel chapter, detailing PowerShell usage is also 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. However 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 is done via the Local Group Policy Editor, which is only available in the Professional, Ultimate and Enterprise editions of Windows 7. For other editions of Windows, try the Registry method covered further above to change these settings.

To access the Local Group Policy Editor go to Start>Search Box, type *gpedit.msc* 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. Note that 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 PC 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 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 defaults 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.

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 remove the items from the list to restore the relevant items in Windows Control Panel.

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. For example, under the User *Windows Components\Desktop Gadgets* subfolder here, the 'Turn off desktop gadgets' setting does precisely that if Enabled. Similarly, if you wish to disable the Flip 3D animated 3D desktop task switcher, you can do so under the *Windows Components\Desktop Windows Manager* subfolder, using the 'Do not allow Flip3D invocation' setting. Browse through all the subfolders and settings here to see if any of them suit your purposes. Keep in mind that it is not wise to use Group Policy to disable settings or features which can be adjusted using normal Windows options.

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 obviously provides less protection against potential problems and is not recommended.

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(s) you want to remove to Enabled.

TURN OFF THUMBNAILS

Folder: User Configuration\Administrative Templates\Windows Components\Windows 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 Aero Shake

Folder: User Configuration\Administrative Templates\Desktop
Setting: Turn off Aero Shake window minimizing mouse gesture

If Enabled, disables the Aero Shake feature, but does not affect Aero Snap functionality.

Add Search Internet Link to Start Menu

Folder: User Configuration\Administrative Templates\Start Menu and Taskbar
Setting: Add Search Internet link to Start Menu

If Enabled, adds a 'Search the Internet' link to the Start Menu, which appears whenever you enter a search term in the Start>Search Box. Clicking this link opens your default web browser and searches on the Internet using your default browser search engine provider.

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 be used to prevent a user from attaching such a device and transferring undesirable software such as malware to the system for example.

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 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 WINDOWS LIVE MAIL 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, Medium and Low risk attachments. By moving certain file types into the Medium or Low category you can access them more easily in Windows Live Mail for example, however this also creates 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. However 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 re-enable or use certain functionality - remember, 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 which underwent a dramatic change as of Windows Vista, and has been further improved in Windows 7. The integrated Windows Desktop Search engine in Windows allows you to quickly find specific files, folders, emails and even programs and Windows features. Searching is no longer about knowing specific details like filename, creation date or location. By typing in a partial or whole word or sentence, the Windows search engine can display the most likely targets almost instantly.

However Windows Search is more than a search tool. People may claim that they already know where all the files on their PC are, and so search isn't necessary. This is not true - Windows Search functionality speeds up access to all programs, files and features. For example, to open a particular picture or song quickly, instead of navigating to it in Windows Explorer you can click the Start button, type part of its name or related information in the Search Box, and it will be instantly displayed in the Start Menu, ready for launching. You can also remove many of your Desktop, Start Menu and Taskbar icons because you can now rapidly access those same programs by simply entering their name in the Search Box instead.

The changes to Windows Search in Windows 7 involve the display of Windows Control Panel items as part of search results, automatically indexing all items linked in your Libraries, and the new Federated Search, which incorporates search functionality that goes beyond looking for resources on your local PC. The display of detailed search results also benefits from the new Content View introduced in Windows 7.

In this chapter we examine the various ways in which searching is possible in Windows 7, 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 Windows Desktop or pin them to the Start Menu or Taskbar for example, there are still many more files and programs on your system which you might want to access as quickly as possible, and the search functionality can help in that regard.

SEARCH BOX

The primary search location in Windows 7 is the Search Box found at the bottom of the Start Menu, accessed when you click the Start button. Extensive use of this Start>Search Box functionality is already made throughout this book to quickly find and launch particular Windows programs, such as typing *services.msc* and pressing Enter to quickly launch the Services Utility in 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 for example. Or if you want to launch the Windows Calculator utility, you can simply type *calc* and press Enter in less time than it would take to click All Programs, then Accessories then Calculator on the Start Menu. Or if you want to launch a web link, type a search starting with http:// and press Enter, and your default web browser will automatically open at the link you have entered. There are many uses for the Search Box beyond merely searching for lost files.

When you conduct a search, the results of any search in the Start Menu Search Box are displayed under one or more of the following search result categories:

§ *Programs* - Lists any search results which match installed programs on your system, including built-in Windows programs and associated help files.
§ *Control Panel* - Lists any search results which match Windows Control Panel components, including associated help files and wizards.
§ *Libraries* - Lists any search results which match files or folders in any of your Libraries, with the name of the relevant Libraries displaying as category headings. This includes any custom Libraries you may have created.
§ *Files* - Lists miscellaneous indexed files which don't fall into the above categories, and includes emails.

By default the top matches from each category are displayed initially, but you can see the total number of matches in brackets next to the category heading. Programs used most frequently are displayed first on the list, and then more results are added over time for each category. To see the full list of results in a particular category, click the category header and a Windows Explorer window will open displaying all the results in Contents view. You can also click the 'See more results' link at the bottom of the search results in Start Menu to open a new Windows Explorer window which shows all the file search results (excluding any programs or Windows Control Panel items) across all categories.

Once search results are displayed, you can open the relevant file or launch the relevant program simply by left-clicking on it in the Start Menu, or double-clicking on it in the Windows Explorer window.

The Search Box is also found at the top of most Explorer-based windows, such as in Windows Explorer itself, or the Windows Control Panel window. The difference is that any searches from these locations by default 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 Windows Explorer window, it will only show results from the currently open folder and any subfolders, not across all indexed locations on your PC. However, when the search results are shown, you will be presented with the option of searching in various other locations as well - at the bottom of the search results there is a 'Search again in' section with links to Libraries, Computer, Custom or Internet:

§ *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.
§ *Computer* - If selected, a search is automatically launched across your 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).
§ *Internet* - If selected, a search is automatically launched in your default web browser using your default browser search engine on the current search term.
§ *Custom* - If selected, you will be presented with a list of locations within which Windows will search. This includes all available drive(s) and folder(s) on your system, any network locations, and the Windows Control Panel. Tick the relevant boxes and they will be added to the list, then click OK to begin a full search through those locations on the current search term. The search time will vary depending on whether any folders you have selected are not indexed.
§ *File Contents* - This additional item appears if any of the other search types above are unsuccessful. If selected, Windows will go through the contents of all available files on the system attempting to match your search terms with the contents of any files. This may take a very long time to complete.

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.

ADVANCED SEARCH

A vital consideration for getting the most out of the Search functionality in Windows is how you form your search queries. By default Windows will immediately begin to match letters or partially entered words with indexed files, programs and Windows Control Panel items, almost 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. Because Windows search indexing stores a range information about each file, you can search for particular attributes of the file beyond just its filename - for example, particular words or phrases in its contents, the name of the user, author or artist who created it, the date it was created, etc.

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 which find what you are looking for much faster, plus you can also save these searches for future use - see further below. 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:email* Finds only email messages 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:AVI* Finds any file of the type .AVI.
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 in the Start>Search Box for any PDF file created, modified or accessed some time after 1 January 2009, type the following:

after:>1/1/09 ext:PDF

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.

Search Builder: If you don't wish to remember the Advanced Query Syntax, fortunately Windows 7 comes equipped to allow you to select the most useful filters it determines are relevant to your search, as part of the Search Builder. To access Search Builder, see the drop down box which appears beneath the Search Box in any Explorer-based window once you've entered a search term. Basic filters are provided for you to click on, and a range of commonly used parameters appear for each one when clicked. For example, initiate a search on the term *doc*, and then click the 'Date Modified' filter which appears - you will be presented with a calendar and an additional list of choices for selecting a specific date, such as Yesterday. Selecting one of these filters inserts the appropriately formatted AQS filter into the Search Box along with your search term, helping you to refine your search.

Every time you use a particular filter in Search Builder, additional filters will appear for you to use in conjunction with the ones you are already using. The Search Builder also records your recent search queries and presents them in the drop down box for you to select again if you wish.

Content View: As noted earlier, search results in Explorer-based windows are presented in the new Content view type, which is covered in more detail in the Basic Features section of the Windows 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 as normal, by right-clicking and choosing another option from the View menu. Content view is recommended though, 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 which may be relevant to your search, including filename, metadata, content, etc. Windows assigns each search result a score between 0 and 1000, with 1000 indicating an exact match. It then displays the results ranked by this score, from highest to lowest.

Dedicated Search Window: If for some reason you don't want to use the Start>Search Box or a Search Box in an Explorer-based window, you can launch a dedicated search window at any time by pressing WINDOWS+F, or the F3 key while on the Desktop. This Search Explorer interface has no details to begin with, and awaits input of a search term in the Search Box at the top right. It then turns into a normal Explorer window once a search is initiated, and displays results in Content view as normal, with additional search options displayed at the bottom of the search listing.

Saved Searches: If you wish to save a particular search for future use, either go to the File menu in the search results window and select 'Save search', or right-click on the search results and select 'Save search'. You will be prompted to save the search as a .SEARCH-MS file under the *\Users\[username]\Searches* directory by default, however you can change the directory if you wish. To use a saved search, simply go to the directory above and click on the name of your saved search to view its results immediately. To delete a saved search, right-click on it and select Delete.

FEDERATED SEARCH

Federated Search is a new feature of Windows Search 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 7 allows you to search a range of resources outside your PC - typically on the Internet - via Windows 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, download the relevant .OSDX file, and once installed, open Windows Explorer and check under your Favorites category in the Navigation Pane for a link to that connector.

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 normal text editor like Windows Notepad.
3. Fill in the correct details where prompted throughout the file - enter the normal site name where prompted for SITE NAME (e.g. Google), and enter the normal 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 it, and give it an extension of .OSDX so that Windows 7 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 Windows Explorer window with your Search Connector highlighted in the Favorites category of the Navigation Pane.
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 Windows Explorer and select Remove.

This is a very handy feature, and hopefully more major sites will come to support it with proper full-featured Search Connectors 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:

In indexed locations, search file names and contents. In non-indexed locations, search file names only: If selected, this option provides the fastest but not necessarily the best results. Any terms you enter in a Search Box will be matched against both the filenames and contents of indexed files, but only the filenames of non-indexed files will be checked. This option is recommended as a balance between speed and quality of search results, as for most basic searches it finds sufficiently useful matches.

Always search file names and contents: This option is the most thorough, searching for your entered terms in filenames and in all relevant file contents across the drive, but this can take quite a while, particularly if large portions of your drive contents are not indexed.

Include subfolders in search results when searching in file folders: If ticked, any time you search within a particular folder in Explorer-based interfaces, all subfolders will automatically be included in the search. Untick this box if you only want to search within the currently viewed folder and not go any deeper. This makes searches quicker but less thorough.

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 undesirable results.

Use natural language search: If ticked, allows the use of natural search queries. For example entering *document by brian* will result in a search for any files with document extensions authored by Brian. You can experiment with this feature, however it is more suitable to less advanced users, as it removes much of the precision from searching which is better achieved through custom AQS filters - see further above.

Don't use the index when searching in file folders for system files: If ticked, this option forces Windows to ignore the 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. System directories are protected in Windows and hence normal user files or downloads won't accidentally be saved there for example.

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.

There are additional Start Menu Search Box-related options found under the Start Menu configuration settings. Right-click on the Start button, select Properties, and click the Customize button under the Start Menu tab. See the following options in this section:

Search other files and libraries: This option determines the behavior of the Search Box in the Start Menu. If 'Don't Search' is selected, search results in the Search Box will exclude files and folders, and only include programs and Windows Control Panel items in the results. If 'Search with public folders' is selected, files and Libraries in public folders will be included in the search along with those in your personal folders. If 'Search without public folders' is selected, only files and Libraries in your personal folders will be included in the search.

Search programs and Control Panel: If ticked, this option allows searches initiated in the Start Menu Search Box to also display programs and Windows Control Panel items in the results. If unticked, only Libraries and files will be included in search results.

You can further refine search behavior by editing the 'Add Search Internet Link to Start Menu' policy in Local Group Policy Editor - see the Group Policy chapter for details.

< 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. Then 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.

However 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 search performance. By default the indexer only indexes the following information:

- All folders in your Libraries, including any custom Libraries.
- All email.
- Offline Files.
- All 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.
- If there are multiple User Accounts on the PC, then for privacy reasons only your own files are added to the index you use, so Windows won't show any search results from the data which other users have on the PC.

The actual index file which holds all 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 enabled under your drive properties. That is, go to Windows 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.

Furthermore, 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 - program and system file folders are excluded. For example, go to the *\Users\[username]\AppData* folder, right-click on the folder and select Properties. Under the General tab, click the Advanced button and you can see that the 'Allow files on this drive to have contents indexed in addition to file properties' box is unticked. This is because by default *AppData* stores a great many temporary, configuration and miscellaneous program-related files which most users would not wish to find. 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 7. It provides extremely fast search results, and allows you to access commonly used files and folders much more quickly than having to fill your Desktop or Taskbar with icons for example. Windows 7 has improved the way it indexes content, as well as the types of content it indexes. Search results are also refined to be of greater relevance, and there are many advanced filtering options available to users to help them conduct targeted searches. Furthermore Windows Search works seamlessly with the Libraries feature, meaning you don't have to worry about manually adding or removing any content for the indexer as long as it is stored in a Library; the index is automatically updated as soon as you change Library contents.

However 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 7 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. Furthermore, the indexer does not start functioning immediately after Windows bootup - 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 of what this signifies. If at any time you start using your system even moderately 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, you can 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, and you may see something like 'Indexing speed is reduced due to user activity', which means indexing is 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 features can be, I strongly recommend against disabling Windows Search, even if you have an SSD for example. However if you still wish to disable Search, see the end of this chapter for details on how to do so.

CUSTOMIZING THE INDEX

If you wish 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 folder 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 Libraries to include all your desired folders 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.

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 drive on which the index resides. 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 searching.

Delete and rebuild index: You can delete and rebuild the 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 \ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex on your primary system drive. If you wish to move the index files to another directory and/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.

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 which 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.

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 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 which 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 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 image files, but can also contain content if they are scanned documents - enabling this feature can reduce search speed if you have lots of scanned TIFF documents, so only enable it if you 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 actually wish to initiate a content 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, though note that this may take quite some time to complete. This will ensure that all 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. 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 which 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 Start Menu Search Box, all these songs will be instantly listed for you to choose from.

To edit a file's details, first right-click on it in Windows Explorer and select Properties. Make sure it is not write protected (if it is, untick the 'Read Only' box, click Apply then reopen the file), and it is not currently in use. 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 field(s) 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 particular 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, 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 in 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 much more quickly when needed.

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 at startup. The benefits of Windows Search are numerous, as it is an integral part of the way Windows 7 operates. The index is also useful even if you have a fast SSD, which is why Windows doesn't automatically disable the Indexer on SSDs. However if after reading this chapter you still feel that you want to disable indexing or remove Windows Search altogether, see the information below.

If you simply want 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 Index will be disabled, as witnessed by going to the Windows Control Panel and opening the Indexing Options component.
3. Go to the Folder Options component of the Windows Control Panel and under the Search tab, select the 'Always search file names and contents' option, as well as the 'Don't use the index when searching in file folders for system files' option. This ensures that Windows doesn't attempt to use the index when searching.

These steps will result in often incomplete and very slow searches, but the Search Index and related processes will not run at any time.

If you wish to go further by disabling and effectively removing all Windows Search-related functionality from Windows 7, 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. Go to Windows 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.
3. 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.
4. Untick the 'Windows Search' box and click OK.
5. Restart your PC as required.

This will remove all integrated Search Boxes from Windows, 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 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 has made refinements to improve its functionality and performance. The primary consideration is that Windows Search is not really about searching for lost files, it's about making access to your files, folders, emails and programs much quicker and easier, regardless of where you store them or what you name them. By using a range of metadata, including actual file contents, Windows Search - with the assistance of the Search Index - 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 still the most-used Internet browser in the world, and many Windows users are comfortable and familiar with it. While I recommend that you begin trialing alternatives to Internet Explorer to see if they can provide you with additional functionality you may like, Internet Explorer is a fast, functional browser, and has a range of security benefits in Windows 7. You should not feel you have to use another browser if you are happy with IE. Windows 7 comes with Internet Explorer 8 already built-in and ready to use. However Internet Explorer 9 is the latest version of the browser, and I recommend that you download and install it from the link above, as it contains a range of performance, interface, functionality and security enhancements over IE8.

This chapter covers all the information you need to be able to configure and optimize IE9 to suit your needs.

< BASIC SETTINGS

To configure Internet Explorer, click the Tools button (the cog icon) at the far top right of the browser, then select 'Internet Options'. You can also press the ALT key, 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 don't want any homepage to load when IE is opened, click the 'Use blank' button; 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.

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. Under the 'Check for newer versions of stored pages' 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 images. I recommend selecting 'Automatically' 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 a 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.

If for privacy purposes you wish at any point to delete any components of your browsing history from the cache, see the Delete Browsing History section below. If you just want to browse privately without storing any cached items or history, see the InPrivate Browsing section later in this chapter.

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 files in its cache to find the components of a web page to load, when it may actually be faster just to reload them from the original site. Therefore I recommend 150MB of disk space for the cache as a balance of size and speed. If you have a faster drive and view more complex sites with lots of large images or scripts you may wish to increase this cache to 250MB or even larger if desired. The maximum possible cache size is 1024MB (1GB).

Current Location: Internet Explorer lists the current location of its cache. This is where all of IE's cached 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 the cache - to a faster drive for example - click the 'Move folder' button. To delete cache contents, it is recommended that you follow the instructions further below rather than manually deleting any files found here.

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.

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. If you don't wish to leave any trace of your browsing for a particular session, you can use the InPrivate Browsing feature of IE, which is covered later in this chapter. In general it is completely safe to tick all of these boxes and click the Delete button to remove all traces of browsing, however this can also decrease the efficiency of your browsing, especially since you will also lose any customizations you may have for particular sites, such as saved passwords. 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 clean out any data from all other sites you've visited. However if you still want to remove all stored content then untick this box as well. In any case once you've 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 as well.

Search: Internet Explorer 9 has removed the separate Search Box found in previous versions of IE. The Address Bar is now also a search box, and hence is now 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 under different categories: your browsing history, your favorites, and the default search engine's suggestions. You can select the 'Turn off search suggestions' link at the bottom of the suggested links box to 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 clicking the Settings button under the Search section of the General tab in Internet Options you will be taken to the 'Search Providers' section of the Add-Ons manager, where you can add or remove 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 IE9. 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 your default provider.

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 Settings 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 IE9 (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' does just that - 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/annoyance 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 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; 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 'Search using copied text' if the copied text is not detected as a valid website address.

Importantly, in Internet Explorer 9, 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.

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.

SECURITY

Security level for this zone: There are four zones 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 and entering their address.
- § Restricted Sites - The opposite of Trusted Sites, which again requires that you specify the address of the individual site(s) you specifically do not trust when visiting them.

The aim of these zones is to allow you to have different security levels depending on the level of risk involved. This is because different security levels can impact on the functionality of a site. 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 browser new/unfamiliar 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 address(es) of the site(s) 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 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 - click the Sites button, and 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 you visit sites you know to be risky, you 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, and despite even the most stringent server security. On balance however, the Medium-High security level, when combined with Protected Mode (see below), is sufficient for the general Internet zone and is a good 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 protection and I strongly recommend that it be left enabled. Note that in Internet Explorer 9, unlike IE7 or IE8, there is no visible indicator on the Status Bar (if enabled) at the bottom of the screen that Protected Mode is on. However if Protected Mode is disabled, a prompt will appear at the bottom of the IE window requesting that you re-enable it.

Privacy

Settings: The 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 particular 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 for example, 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. However 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 preferences for particular sites), and blocking them can impair a site's functionality. If you do decide to block all first party cookies, and/or if you select a higher Privacy setting on the slider, click the Sites button and here 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 sites' 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: New to IE9, the 'Never allow websites to request your physical location' option relates to the Location Services 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 the 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 this box, you can prevent any website from successfully requesting and obtaining your physical location via the 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 which opens when you visit particular sites and/or click on particular links or areas of a site. They are most commonly used for advertising, and 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 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. However this means that you will not be aware that a legitimate site is trying 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 illegitimate popups without blocking legitimate ones, however you can choose High to block most popups - in which case I strongly recommend manually adding desirable/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 if you disable 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 desirable/necessary script-based features from working. Enabling the ActiveX Filtering feature, covered later in this chapter, can also help to a certain extent.

InPrivate: InPrivate Browsing is a feature of IE which allows you to surf the web without leaving any trace of your activities on the PC. This 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 such toolbars and extensions in InPrivate Browsing mode to prevent them from saving 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 in the first place. I generally recommend against installing toolbars and extensions wherever possible, for both security, stability and performance reasons, regardless of whether you use InPrivate Browsing or not.

CONTENT

Parental Controls: Clicking the 'Parental Controls' button opens the Parental Controls section of the User Accounts screen, allowing you to set specific parameters for Internet surfing for particular accounts, provided additional software is installed. This is covered in detail under the Parental Controls section of the User Accounts chapter.

Content Advisor: If enabled, the Content Advisor allows you to attempt to filter out and control access to websites that contain offensive or inappropriate material. Go through each category of content and use the slider below the box to set the restrictions on that category. Once done, click OK and you will be prompted to set a Password, as well as a Hint in case you forget that password. IE will now attempt to restrict content based on content advice from ICRA (Internet Content Rating Association), but this is not a fool-proof method.

Certificates: Certificates are a form of electronic authentication method to verify that a particular website or individual is what/who it/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. I don't recommend altering any of the settings in this section unless you are acting under advice from a trusted tech support person. If a particular site displays a certificate error or warning, I recommend pursuing this further with the site owner or researching via Google before conducting any financial transactions or entering personal information on the site, as advised in this Microsoft Article.

AutoComplete: AutoComplete 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/or 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 function for, but for security purposes I don't recommend enabling any of these options unless you have strong password protection on your User Account and/or the PC is physically isolated from anyone else.

Note that ticking the 'Use Windows Search for better results' box will mean that an item called 'Internet Explorer History' will automatically 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 capable websites. If you don't use these features, I recommend unticking all the boxes on this page.

CONNECTIONS

This section is essentially redundant for most users. You should 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

Default web browser: If you have installed any other browsers, you can choose to set IE as your default browser by clicking the 'Make default' button. Unless you are worried about another browser taking over this default association, you needn't tick the 'Tell me if Internet Explorer is not the default web browser' box for optimal IE startup speed. If you wish to make another web browser your default, see the Default Programs section under the Windows Control Panel chapter for details.

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 generally you will be aware that a site wishes to install an add-on through prompts. However 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 both are safe to install. You can also download a range of Other Add-Ons which provide useful additional functionality for Internet Explorer, such as spell checking. 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 already have Flash and Java installed, but are prompted to install another add-on by a website, then I strongly recommend not doing so unless the site is completely trustworthy, such as Microsoft.com.

Furthermore some software will attempt to install third party browser toolbars as part of their installation process, and these take up viewable space, collect data on your browsing behavior, and add to resource usage unnecessarily. Make sure you pay close attention during the installation of 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 launch 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 you don't frequently use; do a Google search if the name does not seem familiar, and most importantly, uninstall any undesirable add-on programs through Programs and Features in the Windows Control Panel.

The Search Providers category in the Manage Add-ons box is covered under the General section further above; 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.

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, however I want to discuss a few important options in more detail before going into the recommended settings:

Accelerated Graphics - Use software rendering instead of GPU rendering: By default Internet Explorer 9 is designed to use your Graphics Processing Unit (GPU) - also known as your graphics card - to accelerate the display of any graphics-related features. 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 greyed out. However in all other cases, you should untick this box, and you should also make sure you have installed the latest graphics drivers as covered under Step 5 in the Windows Drivers chapter, to ensure optimal performance in IE9.

Zoom: 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 mousewheel. 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). Under the Accessibility section of the Advanced options tab 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.

Security - SmartScreen Filter: As covered under the PC Security chapter, Phishing is a form of deception designed to obtain your personal details, such as passwords and credit card numbers. It is usually done for financial gain, and is becoming an increasingly significant threat. Internet Explorer 7 introduced a built-in Phishing Filter which 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 has been changed to the SmartScreen Filter. The filter has features to detect and block potential malware downloads, and in general it is strongly recommended that you leave the 'Enable SmartScreen Filter' box ticked under the Security section of the Advanced tab. 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. There you will see more 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 still visit the site. In both cases 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, 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' - however 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 by selecting the 'Turn Off SmartScreen Filter' option here, but this is not recommended.

