Covers Windows 10, 8.1, and 7

THE EXPERT'S VOICE® IN MICROSOFT WINDOWS

WINDOWS TROUBLESHOOTING SERIES

Windows Software Compatibility and Hardware Troubleshooting

MAINTAIN OPTIMAL COMPATIBILITY WITH THE OLDER SOFTWARE AND DEVICES THAT YOU NEED TO USE

Mike Halsey, MVP and Andrew Bettany, MVP

Apress®

Windows Troubleshooting Series

Mike Halsey, MVP
Series Editor

Apress®

Windows Software Compatibility and Hardware Troubleshooting

Mike Halsey, MVP

Andrew Bettany, MVP

Apress®

Windows Software Compatibility and Hardware Troubleshooting

Mike Halsey
Microsoft MVP
Sheffield, South Yorkshire, UK

Andrew Bettany
Microsoft MVP
York, North Yorkshire, UK

ISBN-13 (pbk): 978-1-4842-1062-8
DOI 10.1007/978-1-4842-1061-1

ISBN-13 (electronic): 978-1-4842-1061-1

Library of Congress Control Number: 2015949392

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director: Welmoed Spahr
Lead Editor: Steve Weiss
Technical Reviewer: Zeshan Sattar

Coordinating Editor: Kevin Walter
Copy Editor: Kim Burton-Weisman
Compositor: SPi Global
Indexer: SPi Global
Artist: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Any source code or other supplementary material referenced by the author in this text is available to readers at http://www.apress.com/9781484210628. For additional information about how to locate and download your book's source code, go to www.apress.com/source-code/. Readers can also access source code at SpringerLink in the Supplementary Material section for each chapter.

It's astonishing to think that this is my eleventh book, and how it's crept up on me. I'd like to take the opportunity to thank the people who helped me right at the beginning, as without your encouragement, guidance, support, and belief, I wouldn't be where I am today.
My heartfelt thanks go to Kenyon Brown, Claudette Moore, Ed Bott, Jon Hassell and Steve Weiss.

—Mike

Thank you, Annette, for your support and love whilst I have been scribbling away.

—Andrew

Contents at a Glance

Contents

About the Authors

Mike Halsey was first awarded a Microsoft Most Valuable Professional (MVP) in 2011. He is the author of more than ten Windows books, including *Troubleshooting Windows 7: Inside Out* (Microsoft Press, 2010), *Troubleshoot and Optimize Windows 8: Inside Out* (Microsoft Press, 2012), *Beginning Windows 10* (Apress, 2015), and *Windows 10 Troubleshooting* (Apress, 2016). He is also the author of other *Windows Troubleshooting* books in this series.

Based in Sheffield, UK, where he lives with his rescue Border Collie, Jed, he gives many talks on Windows subjects, from productivity to security, and makes help, how-to, and troubleshooting videos under the banner PC Support.tv. You can follow him on Facebook and Twitter `@PCSupportTV`.

Andrew Bettany, a Microsoft Most Valuable Professional (MVP) awardee since 2012 (Windows IT Pro) and Microsoft Certified Trainer, is the technical editor of several titles, and the coauthor of *Exam Ref 70-687: Configuring Windows 8* (Microsoft Press, 2013) and Microsoft Official Curriculum courses 20687D, 20688D, and 20689D (2014). He is the author of multiple books in the Apress *Windows Troubleshooting* series.

A regular speaker and attendee at IT professionals' events, TechEd, and Ignite conferences, Andrew also devotes time to building out the Windows User Group, a United Kingdom–wide community, and manages the University of York IT Academy.

He loves to write, travel, and enjoy the countryside and lives on a small holding close to York in North Yorkshire (UK) with his partner Annette and his five-year-old son Tommy.

About the Technical Reviewer

Zeshan Sattar is head of curriculum development at Agilisys Arch, an apprenticeships training provider in the United Kingdom. He is responsible for devising the training and certification curriculum for apprentices between the ages of 16 and 24. The curriculum includes a diverse range of topics from across the infrastructure and development tracks. Zeshan has delivered training to audiences across the world both in person and via online platforms. Zeshan has also worked and spoken at a number of Microsoft events, including Microsoft Ignite and TechEd.

Windows Troubleshooting Series

When something goes wrong with technology, it can seem impossible to diagnose and repair the problem, and harder still to prevent a recurrence. In this series of books, we'll take you inside the workings of your devices and software, and teach you how to find and fix the problems using a simple step-by-step approach that helps you understand the cause, the solution, and the tools required.

Series Editor
Mike Halsey, MVP

As a Microsoft MVP (Most Valuable Professional) awardee since 2011, the author of more than ten books on Microsoft Windows, and a teacher for many years, Mike Halsey understands the need to convey complex subjects in clear and non-intimidating ways.

He believes that the Windows Troubleshooting Series is a great example of how quality help, support, and tutorials can be delivered to individuals of all technical ability. He hopes you enjoy reading this and many other books in this series, both now and for years to come.

Introduction

When anybody moves to a new version of Windows, the first, and by far the most common question asked is: Will my software and devices work with it? Windows 7, 8.1, and now Windows 10 are all extremely capable when it comes to backward compatibility; however, as operating system features are upgraded, and even completely removed or replaced, and as the hardware driver model improves, it is easy to see why the stuff you need and like to use the most can break.

The good news though is that the range of tools and utilities available to assist with compatibility and to keep you working are both extensive and comprehensive. In this book, we'll guide you through the often complex minefield of managing your legacy, and sometimes even brand-new software and hardware, and show you how to maintain optimal compatibility when you need it the most.

CHAPTER 1

All About Compatibility

Microsoft Windows is the most compatible operating system on the planet, even though it may not always appear that way when you try to get something working that used to work fine.

There are multiple compatibility issues with some older software and hardware on Windows 7, Windows 8.1, and Windows 10, but the fact that you can still install a program written for DOS, or a dot-matrix printer with a parallel connection are testaments to the efforts Microsoft has made over the years to help users keep working with the software and hardware they rely on day to day.

Be it a payroll system, a custom-made web browser plug-in, or an aging piece of hardware, Windows is pretty good at keeping everything working; but not everything will work without problems, and some things refuse to work at all.

These compatibility problems are often blamed directly on Windows, but the truth is that many other factors can come into play to prevent software or hardware from functioning correctly, or even at all. In this chapter we'll look at what those factors are and examine how you can mitigate them.

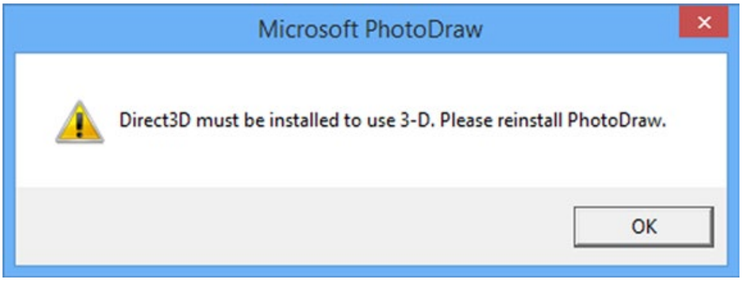
The Common Causes of Compatibility Problems

The most common perception of when compatibility problems will occur is because something is old, but this very often isn't the case, and in fact some of the oldest software and hardware you can use will be the most reliable.

The reason this happens is because back in the days of early DOS and Windows PCs there were fewer configuration options and external features available for software and hardware to use. It was only when later versions of Windows appeared—and started using features such as Direct3D—that compatibility issues began to appear.

As an example, I use on an almost daily basis, a venerable, very easy to use, and powerful graphics package from Microsoft called PhotoDraw 2000 version 2 (I'll leave you to guess when it was released). This package still works fine on my Windows 10 PCs—with only one issue: an inability to use its in-built 3D support on images and objects (see Figure 1-1).

M. Halsey and A. Bettany, *Windows Software Compatibility and Hardware Troubleshooting*,
DOI 10.1007/978-1-4842-1061-1_1



Direct3D must be installed to use 3-D. Please reinstall PhotoDraw.

Figure 1-1. *Some software packages can flag compatibility issues with features that have been removed from newer Windows versions*

This isn't an issue for me, so I continue to use the software; that is at least until I can find the time to learn how to properly use Photoshop.

If I were to run a DOS program, such as the much-loved WordPerfect 5.1 in Windows, then I would very likely have trouble printing from the software, as DOS didn't come with native printer support and each software package had to provide its own print engine and drivers, but every other feature would work fine. Of course, I could use virtualization software and run the program in DOS, but I would still struggle to print.

It's a similar story with hardware: many IT pros and engineers jealously guard and take good care of laptops that have serial ports, as some engineering, medical, and other industrial equipment still use the standard. And companies that require the use of aging parallel printers, for purposes such as payroll, can find that setup and configuration of these devices is no harder than it was back in the days of DOS. I have come across many businesses that happily operate PCs that are over 20 years old that are dedicated to performing a specific task or role.

So if it's not the age of software and hardware that causes configuration problems, it can't all come down to features that have changed within Microsoft Windows over the years… So what causes problems?

It's certainly true that as Microsoft updates and upgrades features in Windows, such as improving the graphics features or updating the hardware driver model, issues can occur, especially if the software or hardware you use isn't updated to reflect those changes.

The period of Windows development from 2000 through to when Windows Vista was released in 2007 was built on the NT kernel, which provided a solid base for original equipment manufacturers (OEMs) and developers to build software, hardware, and drivers. The introduction of User Account Control (UAC) in Windows Vista threw out the NT kernel and redesigned the security model, effectively breaking a great many software packages, especially expensive custom software written for business and industry. This is because when that software was written, administrative privilege workarounds (and cheats) were commonly employed to achieve tasks. This wasn't actually necessary most of the time, and is now generally considered to have been caused by nothing more than sloppy coding.

Table 1-1. *Windows Versions by Release Date with Kernel Version Number*

Name	Version	Released
Windows 1.01	1.01	1985
Windows 1.03	1.03	1986
Windows 1.04	1.04	1987
Windows 2.1	2.1	1988
Windows 2.11	2.11	1989
Windows 3.0	3.0	1990
Windows 3.1	3.1	1992
Windows NT 3.1	NT 3.1	1993
Windows for Workgroups 3.11	3.11	1993
Windows 3.2	3.2	1993
Windows NT 3.5	NT 3.5	1994
Windows NT 3.51	NT 3.51	1995
Windows 95	4.0	1995
Windows NT 4.0	NT 4.0	1996
Windows 98	4.1	1998
Windows 2000	NT 5.0	2000
Windows ME	4.9	2000
Windows XP	NT 5.1	2001
Windows XP Professional x64	NT 5.2	2005
Windows Vista	NT 6.0	2007
Windows 7	NT 6.1	2009
Windows 8	NT 6.2	2012
Windows RT	NT 6.2	2012
Windows 8.1	NT 6.3	2013
Windows RT 8.1	NT 6.3	2013
Windows 10	NT 10.0	2015

It’s true that software and hardware doesn’t need to be old to have compatibility problems, although obviously fewer new applications and devices will be affected. Long gone are the days when OEMs released hardware that would stay on sale for many years, such as printers and scanners. The trend these days has moved firmly to short lifecycles for products, with several major-brand companies refusing to provide drivers for hardware more than a couple of years old once a new version of Windows appears.

This problem is compounded by the fact that, although the hardware driver model is identical in Windows Vista, Windows 7, Windows 8.1, and Windows 10 (bar a few minor updates and security features that have taken place over the years), Windows version authentication is built into many driver installers, so if you were to try and install an older printer that was bought at the same time as a PC running Windows Vista, the installer might say that there is a version mismatch, and the copy of Windows you are using isn't supported, when in fact there should be nothing or little to prevent you from successfully installing the driver.

Third-party software (i.e., software and apps not written and released as part of Microsoft Windows) can also cause compatibility problems with some software, especially custom-made software in business and industry, calling and requiring additional tools, utilities, and plug-ins that have not been updated to reflect changes in newer versions of the OS.

It's not all bad news, however, as Windows includes tools for managing compatibility of both software and hardware, and Microsoft has several enterprise-ready utilities to download that can provide even more help and support. We'll examine all of these throughout this book.

Internal and External Compatibility Factors

So far we've covered, very broadly, the common causes of software and hardware compatibility problems in Windows, but other factors can play a part too, both inside your PC and with external hardware and services that you'll use day to day.

Some of these issues are ones that you may not face currently, but are likely to face in a few short years (and certainly within the lifetime of this book).

Networking Factors

Networking is one area where changes in technology will likely affect older hardware and software, if it isn't happening already.

The speed of the network connection has exponentially grown over the last 10 years. While this sounds beneficial to consumers wishing to download the latest episode of their favorite flashy TV series or to view the latest animated web page, legacy hardware sometimes cannot cope with the gigabit connections that they now encounter. Firmware upgrades to routers and switches may hold off the need to replace the device, but if an organization has legacy hardware providing the business networking backbone, then this should be evaluated for replacement as a matter of urgency.

IPv6 (Internet Protocol version 6) was introduced in recent years as a solution to the problems the aging IPv4 networking protocol was presenting. IPv4 was a 32-bit addressing system that provided a maximum of 4.3 billion addresses, (4.3×10^9). This might seem like plenty, and it's commonly used for the private address space in company networks, but the size and growth of the Internet meant that by 2012, the world had simply run out of address space for every server, computer, and Internet of Things (IoT) device we had attached to it.

IPv6 provides a 128-bit address space, raising the number of connected devices permitted to 340 undecillion, or 3.4×10^{38}. Perhaps, though, one day even this won't be enough as we add our cars, refrigerators, power outlets, and bathroom mirrors to the Internet.

You may find, for example, that you're using network or Internet-connected hardware that simply doesn't support the IPv6 standard, and as your company network and your Internet Service Provider (ISP) moves everything over to IPv6, connection failures might occur without address translation and virtualization services running on your server or in the hardware in your router.

PC Hardware

While problems caused by a lack of available IPv4 addresses are already affecting some of the largest businesses with many PCs, some of the PC hardware you use can also cause problems and issues with software and hardware compatibility.

Processors are a common cause of compatibility problems. You might find, for example, that you need to work on exceptionally large databases or spreadsheets that require the latest 64-bit version of Microsoft Office, but that your PC only contains a 32-bit processor and very possibly not enough memory for the task. Then you would need to obtain a 64-bit copy of Windows, possibly adding to the costs involved.

Alternatively, you might find that you can't even install the latest version of Microsoft Windows because your processor doesn't support features required by the OS, such Physical Address Extension (PAE), No-eXecute (NX), and Streaming Single Instruction, Multiple Data Extensions 2 (SSE2).

You may need to use virtualization software (such as Microsoft's Hyper-V or VMWare vSphere) in your business to consolidate servers, reduce costs, or increase redundancy. You have a 64-bit processor, but you still might not be able to use the software you need unless the processor itself natively supports virtualization.

If you use serial or parallel devices on a PC that comes with just USB support, you will need a dongle adapter. Many of these adapters are cheaply made in the Far East, and finding reliable and up-to-date drivers can often prove to be impossible.

Security Factors

I've already mentioned Microsoft's User Account Control (UAC) security system, which was first introduced on Windows Vista. It can cause problems for software that was coded in a way as to require administrative privileges to perform common and basic tasks.

One of the most common compatibility problems business will encounter is the use of older intranet sites and web browser plug-ins. We'll look at these in detail in Chapter 2, but the problems are caused by two factors.

The first factor is Microsoft's decision during the early years' development of their Internet Explorer (IE) browser to try and define Internet standards rather than follow them. By the time IE had muscled Netscape Navigator out of the way, IE was the dominant web browser worldwide, with some 99% overall usage share.

In the years before Mozilla Firefox and Google's Chrome browsers finally appeared, businesses had little choice but to code their intranet sites and plug-ins to work with IE. Eventually, Microsoft did see the light, and modern versions of Internet Explorer are fully compliant with the web standards used by the other main browsers.

Microsoft's move to a more standards-compliant platform is in itself enough to break compatibility with many intranet sites and plug-ins, and businesses have in many cases stuck with earlier versions of IE that run on earlier versions of Windows, such as XP, to get around the problem.

The simple fact remains, however, that without features like UAC, and with both IE6 and Windows XP being out of extended support, both pose enormous security risks for any business, and so businesses have little choice but to upgrade and find compatibility solutions in order to use their legacy hardware and software.

Certified for Windows. What Does the Logo Mean?

One way to ensure compatibility, especially with hardware, is to buy only products that carry a "Certified for Windows" or a "Windows [x] Compatible" sticker and logo. What does this actually mean though?

When you develop an app for the Store in Windows 8.1 or Windows 10, Visual Studio runs a series of stress tests on the app and its code to check for instabilities, crashes, and security flaws. Only if the app passes all of these tests is it permitted to be released into the Windows Store.

It's the same with desktop win32 software and hardware for Windows—Microsoft runs self-certification schemes for new products. You can find information for software at http://pcs.tv/1DWHgs2 and for hardware at http://pcs.tv/1COnQ1E.

These certification schemes, which permit your product to carry a logo such as those seen in Figure 1-2, work in the same way—they test the resilience of software, hardware devices, and their drivers.

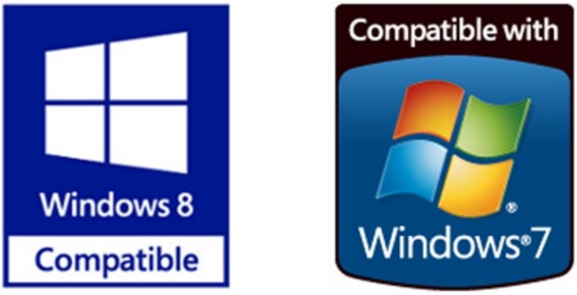


Figure 1-2. *Examples of the certification logos for Windows*

Unlike the Windows app store, however, there is no requirement to pass software and hardware through certification. Indeed, some companies make a conscious decision not to do this because there can be costs involved that they may not be able to easily afford, or because they release so many products that it would be too expensive overall. Customized company software is also unlikely to be certified, given that it's been written for one specific company and for one specific usage scenario.

When you are purchasing software or hardware, however, products that carry the Windows certification logo have been tested for stability, security, reliability, and resilience for one or a range of Windows operating systems, including desktop and server variations.

It's important to stress here that the PC ecosystem, with an almost infinite amount of combinations of installed software and hardware, makes it impossible to determine if or how one piece of hardware or software might interfere with the proper operation of another, although you can be reasonably assured that anything carrying the Windows certification logo will likely be more compatible than something that doesn't.

Summary

The number of factors that can affect software and hardware compatibility in both Microsoft Windows and on our PCs clearly extend far beyond older (legacy) software and parallel printers, and you might be surprised how many of the oldest products will work without any problems or issues at all.

The PC ecosystem, however, does mean that even newer products can face problems, especially if OEMs design them to have a finite lifespan.

In the next chapter, we'll begin by looking at the software that we use, and the compatibility and stability issues that you can face.

CHAPTER 2

Common Software Compatibility Issues

Throughout the technological revolution during the last 30 years, the advances in technology have been often seen as an enabler or catalyst for many beneficiaries, whether they are individuals, businesses, or even society as a whole.

One aspect that we face as technology advances is that change is inevitable and we cannot always preserve backward compatibility. Microsoft has retained this desire at all costs—just look at Internet Explorer (IE); in its latest release, IE tries to maintain automatic compatibility for versions 6 through 11. Imagine if the opposite behavior had occurred; that is, if every time Microsoft released a new, better, faster, or improved version of its bundled browser, every existing web page across the world would need to be rewritten to be viewable within IE. It would be safe to assume that IE would be dropped like a hot stone by users.

Retaining backward compatibility, therefore, is the Holy Grail of software development, and it seems great for everyone. However, in practice it hinders progress, innovation, and agility. We only have to look at the approach that Android and Apple have taken—they consistently upgrade their core operating systems to the latest version at either no or low cost to the user, and this behavior has caused little dissatisfaction among their loyal user bases. As the operating systems upgrade, there is then pressure for app providers to keep in line and upgrade their software to stay “current.”

Unfortunately, the historic and current (for now) method of pricing, licensing, and regular discrete releases that Microsoft has always delivered has created this need for everyone to take a step to change each time Microsoft introduces a new OS.

Backward compatibility has certainly helped Microsoft and other independent software vendors (ISVs) to build loyalty and retain customers who cling to ever-stable versions of the platform.

Over the last couple of decades, though, there have been significant changes that ISVs and giants like Microsoft have implemented, and over time, most businesses and consumers have eventually joined in by adapting to the change.

M. Halsey and A. Bettany, *Windows Software Compatibility and Hardware Troubleshooting*,
DOI 10.1007/978-1-4842-1061-1_2

The following are several significant changes (excluding operating systems) over the past decade:

- Move from Office 97–2003 format (`.doc`, `.xls`, `.ppt`) to Office 2007 and newer format (`.docx`, `.xlsx`, `.pptx`)
- CD/DVD media to ISO downloads
- Executable files to MSIs
- New user privilege model using User Account Control (UAC) introduced with Windows Vista
- Windows Imaging Format (WIM) file-based disk image format used to deploy Windows since Windows Vista
- .NET Framework changes from .NET 1.0 in Windows XP to .NET 4.5 in Windows 8.1
- Automatic Windows updates since Windows 8

In this chapter we discuss how software advancements and innovations can create significant incompatibility issues with previous versions and can cause a major problem and actively prevent customers from keeping up-to-date.

Legacy Software and Windows

Change for the sake of change is not good. Changing just because something is new is not good, unless you are a football or baseball player and demand the latest and greatest. Businesses are generally not like that—they are typically the complete opposite. All businesses should ask the following questions before considering any change to the status quo:

- What are the benefits of upgrading to X?
- What are the disadvantages of staying as we currently are?
- What will it cost to change to X?
- How will we fund the upgrade?
- What are the alternatives to choosing X?

Often when business leaders look at this list, they are typically put off by the cost and the lack of clear reasons why their business should upgrade.

Here is a test: name three things about Internet Explorer 11 that make it compelling to upgrade from version 10? Because it is free is nice, but that is not really a business benefit.

We should be able to list five to ten reasons, if not more, when we think about moving to Windows 7 from XP, or to Server 2012R2 from Windows Server 2003R2.

Often, however, it is sometimes just one thing that is so compelling that we must upgrade. A few years ago, I remember discussing the huge changes in Office 2007 compared to Office 2003. I met a business owner and he told me how he upgraded his entire company from Office 2000 to Office 2007 because of just one new feature. Which one? The feature was the zoom slider, visible in the bottom right of the screen on every version of Office since 2007 (see Figure 2-1). He told me that this feature would save his team a huge amount of time, increasing productivity, and therefore make his business more profitable.

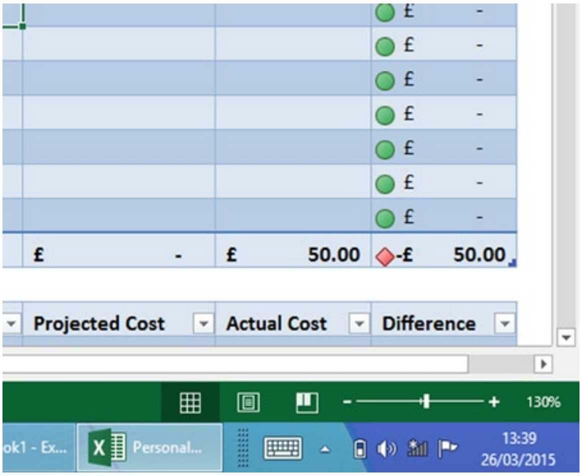


Figure 2-1. *Microsoft Excel Zoom feature*

I heard a similar story when upgrading to Microsoft Excel 2013; this time the killer new feature was Sparklines, which offers the viewer a very small line-chart to indicate measurement change within a range of data. (Personally, I really disliked the change to the ribbon, but I persevered, and now nearly ten years later, I am getting used to it.)

You have to decide, weigh up the pros and cons of each stance, and decide whether you are going to be a Luddite[1] to keep the status quo, or if you are ready to join the hipsters and embrace the pace of change.

■ **Note** We are seeing a current revolution in regard to the seemingly relentless push to toward cloud computing. Already there are clearly two sides to the case: one is to embrace the visible benefits of the cloud, but the other side is to fear about security and trust, cost stability, reliability, and of course, the loss of traditional skills and career prospects once IT is effectively outsourced to the monolithic cloud server providers.

Ultimately, we all see situations from our own vantage point/point of reference.

[1] Luddites were the revolutionaries who tried to prevent the use of machinery during the Industrial Revolution (1811-16) by smashing up the newly installed machines in factories across Britain.

User Group Discussion

In a discussion with a group of businesses at a local user group that I manage, I asked them to imagine two companies: one that had characteristics of a business 200 years ago in the United Kingdom in the industrial revolution, and then look at a start-up business based in California in the last couple of years.

Here are the results. Which characteristics do you agree with?

- **Legacy** = Stagnant, hindered, held back, limited, constrained, choked, frustrated, imprisoned, behind, locked, old fashioned, labor intensive, costly, stable, rigid, established, productive, powerful, static, experienced

- **Start-up** = Agile, responsive, unbound, open minded, free flowing, modern, young, vibrant, efficient, dynamic, spontaneous, entrepreneurial, profitable, growing, evolving, learning, cash strapped

When consulting, I would love the businesses that fell into a middle category—businesses that are stable, established, and wanted to embrace some of the new technology. I like them because they stage the process, publish an adoption rollout place, create desire, deploy, evaluate, and learn from the process. Being established, they would also always settle their invoices on time!

The Windows Blue Screen of Death

If there was ever a phrase that would conjure a feeling of dread upon a user, it was the Blue Screen of Death (BSOD). These occurrences relate to *stop errors*, which terminally halt a previously running system. Such is the destructive and unpredictable nature of a system crash; most system administrators actually fear a BSOD, while at the same time relishing the challenge of investigating and developing a remedy. Thankfully, in almost all cases, it has become a thing of rarity among ordinary users, especially since Windows 7 SP1, and it is rarely reported to the help desk in any significant volume.

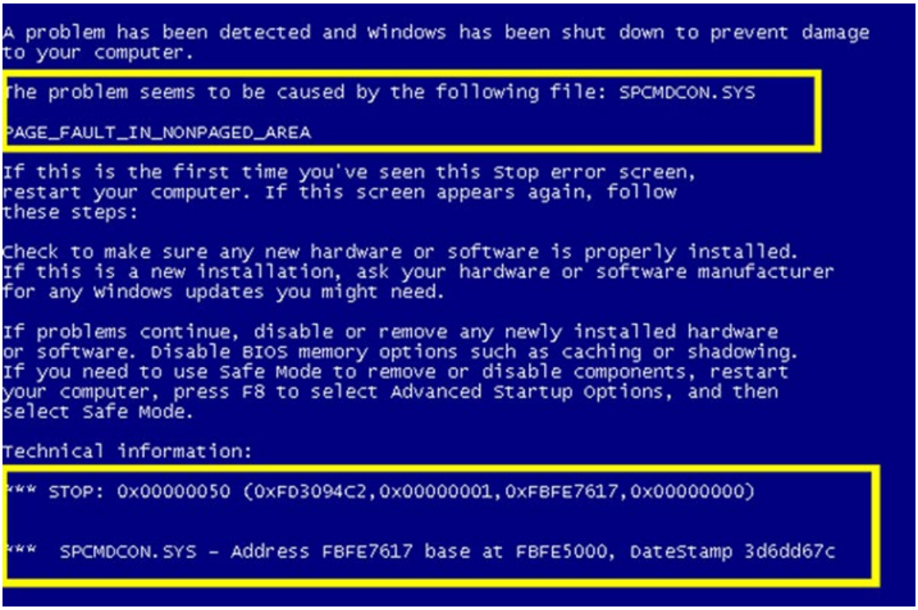
Typical scenarios where a BSOD is still prevalent includes systems belonging to PC hobbyists, systems being modified and upgraded, faulty hardware, systems under heavy load, malware-infested systems, and software conflicts.

Users who like to push the limits of their physical performance extremes also experience highly unstable systems that generate BSOD occurrences. Troubleshooters and computer forensic investigators—who spend a lot of time analyzing networks and packets, and using specialist security software—are best advised to utilize virtual machine technology such as Hyper-V, VMware Workstation, or a similar sandboxed environments that can be safely used.

A BSOD is an unexpected and non-trivial crash of the OS. Users should report each instance, because a persistent BSOD will in all likelihood start to affect other programs, and even the stability of the Windows registry, which could then cause corruption and require a system reinstallation.

Once a BSOD is reported, you should be aware that the system will likely continue to exhibit instability issues unless the root cause of the underlying problem is resolved. This predictability can be used to your advantage when diagnosing BSOD issues, because you should be able to re-create the instance and "force" the system to crash under a controlled and monitored environment.

One key feature of a BSOD is that the system attempts to "catch" the system during the system crash and provides the user with some (useful) information, as shown in the example in Figure 2-2.



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)


***  SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

Figure 2-2. *The Blue Screen of Death*

In Figure 2-2 you can also see that the Windows service SPCMDCON.SYS has failed. From the BSOD, you should be able to gather the following information:

- The stop error number, which uniquely identifies the error
- The stop error parameters, which provide additional information relating to the specific stop error number
- Driver information is available if the source of the problem relates to drivers

Armed with this information, you are able to search online to establish the problem and hopefully a resolution.

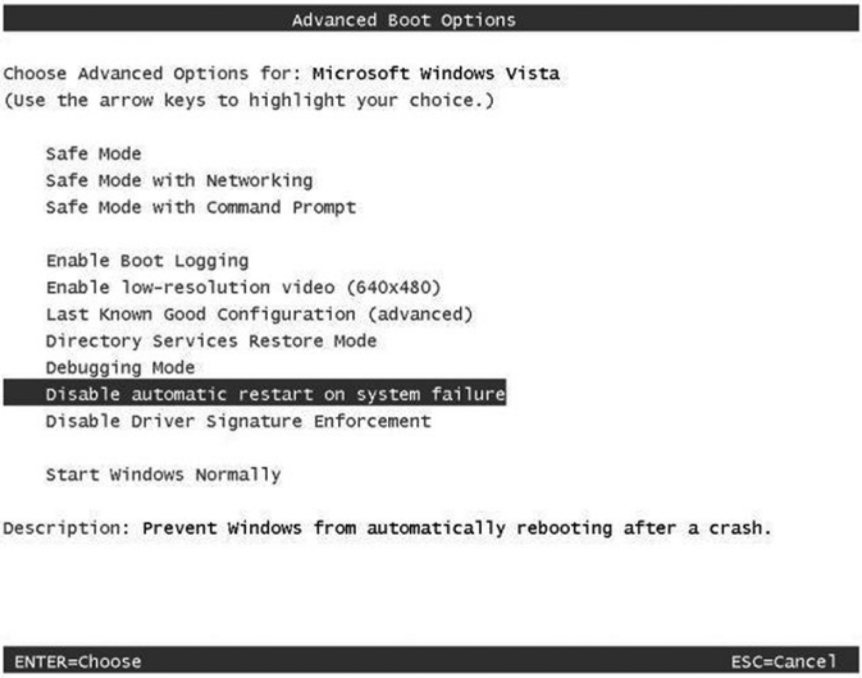
In addition to the information available on the blue screen, if the system is able to be rebooted after the BSOD, either normally or using Safe Mode, it is useful to take a look in the System Event Log and view the error message. For example, a faulty driver during boot up usually has the stop error code STOP: 0x00000050 and an Error EventID of 1003.

■ **Note** If you want to be particularly naughty with a colleague, consider installing the BlueScreen Screen Saver available from Windows Sysinternals at `https://technet.microsoft.com/en-us/sysinternals/bb897558.aspx`. This tool mimics a BSOD and much more.

With more PCs now running 64-bit versions of Windows, we expect to see fewer BSOD due to misbehaving device drivers, which account for 85% of system crashes (caused by issues such as video card drivers and networking devices that provide essential I/O communications at the core of the OS). All 64-bit versions of Windows now require drivers to be digitally signed, which reduces the likelihood of drivers being used by malware. Digitally signing a driver does not prevent poorly written driver code from being installed on a PC, because digitally signing the driver only verifies the code integrity, not the competence of the code author.

