Windows 10 Troubleshooting

Learn to Troubleshoot and Repair Windows 10 Problems Like the Pros Do

—

Second Edition

—

Mike Halsey, MVP

Apress®

Windows 10 Troubleshooting

Learn to Troubleshoot and Repair Windows 10 Problems Like the Pros Do

Second Edition

Mike Halsey

Apress®

Windows 10 Troubleshooting: Learn to Troubleshoot and Repair Windows 10 Problems Like the Pros Do

Mike Halsey
Sheffield, South Yorkshire, UK

ISBN-13 (pbk): 978-1-4842-7470-5 ISBN-13 (electronic): 978-1-4842-7471-2
https://doi.org/10.1007/978-1-4842-7471-2

Copyright © 2022 by Mike Halsey

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

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, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Smriti Srivastava
Development Editor: Laura Berendson
Coordinating Editor: Shrikant Vishwakarma

Cover designed by eStudioCalamar

Cover image designed by Pexels

Distributed to the book trade worldwide by Springer Science+Business Media LLC, 1 New York Plaza, Suite 4600, New York, NY 10004. 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 booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-7470-5. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

For my parents, James and Margaret, who got me started with computers when I was 11 years old and were always supportive and encouraging, and especially for my mother who gave me the push I needed to start a career as an author. This will be my 20th book, so I raise a glass to you both… with thanks!

Table of Contents

About the Author xxiii

About the Technical Reviewers xxv

Introduction xxvii

Part I: Getting Started with Windows Troubleshooting 1

Chapter 1: Introducing Troubleshooting in Windows 10 3

The Three Seashells… 6

The Problems We Encounter 9

Hardware Problems 9

The Tale of the Exploding Charger 10

Software and App Problems 10

Networking Problems 11

Startup Problems 12

OS Installation and Update Problems 12

"Prevention Is Better Than Cure" 13

The Security and Maintenance Center 13

Windows Reliability History 16

Windows Automatic Maintenance 19

Managing Diagnostic Feedback and Privacy 20

Windows' Security Systems 21

Windows Defender Antimalware 21

Windows Firewall 23

Windows App and Browser Control 26

User Account Control 28

Device Security 30

User Account Management 31
Administrators vs. Standard Users 32
Local Accounts vs. Microsoft Accounts 32
User Identity and Sign-In Management 33
An Introduction to Family Safety 37
Managing and Deleting User Accounts 38
Summary 39

Chapter 2: Building a Safe and Secure OS 41

Creating a Recovery Drive 42
Backing Up and Restoring Windows 10 45
Reset 45
System Image Backup 50
Creating a System Image Backup 50
Restoring a System Image Backup 55
Using Windows System Restore 58
Configuring System Restore 62
Using the Windows 10 Media Creation Tool 63
Backing Up Your Files with File History 66
Restoring Deleted and Previous Versions of Files 69
Setting Up and Managing OneDrive 71
Summary 75

Chapter 3: Configuring Windows 10 77

Settings 77
System ➤ Storage 79
Apps ➤ Default Apps 80
System ➤ About 82
Devices ➤ Printers and Scanners/Bluetooth and Other Devices 83
Devices ➤ AutoPlay 83
Phone 83
Network and Internet 84

Personalization 84
Apps 84
Accounts 84
Time and Language 85
Gaming 85
Ease of Access 85
Search 86
Privacy 86
Update and Security ➤ Windows Update 87
Update and Security ➤ Delivery Optimization 88
Update and Security ➤ Windows Security 90
Update and Security ➤ Backup 90
Update and Security ➤ Troubleshoot 90
Update and Recovery ➤ Recovery 90
Update and Security ➤ Activation 91
Update and Security ➤ For Developers 91
Introducing the Control Panel 91
Managing the Virtual Memory, Paging File 92
Managing Remote Connections to the PC 94
Moving the Shell User Folders 95
Creating, Managing, and Deleting Partitions 97
Managing Startup Apps 101
Summary 103

Chapter 4: Fixing Windows 10 Quickly 105

The Disk Cleanup Wizard 105
What Is the Situation with Internet Explorer? 107
Managing IE and Edge 109
Cleaning Temporary and Other Files from IE and Edge 109
Resetting IE 111
Resetting Edge, the Windows Store and Store Apps 112

Defragmenting Your Hard Disks 114
Managing Running Apps and Services with Task Manager 116
Managing win32 App Compatibility 121
Using the System File Checker 125
Using the Automated Troubleshooters 127
Microsoft Answers, Service Status Site, and Being a Twit 129
Summary 132

Chapter 5: Understanding Tasks and Events 133

The Windows Event Viewer 133
Introducing the Microsoft Management Console 133
The Main Events View 137
Making Sense of Error Logs 139
Creating Custom Event Views 142
Creating Event Subscriptions 145
Attaching a Task to an Event 147
Saving, Exporting, and Importing Event Information 153
Summary 155

Chapter 6: Understanding PC Hardware 157

BIOS and UEFI 157
BIOS Virus/Malware Attack 159
Resetting BIOS and UEFI Firmware 161
Power Supplies 164
Jump-Starting a PC 165
The Motherboard 166
The Rear Panel Connectors and Cables 167
Memory 168
Hard Disks, SSDs, M.2, and PCIe Drives 168
Expansion Cards 169

Monitors and Cabling 169
Keyboards and Mice 170
Summary 171

Chapter 7: Diagnosing and Repairing Problems with Hardware and Peripherals 173

Getting USB Devices to Work Reliably 174
Installing and Managing Bluetooth Devices 177
Installing and Configuring Printers 180
Installing Different Types of Printers 180
Finding the Name or IP Address of a Printer 185
Managing Printing Policies 192
Have You Tried [Not] Turning It Off and On Again? 194
Summary 197

Chapter 8: Troubleshooting Startup 199

Have You Tried Turning It Off and On Again? 199
Using Startup Repair 201
The Windows Recovery Options Menu 207
Using the Command Prompt to Repair Windows Startup 210
Summary 212

Chapter 9: Troubleshooting Networks 213

The Network and Sharing Center 213
Configuring Network Connections 216
Managing Network Adapters 222
Managing Network Connections in Settings 223
Network Reset 227
Setting Up and Managing Your Router 228
Troubleshooting Wi-Fi Connection Problems 231
Recovering Lost and Forgotten Wi-Fi Passwords 233
Summary 235

Chapter 10: Troubleshoot and Manage Internet Explorer and Edge 237

Managing IE11 237

Disabling IE 238

Managing Temporary Files in IE 240

Resetting IE11 243

Managing Edge 245

Using Internet Explorer Compatibility Mode 245

Edge System Settings 246

Resetting and Updating Edge 247

Summary 250

Part II: Becoming a Proficient Troubleshooter 253

Chapter 11: Dealing with Common Windows Annoyances 255

User Folders in Incorrect Locations 255

Incorrect File Associations 257

Setting Drive, Folder, and File Permissions 261

Managing Audio Devices 265

Troubleshooting Windows Activation 268

A Note About Windows 10 Extended Support Product Keys 270

Troubleshooting and Resetting Windows Update 271

Troubleshooting Power Loss During an Update Installation 273

Managing and Resetting Windows Search 274

Troubleshooting Slow Startup 275

Windows 10 Hangs on Startup 277

Windows 10 Shuts Down Slowly 278

Windows Fails to Sleep/Resume from Sleep 280

Gaining Access After Bitlocker Lockout 286

Troubleshooting Touchscreen Problems 287

USB Type-C and Thunderbolt Problems 288

No Picture on Desktop PC Monitor or TV 288

Disappearing and Conflicting Drives 289
Understanding the BSOD 290
Summary 294

Chapter 12: Remote Help and Support 295

The Problem Steps Recorder 296
Recording an App with Game Bar 300
Quick Assist 303
Windows Remote Assistance 307
Sending and Responding to a Remote Assistance Request 309
Sending Unsolicited Remote Assistance Offers 318
Remote Desktop 321
Third-Party Remote Support Apps 329
Summary 329

Chapter 13: Repairing Windows Startup Problems 331

Manually Repairing Windows Startup 331
Repairing BIOS Startup Files 332
Repairing UEFI Startup Files 333
Additional Repair Commands for BIOS and UEFI 335
Recreating or Moving the Boot Partition 335
Step 1a: Create a New Boot Partition (Command Prompt) 337
Step 1b: Create a New Boot Partition (Disk Management Console) 338
Step 2: Create the New Boot Files 341
Setting Up and Managing Dual/Multiboot Systems 342
Secure Boot 343
Bitlocker and Dual-Boot Systems 344

Managing Boot Systems with BCDEdit 344
BCDEdit Identifiers 348
BCDEdit Data Formats 348
Examples of BCDEdit Use 349
Effecting Repairs on the Boot Partition Structures 352
Summary 355

Chapter 14: Networks and Internet Connections 357

Checking the Status of a Network Connection 358
Displaying Information About Wi-Fi Networks 365
Prioritizing Wi-Fi Network Connections 368
Diagnosing Network Connection Problems 369
Getting Network Diagnostic Reports from the Event Viewer 369
See the Status of Your Connection with the Performance Monitor 370
See What's Using Your Bandwidth with the Resource Monitor 371
Troubleshooting in the Network and Sharing Center 373
Changing a Network Type Between Private and Public 375
Setting Advanced Network Configuration Options 378
HOSTS, LMHOSTS, and WINS 382
Troubleshooting TCP/IP Connections 385
Ping 385
TraceRT 388
IPConfig 389
Netsh 390
Managing User Profiles 393
Summary 395

Chapter 15: Managing Device Drivers and PC Resources 397

Deciphering the Device Manager 397
Identifying and Installing Unknown Devices 400
Installing Legacy Hardware 406
Uninstalling and Deleting Device Drivers 410

Blocking Device Driver and Device App Installation 411
Finding Device Driver Details and Information 414
Troubleshooting Device Drivers 417
Configuring Driver Parameters 420
Backing Up and Restoring the Driver Store 421
Summary 422

Chapter 16: Windows Update and System Upgrades 423

Deferring Updates in Windows 10 424
Semiannual Channel 425
Long-Term Servicing Channel 426
Choosing How Updates Are Delivered 427
Uninstalling and Blocking Updates 429
Troubleshooting and Repairing Windows Update 431
Repairing the Windows Reset Image 433
Summary 435

Chapter 17: Maintaining App and Website Compatibility 437

Maintaining Compatibility with Win32 Apps 438
Managing Website and Intranet Compatibility 446
Compatibility in Internet Explorer 447
Compatibility in Microsoft Edge 449
Managing Security in IE 450
Resetting IE 455
Managing Security in Edge 456
Setting Your Default Web Browser 458
Using and Managing Progressive Web Apps 461
Program Compatibility Assistant Service 465
The Microsoft Assessment and Deployment Toolkit 466
Windows 365 and Windows Sandbox 466
Summary 468

Chapter 18: Managing Security and Privacy 469

The Last *Pass*Word in Security? 469

To App or Not to App, That Is the Question 470

Memory, Aging, and Neurological Conditions 471

Creating a Strong P455w()rd? 474

Using Two-Factor Authentication 478

Windows Hello 481

Managing Safety and Privacy for Children 483

The Windows Security Center 489

Ransomware Protection 490

App and Browser Control 492

Core Isolation 494

Using the Credential Manager 495

Managing Encryption in Windows 10 497

Using the EFS 498

Managing EFS Encryption with Cipher.exe 501

Managing Device Encryption 502

Encrypting Your PC with Bitlocker 504

Managing a TPM on Your PC and in Windows 10 505

Managing Bitlocker Encryption on Your PC 508

Using Bitlocker To Go 511

Summary 513

Chapter 19: Troubleshooting Viruses and Malware 515

How to Defend Against Malware 515

What Is This Malware Stuff Anyway? 518

Defending PCs Against Malware 519

Defending Your Files Against Ransomware 522

Manually Removing Malware from a PC 523

Microsoft Defender Offline Scan 523

Using Safe Mode and Diagnostic Mode 524

Using a Portable OS to Manually Remove Malware 532

Forensic Investigation and Remove of Malware 533
Step 1: Isolate the PC 533
Step 2: Identify the Malware Processes 537
Step 3: Deactivate the Malware 541
Step 4: Test the Results 544
Step 5: Retest the PC 546
Step 6: Clean Up the Malware 547
Rootkit Removal 548
Using Third-Party Tools to Remove Malware 551
Microsoft DaRT 551
ESET Online (and Offline) Scanner 552
Norton Bootable Recovery Tool 553
Sophos Bootable Antivirus 553
Kaspersky Rescue Disk 553
Kaspersky Ransomware Decryptor 553
AVG Rootkit Scanner and Remover 554
F-Secure Online Scanner 554
McAfee Free Tools 554
D7II 555
RKill 555
Junkware/Adware Removal Tools 555
Microsoft Sysinternals Suite 555
Researching Virus Removal Online 556
Summary 557

Chapter 20: Using Virtualization to Protect PCs 559

Creating and Managing VMs in Hyper-V 561
Managing Networks in Hyper-V 565
Creating Backups of VMs in Hyper-V 568
Managing Hyper-V from PowerShell 570

Booting and Repurposing Your PC from a VM 571
Resetting and Removing Hyper-V Network Connections 572
Creating a VHD 573
Adding a VHD to the Boot Menu 575
Windows Sandbox 578
Windows 365 and Cloud PC 579
Summary 580

Part III: Mastering Windows 10 Troubleshooting 581

Chapter 21: Bomb-Proofing Your PC 583

Creating a Robust Backup Strategy 584
Managing the Work from Home, Workforce 585
Lock Down Your PCs with Group Policy 588
Managing Windows Services 592
Manage Your Local Security Policy 597
Managing Advanced Firewall Policy 599
Summary 604

Chapter 22: Microsoft Sysinternals Suite 607

File and Disk Utilities 607
AccessChk and AccessChk64 608
AccessEnum 609
Contig 609
Disk2Vhd 610
DiskExt 610
Diskmon 611
DiskView 612
DU (Disk Usage) 612
EFSDump 613
FindLinks 613
MoveFile and PendMoves 613
NTFSInfo 614

PsFile 614
SDelete 615
ShareEnum 615
Sigcheck 615
Networking Utilities 615
ADExplorer 615
ADInsight 616
ADRestore 616
PsTools 616
TCPView 620
Whois 621
Process Utilities 622
AutoRuns 622
Handle 624
ListDLLs 624
Portmon 625
ProcDump 625
Process Explorer 626
Process Monitor 629
ShellRunas 630
VMMap 630
Security Utilities 631
LogonSessions 631
Sysmon/Sysmon64 632
System Information Utilities 632
Handle 632
LiveKd 633
LoadOrder 633
RAMMap 634
Miscellaneous Utilities 635
RegDelNull 636

Registry Usage 636
RegJump 636
Summary 636

Chapter 23: Best Practice in the Workplace 637

Education, Information, Cooperation! 637
Education Theory 639
Creating Community Involvement 640
Managing Power and Batteries 640
Sleeping Browser Tabs 645
Managing Users and BYOD PCs 645
Device Management 646
Group Policy 647
Backups' Best Practice 648
Deployment and Recovery Best Practice 649
Managing External and Network Hardware 651
Summary 651

Chapter 24: Managing BYOD Hardware 653

Managing VPNs and Secure Connections 654
Workplace Join 656
Managing Provisioning and Device Enrollment 658
Connecting to an Exchange Account 660
Connecting to Microsoft 365 or Microsoft Azure 661
Work Folders 662
Summary 663

Chapter 25: Getting Advanced Information 665

The Task Manager 665
The Performance Monitor 671
Data Collector Sets 672
The Resource Monitor 674

The Computer Management Console 675
System Information 677
DXDiag 678
Summary 679

Chapter 26: The Registry in Depth 681

Registry Files 682
Registry Keys and Values 684
HKEY_CLASSES_ROOT (HKCR) 685
HKEY_CURRENT_USER (HKCU) 685
HKEY_LOCAL_MACHINE (HKLM) 685
HKEY_USERS (HKU) 686
HKEY_CURRENT_CONFIG (HKCC) 686
HKEY_PERFORMANCE_DATA 686
Registry Value Types 687
Where You Will Find Important Registry Settings 688
The Registry Editor 688
Backing Up and Restoring the Registry 689
Creating and Modifying Registry Keys 690
Using REG.EXE and REGINI.EXE 692
Editing the Registry Using PowerShell 693
Editing the Registry from the Recovery Console 694
Editing Other Users' Registry Databases 695
Connecting to the Registry of Another PC 697
Enabling Remote Administration on PCs 698
Third-Party Registry Utilities 701
Comparing Different Registry Files 702
Summary 702

Chapter 27: Using Scripting Tools for Troubleshooting 705

The Windows Command Line 706

Troubleshooting Using PowerShell 712

Using the Event Log with PowerShell 714

Gathering Disk and File Information 716

Gathering Hardware and Software Information 719

Managing Processes and Services 721

Managing Windows Update 722

Windows Terminal 723

Summary 727

Chapter 28: Windows 10 File Structure in Depth 729

The Windows 10 File and Folder Structure 729

Root Windows Folders 730

Win32 and Store App Folders 731

Windows Operating System Folders 731

User Account Folders 734

Windows Log Folders 734

Windows Temporary File Folders 735

Windows File Types 736

Managing the Shell User Folders 736

Creating and Managing Symbolic Links 739

File Management from the Command Line 741

ChkDsk 741

SFC 742

DISM 743

Disk Partitions and Formats 743

MBR and GPT Partitions 743

Windows File Systems 744

Troubleshooting File and Folder Permissions 745
Understanding Permission Inheritance 749
Checking the Effective Access for a User or User Group 751
Taking Ownership of Files and Folders 752
Using Scripting to Handle Access Control Lists 753
Troubleshooting File and Folder Sharing 754
Summary 755

Chapter 29: Researching Difficult Problems 757

Reading the Windows Log Files 757
Log Text Files 758
Reading .xml and .etl Files 759
Reading .dmp files 761
Searching the Internet for Solutions 764
Microsoft Docs 766
Answers.Microsoft.com 767
Support.Microsoft.com 767
Other Microsoft and Third-Party Support Sites 768
Hardware Driver and Support Sites 769
Third-Party Support Tools 769
Summary 770

Chapter 30: Troubleshooting Difficult Problems 771

"Mike Halsey's Holistic Troubleshooting Agency" 771
Gauging Both Internal and External Factors 773
Using Troubleshooting Tools Together 774
Troubleshooting and Repairing Hardware 776
Minimal Boot Configuration and Jumpstarting PCs 777
Summary 779

Chapter 31: Installation and Restore 781

Troubleshooting the Windows 10 Upgrade 782

Installing Windows 10 783

Obtaining Up-to-Date Installation Media 783

Creating Customized Installation Media 785

Nondestructively Reinstalling Windows 10 786

Reset and Fresh Start 789

Windows 10 SysPrep 791

Summary 792

Index 793

About the Author

Mike Halsey has been a Microsoft MVP (Most Valuable Professional) awardee since 2011 and is a recognized technical expert. As the author of Windows 7, 8, and 10 troubleshooting books and associated video courses, he is well versed in the problems and issues that PC users, IT pros, and system administrators face when administering and maintaining all aspects of a PC ecosystem.

Mike understands that some subjects can be intimidating for some people and that everybody is different, so he approaches each subject area in straightforward and easy-to-understand ways.

Mike is originally from the United Kingdom, but now lives in the south of France with his rescue border collies, Evan and Robbie. You can contact Mike on Twitter at `@MikeHalsey`.

About the Technical Reviewers

Carsten Thomsen is a back-end developer primarily but working with smaller front-end bits as well. He has authored and reviewed a number of books and created numerous Microsoft Learning courses, all to do with software development. He works as a freelancer/contractor in various countries in Europe, using Azure, Visual Studio, Azure DevOps, and GitHub as some of his tools. Being an exceptional troubleshooter, asking the right questions, including the less logical ones, in a most logical to least logical fashion, he also enjoys working with architecture, research, analysis, development, testing, and bug fixing. Carsten is a very good communicator with great mentoring and team-lead skills, and great skills in researching and presenting new material.

Laurent Gébeau works in IT since 1994, where he discovered Windows at Microsoft. Laurent worked as an IT manager in various companies and decided to join Axeperf as co-owner in 2012. Axeperf is an IT company, mainly helping small businesses to move to modern IT (infra, security, and cloud applications).

Laurent is a Microsoft Certified Professional since 1995 and also Microsoft Most Valuable Professional since 2004. He has been awarded for his website and blog, has written some books, and spoken at some public conferences about various Microsoft products.

Introduction

A couple of years ago, I moved from the United Kingdom to the south of France and bought a house in the countryside. This house came with a gîte, which is a guest outhouse that is very common in France. I decided this gîte would become my office, so with the help of a very talented friend and some antique wood found in a neighbor's barn, I set about creating an appropriate desk space in what would be both an office and my own personal computer museum.

This museum contains all of the computers I have used and loved throughout my life, including an original IBM 5150 PC and lots of home computers from Sinclair Research in the 1980s and handhelds from Psion in the 1990s. Among the collection though is an original, shrink-wrapped box containing the floppy disk (both 3.5 inch and 5.25 inch) installers for Windows 3.1.

It's astonishing just how far Windows has come since those shaky, flaky times of 16-bit code. I remember how frustrating Windows 98 was to use, and how utterly unreliable Windows Me could be. When Microsoft released Windows 2000, however, everything started to change.

Yes, XP could still be unreliable and reinstalling it from fresh once a year was always considered good practice if you had the time and resources, but it worked, was stable, and came with some handy extras such as System Restore.

Windows Vista and Windows 7 added even more of these useful tools including the User Account Control (UAC), the Reliability Monitor, and the truly excellent Steps Recorder that was originally only supposed to be a debugging tool for the Windows 7 Beta, but was so popular it remains in Windows to this day.

Throughout all of these feature additions for troubleshooting, diagnosis, and repair, the versions of Windows they shipped with became ever more reliable, in what I call an interesting dichotomy perhaps best expressed by the graph in Figure 1.

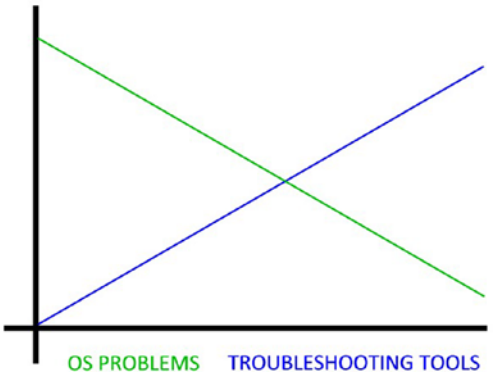


Figure 1. *OS problems vs. troubleshooting tools graph*

For as reliable as Windows 10 is however, and it has been a very, very long time since I have needed to reinstall a Windows OS once a year, problems still arise. This is primarily because of two things: firstly, the sheer volume of third-party software, drivers, and hardware, and secondly, the need to support legacy code dating all the way back to that IBM 5150 PC which was released in 1981.

These included tools and utilities however do allow us to troubleshoot and repair problems much more effectively, and much more quickly than we were ever able to before. This is doubly important in this post-pandemic world where the workplace has been fragmented outward into the homes of employees. Perhaps then this is where this second edition becomes most prophetic, with a heavy focus being placed on supporting those workers, who are very likely using their own computers, and making sure that downtime is minimized and productivity can remain high.

I hope you find this book helpful, educational, and informative. It is designed in such a way as to allow you to dip into and find the information you need fairly quickly, and to see that information at different levels of complexity as your own skills grow and expand. It's certainly been a fun book to write.

PART I

Getting Started with Windows Troubleshooting

CHAPTER 1

Introducing Troubleshooting in Windows 10

The landscape of computing has changed considerably in just the last few short years, and with Windows as much as any other embedded or installable operating system. Since Windows 10 was first released in 2015, we've not seen any operating systems that could genuinely be classed as "new and innovative" but instead have begun to see the signs that the future of computing will be extraordinarily different to its past. Take Windows 10X for example. This was initially announced as a variant of Windows 10 for dual-screen devices, but in fact was far more interesting than that.

Windows 10X was designed by Microsoft to be a direct competitor to Google's Chrome OS, to which Microsoft was losing out in the education market, with Chromebooks also making strong inroads into the business market. Microsoft changed its pitch, instead saying that Windows 10X was designed for frontline workers, i.e., those people who sit or stand with terminals having direct contact with customers, suppliers, and so on, as well as also being designed with the education market in mind.

What made Windows 10X so different, and interesting, was its completely new architecture; it was designed not to run on the PCs and with the software we use today but instead was designed to run the apps and on the hardware we'll use in the future.

Gone was any ability to run the legacy Win32 software that Microsoft had built the huge success that was Windows on top of for so many years, and in its place was a different architecture based entirely on virtualizing apps and streaming them from the Internet.

Microsoft's cloud service, Azure, was also being upgraded and expanded to cope with this bright new future. In essence it revolved around two important technologies,

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_1

Progressive Web Apps (PWAs) and Windows Virtual Desktop (WVD). This would allow a PC in any form factor to either install apps built as websites and run them locally (such as Microsoft's Office web apps of Word and Excel) or use Azure to host and run the installation of older Win32 software that could then be streamed to the device in real time.

All of this sounds wonderful, but it's not without its problems, the first of which is that both of these technologies, and in particular Virtual Desktop, rely on the PC having a permanent and fast connection to the Internet. Technologies such as 5G and fiber broadband help with this, but only really in cities and large conurbations. As I write this, I'm in the middle of a farmland in central France where my nearest neighbor is a cow. I have a spectacular ADSL connection that reaches the heady heights of 3.5Mb/s, and though fiber is being rolled out to my neighborhood this summer, far more people around the world are not so lucky.

France made the decision a few years ago to roll out fiber broadband to every single business and home in the country, no matter how remote they are. It was a bold plan and, so far, one that appears to be working. France is the anomaly, however, with the United Kingdom, the United States, and most other countries failing to provide even basic Internet connections to rural areas.

Why is this a problem when most businesses, especially the large ones, will reside in major towns and cities you ask. The problem comes with our changing work habits. The unfortunate world events of 2020 (if only there was a phrase we could have used to describe seeing that coming) have changed work practices forever, with far more people now working from home on a permanent, or semipermanent, basis. The global pandemic also created a strong desire for many people to move out of the large towns and cities to more rural locations where the air was cleaner and large throngs of people, all rammed together in busy streets, just didn't exist.

You can see where I'm coming from here, can't you, that while technologies such as Windows 10X and Virtual Desktop are fantastic, great for security, stability, the updating of systems, and so on, they're not yet ready for prime time and won't be for many years yet. At least, they won't be able to become the dominant desktop experience for a considerable time.

This leaves us with the venerable old Windows 10 which really hasn't changed very much in the years since its first launch. The reasons for this are many, but primary among them is a need by business to have the underlying technologies and interfaces remain intact, so they don't have to implement large and expensive changes to their

workflows or infrastructure. Sure, many businesses have already ditched their on-premises servers and moved to cloud-based servers instead such as Azure, but the venerable desktop PC will be with us for some time yet.

This brings with it a new set of problems, not the least of which is the changing way we work, and the changing places in which we work today. There's a new need to support remote users, and workers have also started using their own PC hardware (which presents additional security and stability challenges for organizations) and also means that any hope of maintaining uniformity of hardware across any business or organization is now officially a pipe dream.

Windows is a complicated beast, still able to run DOS software from 1985 and some early Windows programs too. When you look at the operating system as a whole, it's amazing really that it works at all. Windows Update is a good example with updates being rolled out on a regular basis to literally billions of different combinations of hardware and software. If you think your laptop is just the same as many others, think again. There's no other laptop like yours anywhere else in the world, with its unique combinations of printer, peripherals, and installed software.

We also need to support older hardware in Windows because many manufacturing processes and even critical infrastructure demand it. We've had USB for decades now, so long in fact that it's gone through many changes and interactions itself. Originally though, it brought an exciting new technology with it, Plug and Play. This allowed the operating system to identify the device that was being plugged in just by interrogating it.

Before this technology came about, however, things were very different. Serial and parallel devices had to be identified and configured manually using setup files, settings tweaks, and scripts. Just getting a serial device to be identified at all could be a challenge that would sometimes occupy a couple of hours.

When it came to the desktop, things weren't that much better. Differences in processor and other technologies from what we use today frequently caused memory leaks, Blue Screens of Death, and crashes. If you were using Windows 95 or 98, there was no easy way to repair the operating system, as even System Restore didn't appear until Windows Me, and that operating system brought its own unique bugs and instabilities that even today cause people to break out in a cold sweat.

With Windows Vista, Microsoft set out to fix all of this. They created a new hardware driver model to reduce, and even eliminate, instabilities and crashes, and completely reengineered the operating system to make it robust, resilient, and reliable. Even today, a Windows Vista system is pretty good to use, and Windows 7, 8, 8.1, and 10 continued to build on that reliability.

With these operating systems came a whole host of new diagnostic and repair tools and utilities: monitoring apps, image backup utilities, CD and USB recovery media creators, and even a pretty amazing Reset utility that can refresh, reinstall, and update the operating system automatically. It's ironic then that as the reliability of Windows versions has increased, so too has the number of tools provided to troubleshoot and repair problems.

Despite all of this, however, and despite the introduction of nonhardware-serviceable PCs such as Microsoft's Surface range, our PCs are still not consumer electronics devices. They just won't work in the same way as your TV or microwave because of one fundamental difference, the hard drive. Because the operating system and all our drivers and apps have to be installed in a volatile way that permits changes to be made to the files so as to enable updating and new installs and simply to allow us to get stuff done, the risk of damage or corruption will always be present. This is opposed to a consumer electronics device such as a smart TV or refrigerator, which performs a single set of tasks repetitively and in a tightly controlled manner.

This highlights another irony, that unlike PCs, the consumer electronics devices we use aren't essential to our working lives. They're not what we rely on to "get stuff done." This means when a PC fails to start, or our apps and hardware won't work, it commonly leads to a crisis. For all its troubleshooting and repair utilities, and despite all the work that's been put into making Windows 10 the most reliable and robust edition of the operating system yet, an ecosystem of millions of apps and hardware devices, not to mention the effects of letting end users loose on a volatile file system, means that problems will still occur.

That's where this book comes in. I'll teach you how to become proficient in troubleshooting all aspects of a PC, how to diagnose and repair the most complex of problems, and what the most common and frustrating problems are.

The Three Seashells…

We all learned the "Dem bones" song at preschool, but it's also true that the hip bone isn't just connected to the backbone but is connected indirectly to every other part of the human body. Everything inside the soft squidgy bag we call our skin is interconnected by muscles, nerves, and tendons. With PCs, things are just as complex. You start with the interconnectedness of all the internal components. These include the motherboard,

processor, memory, graphics chip, hard drive, and power supply, but then extend to the BIOS, hardware drivers, software, operating system and screen, printer, and everything else directly connected to the PC.

Beyond this, however, our PCs are still connected to an ecosystem, the likes of which are too complicated for the average human brain to comprehend in its entirety. Wi-Fi and Ethernet connections connect our PCs to routers, switches, networked devices, security appliances, telephone exchanges, cellular masts, cloud services, data centers, websites, biometric scanners, smartphones, tablets, laptops, desktops, etc.; the list is pretty endless.

This means that long gone are the days when on a stand-alone PC you'd be diagnosing a problem knowing the cause had to be something local to the machine, such as a driver configuration file, software installation, or hardware component. Now we not only have to take into account all of the PCs and network infrastructure around us but look to remote servers and even the fabric of the very building the PC occupies, including what is often many hundreds of meters of cabling.

In a way, this actually makes diagnosing problems simpler, though it may not seem like it at first. This brings me to the fundamentals of troubleshooting any problem with a PC, and the three questions where you should always begin:[1]

- What's changed?
- Is anybody else or other hardware/software experiencing the problem?
- When did the problem start?

The first of these questions is the most important, as nothing ever goes wrong with a PC without something changing. Perhaps a system, driver, or app update has recently been made, a new app or piece of hardware has been installed, or a fan has failed on the motherboard. Has something been faulty recently? Could an engineer have swapped the component (internal or peripheral) with something that *looks* exactly like, but isn't *really* like the original? Has there been a power outage, or was the PC moved over the weekend?

[1] I call these questions the three seashells after the now-infamous three seashells encountered in bathrooms by Sylvester Stallone during the cult movie *Demolition Man* (Warner Bros., 1993). They were fundamental to operation of the toilet but were however completely perplexing to our bemused hero.

Asking what it is that has changed can save valuable time in diagnosing and repairing problems with PCs. To this end, Windows 10 is extremely helpful, keeping records of update and installation operations, even crashes, and app failures, all of which could point to a corrupt file or component.

Next up is to ask if anybody else is experiencing the same problem, or if any other hardware or software is experiencing the same problem. This might include people or computers in your home or workplace, and it immediately helps you diagnose if you're dealing with a problem local to the PC or elsewhere on the network. Outside of this, a quick search on Bing or Google can reveal if anybody else, elsewhere in the world, is being affected by the same problem. Twitter hashtags are a useful resource for this, since if a faulty update or app has been released into the wild, people will begin to complain about it almost immediately, and the feedback you will get online will be instantaneous and give a good indication of both the scale of the problem and any potential fixes that might already exist.

Moving on to when the problem first started is the next step if the answers to questions 1 and 2 haven't already led you to a fix. A PC user might report that a problem has started in the last half hour but might not tell you it's actually a recurrence of a problem that they first saw 2 weeks ago, or that a colleague reported on his own PC the other day.

This is where, as an IT technician, keeping records is a great resource. I dislike paperwork as much as the next person (probably much more in truth), but having a call-logging system in an IT support department that accurately records asset numbers, users, problems, and solutions found can help you see patterns between problems and find solutions more easily.

Some of these links are obvious; when I worked in my first major IT support job, my colleagues and I were taking calls every day for what felt like a year, for PCs from a major manufacturer (who shall remain nameless) that had bought, what we assumed anyway, to be a large batch of very cheap capacitors which were exploding on motherboards, rendering PCs pretty useless. This made it fairly easy and quick to diagnose a PC where the capacitors were installed, as the end result for the user was fairly consistent, and it was only one particular model of PC affected.

Other links can require more investigation, and throughout this book I'll show you how to undertake those investigations, what to look for, how to find the information you need, and how to repair the problems you find.

The Problems We Encounter

Now that you've been left completely baffled and befuddled by the sheer scope of the causes for problems on our PCs, let's spend some time breaking these down into the main problem areas, examining the possible causes of each one.

Hardware Problems

It's a simplification to think of a hardware problem as a faulty or failed component inside a PC. Sure we do have motherboards, graphics cards, processors, memory chips, and hard drives that fail, but occurrences are very rare. Even the more common failure of a fan or a power supply doesn't come close to explaining what the range and scope of hardware problems on our PCs includes.

Cabling is often a cause of hardware problems on a PC; such problems can often appear to be something else, such as the power supply, network card, or monitor. As a matter of procedure, I will always cable-tie and neatly stow cables when installing a new desktop PC, and for a desk where a laptop is to be used, I will use a cable management system to keep them out of the way and tidy. Why do I do this? Well, I'll admit I can be a neat freak and have just a *teeny* amount of OCD (obsessive-compulsive disorder), but it's also good practice and can often completely eliminate the risk of cable and other hardware damage.

How many times have you, a friend, a family member, or a colleague tripped on a power, USB, or network cable? This not only risks damaging the cable (by tearing it, stretching it, or damaging one of its plugs) and the socket(s) it's plugged into but also risks straining a muscle in your leg, hurting a knee if you fall, and even suffering a massive head injury resulting in a concussion and hospitalization, etc. Okay, I might be exaggerating slightly on the last one, but you take my point.

Tip An essential part of any IT pro's diagnostic kit is a selection of known good cables. Be they power, video, or USB, it's always helpful to have a suitable cable close at hand that you can guarantee isn't itself faulty.

Hardware problems aren't just isolated to the PC and attached peripherals on which the problem has occurred. Cabling, routers, switches, and other network architecture in a building can be a cause. In these cases, the problem is unlikely to be isolated to a single PC, which aids diagnosis.

Lastly, let's not forget what is by far the most common cause of hardware problems, the driver. I would, in a very unscientific way, suggest that over 99% of hardware problems are caused by incorrect or faulty drivers being installed, or driver files becoming corrupt after installation.

The Tale of the Exploding Charger

I just want to finish this with a cautionary note about USB charging cables and the chargers themselves. When you put new electrical wiring into your home or workplace, it must meet strict regulatory standards to make sure the cables don't overheat, or devices plugged into the circuit don't keep tripping the breakers. I don't need to tell you this as it's a well-known fact right around the world. When it comes to USB charging cables, however, things are no different.

The problem arises as people need to replace their charging cables as they break or are lost, and then look to purchase ever cheaper cables from the local grocery store or online, and it's becoming a bigger and bigger problem since almost all new devices are now powered by USB type-C cables, from smartphones to laptops.

The problem with cheaper cables is that they're not up to the standards of modern devices, and they're especially not up to the standards of modern "fast" chargers, which can deliver very high wattages in order to charge your device quickly.

A cheap cable simply cannot cope with those wattages, and this is why you occasionally hear or read of stories of cables melting and causing fires. Equally, some cheaper chargers aren't up to standard, especially throwaway chargers purchased from the far-east, and these too can melt, catch fire, or even in some cases explode. It is crucially important, especially if you manage hardware in a work environment, to ensure that the cables and chargers used with devices are up to specification, and capable of handling the high wattages required by our modern IT equipment.

Software and App Problems

If you use an iPad or an Android tablet, then you've only got one port of call to go to for your apps. If you only use Store apps in Windows 10, then, again, you'll only have one place to go to for them. App stores can present huge advantages for both the developer and the end user. Whatever device you use, all apps in the stores are rigorously tested for reliability, stability, and (crucially) malware.

Even so, faulty apps can occasionally make their way through the stores. The autoupdate methods employed by these stores, however, can make it a quick and straightforward job for the developer to distribute a fix. This also helps ensure that all users of the app, which may connect to the Internet or other online services and offline and hardware resources, are all the same version, using the same version of the app, and fully up to date with security and stability patches and the latest features.

If you're using Windows 10, though, it's also extremely likely that some, if not most or perhaps even all, of the software you use won't come from the Store. These *win32* apps that come as downloads from the Internet, or provided on a CD, DVD, or USB Flash Drive, don't have many of the advantages of Store apps. They might come with an updater, but it's always an updater that can be disabled. They are also not sandboxed from other apps, and the operating system, in the way that Store apps are. Lastly, the file system containing the component parts of the app is completely exposed, not even requiring a User Account Control (UAC) prompt to gain access, unlike the Store app folders, which are almost completely inaccessible to everybody, including the system administrator.

Networking Problems

How thick are your walls? I ask this because one of the most common networking problems these days is poor or even nonexistent Wi-Fi connectivity. This might not be so much of an issue in the United States, where walls are commonly made from paper or wood, but in Europe, where buildings can often be hundreds or perhaps even thousands of years old, the walls are slightly thicker and extremely good at blocking radio signals. The walls for my own home, which is a more than 300-year-old country cottage, are a foot and a half thick in some places.

Elsewhere, networking presents complex layers of problems that you won't see elsewhere on a PC. Is your network connection problem caused by the network configuration settings on the PC, the driver, the port, the cable, the switch, more cable, the router's hardware, or a software problem due to a lack up updates in its firmware, yet more cable, the telephone exchange, the cellular mast, a satellite in orbit, or perhaps even a bird that's eaten too much and is stretching an overhead cable when it sits on it or a digger on the building site down the road who has just ripped up the fiber optic cable for the whole neighborhood?

Okay, so I'm kidding about the bird, and most of the network problems you will encounter will still be local to the PC on which the problem occurs. It's important to bear in mind the connectedness of our PCs with other PCs and systems, though, when diagnosing networking issues.

Startup Problems

There is nothing more annoying, and nothing more common in my own mailbag, than problems caused by a PC that simply refuses to start. A nonbooting PC can be caused by many things from the cabling and the power supply (it's also helpful to make sure it's switched on at the mains) to a recent Windows Update or configuration change, power outage, hardware change or upgrade, or perhaps something else entirely.

It's because startup problems are so unpleasant and can seemingly occur at any time that you'll find two chapters in this book teaching you how to repair problems. In Chapter 8 I'll show you how to repair simple and common startup problems, and in Chapter 13 I'll show you what you can do when your copy of Windows appears to be completely dead.

OS Installation and Update Problems

One of the most common problem areas for Windows PCs involves installation and, particularly, updating. When a major update to the operating system is released (what Microsoft used to call a Service Pack), all hell can break loose, and just about everything on a PC can either throw a wobbly (as we say in the United Kingdom) or just break completely.

This isn't helped by the SaaS (Software as a Service) approach that Microsoft has taken with Windows 10, enforcing all updates on all users, all of the time, and not giving people the opportunity to opt out. From a security and stability (and a cost-saving) point of view, this makes complete sense, having everybody on the same, latest, version in the same way we all are with the Store apps we use. Other problems and headaches can be caused, however, that we'll examine throughout this book.

"Prevention Is Better Than Cure"

If you haven't already guessed by now, the first and most fundamental principle of troubleshooting a Windows 10 PC, or any IT system come to that, is to first set it up in such as way as to try and ensure that problems never occur at all. After all, it's well known that if you are responsible for the IT systems for a major corporation, a medium-sized enterprise, or even a small business and something goes wrong, you'll likely get the "Everything's gone to hell, what am I paying you for!" rant.

Ironically, it's also equally likely that if you create a system in such as way as to ensure that almost nothing ever goes wrong, you'll get a variation on the same rant. I for one though know which of the two I'd rather be on the receiving end of; after all, to use another well-known British phrase, "Prevention is better than cure" any day of the week.

To this end, the first three chapters of this book are dedicated to helping you create a PC ecosystem that is, quite literally, bomb-proof (if your office was hit by a major hacking, flood or other natural disaster, or terrorist attack). The next morning (or at most a few mornings after you've finished reading the last chapter of this book[2]) would your business be out of business, or back up and running?

Much of what follows in these first chapters then is based around general principles. These will apply just as equally to your Windows Server system(s) and Internet-facing servers as they will to the PCs on the desks and in the homes and cars of your workers.

Don't think life gets any easier at home. If your college report is due tomorrow and your PC won't start, you're in deep, deep trouble. If your son or daughter can't get online to play a game or chat with their friends, all hell will break loose, and if your partner or significant other can't get online to do whatever the hell it is they do there anyway, then you're actually going to have to spend time *talking* to them instead [shudder!].

The Security and Maintenance Center

Given that we're now eight pages into this book, it's probably about time to start with some actual tech and features of Windows 10, and the Security and Maintenance Center is where I'd like to start; see Figure 1-1. You can find this in the Control Panel

[2] Should a major catastrophe hit your workplace *before* you have finished reading this book, I wouldn't recommend spending a lot of time sitting at your desk with it in your hands where the boss can see you…, they might think you're slacking.

(yes, it's still there, for now anyway). Change the Control Panel view to large or small icons by selecting from the drop-down menu in its top-right corner, and you'll see *Security and Maintenance* listed.

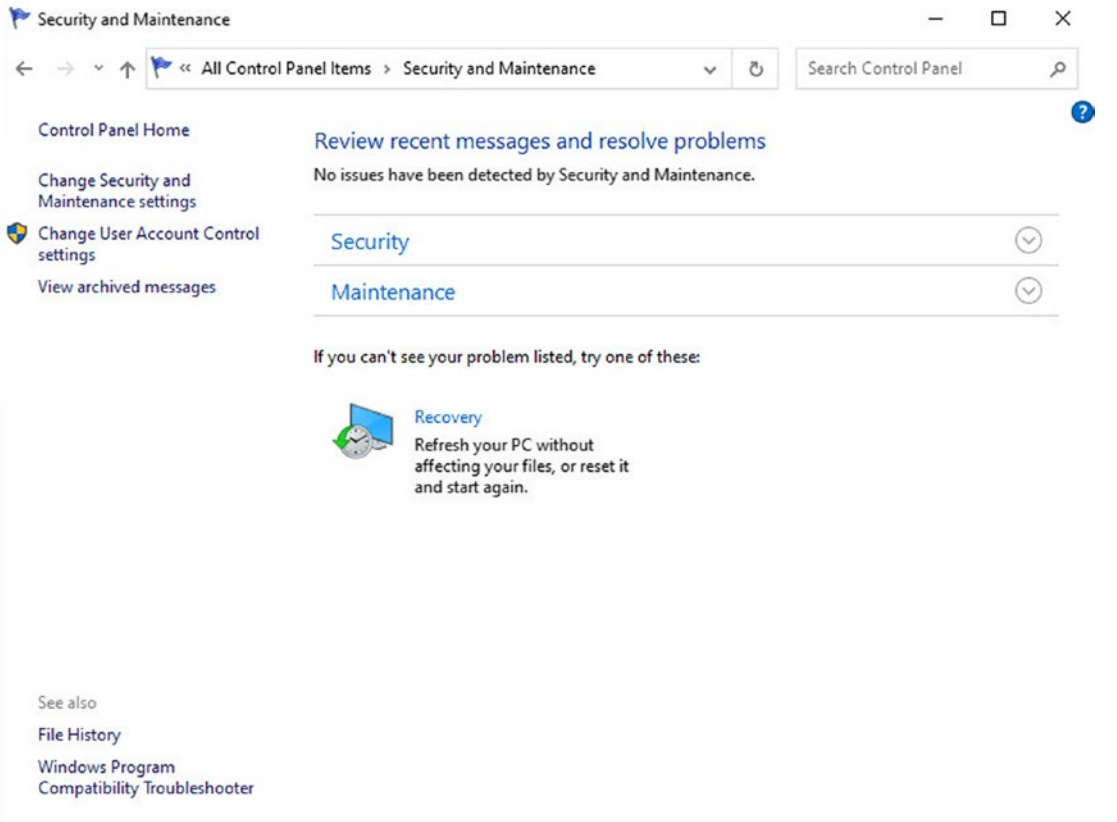


Figure 1-1. *The Security and Maintenance Center*

Windows 10 comes with a wide variety of information and status utilities, but the Security and Maintenance Center is certainly the most important for the general operation of a PC. This importance comes about because maintaining good security on a PC is absolutely crucial to the safe and reliable operation of the machine and your installation of Windows 10.

The Security and Maintenance Center is separated into four main areas. The left panel contains quick links to useful links, such as controlling the UAC security subsystem (which is crucial to a smooth and malware-free operation for your PC and so shouldn't be deactivated). In the bottom left of the window are quick links to features like the Windows Program Compatibility Troubleshooter.

The first quick link, near the top left of the window, is *Change security and Maintenance settings*, and it is here that you control what messages are displayed.

It's the main section to the right of these links that provides information about the security and maintenance status of the PC. It does this by traffic-lighting two expandable sections. If you don't see any messages highlighted in amber or red, it's because everything is working properly and there are no issues. If you do see one, however, as in Figure 1-1, anything highlighted in amber is an alert that something isn't critical but might require your attention. Anything highlighted in red is a critical alert that needs urgent attention; in this case the PC's firewall has been disabled.

Each of the two expandable sections in the Security and Maintenance panel has small down arrows to their right side. Clicking one of these will expand that section to reveal all of the status information and control links within it. Here you can monitor individual items such as your antivirus status.

Expanding the Maintenance section provides quick links to tools and utilities that can be useful in diagnosing and repairing common problems with a PC; see Figure 1-2.

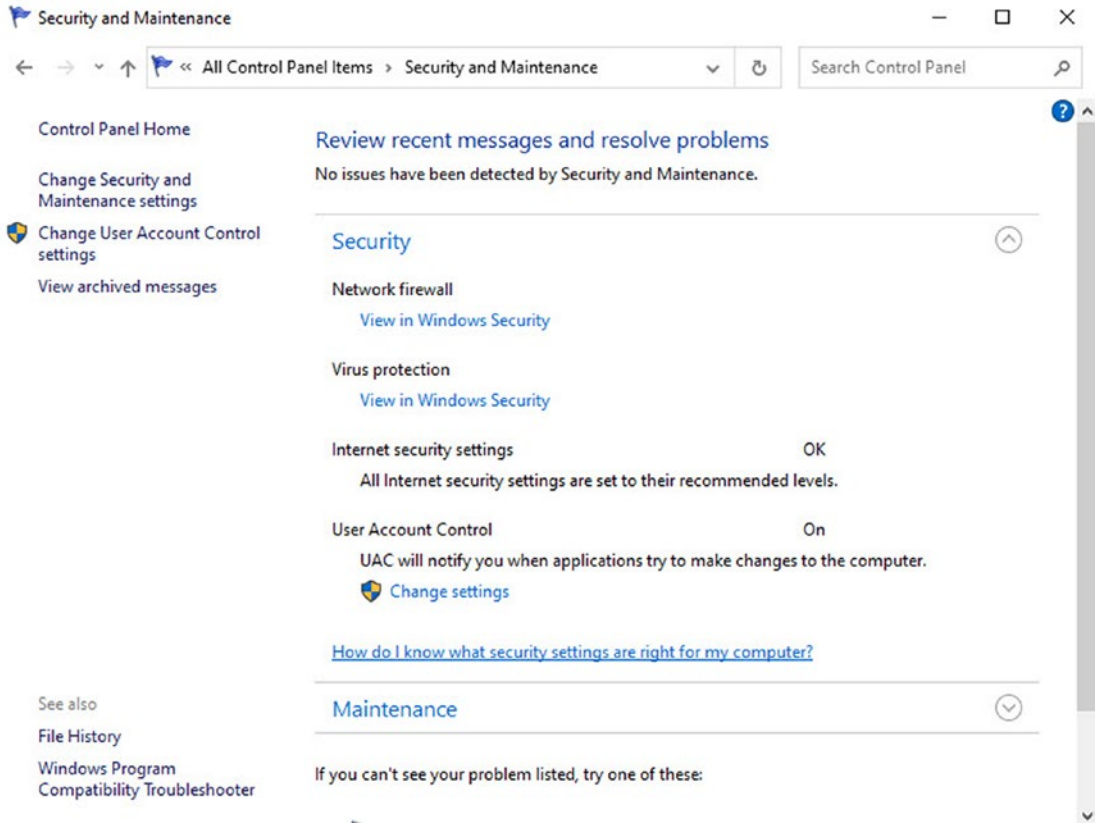


Figure 1-2. *The Maintenance panel contains useful quick links for troubleshooting tools*

Windows Reliability History

Windows' Reliability Monitor, accessed by clicking *View reliability history* in the Maintenance panel, is one of the hidden gems on your PC. It's been around since Windows Vista but is commonly overlooked because it's hidden away, and not highlighted in the Control Panel or Administrative Tools. It displays a horizontal scrolling view with each column in the display a different day when the PC has been in use; see Figure 1-3. If any errors, crashes, or information events have occurred, then they will be highlighted by (i) or (x) symbols on the relevant day.

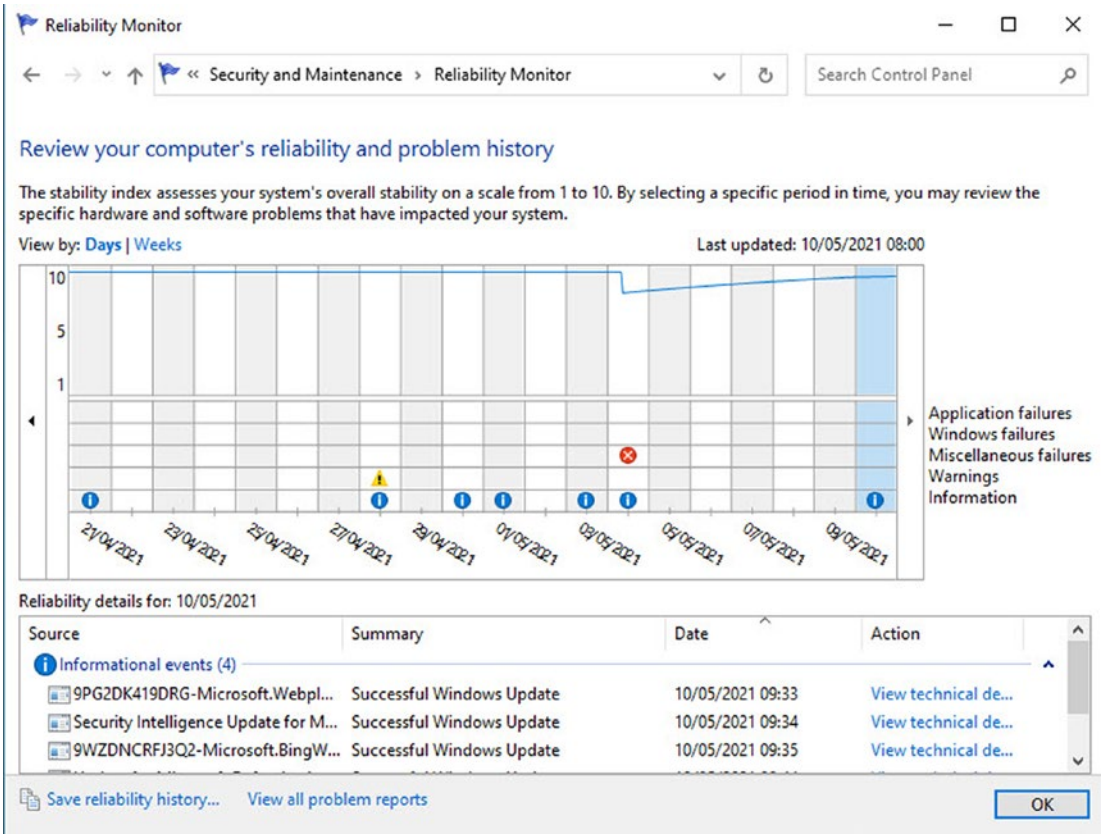


Figure 1-3. *The Reliability Monitor provides information about errors and crashes*

Tip If you are supporting a user remotely from a call center, they can open the Reliability Monitor by searching for *reliability* in the Start Menu or Taskbar search box.

Clicking a day will present a list of all the information and error events that occurred, each with a link to its right to *View technical details* about the problem. This option will provide any relevant information about the event including (for many but not all events) a wealth of technical information about what happened and what apps, resources, or services were involved; see Figure 1-4.

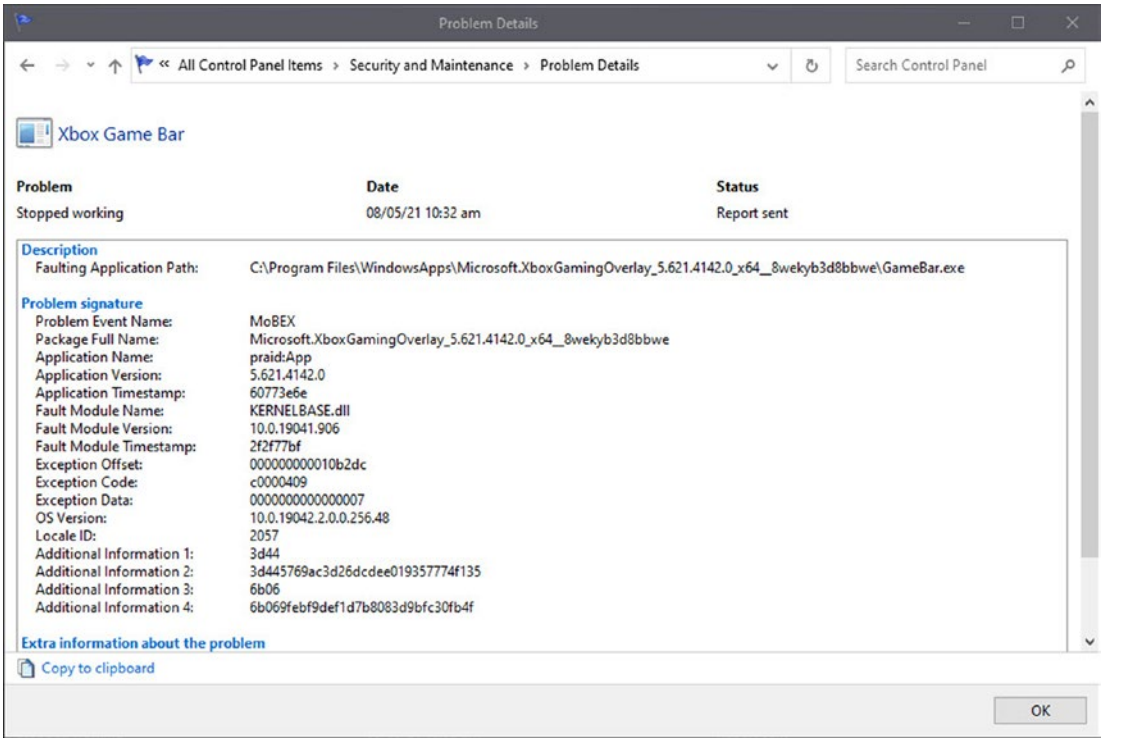


Figure 1-4. *Technical details about problems can be found in the Reliability Monitor*

The technical information displayed will vary depending on the type of problem Windows has encountered, though it may include the name and folder path of an app or system file or the names of crash (.dmp) reports or .xml files that contain information or other details about the problem. Other useful information that can help diagnosing problems is the inclusion of version numbers for any components involved. You might find, for example, that the driver, system file, or app causing a problem is a different version than those you know are stable and consequently supported. Being able to identify incorrect file versions can help in quickly rectifying some problems.

When you have detailed technical information about an event, you will also see a *Copy to clipboard* link in the bottom left of the window. This will allow a user to copy and paste this technical detail into an email if you are remotely supporting somebody or are seeking additional support online or from a colleague.

At the very bottom of the Reliability Monitor window are quick links to *Save [your] reliability history* and *View all problem reports*. These links are less useful for troubleshooting, as they only contain details of problems that Windows has automatically reported to Microsoft in an attempt to find solutions.

Windows Automatic Maintenance

Below the Reliability history in the Security and Maintenance panel are quick links to *Start [automatic] maintenance* and *Change maintenance settings*; see Figure 1-5. This automatic maintenance will perform routine tasks such as running Windows Update, defragmenting any disks that require it, and cleaning up temporary files.

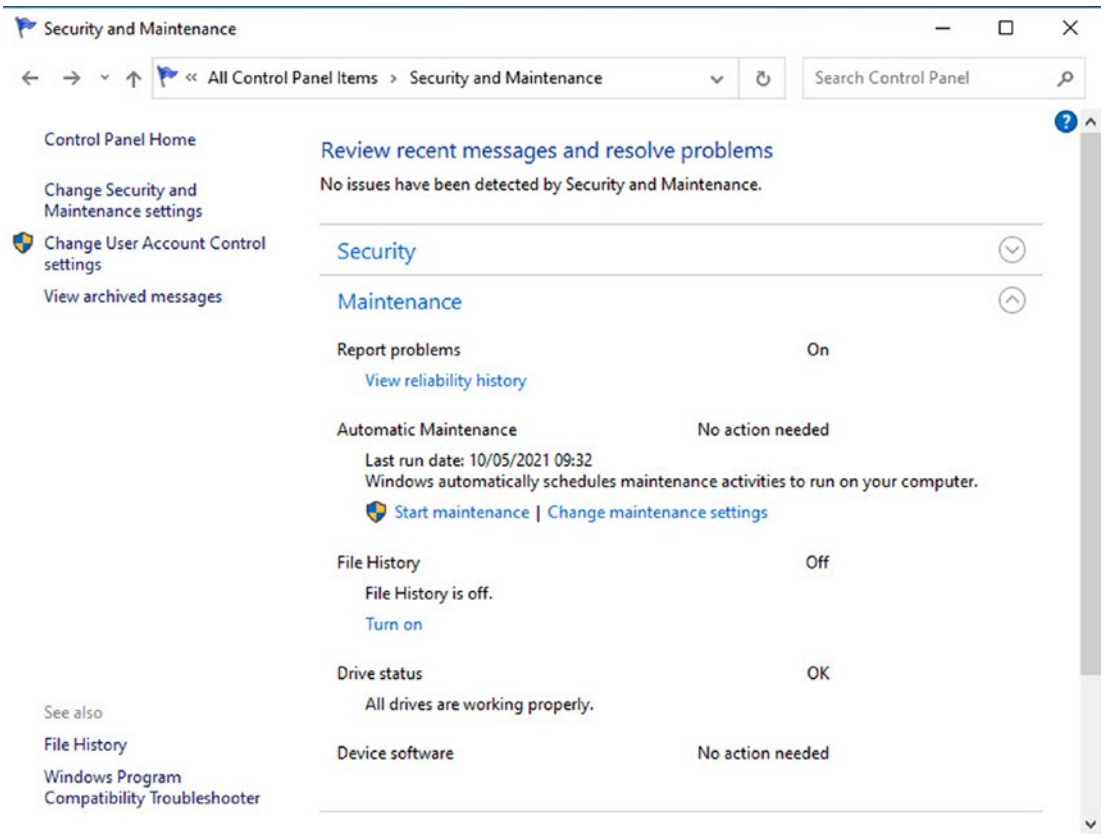


Figure 1-5. *Automatic maintenance can perform routine tasks on a PC*

Note When files are written to disk, the operating system places the file in the next available free space. On some occasions this free space isn't large enough for the file, and so the file is split into two or more parts. This is especially common if storage space is at a premium, such as can be the case with an ultrabook or tablet. Defragmenting a mechanical hard disk can prevent the disk's read arm from having to access different parts of the disk to access the file, which can slow access times. Solid-state drives (SSDs and M.2) do not need defragmenting as they are a random-access storage medium. Defragmenting SSDs can also reduce the life of the drive, as many come with a maximum number of supported write operations during their lifespan. It can be wise to disable defragmentation in the Windows Defragmenter (search for **defrag**) for any SSDs where Windows has not automatically done so.

Managing Diagnostic Feedback and Privacy

I've mentioned that Windows 10 sends diagnostic information about errors and crashes directly to Microsoft to search for fixes that can be implemented automatically. You may not want information about your PC sent to Microsoft, or a user you are supporting may have changed their privacy settings.

These feedback and diagnostic settings are controlled in the *Settings app* in the *Privacy* section. Click *Feedback & diagnostics,* and you'll see an option for **Diagnostics & feedback**; see Figure 1-6. Changing this setting (the options include Required diagnostic data and Optional diagnostic data) can control how much information is shared with Microsoft. It is not possible to disable feedback completely because some telemetry is required by Windows Update, so it knows what hardware you have installed, but clicking the *Get more info about these settings* link takes you to a web page where each of the three settings is explained.

It is worth noting that, because privacy is such a hot topic these days, this panel is updated and changed by Microsoft on occasion, so it might look different when you check it on your own PCs. The basic functionality will not change very much however.

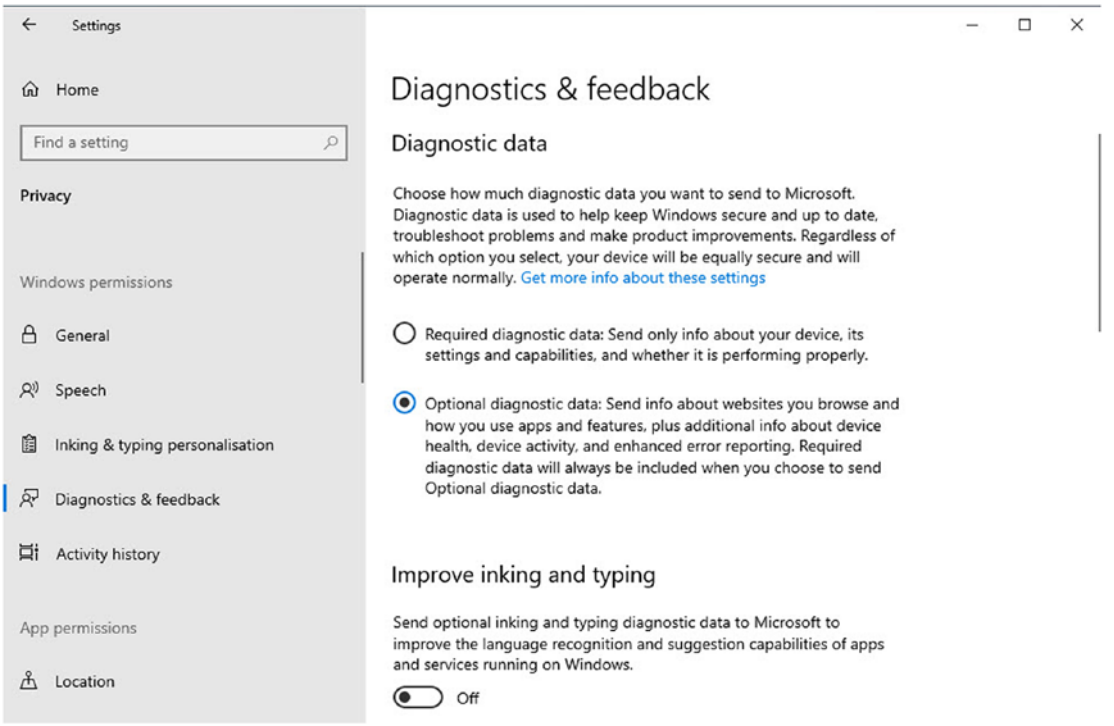


Figure 1-6. *You can control what diagnostic information is shared with Microsoft*

Windows' Security Systems

Windows 10 comes preinstalled on all systems with a variety of security systems, including antivirus protection and a firewall. These systems are crucial to the safe and smooth operation of a PC, and so I want to spend a little time showing you how they can be managed.

Windows Defender Antimalware

Since Windows 8, Microsoft's operating system has come with inbuilt antivirus software. This is called Windows Security. In Windows 10 (as with Windows 8), this is a rebadged version of Microsoft's Security Essentials antivirus and antimalware package.

As packages go it is extremely lightweight, using almost no system resources and not slowing your PC. It's not as effective as some of the dedicated stand-alone packages though and will be disabled if you use one from a third party such as ESET, Kaspersky, or Norton.

Windows Security has two interfaces on a PC. Primarily it is controlled through the Settings app, and you'll find it under *Update & security* listed as *Windows Security*; see Figure 1-7.

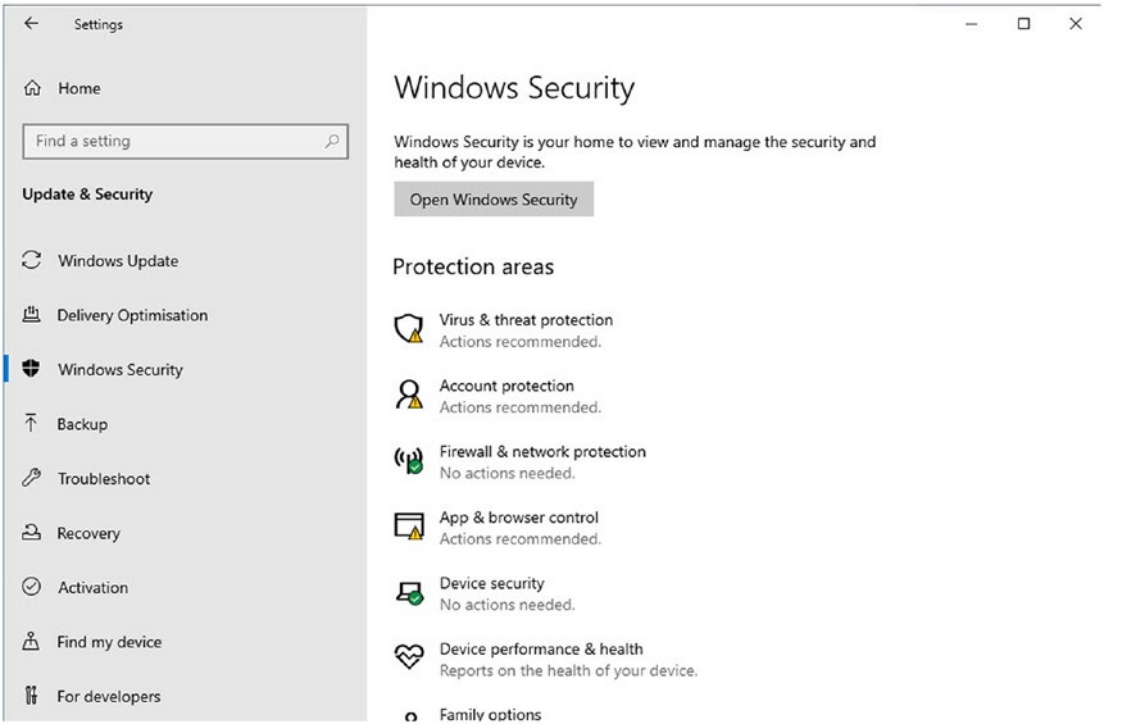


Figure 1-7. *Windows Security is easily controlled through the Settings app*

Here are basic controls to change or check settings for the different security features of your Windows installation, and if you perform troubleshooting on a PC, it's worth having a quick look here to see if Windows Security is active if no other antimalware package is installed on the PC, though the System and Maintenance panel will inform you if there is no antimalware package active at all.

More detailed control (which is a bit of an oxymoron for reasons that will become clear) is available by searching for **Security** in the Start Menu or Taskbar search box to display the full Windows Security desktop interface (see Figure 1-8), though this is also available by clicking the shield icon in the Taskbar system tray.

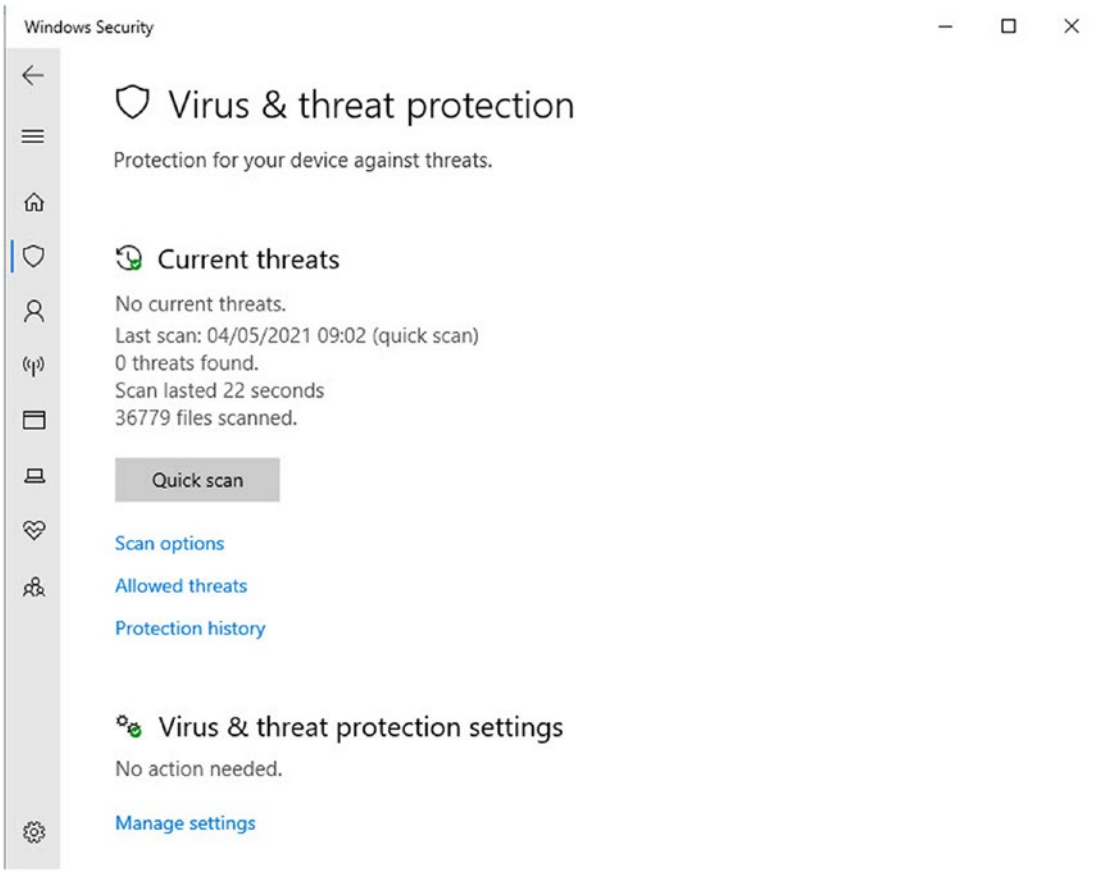


Figure 1-8. *The Windows Security Virus & threat protection interface is easy to read and understand*

The Windows Security panel allows you to manually run scans of your PC, including a *Custom [scan]* option which you can use to scan removable media such as USB Flash Drives. *[Check for] Update[s]* and *Protection History* links can be found within the panel, from which you can manually update the installed antivirus definitions and view any files that have been quarantined or deleted during scans.

Windows Firewall

When you search in the Start Menu or the Taskbar search box for **firewall**, two different options will appear: Windows Firewall with Advanced Security and Windows Firewall. The former, which I shall detail in full in Chapter 18, allows you to create and modify existing and custom firewall rules. The basic firewall in Windows 10, though, is pretty good and a match for anything commercially available.

Like all the other security features in Windows 10, the firewall (see Figure 1-9) is color-coded, so if the firewall has been disabled or if a third-party firewall is being used instead, the panel's sections will be highlighted in red.

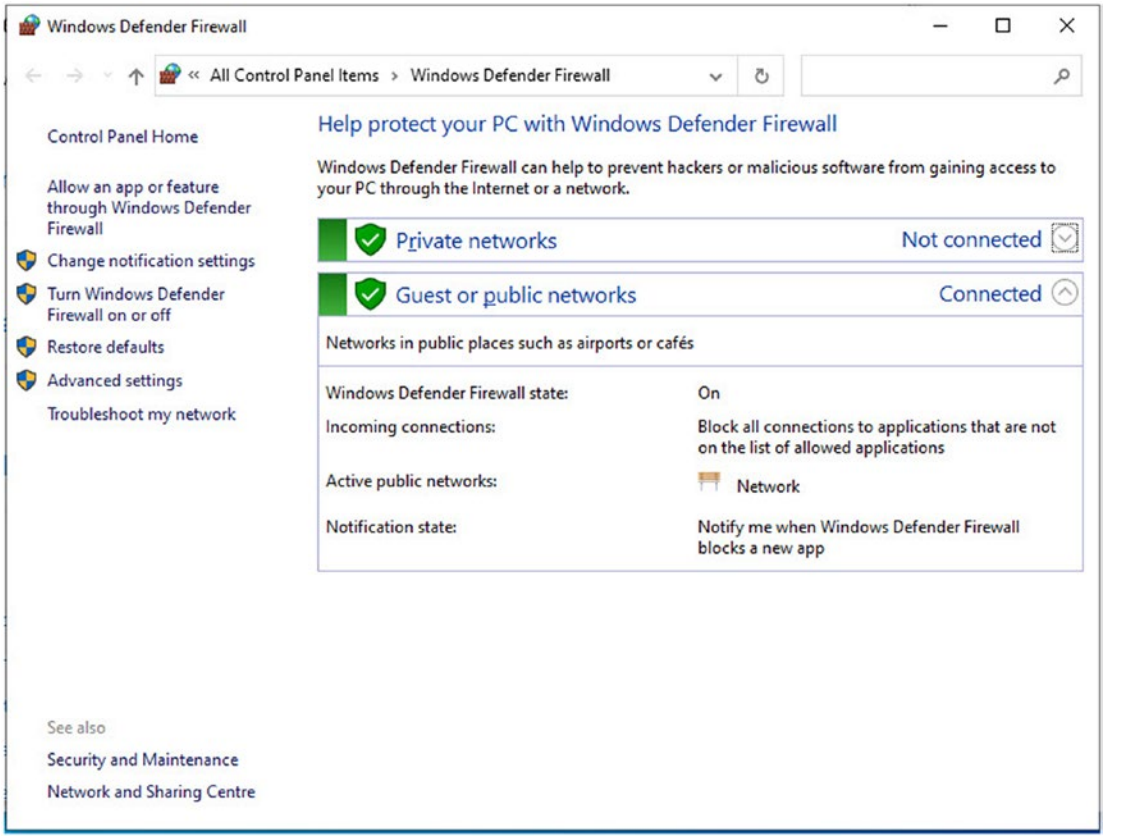


Figure 1-9. *The Windows firewall is basic but highly effective*

The different network types you can connect to will be listed with the currently connected network expanded to display the network name and details about the firewall settings.

In the left panel are various firewall controls including a link to turn the firewall on or off, useful if it's been disabled by accident or by a user who shouldn't have done so.

In the top left of the window is a link called *Allow and app or feature through Windows Firewall*. This can be used if you find that a third-party service or an installed app or game is being blocked when it shouldn't be. A list of all the installed apps and services on your PC will be displayed; see Figure 1-10.

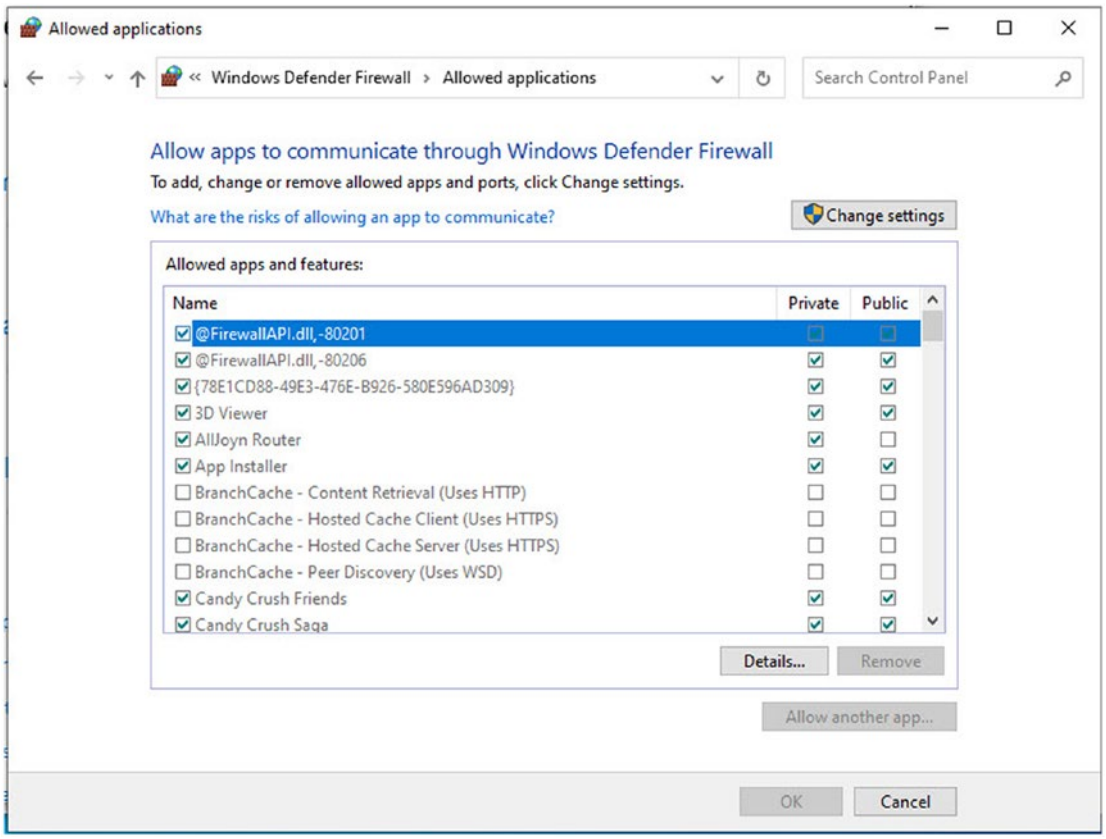


Figure 1-10. *You can manually allow apps and services through the firewall*

To change the settings for a specific app or service, click the *Change settings* button. You will now be able to set access for both Private (home or work) and Public (coffee shop) network types. If the app you want to allow through the firewall doesn't appear in the list, click the *Allow another app* button to display a dialog where you can manually navigate to the app's location on your PC.

It is worth noting that in time it's likely this firewall desktop interface will be retired and replaced, because there is already another interface for the Windows Firewall, and this is in the Settings panel under *Update & Security*, where we also found the antimalware panel. This will ultimately be the main interface for the feature and, while a stripped-down version of the more traditional desktop interface, still provides the information and functionality you need; see Figure 1-11.

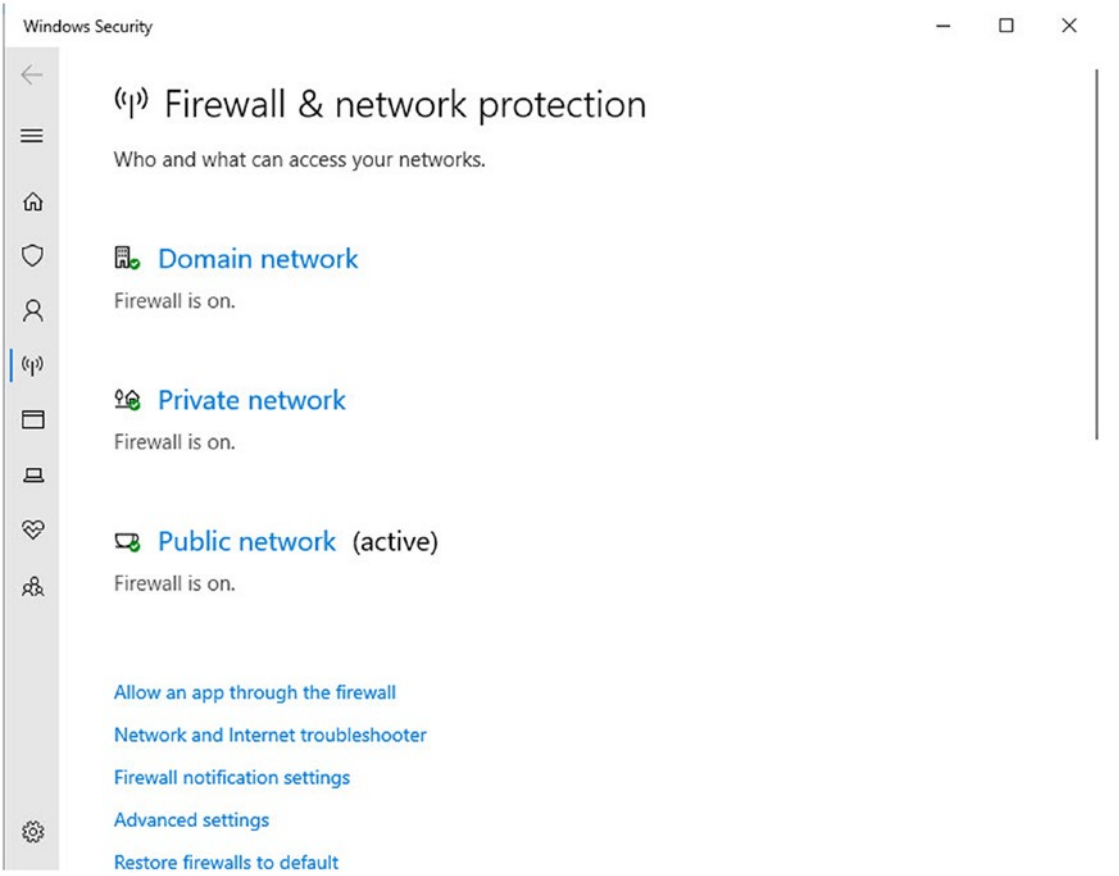


Figure 1-11. *The new firewall settings panel provides a useful interface*

Windows App and Browser Control

Windows App and Browser control, formerly known as Windows SmartScreen, is accessed through the Windows Security settings panel, and it keeps malware off the PC by checking web links and downloads against lists of known unsafe websites and files stored by Microsoft and maintained by all the major antivirus and computer security firms.

There are different and useful settings for App and Browser Control; see Figure 1-12. These include protection from malicious files, apps, and websites, as well as additional protection from exploits that may already exist in Windows 10 but that have not yet been patched (otherwise known as zero-day exploits), and browsing protections.

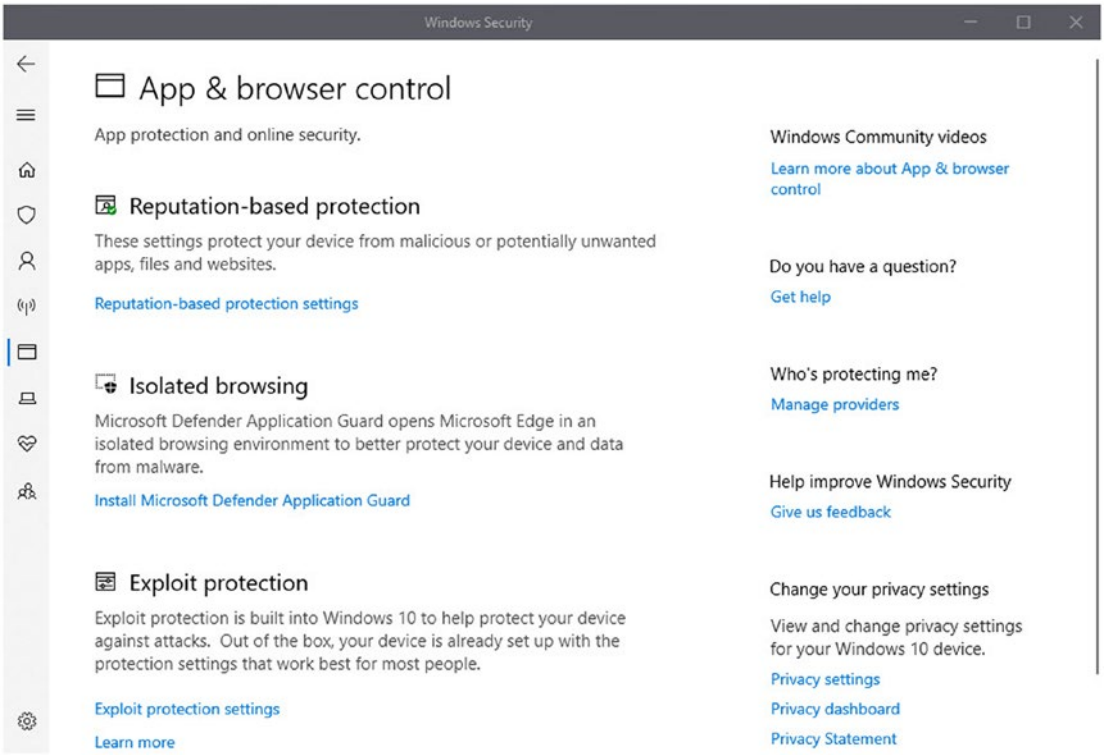


Figure 1-12. *Windows App and Browser Control has several types of protection available*

App and Browser Control is an extremely helpful and useful security feature, but, alas, it's all too easy for a PC user to deactivate it. There are settings available in Group Policy however that you can set across your PCs to enforce strict security for all users (see Figure 1-13), and it is well worth spending time configuring appropriate policies. Search for *Group Policy* in the Start Menu to find these settings, and you will find the specific options in the Group Policy editor under *Computer Configuration* ➤ *Administrative Templates* ➤ *Windows Components*.

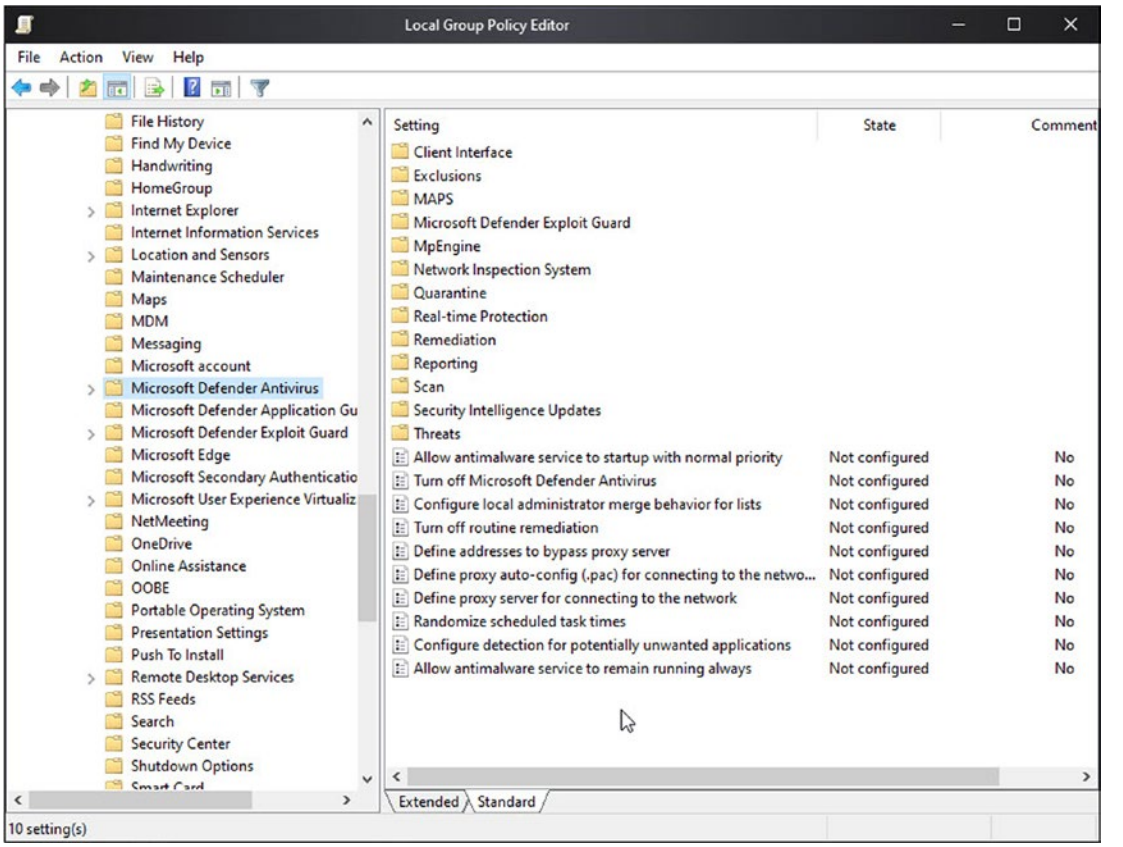


Figure 1-13. *You can set group policy for Windows security services*

User Account Control

At the root or Windows 10's security is the UAC (User Account Control) feature that was first introduced in Windows Vista, annoying so many people at the time. Back in the days of Vista, you couldn't even so much as change your PC's clock to a different time zone without being warned that this change could harm your computer and were you *really* sure that you wanted to do it.

These days, UAC is a much friendlier affair, and it will alert you only to significant events such as the installation of a new win32 desktop app (Windows Store apps do not trigger an alert as the Store has its own security in place) or if you make changes that could affect anybody else who uses the PC. Changes you make that will affect only your own user account are commonly highlighted with a yellow UAC Shield icon on the *OK* button, to alert you to be cautious.

You can open UAC from a link on the left side of the Security and Maintenance panel, or by searching for **uac** in Cortana or the Start Menu. The main UAC interface has a vertical slider with four settings; see Figure 1-14. These range from *Always notify me*, otherwise known as "annoying mode," to *Off*, which I certainly do not recommend, as switching UAC off can allow malware to quietly install itself on the PC.

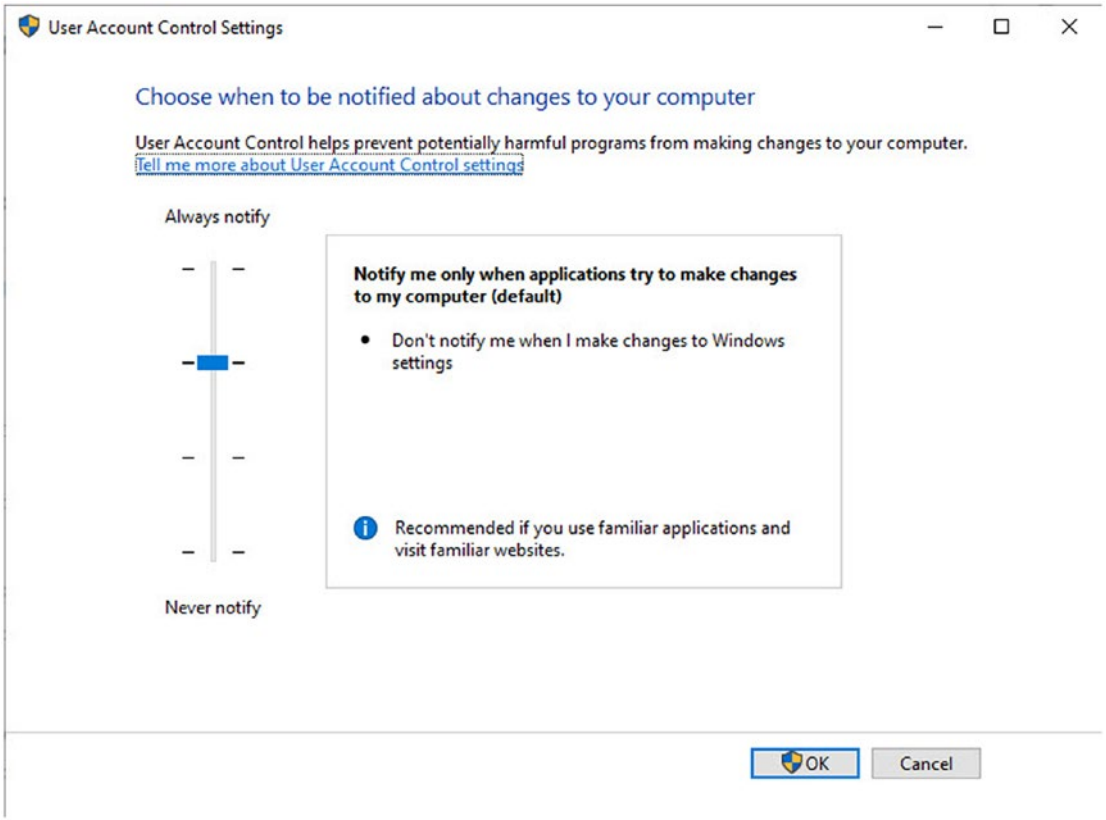


Figure 1-14. *You can control UAC through four different settings*

It is worth noting that at some point, the UAC controls will be fully integrated into the Windows Security panel, at which point that will be the only way to access them. At the time of writing, this has not yet been implemented in Windows 10.

Device Security

An addition to Windows 10, certainly since the first edition of this book was published, can be found in the Windows Security panel under the title *Device security*. Here are options for controlling how Windows 10 security interacts with the hardware on your PC and with its processor and memory; see Figure 1-15.

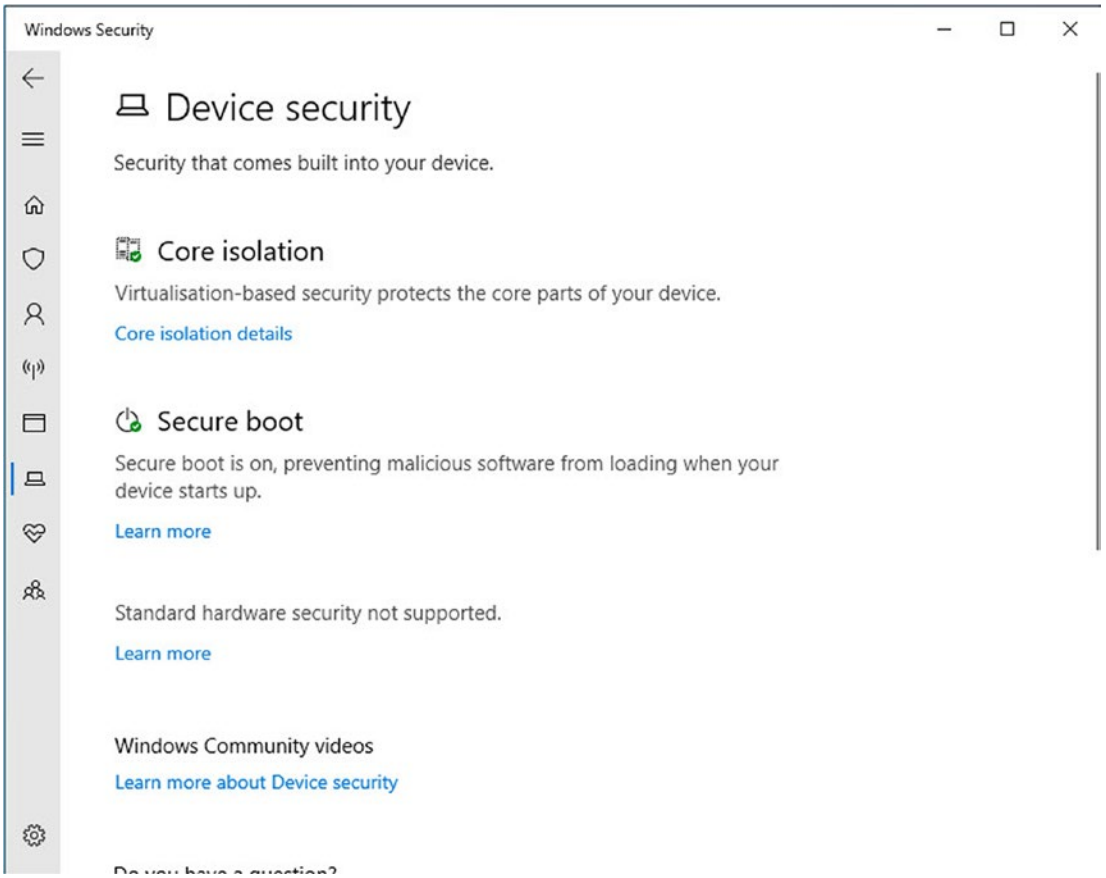


Figure 1-15. *Device security contains features you need to make sure are activated*

Core isolation contains features that have been created by Microsoft in conjunction with the main processor designers at Intel and AMD. They include features that can prevent malware from getting around the security on your PC by directly attacking known hardware exploits in the processor or memory (which of course can never be patched) by inserting malicious code that can cause aspects of the hardware/software interface to fail.

Secure Boot has been around since Windows 8, and has been mandatory on all new Windows PCs since Windows 8.1. It is a security system we will look at in more detail in Chapter 13, and it is sometimes deactivated by anybody who likes to dual-boot their PC with Linux, as some Linux distros don't provide Secure Boot support. Essentially Secure Boot prevents malware from injecting itself into the Windows boot loader, which would enable it to load before any of the other Windows security systems are running.

While this is an overview of the security features in Windows 10, and while they certainly highlight the most important aspects of PC security, we will go into much more detail on security and how to configure and maintain it in Chapter 21.

User Account Management

You might have noticed a common theme running through the section on Windows security in this chapter, that being that users can, and often annoyingly do, deactivate crucial security systems on their PCs because they "find them annoying," "they slow down the PC," which isn't true, or they stop the user "from doing what [they] want," which is very often the whole point, as if the user wants to do something that's blocked by Windows' security systems, it's very likely they shouldn't be doing it anyway.

When it comes to user accounts, it's important to create them in ways that constrain the user to do only what they ought to be doing, and not necessarily what they *want* to be doing. It might be difficult to prevent a user from spending time on Facebook or eBay, or from playing Minecraft (though these are fairly innocuous activities that are unlikely to jeopardize the security of the PC), allowing a user access to file-sharing, adult, or gambling websites (where malware can often hide), or permitting them to install their own apps and utilities on a PC, which does present a serious potential security risk and therefore a serious risk to the stability and operation of the PC and the integrity of its files and the data stored on both it and elsewhere on your network.

Remember that PCs no longer operate in isolation, not even in the home. Malware infecting a PC can quickly spread across the network, affecting other PCs, and even servers and network hardware and storage, and the result can be expensive downtime or even the opening of backdoors into company data that can result in an embarrassing and extremely costly data breach.

Administrators vs. Standard Users

Back in the days of Windows XP, every new user was an Administrator, even the Standard users to a certain extent, because there was no UAC feature to prevent unwanted changes being made to a PC. Administrators can change anything on a PC, anything at all. They can install new software, modify configuration settings, and even delete files in the \Windows operating system folder.

Standard users on the other hand can only make changes that affect their *own* user account, and nobody else's. This can have some downsides in the workplace, especially if a user does need to install the odd extra piece of software (all users can install apps from the Microsoft and Windows Business stores), but it's generally accepted that there should be just one Administrator on a PC (usually the person who knows what they're doing) and that everybody else should be a Standard user.

Local Accounts vs. Microsoft Accounts

If you are using PCs in the workplace, you'll most likely have users set up on PCs using Domain or Azure Active Directory accounts managed by a Windows Server system. Smaller businesses might have users signed into PCs using a Microsoft 365 account, but for everybody else it's the choice between using a Microsoft account to sign into a PC or a local account.

While it is still technically possible to install Windows with a local account (make sure the PC is disconnected from the Internet at the time of installation). Microsoft wants everybody using a Microsoft account because that's what offers the "best experience" and Windows 10 will try, and likely succeed in forcing you to switch to a Microsoft account instead. I just want to list then the pros and cons using Microsoft and local accounts on a Windows 10 PC (Tables 1-1 and 1-2).

Table 1-1. *The pros and cons of using a local account*

Local Account	
Pros	**Cons**
No personal data is shared with Microsoft	Syncing of personalization and Ease of Access settings is not supported
No files are stored in the cloud unless you deliberately set it up	Windows Store cannot be used without Microsoft account sign-in
	OneDrive file sync is not supported without Microsoft account sign-in
	Setup and configuration can take much longer After a reinstall

Table 1-2. *The pros and cons of using a Microsoft account*

Microsoft Account	
Pros	**Cons**
You get the full Windows 10 experience with all features supported and working	Personal advertising data is shared with Microsoft unless you opt out during or after installation
Profile sync across your Windows 10 devices (PCs, laptops, tablets, smartphones) including personalization and Ease of Access options	Integration is built into Microsoft services you may not wish to use
File backup and sync between PCs are possible using OneDrive	
Setup and configuration is partly handled automatically after a reinstall	

User Identity and Sign-In Management

Windows 10 supports many more ways for a user to sign into a PC than just by using a password, but this isn't always a good thing. These additional sign-in methods include picture passwords, where you draw shapes over a picture (fairly pointless but useful for children perhaps); a PIN, such as the one you use for your bank card at an ATM; and Windows Hello, which supports several forms of biometric sign-in from fingerprint readers to iris and facial recognition.

On my desktop PC, I have a webcam that is compatible with Windows Hello. This makes it extremely straightforward to sign in to the PC, as all I have to do is sit in front of the PC and have it recognize my face. It's secure, too; in 2015 *The Australian* newspaper tested it with six sets of identical twins and couldn't fool it into signing in the wrong user. It's worth noting that Windows 10 now supports two separate Windows Hello cameras, which is useful for people who use their laptop at home, plugged into a separate monitor with its own webcam on top.

You're no longer just limited to numerical combinations of insecure PIN codes either, as you can treat a PIN in the same way as a password by using any type of letter or special character in addition to numbers. My own Microsoft account password, as tested at howsecureismypassword.net, has 15 characters and 542 octillion possible combinations. A 4-digit PIN, however, has only 10,000 possible combinations.

You might wonder why I use Windows Hello on my desktop at all, given that a thief could steal the box and hack the PIN. I make sure that all of my PCs are encrypted using Bitlocker, which I'll talk about more in Chapter 18, but my desktop also has the advantage of being securely bolted to a solid wall by use of a land anchor and a steel cable. Nobody's getting access to my data without putting some real effort into it.

The sign-in options in Windows 10 are managed in the *Accounts* section of the Settings app; see Figure 1-16. One of the advantages of using this app if you have a Microsoft account is that it allows you to change your Microsoft account password easily, without having to find the security center on the Microsoft website.

Figure 1-16. *You can manage sign-in options in the Settings app*

There are additional options available to you however in the Windows Security panel (see Figure 1-17) that include Dynamic Lock, which can be used with a Bluetooth device such as a smartphone, to automatically lock (and unlock) the PC when you walk away from the computer taking the device with you.

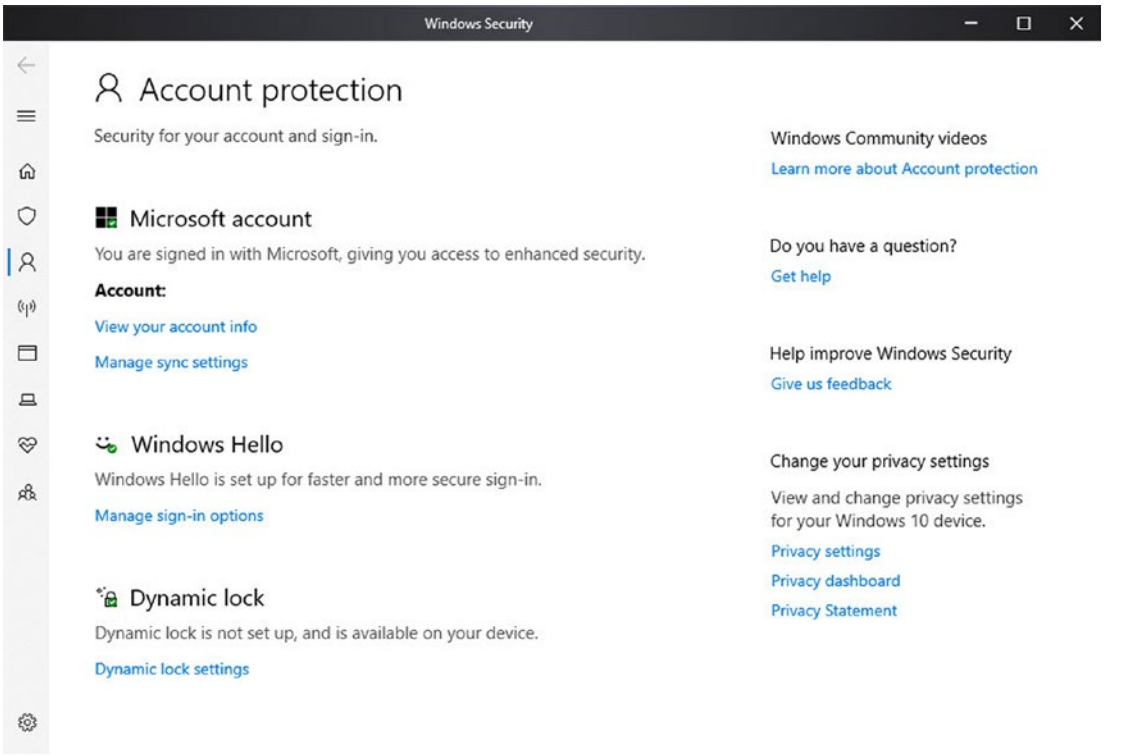


Figure 1-17. *Windows Security contains additional account protection options*

I do stress that if you are using a PC in a business environment, forcing users to create and then enter a long and secure password is by far the best way to ensure the resilience of the PC and your company data. I do have some suggestions for strong password creation however.