Compatibility View: Internet Explorer has a Compatibility View which helps correctly render web pages that 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 essentially changes IE9 into an older version of the browser for the purposes of 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 missing objects/text is visible, and so forth. Most sites will render correctly in IE9, so this is not a common problem. To manually force any page to permanently show itself in Compatibility View, select the 'Compatibility View Settings' option under the Tools menu and add the site to the list. You can also tick the 'Include updated websites lists from Microsoft' to use a pre-compiled list held by Microsoft which determines which sites require Compatibility View to automatically be enabled - more details can be found in this Microsoft Article. Under the Browsing section of the Advanced tab in Internet Options, 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 reloaded and shown in Compatibility View. You can leave this option ticked, however if you notice a site you regularly visit triggering this option, it is better to add it to the list under Compatibility View Settings for faster rendering.

Downloads: By default, when you click on a link to initiate a download from a website, IE will bring up a prompt at the bottom of the screen with more details, allowing you to open the file, or save it to your drive. If you click the Save button, the file will immediately start downloading to your *\Users\[username]\Downloads* directory; you will need to click the small drop-down arrow next to the Save button and select 'Save as' 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.

Security - Enable memory protection to help mitigate online attacks: To be able to change this option you will need to start Internet Explorer by right-clicking on the IE icon and selecting 'Run as Administrator'. If ticked, this option enables Data Execution Prevention (DEP) specifically for IE, which although more secure may cause problems with some older IE plugins and add-ons. I recommend leaving it enabled, however if it causes problems you may wish to either uninstall certain add-ons, or disable DEP for IE, which is not recommended - see the Data Execution Prevention section of the PC Security chapter for more details.

The rest of my recommendations for the more important Advanced settings in IE are provided below. I recommend that the following options be ticked for maximum performance, stability and convenience:

§ Disable script debugging (Internet Explorer)
§ Disable script debugging (Other)
§ Enable automatic crash recovery
§ Enable FTP folder view
§ Enable third-party browser extensions
§ Enable visual styles on buttons and controls in webpages
§ Reuse windows for launching shortcuts
§ Show friendly HTTP error messages
§ Underline links: Always
§ Use Passive FTP
§ Use smooth scrolling
§ Use HTTP 1.1
§ Use HTTP 1.1 through proxy connections
§ Enable alternative codecs in HTML5 media elements
§ Enable automatic image resizing
§ Show pictures
§ Check for publisher's certificate revocation
§ Check for server certificate revocation
§ Check for signatures on downloaded programs
§ Do not save encrypted pages to disk
§ Enable DOM storage
§ Enable Integrated Windows Authentication
§ Enable native XMLHTTP support
§ Enable SmartScreen Filter
§ Use SSL 3.0
§ Use TLS 1.0
§ Warn about certificate address mismatch
§ Warn if POST submittal is redirected to a zone that does not permit posts

I strongly recommend that the following options never be ticked for maximum security and convenience:

§ Display a notification about every script error
§ Allow active content to run in files on My Computer
§ Allow software to run or install even if the signature is invalid

The remaining settings not covered above can be set to suit your taste, or preferably left at their default. If any setting is grayed out then make sure to launch IE with full Administrator privileges; i.e. right-click on the IE launch icon and select 'Run as Administrator'. Furthermore, some settings may only come into effect after closing all instances of Internet Explorer and reopening it again - these are marked with an asterisk.

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 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, mainly to ensure that normal web functionality is maintained. Cookies and other cached internet files will be stored temporarily for example, 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 it.
- 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 stored 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.

Note also that 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 saving and transmitting data about your browsing behavior regardless. For that reason, I recommend ticking this box, but more importantly, resisting the urge to install additional software for IE as much as possible unless it is absolutely necessary and completely trustworthy.

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 or secure browsing 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 in itself is a totally safe add-on, as covered under the Manage Add-Ons section earlier in this chapter. However 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 9 introduces a feature called ActiveX Filtering which allows you to quickly and easily toggle ActiveX controls on or off on a per-site basis without having to alter your main security settings. To enable ActiveX Filtering, click the Tools icon and under the Safety menu select 'ActiveX Filtering' to globally enable or disable this option as desired. 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 on your system.

When enabled, ActiveX Filtering can be easily enabled or disabled on any site 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 grey when filtering is not in effect. Internet 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. This combination will then allow you to run signed ActiveX controls on trusted websites whenever you wish, without allowing them to run at any other time.

TRACKING PROTECTION

Previously called InPrivate Filtering in IE8, Tracking Protection is an improved version of the same feature in IE9 which goes hand-in-hand with InPrivate Browsing. InPrivate Browsing is designed to remove traces of your activity from the PC, but it does not protect your privacy when online. Tracking Protection attempts to do just that, to a reasonable extent, by 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 unnecessary to the functionality of the primary sites. 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. Therefore 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 - though in practice this should be rare. Bear in mind though 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 which provide additional functionality for a site. You can access an Accelerator by highlighting a portion of text on a site for example 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 a range of 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 any).

If you find the Accelerators functionality unnecessary or annoying, then disable all the available Accelerators in the 'Manage Add-Ons' window, and 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.

< ADVANCED SETTINGS

This section contains IE customizations, ranging from the moderately simple to more advanced techniques.

CUSTOMIZE INTERNET EXPLORER'S APPEARANCE

Internet Explorer 9 allows customization of its interface, although in practice there isn't a great deal of scope for changing the way it looks. By default the IE9 interface is already very streamlined, and this is the recommended interface for most users in providing maximum viewable space for web browsing.

However you can customize the IE9 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 the Menu Bar, Favorites Bar, Command Bar, and Status Bar - all of which will take up additional vertical web viewing space in return for more familiar access to IE's primary functions. 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. Note that if you don't want to have the Menu Bar permanently showing, you can open it temporarily at any time by pressing the ALT key.

Favorites, History, Feeds Sidebar: Under the View menu, 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 Stop (x icon) and Refresh (circular arrow icon) buttons from the right side of the Address Bar to the left, right-click on either of these icons 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 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 IE9 interface will temporarily reappear. Even without the interface, you can easily 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 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 it will automatically open in Full Screen mode. You can still toggle it back to normal mode 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.

WINDOWS 7-SPECIFIC FEATURES

Internet Explorer 9 is a native Windows 7 application, and as such provides some additional features not fully supported by other browsers. In particular, Internet Explorer's Jump List contains specific items which can be useful, such as 'Start InPrivate Browsing' and 'Open new tab'. See the Taskbar section of the Graphics & Sound chapter for more details on Jump Lists.

IE9 also introduces the ability to pin individual websites as separate icons to the Windows Taskbar. To do this, open the particular website you want to pin in Internet Explorer as usual, then drag the website's Favicon - the small icon to the left of the site's address in the Address Bar - to the Windows Taskbar, or drag the tab in which the site is open to the Windows Taskbar. This will create a pinned Taskbar item with the website's icon displayed, and when clicked, opens a new IE window at that particular site. IE's interface will also be subtly changed when using this pinned item: the website's icon will be displayed at the top left, and the Back and Forward buttons will also take on the primary color of the website's icon. Furthermore, some sites will have unique tasks appear in the Jump List for their Taskbar item; e.g. if Facebook is pinned, it will add new items to the Jump List, the same as Amazon.com if you are logged into your account. To remove any website from the Taskbar, right-click on it and select 'Unpin this program from taskbar'.

You can also add websites to your Start Menu. Drag the site's Favicon or tab to your Start button and you should see the option to 'Pin to Start Menu' appear. Doing so will add the site's icon to your Start Menu, and when clicked, opens up IE with that site, again the site's icon will be displayed at the far left and the Back and Forward buttons will have changed color appropriately. Any Jump List items will also appear as options in the Start Menu icon's Jump List.

YOUR MOST POPULAR SITES

Another new feature in Internet Explorer 9 is the ability to open up a tab which contains a list of your most popular sites, based on your browsing behavior - as long as you haven't disabled/cleared your History. The Your Most Popular Sites tab lists thumbnails of your ten most popular pages/sites, ranked by how much you frequent said sites. You can access this page at any time in several ways:

§ By going to Internet Options>General>Tabs>Settings and setting the 'When a new tab is opened' option to 'The new tab page'. Now click the New Tab button at the far right of your tab bar to open the Your Most Popular Sites page.
§ By typing *about:tabs* in the Address Bar and pressing Enter.
§ By entering *about:tabs* as your home page address in the Internet Options>Home Page box, then clicking the Home Page button to open the Your Most Popular Sites 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 Advanced tab of Internet Options.

By default, this display of popular sites is 2 rows of 5 thumbnails each, totaling 10 favorite sites/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 Your Most Popular Sites 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 site/page from the Your Most Popular Sites shown by right-clicking on it and selecting 'Remove this page'. If you simply don't like the Your Most Popular Sites feature, you can click the 'Hide Sites' link at the bottom right of the page to remove all site thumbnails from the page, or you can disable your History to prevent IE compiling this list.

INTERNET EXPLORER 64-BIT

If you are running Windows 7 64-bit, by default whenever you launch Internet Explorer from the Taskbar icon or the normal Internet Explorer item in the Start Menu, the 32-bit version of Internet Explorer will open. This is perfectly fine and recommended for most users. However you can launch the 64-bit version of Internet Explorer instead by going to Start>Search Box, typing *Internet Explorer*, then selecting the 'Internet Explorer (64-bit)' item. You can also right-click on this item and select Send to>Desktop to create a permanent icon to use for launching IE 64-bit.

As this Microsoft Article explains, while Internet Explorer 64-bit can be more stable and may be faster, it also has some issues, which is why it is not the default browser version in Windows 7 64-bit. The biggest issue stems from the fact that all add-ons for IE need to match the bit version of IE being used, so 32-bit add-ons will not function correctly on IE 64-bit. Since most of the useful add-ons, such as Flash player, are currently only available in 32-bit form, this makes IE 64-bit less functional than its regular 32-bit version. If you don't use any add-ons at all in IE on the other hand, or have 64-bit add-ons, then you can make IE 64-bit your default version due to its potential benefits.

START WITH INPRIVATE BROWSING MODE ENABLED

By default the InPrivate Browsing mode in Internet Explorer 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 this, you can create a shortcut which opens IE already in InPrivate Browsing mode, ready to go at the start of every session. To do so, follow these instructions:

1. Go to Start>Search Box and type *Internet Explorer*.
2. Right-click on the Internet Explorer item which appears and select Send to>Desktop.
3. Right-click on this new icon and select Properties.
4. In the Target box, go to the very end of the existing text, insert one blank space and then add the *-private* switch. It should look similar to this:

   ```
   "C:\Program Files (x86)\Internet Explorer\iexplore.exe" -private
   ```

5. Click Apply then OK to close the box.

Now whenever IE is launched from this modified 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.

However an interesting added feature of Internet Explorer is the ability to subsequently open the FTP server in Windows Explorer, allowing you to manage file transfer to and from the FTP server easily. To do this, while at an FTP address in IE, open the View menu and select 'Open FTP Site in Windows Explorer'. A Windows 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 Windows Explorer. You can also use the Dual Window Explorer View tip under the Advanced Features section of the Windows Explorer chapter to open two Windows Explorer windows and position them side by side for easier file transfer operations.