Since Windows XP, Microsoft has made major investments in its efforts to stabilize drivers and remediate common mistakes present within drivers. Through vast amounts of usage and crash data, and educating OEM partners with clearer guidance on how to write drivers that are respectful of the Windows kernel requirements, it is refreshing to see that all versions of Windows since XP have become increasingly more stable and exhibit far less driver-related BSOD.

If your system refuses to reboot successfully, or is trapped within a perpetual BSOD that restarts over and over again, you should take the following steps. Press F8 after the BIOS screen appears. From Advanced Boot Options, select **Disable automatic restart on system failure**, as shown in Figure 2-3. This allows you to read and make note of the information contained on the BSOD. You can then allow Windows to attempt a reboot. If the perpetual loop reoccurs, select another option, such as Safe Mode, from the Advanced Boot Options menu.



```
                              Advanced Boot Options

Choose Advanced Options for: Microsoft Windows Vista
(Use the arrow keys to highlight your choice.)

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement

    Start Windows Normally

Description: Prevent Windows from automatically rebooting after a crash.



ENTER=Choose                                                          ESC=Cancel
```

Figure 2-3. *Advanced Boot Options menu*

An example of best practice that I often recommend to system administrators is to configure Windows to always prevent systems from restarting after a stop error. This allows the stop message text and accompanying information to be displayed, and this in turn encourages users to report such occurrences to the help desk.

To disable the system from automatically rebooting, take the following steps:

1. Click **Start**, right-click **Computer**, and select **Properties**.
2. Click **Advanced System Settings**.
3. In the **System Properties** dialog box, click the **Advanced** tab. Under **Startup and Recovery**, click **Settings**.
4. In the **System Failure** box, clear the **Automatically Restart** check box.

These steps can also be configured if the system is booted in Safe Mode.

There are over 300 unique stop codes, and most are quite rare. The full list can be found on MSDN within the Bug Checks (Blue Screens) reference at `https://msdn.microsoft.com/en-us/library/windows/hardware/hh994433(v=vs.85).aspx`.

From data gathered in May 2012 on blue screen crashes on Windows 7 and Windows 7 SP1 machines, over 90% are related to just 20 stop codes. These are grouped into the categories shown Table 2-1, with their distribution as a percentage shown in the second column.

Table 2-1. *Distribution Stop Codes by Category for Windows 7/Windows 7 SP1 in May 2012*

Category	% of Issues	Stop Code
Page fault	18.3%	0xA - IRQL_NOT_LESS_OR_EQUAL 0xD1 - DRIVER_IRQL_NOT_LESS_OR_EQUAL
Power management	13.2%	0x9F - DRIVER_POWER_STATE_FAILURE
Exceptions and traps	17.0%	0x1E - KMODE_EXCEPTION_NOT_HANDLED 0x3B - SYSTEM_SERVICE_EXCEPTION 0x7E - SYSTEM_THREAD_EXCEPTION_NOT_HANDLED 0x7F - UNEXPECTED_KERNEL_MODE_TRAP 0x8E - KERNEL_MODE_EXCEPTION_NOT_HANDLED with P1 != 0xC0000005 STATUS_ACCESS_VIOLATION
Access violations	14.0%	0x50 - PAGE_FAULT_IN_NONPAGED_AREA 0x8E - KERNEL_MODE_EXCEPTION_NOT_HANDLED with P1 = 0xC0000005 STATUS_ACCESS_VIOLATION
Display	12.6%	0x116 - VIDEO_TDR_FAILURE
Pool	7.0%	0x19 - BAD_POOL_HEADER 0xC2 - BAD_POOL_CALLER 0xC5 - DRIVER_CORRUPTED_EXPOOL
Memory management	7.0%	0x1A - MEMORY_MANAGEMENT 0x4E - PFN_LIST_CORRUPT
Hardware	4.5%	0x7A - KERNEL_DATA_INPAGE_ERROR 0x124 - WHEA_UNCORRECTABLE_ERROR
USB	1.8%	0xFE - BUGCODE_USB_DRIVER
Critical object	2.3%	0xF4 - CRITICAL_OBJECT_TERMINATION
NTFS file system	2.1%	0x24 - NTFS_FILE_SYSTEM

User Account Control and Security Permissions

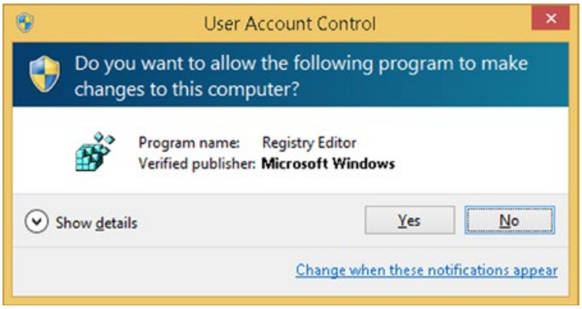
User Account Control (UAC) has shared a love-hate relationship with many users ever since its introduction in Window Vista. Most IT professionals have become accustomed to the security benefits of UAC, but still harbor resentment toward how UAC is implemented and how annoying it can be for the help desk and technical team to administer.

Most software is designed to run on the current OS version in the market. Many companies seek to extend the lifespan of software, and therefore the economic return on investment, by installing older or legacy software on their current OS. With this in mind, UAC proved to be a huge hurdle for legacy software—after all, UAC was a security game changer as far as software was concerned.

Windows XP and earlier legacy software was built without knowledge of UAC. Vista and later operating systems use UAC, which forces applications to run as with standard user privileges, rather than the all-powerful administrative level that was often available in the XP era. Most users are standard users, and if they try to run programs that require elevation, the programs will fail to run.

Other applications that were written in the pre–Vista/UAC timeframe may expect to write files to the Windows operating system areas, or the protected areas of the system drive; these actions are now blocked by UAC.

For users who are using an account that is a member of the Administrators group, when you try to invoke a task or run software that would normally prompt you to enter your administrative username and password, UAC simply offers a prompt (see Figure 2-4), which is called Admin Approval Mode.



User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Registry Editor
Verified publisher: **Microsoft Windows**

Figure 2-4. *Admin approval mode*

While this can be mildly annoying, it does ensure that the user makes a conscious decision to allow operations to run on their computer.

Once UAC has been triggered by a user action or an application requesting elevated access, Windows performs one of the following three options:

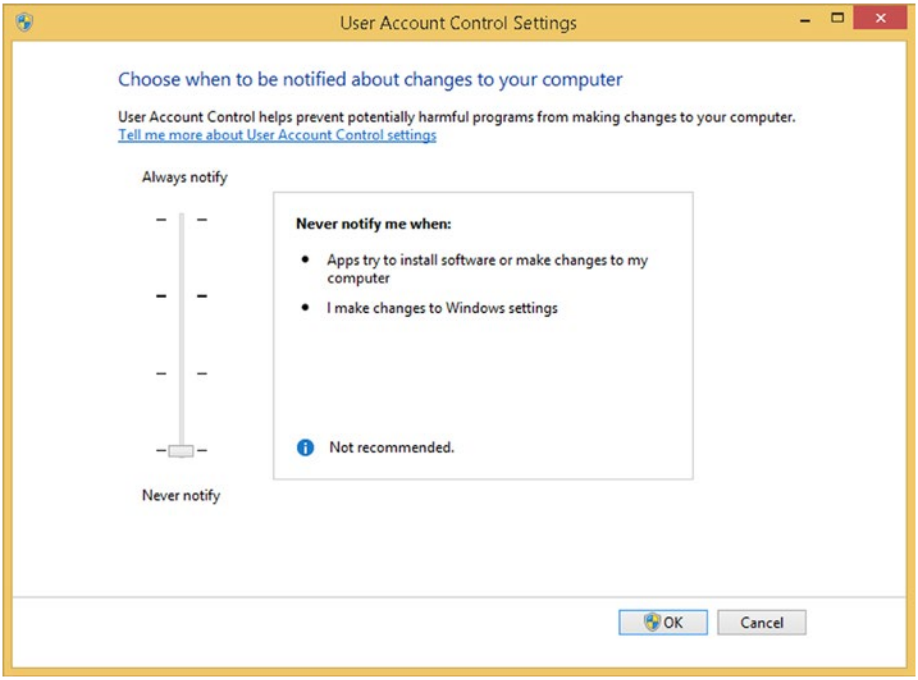
- **Silently elevate**: This option allows elevation without end-user interaction, and it only happens if the user is a member of the Administrators group.
- **Prompt for consent**: The user is prompted with a Yes/No dialog box (similar to the one shown in Figure 2-4). This is the default action if the user is a member of the Administrators group.
- **Prompt for credentials**: The user is prompted to provide credentials for an administrative account. This is the default for all non-administrative user accounts.

All UAC elevations can be configured and even disabled for standard users by modifying Local Security Policy or Group Policy.

In Vista and Windows 7, many users complained to Microsoft that UAC was very "noisy" and that the prompting was too frequent, which lessened the effectiveness of the feature. With Windows 8 and newer, Microsoft has fine-tuned UAC to make it less visible; for example, routine user-initiated tasks.

It is still a recommended practice to operate a “non-admin” model for end users; this prevents unwanted modifications and rogue software being applied to managed desktops. In many situations, software that was designed for XP or earlier versions of Windows can be modified quite simply to ensure that it will operate on current versions. It is, however, worth noting that Windows XP is at the “end of life” support status; it is well over a decade old. And any software built to run on XP is likewise pretty old and may be vulnerable to attackers seeking to exploit the age and legacy nature of the software.

While it is not possible to disable underlying UAC for standard users, it is possible to fine-tune the UAC by using the UAC settings slider (see Figure 2-5). At the lowest position, you can set the UAC to never notify you, effectively turning off UAC for administrative users.



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Never notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Not recommended.

Figure 2-5. *Fine-tuning UAC settings*

In Windows 8.1, UAC has four settings that a user can choose. These are described in Table 2-2.

Table 2-2. *UAC Slider Settings*

UAC Setting	Comments
Always notify	This always prompts the user before making any changes to Windows settings or allowing applications to make changes that require administrative permissions. The most secure setting.
Notify me only when apps try to make changes to my computer (default)	This is the default UAC setting. It only notifies the user before *programs* make changes to the system that requires administrator permissions. If the user manually makes changes to Windows, then UAC remains silent and allows the action. This setting is an improvement over the default setting for Windows 7. Naturally, this setting and all subsequent settings in this list are less secure than the first setting. Malware could simulate the keystrokes of a user and change Windows settings.
Notify me only when apps try to make changes to my computer (do not dim my desktop)	This level is the same as the previous setting, except that the desktop is not dimmed when UAC is initiated.
Never notify	This effectively turns off UAC and offers no warnings or protection against unauthorized system changes. However, if you are signed-in using a standard user account, any changes that require administrator permissions are automatically denied. Extreme care should be taken when using this setting, as applications effectively have the same access permissions as the user that is logged in.

Although we have noted that some legacy software can be challenged by UAC, it is clear that this new security model has dramatically improved system security against rogue software and malware, and UAC is likely to be implemented in future versions of Windows.

Internet Explorer and Browser Plug-ins

Ever since the early 1990s when the World Wide Web was “born,” there have been browsers that allow web pages to be viewed. Over the years, many browsers have emerged, including Netscape Navigator, Internet Explorer, Opera, Firefox, Safari, Chrome, and Windows 10 with Microsoft Edge.

Each browser had its own lifespan; some browsers, like Netscape (which once had 90% market share), faded and were surpassed by new browsers. Due to being bundled with every Windows version since Windows 95 (as an add-on package in Microsoft Plus! For Windows 95), Internet Explorer (IE) became very entrenched within the consumer and business world, primarily because it was (a) shipped with the OS, (b) updated and patched by Microsoft, and (c) embedded into the OS so that administrators could customize and manage the IE use.

Over the years since the emergence of the Internet, a lot has changed to improve the user experience of browsing. The following are just a few of the huge improvements seen in current browsers:

- An adoption of standards-based support, with browsers conforming to the standard set by the World Wide Web Consortium (W3C)
- Extensibility, which allows browsers to add support for additional functionality through plugs-ins
- Security improvements such as HTTPS, security zones, site certificates, protected mode pop-up blockers

Compatibility Issues

Throughout the development life cycle, inevitably there is new functionality introduced due to innovations in technology that advance the browsing experience. However, with each advance comes a trade-off. There are billions of web pages on the World Wide Web; each has been written in a flavor of HTML and each page could be over 20 years old. As browsers are updated to understand newer standards, the earlier standards often need to make way because they would otherwise conflict. One of the big challenges that Microsoft has had with its IE browser over the years is the desire to retain as much backward compatibility support as possible. While this is often great for the web page that was written 10 years ago, the issue with this approach is that the IE has become bloated, slow, and complex. Nearly every other popular browser has decided not to provide extensive backward compatibility.

IE11 shipped with Windows 8.1; it is the last version of Internet Explorer that will be released. Windows 10 ships with the new Microsoft Edge, which is a lightweight web browser that finally removes support for legacy technologies and does not promise to be fully backward compatible. (In Windows 10, both Edge and IE11 will coexist).

Browsing the Internet is very popular, but it has allowed the opportunity for unscrupulous people and organizations to attack private and corporate users via their Internet browsing. Every new browser attempts to protect the user against an ever-increasing array of potential attacks.

A number of valuable built-in IE11 features help protect users from attacks. These include InPrivate Browsing, SmartScreen Filter, and InPrivate Filtering. Each of these features layers another level of complexity that can hinder browser compatibility and the ability to browse legacy web pages without disruption.

The majority of users leave their favorite browser at the default settings, and they seldom deviate from the “safe” position. IT professionals and enthusiasts often need to be able to administer the browser and fine-tune the settings to control its behavior. By understanding the risks associated with browsing, you are able to appreciate how some of security features keep you safe; and you are then able to make a judgement should you need to sacrifice security protection for backward compatibility and ease of use.

A compatibility issue may be reported to the help desk by a user who needs to access a particular web site. This may need to be investigated, and if necessary, the security settings within IE can be modified. IE allows you to configure different levels of security for web sites by using security zones. Some web sites want you to download files, or to run ActiveX controls or Java applets. Internal web sites (intranet sites) and external web sites can be added to one of the following four security zones:

- Local Intranet
- Trusted Sites
- Restricted Sites
- Internet

Each zone has a default security level configured, which helps to protect the OS from malicious attack by a web site. It is normally not necessary to modify these settings. However, there may be web sites that can have a less restrictive level of security, which you can set manually within the zone by moving the slider up for more security, or down for less security. These web sites should be evaluated, and once deemed safe, they can be added to the Trusted Sites security zone, which is less restrictive to the web site and allows the site to exercise more functionality through the browser. At the end of this chapter, you will see that these settings can also be modified using Group Policy.

IE11 Compatibility

We discussed how all browsers try to correctly render the code that makes up a web page, based on the underlying version of HTML. On an older operating system, such as Windows 7, on which we have not updated the IE version, by using the automatic updates, it is using the default IE8. Since IE11 is a more modern version than IE8, it would be fair to assume that IE8 is not as feature-rich or secure as IE11. Web pages that have been recently built, for example in the last few years, and showcase modern web enhancements will not optimally display on a system using IE8.

With IE11, the browser engine actively and silently attempts to ascertain the version of the underlying HTML, and then renders the page by using the most appropriate browser layout engine. So long as the web developer has specified the version of his or her code, IE11 can automatically detect a legacy web page and invoke the correct IE engine required to display the web site.

On older versions of IE, the user is required to enable the Compatibility View feature; but in IE11, this functionality is automatic.

The following are some of the key features of IE11 Compatibility View:

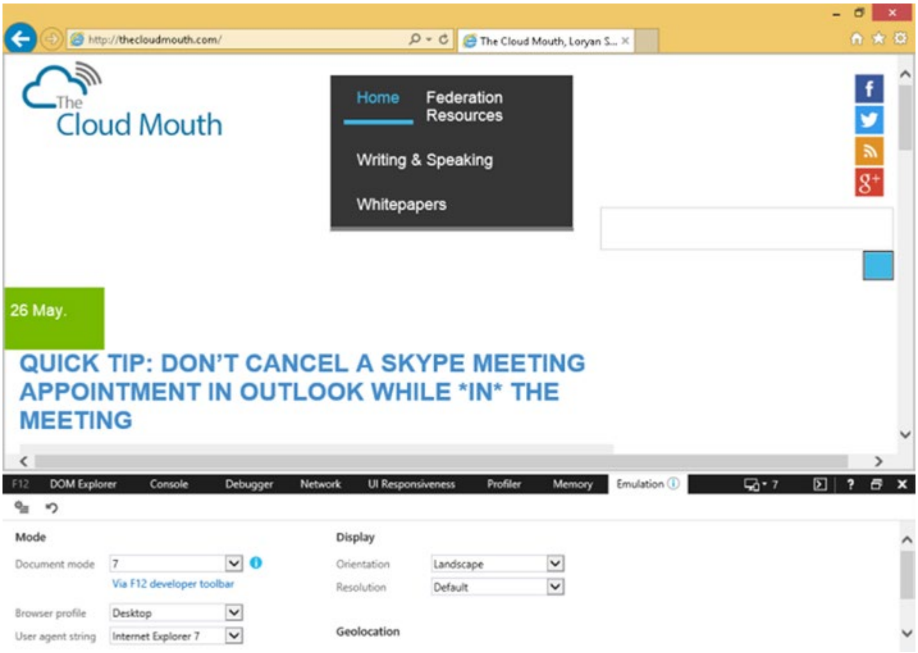
- It invokes standards mode to render web sites by default
- It can “fix” sites that render differently than expected
- Group Policy can populate a list of web sites to use Compatibility View by default
- It can be toggled on/off without requiring the browser to be restarted

- If it is manually invoked for a web site, IE11 remembers the site and the appropriate settings
- It is enabled for intranet web sites by default

By default, all intranet sites are displayed in Compatibility View. This is desirable since many internal web sites tend to be relatively old and not often reengineered to utilize the most current web site technologies.

Should you come across sites that simply do not automatically render correctly in your browser, it is possible to manually change the emulation engine. This is also very useful when testing new web sites prior to release.

Load the web site whose compatibility settings you wish to review. Press F12 to invoke the developer menu. The screenshot in Figure 2-6 shows how a web site renders when viewed on a PC using IE7. Figure 2-7 shows the same web site with the default automatic view in IE11.



26 May.

QUICK TIP: DON'T CANCEL A SKYPE MEETING APPOINTMENT IN OUTLOOK WHILE *IN* THE MEETING

Mode

Document mode: 7
Via F12 developer toolbar

Browser profile: Desktop

User agent string: Internet Explorer 7

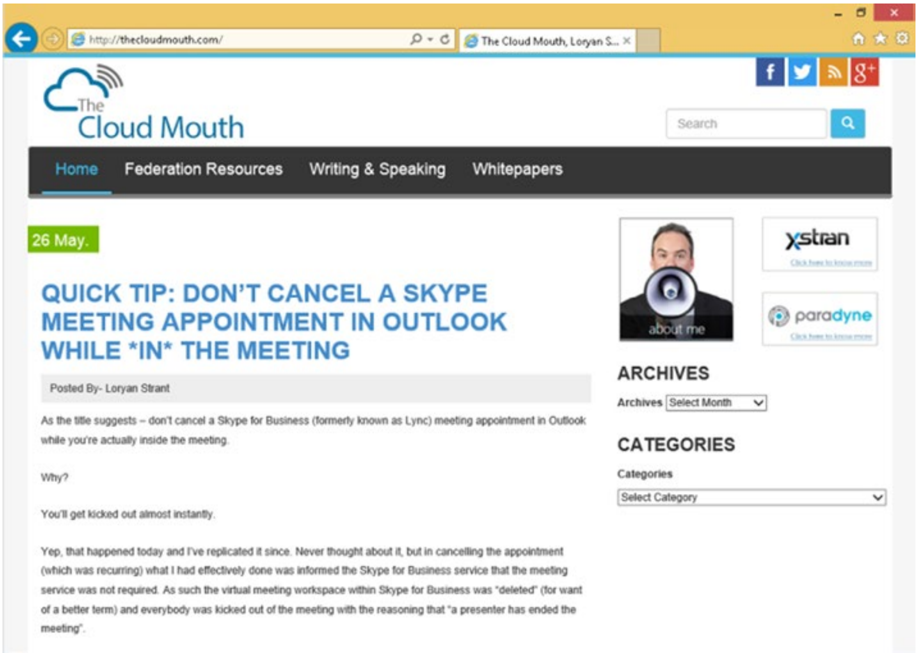
Display

Orientation: Landscape

Resolution: Default

Geolocation

Figure 2-6. Rendering web sites using IE7 emulation



26 May.

QUICK TIP: DON’T CANCEL A SKYPE MEETING APPOINTMENT IN OUTLOOK WHILE *IN* THE MEETING

Posted By- Loryan Strant

As the title suggests – don't cancel a Skype for Business (formerly known as Lync) meeting appointment in Outlook while you're actually inside the meeting.

Why?

You'll get kicked out almost instantly.

Yep, that happened today and I've replicated it since. Never thought about it, but in cancelling the appointment (which was recurring) what I had effectively done was informed the Skype for Business service that the meeting service was not required. As such the virtual meeting workspace within Skype for Business was "deleted" (for want of a better term) and everybody was kicked out of the meeting with the reasoning that "a presenter has ended the meeting".

ARCHIVES

Archives: Select Month

CATEGORIES

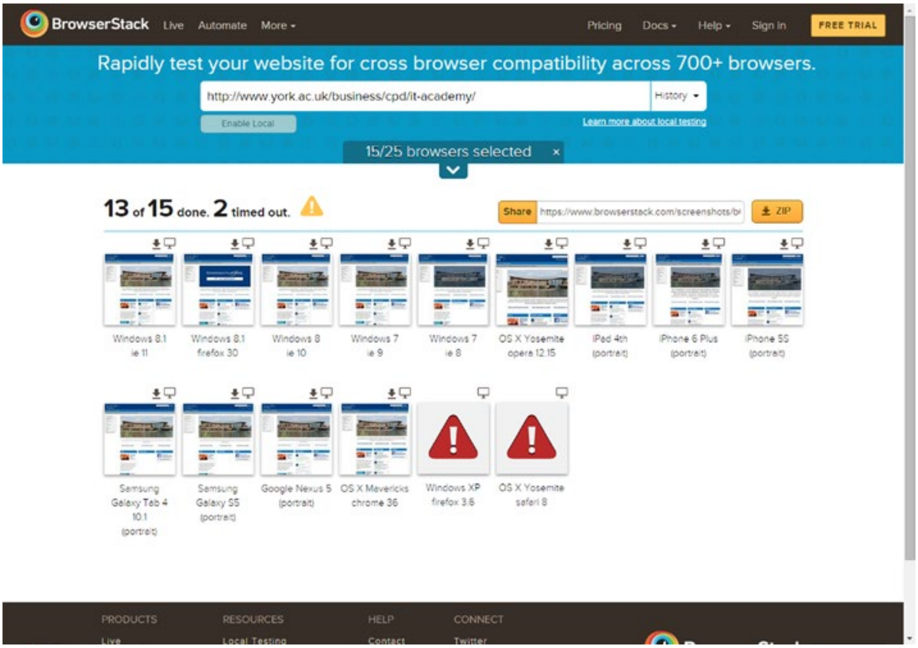
Categories: Select Category

Figure 2-7. *Default IE11 compatibility rendering*

Another setting that you can modify is the User Agent String. This setting identifies which browser is being used to view the web site, and then relays this information back to the server hosting the web site. This is useful for web servers because they may dynamically modify content so that it is optimized for a specific browser.

The developer tool settings are not persistent, and the web site is displayed by the default engine once you exit the settings tool.

There are several online tools that can be used to test how your web site will work across multiple browsers. Some of these tools test the web site by launching a virtual machine, browsing to the web site, and then creating a screenshot of how the web site renders. The BrowserStack free trial can test your web site on 15 popular Internet browsers (see Figure 2-8).



Rapidly test your website for cross browser compatibility across 700+ browsers.

http://www.york.ac.uk/business/cpd/it-academy/

15/25 browsers selected

13 of 15 done. 2 timed out.

Figure 2-8. *Testing web page rendering with BrowserStack*

Browser Plug-ins

We already briefly mentioned plug-ins and explained that they extend the functionality of a browser. Unlike other browsers, Microsoft uses the term *add-on* to refer to plug-ins. Whenever a web site requires an add-on, IE prompts you to install it, and it is available for use if subsequently needed. Organizations using the cloud-based Microsoft Intune service require the Silverlight add-on to be enabled within IE to access the Admin Console to manage devices and users.

The HTML5 and Adobe Flash add-ons are included with IE11, whereas others are bundled with other installed software; for example, the Skype Click to Call add-on locates and highlights any telephone numbers present within web pages.

Often when a free or trial piece of software is installed from a source such as FileHippo or other repository, additional software and browser add-ons are also installed. Most of the time, users do not notice that extra software was installed, or that the browser was modified with a new toolbar or home page. Software that is "piggybacked" within the installer of another app is a very common way for freeware authors to make money, as each successful installation results in a commission from the third-party "parasite."

Users should be mindful of allowing such actions; whereas these installs may seem pretty insignificant at first glance, you can assume that the third-party software could obtain the following facts about its new host:

- The user has administrative rights to the computer
- The user is not risk aware and is vulnerable to attack
- Software updates from the third-party software could have access to the host system

In the Apress *Windows Troubleshooting* books, we have installed numerous tools and applications, such as CCleaner, Skype, and Chrome; each also tries to install additional software or allows the silent updating of itself on a regular basis.

You should know how to review and modify your add-ons in IE. While more add-ons potentially provide additional functionality, the user should also be aware that each add-on must be loaded into memory, which ultimately slows down the browser. Even with a fast computer and a broadband connection, the loading speed of web pages is significantly reduced, because each add-on trawls a page to locate content that matches the add-on capability, such as telephone numbers, addresses, dates, and so forth.

In a few extreme situations (typically home users are the main culprit), we have encountered systems that have multiple IE toolbars, such as those shown in Figure 2-9.

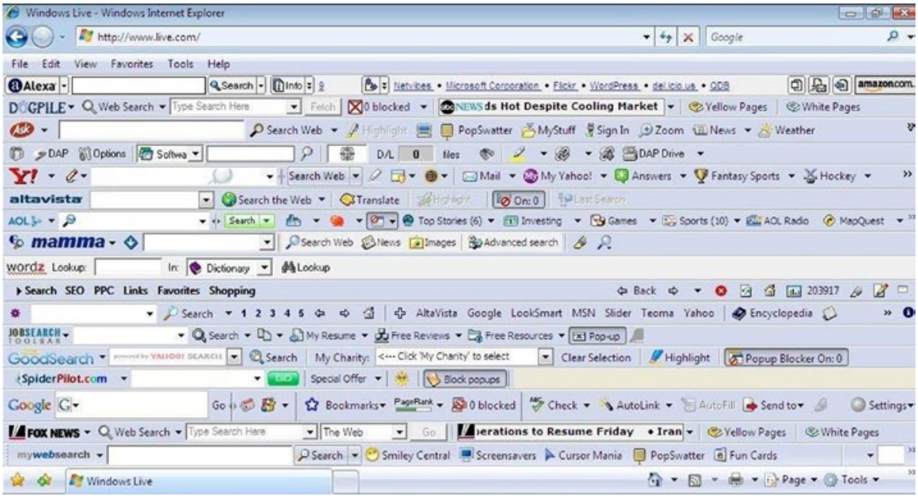

Windows Live - Windows Internet Explorer
http://www.live.com/
Google
File Edit View Favorites Tools Help
Alexa Search Info Netvibes • Microsoft Corporation • Flickr • WordPress • del.icio.us • ODB amazon.com
DOGPILE Web Search Type Search Here Fetch 0 blocked NEWS ds Hot Despite Cooling Market Yellow Pages White Pages
Ask Search Web Highlight PopSwatter MyStuff Sign In Zoom News Weather
DAP Options Softwa D/L 0 files DAP Drive
Y! Search Web Mail My Yahoo! Answers Fantasy Sports Hockey
altavista Search the Web Translate Highlight On: 0 Last Search
AOL Search Top Stories (6) Investing Games Sports (10) AOL Radio MapQuest
mamma Search Web News Images Advanced search
wordz Lookup: In: Dictionary Lookup
Search SEO PPC Links Favorites Shopping Back 203917
Search 1 2 3 4 5 AltaVista Google LookSmart MSN Slider Teoma Yahoo Encyclopedia
JOBSEARCH TOOLBAR Search My Resume Free Reviews Free Resources Pop-up
GoodSearch powered by YAHOO! SEARCH Search My Charity: <--- Click 'My Charity' to select Clear Selection Highlight Popup Blocker On: 0
SpiderPilot.com GO Special Offer Block popups
Google G Go Bookmarks PageRank 0 blocked Check AutoLink AutoFill Send to Settings
FOX NEWS Web Search Type Search Here The Web Go perations to Resume Friday • Iran Yellow Pages White Pages
mywebsearch Search Smiley Central Screensavers Cursor Mania PopSwatter Fun Cards
Windows Live Page Tools

***Figure 2-9.** Multiple IE toolbars installed*

To remove a toolbar in IE, simply right-click the toolbar and click Remove.

To review and disable a specific add-on, follow these instructions:

1. Open **Internet Explorer**.
2. On the **Tools** menu, click **Manage add-ons**.
3. In the **Manage Add-ons** dialog box, in the **Show drop-down** list, click **All add-ons**.

4. Find the name of the add-on that you want to modify in the reading pane. Select an add-on to disable it, and then click **Disable**.
5. To enable an add-on, tap or click it, and then click **Enable**.
6. Close the **Manage Add-ons** dialog box.

■ **Note** Windows RT and the modern app version of IE do not support add-ons.

For system administrators and IT professionals seeking to manage the usage of IE within a corporate environment, one of the major advantages of using IE is the ability to fine-tune the user experience by using Group Policy. There are over 90 GPOs relating to the management of IE11 within Group Policy, which can be found in the following locations:

- Computer Configuration\Administrative Templates\Windows Components\Internet Explorer
- User Configuration\Administrative Templates\Windows Components\Internet Explorer

Summary

This chapter focused on the compatibility issues resulting from using a newer version of Windows. We expect that with each new OS release, reliability and crash resistance will improve. Being aware of potential software compatibility issues on Windows helps IT professionals become more effective and confident when dealing with scenarios such as legacy applications, older web sites, and BSOD in the workplace.

In Chapter 3 you see how hardware and drivers can present additional compatibility issues in Windows. You will revisit application and IE compatibility issues in Chapter 4.

CHAPTER 3

Common Hardware Compatibility Issues

One of the most significant differences between PCs and Macs is user choice. If Bill Gates had chosen to sell preconfigured, ready-made PCs, we most certainly would not have the rich computing ecosystem that we have enjoyed for the last 35 years. Instead, Gates saw how he could make money from software. He successfully signed a contract with IBM that allowed him to license his DOS and then his Windows operating systems to every PC sold.

Microsoft allowed and encouraged third-party hardware vendors to contribute to the PC landscape, and this allowed the number of original equipment manufacturers (OEMs) involved in the computer industry to increase exponentially during the first 10 years, thereby laying down firm foundations that have enabled choice for both consumer and business users.

At the same time, hobbyists and smaller niche vendors created PC bundles that offered more performance or specialized components. The key difference between large distributors and the enthusiast who is able build his or her own custom PC is support. Large PC builders such as IBM, Dell, Gateway, HP, and others dominated the PC hardware market and offered customers choice, ongoing support, and extended warranties. They built and sold complete systems, and offered them via mail order. Customization that allowed the customer to select components from a web shop also enabled more choice and fueled the rapid expansion of worldwide PC sales.