How to Create a Superstrong Password: Top Tips!

It is always a good idea to use a password manager, though the main web browsers such as Chrome and Edge have excellent password managers built-in that can sync across desktop and mobile platforms. If you don't use a dedicated password manager however, these are my top tips for creating superstrong passwords for use on your PC and with websites and Internet services:

- Create passwords that are a *bare minimum* of 12 characters in length.
- Always use a mixture of numbers, uppercase letters, lowercase letters, and symbols.

- Substitute some letters and numbers for other characters. For example, you can use a 5 instead of an s or S; an & instead of a or A; () instead of o, O, or 0; and / instead of the number 7.
- Use a phrase, perhaps a line from a song or poem, instead of a single word to make the password longer.
- Append some unique characters representing the service or website the password is for to the beginning or end of the password to make it unique to that service or website. For example, use ebA for eBay, aMa for Amazon, or g()() for Google web services.
- Choose a format you will use for each word in your password, for example, capitalizing the second letter of each word and substituting the first vowel with a symbol.

An Introduction to Family Safety

While we're on the subject of preventing users from doing things that can adversely affect the security of the PC, it's worth finishing up by talking about children. If you have children, then you also have my sympathies, because you'll be all too aware that especially younger children have almost no idea of what constitutes a risk, either in the playground or on the Internet.

Windows 10 does include Family Safety features, and when you add a new user to the PC, you'll be asked if they are a family member or somebody else. The former option then lets you choose if the person is a child or an adult. Child accounts are automatically hooked into the Family Safety features, which include website filtering, game ratings management, and usage time management for the PC.

For the purposes of maintaining security, it's the website filtering that's the most useful. This can prevent children from accessing adult, file-sharing, or gambling websites where malware is often found.

Note It's worth mentioning that no Family Safety or Child Protection feature, be they from Microsoft, from a third party, or managed by your Internet Service Provider (ISP), can't guarantee to block every attempt by a child to access content that you consider inappropriate. Thus, it is important to maintain good communication with your child on how they can keep themselves safe online, and why it is important for them to do so.

Managing and Deleting User Accounts

As I mentioned earlier, user accounts are managed in Windows 10's Settings app. There's really not much else you can do with them in the Control Panel. If you have a user set up on a PC that's an Administrator when they should really be a Standard user, you can change their account type in *Accounts* and *Family & other people*; see Figure 1-18. Note that you need to be signed in as an Administrator to do this.

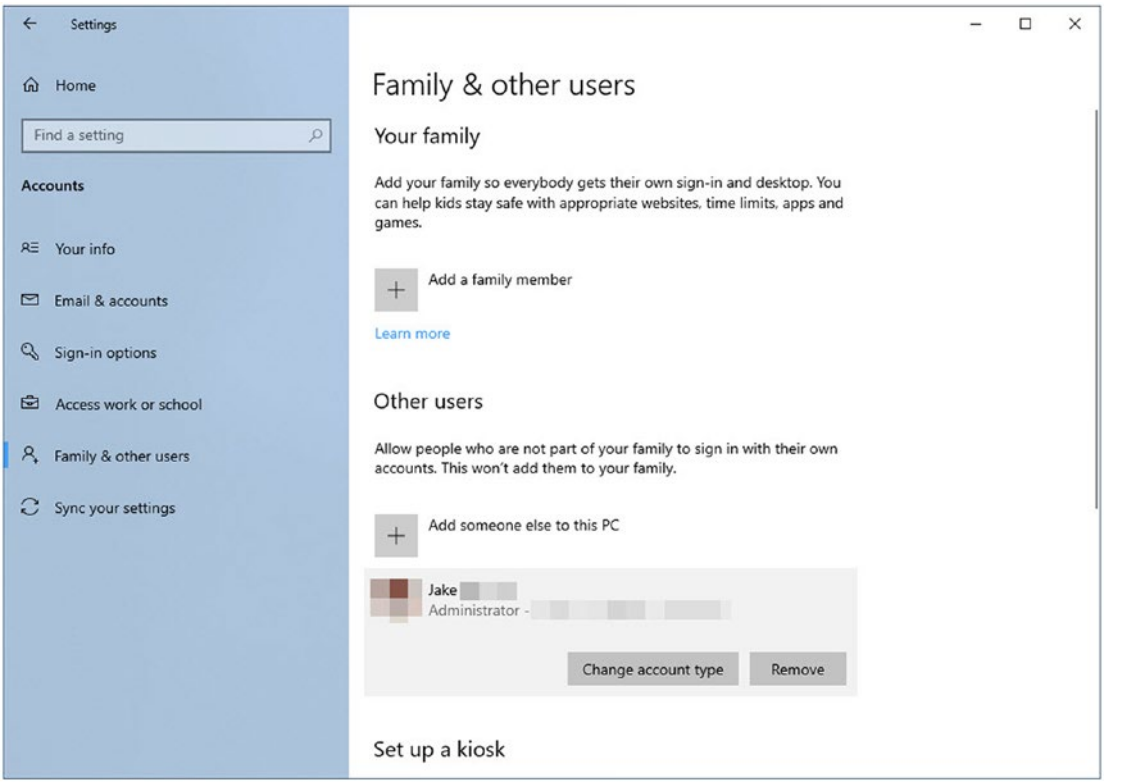


Figure 1-18. *You can change the account type of users in the Settings app*

Sometimes, though, you will want to remove a user from a PC. Clicking in their account name in the Settings app will reveal a *Remove* button. Bear in mind though that removing an account will delete their user folders from the PC, including any files and documents they have created and stored. Always make sure files are fully backed up before performing this action!

Caution Deleting user accounts and their files does NOT securely delete the files and data, which can still be recovered through the use of file recovery apps. To securely wipe currently unused space on your PC, you will need a third-party tool such as CCleaner from `piriform.com`. You can also wipe the free space on your PC by opening the Command Prompt (Admin) from the Win + X menu and typing `cipher /w:[directory name or drive letter]`.

Summary

In the first edition of this book, I finished this chapter by saying "*If I had a dollar for every time I told somebody, even whole rooms full of people, how essential it is to the smooth operation of a PC that basic security and user accounts are properly managed, I'd be writing this book on a beach in the Caribbean rather than in my office in Yorkshire*."

Things must have worked out for me though as obviously some people listened, and while I never made it all the way to Caribbean, I did get to the south of France. In large part this is because there is much greater awareness among the general public now about privacy and security, and how people's own personal data can be sold and abused.

We're not at the tipping point yet though where every PC user takes security as seriously as they should, and with a changing workplace brought about in no small part by repeated worldwide lockdowns due to the Covid pandemic, this presents even greater challenges for IT professionals and system administrators than it did before. This is because of the ever-increasingly decentralized nature of the workforce itself, and of the explosion in the use of workers' own personal computers for the purposes of business.

What makes things worse is not just that it's extremely straightforward to get the security on a Windows 10 PC right but that it's also far too simple for nontechnical people to switch off essential functionality, making understanding the options and tools available to prevent than from doing so ever more essential.

In the next chapter, we'll build on what I've detailed here and look at the tools and utilities available to help make PCs that are resilient and robust while also being easy to manage and restore should something go horribly wrong.

CHAPTER 2

Building a Safe and Secure OS

In the first chapter, as part of introducing troubleshooting in Windows 10 and on different types of PC, I highlighted just how essential it is to maintain good security. Any seasoned IT pro will confirm this is indeed essential, but no more so than creating a robust installation with an equally robust backup plan. Indeed, in these days of cyberattacks, ransomware, working from home, and data privacy, it's never been more essential to have a bomb-proof backup and security strategy, so this is a great place to begin this book proper.

It's ironic, however, that so many people spend so much time troubleshooting and diagnosing problems on PCs when the default action of any system administrator seems to be to simply reimage the machine, wiping the current installation completely and reinstalling a backup image, complete with settings and apps preinstalled. What's not to like about this?

The truth is more complex in that while it *can* be quick and straightforward to simply reimage a PC, it's not always the best option, and in many cases can take considerably longer than tracking down the cause of a problem and repairing it manually.

The reasons for this are many, though they begin with updates for both Windows and your installed apps. Depending on when a system image was made, which could be several years prior to the current problem appearing on a PC, the sheer volume of updates and new app installs necessary to get the user working again could take a prohibitively long time to install and configure. Even if you create regular snapshot images of the PCs on your network, you're not always out of the woods when it comes to problems. One of the quandaries with creating periodic image update snapshots is those snapshots will also inherit any current bugs or issues on the PCs you image, with even an insignificant problem perhaps causing much larger issues over time.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_2

There might even be new apps that need to be installed that the company (or the user) began needing after the system image was made, and other configuration changes can slow the process further. These might have come about because of underlying changes to Windows brought in by a Feature Pack, the twice-yearly update that we used to call a Service Pack.

We end in a situation then where what appeared to be just half an hour reimaging the PC and restoring a full backup becomes upward of a day of sitting in front of the PC installing and updating software, or where a user can't use the machine because it's sitting downloading and configuring apps and updates from the cloud.

Part of the solution to this lies in Windows 10's clever Reset feature, which I'll detail soon, but first of all I want to show you how to do the most important job you'll ever need to do with *any* Windows PC, laptop, or tablet.

Creating a Recovery Drive

One of the biggest disasters that can hit a PC is the inability for it to boot, or boot reliably, to the desktop. In Windows if you can't get to the desktop, or can't start the PC into its recovery options, then you're faced with having to reinstall the OS, and all your apps and configuration options, from scratch. This, as you can imagine, is a pain!

Fortunately, Microsoft has a tool that helps get around this problem, and it creates a Recovery Drive. This is a USB Flash Drive (8GB is a good minimum size) that can optionally include a full backup image of the installed copy of Windows if you have a larger capacity Flash Drive that can support it.

Tip Creating a Recovery Drive for a PC is the single most useful and essential thing you can ever do to aid troubleshooting and repair of Windows PCs. I urge you to create one for each PC you support, and to recommend to friends, family, and colleagues they also create a Recovery Drive for each of their Windows 10 PCs.

You will need a version of the operating system that matches the one installed on the PC. There's no point in trying to rescue Windows 10 Pro with an Enterprise ISO, or an older 32-bit (x86) installation with 64-bit (x64) media, but you should also have an install ISO version that matches the installed version on the PC. If you really can't get a matching version however, it's not the end of the world, as the version you can get

will very likely work. The changes and differences only come about when Microsoft make some bigger changes to Windows under the hood, and this then can create incompatibilities. It is for this reason that you should also refresh your Recovery Drives every year or two, just in case there have been changes to Windows that require an updated drive to be able to boot to the recovery options.

If you're rescuing a PC, then you need the correct media, every time. You can download an up-to-date ISO for Windows 10 from Microsoft directly at **www.microsoft.com/software-download/windows10**, but of course this only works if the latest version is also installed on the PC. If you need a different version, you can get these through your volume license subscription portal or another Microsoft subscription service such as My Visual Studio. You should always avoid downloading an image from any non-Microsoft website, especially from a torrent site. These images can very regularly have malware injected into them.

I should also mention here that DVDs, if you're still using them, have a finite shelf life. Sure, an official Windows 10 DVD from Microsoft will last considerably longer than one you burn yourself, but leaving it in a box, on a shelf, perhaps in the sun, will certainly shorten its lifespan. When will you get an official Windows 10 DVD anyway? I will admit that I've not seen a single one yet, because every PC I've encountered has had a free upgrade from Windows 7 or Windows 8.1 (via download) or has used a bootable USB Flash Drive or DVD with an ISO file downloaded from Microsoft. These days, official DVDs are rare.

Note Windows 10 systems installed on BIOS and UEFI firmware create different system partitions, and, as such, when you start your PC from a Recovery Drive, you need to start in the same way Windows 10 starts. I mention this because many UEFI PCs will permit booting as though it's a BIOS PC, and this may have happened if you installed Windows 10 from DVD or USB Flash. To check if your Windows 10 installation has only one *System Reserved* startup partition, it's been created in a BIOS boot; if there's more than one, it's UEFI. Check the boot options menu on your PC to make sure you start the PC from Recovery Drive the same way or else it won't be able to repair your copy of Windows.

You can create a Recovery Drive by searching in the Start Menu for Recovery, or by clicking *Recovery* in the Control Panel. It's not been moved to the Settings app as I write this, but will inevitably be moved at some point, so if it's not in the Control Panel when you look for it, check the *Update & Security* section of the Settings app instead, as that's where Microsoft will inevitably put it.

With an unused USB Flash Drive plugged into the PC, you can use an "on-the-go" (OTG) cable to plug full-size USB drives into the Micro USB ports on older tablets; click the *Create a recovery drive* link to open a simple wizard in which you will find a check box to also include a reset (system backup) image for the PC; see Figure 2-1.

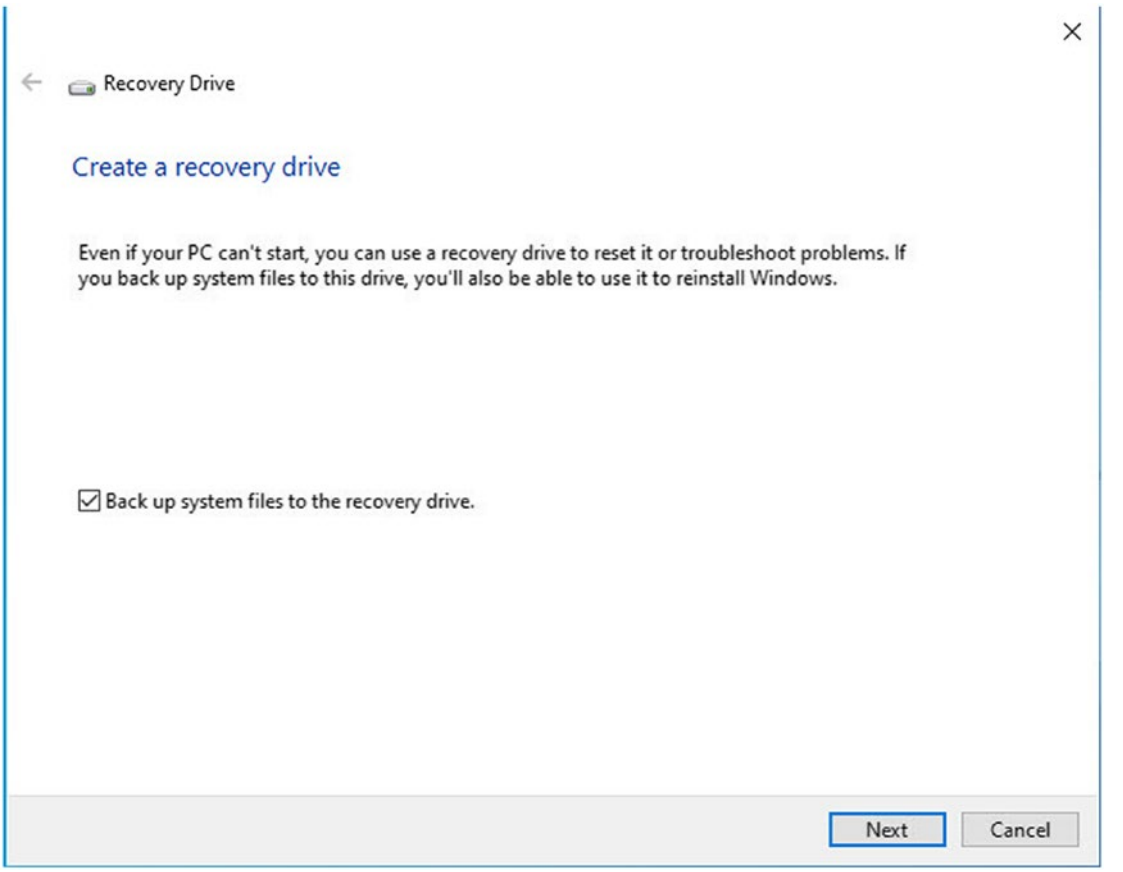


Figure 2-1. *You create a Recovery Drive by selecting Recovery in the Control Panel*

Note You will need to create a separate Recovery Drive for each different type of Windows installation on your PCs, and there are several reasons why. First of all, the hardware drivers on PCs will be different, as will the version of Windows 10 you have installed (Home, Pro, Enterprise, etc.), as I mentioned earlier, though you also need different Recovery Drives for 32-bit and 64-bit Windows installations, as one cannot be used to boot into the recovery options for the other. It might seem odd to consider that we even have 32-bit Windows installations these days, but they still exist on low-power, low-cost tablets and some older convertible laptops.

A Recovery Drive will allow you to start the PC directly into the Recovery options, and I will detail these in full in Chapter 8. Here you can perform actions from a System Restore to a full reimage, as well as gaining access to command-line tools to repair disk and startup problems. You will need to make sure the PC's BIOS or UEFI system is set to permit booting the PC from a USB device in order to use the drive. Some very old PCs that are still in use do not support booting from USB, and for these machines a DVD drive will still be required.

Backing Up and Restoring Windows 10

At the beginning of this chapter, I mentioned that IT pros will commonly want to reimage a PC when encountering a problem. With Windows 10, however, this raises a question: What system imaging tool do you want to use? This is because there are actually two different ones included with the OS. These tools work in different ways; both have their strengths and weaknesses, both have specific scenarios in which they are most useful, and one of them which is likely the better of the two is also probably going to be deprecated in the future and become unusable.

Reset

When you install Windows 10 on a PC, it automatically creates its own system backup image called a "Reset" image. This is cleverly maintained because it updates itself on a regular basis with the latest hardware drivers and Windows Updates so that, unlike a static System Image backup, when it's restored, it won't need updating with months or years worth of updates and drivers.

But! I hear you say. It's commonly a driver or an update that's the cause of a problem in the first place, so what's the point in this? The Reset feature in Windows 10 stores only those updates and drivers that have been installed on the PC for more than 30 days, the reasoning being that if you've been using them for a month already, there's likely nothing wrong with them as you'd have spotted a problem already.

Even better, the reset process doesn't wipe your user account(s) or files. A common problem with the System Image backup process is that a user's files need to be stored either on a server or on a separate partition or hard disk to Windows 10 itself, as the process of restoring the backup completely wipes everything currently on the Windows 10 partition, and replaces it with the contents of the backup.

A Reset image can be restored from the Settings panel; you'll find it in *Update & Security* in the *Recovery* section; see Figure 2-2. Indeed, it's so straightforward a process that a nontechnical PC user can do it without issue. You're asked if you want to *keep your files* [and folders], or if you want to *Remove everything* and wipe the PC (useful if you're selling it or giving it to a friend or family member), and the process is automated from there on.

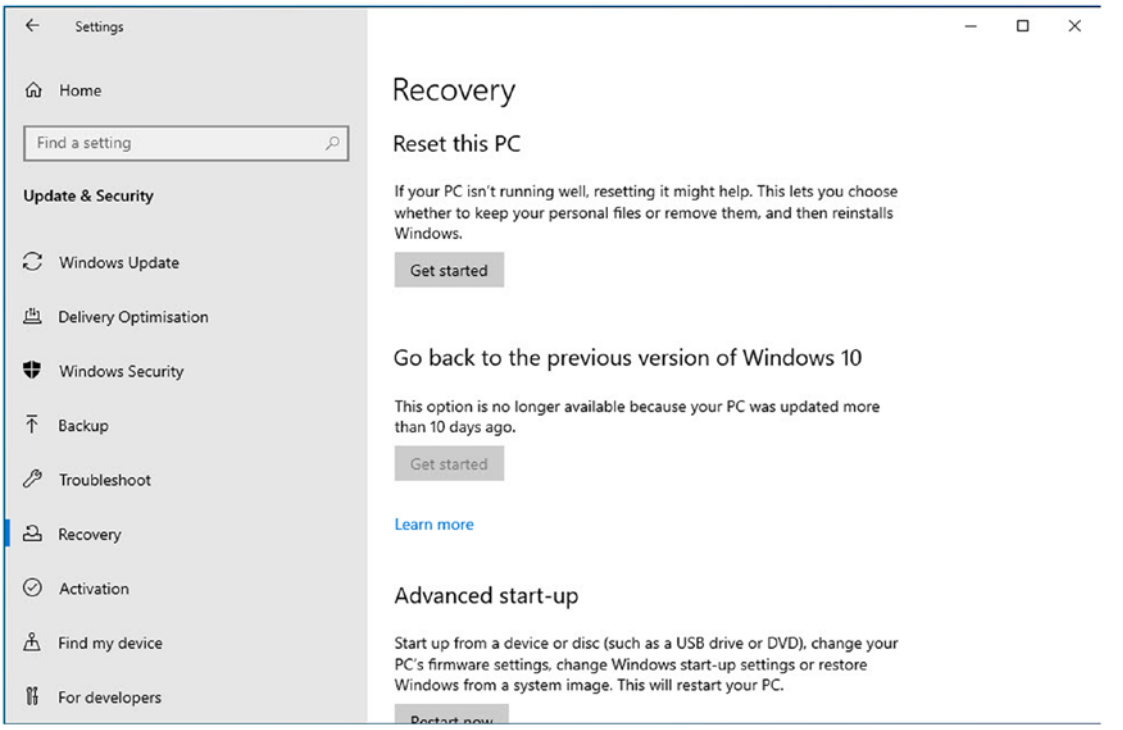


Figure 2-2. *You can reset a Windows PC from the Settings panel*

Note Completely wiping a PC using the Reset facility removes all user accounts and files from the PC but *does not* securely erase them. As I mentioned in Chapter 1, **to securely wipe currently unused space on your PC, you will need a third-party tool such as CCleaner from** `piriform.com`**. You can also wipe the free space on your PC by opening the Command Prompt (Admin) from the Windows + X menu and typing** `cipher /w:[directory name or drive letter]`**.**

On the face of things, this sounds like the ideal solution to image backup problems. End users can do it themselves, nondestructively, with all updates and hardware drivers included and with no risk they'll lose any of their files. What's not to like?

As with everything on PCs, there is a caveat, and it's an important one. A Reset image won't keep any installed win32 desktop apps or any configuration options that can't be easily restored from OneDrive, Azure, or a domain profile. It doesn't keep Windows Store or Store for Business apps either, though the process of reinstalling these is very straightforward compared to win32 software.

Thus, while this is a great solution for a home user that lives solely in the Microsoft Edge web browser, if the user has the full Microsoft Office suite, Adobe Creative Cloud, or any other non-Store apps on their PC, these will all need to be reinstalled and configured from scratch.

Note Windows 10 Reset works by using files located in the WinSXS folder to reimage the OS in such a way so as to keep it up to date. This means that manual checking and repair of the Reset image in the event of an error or corruption (Reset is intended to be self-managing and robust) isn't possible, as there isn't a single image. While Reset is intended to operate effectively 100% of the time, some IT pros (myself included) might want to also manually create a system backup image… just in case of a disk or partition corruption that would prevent Reset from working.

Restoring a Reset Image on a Nonbootable PC

Reset can be invoked from within the Settings panel in Windows 10, as I detailed earlier, and is very easy to operate. However, you might find that your installed copy of Windows 10 isn't bootable, and you cannot launch Reset from the desktop. Alternatively, you might find that the desktop environment is unstable, and crashes such as a Blue Screen of Death (BSOD) occur before you can invoke Reset.

In both cases you can run Reset from the Recovery Options in Windows 10. There are several ways to access this menu:

- From the Settings app, in the *Update & Security* section, click the *Recovery* tab and then click the *Restart now* button in the *Advanced Startup* section.
- From any power control (the Sleep, Shutdown, and Restart buttons in the Start Menu or at the Sign-in screen), hold down the Shift key while clicking *Restart*.
- Start the PC from the Recovery Drive you created for it, because you *did* create one–didn't you!?

Note If your PC is encrypted using Bitlocker (I'll show you how to use this in Chapter 18), you will need your 48-character unlock key. You are prompted to back this up when you encrypt a drive, but if you use a Microsoft account and have chosen to back up the key there (you have to opt into this at encryption time), you can find your keys stored online at `https://onedrive.live.com/recoverykey`.

When the Recovery Options menu loads, you have two further options to choose from depending on whether you want to use the Reset image on the PC's hard drive or a Reset image you copied to the Recovery Drive automatically when you created it.

To reset a PC from an image on the Recovery Drive, click *Use a device* (see Figure 2-3), and select the USB Flash Drive that's your Recovery Drive.

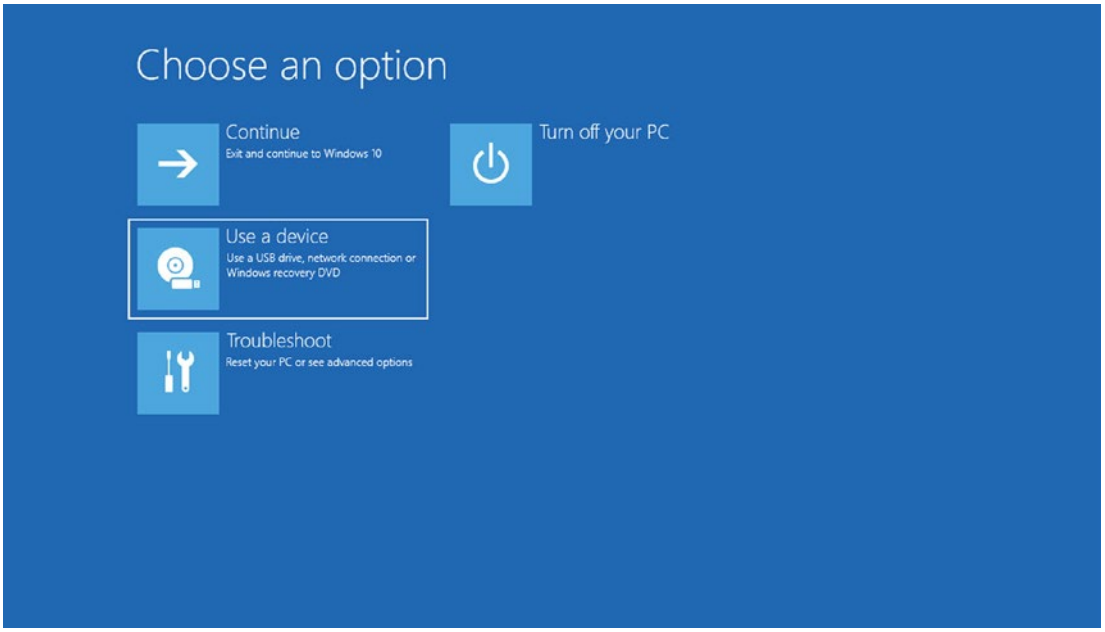


Figure 2-3. *You can click Use a device to reset a PC from an image on a Recovery Drive*

Then, or if you are using the Reset image on the PC itself, click *Troubleshoot,* and at the next screen, click *Reset this PC*; see Figure 2-4. You will then be guided through the process of restoring Windows 10 using the correct Reset image. Note that you will need to know an Administrator password to complete this process.

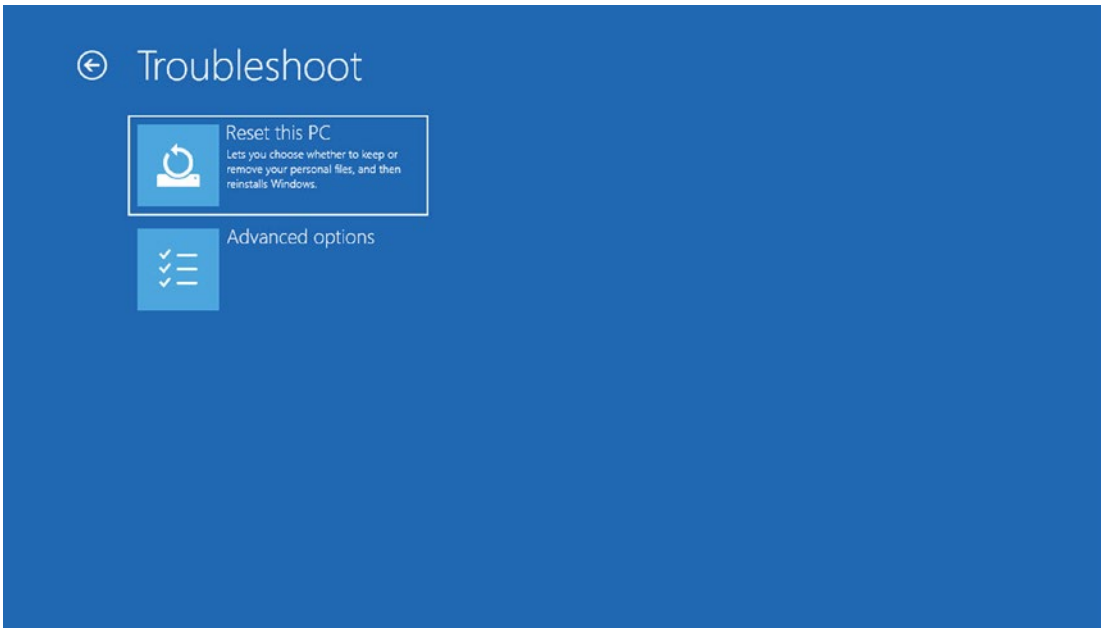


Figure 2-4. *You can reset a PC from the Recovery options*

System Image Backup

If you're a system administrator or an IT pro, the chances are you'll already be familiar with and have used image backup software such as Symantec Ghost or Acronis True Image. Windows has included a System Image Backup feature since Windows Vista, and it offers some compelling benefits over the competition, not the least of which is that backups can be created and restored without the need for any external media (DVD, USB Flash Drive).

Creating a System Image Backup

Oddly, if you search in the Start Menu or the Taskbar search box in Windows 10, no combinations of the words **system**, **image**, and **backup** will display a quick link to the System Image Backup utility. There are two ways to access it, and I'll detail both, though I fully expect both of these to be removed in a forthcoming Windows 10 update as the feature is likely to be deprecated.

The first of these methods is to click *Backup and Restore (Windows 7)* in the Control Panel, and then to click the *Create a system image* link that appears in the top left of the window. The reason I say that I expect for this to be removed in a forthcoming update is that this is included (as it was in Windows 8) to aid migration of users from Windows 7 who

had files backed up using that OS's file backup utility, and in the Windows 8.1 update, it vanished. You should not think of this as a long-term feature of Windows 10 and therefore should not use the file backup utility it also provides.

The other method of accessing the System Image Backup utility is to open *File History* in the Control Panel; a *System Image Backup* link will appear in the bottom left of the window. As I write this, clicking the link opens the *Backup and restore (Windows 7)* page, but this as I mentioned is very likely to change, perhaps even by the time you read this.

The System Image Backup utility opens as a wizard that offers you three locations for storing your backup, on a local hard disk or partition on the PC (this must be an internal drive; USB-connected drives are **not** supported), on one of more DVDs or on a network location; see Figure 2-5.

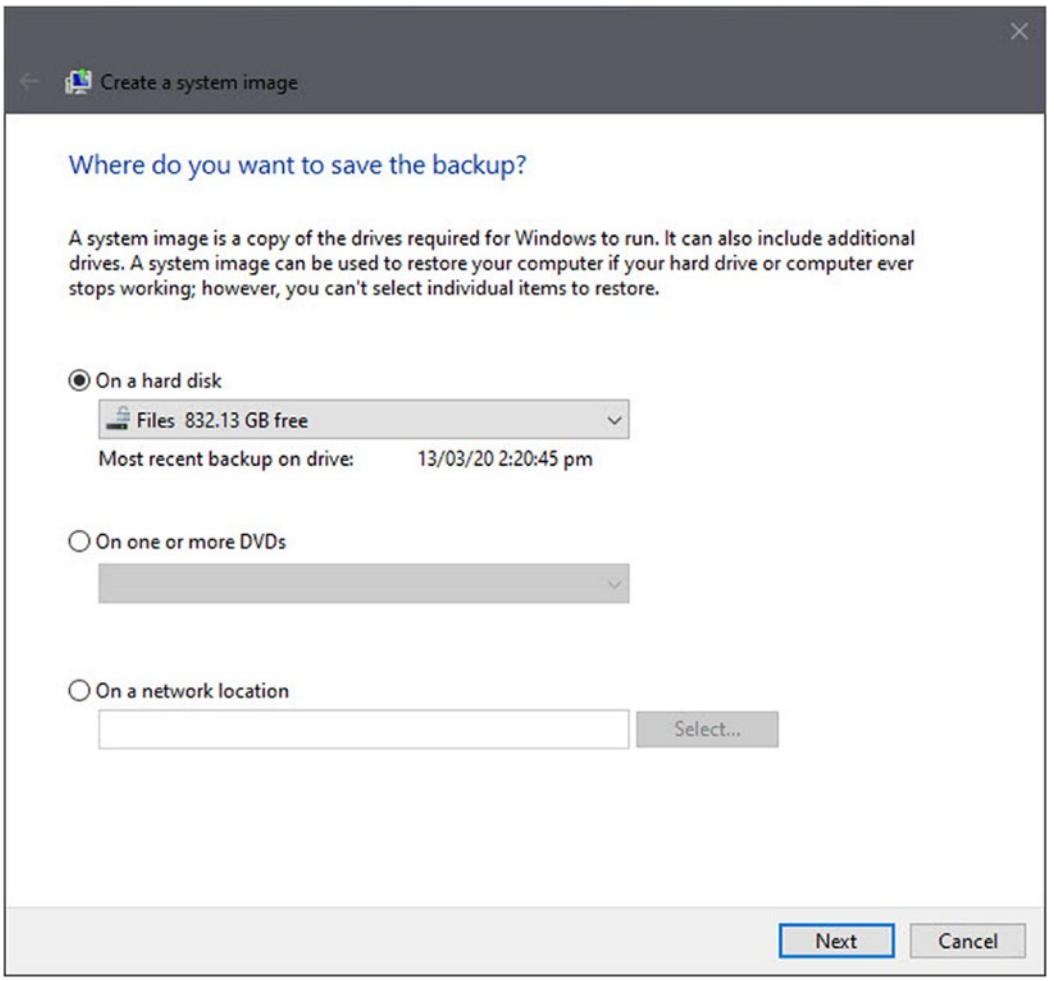


Figure 2-5. *The System Image Backup utility is an easy-to-use wizard*

I want to deal with the issues this can throw up. The first of which is storing your backup on DVDs (Blu-ray burners are also supported). Let's set aside for a moment that burned optical disks tend to have a limited lifespan, and so can't be relied upon for long-term archival storage. A "typical" Windows 10 installation, however, at about 25GB in size would require up to 6 DVDs, and my own most basic installation at around 100GB would require 23 of them. That's a substantial time investment for both creating and restoring the backup, and that's assuming that none of the disks fail in the interim period.

Network storage can also present a problem. You can create your backup on any network location accessible on your PC. This can include server network shares, network-attached storage (NAS), and a USB hard disk plugged into your network router, but… **you must never store a System Image backup on a network share you can only connect to by Wi-Fi**. The reason for this is that the system image can be restored only from the Windows 10 Recovery Options, and these have no way to load Wi-Fi drivers, and as such, cannot connect to remote storage by any method other than by a physical network (Ethernet) cable.

There is also the small matter of your files. On some PCs, where files are stored on a server and synced using a roaming user profile, or where all your files are synchronized to a cloud backup service such as Dropbox or Google Drive, and where you don't have many files, you might be content to leave them sitting in your `C:\Users` folder.

If you use OneDrive however, or if you have more files than can easily and quickly be downloaded from a web service, you should **always** store your files on a separate physical hard disk, or partition on your PC.

The reason for this is that a system image is a full snapshot of the disk or partition on which Windows 10 is installed at the time the backup image is taken. When you restore this backup image, that entire disk or partition will be restored exactly as it was at the time the backup was made. If files are stored on this drive or partition in the `C:\Users` folder (or elsewhere on the same drive), they will overwritten, and older versions of your files will be restored.

With cloud backup services such as Dropbox and Google Drive, this doesn't present too much of a problem, as restoring a backup will require those services to completely resync all of your files downward from cloud storage anyway. OneDrive works differently, however, in that it can simply pick up from where it left off before. The OneDrive client is getting much better with this type of problem, but because it works very differently from the other cloud backup providers, there's never any guarantee.

Caution While this will sync all of your current files down from the cloud, it will also likely back up all the old versions of files, and files you've long since deleted that are included in your backup, to the cloud again.

There's also the fact that including personal files in a system backup will inflate the size of the backup file, perhaps considerably, and if you need to perform a complete format-and-clean reinstallation of Windows 10, you won't restore them anyway.

I'll show you how to move your Shell User Folders (Documents, Pictures, Music, Video, etc.) and how to create new and manage existing partitions in Chapter 3. Moving your files away from your copy of Windows 10 is a good idea anyway, since if you have a major problem with Windows 10 that requires a clean reinstallation of the OS, you won't lose your files in the process.

When you have chosen your backup location, you will be asked which hard disks or partitions in the PC you wish to include in the backup. Anything you can't exclude because it's essential to the operation of Windows 10 is grayed out, and you're likely to not want to select anything else; see Figure 2-6.

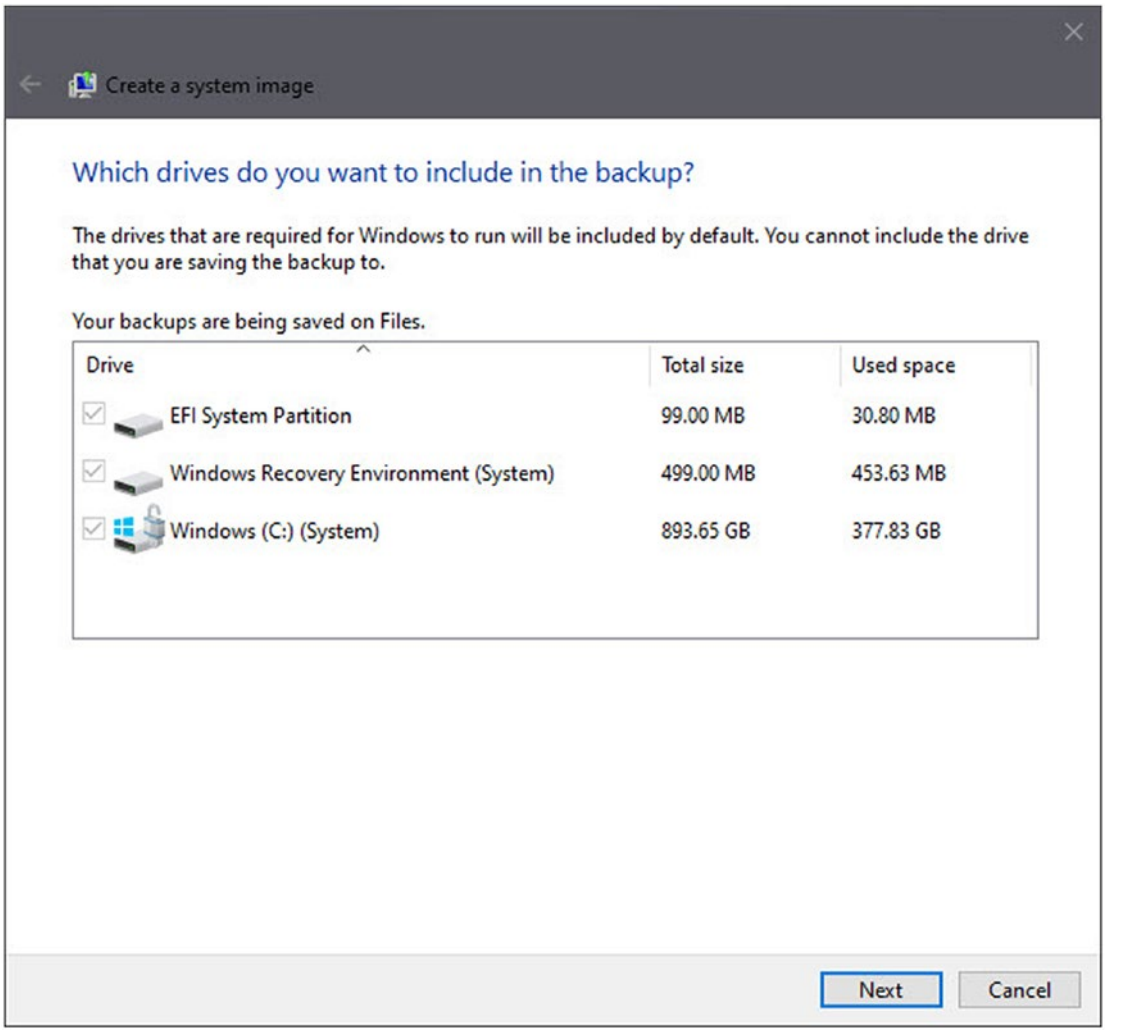


Figure 2-6. *You will be asked what drives or partitions you wish to include in the backup*

I mention this, however, as you may have a small partition on which you store hardware drivers or other setup files for the PC that would be useful to include, or you may have a separate partition on which some win32 apps are installed.

When you click *Next,* you will be presented with details of the backup location and partition inclusion options you have selected, and asked to begin creation of the System Image Backup.

Restoring a System Image Backup

As I mentioned a while ago, you restore a System Image Backup from the Windows 10 Recovery Options. There are, just as with performing a Reset, three ways to access these options (Windows 10 starts up far too quickly for the F8 startup menu to be something I can still recommend). You can open the Settings app, click *Update & Security*, and in the *Recovery* section, click the Advanced Startup button. You can also hold down the *Shift* key on your keyboard while clicking Restart from the Start Menu power options or sign-in screen. You can also start your PC from the USB Recovery Drive *that you definitely created!!* You will need to make sure your PC's BIOS or UEFI system is set to permit booting from USB devices, however.

Caution Do not encrypt a drive or partition containing a System Image Backup with Bitlocker, as the Recovery Console will be unable to see it and therefore be unable to restore it. This does present some potential security issues, which is another reason to store your files away from your Windows installation and to maintain strong passwords and Windows Hello biometric authentication on all user accounts on the PC, as a restored backup will be unencrypted, and you will have to reencrypt it with Bitlocker afterward.

At the Recovery Options screen, click *Troubleshoot* and then *Advanced Options* as seen back in Figures 2-3 and 2-4. You will then see a link to *See more recovery options* which you need to click to then display *System Image Recovery*; see Figure 2-7.

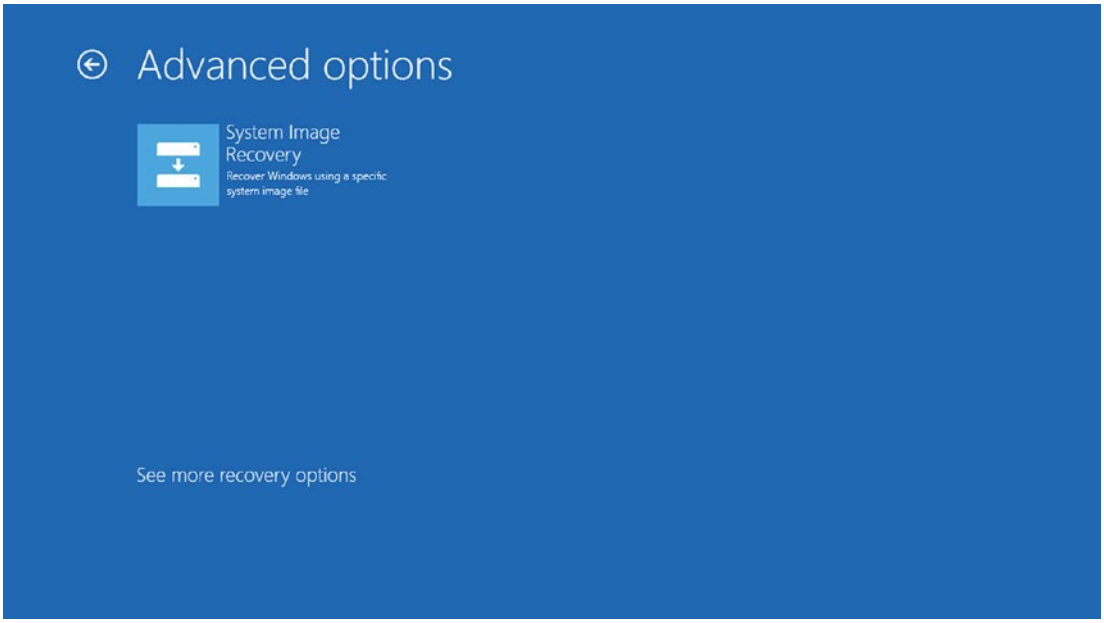


Figure 2-7. *You can restore a system image from the Recovery Options*

If a system backup image exists on the PC, it should be found automatically by the system; if no image is found however, perhaps because you are storing it on a network drive or because the disk containing the backup requires a RAID or another hardware driver, choose the *Select a system image* option, and click *Next*.

If you need to search for a network location, you will be asked for the full address of the network folder containing your System Image Backup in the format `\\server\share`; see Figure 2-8. Alternatively, you can click *Install a driver* to load a RAID or other hardware disk driver.

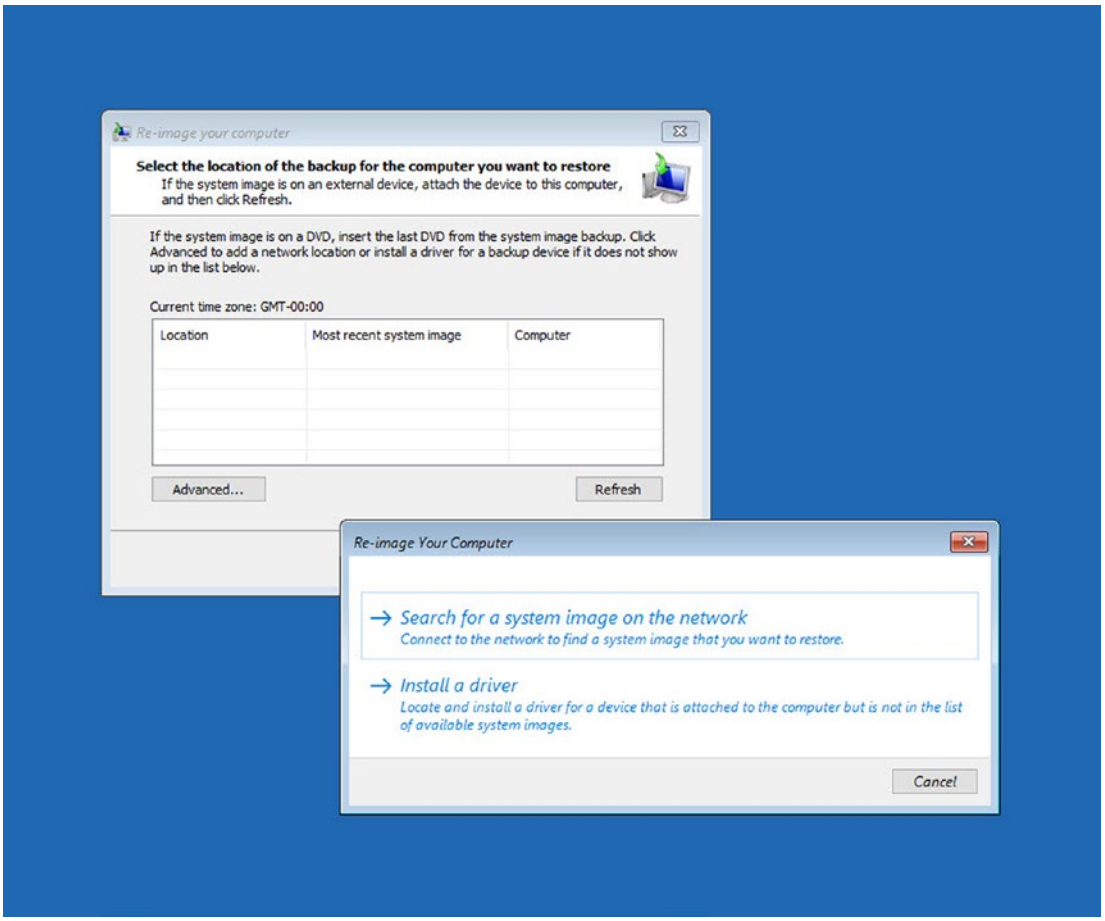


Figure 2-8. *You can search network connections where the PC is connected by an Ethernet cable*

If you do not know this, perhaps because it is managed by your system administrator, you can ask them or, on another PC that also has access to the file share, open its location in File Explorer and then click the icon to the left of the address (breadcrumb) bar to reveal the full network address; see Figure 2-9.

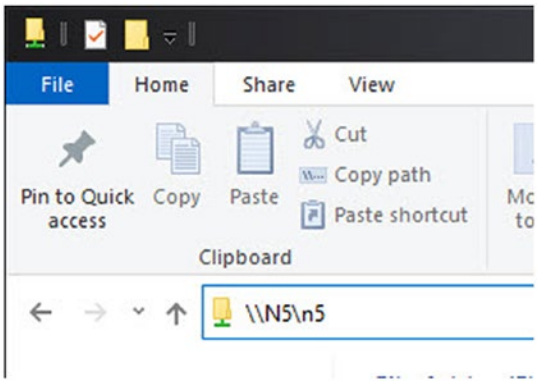


Figure 2-9. *Network addresses can be obtained in File Explorer*

Using Windows System Restore

System Restore has been around since the days of Windows ME, and if like me you're a seasoned (by which I mean older) IT pro, you'll know that people often deactivated it as it was a great place in which viruses could hide, ready to pounce again when a restore was actioned. Fortunately, the advent of User Account Control (UAC) in Windows Vista put an end to that behavior once and for all, and System Restore is now a reliable method to quickly repair a malfunctioning copy of Windows.

What System Restore does is take a snapshot of critical operating system, driver, and app files when a significant change, such as an app or hardware driver install or removal or a Windows Update, is performed. These snapshot files are stored in the hidden `System Volume Information` folders on your hard disks, if you've ever wondered what they were for. Should a change cause something to become unstable or fail to work, System Restore can roll back the change to undo the damage.

There are several ways to access System Restore. If the PC is completely unbootable, starting into the Recovery Options (perhaps using the USB Recovery Drive you made!!) and clicking *Troubleshoot* and then *Advanced Options* will present a System Restore option, as seen back in Figure 2-7.

From within Windows 10, you might be unsurprised to hear that searching in the Start Menu or the Taskbar search box for the words **system** and **restore** won't display it for you. Searching for just **restore** however will display the *Create a Restore Point* option which you can use. Alternatively, opening *Recovery* from the Control Panel will present links to *Open System Restore* and *Configure System Restore*. It's worth noting that I expect these options, as with all Control Panel items to be eventually deprecated and subsumed into the Settings panel, so if it's not in the Control Panel, then you'll know where to look for it.

If you click *Create a Restore Point* or *Configure System Restore,* you will be presented with the System Protection options in the System Properties dialog; see Figure 2-10.

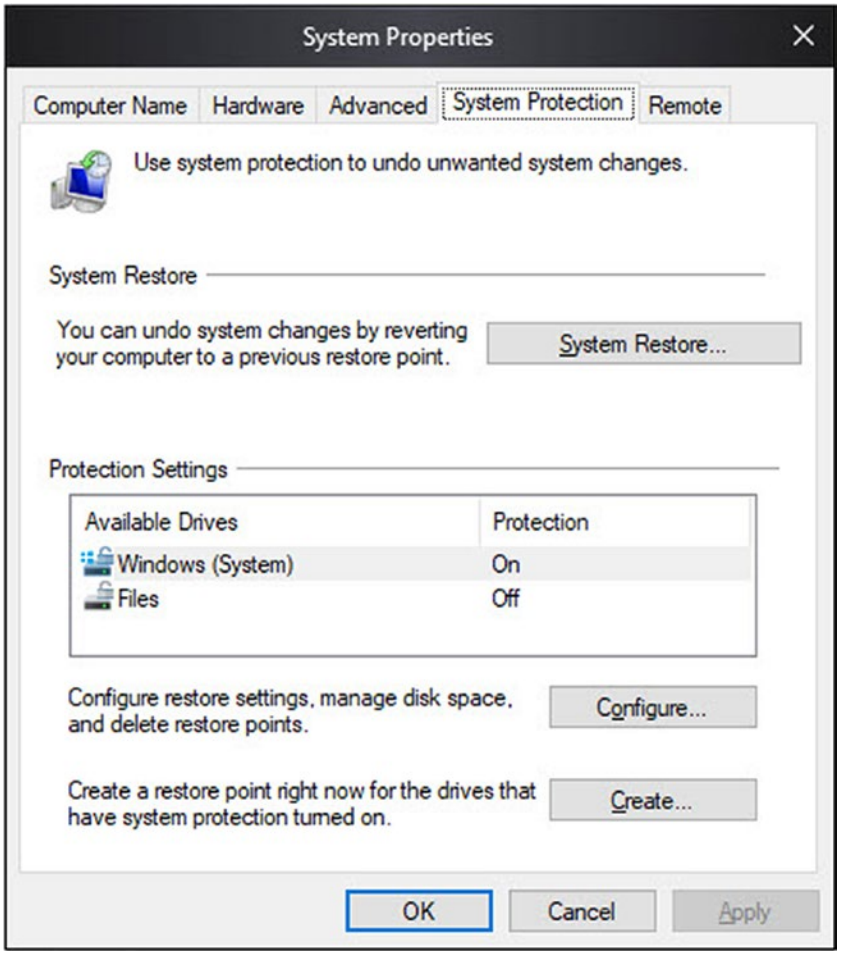


Figure 2-10. *You can create Restore Points manually*

As I mentioned earlier, Restore Points are created automatically when an app or a driver is installed or removed, or when Windows Updates are installed. You can click the *Create* button, however, to manually create a Restore Point if you are making a change that won't trigger the automatic creation of a Restore Point, such as moving the Shell User Folders or editing the Registry.

To restore Windows system files, drivers, and apps back to a previous point in time, click the *System Restore* button or click *Open System Restore* from the recovery panel. This will open a wizard that explains on its first page what System Restore will do.

At the next page (see Figure 2-11), you will be presented with a list of the most recently created Restore Points. If any additional Restore Points in addition to those displayed exist on the PC, in the bottom left of the dialog, there will be a check box to *Show More Restore Points*.

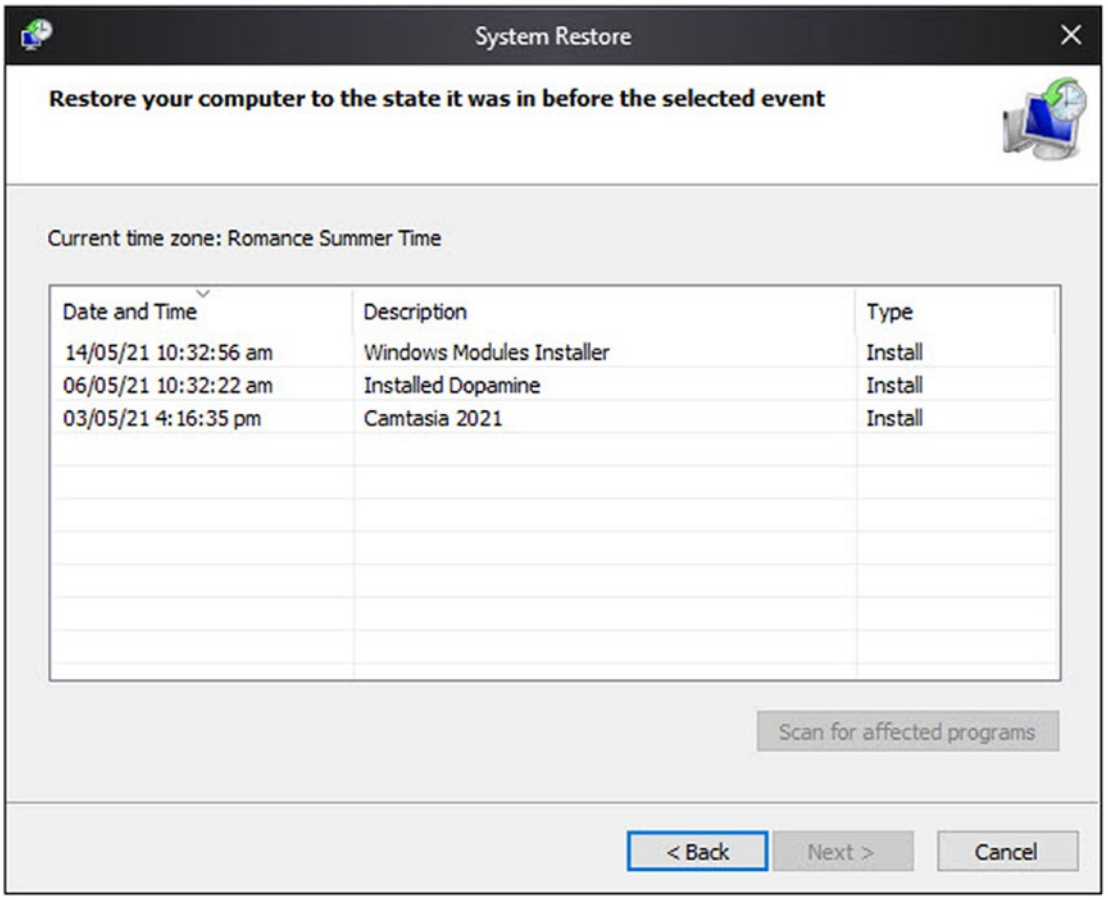


Figure 2-11. *Windows 10 stores several Restore Points from which you can choose*

Once you have chosen a Restore Point, by clicking it once to highlight it, you can optionally click the *Scan for affected programs* button to see what apps might be rolled back to previous versions or uninstalled (see Figure 2-12), in which you can see that removing Camtasia 2021 will adversely affect other installed programs as well that will then have to be updated once again.

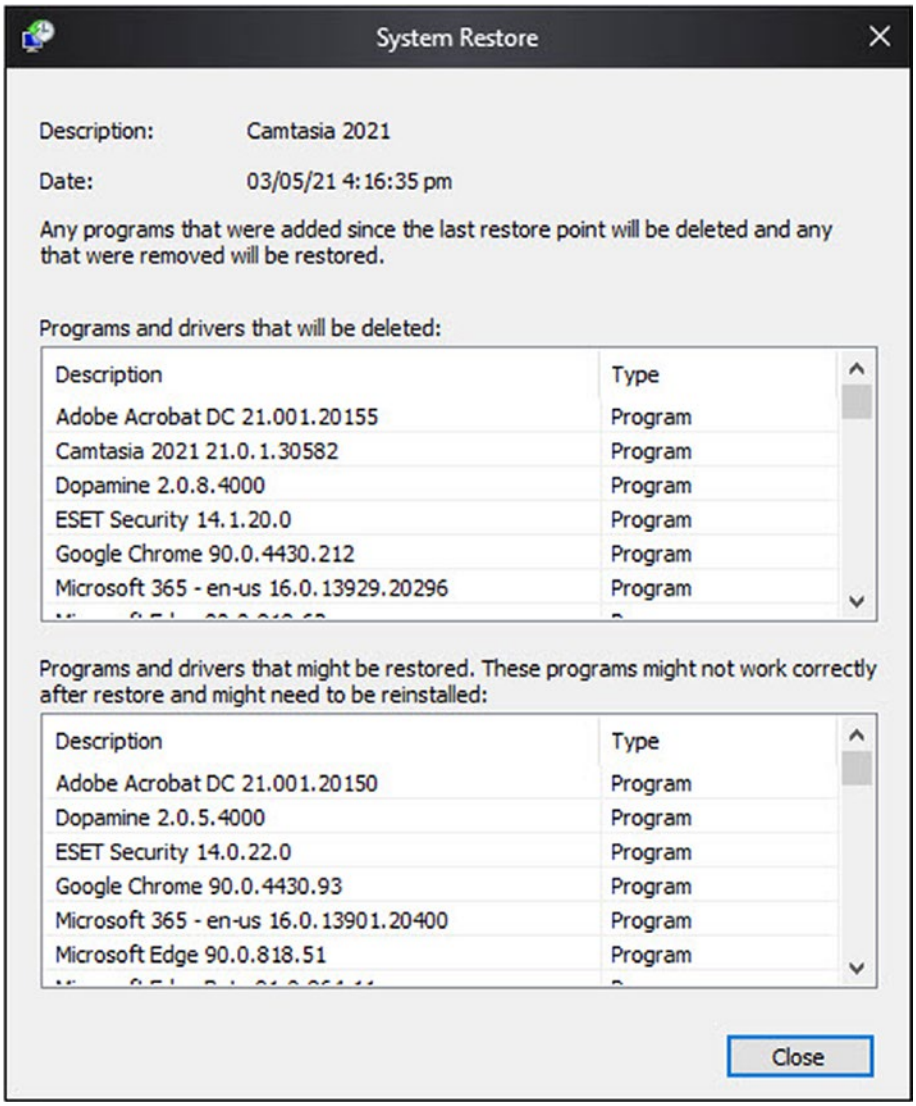


Figure 2-12. *You can see what apps and updates will be removed using System Restore*

When you are happy to restore Windows 10, then click the *Next* button to confirm your actions and begin the System Restore process, during which your PC will restart. I should add this works identically when running System Restore from the Recovery Options menu.

Configuring System Restore

When you install Windows 10, System Restore is configured to run automatically on all the drives on your PC. You might have drives though for files or other purposes that will never be affected by System Restore because you only use them for storing files and documents. Alternatively, you may wish to increase, or reduce, the amount of space System Restore uses on your Windows drive.

You can configure System Restore in the System Properties dialog, accessed by searching for **restore** in the Start Menu or Taskbar search box. Select the disk you want to change the settings for (there may be several in the list), and click the *Configure button*.

As seen in Figure 2-13, you will be able to enable or disable System Protection (another way to describe System Restore that also includes file shadow copies for version control) for that drive, and to change the amount of disk space System Protection uses.

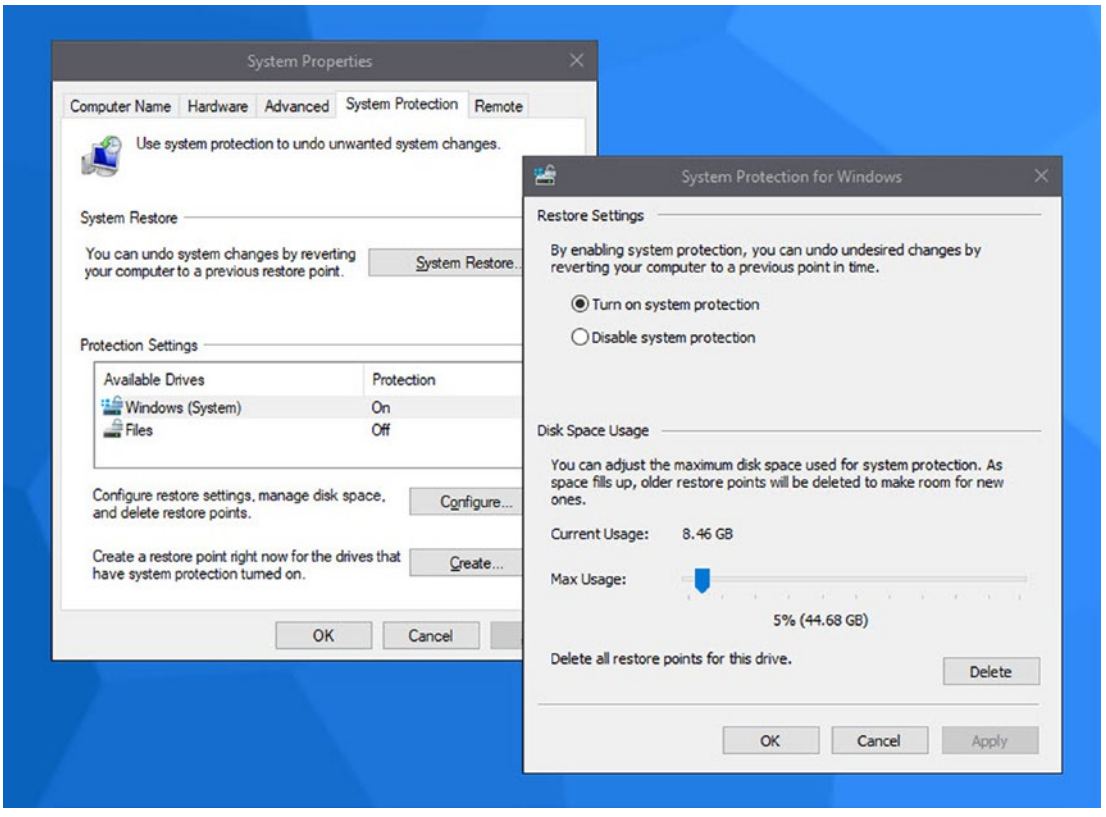


Figure 2-13. *You can manage System Restore on each drive or partition in your PC*

I should put in a note here about shadow copies of files. These hook into Windows 10's File History feature (if you have it activated and if it's not also been deprecated by now, with it being in the Control Panel) and allow you to roll back to old versions of files should you make a change to a file you didn't wish to make. I'll show you how to use File History shortly. File History does not require the drive on which your files are stored to have System Protection activated, as you can choose where it stores its backups.

Using the Windows 10 Media Creation Tool

Did your PC come with installation media for Windows 10? No, mine didn't either. Installation media for Windows 10 is now only ever obtained if you specifically purchase a retail copy of the OS in a store or is available as an additional purchase with a new PC online. If you purchase a new PC with Windows 10 preinstalled, you won't get a disk; if you took advantage of the free upgrade offer from Windows 7 or Windows 8.1, you won't get a disk either.

If something really goes wrong with Windows 10, however, and you haven't created a USB Recovery Drive (which you did, right!?), Windows 10 needs to be completely reinstalled. If you don't have access to a Windows 10 installer download from the volume licensing program or Microsoft's My Visual Studio website, or if the A-Team isn't available (though they probably wouldn't be able to help much either if I'm honest), you can create your own installer, either on an optical disk or on a USB Flash Drive, at any time.

This can come in handy even if you do have an installation DVD for Windows 10. For one thing, this is because the installation media might contain the wrong version of Windows (e.g., Pro when you need Home), but a DVD might also not be much use if you need to reinstall Windows on a modern laptop or ultrabook that doesn't come with an optical drive. For another, a download from Microsoft will always be of the most recent version of Windows 10, whereas the one on your DVD might require several years of additional patches and updates.

Tip If you need to reinstall Windows on a tablet that does not have a full-size USB port compatible with your Flash Drive, you can purchase what's called an "on-the-go" (OTG) adapter cable from good retailers.

You can download the Windows 10 Media Creation Tool free and at any time from www.microsoft.com/software-download/windows10. This tool will ask you if you want to upgrade the current PC or create installation media for another (which includes the current) PC; see Figure 2-14.

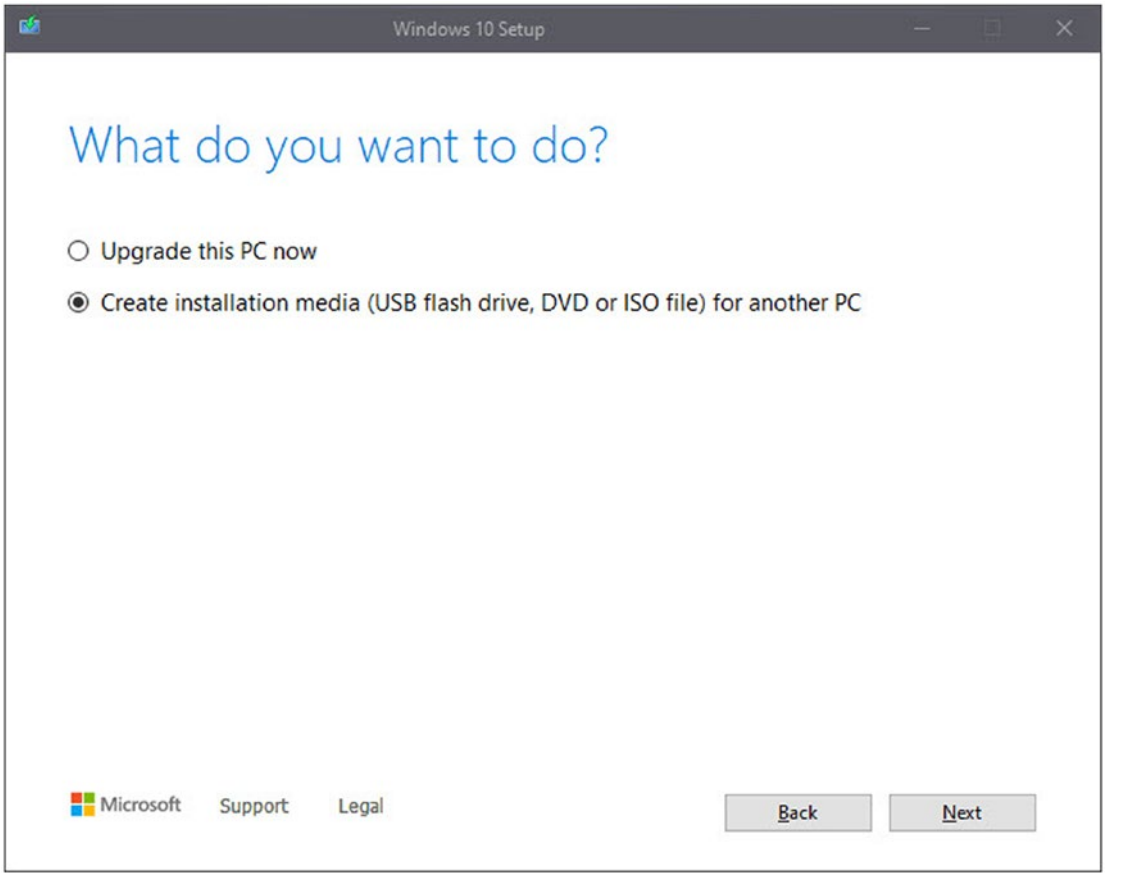


Figure 2-14. *You can create a bootable DVD or USB Flash Drive for Windows 10 using the Media Creation Tool*

You will be asked what language you want Windows 10 to be, what edition of Windows you want (note if it just says Windows 10 it will create media that includes both the Home and Pro versions), and if you want the 32-bit (x86) or 64-bit (x64) version or a dual installer.

Tip If you do not know whether you need the 32-bit or 64-bit version of Windows 10, and can still start the PC to the desktop and open *System* and then *About* in the Settings panel, or *System* from the *Control Panel*, where you will find the current *System type* detailed.

You will then be asked if you want to create a USB Flash Drive (which must be at least 3GB in size, preferably 4GB or larger) or download an ISO (disk image) file. Once you have selected an option, you will either be promoted to insert a USB Flash Drive, which will be formatted by the utility (so make sure there's nothing on it you want to keep) or an ISO file will be downloaded.

Note If you need to perform a format and clean reinstall of Windows 10, and Windows 10 has previously been installed and activated on the PC, you will not need to enter your product key during the installation process as the OS will recognize the PC and activate automatically when it next goes online as Windows licenses are tied to the machine (codes hidden in the BIOS) and not the user account so you can't move that copy of Windows 10 to a new PC. At the product key request page of the installation process, simply click the *skip* button, and continue the installation normally.

If you want to then create a bootable DVD from the ISO file, right-click it in File Explorer, and you will see *Burn disk image* appear in the context list of options; see Figure 2-15. You will be prompted to choose the DVD or Blu-ray drive in your PC and to insert a blank disk.

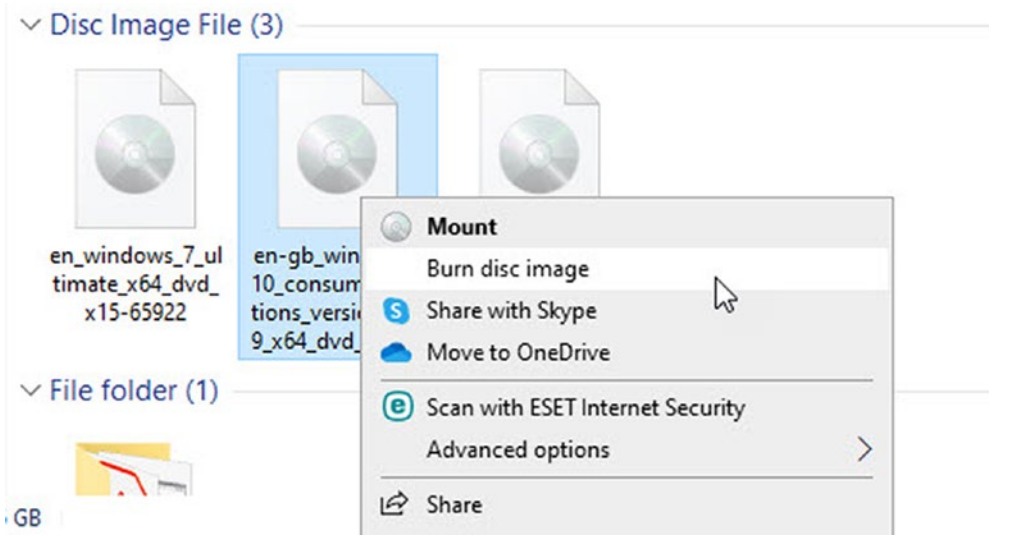


Figure 2-15. *You can burn an ISO disk image to a DVD by right-clicking it*

Backing Up Your Files with File History

Creating a robust system isn't just about creating a backup image of Windows 10. Your PC would be pretty useless if all your files were lost, so having a reliable file backup routine is essential. Fortunately, Windows 10 comes with a file backup and versioning tool that will be instantly familiar to anyone who's used Time Machine on a Mac. It's possible, as with a few other features in Windows 10, however that File History could be deprecated and removed from the OS over time, as the company pushes more and more people to use its OneDrive file backup and sync cloud service, but for now it's sticking around.

File History can be found in the Control Panel but is perhaps more easily controlled from the Settings app. Open *Update & Security* and then *Backup,* and you'll be prompted to *add a [backup] drive* (see Figure 2-16), which can also include local network locations.

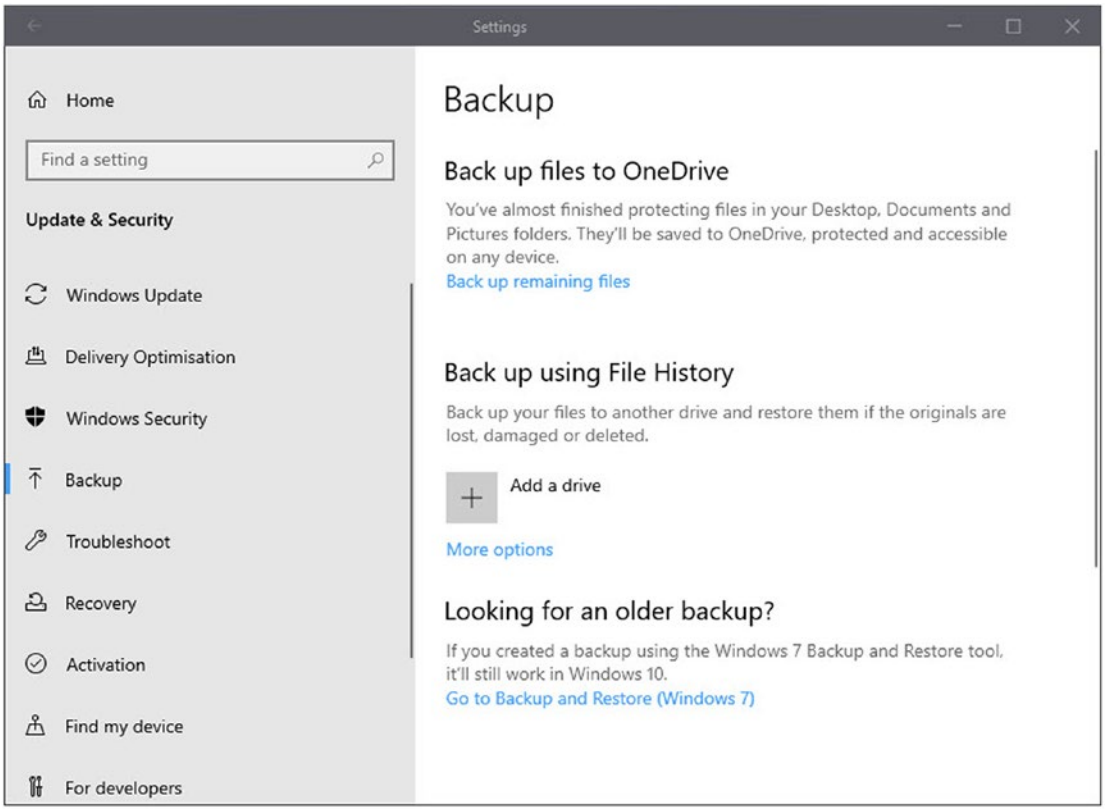


Figure 2-16. *File History is easily controlled from the Settings app*

You can use spare hard disks and partitions in your PC, USB-connected hard disks, or network drives to store your File History backup. Setting it up is a simple matter of selecting a drive on which a **FileHistory** folder will be created. By default, File History will include all your Shell User Folder locations (Documents, Music, Pictures, Video) your OneDrive folder (if you're using it) and anything else in your `C:\Users` folder.

Tip A new version of a file is kept each time a change is made to that file. This includes the file being opened, when its *last accessed* date will be changed. If you have files you open on a regular basis that do not change, such as music or videos, you can prevent your File History drive from filling up with multiple copies of these files by excluding their containing folders from the backup. You should always make sure you *do* keep a backup copy of the files somewhere else, however.

You can manage the settings for File History, though, once it is set up by clicking the *More options* link that will appear in the Backup Settings. This will allow you to control the frequency with which backups are made, how long old versions of files are kept for (this does not include files for which there is only one version), and which folders and included and excluded from the backup; see Figure 2-17.

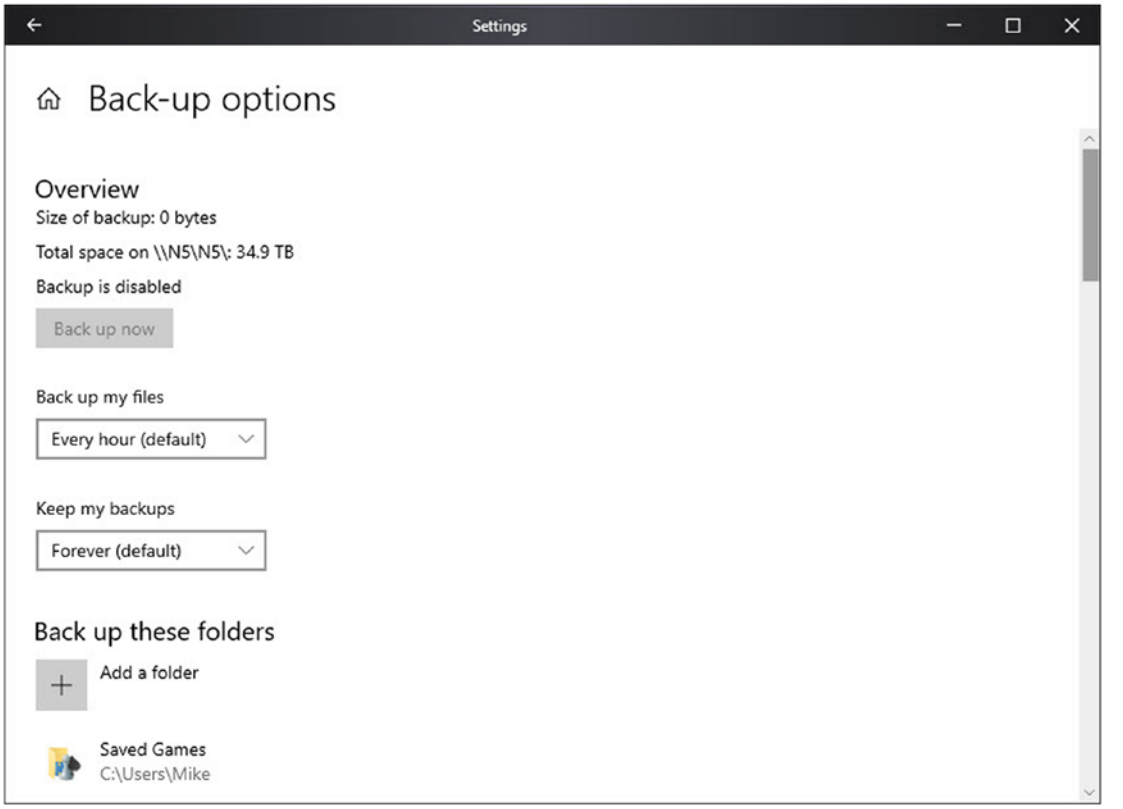


Figure 2-17. *File History can be managed in the Settings app*

Almost everything you need to do with File History can be done through the Settings app, but the Control Panel offers a couple of additional features; see Figure 2-18.

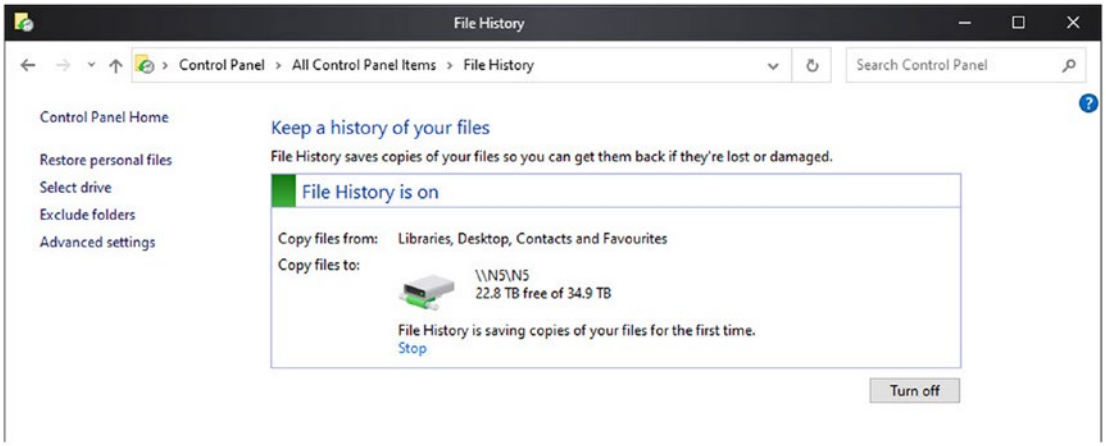


Figure 2-18. *File History in the Control Panel has a few extra options*

Perhaps the most useful of these is seeing how much free space is left on your File History drive. If you find the drive is filling up, you can click the *Advanced options* link on the left of the window and then the *Clean up versions* link. Here you can choose to delete all versions of files older than a specific age or, if you're comfortable that you don't need to restore anything, all but the latest one.

Restoring Deleted and Previous Versions of Files

You can restore deleted and older versions of files in File History by clicking the *Restore personal files* link either in the File History, in Control Panel applet, or in any File Explorer window by clicking the *History* button in the ribbon; see Figure 2-19.

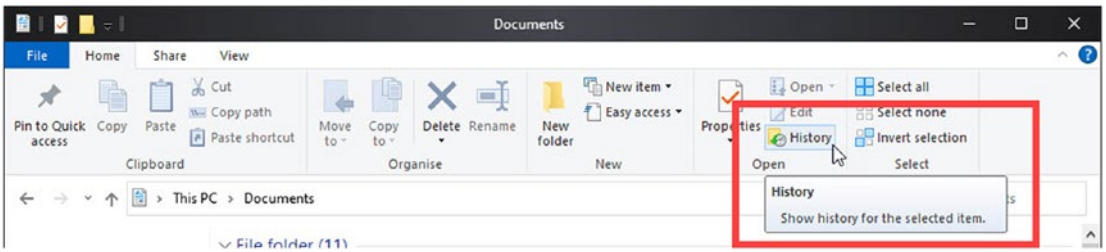


Figure 2-19. *You can restore files directly from File Explorer*

This will open File History at the current drive and folder point, though you can still navigate anywhere within your backup from there. The File History restore window has navigation (back, forward, and up) buttons in its top left and an address bar showing the current folder; see Figure 2-20.

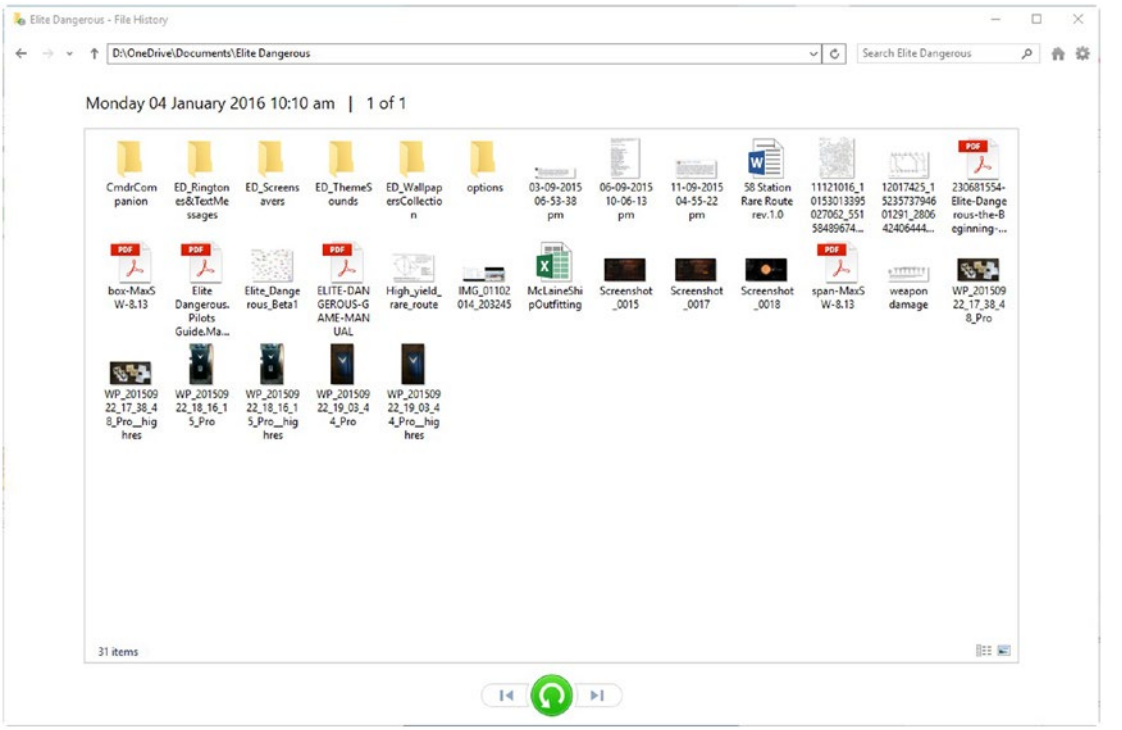


Figure 2-20. *The File History restore panel is easy to navigate and use*

At the bottom of the window are back and forward (by date and time) buttons, with a big green Restore button between them. Once you have navigated to the folder you want to restore deleted or modified file(s) from, use the time buttons to find the correct day and time the backup copy was made, select the file(s) or folder(s) you wish to restore, and hit the big green button. It really is that easy.

Tip File History does not encrypt your files' backup, so you might want to ensure that Bitlocker or Bitlocker To Go is activated on your File History drive. I will show you how to set these up in Chapter 18.

File History is excellent at picking up where it left off after a Windows reset or reinstall, though you will need to activate the feature again. If you really want to dig into the store location for File History, however, all the files are stored in plain, easily accessible format, just as any other file on a hard disk would be. The only difference is that the date and time the backup was made are appended to the end of the file name.

Setting Up and Managing OneDrive

Microsoft's cloud backup and file sync service, OneDrive, comes baked into Windows 10, and while File History might be a great way to keep backup copies of all your files, it won't help if your home or office catches fire (I know, I'm a cheery person really). Now I'm going to add a caveat to this section, as Microsoft *regularly* make changes to the OneDrive client in Windows 10 and, knowing my luck, some of those changes will appear right at the moment this book goes to print.

I do know what some of the changes are, however, so I'll give you a heads-up, as they might change what you're seeing when you read this. The first is that the OneDrive client, which is a little cloud icon that sits in the system tray to the right of the desktop Taskbar, will support both OneDrive and OneDrive for Business accounts (the latter coming with an Office 365 business or enterprise subscription).

The second is that we will be getting the placeholders feature back. This feature, so popular in Windows 8.1, allowed File Explorer to display all of the files you had, whether stored locally on the PC or in OneDrive in the cloud, and you could make files and folders available offline or online only, by right-clicking them. Once this is implemented, we can expect to see "Store [all] files offline" and "Store [all] files online" appear as right-click options on files, folders, and the OneDrive icon in File Explorer.

Fundamentally, however, the setup process for OneDrive shouldn't change very much (he says, hopefully).

To set up OneDrive on your Windows 10 PC, click the cloud icon in the Taskbar system tray, which should appear gray at that point (white when everything is working well), and you will be asked to confirm the location for your OneDrive files store on the PC; see Figure 2-21.

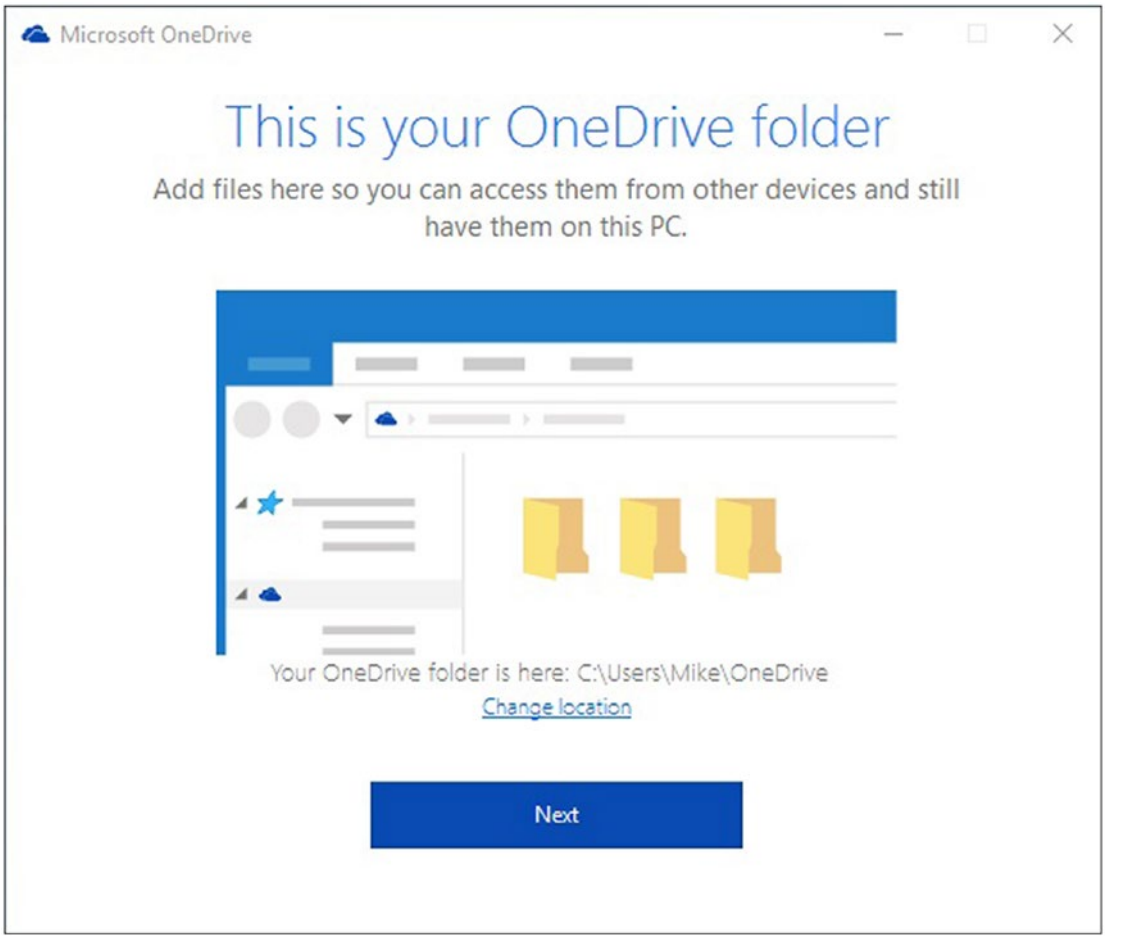


Figure 2-21. *You can change the default OneDrive storage location*

Now, I talked earlier about how you might want to store files on the PC, and this can vary depending on what type of PC you have. If you don't have many files stored in OneDrive (you can purchase more space at any time by visiting `onedrive.live.com/options/ManageStorage` or by purchasing a Microsoft 365 Personal or Home subscription), or if you are using a PC with limited amounts of storage, such as a tablet or ultrabook, you may not want to store all your files on the PC or have that many to store. In this case, choosing the default storage location `C:\User\[YourName]\OneDrive` will probably be fine.

If you have a large amount of files stored in OneDrive, however, and want them all stored locally on the PC as well, click the *Change location* link and select where you want the files stored. Remember that if you have or will create a System Image Backup of

Windows using whatever your personal choice of imagine software, as I detailed earlier in this chapter, you should always store your files on a different hard disk or partition to the one on which Windows 10 is installed. I will show you how to do this in Chapter 3.

Next, you will be shown all the files and folders you have stored in OneDrive and asked to select which ones you want downloaded to the PC; see Figure 2-22. You will be alerted, as is the case here, if you have more files than there is space for on the PC. When you have chosen what files and folders you want stored locally on the PC, click Next.

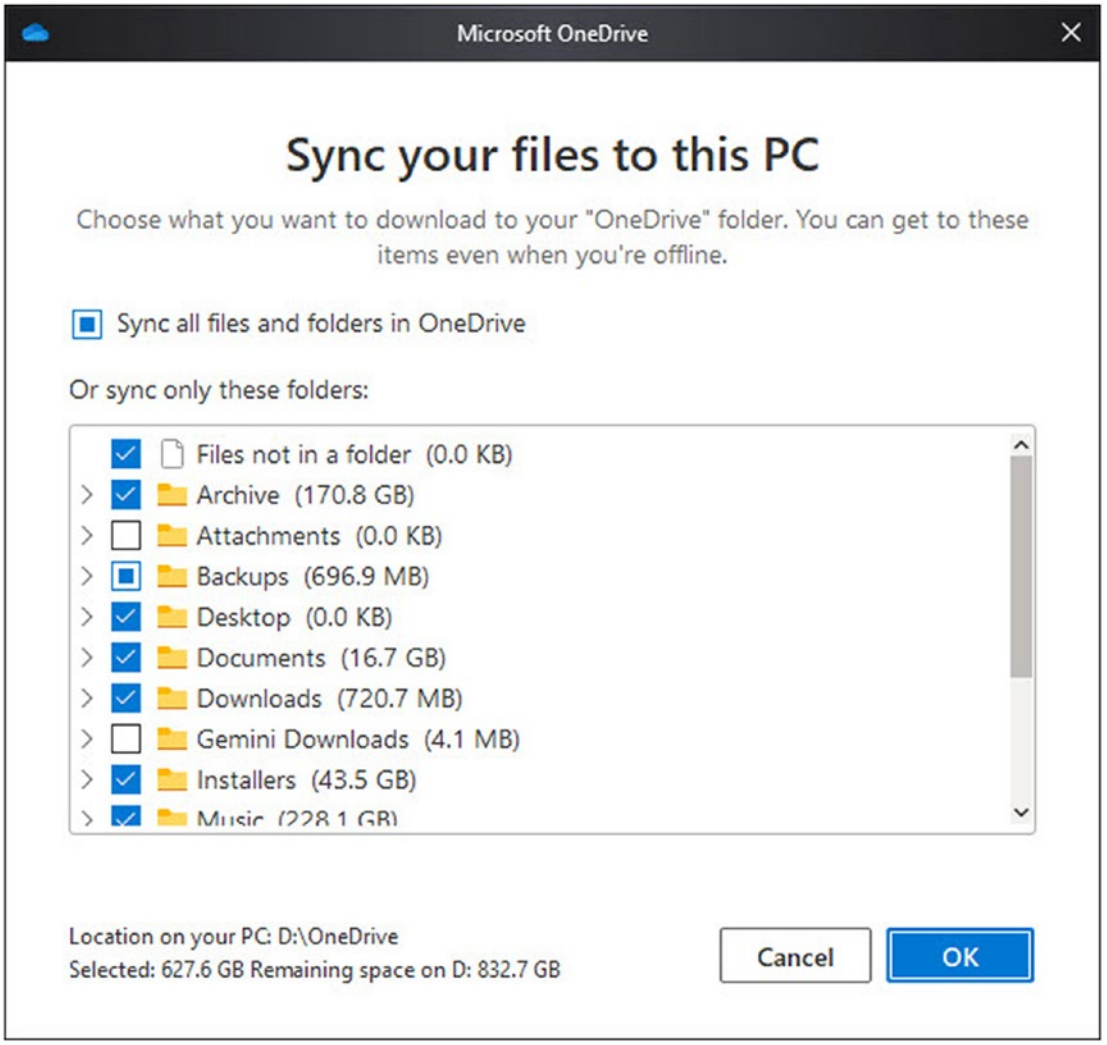


Figure 2-22. *You can choose which folders are synced with OneDrive*

Should you wish to later change which files and folders are stored on the PC, you can click the OneDrive icon in the system tray and select *Help & Settings* and then *Settings* from the panel that appears.

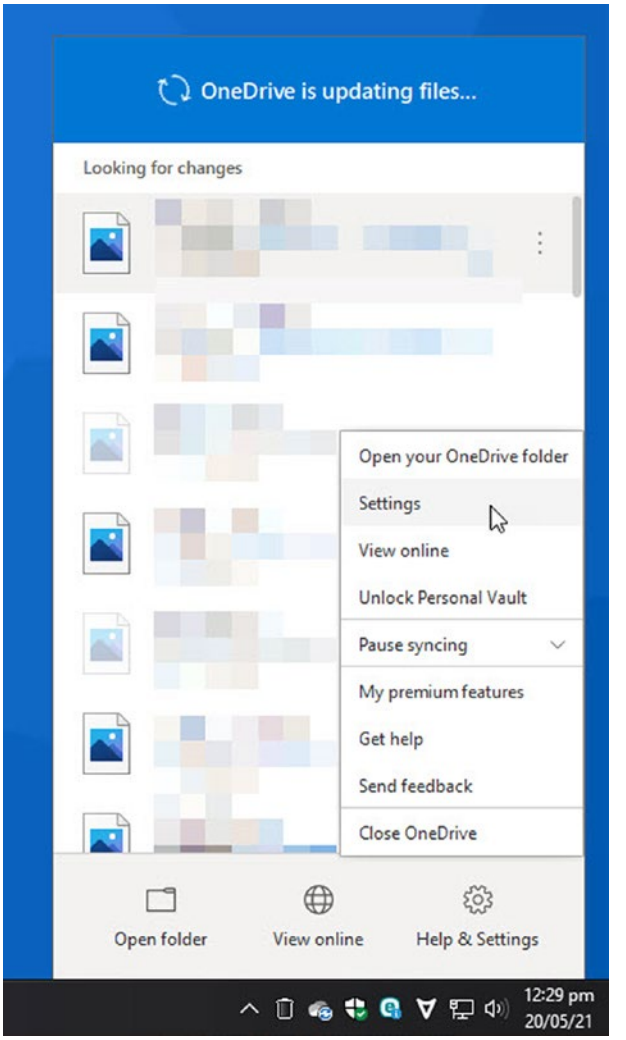


Figure 2-23. *You can change which files and folders are synced locally at any time*

Summary

Back up, back up, back up! Genuinely, the most important part of your PC is its files and apps. Apps can probably be easily replaced, but your files can't. It's crucial therefore to have a robust and, above all, regular backup process in place. Both File History and OneDrive allow you to do this, but other cloud services such as Dropbox, Google Drive, and Amazon S3 are also excellent, and you should shop around to find the best solution to suit your own needs, as some also support offline (local) backups.

Remember that we're now living in an age where ransomware is prevalent. Chapter 19 will provide you with detailed information about how you can remove malware and ransomware from your PC, but I genuinely hope you never need that information. Especially in an organization, small or large, an effective multitiered backup strategy is absolutely essential.

With the advice in this chapter followed, you will have created a robust system (and a Recovery Drive, yeah?) so that no matter what happens, or what goes wrong (short of your only PC blowing up), you'll be able to quickly get back up and running with your files, your apps, and your copy of Windows 10.

In the next chapter, we'll take this all a step further and look at how Windows 10 can be configured in ways that ensure stability, dependability, and durability. This includes the crucial (I think anyway) ability to move your files and data away from your Windows 10 installation.

CHAPTER 3

Configuring Windows 10

While creating a robust backup system, and one that permits the quick and (relatively) straightforward restoration of a fully working copy of Windows 10, is both laudable and necessary (just a reminder that you *did* create that USB Recovery Drive?!), what's likely more important is setting up a PC, Windows 10, and your apps in such a way that they don't break in the first place.

Windows 7 was the first operating system from Microsoft I felt really didn't need to be tinkered with or modified in any way to make it operate well. That's still the case with Windows 10, but knowing what's available, and where to find it, can make creating a robust and resilient system much more straightforward.

Settings

The Settings panel was first introduced in Windows 8 as PC settings. The aim at the time was to create a simplified Control Panel containing the settings and options that nontechnical PC users would most likely need, much more akin to the type of controls found in Google's Android and Apple's iOS operating systems, and indeed Apple's MacOS X at the time as well. In Windows 10 we've seen Settings expanded significantly, though it's still in an early "version 2" form. Over the lifetime of Windows 10, we'll see the full Control Panel and, very likely, the Administrative Tools folded into the Settings interface style.

This means that during the lifetime of this book, some Control Panel elements will move into the Settings panel (so if I detail a Control Panel applet that you can't find, that'll be why). As an example, when Windows 10 first launched, there were nine different settings categories. Currently as I write this, the number has grown to 13.

You'll probably be familiar with Settings to some extent already; for instance, you probably know that it's opened from the Start Menu, by clicking the *Settings* icon (it looks like a cog or gear depending on whether you're outside or inside the United States, and what terminology you use); you will find the Settings icon directly above the Power and Sleep icon.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_3

The Settings panel is divided into different categories (see Figure 3-1), and anybody who's used an Apple Mac over the years will immediately feel at home with it.

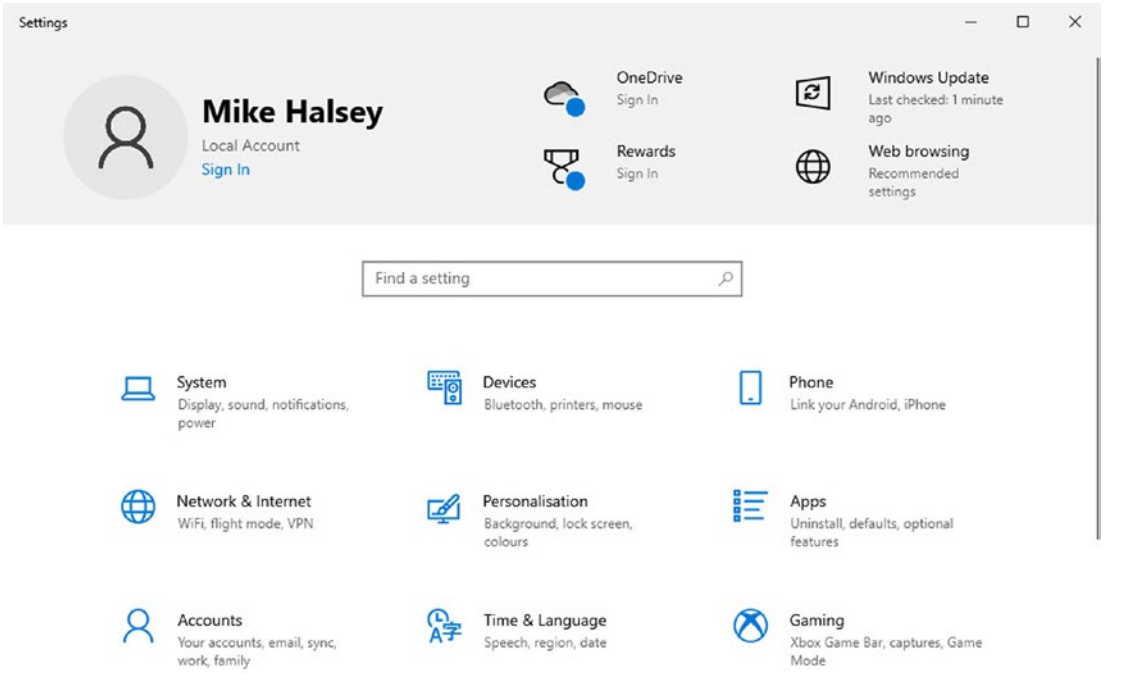


Figure 3-1. *The Settings panel consists of nine main settings areas*

The aim with what I will refer to as this version 2 Settings panel (the version 1 being that which we saw in Windows 8) is to make it as simple and as straightforward to use for everyday PC users as possible. Thus, the available controls are basic. A good example of this is managing printers. The Settings panel will allow you to add and remove printers on your PC, but you need to delve into the *Devices and Printers* panel to access print and management options.

There are also, as you might expect, a great many items which are missing. Some of these are even surprising omissions such as being able to create a USB Recovery Drive for the PC (which you… oh, never mind!) and managing which drives and partitions are protected by System Restore and file versioning. These will inevitably be folded into the Settings panel over time.

If you're troubleshooting a PC, there's really not much here currently to work with except for managing Wi-Fi networks, and I'll talk about how you do this in Chapter 9. For setting up and configuring a PC, however, there's more, and I'll detail the most important that are relevant to creating a reliable and resilient PC.