If you want a more advanced FTP manager, I recommend the free Filezilla FTP utility which provides a range of features in 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 still be slow for sites which have multiple items that need to be downloaded before the page can be displayed, or for large multiple file transfer, especially if you are on a fast connection. 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
```

Again, 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 (e.g. 10 as shown above).

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.

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 - i.e. 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.

ADVANCED CUSTOMIZATION

While Internet Explorer 9 is an excellent browser in many respects, it is limited in the extent to which it can be customized. This is one of the reasons why, if you are interested in undertaking more advanced customization of browser functionality and appearance, you may wish to explore the option of using one of the other free web browsers covered at the end of this chapter.

If you still wish to try advanced customization of IE, you can use the free IE7Pro add-on which despite its name also works with IE8 and IE9. However keep in mind that development for IE7Pro ceased in mid-2010, and it is neither designed for nor thoroughly tested on IE9. It appears to work to a certain extent, but there is no guarantee that all desired functionality in IE7Pro will be available or stable under IE9.

Download and install IE7Pro, but during installation make sure the 'Enable Userscripts Plugin' option is ticked, and then select the 'Do not install ProgSense' option. Once installed, to access the new features which IE7Pro enables, go to the Tools menu in IE and select 'IE7Pro Preferences'. In the window which opens you will see a range of options which you can use to alter the appearance and behavior of Internet Explorer.

For example, using the 'User Scripts' component in the IE7Pro preferences box, you can load up a range of user-made scripts, such as those freely available at UserScripts.org, to achieve a range of customizations - though be aware that some user scripts can be deliberately malicious or annoying, so research a script carefully before enabling it.

The various other functionality of IE7Pro won't be covered here, but clearly this add-on provides users with a great many options for further customization of Internet Explorer if used wisely. Note that if at any time you wish to disable the additional toolbar IE7Pro installs, right-click on the toolbar area and untick the new 'Grab Pro' item. This will also remove the 'IE7Pro Preferences' item in the Tools menu. You can re-enable these again by right-clicking on the toolbar area and reticking the 'Grab Pro' item.

FIX INTERNET EXPLORER

If you are having problems with Internet Explorer, you can browse through this Microsoft Fixit Site. To attempt to automatically diagnose and repair an Internet Explorer issue, you can run through this Microsoft Interactive Support Wizard. Furthermore, you can attempt to reset all of Internet Explorer 9'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 destabilize IE, increase its resource usage, and cause other problems depending on the type and number of add-ons installed. Internet Explorer 9 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 remove unnecessary add-ons in IE. This is important not only for stability and performance, but also for privacy and security purposes.

If all else fails, try uninstalling Internet Explorer 9 by going to the Program and Features component of the Windows Control Panel, clicking the 'View installed updates' link in the left pane, and finding 'Windows

Internet Explorer 9' in the list shown - right click on this item and select Uninstall. Reboot your system and then download and reinstall the latest version of IE9 from the link at the start of this chapter, and of course make absolutely sure you run Windows Update immediately afterwards to install any updates for IE.

< OTHER INTERNET BROWSERS

You may be wondering if there are other reputable browsers you can try if you are not completely happy with Internet Explorer. Fortunately 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 much more customizable, both in terms of interface and functionality, through a truly massive range of free Extensions and Themes. If you want to find out more about Firefox I recommend you read my Firefox Tweak Guide which covers all aspects of Firefox from the basic to the advanced.

You have nothing to lose by trying other browsers out. All of the major browsers, including Internet Explorer, have the essential features required for fast, secure browsing. It all depends on which browser best meets your needs, as there is no outright 'best' browser.

WINDOWS LIVE MAIL

Windows XP had Outlook Express, and Windows Vista had Windows Mail, but Windows 7 does not come with any mail client. Instead if you search for *mail* in the Start>Search Box, you will see a link referring you to 'Go online to get Windows Live Essentials'. Microsoft clearly wants to decouple a range of key features from being included in Windows; not only Windows Mail, but also Windows Photo Gallery and Windows Movie Maker are absent in Windows 7, as are certain features, such as the web filtering portion of Parental Controls. Instead you must install Microsoft's free Windows Live equivalents of this software, or a third party alternative.

Fortunately Windows Live Mail is a reasonable replacement for Windows Mail and Outlook Express, and unless you are already using Office Outlook, or another specific third party mail client, I recommend that you download and install Windows Live Mail. For the most part, Windows Live Mail functions much the same as Vista's Windows Mail. Even though it is part of the Windows Live Essentials suite, this does not mean that your emails are stored online or that you must login using a Windows Live ID. However it does require a bit of customization to get it to look and function like previous Windows mail clients, which is precisely what we cover in this chapter.

< CUSTOMIZING THE INTERFACE

Download the Windows Live Essentials Installer, launch it and during the installation process make sure only the Mail component is ticked for now. You can rerun the installer and select other Windows Live Essential components after reading the other chapters in this guide as required. Once installed, the default appearance and functionality of Windows Live Mail may be confusing and undesirable to users of previous versions of Windows Mail. In this section we cover the initial customization of Windows Live Mail.

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. This may indicate that Windows Live Mail needs to synchronize with some special online account for full functionality, or store your emails online, but this is not the case - you do not need to sign in or synchronize with anything. Signing in 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. As such, most people can simply ignore the 'Sign In' prompts. If you're not signed in, the Sync button becomes a 'Send/Receive' button and simply checks for any new mail and sends any outstanding mail when clicked. Windows Live Mail will behave just like previous Windows mail clients.

The instructions that follow are primarily aimed at bringing Windows Live Mail's look and functionality as close as possible to that under previous mail clients such as Windows Mail and Outlook Express. You may wish to adjust the way Windows Live Mail looks and operates differently, or not at all, so this is only a suggested approach to customization. Note that on a system with multiple 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, which is generally desirable.

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 main Windows Live Mail button at the top left of the window, select Options and 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 main Windows Live Mail button at the top left, select Options, then select 'Email accounts'. Now for every email account, 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, so there is no need for a copy of it to also be stored on your mail server.

STEP 2 - IMPORT SAVED MAIL

The next step is to restore any saved emails you may have exported from Windows Mail or Outlook Express, or from Windows Live Mail itself.

Importing Saved Emails

1. Click the main Windows Live Mail 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.
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 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.

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 add the 'All e-mail' category to Quick Views, which displays all your existing emails, both read and unread, across all your accounts, 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 so that it is not highlighted. 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.

However some users may prefer a unified Inbox and a folder structure in the Folder Pane similar to previous versions of Windows Mail/Outlook Express, rather than the new Quick Views category, especially as Quick Views and its subfolders can't be renamed. The first step towards a more traditional appearance is to 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. You should 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 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 select 'Message Rules'.
6. Click the New button, and in the window which appears, scroll down and tick the 'For all messages' option in the first field, and tick 'Move it to the specified folder' in the second field.
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 at the top of the rules list.

The steps above effectively takes every new email which arrives in the inboxes for your various email accounts, and automatically moves them to the single Inbox folder under 'Storage Folders'. This means you can leave all your email account categories collapsed and taking up minimal space, while the 'Storage Folders' category can be left expanded to show your new emails arriving in the Inbox. The key benefit of this method versus the existing Quick Views is that this Inbox folder will only show new emails, not all unread emails across your accounts - in other words you can still move unread emails to any other subfolder without them appearing in the Inbox as well.

STEP 4 - CUSTOMIZE MENUS AND TOOLBARS

Windows Live Mail now 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. This will collapse the entire ribbon to only show the menu headings. You can then access each of the menu sub-options by clicking 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 shown in Windows Live Mail, including the ones shown at the top of individual emails.

There is a smaller Quick Access toolbar which is also available, and which can be displayed just above or just below the ribbon. Click the small black down arrow to see a range of commands which you can enable/disable on the quick access toolbar. Alternatively, you can right-click on any option in the ribbon and select 'Add to Quick Access toolbar' to add it. 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 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, click the View button and choose 'Select columns'. Here you can select or unselect the columns which are displayed, and also set their order and width.

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.

The steps above should make Windows Live Mail more like previous Windows mail clients, especially with the addition of a unified Inbox.

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. So 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 is the notifications given in the status bar, if the status bar is visible. To see a detailed progress indicator you need to 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 features 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 you don't want; finally, click the main Windows Live Mail button at the top left of the Mail window, and 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 receives feedback and the Live suite evolves. Microsoft periodically releases new versions of Windows Live products, and 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 Vista, because Windows Mail and Windows Live Mail share similar underpinnings. To configure Windows Live Mail, click the main Windows Live Mail button at the top left 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 Live Messenger to automatically open when Windows Live Mail is started. If you don't wish this to occur, or don't use Windows Live 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 back 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. 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 ticked, whenever it is open, Windows Live Mail will automatically check all your email accounts for new messages at the set interval which you specify in minutes.

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. If you want to use another application to handle your mail and/or newsgroups, 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 with the Reading Pane open, 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 'View by conversation' option ticked 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 threads will 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 images appear in HTML formatted emails 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 whether a 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 you send 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 recipient has opened the message and/or 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 also 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.

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 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 covered under the Important Security Tips section of the PC Security chapter. Instead I recommend saving at least the last email from particular individuals whose addresses you wish to keep. See the Contacts section further below for more details.

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 instantly recall 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, then your reply will automatically be in plain text as well. Similarly, HTML formatted email will initiate an HTML formatted reply from you. If you wish to maintain the formatting, tick this box, otherwise untick it. 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 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 when 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.

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 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 the list of words to correct the word if you wish.

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 which contains numbers in them, and/or the original text to which you are replying or forwarding. All three are generally best left 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

The first set of options here apply to dialup users only. When you click the Change button it will open the Internet Explorer Connections tab - see the Internet Explorer chapter for details. 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 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 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 actually stored. 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. 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 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.

< 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 main Windows Live Mail 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 which is usually annoying and/or malicious. The Low option provides basic protection against the most obvious junk email, but can let others through. The High provides more aggressive protection against junk email, but legitimate emails may also get caught up in the filtering. 'Safe List Only' only allows emails 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 will not receive emails from anyone other than people you know, then select the Safe Senders list option and add all 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.

You can also flag individual emails as junk email or unblock/unmark legitimate mail by right-clicking on the 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 other 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 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 option 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 legitimate emails sent to you may 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 valuable 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 hence 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 emails from people you know 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 discernable 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 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, and hence worth more money to them as part of the email lists they sell to other spammers. I strongly recommend unticking this option.

INTERNATIONAL

One of the ways in which you can successfully 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 a known source 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 the country extensions which you wish to have blocked. See this list of TLDs to help you input the right ones. Bear in mind that as noted earlier, many spammers do not use legitimate email accounts, or can use accounts which are from a range of countries, so this method may not necessarily be completely effective. The method below has a 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 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 and highlight particular emails which it considers to have phishing links and content. You should enable setting, particularly if you are less familiar with the appearance of phishing emails, as an added layer of protection. Bear in mind that just because an email gets through this filter, doesn't mean it's safe to click the links in it; conversely just because an email is flagged as suspicious doesn't necessarily mean it's a phishing email. See the Important Security Tips section of the PC Security chapter for various methods of detecting phishing and malware in emails.

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, however 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 as well.

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 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 strongly recommend running in 'Restricted sites zone' mode, as many HTML-based emails are spam or malicious, and most active content is either annoying and/or malicious. For the most part legitimate emails 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: I recommend ticking this option as it 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 which 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 attachments which are flagged as malware. However just because an attachment is not blocked, doesn't mean that it is safe to open - you should still consider the source of the email as to whether it is trustworthy, and then save it to an empty folder and scan it for malware. 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 PC Security chapter for details. For details on how to adjust the Attachment Manager's behavior, see the Handling of Windows Live Mail 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 critical 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. However 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 Start>Search Box, 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 which 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 Windows Live Contacts to create a new contact.

§ You can click the Import button in Windows Live Contacts to import an existing file with contact details, such as your Windows Address Book from Outlook Express.

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 and/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 send itself out to all the people you know, proliferating the malware and causing you some embarrassment. Worse, if someone compromises your User Account then they can see the personal details of not only you, but all your friends and acquaintances as well, and this can be very useful in successfully undertaking identity theft. Instead I recommend keeping emails 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 do a reply to their last email. 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 from stored emails, and the relationship between you and the senders of all these 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 select 'Message rules'. In the window which opens, do the following:

1. Click the New button.
2. Select a condition in the first box (e.g. 'Where the message has an attachment').
3. Select an action to apply to this type of message (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 cater to a range of situations. 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 rule(s) 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, click the box next to it to remove the tick mark 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 above - 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 main Windows Live Mail 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 Windows 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 which contain all the individual messages as .EML files.
6. I recommend using an archival utility such as WinZip, WinRAR or 7-Zip to back these folders up into a single archived file for easier storage.

To restore these emails in Windows Live Mail at any point, simply click the main Windows Live Mail button at the top left and select 'Import messages', select 'Windows Live Mail' and follow the prompts.

BACKING UP ACCOUNTS

To back up your individual email accounts, follow these steps:

1. Click the main Windows Live Mail 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 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 your email accounts, click the main Windows Live Mail 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, particularly 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 Live Mail Solution Center.

However 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. 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 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. However obviously they cannot be accessed in offline mode, and I don't recommend relying solely on an online provider, because if your email account is hijacked for example, you lose access to both your account and any stored emails.

WINDOWS MEDIA PLAYER

Windows Media Player (WMP) is the built-in Windows utility for playing multimedia files. It has many useful features and is actually a very efficient, feature-packed media player, but is often mistakenly dismissed as being bloated. If configured correctly, WMP provides excellent audio quality and all the functionality that most users require for playing movies and music.

Windows 7 introduces Windows Media Player 12 which has been slightly redesigned over previous versions. As part of the integration of Libraries into Windows 7, WMP 12 has the Library view as its primary media management area. The alternate view is the Now Playing view, which has taken on 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, including Codecs and DRM.

I do not cover Windows Media Center configuration as it is too specialized and too varied based on different home theatre setups to be explained adequately in this book. However some of the information in this chapter also applies to Windows Media Center.

< INITIAL SETTINGS

To access Windows Media Player, go to Start>Search Box, type *windows media player* and press Enter, or simply click the Windows Media Player icon in your Taskbar. You can also launch Windows Media Player by going to Start>Search Box and typing the name of a song or movie stored in one of your Libraries, then selecting it.

The first time you launch Windows Media Player, you will be prompted to configure a range of initial 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:

Select Privacy Options: These settings are covered in detail under the Privacy section below. If you are concerned about privacy you can untick them now, and consider whether to re-enable 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 always change whether WMP is your default player, and its file associations, at any time - see the Default Programs section of the Windows Control Panel chapter.

Choose an Online Store: The available options here will vary depending on your region, however if you wish you can set up access to an online media store from within Windows Media Player here. I recommend selecting the 'Don't set up store now' option, and once you've read the information in this chapter, you can browse and select a store by going to the View menu and selecting 'Online Stores'.

Making the correct choices regarding these options requires further information as covered throughout this chapter, and all of the above settings can be configured properly within Windows Media Player at any point, so don't be overly concerned about 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 Windows 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 7; 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. Furthermore, depending on the category chosen, the media files will 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 the Details Pane 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 your media-related Libraries in the Navigation Pane. These include your user-specific Music, Pictures and Videos Libraries. It also includes the Recorded TV Library which is actually not user-dependent, and is stored in *\Users\Public\Recorded TV* by default. 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 into Windows 7 - see the Libraries section of the Windows Explorer chapter for more details.

While you can manage a Library within Windows 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 WMP usage.

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 7. 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 which exist in your Windows 7 media-related Libraries but which are not present in the WMP-specific listing of these Libraries.

More importantly, if you wish to control whether 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 Playlist 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 Playlists created are saved as .WPL files under the *\Users\[username]\Music* folder, and also added to your Windows 7 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 in the playback controls.

Visualizations: This menu allows you to determine the graphics displayed during the playback of audio files. By default, no graphics are shown, which corresponds to the 'No Visualizations' option. 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 computers. 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 which 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.

Shop for more music: This option is the same as the 'Online Stores' option covered in the next section.

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 access the full set of menus in WMP, in Library mode click the Organize button, select Layout and then select 'Show menu bar'. To configure Windows Media Player as covered below, either click the Organize button and select Options, or go to the Tools menu and select Options. Each tab of the Options is covered 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 all that often, the 'Once a month' or 'Once a week' options should be fine; 'Once a day' 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 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.

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 covered further below. Check the preview at the bottom of the box to see an example of how this 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 large file. If you select one of the Windows Media Audio (.WMA) formats, then I strongly recommend 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 desired.

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, however the lossless formats such as .WAV and .WMA lossless don't allow quality change, because they record at 100% of the quality available. The higher the quality, the larger 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.
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 point 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 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 section 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 part of 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/DVD 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 as necessary.

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 burnt as an audio CD, but other media can only be burnt to CD or DVD as data files. If you want to burn pictures or movies to DVD for playback as a proper DVD video disc, you need to use the Windows DVD Maker 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 others.

Burn CD without gaps: 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; you may have to upgrade its firmware - see the BIOS & Hardware Management section.

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 insert this disc into a device which supports .WPL or .M3U Playlists, the device will then 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 sorting.

Windows DVD Maker: If you want to create a DVD Video disc that can be used in a standalone DVD or Blu-Ray player for example, then you need to use Windows DVD Maker for that purpose. Windows DVD Maker can be opened by going to Start>Search Box, typing *dvd maker* and pressing Enter. Usage of Windows DVD Maker is relatively straightforward - the main window provides a file list to which you can add video and image files by clicking the 'Add items' button. Once added, you can rearrange the order in which the items will be played back using the up and down arrows. Click the Options link at the bottom right corner to configure the DVD root menu, aspect ratio, output video format and burning speed, then click OK. If you selected to display a menu, Windows DVD Maker will prompt you to customize the DVD menus, and then to finally click the Burn button to burn to a DVD disc.

Remember that you can also burn any disc using the built-in Burn features of Windows Explorer. Insert a blank or rewritable DVD or CD into your drive, then drag any file or folder to your optical drive in Windows Explorer, and it will be added to a list of files to burn to disc. When ready, click the 'Burn to disc' button in the Command Bar of Explorer and the files will be burned. However this only creates data discs.

To create proper audio or video discs, you must first have prepared the data in the appropriate format before burning to disc. For example, to create a DVD video 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 Windows Explorer it can be played back as a DVD video disc. Various conversion utilities exist to allow you to convert .AVI, .MPG and other video files into the appropriate files and structures for standalone DVD or Blu-Ray playback. The free Avidemux, VirtualDub, tsMuxer and Avi2DVD utilities allow you to edit and convert a range of video files into the appropriate format for burning onto disc and result in proper playback on a standalone DVD or Blu-Ray player.

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, of which there is also a free basic version available. For most purposes, the built-in burning functionality of Windows 7 should be sufficient for most users, as it covers the full spectrum of audio, video and data disc burning requirements.

Windows Movie Maker: On a related note, if you wish to make your own movies, be aware that Windows Movie Maker has been removed from Windows 7. However if you require this functionality, you can install the older standalone Windows Movie Maker 2.6 or the more recent Windows Live Movie Maker - I recommend the older standalone version.

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 stutters and skipping in streaming media playback. The 'Use default buffering' option is usually fine to use, but if you find streaming videos are constantly disjointed, then experiment with increasing the buffer size.

DVD and video playback: These options affect all DVD and video playback, and can be used to help resolve issues with particular videos or DVDs. If your video goes out of sync - sometimes due to lack of sufficient bandwidth - tick the 'Drop frames to keep audio and video synchronized' option. Tick the 'Use video smoothing' option if playing back video with low framerate, as WMP will try to interpolate frames (fill in the blanks) to provide the appearance of smoother video playback.

When playing fullscreen video, if the 'Display full-screen controls' option is ticked, the playback controls will be 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 7 has added 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 Standard TV format displayed on a widescreen monitor - 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 further below 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, 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 here 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 - see further below for details.

If you have privacy concerns, see the Privacy section below for more information. By adding album information, you can make the Windows Search functionality much more useful, since the more details there are about 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

Windows 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 User Account.

PLUG-INS

Plug-ins are various modules which 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 from Microsoft 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 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 common 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 refer to this Windows Media Player 12 Privacy Statement. Essentially, the following basic computer information will typically be sent by WMP to Microsoft along with various 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 the 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 the 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 further above. 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) protection 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 and 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 redownload 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. Microsoft may use the data to determine the rate and type of music piracy around the world for example, however 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 a high a setting, it may prevent you from downloading additional media information or codecs under certain circumstances.

DVD

If you use Windows Media Player to play DVD movies, you can adjust the settings in this section to suit your particular tastes and needs. Click the Change button to implement any content restrictions you want based on movie ratings, and click the Defaults button to set the default languages used for audio, captions and menus in DVDs.

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 which 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 found 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. You can 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 progressively 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 the 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 which effectively increase the perceived size (not volume) 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 SRS WOW 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. SRS WOW effects do not apply when playing back a DVD.

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 can 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.

Dolby Digital Settings: Windows 7 introduces Dolby Digital Plus support in Windows Media Player. The settings here affect all media encoded with Dolby Digital surround sound, and affect the dynamic range of audio playback. You can choose from three presets: Normal is best suited to quality desktop speakers; Night is better suited to laptop or low-end speakers; and Theater is suitable for home theater setups.

Note that you can adjust any slider in these Enhancement features with greater precision by clicking once on the slider and then using your arrow keys for finer control. 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 and acts. To truly customize Windows Media Player, you can use Skins, which alter both the appearance and visible functionality of WMP. 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'. 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 (Program Files (x86) in 64-bit Windows)\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.

There are two options to attain something similar to the Mini Player mode:

- 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 WMP window.
- You can attempt to downgrade Windows Media Player 12 to the previous Version 11, which will then let you use Mini Player mode. The appropriate download is available here and contains instructions within the downloaded archive. However I have not tested this method, nor do I recommend it. There is a very real risk of damaging your Windows 7 installation to the point where neither version of WMP will function correctly, so at the very least create a full backup prior to implementing this, preferably a system image as covered under the Backup & Recovery chapter.

For the most part the various improvements and features in Windows Media Player 12 outweigh the potential loss of amenities in terms of the Mini Player and Advanced Tag Editor.

Finally, if you are having problems running Windows Media Player, or any other media-related features in Windows 7, check the Windows Media Player Solution Center for help in resolving it.

< AUDIO & VIDEO CODECS

A Codec (Compressor Decompressor) is a program which allows audio or video to be compressed and decompressed to or from its original format. Compressed files use special algorithms to achieve their size reductions, and it is the codec which 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 and select 'About Windows Media Player'.
3. Click the 'Technical Support Information' link at the bottom of the box.
4. A new browser window will open and towards the bottom is a list of all the audio and video Codecs installed on your system, the files which 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.

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 one and select 'Un-Register Filter', then you can try to manually delete the relevant file(s), usually found under your *\Windows\System32* directory.

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 Google 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 remember that WMP 12 already has 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 simply 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. The most prominent example is Blu-Ray movie discs, which will not play back on Windows Media Player or any other free media player due to the requirement for proprietary codecs. You will need to purchase a third party media player which can play Blu-Ray movies, such as the latest versions of PowerDVD or WinDVD. Obviously, you must also have a Blu-Ray drive for your PC, and your hardware will also need to meet the Windows DRM requirements to play back HD movies properly, as covered further below.

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 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, especially as the thorough removal of Codecs can be extremely difficult, and in some cases, a full reinstall of Windows 7 may be required to undo the damage caused by a Codec Pack.

64-bit Codecs: Under Windows 7 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 Windows 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 now supports a wider 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 7 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 most compatible with Windows 7, 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, and the quickest route may just be a full reinstall using the latest system image - see the Backup & Recovery chapter. Codecs are one of the biggest culprits in problematic behavior for gamers in particular, so don't install more Codecs than absolutely required, and do not install any Codec Packs no matter how tempting they seem.

< 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, similar to the way Activation is used in Windows 7 - see the Activation chapter for details.

To see if a media file is protected by DRM, 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. Also see further below if you wish to legally avoid DRM protected music.

An additional form of DRM was integrated into Windows Vista, and carries over to Windows 7. It is designed to provide protection for High Definition (HD) video content, such as that provided on the Blu-Ray disc format. This format allow resolutions of 720p and 1080p (i.e. 720 or 1080 vertical lines in Progressive format), whereas standard DVD for example is 480p (NTSC) or 576p (PAL). To ensure that content from an HD format is not being copied, altered, or coming from an unauthorized copy, Windows 7 requires that all of the following conditions be satisfied for protected HD content:

§ 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 HD-DVD or Blu-Ray disc is being used.
§ An activated and valid copy of Windows 7 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 HD-DVD or Blu-Ray content without any problems. Note that any standalone HD-DVD/Blu-Ray playback device 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 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 that it is not running on a Protected Media Path.

There is also the Protected User Mode Audio function, which was introduced in Vista and has been improved in Windows 7. It provides the ability to protect audio content from being unlawfully copied, similar to the protection provided to HD video content.

A key point to note is that none of the above information applies to HD content or audio which 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 7 and Windows Media Player has no noticeable impact since it is all being handled behind the scenes by Windows without any need for user input, similar to a standalone player.

However 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. 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 have transfer restrictions.

§ 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 hence 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 media copies provide a reasonable balance of cost, convenience, protection, the ability to transfer the media between machines, as well as rewarding the creators of the content. Digital downloads may be cheaper and more convenient, but they carry more restrictions and risks.

< OTHER MEDIA PLAYERS

If you don't wish to use Windows Media Player to view multimedia content, there are a range of alternatives including the following popular free players:

VLC
WinAmp
QuickTime Player
iTunes
DivX Player

I can't go into detail about each of these players in this chapter, however they are each good players, depending on your personal preference and specific needs. One particular media player worth noting further however is Media Player Classic. This is a free generic media player which can play back most formats, including some proprietary formats, and is also both easy to use and utilizes very little system resources. Download and launch the *mplayerc.exe* file to start the player - it requires no installation. It also requires no reconfiguration as such, it is ready to be used immediately without any issues.

GRAPHICS & SOUND

Some of the most obvious enhancements to Windows 7 come in the form of graphics-related changes, particularly to the Windows interface. For Windows Vista users, the most prominent graphical change in Windows 7 is the new Taskbar; for Windows XP users, the entire glass-like 2D/3D Aero interface is completely new. Similarly, Windows 7 introduces minor enhancements to audio compared with Windows Vista, but the audio changes between Windows 7 and Windows XP are much more dramatic.

Aside from the more obvious differences, there are a range of changes beneath the hood which make Windows 7 much more efficient in its handling of resources when providing graphics and audio functionality compared to any previous versions of Windows. A basic understanding of the technical changes in Windows 7 is required, and is covered in this introduction before we go any further in this chapter.

Windows 7's graphics capabilities are powered by the Windows Display Driver Model (WDDM) which has been upgraded from the initial Version 1.0 in Vista to Version 1.1 in Windows 7. Under WDDM 1.0, the Desktop Windows Manager (DWM) was introduced, and allowed the combination of 2D and 3D effects which form the transparent Aero interface. In Windows 7, the new WDDM 1.1 adds Graphics Device Interface (GDI) hardware acceleration for 2D graphics, which in turn allows 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.

DirectX is the Application Programming Interface (API) for handling multimedia in Windows. It has various components, including Direct3D for 3D graphics, DirectSound3D for 3D audio, and DirectDraw (now Direct2D) for 2D graphics. 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. DirectX 10 actually contained three versions of Direct3D for 3D graphics (primarily gaming) compatibility purposes: Direct3D 9, which is similar to the DirectX version used in Windows XP; Direct3D 9Ex which was a hybrid of Direct3D 9 for use with Vista's new WDDM 1.0; and Direct3D 10, later 10.1. Windows 7 builds upon DirectX 10.1 by introducing DirectX 11, which adds a range of new features to DirectX 10.1.

The key changes resulting from the implementation of DirectX 11 in Windows 7 is that Direct3D 11 provides new graphics capabilities such as Tessellation to increase object complexity, Multithreaded rendering to improve graphics card utilization, and Compute shader support for processing general data on graphics cards. Direct2D is also introduced to eventually replace DirectDraw for rendering 2D graphics. Direct2D provides hardware accelerated 2D graphics, though note that both the GDI method mentioned earlier and Direct2D are involved in hardware-accelerated 2D graphics rendering in Windows 7, as covered in this Microsoft Article. When rendering the Windows Desktop for example, GDI draws any solid objects and straight lines, including text, while Direct2D is used for the transparency effects and anti-aliasing for example.

As touched upon in the Windows Drivers chapter, WDDM 1.0 graphics drivers - essentially Vista-compatible drivers - still work under Windows 7, however to enable all the benefits described above, you need to use Windows 7-specific WDDM 1.1 graphics drivers.

More details of the graphics and audio changes are provided throughout this chapter, as we examine the entire range of graphics and audio-related functionality in Windows 7.

< WINDOWS AERO

Windows Aero is the Graphical User Interface (GUI) introduced in Windows Vista and implemented with refinements in Windows 7. It is a departure from previous Windows interfaces, because it provides a mix of two dimensional (2D) and three dimensional (3D) components. Some of the prominent features of Aero include:

- Glass-like transparencies on window borders, buttons and desktop elements like Gadgets.
- Thumbnail previews of the contents of currently running applications by hovering your mouse over their Taskbar button or when accessing Task Switcher by pressing ALT+TAB.
- Animated 3D previews of running applications while using the Windows 3D Flip task switcher, accessed by pressing WINDOWS+TAB.
- Animated 3D transition and animation effects, such as when minimizing or maximizing open windows.

Windows 7 adds the following refinements to Aero:

- A redesigned and more functional Taskbar, which is slightly thicker and fully transparent, and allows a range of useful new features as covered under the Taskbar section later in this chapter.
- Transparency effects remain visible even when a window is maximized.
- Aero Peek, Aero Shake, and Aero Snap features for instantly changing the display of windows with various mouse gestures - each covered separately in this section below.
- A touch-capable interface, which when combined with a touch-sensitive screen, allows you to select and manipulate objects by pressing your fingers against the screen. This is part of the reason why the Taskbar has been slightly increased in thickness.
- A range of improved animation and lighting effects which are quite subtle but are often useful.

REQUIREMENTS

To enable Aero on your system, you must meet all of the following requirements:

- You must have Windows 7 Home Premium, Professional, Ultimate or Enterprise editions. You cannot access Windows Aero mode in the Home Basic or Starter editions of Windows 7.
- You must have a supported DX9-capable graphics card with 128MB of Video RAM or higher, and the card must have hardware support for Pixel Shader 2.0 or above. Some integrated/onboard graphics solutions will not meet these requirements even if they have access to 128MB of memory.
- You must be using a proper WDDM 1.0 or 1.1 graphics driver.
- You must have a 1GHz or faster CPU.
- You must have more than 1GB of System RAM.
- Your display must have a refresh rate of more than 10Hz.

To make sure Aero is enabled, you must also have the appropriate settings in Windows. Under the Windows Control Panel open Personalization. Select one of the themes shown under the 'Aero Themes' section. If these are not available, click the Display link in the left pane, then click 'Change display settings', then select 'Advanced Settings'. Under the Monitor tab, make sure the Colors option is set to 'True Color (32 bit)' and click Apply. Go back and again try to select an Aero Theme. If it remains unavailable, then you do not presently meet all the requirements above, and you cannot run the Aero interface.

Additional points to consider when attempting to use Aero:

- You will need a Windows Experience Index score of 3.0 or above on the Graphics component for Aero to be enabled automatically. If you've installed a new graphics card or drivers and you lose Aero, or it still doesn't show up despite having appropriate hardware, drivers and settings as above, see the Windows Experience Index section of the Performance Measurement & Troubleshooting chapter for more details.
- If you are running a very high resolution desktop and/or using multiple monitors then the minimum requirements for graphics card memory will rise. For example, a single monitor running at 2560x1600 resolution requires 256MB of Video RAM for decent performance in Aero.
- If you are using a Mobile PC set to a Power Saver power plan, Windows may automatically exit the Aero interface and switch to the basic interface at any time to save power. If you want to prevent this, go to the Power Options component of the Windows Control Panel and change the plan from Power Saver to one of the other presets, or customize it - see the Power Options section of the Windows Control Panel chapter.

If Aero is still not working for you and you have appropriate hardware and settings, go to the following location in the Windows Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\DWM]

Composition=1
CompositionPolicy=2
```

Change the DWORDs above to the values shown then restart Windows. Aero should now be available to choose under the Themes in Personalization. If it is not then your graphics hardware and/or drivers do not meet the minimum requirements for Aero. You can attempt to run the Aero-specific troubleshooter, as covered under the Troubleshooting section of the Performance Measurement & Troubleshooting chapter.

There are a range of Aero-related features which you can only use when Windows Aero is enabled. These are covered below:

Thumbnail Previews: This feature provides a small thumbnail image of the current contents of a particular application when you hover over a Taskbar item, or when using ALT+TAB task switching. Its functionality is covered in more detail in the Taskbar section further below.

Flip & Flip 3D: Windows Flip is the ALT+TAB task switching function available in previous versions of Windows. However under the Aero interface, accessing Flip by using ALT+TAB brings up a set of thumbnail previews of open windows. Furthermore, by using WINDOWS+TAB for Flip 3D, you can switch to an animated 3D representation of all open windows. If you want to have Flip 3D remain in 3D mode without having to hold down WINDOWS+TAB, use CTRL+WINDOWS+TAB instead; now Flip 3D will remain in 3D mode when you let go, and you can use the TAB key or the arrow keys to cycle through open windows, press Enter to select a window, or press ESC to cancel and return to normal 2D mode.

If you want to disable the 3D Flip functionality altogether, go to the follow location in the Registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DWM]

DisallowFlip3d=1
```

Right-click on the Windows key in the left pane and create a new key called DWM under it. Then click on DWM, and in the right pane create a new DWORD as shown above and assign it a value of 1. Reboot or logoff and logon, and Flip 3D will no longer work. If you want to regain this functionality, simply delete the key above.

Aero Peek: New to Windows 7, if you quickly want to see what is currently on your Windows Desktop, you don't need to minimize or close your open windows. Move your mouse cursor over the small glassy Aero Peek rectangle at the far right of the Windows Taskbar next to the Notification Area to instantly see through all open windows. Move it away to again see your windows as before. Click on the Aero Peek button instead and you will be taken to the Desktop, with all other windows minimized; click on it again to restore the windows to their previous positions. You can also trigger Aero Peek by pressing the WINDOWS key together with the Spacebar, and Peek will remain in effect as long as you hold down the WINDOWS key.

If you wish to alter the speed with which Aero Peek works, go to the following location in the Registry:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
```

```
DesktopLivePreviewHoverTime=400
```

Create the DWORD above and give it a value in milliseconds (1000 milliseconds = 1 second) in Decimal view to determine how long it takes for Aero Peek to fade to the Desktop once you hover your mouse over the Aero Peek rectangle. For example, to make the transition effectively instantaneous, set this to =1. Restart Windows or logoff and logon to see the impact of this change.

If you wish to disable Aero Peek, do the following: go to the Windows Control Panel, select Taskbar and Start Menu, and under the Taskbar tab, untick the 'Use Aero Peek to preview the desktop' box, then click Apply. This will disable the ability to temporarily 'peek' at the Desktop, and only allow the Aero Peek button to be used as a toggle for switching instantly to your Desktop, and back again to your open windows. You can also achieve the same function as Aero Peek by right-clicking on an empty area of the Taskbar and selecting the 'Show the desktop' or 'Show open windows' option as relevant.

Aero Snap: Windows 7 now provides native support for the use of basic mouse gestures on the Windows Desktop. The two most common categories of mouse gestures are called Aero Snap and Aero Shake. Aero Snap allows you to quickly resize open windows 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 Aero 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.

Aero Shake: Based on the same principle as Aero Snap, Aero Shake allows you to quickly minimize all open windows except one. 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 Aero 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 Aero Shake. Restart Windows for the change to take effect. If you want to undo this change, simply delete the value above and restart Windows.

The improved performance and functionality of Windows Aero, combined with its aesthetic aspects and reduced system resource usage means that for any system which supports it, there is no reason to disable it. However if you don't like Windows Aero and its related functionality, you can disable it by going to the Personalization component of the Windows Control Panel and selecting one of the themes under the 'Basic and High Contrast Themes' category, such as the Windows 7 Basic theme.

< 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 this component, 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 components: Desktop Background, Window Color, Sounds and Screen Saver. There are several preset themes displayed under two main categories in the main pane of Personalization - Aero Themes and Basic and High Contrast Themes. Aero Themes, as covered in the Windows Aero section above, are only available if your system supports Windows Aero. The Basic and High Contrast Themes on the other hand are supported by all hardware, though choosing these themes disables Windows Aero and any Aero-related features, including Flip 3D, Thumbnail Previews, Aero Peek, Aero Snap and Aero Shake.