Those readers who remember when the Intel 80386SX processors were all the rage (back in 1988) may also recall an era that predates Plug and Play. It was great when Creative Labs introduced their Sound Blaster sound cards for the PC, because they allowed digitized sound on a PC for the first time. However, in the days before Plug and Play, enthusiasts needed to be knowledgeable about IRQ (interrupt request) lines, DMA (direct memory access), and conflicts; for example, we needed to know that the Sound Blaster card settings needed to work with the PC hardware (I/O port 220, IRQ 7, and DMA 1). The real fun came when there were other peripherals connected to the PC; for example, the parallel port for LPT1 also used IRQ 7, so it was only possible to either have sound or to print—but not both at the same!

Thankfully, Windows introduced Plug and Play (PnP) in 1995, ushering in a new era of computing. Troubleshooting and hardware compatibility issues never fully disappeared with early examples of PnP, and even today we still encounter issues with hardware, drivers, and conflicts—as you will see in this chapter.

M. Halsey and A. Bettany, *Windows Software Compatibility and Hardware Troubleshooting*,
DOI 10.1007/978-1-4842-1061-1_3

Plug and Play

PnP was introduced in Windows 95 to fully automate the detection and configuration of devices. This was a hugely complex feat to attempt, especially when OEMs rarely followed hardware guidelines or the emerging hardware standards, such as PC Industry Standard Architecture (ISA) and Peripheral Component Interconnect (PCI). Initially due to poor success rates, PnP was sometimes referred to as “plug and pray.” Personally, I found it to be very good, but it did require a lot of rebooting and seemed to work best when adding one item of hardware at a time.

Contrast the process from 1990s to the present-day PnP. We are able to take for granted the complexity of how PnP works; during a new installation of a modern version of Windows, such as Windows 8.1, the OS seamlessly autoconfigures every internal and external component, and if connected to the Internet, it pulls down and updates the latest drivers, and installs them as well. Now if everything went well all the time, there would be no need for this troubleshooting book. From time to time, a faulty driver, rogue update, or malware can corrupt your system. While we may no longer need to take a crash-course in IRQ and DMA settings, it is a good idea to know how to roll back a known good driver and understand what to look for when choosing drivers to update manually.

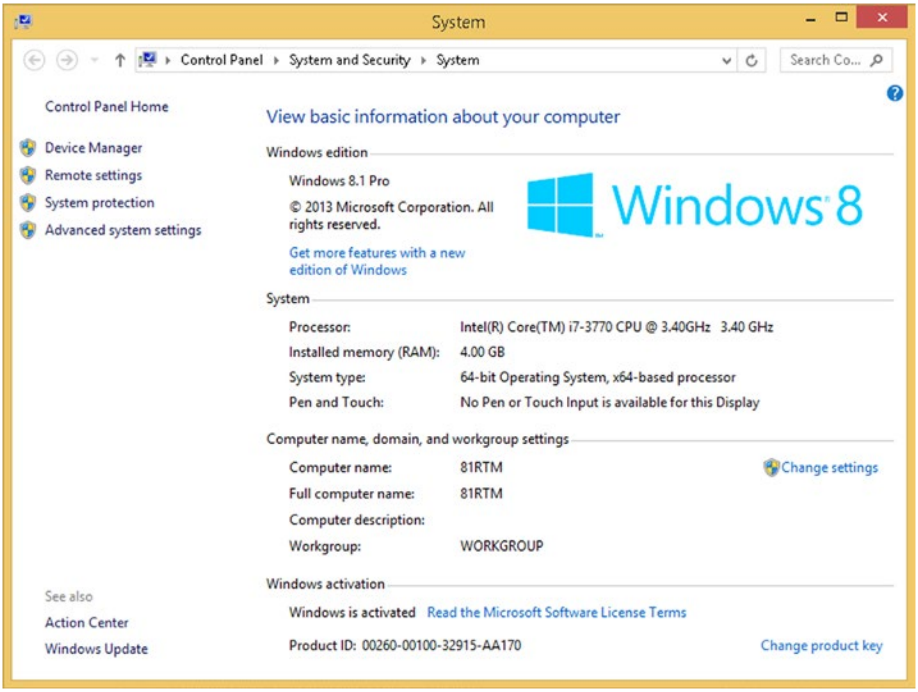
x86 vs. x64 Architecture

All modern computers are either x86 (which uses 32-bit computing) or x64 (which uses 64-bit). 64-bit computers allow the OS to access far more memory than x86, which allows apps to process and hold larger data sets in more memory for operations. Because a 64-bit processor can hold larger integers (numbers) than x86 chips, they have the ability to handle larger calculations and physically deal with considerably more calculations per second. If the app developer has written the underlying code to take advantage of the larger capabilities, then the app also has a performance gain over a similar app written for an x86 architecture.

The term *x86* came from the Intel processors, which were designated 80286 through to 80486; this initial range of “x86” chips were all 32-bit processors. While it is possible to install an x86 version of Windows on a 64-bit capable PC, it is not possible to install an x64 version onto an x86 system.

There are several ways to determine if your PC is using a 64-bit version of Windows, including the following:

- If the PC has more than 4GB of RAM installed, it is most likely to be using a 64-bit version.
- Search for **System** and view the system type information (see Figure 3-1).



System

Control Panel › System and Security › System

Control Panel Home

Device Manager

Remote settings

System protection

Advanced system settings

See also

Action Center

Windows Update

View basic information about your computer

Windows edition

Windows 8.1 Pro

© 2013 Microsoft Corporation. All rights reserved.

Get more features with a new edition of Windows

System

Processor: Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz 3.40 GHz

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: 81RTM

Full computer name: 81RTM

Computer description:

Workgroup: WORKGROUP

Change settings

Windows activation

Windows is activated Read the Microsoft Software License Terms

Product ID: 00260-00100-32915-AA170

Change product key

Figure 3-1. *Determining the PC system architecture*

Only a few years ago, 4GB of RAM seemed like a huge amount of memory, and anything above 16GB required server-class hardware. 32-bit computing can only access 3.2GB of RAM, even if more is installed. With 64-bit architecture, it is possible for Windows 8.1 to access 128GB (Enterprise and Pro versions can access 512GB). For more information about older operating systems, visit the MSDN resource at `https://msdn.microsoft.com/en-gb/library/windows/desktop/aa366778(v=vs.85).aspx`.

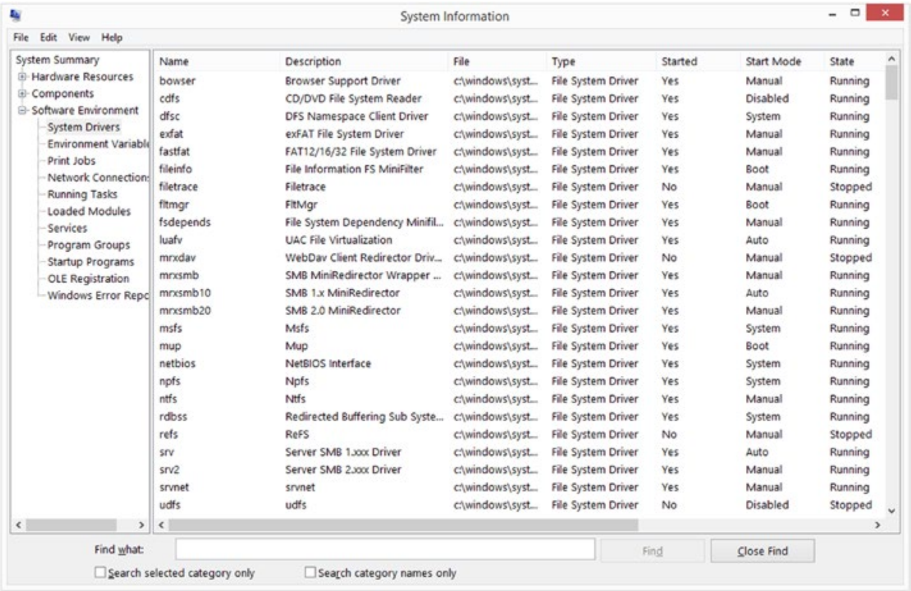
When troubleshooting compatibility issues relating to architecture, it should be noted that 32-bit or 64-bit computing is limited only to the operation of the processor and the software that is installed. All other hardware, such as RAM or peripherals within the system, are architecture agnostic.

Windows File System Drivers

For Windows to be able to interoperate with a specific file system, it requires a low-level driver. Windows supports many file systems, but the majority of them are not commonly known and they work behind the scenes. In this book, we focus on the most common, modern, and emerging file systems, and provide a comparison to legacy files systems where appropriate.

To see a complete list of the file systems that are supported on your Windows machine, load the System Information viewer (see Figure 3-2). Follow these steps:

1. Start the System Information viewer by typing **Msinfo32** in the Start screen.
2. Select **System Drivers** under **Software Environment**.
3. Sort the list of drivers by clicking the **Type** column.
4. View the drivers with the SERVICE_FILE_SYSTEM_DRIVER type attribute.



Name	Description	File	Type	Started	Start Mode	State
bowser	Browser Support Driver	c:\windows\syst...	File System Driver	Yes	Manual	Running
cdfs	CD/DVD File System Reader	c:\windows\syst...	File System Driver	Yes	Disabled	Running
dfsc	DFS Namespace Client Driver	c:\windows\syst...	File System Driver	Yes	System	Running
exfat	exFAT File System Driver	c:\windows\syst...	File System Driver	Yes	Manual	Running
fastfat	FAT12/16/32 File System Driver	c:\windows\syst...	File System Driver	Yes	Manual	Running
fileinfo	File Information FS MiniFilter	c:\windows\syst...	File System Driver	Yes	Boot	Running
filetrace	Filetrace	c:\windows\syst...	File System Driver	No	Manual	Stopped
fltmgr	FltMgr	c:\windows\syst...	File System Driver	Yes	Boot	Running
fsdepends	File System Dependency Minifil...	c:\windows\syst...	File System Driver	Yes	Manual	Running
luafv	UAC File Virtualization	c:\windows\syst...	File System Driver	Yes	Auto	Running
mrxdav	WebDav Client Redirector Driv...	c:\windows\syst...	File System Driver	No	Manual	Stopped
mrxsmb	SMB MiniRedirector Wrapper ...	c:\windows\syst...	File System Driver	Yes	Manual	Running
mrxsmb10	SMB 1.x MiniRedirector	c:\windows\syst...	File System Driver	Yes	Auto	Running
mrxsmb20	SMB 2.0 MiniRedirector	c:\windows\syst...	File System Driver	Yes	Manual	Running
msfs	Msfs	c:\windows\syst...	File System Driver	Yes	System	Running
mup	Mup	c:\windows\syst...	File System Driver	Yes	Boot	Running
netbios	NetBIOS Interface	c:\windows\syst...	File System Driver	Yes	System	Running
npfs	Npfs	c:\windows\syst...	File System Driver	Yes	System	Running
ntfs	Ntfs	c:\windows\syst...	File System Driver	Yes	Manual	Running
rdbss	Redirected Buffering Sub Syste...	c:\windows\syst...	File System Driver	Yes	System	Running
refs	ReFS	c:\windows\syst...	File System Driver	No	Manual	Stopped
srv	Server SMB 1.xxx Driver	c:\windows\syst...	File System Driver	Yes	Auto	Running
srv2	Server SMB 2.xxx Driver	c:\windows\syst...	File System Driver	Yes	Manual	Running
srvnet	srvnet	c:\windows\syst...	File System Driver	Yes	Manual	Running
udfs	udfs	c:\windows\syst...	File System Driver	No	Disabled	Stopped

Figure 3-2. *System Information displaying Windows file system driver*

Driver Signing in Windows

For most of the lifetime of Windows, Microsoft has implemented a program that allowed OEMs, upon payment of a fee, to supply their drivers to Microsoft, which would then carry out extensive testing by the Windows Hardware Quality Lab (WHQL) team. The WHQL tested and verified the compatibility of the driver against the selected operating system, and if the driver was functional, then Microsoft digitally signed the driver and included it in its Upgrade Advisor tool (which replaced the Hardware Compatibility List (HCL) used in the XP timeframe) and made it available as part of Windows Update.

We explained in Chapter 1 how hardware vendors can enroll (and pay Microsoft a fee for the service) in the "Compatible with Windows 7" or later Windows Hardware Certification Program that Microsoft offers. All of this has boosted sales through the reassurance that the device/software is compatible.

In Windows 7 and later versions, hardware drivers have become much more robust than those found in Windows XP and especially the troublesome Vista, which suffered from a fundamental shift in the kernel design and the introduction of UAC.

Windows XP suffered mainly due to the patchwork nature of its own evolution since its 2002 launch. Windows XP had an extremely long life—over 10 years—and in this time had three major service packs (SP), but also thousands of smaller updates during the period that it was still supported by Microsoft. While this may or may not have created an unstable platform for OEMs to write drivers, it did create a headache for the HCL. OEMs decided not to repeatedly subscribe to get their drivers validated for each SP as they released new hardware during the XP lifespan.

Over time, as XP became widely adopted, OEMs cut back with the driver approval process to save money. The lack of requirement to produce drivers verified against Microsoft's strict compatibly testing resulted in the release of drivers that were incompatible, and in several cases, very suspect in terms of performance and reliability.

Windows Vista suffered from a number of driver-related issues at the time of release; the major one being a lack of OEM hardware and driver support. The lack of adequate driver support was primarily due to Microsoft having changed the way in which Windows worked—Vista was a complete rework as far as the kernel, driver support, and the way UAC was used to beef up system security. Nearly every legacy driver no longer worked with Vista. These legacy drivers required a complete rewrite—something that the OEMs did not have the capacity for (and for a period of time, there was a shortage of skilled developers with the up-to-date .NET skills to write them).

Writing drivers for the new Windows took time—both to learn the necessary new skills and to achieve the required driver availability for the installed device population.

■ **Note** Just as with software installation, it is best practice to reboot the PC after each installation of hardware. This effectively creates a point that is either stable or unstable. Some issues may not present themselves to the user until after a reboot. Both are valuable checkpoints if troubleshooting needs to take place subsequent to the installation.

A device driver that is signed includes a digital signature. The signature is an electronic security mark that is trusted by Windows. It only exists to validate that the contents of the driver package (i.e., the driver `.inf` files) have not been tampered with. You can be confident that a digitally signed driver has actually come from the publisher that created the driver package, and that it has not been altered during the journey to your computer. Any tampering or modification of the driver file invalidates the digital signature. Windows is not able to verify its integrity and warns the user that an invalid signature has been detected, by displaying one of the following messages:

- Windows can't verify the publisher of this driver
- This driver has been altered
- Windows cannot install this driver

If Windows displays any of these messages while installing your device, you should stop the installation and visit the device manufacturer's web site to obtain a digitally signed driver for your device.

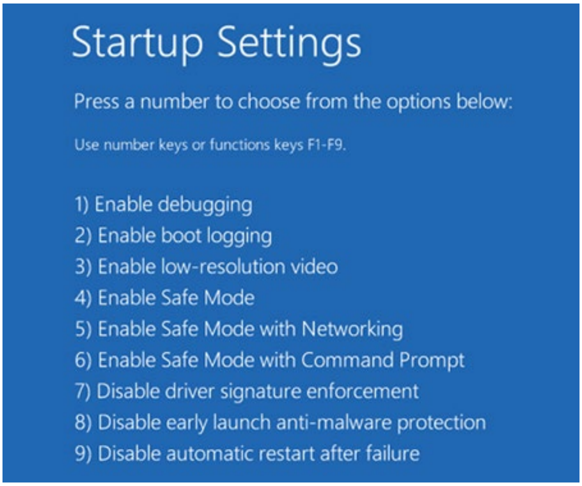
Files that have a digital signature embedded in them and that are downloaded using Internet Explorer are automatically checked to verify the status of the signing authority. If you are sure that there are no problems with a driver, and you want to disable the feature within IE that checks the certificate authority, follow these steps:

1. Open **Internet Explorer**.
2. Select **Internet Options** on the **Tools** menu.
3. Select the **Advanced** tab.
4. Scroll down to the **Security** settings.
5. Clear the **Check for server certificate revocation** check box (this prevents checking HTTPS certificates).
6. Clear the **Check for publisher's certificate revocation** check box (this prevents checking digital signatures on downloaded programs and ActiveX controls).
7. Restart your computer.

The x64-bit version of Windows requires that all drivers be digitally signed; however, if you really want to install an unsigned driver onto an x64 version of Windows 8.1, you can. It requires you to reboot your machine and disable the driver signature enforcement feature. I have seen this workaround work perfectly fine for some users who needed to install Windows 7 drivers onto a Windows 8.1 PC, because they could not find signed drivers for the device they needed to install. Disabling the driver signature enforcement feature is not recommended, except when troubleshooting driver issues, and even then you should exercise caution.

Follow these steps to disable the driver signature enforcement.

1. Search for **PC Settings**.
2. Select **Update and Recovery**.
3. Select **Recovery**.
4. Under **Advanced startup**, select **Restart Now**.
5. On the **Choose an option** screen, select **Troubleshoot**.
6. Select **Advanced options**.
7. Select **Startup Settings**.
8. Select the **Restart** button.
9. On the **Startup Settings** screen (see Figure 3-3), press either the **F7** key or the number **7** key on your computer keyboard to allow Windows to boot.



Startup Settings

Press a number to choose from the options below:

Use number keys or functions keys F1-F9.

1) Enable debugging
2) Enable boot logging
3) Enable low-resolution video
4) Enable Safe Mode
5) Enable Safe Mode with Networking
6) Enable Safe Mode with Command Prompt
7) Disable driver signature enforcement
8) Disable early launch anti-malware protection
9) Disable automatic restart after failure

Figure 3-3. *Disabling Windows driver signature enforcement*

Windows boots with the Driver Signature Enforcement feature disabled, which allows you to install unsigned drivers.

Locating Quality Device Drivers

Most issues that I encounter relate to customers unable to find the appropriate drivers for their systems, often several years after the system was purchased. This can be compounded further if the OS has deviated from the updated OEM installation. Hardware and drivers are normally provided by the OEM when the device is purchased. If you buy a new system, there is normally a CD or DVD included in the box. It is good practice to label this media with the system information, such as purchase date and supplier, and to note the original OS that is installed. This forms the basis of a trusted and reliable starting point should you need to reinstall the system. On my own systems, I create an ISO backup of the driver installation media and then save it to the cloud.

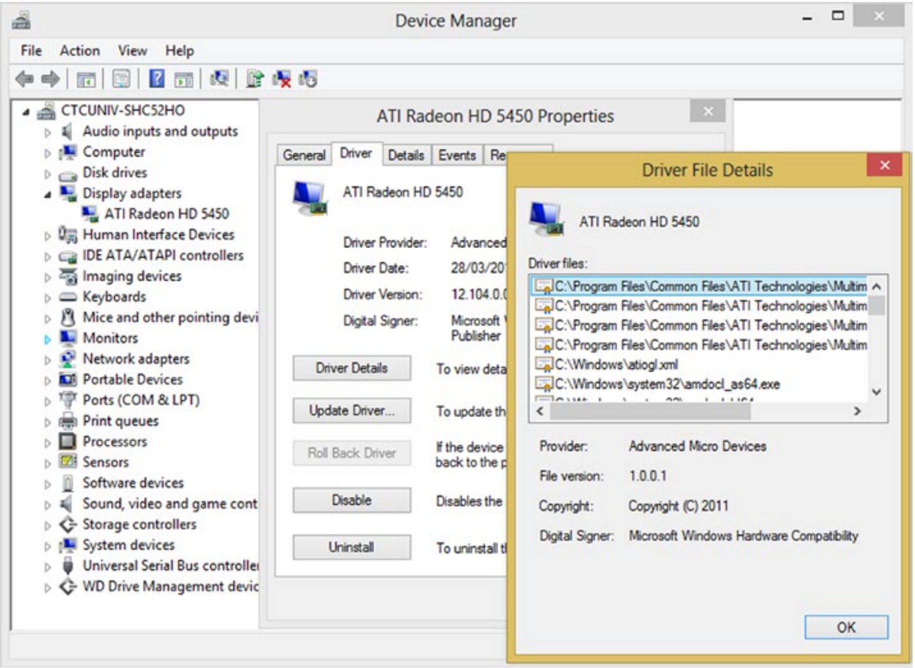
Windows XP through Windows 7 saw a period of OS stability, when there were only three operating systems spanning over a decade, and most systems used the x86 architecture. As users upgrade to newer hardware or upgrade the OS, they are frequently faced with trying to locate drivers that will reliably work with their devices. OEMs often only support hardware for a limited amount of time, which may be just a few years, especially if the OEM regularly updates their range of products. It is common that devices that are only a few years old can become “legacy” and that only the original drivers are available.

When troubleshooting Windows a crash, we often find that hardware driver files are the biggest culprit. So long as you can boot in Safe Mode, you should be able to disable rogue drivers, and if necessary, roll back to an earlier working version.

To locate the driver files associated a specific piece of hardware, you should use the Device Manager applet in Windows, which is extremely good at reporting all the files associated with a specific driver. To access this information, follow these steps:

1. Open **Device Manager**.
2. Select the hardware type.
3. Right-click the hardware device.
4. Click the properties.
5. On the **Driver** tab, click the **Driver Details** button.

Each file is listed with the file name and path, as shown in Figure 3-4.



Driver Provider: Advanced
Driver Date: 28/03/20
Driver Version: 12.104.0.0
Digital Signer: Microsoft
Publisher

Driver files:

C:\Program Files\Common Files\ATI Technologies\Multim
C:\Program Files\Common Files\ATI Technologies\Multim
C:\Program Files\Common Files\ATI Technologies\Multim
C:\Program Files\Common Files\ATI Technologies\Multim
C:\Windows\atiogl.xml
C:\Windows\system32\amdocl_as64.exe

Provider: Advanced Micro Devices
File version: 1.0.0.1
Copyright: Copyright (C) 2011
Digital Signer: Microsoft Windows Hardware Compatibility

__Figure 3-4.__ Displaying hardware device driver files

■ **Note** You must be logged on as an administrator to make any changes to device settings in Device Manager.

If you are unable to locate drivers via installation media, Windows Update, or from the OEM web site, you may be able to copy and use the actual driver files from another functional system.

Within a corporate environment, it is common practice to bundle the device driver files into Windows image deployments, so that if a PC needs to be reinstalled with the corporate image, a freshly imaged machine contains all the correct drivers upon first boot. These driver files are copied to and maintained on the Windows Deployment Services server (WDS) on the network.

Being able to easily locate drivers within Windows can be a lifesaver. Within Device Manager you are also able to verify the file version and name of the driver, which is then useful to help if you are comparing specifications and trying to establish if you have the latest version.

If you need to manually install a device, you should always install the driver prior to connecting the device to the computer. Windows provides a command-line tool, `pnputil.exe`, which when run with administrative privilege, adds a driver manually to the Windows driver store.

The syntax for `pnputil.exe` is as follows:

```
pnputil.exe [-f | -i] [ -? | -a | -d | -e ] <INF name>
```

The parameters available for `pnputil.exe` are listed in Table 3-1.

Table 3-1. *Available Parameters for pnputil.exe*

Parameter	Description
`-a`	Add the identified INF file.
`-d`	Delete the identified INF file.
`-e`	Enumerate all third-party INF files.
`-f`	Force the deletion of the identified INF file. Cannot be used with the `-i` parameter.
`-i`	Install the identified INF file. Cannot be used in conjunction with the `-f` parameter.
`/?`	Displays help.

As you can see from the syntax in Table 3-1, `pnputil` can be used to add or remove driver packages, and also list driver packages that are currently in the store, which is stored in the `C:\Windows\System32\DriverStore` folder.

To list all of the third-party drivers in the driver store in a text file, open an administrative command prompt and type **`pnputil -e >C:\drivers.txt`**.

Maintaining Legacy Hardware

In an ideal situation, you avoid mixing new and old components; it is generally not good practice. However, not all users are able to upgrade their PCs and peripherals at the same time, primarily due to cost, but also equipment has varying service lifetimes that often do not expire at the same time.

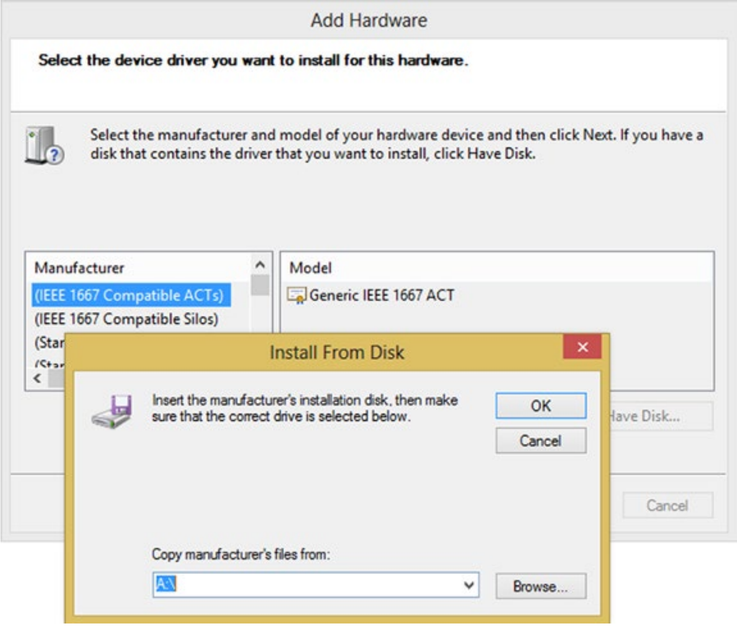
I have clients who continue to use equipment that is 20 years old and still serviceable. There are several issues with using an old peripheral—such as a dot matrix printer or a flatbed scanner—on new PC hardware; these issue include locating and installing drivers, .NET application compatibility, hardware interface support, and consumable supply.

When faced with needing to install older hardware onto new PCs, it may become necessary to locate legacy drivers, as it is unlikely that a modern OS will maintain support for equipment older than five or ten years. When Windows Vista was first released, I saw a poster that declared that Vista included driver support for 1 million devices. Unfortunately, the major barrier to the widespread adoption of Vista during its first year was poor driver availability for legacy devices.

PnP support for peripherals is usually achieved by attaching the peripheral via a USB cable. Modern devices often now connect via Wi-Fi or Bluetooth. However, for older devices, this may not be available; they have legacy connections such as parallel, serial, and COM ports, which are generally now obsolete. Inexpensive adaptor expansion cards are available from specialized components suppliers.

Sometimes a driver that Windows automatically installs creates a problem. To manually install a driver for a device that you do not want the default PnP driver, or if the device is non-PnP, you should use the Add Hardware wizard (see Figure 3-5) by following these steps:

1. Open **Device Manager**.
2. Select the computer name at the top of the Device Manager.
3. Click **Action** from the Device Manager's menu bar and choose **Add legacy hardware** from the drop-down menu.
4. The Add Hardware wizard appears.
5. Click **Next**.
6. Select the **Install the hardware that I manually select from a list** option.
7. Click **Next**.
8. Click **Show all devices** in the list box, and then click **Next**.
9. Click **Have Disk**.
10. In the **Install From Disk** dialog box, enter the directory path of the driver files that you want to install.
11. Click the **.inf** file, and then click **Open**.
12. Click **OK**.
13. Click **Next** twice, and then click **Finish** to complete the installation.



Add Hardware

Select the device driver you want to install for this hardware.

Select the manufacturer and model of your hardware device and then click Next. If you have a disk that contains the driver that you want to install, click Have Disk.

Manufacturer: (IEEE 1667 Compatible ACTs), (IEEE 1667 Compatible Silos), (Star, (Star

Model: Generic IEEE 1667 ACT

Install From Disk

Insert the manufacturer's installation disk, then make sure that the correct drive is selected below.

Copy manufacturer's files from: A:\

Figure 3-5. *Using the Add Hardware wizard to install non-PnP devices*

If you prefer to use the command prompt, you can start the Add Hardware wizard by typing **Hdwwiz.exe**.

Should you have legacy hardware, it is also possible to purchase a USB cable that will allow the connection to be achieved.

Figure 3-6 shows a USB to parallel port connector, which can be used with a legacy printer that does not offer USB support.

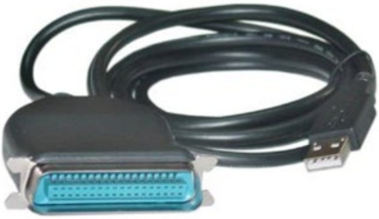


Figure 3-6. *USB to parallel port printer adapter cable*

Managing Devices

All external PnP devices that are added to a computer should automatically appear in Devices and Printers.

The following types of devices are listed in Devices and Printers:

- Portable devices, such as mobile phones, portable music players, and digital cameras
- USB connected devices, such as external USB hard drives, flash drives, webcams, keyboards, and mice
- All printers connected to your computer, whether connected by USB cable, the network, or wirelessly
- Wireless devices, including Bluetooth and wireless USB devices
- Your computer
- Network devices such as network-enabled scanners, media extenders, or network-attached storage (NAS) devices

Each installed device is represented by a photo-realistic image of the device, as shown in Figure 3-7.

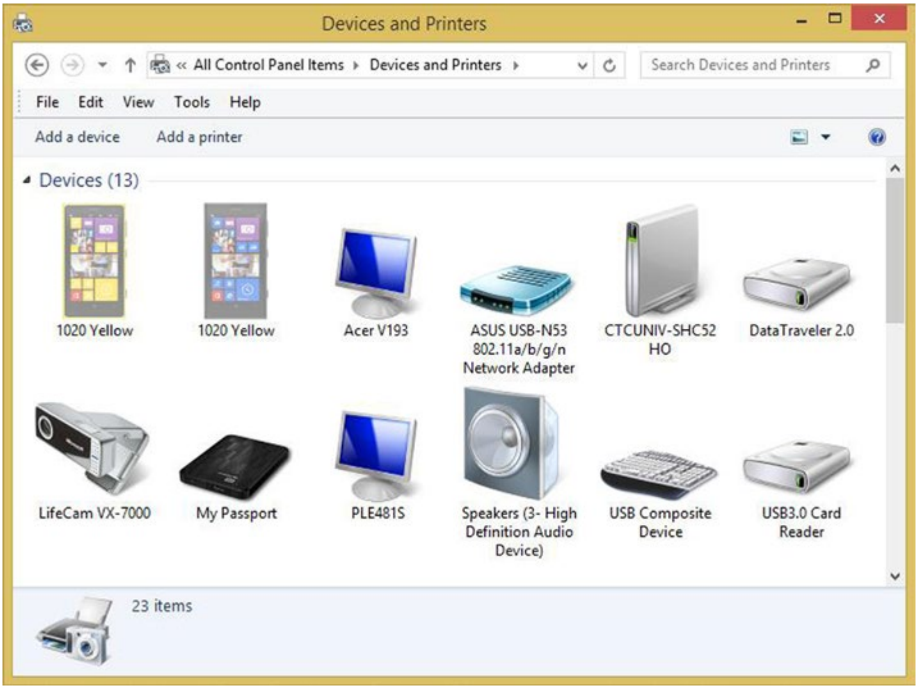
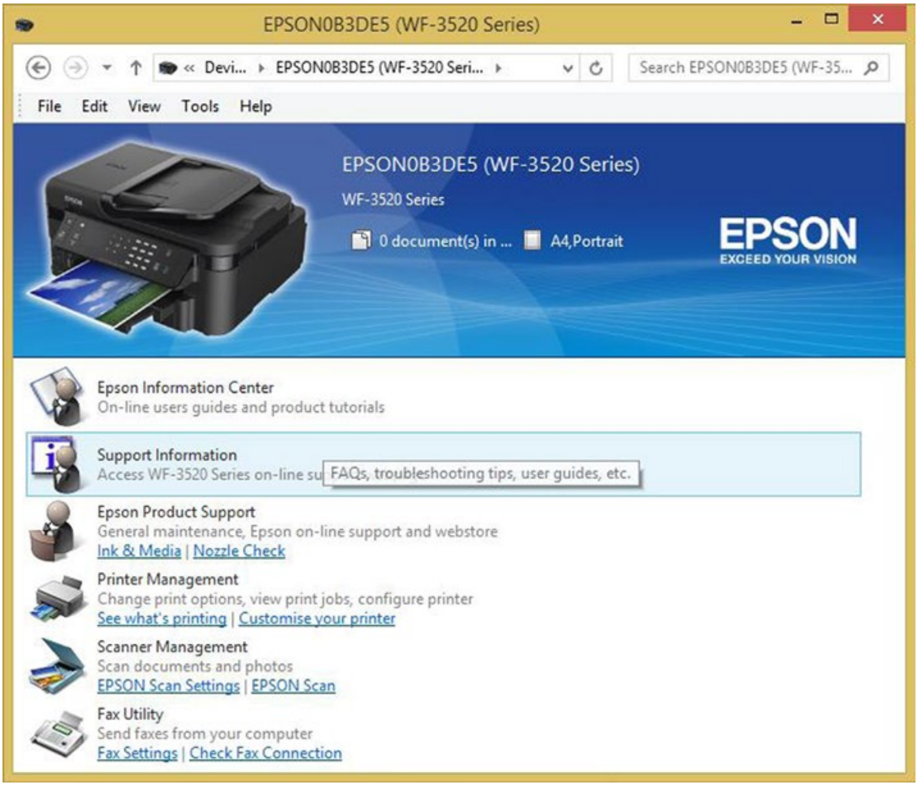


Figure 3-7. *Viewing devices in Devices and Printers*

If you cannot find a device listed in Devices and Printers, you should look in Device Manager.