System ➤ Storage

This is where you can select what drive, partition, or external storage medium (such as a Micro SD card) your new documents, music, photos, and video are stored (using the *Change where new content is saved* option). Crucially, however, it's where you can specify the storage location for Store apps. Changing the storage location here doesn't change the default install location for win32 apps, for which the install location is usually customizable during their installation; it only manages apps that come from the Windows Store or the Windows Store for Business; see Figure 3-2.

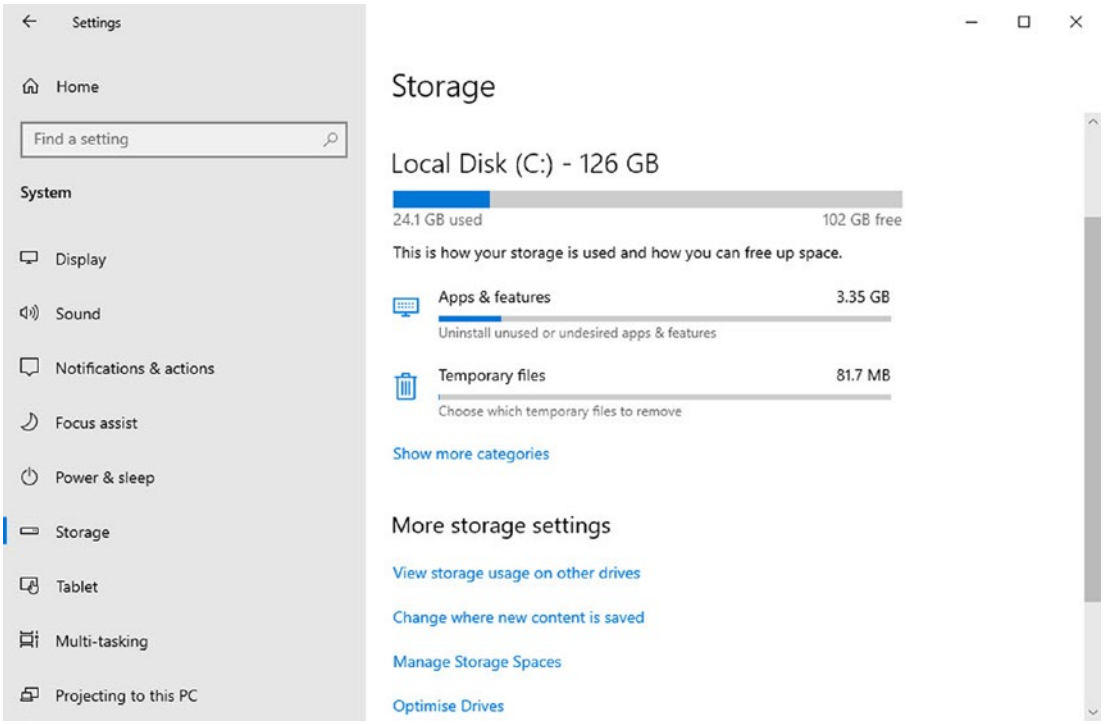


Figure 3-2. *You can manage the Store App install location*

This setting is most useful for people who use tablets (both consumer and pro) in which storage can be at a premium. Some small tablets come with only 16GB of storage, though this can still make them perfectly useful for some tasks in the workplace, and they're certainly useful for people lounging on the couch at home. Even Microsoft's Surface Pro convertible tablets come with a Micro SD card slot for the purposes of storage expansion.

Here comes probably the first top troubleshooting tip to look for, and it's if a user is telling you that they picked up their tablet first thing in the morning to find that, suddenly, none of their apps will work. While it might be tempting to assume they'll need to restart the machine, or it could be a Registry or configuration problem, it's much more likely their teenager slipped the Micro SD card out of their device so they could use it to store more music on their own smartphone.

Apps ➤ Default Apps

The Default apps settings, by which I mean which app is started on your PC when you open a specific file type or web link, is one of the few settings that currently reside in both the Settings panel *and* the Control Panel (which doesn't offer much more functionality, to be honest). Top tip number two is that if you get a call from a user saying they suddenly can't open their Word documents anymore, it's likely because a setting here has been changed, either accidentally by the user or by another app that's trying to steal the file type for itself.

You can actually do quite a bit to manage your default apps in Settings; see Figure 3-3. The default view will show you which apps are set for the most commonly performed tasks on a PC (email, web browsing, picture and photo viewing, music, and video), and you can click one to change the default app.

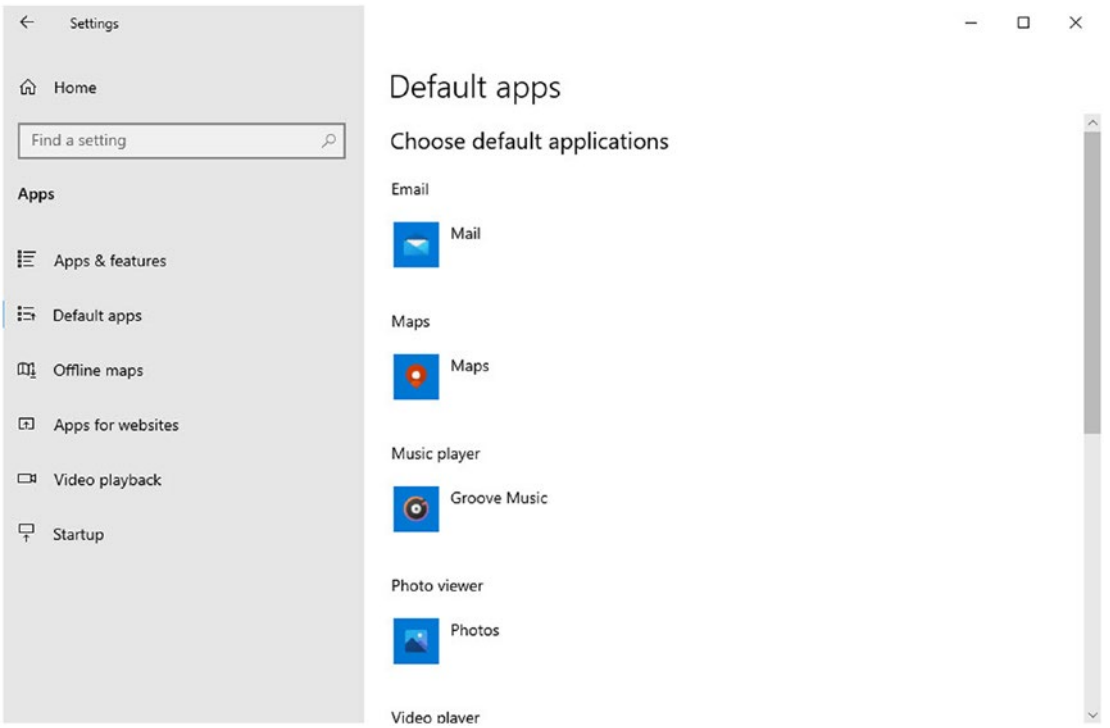


Figure 3-3. *You can manage your default apps in Settings*

Further down the *Default apps* page are several useful quick links:

- *Choose default applications by file type* is useful if your PCs use a custom app that has its own file type. Occasionally, such as after a system configuration change, these file associations can become scrambled. Selecting this option will present a list of all the file types known by Windows 10 on your PC, and you can select the default app for each one.
- *Choose default applications by protocol* is more useful if you have a specific Internet or network link type that is opening with the incorrect app. As an example of this, you might have a convertible laptop with both the Office 365 desktop and Store apps installed, but clicking a link to a PowerPoint file in SharePoint is opening the files in the Store app when the user really wants the win32 app instead.

- *Set defaults by app* is where you will be presented with a list of all your installed store apps. You can select one to choose which file associations it has. This is most useful if you want, for example, a music, video, or photos app to open some but not all of the file types associated with it, as you use another app for a specific file type.

System ➤ About

This is where you can point users if you need them to give you information about their PC and their installed copy of Windows 10; see Figure 3-4. You might, for example, want to know what version of Windows 10 they have installed (to maintain app compatibility), what type of OS they have installed (32-bit or 64-bit), or which version of Windows 10 (Home, Pro, Enterprise, etc.) is installed.

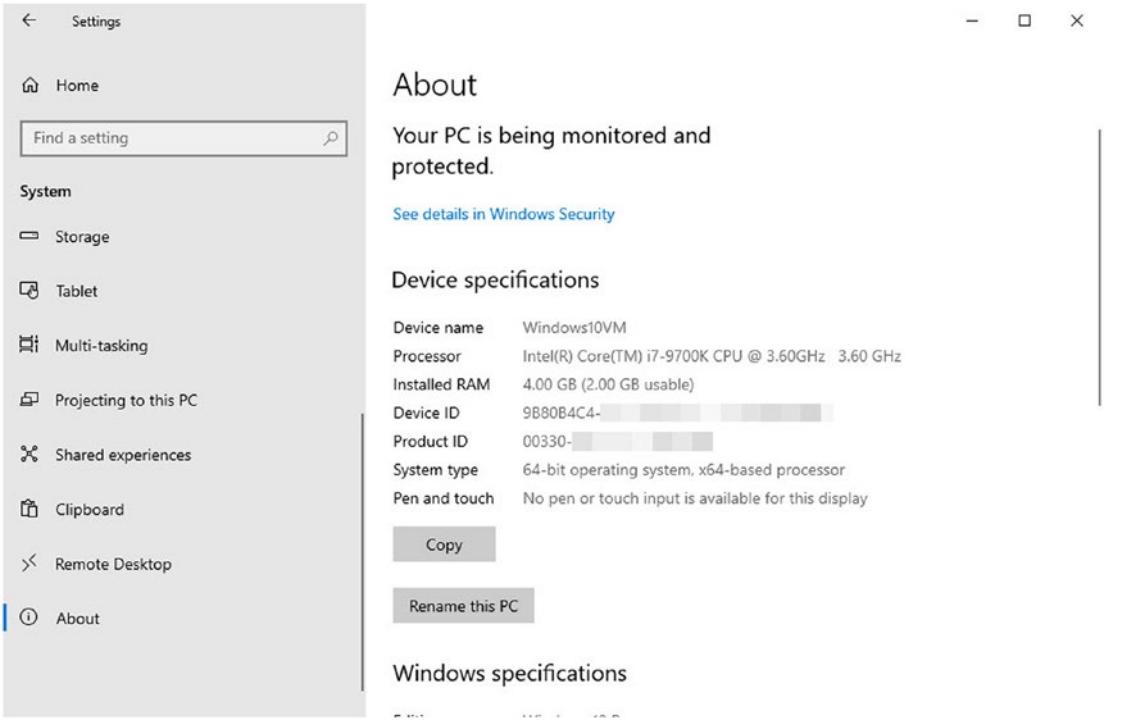


Figure 3-4. *You can get information about the PC and Windows 10 from Settings*

Devices ➤ Printers and Scanners/Bluetooth and Other Devices

I'm going to lump these options together, as both have permission options to download drivers and updates for devices over metered (cellular) connections. If you discover that a user is being billed for too much cellular data, you might want to check the settings here to see if these have been accidentally enabled.

Devices ➤ AutoPlay

AutoPlay governs the behavior of Windows when removable media, such as a USB Flash Drive, optical disk, digital camera, or smartphone, are plugged into the PC. A user might know how (and find it helpful) to have the PC perform a specific action, such as opening an app or File Explorer, and might suddenly find that nothing is happening any more.

It's also useful, however, because File History, which I detailed in Chapter 2, can use USB Hard Disks for backup, and if the incorrect setting is selected here (you will find it in the removable drive drop-down menu), no backups will be made. When you want users to always have an up-to-date backup of their files, this is definitely one to keep an eye on.

Phone

While we're on the subject of devices, you can link your Android or iPhone to your Windows 10 PC. This needs to be done on a per-PC basis but can be useful, and more functionality is being added on a regular basis. This functionality ties into the *Your Phone* app which is preinstalled in newer builds of Windows 10. It allows you to read and send SMS messages, and drag and drop photos from your phone and PC directly from the Windows 10 desktop.

There is additional functionality that is either currently available for some phones and yet to be rolled out universally or earmarked as coming at a later stage. These include being able to receive and make phone calls from your PC using the speakers (headphones) and microphone you have connected, which is great for hand-free calling when you're working, but also being able to view and use phone apps in Windows on your PC's desktop.

Network and Internet

The *Network and Internet* settings really only allow the setting up and removal of connections (Wi-Fi, Ethernet, Virtual Private Network [VPN], dial-up and proxy servers), and you'll still want the full Network and Sharing Center for managing and troubleshooting problems, which I'll talk about in Chapter 9.

This is, though, a useful place for a user to get information about whether network types are set up correctly. If you are remotely supporting a user who can't get access to the work network, you are unlikely to be able to provide Remote Desktop support (we'll cover this in depth in Chapter 12). It could be, however, that the settings for their VPN or proxy server have been deleted (you might be surprised what users feel they don't need on their PCs).

Personalization

As you might expect, personalization is where you can find all manner of customization options for the PC desktop, from changing the wallpaper and color scheme to adding a theme (which amazingly are still in Windows having first been introduced in Windows 95 and subsequently forgotten by just about everybody), adding and checking what fonts you have installed, and customizing the Start Menu and Taskbar.

This last option is perhaps the most useful as you can choose which icons appear permanently on the Taskbar, rather than being automatically hidden in the System Tray, and you can turn system icons (such as the Action Center and Clock) on or off.

Apps

I mentioned the Apps panel a few pages back, but there are some additional options here that can be useful, such as managing the ability to use offline maps (with the Windows 10 default maps app only), but you can also manage your Windows 10 startup apps from this panel.

Accounts

Similarly to the Network and Internet settings, the Accounts settings contain things that a user might feel they want to change or tweak, and in doing so they might accidentally delete or corrupt a setting. Changing their account picture is one thing, but users don't like typing long and complicated passwords into their PCs. If you've not locked down

password management in Group Policy, then you might find a user creating a very basic PIN or picture password on a laptop that contains sensitive company or customer data.

The settings for Azure Active Directory (Azure AD) and Mobile Device Management (MDM) are also found here however. These are essential for company network access to Microsoft 365, and for a company to be able to remotely support (and check the integrity and security of) a PC or Bring Your Own Device (BYOD) machine.

Lastly, the *Sync your settings* options might be seen by some as an annoyance that ties their PC to Microsoft's OneDrive service, but if you have a PC user with specific accessibility needs, making sure that Settings Sync is active can make the difference between a usable and a completely unusable PC.

Time and Language

If you support people who travel with their laptop or tablet around the world, then they'll need to know how to correctly set the time and region settings. At its simplest these settings allow a user to change their current time zone and country (Windows 10 is pretty good at managing everything else).

Occasionally, however, a user might find that a specific app or online service won't work or reports an error. If the user has recently been traveling, these are good settings to check, not just because some online services are location-specific (i.e., only available in certain countries) but because if the clock as set on the PC doesn't match what an app or service expects to see, errors and sign-in failures can sometimes occur.

Gaming

You might be unsurprised to hear that this is the panel containing all the controls you need to manage Xbox integration with your PC; however, it is also where you can manage the Xbox Game Bar, which can occasionally prove useful when troubleshooting a PC. I'll talk more about it in Chapter 12.

Ease of Access

This is where I can get in a little plug for another of my *Apress* books. While there's nothing here that will be useful when troubleshooting a PC, the Ease of Access settings can be used to make a PC easier to use from everybody with color-blindness, to shaky hands, and people who work in noisy environments.

There are an absolute ton of ways that the Ease of Access settings can be useful in day-to-day life for just about everybody. So I strongly encourage you to check out my "**Windows 10 Accessibility Handbook**" [Apress, 2015].

Search

Search is a slightly different beast to what it used to be in Windows. Gone are the days of Windows XP, which had an absolutely stellar search facility, and Windows 7 which included some brilliant advanced query syntax (AQS) which for some unfathomable reason was later removed in Windows 10; search these days is a three-tiered system, searching your local hard disk(s) and network storage, the Internet, and also any business or organization storage you have configured through Microsoft 365 or Azure.

This works both from the search box on the Taskbar and from typing in the Start Menu, but also in the Microsoft Edge web browser, in which a *Bing* search can optionally return results from your business documents and SharePoint pages, alongside Internet results. Oh and Cortana is now gone, being relegated to an optional app, as the service is being refocused by Microsoft as a smart AI to assist with Microsoft 365 and Teams.

Privacy

Privacy is the watchword of the 21st century, and while there's (almost) nothing here that can be useful with troubleshooting, it's well worth spending some time both checking through the options that are available and also locking them down in Group Policy. Let's say, as an example, that you have very strict policies in your organization about the security of the data you hold, but that some employees don't see what the fuss is about. In the Privacy settings, it's possible, without a policy in place, for those users to choose to share data about their PC and usage with Microsoft that might contravene your official policy.

Additionally I mentioned there was almost nothing here that's useful for troubleshooting. There is one setting, *Activity History*, which can store details of the most recent files and documents the user was working on. If somebody complains that all of a sudden the list of their most recently accessed files has disappeared, it could be that they've disabled this option on their PC.

Update and Security ➤ Windows Update

Windows Updates cannot be disabled or ignored in Windows 10, at all! Microsoft enforces a strict policy that all security and stability updates will be pushed to all Windows 10 PCs, and not even businesses with thousands of devices will be immune. However, there are some caveats with this.

If you use Windows 10 Enterprise, feature updates (not essential security and stability ones, mind) can be deferred (paused) for a period of a few months; see Figure 3-5. In Enterprise (and this is managed through a server), these updates, which include new and updates features in the OS, can be deferred for a period of 2–3 years, though this was originally 10 years and Microsoft have moved the goalposts several times already. Windows 10 Home and Pro allow the pausing of updates, but for a shorter period, normally being 35 days.

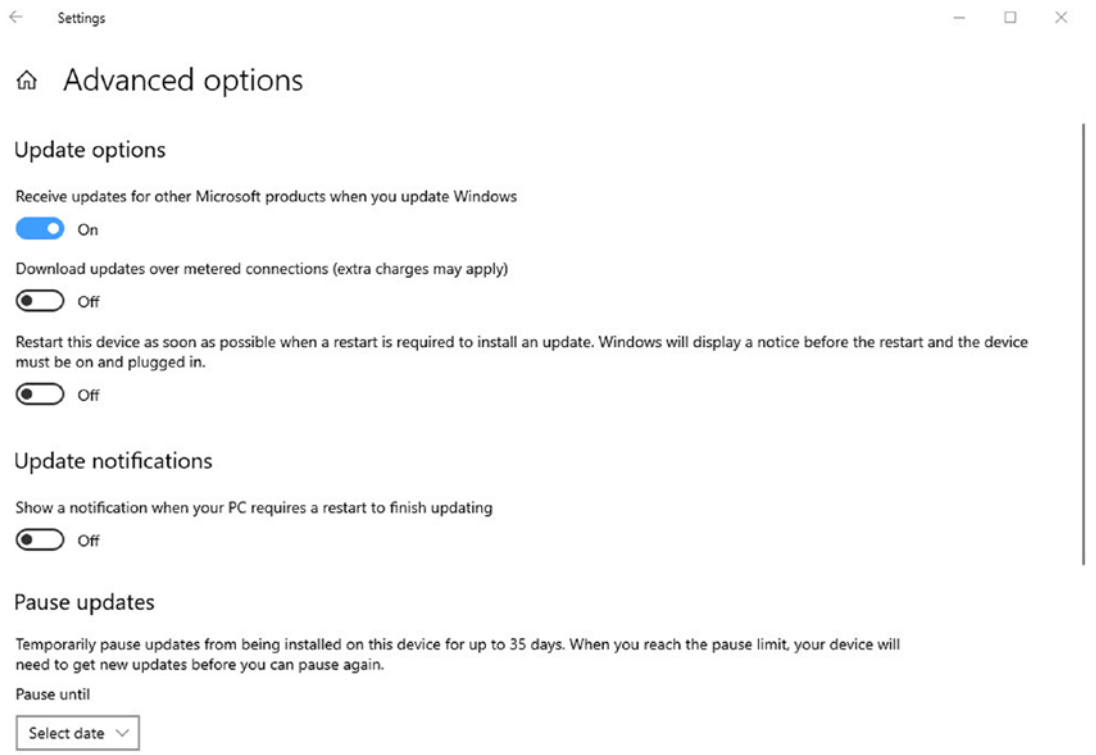


Figure 3-5. *Windows 10 Pro and Enterprise editions permit deferral of upgrade installs*

These deferment options Microsoft have for different Windows 10 editions are called *channels* and include the "Semi-Annual Channel (SAC)" which is for any PC running Windows 10 Home, Pro, or Enterprise and that will install feature updates twice annually as the name suggests. The "Long-Term Servicing Channel (LTSC)" is designed for mission-critical hardware that is not used with everyday software such as Office. This hardware can include point-of-sale terminals, ATMs, medical and engineering equipment, and more.

LTSC is only available with Windows 10 Enterprise LTSB, a special version available direct from Microsoft or through their business partner resellers. PCs will still receive stability and security updates, but all feature updates will be skipped.

Note It's worth noting that with the availability of Windows 11, at the time of writing, it is unclear for how long Windows 10 Enterprise LTSC will be supported. Microsoft have given an end of life date for Windows 10 as being 2025, though they are known for often extending these deadlines, and have not as of yet stated if the LTSC channel builds will be included with this.

If there's one thing that users like fiddling with, it's Windows Update. Either they'll hate updates coming down the pipe and try to turn them off or they'll be bored for a few minutes and think they should check if their PC needs any. Users who are able to check or uncheck the *Pause updates* option could find themselves, potentially at any rate, creating security or stability problems that they'll then blame on anything other than their own actions.

If you have users who sign into their PCs using a Microsoft account, such as people who occasionally use their own PC, or who work from home, you might find them signing up to the Windows 10 Insider preview program. This will download alpha and beta builds of future Windows 10 versions, and these are very commonly known to be unstable and break apps and services.

Update and Security ➤ Delivery Optimization

Despite the strict controls of not being able to opt out of stability and security updates, Windows Update is controllable, especially when it comes to the bandwidth used which can sometimes for a big update bring an office Internet connection to a shuddering halt. Delivery Optimization allows you to decide how and how fast updates download, and where from.

One of the biggest advantages is the option to get Windows Updates from other PCs on your network. This can be especially useful in large workplaces, and it allows just a small number of computers to download the updates which they then share across the network with other PCs they are visible to; see Figure 3-6.

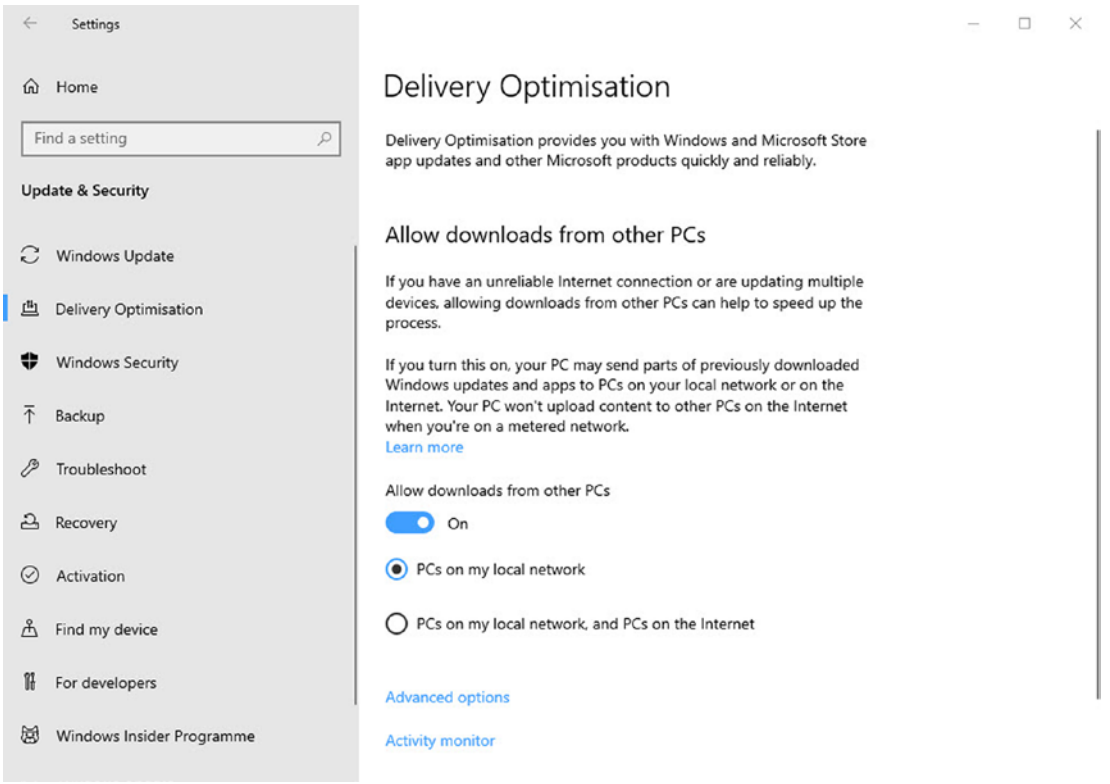


Figure 3-6. *Windows Updates can be shared between PCs on a network*

If you find yourself in a workplace with a limited amount of bandwidth, or if you have bandwidth-intensive work to do, you can click *Advanced options* to choose, in both relative and absolute terms, how much bandwidth can be used by Windows Update, both for downloading them from the Internet and also for sharing them across your network. I will go into much more detail about Windows Update in Chapter 16.

Update and Security ➤ Windows Security

I will detail the Windows Security Center in full in Chapter 18, but the Windows Security panel in Settings is a good place for a general overview of what's going on. This includes traffic-light iconography to tell you quickly about the current status of Windows' or your third-party threat-protection and antimalware software.

Update and Security ➤ Backup

Microsoft's backup "solution" is primarily to push people toward using it's OneDrive service, though that does work well. This is one area of Settings that could change over time as it includes Microsoft's *File History* backup feature. Microsoft have hinted that File History is being deprecated and might be removed from Windows 10 at a later date. We previously looked at backup in Windows 10 in Chapter 2.

Update and Security ➤ Troubleshoot

Now this one is important, but perhaps not for the reason you are hoping. Windows 10 does include a number of automatic troubleshooters. Ordinarily these will kick in on their own when, for example, an application fails to install or a network connection drops. Sadly Microsoft have also hinted these will be deprecated in a future version of Windows 10.

For as long as they remain however, which could be permanently, clicking the *Additional troubleshooters* link will present the list of available troubleshooters, and you can click one to run it. These troubleshooters are fairly basis, and will reset components to their default state to try and fix problems; however, if settings have changed, this can prove surprisingly effective.

Update and Recovery ➤ Recovery

We looked at the Recovery options in Chapter 2, but in this Settings panel are options to either Reset the PC or, on a UEFI system where the PC starts too quickly to get into the BIOS firmware settings, boot into the UEFI firmware directly.

Update and Security ➤ Activation

Like the *Settings* ➤ *About* panel, Activation can provide valuable information about whether the currently installed version of Windows 10 is activated and, therefore, fully operational. It might be that after a reinstallation, Windows 10 does not activate properly. Here you can check the activation status, manually activate Windows 10 on that PC, or if necessary change the product key to the correct one, which might be useful if Windows 10 goes into extended support as happened with Windows 7.

Update and Security ➤ For Developers

For advanced users that need more control over their PCs, the *Developer options* allow features such as the sideloading of apps, which can be useful when developing new applications, to change some of the functionality in File Explorer, and to change advanced settings and options for Remote Desktop connections to the PC. These last settings might be more useful for system administrators, as they include Remote Desktop connection, sleep, and hibernate overrides.

Introducing the Control Panel

Throughout this book, we'll be spending a great deal of time looking at the Control Panel. Unlike the Settings panel, however, where I wanted to detail all the things "helpful" users might want to change on their own, the Control Panel is slightly more impenetrable for novice PC users.

The Control Panel is opened by searching for it in the Start Menu. In its top right is a drop-down *View by:* menu which permits the displaying of a Category view (similar in some ways to the Settings panel), large icons, or small icons; see Figure 3-7. It's been on a crash diet since Windows 8.1 and will be slimmed much further in the years to come, but it remains the place to go for serious PC settings.

As an example, when I wrote the first edition of this book, there were 43 category options in Control Panel; for this second edition, that is now down to 37 as more features and controls are moved into *Settings*. We can possibly expect more Control Panel items to be moved in the coming years, though the release of Windows 11 might yet mean things stay as they are.

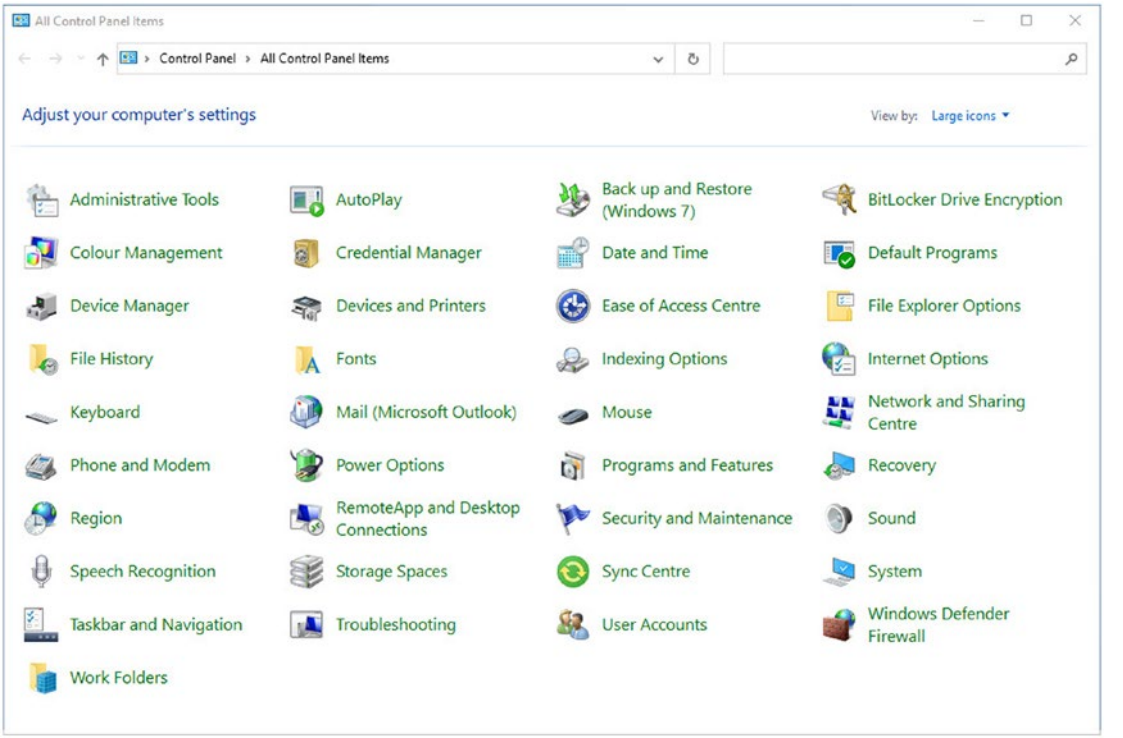


Figure 3-7. *The Control Panel is slimmed from Windows 8.1, but still very useful*

The Control Panel is also home to many subpanels, each of which is significant in its own right. These include the *Devices and Printers* panel, which I'll detail in full in Chapter 7, and the all-important *Administrative Tools*, which contains the advanced management and support utilities for Windows 10 and which I'll cover in depth in various chapters later in this book.

Managing the Virtual Memory, Paging File

While much of the features in Windows 10 can be controlled from the Settings panel, there are a couple of Control Panel applets that you might want to change, the first of which can extend the life of a Solid State Drive (SSD) considerably.

Both of these settings can be found not in the Control Panel because that would be too obvious. Instead search for *Advanced System Settings* in the Start Menu, and click *View Advanced System Settings* when it appears. Navigate to the *Advanced* tab in the window that appears, and in the *Performance* section, click the *Settings* button.

At the next pop-up dialog, click the *Advanced tab* and then the *Change* button for virtual memory. You can now change the virtual memory (paging files) settings to a fixed size, that is, where both the initial and maximum sizes are identical, as in Figure 3-8.

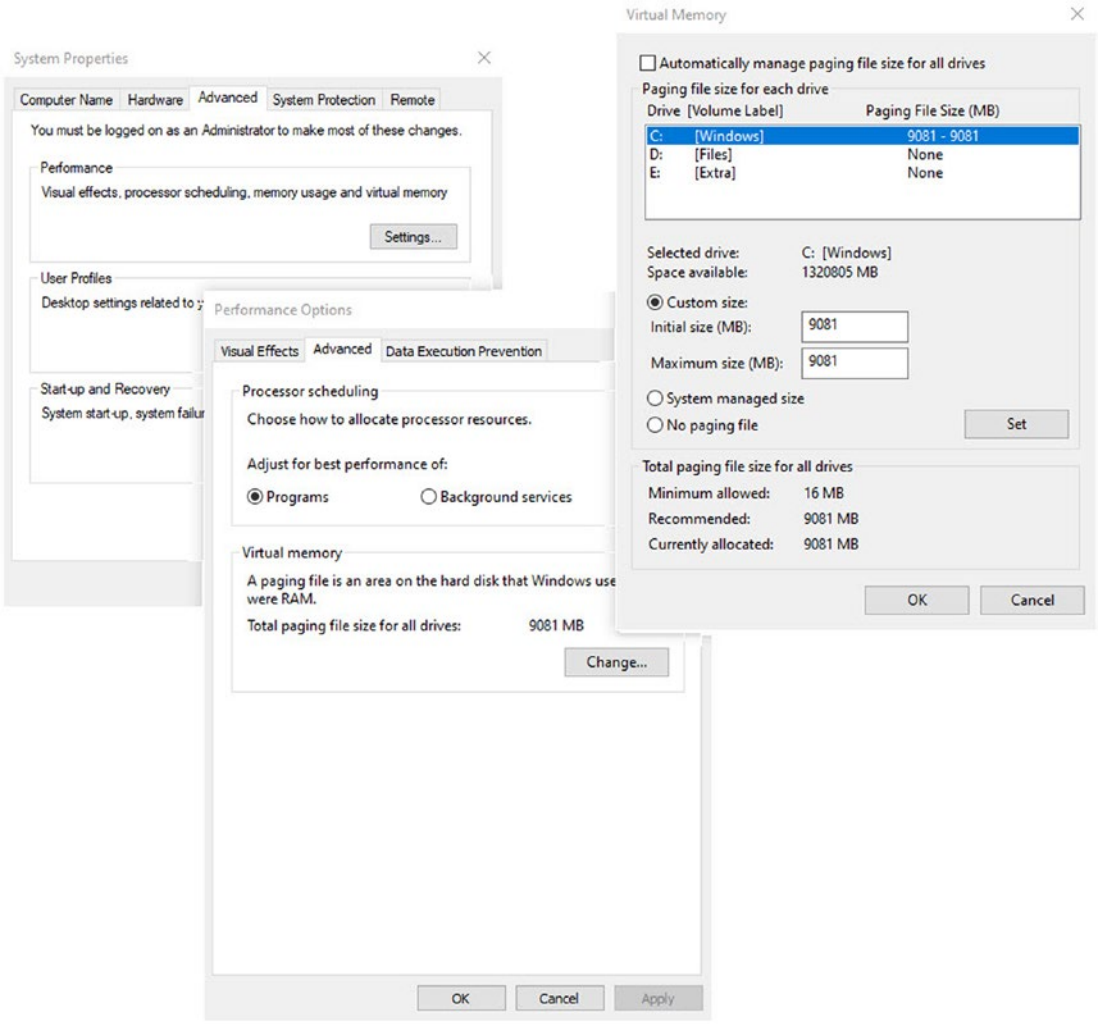


Figure 3-8. *Changing the size of the page file can greatly enhance the life of SSDs*

Windows 10 doesn't really use the paging file as much as previous versions of the OS, as it tends more to keep files in memory than write them to disk. However, the paging file does still exist. This is a temporary store of files that have been swapped out of memory, to speed up the computer and (on older PCs) free up memory space.

By default, the paging file expands and contracts as needed, but all of these file-write operations can slow a disk and even massively shorten the life of an SSD (in fact it can be a good idea to disable the paging file use for SSD systems completely, though this can cause some older software to complain and not work).

Managing Remote Connections to the PC

Additionally, under the *Remote* tab (but also available from the System panel by clicking the *Remote settings* link on the left of the window) are options for allowing or denying remote connections to a PC. If you need to remotely support PCs in the workplace, or are trying to remotely connect to a customer, friend, or family member without success, this is where you should look (or ask them to look, anyway).

You might find that remote connections to the PC aren't permitted, and as such Remote Desktop and using Remote Assistance, both of which I will detail in Chapter 12, won't work. Both of these have their own settings (see Figure 3-9), and you'll need to make sure they are activated if you need them.

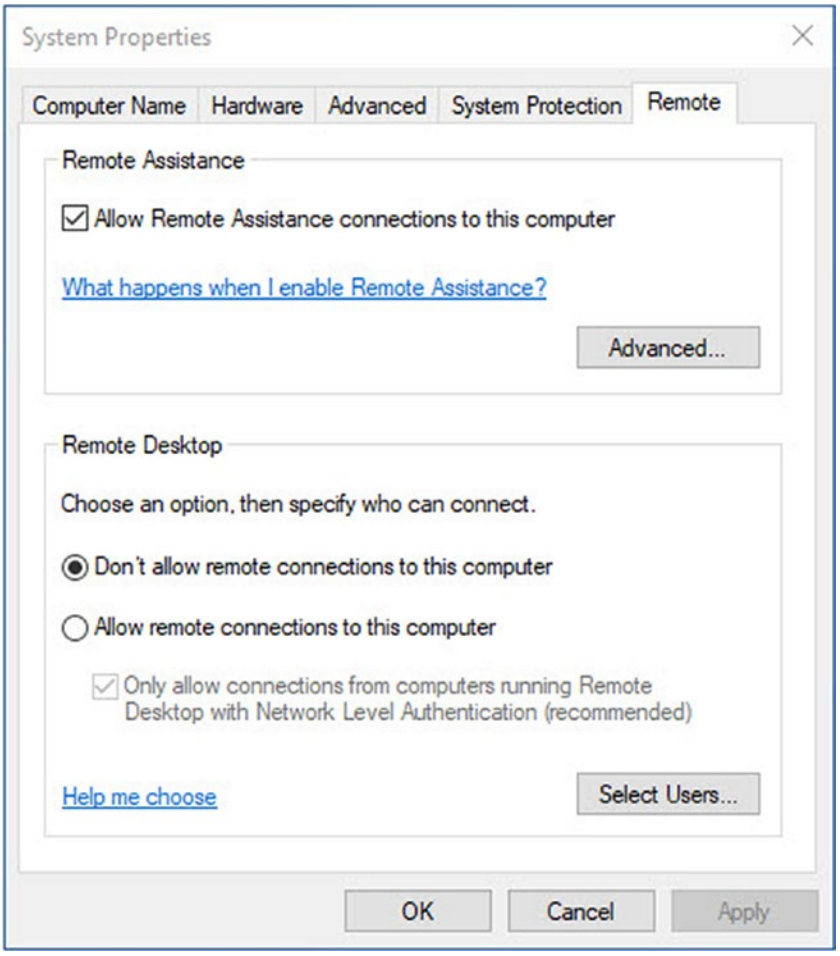


Figure 3-9. *Managing remote connections is essential for PCs requiring remote support*

Moving the Shell User Folders

In Chapter 2, I mentioned that if you create a System Image Backup of Windows 10, regardless of whether you use the utility that comes baked into the OS or a third-party utility from the likes of Symantec of Acronis, it will copy into that backup any files and documents stored in your `C:\Users` folder. Moreover, when you come to restore this backup (which you will at some point), all the new and updated files and folders in the `C:\Users` folder will be completely wiped and replaced with the old ones stored in the backup.

If you store all your files in a roaming server profile on a company domain, or if they're all stored in a Service such as Google Drive or Dropbox, which has to sync all of your files back down from their cloud server on a restore, this won't be too much of an issue. For everybody else, however, and let's face it, all these people too, the prospect of losing all your files and documents is a frightening one.

Fortunately, Windows 10 makes it incredibly easy to move your Shell User Folders (Documents, Downloads, Favorites, Pictures, Music, Searches, Videos) away from your Windows installation. Depending on how your PC is set up, this may be a process that also requires you to create a new data partition on your hard disk (you'll know this is the case if you only have one disk showing in `This PC` in File Explorer), but I'll show you how to do that shortly.

To move your Shell User Folders, open File Explorer and click the small arrow to the right of the icon at the beginning of the Address (Breadcrumb) bar. This will drop down a menu from which you should click your name; see Figure 3-10.

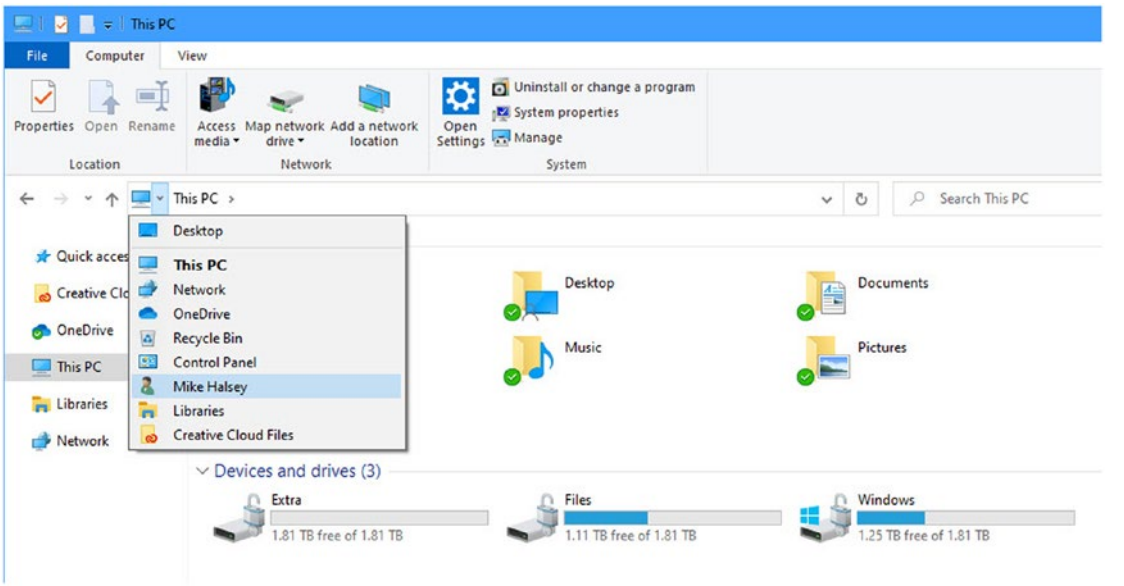


Figure 3-10. *You can access your Shell User Folders easily in File Explorer*

When in the Shell User Folder, follow these simple steps:

1. Select all the folders you wish to move. You can select multiple folders by highlighting them all by holding the mouse button and encircling them, clicking the first and holding down the *Shift* key while you click the last, or by holding the *Ctrl* key while you click each one you want to select.
2. Right-click one of the selected folders, and from the context menu that appears, click *Cut*. Alternatively, you can press Ctrl+X.
3. Navigate to the drive or partition and folder where you want to move your user folders.
4. Right-click in a blank space, and from the context menu that appears, click *Paste*. Alternatively, you can press *Ctrl+V*.

It really is as simple as a cut-and-paste operation to move the user folders. You might be asked for confirmation to move some items, but you can cheerfully click "accept" to these questions. When the operation completes, all your user folders will be moved, with the relevant pointers within Windows 10, having been automatically updated for you. It's a good idea to move your user files when you've first signed into the PC, before you've opened any files. This will prevent those files from becoming locked, stopping Windows from being able to move them.

Creating, Managing, and Deleting Partitions

As I mentioned in the last section, moving your Shell User Folders might require you to create a special files partition on your PC. This will be the case if you don't already have a second hard disk or partition available that's large enough for your files.

This is an easy operation to perform, though there are a couple of steps you might want to perform first to free up slightly more space on your drive, namely, running the *Disk cleanup wizard* to clean temporary and other unwanted files, and then defragmenting your hard disk. Note that defragmenting the drive here also applies to SSDs, which you would not normally defragment. This is because you want all the files on the disk as close to the beginning of the disk as possible.

The first operation is to shrink the size of your Windows partition; you can do this in the *Disk Management* Console, which is most easily accessed from the **Win + X** administration menu. When the console appears, right-click your Windows drive, and from the menu that appears, select *Shrink*; see Figure 3-11.

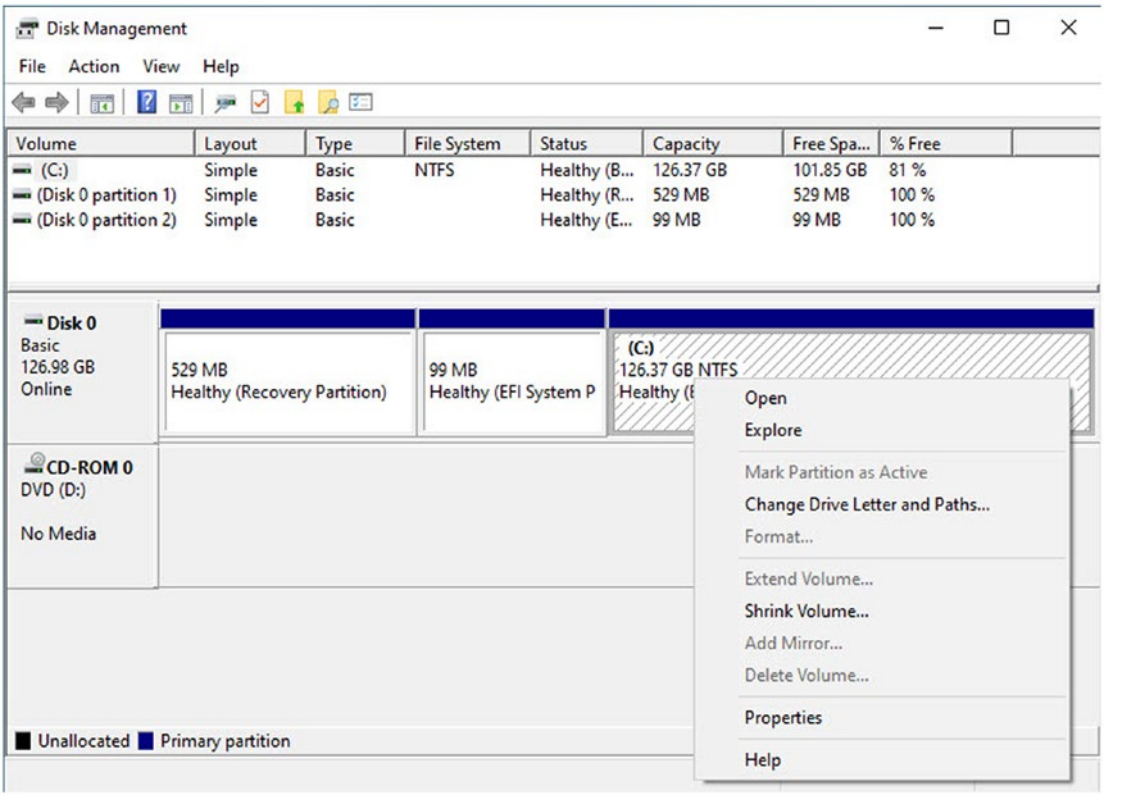


Figure 3-11. *You need to shrink your Windows partition in the Disk Management Console*

You will be asked how much you want to shrink the partition by (if not much is available to you, try cleaning temporary files and defragmenting the disk again); see Figure 3-12.

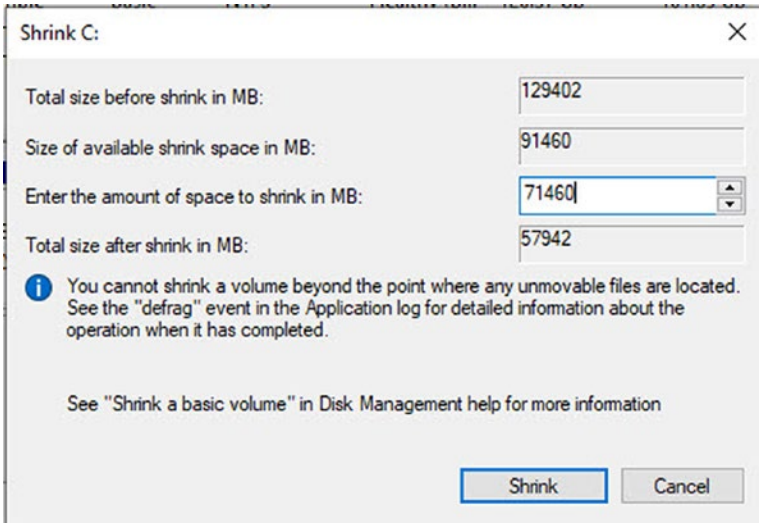


Figure 3-12. *You will be asked how much space you want to shrink the drive by*

When you are deciding how much space to shrink the drive by, think about how much space you will need on your Windows partition. For general usage, 50GB is a good minimum size for a PC using Office software. A heavy PC user or enthusiast might want 250GB (268435) or 500GB (536870), and a gamer might want up to 1TB (1099511) or more.

After the partition has been shrunk, right-click in the *unallocated* space to its right, and select *New simple volume* from the options that appear; see Figure 3-13.

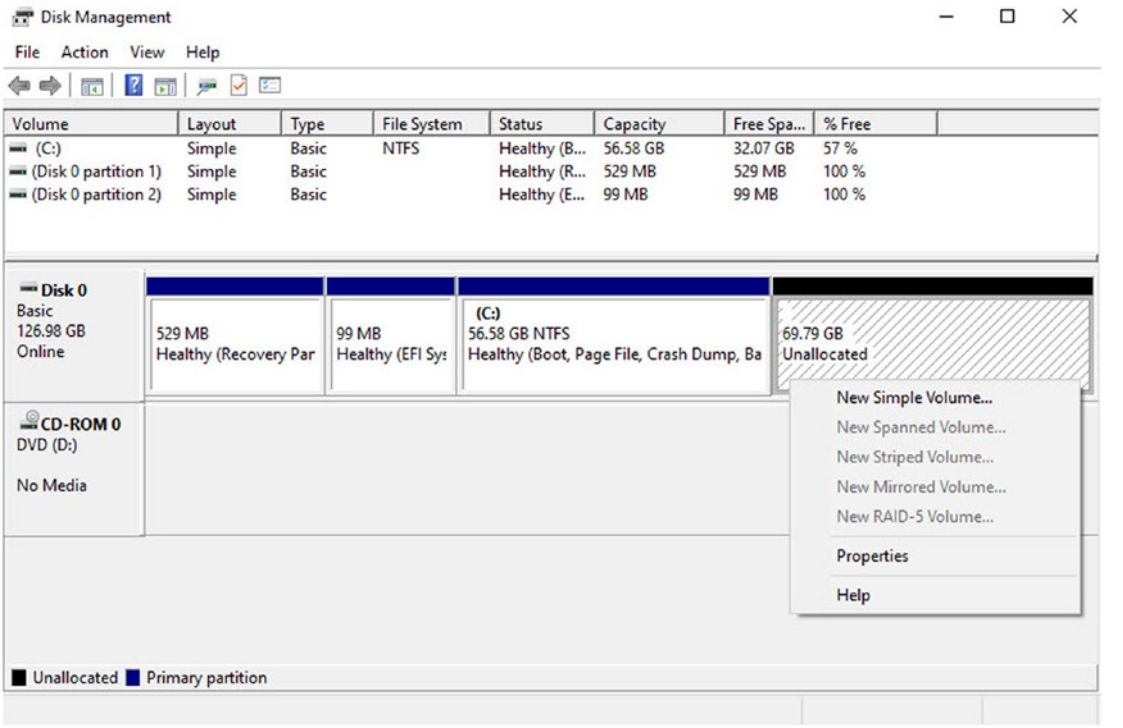


Figure 3-13. *After shrinking a volume, you need to create a new one in the free space*

A wizard will appear with the amount of recommended space for the partition, also being the maximum space available for it. Give the drive a drive letter and (optionally) a name, and click Finish to complete the partition creation. This will give you a new partition on which you can store your files and documents; see Figure 3-14.

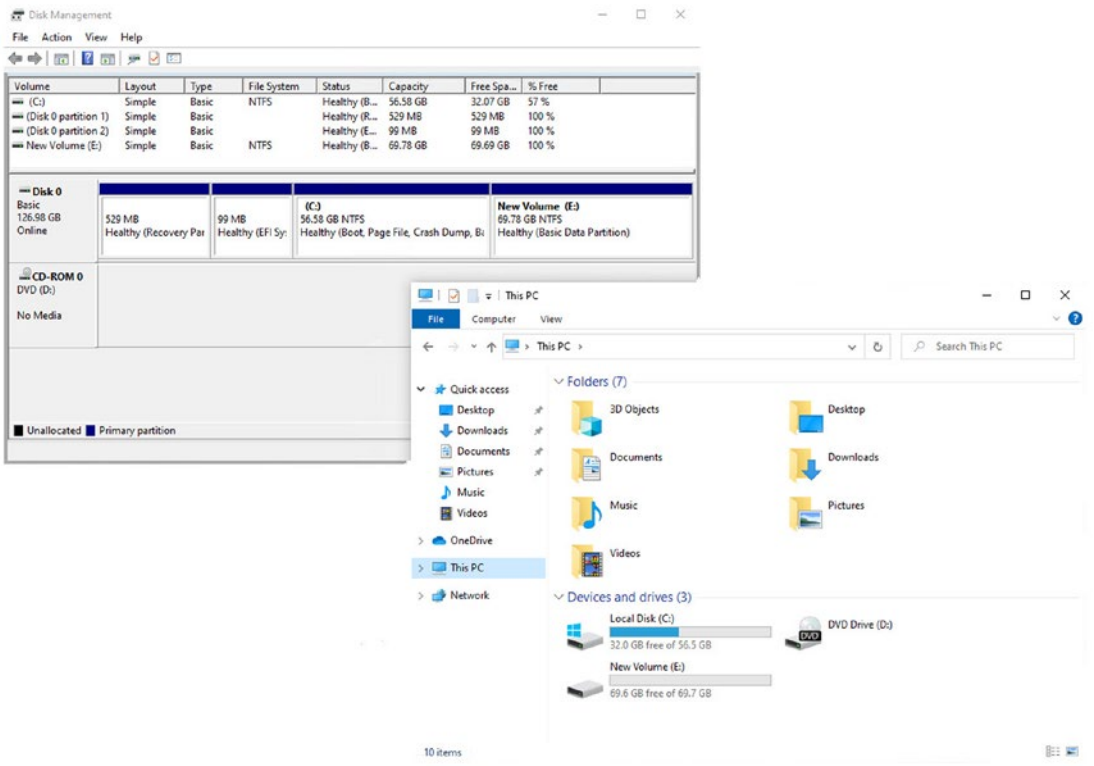


Figure 3-14. *Your newly created partition will appear in File Explorer, ready for use*

Managing Startup Apps

Everybody wants a PC that starts and gets to the desktop quickly, and Windows 10 starts faster than any other version of Windows before it, and with the latest NVMe M.2 drives installed, you can be from a cold boot to the desktop in as little as 7 seconds.

This process can be slowed significantly however by apps that are set to run at Startup. This can include system tray utilities from companies like Adobe, some of which are essential for apps to run, sync utilities for backup and cloud services, updater apps from companies like Apple and Google (that you can run manually when you want to check for updates to apps), and the preinstalled software that comes with your PC when you purchase it, officially known in the trade as "crapware."

Startup apps in Windows 10 are managed through the Task Manager. There are several ways to open this. You can press **Ctrl+Alt+Del** on your keyboard and select Task Manager from the menu that appears, you can right-click in a blank space on the Taskbar

and select *Task Manager* from the menu that appears, or you can run *Task Manager* from the **Win+X** administration menu.

When in the Task Manager, click the *Start-up* tab, and here all of the apps that run at startup on your PC will be listed; see Figure 3-15.

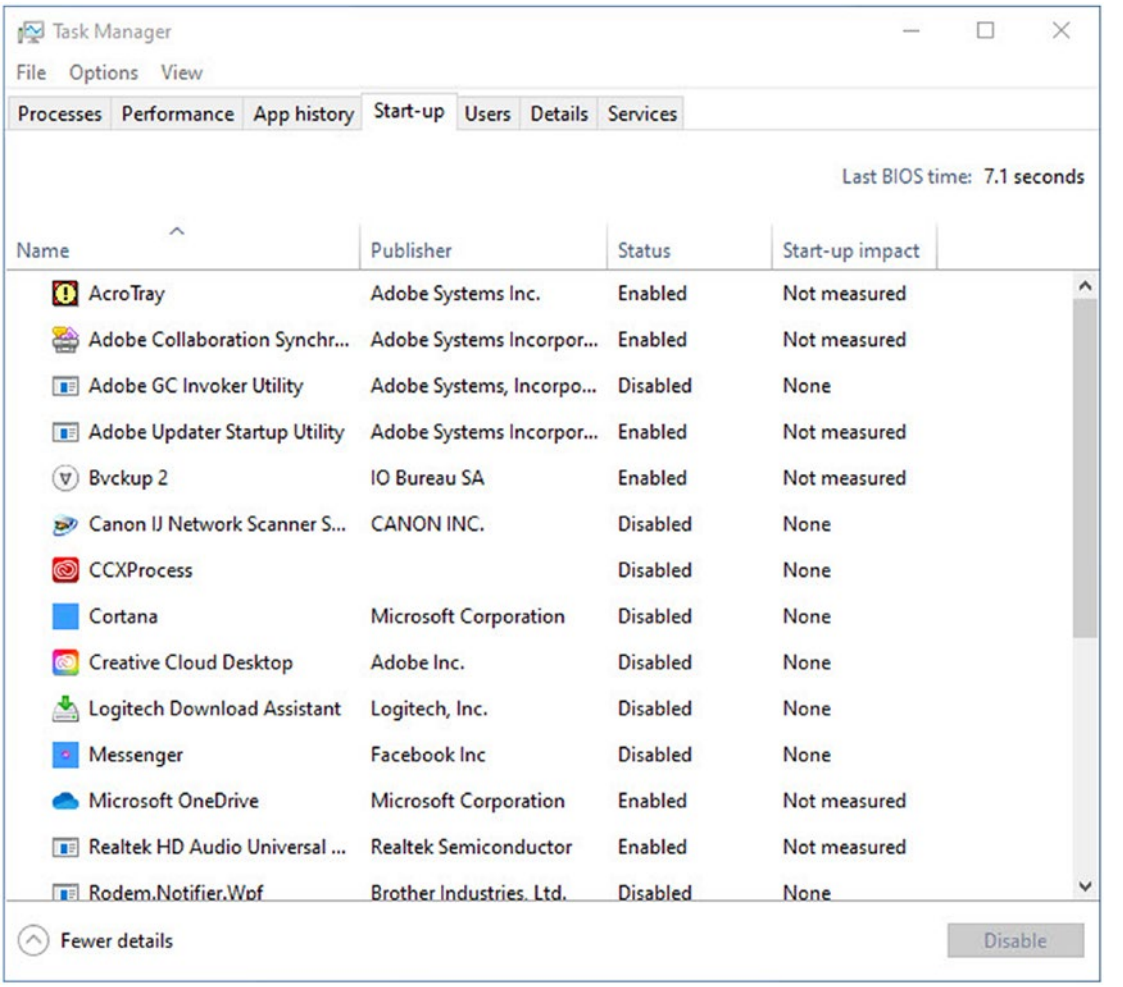


Figure 3-15. *You manage Startup apps in Task Manager*

Each one has a Startup impact assessment rating next to it of Low, Medium, or High. This is the effect that programs have on slowing your PC's startup. Choose the apps you want to disable (you can easily reenable them afterward as they stay in the list) by selecting one and then clicking the *Disable* button in the bottom right corner of the window.

Summary

In this chapter, I've covered everything you need to know to set up, configure, and back up Windows 10 and your files and documents so as to minimize problems, and so that if something drastic does go wrong, you can recover fairly quickly.

Speed is the most important aspect of supporting PCs, however, as time always costs money, and other problems can still arise such as compatibility with older "legacy" apps, especially custom company apps, managing Internet Explorer when that's required for the workplace Intranet or for compatibility with specific plug-ins, and more besides. In the next chapter, then, we'll look at some of the common problems that you can face on PCs, with a focus on diagnosing and repairing them quickly.

CHAPTER 4

Fixing Windows 10 Quickly

While it's always better to prevent problems from occurring in the first instance, when they do occur, fixing them quickly, and even having the end user repair a problem on their own remotely, is always preferable to a time-consuming reimage or reinstall.

The holy grail of repairing a Windows PC has always been to fix any problems within 30 minutes or less, and while some straightforward problems might make for easy fixes, others can prove more bothersome. In this chapter I'll show you the common ways to fix problems quickly and simply.

The Disk Cleanup Wizard

The Disk Cleanup Wizard is one of those esteemed tools that's been in Windows since the dawn of time. Indeed, like other tools and programs including Paint, Notepad, and Solitaire, it almost feels sometime like the OS was built around the need to use them. This tool, however, is much more useful than for just cleaning out temporary files to "free up a bit of space."

You can run the Disk Cleanup Wizard most easily by searching for **disk** or **clean** in the Start Menu or Cortana. If you have more than one disk or partition on your PC, you'll be asked which disk you want to clean (it should default to the drive on which Windows 10 is installed).

The main options present a list of check boxes that include the obvious temporary files and setup files; see Figure 4-1. There's much more to it than this, however. Why clean up temporary files in the first place, though; they don't cause problems, do they? In rare cases they actually can, but there's no way to know for sure unless you delete them.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_4

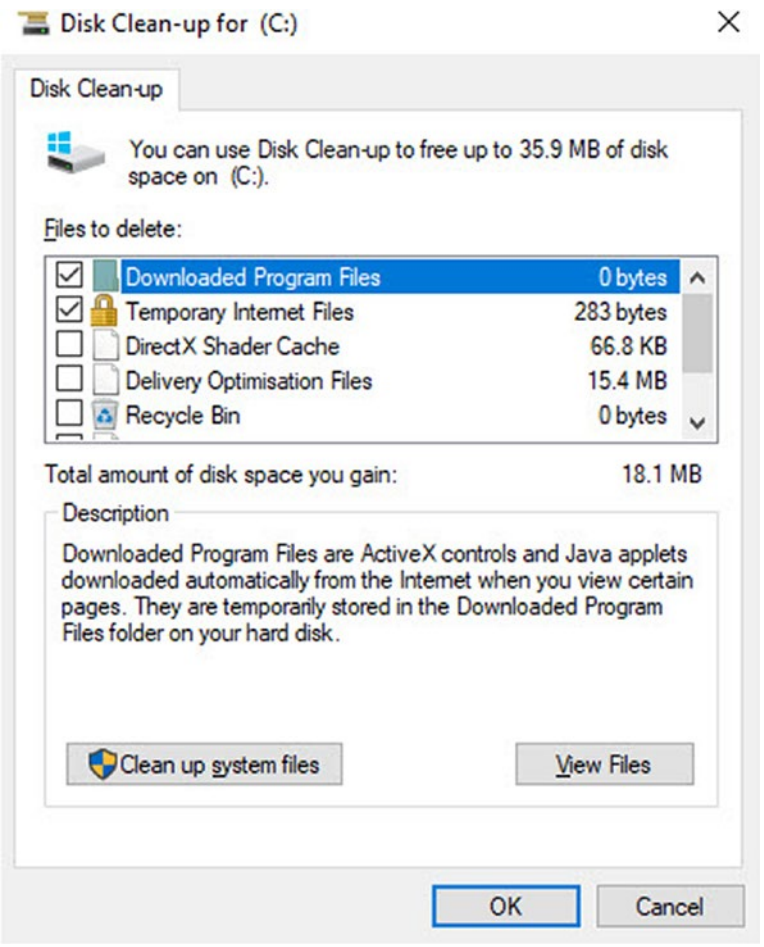


Figure 4-1. *At its simplest, the Disk Cleanup Wizard removes temporary and unwanted files*

Clicking the *Clean up system files* button will reveal additional options. These can include "Windows Update Clean-up" which, if you've recently upgraded the PC to Windows 10, can consist of the previous Windows installation. Windows 10 protects these files for 30 days after the upgrade, so it can be rolled back if necessary. However, they can occupy many gigabytes of space, and on an ultrabook with a small SSD, this can fill much of the available storage on the device.

Two things to note is the option to clean up *Downloaded Program Files*. You might want to uncheck this option as it will delete everything in your Downloads folder, and some people like to keep these if even for a short while. Also the *Thumbnails* option deletes all the created image and document thumbnail files from File Explorer. If you have corrupt thumbnails, and I can't imagine why you would, this could be useful, but otherwise there's no need to delete them, as Windows will only need to spend time recreating them when you open File Explorer again.

Clicking the *More options* tab presents an option to clean up *System Restore and Shadow Copies*. These reside in the *System Volume Information* folders that are hidden on each hard disk or partition. Should System Restore become corrupt, deleting the restore points can reset it.

Tip If you want more power, flexibility, and control than the Disk Cleanup Wizard offers, the market leader in disk maintenance and cleanup is the excellent **CCleaner**, available for free from `piriform.com`.

What Is the Situation with Internet Explorer?

So let's deal with the elephant in the room that is Internet Explorer. Microsoft's first web browser, which dates back to Windows 95 in August 1995, is kaput, defunct, obsolete, etc., so why is it still part of Windows 10? The simplest answer is to assuage the fears of business and corporations that still use plug-ins, or that have Intranets that won't render properly, or that don't work properly in a modern web browser. Be certain though that Internet Explorer is a goner.

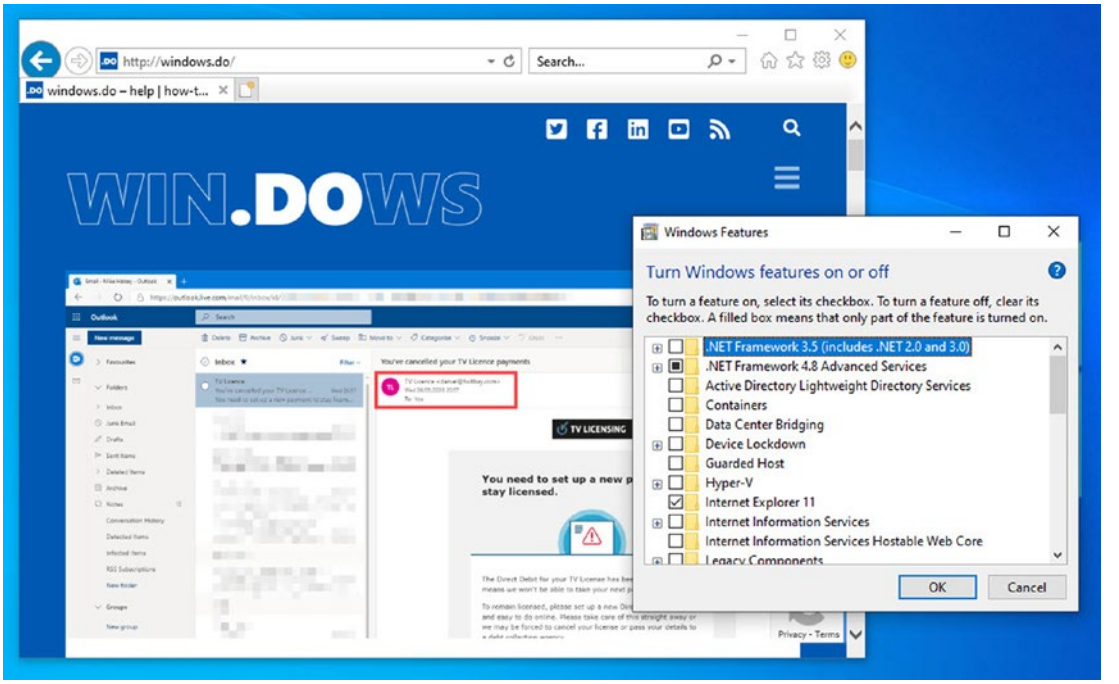


Figure 4-2. *Internet Explorer, they keep threatening to take it away…*

The release of Windows 11 means Microsoft probably will keep Internet Explorer present in Windows 10, as development of Windows 10 will now have stopped, but this in itself is no guarantee of longevity. For the purposes of this chapter however, we will assume that Internet Explorer will remain in Windows 10 and that some of you might still need to use it.

Microsoft have made great strides with Internet Explorer compatibility mode in Edge however. We will look at this in detail in Chapter 17, but the short version is that you can find these settings in Edge, under *Default Browser*; see Figure 4-3.

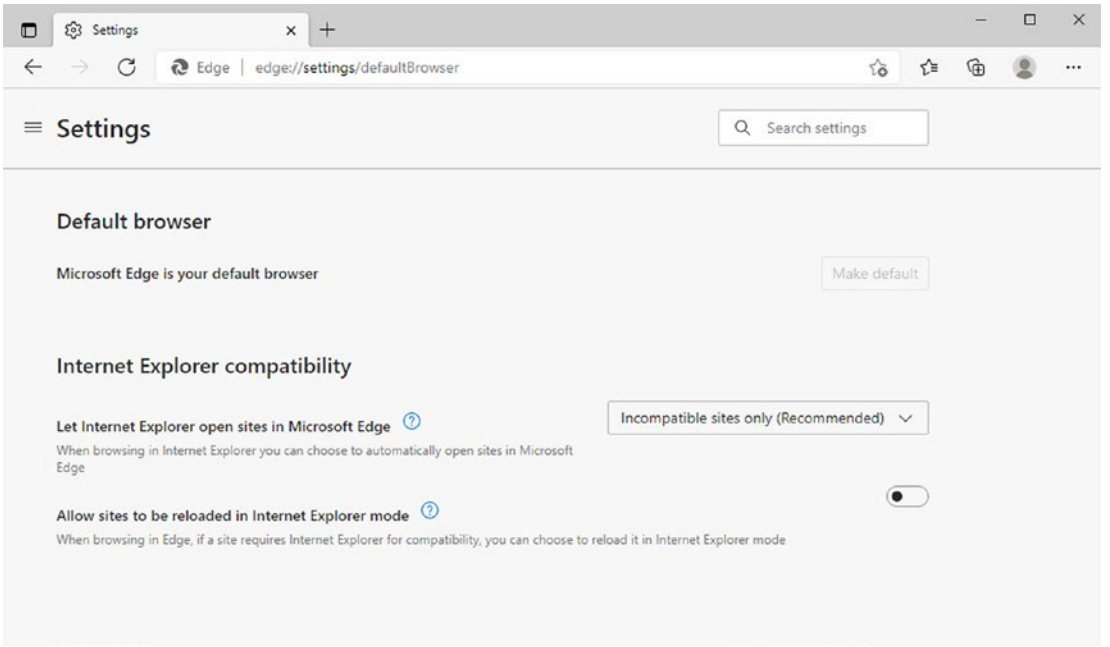


Figure 4-3. *Microsoft's Edge browser maintains compatibility with Internet Explorer*

Managing IE and Edge

If we didn't have web browsers on our PCs, the machines wouldn't, in all honestly, be of that much use to us. Imagine picking up an original IBM PC (with both hands obviously as they were really heavy) or an original Palm handheld (much easier, that one) and finding that neither has an Internet connection. What would you use them for?

Unfortunately, both Internet Explorer 11 (IE11) and Edge are baked into Windows 10, so if they should become corrupt in some way, uninstalling and reinstalling them simply isn't possible. So when your web browser *does* become corrupt (which does happen), what do you do? Is the solution simply to install Google Chrome? Managing IE and Edge is straightforward though, which is good news.

Cleaning Temporary and Other Files from IE and Edge

While the Disk Cleanup Wizard is a great, easy-to-use tool for deleting temporary files from your PC, your web browser can collect additional files you may want to clean from time to time, for example, if the browser is appearing to slow down on startup and use.

To manage temporary and other files in IE, click the Settings icon in the top right of the browser and then click the *Internet options* link from the menu that appears. This will open into the *General* tab of a pop-up dialog. Click the *Delete* button, and you will be presented with check boxes for the things you can delete from the browser's cache; see Figure 4-4.

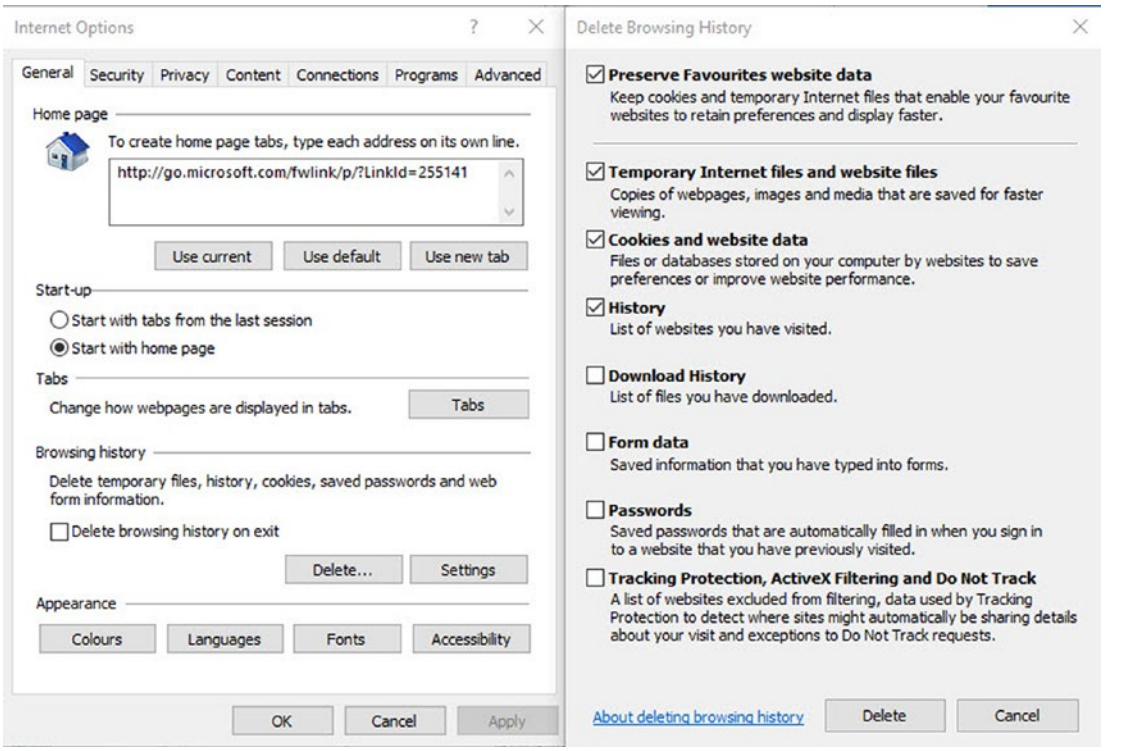


Figure 4-4. *You can delete temporary files and much more from IE11*

With the Edge Browser, click the menu icon (the three horizontal dots) near the top right of the browser window; then, click the *Settings* link. Next, click the *Privacy, search and services* option on the left of the page (note you may first need to click the hamburger menu icon, and you will see a *Clear browsing data* section with a *Choose what to clear* button; see Figure 4-5.

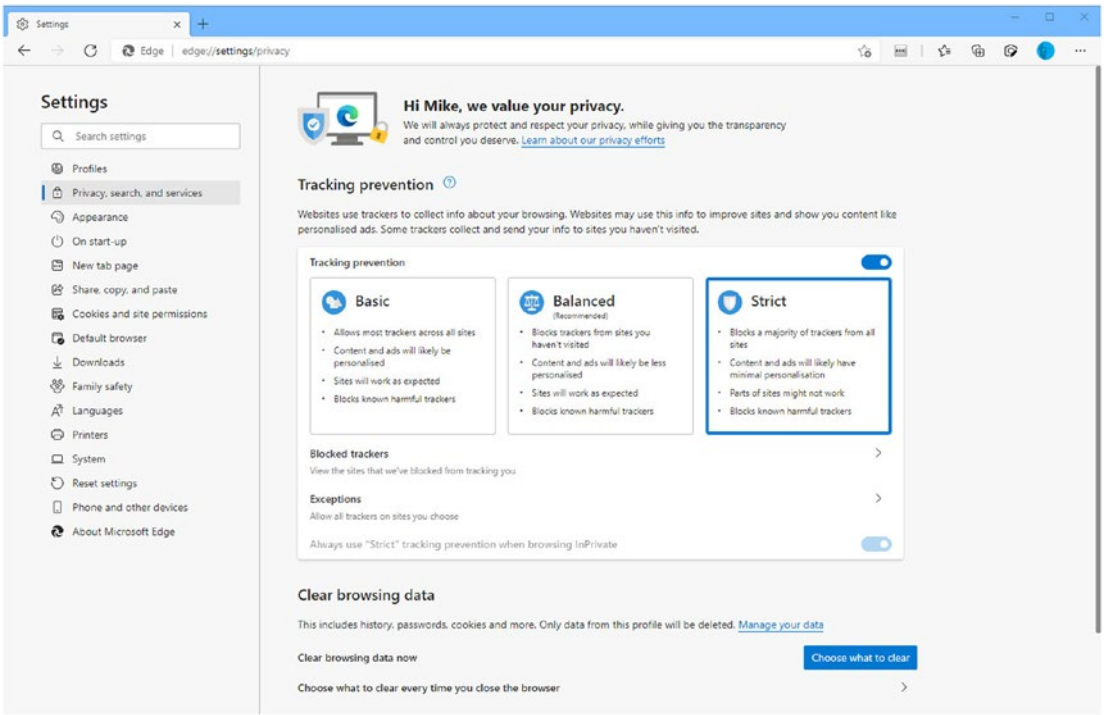


Figure 4-5. *You can clear out the Edge browser as well as IE11*

Resetting IE

If IE is failing to open, or is misbehaving or crashing, it's not possible to uninstall it or install a newer version, but you can completely reset it. This can be done both from within the browser itself and also from the Control Panel if IE11 won't open.

From the browser, click the Settings icon and then the *Internet Options* link. From the Control Panel, click *Internet Options* in either the large or small icon view.

When the Internet Properties dialog appears, click the *Advanced* tab, followed by the *Reset* button. You'll be asked if you also want the reset to delete your personal files (such as temporary files, cookies, and web form data) at the same time as the reset, as something here might be contributing to the corruption; see Figure 4-6. Performing the reset, though, won't delete your Internet Favorites, as they are stored in your Shell User Folder.

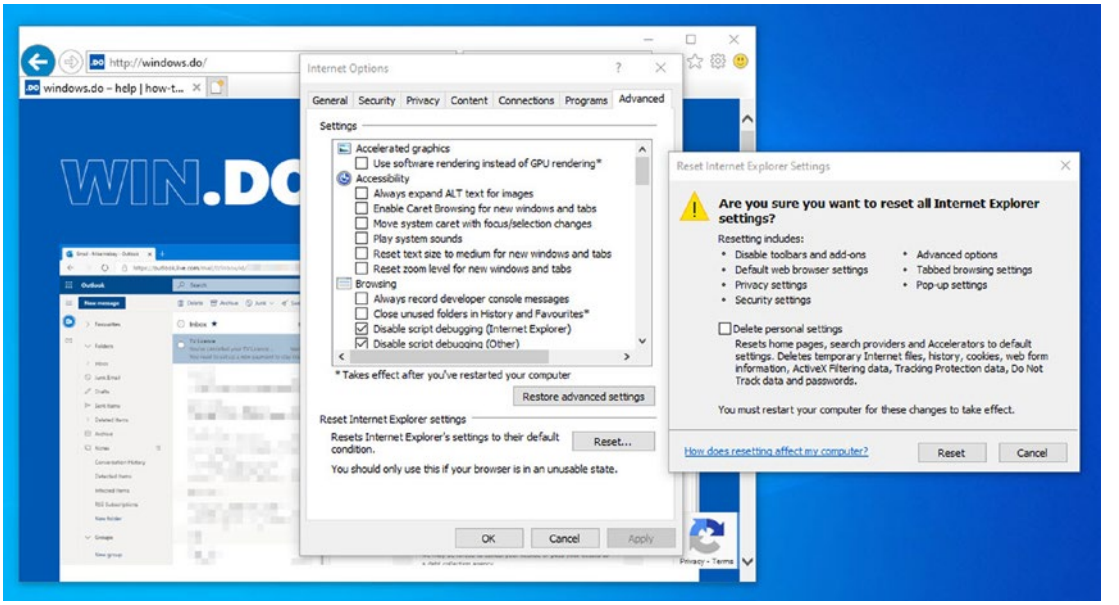


Figure 4-6. *You can completely reset IE11 in Windows 10*

Click *Reset* when you are ready, and this will restore IE11 to its "out-of-the-box" state and get the web browser working again.

Resetting Edge, the Windows Store and Store Apps

Resetting Edge is a very different proposition as, being a Windows Store app instead of a win32 app, it operates very differently and its core files are never accessible to the end user or other apps. Because Store apps are completely sandboxed from both the OS and each other, corruptions are far less likely.

Edge does include an option to reset its settings to their default values, but this is a different ball of wax to completely resetting the app. You can find the Reset settings option by opening *Settings* in Edge from the three dots icon in the top right of the browser and navigating to the *Reset settings* option in the left side menu; see Figure 4-7. Note again you may have to click the hamburger icon near the top left of the window to open this menu.

Figure 4-7. *You can reset settings in Edge, but not the whole app*

You might think that you won't need to ever completely reset Edge, as it's a newer form of web browser, but on occasion, you might find that Edge won't open, won't update, or is misbehaving in some other way. You can fix this by resetting the Windows Store and its core app management files.

In the Start Menu, search for **wsreset**, and when it appears in the search results, right-click it and run it as an Administrator (this is very important); see Figure 4-8.

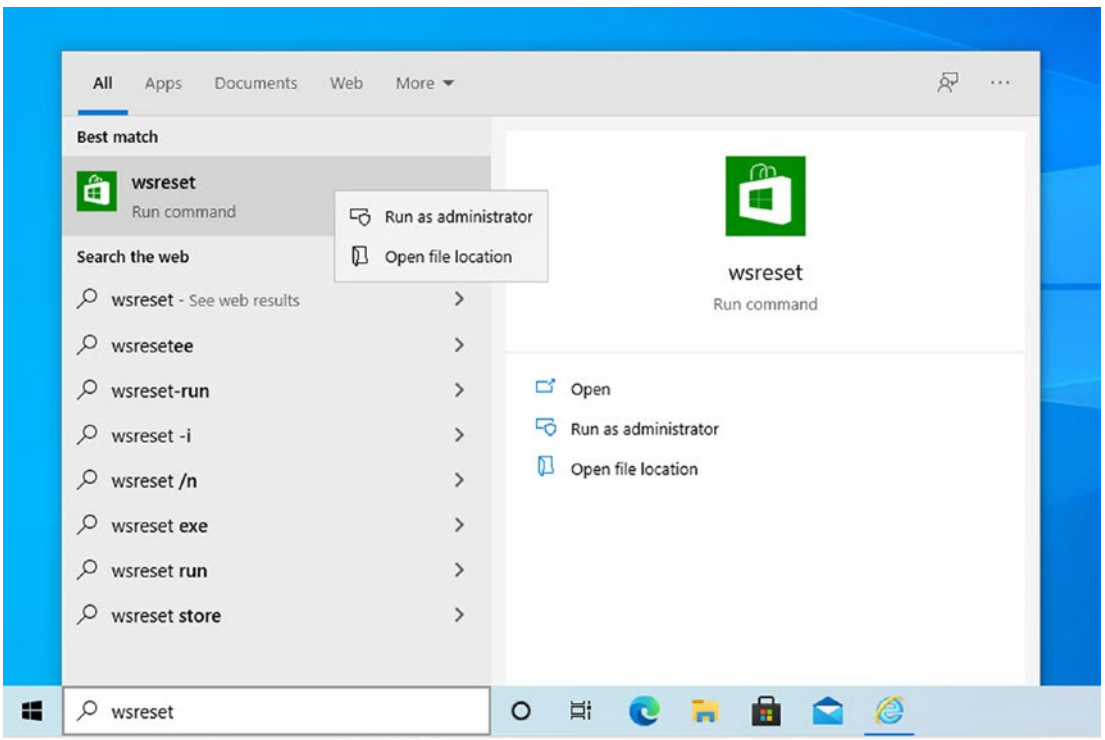


Figure 4-8. *This app resets the cache for the Windows Store and can reset apps*

The WSReset app will report that it's cleared the cache for the Windows Store but also does much more. If you ever find the Windows Store isn't working, or won't download or update apps, this is how to fix it. Additionally, it will also repair problems with installed Store apps themselves. Microsoft has never detailed how this functionality works for security reasons, but it's a useful fix to know about.

When you have run WSReset, you should then open the Windows Store app and check for any updates to Edge which you can do from within the browser by opening *Settings* and clicking *About Microsoft Edge*.

Defragmenting Your Hard Disks

Fragmentation occurs because when you save files on your hard disk, Windows 10 will try to save the file in the first accessible space. Should this space not be big enough for the file, it will save some of the file there, and place the rest of the file in the next available space. If that space isn't large enough for the remainder of the file, it will be split again. This isn't a problem for new installations of Windows and your apps, or for copying or downloading your files to a clean hard disk for the first time, but as a hard disk gets used more and more, and files are changed and deleted, the number of large blocks of free space diminishes, and file fragmentation begins to occur.

I mentioned in Chapter 1 that SSDs and M.2 drives don't suffer from this, the reason being that solid-state disks are a random-access memory storage medium, and therefore pulling a file from multiple locations doesn't slow them down. What slows down mechanical hard disks is the movement of the read arm across the spinning disk platters.

Having fragmented disks on a PC can really slow down the operation of the PC, from Startup to file access, if mechanical disks are used. Windows 10 includes an automatic maintenance system, detailed in Chapter 1, which will automatically defragment drives. What can happen, however, is that defragmentation set to occur when the PC is in use can also slow it down, and if the defragmentation is set to occur when the PC is likely to be switched off, it won't happen at all.

You can change the settings for defragmentation in Windows 10 by searching for **defrag** in the Start Menu or Cortana and clicking *Defragment and Optimize Drives*. The main Defragmenter window lists all of the hard disks and partitions on your PC, along with their fragmentation status; see Figure 4-9.

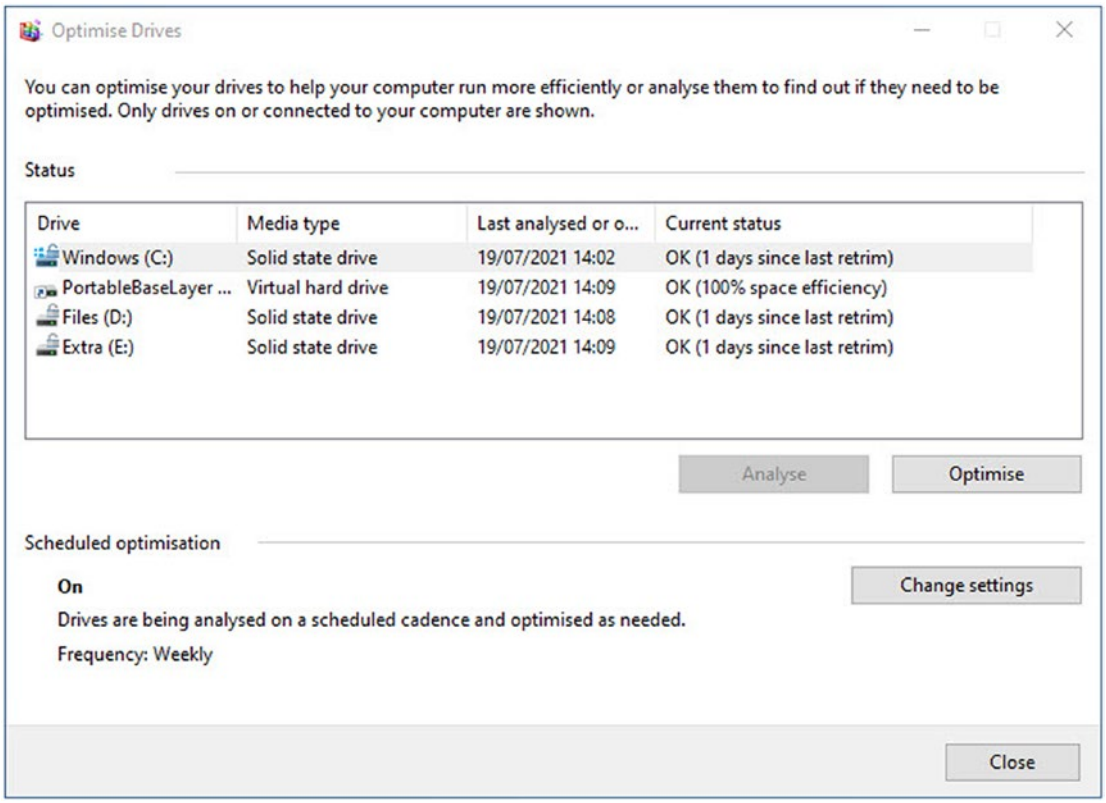


Figure 4-9. *Fragmented disks can really slow your PC*

Clicking the *Change settings* button will allow you to choose which drives will be automatically defragmented by Windows 10, and how often this occurs. You can choose to exclude any solid-state drives should Windows 10 have not already excluded them from defragmentation.

Note You will notice in Figure 4-9 that the solid-state drives say they are (1 day since last retrim). Trim is a feature of SSDs and M.2 drives where the operating system can tell the drive which blocks of data are no longer required and can be deleted. You can consider it a random-access method of defragmenting a disk, and it is useful to leave this feature activated if your drives support it.

Managing Running Apps and Services with Task Manager

The Task Manager is a fantastic little tool for managing and troubleshooting apps and services, and in Chapter 25 I'll show you how to unlock its full potential. Back in Chapter 3, I showed you how to use it to manage your startup apps, but what about apps and both Windows and third-party services that are already running? How can you troubleshoot and manage those?

You can open Task Manager by right-clicking in a black space on the Taskbar, from the **Ctrl+Alt+Del** menu, or from the **Win+X** menu.

If you have an app that is malfunctioning, won't close, or has hung or crashed, you can manage it from the *Processes* tab in Task Manager. Click the name of the app you want to close, and click the *End task* button in the bottom right corner of the Task Manager window; see Figure 4-10.

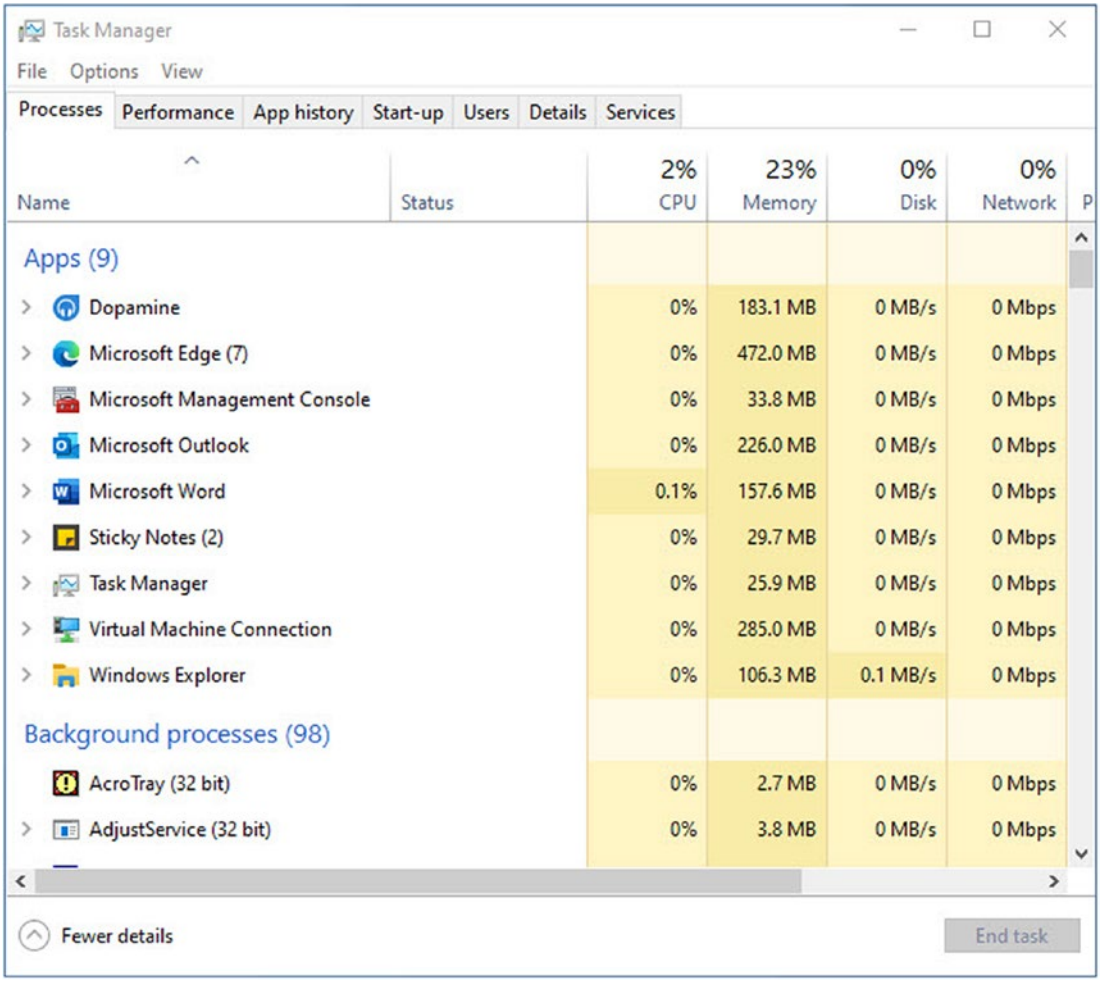


Figure 4-10. *You can manage crashed apps in the Task Manager*

Should you have multiple instances of an app running, and only one has crashed or needs to be forcibly closed, click the ➤ arrow to the left of the app name to expend the list of all running instances of the app. You can then close just the faulty instance.

Sometimes you will have an app that also has dependent apps or services. Think of this as an app consisting of a main app with several subapps running at the same time, all for different purposes but all required for the main app to work.

If a subapp crashes, or if you need to close an app and all of its dependencies for it to work, you can do this from the *Details* tab. Right-click the app, and from the context menu that appears, click *End process tree*; see Figure 4-11.

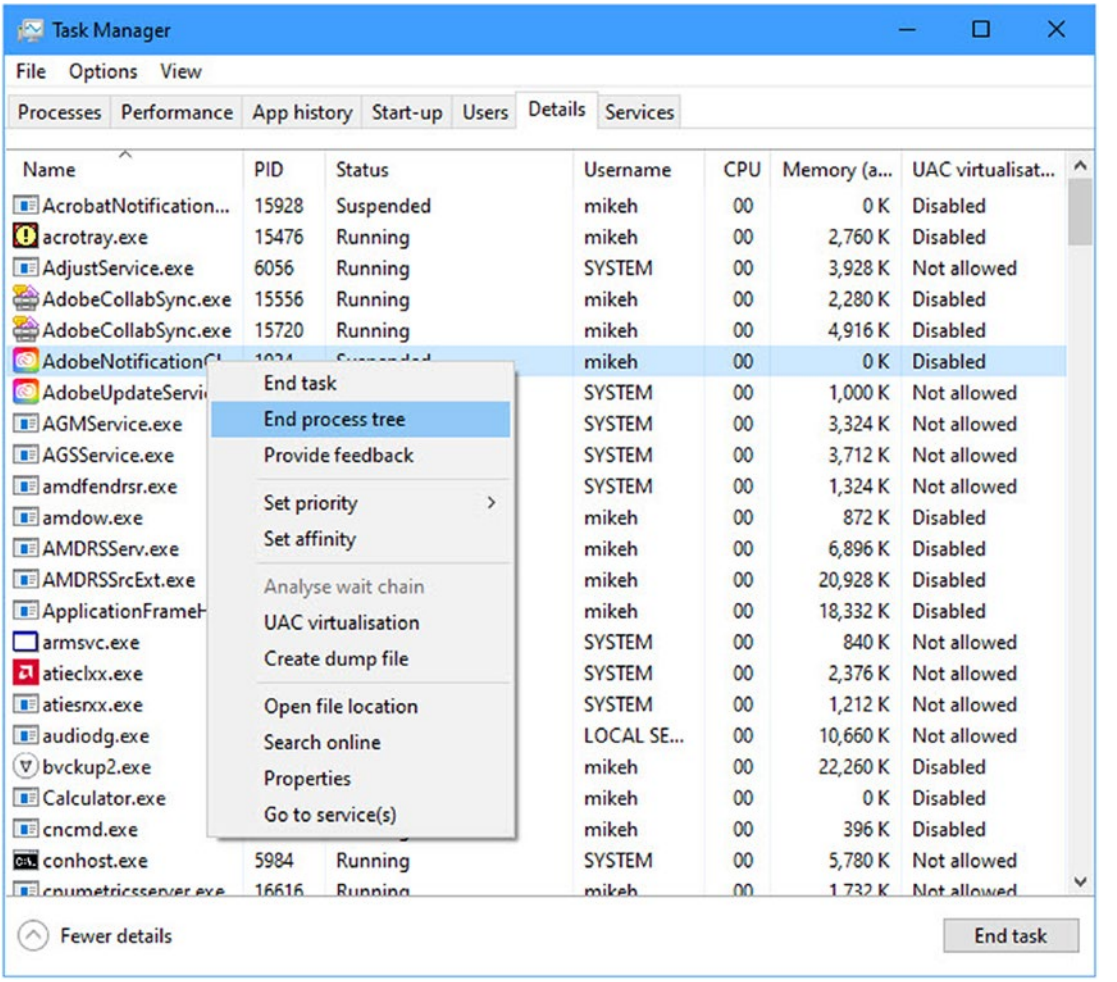


Figure 4-11. *The Details tab allows you to close all the dependencies for an app*

Other app management operations that can be performed by right-clicking an app, service, or process in the Details tab include

- **Set priority**—to change the amount of processor time allocated to the apps from Normal to Below Normal, Low, Above Normal, High, or Real time.
- **Set affinity**—to change which processors or processor cores on your PC are assigned to the app (most useful when assigning individual processors to virtual machines).

- **Analyze wait chain**—can be used if an app has hung, to identify which resources the app is waiting to use, and is required for the process to continue.
- **Debug**—can be used if you have development software installed on your PC, such as Microsoft Visual Studio, to analyze bugs and crashes in compatible apps and services.
- **User Account Control (UAC) Virtualization**—used when some apps require the user to have full administrative rights, but the user is signed into the PC as a "Standard user" instead. This can be common with poorly written legacy apps. Activating UAC Virtualization enables Windows 10 to virtualize protected areas of the OS, such as the file system and Registry, so that the app can operate normally without hanging or reporting errors.
- **Create dump file**—will create a report on a crashed or hung app and report the location of the file so you may read or copy it, or send it to a support technician.
- **Open file location**—for win32 apps, will open a File Explorer window at the location where the app is installed. For Store apps, it will open the temporary app management folder located in the Windows/SystemApps folder and not the protected app store location.
- **Search online**—will open a browser search for the name of the current process, so that you may research it and discover what it is.
- **Properties**—opens the properties inspector for the app, which includes compatibility settings. Note any compatibility setting changes will only work once the app is restarted.
- **Go to Service(s)**—opens the Services tab in the Task Manager, and highlights any service(s) used by the process.

Services are best described as little applets that are designed to perform a specific task, and that are invoked automatically by Windows 10 or your apps as needed. They can manage your printer queue, security features, cloud syncing, and many more aspects of the OS and apps and are provided by both Microsoft and third-party app developers.

These services aren't built directly into apps because they're most commonly shared between multiple apps. For example, Microsoft provides services for font management, network access and discovery, and Bluetooth connections, which many other apps will want to use. Similarly, some apps systems (Adobe Creative Cloud as an example) will have their own data sharing services.

You manage Services primarily in the Services Administrative panel, which we will look at in Chapter 21. You can stop a hung or crashed service in the Task Manager, however, by right-clicking it and selecting either *Stop* or *Restart* from the context menu that appears; see Figure 4-12.

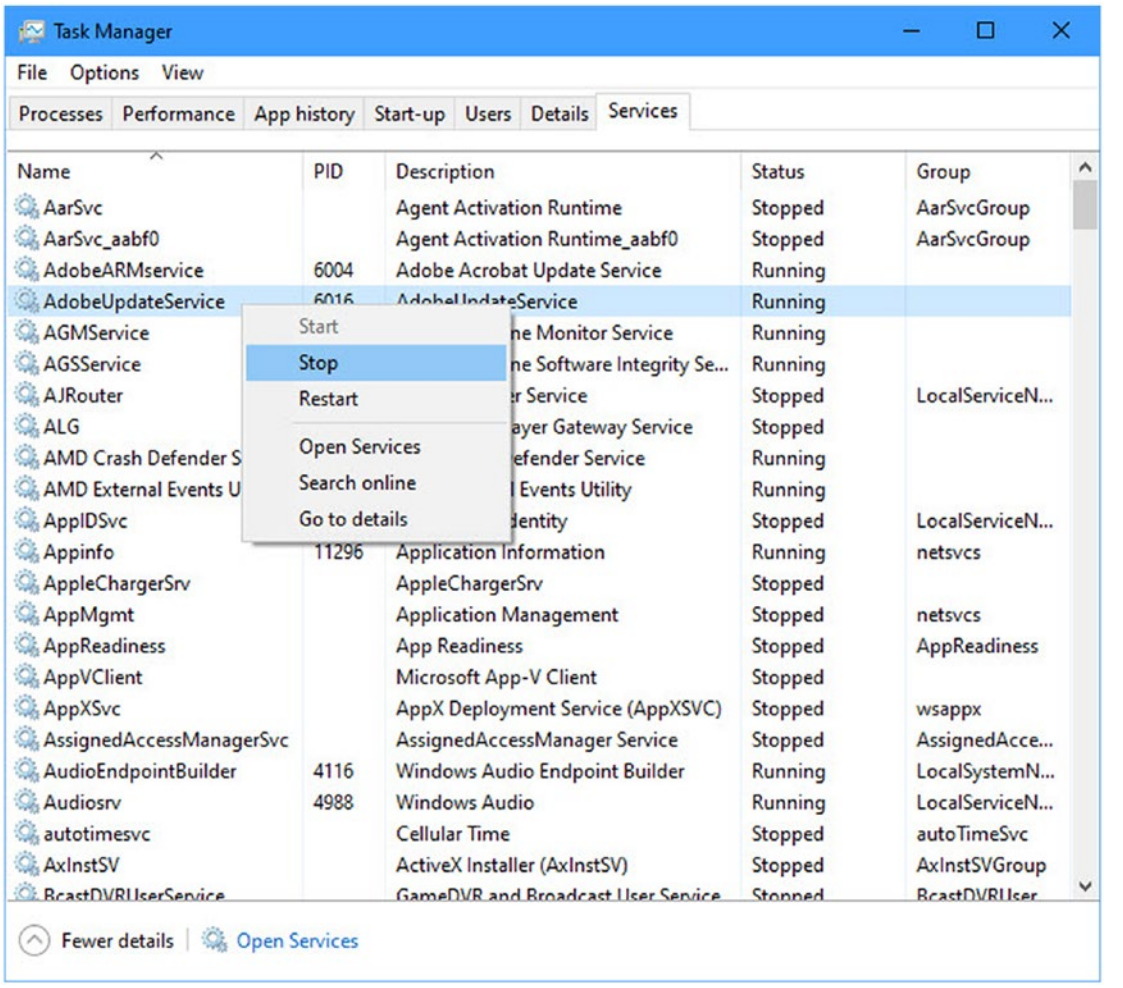


Figure 4-12. *You can start, stop, and reset services in Task Manager*

Services can also be started from the Task Manager if an app or process is reporting that a service it requires isn't running. If you are unsure what a service is, or what it does, you can also search for the service online from this context menu, so as to find out more information about it.

Managing win32 App Compatibility

While we're on the subject of troublesome apps, it's very true that as new versions of Windows have been developed, compatibility with older software has occasionally been broken. In fairness to Microsoft, it does a remarkable job, given all the new hardware, Internet, app, and other protocols that come along on a regular basis, of making sure that older software still has a good chance of working well. As core changes are made to the operating system, however, and as features are removed from Windows, it's inevitable that some app compatibility will break.

A good example of this is an older piece of software I use myself on a regular basis. Microsoft PhotoDraw v2 was released in 2000 and is still popular with a great many people; even though alternatives such as Fireworks and Photoshop can easily outmatch it for power, there's still almost nothing to match it for ease of use.

It's not all good news, however, as while the app works fine almost all of time, I will get an error if I use any of its 3D features; this is because Direct3D, the Windows API it uses, has changed so much over the years that it's now unrecognizable by the software.

"Oh no!" I hear you cry, sarcastically. I know, this is a very minor problem, and if it's the worst app compatibility problem I face, then I'm a pretty lucky guy. For some people who have software that they just love to use/that was withdrawn and never replaced by an alternative/that nothing else has ever come along to match (delete any of these that aren't applicable to your situation), app compatibility can be a significant headache.

There are several reasons for this. I've already alluded to the first, that as Windows has evolved, its features have changed so much that the APIs and DLLs that perform critical functions in the OS, and that are regularly called by apps, just aren't compatible

any more. There's also that some software, especially poorly written software, used workarounds that required the user to have Administrative privileges. I've already detailed one workaround for this with UAC Virtualization a little while ago, but significant headaches can still be caused.

To manage compatibility for a win32 desktop app, you need to access the app properties. Right-click its icon on the Taskbar, and from the context menu that appears, click *Properties*. From the Start Menu, right-click the app and select *More* and then *Open file location* from the context menu. In the window that appears, you can then right-click the app and select its *Properties*.