You are not restricted to the preset themes displayed here, as you can download an additional range of official Windows 7 themes by clicking the Get more themes online link, or by checking the user-made themes available at various sites such as Deviantart. Most themes should come in the form of a .THEMEPACK file which you can simply double-click on to automatically install and apply.

Any custom themes you create or download will appear under the 'My Themes' category at the top of the Themes pane, and you can switch between any theme at any time simply by selecting it, and the appropriate changes will be implemented 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 7. These are stored under the *\Windows\Web\Wallpaper* directory under various theme-based categories. You can select a new location from which to select a Wallpaper by clicking the Picture Location box. You can also choose the 'Solid Colors' category to set a plain solid color Desktop background, or select the 'Pictures Library' option to list all the images stored in your Pictures Library, or simply click the Browse button and go to a specific directory which holds the image file you wish to set as a background. Note that you can change the size of the image icons displayed here the same as in Icon view in Windows Explorer - by holding down the CTRL key and scrolling your mousewheel 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 a copy of the image you have selected, and can be found under the *\Users\[username]\AppData\Roaming\Microsoft\Windows\Themes* directory with the name *Transcodedwallpaper.jpg* - 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. 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 you enter under the 'Change picture every' box. If you only select a single wallpaper, this feature has no impact. 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 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.
- 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 image is larger than the screen size, the same effect as the Fill option is achieved.
- 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 which 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:

Windows Explorer: Any image file can be right-clicked in Windows Explorer and most Explorer-based interfaces and the option to 'Set as desktop background' 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, or the optionally installed Windows Live Photo Gallery, 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. Note that the wallpaper being used in this method will actually be stored under the *\Users\[username]\AppData\Roaming\Microsoft\Internet Explorer* directory instead of the normal Windows wallpaper directory.

In terms of resource usage and performance, given the improvements in Desktop graphics resource management in Windows 7, you should not be overly concerned about the type of wallpaper you choose and should base the decision on what you find most pleasing. While monitoring overall memory usage and the Desktop Windows Manager process in particular (*dwm.exe*), I ran a range of tests and found that when switching between using a non-converted .BMP or .PNG wallpaper image of roughly 6MB size (using the Web Browser method above to prevent automatic conversion), and the same image in 350KB .JPG format, the .BMP and .PNG versions of the image actually resulted in much less overall system memory usage. The *dwm.exe* process would drop from 23MB to 14MB when the non-converted .BMP and .PNG images were used, and overall Available memory would also rise by a similar amount. So if your system is low on RAM you might consider using an uncompressed image, but in any case the difference is marginal at best, and the primary impact is on your video RAM, which when using the Desktop is typically underutilized anyway. The bottom line is you should select a wallpaper which best suits your tastes, not your performance concerns.

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 and a range of original Windows wallpapers here. Another method to find wallpapers of a specific size is to use Google Image Search, enter a search term for your generally desired wallpaper image (e.g. *sky*) and press Enter, then click the Exactly link in the left sidebar, enter a Width and Height in pixels to match your current screen resolution (e.g. Width 1920 Height 1200), then click the Search button.

One feature that Windows Vista Ultimate owners could access for free was the Windows DreamScene animated desktop, allowing the playback of video loops as wallpapers on the Windows Desktop as demonstrated here. This feature is no longer officially available in any version of Windows 7, and has been replaced by the static Desktop Slideshow feature. If you wish to enable a DreamScene-like animated desktop, you will need to use third party software such as Deskscapes. There are also various hacks which attempt to allow the installation of DreamScene on Windows 7, but these are not legal nor recommended, and will not be covered here.

WINDOW COLOR

This area allows you to configure the general color of the Windows Desktop components, as well as the transparency effect used in Windows Aero. Any changes are reflected in real-time, so select various colors and judge their visual impact on your current Desktop. You can use the 'Color intensity' slider to make the colors more or less saturated. If you wish to set a custom color scheme, 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.

If you untick the 'Enable transparency' box, this removes all transparency (glass-like) effects from the Aero interface. It does not disable Windows Aero, as Aero effects such as Aero Peek, Thumbnail Previews and so forth are still in effect. You can also determine how blurry the transparency effect is in the Aero interface by using the Color intensity slider - the further to the right the slider is taken, the more blurry and hence the 'thicker' the glass areas seem to be. For example, if you want to make the Aero transparencies appear almost like glass, click the white color box, ensure the 'Enable transparency' box is ticked, then move the 'Color intensity' slider all the way to the left.

Click the 'Advanced appearance settings' link to open a new window which allows the customization of all the common Windows display elements. Under the Item box you can select each element, and then in any other boxes you can alter parameters ranging from font styles, sizes and colors to the thickness of borders and background colors used. Most of these options only apply if you are using a non-Aero Basic Theme, however some of them apply to Windows Aero as well. For example, to change the font style and size of the text used for icon names, as well as in the Start Menu, select the Icon item in the Item box, then under the Font box select a new font (default is Segoe UI) and under the Size box select a new size (Default is 9), then click the Apply button - the change can instantly be seen when you open the Start Menu, or look at any Desktop icons. If you have the time and patience, you can customize your Windows interface quite thoroughly using the options available here. Note that any changes made here are part of your theme, and can be undone by selecting another theme, or set back to the default by selecting the standard Windows 7 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 which comes into effect after a period of inactivity, and is designed to prevent the screen from having any static images imprinted due to displaying the same image for a lengthy period of time. It's not absolutely necessary, because your Power Options should be set to turn off your display after a set period of inactivity, preferably the default of 20 minutes or less - 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.

In practice it can be useful to set a screen saver which kicks in after a period of perhaps 5 - 10 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 an 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 the 'Allow screen saver during playback' option in WMP 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. However this only works to actually secure your system if your User Account has a password. This is strongly recommended if you work in an environment where the PC is accessible by other people, as it allows you to leave your machine on 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.

SAVING THEMES

Once you've customized the four theme elements covered in the four 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 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 .THEMEPACK format for backing up purposes, or to share it with other people, 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.

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 - which 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 Windows Explorer at the Computer category; a User's Files icon which opens Windows Explorer at the current user's *\Users\[username]* folder; and a Network icon which opens Windows 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 files you install may alter the appearance of these Desktop icons, such as a custom Recycle Bin. This should be fine, as any customizations are usually done to maintain a consistent appearance in a custom theme, and as always you can easily undo a theme simply by selecting another one or creating your own.

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 Pointer 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, 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 pointer theme as a custom Scheme.

You can also choose to disable the shadow displayed under the mouse cursor by unticking the 'Enable pointer shadow' box, and whether themes can change the appearance of the mouse cursor by ticking the 'Allow themes to change mouse pointers'.

CHANGE YOUR ACCOUNT PICTURE

Clicking the 'Change your account picture' link in the left pane of Personalization lets you select an image to use for your User Account. These options are covered in detail under the Managing User Accounts section of the User Accounts chapter.

VISUAL EFFECTS

You can adjust a range of additional settings which help to personalize your Windows Desktop by going to the Windows Control Panel, selecting the System component, clicking the 'Advanced system settings' link, and under the Advanced tab of the window which 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 PC Security chapter.

Under the Visual Effects tab you can select a range of graphical effects to enable or disable within Windows. 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 Aero Peek' which is available under the Taskbar and Start Menu component of Windows Control Panel. This is why you may find some of these options are already ticked/unticked, because you may have adjusted them elsewhere. However there are a range of unique items here, such as 'Animations in the taskbar and Start Menu', which if unticked, removes all animated effects from the Taskbar and Start Menu. For example, with this option unticked, Taskbar Thumbnail Previews and Jump Lists may feel more responsive because there is no animated popup effect applied to their display.

Adjust these settings to suit your taste, and if you are running a slow PC, you may wish to disable a range of these features to increase responsiveness when using the Aero interface. Disabling some of these options can be a good compromise on slower machines, allowing you to keep Windows Aero enabled along with its many useful features, without having to switch to a Windows Basic scheme to maintain responsiveness. On faster machines, 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 in Windows 7.

< DISPLAY SETTINGS

This option 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. You will need appropriate graphics and monitor drivers for all of the features in this section to be displayed - see the Windows Drivers chapter.

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. This method is recommended over reducing your resolution if you wish to increase the text size on an LCD screen, because you should always be running at your native resolution as covered below. If you only wish to periodically increase particular portions of the screen, see the Magnifier section below. If you wish to set a custom size for the text used in the interface and/or alter the font size and style for individual Windows interface elements without altering the size of the entire interface, see the Fonts section later in this chapter.

ADJUST RESOLUTION

If you click the 'Adjust resolution' link in the main Displays window, you will be shown settings which 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 display. If the display is not detected properly and/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, which is the pure digital 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 shown as pixels in the format *Width x Height* (e.g. 1920 pixels x 1200 pixels). The resolution selected here primarily impacts on the Windows Desktop and any applications which run as windows on the Desktop. It does not apply to programs which run in separate full screen mode and have their own resolution settings, such as games. When selecting your Desktop Resolution, if you have 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 should be tagged as '(recommended)' by Windows. Selecting a resolution below your native resolution will result in blurry graphics and text; only the native resolution provides the sharpest and most accurate display output. 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 which is too small, you can adjust the interface size as covered further above by clicking the 'Make text and other items larger or smaller', or you can independently adjust only the text size as covered under the Fonts section later in this chapter.

Orientation: This option determines the direction in which the Windows Desktop is displayed. Landscape is the default for most monitors, where the width of the image is greater than its height, which matches the dimensions and orientation of a normal display. 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 monitors whose panels can be rotated on their stands.

If you click the 'Advanced settings' link, a new window opens which contains 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 which provide much greater information than listed here.

Monitor: This tab provides details of your monitor, and has two important monitor-specific settings: Screen refresh rate and Colors. The screen refresh rate is the number of times per second (measured in Hertz) your monitor refreshes the currently displayed image. This is called Refresh Rate, and is a complex setting which requires detailed knowledge before adjusting - see the Refresh Rate section of the Gamer's Graphics & Display Settings guide for more information. The Color option determines the complexity of color reproduction on your monitor. The 'True Color (32-bit)' option is recommended for most users; the 'High Color (16-bit)' option will reduce color complexity and hence not look as good. Note that Windows Aero will not be available unless you select 32-bit color depth.

Troubleshoot: You can click the 'Change settings' button (if available) to access the 'Graphics Hardware Acceleration' slider. Normally this slider should be at the far right for full graphics functionality. However if you are troubleshooting a graphics-related issue, lower this slider and test to see if this resolves the problem. If the problem is resolved when the slider is at None or Basic, then the issue is likely with your graphics driver as it controls the more advanced graphics functionality. If the button is grayed out, your current graphics driver does not support this functionality, hence it can be ignored.

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 more user-friendly method of configuring color output on your system.

Graphics Card Name: The tab bearing your graphics card name contains the means by which you can access further graphics-card specific settings. It is important that you set these up correctly as they control the bulk of your graphics card's advanced 3D functionality, particularly in games. See the Nvidia Forceware Tweak Guide or ATI Catalyst Tweak Guide as relevant for more details.

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, which is new to Windows 7. You can access this feature directly at any time by going to Start>Search Box, typing *dccw.exe* and pressing Enter. This feature is important in ensuring that your monitor displays its output as accurately as possible, as close as possible to the way content creators intended. When launched, it opens a new wizard which 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 display accuracy. When the calibration process is completed, the utility allows you to quickly compare your previous settings with your current settings 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 strongly 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 and/or high-contrast display settings.

ADJUST CLEARTYPE TEXT

Clicking the 'Adjust ClearType text' link in the left pane of the Display window will open the ClearType Text Tuner utility, which is an automated utility for adjusting the legibility of fonts on LCD monitors. This feature is covered in more detail under the Fonts section in this chapter.

The 'Change display settings' link takes you to the same settings as the 'Adjust resolution' link covered in the relevant section earlier in this chapter. The 'Set custom text size (DPI)' link is covered in more detail under the Fonts section later in this chapter.

MULTIPLE MONITORS

Multiple monitor setups are not covered in any detail in this book, however if you run a dual or multi-monitor configuration in Windows 7, there are a range of additional features 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.

Note that if you are connecting Windows 7 to multiple displays, press WINDOWS+P to open a quick menu for selecting which display(s) to send output to at any time.

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 Start>Search Box, 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 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.

Note that Full mode and Lens mode are only available if Windows Aero is enabled.

< TASKBAR

The Taskbar is the long bar which sits at the bottom of the screen on the Windows Desktop. It has been significantly redesigned for Windows 7. Dubbed the Superbar by some, the new Taskbar is designed specifically to merge 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 more transparent, and slightly larger than previous versions, to increase the visibility of the icons held there, and to allow easier selection by both mouse and human finger as part of Windows 7's new touch capabilities. The new Taskbar allows for a wide range of useful features which are detailed below. Note that for full Taskbar functionality as covered below, you must be using the Windows Aero interface, otherwise most of these features will not function in the manner described. See the Windows Aero section of this chapter for more details.

TASKBAR ICONS & EFFECTS

The icons in the Taskbar now have a range of additional features and effects. They act as a launching point for programs, or to switch to an open window as before, but these two functions are merged in Windows 7. You can pin a program permanently to the Taskbar, but if you open a 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 will also be represented by a single Taskbar icon. The way Windows 7 prevents confusion is by using various effects to differentiate the status of the various icons in the Taskbar.

An open program or window's icon will appear in the Taskbar with a transparent pane surrounding it. If a program has multiple instances or windows open, then there will be multiple layers of glass panes shown under that program's Taskbar icon. The currently highlighted or selected program/window will have a color-tinted pane surrounding it, with the color of the pane determined by the dominant color of the program's icon. For example, when Windows Explorer is being used, the yellow Windows Explorer folder icon on the Taskbar will have a yellow-tinged Aero glass pane around it. If you highlight any open window icon in the Taskbar, it will also show a color-tinted highlight. Inactive programs, such as pinned items which are not open, will have no pane surrounding them, 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, in Windows 7 the Taskbar icon now pulses gently in a soft color, requesting that focus be shifted to it.

Additionally, when a program is active and running a process which 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 Windows Explorer, even if the Explorer window is not visible or is minimized, a green progress bar-like fill effect will start moving across the Windows Explorer folder icon pane in the Taskbar, indicating the actual progress of the task. This allows you to monitor lengthier tasks without having to keep the application window visible in the foreground.

Program icons can be placed permanently on the Taskbar, just as they could in the previous Quick Launch Bar. By default Internet Explorer, Windows Explorer and Windows Media Player come already pinned to the Taskbar, next to the Start button. You can pin almost any program to the Taskbar by right-clicking on its icon 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, not remove it from the Taskbar. 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 new feature of Taskbar icons 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. These features include 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 which appear in the Jump List, such as Recent, which shows any recently opened files or folders. It should be noted that the Recent functionality of Jump Lists is also available on the Start Menu for various programs pinned there as well. If a small black arrow appears to the far right of a program in the Start Menu, click it and a Recent section will expand to show recently opened files for that program. You can click these to open the program with that file. If you want to permanently keep a particular Recent item in the Start Menu, right-click on it and select 'Pin to this list', preventing it from being bumped down and eventually moved off the Recent list. Conversely, right-click on an item here and select 'Remove from this list' to remove it immediately from the Recent listing 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 Start Menu tab, if the 'Store and display recently opened items in the Start menu and the taskbar' box is ticked, then the Recent category will appear in Jump Lists where relevant. If you want to disable the Recent feature, untick the box and click Apply. If you want to temporarily clear your Recent categories 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 how many items appear in the Recent category for Jump Lists by clicking the Customize button under the Start Menu tab of the Taskbar and Start Menu properties. At the bottom of the Customize Start Menu window, alter the 'Number of recent items to display in Jump Lists' option accordingly, then click OK and Apply. This applies to recent items in both Taskbar and Start Menu Jump Lists.

Programs which provide full support for Jump Lists have other available options and categories depending on the program. All native Windows 7 programs have full Jump List support, including Windows Media Player 12, Internet Explorer 8, and Windows Explorer. For example, right-click on the Windows Media Player icon in the Taskbar, and you will find a Tasks category which allows you to 'Play all music'. There are additional Jump List-related features available in WMP - see the Windows Media Player chapter for details. Similarly, Internet Explorer 8's Jump List can show frequently visited websites. Windows 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 Windows Explorer's Jump List. See the Advanced Features section of the Windows Explorer chapter for ways in which you can customize the Windows Explorer Taskbar icon.

THUMBNAIL AND FULL SCREEN PREVIEWS

First incorporated into Windows Vista, Thumbnail Previews allow you to see a live thumbnail-sized preview of the actual contents of an open window when hovering your mouse cursor 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 Aero Peek, it fades all other open windows away to 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.

Windows 7 provides additional functionality for thumbnail previews. In keeping with the subtle visual refinements that the rest of the Taskbar features receive, moving your focus between various thumbnail previews sees a smooth transition animation between different-sized preview windows. More importantly, programs can now display multiple thumbnail preview windows under a single icon in the Taskbar. This depends on appropriate program support, but one example can be seen when opening multiple tabs in Internet Explorer 8 - go to the IE8 icon in the Taskbar and 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 and hide the browser window behind another window (don't minimize it). When you can click to view the thumbnail preview for your browser, the video will be shown playing in the thumbnail preview. However whether the thumbnail preview continues to remain live when your 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 12 on the other hand will continue to play a video in its thumbnail preview, even when it is minimized. In fact Windows Media Player 12 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 do so as covered below.

To disable the Thumbnail Preview animation effects, which can help make thumbnail previews feel more responsive, go to the Windows Control Panel, select System, click the 'Advanced system settings' link in the left pane, then under the Advanced tab click the Settings button under Performance. Under the Visual Effects tab untick the 'Animations in the taskbar and Start Menu' and click Apply to disable all animations used in the Start Menu and on the Taskbar. There is also a setting here called 'Save taskbar thumbnail previews' - in my experimentation this 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 for some purpose. 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 (1000 milliseconds = 1 second) for 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, if you wish to disable thumbnail previews altogether, unfortunately Windows 7 has removed the ability to easily disable this function. Methods which worked with previous versions of Windows, and with pre-release builds of Windows 7, no longer work on the retail version of Windows 7. The best method for preventing thumbnail previews from appearing 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 never be seen. Of course if you effectively disable thumbnail previews in this way, then they also won't display for useful purposes such as the Windows Media Player Thumbnail Player mode.

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 below. Furthermore, if unticked, this option allows you to increase the height of the Taskbar by dragging the edge of the Taskbar outward. However locking the Taskbar does not prevent you from reorganizing the existing 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 allotted to programs, and provide a cleaner look to your Desktop, but can slightly reduce the speed with which you can access Taskbar icons and the Start button.

Use small icons: If ticked, this option forces the Taskbar to go back to a more traditional size, and reduces 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. 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 each program will each display a separate tab in the Taskbar, complete with a small icon and descriptive text within each tab. The only difference between these 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, programs which are pinned to the Taskbar will remain as icons.

So if you want the Taskbar to look more like previous versions of Windows, tick the 'Use small icons' box here, then select 'Never combine' for the Taskbar buttons option, and you will have much the same appearance. Even the Quick Launch bar will be reinstated in a manner of speaking, because pinned programs will always be displayed at the far left of the Taskbar as small icons, distinct from the active program/window tabs on the rest of the Taskbar.

TOOLBARS

Aside from displaying program icons (or tabs) on the Taskbar, you can also insert additional items to provide extra functionality 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.

Windows Media Player: There is no longer a Windows Media Player Toolbar to hold the Mini Player mode in Windows 7. See the Advanced Features section of the Windows Media Player chapter for more details and alternatives.

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 show 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.

Tablet PC Input Panel: This item places an icon on the Taskbar which when clicked opens the Tablet PC Input Panel. For anyone without a Tablet PC, it is simply a novelty and is not needed.

Desktop: If selected, this item places a Desktop Toolbar on the Taskbar, which when clicked opens a list of categories that you can select, corresponding to the main categories in the Navigation Pane of Windows Explorer. These can provide quicker access to common resources including the Windows Control Panel and your personal folders and Libraries.

New Toolbar: If selected, you will be prompted to choose a folder. The folder you select will be added as a Toolbar to the Taskbar, and when clicked, will open all its immediate subfolders in a menu, allowing you to navigate to any file or folder underneath your chosen folder.

Quick Launch: This item is not available by default in Windows 7, because the new 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 icons, 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 Windows 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. If you want this type of functionality, see the third party utilities at the end of the next section.

ADDITIONAL FEATURES

The Taskbar provides several additional miscellaneous features which some users will value. One of the most useful of these is the ability to launch or switch to any icon 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 Windows Media Player which is the third item from the left by default on the Taskbar, press WINDOWS+3, that is, the WINDOWS key and the 3 key at the same time. If a program being selected in this manner is already open, this method will switch to that program window.

There are additional interesting tips to consider. 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 Aero Snap to arrange two windows next to each other.

If you don't like the changes brought about by any of the options above, click on a window then right-click on the Taskbar and an Undo option will appear. For example, if you select Cascade Windows and decide you don't like the result, click on a window, then right-click on the Taskbar and select 'Undo cascade windows' to revert all open windows back to their original size and location.

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 Aero Peek button on the end of the Taskbar.

Start 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 which provide a different interface and additional functions. RocketDock and ObjectDock are the two most popular Taskbar-like utilities for Windows. Both are free, however ObjectDock requires purchase for access to more advanced features.

< START MENU

The Start Menu is an important component of Windows that not only contains links to your most commonly used programs and Windows features, it is also integral for quick access to the Windows Search functionality, as well as system Shutdown-related features.

As of Windows Vista, the default Start Menu was altered away from the Classic View in Windows XP to one which provides a list of individual programs on the left side, along with a list of common Windows features and locations on the right. An 'All Programs' folder at the bottom of the Start Menu provides an additional list of most of the programs and utilities installed on your system. Most noticeable for XP users is the Search Box at the very bottom of the Start Menu. Windows 7 does not visibly alter the Start Menu greatly from what was introduced in Vista, with the exception of removing the ability to switch to Classic View.

The Start Menu in Windows 7 does provide several new features. In particular, Jump Lists are incorporated into the Start Menu, allowing recently opened files to be displayed for programs, denoted by a small black arrow next to the program - see the Taskbar section earlier in this chapter for more details. The various links to personal folders, such as the Documents, Pictures, Music and Videos links which can be placed at the right side of the Start Menu, are now linked to the Libraries of the same name, rather than directly to your personal folders - see the Libraries section of the Windows Explorer chapter. The Search Box has also altered slightly in its options, as covered under the Windows Search chapter.

Customize Start Menu

To customize the Start Menu, right-click on the Start button and select Properties, or go to the Windows Control Panel, select the Taskbar and Start Menu component, then click the 'Start Menu' tab. Click the Customize button to access detailed customization options, each covered below. Any changes you make will only come into effect if you click OK then click Apply. The options are as follows:

Link vs. Menu: Where applicable, if the option to 'Display as a link' appears for a particular setting in this window, this makes the relevant component appear on the Start Menu as an item which launches that particular location or feature when clicked. If the 'Display as a menu' option is selected instead, the component appears on the Start Menu but when hovered over or clicked, it opens a menu list instead. You can still launch a component set to display as a menu by right-clicking on it and selecting Open. As expected, selecting the 'Don't display this item' removes the component from the Start Menu altogether.

Computer: This option controls whether the Computer item appears on the Start Menu. The Computer item corresponds to the Computer category shown in Windows Explorer, and displays all your available drives.

Connect To: If ticked, places a 'Connect To' link on the Start Menu which when clicked opens the Network Location box, which can also be accessed by clicking the Network icon in the Notification Area. If you're not connected to a network of PCs, and don't switch your Network Location often, untick this option.

Control Panel: This item allows quick access to the Windows Control Panel. I recommend selecting 'Display as a link', since the menu version can be quite large.

Default Programs: If ticked, places a 'Default Programs' link on the Start Menu, which accesses the Default Programs options, covered under the Default Programs section of the Windows Control Panel chapter. This is not necessary for daily usage, and is also readily available under the Windows Control Panel, so I recommend unticking this option.

Devices and Printers: If ticked, places a 'Devices and Printers' link on the Start Menu, which opens the Devices and Printers window. See the Devices and Printers section of the BIOS & Hardware Management chapter for details.