■ **Note** Devices and Printers is not a replacement for Device Manager and it does not display every device. It does not show internal hard drives, disc drives, sound cards, video cards (graphics cards), memory (RAM), processors, speakers connected via conventional speaker wires, or devices that use a PS/2 or serial port, such a mouse or a keyboard.

If you right-click a device icon within Devices and Printers, you can select from a list of device tasks related to the capabilities of the device. For example, you might be able to browse to files on an attached storage device, play music from a media player, or view a printer's print jobs. In addition to the right-click functionality, some modern devices that support the new Device Stage feature in Windows allow you to double-click the device to open advanced, device-specific features (see Figure 3-8).



EPSON0B3DE5 (WF-3520 Series)

« Devi... ▸ EPSON0B3DE5 (WF-3520 Seri... ▸

Search EPSON0B3DE5 (WF-35...

EPSON0B3DE5 (WF-3520 Series)
WF-3520 Series
0 document(s) in ... A4,Portrait

Epson Information Center
On-line users guides and product tutorials

Support Information
Access WF-3520 Series on-line su FAQs, troubleshooting tips, user guides, etc.

Epson Product Support
General maintenance, Epson on-line support and webstore
Ink & Media | Nozzle Check

Printer Management
Change print options, view print jobs, configure printer
See what's printing | Customise your printer

Scanner Management
Scan documents and photos
EPSON Scan Settings | EPSON Scan

Fax Utility
Send faxes from your computer
Fax Settings | Check Fax Connection

Figure 3-8. *Device Stage view*

Managing Printers

Within a business environment, nearly all users need to print from time to time. Administrators can preinstall printers onto a computer using Group Policy Preferences or use legacy logon scripts. There are several ways in which a user can add a printer to their device. The method that I really like (because it is very intuitive and easy for the user to understand) is to browse within File Explorer to the networked printer (or to the computer, if it is attached to a computer) and then install the printer simply by right-clicking the shared printer icon and selecting Connect (see Figure 3-9).

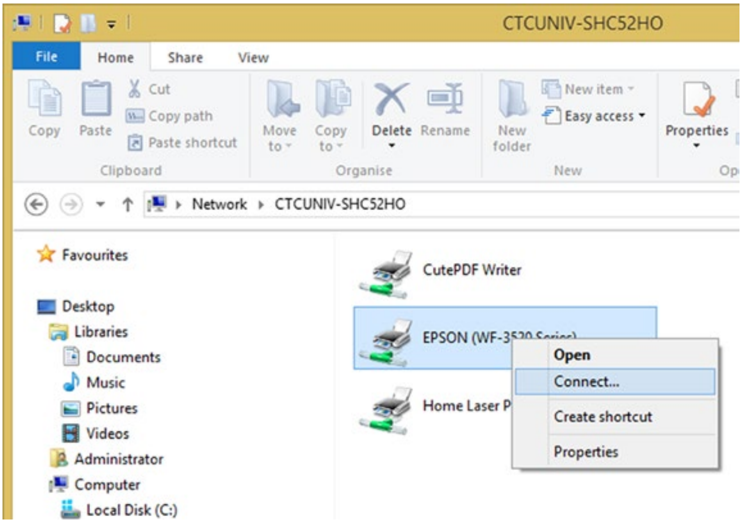
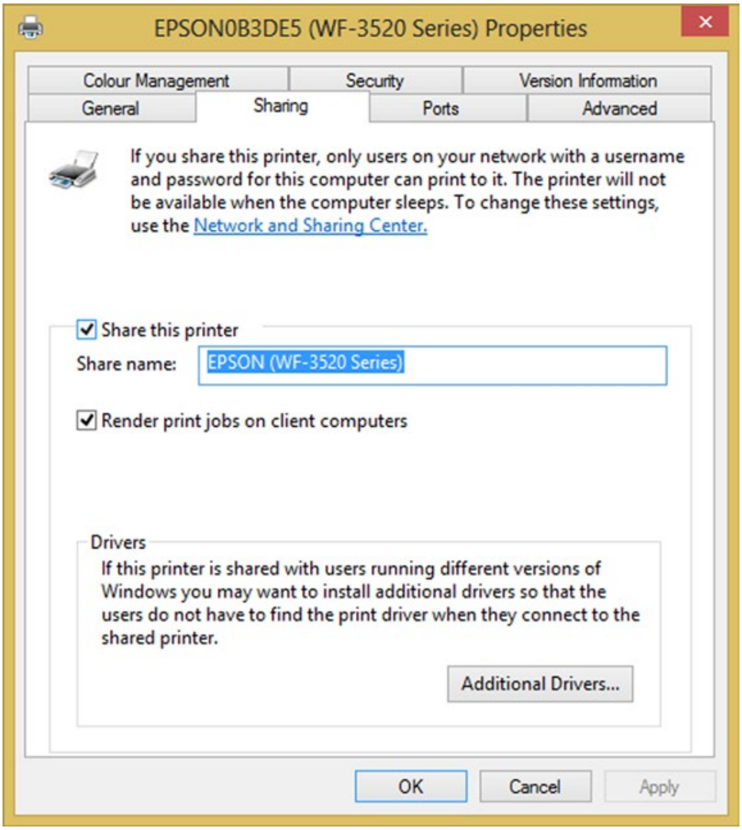


Figure 3-9. *Connecting to a shared printer using File Explorer*

If the printer is not displaying, you should make sure that it is available for sharing. This can be checked on the sharing PC by opening the printer properties and checking that the **Share this printer** check box is selected, as shown in Figure 3-10.



If you share this printer, only users on your network with a username and password for this computer can print to it. The printer will not be available when the computer sleeps. To change these settings, use the Network and Sharing Center.

☑ Share this printer

Share name: EPSON (WF-3520 Series)

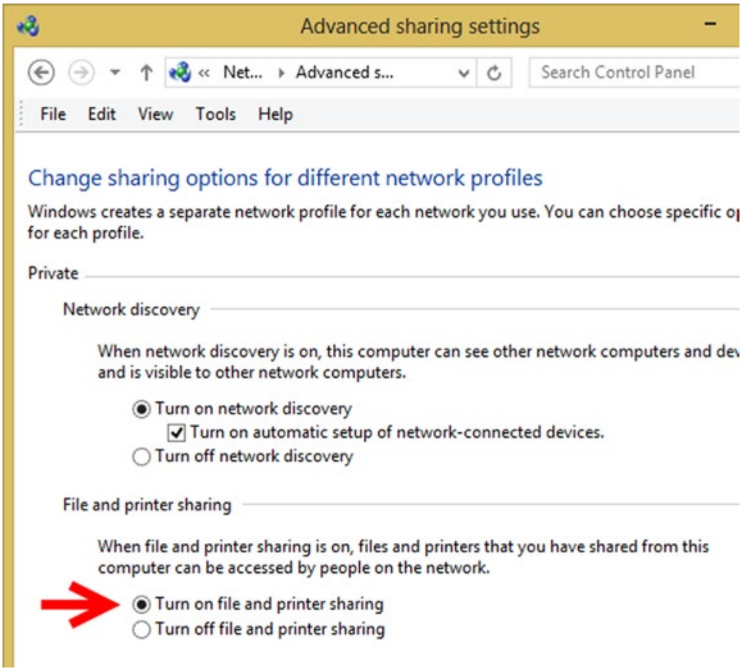
☑ Render print jobs on client computers

Drivers

If this printer is shared with users running different versions of Windows you may want to install additional drivers so that the users do not have to find the print driver when they connect to the shared printer.

Figure 3-10. *Sharing a printer over the network*

If the printer is still not displaying, you should make sure that **File and printer sharing** has been enabled within the **Advanced sharing settings**, which is found in the Network and Sharing Center (see Figure 3-11).



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific o
for each profile.

Private

Network discovery

When network discovery is on, this computer can see other network computers and dev
and is visible to other network computers.

● Turn on network discovery
☑ Turn on automatic setup of network-connected devices.
○ Turn off network discovery

File and printer sharing

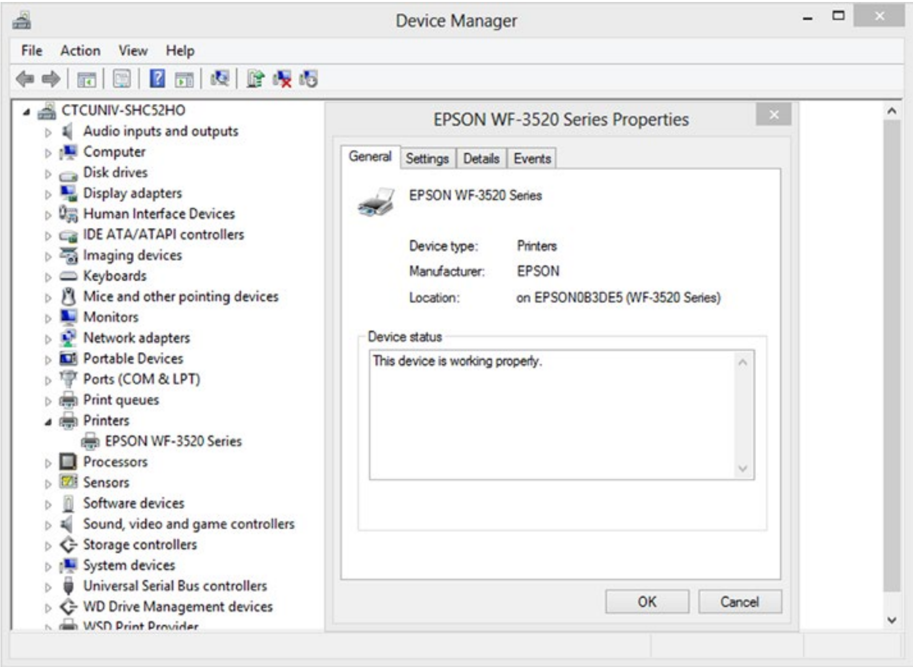
When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

Figure 3-11. *Enabling file and printer sharing*

When configuring or troubleshooting devices, a feature that I very much like offers the ability to revert a device to use a previously installed driver, without the need to manually reinstall the driver. This feature is called Driver Rollback; it works unless you used the device uninstaller to remove the previous driver.

Unfortunately, it is not possible to use Driver Rollback within Device Manager for a printer driver. Printers do not support driver rollback (see Figure 3-12).



EPSON WF-3520 Series

Device type: Printers

Manufacturer: EPSON

Location: on EPSON0B3DE5 (WF-3520 Series)

Device status

This device is working properly.

Figure 3-12. *Driver Rollback is not available for printers*

If you want to change or update a driver for an installed printer, perform the following steps:

1. Search for **Print Management** and open the **Print Management MMC**.
2. In the left pane, click **Print Servers**, click the applicable print server, and then click **Printers**.
3. In the center pane, right-click the printer with the driver that you want to change or update, and then click **Properties**.
4. Click the **Advanced** tab.
5. Select a new driver from the **Driver** box, or click **New Driver** to install a new printer driver.

If you need to troubleshoot a printer, you should locate the device within **Devices and Printers**, and then right-click the icon and select **Troubleshoot**, which launches the printer troubleshooting wizard.

The Windows built-in troubleshooters are quite advanced. Windows 8.1 automatically performs many checks on a device before presenting you with potential issues that may need to be resolved. The printer troubleshooter checks the following issues:

- Whether the printer is the default printer
- Whether the printer is shared
- Whether the printer is out of paper
- Whether the printer is out of toner or ink
- Whether the printer has a paper jam
- Whether the printer driver requires an update
- Whether the PnP driver is working
- The network/USB connectivity
- Whether the printer is turned on/off
- Whether the print spooler service is experiencing problems or not running
- Whether a print job in the print queue is preventing other jobs from printing

Hopefully, you agree that the printer troubleshooter offers quite a comprehensive list of tasks.

During consulting visits, I often recommend that the helpdesk advise their end users to first try to resolve problems by using the built-in troubleshooters. In most situations, this can reduce operational downtime and speed up the problem resolution.

Video and Graphics Cards

Video and graphic cards deserve a special mention due to their specialized nature. For many corporate customers, the bundled or onboard graphics card shipped with the PC is normally adequate for everyday use. However, for a graphic artist, computer-aided design (CAD) technician, gamer, or PC hobbyist, the graphics card can be a very expensive component—second only to the processor. Most gamers require a 3D graphics processing unit (GPU) with HD or 4K performance, whereas for the average business user, this is unimportant. The development of advanced graphics cards has accelerated over the last decade. Today, high-end graphics cards, such as the EVGA GeForce GTX Titan X (see Figure 3-13) cost in excess of $1,000 and allow the serious gamer to game on large-monitor displays at super-fast frame rates in full 4K surround.

Figure 3-13. *The water-cooled EVGA GeForce GTX Titan X Hybrid graphics card*

Due to the complex and advanced nature of graphics cards, it is essential that device drivers are sourced only directly from the OEM and that they are carefully installed in accordance with the OEM instructions.

The PDF instructions for the EVGA GeForce GTX Titan X card (shown in Figure 3-13) that accompanies the latest drivers is a whopping 54 pages in length.

Gaming graphics card drivers are updated quite frequently so that the cards remain compatible with the latest new games as they are released. Games designers and developers are in a constant competition with each other to attract gamers, hoping that they will favor their game, which keeps pushing the boundaries of realism on screen.

For more modest display adaptors and graphics cards, it is still essential that the correct driver version is installed so that the display is optimally rendered. Whenever I build or service a PC, I always make a note on the rear case of the exact model of the graphics card, so that if I need to reinstall the driver, I am able to exactly match the card model to the list of graphic card device drivers on the OEM web site without needing to remove the case cover and inspect the card or locate the original packaging or instructions.

The two largest producers of PC video graphics cards are NVIDIA and ATI. Through a process of yoking together multiple video adapters to provide higher graphics performance, gamers were able to purchase two lower-valued cards that would outperform a single higher-priced adaptor. (NVIDIA named their yoking technology Scalable Link Interface (SLI), whereas ATI's is called CrossFireX).

Since Windows Vista, all video cards drivers must support the Windows Display Driver Model (WDDM) architecture. Windows Vista supported WDDM version 1.0 and required at least Direct3D 9–capable video cards. Each subsequent version of Windows supports additional WDDM features, with Windows 10 expected to support WDDM 2.0, which allows more offloading from the CPU to the GPU.

Summary

Locating and installing the correct (an often the latest) device drivers are an essential component in keeping your system in good running order. Windows regularly attempts to locate the latest drivers as part of the built-in automatic updating. When a driver fails to perform optimally, you are able to perform a driver rollback to revert the driver to the previous one.

As you saw in Chapter 2, a corrupt or incorrect device driver creates an unstable system, resulting in frequent system crashes and BSOD, which can cause data loss and other failures due to the increased frequency of system power-cycling.

In Chapter 4 you will look at the types of software compatibility issues that can affect applications running on Windows, and the tools that are available to mitigate these issues and maintain compatibility.

CHAPTER 4

Resolving Software Compatibility Issues

Whenever there is a new version of Windows launched, there are typically some issues that relate to ensuring backward compatibility. Most software is supported by the independent software vendor (ISV) for the specified lifespan of the software, which could also be aligned to one or more host operating system platforms. For example, Office 2003 was released by Microsoft in October 2003; it was compatible with Windows 2000 and supported on Windows XP and later. Mainstream support for Office 2003 ended on April 14, 2009, and extended support was terminated on April 8, 2014.

Each ISV determines the lifespan of its software, and each software version is designated a version number, date, or name. Version changes can be a result of new functionality, bug fixes, or new security features incorporated into the software. Most customers accept that new features accompany a new version, and therefore they choose to upgrade based on the desirability or the need to use these features. Most customers become frustrated when a perfectly workable version of the software that they use becomes unsupported or end-of-life (EOL) in an effort by the ISV to force an upgrade or change on the customer.

Changing software can also present a financial headache for businesses. New software typically incurs a cost to the business in terms of purchasing new software licenses and providing training for both end-user and support staff. It is common that newer software can deliver higher performance gains, but often this requires new hardware, such as a faster processor, more memory, or faster GPU to support more pixels or multiple screens support.

Businesses need to balance the costs of buying newer versions of software vs. the risks of remaining on older software. This is true for both the OS and the applications. An old application is potentially vulnerable to malicious attacks if it is no longer supported and adequately patched by the ISV.

Ultimately, the most common issue that you see with software compatibility is where an application that a user is entirely happy with, and has no operational need to change or to upgrade, no longer works on a new computer or new OS.

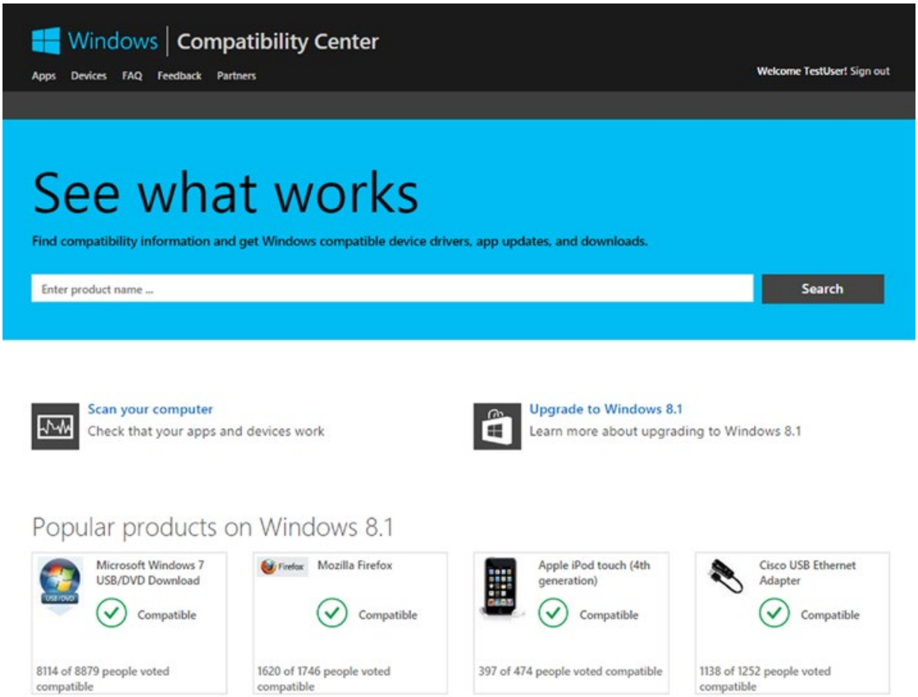
In this chapter you explore and learn how to use Windows built-in tools, and a few external tools, to mitigate against the disruption and headaches that you might face when dealing with software changes.

M. Halsey and A. Bettany, *Windows Software Compatibility and Hardware Troubleshooting*,
DOI 10.1007/978-1-4842-1061-1_4

Windows Compatibility Center Web Site

Microsoft has created a new web site for users to find compatibility information, Windows-compatible device drivers, applications updates, and downloads. This web site also scans the user's computer to check which applications work properly.

The Compatibility Center (see Figure 4-1) is located at https://www.microsoft.com/en-us/windows/compatibility/CompatCenter/Home. It replaces the Windows-compatible hardware and software web site that was very popular during the migration from XP to Vista in 2007.



See what works

Find compatibility information and get Windows compatible device drivers, app updates, and downloads.

Scan your computer
Check that your apps and devices work

Upgrade to Windows 8.1
Learn more about upgrading to Windows 8.1

Popular products on Windows 8.1

Microsoft Windows 7 USB/DVD Download
Compatible
8114 of 8879 people voted compatible

Mozilla Firefox
Compatible
1620 of 1746 people voted compatible

Apple iPod touch (4th generation)
Compatible
397 of 474 people voted compatible

Cisco USB Ethernet Adapter
Compatible
1138 of 1252 people voted compatible

Figure 4-1. *Windows Compatibility Center*

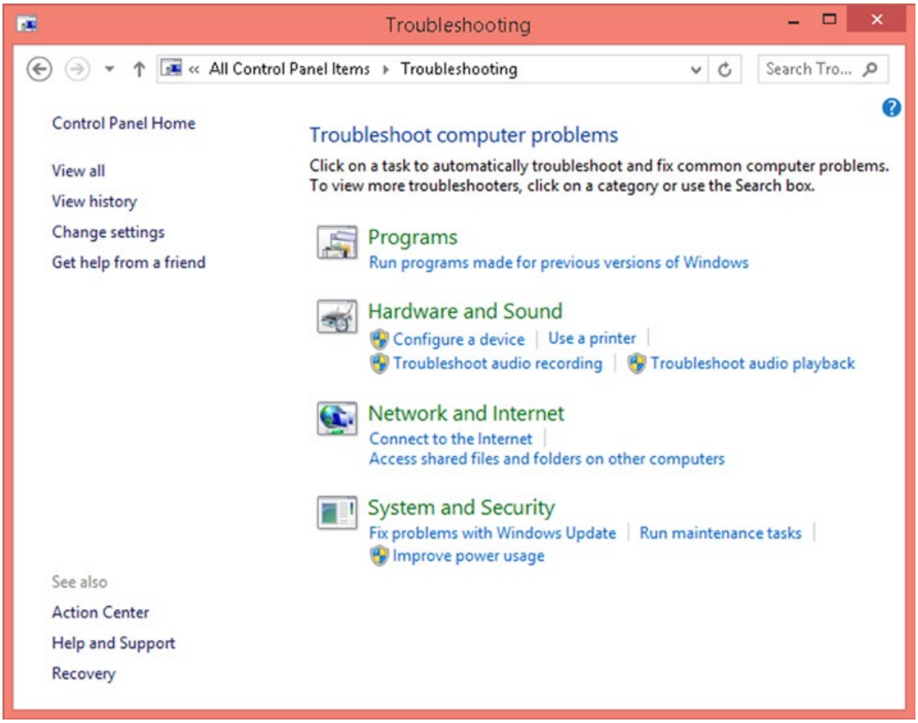
The Compatibility Center is designed to allow end users and enthusiasts to perform automated system scans of all the hardware and software on their devices, and then produces a report that details which applications and devices work with the latest version of Windows.

The Software Compatibility Troubleshooter

Most applications designed for Windows 7 and earlier versions work automatically on Windows 8.1 and newer. However, when an older program fails to work properly on your current OS—for example, it runs slowly or not at all—you should attempt to resolve the problem by using the Program Compatibility troubleshooter, which runs the software while simulating the behavior of an earlier version of Windows. Often this relatively simple process can resolve the problem and allow the program to run.

You can open the troubleshooting tool by following these steps:

1. Open the **Control Panel**.
2. Under **System and Security**, click **Find and fix problems**.
3. Within the **Troubleshooting** screen, click **Run programs made for previous versions of Windows** (see Figure 4-2).



Troubleshoot computer problems

Click on a task to automatically troubleshoot and fix common computer problems. To view more troubleshooters, click on a category or use the Search box.

Figure 4-2. *Using the built-in program compatibility troubleshooter*

4. On the **Program Compatibility Troubleshooter** screen, click **Next**.
5. Select the program that is having problems, and then click **Next**.
6. Once Windows has modified the settings, click the **Try recommended settings to run the application using the recommended compatibility settings** option.
7. Click **Test the program**.
8. Once the program opens, you should evaluate to see if the problems still occur.
9. Close the program and return to the troubleshooting wizard. Click **Next**.
10. Choose one of the following three options, or click **Cancel** to abort the process:
    a. Yes, save these settings for this program
    b. No, try again using different settings
    c. No, report the problem to Microsoft and check online for a solution
11. If the program behaved correctly, you should click **Yes**. The troubleshooting is complete. Click **Close** to close the troubleshooter.

Chapter 2 discussed how UAC can cause issues with legacy applications that were written before UAC was commonplace, or when the application expects to run with administrative credentials.

The Program Compatibility Troubleshooter wizard also allows you to test the operation of the program as an administrator by running the program using administrative credentials. To run the program in this way, click the **Advanced** option on the Program Compatibility Troubleshooter main screen. Select **Run as administrator**. At the UAC prompt, you can be either an administrator or provide administrative credentials. The Program Compatibility Troubleshooter wizard then leads you through the same option screens as before.

If you clear the **Apply repairs automatically** check box when using the Advanced option on the troubleshooter, it displays a list of the possible fixes, which you can choose from if any are found.

■ **Note** You should be careful when allowing the Program Compatibility Troubleshooter to run the program using administrative credentials, unless you are completely sure that this is the issue, or if the ISV has advised that this is an approved compatibility workaround.

If the **Try recommended settings** do not work, you should rerun the Program Compatibility Troubleshooter; but this time, select the **Troubleshoot program** option. Follow the wizard again and work through a number of scenarios, such as

- The program expects to run on a previous OS, such as Windows 8, 7, Vista SP2, or XP SP3.
- The program needs additional permissions to run, such as an administrator.
- The program needs a different display environment, such as reducing the resolution or DPI scaling.

The wizard also offers a combination of these scenarios. Frustratingly, the wizard does not allow you to go backward—if you make an incorrect selection, you need to cancel and rerun the wizard.

In addition to the troubleshooter, you can also configure compatibility settings directly on the application by using the Compatibility tab found in the application's properties.

1. Locate the application executable or the application's shortcut within **File Explorer** (from the **Start** screen, right-click the application tile and select **Open file location**).
2. Right-click the application executable or the application's shortcut, and then click **Properties**.
3. On the **Compatibility** tab, select the settings you want to modify and click **OK**.
4. Rerun the application. Determine if the fix worked.

Using the compatibility setting directly on the application allows you to configure additional settings; for example, you could do the following:

- Reduce the display
- Force the application to run in a 640 × 480 screen resolution
- Apply the application fixes to all users on the computer

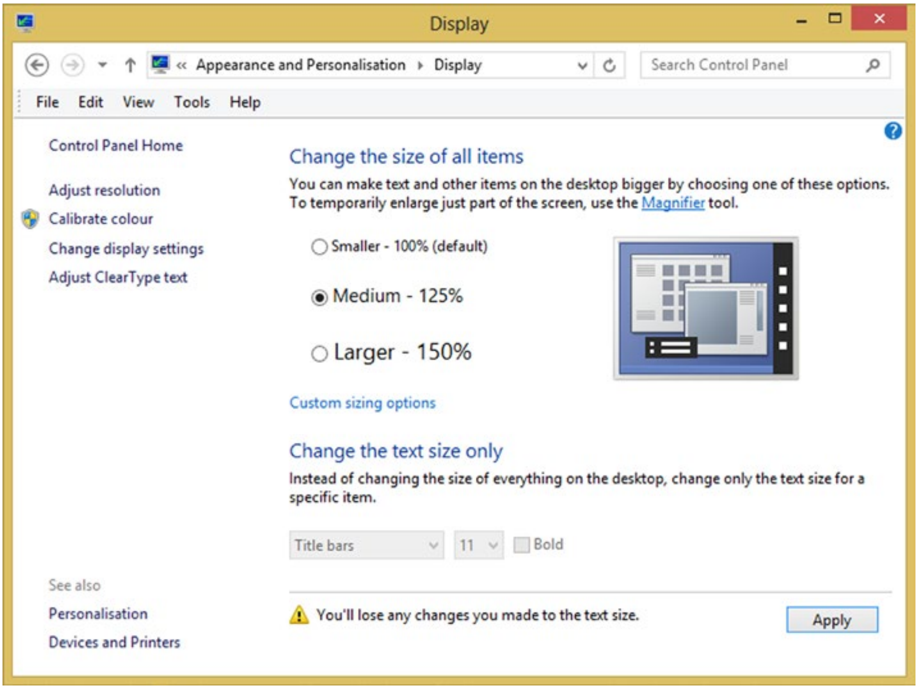
You can also launch the Program Compatibility Troubleshooter from within the Compatibility tab.

■ **Note** You should be careful when using the Compatibility tab rather than the Troubleshooter, because this method does not offer any recommendations on how to fix problems with an application. An inexperienced user could potentially make configuration settings that are harmful to the computer.

DPI Scaling

If you are using a Surface or Ultrabook, you may notice that these new devices have extremely high screen resolutions. By default, Windows scales the screen to magnify the size of text and other items on the screen so that they appear larger and are easier to view. You can modify this by launching the display utility directly by typing **dpiscaling.exe** in the Start screen, or it can be run from the Control Panel by performing the following steps:

1. Open the **Control Panel**.
2. Click **Appearance and Personalization**.
3. Within the **Display** section, click **Make text and other items larger or smaller**.
4. On the **Display** screen (see Figure 4-3), change the size setting as required, and then click **Apply**.



Change the size of all items

You can make text and other items on the desktop bigger by choosing one of these options. To temporarily enlarge just part of the screen, use the Magnifier tool.

○ Smaller - 100% (default)

● Medium - 125%

○ Larger - 150%

Change the text size only

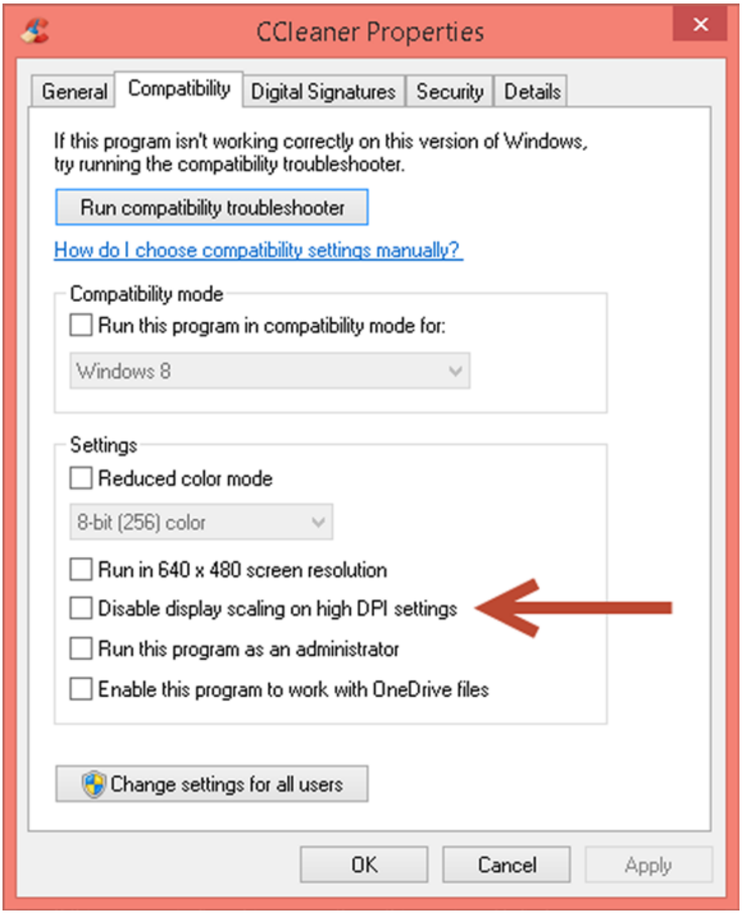
Instead of changing the size of everything on the desktop, change only the text size for a specific item.