There are several ways to manage app compatibility. Perhaps the easiest of these is to run the Compatibility Troubleshooter, from the button that is under the *Compatibility* tab of the app properties dialog. This will ask you a series of questions about the app, and then set compatibility for you, asking you to run the app and report back if things worked or not.

If you want finer control, there are a couple of things you can do. The Compatibility Mode option (see Figure 4-13) is a drop-down menu that allows you to set compatibility for the app from Windows 8, all the way back to Windows 95. It's notable here, however, that where Service Packs for an OS brought about significant changes to features or performance, such as XP and Vista, additional options are available.

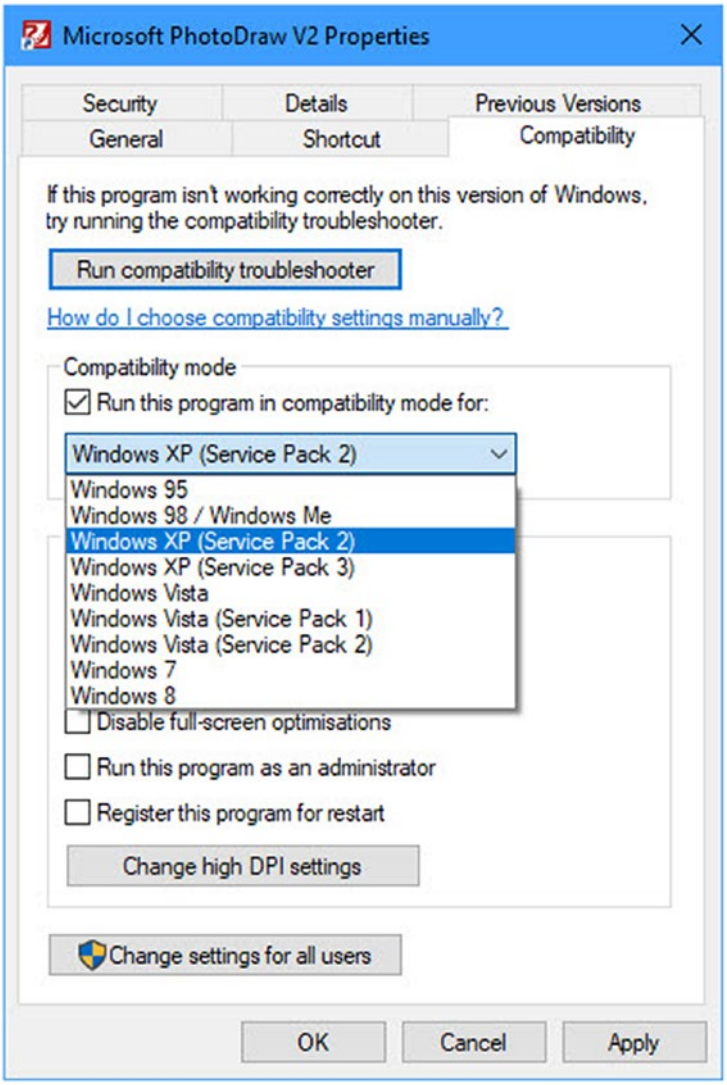


Figure 4-13. *You can set compatibility for apps all the way back to Windows 95*

This might not be enough, however, as you might find that, for example, the app displays incorrectly on high-DPI screens such as UHD/4K monitors or other screens where display scaling is used to make the screen more legible.

Tip Some app compatibility can be managed by running a virtual machine with an older operating system installed, in which the app ran properly. There are security considerations to make with this approach, however, and I will detail Virtualization in Chapter 20.

Other options are also available, such as forcing the app to run constrained in a 640- by 480-pixel frame and forcing the program to always run as an Administrator; see Figure 4-14. Bear in mind that this last option is not the same as UAC Virtualization and will require *actual* administrative rights for the use on that PC.

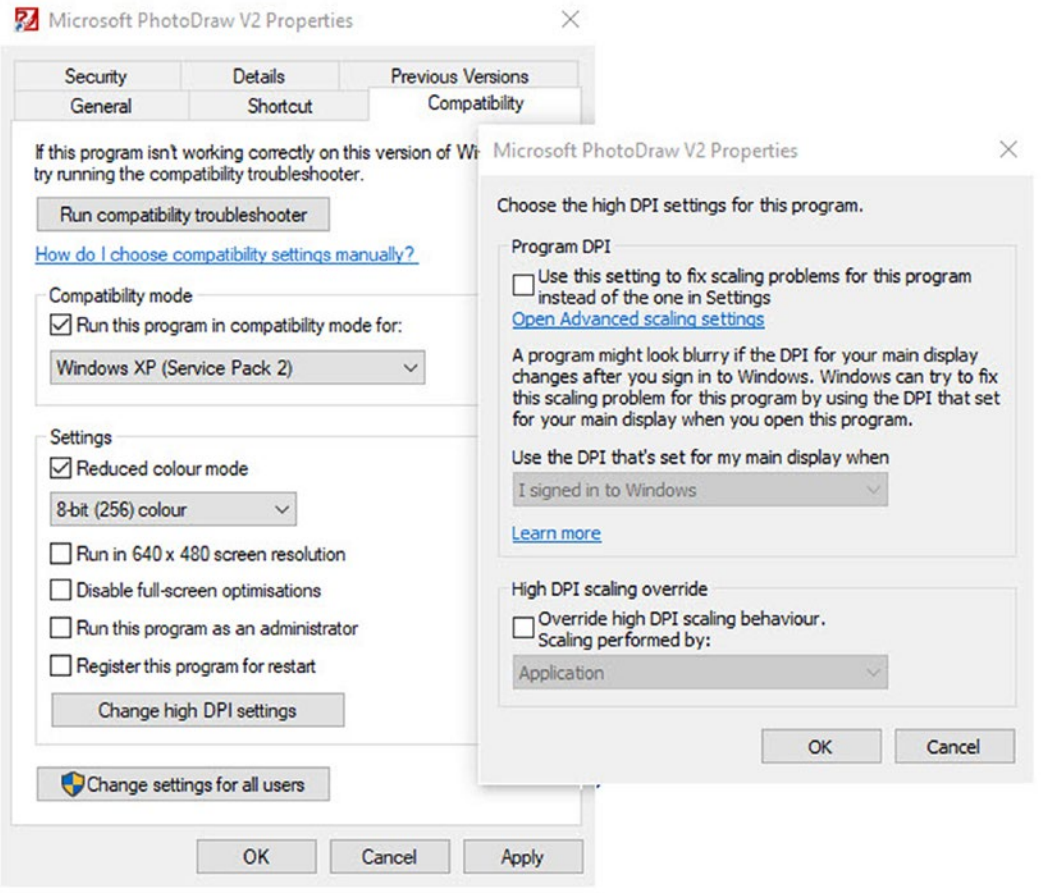


Figure 4-14. *Additional compatibility options are available*

Tip For large organizations, Microsoft provides two tools to help manage app compatibility: the Application Compatibility Toolkit and Standard User Analyzer. You can download these as part of the Windows 10 Assessment and Deployment Toolkit (ADK) from `http://pcs.tv/1P7HwIp`, and they're detailed in full in my book *Windows Software Compatibility and Hardware Troubleshooting* (Apress, 2015).

Using the System File Checker

If there were two hidden troubleshooting tools that every system administrator should know about, and that make me go all "Squeee," one would be the Problem Steps Recorder, which I'll detail in Chapter 12, and the other is the System File Checker. Essentially, the System File Checker scans every file that makes up Windows 10 and compares their integrity details (checksums) against what's stored in its database. If it finds any file that doesn't match, perhaps because it is corrupt or has been altered, then it can replace it with an original.

There are some caveats with this, however. The first is that it will take replacement files from Windows 10 install media, but doesn't work with Windows 10 installations that come on USB Flash Drives. It only works with DVD installation media (so a USB DVD drive will be required for ultrabooks and tablets). The second caveat is that any file it pulls from the DVD must match the version number of the one currently installed on the PC. This means that your DVD must be a Windows install disk that contains the most recent annual update (Service Pack) that's installed on the PC.

This latter issue isn't as much of a problem, however, as it used to be when you had to perform complex operations to merge a Service Pack into a DVD. If you have access to a volume licensing or MSDN subscription, you'll be able to download an ISO disc image file that contains the most recently released version of Windows 10. The way Windows Update now works, unless you're in the Enterprise and on the Long-Term Servicing Branch, in which only security and stability updates are installed, this will work fine.

For everybody else, the Windows 10 Media Creator I detailed in Chapter 1 is a great way to get free access to the latest installation ISO file. To burn this file to DVD, right-click it, and select the *Burn disc image* option from the menu that appears.

To use the System File Checker, open *Command Prompt (Admin)* from the **Win+X** menu. In the Command Prompt, type `SFC /SCANNOW` and press Enter; see Figure 4-15.

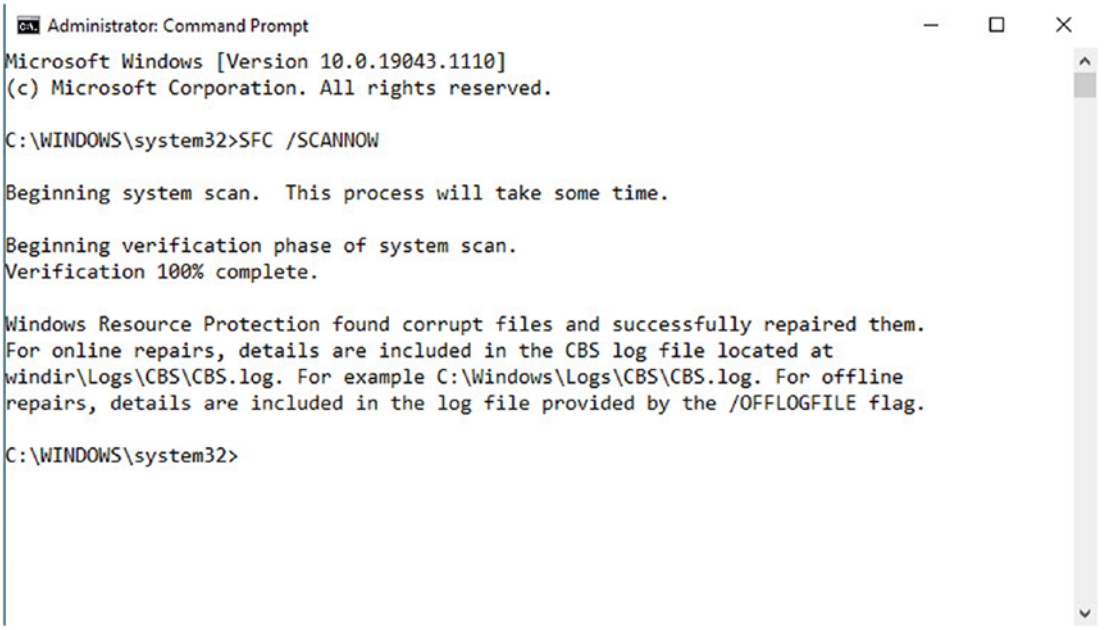


Figure 4-15. *The System File Checker is run from the Command Prompt*

If any files are found to have changed or become corrupt, the file will be automatically copied from the DVD (if it's already in your optical drive), or you'll be prompted for the DVD. Other command switches that can be used with the System File Checker are

- **/VERIFYONLY**—scans the files on the PC but does not attempt autorepair
- **/SCANFILE=C:\Folder\Filename**—scans a specific file and repairs it if it finds it has changed or is corrupt
- **/VERIFYFILE=C:\Folder\Filename**—as Scanfile, but does not attempt auto repair
- **/OFFBOOTDIR=C:** and **/OFFWINDIR=C:\Windows**—used with /ScanNow and /ScanFile if the file must be repaired offline (on a restart) because it is a critical system file, or is currently in use

Using the Automated Troubleshooters

Windows' Automated Troubleshooters are something I mentioned briefly in Chapter 1 when talking about the Security and Maintenance Center. Essentially, they are little applets that fix common problems by resetting components to their default state. Bear in mind that Microsoft haven't been clear about the future of these troubleshooters. While they have been folded into *Settings*, Microsoft have previously stated they're to be deprecated.

As I've already mentioned, you can find the Automated Troubleshooters through the *Settings* panel, by clicking *Update & Security* ➤ *Troubleshoot* and then *Additional Troubleshooters*; see Figure 4-16.

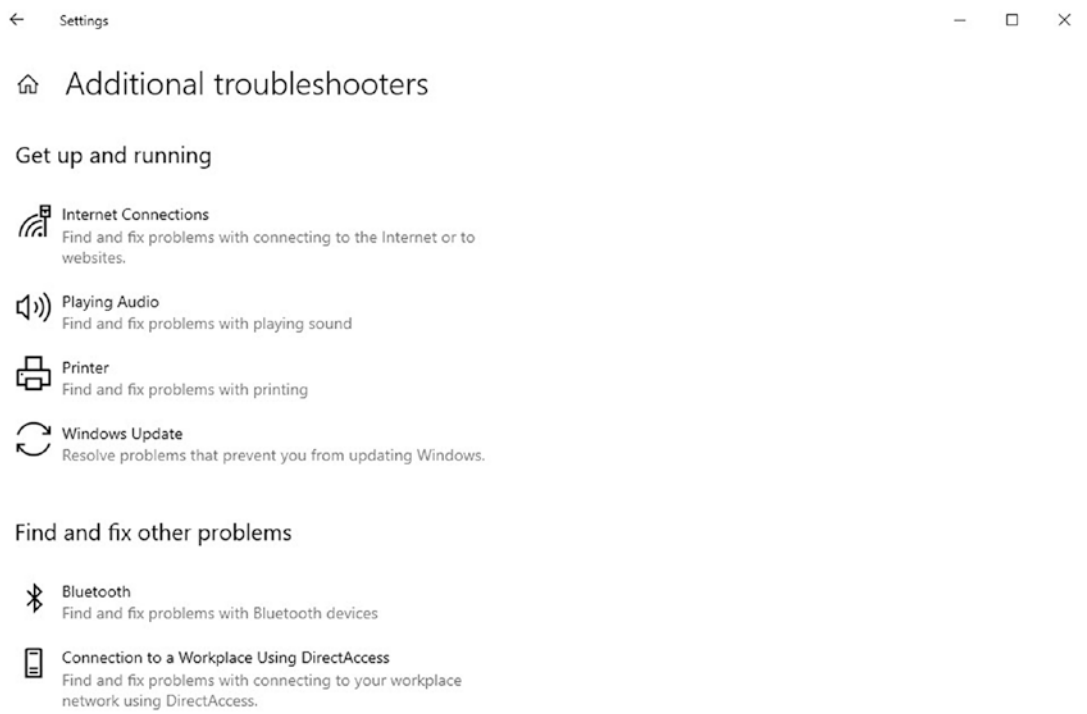


Figure 4-16. *The Troubleshooting options from the Control Panel*

The Troubleshooters are split into different sections: Bluetooth, Incoming Connections, Network Adapter, Search and Indexing, etc. When a troubleshooter has run, you will see usually a *View detailed information link* (see Figure 4-17), which can provide you with useful information on what it has found, or not found, and what it could or could not repair.

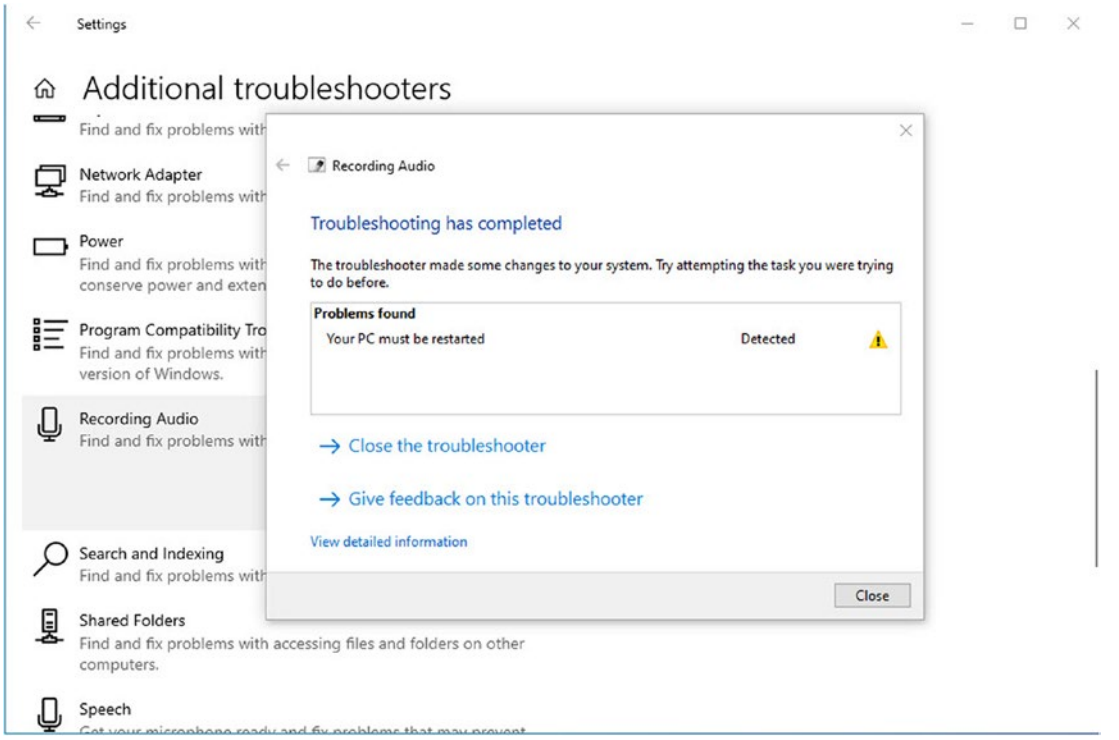


Figure 4-17. *Each troubleshooter is a self-contained wizard*

Each troubleshooter works in its own way. For example, some might ask you questions, while others will get on and try and find any problems they can. As I have already mentioned, the troubleshooters are best for everyday problems, as they work by resetting Windows and other components to their default state. They're not able to diagnose complex problems.

If you find that an Automated Troubleshooter doesn't exist for the problem you want to solve, a look on the Microsoft support website at `Support.Microsoft.com` can often reveal additional troubleshooters you can download and run, including for Microsoft accounts and the Windows Store.

Microsoft Answers, Service Status Site, and Being a Twit

Something I always encourage people to do before they contact support is to search online for a quick solution to the problem they are facing. By far the best place to go to find these quick solutions is the Microsoft Answers website, `answers.microsoft.com`. Here, Microsoft engineers and support staff, technical experts, and many of my fellow MVPs will quickly, and with easy-to-understand explanations, answer your technical questions and point you toward solutions; see Figure 4-18.

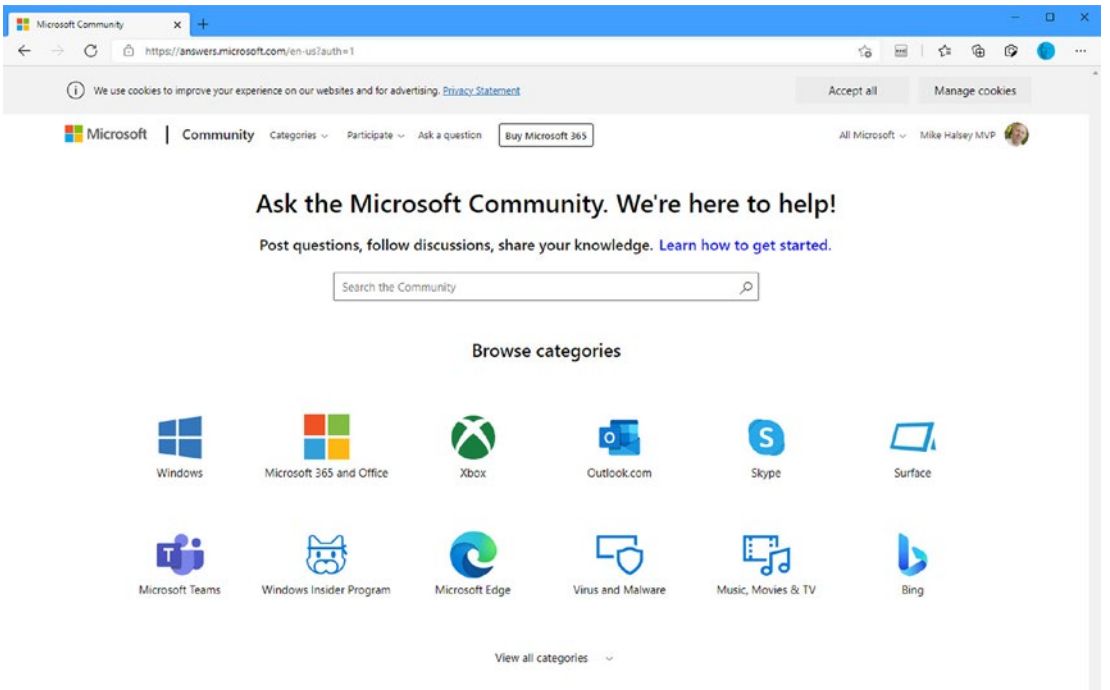


Figure 4-18. *Microsoft Answers is a great resource for finding help and guides*

You might find, for example, that the fix is extremely simple, or that it's not a problem on your PC because lots of other people are experiencing the same issue, or that Microsoft or a third-party company will need to issue a patch or driver update, in which case you'll need to be patient and keep an eye on the problem.

Anything can be searched for online, including error codes (they start with 0x…) and more generic problems. If you are encountering a problem with a Windows Update, new feature, app, or Microsoft service such as OneDrive or Microsoft 365, it can also be a good idea to check both Twitter and the Microsoft service status pages (`portal.office.com/servicestatus` for Microsoft 365, Outlook.com, and OneDrive.com); see Figure 4-19.

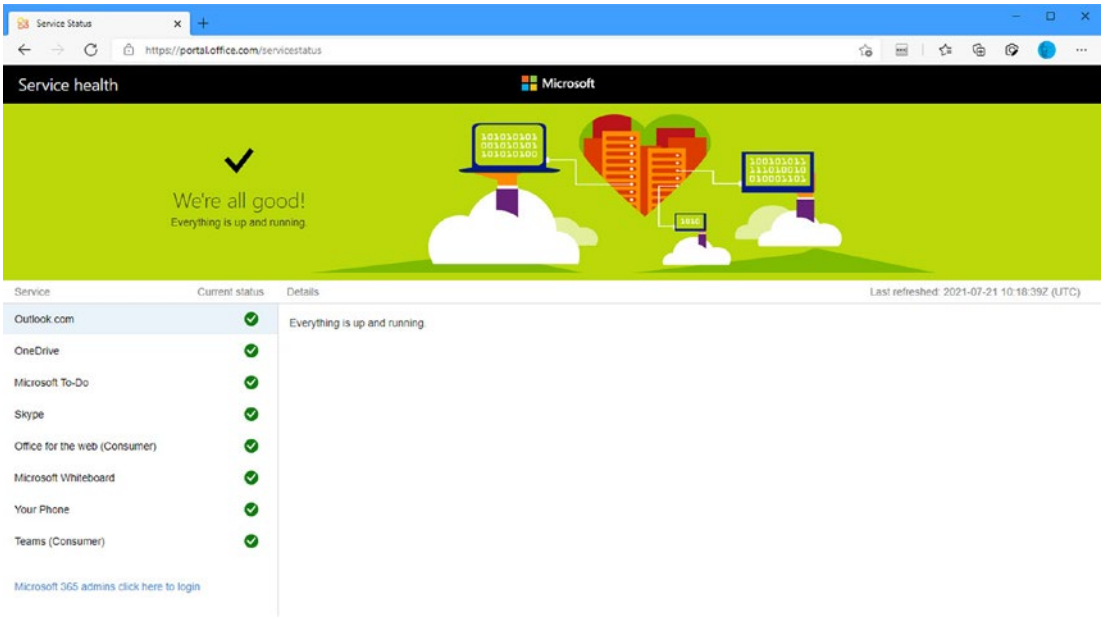


Figure 4-19. *Microsoft's office services status page is very useful*

Additionally, Microsoft's Azure cloud services have their own service status page, which you can find online at `status.azure.com`, and this provides both service and regional updates for all Azure services. This can be useful if you are trying to diagnose a problem that a Windows 10 machine is having connecting to Azure cloud services; see Figure 4-20.

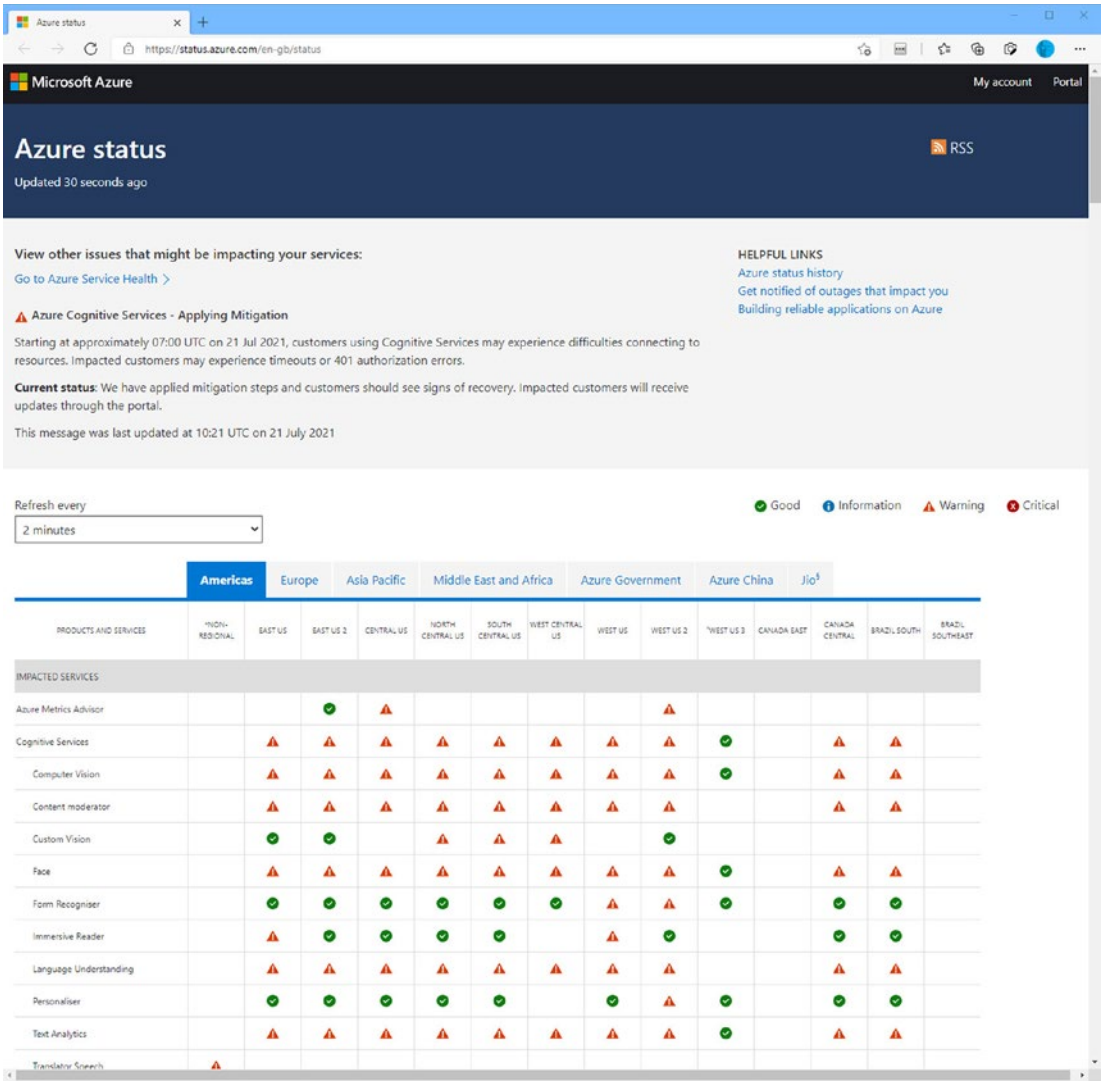


Figure 4-20. *Microsoft's Azure cloud services have their own online status page*

Third-party websites such as `isitdownrightnow.com` and `downdetector.com` also exist to help you see the current status of online services, though, as I have already mentioned, probably the best by far is Twitter, where a quick search for a name or hashtag will reveal that it takes just a few seconds for the masses to begin complaining when they can't get access to online services they need.

Summary

Clearly, some problems within Windows 10 can be fixed quickly and simply. Others can be searched for online for quick fixes, and, provided you know where to look, service status pages are available for all Microsoft, and many other, online services.

Sometimes though, quite often if I'm honest, you need significantly more detail and information about a problem in order to diagnose it. This can be especially helpful if you need to hunt through hundreds of online pages to find the one that applies to you, or if you need to send technical data to a support engineer (or if you are the engineer and need to request the information).

In the next chapter, then, we'll look at how you gather this information, what tools exist to help you get access to it, and how you can make sense of what can be some very technical information.

CHAPTER 5

Understanding Tasks and Events

It's one thing to have facilities that enable you to fix Windows and PC problems quickly, but this still depends on either you or Windows being able to identify the problem almost at the moment it's seen. If the issue is harder to identify, it doesn't mean you can't still repair the problem in short order, but it really helps if you know what you're looking for.

In Chapter 1 I detailed the Reliability Monitor, an incredibly helpful tool that is a brilliant starting point for diagnosing all types of problems on a PC. These include service and Windows component failures and crashes, app crashes, Windows Update or installation difficulties, hardware driver failures, and more besides.

What happens, though, if you want or need more detailed information about problems? Better still, what if you want to be alerted to the problem when an error or crash occurs? The good news is that Windows 10 includes tools that can do both of these things, and they're fairly easy to use as well.

The Windows Event Viewer

The Windows Event Viewer (sometimes called the event log) stores details of everything that happens in the OS, from routine operations to crashes and even Blue Screens of Death (which I now like to call the Blue Unhappy Emoticon of Death).

You can open the Event Viewer by searching for **event** at the Start Menu, or by clicking *Administrative Tools* in the Control panel, and then clicking the *Event Viewer* icon.

Introducing the Microsoft Management Console

This is probably a good time to introduce the Microsoft Management Console (MMC), which is a standard window layout used by the Event Viewer and many other Windows tools and utilities that I'll detail throughout this book, including the Hyper-V virtualization utility.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_5

Figure 5-1 shows the main Event Viewer window. This consists of three vertical panels, each of which I'll cover in more detail shortly. To summarize what you're seeing, however, I'd encourage you to open the Event Viewer on your own PC at this stage and have a look around as you read this: the left panel contains the main categories of views of options available, the right panel contains context-sensitive commands and options, and the central panel contains the main information provided by the particular tool or utility you have opened.

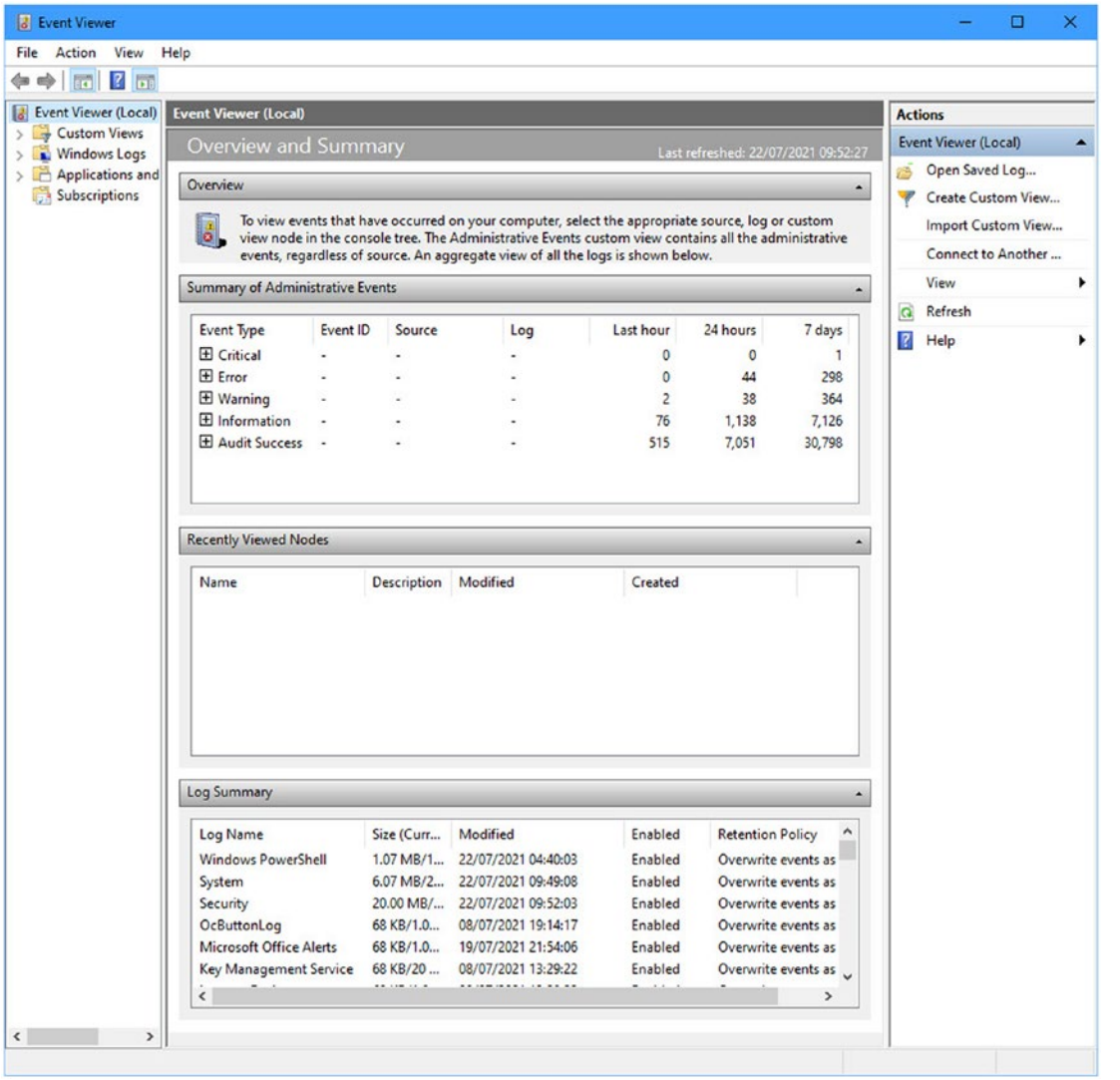


Figure 5-1. *The Event Viewer is split into three vertical panels*

The Category/Views Panel

Obviously, depending on what MMC you have open, the information displayed in the three vertical panels will be different. In the Hyper-V MMC, for example, the left panel will display the available root PCs and servers that can contain Virtual Machines (VMs). The Local Security Policy and Group Policy MMCs will display the different groups you can specify policies for. The Advanced Firewall will display options for inbound and outbound security rules, and the Event Viewer, seen in Figure 5-2, displays the different category areas that Windows stores event logs for.

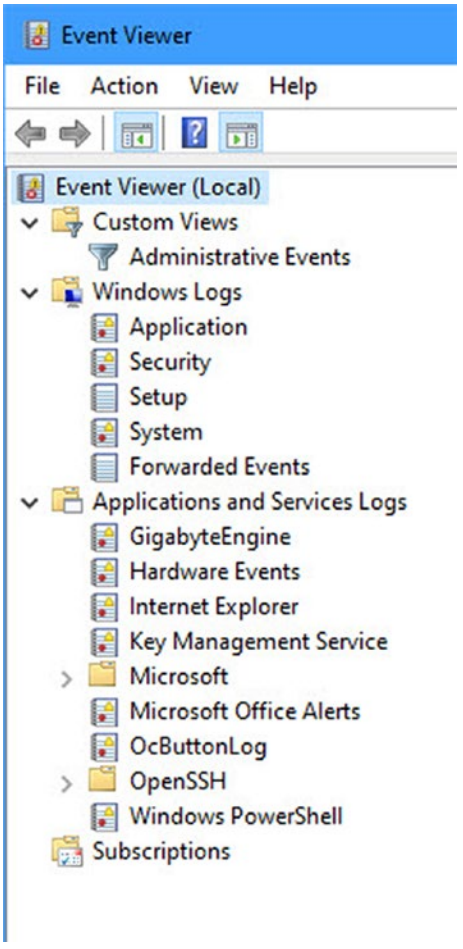


Figure 5-2. *The Category/Views panel is always to the left of the MMC*

In the Event Viewer, the options available in the left side panel allow you to filter the event logs viewed by specific types. These are categorized as follows:

- **Custom views**—created by you to monitor specific events on a PC
- **Windows logs**—contain event log information for Windows events only
- **Applications and services logs**—contain logs for installed apps and both Windows and third-party services
- **Subscriptions**—allow you to collect logs from multiple remote computers and virtual machines and store them to view locally

The Actions Panel

The Actions panel sits to the right of MMC windows and contains both global and contextual commands and options; see Figure 5-3. These will change depending on which MMC you have open and what you are currently doing in that MMC.

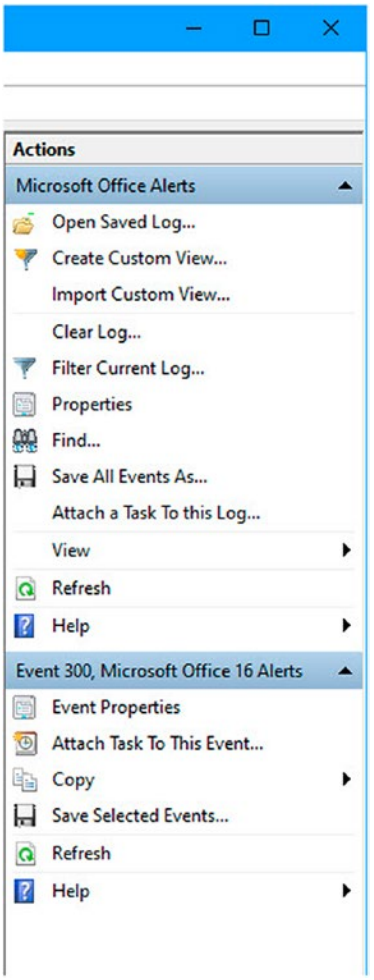


Figure 5-3. *The Actions panel sits to the right of the MMC*

For example, in the Hyper-V MMC, the options will include creating VM and network switches. In the Disk Management MMC, they will include disk and partition management tools, and in the Event Viewer, they will include ways to interact with, create, save, and view the properties of events and event logs.

The Main Events View

The central panel in the Event Viewer is where the event logs themselves are displayed. When you click the root option in the left panel *Event Viewer (Local)*, you will see the central columns separate into four collapsible panels; see Figure 5-4.

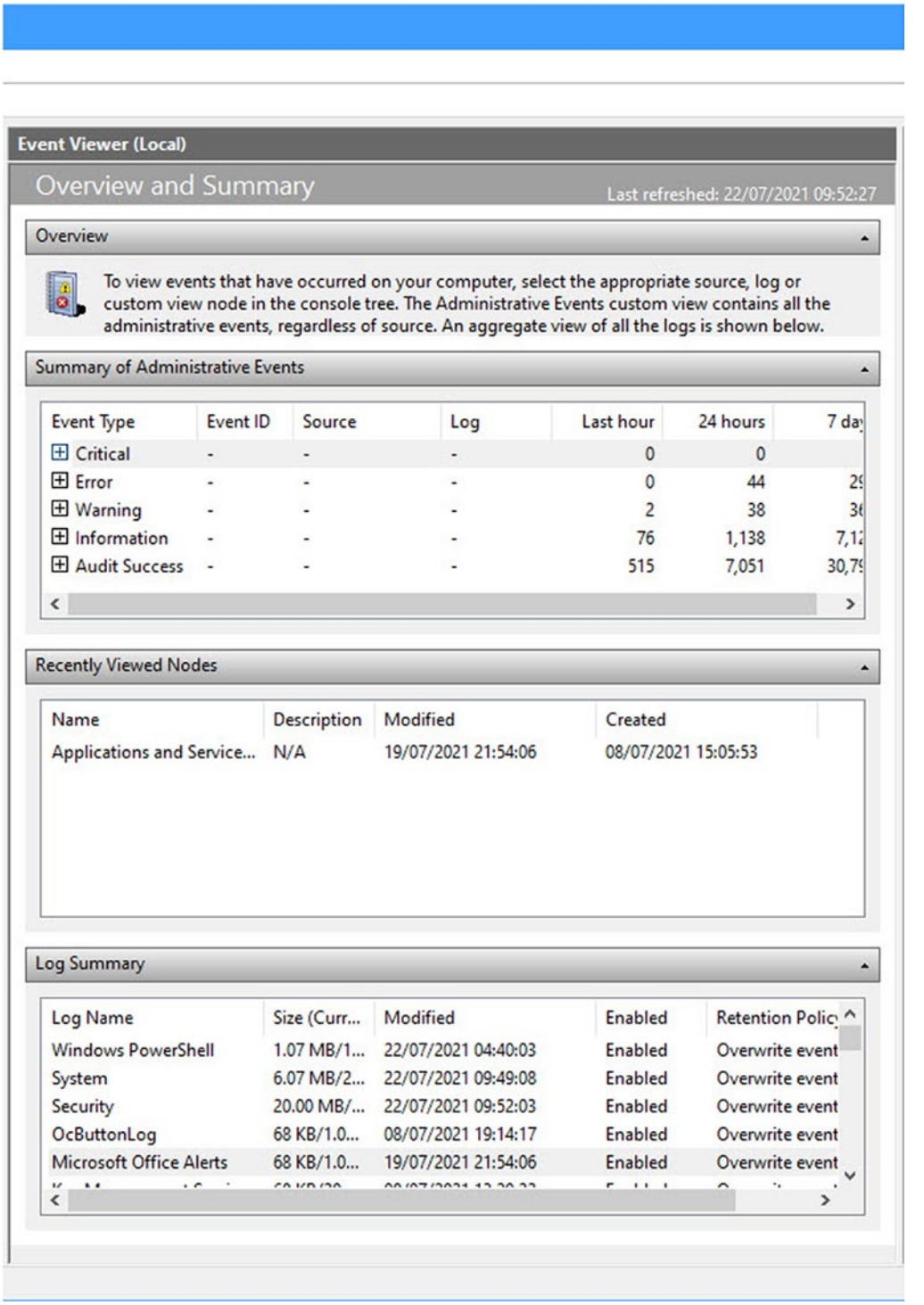


Figure 5-4. *The central panel in Event Viewer displays the event logs*

- **Overview**—displays a text description of the view you have open
- **Summary of administrative events**—separates all the event logs stored on the PC into six different categories:
  - **Critical** errors are the ones that result in a sudden PC stop, such as a Blue Screen of Death, a Windows core (kernel) component failure, critical driver stop (such as a critical graphics driver error), or a power problem.
  - **Error** messages are generated when a Windows component, app, or service fails.
  - **Warnings** are generated when a Windows component, app, or service generates a message or error that does not cause a stop event to occur.
  - **Information** is generated whenever a service or component starts, or when an event such as an update, installation, or event in an app is recorded.
  - **Audit success** information is generated when a successful routine operation, such as starting up the PC and booting to the Windows desktop, completes.
  - **Audit failure** events are generated when a routine operation does not complete or reports an error.
- **Recently viewed nodes**—quick links to the events you have been viewing most recently
- **Log summary**—provides technical information about the currently displayed event or events

Making Sense of Error Logs

You open event logs by clicking the event categories until you arrive at a list of recorded events, and then click one event to select it. The view will then change to a list of the events for that category in the top center of the window, with details about the currently selected event below it; see Figure 5-5.

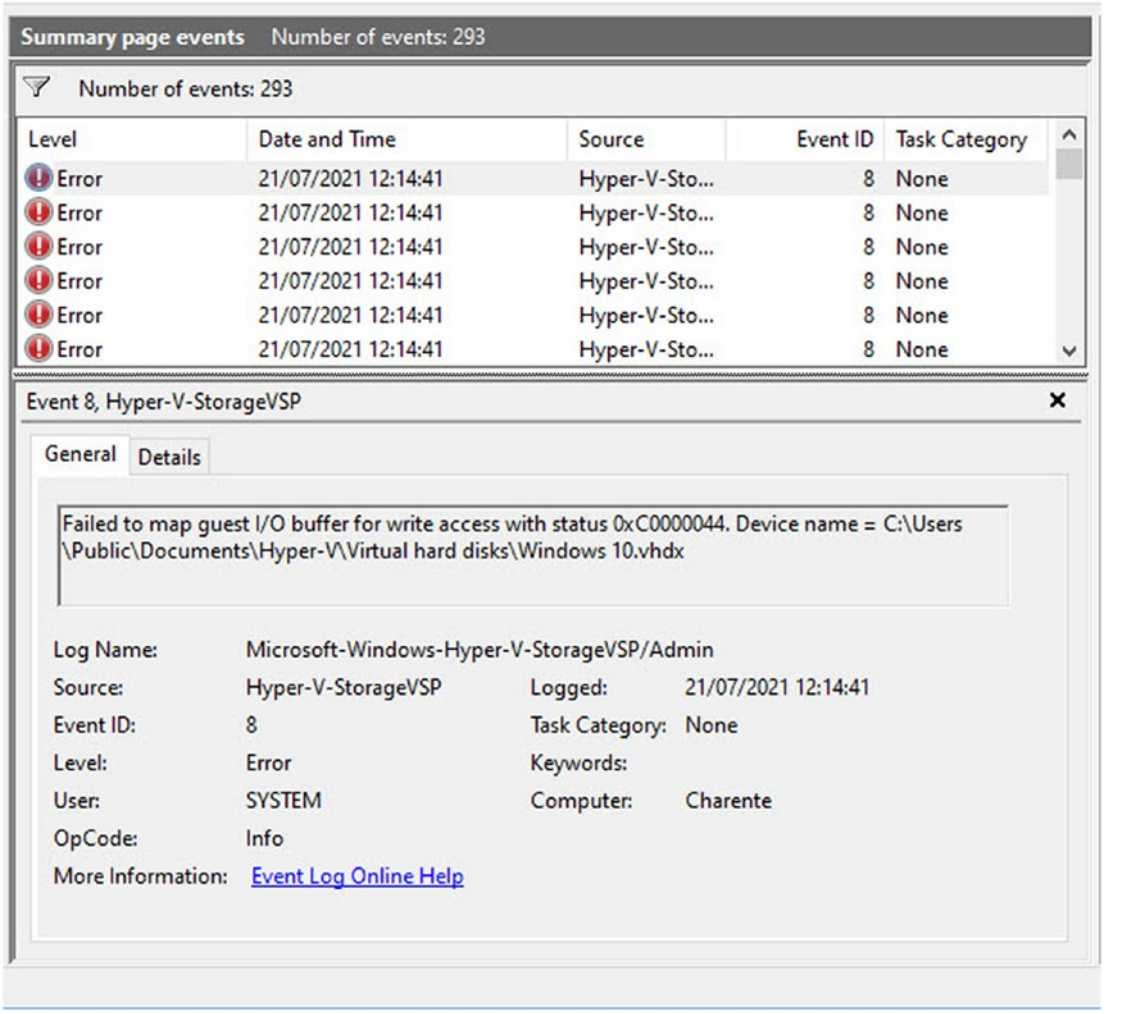


Figure 5-5. *Opening an error log displays verbose and specific details of the event*

So how do you go about deciphering details of an event in Windows 10? When it comes to diagnosing and troubleshooting problems, there are several useful things you can look for:

- **Frequency of the event**—This can be gathered from checking the event ID (55 in the example given) and matching it to the number of times, and the frequency with which the event occurs. In this case, a disk file structure error is being repeatedly discovered. Examining the frequency of events might reveal that the error being reported isn't new but has been occurring for some time.
- **Verbose description of the event**—This is detailed at the top of the *General* information panel. A plain-text description of the event will be given; this can sometimes give you all the information you need on its own. In this case, I have a write access issue with a virtual machine file.
- **Error code**—These always start 0x; in the preceding example, it's 0xC0000044. Error codes can be incredibly useful when searching the Internet to find solutions to problems.
- **App or service file name and version numbers**—In Figure 5-6, you will see an error reported when the Skype win32 app has crashed (which was very annoying at the time, as I was preparing for an important webcast with a major firm in the United States). Here we have extremely detailed information, including a 0x error code. Additionally, the event log contains details of the exact apps and services, and their file paths, which have crashed. You can also see at the top of the information panel the exact version numbers for those files, in this case *SkypeHost.exe* and *SkyWrap.dll*. Searching for information about file version numbers online can often reveal other people having issues, and perhaps suggestions for more stable installations you can use instead.

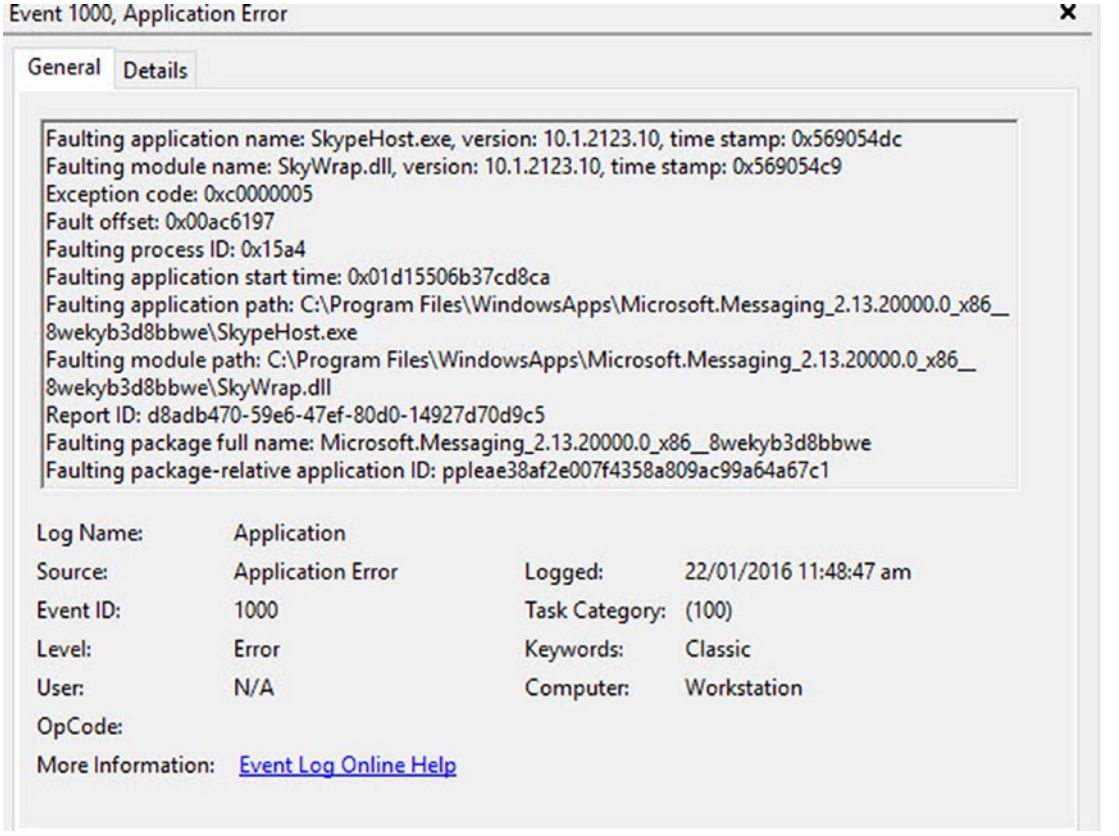


Figure 5-6. *Extremely detailed technical information can be gained from the Event Viewer*

Note The *Details* tab in the Event Viewer, when a specific log is displayed, shows the information in a friendly or XML view that can be copied by right-clicking it (no selection is necessary), and then pasted into an email or other document for a support technician.

Creating Custom Event Views

If you are searching for specific information—perhaps you are asking a user to send you event information from his own PC—you can create a custom view. This will create a subset of the whole event log that can be viewed in the Event Viewer under the *Custom Views* section or saved as a file and exported via email or another method to be read on a different PC.

Clicking *Create Custom View* in the Actions panel will allow you to filter the event log using a wide variety of methods; see Figure 5-7. You can filter your custom view in the following ways.

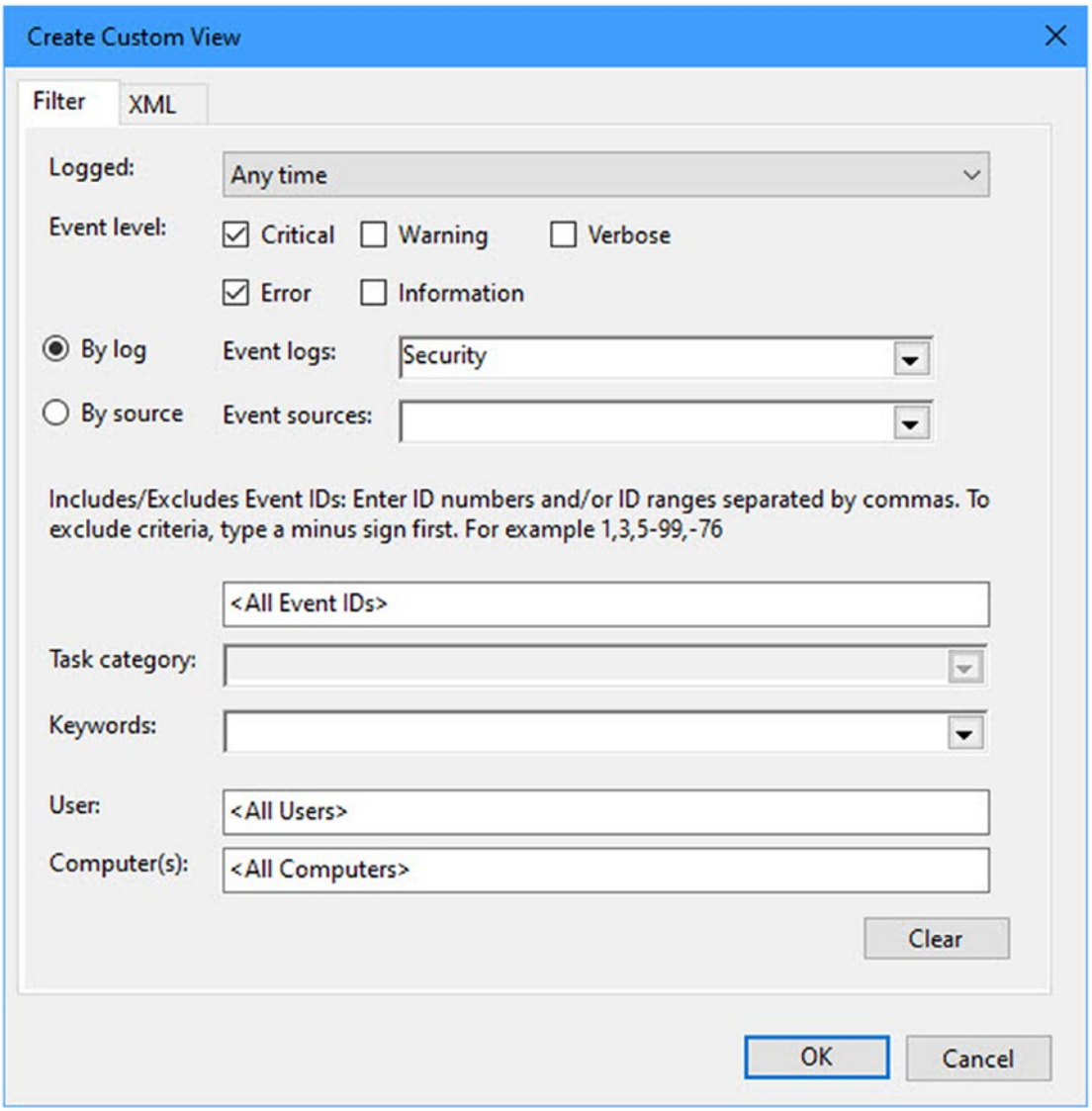


Figure 5-7. *You can create custom event views in Windows 10*

- **Logged**—allows you to capture events from any time, the last hour, last 12 hours, last 24 hours, last 7 days, last 30 days, or you can specify a custom date and time range.
- **Event level**—lets you specify the error types you want to include from Critical, Error, Warning, Information, or Verbose information.
- **By log**—lets you specify the events to keep by their main category, the categories seen in the left panel of the Event Viewer; these include Windows logs, Applications and Services logs, and so on.
- **By source**—lists a vast number of Windows services and features from which you can choose; for example, you might want events about the narrator, various Hyper-V services, or specific kernel (core operating system file) errors.
- **Event IDs**—you can specify <All event IDs>, the default option, or one or more specific event IDs.
- **Task Category**—this is not displayed for all options, but the Task Category is displayed to the right of the event ID in the events list and might be either a number or a text description.
- **Keywords**—specific error descriptions you want to select; you can choose from All keywords (the default option), Audit failure, Audit success, Classic, Correlation hint, Response time, SQM, and WDI Diag. When you are viewing the details of an error, the keywords associated with that error will be displayed in the General error details. Selecting keywords can help you find related errors and crashes.
- **User**—helps you choose between <all [the] users> on the PC and a specific user if more than one person uses the PC and only they are experiencing problems.
- **Computer**—similar to users, but helps you choose which computer you wish to view events for. This can be used when subscribing to events from remote computers, which I shall cover shortly.

Tip When you are viewing a custom view, you can click *Filter Current Custom View* in the Actions panel to narrow the information contained. This can help narrow your searches for problems.

Creating Event Subscriptions

If you are managing multiple PCs on a domain or by using Azure AD, you can subscribe to event logs from multiple computers, and these events will then appear as custom logs in the *subscriptions* section of the Event Viewer.

To have a subscription, both the **Windows Remote Management (winRM)** and **Windows Event Collector (wecsvc)** services must be running on both the machine sending and the machine collecting the logs. In addition to the method detailed in the following, you can also manage these in the Services panel, which I will detail in Chapter 19. You can then set up a subscription by following these instructions:

1. Click *Command Prompt (Admin)* in the **Win + X** menu, and click through the UAC security notification.
2. On each source PC, type `winrm quickconfig` and press Enter.
3. On the collector PC, type `wecutil qc` and press Enter.
4. Open *Computer Management* from the Administrative Tools on each of the source PCs:
    a. Select *Local Users and Groups* in the left side panel of the Computer Management Console, and then click *Groups* in its drop-down.
    b. Right-click in a blank space in the central panel, and then click *New Group* from the context menu that appears.
    c. To add the collector PC, click *Add*, and then in the dialog that appears, click *Object Types* and select the *Computers* check box.
    d. Add the collector PC's name to the local groups information, as you would add a local user account.

5. Back in the Event Viewer on the collector PC, click *Subscriptions* in the left panel and then *Create Subscription* in the Actions panel.

6. In the wizard dialog that appears (see Figure 5-8), add a subscription name and description, and then select the computers you wish to collect logs from.

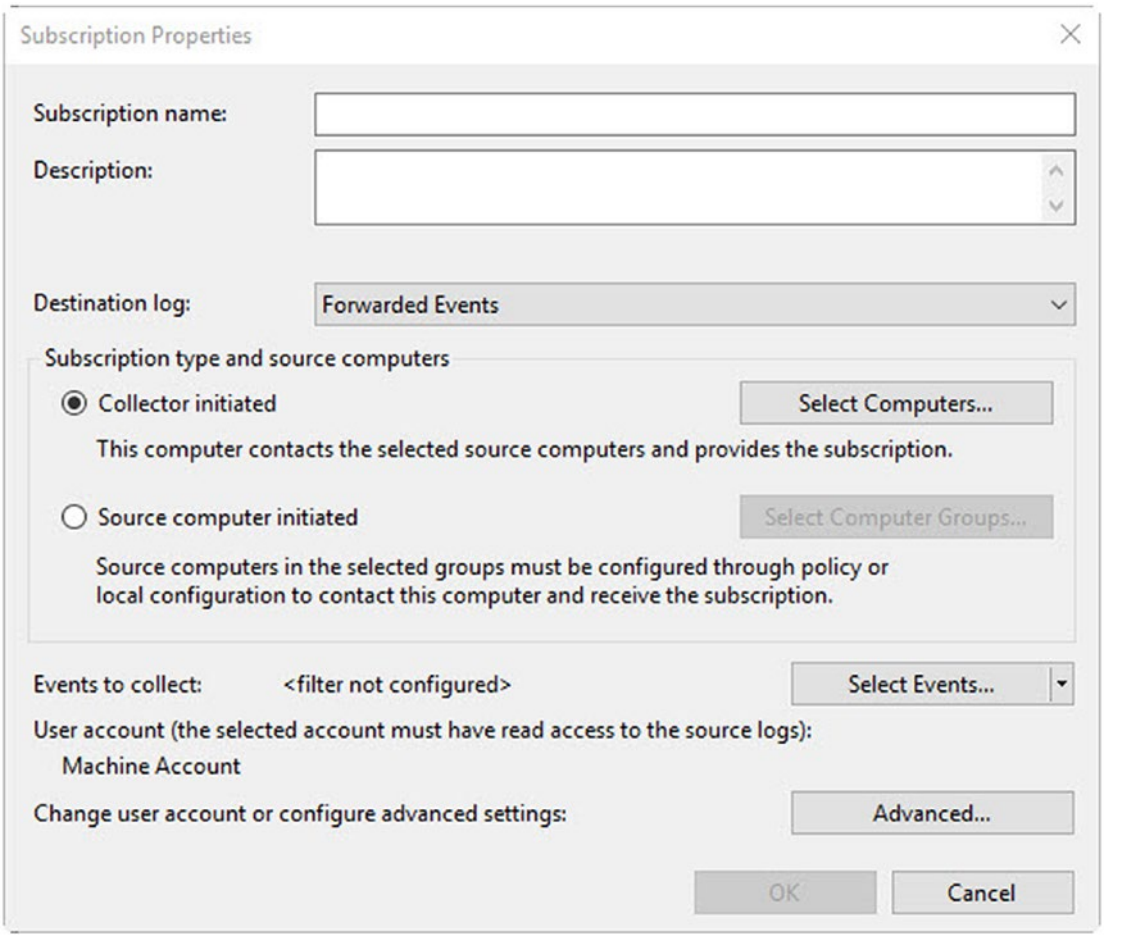


Figure 5-8. *Event subscriptions are created through a wizard interface*

7. Click the *Select Events* button to configure the Event Log collector as detailed in the "Creating Custom Event Views" section of this chapter. Alternatively, you can click the down arrow to the right of this button and import an existing custom view.

8. Optionally now, click *Advanced* to specify the user account this subscription is to be for (only required if more than one user account is found on the collector PC), and any bandwidth restrictions you wish to put in place. Note that the `winrm quickcfg` command detailed in step 2 also needs to be run on the collector PC if you want to change the Delivery Optimization (bandwidth) options, and if you are specifying a specific user on the collector PC to use the subscription, that user will need to be added to the accounts on each source PC as well.

Attaching a Task to an Event

Sometimes when an event occurs, you want the user on the PC or a support person to be notified, perhaps even a PowerShell script or a repair utility to automatically run to fix the issue. In the Event Viewer, you can do all of these things.

With an individual event selected (you can also attach tasks to custom views to perform an action whenever something new is added), click *Attach Task to this Event* (or Attach Task to this Custom View) in the Actions panel. This will display a wizard dialog.

At the first page of the dialog, check that the event name is correct, or give the task a custom name, and then give the task a verbose description; see Figure 5-9. This can help people identify what the task is for should it no longer be needed.

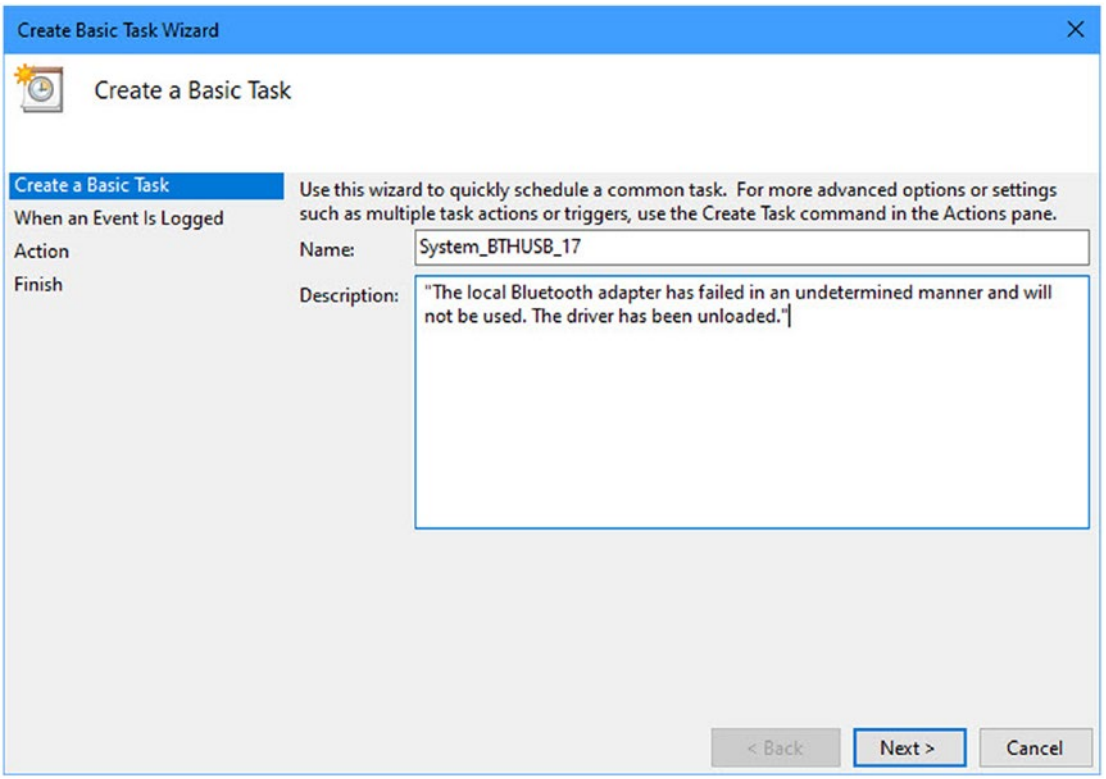


Figure 5-9. *You need to give a task a name, and you may also give it a description*

Click Next and the next screen is likely going to be grayed out as the event information has already been selected; see Figure 5-10. If the boxes are not grayed out, select the log, source, and event ID information you wish to create the task for.

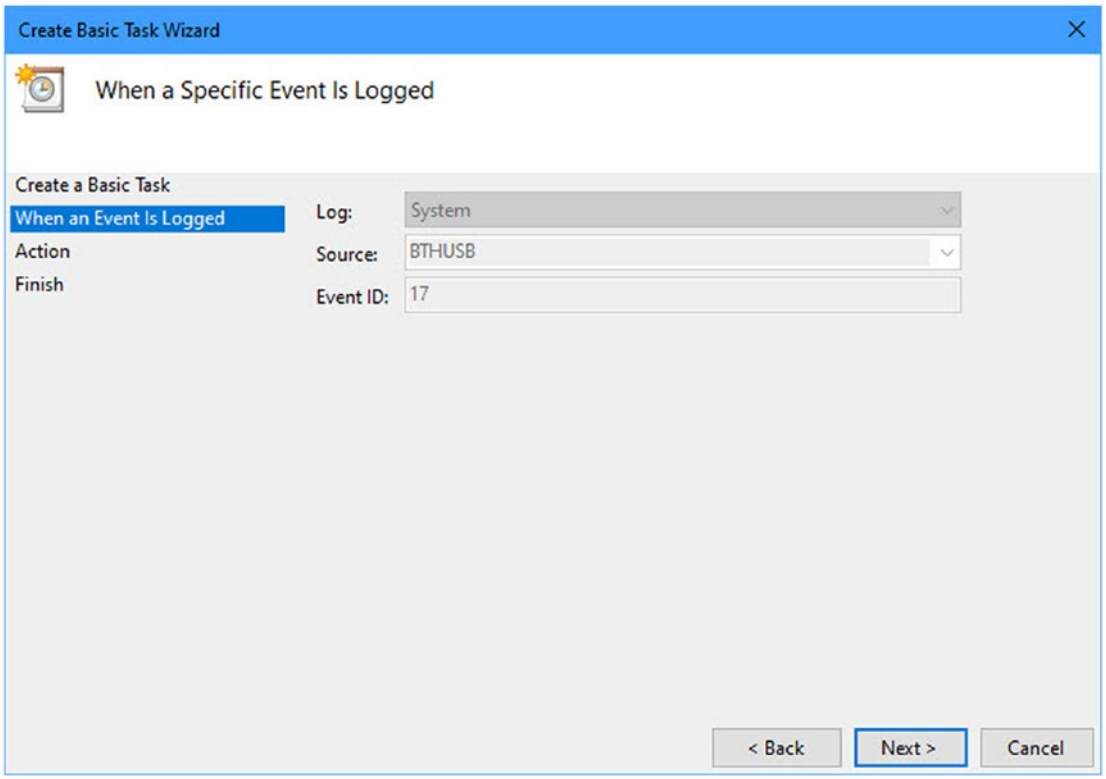


Figure 5-10. *The event information is usually selected for you*

At the next screen, you can choose if you want the task to start a program, send an email, or display a message; see Figure 5-11. We'll look at each of these in turn.

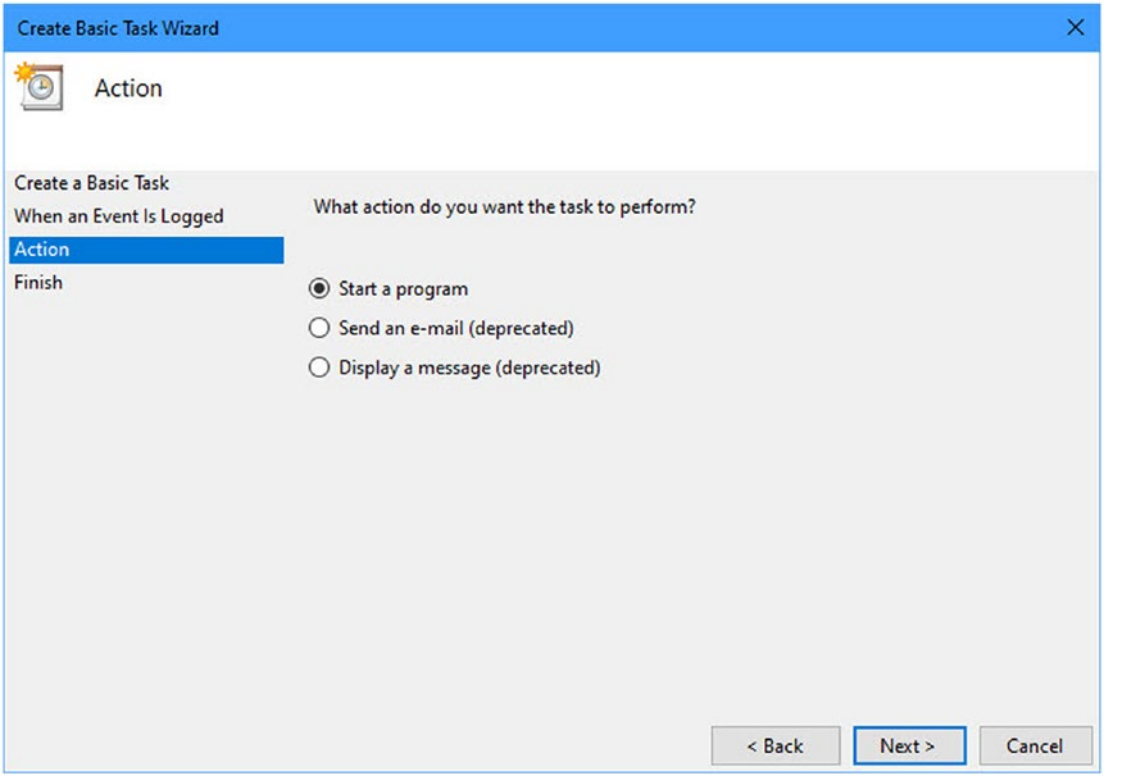


Figure 5-11. *At the next screen, you decide what you want the task to do*

If you choose to run a program, you can choose an app or a script (command line or PowerShell) to execute when the event occurs. This can include an autorepair script or utility that you have been provided with, or one that you custom-write yourself; see Figure 5-12. You can add command-line arguments if required.

It's worth noting that both the send and email and display a message options are marked as deprecated. This means that they're no longer going to be developed further and that they could be removed from Windows 10 at a later date. In fairness though, they were deprecated when Windows 10 was first released and they're still present, so it's safe to assume they're likely going nowhere fast.

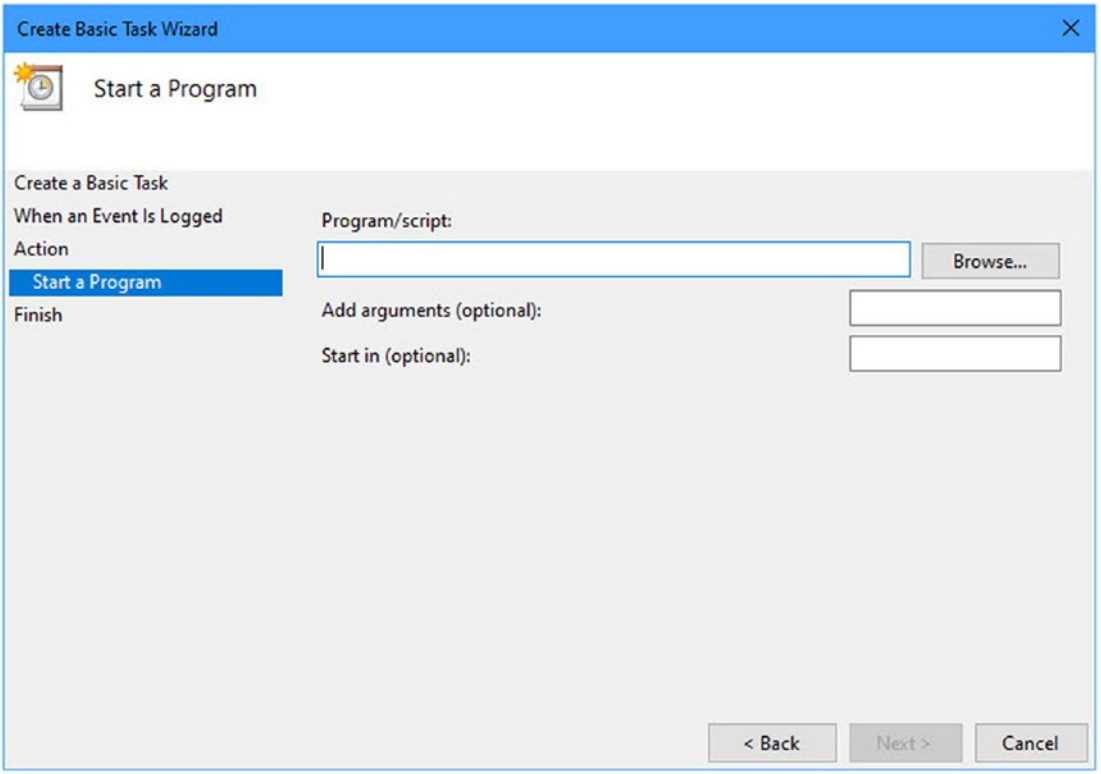


Figure 5-12. *You can choose a program or script to run on the event occurrence*

Sending an email doesn't require an email app to be installed on the PC; see Figure 5-13. You specify the details for the email, which must contain a fixed message, and the SMTP (email out) server. Additionally, you can attach a file to the email, such as an error log. I will detail where these can be found in Chapter 27.

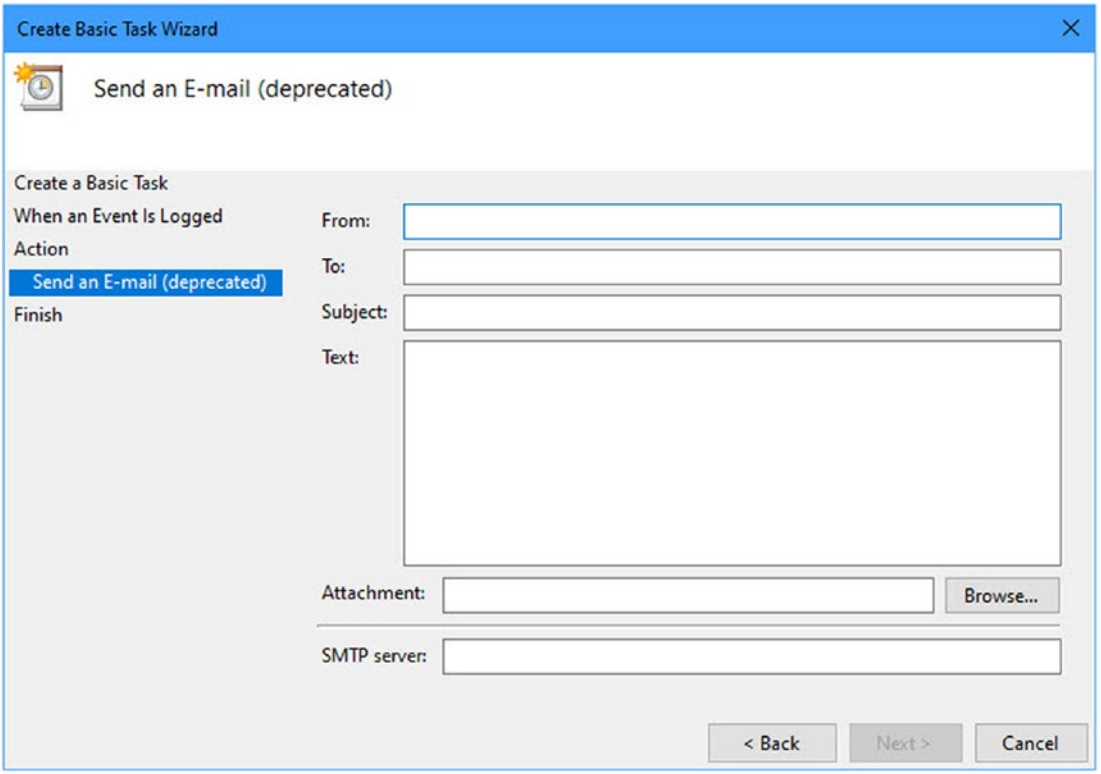


Figure 5-13. *Sending an email does not require an email app to be installed on the PC*

You can also choose to display a message on the user's screen as a pop-up dialog; see Figure 5-14. This could perhaps ask the user to stop what they're doing and call Support right away, so that up-to-date logs can be collected, but also so that support can be told exactly what it was the user was doing at the time the event occurred.

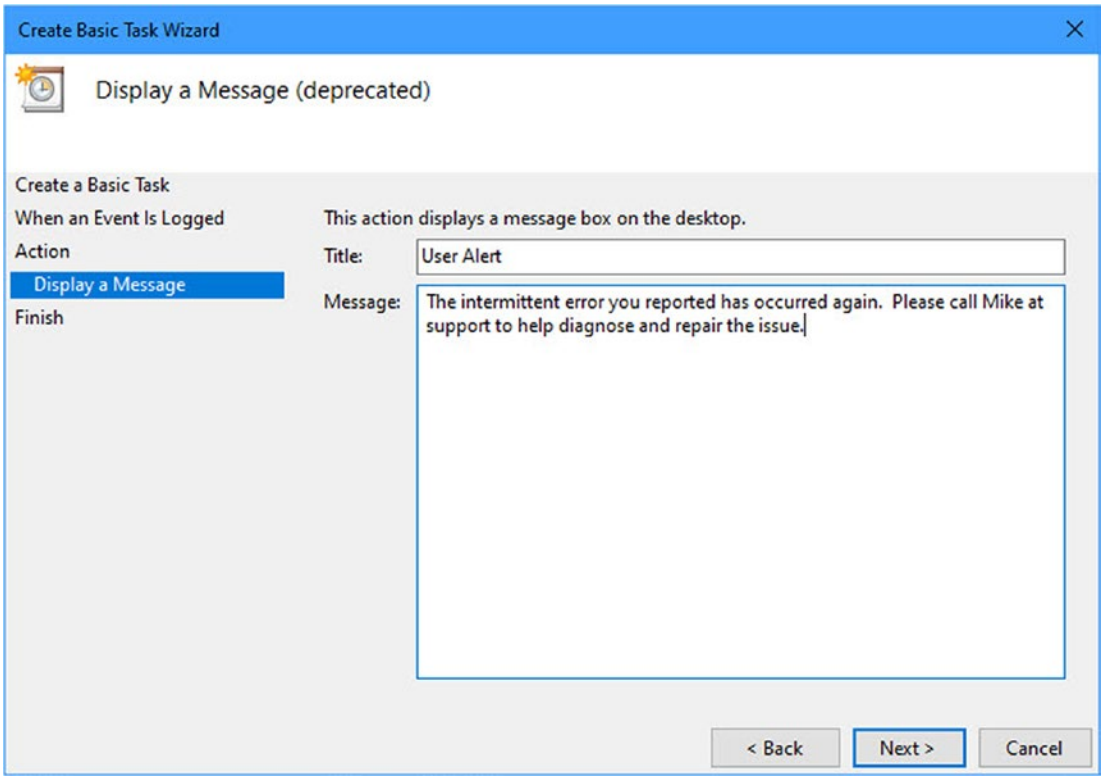


Figure 5-14. *A message can be displayed on the user's screen*

Note Tasks can be managed in the Task Scheduler MMC: search for **task** in the Start Menu or Cortana. Click the *Event Viewer Tasks* section in the left panel, and you can right-click your created event tasks to disable them, export them (for use on other PCs), change their properties, or delete them when they are no longer required.

Saving, Exporting, and Importing Event Information

Sometimes, the information in the Event Viewer will need to be sent to a third-party support person so that you can digest it properly on the train home. You can save any and all information in the Event Viewer as Event Viewer (.evtx) files. These can then be read in a standard web browser.

In the Event Viewer, select one or more events (you can select all events in a list by clicking the top event, then holding **Shift** when you click the bottom event, or by holding **Ctrl** and clicking all the events you wish to highlight) by right-clicking them and selecting *Save Selected Events* from the drop-down menu that appears; see Figure 5-15. You can also save all events from a custom view by right-clicking the custom view in the left panel.

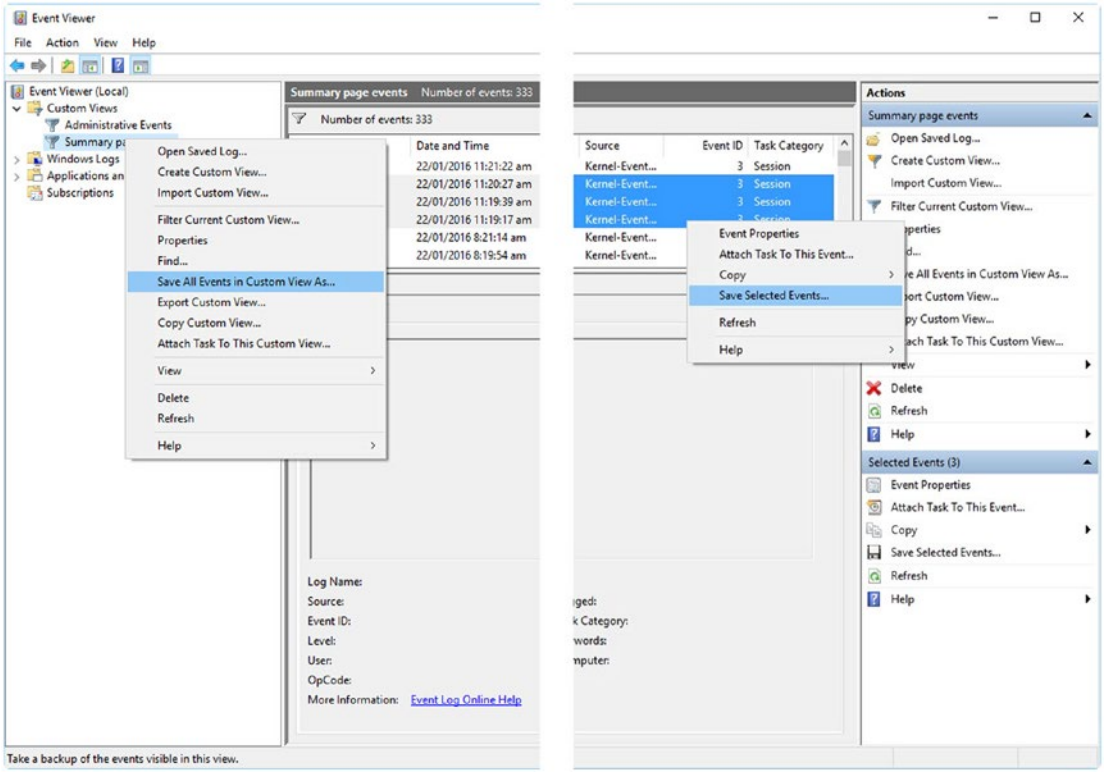


Figure 5-15. *You can save events as XML data in the Event Viewer*

This file can be saved or sent to a support technician and opened by clicking *Open Saved Log* in the Actions panel of the Event Viewer on any Windows PC. It will then appear in the *Saved Logs* section of the Event Viewer, where it can be viewed and reviewed.

Summary

The Event Viewer is a huge repository of useful information, and just about everything you need to know to diagnose and repair problems, crashes, and instabilities can be found within its logs. This is why it justified an entire chapter, all to itself.

When it comes to understanding the inner working of the PC file system, the Event Viewer can be indispensable, though I will detail the Windows file system in full in Chapter 27. In the next chapter, however, we'll look at PC hardware, including all the different technologies you will encounter as an IT pro.

CHAPTER 6

Understanding PC Hardware

The Windows operating system as installed on your PC is extremely complex, literally consisting of tens or even hundreds of thousands of configuration files, shared APIs, drivers, programs, and more besides. The hardware in our PCs isn't any less confusing, and even if you're using a convertible tablet or ultrabook that's not serviceable by the user because the case is sealed and all components are soldered onto the motherboard, there are still hardware factors you need to know about when troubleshooting problems.

BIOS and UEFI

BIOS (Basic Input, Output System) and UEFI (Unified Extensible Firmware Interface) are the place to start. They exist in ROM (Read-Only Memory) on a chip on the PC's motherboard, and they are referred to as firmware. The firmware is the software layer that exists between the operating system and the PC's hardware; its job is to tell the OS how to communicate with the hardware. Think of it as a hardware driver, as there are similarities, but one that's required by the operating system at the very beginning of startup, so that the OS knows where to find and how to spin up the hard disk and other hardware components, such as the screen, so that it can load its core files and interface.

Firmware shares more in common with the solid-state drives (SSDs) we use in PCs these days than with memory chips, in that it's nonvolatile. This means that like the storage chips on SSDs, but unlike chips on our PCs memory cards, its contents aren't wiped when the electricity supply is switched off.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_6

BIOS was invented in 1975 by a man called Gary Kildall (yup, this was back when one person could invent a technology that we now all take for granted[1]), when it was first used with the CP/M operating system that he also created. IBM created their own BIOS in a deal with Kildall to offer CP/M with their first PCs. The story of how IBM originally contacted Kildall, and the story about how Microsoft's MS-DOS became the dominant PC operating system, which was far more popular with end users than CP/M, has fallen into tech mythology; you can read more about it at http://pcs.tv/1NupOJv.

What I believe to be the far more interesting story is how IBM-compatible machines (and the PC market as we know it) first came about. IBM was unwilling to license its BIOS to other companies, but the Compaq Computer Corporation really wanted to release IBM-compatible PCs. They couldn't just copy IBM's BIOS, however, as that would have infringed copyright, so instead they set up two teams to manage the task.

The first of these teams reverse engineered the IBM BIOS, making detailed notes about what it did and how it operated. The second team, working from the notes from the first team, but without having any access to the IBM BIOS themselves, wrote a new BIOS that would perform all the same operations. Because Microsoft had deliberately signed a deal with IBM that allowed them to sell MS-DOS to whoever they wanted, the PC compatibles market was born, and no copyright was infringed, at least not according to the law.

IBM did eventually publish the full details of its BIOS, and several other companies including Phoenix Technologies and Award Software created their own compatible versions that are still seen on billions of PCs and laptops in use today.

BIOS served PC makers well for 30 years (even though it was only supposed to be used for about 7 years before being replaced). The problem with BIOS is that it wasn't written to support all the technologies that came after it, such as USB. This made it slow to access and identify hardware at the PC's startup, and its operation on a ROM chip with no inbuilt security also made it vulnerable to attack by malware. Some of this malware would corrupt or wipe the BIOS completely, rendering a PC unusable unless complex fixes were implemented and the firmware reflashed.

[1] One of my personal favorite heroes of tech is the Hollywood actress Hedy Lamarr. She starred in many blockbuster films as a leading lady between 1938 and 1958, but was also a scientific genius, creating radio technologies for the US Navy that are still used in Bluetooth and Wi-Fi today. I can recommend the documentary "Bombshell" (Reframed Pictures, 2017) which is a fascinating look at her life and achievements.

UEFI was the solution to the woes of the BIOS. It came about from a forum consisting of major technology companies including Microsoft, Apple, Intel, AMD, and Dell, and the companies behind the currently in use BIOS firmware. The UEFI specification was first written by Intel, and it permitted a more flexible, configurable, scalable, and, above all, faster firmware system for PCs; it could also include advanced security to protect both itself and the operating system from malware.

You will typically access the BIOS or UEFI on a PC by pressing Esc, Del, F2, or F12 on your keyboard at PC startup, but tablets will commonly have a button combination to press such as power and volume up. You should check the documentation that came with your device, as the method used will vary depending on the PC you use. The UEFI system can also be accessed from within Windows 10 (and from a USB Recovery Drive). To do this, open the Settings app, then click *Update & security*, then click *Recovery*, and then click the *Restart now* button in the Advanced Startup section. When the boot options menu appears, click *Troubleshoot*, then click *Advanced Options*, and you will see a *UEFI Firmware Settings* button.

BIOS Virus/Malware Attack

As I have already mentioned, one of the biggest issues with BIOS is its complete lack of any type of security. The only security it has, in fact, is User Account Control (UAC) in the host OS blocking malware at the user level. Given that the BIOS is essential in order to get Windows to start on the PC, however, means that it's *very* vulnerable to attack. There are several different ways to troubleshoot and repair BIOS systems on PCs, and this will depend on what's wrong with the BIOS.

It's actually very rare these days for viruses to attack the firmware on PCs. There are several reasons for this, including that UAC on PCs since Windows Vista is extremely good at defending against viruses. There's also the point that every PC sold since the release of Windows 8.1 has a UEFI firmware system, which was mandated by Microsoft. Malware writers these days simply don't want to take down our computer systems, however. In fact, they need our computers operating so they can either get access to, and steal, our personal data or to hold us to ransom for it, or to use the PC as part of a mesh network to attack companies and governments with Distributed Denial-of-Service (DDoS) attacks.

That isn't to say that a direct malware attack on a PC's BIOS isn't still possible in some circumstances. Let's say you work for a company or a government department that provides or manages critical infrastructure for a city or perhaps an entire country. This can include cellular networks; Internet access; water, rail, and road; networks; electricity; gas; and even nuclear power. Both governments and a very small number of hacking groups are regularly, perhaps even constantly, trying to disrupt these networks: perhaps to destabilize a country with whom they disagree or to slow down the ambitions of another, and we do hear about these skirmishes between nations on the television news from time to time.

This becomes important when you recognize that critical systems require incredibly robust and stable software and operating systems. By this, I am referring to software and operating systems that have proven themselves reliable over very long periods of time. This means that this infrastructure often runs on very old Windows versions and very old software. Windows XP, which fell out of all support from Microsoft in 2014, is still commonly used by companies, governments, and military forces around the world. Indeed, it was only in the early 2000s that militaries in the United States and United Kingdom began to migrate their systems away from Windows NT 4, which had become known as "Windows for Warships."

These older operating systems, software, and BIOSes are significantly more vulnerable to attack than a modern PC with Windows 10 and UEFI firmware, despite additional security always being put in place at a network level. The end result is that they present a very tempting target for hackers and government agencies, though it's helpful at least that these PCs don't tend to be restarted very often.

Should a BIOS attack take place, however, or should one be possible on your system, you should make sure you keep a copy of, or a quick link to, the firmware flashing utility or dedicated malware removal tool on the motherboard manufacturer's website. These can often find themselves removed from the Internet as older hardware falls out of general use (which is why keeping your own copy of the firmware flashing tool is necessary). You will generally run this from a floppy disk (remember those?) or from a Flash Drive in a dedicated port on the motherboard at the PC's startup after resetting the BIOS, which I'll talk about in a minute.

Resetting BIOS and UEFI Firmware

While it's not uncommon for BIOS firmware to become corrupt on desktop PCs, it's much less common for UEFI firmware. If you have a small spike in the electricity supply, or if the power is suddenly cut to the PC, the resultant electrical activity can corrupt the firmware as stored on the BIOS chip. Also, if you're updating the BIOS on a PC and the power fails, this too will (fairly obviously) corrupt the BIOS. In this last circumstance, you'll also need the reflashing tool you can run from a floppy disk or USB Flash Drive.

Figure 6-1 shows the method by which you can reset the BIOS or UEFI on a desktop PC. There is a battery and what's called a Clear CMOS (complementary metal–oxide–semiconductor) jumper. You can usually reset the BIOS or UEFI on a PC by moving this jumper, which covers two out of three available pins, to the other end of its base (still covering the center pin), and leaving it for a few seconds before putting it back where it was before. You may also find it helpful to remove the battery.

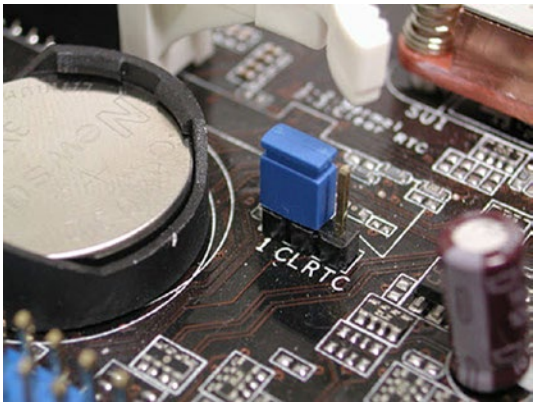


Figure 6-1. *You can reset a BIOS by removing the battery on the motherboard and resetting the Clear CMOS jumper*

Tip Some modern desktop PCs come with a button on the back of the machine or on the motherboard that you can press to reset the BIOS or UEFI firmware.

On laptops and tablets, BIOS firmware corruption is rare. This is because, being battery operated and always plugged into grid power by means of a transformer, they are significantly less vulnerable to the electricity spikes that can corrupt a BIOS. However,

should a corruption occur, you will need to refer to the servicing guide (or an authorized service center) and dismantle the PC's case to find out how the BIOS or UEFI firmware can be reset.

Additionally, if you can load the BIOS or UEFI firmware on the PC, there will be an option to *Restore Defaults* or *Load Optimized Defaults* that you can choose; see Figure 6-2. This will reset the BIOS to its default state.

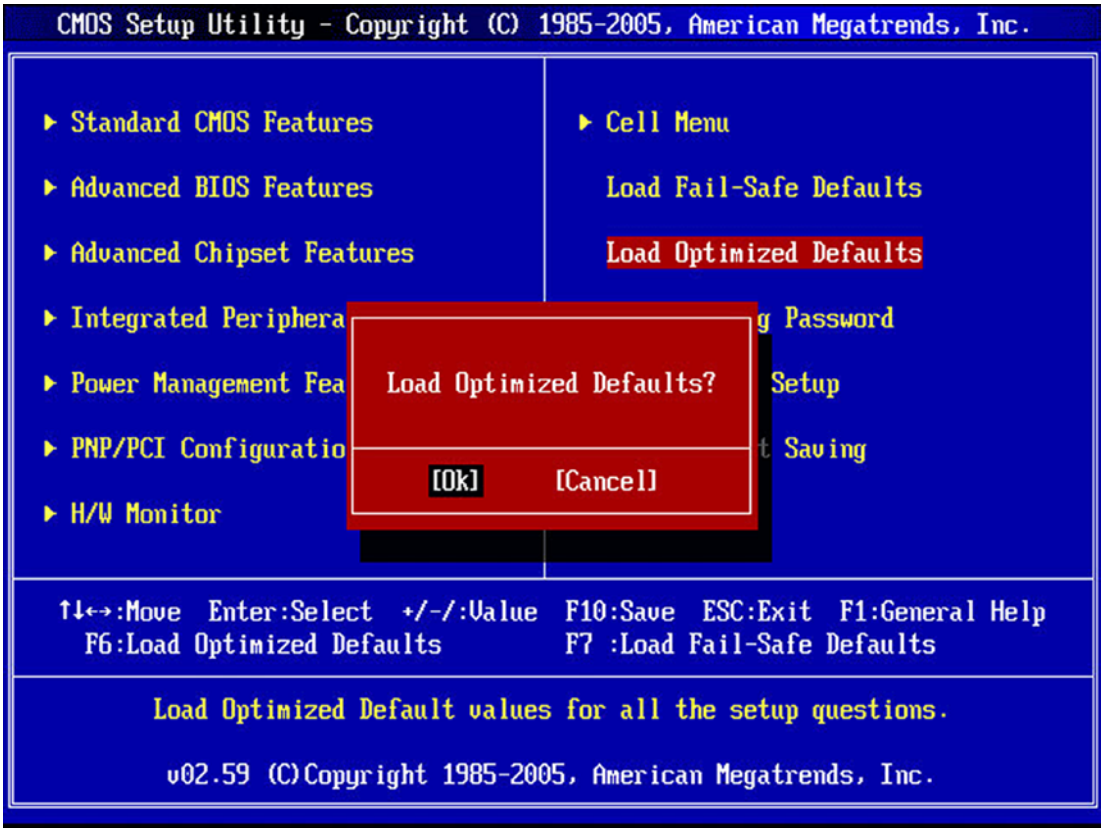


Figure 6-2. *You can Restore Defaults or Load Optimized Defaults from within a BIOS or UEFI*

PCs, BIOS, UEFI, and Overclocking

Overclocking is the process of forcing the hardware in your PC, usually the processor (CPU) and memory, to operate faster than their normal (optimal) speed. PCs are commonly overclocked when they're to be used for speed-intensive tasks

such as gaming or video production. Not all PC components support overclocking, and some components can be damaged if forced to work faster than their standard clock speed, which is measured in megahertz (MHz) or gigahertz (GHz).

The overclocking process is managed either in the BIOS or UEFI interface (see Figure 6-3), or through the use of a utility provided by the motherboard manufacturer that then changes settings in the firmware itself.

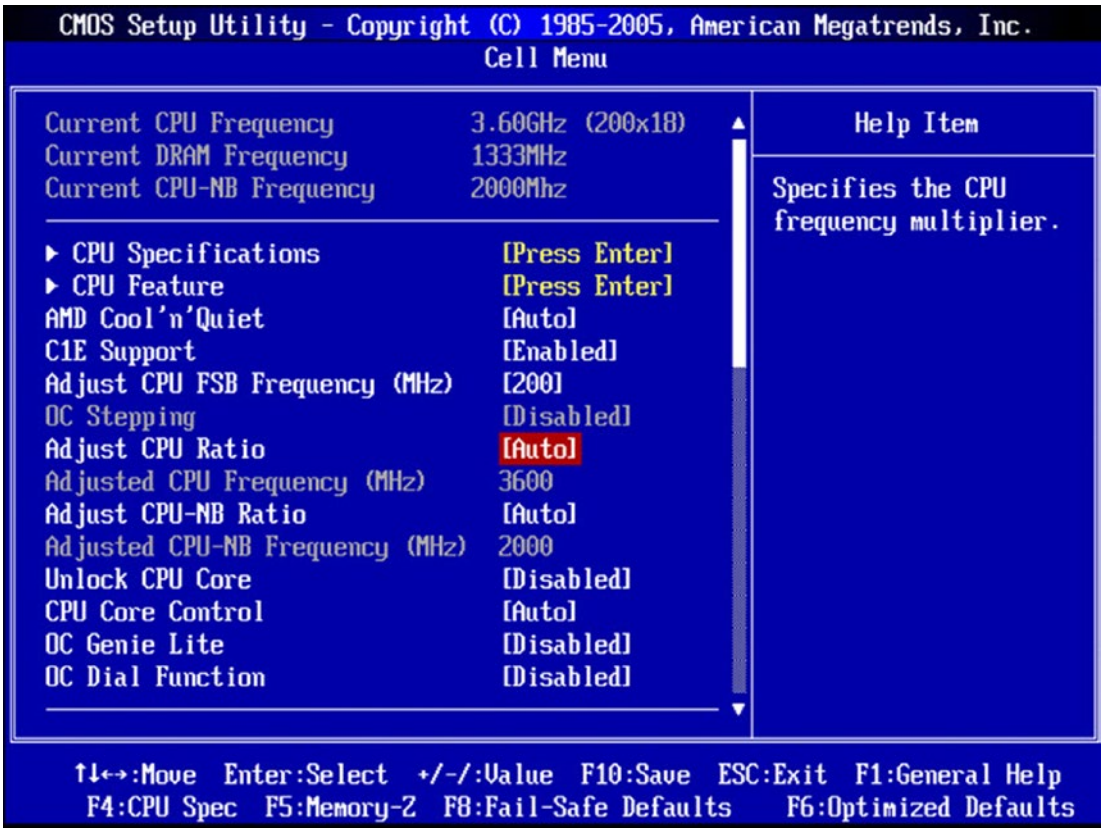


Figure 6-3. *Many PC motherboards support overclocking of components*

Overclocking is a complex process and not for the faint-hearted. It involves manipulating the clock speed (frequency) and power regulation for components that sometimes run on microvolts and have transistors only nanometers (nm) across.

Normally, PCs are very good at recognizing if overclocking is incorrectly configured or can damage the components in a PC. Should this happen, it will likely stop the PC at the firmware screen at startup, report that "Overclocking has failed," and prompt you to reconfigure the firmware with more appropriate settings.

Should a PC be misbehaving, however, and suffering from unexpected crashes, Blue Screens of Death, or overheating, it might be worth checking if overclocking has been enabled on the machine.

Power Supplies

There are two types of power supply for a PC: internal and external. A desktop PC will (unless it's a small-form-factor [SFF] machine) have an internal power supply (PSU). SFF PCs, laptops, and tablets will come with an external "brick" that plugs into grid power when required.

Power supplies fail on PCs more than any other component, and this is especially true of internal PSUs, as they have moving parts in the fans, often sit on the floor, and have vents that allow them to collect dust. Indeed, all electrical equipment will collect dust because of the electromagnetic fields it creates. If you've ever wondered why there always seems to be more dust behind your PC than anywhere else in your home or office, this is why. It's not just dust either, as pet hair will also be attracted by the electromagnetic fields, so it's wise not to brush your dog next to your desktop PC.

There are many PC problems that can be attributed to a faulty power supply. I'd like to detail these each in turn:

- **Failure to power on**—I want to begin with this, since while it might seem obvious that the power supply in the PC has failed if the PC fails to start, this isn't always the case. If you press the power button on the PC and the lights flicker or turn on for a second before powering off again, then the power supply will be the likely culprit. However, if you press the power button and absolutely nothing happens, it could also be the PC's motherboard or the case power button. The power button plugs into the motherboard and sends a signal to the PSU to switch on. If this signal doesn't reach the PSU, it can *appear* that is faulty when in fact it isn't. You can test this by jump-starting the PC, which I will detail shortly.
- **Sudden power loss**—This is another problem that may appear to be the power supply when it actually isn't. In some ways this is harder to diagnose, as you can't often jump-start the PC because it needs to be left on for a while before the problem occurs. You can check if other

devices in the home or office are experiencing the problem, however, as it could be an electrical wiring fault. Try a different power socket and/or a different power lead before diagnosing the PSU.

- **Blue Screens of Death and other crashes**—If your PC is experiencing sudden and seemingly unrelated Blue Screens of Death or mysterious app crashes, it could be the PSU. Look for a pattern, such as if you're gaming or performing other power-intensive tasks such as rendering video, recalculating a large spreadsheet, analyzing a huge data set, and running a lot of apps simultaneously. A power supply is like an automobile engine, in that over time its power will diminish. A PSU that provided more than enough power for a PC when it was new might not be able to produce enough watts after a few years.

When diagnosing a PSU in a PC, especially if you suspect it's generally down on power, the best method is to unplug some of the power cables from all the components inside the PC that aren't essential. This can include all but the primary hard disk or SSD (M.2 drives plug directly into the motherboard and take their power from that), the optical drive, and any PCIe (PCI Express) or additional graphics cards that may be installed. This can help you determine if the PC will start if less power is being drawn from the PSU. Should this be the case, then it will point to the PSU being old and needing replacement.

Jump-Starting a PC

You'll probably be familiar with the concept of a jump start. This is when you'll use the battery from one motor engine, usually an automobile, to power the startup of another engine. It works the same way with a PC, and this can be a great way to diagnose conclusively whether a power supply has failed or if it's another component in the PC.

You might have guessed by now that to jump-start a PC, you'll need either a spare PC with a similar type of PSU (you can only jump-start desktop PCs with PSU because of this) or you'll need a spare power supply.

It's possible, but fiddly, to jump-start a PC from the power supply in another without first removing the PSU from the other machine's case. The power leads inside a PC aren't very long, however, so it's generally safer and more advisable to perform some minor surgery on the working PC and pop out the PSU first.

You don't need to plug every power lead into the faulty PC, just the power leads to the motherboard, which are normally a 24-pin block and a 4-pin block; (optionally) the leads for the primary hard disk or SSD; and, if required, the graphics card. If the PC then springs into life, you'll know that the PSU in the faulty PC is to blame.

The Motherboard

The motherboard in a PC is where it all happens—where the action takes place. In recent years there have been real advances made in motherboard and processor technology that have made them much more reliable and robust. As an example of this, new processors have removed the requirement for motherboards to have a Northbridge chipset.