Documents: This option places a Documents item on the Start Menu which links to your Documents Library, not your *\Users\[username]\Documents* folder. This means that if chosen to be displayed as a link, clicking it will take you to the Documents Library, and if chosen as a menu, it will list all the folders currently linked to your Documents Library. The only way to disable this behavior is to attempt to disable Libraries altogether, which is covered under the Libraries section of the Windows Explorer chapter. To access your personal folders directly, you can enable the 'Personal folder' component covered further below.

Downloads: This option places a Downloads item on the Start Menu. In this instance, the Downloads component links directly to the *\Users\[username]\Downloads* directory, not a Library, even if this folder is included as part of a Library.

Enable context menus and dragging and dropping: If ticked, allows you to move, add or remove items in the Start Menu just as you would in Windows Explorer. It also allows you to use the right-click context menu on Start Menu items, which is important if you want to rename program icons, pin/unpin items or run a program as Administrator from the Start Menu for example.

Favorites Menu: If this option is ticked, the Internet Explorer Favorites will be displayed on the Start Menu as a menu. It is not possible to switch this folder to point to your bookmarks in other web browsers, so if you don't use Internet Explorer as your default browser you may want to untick this. For more advanced users, you can attempt to use XMarks to synchronize your other browser's bookmarks with Internet Explorer's Favorites, and hence make this feature more useful.

Games: This option places a Games component on the Start Menu, which is linked to the Games Explorer feature of Windows - see the Gaming section later in this chapter for more details.

Help: If ticked, the 'Help and Support' component is shown on the Start Menu, allowing you to access the Windows Help functionality. You can disable this and bring up Help and Support at any time by pressing F1 when using a particular Windows feature to get context-sensitive help.

Highlight newly installed programs: If ticked, this option will highlight in orange the launch icon and/or folder for any recently installed program(s) on the Start Menu. This generally isn't necessary unless you install multiple programs at a time and subsequently forget about them.

Music: This option places a Music component on the Start Menu, linked to the Music Library.

Network: If ticked, this option places a Network component on the Start Menu which when clicked takes you to the Network category in Windows Explorer. Untick unless you are on a network.

Open submenus when I pause on them with the mouse pointer: If ticked, this option allows you to open relevant folders or menus on the Start Menu simply by hovering your mouse over them. This includes the All Programs menu at the bottom of the Start Menu, as well as any components set to 'Display as a menu'. If disabled, you can only open these items by clicking on them.

Personal Folder: This option displays a component on the Start Menu with your username as its title. When selected it displays the subfolders of your *\Users\[username]* directory. This can be useful instead of or along with the other Start Menu components which link to your Libraries, because this component gives you direct access to the personal folders rather than being linked to a Library. I recommend selecting 'Display as menu' for this purpose.

Pictures: This option displays a Pictures component on the Start Menu which links to your Pictures Library.

Recent Items: If ticked, this option places a Recent Items component on the Start Menu, which when clicked shows a listing of your recently opened files. You can clear this list at any time by right-clicking on the Recent Items component in Start Menu and selecting 'Clear recent items list'. You can disable it by unticking this option, or by unticking the 'Store and display recently opened items in the Start menu and the taskbar' option under the Start Menu tab of the Taskbar and Start Menu Properties window, although this also disables the display of recent items in Jump Lists.

Recorded TV: This option displays a Recorded TV component on the Start Menu, linked to the Recorded TV Library which actually resides under the global *\Users\Public* directory, not your personal folders.

Run Command: If ticked this places a 'Run...' item on the Start Menu, which when clicked opens a Run box for entering command line commands. Alternatively you can open a Run box at any time by pressing WINDOWS+R. The Search Box in the Start Menu can also execute most commands in much the same way as a Run box.

Search other files and libraries: This option determines the behavior of the Search Box in the Start Menu. Depending on the option chosen here, you can exclude some or all files and Libraries from being displayed as part of search results. It is covered in more detail under the Search Methods section of the Windows Search chapter. It is recommended that 'Don't Search' not be ticked, as this will greatly reduce the usefulness of the Search Box in accessing your own files and folders.

Search programs and Control Panel: If ticked, this option determines whether searches initiated in the Search Box also display programs and Windows Control Panel items in the results. See the Search Methods section of the Windows Search chapter for more details. It is recommended that this option be ticked to allow quicker access to installed programs and Windows features via the Search Box.

Sort All Programs menu by name: If ticked, your All Programs menu in the Start Menu will have all the items it contains automatically arranged in alphabetical order. This is recommended, however you may wish to rearrange things manually, in which case untick this option. Note that when this option is selected, the 'Sort by name' context menu item will not appear when you right-click on any item in All Programs; with it disabled, the context menu entry will reappear, allowing you to manually force an alphabetical sort by name on any folder of All Programs whenever you wish.

System Administrative Tools: The Administrative Tools are covered in the Administrative Tools section of the Windows Control Panel chapter. This option allows you to choose whether to display them on the Start Menu. They can also be accessed via the Windows Control Panel, and under All Programs>Administrative Tools as well.

Use large icons: If ticked, the main items in the Start Menu will use the default larger icons. If you want a more compact Start Menu, untick this option.

Videos: This option allows you to display a Videos component on the Start Menu which links to your Videos Library.

Number of recent programs to display: This setting controls the maximum number of recently used programs to display in the Start Menu if the 'Store and display recently opened programs in the Start Menu' setting is ticked - see further below for more details.

Number of recent items to display in Jump Lists: This setting controls the maximum number of recent items to show in Jump Lists, both in the Start Menu and on the Taskbar. This option is only available if the 'Store and display recently opened items in the Start menu and the taskbar' setting is also ticked - see further below for more details.

Once you've made all applicable changes, click OK then make sure to click the Apply button on the main Start Menu tab otherwise you will not see your changes applied.

You can also manually reorganize or change the shortcuts and folders shown in the Start Menu by going to the following directories:

§ *\Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu* - Contains your user-specific Start Menu entries.

§ *\ProgramData\Microsoft\Windows\Start Menu* - Contains the system-wide programs and folders under the 'All Programs' item in Start Menu.

Finally, at the bottom of the main Start Menu tab of the Taskbar and Start Menu Properties window, you can alter several options:

Power button action: This setting controls what the power button shown in the bottom right of the Start Menu does. By default it displays the Shutdown option and hence is set to shut down your PC when you click this button. However you can change the default action by altering this option to select another action to take when the button is clicked. The button's text will change accordingly. Note that you can always access additional shutdown-related options by clicking the small white arrow to the right of the button on the Start Menu. Alternatively, you can bring up a Shutdown menu by pressing ALT+F4 on the Desktop. You can also add custom shutdown, restart and similar icons directly to your Desktop or Taskbar as covered under the Icons section later in this chapter.

Store and display recently opened programs in the Start menu: If this option is ticked, any recently opened programs will be shown in the Start Menu, the number of which is determined by the 'Number of recent programs to display' option covered further above.

Store and display recently opened items in the Start menu and taskbar: If this option is ticked, then if you have the 'Recent Items' component showing in the Start Menu, it will display a list of your recently opened files. Furthermore, this item controls the display of recent items in Jump Lists, both on the Start Menu and on the Taskbar. The number of recent items displayed for Jump Lists is determined by the value set for the 'Number of recent items to display in Jump Lists' option covered further above.

CLASSIC START MENU

If you prefer to have the Classic View for the Start Menu, similar to the way the Start Menu appears in Windows XP, then there are two ways of doing this. The easiest and neatest method involves using the free Classic Shell utility, which restores the Classic View for the Start Menu. It also contains several other features which replicate other classic Windows Explorer-based elements available in previous versions of Windows.

If you don't wish to install a utility to undertake this function, you can instead add a second Start button next to the original Start button which opens a menu similar to the Classic Start Menu. This gives you the best of both worlds. Follow these instructions:

1. Right-click on an empty area of the Taskbar, select Toolbars, then select New Toolbar.
2. Navigate to *\ProgramData\Microsoft\Windows\Start Menu* and click the 'Select Folder' button.

This item allows you to access a Classic Start Menu of sorts, however you can customize this further as follows:

3. Right-click on an empty area of the Taskbar and select 'Lock the taskbar' to unlock the Taskbar.
4. Right-click on this Start Menu Toolbar, and under the View menu select 'Large Icons', and also untick the 'Show Text' and 'Show Title' options in the main menu, reverting this Toolbar to a large folder icon.
5. To change the icon for this Toolbar to something more appropriate, right-click on one of the other icons in the menu for this Toolbar (e.g. the Default Programs icon) and select Properties.
6. Click the 'Change Icon' button and browse to the file *ehres.dll* under *\Windows\ehome\* - this file contains a green Start button icon which you should select and click Apply.
7. On the Toolbar, drag and drop this green Start button icon to the very left of the Toolbar icons.
8. Grab the dotted gray handle next to the normal blue Start button, and drag it to the far right of the Taskbar until the green Start button jumps to the far left of the Taskbar.
9. Drag the same dotted gray handle for the icons at the right side of the Taskbar to the left, until only the green Start button is visible along with your normal Taskbar icons.
10. Right-click on an empty area of the Taskbar and select 'Lock the taskbar' to lock the Taskbar again.

You can now click on the small double arrows next to the green Start button to open a Classic-like Start Menu. There is one last step:

11. If you wish to add your user-specific Start Menu items to this general Start Menu listing, you will need to copy all of the shortcuts from the entries in your *\Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu* directory to the *\ProgramData\Microsoft\Windows\Start Menu* directory.

If you wish to remove this second Start Menu at any time, right-click on an empty area of the Taskbar, select Toolbars and select 'Start Menu'.

Windows 7 has deliberately phased out the Classic Start Menu to encourage users to become accustomed to the new Start Menu. Remember that using the new Start Menu, you can access any program instantly, either by pinning it to your Start Menu or your Taskbar, or simply entering its name or any custom tags or unique attributes in the Search Box on the Start Menu. And of course you can always drag and drop any program link to the All Programs section of the Start Menu, should you wish to access it quickly from a full menu of programs on your system. I recommend getting used to and taking full advantage of the new Start Menu.

< NOTIFICATION AREA

The Notification Area was previously known as the System Tray in Windows XP, and 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 for the most part 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 by default. 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 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 switch to a calendar showing only months; then by clicking the year header you can switch to a calendar displaying only years; and then by clicking the decade header, you can switch to a calendar displaying groups of decades.
- Volume - The Volume icon allows access to the system-wide 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 or the Speaker icon respectively. These functions are covered in more detail in the Sound section of this chapter.
- Network - When clicked, the Network icon displays the current Network Location, and also allows access to the Network and Sharing Center - see the Network and Sharing Center section of the Windows Control Panel chapter for more details. Unlike previous versions of Windows, the Network icon does not provide an animated display of incoming/outgoing traffic on your network connection. To get simple information about the level of Network activity, open Task Manager and view the Networking tab. To have a Network icon which behaves similar to the one in Windows XP, install this free Network Activity Indicator utility. You can also use the Network Meter Gadget which displays upload and download speeds at a glance.
- Power - This option appears if you are using a computer which 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 which use 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 PC Security chapter, as well as the Windows Action Center section of the Performance Measurement & Troubleshooting chapter.

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 which 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 icon from the Notification Area, but allows notifications to be shown if necessary, including various icons which 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 it 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.

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 and 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 loading at startup or providing unnecessary prompts.

The programs listed in the Notification Area Icons customization window can include inactive or uninstalled programs. Over time this can make the window quite cluttered, so if you wish to remove the Notification Area entries for programs which are no longer installed then 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 regenerate them. Some icons may be missing for inactive programs until that particular program is launched again and detected by Windows in the Notification Area. There is also an automated free Tray Cleaner utility which attempts to do the same thing, however it may not remove all old entries.

You can override your normal choices in this Notification Area Icons customization window at any time by ticking the 'Always show all icons and notifications in the taskbar' box to force all programs and notifications to be seen in the Notification Area, and none will be hidden. This is useful if you quickly want to check for any new or hidden programs which have quietly added themselves to your startup programs for example, or if you can't find a notification or program icon for a newly installed program.

If you wish to completely remove the Notification Area from the Taskbar - though this 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.

< GADGETS

Introduced in Windows Vista, the Windows Sidebar was a location which held individual Sidebar Gadgets. Windows 7 removes the Sidebar but leaves the Gadgets functionality intact. Gadgets are small programs which display a range of useful information and can also provide features that can be more conveniently accessed on the Desktop. Unlike Windows Vista, Window 7's Gadgets only float on the Desktop, however they can snap neatly into position when close to each other, or when close to the edges of the Desktop.

Window 7 also reduces the performance impact of the Gadgets, by removing multiple instances of the *Sidebar.exe* process. Furthermore this process only starts when you add a Gadget to the Desktop, otherwise it remains disabled. In fact if you wish to disable Gadget functionality at any time, you can right-click on an empty area of the Desktop, click the View menu and select 'Show Desktop Gadgets' to unselect it and thus disable all Gadget-related resource usage at once. You can do the same thing to regain all your Gadgets and recommence the *Sidebar.exe* process.

ADD OR REMOVE GADGETS

To add a Gadget to the Desktop, either right-click on an existing Gadget and select 'Add gadgets', or go to Windows Control Panel and select Desktop Gadgets. Windows 7 comes with several default Gadgets such as Calendar, Clock, Weather and CPU Meter. While these are handy, the true power of Gadgets comes from the ability to download and install a wide range of user-made Gadgets, available when you click the 'Get more gadgets online' link at the bottom of the Add Gadgets window, or you can browse the list here. Note that Microsoft recently closed the Gadget Gallery, and instead now lists only a handful of third party gadgets for download. The links below are to a third party site which should be safe to use, but as always, first download any gadget and scan it with at least one malware scanner before installing it.

To install a Gadget, either download the .GADGET file and double-click on it to install it, or click the Download/Install button on the Gadget site to initiate installation. It should be added to your Desktop, but it will also be added to your Add 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 Add Gadgets window and select Uninstall.

There are a wide range of Gadgets which you can use, some of which I have recommended throughout this book to add desired functionality to Windows, and several of which I mention below as good examples of the types of free Gadgets available which you might like to try:

§ 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. For notebook PCs you can use this NoteBook Info Gadget which provides similar functionality but also has features such as battery charge.

§ Google Gadget - This Gadget allows you to launch any Google search from your Desktop, opening the search results in your default browser.

§ 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.

§ BBC News Gadget - Provides a range of feeds from BBC News. Requires Microsoft Silverlight 3 to be installed.

There are thousands of available Gadgets for Windows 7, since most Windows Vista Sidebar Gadgets also work on Windows 7. 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. Just 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, and only after reading any user reviews indicating the usefulness of it. Also use Task Manager to briefly check your CPU and Memory usage, as some user-made Gadgets might be resource intensive, outweighing their usefulness.

CUSTOMIZE GADGETS

You can customize any Gadget using a range of options available when you right-click on a Gadget itself, or move your mouse over the Gadget and click the relevant icons which appear next to it. The common options are covered below:

Add Gadgets: This opens the Add Gadgets window allowing you to place additional Gadgets on the Desktop.

Move: Allows you to move a Gadget along the Desktop, however the quickest method is to left-click and drag the Gadget like any other Desktop object, or grab the gray dotted 'Drag Gadget' area to move it around.

Always on Top: This option forces a Gadget to always remain on top of other open windows.

Opacity: Determines how transparent a Gadget is, with 100% being completely opaque (non-transparent). Even at 20%, which is the greatest transparency level possible, the Gadget turns completely solid whenever you hover your mouse over it.

Options: This opens up any available options for the Gadget, allowing you to further customize the Gadget's appearance and functionality if applicable. Some Gadgets have few if any options; it depends on the Gadget's creator as to how customizable it is. You can also access the Gadget options by clicking the spanner icon when you hover your mouse over the Gadget.

Close Gadget: Removes the Gadget from the Desktop. You can also close the Gadget by clicking the X icon when you hover your mouse over the Gadget.

Remember that if you want to quickly glance at any of your Desktop Gadgets, you can use Aero Peek to do so - see the Windows Aero section earlier in this chapter.

Gadgets usually have a relatively insignificant impact on normal Desktop performance and responsiveness unless you have very low system memory. Check the Task Manager to observe how much memory the *sidebar.exe* process is consuming. Gadgets have no impact on gaming performance since everything on the

Desktop is suspended when a full screen application is launched. Far from being just a gimmick Gadgets can actually be very useful as informational tools and even help in troubleshooting problems - for example you can use a CPU Meter Gadget to readily display and monitor real-time CPU or memory usage while using certain programs. I recommend spending the time to find Gadgets to suit your needs, but of course don't just load up your Desktop with lots of them.

< STICKY NOTES

Sticky Notes is a very useful feature which is similar to a Desktop Gadget. Only available on Windows 7 Ultimate, Professional and Home Premium editions, it allows you to place small 'sticky' notes anywhere on your Desktop, similar to a physical Post-It note. To access this feature go to Start>Search Box, 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.

Just like a Gadget 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 or Gadgets, 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 displays your Sticky Notes in its thumbnail preview, and also brings all Sticky Notes to the forefront of any open windows when clicked.

A Sticky Note is also 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 which is 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. However 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 + mousewheel 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 7 comes with several basic tools for capturing, viewing and editing images. These are covered in this section, along with several tools which can do a better job than the built-in Windows utilities.

Image Capture

If you wish to capture an image, whether from a game or on the Desktop, you can use press the 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.

An easier way to capture and save a screenshot of any portion of the screen is to use the Windows Snipping Tool. When you're ready to capture a screenshot, go to the Start>Search Box, type *Snipping* and press Enter. The Snipping Tool will open and the screen will be slightly grayed out. You can drag your cursor around the portion of the screen to be captured and when finished, let go - the Snipping tool will show the captured portion 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 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, I recommend using the FRAPS utility to capture multiple screenshots during a game. It also allows for video capture and benchmarking functionality 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 Windows Photo Viewer by default. 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. However there is a free enhanced version of Windows Photo Viewer called Windows Live Photo Gallery. This version integrates into Windows 7 seamlessly, providing similar functionality to Windows Photo Viewer with additional features such as the ability to edit an image in a range of ways when the Fix button is clicked. If Windows Live Photo Gallery doesn't become the default application for all the required image formats, manually associate it with the relevant file types - see the Default Programs section of the Windows Control Panel chapter for details.

Note that when you edit an image with Windows Live Photo Gallery, the original image is backed up to the *\Users\[username]\AppData\Local\Microsoft\Windows Photo Gallery\Original Images* directory. You can switch back to the original image by clicking the Revert button when editing that image.

You can also install a range of free add-ons called Plugins for Windows Photo Gallery, which enhance its functionality.

If you want to edit an image in more detail, you can open it in Windows Paint, which can be accessed either by going to Start>Search Box, typing *Windows Paint* and pressing Enter, or by right-clicking on the image in either Windows Photo Viewer or Windows Live Photo Gallery and selecting Open With>Paint. Windows Paint has been redesigned for Windows 7, and uses the Ribbon interface which is also used by Windows Wordpad, as well as recent versions of the Microsoft Office Suite. 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 a more advanced form of these 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 PC 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 expands this font collection with several additional fonts including Gabriola, Segoe UI Light, Segoe UI Semibold, and Segoe UI Symbol. Windows 7 also introduces the DirectWrite API for improved text display. A range of parameters relating to the display of fonts in Windows 7 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 in Vista and subsequently Windows 7, ClearType is the technology used to make fonts smoother and clearer on LCD displays. It is enabled by default in Windows 7, however 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. Alternatively simply type *ClearType* in the Start>Search Box and press Enter. 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 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 by going to the Windows Control Panel, opening the System component, clicking the 'Advanced system settings' link in the left pane, or alternatively typing *systempropertiesadvanced* in the Start>Search Box and pressing 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.

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 set through the ClearType utility, however 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 instead 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.

Bear in mind that 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 smooth and enhance text for PDF documents.

Furthermore, in some cases, even if you disable ClearType, Windows will retain ClearType for certain fonts such as Segoe UI - which as noted earlier, is the primary font used for much of Window 7's interface - to ensure that all prompts, dialog boxes, warnings and so forth display text precisely as intended, with no cut-off words for example. You can however manually change the font used for various interface components, and this is covered further below.

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, you can click the 'Set custom text size' link in the left pane of the Display component.

In the window which opens, you can adjust the Dots Per Inch (DPI) font scaling to a different size from the default of 96 pixels per inch, which is considered 100% by Windows. 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 your selection, and when you are comfortable with the new text size, click OK. The 'Use Windows XP style DPI Scaling' box can be ticked to prevent older programs which were not originally designed to work with Windows 7's DPI scaling 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.

Font Management

Accessible under Windows Control Panel, the Font component allows you to manage all the fonts currently installed in Windows 7. 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 Font folder.

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, 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 in the left pane for general font-related settings. Here you can tick the 'Hide fonts based on language settings' box to hide any fonts which are 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 is not recommended.

Custom 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 Start>Search Box, typing *eudcedit* and pressing Enter. It allows you to create custom fonts which you can then insert into documents using the Character Map utility, which can be opened by going to Start>Search Box, typing *charmap* and pressing Enter.

If you wish to change the actual fonts and font sizes used for particular Windows interface elements, open Personalization in the Windows Control Panel, click the Window Color option at the bottom of the window, then click the 'Advanced appearance settings' link. You can now select a particular component of the interface in the Item box, and not only customize its size and color, but for relevant elements, you can also change the font style and font size used. To see the impact of your changes, you can either view the changes in the preview window provided, or click the Apply button and the changes will be implemented to the Windows Desktop immediately. See the Personalization section of this chapter for more details.

If you don't want to change fonts for individual Windows elements in this way, you can apply a global change to all the fonts used for the interface by remapping existing Windows font families stored under the following locations in the Registry:

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

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

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\FontMapper\FamilyDefaults]
```

```
[HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache]
```

By specifying different font names and filenames in the relevant keys above, you can change the fonts which Windows 7 uses. For example if you change the following value:

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

```
Segoe UI (TrueType)=segoeui.ttf
```

to

```
Segoe UI (TrueType)=arial.ttf
```

This will tell Windows to use the Arial TrueType font in all places where Segoe UI would normally be used in the Windows interface. Restart Windows or logoff and logon for the change to be implemented.

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.

< ICONS

Icons are the images used to represent programs, files and folders in Windows. Windows 7 uses an icon system introduced in Vista, designed to allow scalable icons. As a result, all system icons in Windows 7 can be smoothly resized from very small to very large, without losing any significant amount of quality. To demonstrate this, in Windows Explorer go to any directory with a range of files, right-click and select View>Extra Large Icons, then either by clicking on the View button in the Command Bar and using the slider there, or by holding down the CTRL key and using you mouse scrollwheel, 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 also scale smoothly. Only icons which have not been created for Vista or Windows 7's icon rendering engine will exhibit signs of quality degradation as they as scaled up or down. See the Windows 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 Windows Explorer, able to be resized by right-clicking on the Desktop and using the View menu, or using the CTRL+Mousewheel method. Under the View menu you can also select whether to let Windows 'Auto Arrange' the icon layout, or 'Align to Grid' to place an invisible grid on the Desktop that icons will 'snap' to when moved. You can even disable Desktop icons if you so wish.

Fortunately 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 add 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 the icon names you will have to manually edit each icon's name.

REMOVE SHORTCUT ARROWS FROM ICONS

By default Windows adds a small arrow to the bottom left of any icon which represents a Shortcut link rather than a normal file, folder or program. This is to differentiate links - which are usually safe to delete or move - from actual files or programs. However 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
```

Note that the value name is indeed 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 and restarting Windows.

If you prefer an automated way of applying this change, you can use the old free version of the FXVisor program - download either the FXVisor 32-bit or FXVisor 64-bit version as relevant.

Remove '- Shortcut' from New Shortcuts

Whenever you create a new 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 Windows Desktop and in Windows Explorer for example. If you are experiencing problems with your icons displaying incorrectly, go to the *\Users\[username]\AppData\Local* directory under your personal folders 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 saved positions at any time. To give you this added functionality do the following on Windows 7 32-bit:

1. Download the file Layout.zip and extract the contents to an empty directory.
2. Copy the *Layout.dll* file to your *\Windows\System32* directory.
3. Double-click on the *Layout.reg* file to automatically make the appropriate changes to your Registry.
4. Go to your Desktop and arrange all your icons as you would like them to be saved.
5. Once done, right-click on the Recycle Bin and select the new 'Save Desktop Icon Layout' option. The positions of all the icons are now saved.
6. You can move the icons around freely and whenever you want them restored to their original saved positions, right-click on Recycle Bin again and select 'Restore Desktop Icon Layout'.