Title bars 11 □ Bold

You'll lose any changes you made to the text size.

__Figure 4-3.__ Modifying DPI scaling global setting

These settings are stored within the user account profile on a per-user basis. Some applications may struggle with the DPI scaling. You may need to disable display scaling either for the whole computer using the dpiscaling.exe utility or just for that particular application. A per-application modification can be achieved by selecting the **Disable display scaling on high DPI settings** on the Compatibility tab, as shown in Figure 4-4.


CCleaner Properties
General
Compatibility
Digital Signatures
Security
Details
Run compatibility troubleshooter
How do I choose compatibility settings manually?
Change settings for all users
OK
Cancel
Apply

If this program isn't working correctly on this version of Windows, try running the compatibility troubleshooter.

Compatibility mode

□ Run this program in compatibility mode for:

Windows 8

Settings

□ Reduced color mode

8-bit (256) color

□ Run in 640 x 480 screen resolution

□ Disable display scaling on high DPI settings

□ Run this program as an administrator

□ Enable this program to work with OneDrive files

Figure 4-4. *Modifying DPI scaling global setting*

Program Compatibility Assistant

Windows 8 introduced a new feature called the Program Compatibility Assistant (PCA), which aims to help end users run desktop applications that worked in earlier Windows versions but have difficulty on Windows 8.1 and newer.

Windows 8.1 includes three compatibility modes that represent the most common scenarios:

- Windows XP SP3
- Windows Vista SP2
- Windows 7

PCA works by tracking when a user runs an application and identifies whether there are any symptoms of certain known compatibility issues present during the operation. If PCA detects any issue symptoms, it advises the user with information so that they can chose to apply a suggested fix that will help the application run better.

Once the application fix is applied, the PCA monitors the operation of the application once more to verify that the fix worked; if the fix failed, it is reverted and PCA stops monitoring the failing application.

The following are some of the most common scenarios that PCA monitors:

- The app fails to install or uninstall
- The app fails to launch due to administrative privilege
- The app fails while attempting to modify Windows files
- The app fails due to unsigned drivers on 64-bit Windows 8

A list of all the scenarios that PCA tracks and recommends fixes for is at https://msdn.microsoft.com/en-us/library/windows/desktop/hh994464(v=vs.85).aspx.

Microsoft Application Compatibility Toolkit

The Program Compatibility Troubleshooter is ideal for resolving compatibility issues for a small number of applications. It is a useful tool for the help desk or enthusiast tackling ad hoc issues. However, enterprises seeking to migrate at scale (such as resolving hundreds or even thousands of applications) need to have a systematic and industrial tool to tackle the problem.

For larger organizations, Microsoft provides an enterprise tool called Microsoft Application Compatibility Toolkit (ACT), which covers all the tasks required to solve most compatibility issues within a large business.

When faced with a large amount of compatibility testing, it is best practice to make an inventory of which applications are prevalent on the systems, and then triage the applications into categories that indicate priority, usage frequency, scale of usage, desirability to keep, value to the organization, cost to replace, modern variants, and available alternatives.

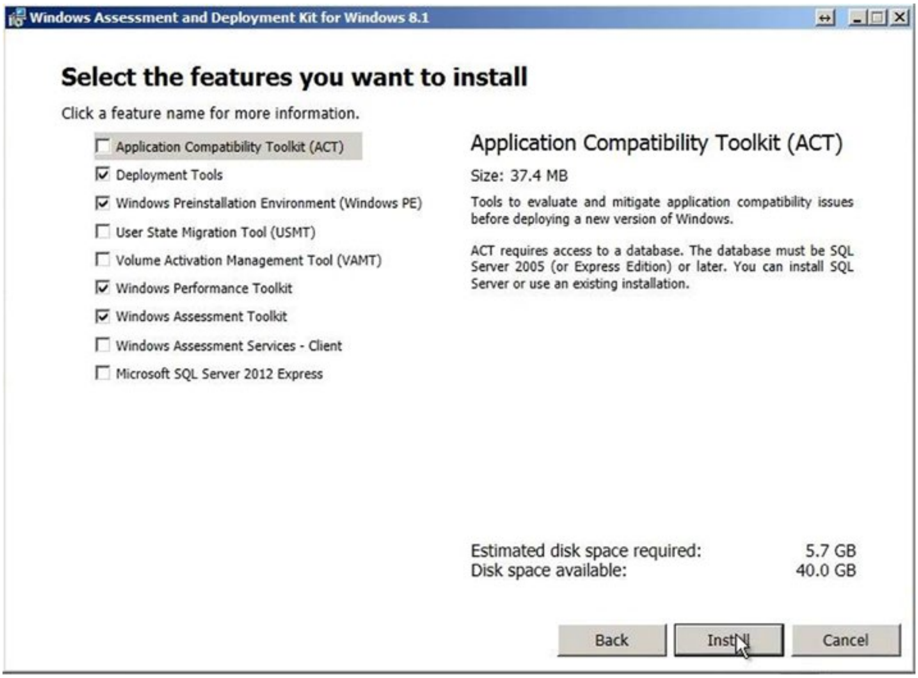
ACT allows the IT pro to focus on the following areas of application compatibility:

- Extensive data collection and application inventory
- Analysis of data collected
- Suggested remediation steps for known application compatibility issues
- The application of common compatibility fixes
- Review and repair issues relating to user account privilege issues

ACT is a free toolkit downloadable from the Microsoft Download Center. It is part of the Windows Assessment and Deployment Kit (Windows ADK) for Windows 8.1 Update. It is available at https://www.microsoft.com/en-us/download/details.aspx?id=39982. The full Windows ADK is approximately 5.7GB; the ACT component just 37.4MB.

ACT requires either a full version of SQL Server or SQL Server Express to hold the application inventory database that is generated during the process. Unless you already have SQL Server, I suggest using the latest free version, such as SQL Server Express 2014, as it is more stable than SQL Server Express 2012.

You can deploy the SQL Server and the ACT database onto a server OS, (for scalability), as shown in Figure 4-5.



Windows Assessment and Deployment Kit for Windows 8.1

Select the features you want to install

Click a feature name for more information.

- ☐ Application Compatibility Toolkit (ACT)
- ☑ Deployment Tools
- ☑ Windows Preinstallation Environment (Windows PE)
- ☐ User State Migration Tool (USMT)
- ☐ Volume Activation Management Tool (VAMT)
- ☑ Windows Performance Toolkit
- ☑ Windows Assessment Toolkit
- ☐ Windows Assessment Services - Client
- ☐ Microsoft SQL Server 2012 Express

Application Compatibility Toolkit (ACT)

Size: 37.4 MB

Tools to evaluate and mitigate application compatibility issues before deploying a new version of Windows.

ACT requires access to a database. The database must be SQL Server 2005 (or Express Edition) or later. You can install SQL Server or use an existing installation.

Estimated disk space required: 5.7 GB
Disk space available: 40.0 GB

Figure 4-5. *Installation of the Windows ADK*

You would then deploy the Inventory Collector onto the clients, or you can install all the Server components onto a Windows 8.1 machine, which is useful for testing purposes because this allows you to test the functionality of the tool without requiring a full client/server configuration. The installation is straightforward. You should create a new database for storing the data collected.

The key management interface of ACT is the Application Compatibility Manager (ACM), which holds the results of the investigations. To inventory the software that is being used across corporate client PCs and devices, you need to create a new Data Collection Package, which acts as a collection agent on each client. This can be either an inventory or runtime analysis package, as shown in Table 4-1.

Table 4-1. *Data Collection Package Types*

Package Type	Description
Inventory collection package	Automatically gathers a list of installed applications and device components from a PC
Runtime analysis package	Monitors applications when they are run

This is an MSI file that needs to be deployed to the client machines, which could be achieved using Group Policy, a shared folder, or another deployment method. For the duration of the monitoring, the collection agent runs silently, recording in detail which applications have been launched on each client. The collector also collects additional settings, such as whether an application required UAC elevation and whether any existing local application compatibility settings have been configured.

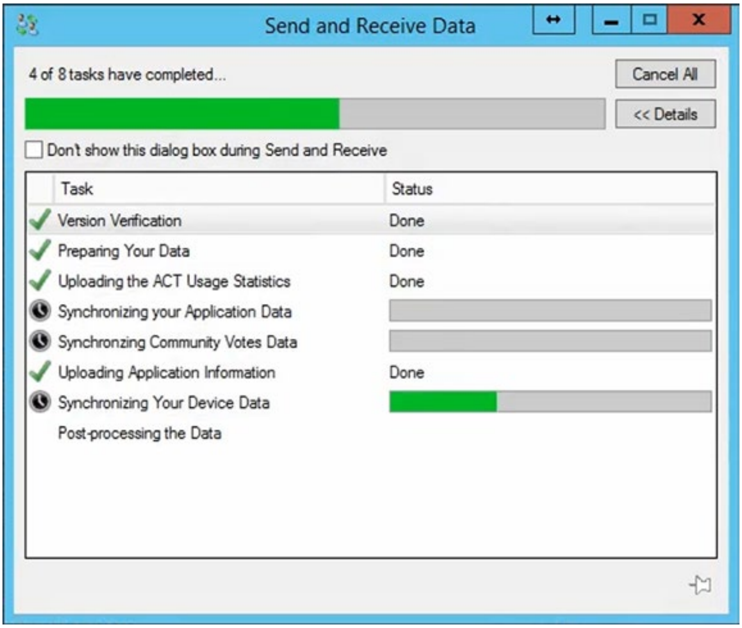
Within a corporate environment, you should configure the collector to operate over a three-day window (default), or even a month, depending on the number of applications that are likely to be present and the frequency of use. For example, if the organization only uses a special accounting utility to synchronize data from branch offices once a month, then you need to ensure that the collector runs for at least one month to capture the application data.

The collector syncs the data from the client back to a shared location logging area on the processing server, and the sync interval is configured.

■ **Note** One common glitch I have encountered with Window ACT is that sometimes the ACT Log Processing Service stops working soon after a reboot. A workaround for this is to replace the Local Service account with an Administrator account.

Once the data has been collected, the ACM displays an inventory of all the applications, version numbers, and vendor details that have been detected from all the computers under analysis.

The real power of the ACM tool comes when you click **Send and Receive** on the toolbar to share your collected data with Microsoft and then you retrieve information relating to your applications from Microsoft (see Figure 4-6).



4 of 8 tasks have completed...

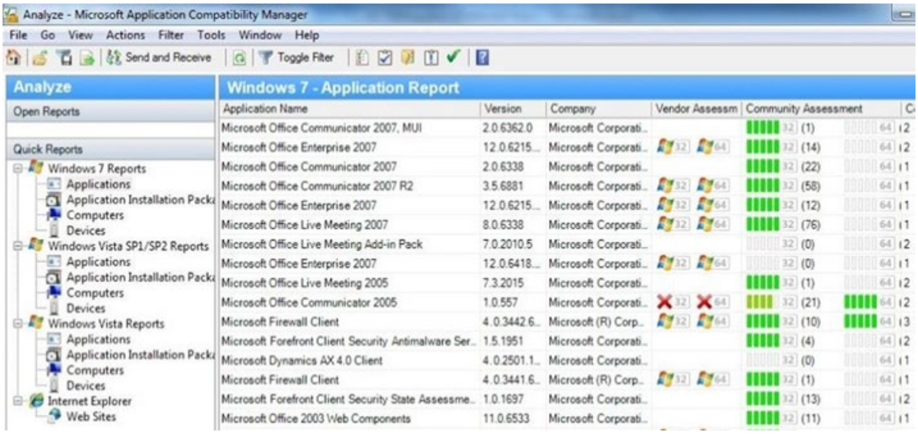
□ Don't show this dialog box during Send and Receive

Task	Status
✓ Version Verification	Done
✓ Preparing Your Data	Done
✓ Uploading the ACT Usage Statistics	Done
Synchronizing your Application Data	
Synchronzing Community Votes Data	
✓ Uploading Application Information	Done
Synchronizing Your Device Data	
Post-processing the Data	

***Figure 4-6.** Sending application collection data to Microsoft*

In return for sharing your data, you gain access to their huge application database, which is built from vendors and other companies performing the same task as you.

Once the sync is complete, you have a rich report (see Figure 4-7) that shows which of the applications are compatible and how any issues may be resolved.

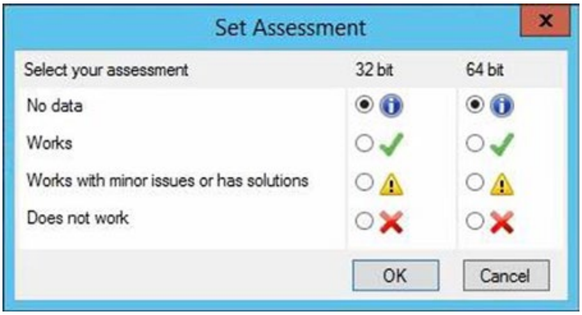

Analyze - Microsoft Application Compatibility Manager
File Go View Actions Filter Tools Window Help
Send and Receive
Toggle Filter
Analyze
Open Reports
Quick Reports
Windows 7 Reports
Applications
Application Installation Packa
Computers
Devices
Windows Vista SP1/SP2 Reports
Applications
Application Installation Packa
Computers
Devices
Windows Vista Reports
Applications
Application Installation Packa
Computers
Devices
Internet Explorer
Web Sites

Windows 7 - Application Report

Application Name	Version	Company	Vendor Assessm	Community Assessment	C
Microsoft Office Communicator 2007, MUI	2.0.6362.0	Microsoft Corporati...		32 (1) 64	2
Microsoft Office Enterprise 2007	12.0.6215...	Microsoft Corporati...	32 64	32 (14) 64	2
Microsoft Office Communicator 2007	2.0.6338	Microsoft Corporati...		32 (22) 64	1
Microsoft Office Communicator 2007 R2	3.5.6881	Microsoft Corporati...	32 64	32 (58) 64	1
Microsoft Office Enterprise 2007	12.0.6215...	Microsoft Corporati...	32 64	32 (12) 64	1
Microsoft Office Live Meeting 2007	8.0.6338	Microsoft Corporati...	32 64	32 (76) 64	1
Microsoft Office Live Meeting Add-in Pack	7.0.2010.5	Microsoft Corporati...		32 (0) 64	2
Microsoft Office Enterprise 2007	12.0.6418...	Microsoft Corporati...	32 64	32 (0) 64	1
Microsoft Office Live Meeting 2005	7.3.2015	Microsoft Corporati...		32 (1) 64	2
Microsoft Office Communicator 2005	1.0.557	Microsoft Corporati...	✗ 32 ✗ 64	32 (21) 64	2
Microsoft Firewall Client	4.0.3442.6...	Microsoft (R) Corp...	32 64	32 (10) 64	3
Microsoft Forefront Client Security Antimalware Ser...	1.5.1951	Microsoft Corporati...		32 (4) 64	2
Microsoft Dynamics AX 4.0 Client	4.0.2501.1...	Microsoft Corporati...		32 (0) 64	1
Microsoft Firewall Client	4.0.3441.6...	Microsoft (R) Corp...	32 64	32 (1) 64	1
Microsoft Forefront Client Security State Assessme...	1.0.1697	Microsoft Corporati...		32 (13) 64	2
Microsoft Office 2003 Web Components	11.0.6533	Microsoft Corporati...		32 (11) 64	1

***Figure 4-7.** Application Report summary after synchronization with Microsoft*

If you notice an application in the list that you know works on your OS, you can update the metadata relating to this entry and share this with both Microsoft and the community. This can be created by right-clicking the application and selecting **Set Assessment**, and then configuring the most appropriate option in the Set Assessment window (see Figure 4-8).



Select your assessment	32 bit	64 bit
No data	● ⓘ	● ⓘ
Works	○ ✓	○ ✓
Works with minor issues or has solutions	○ ⚠	○ ⚠
Does not work	○ ✗	○ ✗

Figure 4-8. *Manually creating an application assessment*

The next time you click the **Send and Receive** button, the data for your assessment and any other recently updated applications will be synchronized.

If you have custom applications and executables that may have been written for your company, these will not show in the list of applications in Figure 4-7 unless they were deployed using an installer. To review the compatibility status of these applications, you can deploy the stand-alone runtime-analysis package, which is created by choosing the **Collect** option in the ACM, and then selecting File ➤ New, and building a runtime analysis package. This creates another MSI package to be deployed. Once installed on the client machine, the tool can be launched by clicking the Microsoft Compatibility Monitor icon on the Start screen.

The Compatibility Monitor (see Figure 4-9) allows you to start or stop data collection, and also provides compatibility feedback on the application under review.

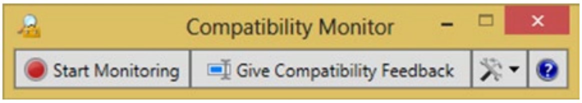


Figure 4-9. *Using the runtime-analysis compatibility monitor*

There are five steps to using the Microsoft Compatibility Monitor, as described in Table 4-2.

Table 4-2. *Using the Microsoft Compatibility Monitor*

Step	User Action
Monitor your computer for compatibility issues	Click Start Monitoring.
Use your applications	N/A
Close your applications and stop monitoring	Click Stop Monitoring.
Rate the compatibility of your application(s)	Click Give Compatibility Feedback and rate the compatibility.
Report a compatibility issue with your application(s)	Click Give Compatibility Feedback and add details

Shims

A *shim* is a compatibility fix that allows the application to be fooled into believing something is true when in reality it is not. Within the ACT parlance, a shim is called *mitigation*. For example, a common shim is needed when an application expects to run on Windows XP and it will not run on a later version. A shim acts between the application and the OS; it lies to the application about the OS version, so that the application believes that it is running on XP, when in actuality the OS is Windows 7 or newer. Applications are completely unaware that a shim is in place, intercepting the calls between the application and the OS, and vice versa.

Microsoft has written hundreds of fixes. Mitigations may be applied to fool the application by utilizing newer technologies, such as virtualized file locations for granting access to restricted areas like `C:\Windows\System32`, or forcing the application to run with administrative privileges, or to think it is using an older version of IE when in fact it is using one of the newer versions of IE.

We mentioned earlier how the compatibility mode can be used in smaller scenarios to fix compatibility issues; the OS is then applying a shim based on the choices that you made within compatibility mode.

Standard User Analyzer

Included within the Microsoft Compatibility Monitor is a useful tool called the Standard User Analyzer (SUA). It can be launched by clicking the tool icon on the right side of the Microsoft Compatibility Monitor application (see Figure 4-9).

The SUA allows you to launch and monitor a target application, capture useful information to drill down into the specifics of how the application is run, and identify information about the application, such as the user-level privileges required, the working directory, and registry keys used.

The underlying tool that the SUA uses is the Application Verifier (AppVerif.exe), which is a development tool to dynamically monitor application actions while the application runs. It also forces the application to undergo several stresses and tests, and generates a report about potential errors in application execution or design. The first time that you attempt to launch an application within SUA, you may be required to download and install the Application Verifier. You can manually install the tool from www.microsoft.com/en-us/download/details.aspx?id=20028.

After you have started the SUA, you should then launch the target application and test to see if the application behaves correctly. If the application misbehaves or crashes during the test, the SUA will capture useful data that can then be reviewed in the SUA tool.

The workflow for using SUA is shown in Figure 4-10.

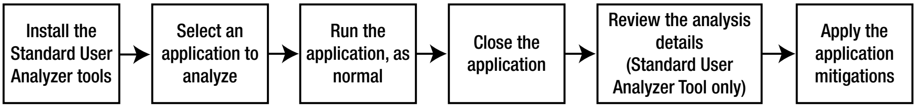
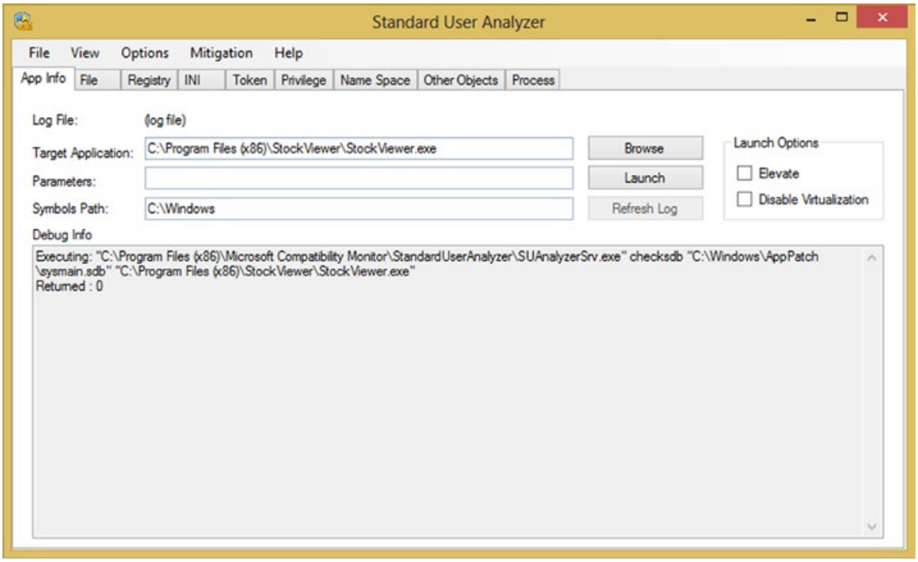

Install the Standard User Analyzer tools
Select an application to analyze
Run the application, as normal
Close the application
Review the analysis details (Standard User Analyzer Tool only)
Apply the application mitigations

Figure 4-10. *The SUA workflow*

To practice using the SUA, you can use the demo application called StockViewer.exe, which can be obtained from Chris Jackson's blog at http://blogs.msdn.com/b/cjacks/archive/2008/01/03/stock-viewer-shim-demo-application.aspx.

After you load StockViewer.exe in the SUA (see Figure 4-11) and launch the application, the SUA monitors the application failures.



Log File: (log file)
Target Application: C:\Program Files (x86)\StockViewer\StockViewer.exe
Parameters:
Symbols Path: C:\Windows

□ Elevate
□ Disable Virtualization

Debug Info

```
Executing: "C:\Program Files (x86)\Microsoft Compatibility Monitor\StandardUserAnalyzer\SUAnalyzerSrv.exe" checksdb "C:\Windows\AppPatch
\sysmain.sdb" "C:\Program Files (x86)\StockViewer\StockViewer.exe"
Returned : 0
```

Figure 4-11. *Using the Standard User Analyzer*

Once you refresh the SUA log, you will see all the application actions with Windows that the SUA has monitored. Much of this information is relevant to developers who understand errors such as stack traces, processes, and namespace errors.

IT pros can attempt to use the Mitigation menu item and implement some of the fixes that SUA suggests. You can apply the fixes that are suggested, such as ForceAdminAccess, or enable your own choices. Once the selected fixes are applied, the SUA generates the fix—a shim database (`.sdb`) file is applied to the application when it is run.

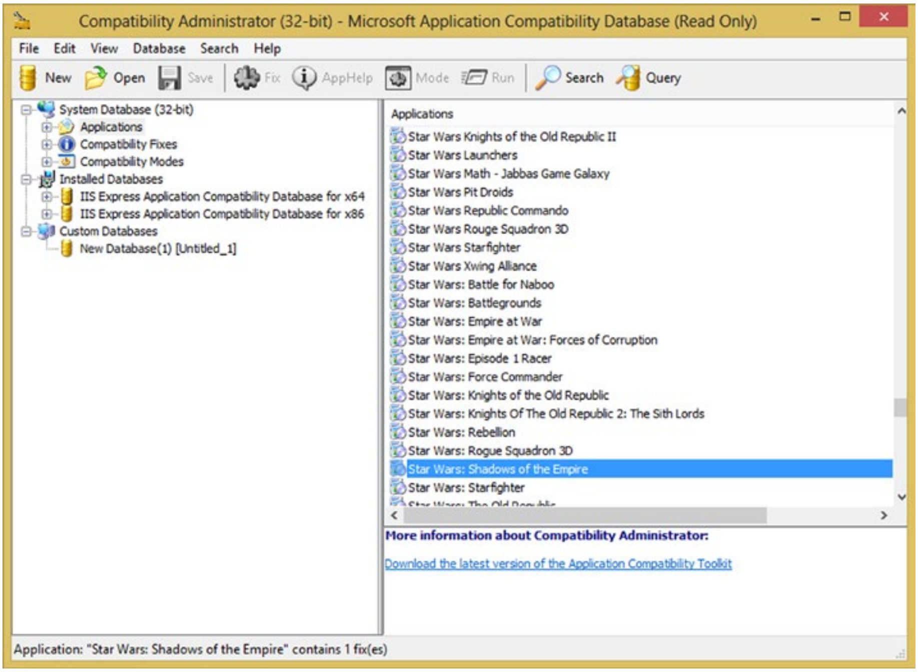
Compatibility Administrator

One of the limitations of the SUA is that it only analyzes and recommends fixes for applications one at a time, and the applied mitigations only work on the local machine. You need to use the Compatibility Administrator, which is part of ACT, to create enterprise-ready shims for your applications. The Compatibility Administrator has been continually updated and expanded over the last 10 years and now includes fixes, shims, and support for a staggering number of 32-bit and 64-bit applications, as shown in Table 4-3.

Table 4-3. *Scale of Fixes Provided in Compatibility Administrator*

Data	32-bit version	64-bit version
Applications	7222	383
Compatibility fixes	398	119
Compatibility modes	86	32

In addition to the applications, there are also hundreds of prepackaged shim fixes and compatibility modes within the tool that can be applied to your applications (see Figure 4-12). If the application that you need to fix is listed, you can click **Run** on the toolbar to test the fix by launching the application with the Compatibility Administrator.


Compatibility Administrator (32-bit) - Microsoft Application Compatibility Database (Read Only)
File
Edit
View
Database
Search
Help
New
Open
Save
Fix
AppHelp
Mode
Run
Search
Query

- System Database (32-bit)
  - Applications
  - Compatibility Fixes
  - Compatibility Modes
- Installed Databases
  - IIS Express Application Compatibility Database for x64
  - IIS Express Application Compatibility Database for x86
- Custom Databases
  - New Database(1) [Untitled_1]

Applications

Star Wars Knights of the Old Republic II
Star Wars Launchers
Star Wars Math - Jabbas Game Galaxy
Star Wars Pit Droids
Star Wars Republic Commando
Star Wars Rouge Squadron 3D
Star Wars Starfighter
Star Wars Xwing Alliance
Star Wars: Battle for Naboo
Star Wars: Battlegrounds
Star Wars: Empire at War
Star Wars: Empire at War: Forces of Corruption
Star Wars: Episode 1 Racer
Star Wars: Force Commander
Star Wars: Knights of the Old Republic
Star Wars: Knights Of The Old Republic 2: The Sith Lords
Star Wars: Rebellion
Star Wars: Rogue Squadron 3D
Star Wars: Shadows of the Empire
Star Wars: Starfighter
Star Wars: The Old Republic

More information about Compatibility Administrator:

Download the latest version of the Application Compatibility Toolkit

Application: "Star Wars: Shadows of the Empire" contains 1 fix(es)

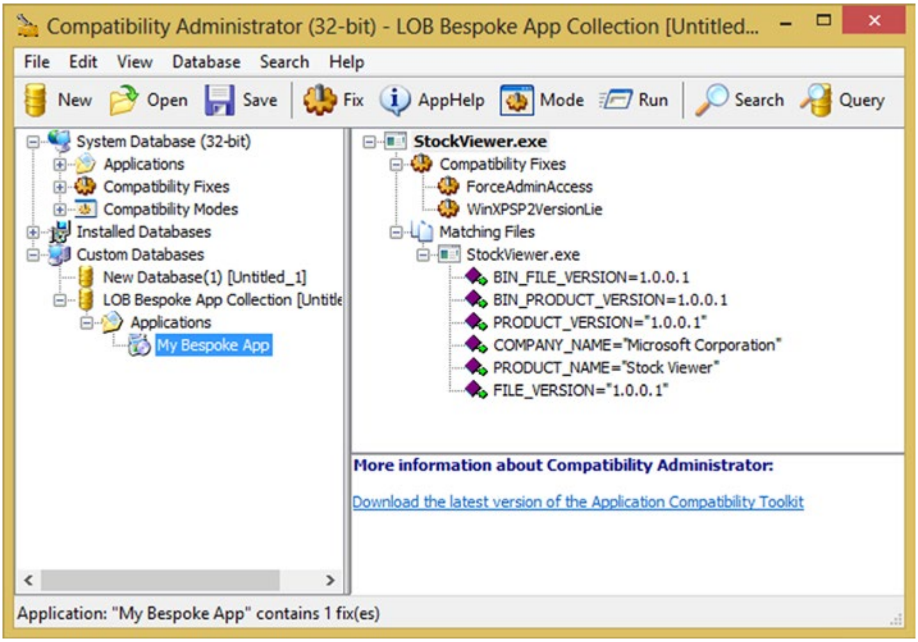
Figure 4-12. *The Compatibility Administrator interface*

For enterprises that have custom or bespoke applications, or an application that is not listed in the Compatibility Administrator, you need to create a new custom database to hold your own application shims and compatibility modes.

Once you have built and tested the necessary fixes for the applications, you are able to save the database and then deploy it as a package of fixes to your reference computer for testing prior to enterprise deployment. Once the reference machine has the compatibility database installed, all applications that are referenced in the database should then be fixed.

When configuring a fix, you must use the correct architecture version of Compatibility Administrator that corresponds to your application; for example, x64 or x86.

To illustrate the process, I used a special app (Stock Viewer) to create a new custom database called LOB Bespoke App Collection, as shown in Figure 4-13. I followed the wizard to specify the compatibility mode (none), and then I added two compatibility fixes (*ForceAdminAccess* and *WinXPSP2VersionLie*). Finally, the shim was applied to those files that match the file characteristics specified in the Matching Files section.



BIN_FILE_VERSION=1.0.0.1
BIN_PRODUCT_VERSION=1.0.0.1
PRODUCT_VERSION="1.0.0.1"
COMPANY_NAME="Microsoft Corporation"
PRODUCT_NAME="Stock Viewer"
FILE_VERSION="1.0.0.1"

More information about Compatibility Administrator:

Download the latest version of the Application Compatibility Toolkit

Application: "My Bespoke App" contains 1 fix(es)

Figure 4-13. *Configuring custom applications in Compatibility Administrator*

You should add all the applications that you are migrating over to the newer OS to your custom database. These are then bundled together and exported to an `.sdb` package file, ready for deployment.

■ **Note** If you modify the application file name, the shim will no longer work and you will need to re-create the shim.

Once you have deployed the `.sdb` file to all computers that will use the custom application, you need to install the fix so that Windows is aware of the fixes required. Installing the `.sdb` file can be performed using Group Policy, PowerShell, or a logon script. To simplify deployment, it can be shared on the corporate network.

You need to use the `sdbinst.exe` command to install the fix alongside the application. For example, to install the fix shown in Figure 4-13, you could use `sdbinst.exe -q "C:\Program Files (x86)\StockViewer\fix.sdb"`.

Once you have installed the `.sdb` file, you should then be able to launch your application and it should operate without any errors.

■ **Note** Developers who write their own code and need to verify that the code will work on current versions of Windows should download the Windows and Windows Server compatibility cookbook: Windows 8, Windows 8.1, and Windows Server 2012, available at `https://www.microsoft.com/en-us/download/details.aspx?id=27416`.

Resolving Browser Plug-in Compatibility Issues

Users often do not understand how add-ons can affect their browsing performance, either positively through increased productivity, or negatively when add-ons slow IE performance. The majority of add-ons are harmless and can be very beneficial to users. They can also boost productivity when used correctly. Help desk technicians and administrators should consider how add-ons will be handled within an organization; if they want to actively manage add-ons, they can choose to disable or enable them. As an alternative, the management of IE add-ons can be left entirely to the end user; only when issues arise would the help desk become involved.