If you've ever looked at a motherboard, usually a slightly older one now for the reason I detailed, and seen a chip with its own heat sink or fan in the middle of the board, this was the Northbridge. This chip handles all the communications between the processor (CPU), memory, and the installed PCIe expansion cards. As a result, it would have a lot of work to do and get extremely hot. A motherboard with a Northbridge chipset would sometimes fail when this chip would overheat.

So what else can go wrong with motherboards? As the technology involved in manufacturing electronics has evolved, we've moved away from large transistors and resistors, each attached to the motherboard with two short wires (and do you remember valves?). Surface-mount technology means that you can't snap most components on a motherboard, as they're mounted, quite literally, flat to the surface of the board.

There are components that can become gunked with dust (and fine pet hair), break, or fall off. Dealing with this last point first, the most obvious example of this is the connection block on which the wires to the power and reset buttons, and case power and disk activity lights, connect to the board. Some modern PCs come with special blocks that lock these flimsy cables firmly in place. For most PCs, however, it's all too easy for one or more of these wires to become detached from the motherboard, especially if it's moved.

Other components, such as some expansion cards or perhaps a Trusted Platform Module (TPM) encryption card, can also become dislodged when a PC is moved. If this happens, and a PC is misbehaving, it's a good idea to disconnect the power to the PC and then make sure everything is seated properly on the motherboard.

Where there are places that dust and pet hair can collect, such as PCI sockets or in fans, these should be cleaned occasionally, as dust, let's not forget, conducts electricity and collects static. When the components in a PC can often measure in just nanometers, this can make then very vulnerable to even miniscule voltage discharges.

On the subject of fans, bear in mind that these do wear out over time. If a PC is getting old, check the CPU fan especially, as an overheating processor can result in it cracking and becoming useless. Case fans that don't work, or that perhaps have been unplugged because the user thought they were too noisy, can reduce the airflow needed to keep the components in a PC case cool.

Note It's not unheard of when a PC overheats, for a moderately tech-savvy user to go into the BIOS or UEFI settings and raise the processor temperature threshold at which the PC will cut out, putting a password on the firmware can prevent this if your motherboard supports it.

The Rear Panel Connectors and Cables

In the first edition of this book, I wrote at this point, "If I had a dollar for every time somebody had plugged something into the wrong socket at the back of a PC, I'd be writing this book from my villa in the South of France." Well I must have been doing something right as, while not a villa, I *am* writing this second edition from my new home in the south of France. In these days of USB sockets, it's easy sometimes to forget that audio often doesn't work because the speakers have been plugged into the wrong audio socket (for reference, it's the green socket you need first), or the monitor has been plugged into the motherboard, when there's a PCI graphics card managing the output instead.

What's often overlooked, however, is good cable management. Some of these cables, VGA and DVI graphics cables, for example, are screwed into place. Others, such as USB cables, sit firmly some way inside the rear panel sockets. An accidental kick or sudden bang can damage not just the cable and plug but the entire back panel and, by definition, the motherboard.

Memory

I was going to say something prophetic about memory, but then the power went out and I forgot it. When diagnosing problems or even potential problems with memory, you can try to remove all but one memory card from the PC and then try different cards in sequence (and in different sockets) to see if a problem exists.

Additionally, Windows 10 includes a specific memory diagnostic utility that can be run by searching for **memory**, funnily enough, in the Start Menu. This will prompt you to restart the PC to run its tests; see Figure 6-4. If any memory faults are found, they will be reported upon restarting the PC.

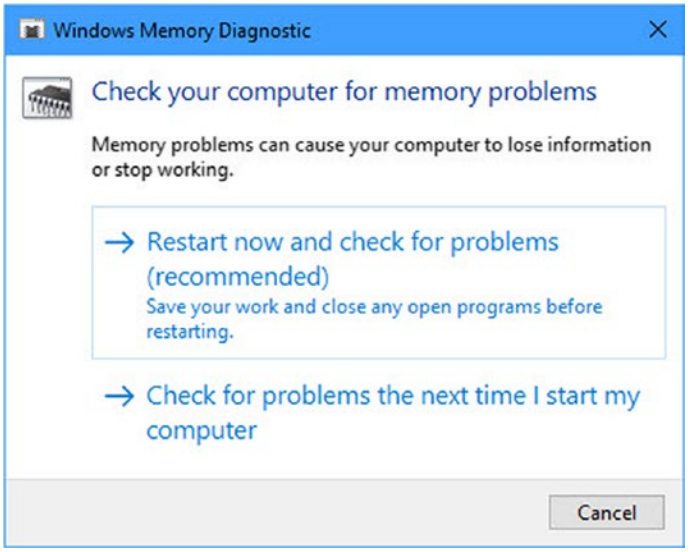


Figure 6-4. *You can test for memory hardware errors from within Windows 10*

Hard Disks, SSDs, M.2, and PCIe Drives

Blimey! Do you also remember a time when you'd plug a regular 3.5-inch hard disk into a PC to use as storage? These days these hard disks are becoming increasingly rare, and the only ones I still use are in my NAS (network-attached storage) drive. There have been attempts to release hybrid drives that contain a limited amount of solid-state storage for caching commonly accessed files. These days we're far more likely to be using an SSD or an M.2 drive (which is an SSD on a card that slots directly onto the motherboard).

Some PCs will include a PCIe card that can be used either as storage in addition to the main hard disk or as the boot drive for Windows itself. There is a distinction between the two, as not all of these cards can be used to host the operating system on the PC. They will usually also require additional drivers to operate before Windows 10 can "see" the drive.

There's usually not that much you can do to diagnose hard disk (I'm using the term generically here) faults, but some BIOS and UEFI systems come with monitoring tools, sometimes called SMART monitoring, which will alert you to an impending disk failure. In Chapter 3, I showed you how to set up and manage disk partitions using the inbuilt Windows 10 Disk Management utility, and in Chapter 11 I'll show you how to manage disk and file permissions.

Expansion Cards

I've mentioned PCIe expansion and graphics cards several times throughout this chapter. They're used for everything from gaming graphics to superfast storage. There's not much that can go wrong with PCIe cards as, unlike previous generations of expansion cards, they don't tend to come loose (not very often anyway) when the PC is moved, and graphics cards often have an additional clip on the socket to hold the card securely in place; moreover, cards that require extra power tend to have those power cables clipped into place.

One of the advantages of troubleshooting PCIe cards is that they can quickly be removed from the PC and placed into another PC to see if the problem recurs. Note that you might need to install drivers on the test PC for the hardware.

Monitors and Cabling

I mentioned cabling earlier in this chapter, but it's really important to get cabling right. You might have a hole in a rear corner of your desk in which you can put cables to keep them tidy, and perhaps a mesh or other type of channel under the back, or just behind the desk in which you can lay cables. These aren't just for aesthetics' sake; they're extremely useful for making sure that your cables are out of the way, that they can't be pinched or snagged easily, and that people won't trip over them.

If you are connecting your PC to a monitor using a VGA or DVI cable, the cable will likely be screwed into the PC at both ends. This means that if somebody trips over the cable, the monitor is likely to come crashing to the floor. Network cables are also prone to this, but if a network cable that's plugged into the back of a PC is caught, the end result will likely be that the cable is stretched and damaged and that the plug might snap.

When it comes to monitors not working, always bear in mind that workers just *love* rearranging their desks. This will mean they'll move their monitor occasionally and unplug and replug the cables at its rear. Should they plug the video cable into the wrong socket at the back of the monitor, they'll not get a picture until they change the input selection on the onscreen display.

Note Some USB devices, printers, and Wi-Fi dongles especially don't work when unplugged and plugged back into a different USB port on the PC. I had a bit of an argument a few years ago on my Windows 8 troubleshooting book with a senior member of the Windows Product team at Microsoft about this, in which he said the problem didn't exist because they had no record of it. Believe me, it does exist, but it is easily fixed by unplugging the device and plugging it back into a different USB port to force Windows to reload the driver.

Keyboards and Mice

If there were ever pieces of hardware that could be fixed by simply unplugging and plugging in again, then they are keyboards and mice. It's fairly common, however, with wireless keyboards and mice that come with a USB dongle you plug into the PC, which they won't work when the PC starts. This is because they're not being properly recognized by the PC. Moving them to a different USB port can fix the problem.

Note I want to talk for a moment about Bluetooth audio. It's a little-known annoyance that Windows 10 PCs can't connect to more than one Bluetooth audio device at a time. So if you have Bluetooth speakers for your laptop, and you also pair Bluetooth headphones with it, an incompatibility will occur and you won't be able to use them.

Summary

This chapter was quite difficult to write, as PC hardware has changed fundamentally in the last few years, and there's now very little that goes wrong with it. From processors that integrate the functions of the Northbridge chipset to USB type-C plugs that will pull free from a PC more easily than older designs, hardware is pretty robust.

Where problems do occur is either with moving parts (such as fans), those that still get extremely hot (like the PSU), driver support in Windows, or limitations within the operating system itself, such as the aforementioned Bluetooth audio limitation.

Safely using hardware is more a case of prevention and cable management than of finding the solutions to problems. Sometimes, though, problems do still occur, and in the next chapter, I'll show you how to troubleshoot the most commonly occurring hardware issues.

CHAPTER 7

Diagnosing and Repairing Problems with Hardware and Peripherals

Getting hardware devices to work with your PC should be a simple matter of plugging the device in, or connecting to it across the network, and getting going. But guess what… it's very often not that simple. At least long gone are the days of parallel and serial devices (well, except for some engineering and other specialist applications) where configuring a device often meant the manual editing of text configuration files, and configuring multiple settings in the Windows Device Manager and on the device itself to get everything to work.

USB (Universal Serial Bus) was designed to eliminate all that, with code embedded into devices that would identify them to the host operating system. Newer peripheral connection technologies such as Thunderbolt and USB Type-C adopted this system, and devices that connect to your PC over a network or via Bluetooth will also identify themselves, making installation and configuration simple.

In theory, anyway. In practice, it's often not that easy to get devices installed, and when they are installed, all that's often needed to get the connection to break is a restart of your PC. In this chapter, we'll look at the common problems associated with installing and troubleshooting hardware, and the steps you can take to fix them.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_7

Getting USB Devices to Work Reliably

USB devices were designed in the mid-1990s to eliminate most of the problems associated with hardware device installation. As I've already mentioned, a USB device identifies itself to the host operating system by means of DEV_ (Device) and VEN_ (Vendor) codes, and I'll talk more about these in Chapter 15. These codes help Microsoft Windows (and all other operating systems) to marry the device with the correct driver, and to configure it appropriately.

There are sometimes problems with USB devices, however. Perhaps the best known of these is that USB drivers sometimes tie a device to a specific port on the PC. This is especially true of printers and Wi-Fi dongles, and means that should the PC be moved, or the device unplugged for some reason, plugging it back into a different USB port suddenly results in the device not working. This can be frustrating for users, and you may get calls from people saying that they cleaned their PC and all of a sudden they can no longer get Internet or network access. Unplugging the USB device and trying different USB ports solves this problem, either by moving the device to the port it was in originally or by forcing Windows 10 to reload the device drivers if it's plugged into a different USB.

Note USB game controllers can suffer from mapped-button loss when moved from one USB port to another on a PC.

USB Storage, in the form of Flash Drives, SSDs, and hard disks, are everywhere these days, but who clicks the Safe Eject option hidden in the Windows system tray; see Figure 7-1, when they unplug them?

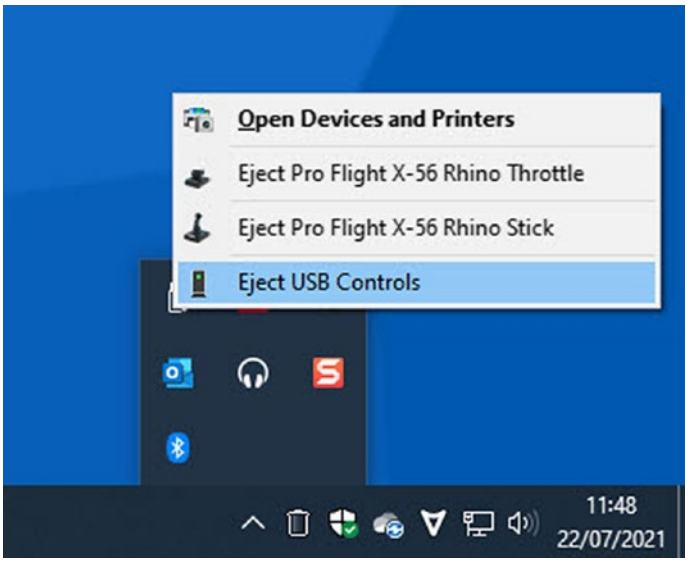


Figure 7-1. *You can safely eject USB storage devices without causing data corruption*

I will admit to being as guilty of this as most other people. It works fine 999 times out of 1000 to just unplug the USB storage device; when you plug it into another PC, or a smart device like a modern television, it just works. It's that 1 time in 1000, though, when it doesn't, that can completely corrupt the USB storage drive, rendering everything on it unusable. If you're just transporting files from one PC to another in the office, that can be inconvenient. If, however, you're sending someone out of the office with files for a presentation, this can be embarrassing at best, and a major failing at its worst.

By default, Windows 10 sets all USB storage devices to be suitable for "quick removal." You can check this by right-clicking the drive in File Explorer and selecting its *Properties*. In the dialog that appears under the Hardware tab (and making sure the correct device is selected as all your drives will appear in this list), click the *Properties* button; then, at the next dialog, click the *Change Settings* button, and then click the *Policies* tab, which will appear; see Figure 7-2).

Tip Sometimes a USB Flash Drive or external hard disk will report a corruption error, but will often work fine regardless. A quick *scan and fix* will almost always sort the problem.

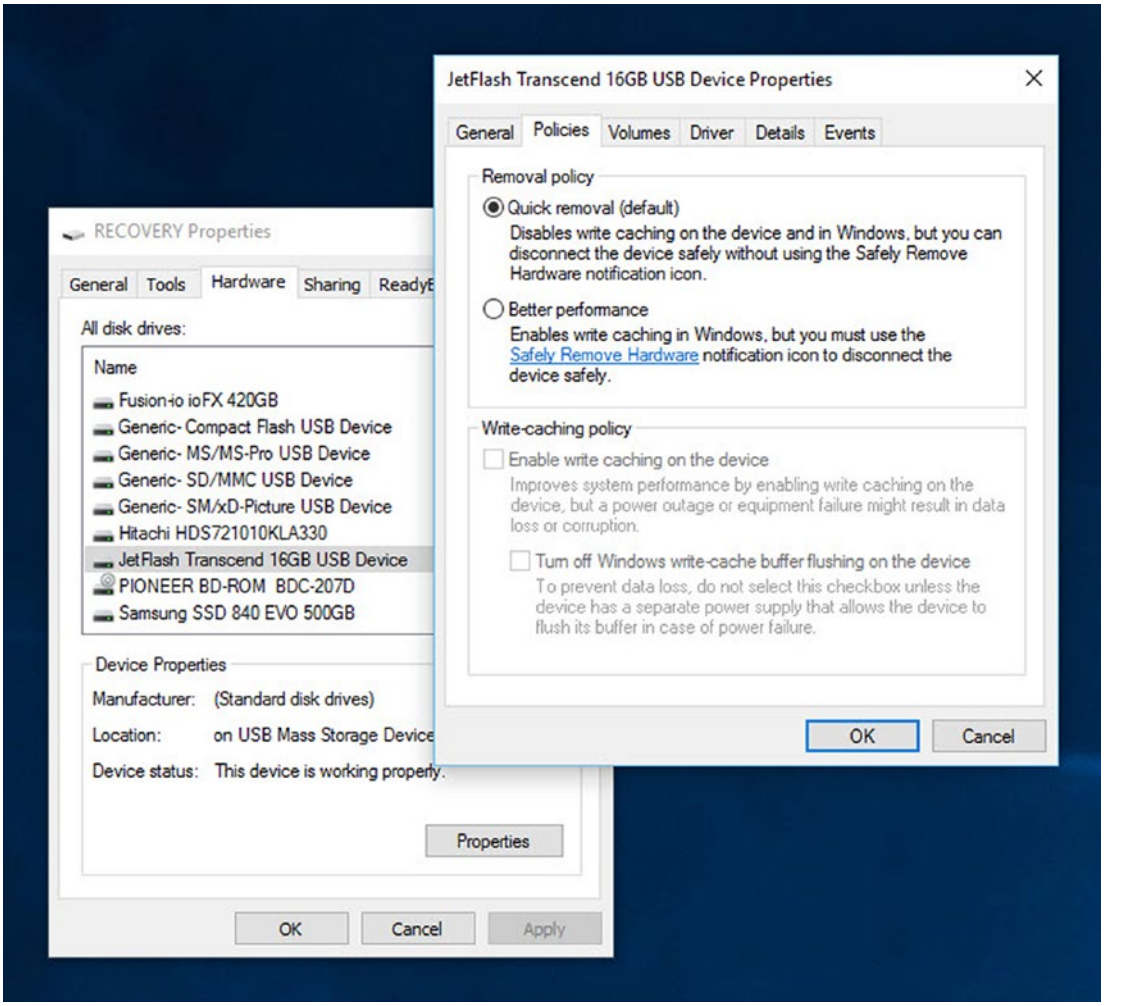


Figure 7-2. *You can check if a drive is configured for quick removal*

Note It's worth pointing out that, in a very few cases, and I have experienced this myself, that even setting a drive for quick removal doesn't guarantee the drive will not be corrupted when removed. It's always best practice to tell users to safely eject USB devices before removal as a precaution.

Installing and Managing Bluetooth Devices

Bluetooth was supposed to be the "holy grail" of hardware devices used with PCs and modern computing devices, able to connect completely wirelessly at a range of up to 10 meters initially, and more than 100 meters today. Unfortunately, in more cases than not, it's the "Holy cr**!" of device management instead.

Bluetooth devices in Windows 10 are added and removed from the PC primarily through the Settings app; see Figure 7-3. You can add a Bluetooth device to your PC by opening *Settings* and navigating to *Bluetooth & other devices* and then clicking the *Add Bluetooth of other device* button.

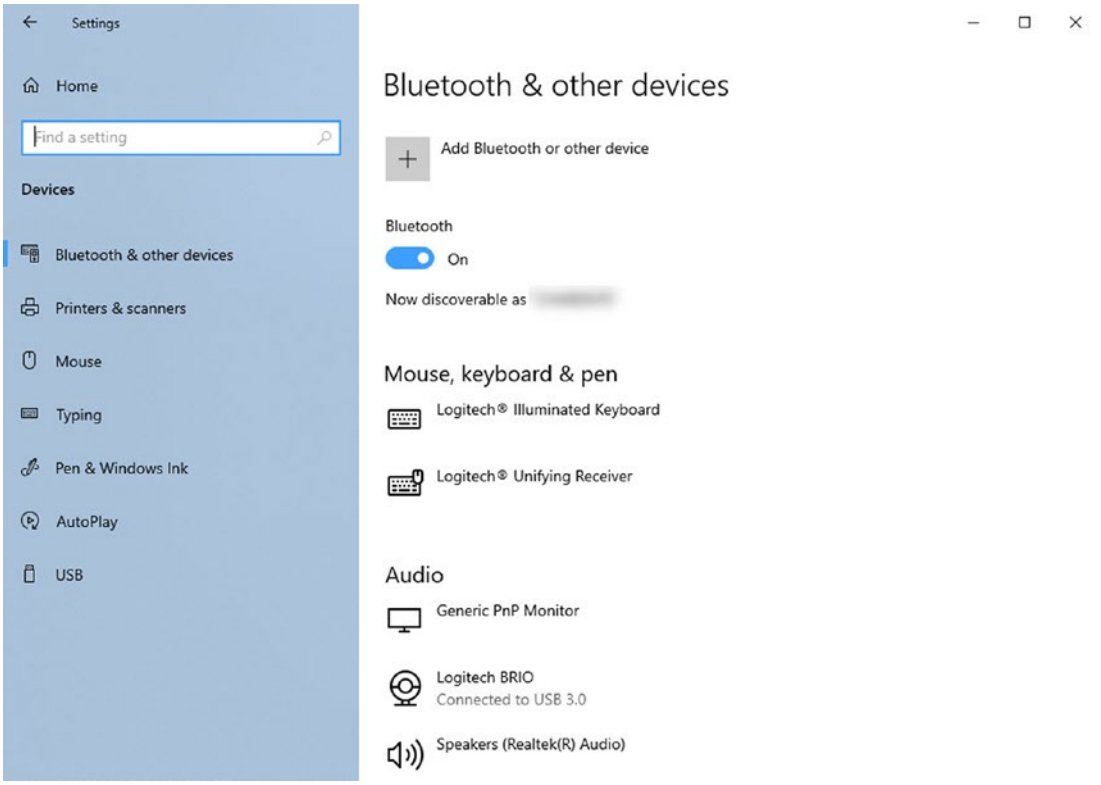


Figure 7-3. *You can add and remove Bluetooth devices in the Settings app*

There are some idiosyncrasies with Bluetooth devices, however. Perhaps the most annoying is that Windows 10 PCs won't connect to more than one Bluetooth audio device. This means if you have both Bluetooth speakers and headphones, you'll need to either choose which one you want to use or uninstall one before installing the other.

Additionally, some Bluetooth devices don't like being removed (uninstalled) and can sit in the Settings app, trying to uninstall when actually they're not. To get around this, you can also uninstall Bluetooth devices in the *Devices and Printers* panel by right-clicking them; see Figure 7-4.

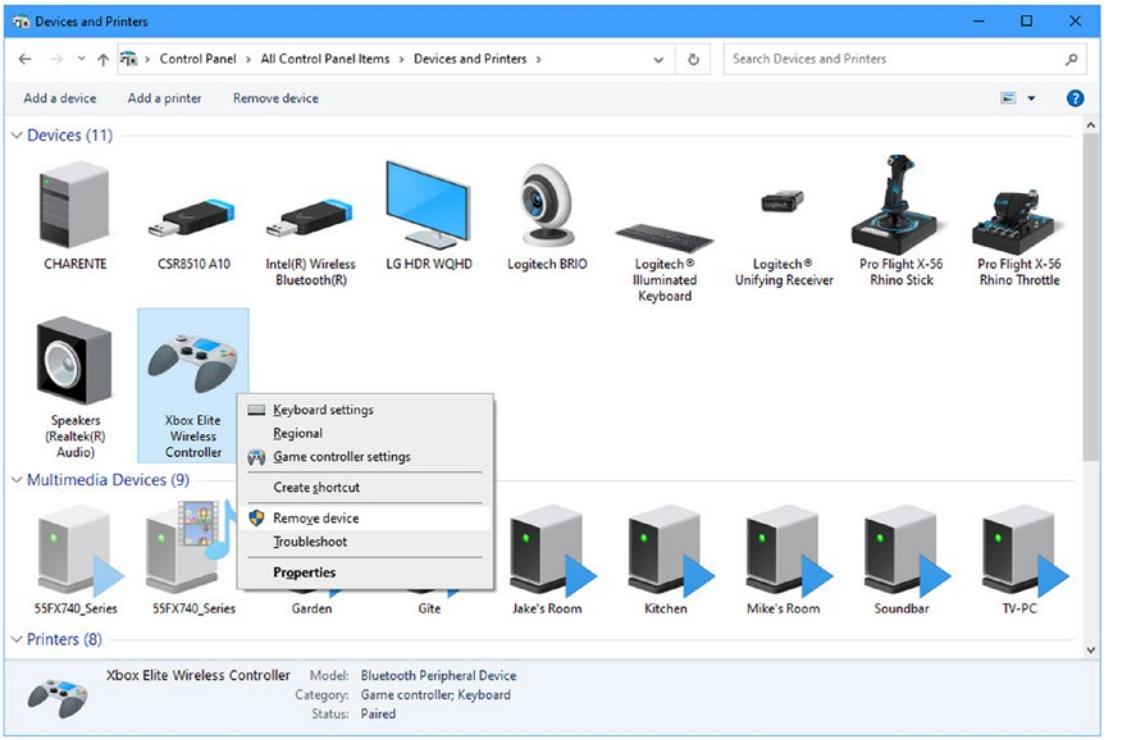


Figure 7-4. *Bluetooth devices can be removed in the Devices and Printers panel*

Sometimes you might find that a PC isn't identifying Bluetooth devices at all. In this circumstance, discoverability for Bluetooth devices might have been disabled. In the Bluetooth section of the Settings app, click the *More Bluetooth Options* link (note you can also right-click the Bluetooth icon in your system tray and click *Open Settings*). Here are several options which include your PC being discoverable by Bluetooth devices, and whether you are alerted when a Bluetooth device wishes to connect to the PC; see Figure 7-5.

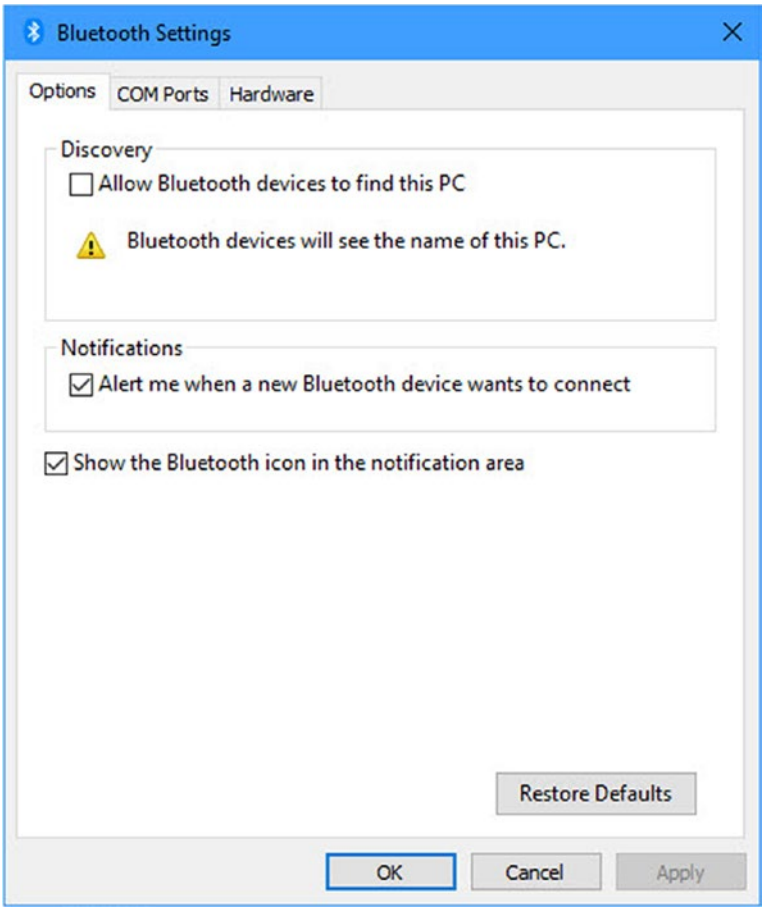


Figure 7-5. *Bluetooth settings that can affect device discoverability are available*

Additionally, the *Hardware* tab in this dialog will provide quick links to your Bluetooth hardware devices, which can be useful if a device is incorrectly installed or configured, or a driver update needs to be applied.

Installing and Configuring Printers

What type of printer do you or your business use? A USB printer? A Wi-Fi printer? A network printer? Perhaps you use a printer that connects via NFC or that uses Wi-Fi Direct to create its own ad hoc wireless network. You might even be using an older Serial or Parallel printer for bespoke applications such as payroll. In short, there are more ways to connect printers to a PC than for any other type of device.

When it comes to configuring printers, there are also a plethora of options. You might want to reduce your costs by restricting printing to black ink only, or to enforce duplexing (double-sided) printing. You might want to restrict the hours during which the printer will be available, or enforce security policies on what people can print.

This all means that printers can sometimes be difficult to troubleshoot when something goes wrong, so getting them set up correctly to begin with is the best way to help avoid problems from occurring.

Installing Different Types of Printers

Whatever type of printer you need to install on a PC, you'll do it from the *Devices and Printers* panel, which can be found on a Start Menu or within the Control Panel. At the top left of this panel are two quick links to *Add a device* (which can include Bluetooth and other devices that aren't automatically detected by Windows) and *Add a printer*. Clicking this second link will start Windows 10 searching for any available printers either attached to your PC, on your local network, or that have set up their own ad hoc network; see Figure 7-6.

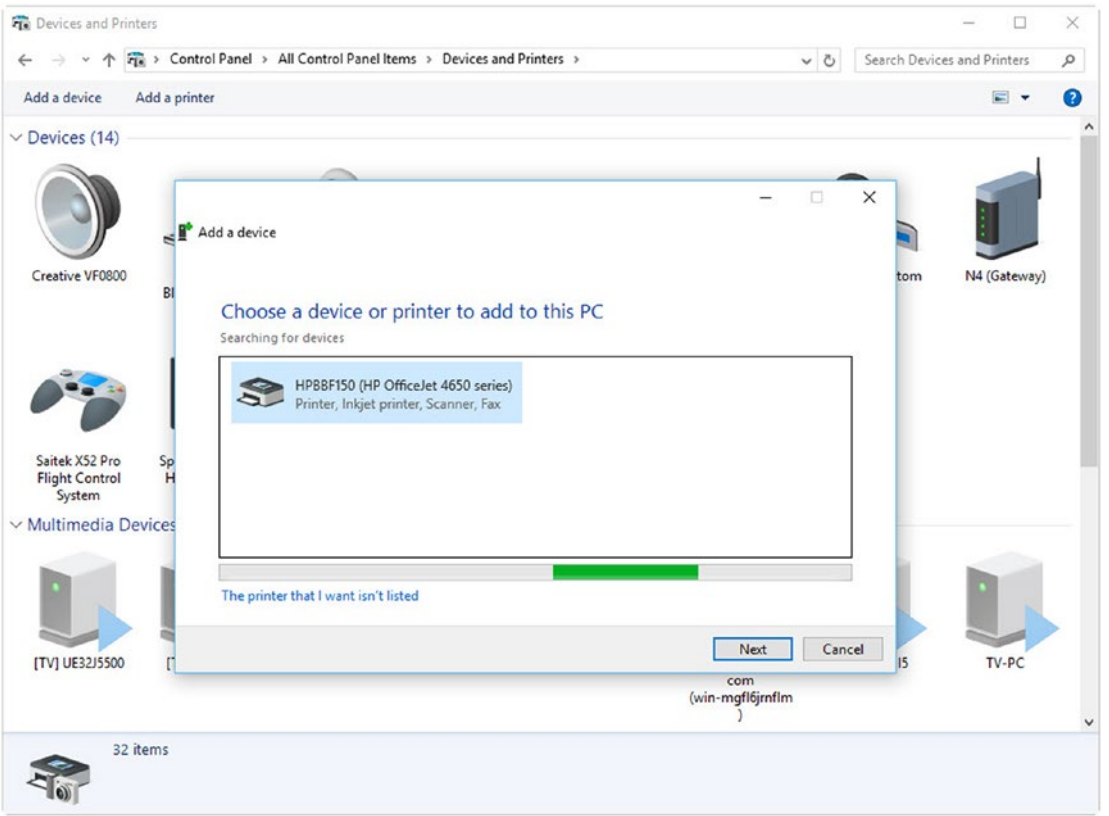


Figure 7-6. *Click Add a printer in the Devices and Printers panel to install new printer*

If your printer isn't discovered however, click the link *The printer I want isn't listed*. This will open a dialog (see Figure 7-7), in which you can install many different types of undiscoverable printer.

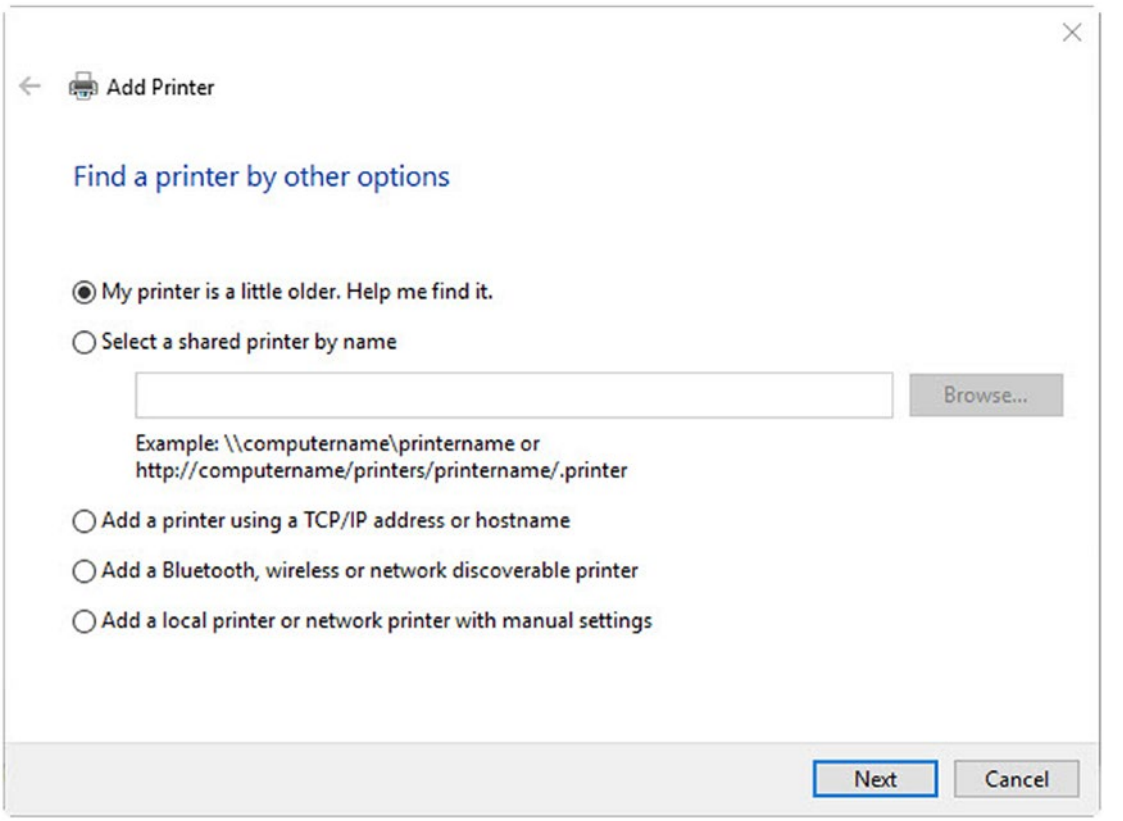


Figure 7-7. *Windows 10 makes it easy to install network and undiscoverable printers*

If you are installing a network printer, there are two ways to do this. The first is to type the network name of the printer; this will come in the format `\\server[computer]name\printername` and will be provided by your IT administrator, or by typing its IP address. I'll show you how to find both of these from another PC shortly.

Tip When installing a Bluetooth or other type of wireless printer, click the *Add a device* link in the Devices and Printers panel, as this will search for devices that may not immediately identify themselves as printers, and it is also the utility that the *Add a Bluetooth, wireless or network discoverable printer* option will launch anyway.

If you are installing a Serial or Parallel printer, which cannot be automatically detected by your PC, choose the *Add a local printer or network printer with manual settings* option. This will ask you which port on the PC the printer is attached to; see Figure 7-8. You can also create a new port if you are using software emulation for ports, and have connected the device through a USB to Serial/Parallel adapter.

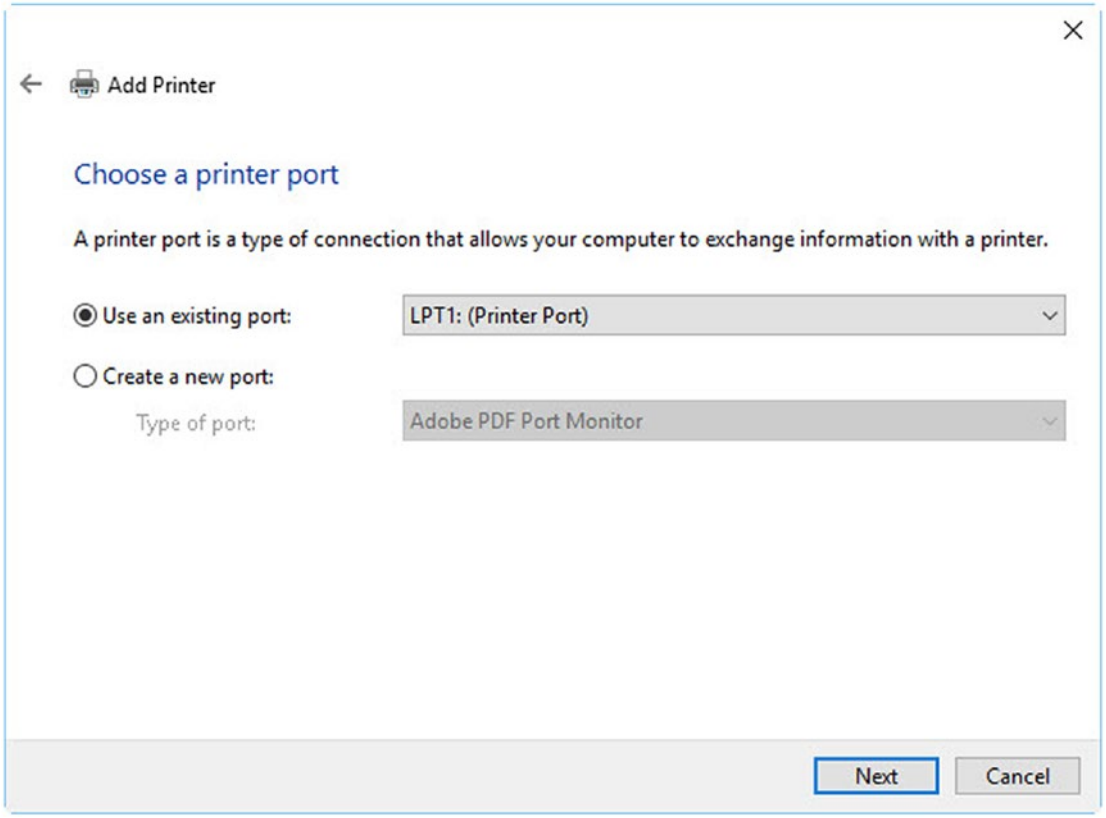


Figure 7-8. *You can manually add Serial and Parallel printers*

If you are unsure what Serial (COM) and Parallel (LPT) ports are available on your PC, open Device Manager from the Win+X menu and expand the *Ports* section; see Figure 7-9. This lists all of the ports installed on the PC with their COM and LPT number assignments.

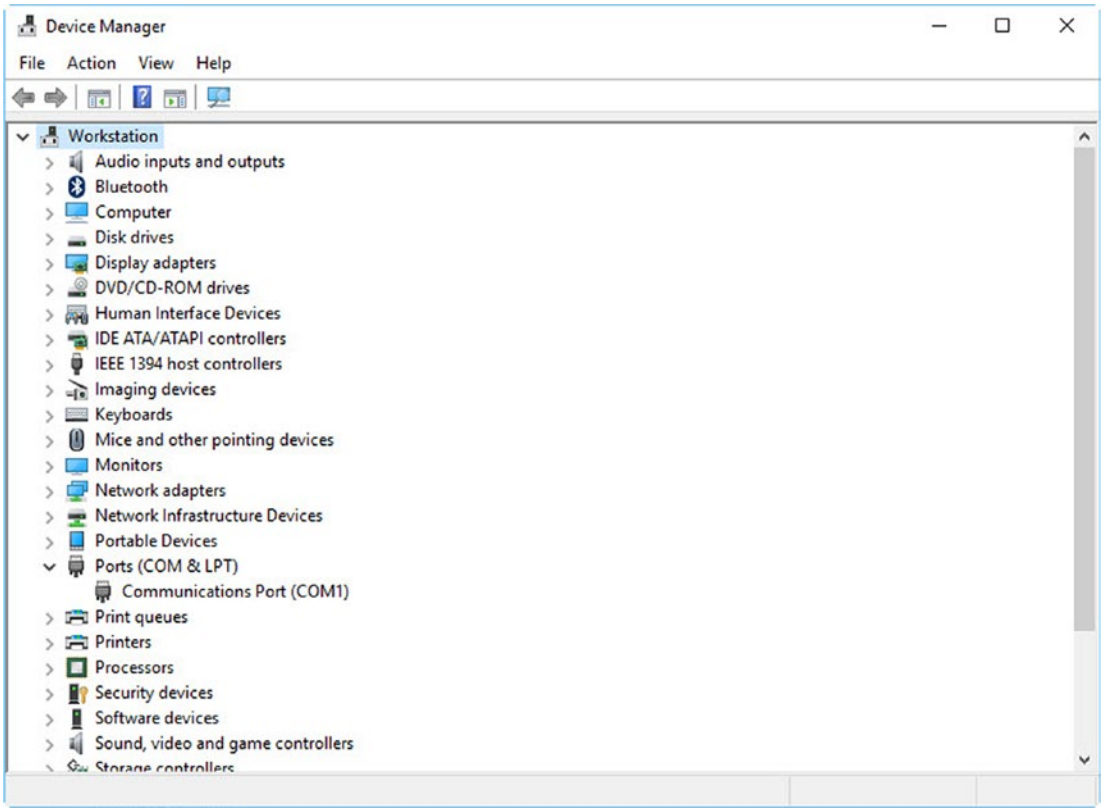


Figure 7-9. *Device Manager lists all the legacy ports installed on a PC*

When you click *Next*, you will be asked to install the driver for the printer. Windows will present a list of all the available drivers (those that ship with Windows or have previously been installed) by manufacturer and model; see Figure 7-10. If you want to install a specific driver from a CD, USB Flash Drive, or floppy disk (remember we're talking about legacy hardware here), click the *Have Disk* button.

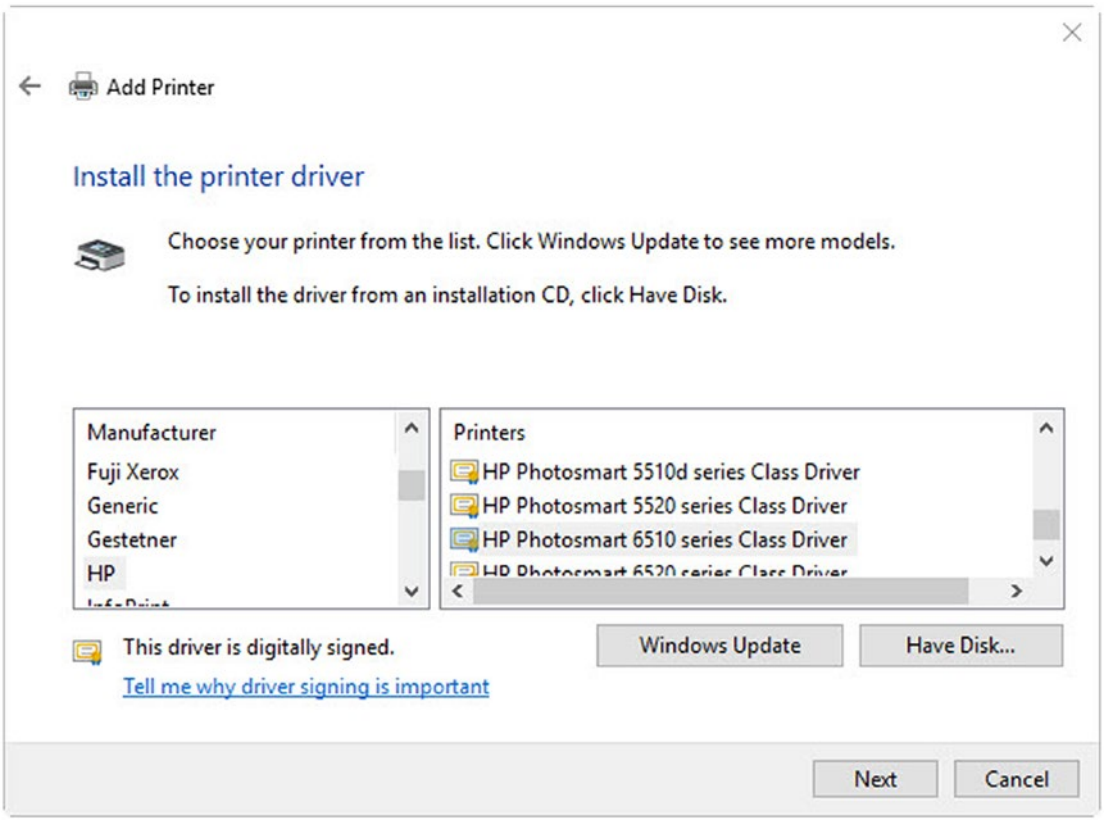


Figure 7-10. *You can manually install the driver for a legacy printer*

Finding the Name or IP Address of a Printer

I mentioned earlier that if you install a network printer, you will need its address and name on the network, or its IP address. Both of these can be obtained from a PC on which the printer is already installed, and looking them up can save a call to IT support. Let's look at the latter of these first. In the Devices and Printers panel on the PC on which the printer is already installed, right-click the printer, and select *Printer Properties* from the menu that appears. In the dialog that opens, click the Ports tab and find your printer in the list; see Figure 7-11.

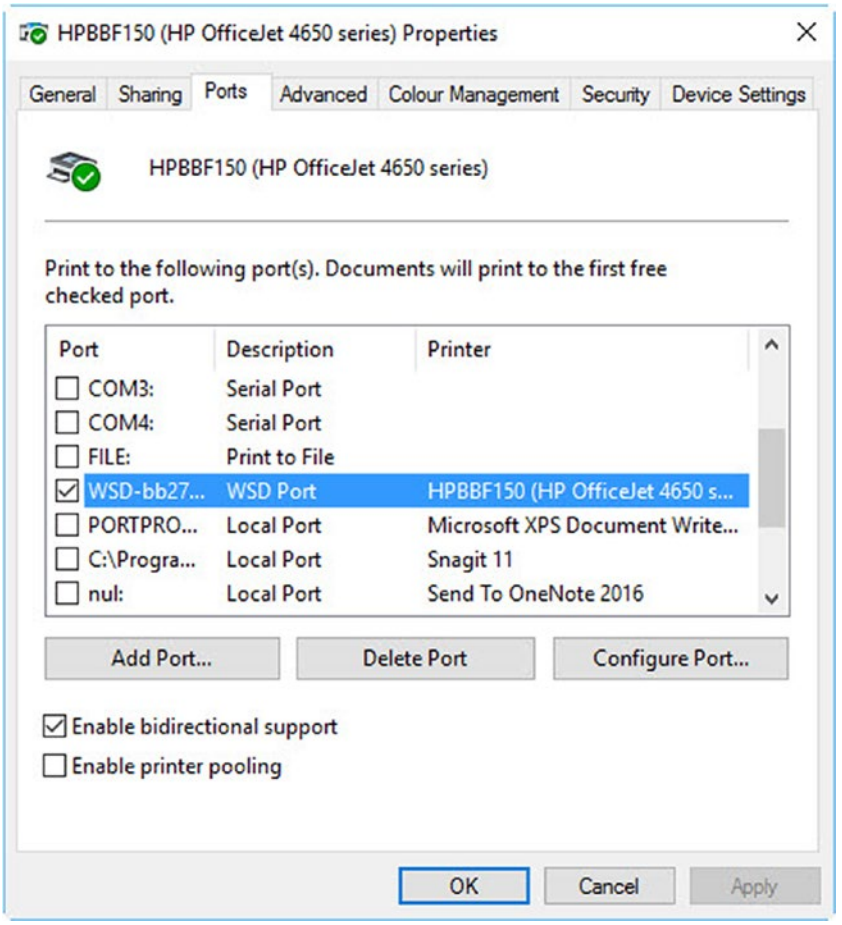


Figure 7-11. *You can often discover the IP address of a printer in its properties dialog*

While this is a good way to reveal the IP addresses of printers in a typical workplace, it doesn't always reveal the information you need. For example, in Figure 7-11 the printer is listed as being on a WSD Port. This stands for *Web Services for Devices*, and these are devices that include Internet functionality, such as being able to print to the printer from anywhere in the world via an app or special email address.

There are a couple of additional ways to get access to a printer's IP address however, though you may not have access to both. The first is to check the IP address in the connected devices page in your home or office router; see Figure 7-12.

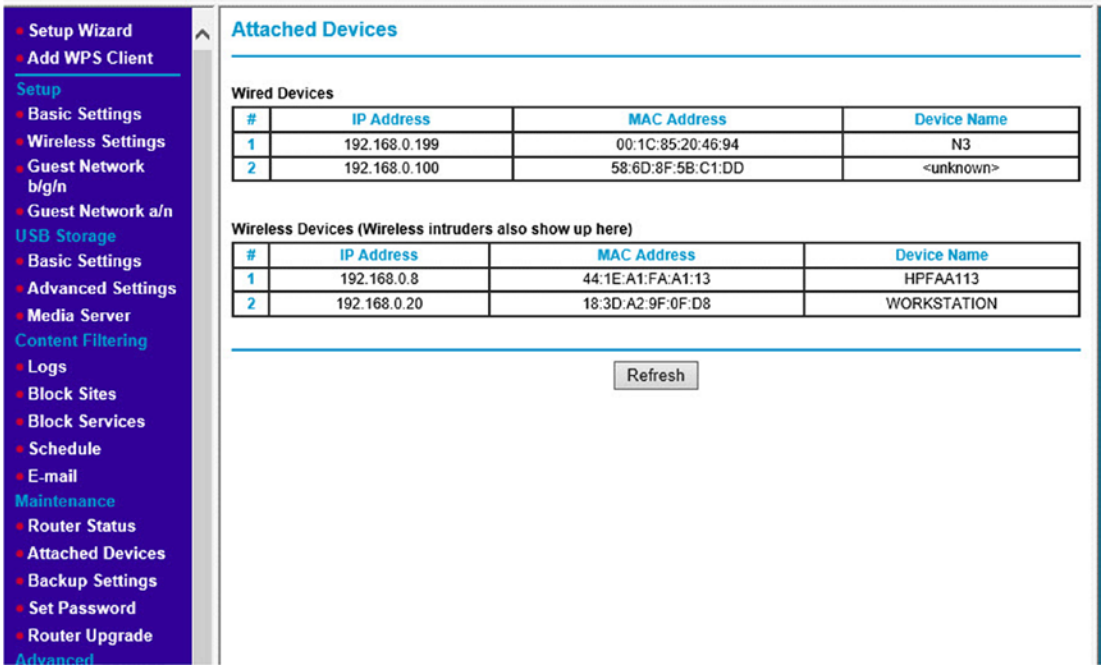


Figure 7-12. *You can check the local IP addresses of devices in your router*

Additionally, and this isn't the case for all printers, click the *Network* link in File Explorer and right-click the network printer. You may see an option such as View device web page (see Figure 7-13), which can open a browser page with status information about the printer itself.

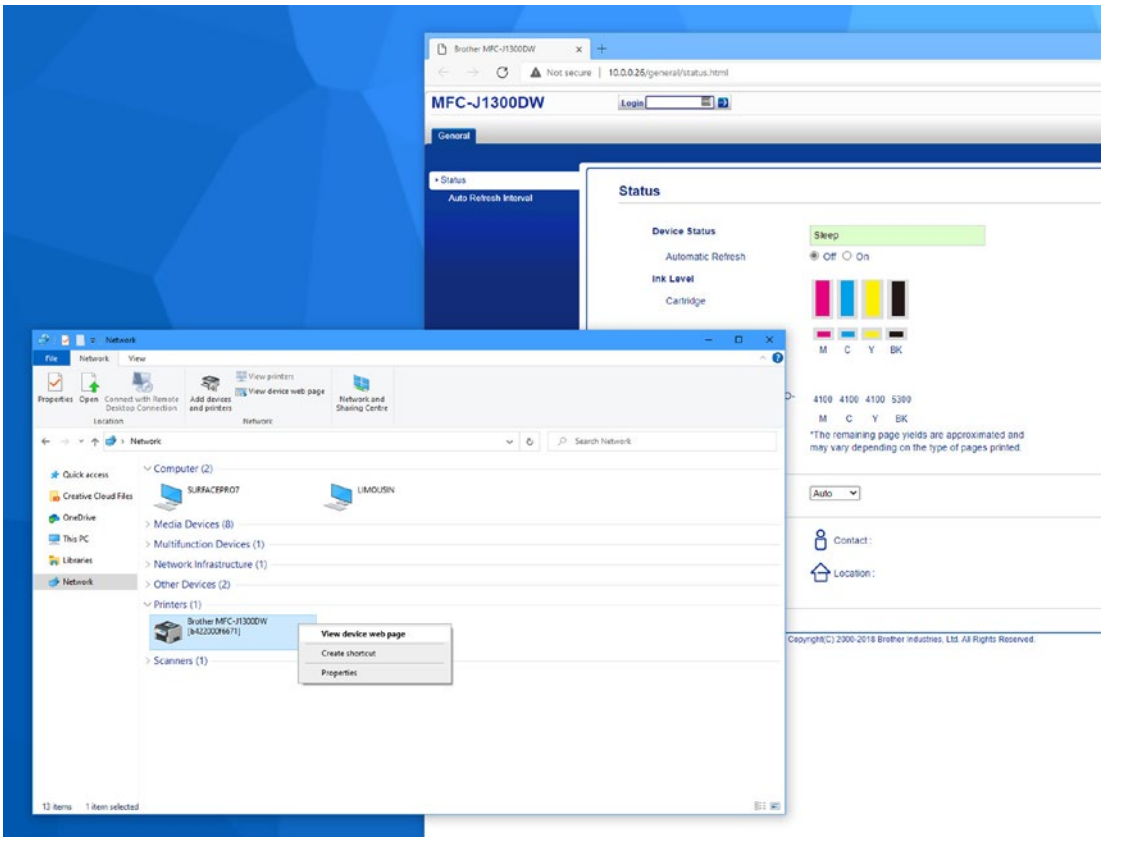


Figure 7-13. *Some printers offer web-type status pages*

You can also check the *Properties* of the printer with a right-click in File Explorer, which will often reveal its IP address; see Figure 7-14.

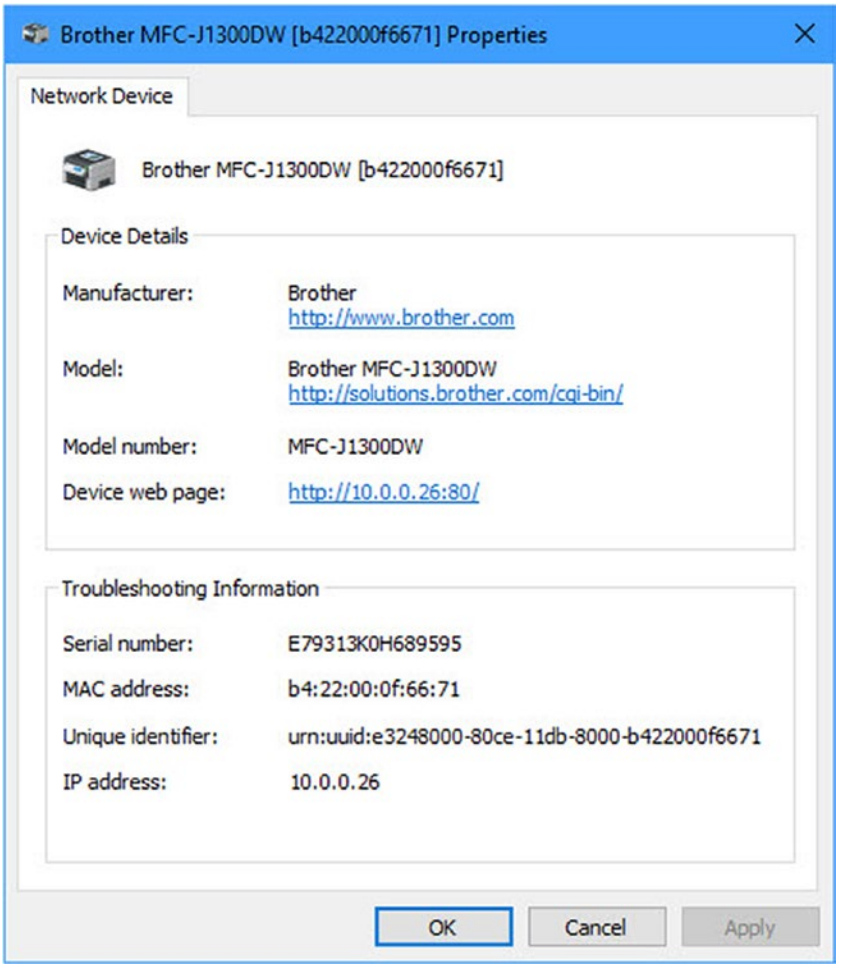


Figure 7-14. *Checking the properties of a network printer can sometimes reveal its IP address*

If the printer is shared from a specific PC, there are two places you will need to go to find the information you need, both of which you will need to get from the host PC. The first of these is the computer [Device] name. Open *System* from the Settings app, and then click *About* to reveal the PC name; see Figure 7-15.

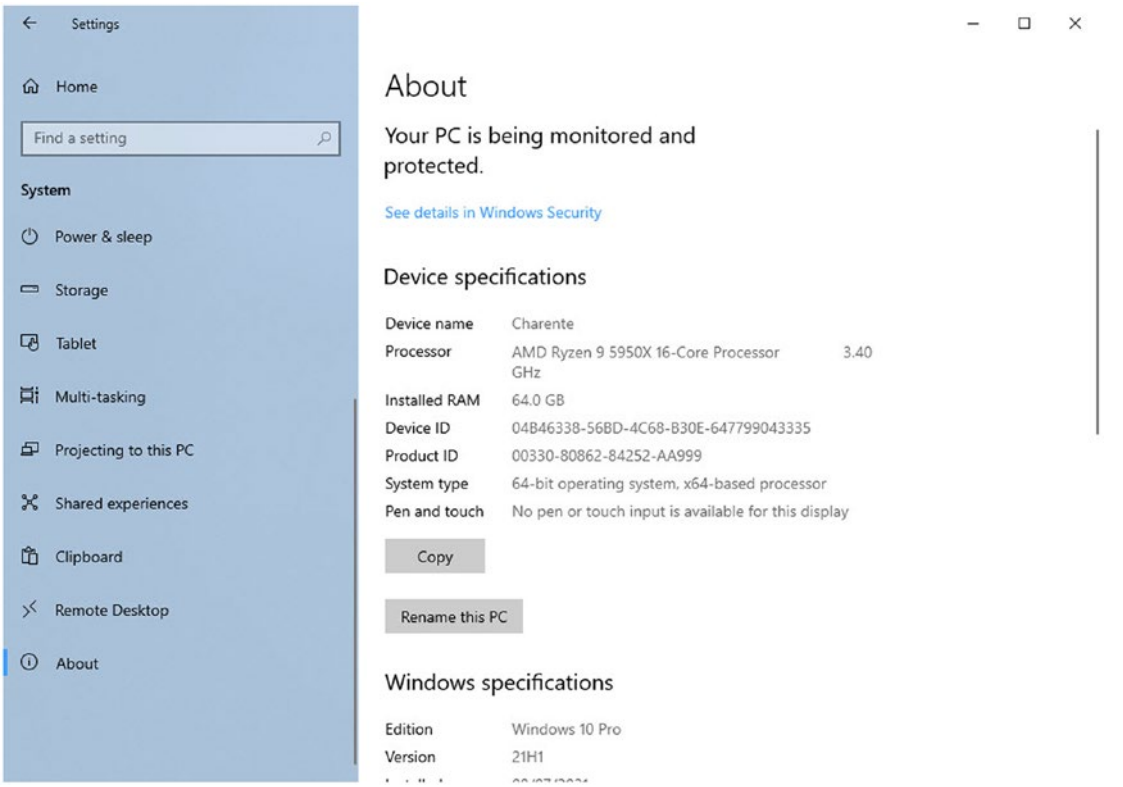


Figure 7-15. *You will need the name of the host PC to install a shared printer*

Next, in the Devices and Printers panel on the host PC, right-click the printer and open the Printer Properties panel. Click the Sharing tab and make a note of the printer name; see Figure 7-16.

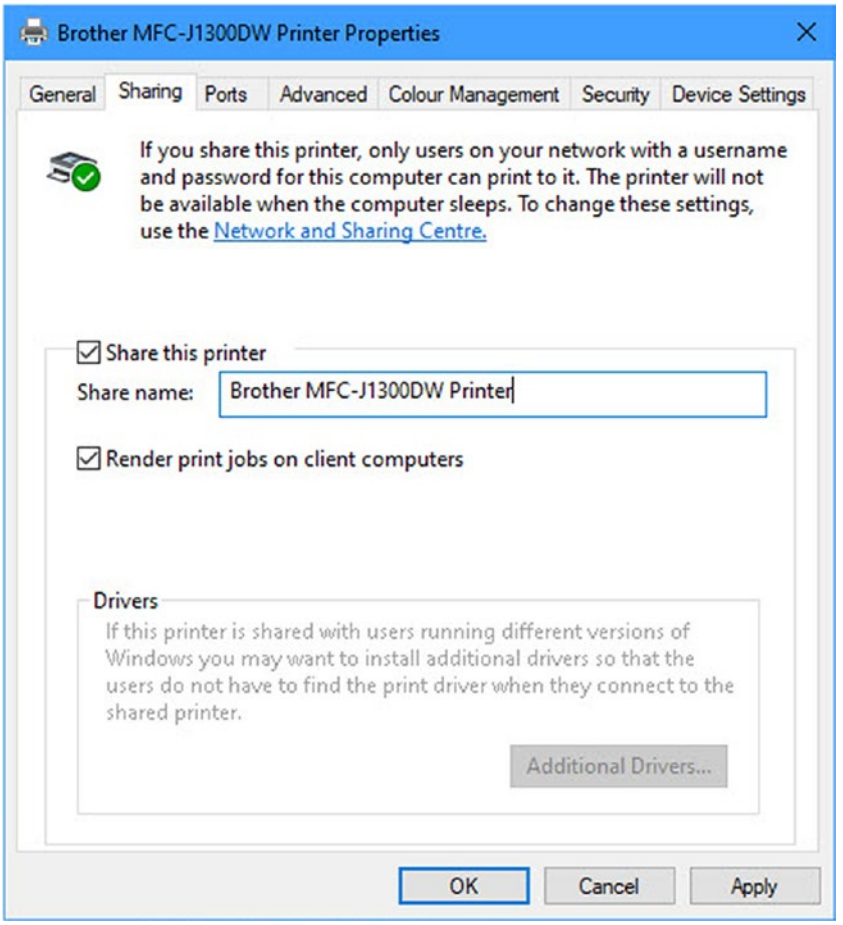


Figure 7-16. *You will also need the shared printer name from the host PC*

In this example, then, we see that the network address for the printer is `\\Workstation\HPBBF150`.

Note In the Sharing tab of the printer properties on the host PC, you might find it useful to click the Additional Drivers button. The host PC can provide the drivers for the printer automatically to other PCs, but it does not automatically provide both the 32-bit (x86) and 64-bit (x64) drivers. Checking both options can help make sure all Windows 10 devices can easily connect to the printer.

Managing Printing Policies

While not specifically a Windows Troubleshooting issue, you might find that people call you on occasion to complain that they simply can't print the documents they need to. This might be because the printing and security policies set up on the printer are prohibiting their access, so I'd like to spend a short period looking at what these are, and how they are configured.

Policies for printers are managed in the Printer Properties dialog we've already looked at. The Advanced tab contains the first set of policies that can affect users' use of a shared printer; see Figure 7-17.

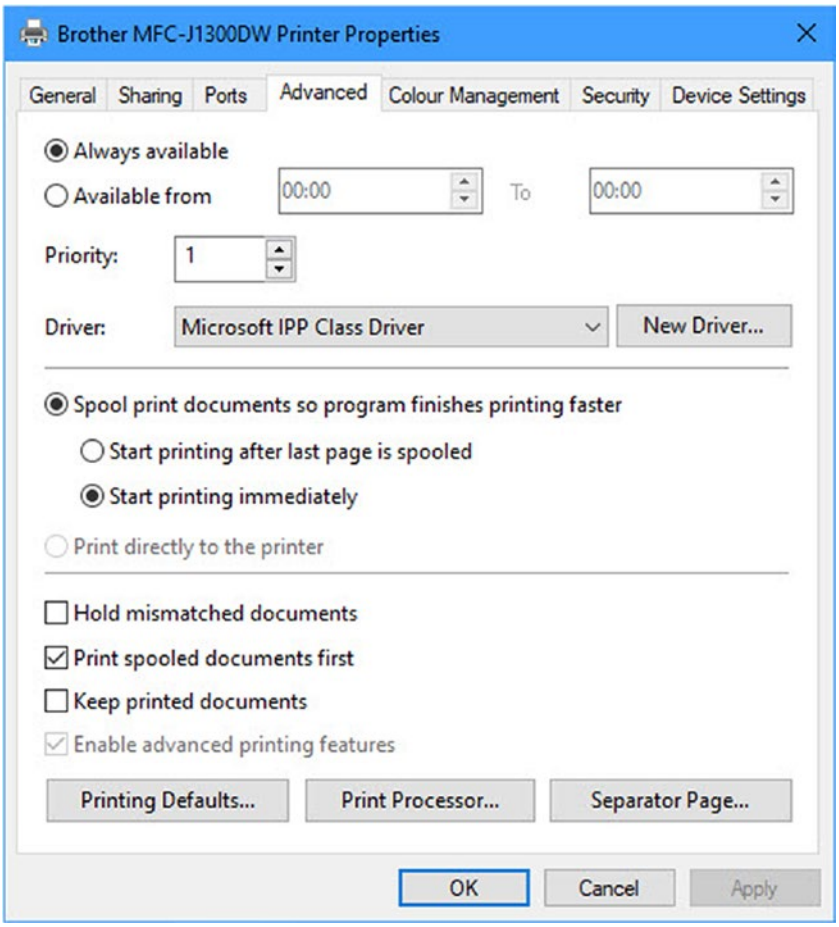


Figure 7-17. *You can set many different policies for a shared printer*

The options available to set for a shared printer (or even the printer connected locally to the PC) include being able to set times of the day when the printer can be used (useful if a teenager at home is fond of printing photos of their favorite pop idol at three in the morning).

At the bottom left of this dialog is a *Printing defaults* button. Click this for control over how and what inks or toner the printer will use when a job is sent to the device. You might want to specify, for example, that all printing should be duplex and only be in black and white, which can save large amounts of money. Should somebody want to print in color, or single-sided, they will then need to manually change the print settings each time they wish to use those different settings.

Should a printer (or the PC) be used for color-sensitive work, such as photo or video editing, clicking the *Color Management* tab will allow you to load and customize individual color profiles for the printer, and for your PC's monitor.

If users are unable to print, this might also be down to them not having access to that specific printer. Access permissions can be managed in the *Security* tab, where you can specify individual or groups of users who can print to, and manage both the print queue and the printer settings itself; see Figure 7-18. This can be useful if you do not want users to be able to change your duplex, black-and-white–only policy back to single-sided and color.

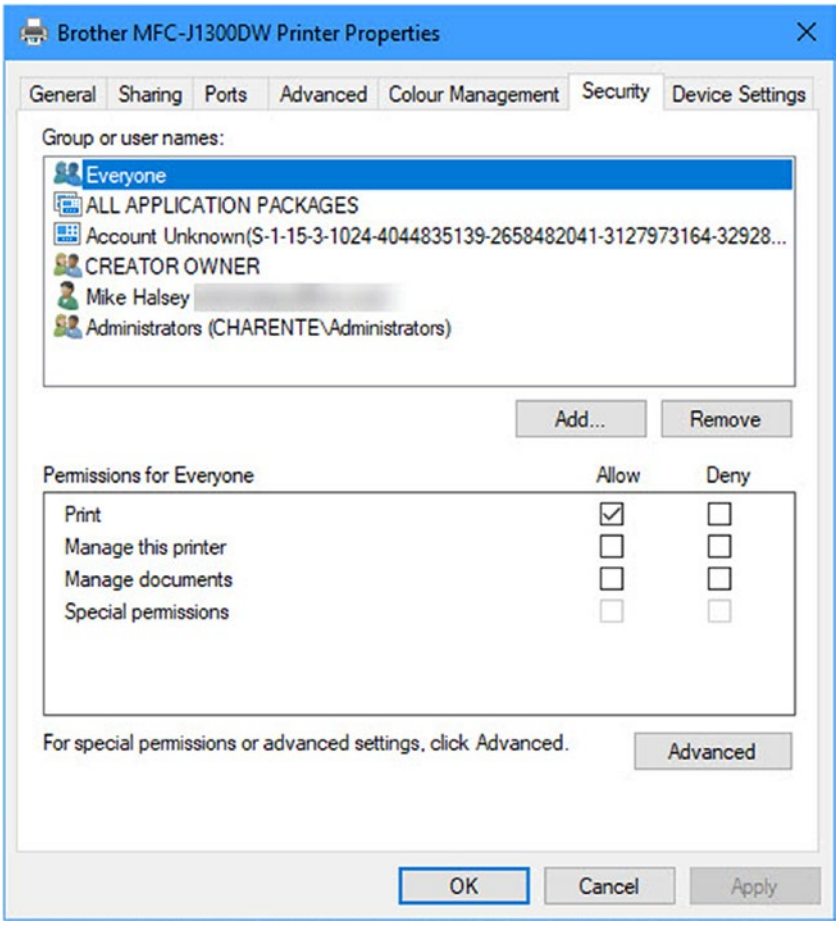


Figure 7-18. *You can manage access permissions for individual printers*

Have You Tried [Not] Turning It Off and On Again?

So, what happens when you can't connect to a printer, or you send a print job and nothing appears at the other end? Normally the response in this scenario is to turn it off and on again. (I can't believe I got all the way to Chapter 7 before saying that!) This isn't always the best approach to take with printers, however, for several reasons:

- Other people might also be using the printer, and you can interfere with their print jobs, which are very likely to be far more important than your own.
- Restarting a printer might not clear the print queue, which is managed by each PC connected to the printer.

So, if it's not the best solution to restart the printer if you can't connect to it, or print to it, what do you do? Well, if you're in a home environment, let's start by saying you're probably completely fine to turn the printer off and restart it. This can often make the printer spring back into life on a network, though any jobs already sent to it by the PC will be lost. It's not uncommon, especially with Wi-Fi–connected printers, that you might need to uninstall and reinstall the printer on a PC. This could be for several reasons, such as that the port assignment has become confused and a conflict with another device is confusing the operating system.

Right-clicking the printer in the Devices and Printers panel and clicking *See what's printing* (or double-clicking the printer icon that will appear in the System Tray when a job is sent to the printer) will reveal the printer queue. This is a great way to determine if the user has actually sent the job to the correct printer, which is a **very** common cause of printing failures!

In the print queue window, you will see a complete list of all the jobs sent to the printer, and which user or PC has sent them. Double-clicking a job will open a properties dialog for that job; see Figure 7-19. Here you can manage additional functionality such as setting the priority for the print job (effectively sending it to the top of the queue). You can also see if time restrictions are in effect.

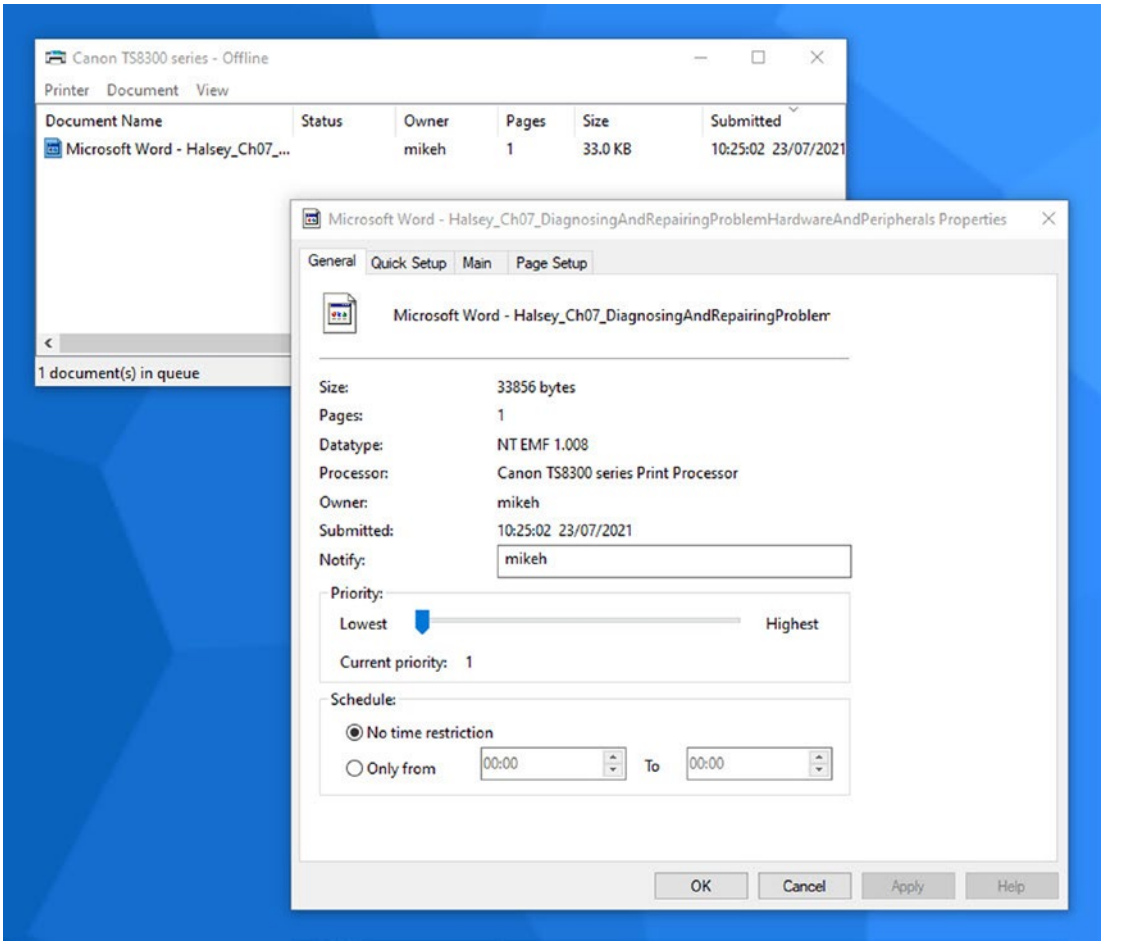


Figure 7-19. *You can set print priority and manage other settings from the Print Queue window*

If print jobs are snarled up, you can cancel individual jobs by right-clicking them and selecting *Cancel* from the options that appear. Additionally, the Printer menu offers the option to cancel all jobs for the printer simultaneously; see Figure 7-20. It's worth noting, however, that with some badly snarled print queues, a restart of both the printer and the PC that sent the job might also be necessary.

Tip Another way to fix a snarled print queue is to restart the *Print Spooler* service, in the Services panel. I will show you how to do this in Chapter 19.

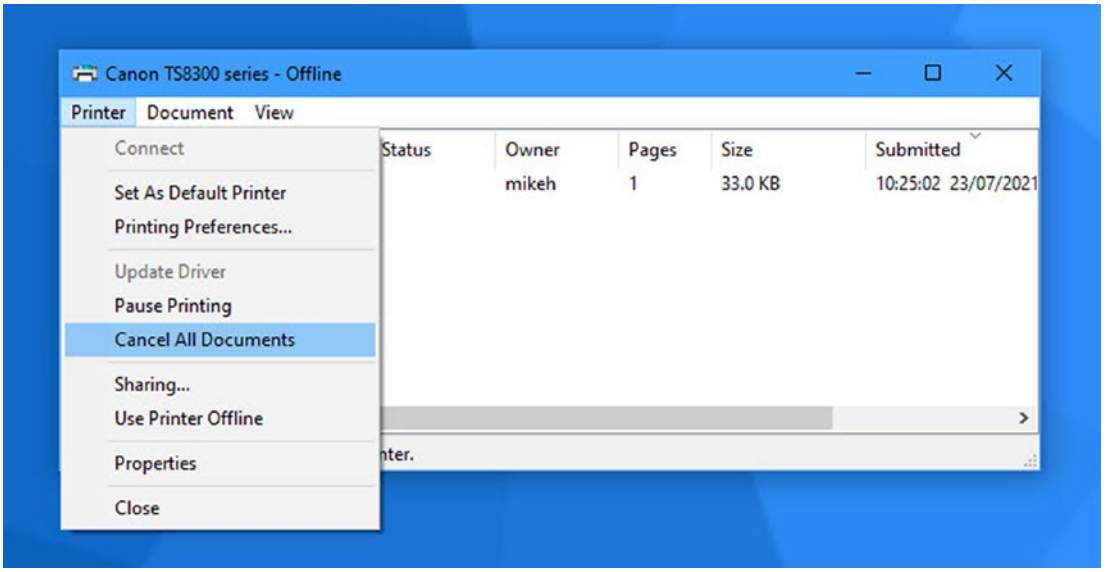


Figure 7-20. *You can completely clear the print queue from the Printer menu*

Tip Printers contain more moving parts than any other component in an office environment, and as such there's much that can go wrong with rollers and other paper-feed mechanisms. However, should your printing come out blurry or distorted, there will be an option in the printer's own options (you should refer to the printer manual to find exactly where) to clean the print heads or to also realign the heads. Performing these actions can fix some issues with poor-quality output.

Summary

Good management of devices is crucial to making sure that problems don't occur and, as printers are the most used accessory in any home or office environment, good setup and management of a printer can make the difference between a quiet day for a support technician and a very difficult one.

While we're on the subject of having a difficult day, however, nothing can be more bothersome for a user or IT pro than a PC that fails to start at all, so in the next chapter, I'll show you how to fix common startup problems and use Windows 10's inbuilt tools to get a PC booting to the desktop.

CHAPTER 8

Troubleshooting Startup

Nothing is more annoying than a PC that won't boot to the desktop, so knowing how to get a Windows 10 installation working again quickly is a skill every IT technician and professional should know. In Chapter 13, I'll show you how to get inside the Windows 10 boot system and effect manual repairs for the worst scenarios, but as expediency is always the order of the day when it comes to diagnosing and repairing PC problems, I want to start with the things you can do to get Windows booting again quickly.

Have You Tried Turning It Off and On Again?

In order to be able to quickly repair startup problems in Windows 10, it's useful to understand what issues can affect startup, and what the common problems are that occur. There aren't actually too many things that can affect startup, but knowing what's happened can often help quick diagnosis and guide you toward the correct repair method:

- **Improper shutdown** is by far one of the most common causes of Windows being unable to boot. This can occur either by the user switching the PC off improperly (pressing and holding the power button for 4 seconds, or switching the PC off by pulling the power cord out of the wall or at the back of a desktop PC, which can often occur when people trip over them risking damage to the cable and PC in the process). However, it can also be caused by a power outage, and in some parts of the world, these can be quite common. Improper shutdown can corrupt some of the startup files, or perhaps corrupt the startup partition. In this case the more advanced methods detailed in Chapter 13 might be needed if the methods detailed in this chapter don't help. For example, where I live in France there is only a single-phase electricity supply, instead of the

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_8

two-phase supply of countries including the United Kingdom and United States. The upshot, without getting too technical, is the supply is much more prone to spikes in France, and so all my valuable computer and electrical equipment has to be permanently plugged into Uninterruptible Power Supplies (UPS) to stop them blowing up in a storm, as surge protectors simply don't cut it here.

- **Botched driver or update installation** is another common reason for a PC failing to start. This can include Windows Updates and hardware driver installs and updates. It's worth noting that graphics drivers can be particularly prone to this problem, as they are embedded deep into the OS. These problems can be repaired from the System Rescue Options menu.
- **BIOS or firmware update** is something I'll mention even though it's not strictly a Windows startup problem. I detailed how to repair a BIOS or UEFI firmware system in Chapter 6.

Note With Microsoft's Surface range of computers, many driver updates are named as firmware updates. They're really not; instead, they're motherboard or graphics drivers. This means that if a "firmware update" with a Surface device results in Windows 10 being unable to boot, a System Restore can still often fix the problem.

- **Hardware change or update** can also cause Windows 10 to not start. Perhaps a component has failed (such as the motherboard) and been replaced. With some hardware in the PC (memory, CPU, hard disk), you can swap them out and restart the PC with ease. Motherboards are different, however, and unless you have an identical model, you might be faced with reinstalling Windows 10 from a format due to the way drivers are embedded into the OS. Additionally, adding or changing hard disks in a PC can swap their drive assignments on the motherboard (Drive 0, Drive 1, etc.), and this can result in the PC attempting to load Windows from the wrong drive. Swapping the drive data cables can often fix this problem.

There are ways that common startup problems can easily be fixed, not the least of which is just turning the device off and on again (yup, that old trick). Additional quick methods exist, however, to help you get up and running quickly:

- **Undoing whatever it is you just did** is usually a good way to get the PC working again, and will normally occur if you have changed the hardware in some way. Perhaps you've installed a new piece, or changed a piece of hardware. Changing things back to the way they were before will often get the PC working again, and give you time to diagnose what caused the problem.
- **Booting with or without the power lead** on a laptop or tablet can solve some startup problems. It might be that a PC is unable to start because it's just not got enough power to get it going. Alternatively, it might be that on a laptop or tablet, a fault with the power brick or the power plug is causing interference that is preventing startup from occurring.
- **Using a minimal boot configuration** can often help too, and can help you diagnose the real cause of the problem. Unplugging all unnecessary cables and devices (network, USB, etc.) and starting the PC without them can sometimes rectify the problem. It's not uncommon for a PC to hang at startup because of a glitch with the network cable or signal. In these cases, unplugging the network cable results in the PC being able to continue booting.

Using Startup Repair

If Windows 10 fails to start correctly two or three times, then the automated Startup Repair system will be invoked. This works by resetting startup components in the OS to their default state, and this can fix some of the easier-to-diagnose and most common startup problems with the OS.

You can run Startup Repair manually from a System Recovery Drive or from a Windows 10 installation media by opening the System Recovery menu (click *Repair your Computer* at the Setup screen if starting from installation media) and then clicking *Troubleshoot* and *Advanced Options*. You will see *Start-up Repair* listed at the next screen; see Figure 8-1.

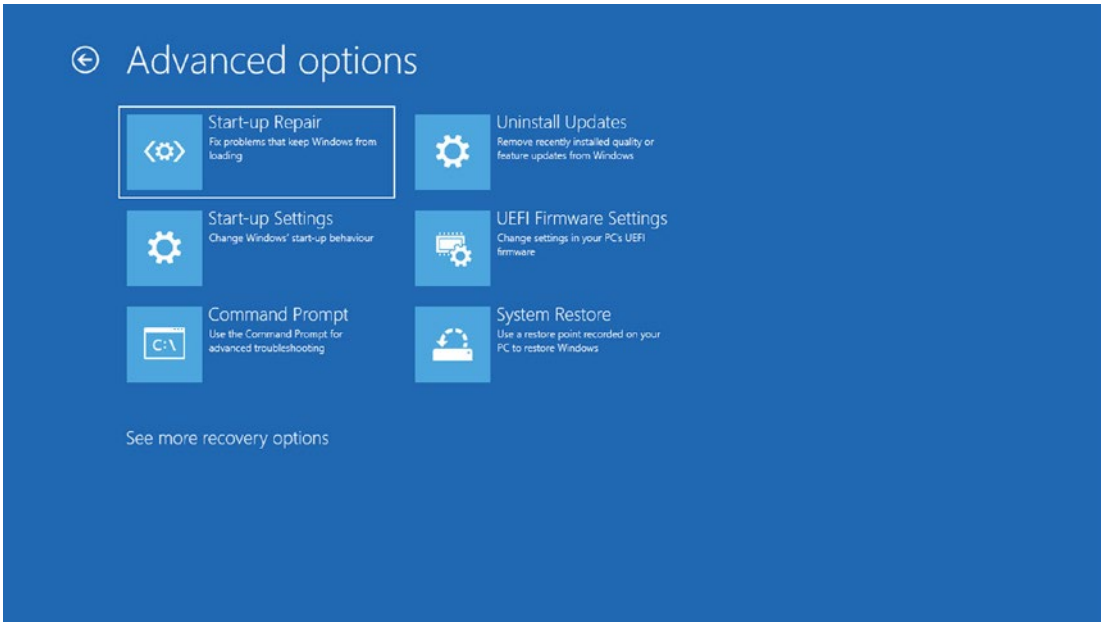


Figure 8-1. *You can run Startup Repair manually from the Recovery Options*

Note If an Administrator password is set on the PC, it will be necessary to enter this when performing many tasks within the Recovery Environment, and you may require a Bitlocker unlock code for some tasks as well.

You may be asked for the Administrator password and your Bitlocker recovery key if your drive is encrypted. If Startup Repair is able to fix the problem, it'll do so, and you'll be asked to restart the PC. If it isn't though, perhaps because it's unable to identify the problem, then you'll be prompted and given the details of the log file it created during the repair process; see Figure 8-2.

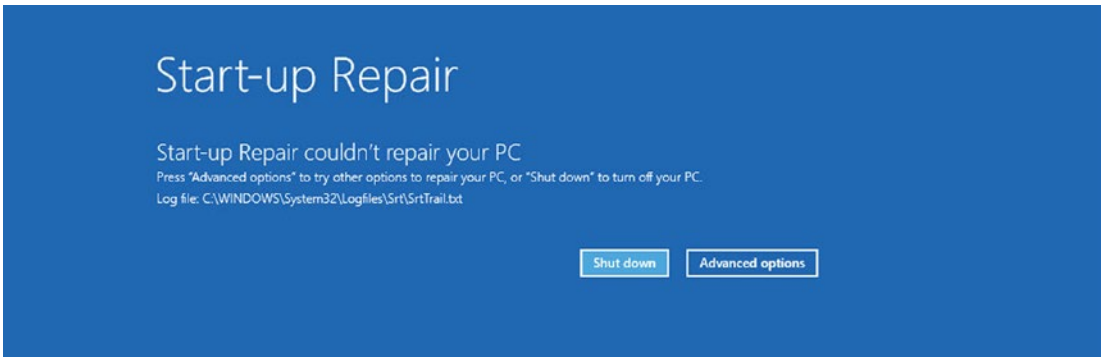


Figure 8-2. *You will be shown the location and name of the repair log file if Startup Repair cannot fix the problem*

Clicking *Advanced Options* at this point will return you to the Recovery Options menu, where other repair options are available to you. If you open the log file, you'll be shown details of all the tests performed by Startup Repair, with any errors discovered detailed; see Figure 8-3. You can use this information to help diagnose and get to the root cause of the problem.

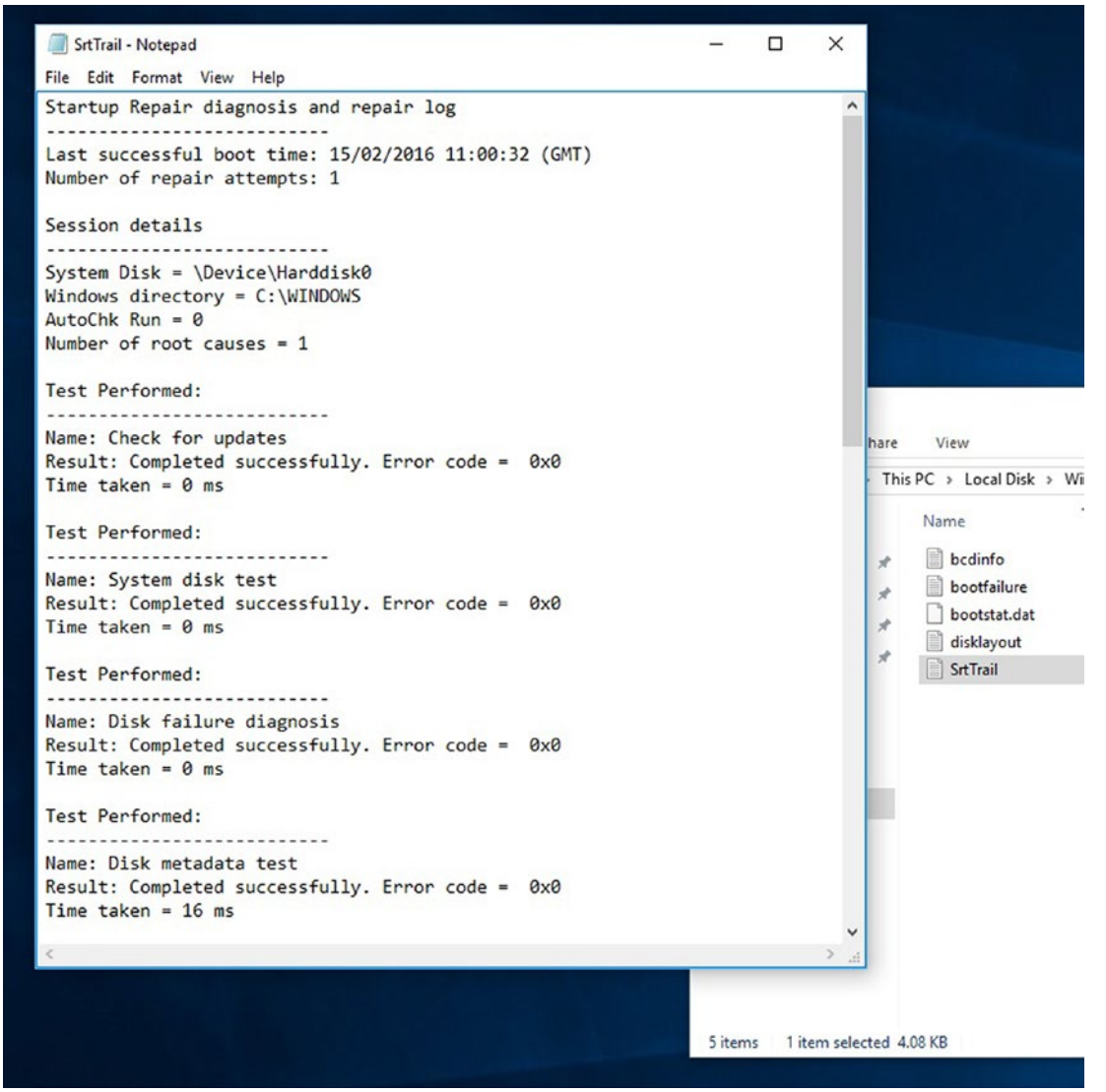


Figure 8-3. *The repair log file contains details of all the tests performed*

To open these log files from the Recovery Options menu, click *Troubleshoot* and then *Advanced Options*, and open the *Command Prompt*. When the Command Prompt is open, type **Notepad** and press Enter to open the text file reader/editor app. In this you can open the log file; see Figure 8-4. Note that you will by default be in a `\Windows\System32` folder, but you will be on an X: (boot) drive, which is actually a hidden boot partition. You will need to navigate to the drive on which you have Windows installed (usually the C: drive) to see the log files.

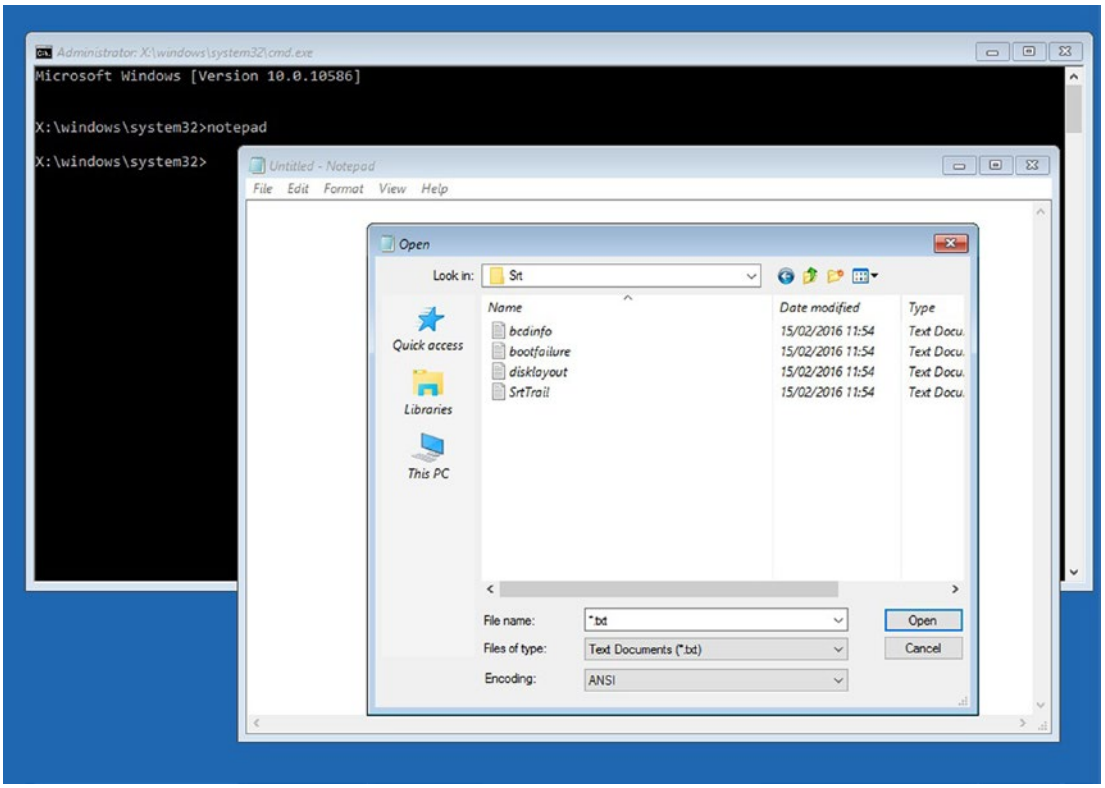


Figure 8-4. *You can open and read log files from the Recovery Environment*

Also in this *Logfiles* folder, you will see a **bcdinfo** file. This will provide details of the boot setup for Windows 10, and it can be worth checking; see Figure 8-5.

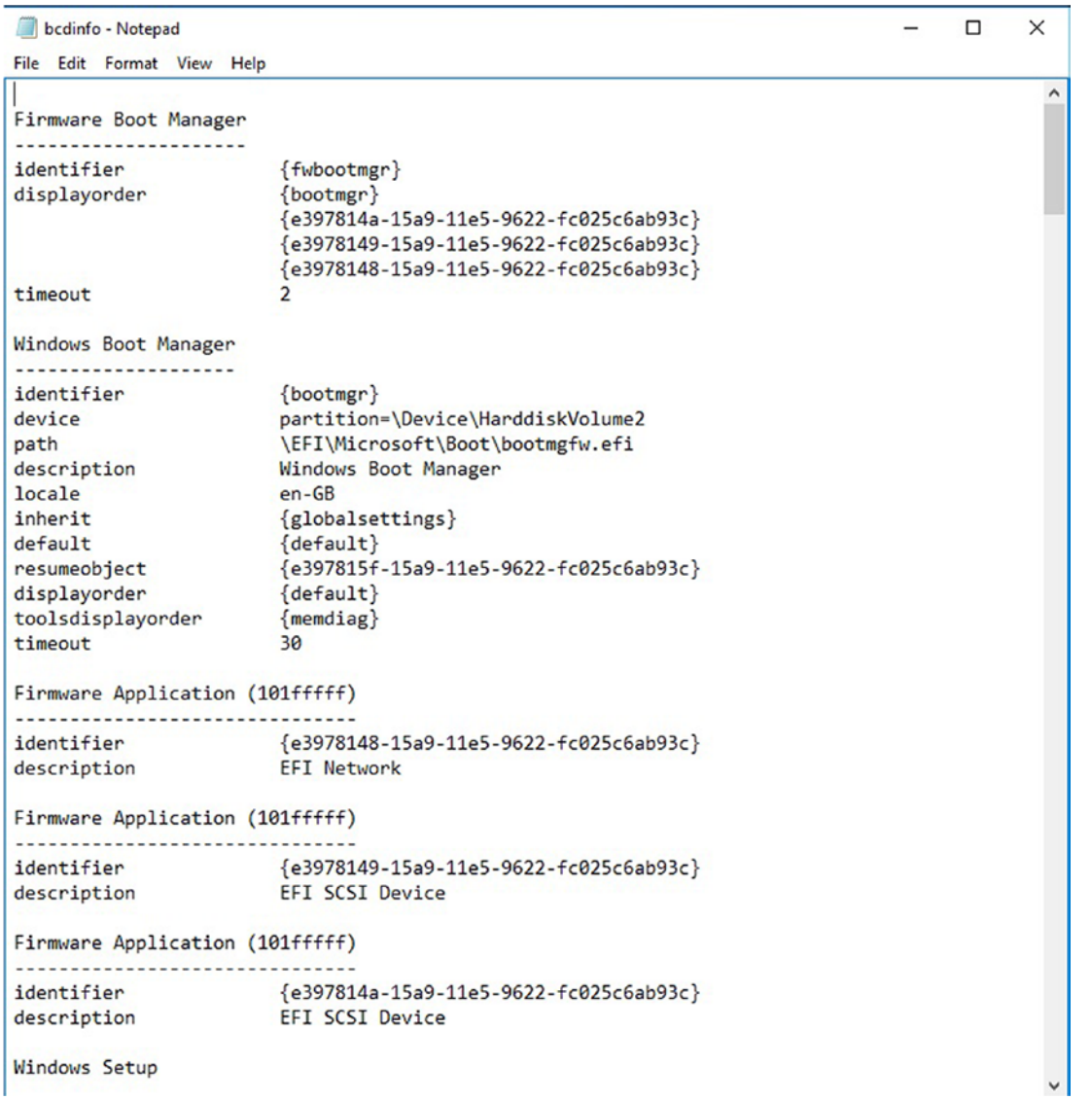


Figure 8-5. *The bcdinfo file contains details about the boot system*

You will see your individual operating systems listed in this file, with Windows 10 listed as *Windows Setup* and *Windows Boot Loader*. Check the driver letter assignments for the OS to see if they are correct. If you need to change these, you can use the **BCDEdit** utility, which I will show you how to use in Chapter 13.

The Windows Recovery Options Menu

I've already talked a bit about the Recovery Options menu in this chapter, but I want to show you the other tools available there to help you fix Startup problems in Windows 10 quickly, as there are a few.

As I've already mentioned, there are a few ways to get to this menu; see Figure 8-6. You can start your PC from a USB Recovery Drive, or from Windows 10 installation media (where you'll need to select *Repair your computer* at the installation screen), and Windows 10 will try to load this automatically if it cannot start two or three times.

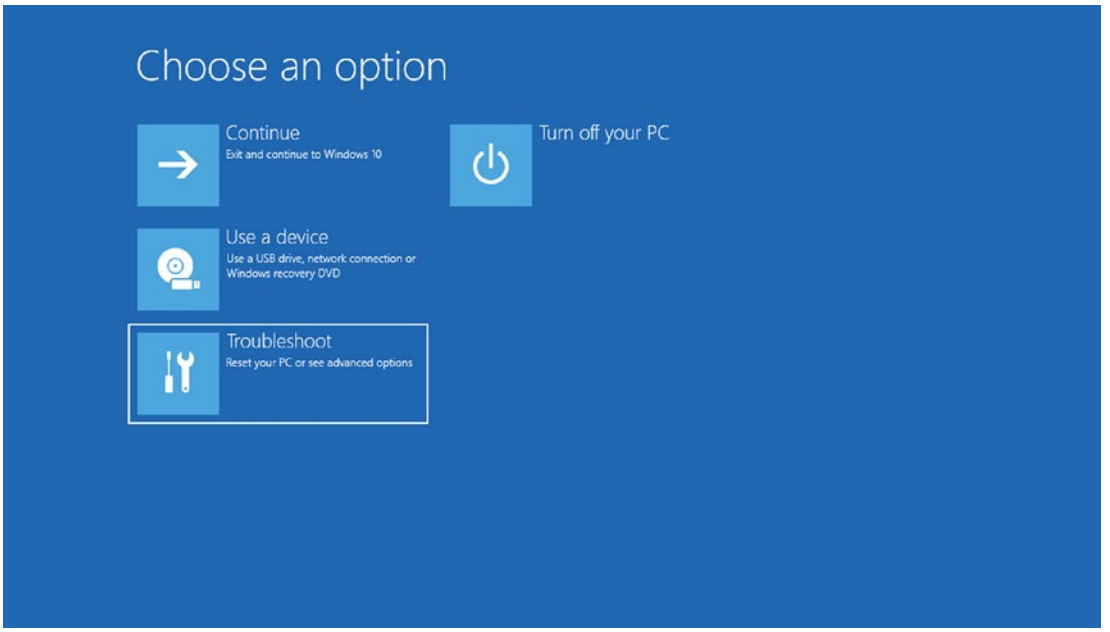


Figure 8-6. *The Recovery Options menu in Windows 10 contains many useful tools*

It's in the *Troubleshooting* ➤ *Advanced Options* menu that most of the really useful options appear; see Figure 8-7. I want to detail the options that are available here that can help you repair Windows 10 startup quickly:

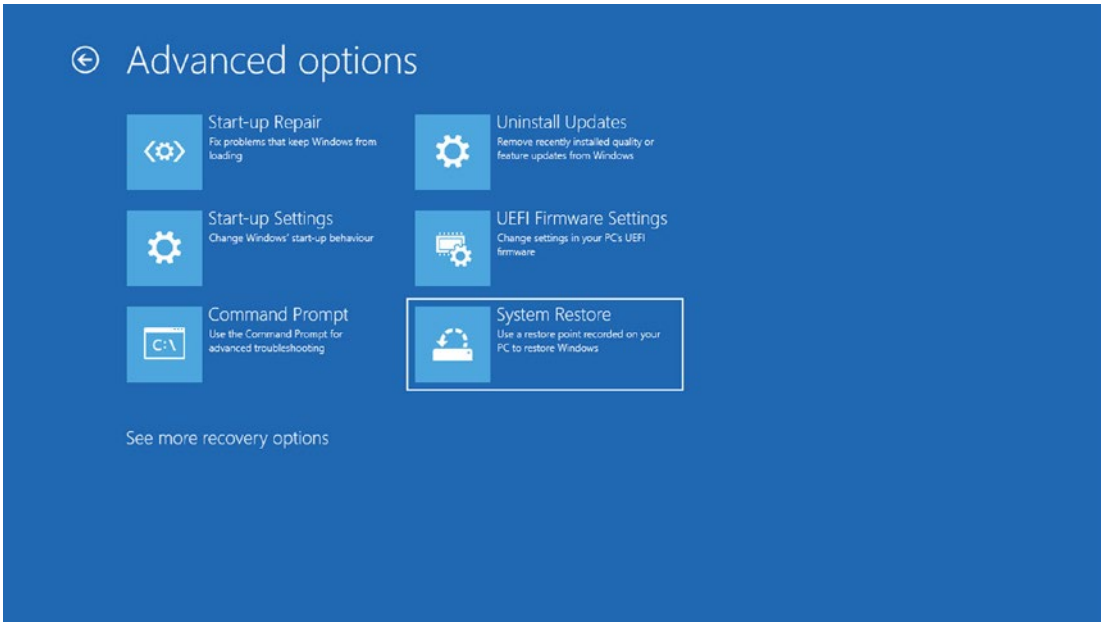


Figure 8-7. *The Advanced Recovery Options are where all the Startup Repair action takes place*

- **System Restore** is most useful if a Windows Update or another installation such as a hardware driver installation has resulted in the PC being unable to start. You can use System Restore to roll the Windows 10 system files back to the point before that installation occurred, whereupon you can install the offending item again, block it, or search for an alternative to install.
- **Command Prompt** is something I'll talk about in more depth shortly.
- **UEFI Firmware Settings** will appear as an option if you are not using the older BIOS firmware system on your motherboard. This is a quick-launch button to open the UEFI settings panel, in which you can check settings such as the disk boot order (which might have become corrupt or altered).
- **Uninstall Updates** can be used to roll back changes made by Windows Update, including Feature Packs which have caused startup to become unstable.

- **Start-up Settings** will open what might be considered a more traditional boot options menu; see Figure 8-8. This includes yet more options.

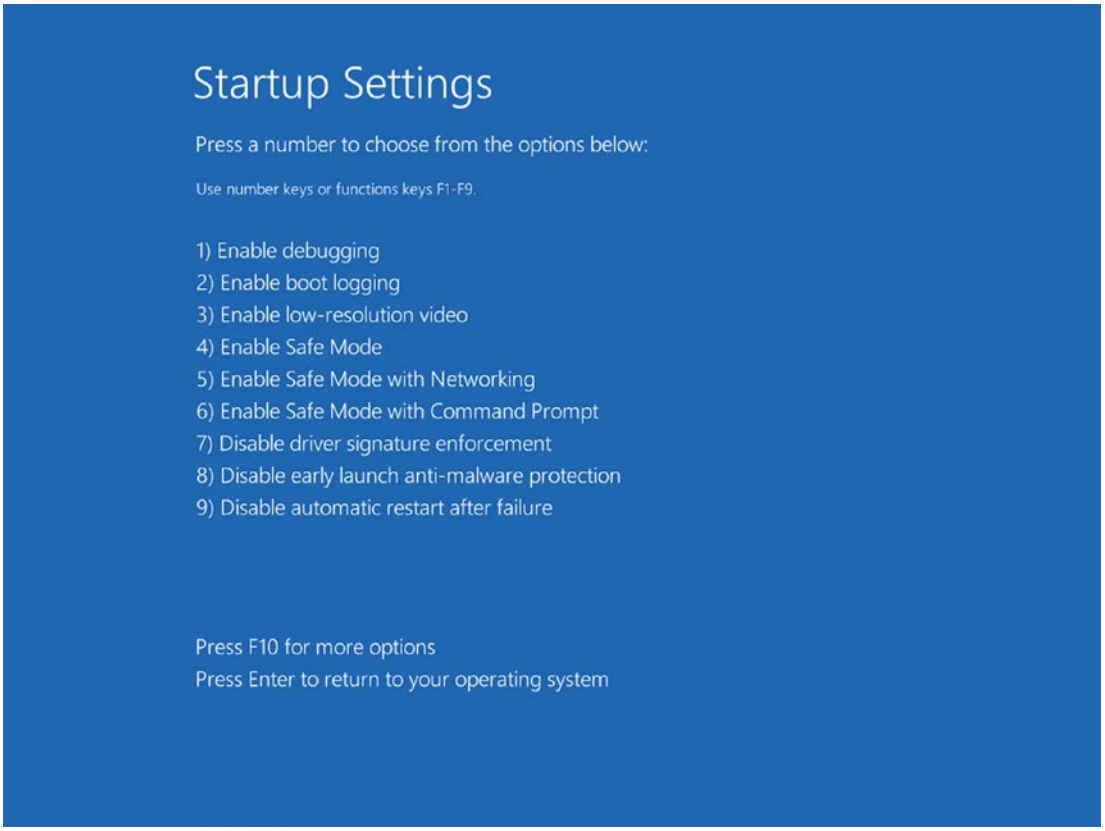


Figure 8-8. *Additional startup settings are available including Safe Mode*

- **Enable Debugging** activates the inbuilt debugger for the Windows kernel (the core OS files). If the PC is connected to another computer running a debugger, this information can be collected by the remote machine for diagnosis. This connection can be made via a null-modem cable, IEEE 1394 (FireWire) cable, or USB. Full details of how to use this feature are available at `http://pcs.tv/1XsRKFf`.
- **Enable Boot Logging** will start Windows 10 normally, but will create a file called C:\Windows\ntbtlog.txt containing details of all the files and drivers loaded at startup. This file can be accessed using Notepad, either at the desktop or through the Command Prompt, to help you diagnose and repair problems.