If you are using Windows 7 64-bit, the above method won't work. You must use the Dips64 utility instead. Install Dips64, then to save or restore Desktop icon positions at any time, left-click on an empty area of your Desktop to make sure no icon is highlighted. Hold down the SHIFT key while right-clicking on the empty spot on the Desktop to access the relevant 'Save icon positions' and 'Restore icon positions' context menu options.

SET SPACING BETWEEN ICONS

To adjust the spaces between your Desktop icons, you can manually move them. However if you've chosen automatic spacing - that is, right-click on the Desktop and select View>Align icons to grid - then you can adjust the fixed vertical and horizontal spaces placed between each icon by doing the following:

1. Right-click on the Desktop and select Personalize.
2. Select the Window Color option at the bottom of the window.
3. Click the 'Advanced appearance settings' link.
4. Under Items select 'Icon Spacing (Horizontal)' and 'Icon Spacing (Vertical)' one at a time, and edit their values to determine how many pixels are placed between the icons. The defaults are 43 pixels between icons. Smaller values squeeze them closer together, higher values spread them further apart.
5. Click Apply after each change and the impact should immediately be visible on your Desktop icons.

However by changing these icon spacing values, you will also change the spacing between all icons in windows, such as those in the Windows Control Panel window for example.

CREATE CUSTOM SHUTDOWN, RESTART, SLEEP OR LOCK ICONS

Instead of using the Shutdown, Restart, Sleep or Lock options available from the Shutdown button on the Start Menu, you can create icons which automatically perform the same functions with just a double-click. These icons can then be placed on the Desktop or pinned to the Start Menu or Taskbar 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 something descriptive like *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 which 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 something descriptive like *Restart* and click Finish.

Lock Icon:

To create an icon which automatically locks the workstation 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:

1. In the first box of the Create Shortcut Wizard, type the following and click Next:

   ```
   rundll32.exe User32.dll,LockWorkStation
   ```

2. Call the shortcut something descriptive like *Lock* and click Finish.

Sleep Icon:

To create a Sleep icon which 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 something descriptive like *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). Also note that once these processes begin they can't be aborted. If you want more command line switches which can be used with the shutdown command, open a Command Prompt, type `shutdown /?` and press Enter.

If you don't want to create custom icons for these functions, use the Control System with Clock Gadget instead.

Icon Creation and Customization

Windows 7 uses scalable icons which 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 7 icons are fully compatible with Vista, and vice versa, since Vista introduced this new icon system. They are also backward compatible with Windows XP, however only lower resolution versions of the icon (16x16, 32x32 and 48x48) will be shown in XP.

If you wish to create or edit Windows 7 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 Windows Explorer chapter.

< SOUND

One of the major changes which 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 7 continues with the use of this new audio model with some minor technical refinements.

The Windows audio stack (software sub-system) 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 designed such that 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 driver. However the latest audio drivers are still important and 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 7, and thus cannot access these hardware-accelerated effects. This is not a major issue, as it primarily affects older games and applications which used DirectSound to provide advanced audio effects. All recent games use the OpenAL API, or their own custom audio solutions designed for the new Windows audio stack, and hence are not affected. However for older games which only support DirectSound audio, if you own a Creative Audigy or X-Fi-based sound card use the Creative ALchemy utility as a workaround to regain the additional audio effects; if you have a Realtek-based onboard sound chipset, you can use the Realtek 3D SoundBack utility.

Windows 7 adds several technical refinements to the audio model, as covered in this Microsoft Article. In short, these include improved stream management and device detection allowing Windows to determine the type of device connected and stream audio to or from it more appropriately and seamlessly; improved HDMI audio support; improved support for communication devices such as Voice Over IP (VOIP); and refinements to the Volume Mixer interface.

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 which 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 it, 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.

Under the new Windows audio stack, 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. Just like the master volume slider, the Volume Mixer allows you to set the volume level for each application, and to mute/unmute each specific application's sounds. Importantly, there is a

'System Sounds' slider here which controls the level for general Windows sounds. You can also access the Sounds tab of the Sound component - which is covered further below - by clicking the icon at the top of the 'System Sounds' slider.

Windows will only display an application in the Volume Mixer if they have been used to play back audio at some point in the past. Furthermore, Windows remembers the volume level you set in the Mixer for a particular application, even if it is not active.

You can also access a new option in Windows 7 which affects the display of volume sliders. 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 SPDIF 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 audio configuration options in Windows 7, 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'. The options in this section are covered below.

PLAYBACK

This tab lists all the available sound playback devices on your system. This includes devices such as speakers, headphones, and various output channels supported by your sound device, such as SPDIF. 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 which you are certain you will not use, and select 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 an empty area of 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 a set of speakers 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 general details about your audio hardware and connections. You can also change the icon used for this device by clicking the 'Change icon' button - this icon appears 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 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 enhance audio playback features covered in detail in this Microsoft Article. Note that this tab may have been removed or altered when you installed drivers for your audio device. The full set of basic enhancements are summarized below:

- 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.
- Virtual Surround - Converts multi-channel sound to two-channel, and back again if required.
- Loudness Equalization - Attempts to maintain a more constant sound level across a range of sources.
- Room Correction - Through the use of a microphone Windows can automatically calibrate a multi-channel home theater setup.
- Headphone Virtualization - Creates a 3D sound environment for headphones.
- Bass Boost - Boosts the Bass response on smaller speakers such as mobile PC speakers.

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 for adjusting enhancements, those should provide better quality audio enhancements as they are tailored to your sound device's capabilities. If you wish to experiment with the above enhancements however and they are unavailable to you, uninstall your sound device's drivers - see the Windows Drivers chapter. Regardless of whether you use these enhancements or those which 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, although bear in mind that this 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 which 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 devices on your system. The descriptions for options in this section are much the same as those under the Playback tab above. Note that in Windows 7, you can now 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. You can even disable the Windows Startup sound by unticking the 'Play Windows Startup sound' box, and disable the sound for the Windows Exit event to speed up startup and exiting.

Furthermore, for the sound events you do wish to keep, you can assign the same sound to several types of warnings to reduce resource usage. For example, you can assign the *Windows Exclamation.wav* sound to all general system warning sounds including Asterisk, Critical Stop, Default Beep, System Notification, and Windows User Account Control. By assigning the same sound to multiple events you will still get audible alerts of certain events, but you save memory since only one sound has to be loaded up, regardless of how many uses it may have. Of course this reduces the descriptive power of the sound, but in most cases the average user will be able to tell what the sound relates to due to associated visual prompts.

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 sounds 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, in the Start>Search Box. These can vary greatly and are not covered in this chapter, however these additional configuration options are very important as they can have a major impact on performance and audio quality in Windows 7 - 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 advanced high definition audio, and are actually more likely to work without any problems with the new Windows audio stack, since this is precisely the type of hardware it was designed for. As long as you find relatively recent Windows 7 drivers for the 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 Windows features.

Gaming on Windows 7 is very similar to gaming under Vista, but has notable changes compared to Windows XP. Windows 7 continues the use of the Games Explorer, introduced in Windows Vista, as a central location for launching and managing games. Windows 7 also provides native support for DirectX 11 and DirectX 10, both of which are available in Windows Vista, but neither of which can be used under Windows XP.

DIRECTX 11 AND GAMING

Covered in the introduction to this chapter, DirectX 11 allows for additional graphics capabilities such as Tessellation to increase object complexity, Multithreaded rendering to improve graphics card utilization, and Compute Shader support as part of Shader Model 5.0 for processing general data on graphics cards. Unlike the transition from DirectX 9 to DirectX 10, DirectX 11 is an extension of the features of DirectX 10, not a re-write, and as such, some of the features of DirectX 11, such as multithreaded rendering improvements, can also be utilized on existing DirectX 10-capable graphics cards. Tessellation and other Shader Model 5.0 features on the other hand require dedicated DirectX 11-capable graphics cards, which is restricted to the ATI HD 5000 series or Nvidia GeForce GTX 400 series graphics cards or newer.

To take advantage of the benefits of DirectX 11 in Windows 7 you need all of the following:

§ A WDDM 1.1 graphics driver, as covered in the Windows Drivers and Memory Optimization chapters, as well as at the start of this chapter.
§ A DirectX 11-capable graphics card.
§ A game or application written specifically to take advantage of DirectX 11 features.

While WDDM 1.1 graphics drivers are now widely available, and DirectX 11 hardware is available as well, the number of games with DirectX 11 support is somewhat limited as listed in this Wikipedia Article. Part of the reason for this is that most PC games are originally designed for console hardware, and such hardware is limited to DirectX 9.0. This means that even if implemented in a PC game, DirectX 11 features may not be extensive or provide much visual or performance difference over DirectX 10 or 9. Indeed DirectX 11 features may decrease performance significantly in return for minimal visual enhancement if not implemented properly, so where possible you may wish to select DirectX 10 or even DirectX 9 rendering paths to provide added performance in games.

If you have DirectX 11-capable hardware, you can see the types of changes possible with DirectX 11 by using the free Unigine Heaven utility as covered under the Third Party Tools section of the Performance Measurement & Troubleshooting chapter. For DirectX 11-capable ATI graphics card owners, you can also try these free ATI DirectX 11 Demos; for DirectX 11-capable Nvidia graphics card owners, try these free Nvidia DirectX 11 Demos.

DirectX 11 clearly provides the potential for unprecedented levels of realism and graphics complexity, the key issue is whether games developers can viably take advantage of such a potential on the PC. Given DirectX 11 graphics hardware is completely backwards compatible and runs DirectX 10 and DirectX 9 extremely well, if you're purchasing a new graphics card it is worth investing in a DirectX 11-capable card wherever possible.

Games Explorer

Games Explorer is the central location for games in Windows 7, both for the games built into Windows such as Hearts and Solitaire, as well as any games you install. You can access it by clicking the Games item on the Start Menu, or by going to Start>Search Box, typing *games* and pressing Enter. Games Explorer is designed to replace the need for having multiple Desktop icons for games. To make access to Games Explorer easier, drag and drop the Games item from your Start Menu onto your Desktop or the Taskbar - though note that if added to the Taskbar it becomes a location under the Windows Explorer folder; to alter this behavior, see further below.

Games Explorer is based on Windows 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 Windows 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 highlighted, providing additional information on the game; and a Preview Pane 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.

By default Games Explorer contains a range of Windows games, and includes several Internet-based games, some of which were not available in previous versions of Windows: Internet Backgammon, Internet Checkers, and Internet Spades. You can uninstall any of these games by using the 'Turn Windows Features On or Off' link under the Programs and Features component of the Windows Control Panel. You can also remove the 'More Games from Microsoft' icon - which simply points to this Microsoft Games Site where you can download additional free and non-free games - by unticking the 'More Games' component under the Features selection list. See the Programs and Features section of the Windows Control Panel chapter for more details. For the most part, there is no need to uninstall these games, as there is no performance benefit in doing so, and you can easily remove them from view in Games Explorer by right-clicking on the relevant game and selecting 'Hide this game' - see further below for more details of hiding and unhiding a game.

Installing any 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 game service like Steam. If a game icon is missing from Games Explorer, you can drag and drop its launch icon from the Start Menu, 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, as detailed in this Privacy Statement. 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 and problems, 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 Search Box.

In addition to these options, there are other features and customization options worth noting in Games Explorer:

Tools and Parental Controls 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, there are no new options here. The same goes for the Parental Controls button which takes you to the Parental Controls screen, covered in more detail under the Parental Controls section of the User Accounts chapter.

Layout: If you want to streamline 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 / Pin to Start Menu: If a game is right-clicked, these options can be selected to pin a specific game icon to your Taskbar or Start Menu, allowing you to launch that game directly from the Taskbar or Start Menu without having to open Games Explorer. You can also do the same thing by dragging and dropping games from Games Explorer into the Taskbar or Start Menu.

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 Games section right-click on the game and select 'Create Desktop Shortcut', then drag and drop this 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.

Add Box art and Details: For any game in Games Explorer, you can add box art and various other details by firstly ensuring that the 'Download art and information about installed games' setting is ticked under the main Options window for Games Explorer. However older games and Steam games may still not update with box art and other details, so you must add these in manually. The best method is to use the free Game Explorer Editor utility. This utility provides a graphical interface for properly editing and configuring games in Games Explorer. Its usage is relatively straightforward, however if you want more instructions click the Tutorial link on the left side of the site. To find box art for a game, find the game's listing on AllGame and use the box art displayed there. Note that you cannot edit the Ratings for games, as these must be digitally signed to work.

If you wish to manually edit the details for a game, these are held in 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 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 best edited using the Game Explorer Editor, as they require particular custom files to operate properly.

Some games installed on Steam may appear properly in Games Explorer, but others won't appear at all, and if their Desktop icon is dragged and dropped into Games Explorer, will not show up correctly. To add Steam-based games into Games Explorer and customize them properly, you can use the free Steam Assistance Project. Upon installation the program will automatically try to detect your Steam games and allow you to select from a list of those detected, or manually add a game. The information and art displayed for each Steam game can then be thoroughly customized as desired. Once the process is completed, and if you are happy with the results, the program can be uninstalled at any time without removing your customizations.

Customize: One of the most noticeable changes made to Windows 7's Games Explorer is the removal of the Customize right-click option for a game. In Vista this provided users with the ability to edit a game shortcut, allowing for tweaks and customizations to be added directly to the shortcut. This has been deliberately removed in Windows 7, as explained by a Microsoft employee in the comments in this Microsoft Article, because it is believed that removing this option simplifies Games Explorer for the majority of customers.

Fortunately it is still possible to customize a game shortcut in Games Explorer in two ways. The first method involves finding a game's existing Desktop icon, or opening Windows 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 an existing icon for that game in Games Explorer, you can right-click on it and select 'Hide this game' to remove it. Finally, edit this new shortcut you added to Games Explorer to add box art and other information using the Game Explorer Editor utility.

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 Windows 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.

You can also add or remove menu options for Games Explorer game icons in a similar manner. Under the *\PlayTasks* directory, there are several subfolders numbered *\0*, *\1*, *\2*, *\3*, etc. The *\0* subfolder contains the launch icon for the default Play command, which executes when the icon is double-clicked. The other folders contain various other right-click menu functions, such as links to Support or Readme.txt files. You can edit, rearrange or delete any of these shortcuts, or you can create new ones. To add an entirely new right-click menu entry, create a new subfolder under the relevant *\PlayTasks* folder, name it with the next highest number available, and place a shortcut under that folder with an appropriate name. This shortcut will then appear as an extra right-click menu entry for that particular game in Games Explorer.

Pin Games Explorer to Taskbar: If you move the Games Explorer shortcut to the Taskbar - such as dragging and dropping the Games item from the Start Menu to the Taskbar - this will only pin an additional Games location to the existing Windows Explorer folder icon's Jump List. Fortunately you can drag and drop individual game icons from within Games Explorer to the Taskbar, and these will be created as separate icons. However to create a separate Games Explorer icon for pinning to the Taskbar, do the following:

1. On the Windows Desktop, in an empty location right-click and select New>Shortcut.
2. For the location, enter the following exactly as shown:

```
%SystemRoot%\explorer.exe /E,::{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}
```

3. Name the Shortcut appropriately, such as *Games*.
4. Right-click on this new Shortcut, select Properties and click the 'Change icon' button.
5. Browse to the *\Windows\System32* folder, select *imageres.dll*, find the Games Explorer icon, select it and click OK, then click Apply and OK again to close the Properties box.
6. Right-click on this shortcut and select 'Pin to taskbar'.

This custom shortcut to the Games Explorer will now display separately to the Windows Explorer folder icon, and provides a convenient way of accessing all your games from the Taskbar.

OLDER GAMES

If you are having problems running older games under Windows 7, keep in mind the following:

§ If UAC is enabled, make sure the game is being run in Administrator mode. Older games will not request Administrator level privileges even if they require it, and hence may 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 PC Security chapter for details.

§ Right-click on the game's Desktop shortcut or the original game executable, select Properties, and under the Compatibility tab select 'Run this program in compatibility mode for' and select first 'Windows Vista', then 'Windows XP (Service Pack 2)' to see if this resolves the issue.

§ If the game was made around 2005 or prior, 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 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 very old 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 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.

OVERCLOCKING

When people want additional performance from their PC, they may undertake a procedure called Overclocking. This is the process of increasing the clock speed of a component beyond its normal specifications, hence the term 'over clocking'. 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 this 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? The 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 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 both at the hardware and software level which must be taken into account to achieve proper stability. This chapter examines the general theory and operation of overclocking, and is a starting point for people interested in this topic.

< BENEFITS AND DRAWBACKS

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' attached to overclocking - 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

§ There are 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.

§ The overclocked component, and therefore your entire system, may become unstable and crash randomly - 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 mistakenly blame Windows, their drivers or the game or application instead. 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 on your system can result in instability leading to data corruption, up to and including the loss of all your data. Often this data corruption can occur subtly over time without any indication or warning.

§ Excessive heat can damage or permanently kill a component - 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, so it is not as rare as might be thought.

§ Overclocking automatically voids the 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 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 specifications.

§ Overclocking reduces the life span of the component - since an overclocked component is working beyond specification and working 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.

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 simply because people flippantly encourage you to do it. Overclocking is easy, but overclocking properly and with perfect stability is actually very difficult.

< METHODOLOGY

The precise details of how to overclock vary depending on your particular hardware configuration and BIOS options. The information below is only indicative and designed to give you a broad idea of the types of steps involved in overclocking; for more detailed information see the guides linked to at the end of this chapter. Importantly, before commencing any type of overclocking you must make sure you are totally familiar with the exact brand, model and default specifications of your major hardware components. If necessary refer to any packaging or manuals which came with your system, and more importantly, see the System Specifications chapter for links to tools which can help you identify your components and their precise capabilities in detail.

Also make sure that before changing any BIOS settings for the purposes of overclocking that you record your existing BIOS settings. This is because in some cases when overclocking beyond the point of stability, you will have to reset your BIOS - or it may reset automatically - back to its factory default settings, losing any customized settings you've put in. So document the major BIOS settings which you've altered through any general BIOS customization.

CPU OVERCLOCKING

Overclocking a CPU typically involves entering the BIOS and increasing the speed of the Front Side Bus (FSB) or QuickPath Interconnect (QPI) for Intel CPUs, or HyperTransport (HTT) for AMD CPUs. The FSB/QPI/HTT is the main pathway (Bus or Interconnect) between your major system components, and as its speed increases, information is transferred back and forth more rapidly between all your major components working off this bus speed. There are various settings in the BIOS which alter the speed of these buses or interconnects, however depending on the setting used, you may also be increasing the speed of other components, such as your system RAM. Check the relevant settings in your motherboard manual.

Your CPU also has a Multiplier, which as the name suggests sets the overall CPU speed in MHz as a multiple of the main Bus/Interconnect speed. For example, on a system with an effective Bus speed of 200MHz and a CPU that has a multiplier of 20, the result is a CPU speed of 20x200 = 4000MHz = 4GHz. Some CPUs have their multiplier locked at the hardware level, which means you can't actually change it, so the only method of adjusting the CPU speed in such cases is by altering the Bus speed.

RAM OVERCLOCKING

Increasing the speed of your RAM is dependent on a number of factors. Overclocking refers to the process of increasing the clock speed of a component; in the case of system RAM this involves raising the main system Bus/Interconnect frequency, or simply raising the RAM's Frequency directly to alter the RAM's speed in MHz, depending on your available BIOS options. However you can also alter the Timings (Latency) of a memory chip such that it refreshes faster between operations, meaning less waiting time between each operation and hence faster performance.

Whether increasing RAM speed or lowering latency is the better option is not clear. There is no set answer - it all depends on your particular hardware and the applications you most commonly run as to the precise combination of RAM speed and RAM latency which will perform best and with greatest stability, so you will have to experiment. Generally speaking, applications or games 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 and particularly games which primarily require very complex calculations with repeated access to information in memory will benefit more from lower RAM latency. Obviously some applications and games require both, so again, there is no clear-cut answer.

RAM overclocking also depends a great deal on how many sticks of RAM you have, their quality, and how similar they are. Because your RAM DIMMs (Dual Inline Memory Modules, also referred to as 'sticks') have to work together in your system, if you have two or more sticks of RAM in your system, you must try and ensure that firstly they are all equally matched in terms of rated speed and timings, and secondly that they should ideally be from the same brand and model of RAM. RAM chips can vary in quality and performance, so having mixed brands or types of RAM can lead to a variety of problems - even when running at default speeds.

GRAPHICS CARD OVERCLOCKING

The following is a modified summary from the overclocking section of the ATI Catalyst Tweak Guide and Nvidia Forceware Tweak Guide. It applies to all graphics cards regardless of brand, however if you are an ATI or Nvidia graphics card user please read through the relevant guide above for full details.

The modern graphics card is a lot like a small computer by itself. It has a Graphics Processing Unit (GPU) which is the graphics equivalent of the CPU, it sits on a motherboard-like Printed Circuit Board (PCB), and has its own Video RAM (VRAM). And just like a computer system, the components on a video card can be overclocked to increase performance. Overclocking a graphics card involves increasing the frequency of the GPU (also called the Engine or Core) and/or the Video RAM (also called VRAM or Graphics Memory). 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 performance the higher you overclock each component. To overclock your video card, ideally you'll need a tool which allows you to change the clock speeds of the Core and the VRAM - you can use RivaTuner or ATI Tray Tools for these purposes.

Overclocking your video card is similar to CPU overclocking and RAM overclocking combined - simply increase the clock speed of the Core/Engine, and/or the clock speed of the Graphics Memory, both of which are measured in MHz. The Core generates graphics data, and depending on your CPU and the rest of your system specifications, increasing the core speed can result in a small or large overall performance improvement. The Video Memory transfers information to/from the Core, and increasing its speed can once again improve performance either slightly or significantly, in conjunction with your Core speed and the speed of the rest of your system.

All other things being equal, the higher the resolution being used for a 3D application or game and the higher the graphics settings, and the more recent the game, the greater the potential for graphics card overclocking to yield bigger improvements in performance. This is because newer and more graphically intensive games running at higher resolutions rely heavily on the GPU for their performance.

Remember however that if you have an old or low-end graphics card then overclocking is unlikely to improve performance dramatically. The reason for this is that lower end graphics cards simply do not have optimized hardware support for the advanced functionality demanded by recent games, such as the latest Pixel Shaders and Vertex Shaders. If your card does not have hardware support for a required advanced function, such as a new DirectX 11 feature for example, then overclocking cannot surmount this handicap.

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 and/or to push a component further, you will have to increase the voltage to these components. The three main components that can benefit from voltage tweaking are the CPU, the graphics card and RAM. The two main voltage adjustments you will find in almost any BIOS are CPU Voltage and RAM Voltage, and these are explained below.

CPU Voltage: This is the amount of voltage applied to the CPU. The base voltage will vary depending on the CPU architecture, however make sure to note what your CPU's default voltage is before raising it. The only reason to alter the CPU voltage from its default is that when overclocking your CPU you may notice that you cannot overclock it beyond a certain point, or that you experience a lot of instability at higher clock speeds.

Raising the CPU voltage by a small increment in your BIOS may allow the CPU to regain stability and/or allow you to push the CPU further. The theory behind raising the CPU voltage is more complex than just supplying more juice to the CPU, and you can read about it in this Wikipedia Article. The most important thing to understand is that upping the voltage beyond a certain point can result in permanent damage to your CPU, and strictly speaking any increase in the voltage can further shorten the life span of a CPU. However for the most part a small bump in voltage can help stabilize an overclocked CPU that is acting slightly unstable. Check your motherboard manual to determine the maximum safe voltage for your CPU, and remember that more voltage always equals more heat, which requires greater cooling to maintain safe temperatures.

RAM Voltage: Sometimes called DRAM Voltage, this is the amount of voltage for the RAM DIMMs. Just like CPU voltage, increasing RAM voltage can improve stability at higher clock speeds. This is particularly true if you're experiencing random reboots or sudden crashes to desktop, as these are almost always RAM related in some way. Once again, increasing the voltage to your RAM can result in permanent damage so do not overvolt by a substantial amount without first consulting with your motherboard manual to determine the maximum safe voltage level. Implement any increase in RAM voltage in very small increments, and provide additional cooling to prevent heat buildup in the area surrounding the RAM.