IE11 allows four types of add-ons, as described in Table 4-4.

Table 4-4. *Types of Add-ons Supported by IE11*

Add-on	Description
Search Providers	The browser provides suggestions based on your search criteria.
Accelerators	Whenever the user highlights text on a web page, a blue Accelerator icon appears, which adds functionality such as email, map, search, translate, and many other tasks.
Web Slices	Real-time information from the Web displays on the Favorites bar
Toolbars	Additional toolbars that provide extra functionality

Prior to implementing changes to the default behavior of IE, you should consider end-user training. Although some Windows upgrade training may be offered within an organization, IE-specific training is often overlooked. This may be because IE has been a part of Windows for as long as most users can remember; they are familiar with the basic operation of IE. Since most of the enhancements that each successive version of IE brings are either related to security protection or increased productivity, it often proves beneficial to provide some end-user training on new IE features.

One historical issue relates to users adding a plug-in to support Adobe Flash Player. Since IE10 on Windows 8, and IE11 on Windows 8.1 and Windows 10, Microsoft has built Adobe Flash Player directly into the browser, so there is no need for add-on support or external Flash updates. Microsoft does not plug any security fixes through Windows Update.

Despite built-in support in the latest versions of IE, Flash Player remains a high-risk target for security exploits, and for this reason, it is often disabled within many organizations. This can be achieved on a per-user basis via disabling Flash Player in Manage Add-ons or via Group Policy.

If the frequency of add-on–related issues reported to the help desk is high, the organization can choose to adjust how add-ons are allowed or disabled for users.

The first option is to configure on a local PC level, using Local Group Policy settings (the starting location is Computer Configuration ➤ Administrative Templates ➤ Windows Components) to modify the options in Table 4-5.

Table 4-5. *Local Group Policy Objects to Configure IE11 Add-ons*

Policy Location	Settings Available
Internet Explorer	Turn off add-on performance notifications Automatically activate newly installed add-ons Do not allow users to enable or disable add-ons
Internet Explorer ➤ Internet Control Panel ➤ Advanced Page	Do not allow resetting Internet Explorer settings Allow third-party browser extensions
Internet Explorer ➤ Security Features ➤ Add-on Management	Add-on List Deny all add-ons unless specifically allowed in the Add-on List Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects

Alternatively, you can restrict specific add-ons via Group Policy. To enable or disable a specific add-on, you need to reference the unique Class ID (CLSID) for the add-on.

To obtain the CLSID for the add-on that you want to enable or disable, perform the following steps:

1. Open **IE**, click **Tools**, and then click **Manage add-ons**.
2. Double-click the installed add-on that you want to modify.
3. On the **More Information** screen, click **Copy**, which copies all the add-on metadata.
4. Close **Manage Add-ons** and **Internet Explorer**.
5. Paste the data into **Notepad**, and then copy the **Class ID** value.
6. Open the **Group Policy Management Editor** (if using a server-based environment) and navigate to **Computer Configuration ➤ Policies ➤ Administrative Templates ➤ Windows Components ➤ Internet Explorer ➤ Security Features ➤ Add-on Management**.

7. Open the **Add-on List Group Policy Object**, choose **Enabled**, and then click **Show**.

8. The **Show Contents** box appears. In **Value Name**, paste the Class ID.

9. In **Value**, chose from the following options:

    - [0] the add-on is disabled and users can't change it
    - [1] the add-on is enabled and users can't change it
    - [2] the add-on is enabled and users can change it

10. Click **OK** and close the Group Policy Editor.

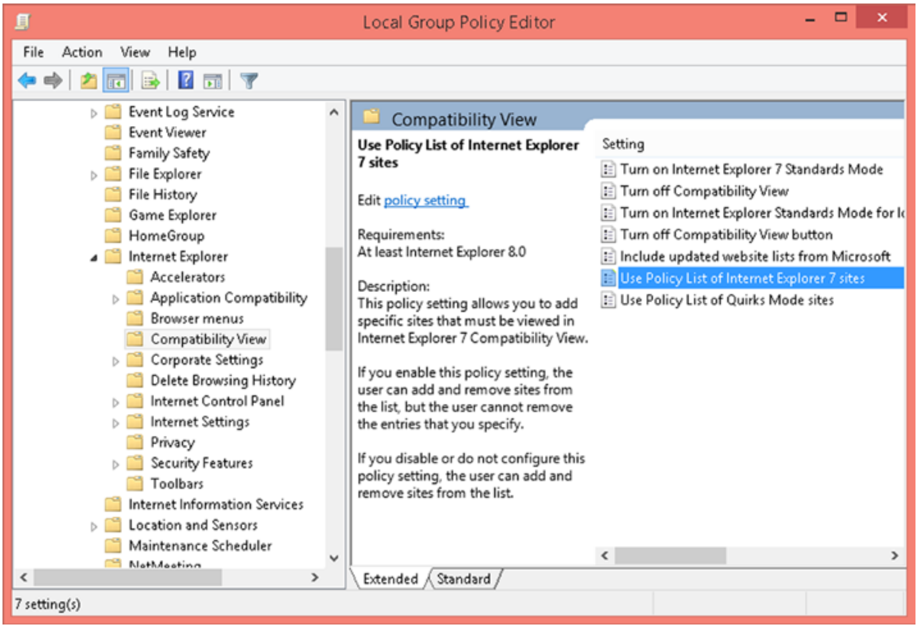
■ **Note** If you are interested in other configurable policy settings, you can review over 3,600 that are listed in the reference spreadsheet. It is available for download; see Group Policy Settings Reference for Windows and Windows Server at `www.microsoft.com/en-gb/download/details.aspx?id=25250`.

Resolving Internet and Intranet Site Compatibility Issues

With new web site features appearing all the time across the Web, it is often a race for browsers to keep up-to-date. You saw in Chapter 2 how it is possible for IE to autosense the most appropriate browser compatibility mode to a render web site. This works very well for the most common situations; however, there are often web sites that load with errors or require plug-ins to display properly.

Intranet sites are often the main culprit because they are often written by non-web professionals. And whereas the physical content may be periodically updated, the underlying HTTP code is seldom upgraded to meet the current standards that would be enabled by default if the web site was created anew. It is generally accepted that internally hosted intranet sites are trustworthy (although this should never be taken for granted); therefore it is normal practice to add intranet sites to the local intranet security zone within IE, because configuring this option can help resolve security-related compatibility issues.

You can attempt to resolve age-related issues on how IE renders a web site by using the IE11 Compatibility View feature. Manually add the intranet and other web sites to the Compatibility View list so that IE always opens the web site in Compatibility View mode. Within a corporate environment, IT pros can deploy IE11 with a list of preset web sites, including the intranet, to use Compatibility View. These lists can be deployed via the **Use Policy List of Internet Explorer 7 sites** policy setting (see Figure 4-14).



Use Policy List of Internet Explorer 7 sites

Edit policy setting

Requirements:
At least Internet Explorer 8.0

Description:
This policy setting allows you to add specific sites that must be viewed in Internet Explorer 7 Compatibility View.

If you enable this policy setting, the user can add and remove sites from the list, but the user cannot remove the entries that you specify.

If you disable or do not configure this policy setting, the user can add and remove sites from the list.

Setting
- Turn on Internet Explorer 7 Standards Mode
- Turn off Compatibility View
- Turn on Internet Explorer Standards Mode for lo
- Turn off Compatibility View button
- Include updated website lists from Microsoft
- Use Policy List of Internet Explorer 7 sites
- Use Policy List of Quirks Mode sites

Figure 4-14. *Pre-populating web sites to use Compatibility View*

Various other options can be found in the following location within Group Policy: Administrative Templates ➤ Windows Components ➤ Internet Explorer ➤ Compatibility View.

On an unmanaged system, if a user is having trouble with add-ons, or IE is not behaving properly and the user suspects that there is a misconfigured option, it is useful to have the user reset their IE to the default settings, which removes all add-ons and customizations.

1. Open **IE** and click the **Tools** button.
2. Click **Internet options**.
3. Click the **Advanced** tab, and then click **Reset**.
4. In the **Reset Internet Explorer Settings** dialog box, click **Reset**.
5. When IE finishes applying the default settings, click **Close**, and then click **OK**.
6. Restart your PC for the changes to take effect.

Summary

Managing and maintaining a business environment of hundreds or thousands of devices with a similar number of deployed applications can be a complex undertaking. Deciding to upgrade the OS is normally a decision not taken lightly and often involves many months, if not years, of planning, testing, and piloting before deployment.

Compatibility is still one of the major concerns that most IT pros voice when discussing issues about upgrading. Because compatibility is such a major concern that organizations often delay the implementation of a new OS, Microsoft has greatly improved its available tools and overall reliability so that older applications can work with modern versions of Windows.

Leaving software behind, in the next chapter we will revisit device drivers in more detail and also take a look at how to boot Windows when your system becomes unresponsive.

CHAPTER 5

Resolving Hardware Compatibility Issues

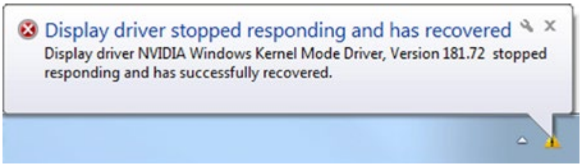
We all love our hardware—whether it is a traditional PC, laptop, or tablet—but when it goes wrong, it really goes wrong. In this chapter, we're going to look at drivers. These small pieces of code are significant because they tell our OS how to drive the devices that are either built-in or that we add-on. This might be an exaggeration, but it's certainly true that drivers can cause significant issues on PCs. But why do they do this?

Graphics drivers are perhaps the worst offenders, but they're also a special case. Unlike the drivers for audio, USB, and other devices, such as printers and biometric sensors, the graphics driver is needed very early on when a PC boots, and it's one of the first components the Windows boot system loads.

This results in the graphics driver being embedded deep within the workings of the OS, which means that unlike other drivers, if this one fails in any way, the whole system can collapse around it, because of its importance to the OS experience.

Other drivers, such as the ones I mentioned, are loaded after the core OS is already residing in memory, and as such, all of the management and reporting tools that handle driver crashes and conflicts are running. If one of these drivers fails, then it's a much simpler task for Windows to restart it.

As an example of this, you might have experienced the message "Display driver stopped working and has recovered" (see Figure 5-1). This is a great example of how modern versions of the Windows OS, which use the newest version of the driver model that was introduced with Vista, can successfully manage driver crashes without disturbing the user experience.



Display driver stopped responding and has recovered

Display driver NVIDIA Windows Kernel Mode Driver, Version 181.72 stopped responding and has successfully recovered.

Figure 5-1. *Windows alerts you when a driver crashes and needs to be restarted*

M. Halsey and A. Bettany, *Windows Software Compatibility and Hardware Troubleshooting*,
DOI 10.1007/978-1-4842-1061-1_5

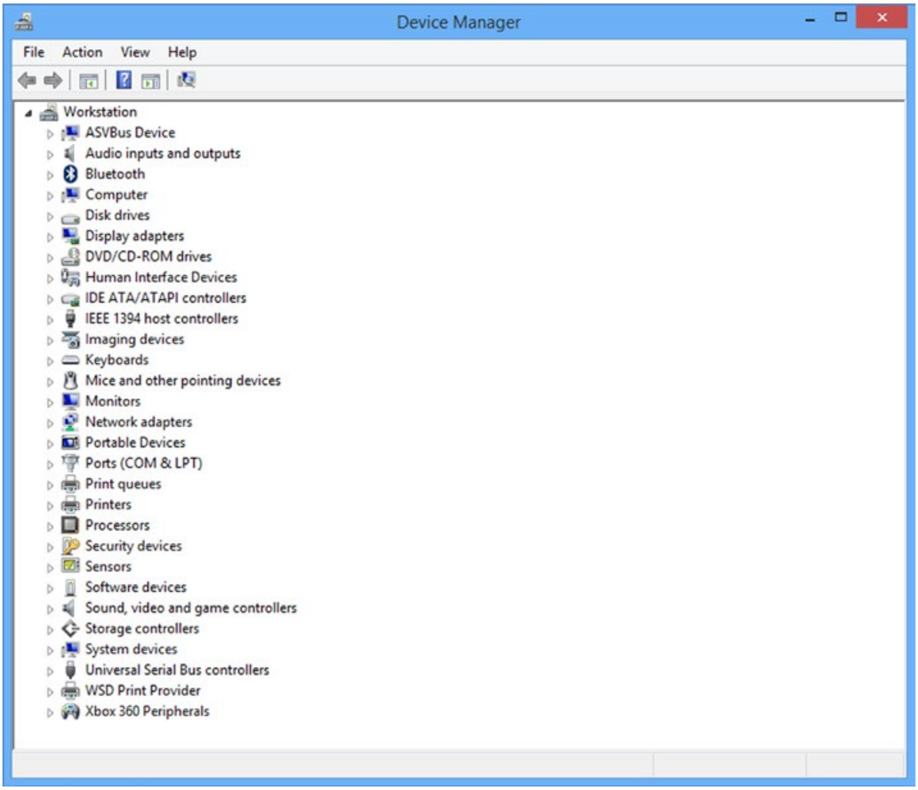
In cases such as this, you might find that your screen flickers momentarily while Windows closes and then restarts the driver. If a driver (such as a USB device) crashes, you might hear the sound Windows makes when you unplug and reattach the device, but if an audio device fails and restarts, you might hear nothing at all.

Should the graphics driver or another driver (the most common being those associated with functionality on the PC's motherboard) fail during boot time, however, the chances of getting a Blue Screen of Death (BSOD) are greatly increased. This is because the management tools for drivers aren't available until Windows finishes loading, and if startup cannot continue without a specific driver functioning properly, the boot system will simply halt on the error.

It's possible to troubleshoot, diagnose, and repair driver problems on PCs in more ways than perhaps any other part of the Windows OS; and in this chapter, we'll detail them all.

The Windows Device Manager

Hardware and the software drivers are managed in the Device Manager (see Figure 5-2). This is probably the one administration panel in Windows that people are most familiar with.



- Workstation
  - ASVBus Device
  - Audio inputs and outputs
  - Bluetooth
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - IEEE 1394 host controllers
  - Imaging devices
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
  - Portable Devices
  - Ports (COM & LPT)
  - Print queues
  - Printers
  - Processors
  - Security devices
  - Sensors
  - Software devices
  - Sound, video and game controllers
  - Storage controllers
  - System devices
  - Universal Serial Bus controllers
  - WSD Print Provider
  - Xbox 360 Peripherals

Figure 5-2. *The Windows Device Manager*

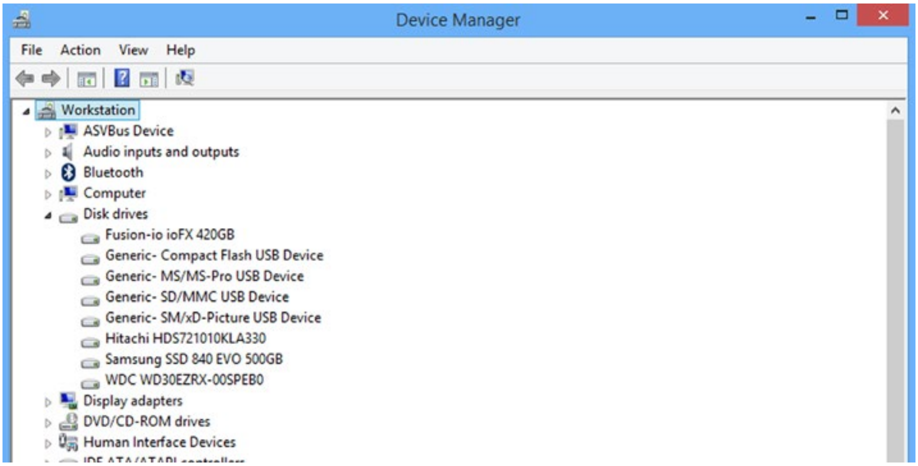
You can open it from the Control Panel, by searching for it at the Windows 8.1 Start screen or in the Windows 7 or Windows 10 Start menu search box. Additionally, in Windows 8.1 and Windows 10, you can right-click the Windows button on the desktop taskbar (or press the Windows key + X) to display the administration menu where Device Manager is an option.

■ **Note** You can also open the Device Manager from the Command Prompt or from the Start menu or Start screen search box by typing **devmgmt.msc**.

All devices are categorized in the Device Manager, but this varies by the hardware you have installed. All PCs feature categories such as Computer, Disk Drives, Display Adapters, Network Adapters, Processors and System Devices, and you might see additional categories, such as Bluetooth, Biometric Devices, Security Devices and Sensors.

■ **Note** In Windows 10, you can install and uninstall Plug and Play hardware in the Settings app. There are no management features for device drivers available here, however, including the updating or disabling of devices. Also, the Settings app only shows a subset of all the devices installed on a PC.

Clicking the arrow to the left of a category in Device Manager expands the category, displaying all the hardware (or software) devices contained therein (see Figure 5-3).

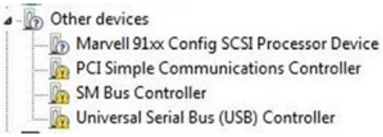


```
◢ Workstation
    ▷ ASVBus Device
    ▷ Audio inputs and outputs
    ▷ Bluetooth
    ▷ Computer
    ◢ Disk drives
          Fusion-io ioFX 420GB
          Generic- Compact Flash USB Device
          Generic- MS/MS-Pro USB Device
          Generic- SD/MMC USB Device
          Generic- SM/xD-Picture USB Device
          Hitachi HDS721010KLA330
          Samsung SSD 840 EVO 500GB
          WDC WD30EZRX-00SPEB0
    ▷ Display adapters
    ▷ DVD/CD-ROM drives
    ▷ Human Interface Devices
      IDE ATA/ATAPI controllers
```

Figure 5-3. *Viewing specific devices in the Device Manager*

In this example, there are hard disks, including an SSD, two mechanical hard disks, a PCIe Flash storage card, and a multicard reader.

If a device is not functioning correctly or is uninstalled, you are alerted with either a question mark icon or a yellow warning triangle to indicate that it is “unknown” (see Figure 5-4). The Device Manager automatically expands any category where you need to be alerted to a problem, and it also places any device that it cannot properly identify and categorize in an Other Devices category.



Other devices
- Marvell 91xx Config SCSI Processor Device
- PCI Simple Communications Controller
- SM Bus Controller
- Universal Serial Bus (USB) Controller

Figure 5-4. *Windows alerts you about malfunctioning or uninstalled drivers*

Installing, Uninstalling, and Updating Drivers

There are several different ways to install drivers in Windows, and different sources from which you can get the driver. It’s this second point that I’d like to address first, as each source has its pros and cons.

The first and perhaps the most obvious is the manufacturer’s web site, although you will have received an installation disc with the hardware that contains drivers. Windows Update is a reliable source of drivers, but there can still be problems because some drivers in Windows Update are older than those available on the manufacturer’s web site. This can cause incompatibilities and instabilities in Windows. Many web sites also exist to store older versions of drivers; `www.oldversion.com` is one such example.

Table 5-1. *The Pros and Cons of Obtaining Hardware Drivers from Different Sources*

Source	Pros	Cons
Windows Update	All drivers are digitally signed	Some drivers are older and can cause instabilities.
Manufacturer’s web site	The latest and most up-to-date drivers (including beta drivers)	Drivers may not be digitally signed; beta drivers can be unstable. Older drivers may not be available.
Driver archive web site	Useful for finding legacy drivers	Drivers may not be digitally signed, may cause incompatibilities, and could contain malware.
Original installation disc	Official drivers from the manufacturer	Drivers may be old and may not be compatible with your Windows version

The easiest way to install a driver is to run its installer package. If a piece of hardware has been identified in Device Manager, but has not been installed, right-click the device, and in the context menu that appears, click **Update Driver Software** (see Figure 5-5).

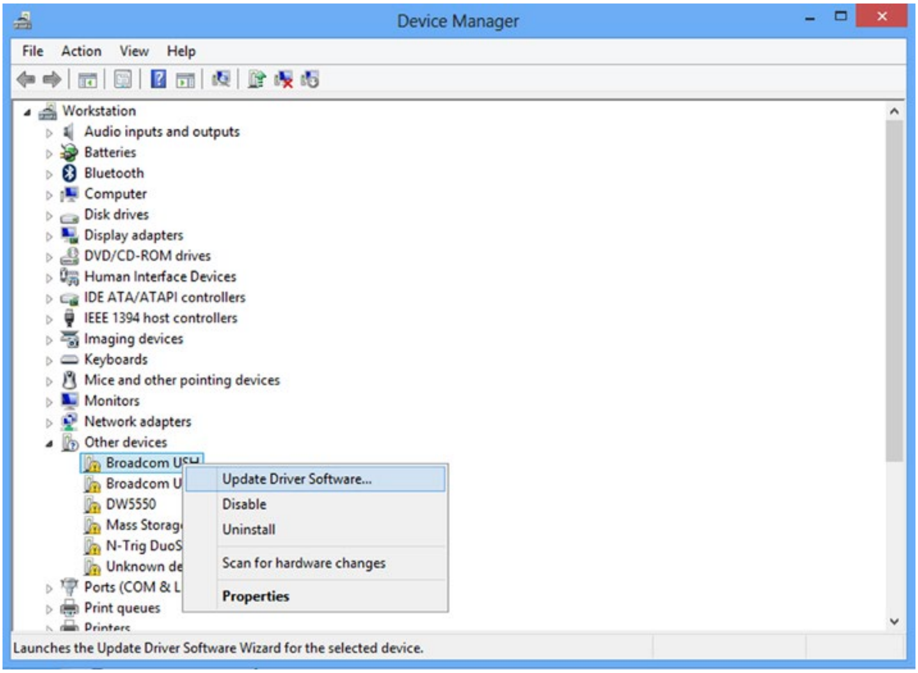


Figure 5-5. *You can right-click a device to install its driver*

Bypassing the Windows Version Check by Unzipping Drivers

On occasion, you find a driver that will not install because it doesn't support the version of Windows that you are using. You might find this if you are using hardware that was designed for Windows Vista or Windows 7, but is no longer sold and you wish to install it on Windows 10.

■ **Note** The Windows driver model for Windows Vista, Windows 7, Windows 8.1, and Windows 10 is the same, although some minor changes have been implemented over the years. Drivers installed for Windows Vista should work fine in Windows 7, Windows 8.1, and Windows 10.

All is not lost, however, because many (though not all) driver installers can be unzipped to your PC using a package such as WinRAR, which you can download at `www.rarlab.com`.

In Figure 5-6, you see the installer for the Chipset, Graphics, Camera, and Audio on an HP Stream 7 tablet. It looks like a standard application—and indeed that's what it is—except that like many drivers, it is merely an executable archive file; unzipping its contents to a folder reveals the Setup.exe file, along with a folder for specific drivers for different Windows versions.

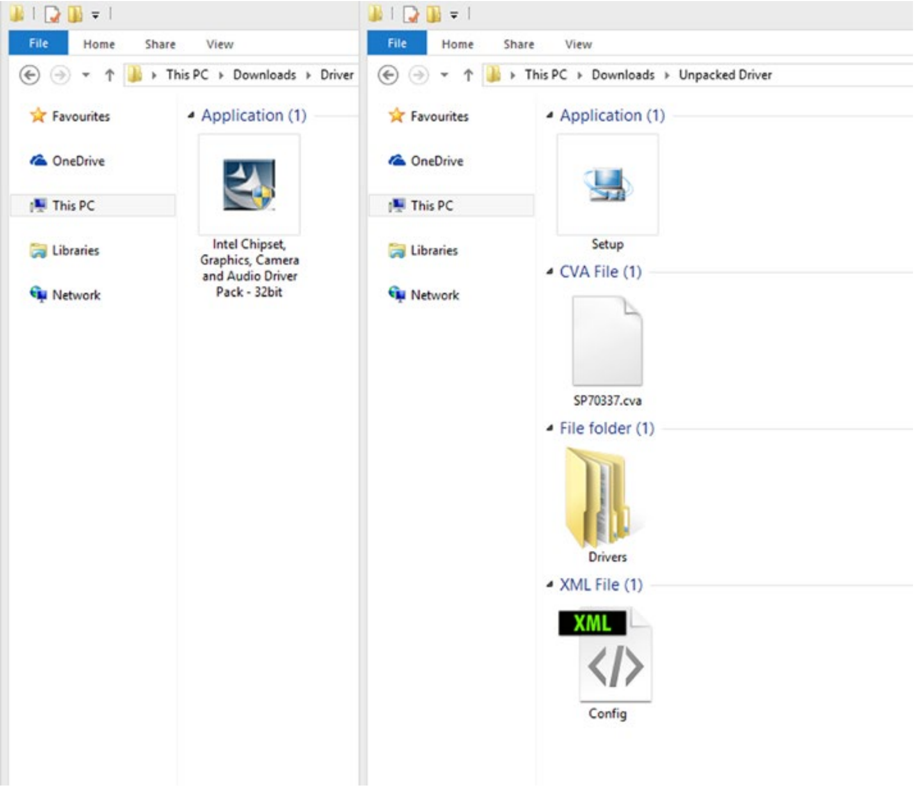


Figure 5-6. *Some drivers can be unzipped*

Exploring the contents of this Drivers folder (it may be named differently for other drivers) reveals all the full driver files for the particular hardware (see Figure 5-7). Each of these can either be run individually, if it is an executable file, or installed manually in the Device Manager, bypassing the Windows version check in the Setup.exe program.

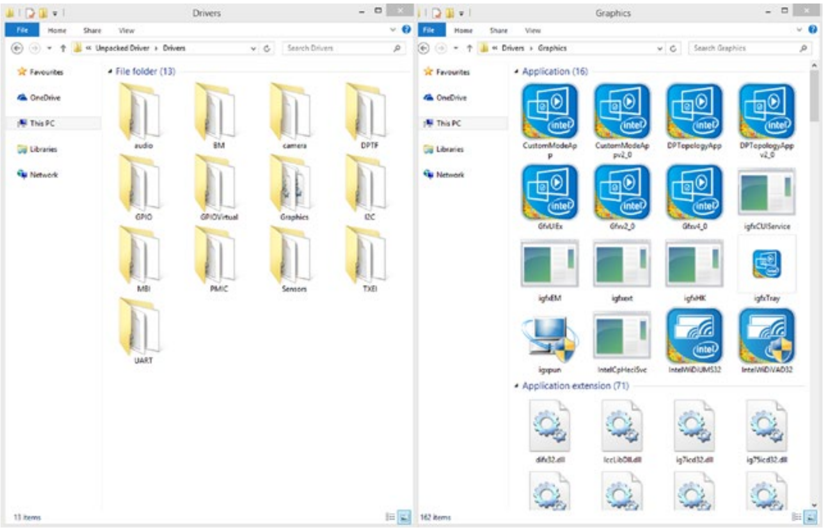
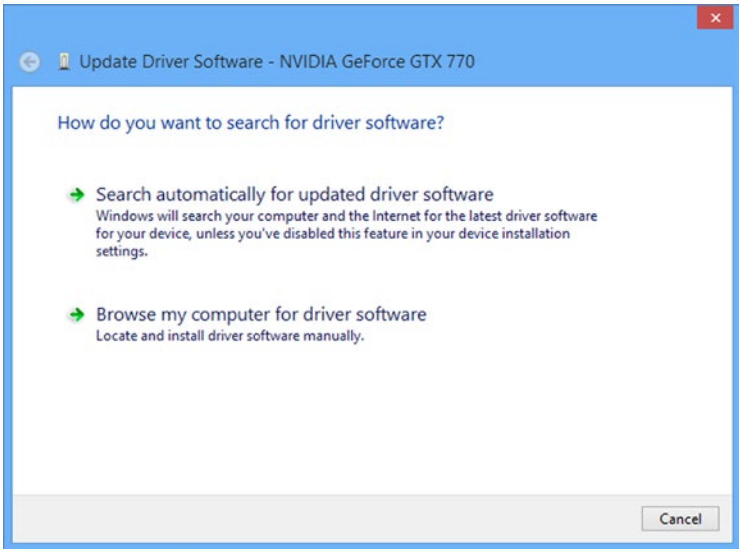


Figure 5-7. *Unzipping an installer package reveals the full driver install files*

Installing Device Drivers

When you install a device driver, you are first asked if you want to **Search automatically for updated driver software** or if you want to **Browse [your] computer for drivers software** (see Figure 5-8).


Update Driver Software - NVIDIA GeForce GTX 770

How do you want to search for driver software?

→ Search automatically for updated driver software
Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.

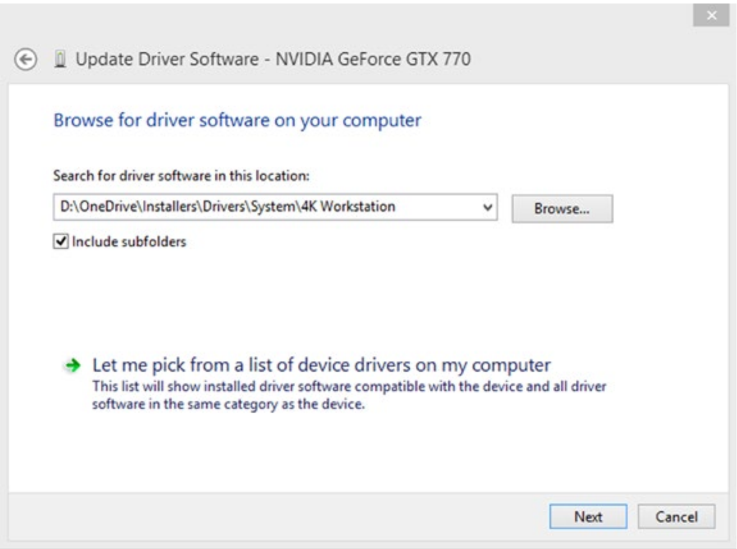
→ Browse my computer for driver software
Locate and install driver software manually.

Cancel

Figure 5-8. *Windows asks if you want it to search for a driver, or if you already have the driver file*

Clicking the **Search automatically** option searches both Windows Update (if you have a live Internet connection) and the driver store folder on your PC. This driver storage folder contains both the drivers that are supplied with your copy of Windows and the drivers that have been previously installed.

Choosing the **Browse my computer for driver software** option displays two more options (see Figure 5-9).



Update Driver Software - NVIDIA GeForce GTX 770

Browse for driver software on your computer

Search for driver software in this location:

D:\OneDrive\Installers\Drivers\System\4K Workstation

☑ Include subfolders

Let me pick from a list of device drivers on my computer

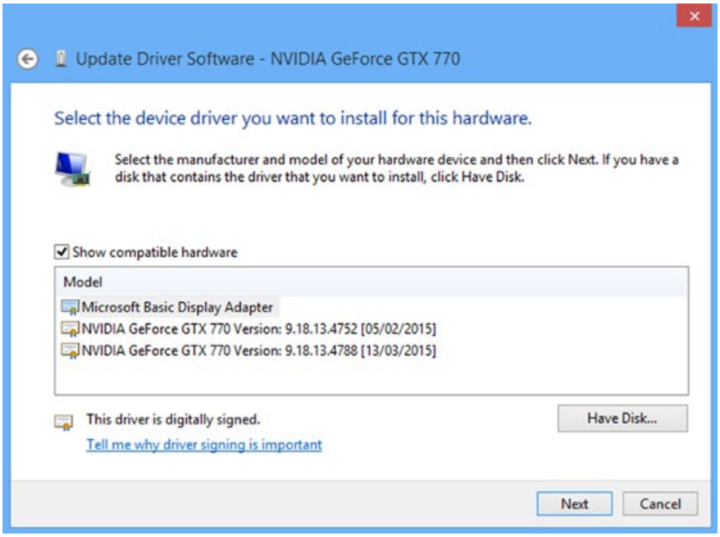
This list will show installed driver software compatible with the device and all driver software in the same category as the device.

***Figure 5-9.** Choosing to install a driver manually presents additional options*

Here you can choose a folder on your computer (or network) where the downloaded driver is available, or you can choose from one of the drivers already available on Windows.