- **Enable Low-Resolution Video** will start the PC in an 800-by-600-pixel resolution. It's mostly here for legacy support on older systems, but might prove useful for diagnosing problems with some graphics drivers.
- **Enable Safe Mode/Safe Mode with Networking/Safe Mode with Command Prompt**. I'll detail how to use Safe Mode, which is a reduced-functionality mode, fully in Chapter 19, but it can be a useful environment for uninstalling problematic components in Windows 10.
- **Disable Driver Signature Enforcement** will allow unsigned (nondigitally signed) drivers to be loaded at Startup. This can be useful if you are troubleshooting a problem with a driver which has not been submitted to Microsoft's certification process.
- **Disable Early Launch Anti-Malware Protection** can be useful if you suspect it's a problem with your antimalware software, or an update to that software that's preventing Windows 10 from starting. By default, and for reasons of security, Windows 10 loads your antimalware software before any other apps. However, if it is causing a problem, startup can hang at that point unless you select this option to allow the software to start at the same time, and in the same way, as other apps.
- **Disable Automatic Restart After System Failure** can be useful if your PC is displaying a Blue Screen of Death (BSD) (what I now call the Blue Unhappy Emoticon of Death) but is restarting automatically before you can read the message. I will detail Blue Screens in more detail in Chapter 11.

Using the Command Prompt to Repair Windows Startup

While it's annoying and frustrating that you can't use PowerShell from the Recovery Console (hopefully this will change in the future), even though the available option is limited and doesn't support the full range of commands available at the desktop, the Command Prompt as run from the Windows Recovery Environment can be a very useful tool for quickly repairing Windows 10 startup problems.

In the Command Prompt here, the following commands are available to you:

- **Attrib** is used to change the permissions (read, write) on files.
- **Bootrec** is a tool I'll detail fully in Chapter 13. It is used to repair the Master Boot Record (MBR) and Boot Configuration Data (BCD) for the PC.
- **Bcdedit** is another tool I will detail in Chapter 13. It is to edit and make changes to the Windows BCD.
- **Cd** is used to change the current directory. You can specify a directory, that is, `cd \Windows`, or go back a folder using `cd`.
- **Chkdsk** is used to check the hard disk for errors. It is commonly used with the switches `/F` (fix errors), `/R` (recovers unreadable information in bad sectors), and `/X` (forces the volume to dismount if necessary). Additional commands are available and detailed on the `/?` Switch.
- **Copy** will make a copy of a file in the format `Copy C:\Folder1\File.ext C:\Folder2\NewFile.ext`.
- **Del** will delete a file.
- **Dir** will list the contents of the current directory or folder.
- **Diskpart** is a tool I'll detail in Chapter 13. It contains powerful disk management and partitioning tools.
- **Icacls** is used to modify file and folder permissions and modify access control lists.
- **Mkdir** is used to create a new folder.
- **More** displays output one screen at a time.
- **Move** can move a file or files from one place to another, and is used with the same syntax as Copy.
- **Ren** is used to rename a file or folder.
- **Rd** can remove an empty folder.
- **Type** displays the contents of a file, such as a log file.
- **Xcopy** is a more advanced version of copy, with more options available.

In addition to these commands, the following apps can be run from the Command Prompt:

- **Notepad**, as I detailed earlier in this chapter, can be used to read log and error files.
- **Regedit** is something I will detail in full in Chapter 19. It is used for making changes to the Windows Registry.
- **Rstrui** is used to start System Restore from the Command Prompt.

Summary

In Chapter 13 I'll detail how you can, if necessary, manually repair the Windows 10 boot system, but the tools and utilities in the Recovery console can help get a nonbooting system working again quickly and in a straightforward manner, and let's be honest, that's what everybody needs when their PC won't start.

Aside from Startup however, there's one other feature of PCs that drives us nuts when it won't work. This is networking. If we can't get access to our network files or (heaven forbid) the Internet, then the world can seem to come crashing down. I've seen people over the years who seem to completely forget how to feed themselves and stand upright if they lose their Internet connection. Needless to say, we'll be covering this in the next chapter.

CHAPTER 9

Troubleshooting Networks

Next to being unable to boot a PC to the desktop, by far the most irritating problem anybody can have with PCs is being unable to access networks, especially the Internet. We pretty much live our lives online both at home and at work. If you're wanting to do some shopping or banking, you want to be online. If you need access to the college library system or resources for your dissertation, you need to be online, and if you're collaborating on files with colleagues for an important project, you need network and/or Internet access.

Most network problems, in fairness, are pretty easily fixed, and the good news is that the tools that Microsoft provide as part of Windows can really help in this regard. These tools and utilities haven't changed that much in 15 years, which makes them both mature and reliable. They're also comprehensive, so let's spend some time looking at what each is, and how they can be used to troubleshoot and repair network and Internet connection problems.

The Network and Sharing Center

The Network and Sharing Center is the main hub for controlling and managing network and Internet connections on the PC, certainly from a troubleshooting standpoint as well as from a management and troubleshooting perspective; the Settings app (which I'll detail later in this chapter) isn't as useful. You can open it from within the Control Panel.

The Network and Sharing Center is standard Windows console fare, with quick links to network utilities in the top left corner, more quick links to related Control Panel items in the bottom left corner, and a panel-style main section containing network connection information, and further links to tools; see Figure 9-1.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_9

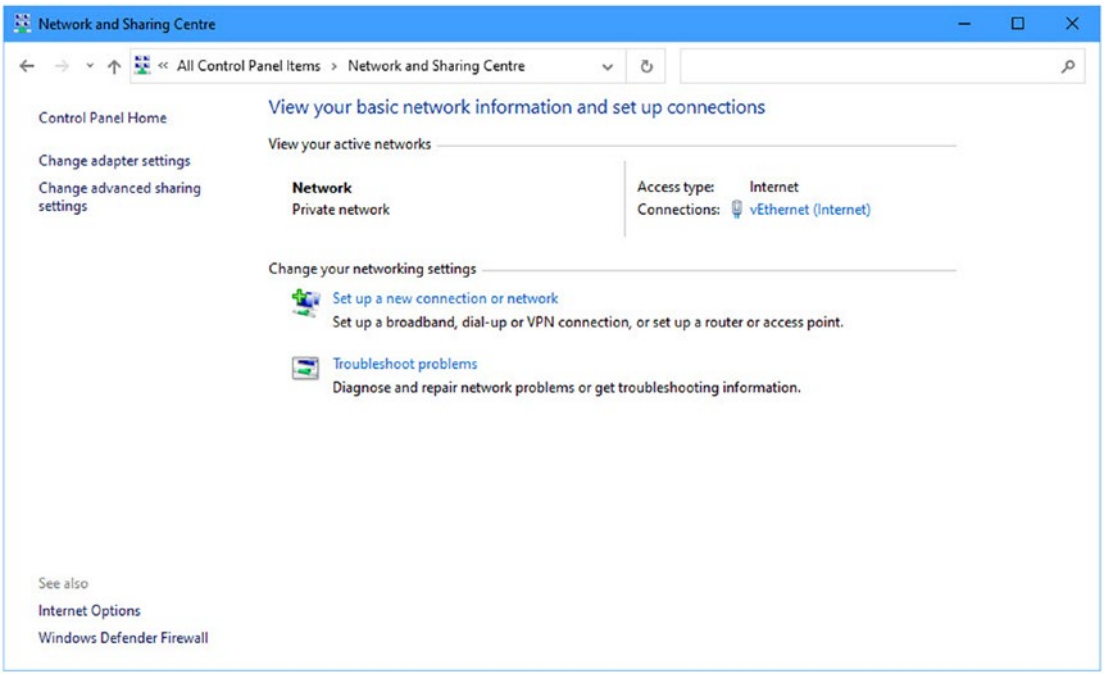


Figure 9-1. *The Network and Sharing Center in Windows 10*

You can get quick information about the current status of a connected network by clicking the *Connections [network name]* link near the top right of the window. This displays details of both the IPv4 and IPv6 connectivity (as you might be connected via one but not the other), the length of time the connection has been active, and the current network speed. Perhaps most useful is the Activity monitor. This will show you in real time the number of data packets being sent and received by the PC; see Figure 9-2.

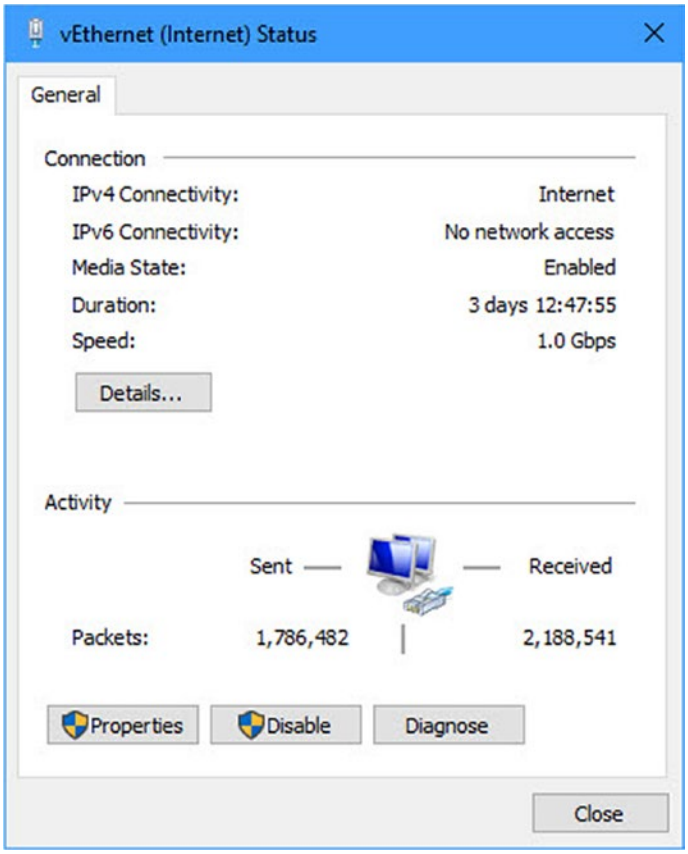


Figure 9-2. *You can get quick status information about the current network connection*

On a working network connection, there should be a fairly constant stream of data passing back and forth, even if you're not doing much with the computer. This data will primarily be handshaking with the router, to maintain the connection, but other apps and services (from cloud sync and backup apps to Windows Update and time sync) will also be running.

If at any time you want to know exactly what is using your network bandwidth, you can open the Resource Monitor by searching for **resource** in the Start Menu. This will display a full list of all the apps and services that are communicating with a server or the Internet, complete with details on the amount of data they are sending and receiving and, perhaps most usefully, the name or IP address of the local or web server they are communicating with; see Figure 9-3.

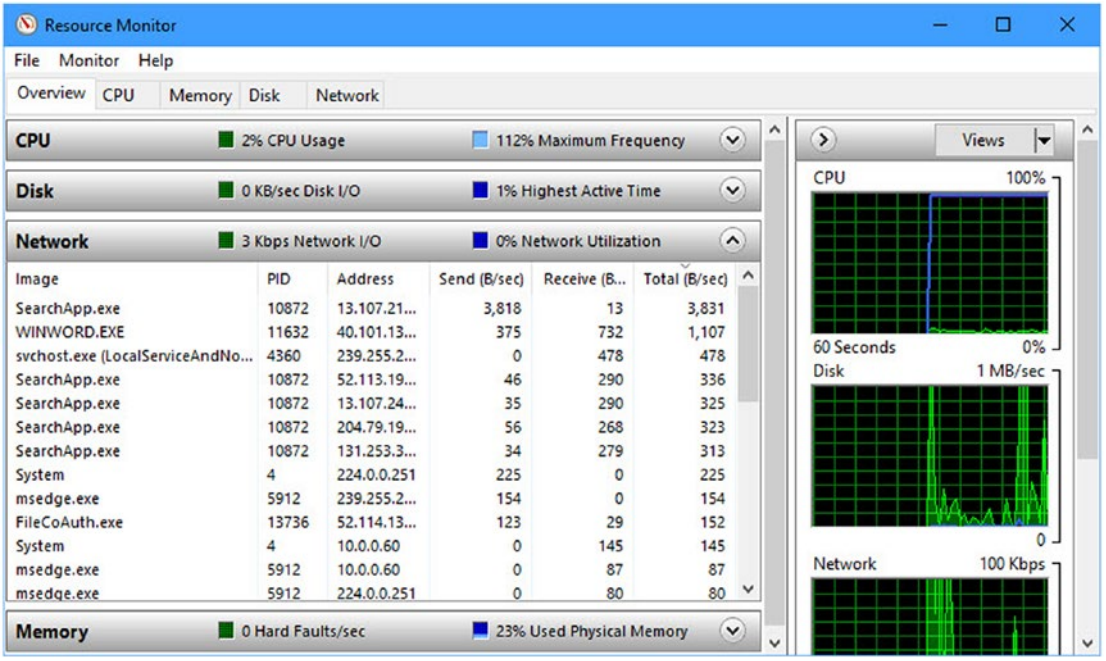


Figure 9-3. *The Resource Monitor can provide details of all network activity*

If you ever suspect that an app or service, or perhaps a piece of malware, is hogging network bandwidth on a PC, the Resource Monitor is definitely the place to check. On a network with multiple PCs, your router may provide a feature whereby you can check the current network usage for each connected PC and device (you should check the documentation that came with your router). You can then use this information to identify the bandwidth-hogging PC, and narrow it down to the specific app or service that's causing the problem.

Configuring Network Connections

Back in the Network Status dialog I showed you in Figure 9-2, there are four buttons which can provide further information about the current network and its status. The first of these is the *Details* button, which will display further information about the current network connection; see Figure 9-4.

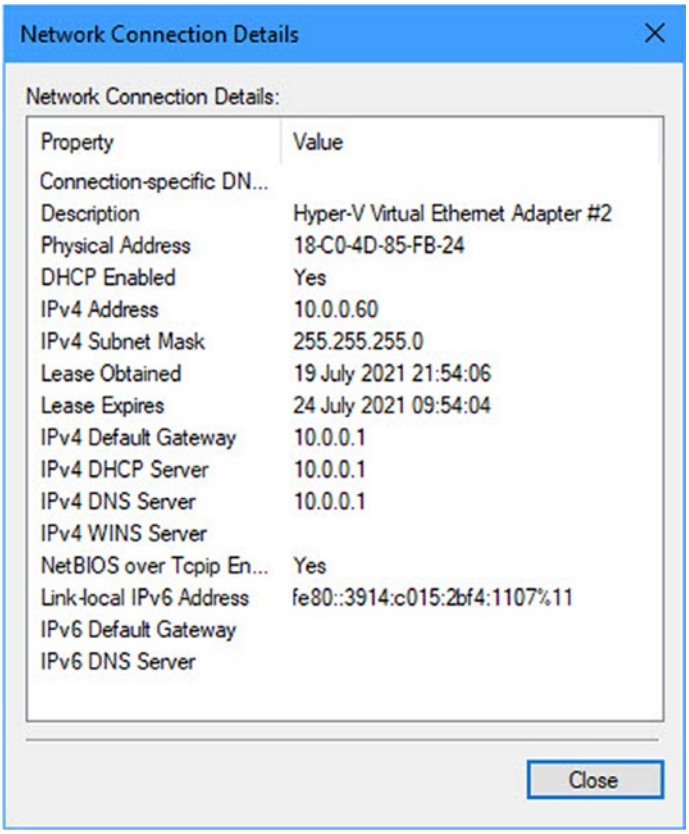


Figure 9-4. *You can get advanced information about the current network connection*

This information includes the IP address(es) of the PC on the network and information about the activation status of services such as Dynamic Host Control Protocol (DHCP), which is used to autoassign IP addresses by a router, and which might need to be disabled in some business-specific circumstances.

At the bottom of the Network Status dialog are three buttons. *Disable* is a quick link to disable (and reenable) the connection. *Diagnose* will launch an automated troubleshooter that can fix some problems by resetting the connection to its default state. The remaining button, *Properties*, will display advanced configuration options for the connection; see Figure 9-5.

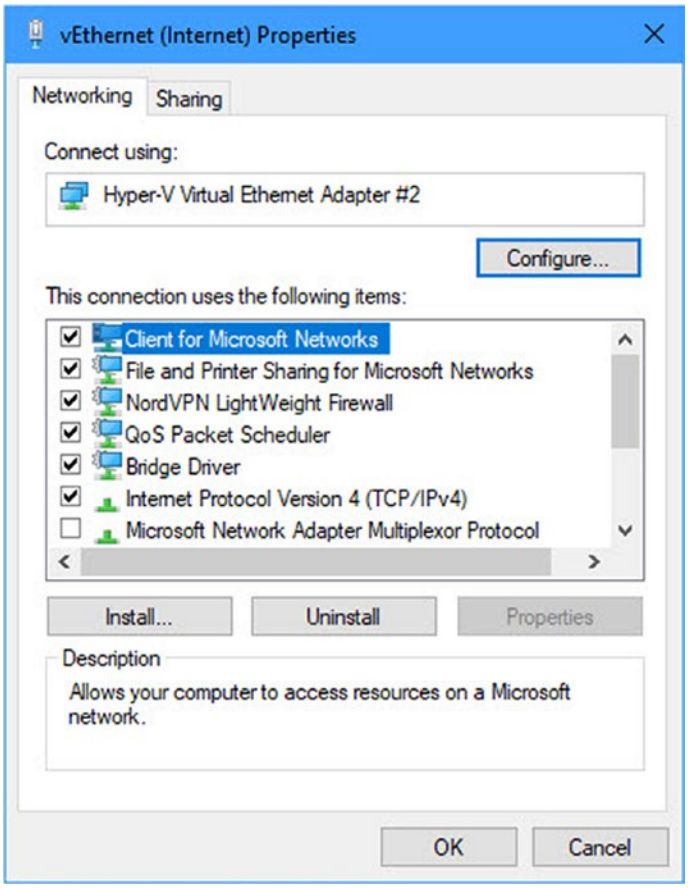


Figure 9-5. *You can manage advanced configuration options for the network connection*

There are two tabs in the Network Properties dialog; I want to deal with the second tab first as it's the more straightforward of the two. The *Sharing* tab contains options that allow the sharing of the computer's network connection with other PCs. Let's say that you have one PC connected to the Internet during a period of Internet downtime, with the only connected PC doing so through the user's cellular phone. This connection can be shared with other PCs but only if all are connected via a wired network. This feature is mostly a legacy hangover from the days when one PC had to be physically plugged into a USB broadband or dial-up modem, though there may still be occasions when it's useful.

Okay, so back to the *Networking* tab, which is by far the more important of the two. Here you will see a list of network services and protocols available to and in use by the network connection. These include, as you saw in Figure 9-5, services such as "Client

for Microsoft Networks," which allows the PC to connect to other Windows PCs, and "File and Printer Sharing," which can also include features and services such as Hyper-V switches.

Perhaps the most useful, certainly from a troubleshooting standpoint, are the IPv4 and IPv6 options. For some, but not all, network services in the list, but certainly for the IPv4 and IPv6 options, you can click the *Properties* button to get access to additional configuration settings.

The IPv4 options (see Figure 9-6) allow you to choose if IP (Internet Protocol) and DNS (Domain Name System) addresses are automatically assigned on handshaking between the PC and the router, or if they should be statically assigned instead. Note that static addresses need to be assigned on both the PC and the router. The Alternate Configuration tab allows for laptops and tablets that are used on more than one network. You might, for example, need to assign static IP addresses for PCs at work, but have users switch to router-assigned dynamic IP addresses when they take the device out of the workplace.

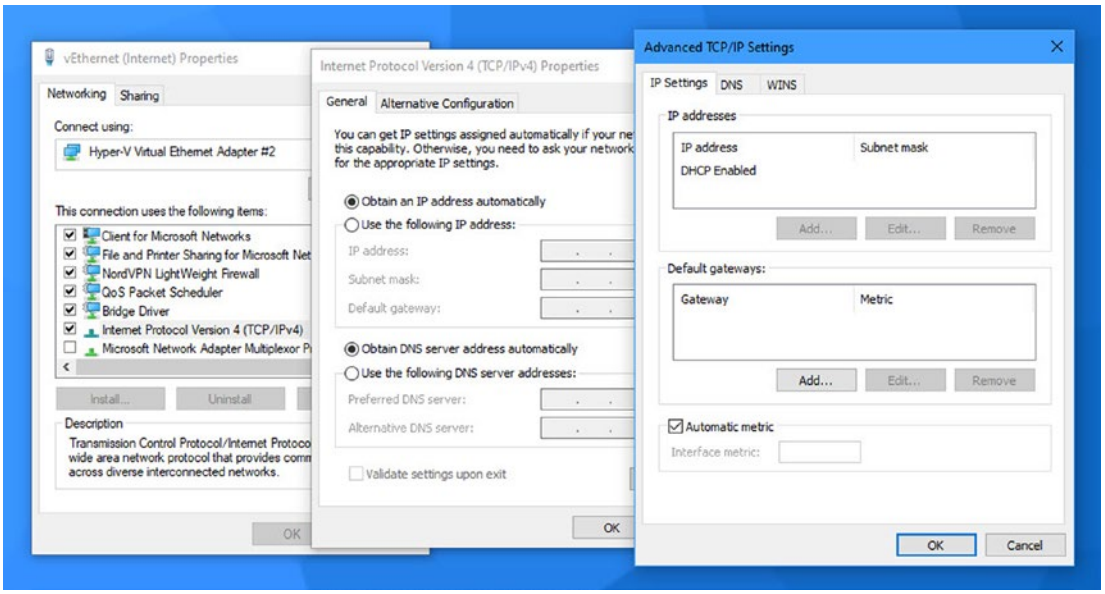


Figure 9-6. *You can manage IPv4 options in Network Settings*

Any additional options that need to be set or checked will be because they are already specified by the network administrator. These can include whether multiple DNS addresses need to be specified for the PC and if the default gateway (normally 192.168.x.x) must be specified.

IPv6 settings can also be configured, although because of the different way that IPv6 operates, not all of the features available for IPv4 connections are available such as WINS (Windows Internet Name Service); see Figure 9-7.

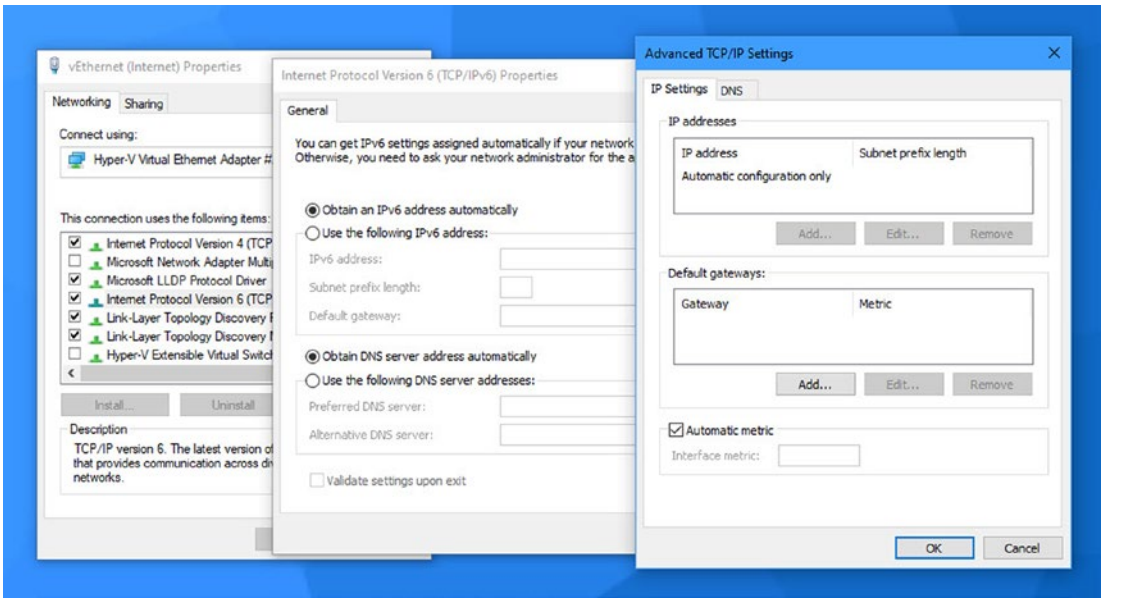


Figure 9-7. *You can configure IPv6 settings in the Network Properties*

You may find that a network Service or Protocol that you require for network access isn't installed. This might be required for high-security implementations or where custom network hardware is in place. Alternatively, you might have an older mission-critical PC still running a Base-T network system, and have to install a specific protocol to permit network connections. To add a missing Service or Protocol, or to install a driver to permit access to another specific PC that requires it, click the *Install* button in the Network Properties dialog. Here you will be prompted for a driver file or disk to install the feature you require, or with a list of available services that Windows 10 can install automatically, but that are disabled by default, perhaps for security reasons; see Figure 9-8.

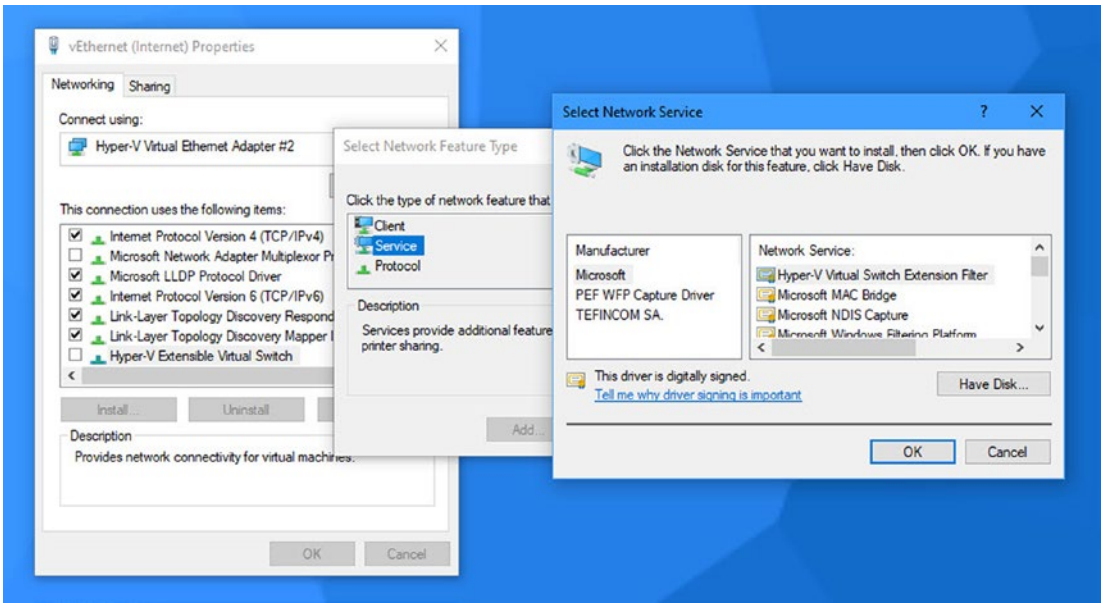


Figure 9-8. *You can install missing network services or protocols*

Lastly, the Network Properties dialog contains the *Configure* button. Clicking this will display the driver options for the network device, and I'll talk you through driver install and maintenance in full in Chapter 15. However, the Advanced tab in the driver properties will allow you to set and change properties for specific hardware driver properties; see Figure 9-9.

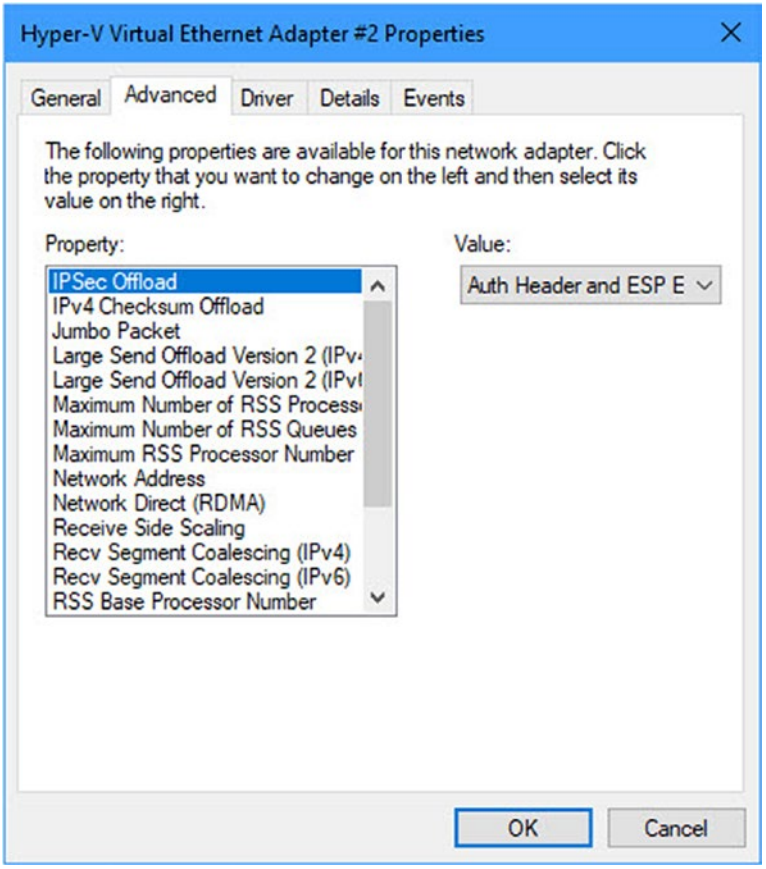


Figure 9-9. *The Configure options permit settings of specific settings for the network driver*

These settings will vary depending on what type of network connection you have installed, but can include checksum and authentication settings, both of which are used by Windows 10 to determine if data is being sent and received correctly, and without errors.

Managing Network Adapters

In the top left of the Network and Sharing Center is a *Change adapter settings* link. Clicking this will display a list of all the network adapters currently installed on the PC; see Figure 9-10. Double-clicking any of the displayed adapters will open its properties dialog, as detailed earlier, but additional functions are available on a right-click. Note that if, like I do, you have virtualization and a VPN installed on your PC, the number of adapters can look fairly daunting.

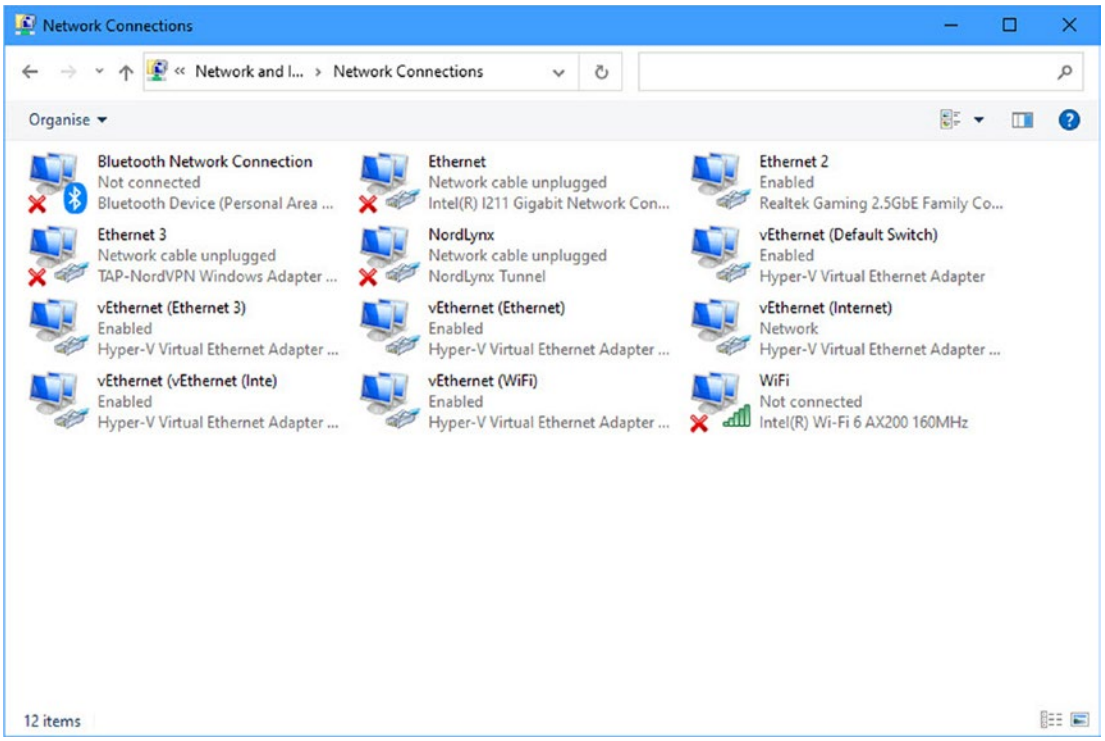


Figure 9-10. *You can view details of all the network adapters installed on the PC*

These additional functions include being able to quickly enable and disable a connection (disabled connections are shown in Figure 9-10 with red cross icon overlaid on them). Additionally, an option exists to *Bridge* several connections. Bridging allows you to bring multiple connections together as though they were a single connection such a using two 10-GbE ports as a single fast 20-GbE link.

Managing Network Connections in Settings

Many network management and connection options have been moved to the Settings panel in Windows 10. Indeed, we can expect more options to be moved here in the future, perhaps even by the time you read this, as the Control Panel has been gradually reduced in functionality and eventually will be removed from the OS completely.

The Settings panel, as I detailed at the beginning of this book, is designed primarily to permit nontechnical PC users to be able to perform the tasks they require, and the *Network & Internet* settings are no different. These easy to understand and use settings allow people to perform actions such as to connect to Wi-Fi networks and VPNs (Virtual Private Networks) (see Figure 9-11) and to set proxy settings for a network if required.

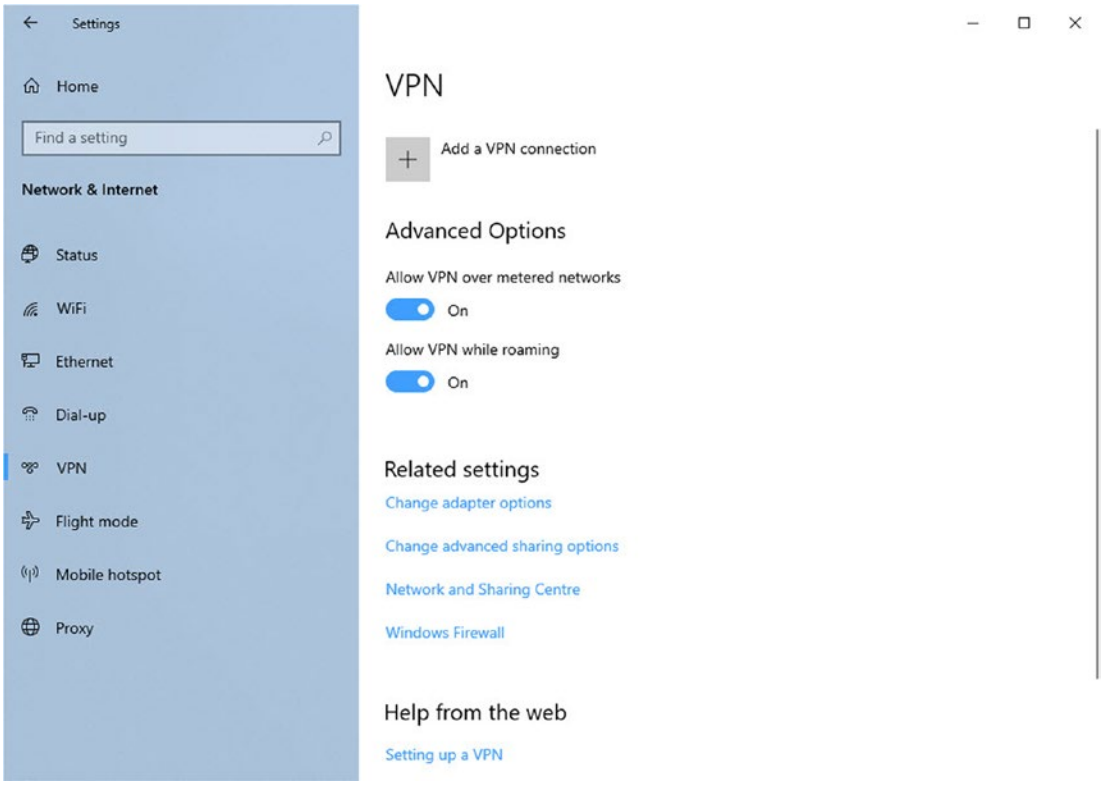


Figure 9-11. *The Settings panel is your main hub for creating network connections*

Where links appear below options in the Settings app, these will almost always open Control Panel applets, as detailed earlier in this chapter. Two notable exceptions however are the *Advanced options* and *Manage WiFi Settings* links in the Wi-Fi section (which will not appear if Wi-Fi is not available on your PC).

The first of these will allow you to set the currently connected Wi-Fi network as a metered connection. This can be useful if you have a limited data plan on a PC that does not support unlimited data usage. Setting a Wi-Fi connection as metered will restrict the data used by features as LiveTiles, but can also crucially affect Windows Update, and its ability to search for and download updates and patches to the PC.

The *Manage WiFi Settings* link is significantly more useful, however. It's common that settings for some Wi-Fi connections become corrupt, and suddenly the user is unable to connect to the network. The *Manage known networks* section of this panel allows you to force Windows 10 to forget its settings for any Wi-Fi network. This can be achieved by clicking the network, whereupon a Forget button will appear; see Figure 9-12.

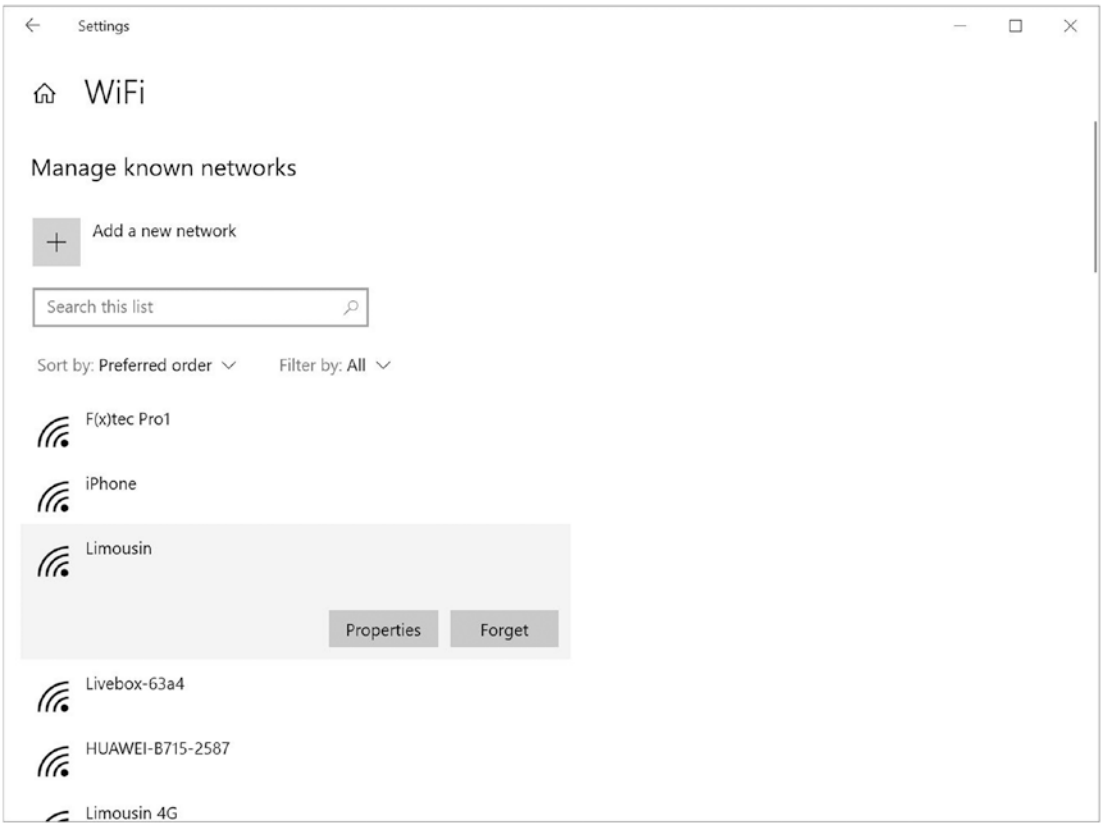


Figure 9-12. *You can force Windows 10 to forget individual Wi-Fi networks*

Tip You can disable Wi-Fi Sense using the Windows Registry by navigating to `HKLM\SOFTWARE\Microsoft\DataCollection\Default\WifiAutoConnectConfig` and creating a new DWORD called `AutoConnectEnabled` that has a value of `0` (`zero`).

While Wi-Fi connections can be managed within the Settings app, there's not much available for management of other network types. There's no management available for Ethernet connections at all, as they're just sort of on or unplugged. VPN settings just allow you to add or remove a connection and change the roaming settings for the connection, and the dial-up connections panel merely throws you into the classic Control Panel.

One exception is the proxy settings, which contain advanced controls should you need to use a proxy server on your PC (perhaps because you work in a security-conscious industry); see Figure 9-13. You can set up proxy servers automatically, through detection by Windows, or manually. Should there be a problem with a connection, it's worth having a look here to see if the proxy server settings have been disabled or have become corrupt.

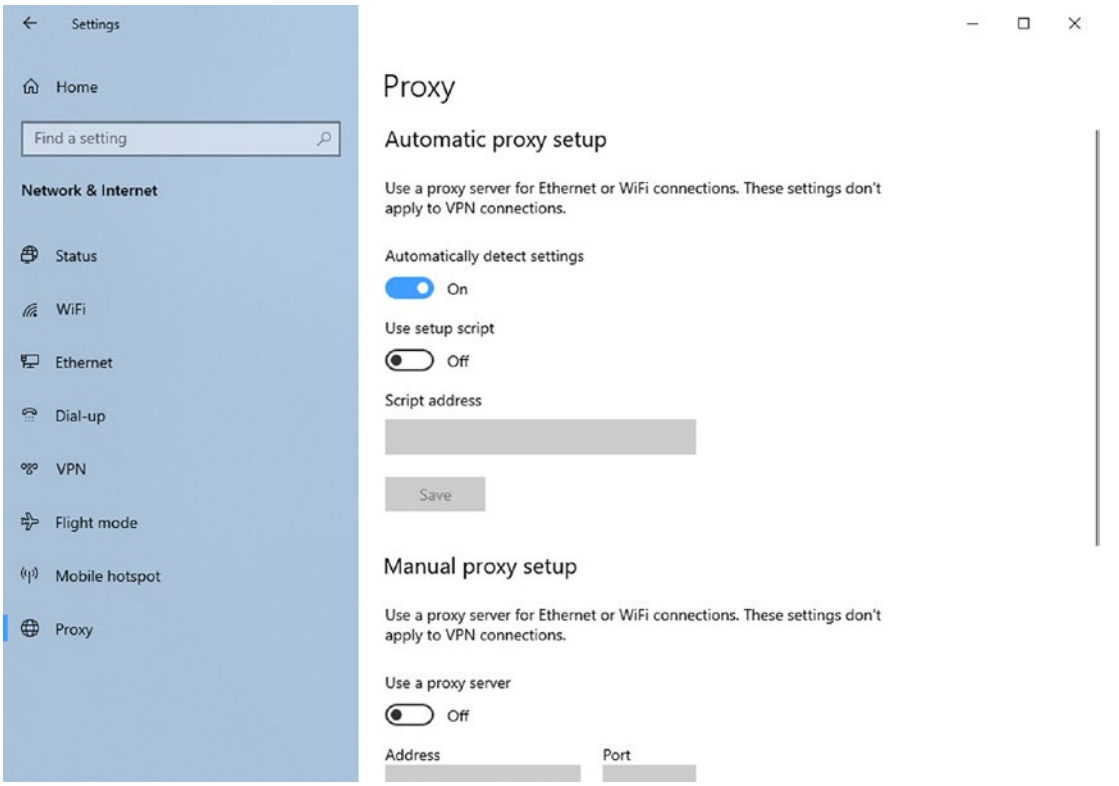


Figure 9-13. *You can configure all proxy server settings in the Settings app*

The main *Network & Internet* status screen in Settings however has had useful tools added to it since Windows 10 launched. This includes being able to see data usage for all your installed apps on the current network connection (both for Ethernet and Internet); see Figure 9-14. This can help diagnose apps that are hogging bandwidth.

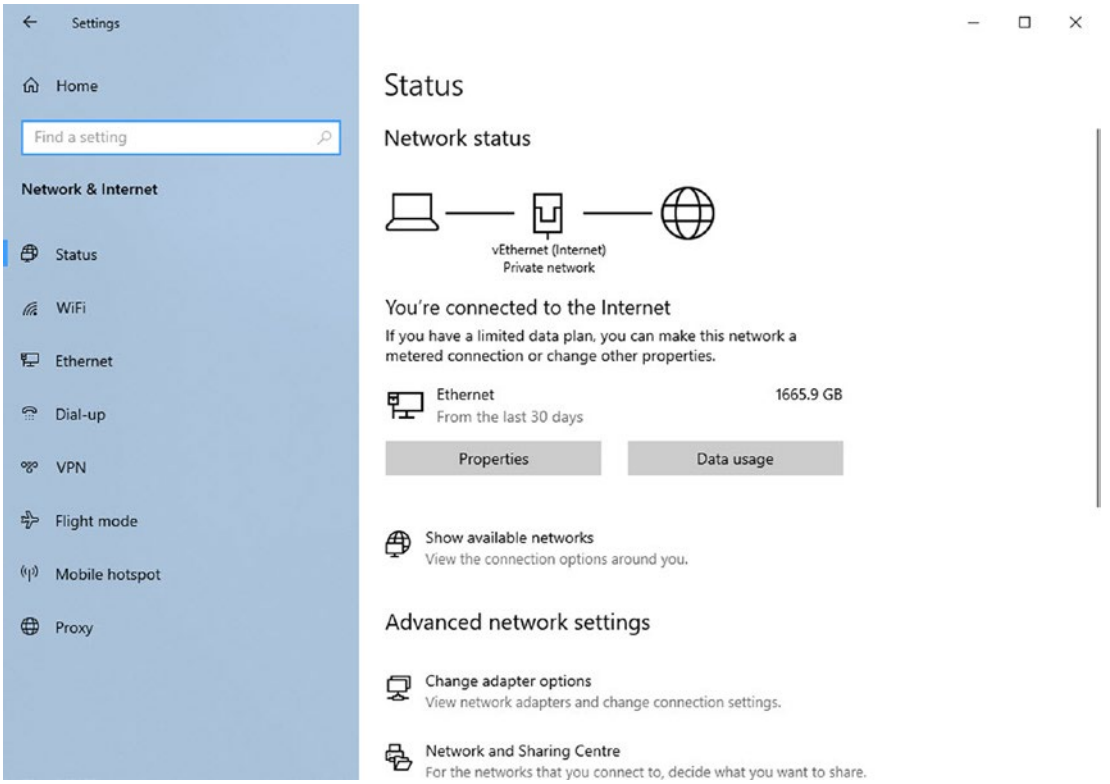


Figure 9-14. *Useful network tools have been added to Settings*

Network Reset

By far the most interesting and useful addition to Network Settings in Windows 10 since its launch is the *Network reset* feature. This is hidden away on a link at the bottom of the Status page, for some unfathomable reason, but can be incredibly useful when you encounter a problem; see Figure 9-15.

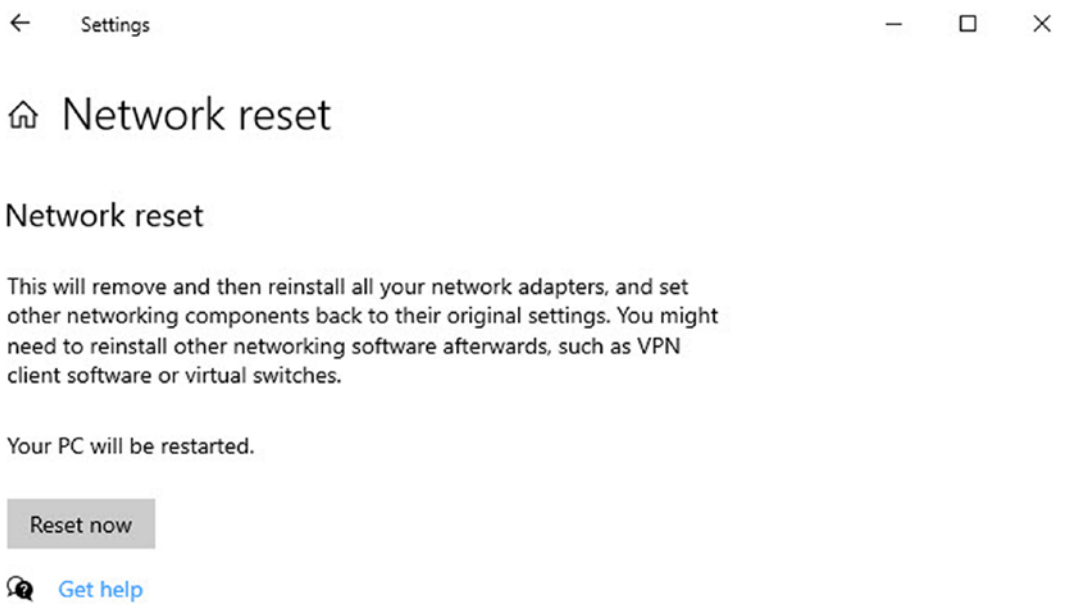


Figure 9-15. *The Network Reset feature is a wonderful yet very hidden tool*

As detailed when you click its link, Network reset does far more than reset network components to their default state as the Automated Troubleshooters do. Instead, it completely uninstalls and reinstalls your network drivers, very useful if you encounter a problem you can't resolve.

Setting Up and Managing Your Router

This may seem like an obvious thing to say to an IT pro, but it really is crucial to configure a router correctly and make sure that it has a secure access password. The number of times I have encountered routers, even in the business space, where the username and password are both set to "admin" is alarming.

Caution The default username and password for almost any router are available to find online, via a quick search for the manual, or the manufacturer's default settings. You should always change the username and password on all routers you own.

The first challenge, however, can be finding the IP address of your router, as different router manufacturers use different default IP addresses, and the router IP address range can be changed by an administrator after installation anyway. As an example, Linksys routers tend to use the default IP address 192.168.1.1. D-Link and Netgear routers however commonly use 192.168.0.1 (by far the most common address), and some Belkin routers use 192.168.2.1.

You can find the IP address of your router by opening *Command Prompt* from the Win+X administration menu and typing the command `ipconfig`; see Figure 9-16.

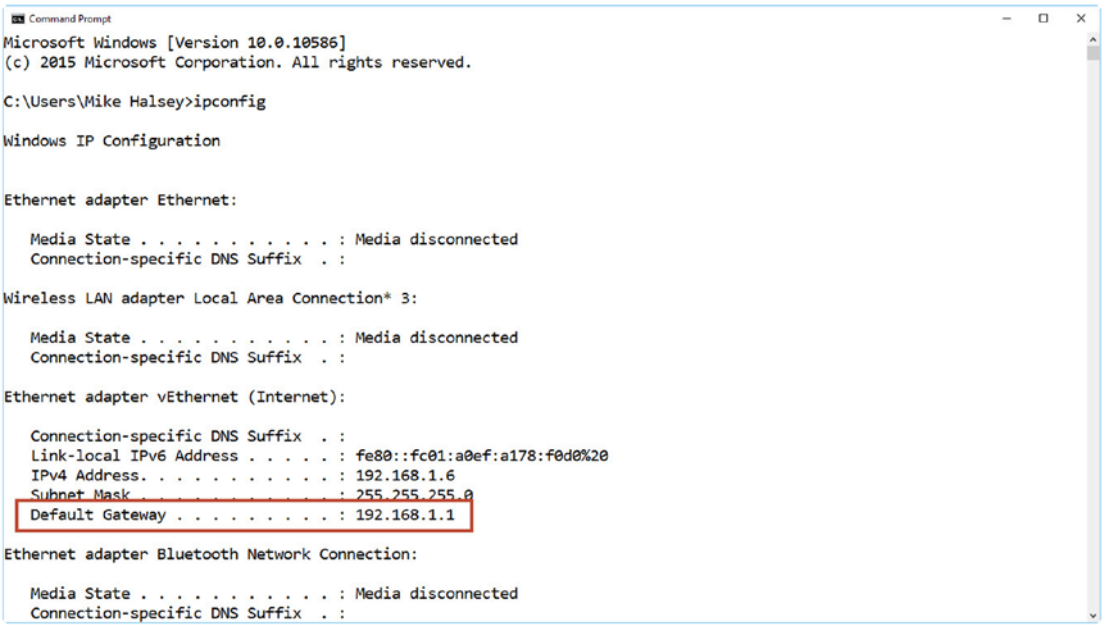


Figure 9-16. *You can find the IP address of your router from the IP Config command*

In the ipconfig results, look for the "Default Gateway" for your network connection. This is the router through which traffic is directed. This will be the address of your router on the network.

Note For most scenarios, looking for the Default Gateway in the `ipconfig` results will reveal the address of the router; however in some enterprise scenarios, it may instead reveal the address of a security, or web filtering appliance.

Of course, and you'll laugh that I've mentioned this as the second way to find the IP address of the router. You can always go and have a look at the label on the underside of the router, which will more than likely have its default IP address written on it.

When you are signed into the router, please, please, please make sure that the very first thing you do is change its access password to something secure. Once this is done, you will find that different manufacturers use different router interface software, and this can even vary across different routers in their own range. Figure 9-17 shows the router interface in this example of a Netgear router.

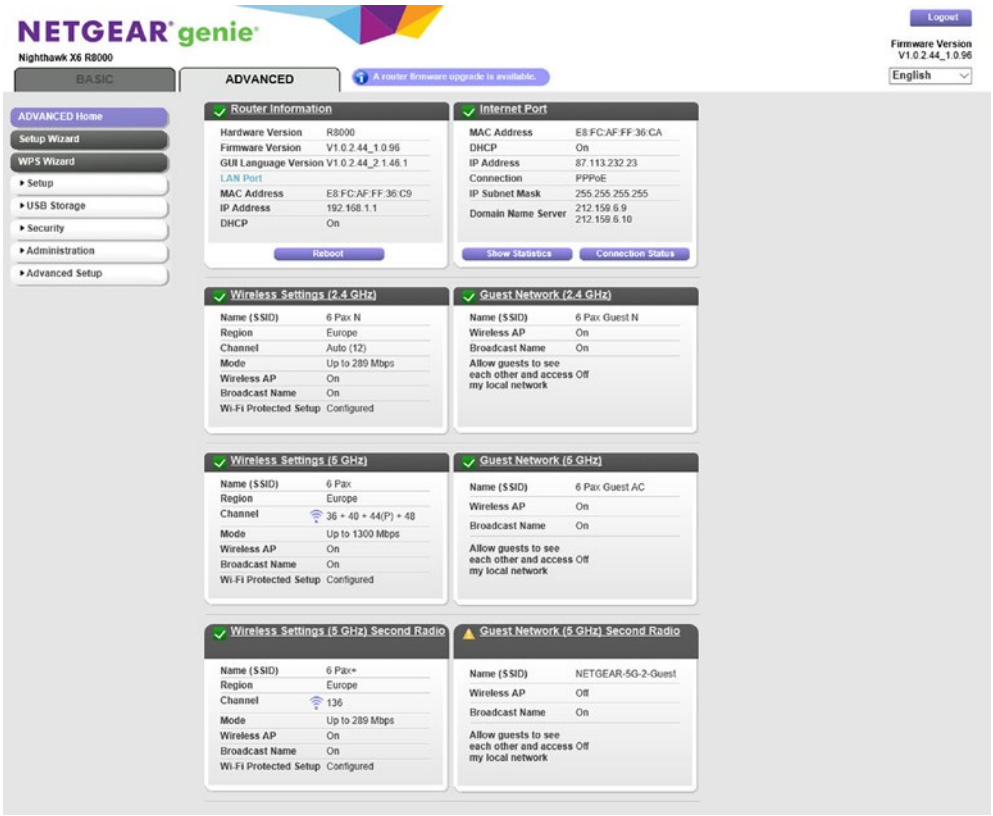


Figure 9-17. *Different manufacturers use different router interfaces, and even different interfaces across their products*

The more advanced the router, the more advanced the features it will provide. These can include web filtering, parental controls, and using USB-attached printers and storage with the router. Guest Wi-Fi networks can be extremely useful, especially if you share documents across your network from a USB drive or a network-attached storage (NAS) drive. A guest network can provide Internet access for visitors to your home or workplace, without them also having access to devices and storage on the network.

If the router you are using is a free model that was provided by your ISP, it's unlikely to support these advanced features. Routers that you purchase separately, however, do often support advanced functionality such as access control and website blocking and scheduling; see Figure 9-18.

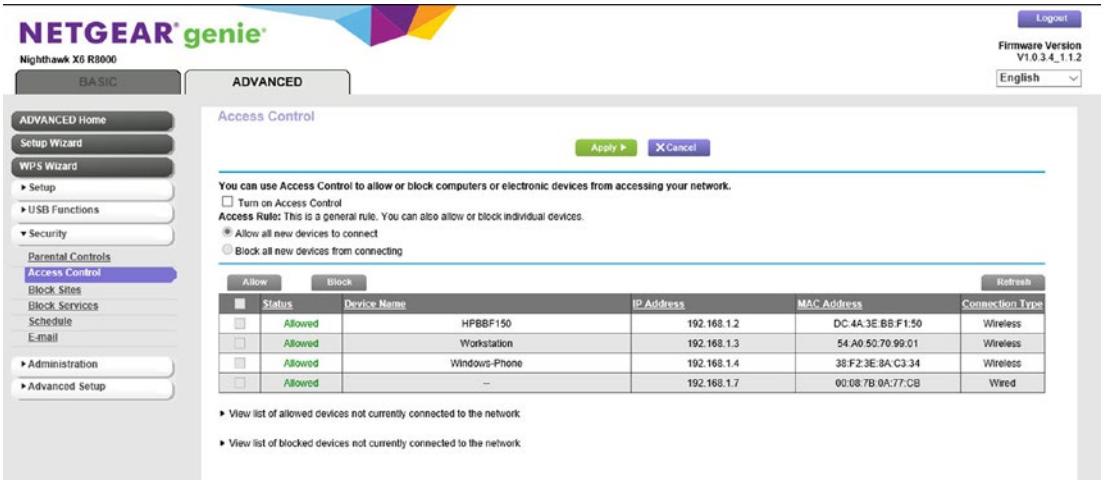


Figure 9-18. *Many routers offer advanced security and other controls*

Troubleshooting Wi-Fi Connection Problems

In Chapter 14, I'll show you how to diagnose and repair complex network problems, but one of the most frustrating can be a poor Wi-Fi signal. This can be caused by a multitude of different things, and can even be affected by where you live in the world.

By this I mean that in some parts of the world, most notably Europe and the Middle East, buildings are not only commonly constructed from much thicker stone and brick than in places such as the United States and Canada, but sometimes these buildings are hundreds, maybe even a great many hundreds, of years old. My own home and office, for example, is a 350-year-old French cottage, where some of the walls are a full 18-inch (46cm) thick.

Wi-Fi signals really don't like strong brick and stone construction, and so if you're (as an example) traveling from the United States to Italy on business and then find that you're getting an awful Wi-Fi signal, it could be the building you're sitting in that's causing it.

Good placement of your Internet router is crucial therefore to maintain a good all-around Wi-Fi signal. Where this isn't possible, access point or Wi-Fi mesh hardware can be installed to boost the Wi-Fi signal into parts of a building where it's weak. Additionally, if you have an old Internet router collecting dust, you may be able to reconfigure it as a wireless access point. The settings for this, if your router supports it, will be found in its advanced settings; see Figure 9-19.

Figure 9-19. *Older routers can often be reconfigured as an access point*

Other factors can affect Wi-Fi signals, however. These include radio and other signals broadcast from devices such as older televisions and even microwave ovens, so keeping these devices away from the PCs in your home of office can assist with maintaining a good Wi-Fi connection.

Lastly, you can also get interference on Ethernet network cabling used for PCs and other systems such as Voice-Over-IP (VoIP) telephony systems. Common network (and other types of) cable are built using a method known as UTP, which stands for unshielded twisted pair. UTP cables are susceptible to interference caused by radio and other signals. Shielded cabling is available, though slightly more expensive, and you might want to consider purchasing shielded cabling when installing network systems in your home or workplace.

Recovering Lost and Forgotten Wi-Fi Passwords

An issue that can trouble people a lot is people forgetting Wi-Fi passwords. There are two simple ways to recover a Wi-Fi password, depending on whether the user is currently connected to that network or not. If they *are* currently connected and just want the password to, for example, pass it on to another colleague, open the *Network and Sharing Centre*, click on, or right-click depending if you are on the main screen or the adapter settings screen, the current Wi-Fi connection.

Select *Properties* from the context menu that appears, and in the pop-out dialog that appears, click the *Wireless Properties* button. Another dialog will appear in which you click the *Security* tab at the top and then you have a *Show characters* check box that will reveal the *Network security key*; see Figure 9-20.

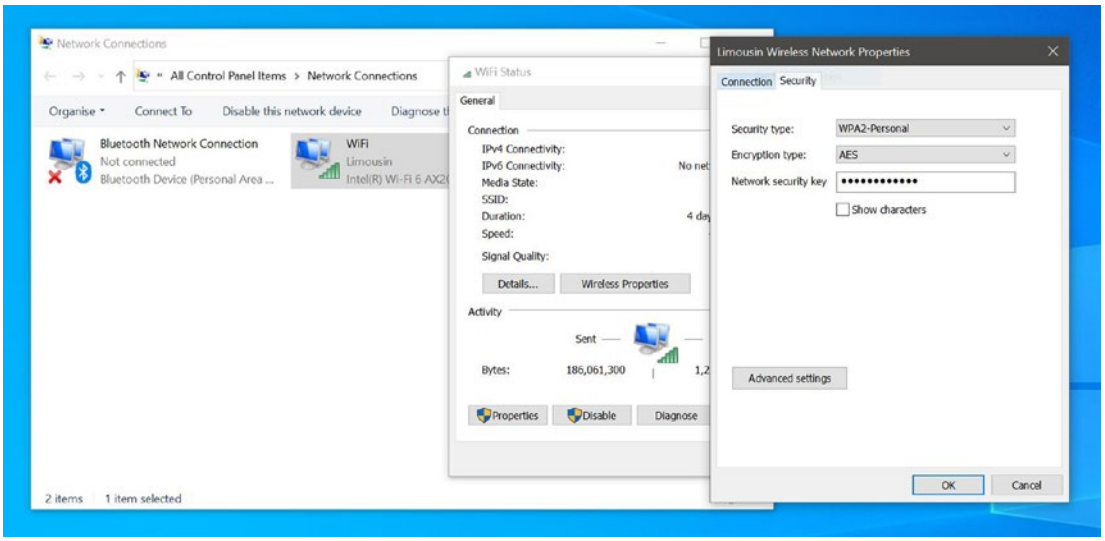


Figure 9-20. *You can recover a Wi-Fi password from the Network and Sharing Center*

If the user is not currently connected to the wireless network, then you will need Administrator access. From the Start Menu, search for **netsh** and run it as an Administrator (this is required). A Command window will appear in which you type the following commands:

wlan show profile – lists all of the stored Wi-Fi networks on the PC.

wlan show profile "Wi-Fi Profile Name" key=clear – which will display detailed information about the Wi-Fi network, including the security key, which will appear in plain text in the *Key content* field; see Figure 9-21.

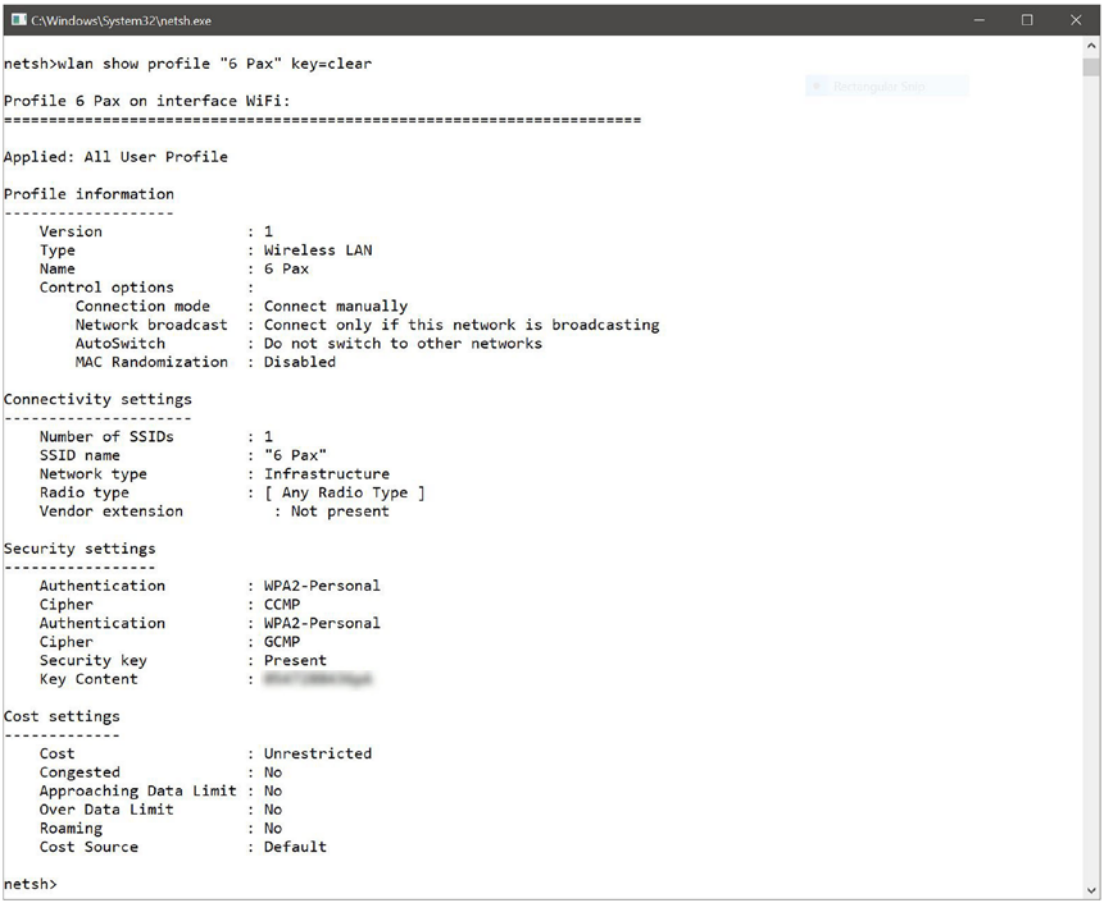


Figure 9-21. *You can recover any stored Wi-Fi password on a PC*

Summary

Despite all the network diagnosis and troubleshooting methods covered in this chapter, we've really only scratched the surface of the subject. As we progress to more advanced subjects in this book, we'll cover these things in much more detail in Chapter 14.

In the next chapter, however, we'll deal with the other essential component for Internet access, the web browser. Both the Edge browser and Internet Explorer have advanced configuration and troubleshooting options and features available, but neither can be uninstalled and reinstalled from the OS, so I'll show you how to troubleshoot them.

CHAPTER 10

Troubleshoot and Manage Internet Explorer and Edge

If the most important aspect of using our PCs is getting network and Internet access, the second most important is the web browser, of which Windows 10 has; well, we'll say they have one and a bit because while many people are finding new love with Microsoft's Edge Browser, Internet Explorer's relationship with the world is perhaps best described as "it's complicated."

The fact is that Internet Explorer 11 is *finally* coming/came to the end of its life on June 15, 2022 [Delete as applicable], but with an announced end of life date for Windows 10 announced for 2025, and with huge corporations still reliant on IE11 for maintaining compatibility with older ActiveX controls and intranets, this pundit would not expect to see it disappear from the OS, even if/when (it's turning into one of those chapters [Ed]) the operating system goes into a period of extended support as Windows 7 did.

So we're left with a complicated will they/won't they situation where Internet Explorer just keeps hanging on. For the purposes of this book then, and given there's a fair and reasonable chance that some of you still use IE11 in your organizations, I'm going to assume that IE11 will never disappear from Windows 10.

Managing IE11

So let's begin with IE, as the type of person most likely to be reading this will be using Windows 10 in a business or enterprise environment. Unlike previous versions of Windows, where as the years progressed so did the version number for the available copy of IE, the version that ships with Windows 10, IE11, will be the very last version of

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_10

the browser. There will be no updates in the future except for security patches. It's also extremely unlikely (I'd say it's never going to happen) that newly ratified and released Internet browsing standards will be included in IE. IE in Windows 10 is merely there to maintain compatibility with *older* sites for which the compatibility tools in Edge don't work.

Disabling IE

Edge is a very different beast from IE by virtue of being a Windows Store app. This means that, as with all other Store apps, it runs in its own protected bubble of memory, and its core files are hidden away with such tight security that even an Administrator can't access them. As a result, Edge is (as I write this) the most secure web browser available for any OS. As other browsers are recompiled as Store apps, they too will be able to take advantage of this advanced security, but it certainly makes Edge pretty much unhackable.

If security is important to you or your business, you might want to minimize the risk of attack for your systems. You can do this by disabling any part of the OS that's potentially vulnerable. This includes IE, which, as a desktop Win32 app, has its core files visible and vulnerable to anybody with administrative rights.

You can disable IE11 from the *Apps and Features* panel, most easily accessible from the Win+X administration menu. In this panel is an *Optional features* link that, when clicked, will display a list of all the Windows 10 features that can be disabled, or that haven't yet been enabled; see Figure 10-1.

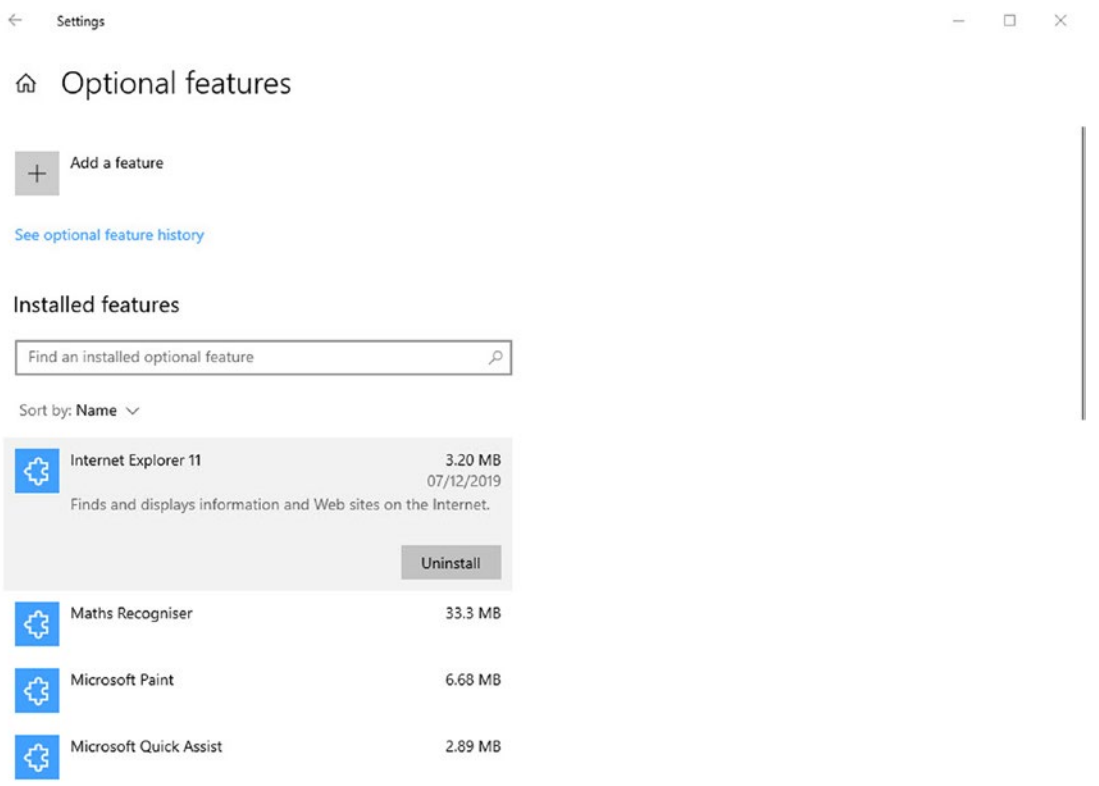


Figure 10-1. *You can remove IE11 in the Settings panel*

Additionally you can click *Programs & Features* in the Control Panel and then click the *Turn Windows features on or off* link on the left of the window to display a list of removal features including IE11; see Figure 10-2.

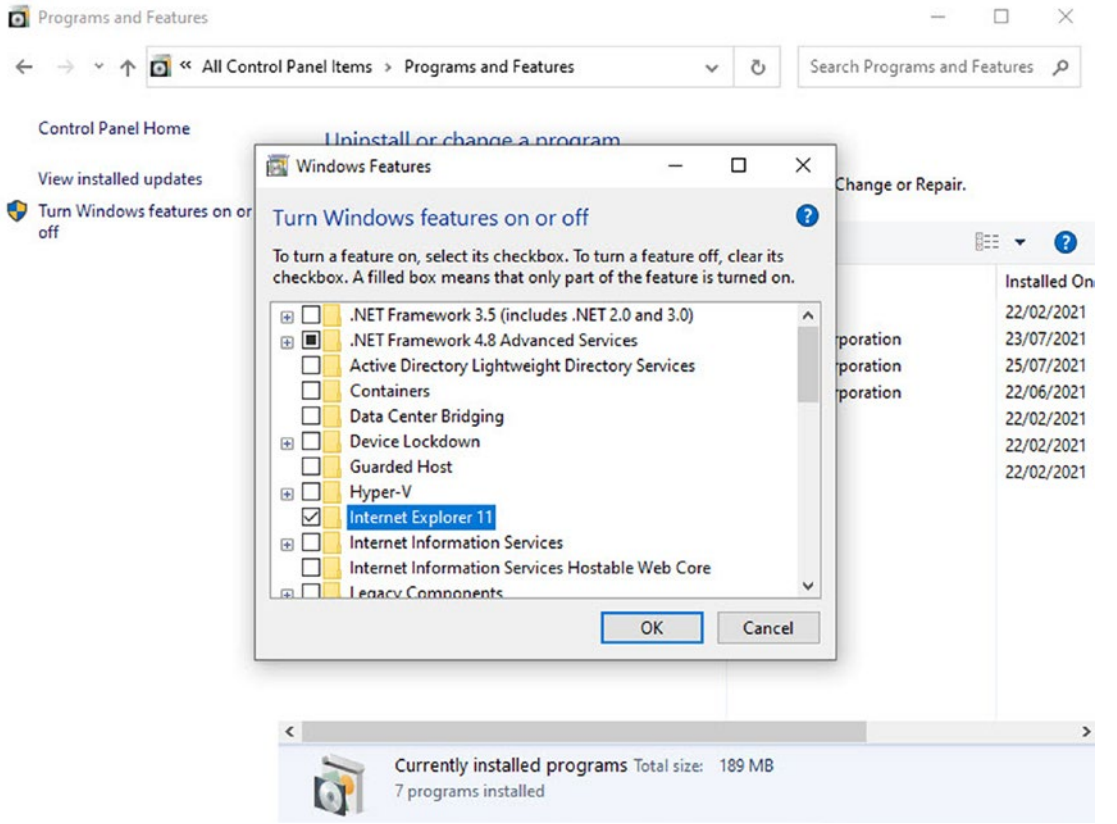


Figure 10-2. *You can disable IE from the Programs and Features panel*

It's worth bearing in mind that much of the underpinnings of IE also forms the basis of some other Windows utilities, many of which you can't disable or be without, such as File Explorer. Should a hacking or virus attack modify or delete some core files for IE, it's possible that other UI elements could also be affected. However, disabling IE prevents any users on the PC from being able to access it, and if users can't access it on the PC, it makes it significantly harder for malware to attack it as well.

Managing Temporary Files in IE

The primary way for malware to attack your PC through a web browser is to get you or the browser to download files containing malicious code. These can sit in the temporary files store for your web browser, waiting to be run again, as the temporary files store helps make sure the web pages you visit often load quickly.

The security-conscious among you can manage these temporary files in IE11 through the Internet Options panel. This is available either in the Control Panel or through the Settings icon in the top right corner of the browser.

I'll show you through all the options available in Internet Options in Chapter 17, but under the General tab, you will see a *Browsing history* section. Here there is a quick check box option to always *Delete [the] browsing history on exit*, which will delete most temporary files from the PC. Click the Settings button, however, and more options will become available; see Figure 10-3.

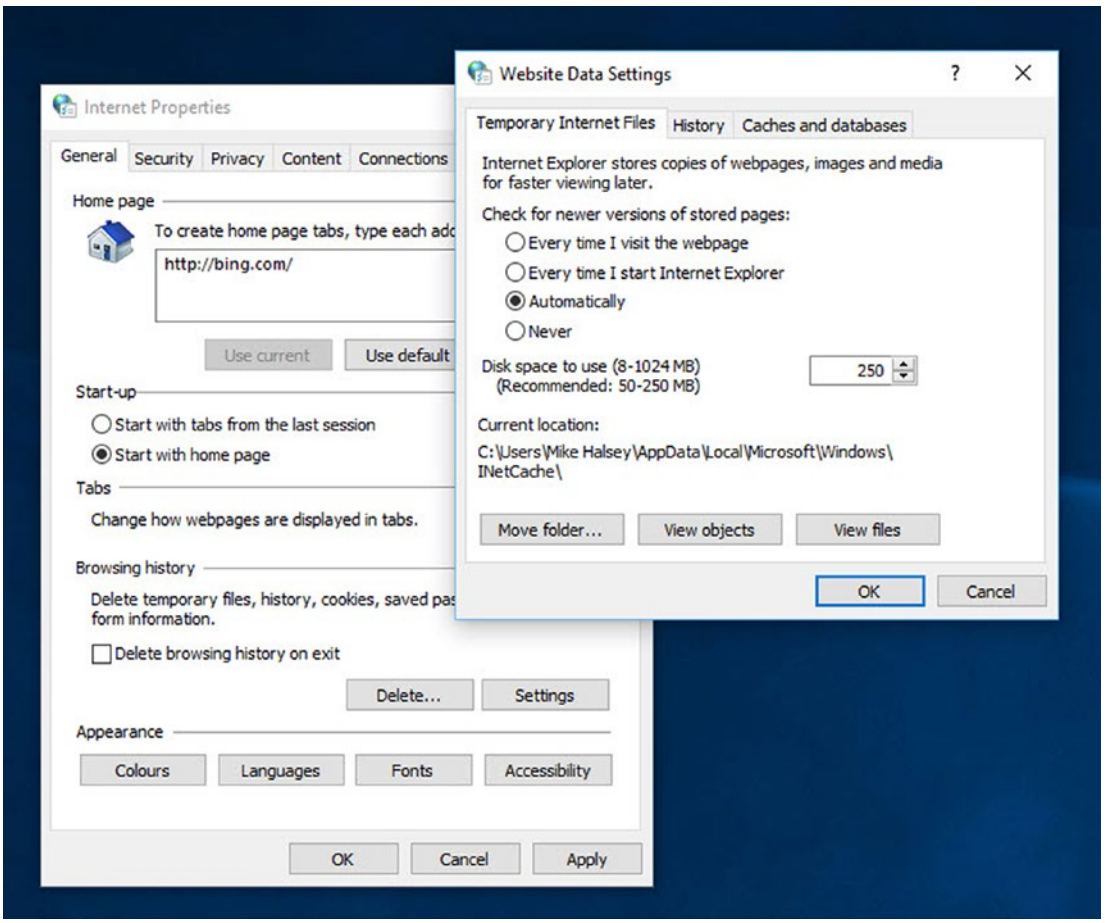


Figure 10-3. *You can manage the default options for managing temporary files in IE11*

Under the *Temporary Internet Files* tab, you can control how often the temporary files are refreshed. The default setting is for IE to manage the setting automatically and refresh the temporary files only if it detects that a web or intranet page has changed. You can, however, force IE to check every time the browser is started, every time a page is visited, or never.

You can also control the amount of space allocated on the PC for temporary files. Unfortunately, this doesn't allow you to eliminate the files altogether, with a minimum required disk space of 8MB, but it can help minimize the space in which malware can reside.

At the bottom of the panel are buttons to move the temporary files store, perhaps to a protected area on the PC, such as a different partition; to *View objects* in the store (these are downloaded programs); and to *View [all the] files* in the temporary files store. Opening this will help you manually delete the files should you wish.

The *Caches and databases* tab will also allow you to determine what if any websites and intranet sites can store database caches on your PC. You can disable these completely; however, you might find that your intranet requires this feature to be active.

Back in the main Internet Options panel, clicking the *Delete* button will allow you to delete temporary and other files from IE manually. These include form data from websites and intranets, your downloaded files history, and stored passwords; see Figure 10-4.

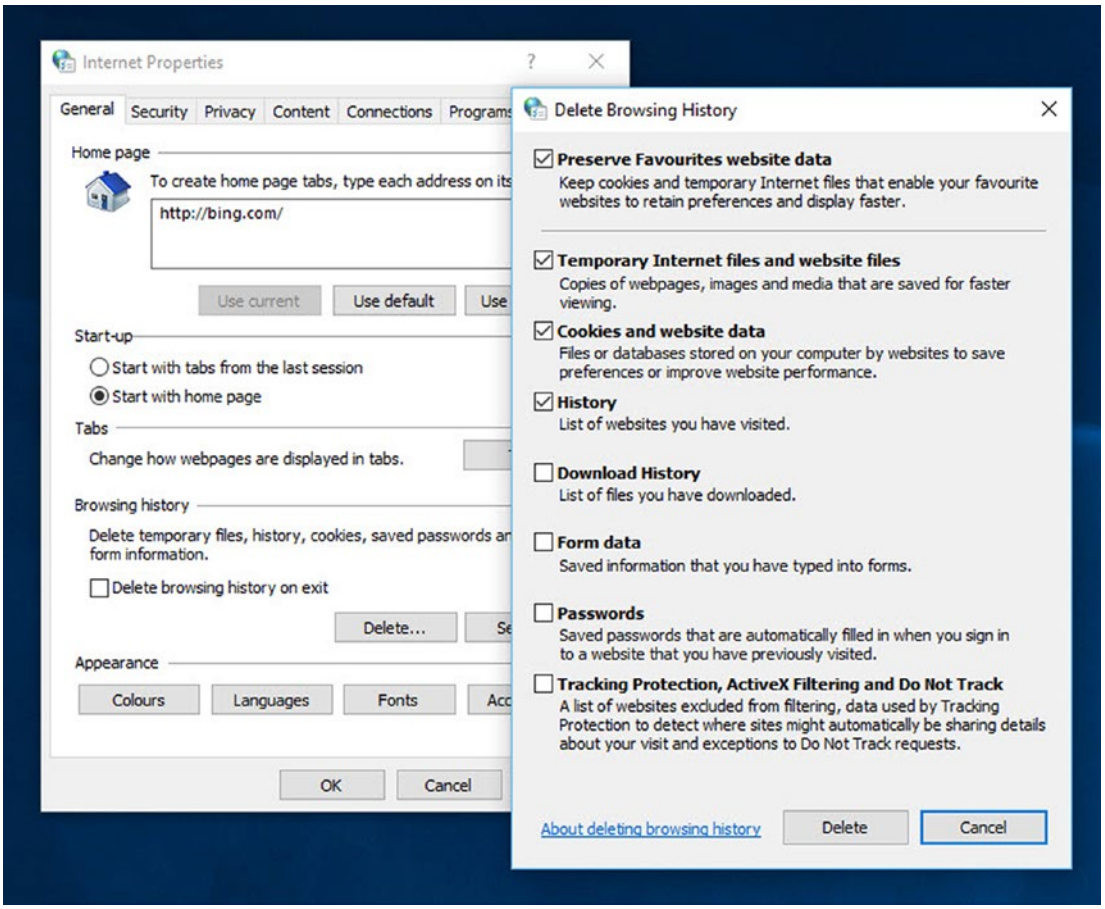


Figure 10-4. *You can delete temporary and other files from IE11 manually*

Resetting IE11

Something both IE and Edge have in common is that, because they're integral parts of the Windows OS, neither can be uninstalled nor reinstalled. This can present a problem should their core files become corrupt. While corruption is far less likely with Edge because of the protected way its core files are stored, with IE, this can be a pain.

With previous versions of Windows, you could install a newer version of the browser to fix the problem, or you could manually download the installer for the browser if it was an update of the version that originally shipped with Windows and perform a reinstall.

There is no stand-alone installer, however, that's compatible with Windows 10. Even extracting the installer's core files using software such as WinRar won't help you (this is a great trick for installing software and drivers that I'll detail in full in Chapter 15).

However, all is not lost! IE can be completely reset, effectively reinstalling it and at least setting it back to the point it was at when Windows 10 was first installed on the PC. This doesn't affect any patches and updates that have been installed afterward from Windows Update, but it's a good way to get the browser working again.

You can reset IE11 from the Internet Options panel, which if IE11 isn't working is best accessed from the Control Panel. On the *Advanced* tab, you will see a *Reset* button. Clicking this will inform you what the reset process will do, and give you the added option of completely clearing out the browser at the same time, just in case it's personal or temporary files that are causing or contributing to the problem; see Figure 10-5.

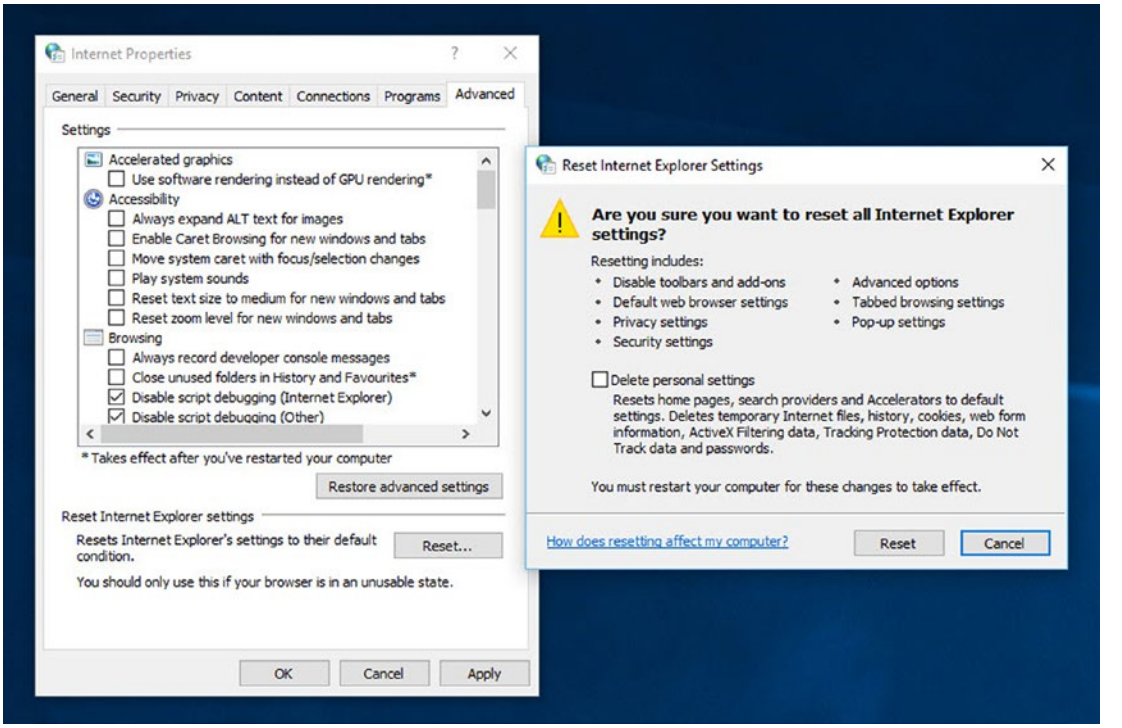


Figure 10-5. *You can reset IE11*

Resetting IE11, and even *Deleting [the] personal settings,* doesn't delete your Internet Favorites, which are stored elsewhere in your Users folder, but it can be a great way of getting a faulty or malfunctioning installation of IE11 working again.

Managing Edge

Microsoft's Edge browser has gone through several different versions, starting with a Microsoft Store (Universal Windows Platform) UWP App version that shipped with Windows 8 to a more modern and compatible browser based on Google's Chromium browser code base. This makes it completely compatible with Google Chrome right? Well you might think so and in practice this would be true. It would definitely be more compatible than IE ever was and more compatible than the first versions of Edge that shipped a few years ago.

Note Microsoft Edge is a fairly new product as I write this, and is being expanded on and improved all the time. While this means it is unlikely that features will be removed, they may be shuffled around and the settings interface tweaked from time to time. There is a search box in Edge's Settings you can use to find things if they move however.

However, this is all dependent on support from the companies behind the websites that you visit. While most will be perfect and you'd never notice the difference between Edge and Chrome, some haven't (yet) been updated to accommodate the new browser, and these will either stick you in an IE mode or render the page as though you were still using the UWP version. This will change over time, but bear in mind that some websites still need some attention.

Using Internet Explorer Compatibility Mode

I think it can be safely said that the Internet Explorer compatibility mode in the UWP version of Edge was pretty awful. Fortunately the new Chromium Edge (nicknamed Chredge by renowned Microsoft journalist Mary Jo Foley) has had a far better IE compatibility mode included over time. You can access this in the browser settings (the three-dot icon in the top right of the browser window) in the *Default browser* panel. You can choose between different options including using IE mode only when the browser detects an incompatible site, always or never; see Figure 10-6.

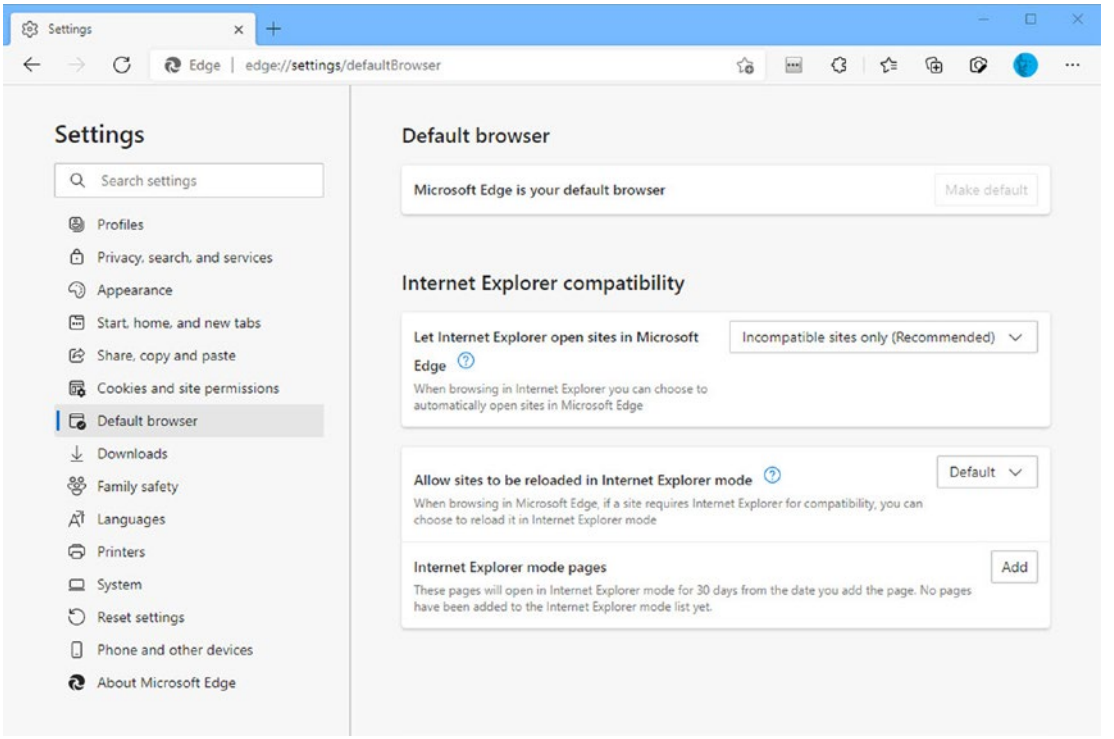


Figure 10-6. *IE mode in Edge is much better than it used to be*

There is also an *Add* button in the *Internet Explorer mode pages* section that allows you to force web pages to open in IE mode. At the moment however this seems limited to just 30 days, presumably because Microsoft do not want business and organizations to use it as an excuse to not update code that is potentially very vulnerable to malware and attack.

Edge System Settings

There are a great many settings in Edge that I suggest you have a look at, including the very strict privacy controls that, to be frank, you'll never get from Google, and the *Privacy, search and services* settings where you find options for clearing temporary and other files from the browser, which could include malware download manifests if you are infected. Of the settings you might need most in your organization however are the *System* options. Here you will find settings for using hardware acceleration, which could cause problems especially with some older PCs; see Figure 10-7.

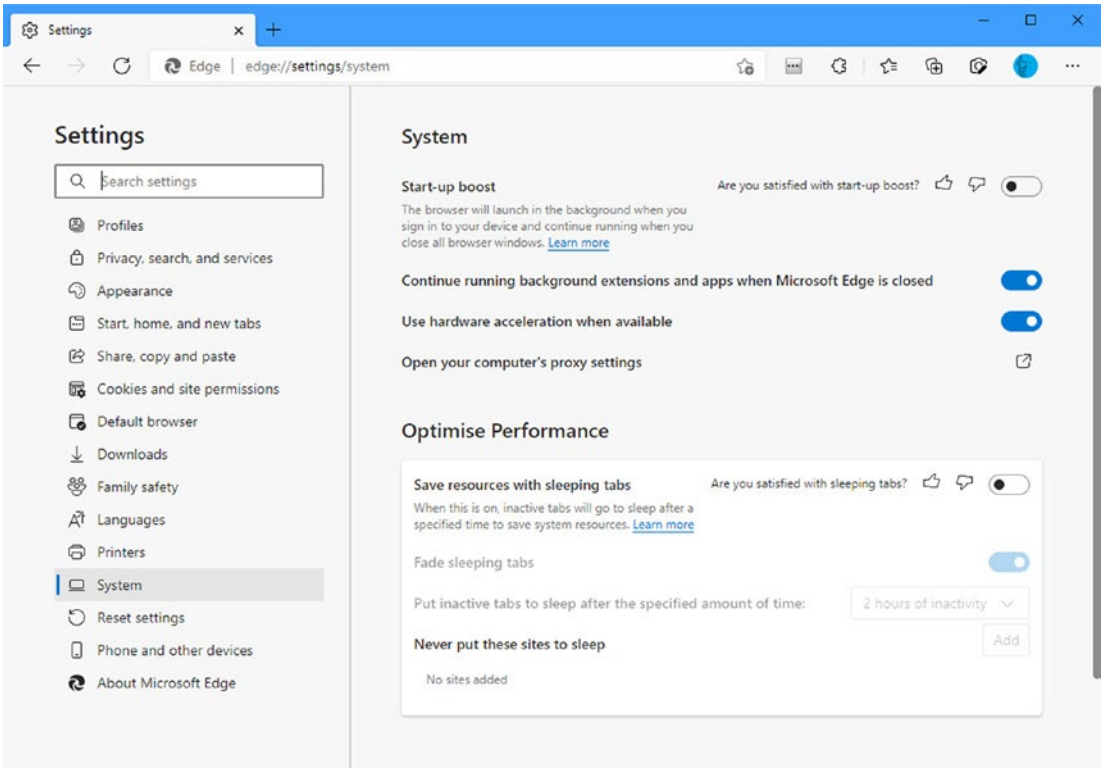


Figure 10-7. *You can enable and disable hardware acceleration in Edge*

One other feature that could be very useful on some older PCs is *Sleeping tabs*. This suspends open tabs in the background. While this feature is very unlikely to ever cause a problem, it could be a useful way to fix problems on older hardware, especially where the user keeps a lot of browser tabs open at once.

Resetting and Updating Edge

You might think that if you have a problem with Edge, it being a store app, you can use the *wsreset* feature in the Start Menu to reset it. That was the old edge however. Chromium Edge however is a full win32 program. You might be able to find it and download it from the Microsoft Store, but that's only because Microsoft have slowly been expanding the store to include additional program types, including Universal Web Apps (UWP) that are effectively a web page in a downloadable container.

There are two different ways to reset Edge. The first will just reset the browser's internal settings and is usually the first thing to try if you experience a problem. In the browser open its *Settings*, and in the *Reset settings* panel, click the *Restore settings to their default values* link; see Figure 10-8.

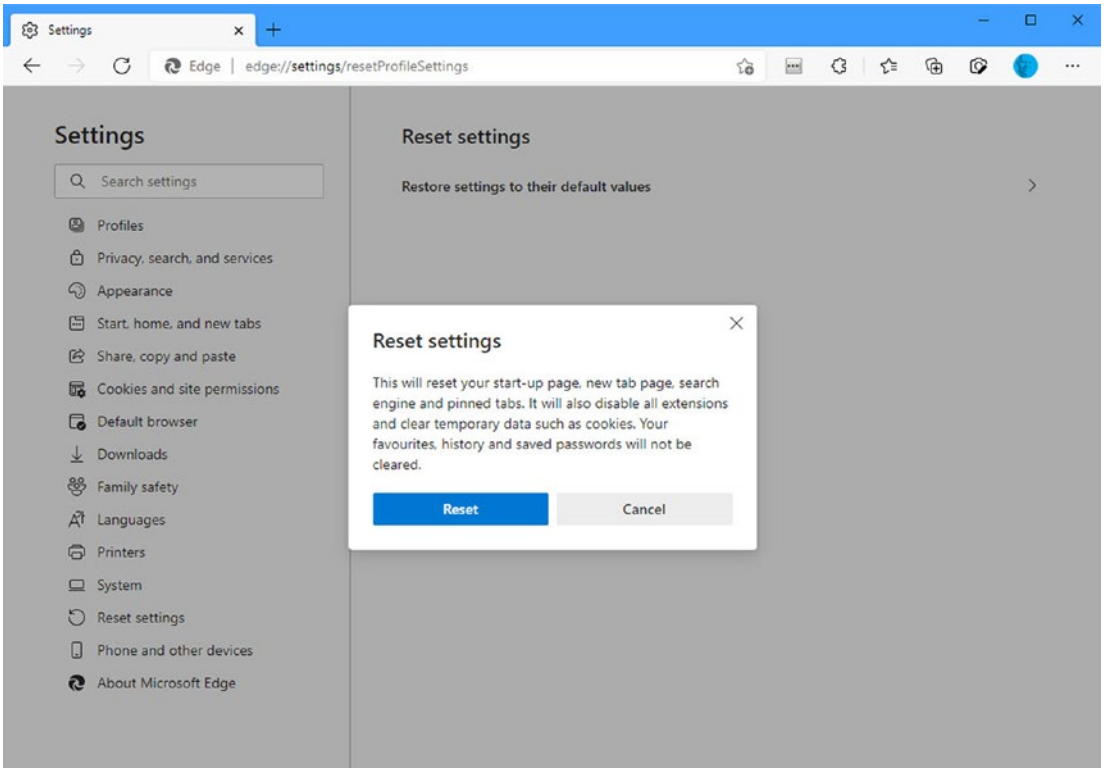


Figure 10-8. *You can reset Edge's settings to their default state*

If you need to fully reset the app however, you can do this from the main Windows 10 *Settings* panel, accessed from the Start Menu (I know, it's unhelpful when multiple things have the same name but are completely different [Outlook in Microsoft 365, Outlook on the Web, Outlook Android and iOS apps, and Outlook for Mac as an example, all of which are completely different and have different functionality from one another]).

When you're in *Settings*, click *Apps* and then *Apps & Features* (this is also available directly from the Win-X menu), then find *Microsoft Edge* in the list of installed apps, click it once to reveal the *Modify* button, and click through the UAC (User Account Control) security prompt to reveal a new pop-up with a *Repair* button as seen in Figure 10-9… got all that?

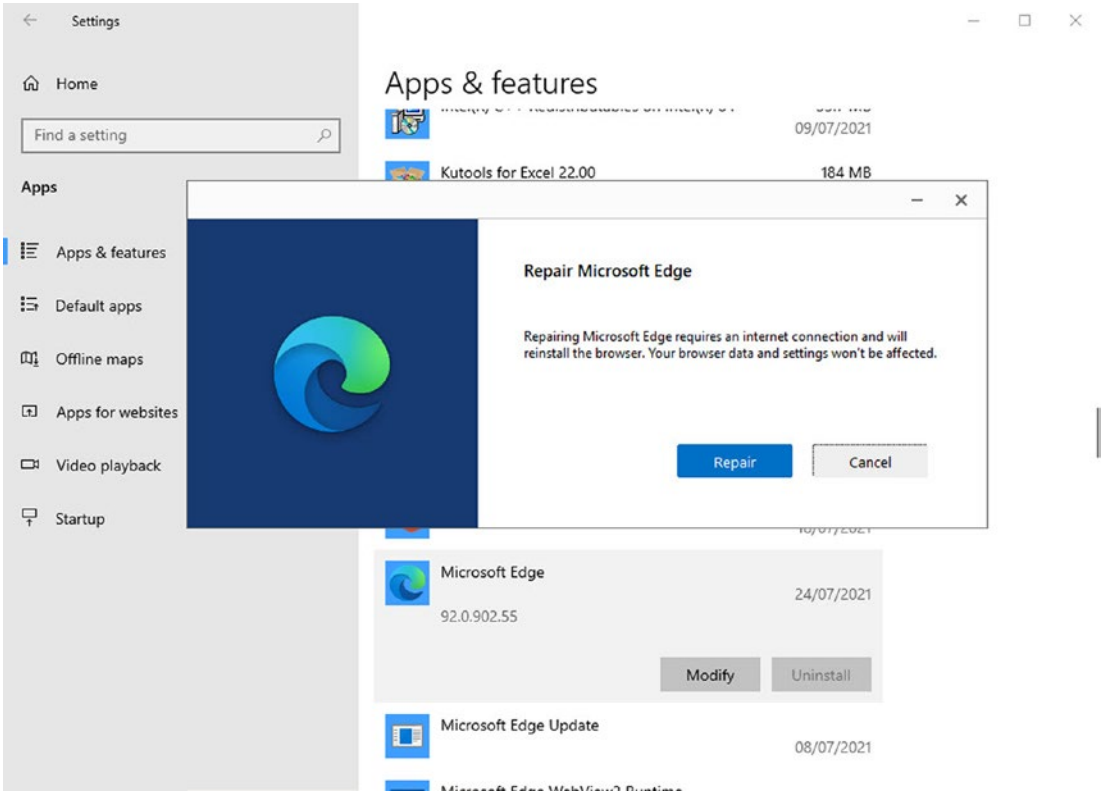


Figure 10-9. *You can repair a broken Edge installation*

Sometimes however, the browser can be fixed by just applying an incoming update. You can check if a new update is available by going into the browser *Settings* and clicking the *About Microsoft Edge* option; see Figure 10-10. If an update is available, you will be notified here to restart the browser, and the update will be installed in just a couple of seconds.

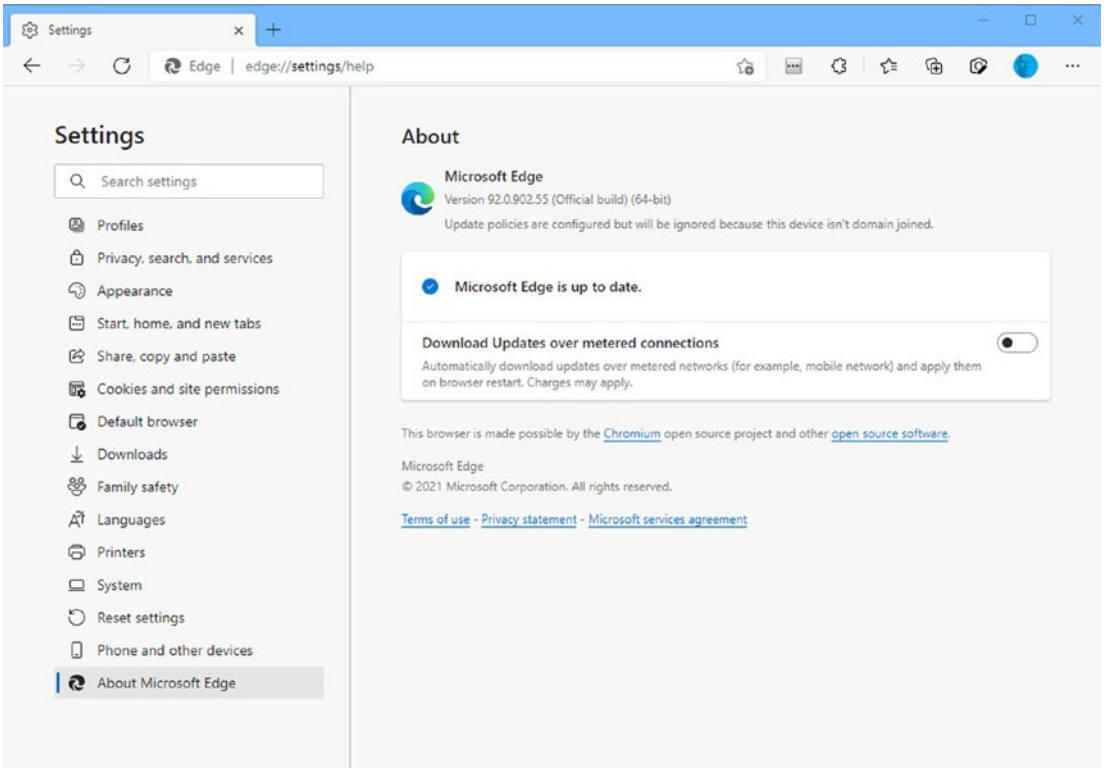


Figure 10-10. *You can update Edge from directly within the browser*

Should you need to completely uninstall and reinstall the Edge browser on a PC, you can always download the latest build from `www.microsoft.com/edge`, but do bear in mind that the newer installations of Windows will prevent you from uninstalling it completely. You can still reinstall though by downloading a new versions from the Web.