You can view your existing system voltages in the BIOS, however if you want a utility to monitor system voltages from within Windows, use the free CPU-Z or HWMonitor utilities. See the System Specifications and BIOS & Hardware Management chapters for other utilities which may also be useful.

There may be additional voltage settings in your BIOS, and unless you have full knowledge of what they do, and what a safe adjustment is, do not alter them as you can permanently damage your components this way.

< 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 your overclocking is contributing in some way to it, or is the sole cause of it. You will have to lower or remove your overclock and/or increase your cooling. Details on how to correctly test your system for stability are covered in the Third Party Tools section of the Performance Measurement & Troubleshooting chapter, but 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 overclock 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 even 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 of the BIOS & Hardware Management 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 experience instability regardless of any other settings you alter. Invest in a good PSU before considering overclocking your system.

COOLING

If you are overclocking, you need to know what the safe temperature range is for all of your major components. There is no single 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, however the temperature limits are different for various hardware, and in any case you should never let your component become hot enough to get close to these limits, since prolonged operation at such temperatures reduces the lifespan and increases potential instability. See the Hardware Management section of the BIOS & Hardware Management chapter for more details on cooling. Just like a good PSU, if your system does not have decent cooling, then overclocking is a waste of time as it will simply result in system instability and eventual damage to your components.

COMPARING OVERCLOCKS

One of the most common statements heard when people compare overclocks or are told that their overclock is unstable is: "But someone else who has the exact same system can overclock it much higher than me and their games don't crash - it must be a game bug!". A comment like that demonstrates a complete lack of understanding of some fundamental principles of overclocking:

§ 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 which factory they were produced in and which revision they are; that is, how early/late into the production run they were produced. For CPUs this is called Stepping.

§ No two people have the exact same conditions for their overclocking. 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 software environment will not be identical to anyone else's. You may have sub-optimal software settings, background programs that are the source of conflicts, or malware causing problems, or you may even have data corruption.

§ No two games or programs are identical in the way they use resources and stress components on your machine, and hence 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 and will crash most of the time.

Researching Overclocking

Having stressed the importance of researching overclocking before you dive into it, I recommend that you start by referring to the following guides as relevant for more details. This is obviously not a definitive list of places to research, nor have I personally tested out all the procedures in these guides - they are simply a good starting point, and provide an indication of the types of practical procedures involved in overclocking particular hardware:

General Overclocking Guide 1
General Overclocking Guide 2
Core2Duo Overclocking Guide
Core i7 Overclocking Guide
Core i5 Overclocking Guide
AMD CPU Overclocking Guide
GeForce GTX 275 Overclocking Guide
AMD HD 5750 Overclocking Guide

This chapter has been just a taste of the information available on overclocking. Don't rush into overclocking, do it slowly and methodically, and search Google and various tech forums for peoples' experiences with overclocking hardware 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. However 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. Also, no two systems are identical so don't just automatically assume 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 you have the right tools and knowledge to undertake it properly, and if in doubt, 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.

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 performance measurement tools. By the same token, you may be trying to resolve a problem which 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.

Fortunately Windows 7 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 is the Performance Information and Tools and Troubleshooting components of the Windows Control Panel.

In addition to Window 7's built-in tools there are a range of third party programs which will further help you in benchmarking your performance and tracking down the cause of a problem.

In this chapter we look at the various tools and methods for measuring performance and troubleshooting system problems.

< WINDOWS EXPERIENCE INDEX

One of the first things Windows 7 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 you to measure your system's performance and detect any weak or problematic areas.

The results of the WEI are shown as a series of five sub-scores, culminating in a single base score shown 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.

Windows 7 continues with the WEI model introduced in Vista, however the score ranges have been expanded from a maximum of 5.9 to a new maximum of 7.9 to take account of new hardware, such as SSDs and the latest graphics cards. Windows uses the base score and sub-scores to determine a range of things, such as whether your system can display Windows Aero, or whether to disable SuperFetch for example, so this score is quite 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 the following types of tests:

- Compression and decompression using the LZW compression algorithm.
- Compression and decompression using the Windows compression algorithm used for hibernation files, ReadyBoost and other features.
- Encryption and decryption assessment.
- Computing hashes.
- Encoding of video.

The new score ranges above 5.9 in the Processor tests are for quad-core CPUs, and only eight-core CPUs can reach the maximum 7.9 score.

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. However the highest score attainable is constrained by the actual amount of system RAM (minus any memory reserved for graphics). For example, any system with less than 1.5 GB of available system RAM can only score a maximum of 4.5.

Graphics: This score is mainly used to determine how your system will run Windows Aero and play back Windows Media Video. It measures video memory bandwidth (in MB/s), however note the following restrictions:

- If your graphics card does not support DX9 then it can only score a maximum of 1.0.
- If the system supports DX9 or higher, but does not have a proper WDDM 1.0 or 1.1 driver than it can only score a maximum of 1.9.

Gaming Graphics: This score is calculated based on how many Frames Per Second (FPS) your graphics card can display for various D3D tests, in DirectX 9 and/or DirectX 10 modes. However note the following:

- If the graphics card does not support DirectX 9 then it can only score a maximum of 1.0.
- If the system supports DirectX 9 and has a WDDM 1.0 driver, it will score at least 2.0.
- If the graphics card doesn't support Shader Model 3.0 or higher then the maximum score possible is 4.9.
- If the graphics card is only running a WDDM 1.0 driver, the maximum score possible is 5.9.
- If the graphics card supports DirectX 10, is using a WDDM 1.1 driver, and can achieve around 40FPS or more at normal resolutions (e.g. 1280x1024), it can score in the 6.0 - 6.9 range.
- If the graphics card supports DirectX 10 or higher, is using a WDDM 1.1 driver, and can achieve higher framerates at higher resolutions, it can score in the 7.0 - 7.9 range.

In both the Graphics and Gaming Graphics components above, scores above 5.9 are only achievable by newer more powerful graphics cards running appropriate graphics drivers.

Primary Hard Disk: This score is calculated based on your primary drive's bandwidth measured in MB/s. All modern hard drives will score a 2.0 or above, though traditional hard drives are restricted to a maximum score of 5.9. Additional tests focusing on random read, random write, and flush assessments have been added to determine the presence of Solid State Drives, and SSDs which perform well in both sequential and random I/O scenarios obtain a score higher than 6.0. In particular, a score of 6.5 or higher indicates the presence of a fast SSD and in turn Windows will automatically disable certain drive-related features such as SuperFetch. However simply having an SSD does not guarantee a high drive score, as some older SSDs are not sufficiently fast in all respects to warrant getting 6.5 or above.

Looking at the overall base score, which is determined by the lowest sub-score resulting from the above tests, the breakdown of the type of overall system performance to expect in Windows 7 is as follows:

§ *Base Score 1.0* - This is the absolute minimum specifications needed to run Windows 7, but without Windows Aero and with a range of general performance problems. Best used only for things like email, Internet browsing and Solitaire.
§ *Base Score 2.0* - This is the recommended minimum specification to run Windows 7, and may be able to run Windows Aero but with some performance issues. Similar usage scenario as above, but with slightly more responsiveness.
§ *Base Score 3.0* - This is the average Windows 7 system which can run Windows Aero and perform reasonably well in normal applications, and provide basic performance in games.
§ *Base Score 4.0* - This machine will run Windows 7 well and be quite responsive, even in multitasking. Runs most applications and some games reasonably well.
§ *Base Score 5.0 - 7.9* - This machine is a high-end machine suitable for excellent performance in gaming, multimedia and multitasking. The actual tasks in which this machine excels depend on which particular components have the highest scores.

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. 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, and its existing weaknesses. The idea is that it highlights the weakest link of the main hardware components of your system, and there is good reason for this: your system is only as fast as its weakest link.

For instance, on a PC which scores a 7.0 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 you will run into problems with gaming. For example if the Memory or Primary Hard Disk score of the same machine is below 3.0, this means that while your graphics card can easily handle intensive 3D rendering for a game, your 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 you may not be able to run some games at all due to insufficient RAM. To achieve a balanced machine, ideally all your sub-scores should be similar to each other, and if you are looking to upgrade your system, then it would be wise to pay attention to which components are scoring lowly. If you want to view other peoples' scores, check on your favorite online forum, or at a site like WEI Share.

If you're buying a pre-built system then make sure it has a good base score, and don't accept any statements that the Windows Experience Index is not important. While WEI should not be the only factor you use in making a purchasing decision, a low WEI is an indication of potentially low performance and can also result in certain features being disabled in Windows.

WINDOWS SYSTEM ASSESSMENT TOOL

Windows takes the performance information it obtains from the Windows System Assessment Tool (WinSAT), used to calculate the Windows Experience Index, quite seriously. For example if you don't score 3.0 or higher in the Graphics component, then Windows 7 will not enable the Windows Aero interface. If you have an SSD but it is a slower model, then Windows will not disable certain features which are unnecessary for fast SSDs. Games can use WinSAT's performance information to automatically customize or disable certain game settings based on your score, although note that your score will not prevent you from playing any game, even if you don't meet its WEI requirements.

In short the WEI score is fairly important, and not just haphazardly put together. Therefore one of the first things you should do is to 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 individual scores 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 from WinSAT are stored in your *\Windows\Performance\WinSAT\DataStore* directory in an .XML file which you can open to see the details if you wish. 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 which provides an overview of your system's stability and problem history. You can launch it by going to Start>Search Box, typing *reliability* then pressing Enter, or by opening the Action Center from the Notification Area, clicking the Maintenance heading, then clicking the 'View reliability history' link.

The main feature of the Reliability Monitor is a System Stability chart which 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 arrows on either side of the graph 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 which may contain Errors (red X), Warnings (yellow exclamation) or Information (white i) events 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. 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 events than Event Viewer, which is why it is recommended for most users in the initial identification of problems.

To investigate any event, 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 bottom of the Reliability Monitor, which opens the Action Center Problem Reports window and displays all queued problem reports - see 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 of 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 7 installation should have very few if any errors or warnings, and hence should always be close to the 10 index score. From personal experience I can assure you that it is entirely possible for a correctly configured system to remain at or close to the 10 score for long periods of time.

< TROUBLESHOOTING

Whether you are having an immediate problem with a particular device, program or Windows feature, or if you want to troubleshoot a potential problem identified by the Windows Experience Index or Reliability Monitor, the simplest method of doing so is to start by using the built-in Troubleshooters introduced in Windows 7. 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, Appearance and Personalization, and System and Security.

You can obtain additional troubleshooters by clicking Yes to the 'Do you want the most up to date content available for troubleshooting' box at the top of the Troubleshooting window. This will download additional troubleshooters if available when you select any category, and is recommended to make sure you have access to the latest troubleshooting utilities in Windows 7. You can alter the settings for the troubleshooter functionality by clicking the 'Change settings' link in the left pane:

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 in the main Troubleshooting window.

Allow users to browse for troubleshooters available from Windows Online Troubleshooting service: If ticked, this allows all users on your PC to download additional available troubleshooting utilities.

Allow troubleshooting to begin immediately when started: If ticked, allows a troubleshooter to begin immediate detection of issues when launched. Not recommended unless you are an extremely novice user.

To initiate troubleshooting, click one of the 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 which 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. You can also click the 'View detailed information' link which then appears to find out more about the particular problems detected and repairs suggested. This must be done for every troubleshooter separately, and these steps will ensure that the troubleshooter provides you with details on the actual tests run, the types of issues 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 intermediate to advanced users, as it gives you greater information and control over the changes being made to your system.

There are additional resources available here to assist beginners, such as the 'Get help from a friend' link, 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 trusted individual. There is also a link to the Problem Steps Recorder, which is covered further below.

The Troubleshooting window is of greatest benefit to beginner users who have common problems that Windows can readily detect and resolve, or provide simple links or instructions for users to resolve the issue themselves. However 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 troubleshoot and resolve such issues on your own.

Problem Steps Recorder

The Problem Steps Recorder utility is new to Windows 7, and can be found under the 'Get help from a friend' link in the Troubleshooting window, or by going to Start>Search Box, typing *psr* 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 which can be viewed in Internet Explorer, and can also be sent to a tech support person who can then view precisely what steps you undertook and what images 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, which is 25 by default.

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 family member or a 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 which records your steps as full motion video, then you can 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 PC 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 sections throughout this book. The primary unique feature under Maintenance is Problem Reports, which is covered in this section.

As part of Windows Error Reporting functionality, Windows 7 will record any problems you experience with applications or Windows. These problem reports can be viewed and sent to Microsoft to check for available solutions. To view all unsent problem reports, click the 'View problems to report' link in the

Maintenance area of Action Center; to view all problem reports, both sent and unsent, click the 'View all problem reports' link at the bottom of the Reliability Monitor, or go to Start>Search Box, type *view all problem* and press Enter.

To see full details of the problem, click the 'View technical details' link next to the relevant problem. In particular, note the specific file or feature which has triggered the problem report. 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 report to Microsoft by making sure there is a tick in the box next to the relevant problem report(s), and then clicking the 'Check for solutions' button or link. If available, you can also select the 'Check again for solutions to other problems' box to re-report earlier problems and see if there is a revised solution available.

When checking with Microsoft for a solution, the information sent to Microsoft is detailed in this Microsoft Article, and 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 to confirm sending this information, though Microsoft will not use this information to identify or contact you. You can review the information being sent before confirming this request. If Microsoft requires more information regarding a problem you reported, you will be prompted to send the 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.

If you have any doubts, you can untick, or right-click and select delete, any problem(s) for which you do not wish to send a report to Microsoft before clicking the 'Check for solutions' button. Furthermore, to customize this 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 automatically check for solutions, 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.

If you are certain you will never use this functionality, you can disable it. This 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 less advanced users. Most of the time though you will have to do further investigation on your own to work out the source of a problem. Even if you find no 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 main Performance Information and Tools window, 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 going to Start>Search Box, typing *eventvwr* 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, however learning to use it can improve your chances of finding out about problems or performance issues. For a more user-friendly display of the more 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 which 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 (1000ms = 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 problem, when in fact it is not particularly significant. Regardless, this form of automated diagnostic provides information which 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, 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 to the right.
3. Double-click on the Event ID which 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 and are not 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 instead you can try searching the official Microsoft Error Message Center or try this Event ID Site or Google 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 all Errors in the Overview and Summary. 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.
- 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 has been resolved through some other action, such as uninstalling the problematic program or patching it with an update. Focus on issues which occur often and more recently. If the error is very recent, such as during your latest session, consider what you have done recently that may have triggered it. For example, have you recently disabled a particular Service or made a Registry change?
- Remember that a log showing many events may just be the same issue which has occurred repeatedly every time you start your PC. That is, 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. You can 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 which are presented to you in Event Viewer, click the 'Create a custom view' link in the right pane, and 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 which can help you refine where a problem is occurring if you take some time to go through it. Fortunately Windows 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 going to Start>Search Box, typing *perfmon* 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 and games need - this can help identify any bottlenecks.

To begin monitoring resource usage, open the Performance Monitor, and in the System Summary window you can see a snapshot of various system parameters in real-time. This type of information is covered further under the Resource Monitor section 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 graph will now update to start mapping all the variables you've added, and you can see in the legend at the bottom of the graph the components being mapped, the color for each component, and you can tick or untick particular ones if you wish to temporarily show or hide them. Remember that since the Y (vertical) axis scale is fixed, some components will not display in any meaningful way when using a common scale. However you can change the way the graphed data is displayed in two ways:

§ The simple method involves clicking the 'Change graph type' button and selecting either Histogram, or Report view in particular which may be much more meaningful.

§ 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 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 go to Start>Search Box, type *perfmon /report* 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 still highlight these.

Ideally you should run several System Health Reports, firstly 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, though again these are usually highlighted in the section above, so you can browse them for more detailed information. The Resource Overview section 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 the small triangle at the far right of a particular category, or you can jump directly to specific areas of the report by left-clicking once on the report icon in the middle of any of the category toolbars, 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 under the 'Advanced Tools' link in the Performance Information and Tools component of Windows Control Panel, or by clicking the 'Resource Monitor' button under the Performance tab of Task Manager, or by going to Start>Search Box, typing *resmon* and pressing Enter.

Under the main Overview tab, you can see the four categories: CPU, Disk, Network and Memory. Clicking on any one of these categories expands that section, showing its components. However 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. For example, to see all the resources used by a particular process, click the Image column; to see all resources used by a particular file, click the File column; to see the process currently writing or reading the most to disk, click the Write or Read column respectively. 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 'Start Task Manager'.
§ Go to Start>Search Box, type *taskmgr* and press Enter.
§ Right-click on the Taskbar and select the 'Start Task Manager' item.
§ Press CTRL+SHIFT+ESC to bring up Task Manager.

By default Task Manager only shows the running processes for your particular User Account. To see all running processes, including System and Network processes, click the 'Show processes from all users' button under the Processes tab. This will provide the most detailed view of what is running on your PC at the moment, and is always the recommended view. Task Manager has a range of uses, and we look at the most important of these in this section. Each tab is covered in its own section below:

APPLICATIONS

This tab of Task Manager contains a list of any running programs, but does not include those running in the background, such as Windows services and utilities, driver-related programs, programs in the Notification Area and so forth. As such it is not a complete list of programs running on your system. However you can use it to highlight a particular program on the list, and if it is frozen and unresponsive, click the 'End Task' button to force Windows to close the program. You can also see the processes associated with a program by right-clicking on it here and selecting 'Go to Process', which takes you to the relevant processes under the Processes tab.

PROCESSES

This tab lists all processes currently running on your PC, as long as you have clicked the 'Show processes from all users' button. You can view a range of real-time details about each process by going to the View menu, clicking the 'Select Columns' item, and then ticking the appropriate columns to have these details display under relevant columns in Task Manager. The full list of column items is covered in more detail in this Microsoft Article. I recommend that you at least have the CPU Usage, Memory - Private Working Set, Memory - Commit Size, and Description columns active to monitor CPU and memory resource usage. 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 Windows 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 a 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.

Services

This tab lists all Manual and Automatic Services on the system, and whether they are currently running or not - see the Services chapter for more details. You can right-click on any Service and select 'Go to Process' to see which process is associated with it. In most 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.

Performance

This tab is similar to the Resource Monitor utility, and indeed a 'Resource Monitor' button is available here for more advanced users. However this area is sufficient for basic monitoring of resource usage, as long as you understand the data being displayed - the memory information in particular can be confusing, so it will all be clarified in detail below:

Graphs

This section at the top of the Performance tab in Task Manager displays several graphs for easy interpretation of current resource usage information at a glance. Note that if you double-click on the graph display, it will maximize to only show the CPU-related graphs. The components shown are:

§ CPU Usage - This bar graph shows the total proportion of all available CPU resources currently being 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% and the other is at 0%, the bar graph shows a total CPU usage of 50%. This graph corresponds with the 'CPU Usage' percentage shown at the bottom of the Task Manager window.

§ CPU Usage History - This section displays line graph(s) showing your CPU usage history for each individual core on your CPU. There is a separate graph for every core, and in the case of HyperThreading CPUs, a separate graph for each virtual core as well. You can alter this by going to the View menu and under the 'CPU History' item selecting 'One Graph, All CPUs' to display a single history graph for all cores. This is not recommended, as being able to see which cores are working the most is a useful feature. Under the View menu you can also tick the 'Show Kernel Times' item to display the amount of CPU resources used by the Kernel (core Windows software) as a red line.

§ Memory - This bar graph shows the amount of physical RAM currently in use by the system. It is approximately equivalent to Total RAM minus Available RAM.

§ Physical Memory Usage History - Displays a history of the physical RAM usage, similar to the history of CPU usage above it.

Physical Memory (MB)

This section provides a breakdown of the usage of your physical memory, which is your system RAM, in Megabytes (MB). The components shown are:

- Total - This is the total amount of RAM installed in your system.
- Cached - 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 under the Memory Optimization chapter for details.
- Available - This is the amount of memory available for use by any process if required. It is approximately the sum of Free RAM plus Cached RAM.
- Free - This is the unused portion of RAM; it does not currently contain any useful data.

For more details of physical memory usage in Windows, see this Microsoft Article.

Kernel Memory (MB)

This section provides details on two important resources used by the core of Windows to store various key data. The Nonpaged memory pool stores the portion of this 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; the Paged memory pool stores the portion of the data which can be safely paged out to disk at any time. Importantly, these values are not a measure of the size of the Pagefile - this is shown in the Commit item under the System area, covered below.

For more details of Paged and Nonpaged Pool memory, see this Microsoft Article.

System

This area provides several different pieces of information on various aspects of running processes, as well as system uptime, as covered below:

- Handles - The total number of unique objects in use by all processes, such as files and Registry keys.
- Threads - The total number of threads being run by all active processes on the system.
- Processes - The total number of individual processes running on your system, as individually listed under the Processes tab. This figure is also displayed at the bottom of the Task Manager window.
- Up Time - The length of time since the PC was last started, in days:hours:minutes:seconds format.
- Commit (GB) - This is displayed in the form 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 will 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.

For more details of processes and threads, see this Microsoft Article; for more details of handles, see this Microsoft Article; and for more details of committed memory, see this Microsoft Article.

NETWORKING

This tab graphs your network adapter's utilization as a proportion of its maximum possible throughput. Under the View>Network Adapter History menu item you can choose to also graph 'Bytes Sent' and 'Bytes Received', along with or instead of the default, which is a combination of both. If you click the 'Select Columns' item under the View menu, you can also add various data columns to the table underneath the graph, allowing you to see precise statistics on various communication parameters. This can help you track the type and amount of Internet communication a particular application is undertaking at any time for example.

USERS

Displays all users who can access the system in the current session. It allows you to view a range of details, as well as logoff or disconnect any user if required.

GENERAL USAGE

The most common use for Task Manager is to allow you to close a problematic program/process which is otherwise unresponsive, or has apparently frozen the system in some way. Whenever a program stops responding, Windows should automatically prompt you to close the non-responsive program. However 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 responsiveness to the system and allow you to open Task Manager, and either under the Applications tab or under the Processes tab, select the relevant program and choose 'End Task' or 'End Process' as applicable. Windows 7 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 your PC to shutdown by holding down the power button 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 under the Processes tab make sure to click the 'Show processes from all users' button, then click the CPU column header such that the highest numbers are shown at the top. When your system is relatively idle, the largest proportion of CPU usage should go to the 'System Idle Process', typically around 95-99% of CPU usage. The System Idle Process is not actually using that much in CPU resources, it is forcing all available cores of the CPU into power saving mode. So this is normal and desirable, not something to worry about. At other times while your system is idle, there may be periods when the Windows Disk Defragmenter or Search Indexer are running, and thus will show up as using resources. However no background Windows task will use large amounts of CPU resources if Windows detects that you are trying to undertake another task which requires those resources.

In some cases a program can become caught in a loop or have some other kind of error which causes it to use up all available CPU resources for no apparent reason, or out of all proportion to the task it is undertaking. You can manually end the process, restart the program and see if it happens again - if so then the program bears further investigation.

Yet another common use for Task Manager is to detect background processes or services which a recently installed program may be running without your knowledge. An examination of all running processes may mean that you spot a new process, which you can either right-click and select 'Open File Location' to see where it resides on your system, and/or right-click and select 'Search Online' to find out more about. Similarly, any new services bear investigation, by right-clicking on them and selecting 'Go to Process'. This is also a very useful way of detecting potential malware on your system, as most malware can't hide from the list of running processes in Task Manager. Once you have found an unnecessary new process or service, you can remove it as covered in the Startup Programs, Services or PC Security chapters as relevant.

If you can't easily resolve a process-related issue, then you can create a special file which 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 this file and 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 set the priority and affinity for each process. These functions and related Windows settings require more detailed explanation.

Set Priority: Right-click on a process under the Processes 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 7 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 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 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, and click the Settings button under the Performance section of the Advanced tab. In the window which 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 which makes a particular thread or process run on a particular core of a multi-core CPU. This can result in improved performance, but has to be weighed against the fact that it can also work to reduce load balancing across all cores of a CPU. You can manually alter the affinity for a particular process by right-clicking on it under the Processes 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 would be for troubleshooting purposes, such as in the case of an old program not designed for multi-core CPUs which is displaying odd behavior. 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 alter affinity on a Windows system file in this manner.