The first option lets you browse to any folder on your PC and select **include [all of the] subfolders** for your chosen location. For example, you may have a folder for drivers and software on your PC or laptop, within which there are subfolders of downloaded drivers, or ones copied from the CDs that came with the PC.

Selecting a driver from the list of device drivers on your computer displays any drivers that Windows detects is compatible with your hardware (see Figure 5-10).



Update Driver Software - NVIDIA GeForce GTX 770

Select the device driver you want to install for this hardware.

Select the manufacturer and model of your hardware device and then click Next. If you have a disk that contains the driver that you want to install, click Have Disk.

☑ Show compatible hardware

Model
Microsoft Basic Display Adapter
NVIDIA GeForce GTX 770 Version: 9.18.13.4752 [05/02/2015]
NVIDIA GeForce GTX 770 Version: 9.18.13.4788 [13/03/2015]

This driver is digitally signed.

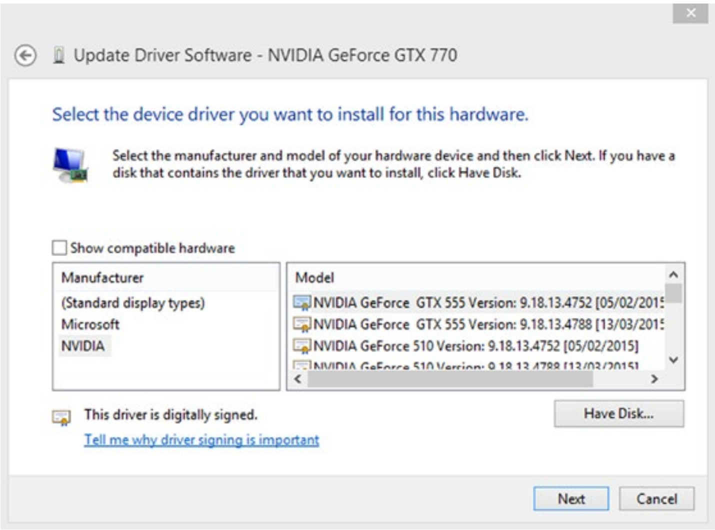
Tell me why driver signing is important

Figure 5-10. *Windows first displays drivers that it has detected are compatible*

If the hardware you seek is present in the list, you can select it and click **Next** to install the driver. There are two additional options, however.

The first of these is a **Have Disk** button. You might want to use it if Windows has correctly identified a driver, but the version of that driver is older, or perhaps causes issues on your PC.

The second option is the **Show compatible hardware** check box. Unchecking this displays a list of all the hardware drivers that are available on your PC for the particular device type you have selected (see Figure 5-11).



Update Driver Software - NVIDIA GeForce GTX 770

Select the device driver you want to install for this hardware.

Select the manufacturer and model of your hardware device and then click Next. If you have a disk that contains the driver that you want to install, click Have Disk.

☐ Show compatible hardware

Manufacturer
(Standard display types)
Microsoft
NVIDIA

Model
NVIDIA GeForce GTX 555 Version: 9.18.13.4752 [05/02/201
NVIDIA GeForce GTX 555 Version: 9.18.13.4788 [13/03/201
NVIDIA GeForce 510 Version: 9.18.13.4752 [05/02/2015]
NVIDIA GeForce 510 Version: 9.18.13.4788 [13/03/2015]

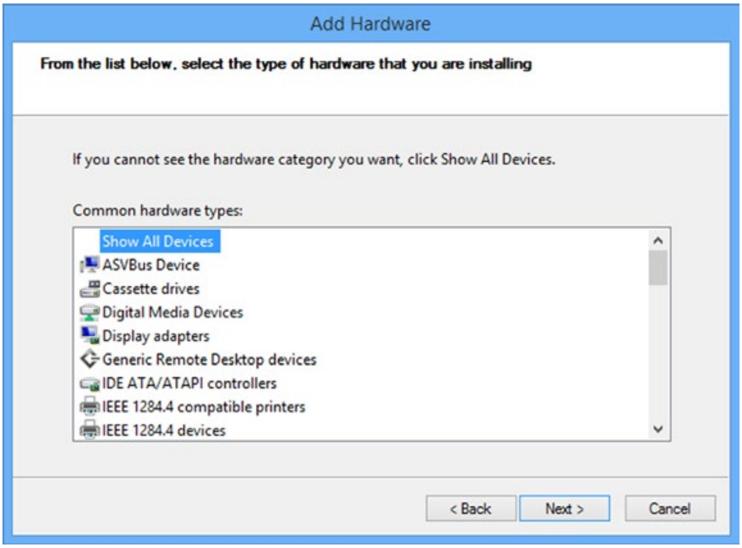
This driver is digitally signed.

Tell me why driver signing is important

Figure 5-11. *You can choose from many drivers that come with your copy of Windows*

The list of available drivers varies depending on the version of Windows and which service pack you are using; or in the case of Windows 8.1 and Windows 10, the major update pack that is installed.

■ **Note** If the device type you are installing is listed as **Other devices**, you are presented with a list of all device types available. For the drivers to appear, you need to select the correct device type (see Figure 5-12).



Add Hardware

From the list below, select the type of hardware that you are installing

If you cannot see the hardware category you want, click Show All Devices.

Common hardware types:

Figure 5-12. *You can choose from a wide range of device types when installing legacy devices*

Installing Legacy Device Drivers

While Windows is extremely good at recognizing and automatically installing modern hardware, the *Plug and Play* feature was only introduced with USB. Any pre- and some non-USB hardware, and even some earlier USB devices, won't be automatically detected.

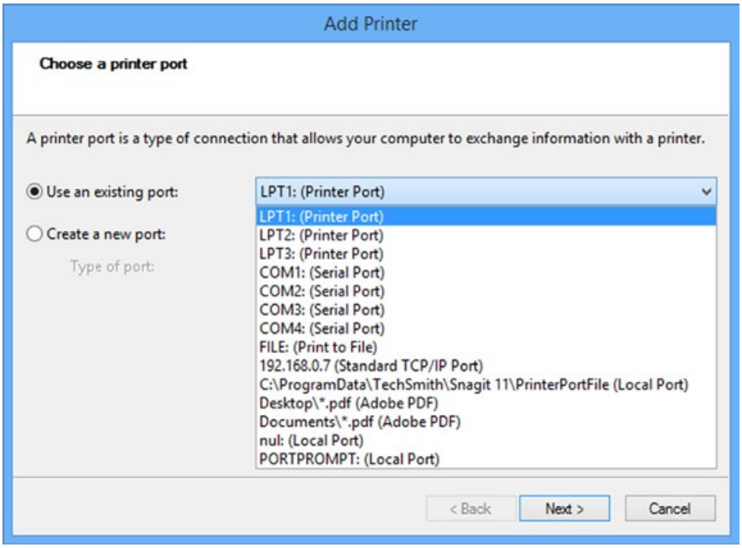
If you are installing a serial or parallel device, for example, it will not even show in Device Manager as an **Other device**[s]. All is not lost, though. In the Action menu in the Device Manager, click the **Add legacy hardware** option to install it.

You are first asked if you want Windows to automatically detect the device or if you want to install it manually. The first option works for some device types, such as some early USB devices or non-USB devices with more modern interfaces (e.g., Firewire or DIMM or PCIe SSDs).

Choosing to install the driver manually displays a list of all the different device types included with Windows (see Figure 5-12).

The options you get from here will vary, depending on the hardware type you have selected. For example, choosing to install a dial-up modem displays a wizard asking you to make sure that your modem is switched on and to quit any programs that might be using it (because some software can lock a device), with an additional option to choose and install the modem manually.

If you choose to install a printer (see Figure 5-13), however, you are given the option to use an existing port based on what the printer is attached to (LPT ports are for parallel printers), or to create a new port for the device (perhaps because the parallel ports on your PC are not yet installed).



Add Printer

Choose a printer port

A printer port is a type of connection that allows your computer to exchange information with a printer.

● Use an existing port: LPT1: (Printer Port)

○ Create a new port:

Type of port:

- LPT1: (Printer Port)
- LPT2: (Printer Port)
- LPT3: (Printer Port)
- COM1: (Serial Port)
- COM2: (Serial Port)
- COM3: (Serial Port)
- COM4: (Serial Port)
- FILE: (Print to File)
- 192.168.0.7 (Standard TCP/IP Port)
- C:\ProgramData\TechSmith\Snagit 11\PrinterPortFile (Local Port)
- Desktop*.pdf (Adobe PDF)
- Documents*.pdf (Adobe PDF)
- nul: (Local Port)
- PORTPROMPT: (Local Port)

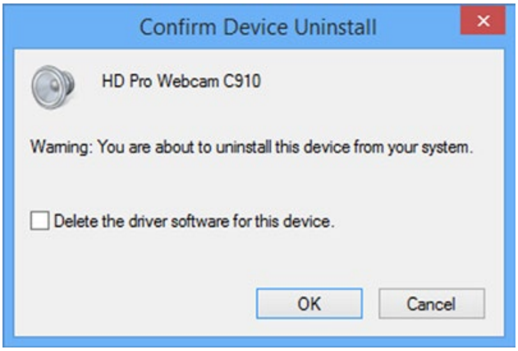
Figure 5-13. *The install options for legacy hardware include additional wizards*

Disabling and Uninstalling Device Drivers

You may find that you want to disable a device or uninstall it completely. Disabling a device can be useful if it is faulty, but you cannot physically remove it; for instance, if it is built into a laptop's motherboard. I experienced this most recently with a touch screen, where the plastic bezel surround had come slightly loose, causing the touch panel to malfunction and constantly believe it was being touched in a very specific spot. Disabling the device (which in this case I had to do in Safe Mode) stopped the problem until I could get the bezel snapped back into place correctly.

You can disable or uninstall a device by right-clicking it in the Device Manager and selecting either Disable or Uninstall from the options that appear.

Some, but not all, drivers also give you a **Delete the driver software for this device** check box option (see Figure 5-14).



HD Pro Webcam C910

Waming: You are about to uninstall this device from your system.

□ Delete the driver software for this device.

Figure 5-14. *Some device drivers include an option to delete the driver files from your PC*

Checking this option can be useful if you have a driver that is unstable and causes problems, incompatibilities, and crashes, because it prevents that driver from being automatically reinstalled when you restart the PC, or check for hardware changes or drivers in Windows Update.

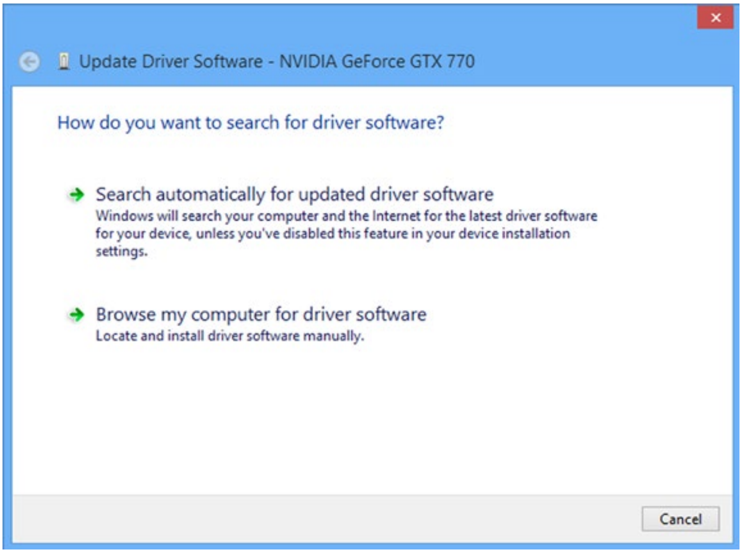
Updating Device Drivers

There are several ways to update device drivers in Windows. Some, but not all, drivers come through Windows Update, and these drivers are always digitally signed. As I've mentioned previously in this chapter, however, drivers delivered through Windows Update can be slightly older due to the length of the submission process, and they are not immune to causing incompatibilities or other problems on a PC.

You might have software running on your PC that can automatically check for driver updates; graphics drivers, in particular, come with utilities for this. Your PC may have come with its own update utility that checks for updated drivers as your PC's manufacturer issues them.

If you want to check for an updated driver manually, you can do so by right-clicking the driver in Device Manager and then selecting the **Update driver software** option.

You have two options (see Figure 5-15): search automatically or browse your computer for updated drivers.



Update Driver Software - NVIDIA GeForce GTX 770

How do you want to search for driver software?

→ Search automatically for updated driver software
Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.

→ Browse my computer for driver software
Locate and install driver software manually.

Figure 5-15. *Windows can search for updated drivers in Windows Update*

It's important to note here that that the **Search automatically for updated driver software** searches your PC's locally stored drivers for updates, but only searches Windows Update online. Should you wish to download drivers from another source, such as the manufacturer's web site or from the PC maker, you will need to do this yourself.

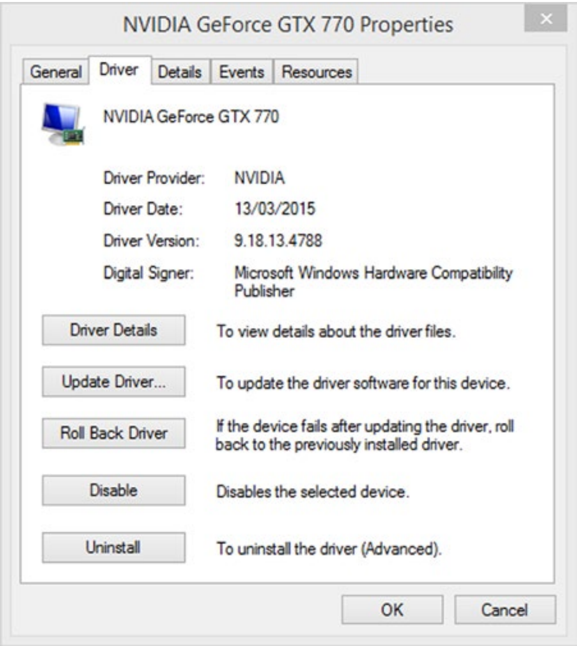
The rest of the process works the same as when you install a new driver, as detailed earlier in this chapter.

Rolling Back Driver Changes

You may find that a driver update sometimes installs a newer driver that is unstable, or that causes a problem on the PC. You don't need to uninstall the driver and reinstall the older one; and given that not every driver presents the check box option to remove its files from the PC, this is a good thing.

Instead, you can roll back an updated driver to its previous version by right-clicking the driver in Device Manager and selecting its Properties.

In the Properties dialog, click the **Driver** tab. You will see a **Roll Back Driver** button (see Figure 5-16).



NVIDIA GeForce GTX 770 Properties

NVIDIA GeForce GTX 770

Driver Provider: NVIDIA

Driver Date: 13/03/2015

Driver Version: 9.18.13.4788

Digital Signer: Microsoft Windows Hardware Compatibility Publisher

To view details about the driver files.

To update the driver software for this device.

If the device fails after updating the driver, roll back to the previously installed driver.

Disables the selected device.

To uninstall the driver (Advanced).

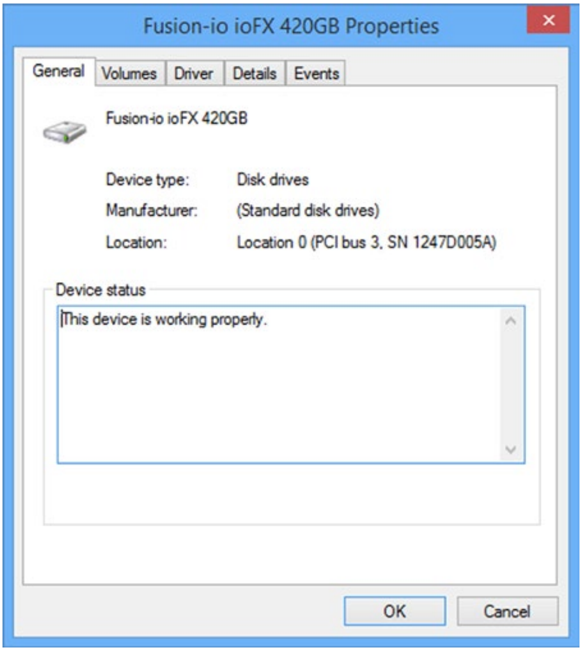
Figure 5-16. *You can roll back updated drivers to the previous driver*

You can use this roll back feature to remove the currently installed driver and reinstall the previous one. This feature only stores the last driver that was installed; it does not keep copies of previous drivers that were installed over time.

■ **Note** The Roll Back Driver feature requires System Restore to be active for it to work. If you have disabled System Restore on your PC, this option is grayed-out and unavailable.

Managing Driver Properties

Double-clicking a driver (or right-clicking it and selecting Properties from the context menu) opens its properties inspector (see Figure 5-17).



Fusion-io ioFX 420GB

Device type: Disk drives

Manufacturer: (Standard disk drives)

Location: Location 0 (PCI bus 3, SN 1247D005A)

Device status

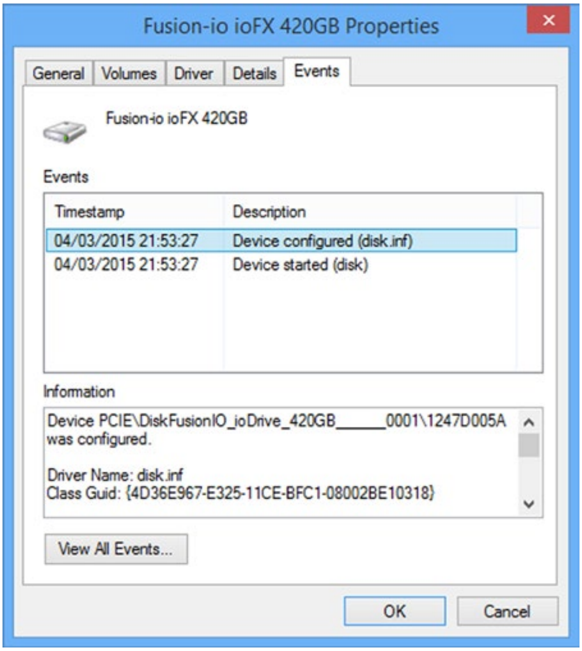
This device is working properly.

Figure 5-17. *The properties inspector for a device driver*

The tabbed interface for the drive varies by the type of device that you have open. All devices display General, Driver, Details, and Events tabs. Disk drives also display a Volumes tab, where you can find information about the partitions located on that disk, and other drivers may display tabs for Advanced, Resources, Power Management, or Settings.

■ **Note** You can find a complete list of the information and error codes that appear in the Device Status box on the Microsoft Support web site at `http://pcs.tv/1JAkN5z`.

If there are any problems with a device, such as it is not working, you are informed in the General tab. We'll look at the Driver and Details tabs later in this chapter. The Events tab is also where problems and errors are reported, along with general audit information about device operation (see Figure 5-18).



Fusion-io ioFX 420GB

Events

Timestamp	Description
04/03/2015 21:53:27	Device configured (disk.inf)
04/03/2015 21:53:27	Device started (disk)

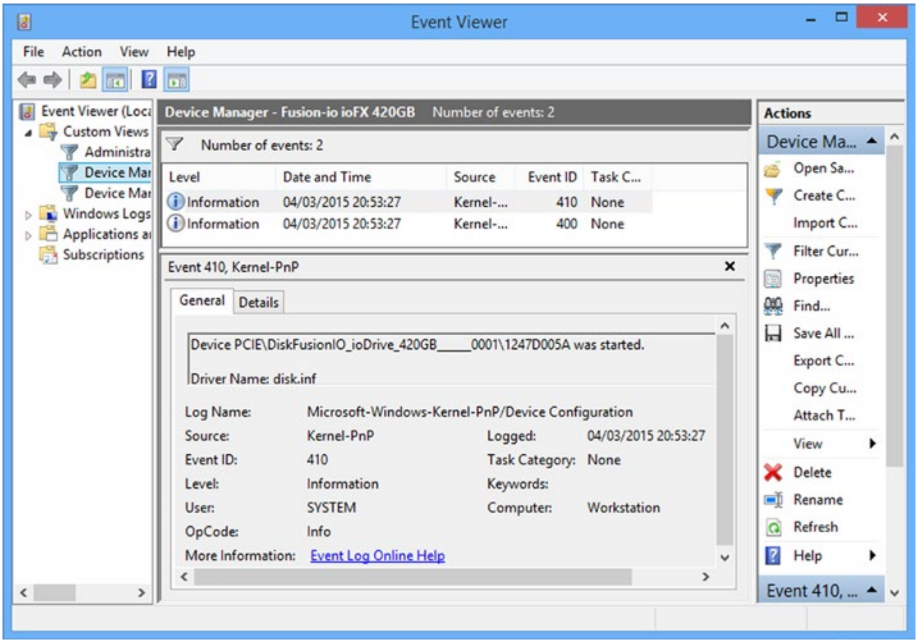
Information

Device PCIE\DiskFusionIO_ioDrive_420GB______0001\1247D005A was configured.

Driver Name: disk.inf
Class Guid: {4D36E967-E325-11CE-BFC1-08002BE10318}

Figure 5-18. *The Events tab contains details of audit processes, errors, and crashes*

Clicking the **View All Events** button opens the Windows Event Manager; here you can get detailed information on driver crashes, errors, and other events (see Figure 5-19).



Device Manager - Fusion-io ioFX 420GB   Number of events: 2

Number of events: 2

Level	Date and Time	Source	Event ID	Task C...
Information	04/03/2015 20:53:27	Kernel-...	410	None
Information	04/03/2015 20:53:27	Kernel-...	400	None

Event 410, Kernel-PnP

Device PCIE\DiskFusionIO_ioDrive_420GB_____0001\1247D005A was started.

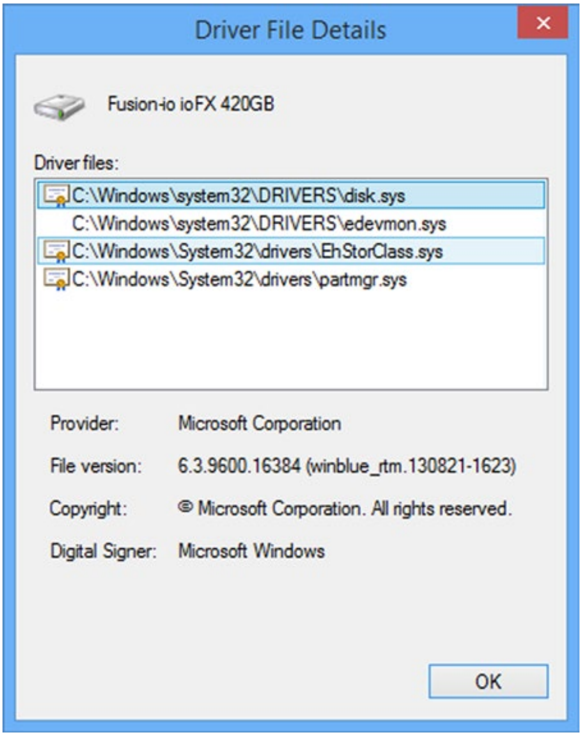
Driver Name: disk.inf

Log Name:	Microsoft-Windows-Kernel-PnP/Device Configuration		
Source:	Kernel-PnP	Logged:	04/03/2015 20:53:27
Event ID:	410	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Workstation
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 5-19. *You can view driver events in the Event Viewer*

If an error or crash has occurs, you see a Windows error code. Stop error codes, for example, are in a 0x00000000 format, where the numbers change but the *x* remains in place.

Clicking the **Driver** tab in the driver properties dialog presents a **Driver Details** button. You can click this to get a list of all the files (and their locations on your PC) that make up a particular device driver (see Figure 5-20).



Fusion-io ioFX 420GB

Driver files:

C:\Windows\system32\DRIVERS\disk.sys
C:\Windows\system32\DRIVERS\edevmon.sys
C:\Windows\System32\drivers\EhStorClass.sys
C:\Windows\System32\drivers\partmgr.sys

Provider: Microsoft Corporation
File version: 6.3.9600.16384 (winblue_rtm.130821-1623)
Copyright: © Microsoft Corporation. All rights reserved.
Digital Signer: Microsoft Windows

Figure 5-20. *You can get details of all the files that make up your device driver*

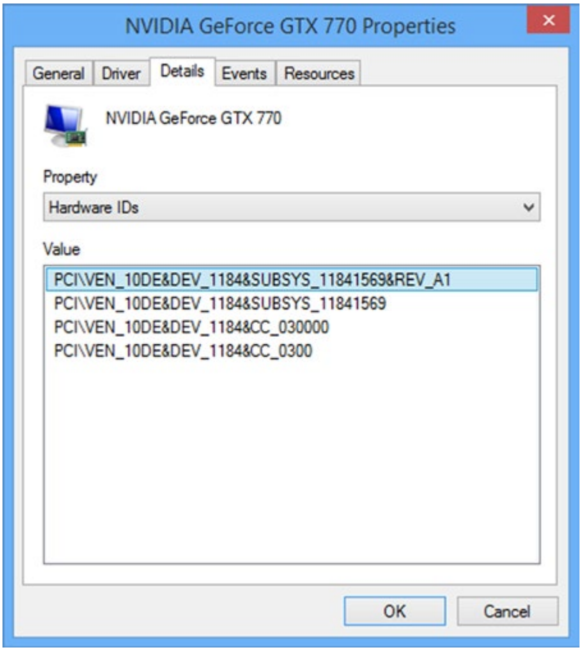
This file list can be useful if, for example, you need to completely uninstall a faulty driver, but the check box option to delete all the driver files from your PC isn't available, so you need to delete the files manually.

■ **Note** Some drivers may share files, and so in some rare cases, manually deleting a driver file may cause another device to become unstable or fail to operate.

The last tab in the driver properties dialog is the Details tab. The information available in the drop-down dialog here varies, depending on the hardware you have installed, but this is where you can check useful information, such as the driver version.

One particularly useful piece of information that can be obtained here is the Hardware ID[s], which can be used to identify hardware that Windows is unable to identify automatically.

Each piece of hardware comes with two unique codes embedded in the device. These are the Vendor and the Device IDs, which are identified by VEN_ and DEV_ codes (see Figure 5-21).

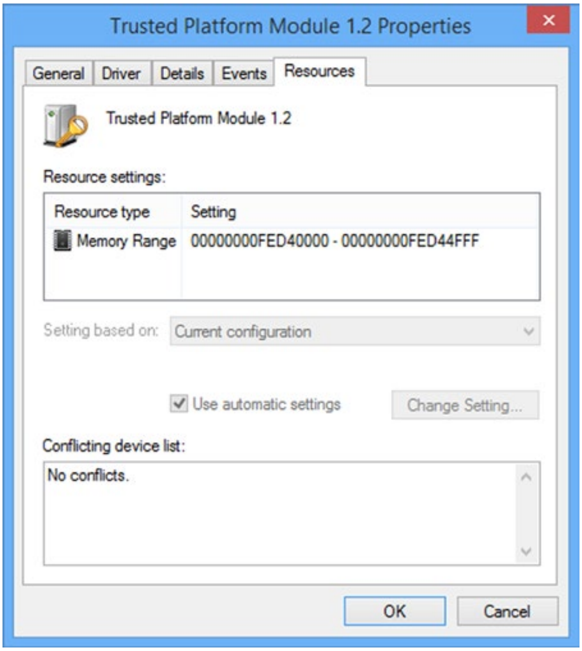


PCI\VEN_10DE&DEV_1184&SUBSYS_11841569&REV_A1
PCI\VEN_10DE&DEV_1184&SUBSYS_11841569
PCI\VEN_10DE&DEV_1184&CC_030000
PCI\VEN_10DE&DEV_1184&CC_0300

Figure 5-21. *You can identify hardware by its VEN_ and DEV_ IDs*

Armed with these codes, which in the example given are VEN_10DE and DEV_1184, you can search online to find what the device is. This can help with downloading and installing the correct driver.

Lastly, in the device properties panel, some devices have a Resources tab, detailing settings such as memory usage or IRQ addresses (see Figure 5-22).



Trusted Platform Module 1.2 Properties

Trusted Platform Module 1.2

Resource settings:

Resource type	Setting
Memory Range	00000000FED40000 - 00000000FED44FFF

Setting based on: Current configuration

☑ Use automatic settings

Conflicting device list:

No conflicts.

Figure 5-22. ***Some drivers have a Resources tab with extra details***

Some settings can be changed on a few drivers (but not many). If settings are available for configuration, you are able to uncheck the **Use automatic settings** option and click the **Change Setting** button.

Using Safe Mode and Diagnostic Mode

If you are a seasoned PC user, you are likely aware of Safe Mode. It is a reduced functionality mode—into which you can start Windows—that only loads the basic drivers needed to operate the PC, so that you can make changes and repair problems.

Safe Mode can be accessed from the boot options menu; although how you access this in Windows 7, Windows 8.1, and Windows 10 is different because of the speed with which Windows 8.1 and Windows 10 starts. In Windows 7, press the **F8** key on your keyboard after the BIOS/UEFI screen has disappeared but before the Starting Windows logo appears. The Boot Options menu will then appear with several Safe Mode options.

The following are the three options available to you:

- **Safe Mode**: A standard reduced functionality mode with a minimal set of drivers and services loaded.
- **Safe Mode with Networking**: A reduced functionality mode with network drivers loaded.
- **Safe Mode with Command Prompt**: A non-GUI Safe Mode enabling work in the Windows Command environment.

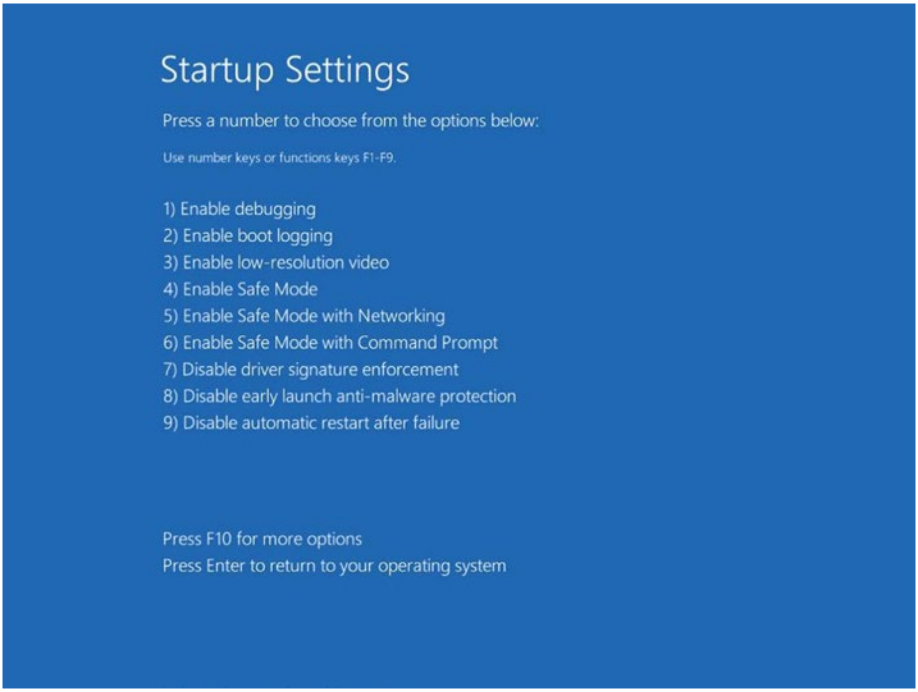
Windows 8.1 and Windows 10 start so quickly, however, that you have literally milliseconds in which to press F8. There are other options, however. If you can get to the Windows desktop, hold down the **Shift** key when you restart the PC to access the Startup Options menu.

If you cannot boot to the desktop, you can use a USB Recovery Drive (created in the Control Panel ä Recovery options), which takes you to Startup Options.

When you are viewing the Windows 8.1 and Windows 10 blue startup options screen, you can find Safe Mode by doing the following:

1. At the main Windows 8 recovery screen, click **Troubleshoot**.
2. At the next screen, click **Advanced options**.
3. Finally, click **Startup Settings**.