Summary

Edge and IE really highlight the differences between modern and older win32 apps. With IE11 you can pretty much manage the browser and its core files in a variety of ways, but this also means that malware can get access to the core files too. With Edge, the system is far more robust, with modern underpinnings and strong security baked-in.

This isn't to say that damage can't be done, and instructions I found commonly floating around the Internet can render the Edge browser completely unusable and unable to start. The lesson here is to follow any instructions with care, and to make sure you have an image backup of your Windows 10 installation you can fall back on if need be.

I'll show you how to manage compatibility with websites and intranet sites, and how to manage privacy and security in IE11, in Chapter 17, but we're going to throw ourselves directly into troubleshooting in the next chapter by looking at how we fix the most common Windows 10 annoyances.

PART II

Becoming a Proficient Troubleshooter

CHAPTER 11

Dealing with Common Windows Annoyances

PCs can be annoying, frustrating, irritating things to use when something isn't working as it should, from files that won't open to storage you can't access, sound that won't play, irritating activation messages 2 years after you'd activated Windows, Windows Updates that won't install, slow and hanging startup and shutdown, encryption lockouts, faulty touch screens, nonfunctioning USB devices, not having a picture on your monitor, and Blue Screens of Death (BSOD) with perpetual restarts. Things that might in essence be "straightforward" problems can cause enormous headaches and loss of productivity.

In this chapter, I'll deal with all of these issues and more, and show you how to quickly repair every single one of them. When you fix a PC that has a problem like these, people will look at you wondering how the hell you did it, and how you did it so quickly. In the words of Scotty from Star Trek, "How else can I keep my reputation as a miracle-worker."

User Folders in Incorrect Locations

Let's begin with one of the most irritating things a PC can do, fail to show you any of your files and folders. Windows 10 makes it extremely easy to move the Shell User Folders (Documents, Pictures, Music, etc.) as you can either open the folder's *Properties* and change the *Location* information or simply cut and paste the folder from one place to another.

What is less helpful though is when a corruption occurs that changes the locations of these folders for you, and then refuses to allow you to change them back again. Here is where some Registry editing is required. The advantage of making such changes in the Windows Registry is that you can make whatever changes you require, but they're

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_11

not implemented until the next reboot at which, we hope, startup is clean and there's nothing to prevent the change(s) being implemented.

You can open the Registry Editor by searching in the Start Menu for **regedit** and clicking through the UAC (User Account Control) prompt. I'll detail the Registry Editor in full in Chapter 26, and there's some fantastic stuff you can do with it, but for the purpose of expediency here, navigate to `HKEY_CURRENT_USER` ➤ `SOFTWARE` ➤ `Microsoft` ➤ `Windows` ➤ `CurrentVersion` ➤ `Explorer` ➤ `Shell Folders`; see Figure 11-1.

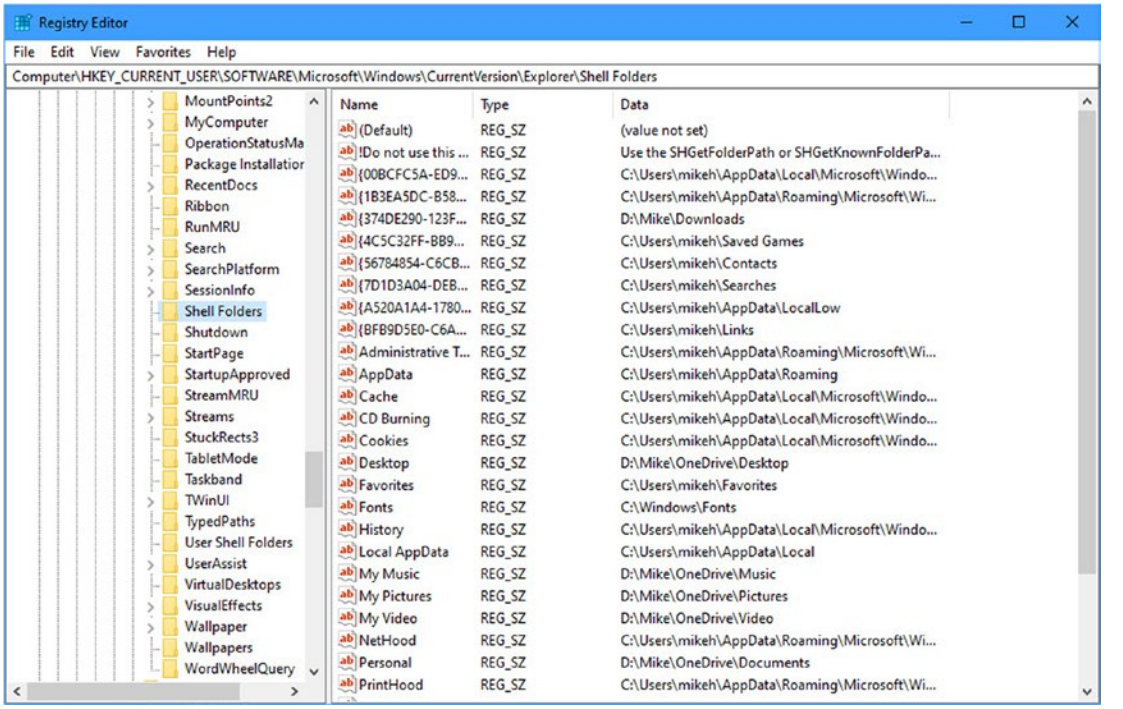


Figure 11-1. *You can change the Shell User Folder locations in the Registry*

In addition to the main folders, editing the user folders in the Registry also gives you access to the default folder locations for things such as Fonts, Roaming Profiles, Local Application Data, and more, in case a corruption has occurred for one of those locations (though this is very rare).

Right-click the Registry entry you need to change, and select *Modify* from the context menu. When you are done making your changes, you can close the Registry Editor and restart your PC for the changes to come into effect.

Incorrect File Associations

Few things are more annoying than files that won't open. Whether you're at work, at home, or studying, you want the files you have to always open correctly and in the right app. Windows 10 to its credit is fairly good with its notifications; if it doesn't recognize a file type, it will display a helpful dialog with a list of installed apps on your PC from which you can choose.

Where it all falls down, of course, is that because the OS can't recognize the file type, it has absolutely no idea what types of app it should display, and as it can only display a few apps in the dialog, it will commonly get things wrong.

It's a straightforward process to repair file associations, however, and there are two ways to manage it, the first of which is very straightforward for nontechnical PC users. This method is in the Settings app. Navigate to *Apps* and then *Default apps,* and you will see default app options for email, maps, music, photos, video, and web browsing; see Figure 11-2. This covers the basics for typical home PC users and will most likely be useful when they have installed a new music or photos app or a new web browser, but it's not opening when they click a file or link.

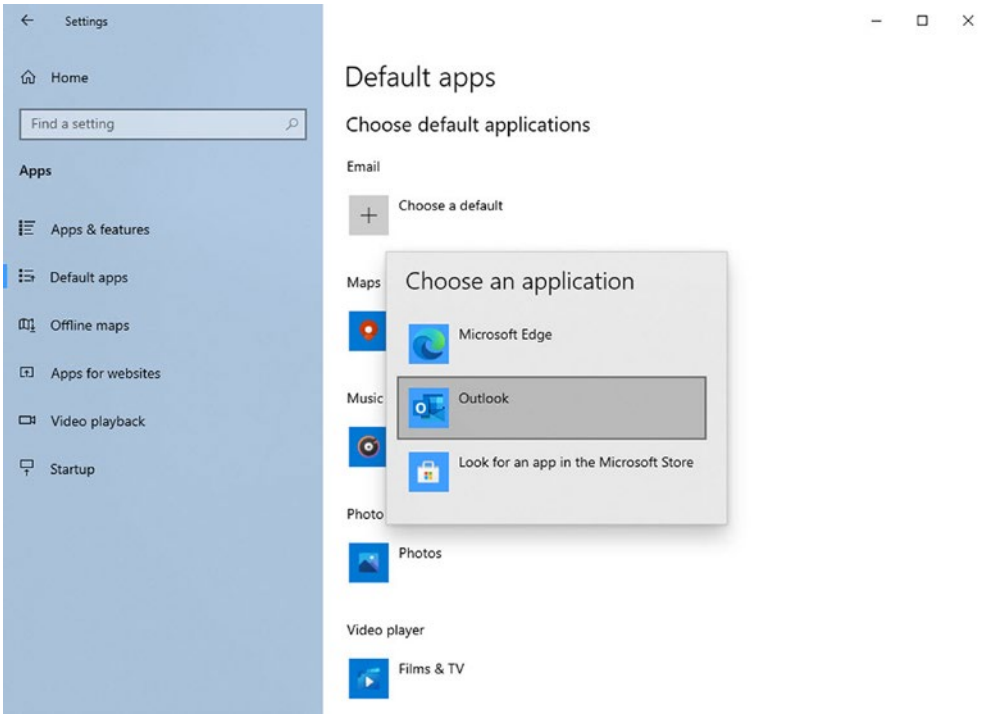


Figure 11-2. *You can set a few app associations in the Settings app*

There are some additional options to help users, however, for other file types. At the bottom of the list are three links. The first of these is *Choose default applications by file type*, which is the option to choose if you have, for example, an Office app that won't open a file, or a file that's opening in the wrong app. To set the file association correctly, you will need to know the file extension of the file you are trying to open. These file extensions are listed on the left side of the window, with their default app association, if one is set, to their right; see Figure 11-3.

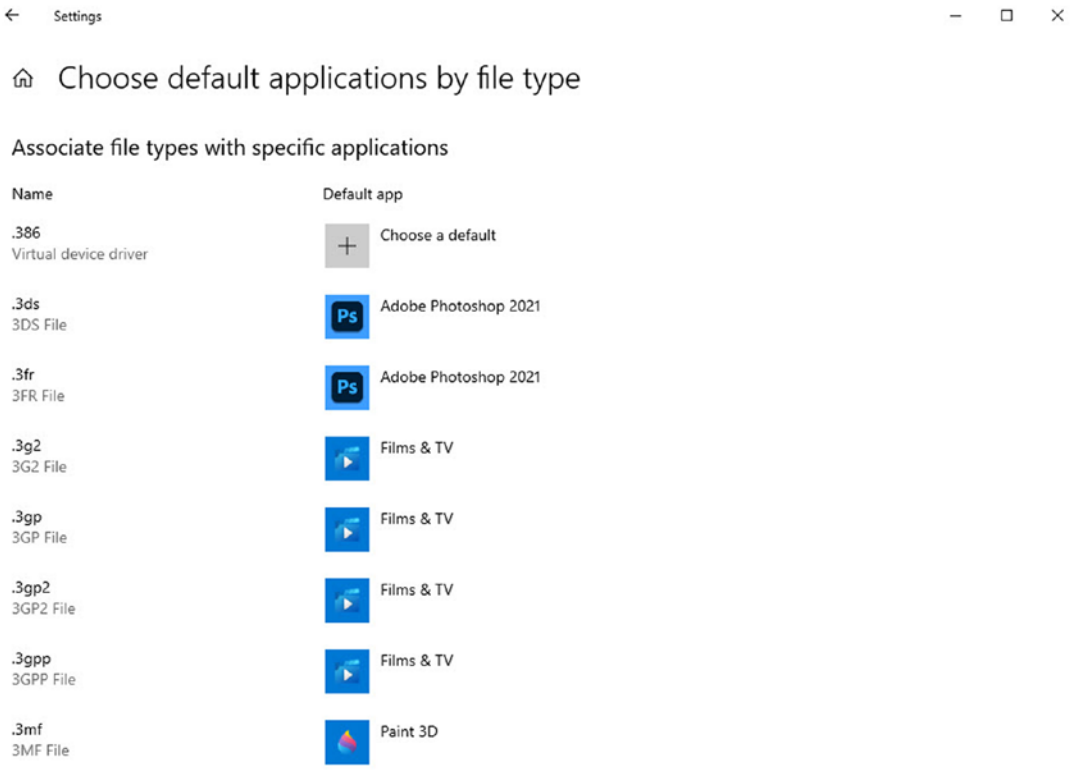


Figure 11-3. *You can set file associations by file type*

Where this method falls down is that clicking the *Choose a default [app]* button will ask you to "Look for an app in the store." This will work for some users and even some businesses, as some win32 desktop apps will be available in the Windows Store. For everybody else, however, you will need to resort to the Control Panel, and I will detail this shortly.

Tip You can display the extensions for all files in File Explorer from the *View* tab on the Ribbon, by checking the *File name extensions* option.

The second of the three links at the main Default apps page is *Choose default apps by protocol*. A protocol is a nonfile element such as a web link (URL), map, DVD burning command, or creating email link. You can see a list of protocols in the left of the window, with their default app association to their right; see Figure 11-4.

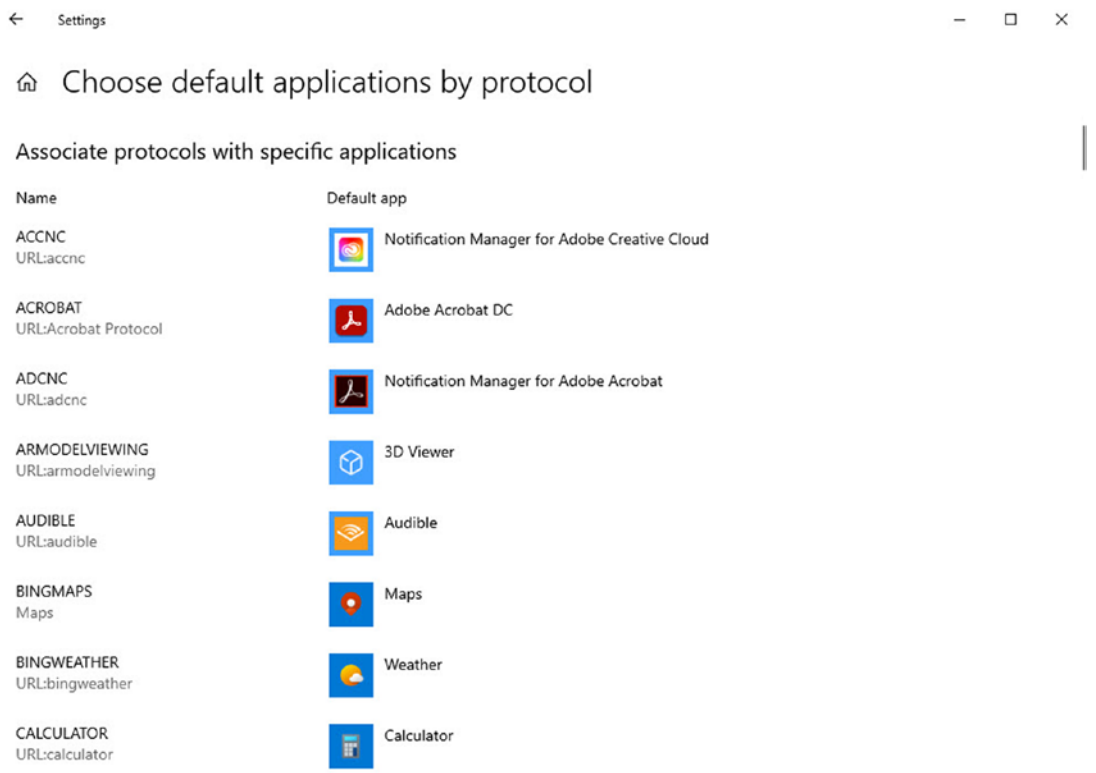


Figure 11-4. *You can set app associations by protocol*

The last link at the Default apps page is *Set defaults by app*. This will display a list of all the installed Store apps and win32 desktop apps on your PC. You can click one to check its file defaults (as one app might open many different file or protocol types) and set all the defaults for the app, or choose which file types or protocols to associate with that app; see Figure 11-5.

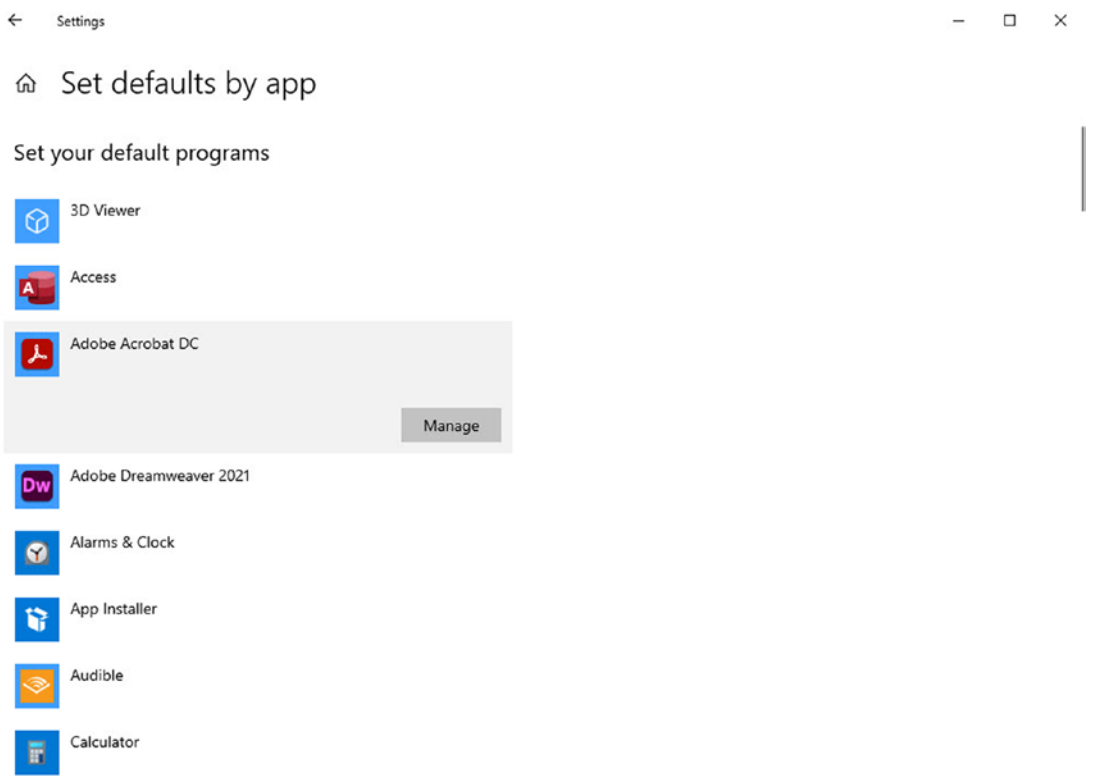


Figure 11-5. *You can get finer control of app associations in the Control Panel*

In the Control Panel, the *Default Programs* options are still available; however, they just link through to *Settings* nowadays. The one exception is the *Change AutoPlaysettings* which, at least for now, remains as a Control Panel applet where you can choose what happens when you plug in something like a USB Flash Drive or memory card; see Figure 11-6. This is a setting I universally switch off on all of my own PCs as for as helpful as AutoPlay is, I find it opening the wrong app on far too many occasions.

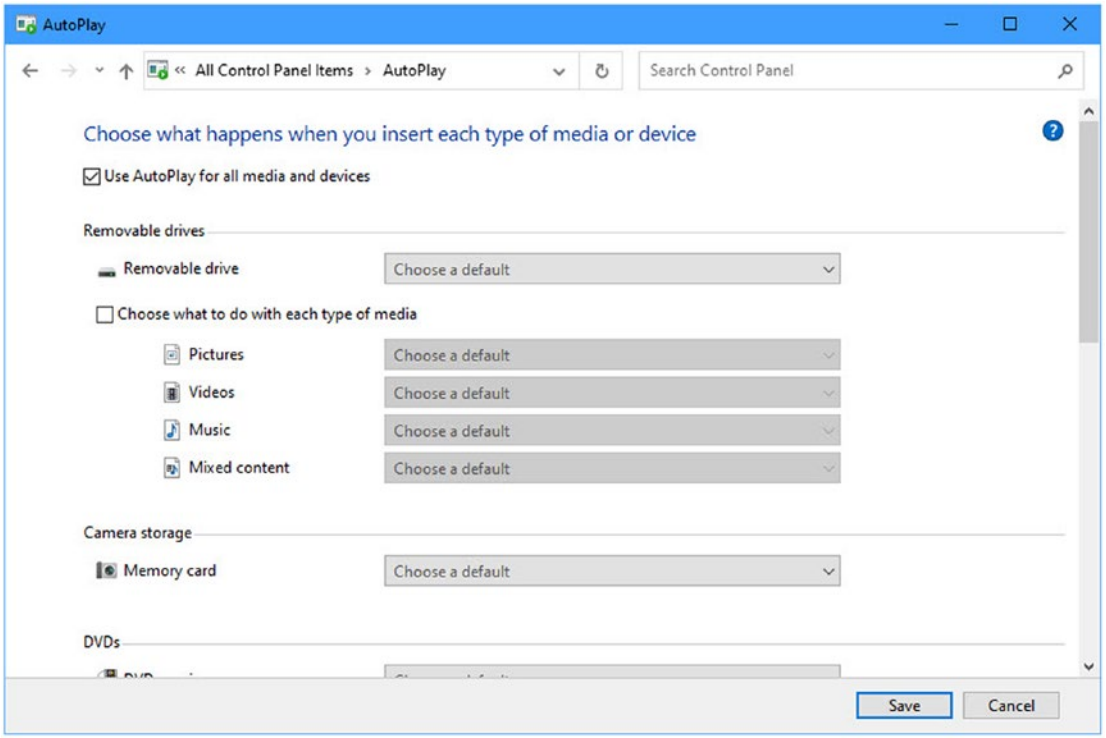


Figure 11-6. *You can still set AutoPlay options in Control Panel*

Setting Drive, Folder, and File Permissions

Sometimes, however, users simply won't have access to drives, file(s), or folder(s) that they really need, and should be able to get access to. This can occur for several reasons, the most common of which is a reinstallation of Windows. In this scenario a new user account will be set up, but the files required by the user might still be residing in the C:\Users\OldUserName\ folder. When you try to open this folder to move the files to the new user file store, you will get an access error, because the folder is locked and you don't have permission to access it.

To fix this issue, you need to first be signed into the PC as an Administrator. Right-click the file, folder, or disk, and select *Properties* from the context menu that appears; this will open a Properties dialog for the item where you need to navigate to the *Security* tab; see Figure 11-7.

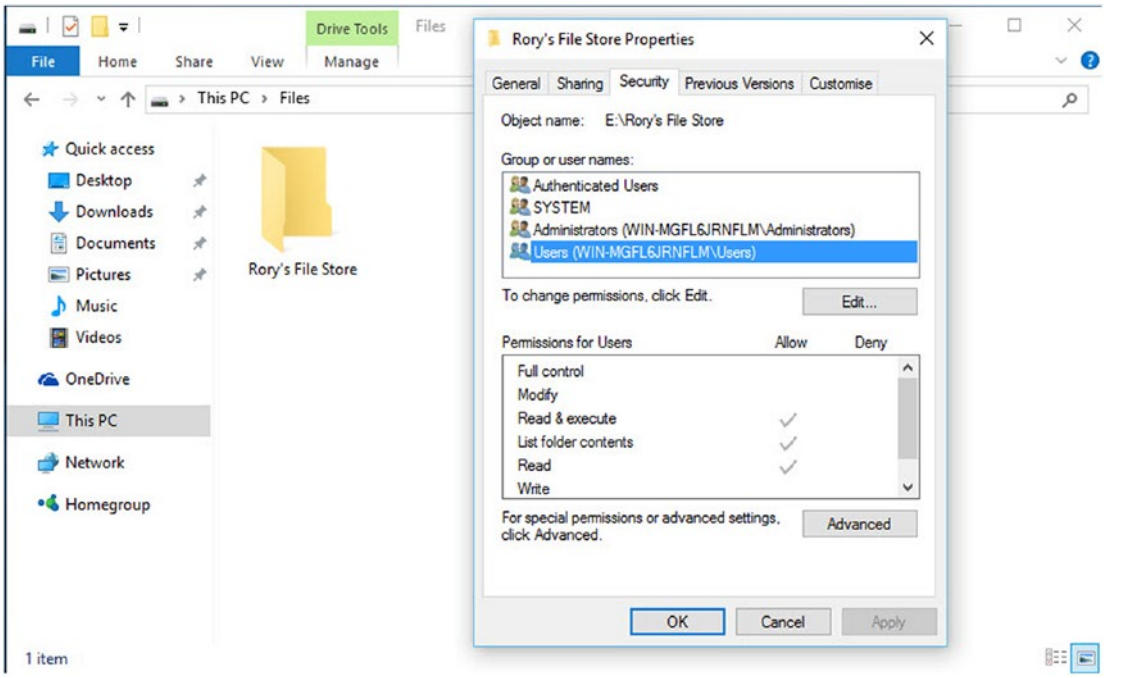


Figure 11-7. *You manage disk and file permissions from within File Explorer*

Here you can see the user groups, and individual users if specified, who are set up on the PC. Clicking one will display their permissions. To change permissions for a user or user group, click the *Edit* button. This will turn each of the available options into a check box. Additionally, it offers *Add* and *Remove* buttons. These are used for adding or removing users from the permissions list; see Figure 11-8.

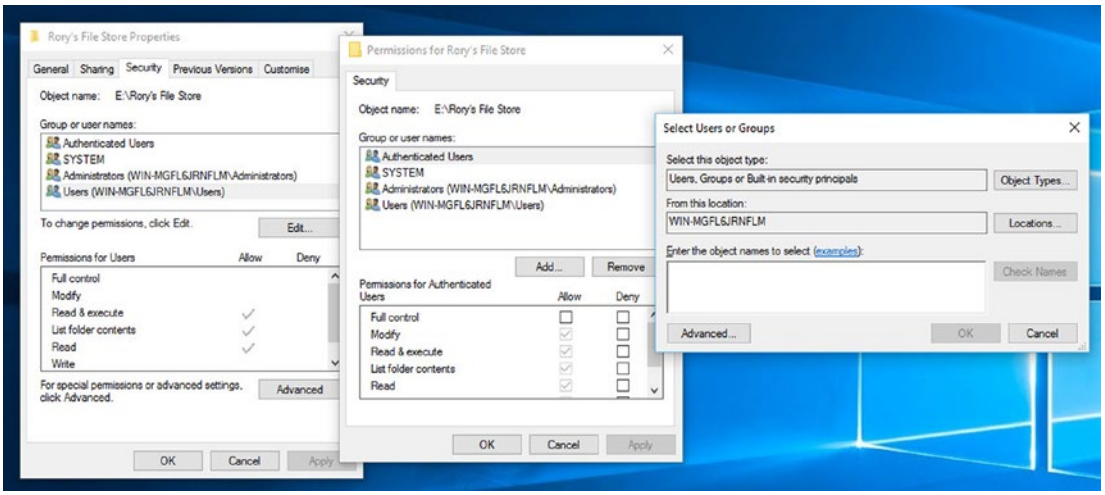


Figure 11-8. *You can add or remove users from the permissions list*

You might want to add a user if the files or folders you are setting permissions for don't reside on the PC, but sit on a network-attached storage drive or on another PC or server to which you have access. Type the name of the user in the format *Computername\Username,* and click the *Check Names* button.

If you are unsure of the computer name or the username, you can click the *Advanced* button, which will allow you to search for users. The dialog that appears will allow you to search different computers on your network, by clicking the *Locations* button, and for user of the PC with the *Find Now* button; see Figure 11-9. You can then double-click a user (or press Ctrl to select multiple users) to select them.

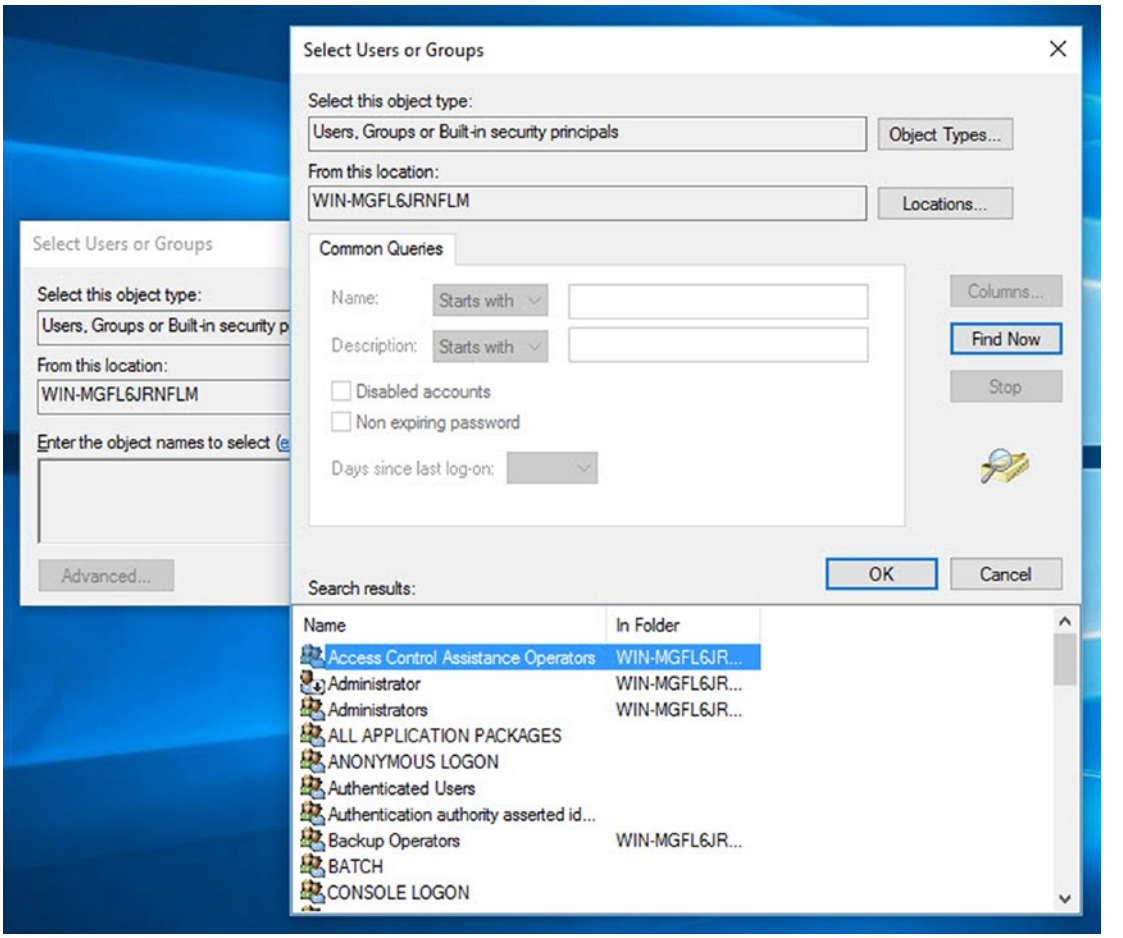


Figure 11-9. *You can search for users on the PC or network*

Sometimes, however, especially as is the case with old user folders, you will want to change the "Owner" of the folder or files to take ownership of them. You can do this from the file, disk, or folder Properties dialog by clicking the *Advanced* button. This will display an advanced permissions dialog, and there are a few different things you can do here. To change permissions, however, click the *Change* button near the top center of the window, next to the current "Owner" name. This will display a user dialog, the same as the one I've just detailed, in which you can search for a user on the PC; see Figure 11-10.

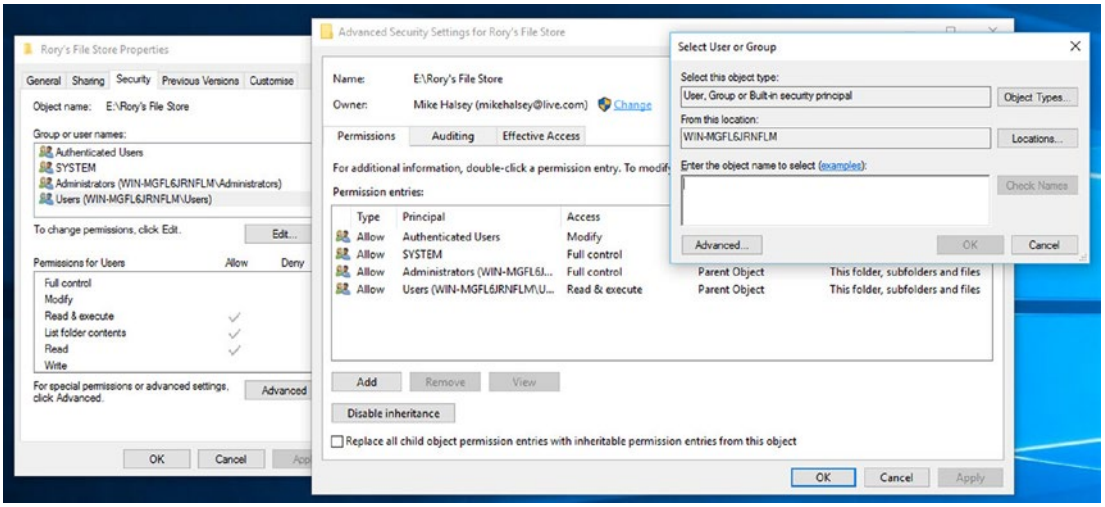


Figure 11-10. *Taking ownership allows you to change the "owner" of files, folders, and drives*

Something else that can prove useful if you're having difficulty accessing files or folders is to enable or disable permission "inheritance," using the button and check box near the bottom left of the window. Inheritance is where you have a tree of nested folders and want to either set the permissions for them to be all the same or disable this feature so that folder permissions are assigned individually.

In short, inheritance is where a folder and its contents will "inherit" their security permissions from the folder above them. This follows all the folders back to the root drive. If you find that, for example, you're creating folders or files that have incorrect permissions, then inheritance is probably not configured. Open the properties for the root folder and enable inheritance for the tree.

Managing Audio Devices

We've all encountered this. You plug some headphones into your PC, connect a Bluetooth speaker, or try to make a call over Skype, and the sound on the PC either doesn't play at all or plays through the wrong device. Now that we commonly use our PCs with hardware such as Bluetooth speakers and gaming headsets, it should be straightforward for people to switch between audio devices, or you would expect Windows 10 to do this automatically.

Alas, when you click the audio icon in the system tray, at the far end of the Taskbar, you're presented in Windows 10 only with a volume slider but no way to change the displayed audio device; see Figure 11-11.

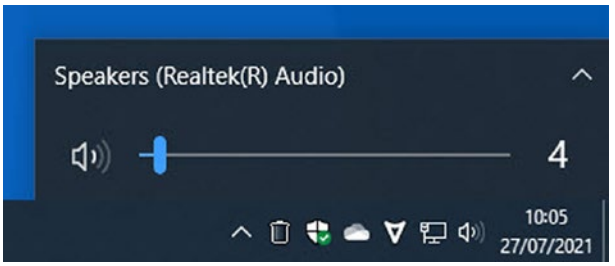


Figure 11-11. *The volume control in Windows 10 doesn't let you switch audio devices easily*

In order to change the audio device, you must right-click the audio icon (you can also open *System* and then *Sound* from Settings) and select *Open Sound settings*; see Figure 11-12.

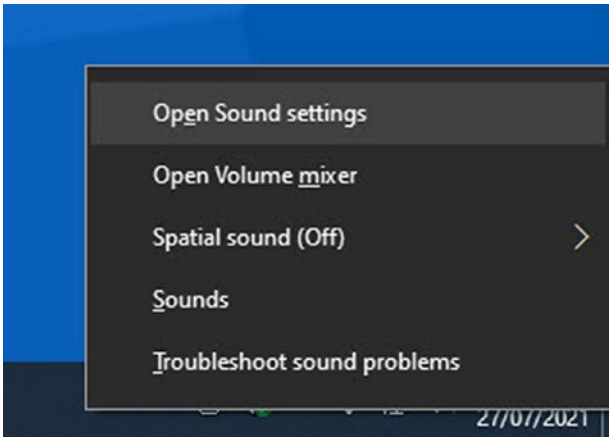


Figure 11-12. *You need to right-click the audio icon to change the sound device*

Once you have the audio dialog open, you are free to change your audio device to the correct one. It's worth noting, especially with regard to communications headsets, that two "Set default" options are available. Figure 11-13 shows that you can set an audio device either as the default or as the default for *Input* (aka microphone) and one for *Output*.

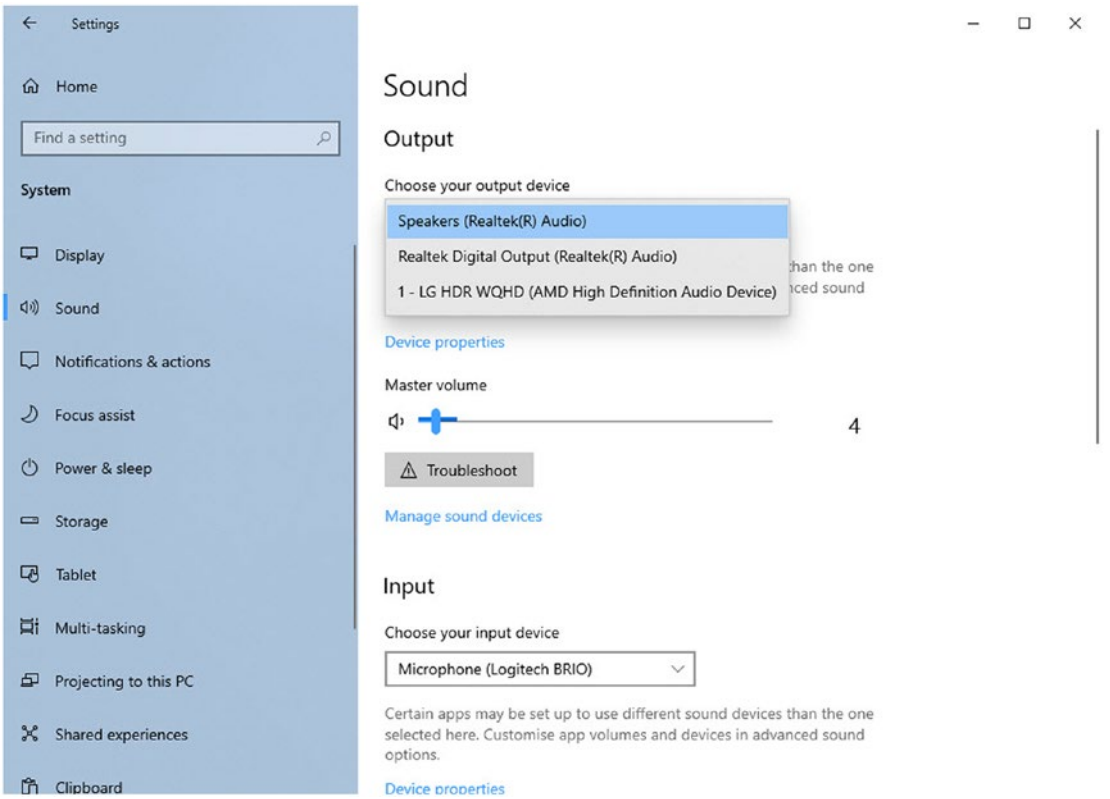


Figure 11-13. *You can set a device as the default device or the default communications device*

Scrolling down the Settings page, you will see a *Sound Control Panel* link which will take you to the older sound devices options (see Figure 11-14), which some people might prefer as it can offer more control.

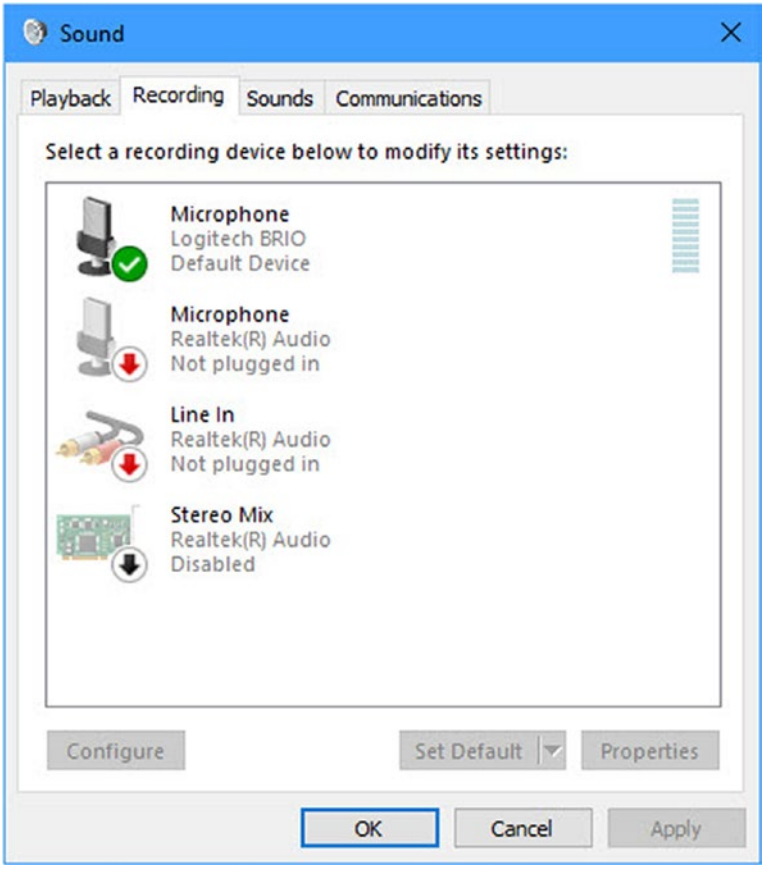


Figure 11-14. *Some Sound Control Panel options are still available*

Troubleshooting Windows Activation

It's not uncommon for a PC to start with a black desktop and a message saying that either your copy of Windows isn't activated or, worse, it's not a genuine copy of Windows. This is a rare, though annoying, circumstance. It occurs because the file containing the registration and activation status of the PC couldn't be found, or wasn't loaded at the PC's startup due to a glitch.

The good news is that this is extremely easy to fix, as all you need to do is restart the PC. Sometimes you may need to fully shut it down and restart it, but a general restart will almost always fix the problem. I say almost always because I have seen only a tiny handful of incidents where the message has persisted. If you are certain that your copy

of Windows 10 is genuine (i.e., that you upgraded from Windows 7 or Windows 8.1 when the free offer was on in 2015/2016, or because the copy of Windows 10 came with a new PC or you bought a retail copy), then you can try reentering your activation key

You can do this in *Settings* by opening *System* ➤ *About*, and you will see a link called *Change the product key or upgrade your edition or Windows*. This will display your activation status and also allow you to reenter or change the product key as is necessary; see Figure 11-15. If this doesn't work, you could have a bad Registry corruption and can try a System Restore which I detailed in Chapter 2. If that doesn't work, you may need either to reset or reinstall Windows.

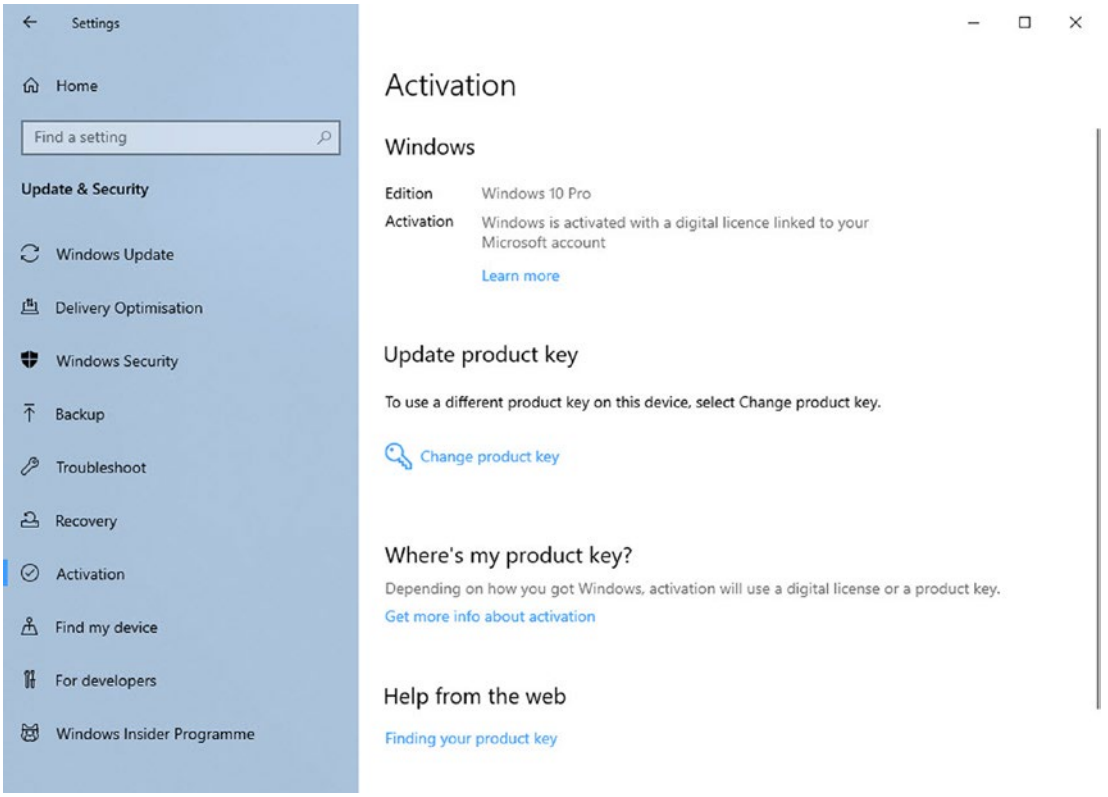


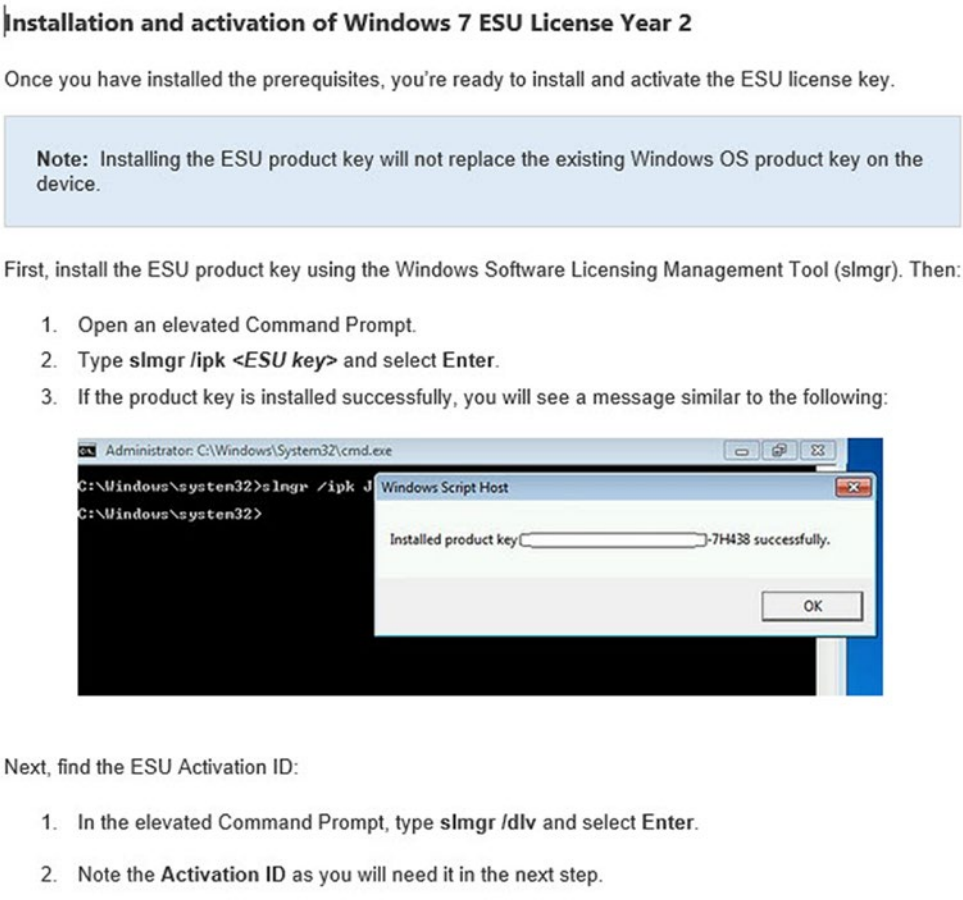
Figure 11-15. *You can change or reenter your product key in Settings*

Information about Windows licensing and activation can be found online at **`http://windows.microsoft.com/windows/genuine`**, and it's not unheard of for independent PC makers (such as those on your Main Street) to sell PCs with pirated copies of Windows.

A Note About Windows 10 Extended Support Product Keys

Windows 10 at the end of its life will very likely go into extended support. This is fairly inevitable after the success of the paid-for extended support for Windows 7. Given that the underpinnings of Windows 10 and Windows 11 are identical, and that the Windows 7 extended support has raised an absolute fortune for Microsoft, they'd be a bit daft not to.

Each year you purchase extended support, you will receive a new product key with a specific number of licenses to cover the PCs you use. You will also receive instructions on how to activate these keys on your PCs as I did when I took out extended support for my own Windows 7 Media Center PCs; see Figure 11-16. And yes, I still use Windows Media Center every day and love it so much I paid for extended support.



Installation and activation of Windows 7 ESU License Year 2

Once you have installed the prerequisites, you're ready to install and activate the ESU license key.

Note: Installing the ESU product key will not replace the existing Windows OS product key on the device.

First, install the ESU product key using the Windows Software Licensing Management Tool (slmgr). Then:

1. Open an elevated Command Prompt.
2. Type **slmgr /ipk** ***<ESU key>*** and select **Enter**.
3. If the product key is installed successfully, you will see a message similar to the following:

Next, find the ESU Activation ID:

1. In the elevated Command Prompt, type **slmgr /dlv** and select **Enter**.
2. Note the **Activation ID** as you will need it in the next step.

Figure 11-16. *Instructions for Windows 10 Extended Support product keys might not be necessary*

These instructions will ask you to use the *slmgr* license tool that's built into Windows to change the key. This is fine for an enterprise scenario where you have dozens of perhaps even hundreds of PCs to update. If you only have a handful though, it can be simpler to just open *Settings* ➤ *System* ➤ *About* ➤ *Activation* and enter the new product key there.

Troubleshooting and Resetting Windows Update

Sometimes, though fortunately not very often, Windows Update becomes corrupt and will flatly refuse to either download or install updates. This is more than an annoyance as it will prevent essential security and stability updates from being installed on your PC. It happens when one or more of the downloaded updates are corrupt and unreadable.

Should this happen, you will need to reset Windows Update. You should restart your PC at this point (as if the Windows Update process is running, it will prevent you from deleting some files). The first thing to do will be to temporarily shut down the services that run Windows Update, as with these running you will be unable to delete the appropriate files. Open **services** from the Start Menu, and find *Windows Update* and *Windows Update Medic Service* in the list. Right-click each one, and select *Stop* from the context menu that appears; see Figure 11-17.

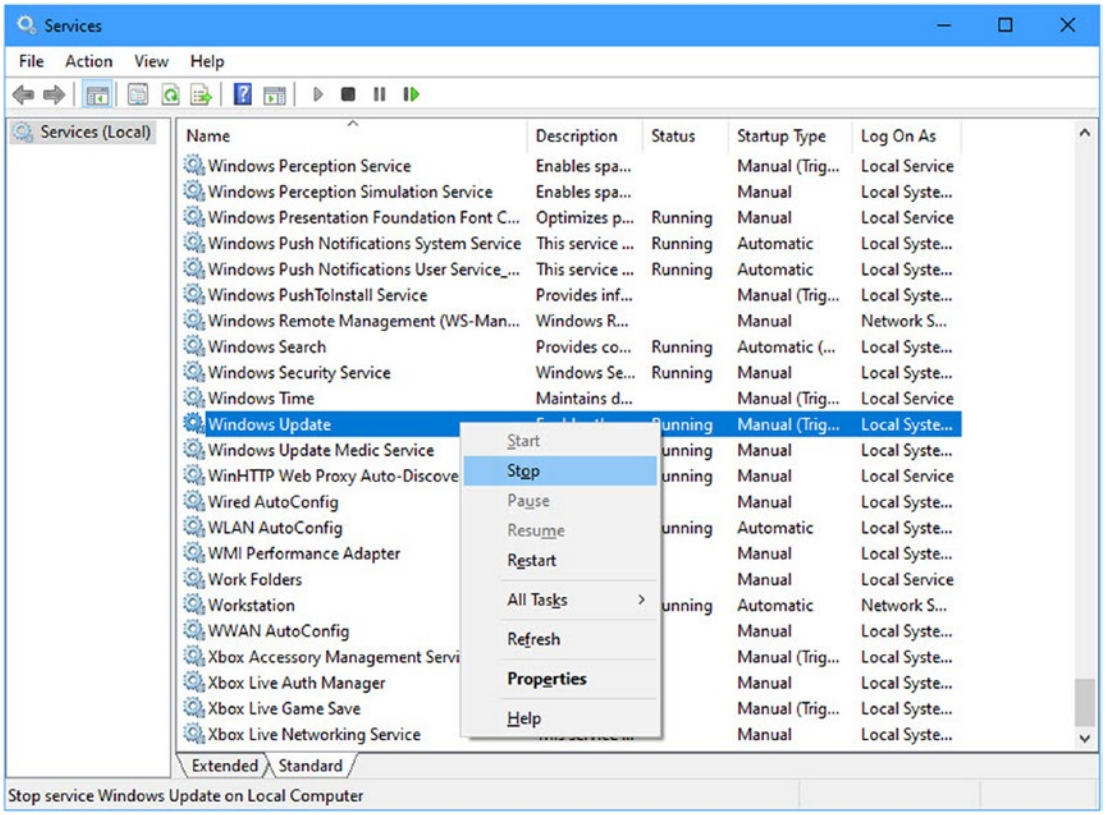


Figure 11-17. *You need to stop the Windows Update services*

Next, open File Explorer and navigate to `C:\Windows\SoftwareDistribution`; see Figure 11-18. You should then delete **all** the contents of this folder, and Windows Update will be reset. Restart the PC when you're done, and the Windows Update services will begin running again automatically.

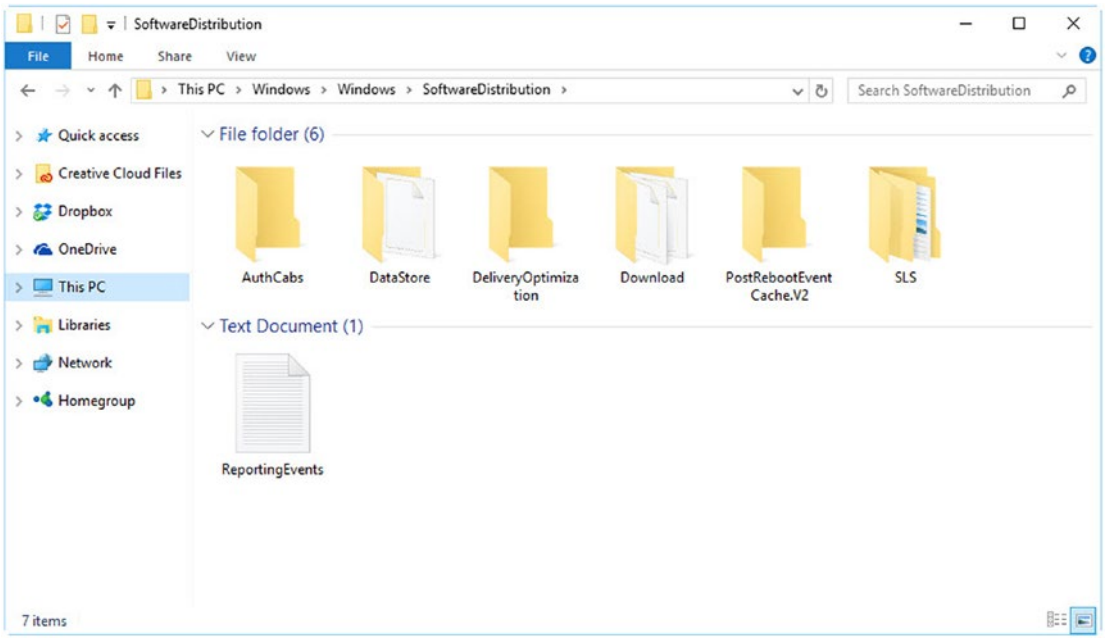


Figure 11-18. *You can delete the contents of the SoftwareDistribution folder to reset Windows Update*

Troubleshooting Power Loss During an Update Installation

Windows 10 is incredibly resilient during the installation of updates, and despite the operating system asking you not to turn off your PC when updates are being installed, doing so is unlikely to harm it. In fact the Windows Update system is **so** resilient that I have tried repeatedly in the past to break the OS by forcing the power off during major update installations, only to fail to break the OS on every occasion. Every time I tried, the installation just restarted when I switched the PC back on.

My best efforts to break my own PC notwithstanding (see the lengths I go to for you all?) it's not beyond the realms of possibility that something could break on a PC at some point in the future. It's easy to rectify, however, so long as you have created a USB Recovery Drive (remember those?). If you start the PC from the Recovery Drive, you can run System Restore and roll the OS back to a point before the update installation took place; see Chapter 8 for details on how to do this. This will fix your copy of Windows.

Managing and Resetting Windows Search

In the same way that downloaded Windows Update files can become corrupt, so too can the database used by Windows 10's search engine. Resetting this database (called the Search Index) is a very simple and straightforward operation. Open the Control Panel and then click *Indexing Options* (I won't recommend searching for Indexing options on this occasion). When the Indexing Options dialog appears, click the *Advanced* button, and in the dialog that appears, under the *Index Settings* tab, you will see a Troubleshooting section with a Rebuild button; see Figure 11-19. Click this to delete the current index and rebuild it from scratch.

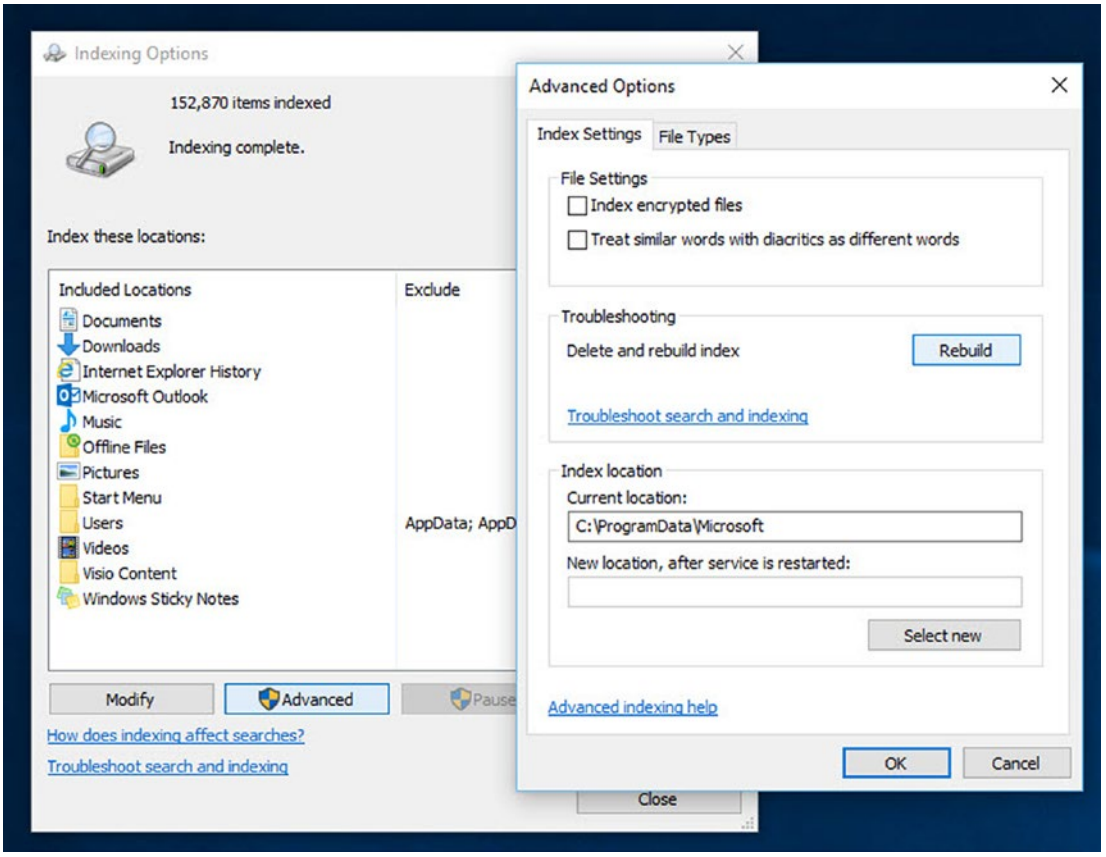


Figure 11-19. *You can ask for Windows to search to delete its database*

Troubleshooting Slow Startup

It wasn't too long ago that we'd switch our computers on in the morning, and then go and make a cup of coffee while the boot sequence ran. After 5 or so minutes we'd be confident that when we returned to the PC, we'd be faced with the sign-in screen. Nowadays a modern PC will start up in seconds, even from cold, which is great news for PC users, but bad news for coffee sellers.

This is especially useful when returning to your PC after a break or from lunch, when you or, more honestly, your boss wants you working again as quickly as possible. But what happens when you have a normally speedy PC that's suffering from slow startup?

Troubleshooting slow startup is fairly straightforward in Windows 10, as it's almost always going to be your apps that are slowing things down. I say "almost always" because if you have a PC with a mechanical hard disk, it may need defragmenting. A fragmented disk won't slow the PC much, but you will probably notice the difference.

To manage your startup apps, open the Task Manager. You can do this from the *Win+X* menu, from the *Ctrl+Alt+Del* menu, or by right-clicking a blank space on the Taskbar. Once the Task Manager is open, click the *Start-up* tab, where you will see all your startup apps listed; see Figure 11-20.

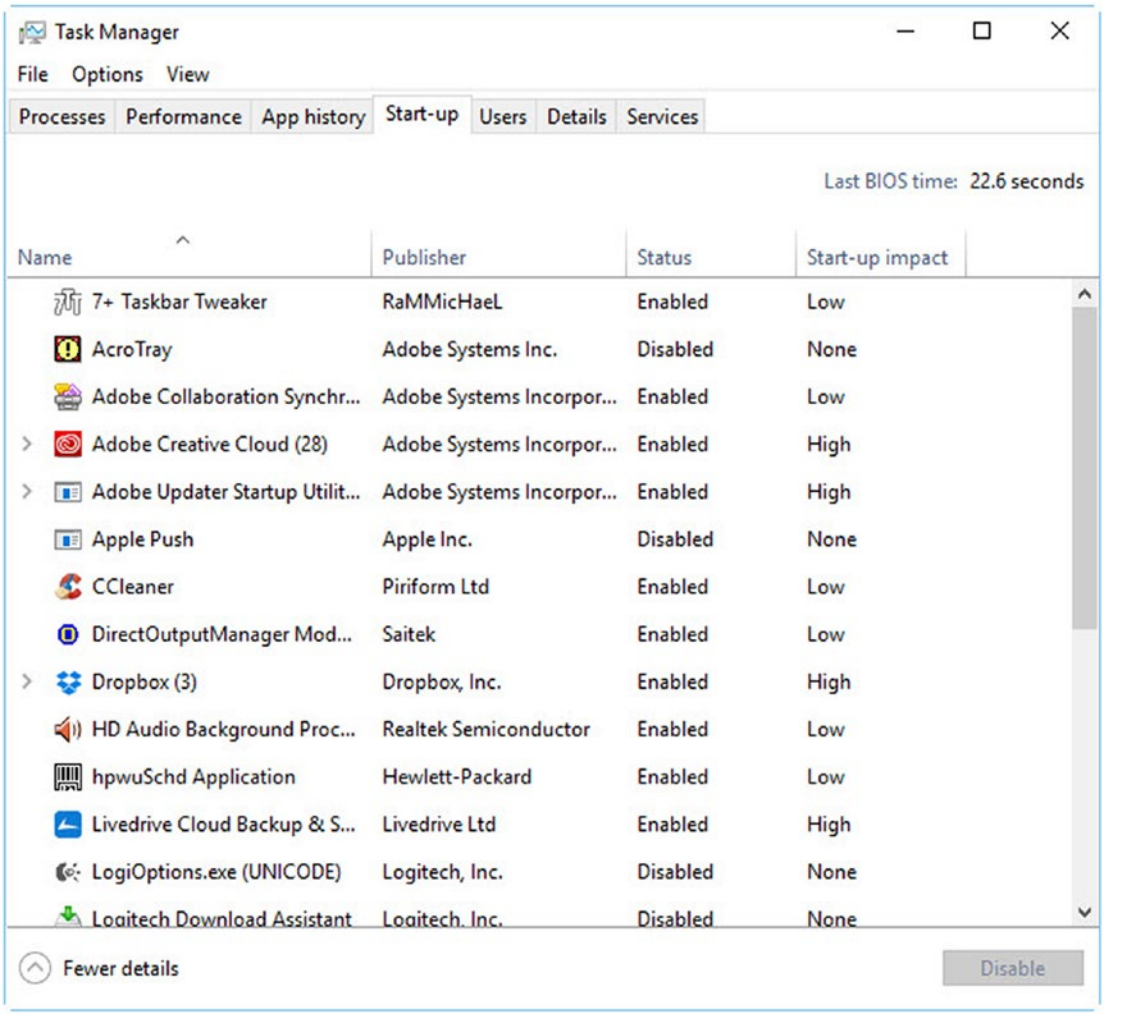


Figure 11-20. *You can manage startup apps in Task Manager*

Next to each is a *Start-up impact* rating. This will appear after the first few startups since an app was installed (obviously, it's impossible for Windows 10 to measure the Startup impact on an app that's only just been installed). The ratings show Low, Medium, or High, with the apps rated high being the ones that will slow your PC's startup the most.

In Figure 11-20 we can see that Adobe Creative Cloud, Adobe Updater, and Dropbox are all rated high (which should be very annoying for both companies as they should know better!). You can click any startup app, and the *Disable* button will become clickable, so you can stop that app from running at startup.

Windows 10 Hangs on Startup

Occasionally you might find that your PC doesn't start at all, and you're left with either a spinning loading icon or just a black screen. There can be several reasons for this:

- Network connections can cause a stalled startup. If your PC is connected to the network via an Ethernet cable, unplug this temporarily and see if startup continues. Should this be the case, it's likely your network driver will need to be updated to prevent this from happening each time you switch on the PC.
- Sometimes a PC will hang at the BIOS/UEFI screen with an error. This will be most commonly because the BIOS/UEFI system is being reset each time the PC starts (which likely means you will need to put a new battery on the motherboard), or because the BIOS/UEFI settings are either corrupt or unstable. You can fix the latter by entering the BIOS/UEFI interface and selecting the "Load optimized defaults" option, or by resetting the BIOS using the motherboard jumper I detailed in Chapter 6.
- If you get the message "No operating system found," it's likely that there is a hard disk inconsistency, either in the BIOS/UEFI or with the disk itself. In the BIOS/UEFI interface, the default boot order might have been changed (perhaps because of a BIOS/UEFI reset), and the PC is trying to load the operating system from another disk, perhaps a network boot or removable drive, where no operating system exists. Alternatively, have the drives in the PC been changed recently? If you have performed maintenance or cleaning on the PC, is the hard disk on which Windows 10 is installed plugged into the same motherboard SATA socket it was before? These are assigned Drive 0, Drive 1, and so on by BIOS and Windows, and the OS boot loader will expect to find its files on the same drive it was installed on.
- Lastly (and this one is almost comical, though you may be surprised how often it occurs), if you have recently installed Windows 10 but keep seeing the setup screen when you start the PC, this is because you need to unplug or remove the USB Flash Drive or DVD containing the Windows installer.

Note Windows 10 never truly shuts down completely, as it always hibernates some part of memory to disk to aid in a quick startup. Sometimes this will become corrupt, causing startup problems. To rectify this hold down the *Shift* key when selecting *Shutdown* from the Start Menu. This will force the PC to do a full, rather than a hybrid, shutdown. Alternatively, if the PC won't start, hold the power button for 4 seconds during startup to force a manual shutdown.

Windows 10 Shuts Down Slowly

Just as annoying as a slow startup is when the PC won't shut down, or shuts down extremely slowly. Normally when you shut down the PC, if any apps are still running, you will be presented with a list of the apps and asked if you want to force them to shut down, or if you want to wait for Windows 10 to shut them down itself.

Sometimes, if you're like me, you'll hit the force shutdown button and walk away. On other occasions, however, you might just get up and walk, and then come back some time later to discover the PC is STILL trying to shut down the apps.

There are some changes you can make to the Registry, however, to speed up the shutdown of your PC. You can access the Registry Editor by searching for **regedit** at the Start Menu.

Caution Always be careful in making changes to the Windows Registry. Make a backup of the Registry from its *File* menu so the Registry can be restored should a change cause Windows to become unstable. This can be achieved from the Recovery Panel if necessary; see Chapter 8 for details of how to run the Registry Editor in the Recovery Panel. If you have encrypted your hard disks using Bitlocker, you should copy the Registry backup file to a nonencrypted drive.

There are two options you can change in the Registry to affect Windows Shutdown:

- `HKEY_LOCAL_MACHINE` ➤ `SYSTEM` ➤ `CurrentControlSet` ➤ `WaitToKillServiceTimeout` is set by default at 5000 milliseconds (5 seconds). This setting determines how long the OS waits for

Windows and third-party services to close before notifying the user the service is not closing. You may wish to increase this number to 50000 if services require longer to quit.

- `HKEY_CURRENT_USER` ➤ `Control Panel` ➤ `Desktop` ➤ `WaitToKillAppTimeout` will need to be created as it doesn't exist by default in Windows 10; see Figure 11-21. This key determined how long the system waits for user processes to end before notifying the user. The time is stated in milliseconds (20000 being 20 seconds). You can force shutdown by changing the value to **1**, though be aware that forcibly closing any apps with open files may result in loss of data.

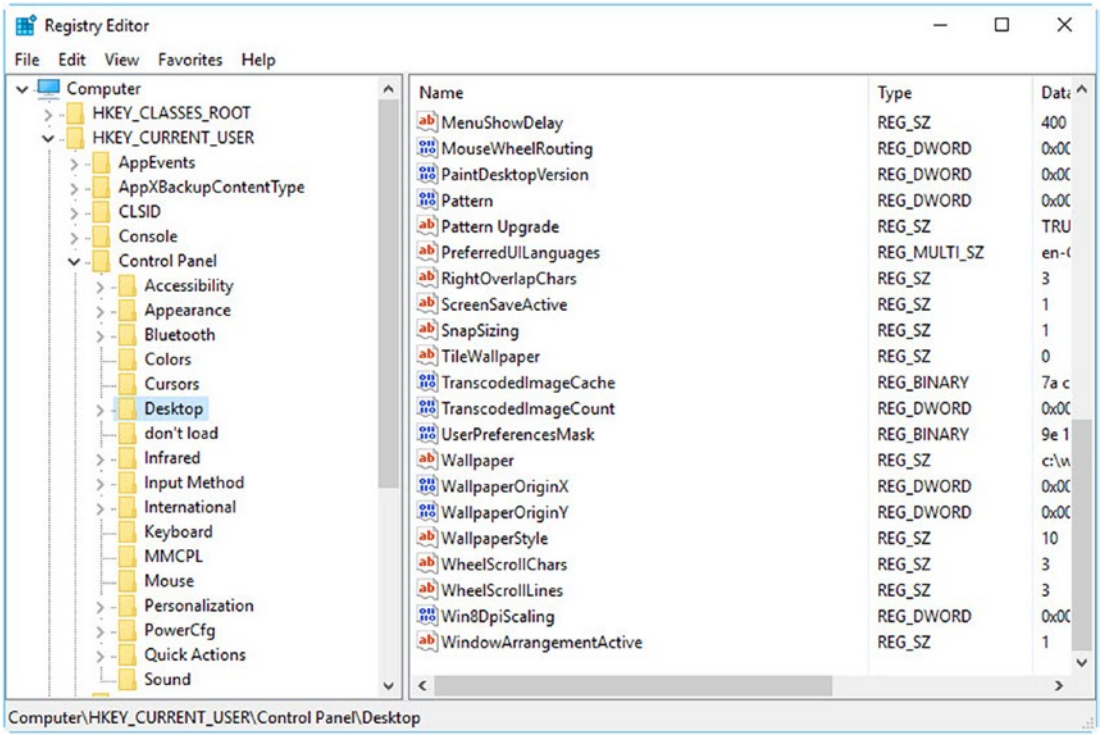


Figure 11-21. *WaitToKillAppTimeout doesn't exist in Windows 10 and needs to be created*

Windows Fails to Sleep/Resume from Sleep

I mentioned a little while back that Windows 10 doesn't really shut down, instead going into a deep hibernation so as to help it restart quickly. By far the quickest, and now extremely common and popular, way to shut down a Windows PC is to put it to sleep. Whether you simply close the lib on your laptop, press the sleep button on your tablet, or activate sleep from the Start Menu on a desktop, sleep keeps the current memory active so the PC can start to the desktop within a second or two.

Sometimes this doesn't work however, and you need to troubleshoot the Sleep feature in Windows. There are different sleep states available for PCs, laptops, and tablets, and you can check which ones are supported on your hardware by opening a Command Prompt window and typing `powercfg/availablesleepstates`; see Figure 11-22.

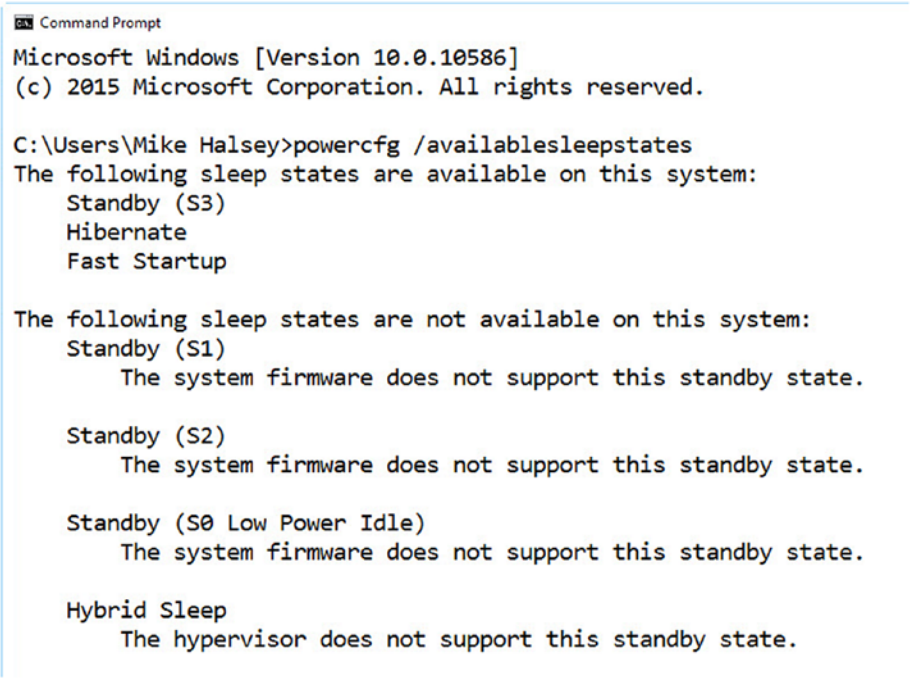


Figure 11-22. *You can use the PowerCFG command to check sleep state compatibility*

In this example we can see the S0, S1, S2, S3, and Hybrid Sleep states and so on, and that only S3 is supported on this PC. But what are these different states and which should you choose for your PC?

- **S0** is a low-power idle state where power is used at a normal rate, but where unused devices, such as the hard disk, can be powered down as necessary.
- **S1** is the first Sleep state for PCs. Power consumption is less than with the S0 state, but greater than the other states. In this state, both the process and communications bus clocks are stopped. This is the first state the system goes into when you put it to sleep.
- **S2** is similar to S1, but in this state, the processor does not receive power and is reset on startup. This causes the system cache to be lost and causes more of a "reset" to the system than with S1. S2 is engaged after a period of sleep in S1.
- **S3** is very similar to S2; however, in this state only power to the system memory is maintained. S3 is engaged after a period of sleep in S2.
- **S4** is the lowest-power sleep state and all devices are powered off. Memory is moved to a hibernation file on the disk and reloaded on startup. S4 is engaged after a period of sleep in S3.
- **S5** is a shutdown state for the PC. S5 is engaged after a period of sleep in S4, when the power gets low.
- **Hybrid sleep** is designed for desktop PCs and is a combination of sleep and hibernate: any open documents and files are held both in memory and on the hard disk, so that work can continue even after a power failure.
- **Connected standby** provides an instant-on sleep state. This power state requires compatible hardware support and suspends the state of the OS while maintaining it with a tiny power draw.

If you find that a device isn't waking up, or is misbehaving when you put the PC to sleep, you can use the **powercfg /devicequery** command to determine what hardware devices in your PC support each sleep state. The command is used in the format **powercfg /devicequery s1_supported** and so on through to **S4_supported**. Each will provide a list of the installed hardware that's okay at that level of sleep. Use the command **powercfg /devicequery /?** to see all available command options.

You can also troubleshoot Sleep and power management on a PC using the **powercfg** command with the switches **/batteryreport**, **/sleepstudy**, and **/energy;** see Figure 11-23. These commands save reports to your hard disk as HTML files that can be opened in a web browser. Again more options are available on **powercfg /?**.

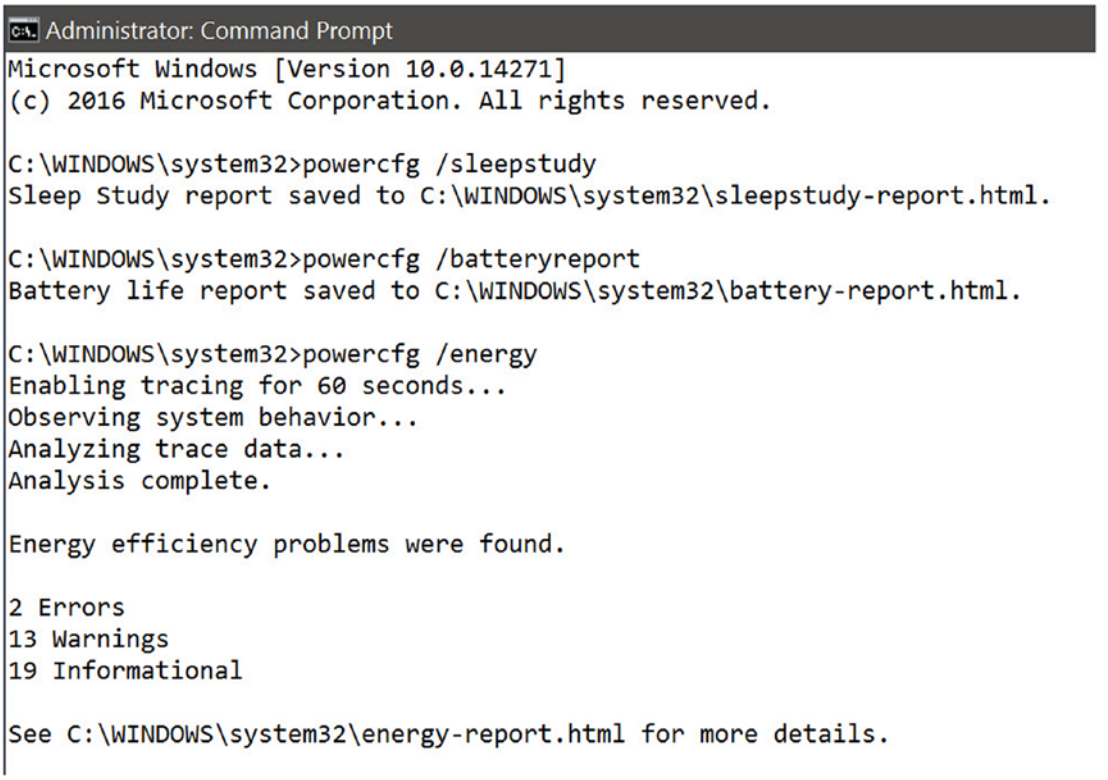


Figure 11-23. *You can troubleshoot power, battery, and sleep issues*

The Battery Report will apply only to laptops and tablets and will provide detailed metrics on power usage and battery capacity over the last few days. The Power Efficiency Diagnostics Report, however, can help you ascertain if the power management options set in Windows are optimal for your device.

In Figure 11-24, you can see a typical Power Efficiency Diagnostics Report. There are warnings here that the power settings for this particular PC are not set correctly. The descriptions are all in plain language so you can determine what changes, if any, you can make to improve power management on the PC.

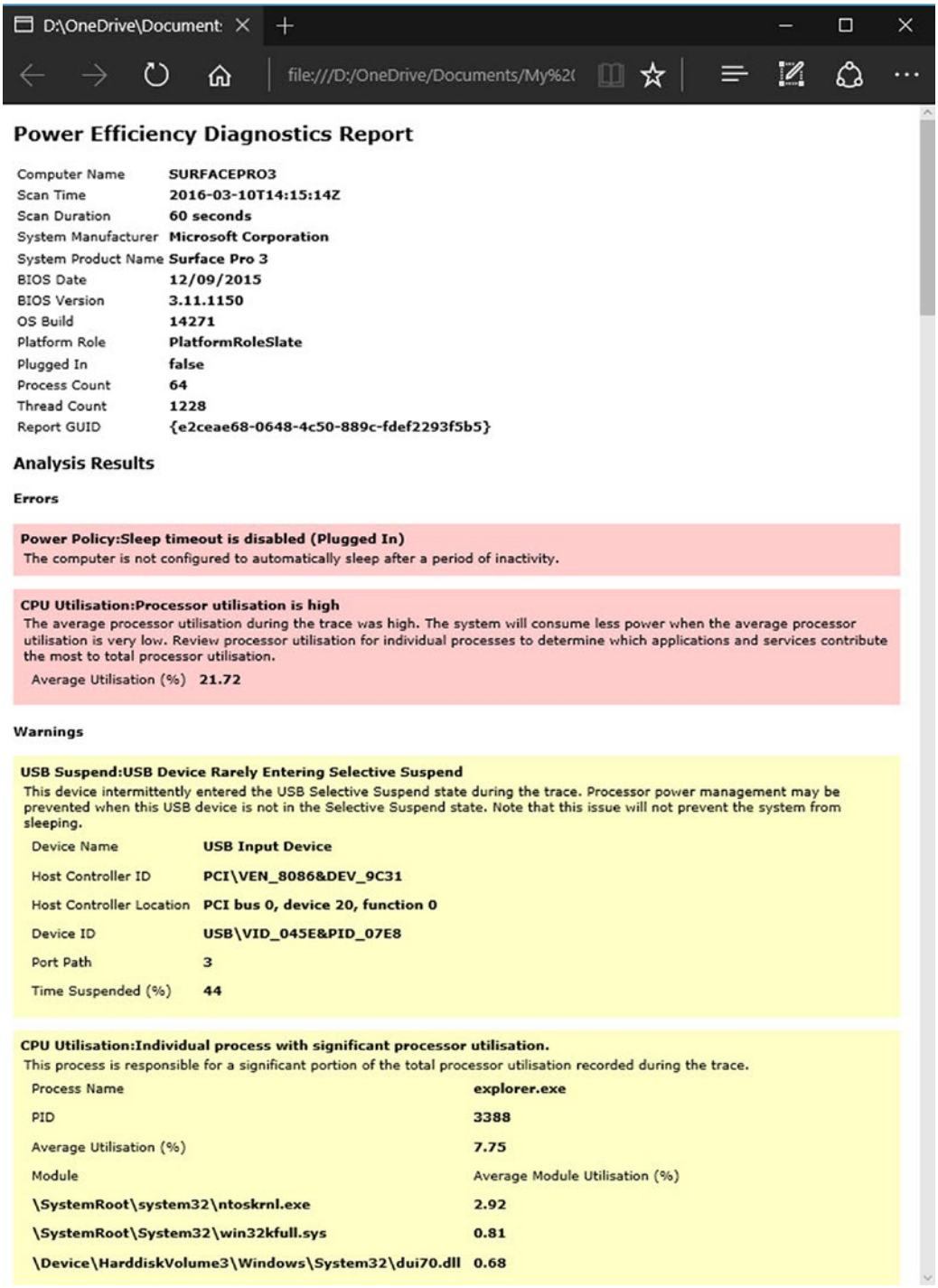


Figure 11-24. *The Power Efficiency Diagnostics Report can help you determine if your power settings are correct*

The Sleep Study provides extremely detailed graphics and metrics to show power consumption for the PC when it is in a sleep state or Connected Standby; see Figure 11-25. The information includes what components in the PC were still drawing power, and how long they were active for during sleep. This includes the "Top Five Offenders" for power usage.

Figure 11-25. *The Sleep State report is extremely detailed and useful*

Windows 10 is able to wake periodically during sleep to check for updates, perform maintenance, and update LiveTiles in the Start Menu. At the bottom of the Sleep Study are details of all the apps and services that have been active during these wake states; see Figure 11-26. You can use this information to determine if something is waking the PC too often, or using too much power at those times.

Srum Data

Data obtained from the SRUM database.

Energy Estimation

APP ID	TOTAL (mJ)	CPU (mJ)	DISPLAY (mJ)	DISK (mJ)	MBB (mJ)	NETWORK (mJ)	SOC (mJ)	OTHER (mJ)
\Device\HarddiskVolume3\Windows\System32\svchost.exe [mikeh]	258268	2639	0	254932	0	697	0	0
System [SYSTEM]	31736	2553	0	23040	0	6143	0	0
\Device\HarddiskVolume3\Windows\System32\svchost.exe [utcsvc] [SYSTEM]	14878	1269	0	6081	0	7528	0	0
\Device\HarddiskVolume3\Windows\System32\svchost.exe [netsvcs] [SYSTEM]	3262	496	0	2002	0	764	0	0
\Device\HarddiskVolume3\Program Files\ESET\ESET Smart Security\ekrn.exe [SYSTEM]	2516	295	0	44	0	2177	0	0
\Device\HarddiskVolume3\Windows\System32\svchost.exe [LocalServiceNetworkRestricted] [LOCAL SERVICE]	1545	480	0	1061	0	4	0	0
\Device\HarddiskVolume3\Windows\System32\svchost.exe [NetworkService] [NETWORK SERVICE]	1322	775	0	0	0	547	0	0
\Device\HarddiskVolume3\Windows\System32\svchost.exe [LocalSystemNetworkRestricted] [SYSTEM]	1077	168	0	909	0	0	0	0
Memory Compression [SYSTEM]	1015	23	0	992	0	0	0	0
System Interrupts [SYSTEM]	935	621	0	0	0	0	314	0
\Device\HarddiskVolume3\Windows\explorer.exe [mikeh]	326	78	0	144	0	104	0	0
\Device\HarddiskVolume3\Windows\System32\lsass.exe [SYSTEM]	325	325	0	0	0	0	0	0
\Device\HarddiskVolume3\Windows\System32\LogonUI.exe [SYSTEM]	294	4	0	290	0	0	0	0
\Device\HarddiskVolume3\Windows\System32\svchost.exe [RPCSS] [NETWORK SERVICE]	273	273	0	0	0	0	0	0

Figure 11-26. *The Sleep Study also details apps and services using power during wake states*

Armed with all the information the powercfg commands and reports have given you, you can then modify the standard sleep settings for the PC to ensure Sleep operates properly on the PC. In the *Power Options* in Control Panel, click *Choose what the power button does,* and then click *Change settings that are currently unavailable*.

Now you will be presented with a list of the available and supported sleep states for your PC; see Figure 11-27. Each, including Fast Start-up, can be disabled should it be causing a problem on the PC. Fast Start-up is the feature I mentioned earlier where some parts of memory are saved to disk as a hibernation file. If you wish for your PC to clean start each time you switch it on, you can disable this feature.

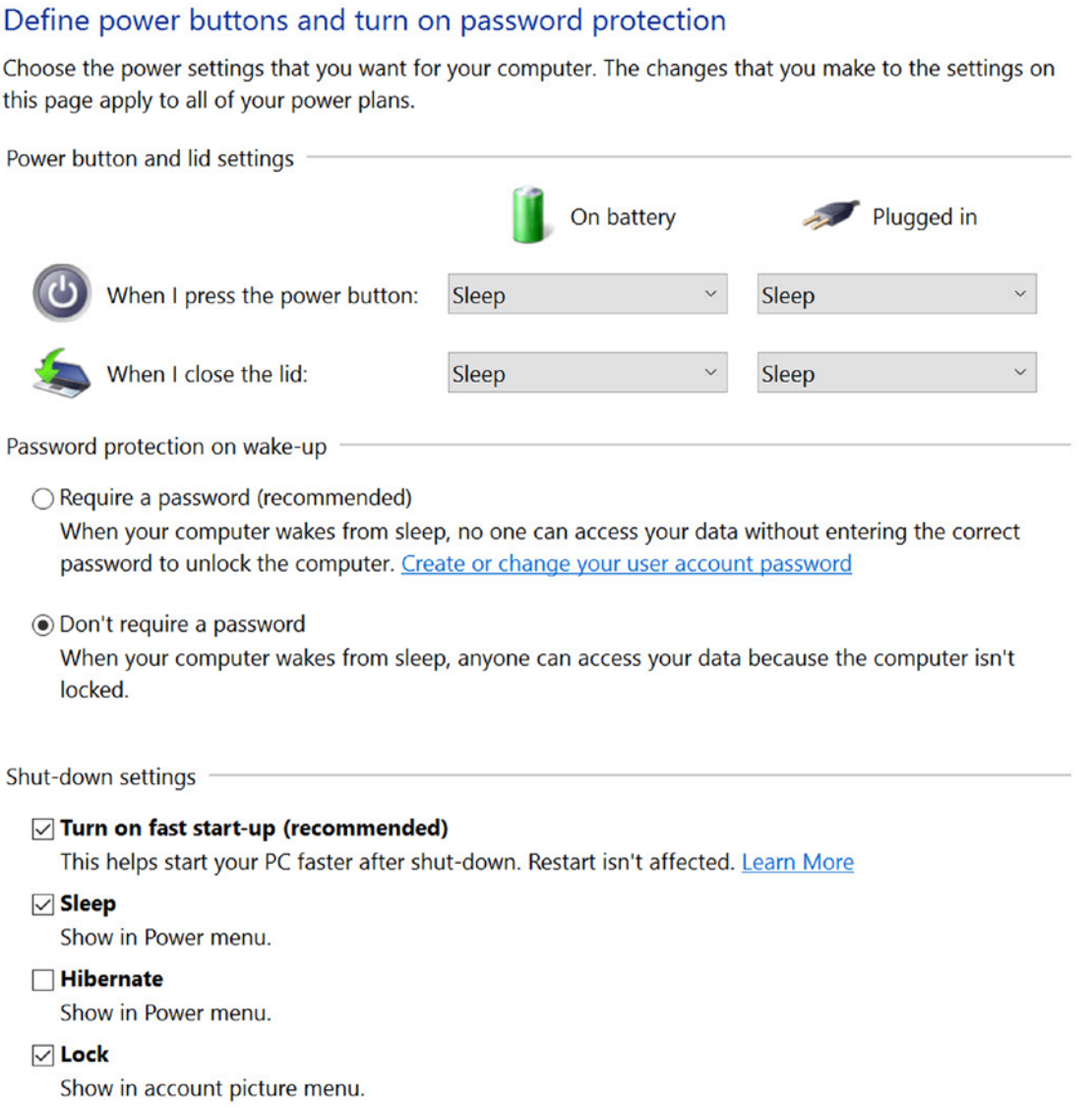


Figure 11-27. *You can disable sleep states that are causing problems on your PC*

Gaining Access After Bitlocker Lockout

Sometimes, perhaps after a disk corruption (even a small one can cause this), you can find yourself locked out of the PC until you can enter your 48-character unlock key; see Figure 11-28. It's also worth noting that on some PCs such as Microsoft Surface Pro and Surface Book lines, Bitlocker is enabled automatically if you sign into the device with a Microsoft account.

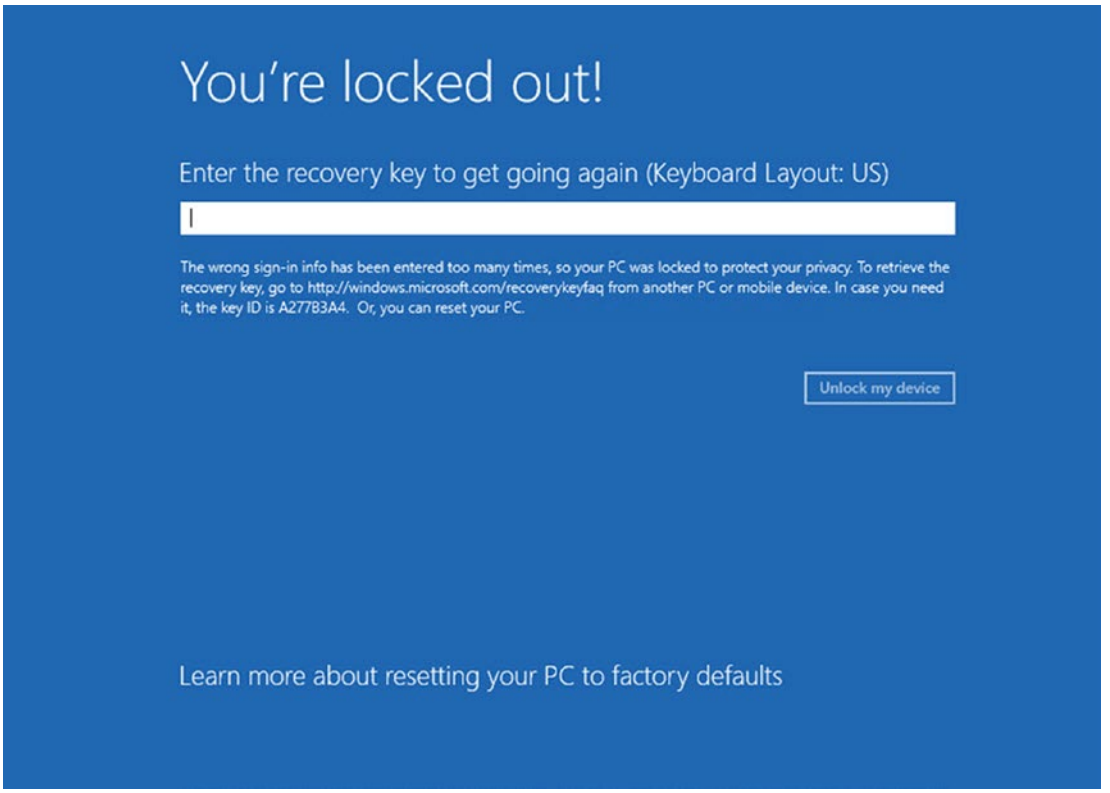


Figure 11-28. *You find yourself locked out of your PC by Bitlocker*

I strongly recommend that when you encrypt a drive with Bitlocker, you tell Bitlocker to save a copy of the unlock key to your Microsoft account, as then you can save the bookmark *https://onedrive.live.com/recoverykey* to your smartphone or another device. From this website you will be able to see your Bitlocker recovery keys, so you can enter them on your PC.

Troubleshooting Touchscreen Problems

If a touch screen isn't working on your device, then it will certainly be the driver that's either missing or corrupt. On a tablet or touchscreen laptop device, this can be extremely annoying, but there are a couple of things you can do in advance, just to make sure you're okay should this happen.

Having a Bluetooth keyboard and mouse that you can use with the tablet is a very good idea; obviously laptops have their own inbuilt keyboard. However, you may not want to purchase Bluetooth, as you might have a USB-wired keyboard and mouse that you can use instead. Tablets don't tend to come with full-size USB ports, however, usually shipping with either Micro-USB or USB Type-C ports. If this is the case, it can be extremely wise, especially should you need to reinstall Windows, to purchase a USB on-the-go (USB OTG) cable. This is a USB extender cable that will plug into your Micro-USB or USB Type-C port, and it has one or more standard USB ports at its other end. I will show you how to troubleshoot hardware drivers in Chapter 15.

I once dealt with a neighbor's all-in-one touchscreen desktop PC where the interface was going completely haywire. It transpired that the touch screen itself had developed a fault, and was recording input all over the place. This obviously made the PC unusable with things seemingly opening and clicking on their own. The solution here was to restart the PC into Safe Mode and disabling the touchscreen driver. You can access Safe Mode by booting to the recovery options menu from a Recovery Drive or Shift-Restart and selecting *Troubleshoot* ➤ *Advanced Options* ➤ *Start-up Settings* ➤ *Restart* and then selecting *4) Safe Mode* from the menu that appears. This restarted the PC without the touch screen being active.

USB Type-C and Thunderbolt Problems

Similarly as with touch screens, any problem you encounter with USB Type-C and Thunderbolt devices not working is likely to be a hardware driver problem. Check in the Device Manager to see if there are any "unidentified" or "uninstalled" devices. I will show you how to manage device drivers in Chapter 15.

No Picture on Desktop PC Monitor or TV

Sometimes, especially after cleaning, moving, or updating a desktop PC, you might suddenly find that you have no picture on your monitor. However, this can also extend to media or gaming PCs that you have plugged into a TV via HDMI or DisplayPort.

Regarding standard PC monitors on business PCs, the most common cause is that whoever has been cleaning or moving a PC has plugged the monitor into the wrong video socket, perhaps the one on the motherboard back panel when a graphics card is installed. The cause also could have been a BIOS update, however. On older PCs, a BIOS

reset can set the default video output to the motherboard when your monitor is plugged into a PCIe graphics card. To rectify this, you will need to plug your monitor into the motherboard graphics output (you might need a cable adapter for this and it's useful to have one in your toolkit) and change the BIOS setting back.

Situations where TVs and even some monitors have no picture after a PC resumes from sleep are actually very common, and you should check for an updated graphics driver. It's caused by the HDMI or DisplayPort system going into a low-power state during sleep and not waking properly. Unplugging the video cable from the TV and plugging it back in will refresh the connection.

If a PC has been moved or cleaned, it is also possible that the video cable has been plugged into the wrong socket on the back of the display. This is increasingly common in an age where our monitors can come with two or three HDMI or DisplayPort sockets.

Disappearing and Conflicting Drives

You might already have encountered this already as it's not that uncommon. You plug a USB Flash Drive into your PC, and it doesn't appear in File Manager. Alternatively, you have a backup set to run periodically to an external hard disk, but one day the drive suddenly disappears from Windows, even though it's plugged in and switched on.

This is caused either when a drive is plugged into the computer and not correctly identified by the OS or when Windows tries to assign a driver letter that's already in use by another drive. In both cases the new drive will be present, but won't have a drive letter (C:, etc.), so you can't see it in File Explorer.

To fix this, open *Disk Management* from the Win+X menu, and look for the disk in the window that appears (it's usually somewhere near the bottom). Right-click the drive, and select Change drive letter and paths from the menu that appears. A dialog will appear that will let you add or change the drive letter (see Figure 11-29), after which the drive will appear in File Explorer.

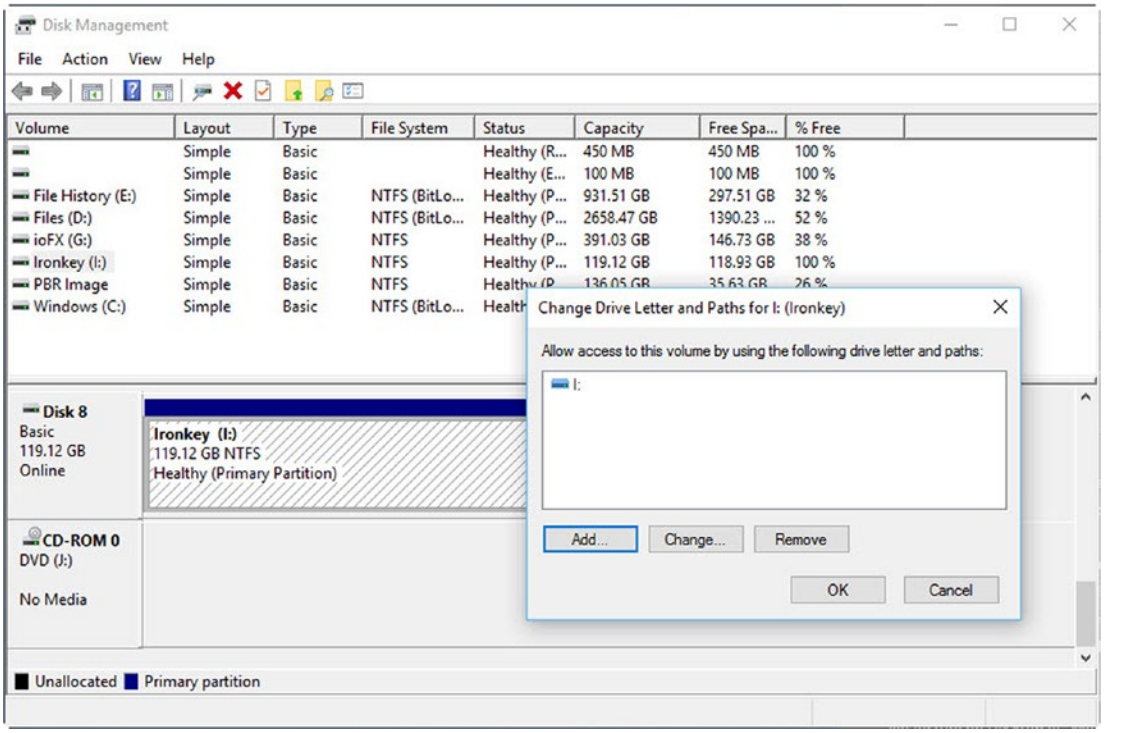


Figure 11-29. *You can assign and reassign driver letters for drivers that require it*

Understanding the BSOD

Microsoft watchers and IT pros may still refer to Windows 10's critical stop screen as the BSOD, but I prefer these days to call it the "Blue Unhappy Emoticon of Death" because of the change it underwent in Windows 8. This change, if I'm honest, wasn't an improvement as the legacy BSOD provided far more information for the user than the new one does. But, you have to live with what life gives you!

While the legacy BSOD gave you useful information such as the name of the file or driver that had caused the crash, Windows 10's BSOD only gives you an error description. You can find this in the bottom right of the BSOD (see Figure 11-30), where the error is HAL_INITIALIZATION_FAILED.

You can search online for the error, or if the PC has told you it's been collecting information as in the example in Figure 11-30, you will be able to find this in a .dmp memory dump file. Windows stores these in the `\Windows` folder as MEMORY.DMP. If you can't find a file when you get back to the desktop, open *System* from the Control

Panel, then click *Advanced System Settings,* and in the dialog that appears, click the *Advanced* tab and the *Settings* button in the Start-up and Recovery section. Additionally, Blue Screens in Windows 10 include a QR code which, if you can open a scanning app on your phone or tablet quickly enough, you can scan to take you directly to a Microsoft support page, related to that error. I say quickly enough, because the blue screen will only remain visible for around 30 seconds before your PC restarts.

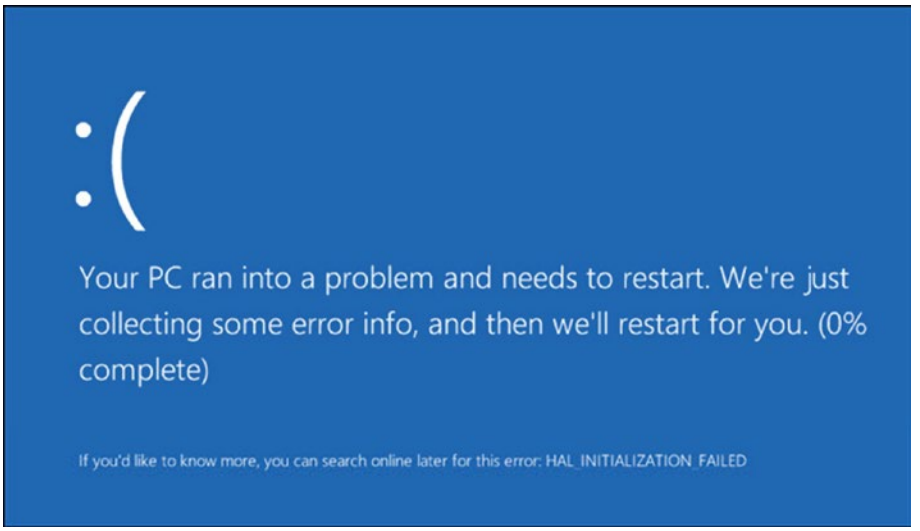


Figure 11-30. *The error description appears in the bottom right of the BSOD*

In the dialog that appears, you will see options to control Blue Screens, including the dump file name and location, and if the PC should automatically restart after a Blue Screen; see Figure 11-31. You can disable the automatic restart here if you want time to read the error name on the BSOD, but automatic restart (sometimes known as the perpetual restart, as it happens over and over) can also be disabled from the Windows recovery options, as I detailed in Chapter 8.