As you can see, the 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 which 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.

For example, 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 the actual Commit Limit and Peak Commit Charge - both critical for determining the correct Pagefile size as covered in the Windows Memory Management section of the Memory Optimization chapter. Importantly, you can also see actual Pagefile and drive 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 useful tool to have on your system, though it is targeted towards intermediate to advanced users.

< WINDOWS MEMORY DIAGNOSTIC

Windows Memory Diagnostic is a built-in troubleshooting utility that is usually triggered when Windows detects that a problem may be caused by your physical memory (system RAM or CPU caches). To operate it needs to run at startup because that is the optimal time when RAM is free of any operating system or other software components residing in it. 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 going to Start>Search Box, typing *memory* and pressing Enter.

The tool must be run at the next reboot, but 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 and/or you suspect memory problems it is strongly recommended that you run the test as soon as possible to prevent any further data corruption or loss due to faulty or unstable memory.

Windows Memory Diagnostic conducts a series of tests to determine whether your memory subset is faulty. Advanced users can choose which tests it run 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 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, however if your memory subset is clear of problems then no issues should occur. 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 reducing the RAM latencies too much. See the Overclocking chapter.

§ Rerun the tests with only one stick of RAM. 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 BIOS & 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. However keep in mind that if the tool does detect a problem it is very likely that your RAM is physically faulty or mis-configured in your BIOS, and if ignored will lead to further problems and potentially serious data corruption or 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 which cannot easily be resolved. Some problems are caused by faulty hardware or adverse conditions (e.g. overheating), or by incompatible software or problematic drivers, and these are virtually impossible for Windows to self-diagnose. However you can investigate these issues further yourself to work out what the problem may be related to.

For most major errors you will receive a Blue Screen of Death (BSOD) error, often listing an error message and an error code. By default Windows is set to automatically reboot when it experiences a serious error, so you will have to open Windows Control Panel, select the System component and click the 'Advanced System Settings' link in the left pane, or go to Start>Search Box, type *systempropertiesadvanced* 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 show details of the error, and I recommend you make a note of the exact error message and any error number(s) provided.

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 exit 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 resolve any type of Windows error, search through the following official Microsoft resources:

Microsoft Fix It Solution Center
Microsoft Knowledgebase
Microsoft TechNet
Windows 7 Solution Center
Microsoft Events & Errors Message Center

If nothing is found in the resources above, search Google 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 which 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 which 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.

3DMark 11 is the latest version of this benchmark, and is designed for use only on Windows Vista and 7 and only on DirectX 11-capable graphics hardware. To run the free Basic Edition of 3DMark 11, you need to click the 'Upgrade Later' button after launching the program, and you will then be restricted to a single resolution (1280x720) throughout the benchmark. Click the 'Run 3DMark 11' button to commence the tests. At the end of the run the benchmark will present a final score. You can use this score to compare with other people who have run the benchmark at the same settings and this will tell you whether your system is relatively faster or slower, and if compared with others who have very similar system specifications, it will also tell you whether you have room to improve on your particular system. Note that some systems which 3DMark considers 'similar' to your system may be heavily overclocked just to get a high 3DMark score and are not particularly stable for day-to-day use.

If you don't have a DirectX 11-capable graphics card, you can download earlier versions of 3DMark from here. Although these won't necessarily stress your system the way 3DMark 11 does, and hence are not indicative of how well your system can run modern games, they still provide you with a score that can be used for comparative purposes. Scores are not comparable between different versions of 3DMark.

UNIGINE HEAVEN

Heaven is a free DirectX 11 benchmark which also supports DirectX 9, DirectX 10 and OpenGL graphics functionality. To run the benchmark, launch Heaven and adjust the settings as desired, then click the Run button. The Heaven demo will begin, but 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 the same settings as you to gauge your relative performance. Note there are also Tropics and Sanctuary benchmarks available from the link above, which both support DirectX 10 and DirectX 9 as well as OpenGL.

RTHDRIBL

RTHDribl (Real Time High Dynamic Range Image-Based Lighting) is an older DirectX 9 tech demo and not specifically designed as a benchmark or stress tester. It does not have a series of tests to run, so simply start up the program and observe your framerates in the top left corner. You can turn off the text shown on the screen at any time by pressing F1 and F3. You can also cycle through a range of object shown (Press O), the materials used on their surfaces (Press M), and the backgrounds used (Press L). You can change the display resolution or increase the size of the program's window, either of which will increase the load on your graphics card.

To use it as a stress tester, go to the File menu and select 'Config Display'. In the Direct3D Settings window which opens, select the 'Fullscreen' option, then select the highest available resolution. You don't need to alter any of the other options on this screen unless you know what you're doing. Click OK and the changes will be implemented. Now start the Auto Demo mode by pressing F5, or select 'Enter Planet Demo' under the Demo menu, and let the program run for a while. Any graphics instabilities on your system will soon become apparent through crashes, artifacts or glitches. You can put further stress on the graphics card by changing the Multisample setting under the Options menu to progressively higher values.

LIGHTSMARK

Many graphical benchmarking utilities are based on Direct3D, because this is the most common API used for developing games for Windows. However Lightsmark is an advanced OpenGL-based utility which is free and easy to use. Simply launch the program, select your screen resolution and then click the 'Start Benchmark' button to begin an automated benchmark sequence. At the end of the run you will be given an average framerate for the run which you can compare to other machines running Lightsmark at the same resolution.

FURMARK

FurMark is an intensive OpenGL-based benchmark which also doubles as a stress tester. Installing and running the program results in a run through a series of tests, with results provided at the end. You can upload and compare these results online 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 and/or is overclocked too far.

GAME BENCHMARKS

The graphical benchmarks above are very useful, however they are all entirely synthetic. The most realistic form of graphical benchmarking and stress testing is through the use of the benchmarking features in recent games. Modern PC games are the most 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 which starts and stops 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, play it continuously for a sustained period of time at very high settings, such as two or three hours. 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 systems, not the game.

PCMARK

PCMark is a general benchmarking utility from the makers of 3DMark. It runs a series of tests based on such things 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.

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 benchmarks for our purposes.

Click the Benchmarks tab and you will see modules such as Processor Arithmetic, Physical Disks and Cache and Memory. 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 at the top of the module. You might want to record the score(s) somewhere. 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 drop down boxes.

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 them once, if you want to stress test a component simply refresh the benchmark repeatedly (by pressing F5) whenever it completes each run. Alternatively, if you want to automate the process, Sandra has a Burn-in Computer 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 which 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 your 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 which only 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 real-world applications and games running without problems indicate 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. 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 which has been covered in various chapters of this book, including 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.

MEMTEST

MemTest is a Windows-based memory test which will help in stress testing your Windows memory configuration and RAM to detect any potential problems. To use MemTest simply launch the program, and I recommend manually entering the amount of RAM you wish to test - for example, enter 512 to test 512MB of RAM, 1024 for 1GB of RAM, or 2048 to test 2GB of RAM. You may need to run multiple instances of MemTest to use up all 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 or more. If running the test triggers any errors, Windows-related warnings or prompts, then you have potentially faulty RAM and/or mis-configured BIOS or Windows settings, which can lead to many types of system problems. To test only your physical RAM, run the Windows Memory Diagnostic as covered earlier in this chapter, or MemTest86+ below.

MEMTEST86+

Memtest86+ is similar to the Windows Memory Diagnostic tool in that it tests your memory before Windows loads into memory. This is a much more accurate way to test your physical RAM and memory subset free of any memory spaces taken up by the operating system. The version of Memtest86+ you download is based on which device you wish to use at bootup, whether CD, Floppy or USB flash drive. Once booted on this device, your system will launch Memtest86+ and test your RAM. Any errors indicate BIOS or physical RAM problems.

That covers the main performance measurement and troubleshooting tools you can use to solve problems and optimize your system. There are many other programs which can be used for this purpose, but the ones in this chapter should be the most reliable and the easiest to use under Windows 7. Importantly, despite promises you may read to the contrary, there are no tools which 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 tool actually exists. The causes of PC problems are often very complex and inter-related, and can be a combination of hardware problems along with incorrect settings and/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 your PC 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 understand how your system works combined with research and thought. If there really was an easier way or automated utility to resolve problems, everyone would be using it by now, and similarly Microsoft would have purchased the rights to it and incorporated it into Windows 7, rather than providing so many different diagnostic and performance measurement tools.

CLEANING WINDOWS

As you use your system in day-to-day activities, a range of unnecessary temporary, backup and log files can build up 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 aren't, 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 permanently deleting desirable files on your system. It exists as a hidden folder called *\$Recycle.bin* on every drive of your system. Any file or folder you highlight and press the Delete key, or right-click and select Delete, will be moved to the Recycle Bin 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 removed from view, and the area it resides in on the drive is simply marked as available space, but you can still recover these deleted files in some cases - see the Data Recovery section of the Backup & Recovery chapter for relevant methods.

To access the Recycle Bin configuration options, right-click on the Recycle Bin icon on your Windows 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 allocated to 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 chosen to be deleted will bypass the Recycle Bin and be deleted permanently. I strongly recommend against ticking this option, as the Recycle Bin gives an added level of protection against accidental deletion of important files. 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 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 as it can quickly become an unnecessary annoyance.

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 in the left pane. 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) and/or Recycle Bin (empty) icons here, click the 'Change icon' box, 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 Menu. 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 Windows 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, so you may prefer to pin it to your Start Menu if you wish to retain that aspect of its functionality.

< DISK CLEANUP

The built-in Disk Cleanup utility provides the ability to automatically find and safely remove a range of unnecessary files. To access the Disk Cleanup utility, open Windows Explorer, right-click on the drive you wish to clean, select Properties and under the General tab click the 'Disk Cleanup' button. Alternatively go to Start>Search Box, type *cleanup,* press Enter and select the drive to clean. To access all the cleaning options click the 'Clean up system files' button, and if prompted reselect the drive you want to clean.

There are two main tabs in the Disk Cleanup window, though the 'More Options' tab is only visible if you have clicked the 'Clean up system files' button:

Disk Cleanup: There are a range of components you can choose to clean out. Highlight each one and a description will appear in the box below. All of these categories are safe to remove, as none are necessary for Windows to function correctly. If in doubt, highlight a category and click the 'View files' button if available to see precisely which files and folders will be deleted. Note that categories are only shown if there are relevant files to be cleaned out, so the same categories may not be displayed each time you run this utility.

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, 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 Windows Explorer. Deleting these files means they will have to be recreated the next time you view such folders, which can slow down browsing. See the Basic Features section of the Windows 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 problem reports to Microsoft for which you want a solution.

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 under 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, also removing any older Shadow Copies as part of this process. These features are covered in more detail under the System Protection section of the Backup & Recovery chapter. If your system is performing without any problems and you don't believe you will need to restore any Previous Versions of a file then it is usually fine to click this option, as older Restore Points and Previous Versions can often take up a substantial amount of disk space.

ADVANCED DISK CLEANUP

There is a more advanced form of the Disk Cleanup utility which 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 at the Start>Search Box:

```
Cleanmgr /sageset:1
```

The number after the `/sageset` switch can be anything from 0 to 65535, it is simply the specific place in the Registry that your options will be saved. You cannot specify a particular drive to clean files for using this method, as this applies to all drives and partitions, so use 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 possible categories here. All categories have descriptions provided when highlighted, but it is important to note in particular the following:

§ Previous Windows installation(s) - If Windows 7 found any files or folders which were not compatible when doing an in-place upgrade install over a previous version of Windows, it will store them in a series of folders called *Windows.old*. You can view their contents in Windows Explorer to see if there's anything you want to keep, otherwise they are best deleted.

§ Setup Log Files - Ticking this option removes any log files created during Windows Setup. These are not normally needed, and best removed if your system is not showing any problems.

§ Temporary Windows installation files - Ticking this option removes a range of temporary installation files created during Windows installation. These files can be removed without any problems.

§ Files discarded by Windows Upgrade - During an Upgrade Install of Windows 7, any non-system files which Windows cannot move across are backed up just in case. If none of your personal files are missing after an in-place upgrade install, you can tick this option to remove these files.

§ Windows upgrade log files - Log files created during installation of Windows which can be used for troubleshooting purposes. If your installation process was trouble-free, these can safely be deleted.

Once you have selected the relevant options, click OK. However nothing will be deleted yet - your settings have been saved. You can now run advanced Disk Cleanup with these saved settings at any time by typing the following in a Command Prompt or in Start>Search Box:

```
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 Cleanup method further above is safer and more configurable, making sure it doesn't have inadvertent impacts on other users and/or other drives on your system.

< SERVICE PACK CLEANUP

If you have installed Service Pack 1 on an existing installation of Windows 7, it will create a range of backup files which allow you to uninstall the service pack if necessary. However for all intents and purposes, once you've installed SP1 there should never be any need to uninstall it again, so to delete the unnecessary backup files and redundant versions of system files and reclaim some disk space, you can use one or both of the following methods:

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

```
dism /online /cleanup-image /spsuperseded
```

This will tell the Deployment Image Servicing and Management (DISM) utility to begin removing all files which have been superseded as a result of newer versions being installed via SP1. The process can take a while, but a progress indicator is provided.

Alternatively, open the Disk Cleanup utility as covered earlier in this chapter, click the 'Clean up system files' button, then scroll down to the newly available 'Service Pack Backup Files' item which now appears in the files to delete box, tick it and click OK.

Once the cleanup process is complete, you will no longer be able to uninstall SP1, but as noted this is something that is not recommended anyway. If you are having major issues with your system after installing Service Pack 1 then it is strongly recommended that you reinstall Windows 7 and then apply SP1 immediately after a fresh installation.

< CCLEANER

CCleaner is a free utility which can find and remove a wide variety of potentially useless files on your system. CCleaner automates a task that you can perform manually to some extent, but which is more complicated and takes longer to do by hand. If used with caution it is usually 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 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.
3. Under the Include and Exclude sections you can manually add particular files or folders which you would specifically like CCleaner to scan for deletion (or exclude from deletion). This is only recommended if you know for certain that the contents of these files or folders are safe to delete.
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 which are required for the current session.

To start the cleaning process, first make sure you close all open applications to prevent 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 all 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.

§ Windows Explorer - All options can be ticked, however I recommend unticking 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. I also recommend unticking the 'Taskbar Jump Lists' functions unless you don't use the Recent functionality of Jump Lists. See the Taskbar section of the Graphics & Sound chapter for details.

§ System - All options can be ticked, but bear in mind 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, clearing '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. For security purposes you can tick the 'Wipe Free Space' option, but I recommend against this, as it prevents you from recovering any accidentally deleted files and also makes cleaning very lengthy.

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 - deletion of application-specific files can result in the loss certain custom preferences for example. Also be aware that CCleaner may automatically add and enable new options here when you install new applications, so check under this tab regularly.

Once you have ticked all the relevant options, click the Analyze button and after a while CCleaner will come up with a list of files it wants to delete. However the results are shown in summary form, which can make it difficult to determine what will be deleted. Right-click in the analysis window and select 'View detailed results' to see precisely which files are going to be deleted, and scroll through the list to make sure no desirable files are here. If in doubt, go back and untick any options, then click the Analyze button again.

When you are satisfied that the files to be deleted are truly unnecessary, click the 'Run Cleaner' button and the files will all be permanently deleted.

There are two more useful functions of CCleaner covered in this book:

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.

CCleaner is a useful tool in removing a range of unnecessary files, but caution is required, as Windows 7 is already quite good at maintaining itself and thus does not 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 with CCleaner is actually slowing down normal

Windows and 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 in your system. If you don't trust an automated cleaner, or just want to be certain of what it is you are deleting, read the following. However this method is not recommended for beginners as it requires a reasonable level of knowledge and personal judgment in determining which files to delete and which to keep.

Before manually cleaning out any files, first close all open applications and games as some of these may have created temporary files that cannot be deleted because they are in use, and would be pointless to delete. Then restart your system just to be certain, as Windows will remove many unnecessary temporary files upon shutdown. Now make sure that the option to move files to the Recycle Bin is enabled. This will provide protection against accidentally deleting a necessary file.

To begin with, it is safe to delete any files or folders beneath 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) - for 64-bit users
\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 which has created the software rather than the software itself - a quick check on Google should help you determine which programs the folders relate to if in doubt. Certain programs may have files which are 'in use' and can't be deleted - see the section 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. Press WINDOWS+F to open the advanced Windows Search functionality, then type the following in the Search Box and click the Computer option at the bottom to conduct a full search for these file types:

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.

I do not recommend simply deleting all the results you discover for each of the 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 which you know no longer exist on your system.

As noted in the CCleaner section, do not regularly clean out the contents of Windows directories such as *\Windows\Prefetch*. These directories are self-maintaining and there is greater potential for reducing performance or harming functionality in removing these files.

The key thing to understand is that, aside from deleting certain Windows or program files or folders for troubleshooting purposes - such as deleting the Icon Cache as covered under the Icons section of the Graphics & Sound chapter - there are no performance or functionality benefits to be had by deleting unnecessary files. This is only done primarily to reduce clutter and free up disk space. Given most of these potentially unnecessary files are very small, and often hidden from view, there is no need to risk a loss in functionality or performance by deleting lots of 'unnecessary' files as some sort of optimization procedure.

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 reasons for this:

The most obvious reason is that the file is actually in use by an installed program. Close all open programs, reboot and try again. If the problem persists, then it is likely a background program or driver that 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 prevent a particular file from being loaded into memory by temporarily disabling the related program with a utility like MSConfig or Autoruns, then rebooting and try 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 PC Security chapter.

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 it is primarily malware-related files which 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, then click the 'Unlock All' button to unlock the file. Alternatively choose from the list of actions at the bottom left of the box shown, and reboot if necessary for the action to complete.

After deleting all 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 the files you have deleted are genuinely no longer needed. In general the Disk Cleanup 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 which does not correctly remove all portions of itself from your system. In any case, cleaning Windows 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 7 has improved its self-maintenance procedures, and by default schedules a range of important tasks to run on a weekly basis, such as defragmenting the system and scanning it for malware, this is not a replacement for proper system 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 depending on how you are using your PC.

For the reasons above, I can't provide an all-encompassing maintenance schedule which everyone should follow. This entire book contains a wealth of information and recommendations designed to help you understand how best to maintain your PC. By having appropriate knowledge of the various features in Windows, you will come to know how to configure Windows 7's automated maintenance tools, and when to manually intervene as necessary. For the purposes of providing some basic guidelines however, I provide 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 - for example, the Defragment step doesn't apply to people using SSDs, as explained under the Drive Optimization chapter.

STEP 1 - MAINTAIN SECURITY

Action: Run Windows Update, then update malware scanners and run a full manual scan of all drives.
Frequency: Once a week at least, and also scan individual downloaded files before use with MSE.

See the PC Security chapter for details.

STEP 2 - CHECK STARTUP PROGRAMS & SERVICES

Action: Use MSConfig to quickly check under the Startup and Services tabs for any newly installed startup programs or non-Microsoft services. Identify any new or unfamiliar entries and disable unnecessary ones as required, first by checking the program's own options, then using Registry Editor or Autoruns as necessary.
Frequency: After every new program or game 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 the automated Backup utility to create/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 at least.

See the Backup & Recovery chapter.

STEP 4 - CLEAN WINDOWS

Action: Run the Disk Cleanup utility, then CCleaner. Do a manual clean out of remaining unnecessary files.
Frequency: Once a week at least, and also after major updates, program installs and uninstalls.

See the Cleaning Windows chapter for details.

STEP 5 - CHECK DISK

Action: Use the Check Disk utility to do a full disk scan and automatic repair of the primary system drive.
Frequency: Once every month at least.

See the Drive Optimization chapter for details.

STEP 6 - DEFRAGMENT

Action: Use the Windows Disk Defragmenter to run a full defragmentation of the drive.
Frequency: Once a week at least. Also after every major program or game install/uninstall, or any manual game or Windows patching, such as after Windows Update or driver installations.

See the Drive Optimization chapter for details.

Some of 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 ensuring that your data remains secure, your system remains as responsive as when you first installed Windows 7, and you don't keep running into 'mysterious' crashes and problems. Of course proper system knowledge and prevention are also two key aspects of system maintenance.

SCHEDULED MAINTENANCE

Windows 7's Task Scheduler allows you to create and customize a range of automated tasks for maintaining your PC. For example, if you leave your machine on overnight, you can schedule certain utilities to run at that time, especially for lengthier tasks such as full manual malware scans or disk defragmenting. Even without appropriate scheduling options in a program, you can use Task Scheduler to launch tasks at particular times in case you forget to do so manually. 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, piracy tools and pirated software, constant upgrades and downgrades of leaked drivers, etc. are one of the major reasons why many systems are so unstable and insecure, beyond Windows 7's capabilities of managing 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 you will find that it remains stable and performs well for a very long time.

CONCLUSION

That brings *The TweakGuides Tweaking Companion for Windows 7* 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	27 November 2009	Nil - First Release.
1.1	23 June 2010	This is a relatively minor revision in terms of actual information changed or added. However a thorough edit of the book was undertaken to find and correct a large number of typographical, grammatical and descriptive errors. All pages - Fixed any dead or inaccurate hyperlinks. All pages - Fixed any typographical/grammatical errors. pp.60 - Added UEFI details. pp.97 - VistaBootPro utility renamed to DualBootPro. pp.115 - Instructions for 'Show preview handlers in preview pane' option fixed. pp.129 - God Mode tip added. pp.137 - Intel Matrix Storage Manager renamed to Intel Rapid Storage Technology driver. pp.224 - Corrected Master File Table description. pp.235 - Added Mouse Acceleration Fix utility. pp.242 - Corrected Tablet PC Optional Components description. pp.299 - Corrected Increase Maximum Simultaneous Connections tip. pp.300-301 - Added IE7Pro utility instructions. pp.324 - Added Avidemux, VirtualDub, tsMuxer and Avi2DVD utilities. pp.357 - Added Classic Shell utility. pp.358 - Added Network Activity Indicator utility. pp.362 - Added Sticky Notes section. pp.369-370 - Fixed 'Custom Shutdown, Restart, Sleep or Lock Icons' instructions. pp.375-379 - Revised and updated the Gaming section. pp.389 - Added WEI Share link in place of Share Your Score. pp.417 - Added Unlocker utility.
1.2	23 February 2011	All pages - Fixed any dead or inaccurate hyperlinks. All pages - Fixed any typographical/grammatical errors. pp.32 - Removed 3DMark System Information utility. pp.33,416 - Clarified HD Tune's SSD support. pp.52 - Added DBAN utility. pp.73 - Added Device Stage Visual Editor Tool. pp.78,80 - Replaced vLite with RT Se7en Lite utility. pp.97-98 - Updated EasyBCD instructions. pp.127 - Added Edit 'New' Context Menu tip. pp.134-135 -Updated Service Packs section for SP1. pp.144 - Updated Driver Sweeper instructions. pp.188-191 - Revised Microsoft Security Essentials instructions for MSE 2.0. pp.191-192 - Replaced A-Squared Free with Emsisoft Anti-Malware instructions. pp.215 - Added Secure Erase Guide link. pp.287-305 - Revised Internet Explorer chapter for IE9. pp.306-320 - Revised Windows Live Mail chapter for the new version of WLM. pp.336 - Added details of Blu-ray playback on Windows 7. pp.368 - Added Windows Photo Gallery Plugins link. pp.370 - Added gdipp link. pp.383 - Added Steam Assistance Project instructions. pp.413 - Updated 3DMark instructions for 3DMark 11. pp.420 - Added Service Pack Cleanup section.

1.3	5 January 2012	This is a very minor revision in terms of actual information changed. The most significant change comes in the form of updating a large number of hyperlinks throughout the book. All pages - Fixed any dead or inaccurate hyperlinks. All pages - Fixed any typographical/grammatical errors. pp.65 - Clarified AMD CPU compatibility for Real Temp & Core Temp. pp.97 - Updated EasyBCD download instructions. pp.205 - Strengthened warning against disabling Rdyboost.sys driver. pp.365-366 - Added notice of Windows Gadget Gallery being shut down. Gadget links now point to a third party site, not Microsoft, and hence suitable precautions must be taken.