Your PC will restart and the Startup Settings (see Figure 5-23) will display. These are the same as the options in Windows 7. Press the number next to the option you that you want to launch it with.



Startup Settings

Press a number to choose from the options below:

Use number keys or functions keys F1-F9.

1) Enable debugging
2) Enable boot logging
3) Enable low-resolution video
4) Enable Safe Mode
5) Enable Safe Mode with Networking
6) Enable Safe Mode with Command Prompt
7) Disable driver signature enforcement
8) Disable early launch anti-malware protection
9) Disable automatic restart after failure

Press F10 for more options
Press Enter to return to your operating system

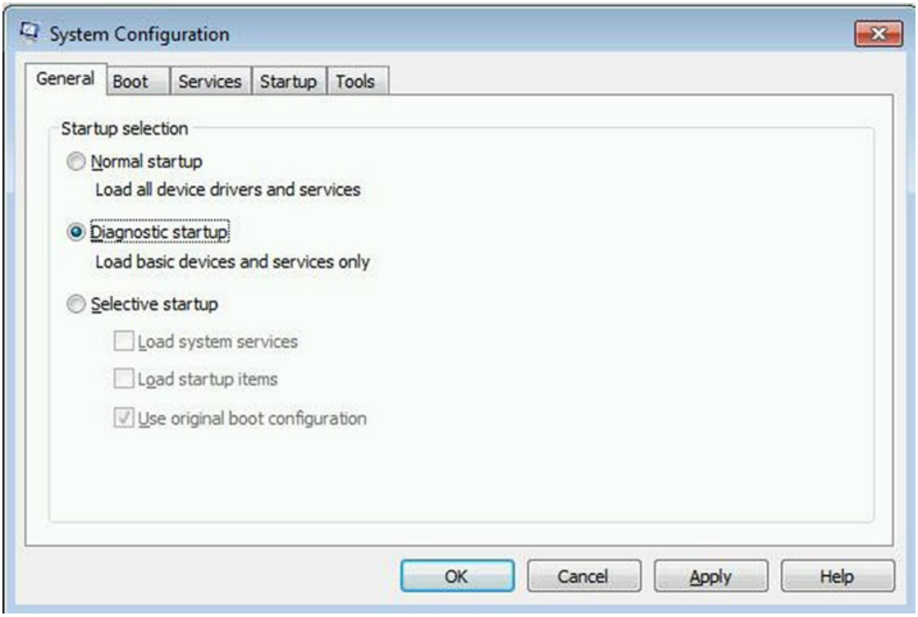
Figure 5-23. *The Windows 8 Startup Settings menu*

■ **Note** If your PC is experiencing BSOD and restarting before you can get a good look at the error, select **Disable automatic restart after failure**. This will set the PC to stop on the blue screen so that you can read it.

Diagnostic Mode

Not every driver problem can be repaired in Safe Mode, however; for example, only very basic graphics drivers are loaded, so installing updated ones is not always possible. Microsoft has thought of this, however, and also includes a Diagnostic Mode.

You access Diagnostic Mode from the System Configuration panel (see Figure 5-24), search for *Msconfig* in the Start menu in Windows 7 and Windows 10, or at the Windows 8.1 Start screen. You start Diagnostic Mode by selecting the **Diagnostic startup** option under the General tab.



Startup selection

○ Normal startup
Load all device drivers and services

● Diagnostic startup
Load basic devices and services only

○ Selective startup
□ Load system services
□ Load startup items
☑ Use original boot configuration

Figure 5-24. *The Msconfig panel*

Diagnostic Mode is a halfway house between Safe Mode and the full desktop, and it permits access to Windows features that are unavailable in Safe Mode, such as some administrative options, the Network and Sharing Center, and Windows Defender.

Diagnostic Mode also loads a more advanced graphics driver, permitting you to use the full resolution of your monitor (see Figure 5-25), because it loads more drivers and services than Safe Mode.

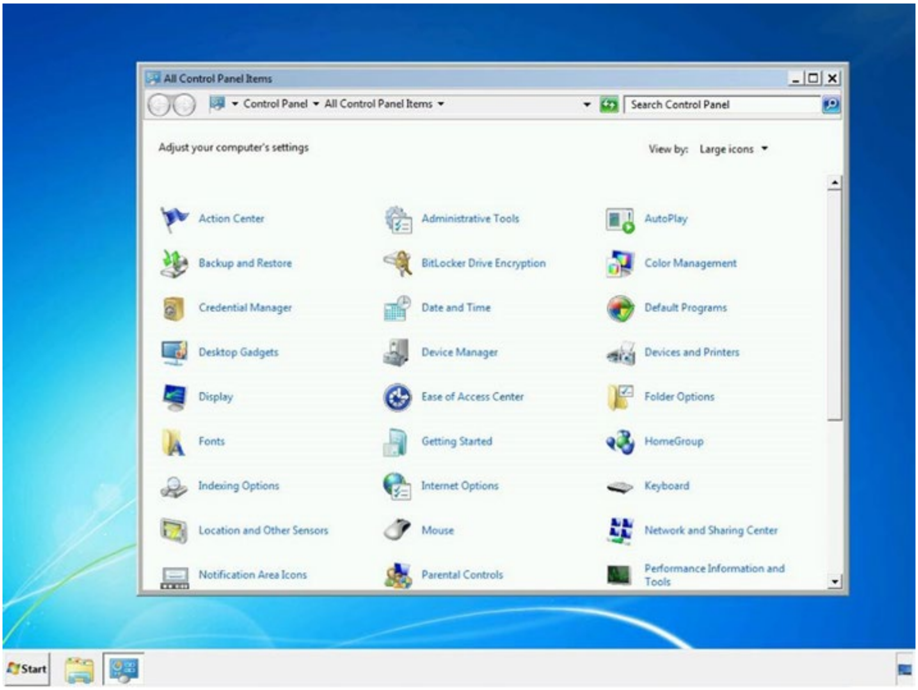


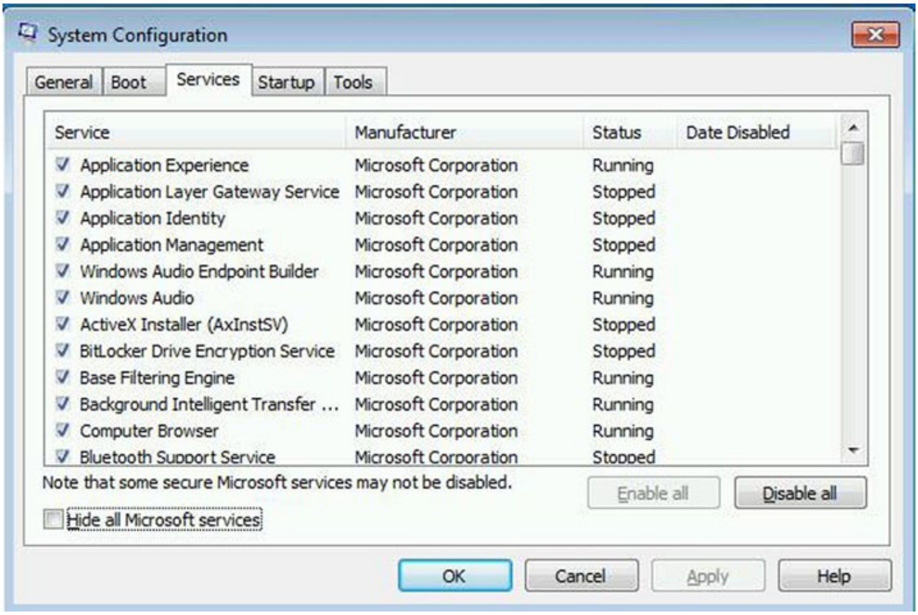
Figure 5-25. *Windows Diagnostic Mode*

It’s important to note that activating Diagnostic Mode from the System Configuration options (as with Safe Mode, which I explain shortly) locks the PC into that startup option until you access Msconfig again and deactivate it by selecting **Normal Startup**.

Diagnostic Mode looks much more like a full Windows desktop, but what it doesn’t do is load any third-party (non-Microsoft) startup programs or services. If you suspect that a third-party program or service is causing a problem, you can use Diagnostic Mode to disable, upgrade, or uninstall it.

Disabling startup programs in Windows 7 and Windows 8.1/Windows 10 is handled differently. In Windows 7, click the **Startup** tab in the System Configuration panel to see all of your startup programs listed. In Windows 8.1 and Windows 10, the Startup tab still exists, but it is empty. To disable startup programs in Windows 8.1 and Windows 10, open the Task Manager (Ctrl+Alt+Delete on your keyboard, or right-click the taskbar) and you will see a Startup tab. Once a program is selected, a Disable (or Enable) button appears in the bottom right of the window.

If you want to disable third-party or even Windows services in Windows, search for *services.msc* at the Start screen or Start menu search box. This displays the full Services management window. However, you can also disable services from the System Configuration panel via the Services tab (see Figure 5-26).



Service	Manufacturer	Status	Date Disabled
☑ Application Experience	Microsoft Corporation	Running	
☑ Application Layer Gateway Service	Microsoft Corporation	Stopped	
☑ Application Identity	Microsoft Corporation	Stopped	
☑ Application Management	Microsoft Corporation	Stopped	
☑ Windows Audio Endpoint Builder	Microsoft Corporation	Running	
☑ Windows Audio	Microsoft Corporation	Running	
☑ ActiveX Installer (AxInstSV)	Microsoft Corporation	Stopped	
☑ BitLocker Drive Encryption Service	Microsoft Corporation	Stopped	
☑ Base Filtering Engine	Microsoft Corporation	Running	
☑ Background Intelligent Transfer ...	Microsoft Corporation	Running	
☑ Computer Browser	Microsoft Corporation	Running	
☑ Bluetooth Support Service	Microsoft Corporation	Stopped	

Note that some secure Microsoft services may not be disabled.

□ Hide all Microsoft services

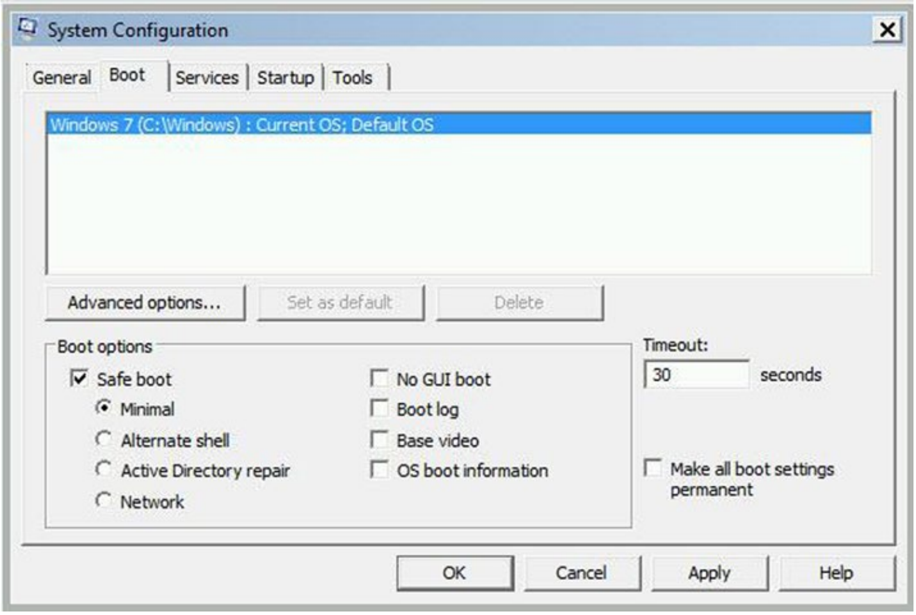
Figure 5-26. *Disabling Windows Services at startup*

The System Configuration panel has a **Hide all Microsoft services** check box that can be useful for managing services. Selecting this option changes the display to list only third-party services.

Don't forget that just like the startup options in the System Configuration panel, anything you disable needs to be reenabled before it will work again.

Forcing Safe Mode

Just as you can use the System Configuration panel to force Diagnostic Mode, so too can you use it to force Safe Mode. In many ways, this gives you greater control and flexibility over the use of Safe Mode than you get from the Windows boot options menu (see Figure 5-27).



Windows 7 (C:\Windows) : Current OS; Default OS

Boot options

☑ Safe boot

● Minimal

○ Alternate shell

○ Active Directory repair

○ Network

☐ No GUI boot

☐ Boot log

☐ Base video

☐ OS boot information

Timeout: 30 seconds

☐ Make all boot settings permanent

Figure 5-27. Forcing Safe Mode in Windows

The Boot tab contains the options for Safe Mode, with the default option being Safe boot ä Minimal. The following are the other options that are available:

- **Safe boot: Minimal** opens Safe Mode running critical Windows services only.
- **Safe boot: Alternate shell** opens the Command Prompt with Windows running critical services only. In this mode, both networking and File Explorer are disabled.
- **Safe boot: Active Directory repair** is used for troubleshooting a domain controller within a corporate environment. Selecting this option runs critical services in addition to Active Directory.
- **Safe boot: Network** runs Safe Mode with critical services and networking enabled.
- **No GUI boot** allows you to not display the Windows welcome screen when starting.
- **Boot log** is perhaps the most useful option, storing a log file of the entire startup process in the `%systemroot%Ntbtlog.txt` file.
- **Base video** forces Safe Mode to use standard VGA graphics drivers.
- **OS boot information** displays driver names as they are loaded at startup.

Don't forget that just as with Diagnostic Mode, enabling Safe Mode in the System Configuration panel also requires you to later disable it to allow Windows to start normally again.

Cables and Physical Hardware Faults

When Apple first introduced the MagSafe charging plug, it was hailed as the solution laptop owners had been waiting for. No longer would they trip over their power lead and bring their expensive laptop crashing to the floor, because the plug would simply and harmlessly pull away from the laptop instead.

A variation on MagSafe was later adopted by Microsoft for its Surface tablets, but alas they all now seem to have gone the way of the dinosaurs, in favor of small USB charging sockets instead.

If you trip over a cable that's attached to your PC or laptop, and the machine ends up crashing to the ground, it'll be fairly obvious to you afterward what the cause is if a fault develops.

Sometimes, however, problems with cables and plugs can be harder to diagnose. It's always best practice to keep all cables safely hidden away where people can't grab them or trip over them, but damage can still occur.

Network cables are especially prone to damage when pulled, and since they're used on everything from PCs and laptops to printers and switch boxes, it's a problem that can affect many pieces of hardware.

It's always a good idea when diagnosing a hardware problem to first check if any cables or plugs are damaged, and in some extreme cases, if the hardware is actually switched on. (You may laugh, but you'd be surprised how often this is the cause!) Many IT pros keep a selection of "good cables" that they know work well and reliably. Having a set of good cables can help you check if an existing cable is faulty, as you can swap them to see if this rectifies problem.

Additionally, it's worth checking if the socket itself might be damaged. (Be careful with power outlets!) Damaged sockets can cause PC issues, with power and networking sockets being the most common.

On occasion, pulled plugs and leads can also cause physical damage to the PC socket, which is a very good argument for keeping cables safely out of the way, and perhaps even secured with cable ties.

Other problems that can occur include something as simple as plugging a USB 2.0 device into a USB 3.0 socket (or the other way around), which can affect the performance of the device.

Inside a desktop PC's casing, problems such as badly seated PCI cards, a loose processor fan or heatsink and loose internal cabling can occur. Also, poor ventilation is caused by dust build up, the blocking of ports by internal components, or by placing the vents right up against a wall or other barrier.

When diagnosing a problem, it's worthwhile to check whether the PC has been moved recently, so that you can tell if anything has come loose, been dislodged, or was damaged.

Age and simple wear and tear also contribute to problems. Moving parts such as the case and processor fans (and graphics card fans) wear over time and eventually fail. Mechanical hard disks also eventually fail, some faster than others, causing data loss and blue screens.

When working with hardware, it's essential to have the right toolkit and to work safely (especially where electricity is concerned). I'll talk more about safe working in Chapter 6; engineers' toolkits for IT hardware can be picked up online and in electronics stores.

Summary

Device drivers come in all varieties and include both hardware and software drivers. Some have additional options and settings hidden away in the driver, with others needing manual installation when Windows is unable to identify them.

The sheer number of variations with device drivers therefore means that they are very often the number-one cause of problems on a PC.

Other factors can still cause problems, however, such as environmental complications, human intervention, and unsafe operation. In the next chapter, we'll look at how each of these can affect your PC—its software and its hardware.

CHAPTER 6

External Factors That Affect Hardware

In the last chapter, you looked at how physical hardware faults and cable breaks can be the cause of problems on a PC, and indeed tripping over power and USB cables is a common hazard in the workplace, where many a laptop has come to a shattering end.

The contributory factors for hardware problems with PCs, however, don't end with the devices that are plugged into them. All around you are things that can cause problems on a PC, and in this chapter that's exactly what you're going to look at.

Safely Working with Hardware

Before we jump into this subject in detail, though, I want to spend a little time looking at how you can work safely with your PC's hardware, and why it's important to do so. You might always exercise common sense when working with hardware, but the people around you, including those on your own team, might not do so.

Indeed, when I wrote my first Windows troubleshooting book some years ago, I devoted half a page to how you can safely vacuum the inside of a PC in what I called my "Drying the dog in the microwave moment." This was because while it was perfectly obvious to me that the vacuum cleaner should be on a low power setting, and that a soft brush attachment should be used to very gently brush the components inside the PC, other people might not be so gentle and would ultimately damage their components by using too much force.

Watt on Ground?!

Computers, as we all know, run on electricity (it's always nice to state the completely obvious once in each book). What people sometimes tend to forget, though, is that so do we. Without an electric current running through our bodies, our hearts would stop, our brains wouldn't function, and we'd simply fall over and die.

M. Halsey and A. Bettany, *Windows Software Compatibility and Hardware Troubleshooting*,
DOI 10.1007/978-1-4842-1061-1_6

Now we can't compare the electric current that runs through our bodies to that which runs through our PCs, because the human body runs on tiny voltages. What's important to remember is that the components in our processors, memory chips, and motherboards, which are in some cases only a few nanometers wide, run on voltages that are just as tiny, if not more so.

This is compounded by the fact that the human body often acts in a similar way to an electromagnet. There is a significant amount of iron in our blood, and as electrical signals pass around the human body and through the brain, they can generate an electromagnetic field. It's because of this that you sometimes get a small electric shock when you touch something that is grounded, such as the call button on an elevator, or a stair railing.

Now I'm no expert in either biology or physics, as you might have guessed, but it's clear that if we can ground ourselves on a stair railing, we can also ground ourselves on components inside our PCs.

For this reason, it's essential that you work in a safe and grounded environment. You can do this in several ways. The first of these is to wear an antistatic wristband when working with your PC (see Figure 6-1).

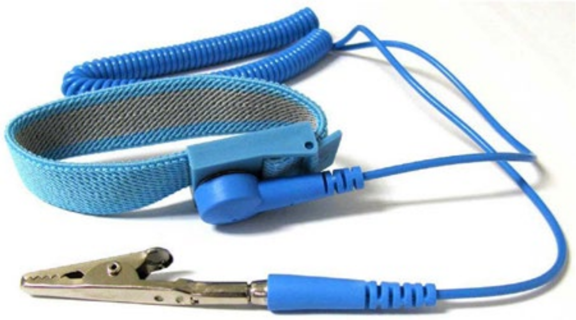


Figure 6-1. *An antistatic wristband can help prevent you from passing current into your PC*

■ **Note** For laptops, you should always remove the battery, if possible. If the laptop or tablet does not have a removable battery, ensure that the PC is properly switched off and not in sleep mode or hibernate mode.

Wearing an antistatic wristband around your wrist and clipping the other end to the PC's case can harmlessly dissipate any current in your body. If you use a power system in your country that includes an earth line, or if earth lines are supported but not commonly used (such as in the United States), then first plugging the PC into the wall socket with a lead that includes an earth pin and wire, will safely dissipate the excess electricity in your body. *Remember to unplug the PC from the mains electricity, however, before you start working on it.*

Any other material that can conduct electricity can be used to ground your body. (Except water, obviously, as that would be stupid. And now I'm thinking about that poor dog again!) This includes wood, and a wooden desk is a good place to repair a PC. Just to restate, you should not repair a PC in a garden pond or at the beach.

Something to avoid, however, is nylon carpet, which is common in the workplace, especially if you have carpet tiles. Nylon generates static electricity when you rub compatible materials over it, such as non-rubber-soled shoes. Try to work on a solid wood or tiled floor if possible.

■ **Note** If you are working on a laptop or tablet that cannot easily be grounded, attaching an antistatic wristband to a metal or wooden desk can also effectively ground your body.

Being Safe and Stable

The next consideration is *where* you will work on the PC. For all of you who have repaired PCs over the years, you have likely, at some time or another, looked with envy at a large workbench with plenty of space for working, and storage racks for tools and equipment. In truth, though, while a dedicated work bench is a useful luxury, what's really needed is a good, stable worktop.

Always check the table or desk on which you will be working on a PC. If it wobbles, then it shouldn't be used. Sticking some beer coasters under a table leg to stabilize it might a suitable action in a bar, but it is not for safe PC work. The reason is that the components inside the machine are, in some cases, extremely fragile, and a sudden tilt or shake can cause your hand to damage something.

Having plenty of clear space also helps. Shelves on which you store tools and equipment are a hazard to anything below them if knocked accidentally; this includes your work area.

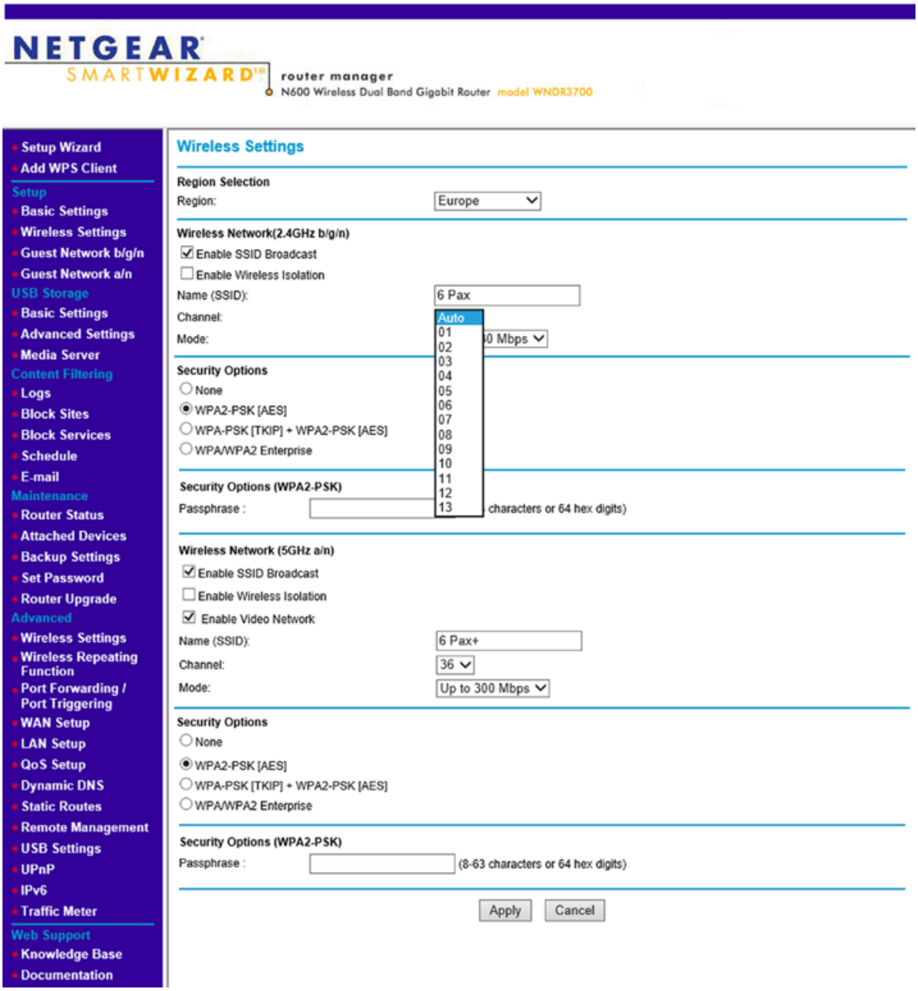
Attack of the Interferoids!

How many times have you been using a laptop or tablet and just had an awful Wi-Fi signal? This is usually compounded by the fact that you scream, "The router is only ten feet away!!" while tearing out what remains of your hair.

The reason problems such as this occur is due to a number of environmental factors that can interfere with our devices.

The most obvious and likely cause of interference is other devices, especially Wi-Fi and Bluetooth devices interrupting or confusing your signal. In truth, however, this almost never happens because the radio frequency spectrums for different types of devices are heavily regulated around the world. Even in countries where there is little or no such regulation, the devices in use still comply with the regulations of other countries.

Very rarely you might find Wi-Fi problems caused by a router, but only really on older hardware. To rectify this, you can access the Wi-Fi network settings in the router and switch it to a different channel (see Figure 6-2). If your neighbor is using a router similar to your own, and both are set to the default channel 1, changing to something else, such as channel 7, can quickly solve most problems.



Wireless Settings

Region Selection
Region: Europe

Wireless Network(2.4GHz b/g/n)
☑ Enable SSID Broadcast
□ Enable Wireless Isolation
Name (SSID): 6 Pax
Channel: Auto
Auto 01 02 03 04 05 06 07 08 09 10 11 12 13
Mode: 0 Mbps

Security Options
○ None
● WPA2-PSK [AES]
○ WPA-PSK [TKIP] + WPA2-PSK [AES]
○ WPA/WPA2 Enterprise

Security Options (WPA2-PSK)
Passphrase : characters or 64 hex digits)

Wireless Network (5GHz a/n)
☑ Enable SSID Broadcast
□ Enable Wireless Isolation
☑ Enable Video Network
Name (SSID): 6 Pax+
Channel: 36
Mode: Up to 300 Mbps

Security Options
○ None
● WPA2-PSK [AES]
○ WPA-PSK [TKIP] + WPA2-PSK [AES]
○ WPA/WPA2 Enterprise

Security Options (WPA2-PSK)
Passphrase : (8-63 characters or 64 hex digits)

Figure 6-2. *Changing the Wi-Fi channel in your router settings*

You might be surprised by which other devices in the home and workplace can cause radio or other types of interference for your computers, and not just for wireless communication such as Wi-Fi and Bluetooth.

Older televisions, refrigerators, “ham” radios, and other devices can cause interference if placed too close to your PCs or network hardware. The rule here is to avoid placing anything near PCs that uses radio frequencies or that has a powerful motor. This is, of course, yet another reason why microwave ovens should be kept at a safe distance.

UTP Network Cables

Most network cables, including those used for telephony and VoIP systems, are designed using a technique called *unshielded twisted pair*, or UTP. The reasons for this are primarily based on the lower costs for producing such cables, compared to more resilient solutions such as fiber-optic cable.

UTP cables, as the name suggests, are susceptible to interference, both radio and electrical. For this reason it’s a very good idea to keep your network cables away from the power leads for your PCs, and from other electrical equipment, such as uninterruptable power supplies (UPS).

Shielded cables are available, but are more expensive than standard cable, and you can also get shielded cables for other PC purposes, such as display and USB leads.

Hitting a Wall

Earlier in the chapter, I wrote about the problems you can face in getting a good and stable Wi-Fi connection. After all, you might have a super-fast broadband line, but struggle to get a reliable 5Mbps on your laptop.

The most common causes of Wi-Fi connection problems are range and line-of-sight. Try placing your Wi-Fi router in a central location, without barriers around it, and not too far from your PCs.

What do I mean by barriers? People in some countries, such as the United States, are often frustrated by Wi-Fi connection problems when they travel to other parts of the world, such as Europe. The big difference between these two parts of the world is the building materials used in constructing homes and offices.

Some countries, such as the United States, use wood and other light materials to construct buildings. These light materials allow Wi-Fi and other radio signals to pass through them fairly easily.

In other parts of the world, however, such as Europe, it is common to use brick construction, and a large proportion of the buildings still in use are constructed from heavy stone, sometimes many hundreds of years old, and where the thickness of walls can often reach 12 inches or more. These materials very effectively block Wi-Fi and other radio signals, including those of cellular networks.

In some cases, you might find that you want to use Wi-Fi repeaters or range extenders (and perhaps even a femtocell to improve the signal of your mobile phone, which runs your phone signal through your broadband line).

Beware the Humans

It's often argued that a PC that's left in the box and never touched by a user will work reliably for many years without ever encountering a single problem. The point of this statement is that nothing ever goes wrong with a PC without a person being directly involved in some way.

A few years back, I worked for a major IT firm, providing support for blue-chip companies. One day, a colleague took a call from a manager at one of these companies, who said that his keyboard wasn't working.

He'd decided that his keyboard was dirty and had taken it upon himself to fill his sink with hot, soapy water and give the keyboard a good scrub. Acknowledging that using it while it was wet would be a bad idea, he hung it up to dry overnight, but discovered come morning that nothing would work.

My colleague, on checking the asset tag code, had to point out to the man that the reason his keyboard didn't work was because it was built in to the rest of his laptop!

This is a fairly extreme case, but we have all heard stories similar to this over the years. For example, I remember calling an office manager about a non-functioning printer that one of his staff had reported the previous day.

He was bullishly adamant that his staff would have checked all the cables on the printer and the PC; that they'd have checked the mains power lead, the mains electricity socket, and so on. However, he felt the need to meekly apologize when I asked him if the printer had been switched on.

It's not the fault of the "users" in any way. Computers, even tablets, are still very complex pieces of equipment, and while some people might find navigating their way around an operating system fairly straightforward, others face a much steeper learning curve. When it comes to the hardware of a PC and its device ecosystem, a great many people are completely lost at sea.

Everything boils down to training, and a company that wants a productive and happy workforce should be prepared to invest time and effort in effectively and appropriately training their staff in what they need to know to use their IT equipment. There's little point in training beyond this, but finding the happy medium at which staff will understand everything they need for day-to-day use can be a tremendous asset.

Additional Environmental Factors

You might think that once you've eliminated human error, thick walls, refrigerators, CB radios, unshielded cabling, and the Romans from the equation, there wouldn't be much else to diagnose. Setting aside the problems of damaged cables and sockets I detailed in Chapter 5, however, you'd be surprised that planet Earth and Mother Nature herself can be very unkind to our PCs.

Heat and cold can affect PCs in quite profound ways. It wasn't very long ago that our laptops and early mobile phones had LCD screens that would refresh only very slowly when used outside during the winter months, and hardware that would fail to respond at all if it were a particularly bad winter.

Indeed, all modern technology comes with details of its temperature tolerances, although the equipment we use now is so resilient to these factors that we often tend to ignore, or even discount, such things.

Air conditioners and vacuum cleaners (yes, those things again) can throw up large volumes of dust that settle on case vents, and behind PCs and accessories on desks. It's odd to think that vacuum cleaners can throw dust around a room rather than suck it up, but it's also very true that many vacuum cleaners suck … and suck big-time, especially when not used thoroughly.

Pet hair is another common annoyance for PCs and hardware, although it is not common in the workplace. Just like dust, it is attracted by the electromagnetic fields generated by electrical equipment and it can be found in great clumps behind many home computers.

I've even encountered laptops with problems caused by birds flying overhead, although the less time we spend going into that problem, the better.

Summary

So what's the point of all this? When you're diagnosing and repairing a problem with a PC or a piece of hardware, especially if you're doing it remotely over the phone, it's all too easy to fall back on your IT training and look solely for technical problems.

The world we live in, however, is much more diverse, and can throw up many more diverse problems as a result. The foundation for great IT support is being able to both think and look outside of the box, and this applies as equally to software as it does to hardware.

Throughout this book, we've examined every aspect of diagnosing and troubleshooting problems, and armed with all of this information and an open-minded view of everything else that can contribute to problems, there shouldn't be anything you cannot fix.

Index

M. Halsey and A. Bettany, *Windows Software Compatibility and Hardware Troubleshooting*,
DOI 10.1007/978-1-4842-1061-1