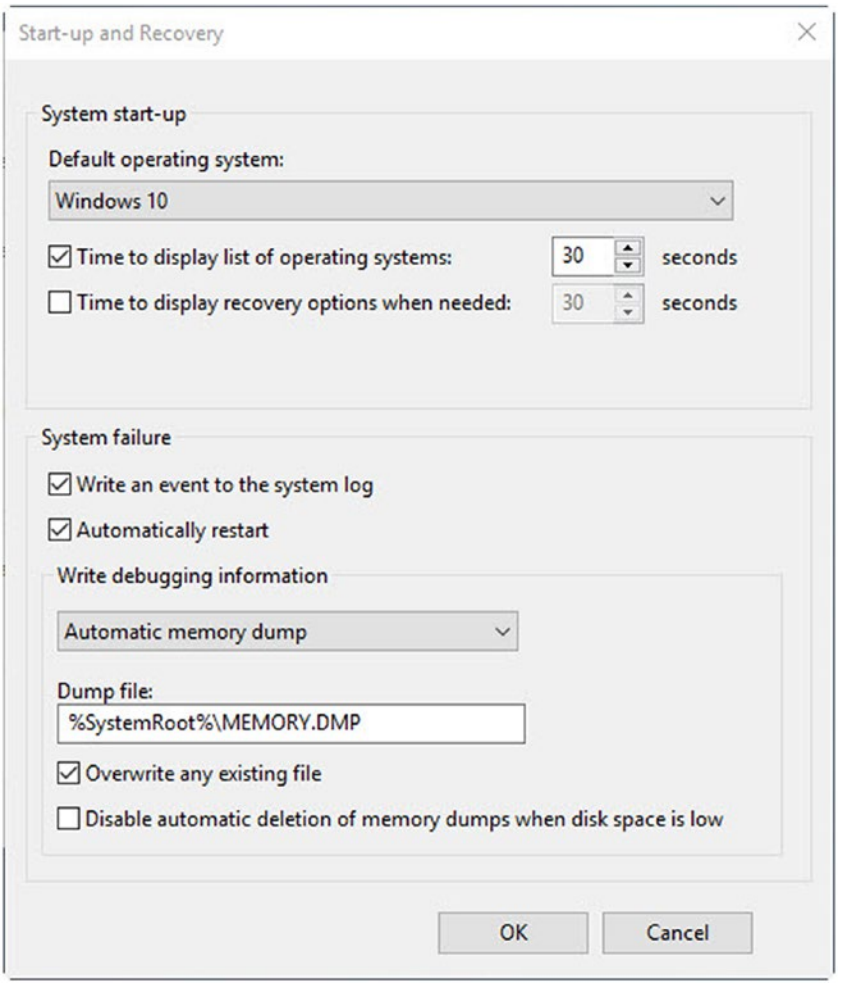


Figure 11-31. *You can find the default location for the BSOD error log in the System options*

The question now is: How do you open and read a .dmp memory dump file? There's no way to easily read this in Windows 10, and you'll need compatible software such as Microsoft Visual Studio to open and read its contents. For this, I recommend a free utility called BlueScreenView, available from `www.nirsoft.net/utils/blue_screen_view.html`, which will help you find and read BSOD files on your PC.

Reading the MEMORY.DMP file can reveal further information about the cause of the crash. In Figure 11-32 you can see a dump file opened using BlueScreenView, which also details the error code, **0x000000ef** in this case. Searching for error codes online can often reveal much more helpful information than just searching for the error name.

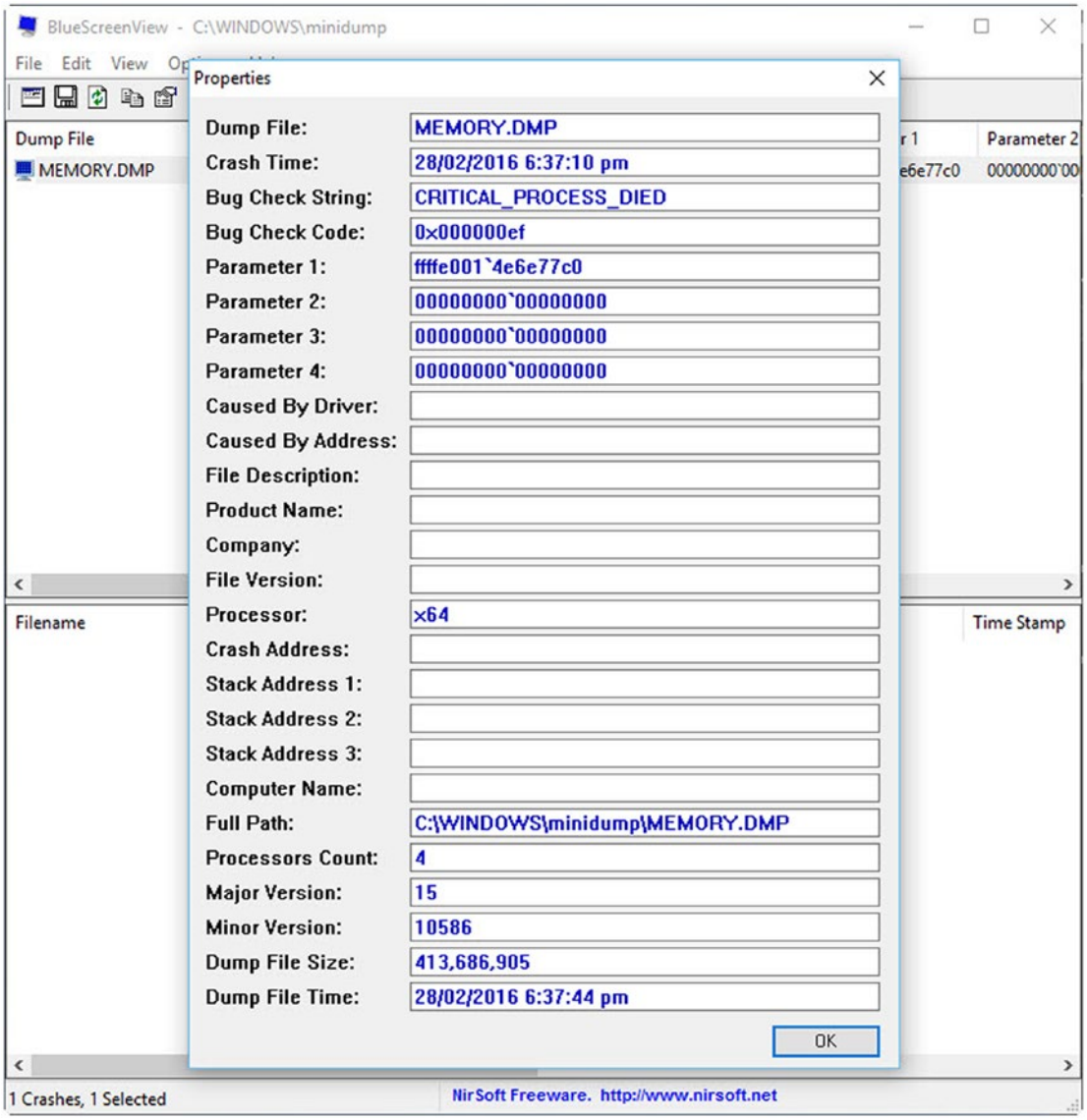


Figure 11-32. *MEMORY.DMP files contain more information about crashes*

Summary

Windows 10 is not a perfect operating system. Since its release it has included bugs and idiosyncrasies the same as any other OS. While some of these are admittedly Microsoft's fault, it's astonishing to me sometimes how stable, secure, and robust the operating system is, given the almost infinite combinations of software and hardware available for PCs.

While problems such as those listed in this chapter are straightforward to fix, sometimes you're just nowhere near the PC you need to support. In the next chapter, then, we'll examine all the remote support options for PCs, including some little gems of tools you may never have heard of.

CHAPTER 12

Remote Help and Support

One of the biggest challenges in either providing or receiving IT support is that of distance. Long gone are the days when 90% or more of all PCs sold were hulking-great desktops. Now, desktops are still prevalent in offices where workers are static, and for PC gamers at home, but for everybody else the move to laptops and tablets is well established.

The pandemic of 2020 changed things further still, with huge percentages of the workforce staying at home, and a great many reluctant to return to the office full time afterward. These people are using a variety of computers to access the company's systems, from corporate-provided laptops to their own home PC.

One of the challenges with mobile PCs however, even ones that are intended for use at the office most of the time, is that you can pretty much guarantee they'll be away from the home or office when they need support. Something will go wrong on the train, or in the airport lounge, or at a remote or a customer's office, or when the user is on their vacation (though in the last instance they'll likely have the sense to enjoy whatever they went there for and leave the PC until they return home). On top of this is the possibility that you will be required to provide urgent support when you're away or out and about.

Partly, this "Murphy's law" guarantee of problem occurrence is down to the fact that when we're on the move, we don't have access to the quick fixes you get when back at base. There's often no good Internet connection for downloading a driver, or a copy of a backup installer on a network share. When it comes to something occurring such as a Bitlocker encryption lockout, which I mentioned in the previous chapter, you can't always quickly refer to another PC and find the code you need.

The rest of the problem lies in how people like to work and use their PCs in the 21st century. We enjoy being able to type up notes for a meeting while sit on the train, just an hour before it starts. We like being able to sling our PC into a bag and work on a dissertation in the sunshine of a pub garden.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_12

But if you need to support these people, how can you do so? Well, there are two options, the first of which is with tools the user can use themselves, which is extremely helpful in a place where there is little, no, or patchy Internet coverage. The other tools are remote access and control utilities to help you use the remote PC as if it were sat in front of you on your desk… almost.

The Problem Steps Recorder

One of Windows' best hidden gems is the Problem Steps Recorder, launched by searching for **psr** at the Start Menu, where *Steps Recorder* (Desktop app) will appear as a search result. This is a screen recording and annotation tool that was initially included with the Windows 7 beta builds, to help testers record bugs and problems with the OS. It was so incredibly popular, however, that Microsoft agreed to keep it in the final build, and it remains in Windows to this day.

The Problem Steps Recorder opens as a toolbar with just four controls; see Figure 12-1. This makes it suitable for use by end users who might have no or only limited technical knowledge.

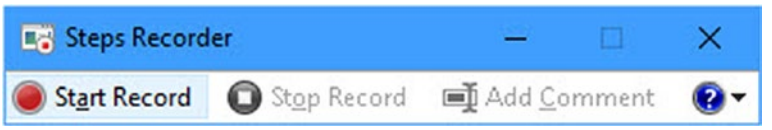


Figure 12-1. *The Problem Steps Recorder toolbar*

When you want to record a problem on a PC, just click the *Start Record* button, which will then change to a *Pause Record* button. This can be useful if you want to omit certain steps from the recording, perhaps because they're not relevant, or perhaps because recording them will contravene a company security or privacy policy. Additionally, an *Add Comment* button (see Figure 12-2) will pause the current recording and present a text box in which a comment can be typed.

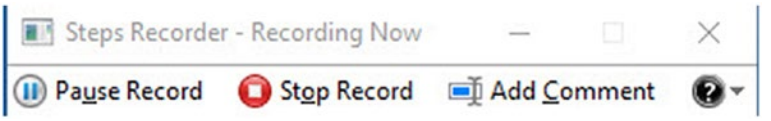


Figure 12-2. *Pause Record and Add Comment buttons appear when you are recording your screen*

When the recording is finished, click the *Stop Record* button, and the toolbar will change to a full window containing the output from your recording session. At the top of this is a save button (see Figure 12-3) that will prompt you to save the recording as a ZIP file, which can then be sent to yourself or another support person for examination.

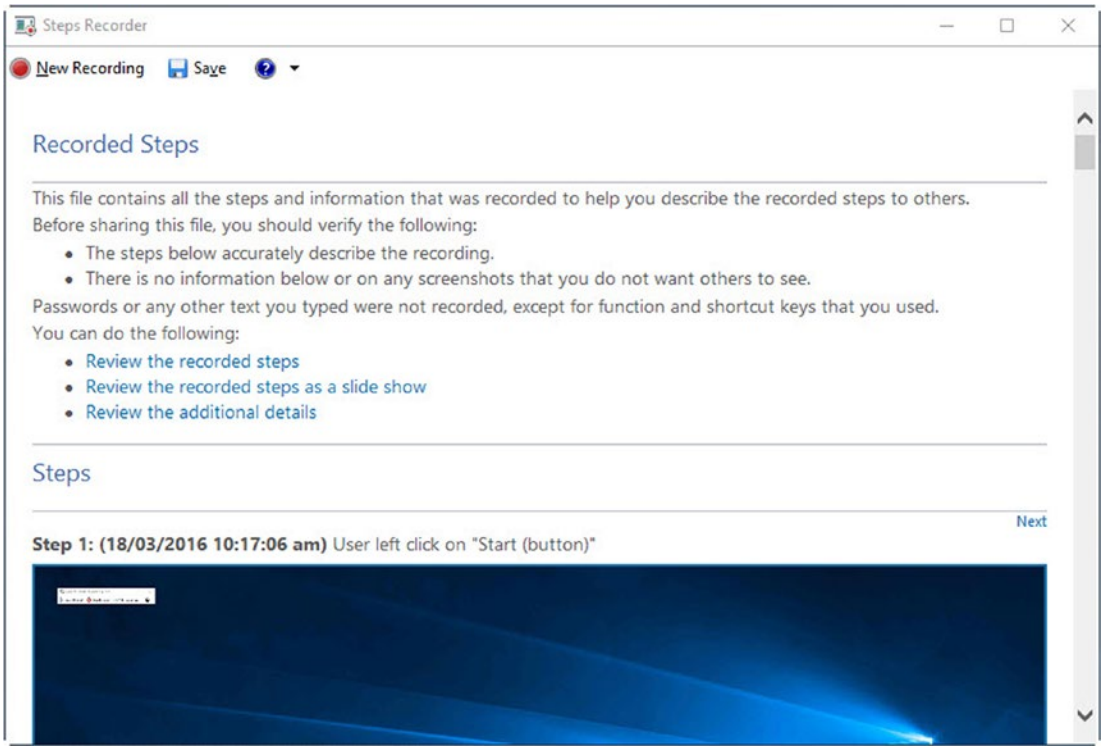


Figure 12-3. *When you stop recording, you have an option to save the output file*

This ZIP file contains an HTML document that will open in a web browser and be formatted as you see in Figure 12-3. It's split into different sections. The first section shows a series of annotated screenshots, with the item onscreen that the user has clicked, or that is in focus, highlighted with a green border; see Figure 12-4. This helps you follow the "narrative" of what's going on, and check what's being clicked, activated, and so on. Above each screenshot is a plain text description of what has happened.

Tip The screenshots can appear very small, especially if the screen being recorded is of a very high resolution, such as the 4K screen seen in Figure 12-4. You can enlarge each screenshot by clicking it.

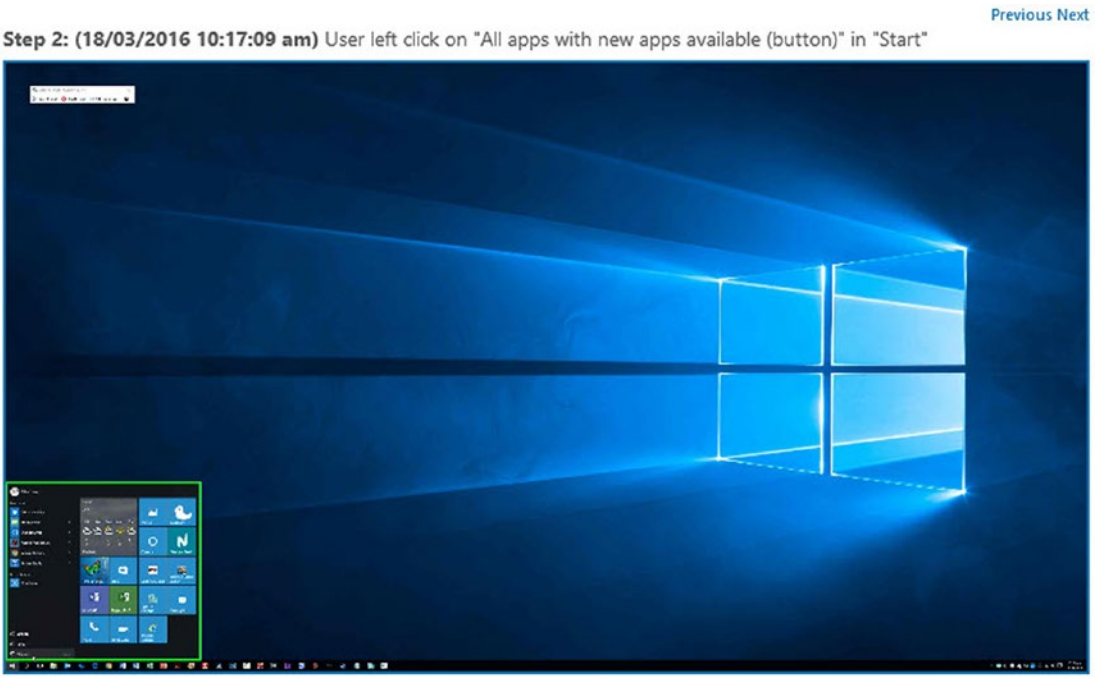


Figure 12-4. *Each screenshot is annotated to show what the user is doing*

Where the user has written a comment the screenshot will be grayed, and the comment will appear in double quotes above it; see Figure 12-5.

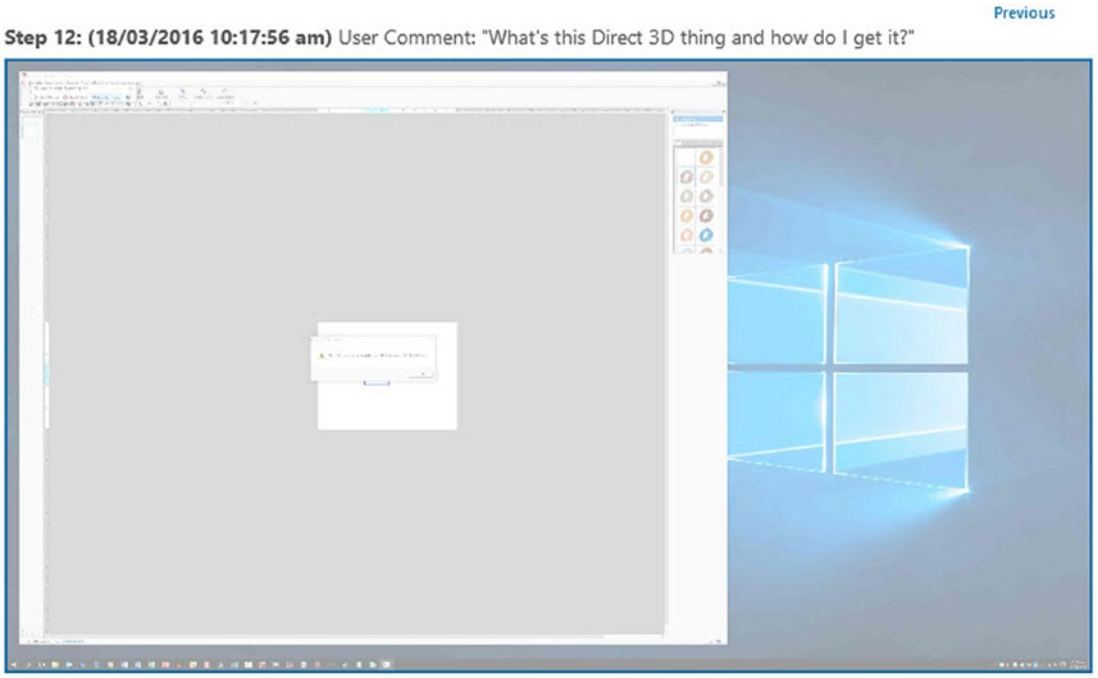


Figure 12-5. *Screenshots where a comment have been typed are grayed out*

At the bottom of the document are technical details; see Figure 12-6. These include the text descriptions from each screenshot, with details of apps, services, or other OS features used, complete with version numbers (which can be incredibly useful when diagnosing problems). The current version number of their copy of Windows 10 is also included, so you can check if an update might be available to help solve the problem.

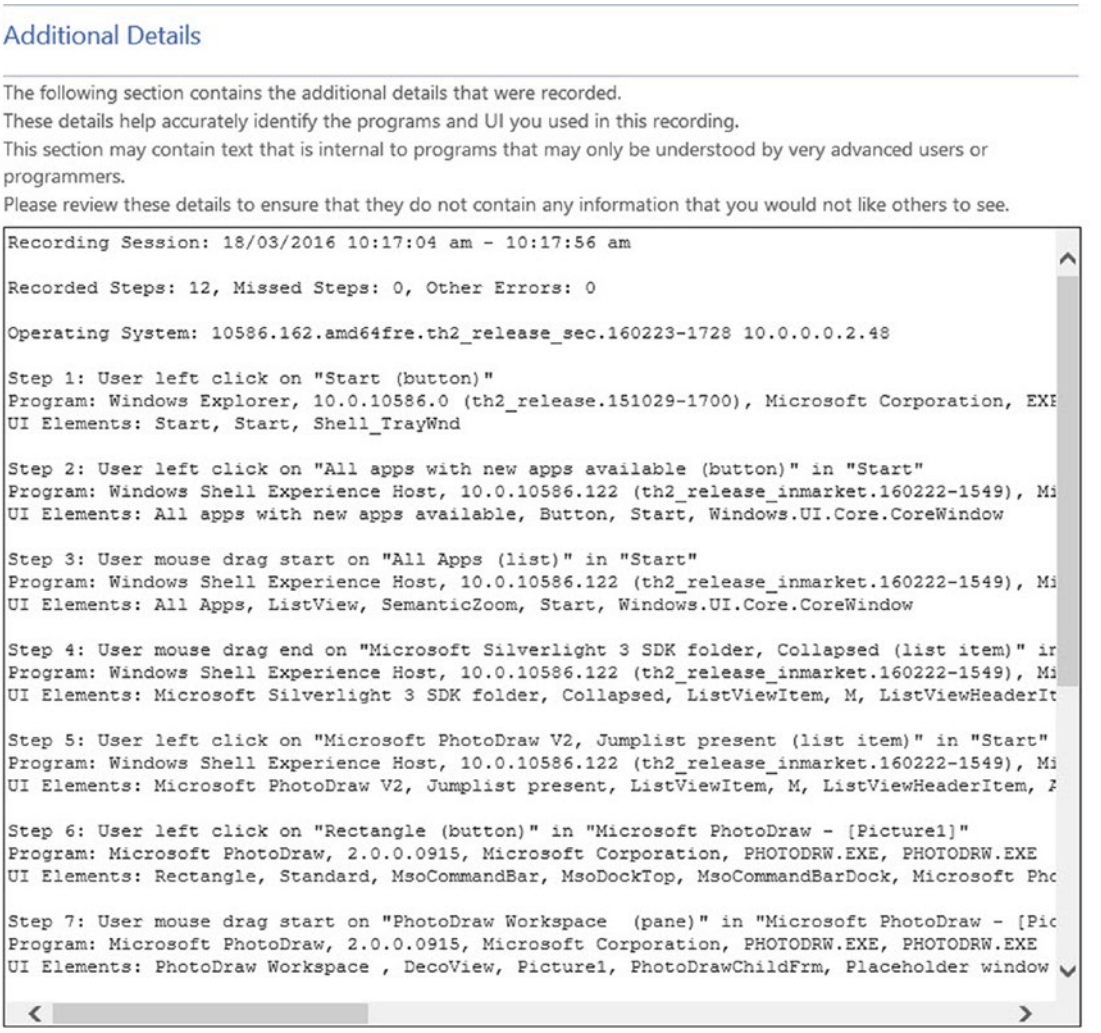


Figure 12-6. *Technical details can be found at the bottom of the document*

Recording an App with Game Bar

While the Problem Steps Recorder is an incredibly useful tool that provides an output file that can easily be emailed to a support person, sometimes annotated screenshots don't provide all the information you need. This is when one of Windows 10's Xbox gaming features can prove useful (and I'll bet you didn't see that one coming).

Note The Game Bar feature is available in both the Home and Pro editions of Windows 10, but may be disabled in Windows 10 Enterprise.

Game Bar is opened by pressing the *Windows key* + *G*, and the user will probably have to confirm that the currently running app is a game. It opens as a series of toolbars, with one called *Capture* that's similar to the Problem Steps Recorder; see Figure 12-7. However, Game Bar is locked to a single app and won't record anything outside of that app, so the user should be using an offending app before she launches Game Bar, and this also means it's no good for general recording of the desktop as it can't be used to record the desktop.

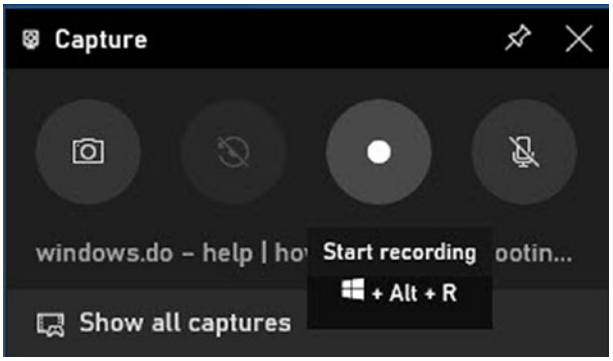


Figure 12-7. *Game Bar can record video*

At the top center of your screen, you will see a main control panel, on the right of which sits a settings icon that includes General, Shortcuts, and other options. The Shortcuts options offer an at-a-glance view of the keyboard commands you use to control recordings with Game Bar; see Figure 12-8.

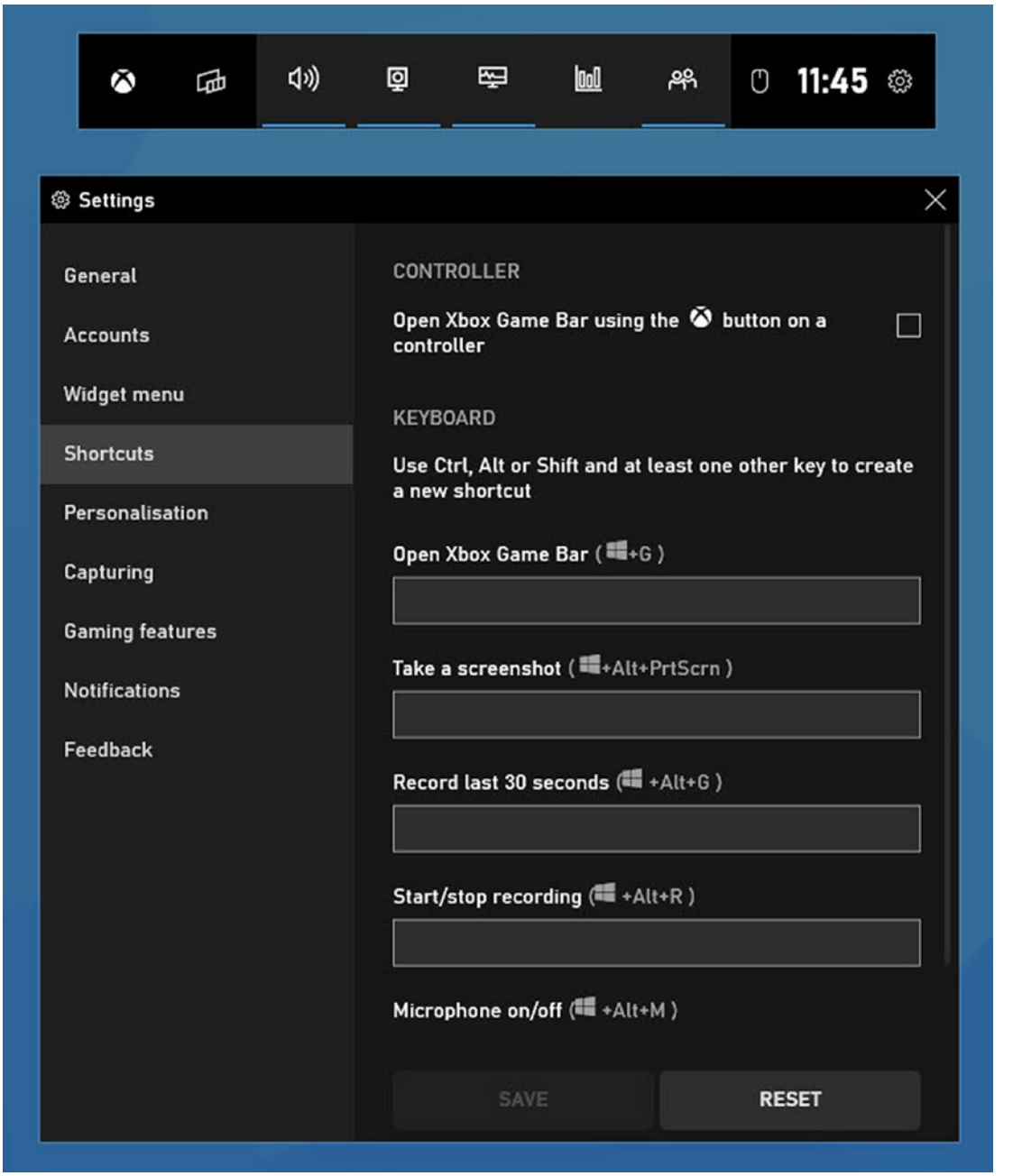


Figure 12-8. *Game Bar settings include details of its control shortcut keys*

When you are recording an app with Game Bar, it will be minimized to the top right of the app window (see Figure 12-9) to indicate that recording is taking place. You can stop a recording by pressing the *Win* + *Alt* + *R* key combination, or by opening the Game Bar again by pressing *Win* + *G*.

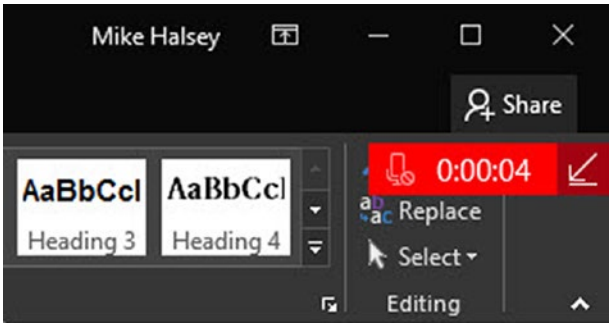


Figure 12-9. *Game Bar signifies it's recording in the top right corner of the app*

When you stop a recording, it will be automatically saved as an MP4 video to the *User folders* ➤ *Videos* ➤ *Captures* folder.

Quick Assist

If you sign into your PC using a Microsoft Account, and if both yourself and the person to whom you are providing support are using Windows 10, then a feature called *Quick Assist* can make the task of providing remote support extremely easy, both for yourself and the recipient. You will find Quick Assist in the Start Menu, and you should tell the person to whom you will be providing support to look for it too.

When you Start Quick Assist, you will be asked if you want to *Get assistance*, or *Give assistance*; see Figure 12-10. Clicking *Give assistance* will prompt you to sign in with your Microsoft Account, as this support app uses a Microsoft peer-to-peer system to connect the two PCs.

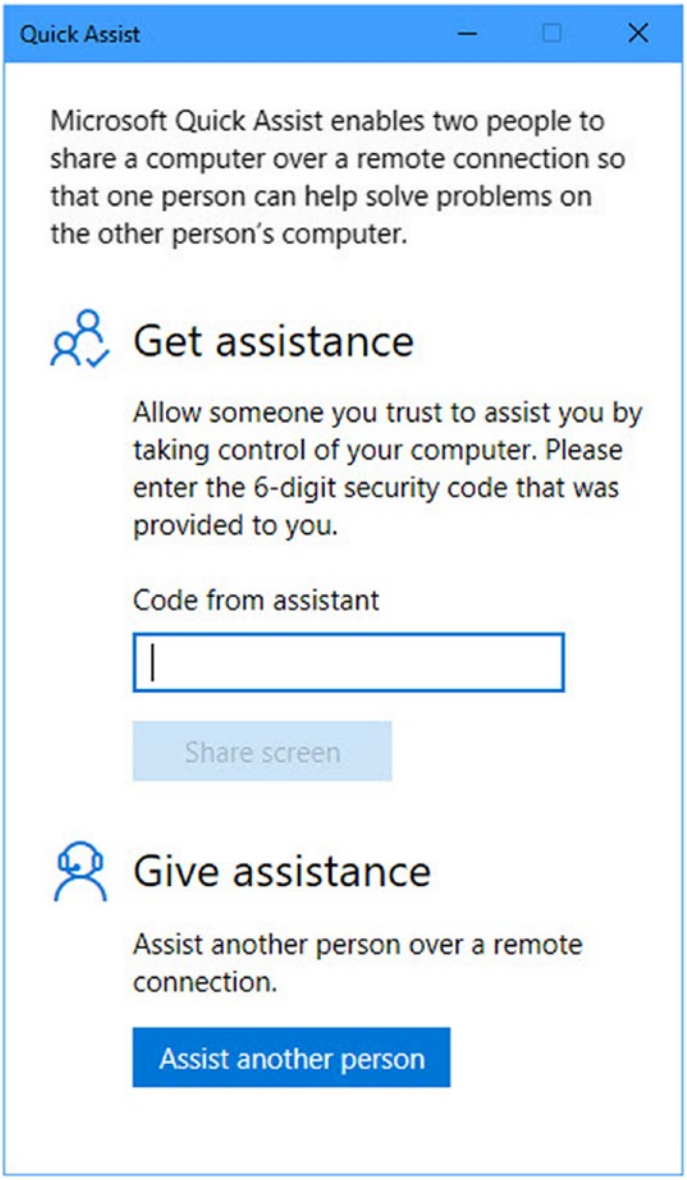


Figure 12-10. *You can give assistance to people who are also running Windows 10*

When you have verified your account, you will be given a six-digit security code that must be typed into the PC where assistance is required; see Figure 12-11. The code expires in 10 minutes, and you are given quick links to copy the code to your clipboard, so it can be pasted into an instant message or email, or sent directly via email (you will need an installed and configured mail app for this to work). The *Provide instructions* link will tell you where to point the user receiving support, so they can also open Quick Assist.

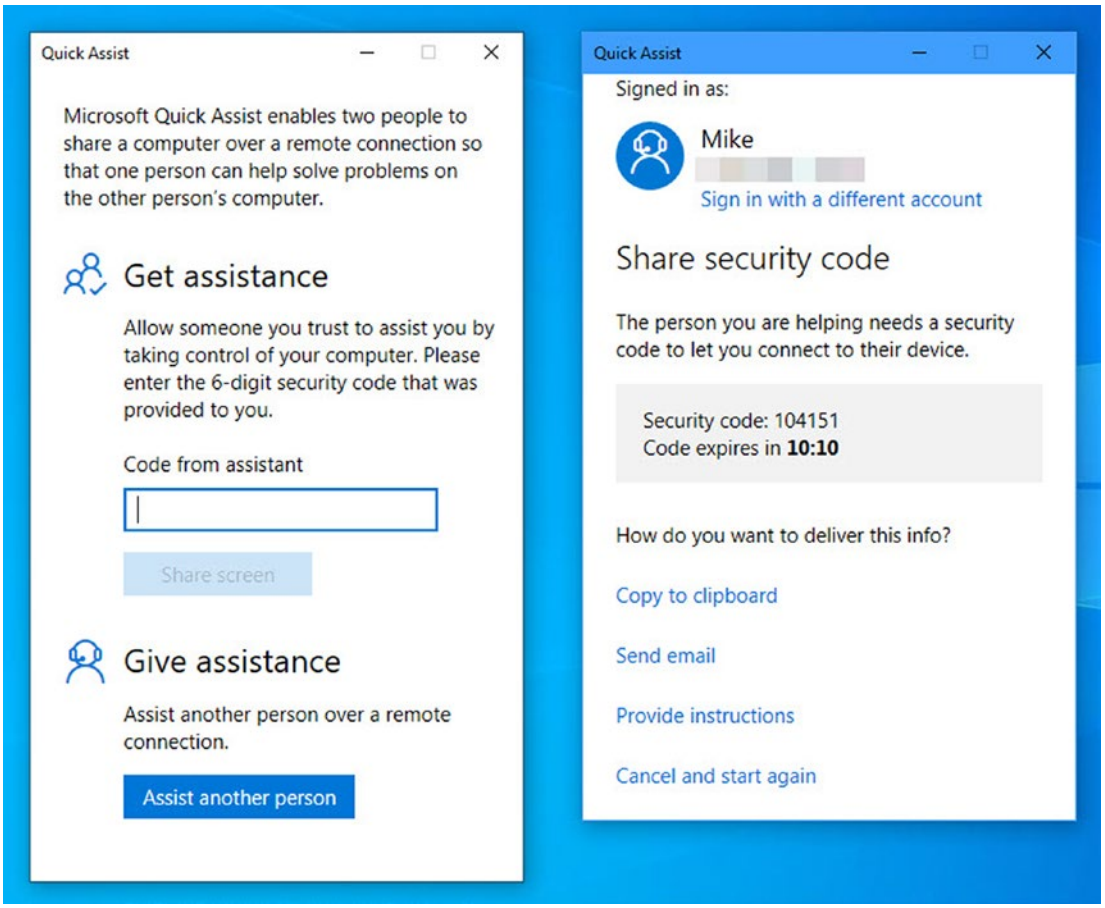


Figure 12-11. *A security code must be typed into the Quick Assist app on the PC receiving support*

Once the code has been entered, the user receiving support will be told that you will be taking control of their PC, and for their permission for this to happen; see Figure 12-12.

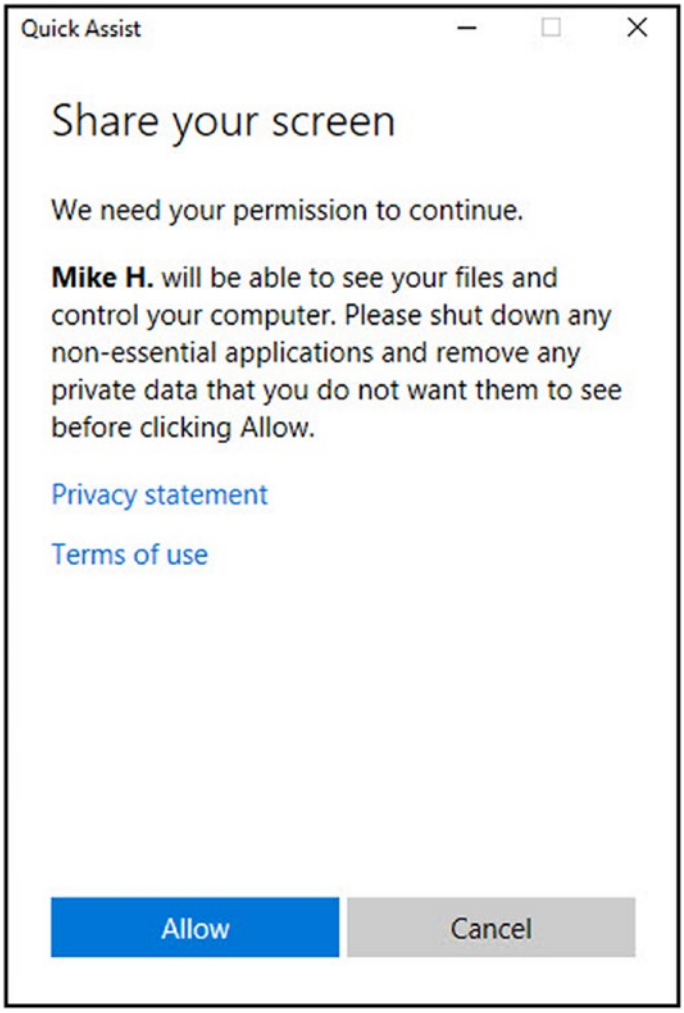


Figure 12-12. *The person receiving support will be asked to confirm you can control their PC*

Once permission has been granted, the main support window will appear, in which you will see the desktop of the remote PC; see Figure 12-13. The controls for the app at this point are very easy to use and intuitive. You can annotate on the screen, perhaps to show the remote user something of which they should be aware. This works because the remote user can see what is happening on their screen at all times.

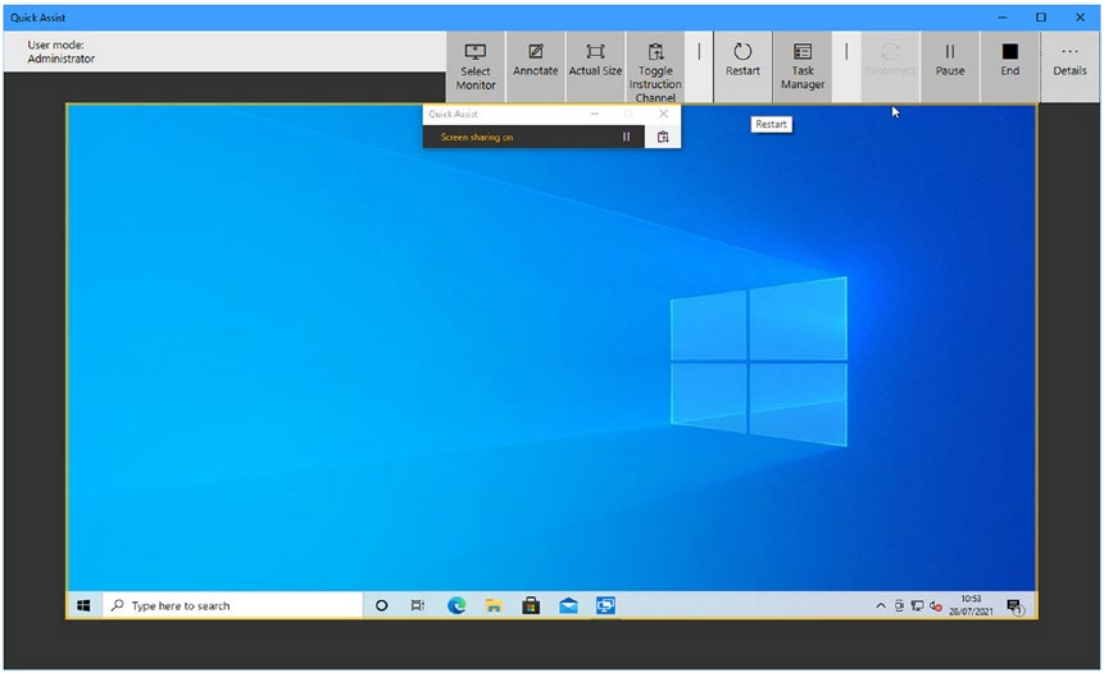


Figure 12-13. *The Quick Assist window is easy to navigate and has simple controls*

Perhaps the most useful feature of the Quick Assist app however is the ability to restart the remote PC. This is a function of Remote Desktop when used in business environments, but the Windows alternative app, Remote Assistance, which I will detail shortly, doesn't offer this functionality. When you have finished providing support to the remote PC, click the *End* button in the top right corner of the window.

Windows Remote Assistance

If you're in a scenario where you can get remote access to a PC but are not using a Microsoft Account, there are two ways to achieve this. In a business environment, you're best of using Remote Desktop, which I'll detail later in this chapter. However, you might be supporting a home user or a small business that doesn't have its own dedicated IT engineer.

There are plenty of third-party remote support packages available, some of which are free to use. TeamViewer, available from `www.teamviewer.com`, is one of the most popular as it's very straightforward for a nontechnical person to use on their PC, but it's also nonintrusive on their system and offers significant functionality for a support technician.

You don't need third-party software, however, to provide remote support to people, as Windows has for many years included its own Remote Assistance feature called, perhaps unsurprisingly, Windows Remote Assistance. You can find it in the Control Panel, but first it is important to establish that Remote Assistance requests are enabled on the PC that requires support.

To achieve this, search for **Remote Assistance** in the Start Menu, and click *Allow Remote Assistance Invitations to be sent from this computer*. This will open a dialog (see Figure 12-14), where a check box is visible in which you can approve, or deny, permission for Remote Assist on the PC.

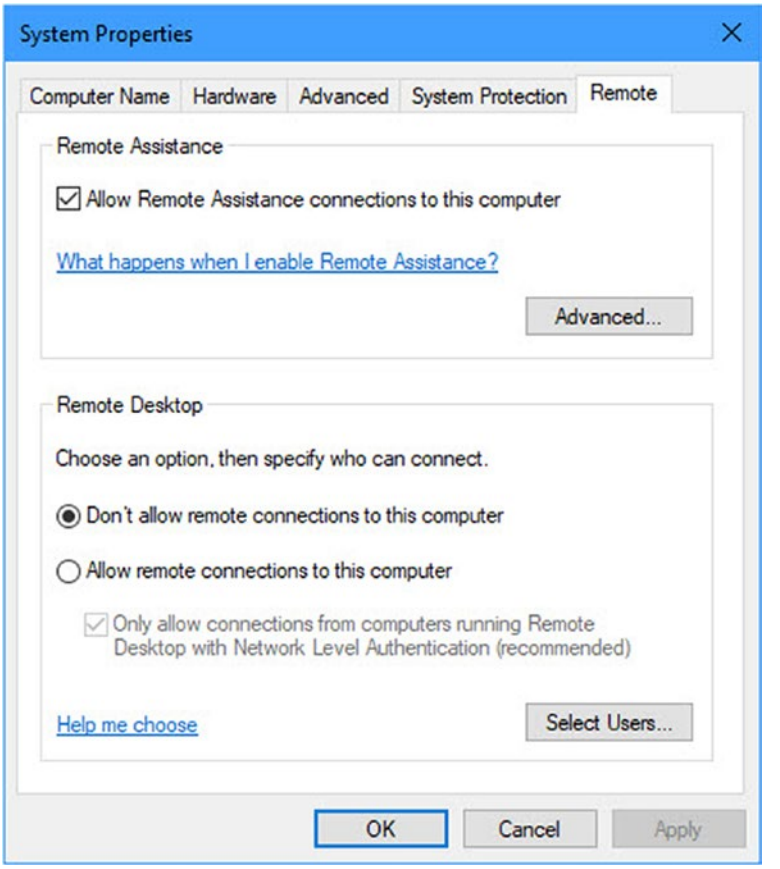


Figure 12-14. *Remote Assistance needs to be activated on the PC requiring support*

You will want the user to make sure the Remote Assistance option is checked. Clicking the *Advanced* button provides additional options you may want the user to check, including whether the PC can be controlled remotely, and how long Remote Assistance invitations remain active; see Figure 12-15.

Note You'll notice this is also the dialog in which Remote Desktop is activated on the PC. We'll be coming back to this later in the chapter.

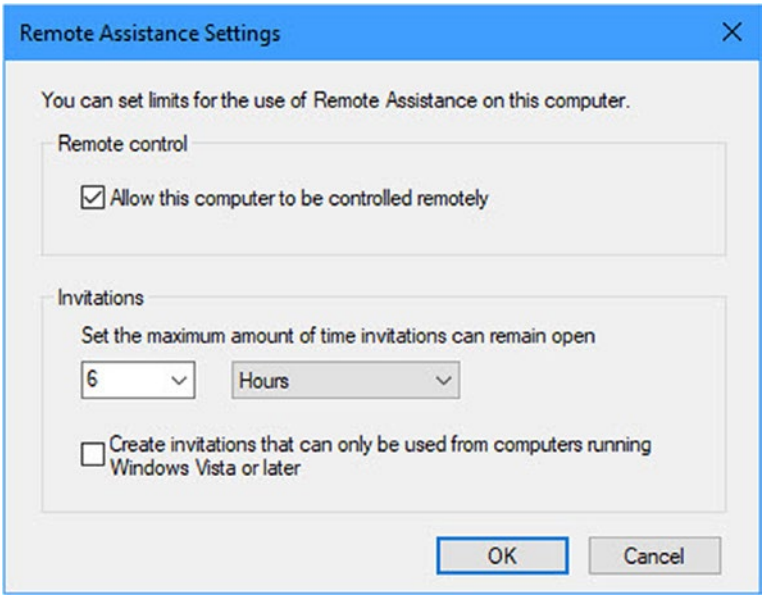


Figure 12-15. *Advanced options are available for Remote Assistance*

Sending and Responding to a Remote Assistance Request

Ironically, at this point, the process of talking a user through instigating a Remote Assistance request isn't as straightforward as searching in the Start Menu for Remote Assistance. They'll need to search instead for **Troubleshooting** and open *Troubleshooting (Control Panel)*. When the Troubleshooting panel opens, you'll need to ask the user to click the *Get help from a friend* link near the top left of the window; see Figure 12-16.

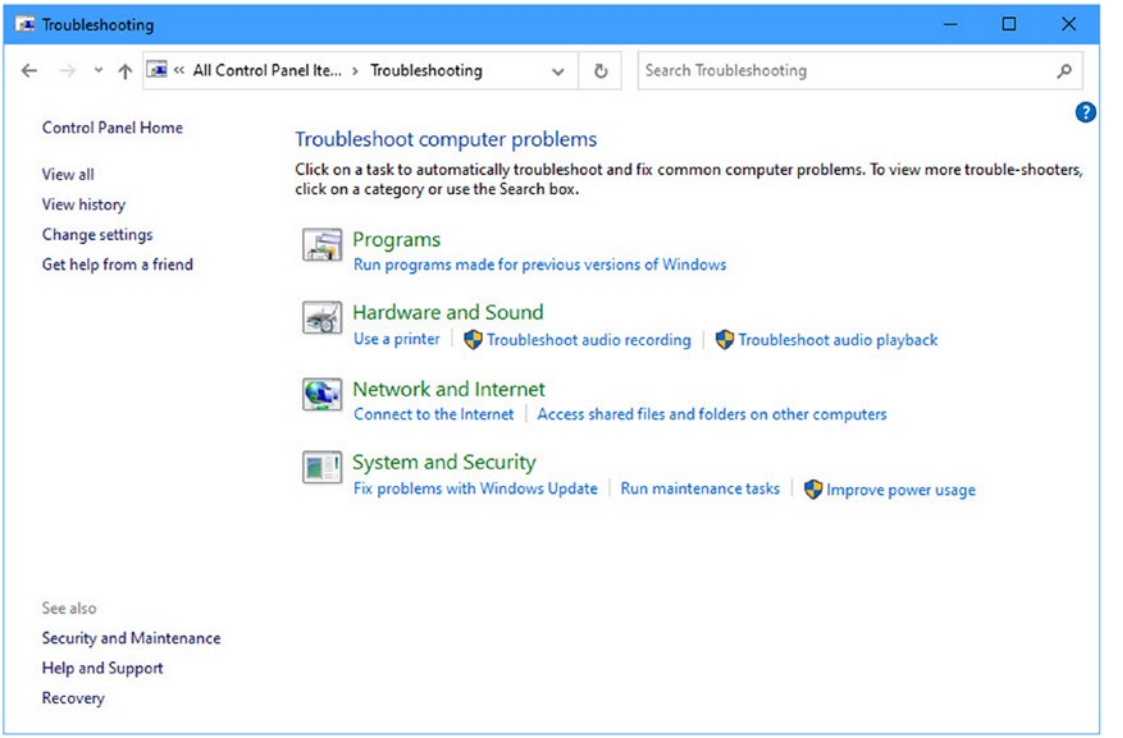


Figure 12-16. *Remote Assistance requests are instigated from the Control Panel*

At the next panel, the user will see an option to "Invite someone to help [them]"; see Figure 12-17. Below this, you'll see an *Offer Remote Assistance to help someone* link, but don't think that you can use this to instigate a Remote Assistance session, as it's quite badly worded and only applicable to connections made over a corporate network, where prior configuration has already been implemented on all PCs.

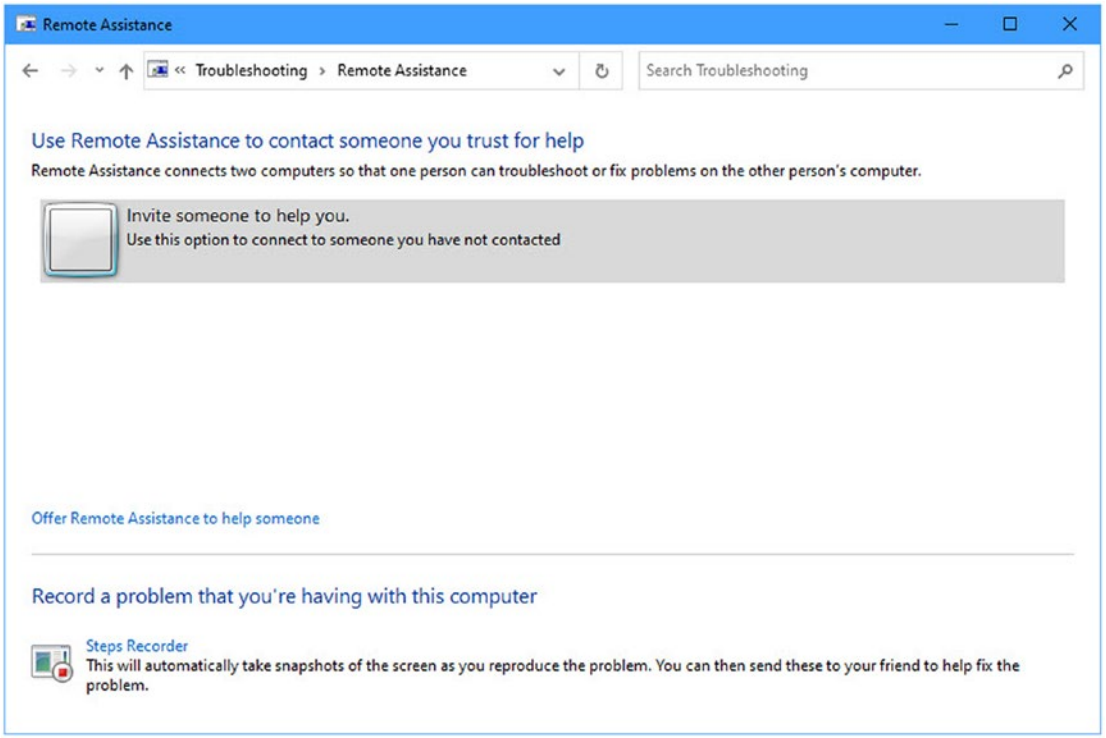


Figure 12-17. *Remote Assistance must be initiated from the PC requiring help*

When the user requiring help clicks the *Invite someone to help you* button, they will be presented with three options for how to send the request: *Send the invitation as a file*, *Use email to send an invitation*, and *Use Easy Connect*; see Figure 12-18.

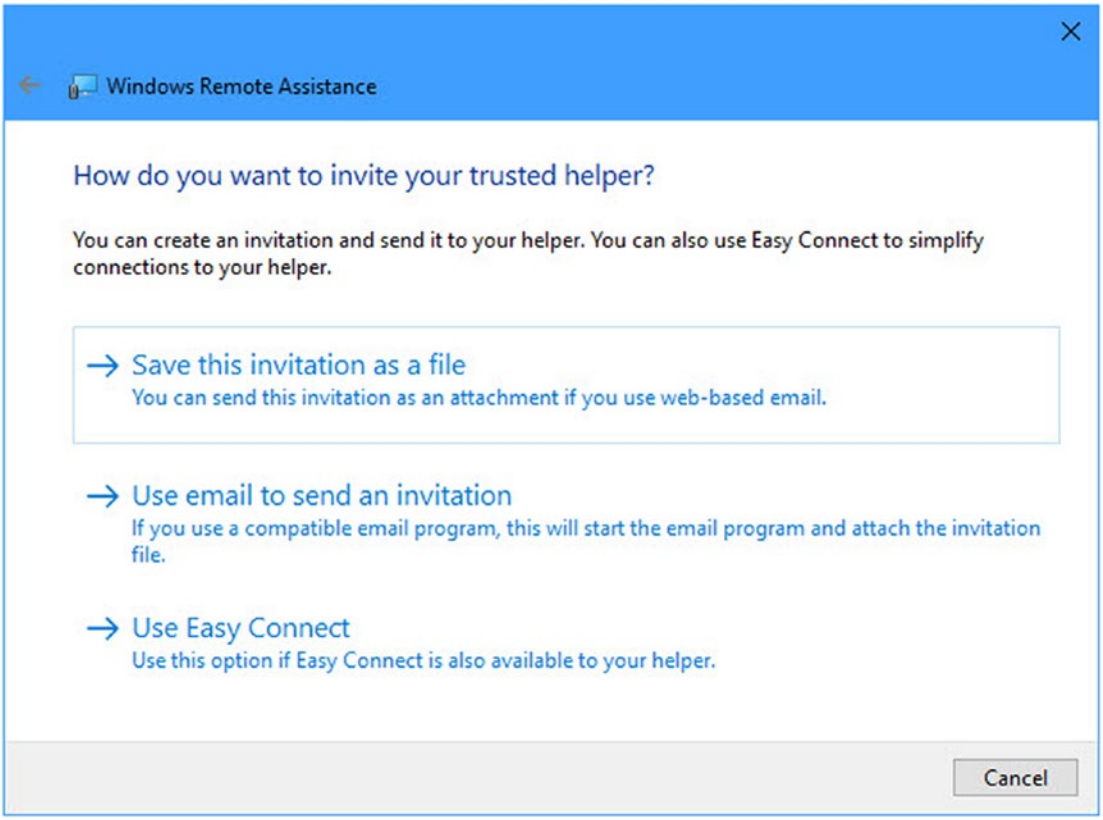


Figure 12-18. *Remote Assistance requests can be sent in three ways*

- **Send this invitation as a file** will save a file to a location of your choice on the PC (the desktop by default). This file can then be attached to an email, and it is best if the user is using either webmail or an email Windows Store app. The reason for this is because the…
- **Use email to send an invitation** option is only available if you are using a Win32 desktop app, such as Outlook as shipped with the full desktop edition of Microsoft Office. It is grayed out for Windows Store apps.

- **Use Easy Connect** is a Microsoft system that uses a peer-to-peer network for securely transmitting a Remote Assistance invitation. Easy Connect might be grayed out and unavailable on the PC for several reasons, one of which being that Windows 10 doesn't feel the available Internet bandwidth is good enough to maintain a connection, but it can also be because the Internet router doesn't support Easy Connect.

Note In order for a router to support Easy Connect, it must support Peer Name Resolution Protocol (PNRP). You may also need to open access to port 3389 on the router. Details of PNRP compatibility and advanced configuration will be available in your router's documentation. Not all routers will support Easy Connect, and it's likely that cheap, ISP-supplied routers will be light on features.

When an invitation is sent, a dialog displaying an access password is displayed onscreen; see Figure 12-19. This password will be required in addition to the invitation file to provide access to the PC.

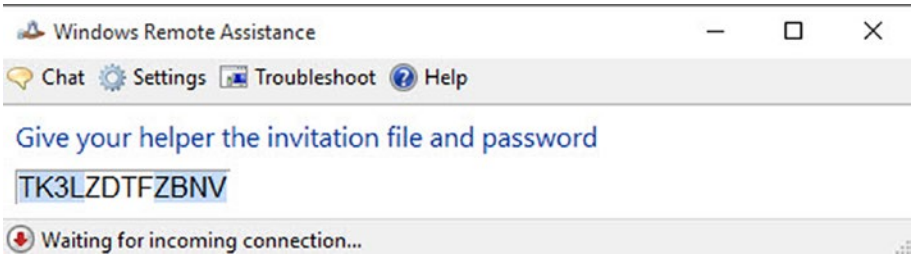


Figure 12-19. *A password is provided for added security*

On the PC providing support, a password dialog will appear when the invitation file is opened; see Figure 12-20. You will probably need to be on the phone to the user at this point so they can tell you the password, but also because you still have to request control of the PC.

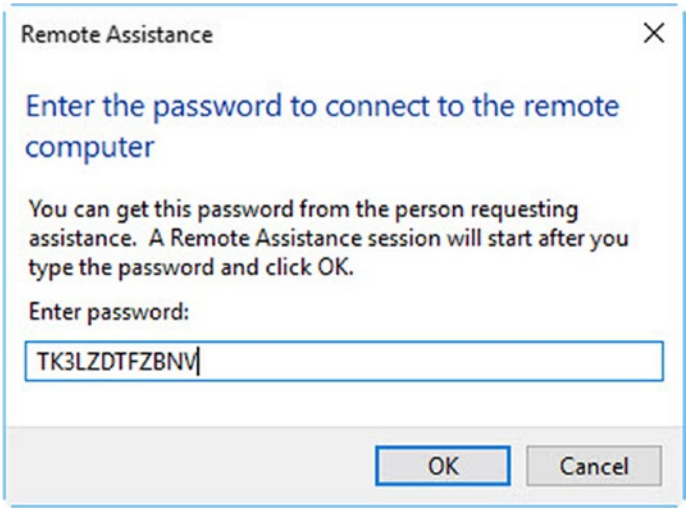


Figure 12-20. *The password needs to be entered on the PC requesting access*

If you are using Easy Connect to provide Remote Assistance, in the *Troubleshooting ➤ Get help from a friend* panel, click the *Offer Remote Assistance to help someone* link, and then click the *Use Easy Connect* option. This will open the password dialog.

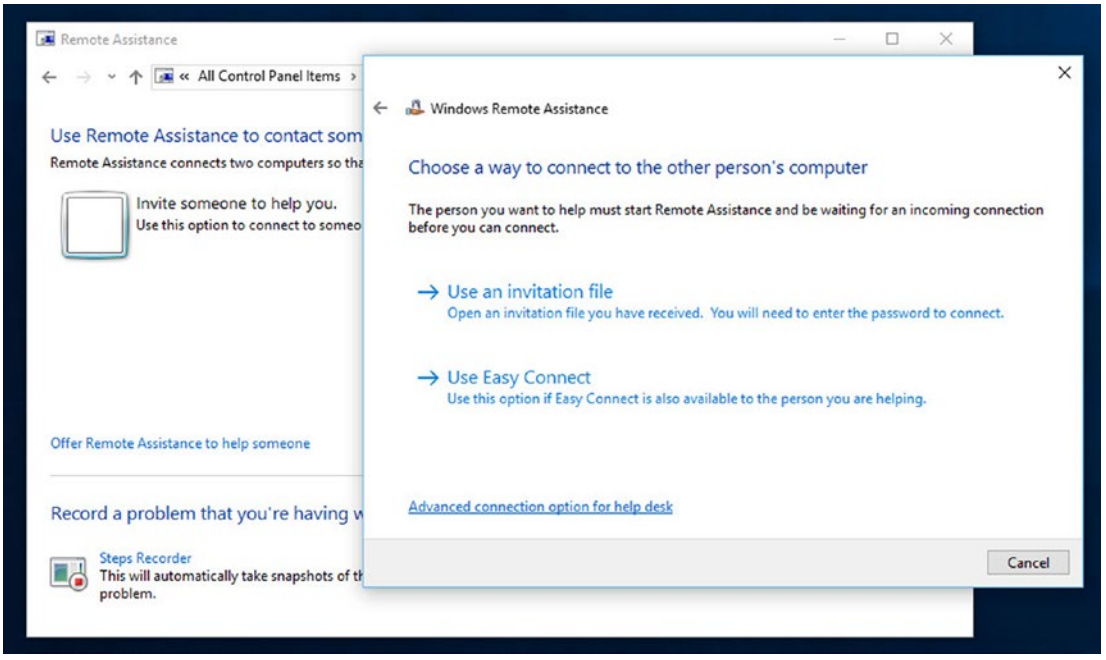


Figure 12-21. *If you are using Easy Connect, you should connect via the Control Panel*

On the screen of the PC requiring help, a dialog will appear asking for permission to initiate the Remote Assistance session; see Figure 12-22. The user on that PC will have to click *Yes* on this dialog before the session can begin.

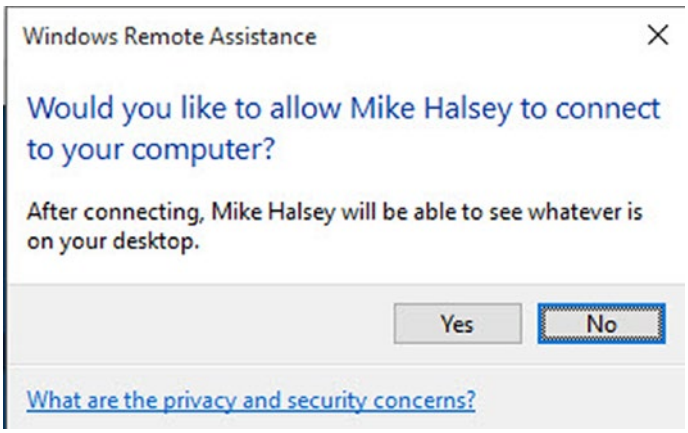


Figure 12-22. *Permission needs to be granted for the Remote Assistance session to begin*

There is one more thing that needs to be done before you can really provide remote support. In the top left of the Remote Assistance window, you will see a *Request control* button; see Figure 12-23.

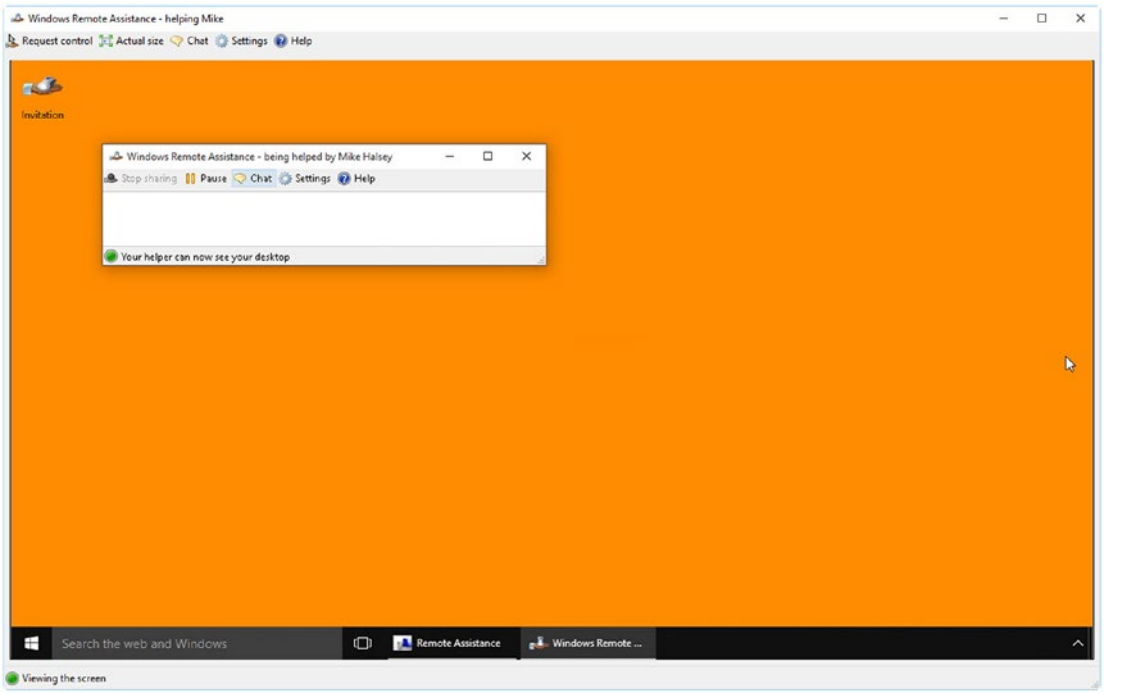


Figure 12-23. *You have to request control of the user's PC*

When you click this, a dialog will appear on the remote PC that only the user of that PC can interact with. This dialog asks for permission for you to share control of their PC; see Figure 12-24.

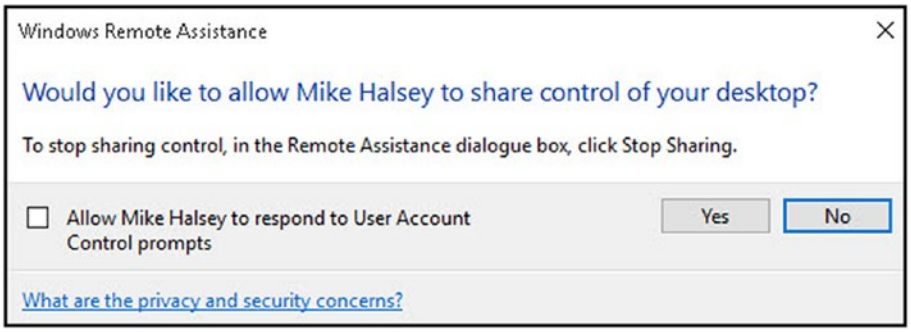


Figure 12-24. *Permission needs to be given for remote control*

It's important to note here that before you ask the user to click *Yes* and give you remote control of their PC, you will probably want them to check the box to *Allow [you] to respond to User Account Control prompts*. If they don't check this dialog, then only they will be able to respond to any UAC prompts that appear during your remote session.

The Remote Assistance dialog on the host PC now changes to present the user on that PC several options, some of which are also available to the person providing support; see Figure 12-25.

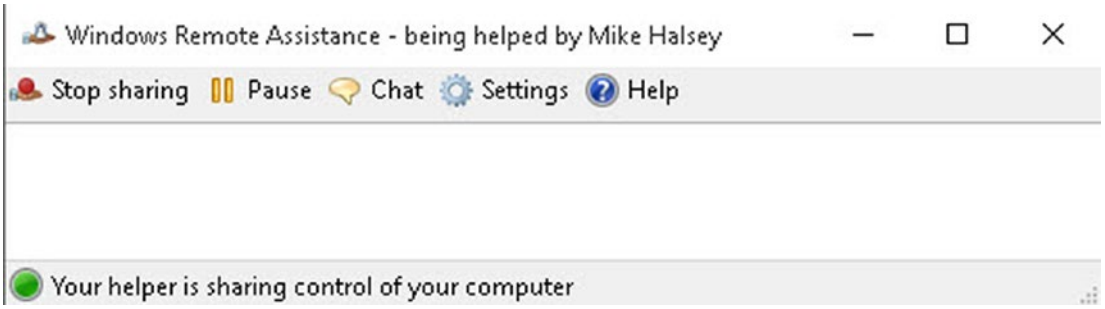


Figure 12-25. *The user of the host PC has various options available*

These include opening a chat window, so you can keep the user informed of what you're doing without needing to keep them on the phone. Settings are also available in which you can change the quality of the connection (see Figure 12-26), and these offer an option for the user receiving support to terminate the connection by just pressing the Esc key on their keyboard should they wish.

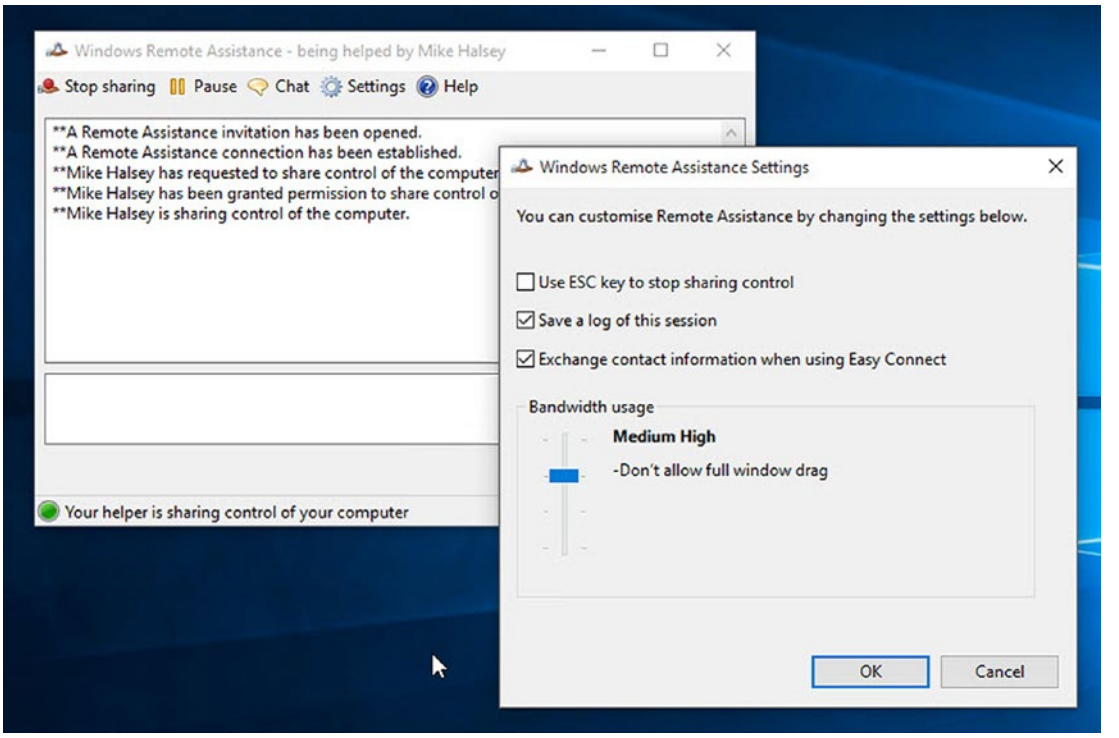


Figure 12-26. *Settings are available for Remote Assistance, as is a chat window*

Sending Unsolicited Remote Assistance Offers

I mentioned earlier in this chapter that you can use Remote Assistance in a company environment without a Remote Assistance invitation needing to be sent. This requires configuration in Group Policy, which you can open by searching for **gpedit** in the Start Menu.

This type of Remote Assistance request is called an unsolicited request, and, as you can imagine for reasons of security, it's disabled in Windows 10 by default. In the Group Policy Editor, navigate to *Computer Configuration* ➤ *Administrative Templates* ➤ *System* ➤ *Remote Assistance,* and double-click the *Configure Offer Remote Assistance* policy. You will need to enable this policy on each machine that you want to receive unsolicited Remote Assistance requests; see Figure 12-27. Available options include being able to automatically control the PC, or just view it.

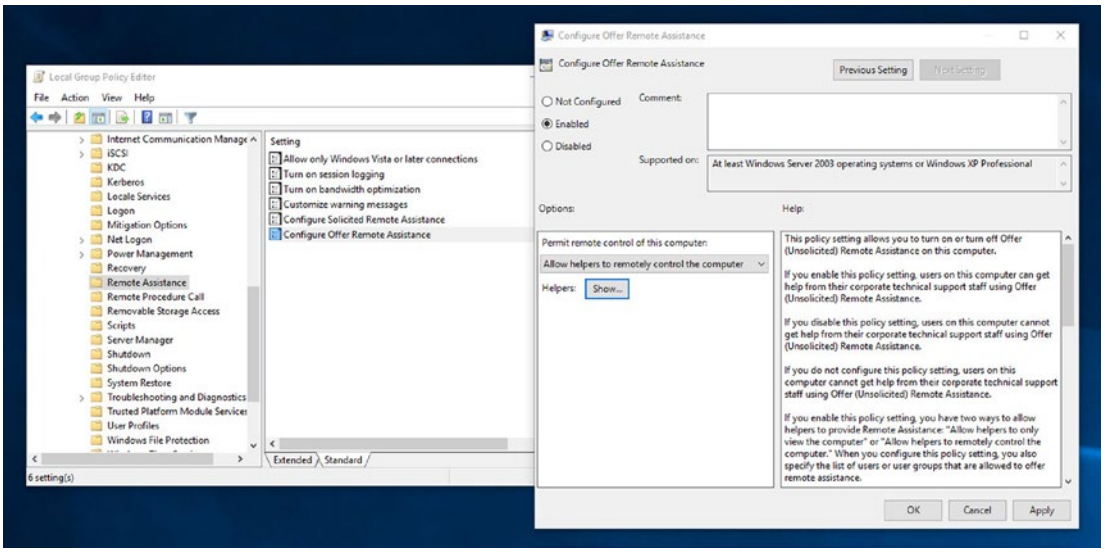


Figure 12-27. *Group Policy needs to be configured to allow unsolicited Remote Assistance*

You then need to configure the "Helpers" who can access the PC. This can be either individual users or user groups, but they must be in the following format: domain_name\username or domain_name\groupname.

In the Windows Advanced Firewall, you need to ensure that the *Remote Assistance (RA Server TCP-In)* inbound rule is active and that it will allow offers for assistance; see Figure 12-28. I will show you how to use the Advanced Firewall in detail in Chapter 21.

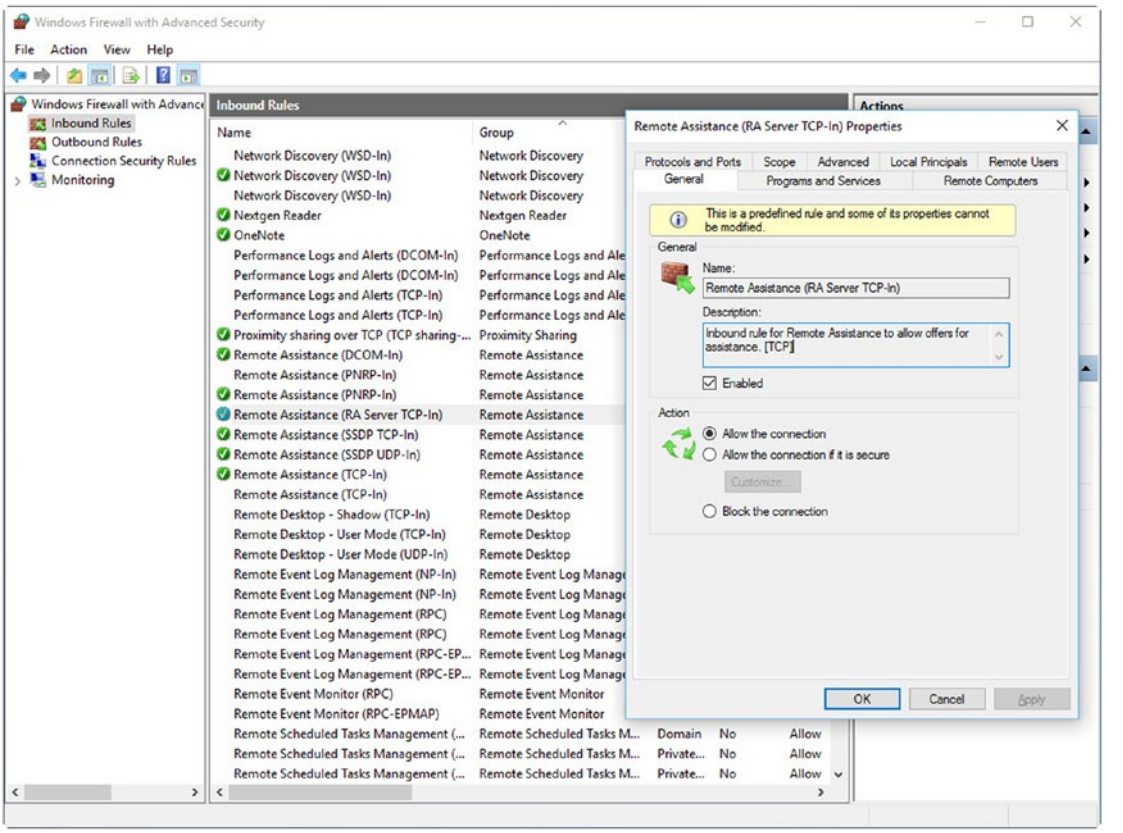


Figure 12-28. *The Windows Firewall also needs to be configured to allow connections*

With these configured, an unsolicited Remote Assistance session can then be instigated from the *Troubleshooting* Control Panel, by clicking *Get Help from a Friend* ➤ *Offer Remote Assistance to help someone*, and then clicking the *Advanced connection options for help desk* link, and entering the name or IP address of the computer to which you want to connect; see Figure 12-29.

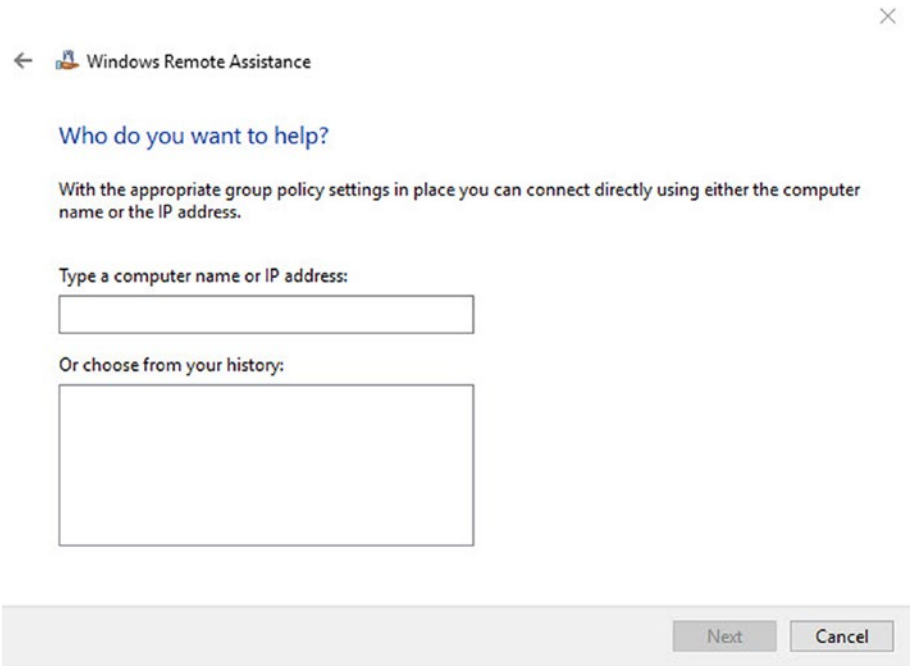


Figure 12-29. *Unsolicited Remote Assistance can be instigated by computer name or IP address*

Remote Desktop

An alternative to Remote Assistance is the Windows Remote Desktop feature, and this is much more common in the workplace. Again, it needs to be activated on each PC. Search in the Start Menu for **allow remote**, and open *Allow Remote Access to your Computer* when it appears in the search results.

This takes you through to the Settings panel, and you will see a switch to enable or disable Remote Desktop; see Figure 12-30. The *Advanced settings* link will then display additional options you might find useful in your organization, such as requiring remote PCs to be from within your own corporate network.

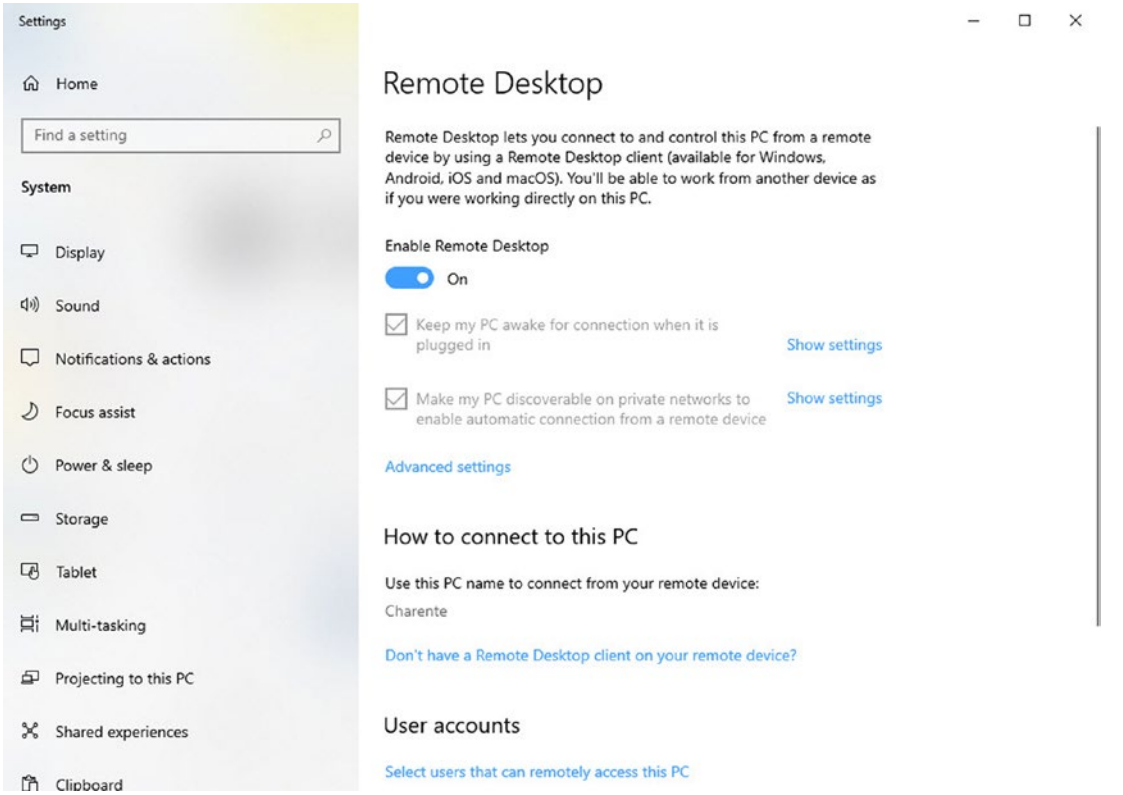


Figure 12-30. *The main Remote Desktop options have been moved to Settings*

The original Control Panel options are still in Windows 10, but you can't access them directly from a search or the Control Panel. Instead, it's best to search for **assist**, and open the *Allow remote assistance invitations…* option when it appears in the search results. This will open a dialog with Remote Desktop options, and is the same dialog we saw when we were making sure Remote Assistance connections can be made with the PC, but you'll see that further down the dialog are options for Remote Desktop; see Figure 12-31.

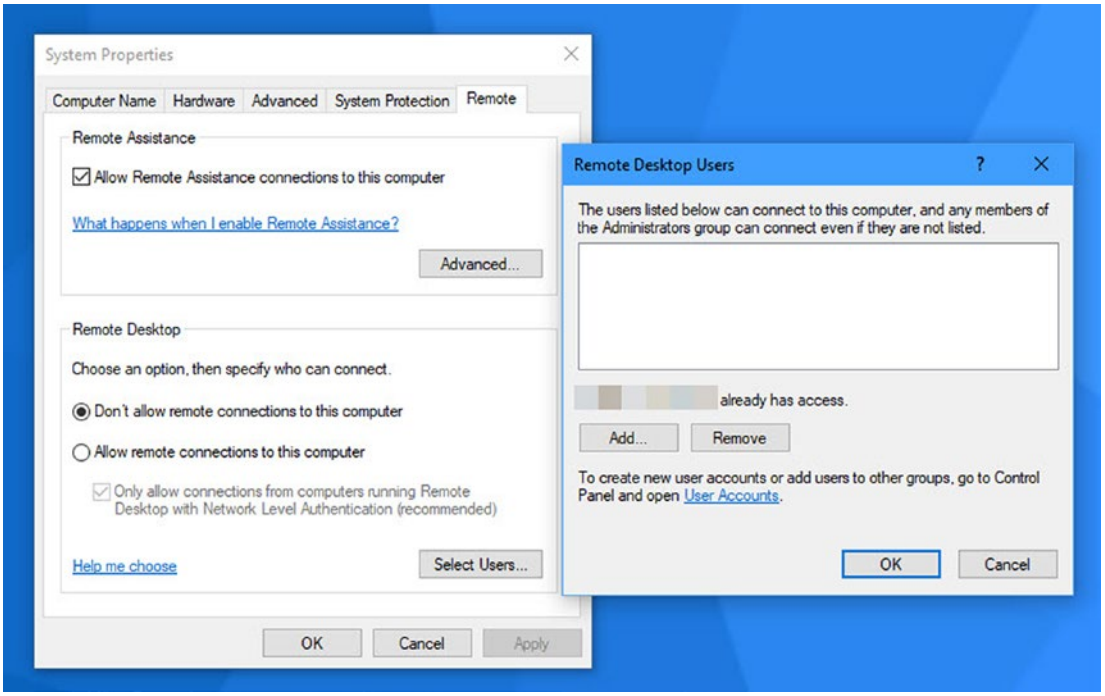


Figure 12-31. *You need to enable Remote Desktop on each PC*

Remote Desktop is disabled by default, so you need to *Allow remote connections to [the] computer* and then click the *Select Users* button. Here you can configure which users or user groups can access the PC. These should be in the format, domain_name\username or domain_name\groupname, but clicking the *Add* button will allow you to search for users and groups in the Domain directory.

To initiate a Remote Desktop session, you will need the computer's name. This can be gained either from the System section of the Control Panel or from the System section in the Settings app; see Figure 12-32.

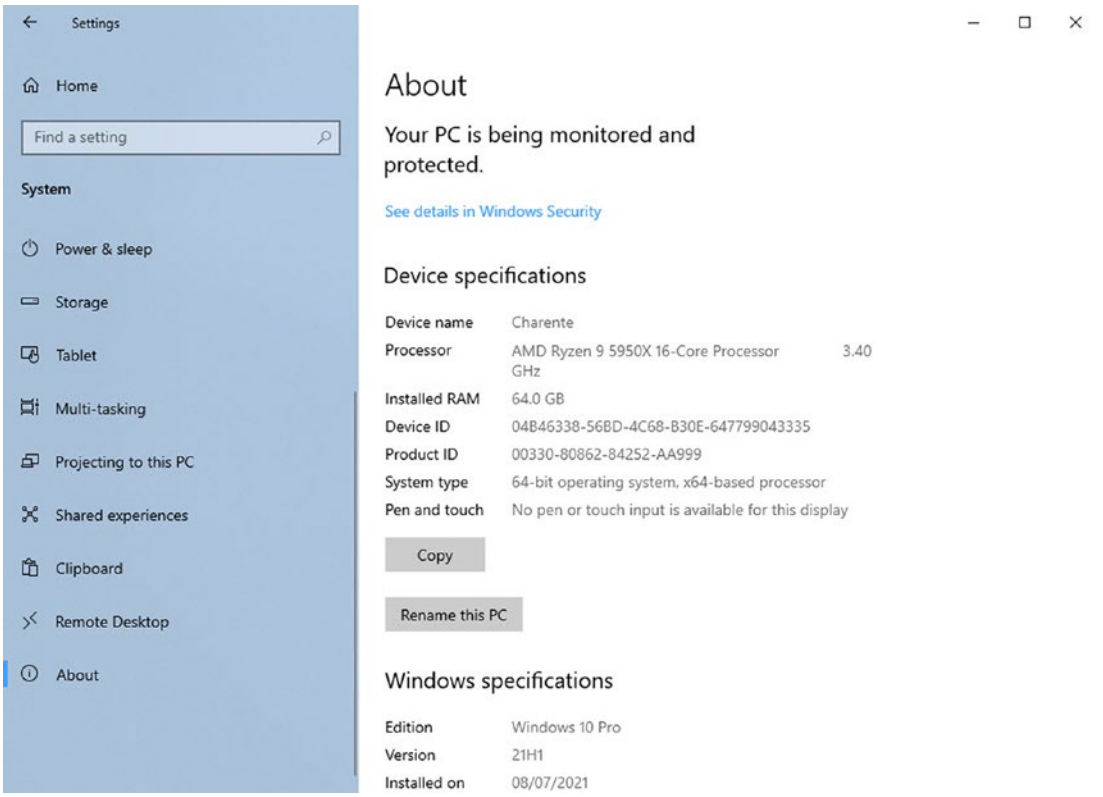


Figure 12-32. *You can get the computer name from the Settings app*

On the PC you wish to use to access the remote computer, search for **Remote Desktop** in the Start Menu, and click *Remote Desktop Connection* when it appears in the search results. This will display a dialog in which you enter the name (with domain pointing if necessary) for the computer to which you wish to connect; see Figure 12-33.

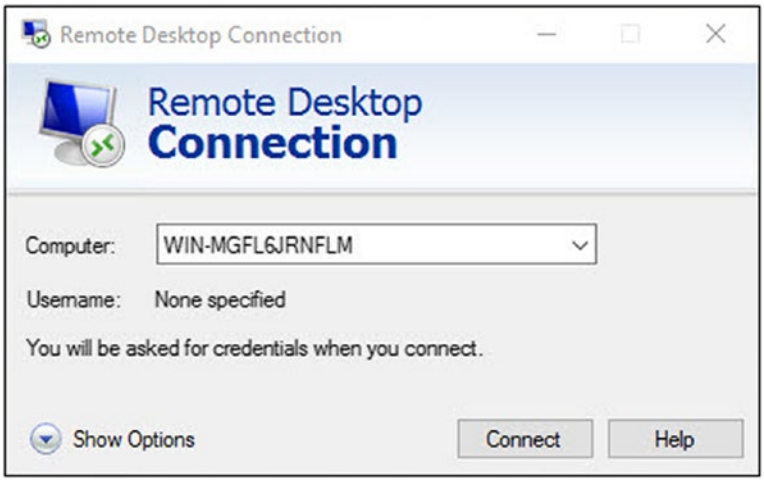


Figure 12-33. *At its simplest, Remote Desktop just asks you for the name of the PC to connect to*

You will be presented with a security dialog and asked to confirm that you do intend to connect to the remote computer; see Figure 12-34. There is a *Don't ask me again for connections to this computer checkbox*, and if you click the *Show details* button in the bottom left corner of the dialog, you can choose if you want to share the drives, clipboard, printers, and other supported Plug and Play devices on your PC with the remote PC.

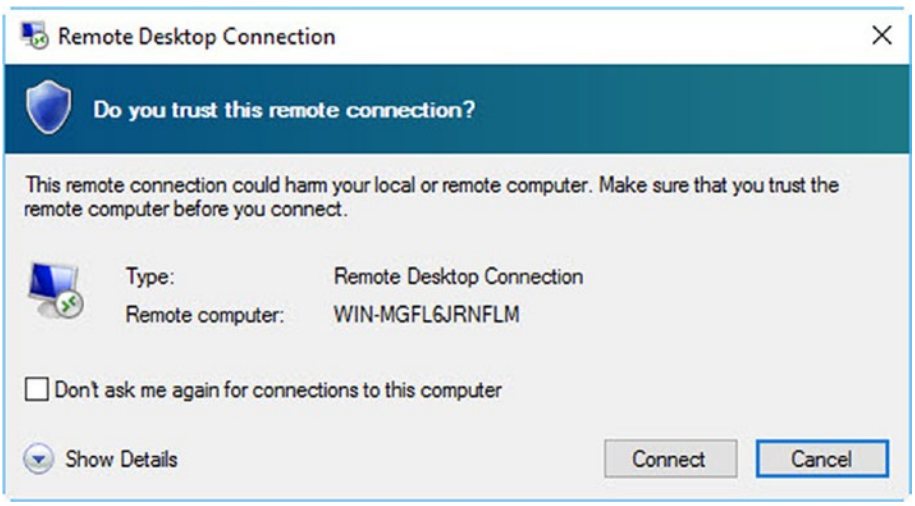


Figure 12-34. *You will be presented with a security dialog before the connection is made*

You will be asked to sign into the remote PC with credentials that have previously been configured as authorized, and you will then be presented with a security certificate for the remote PC that you can review, or click another *Don't ask me again for connections to this computer* check box; see Figure 12-35.

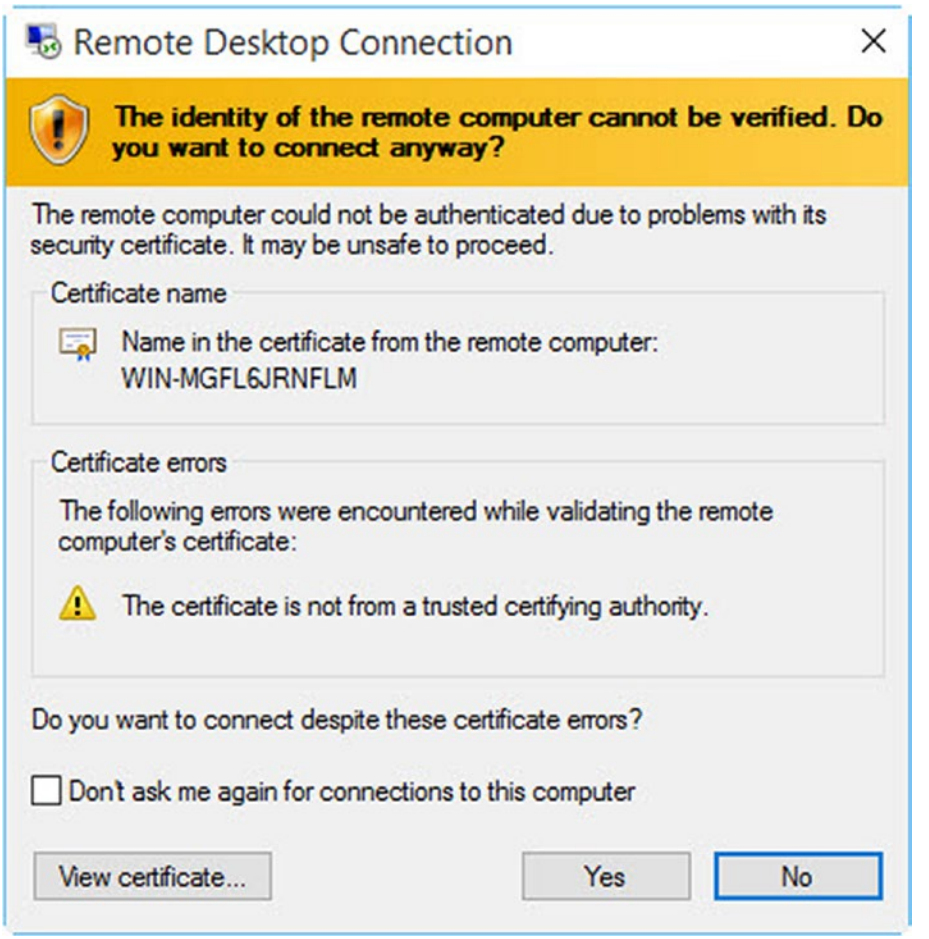


Figure 12-35. *You are presented with a second security certificate when you sign into the remote PC*

When you are using Remote Desktop, any other users will be signed out of the PC, so they won't be able to see what you're doing. Remote Desktop will also run full-screen with a toolbar accessible at the top center of your screen; see Figure 12-36. This toolbar may be hidden, but moving your mouse to the top center of your screen will make it appear, and you can click the *pin* icon to lock it in place so that it is always visible.

Figure 12-36. *Full-screen Remote Desktop is controlled by a bar at the top center of your screen*

Should you wish to run your Remote Desktop connection with different settings, such as at a different screen resolution, you can click the *Show options* button at the main Remote Desktop Connection dialog. This will expand the dialog to offer options such as display, bandwidth, and advanced settings; see Figure 12-37.

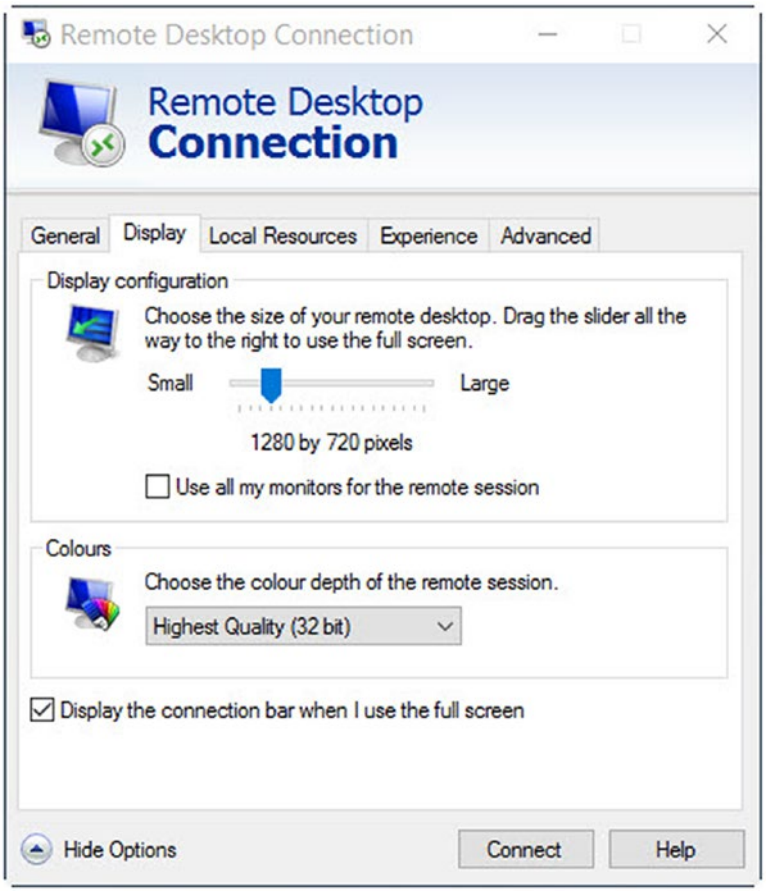


Figure 12-37. *Additional options are available for Remote Desktop*

You may want to choose, for example, what hard disks are available to the remote PC. This can be useful for transferring files or hardware drivers. You can achieve this by clicking the *Local Resources* tab and then clicking the *More* button

in the *Local devices and resources* section. This will open another dialog, in which you can select what hard disks on your PC will be accessible to the remote PC; see Figure 12-38.

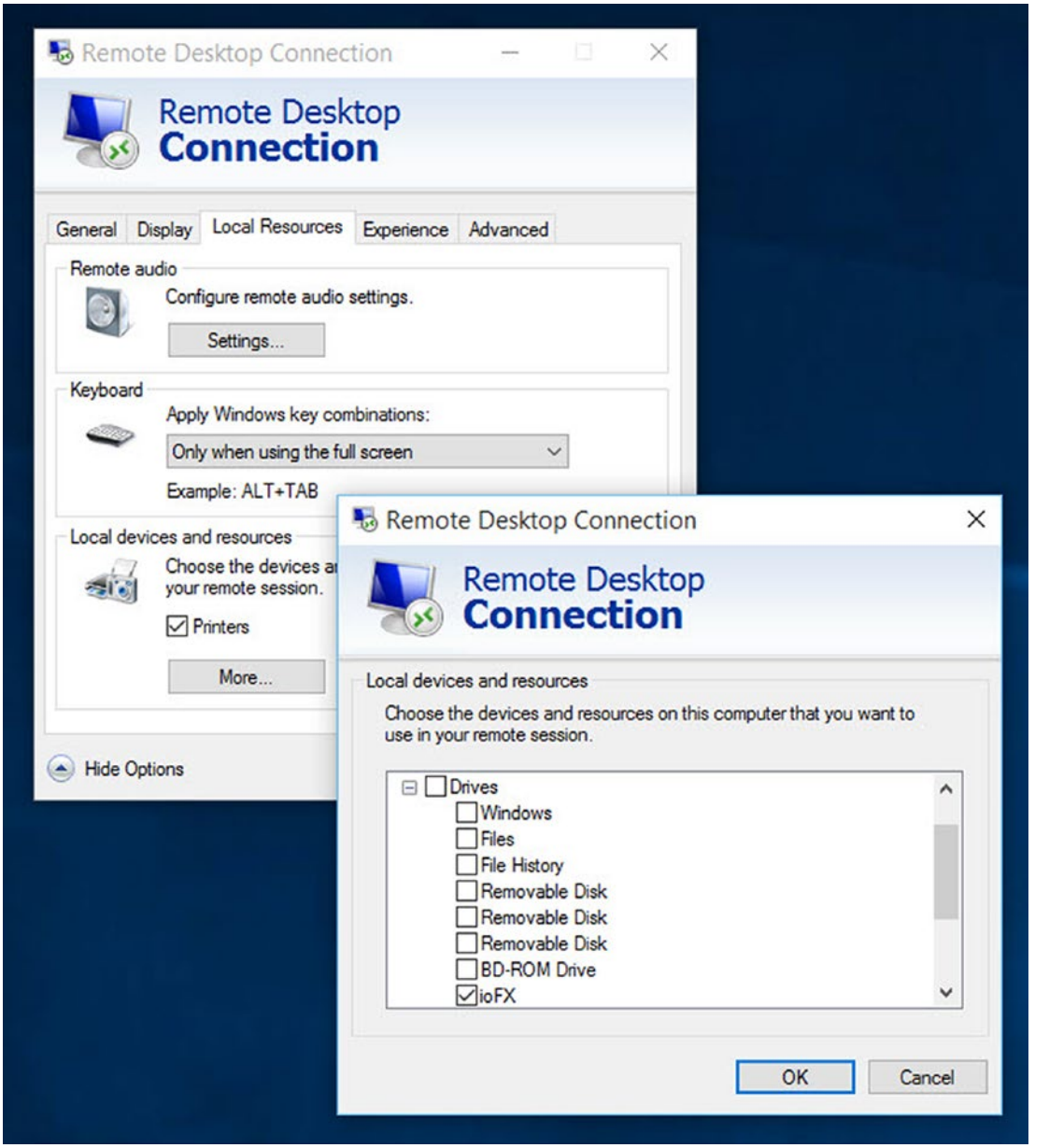


Figure 12-38. *You can choose which drives are accessible to the remote PC*

Third-Party Remote Support Apps

While Windows 10 includes a few pretty useful and effective tools for providing remote support, there is a blossoming third-party market also, some offering features simply not available in the Windows 10 bundled utilities.

I won't go into detail here about how they work as they are being constantly developed and upgraded, but the most popular (in no particular order) are

- **TeamViewer** – `www.teamviewer.com`
- **GoToMyPC** – `get.gotomypc.com`
- **RealVNC** – `www.realvnc.com`

Summary

Certainly, there are plenty of options available to you for supporting users and troubleshooting PCs remotely, and Remote Desktop is extremely popular in larger businesses. Tools such as the Problem Steps Recorder are easy enough for nontechnical people to use, and that can provide an extremely valuable support option when remote access isn't possible, perhaps because the user is on a metered broadband connection.

Back in Chapter 8, however, I dealt with a far more prickly issue, and one that cannot be easily supported remotely, if at all: Windows 10 PCs that simply won't start up. I showed you how to use the automated troubleshooting and repair options, but in the next chapter, I'll show you how to get inside the guts of the Windows Startup system and effect repairs manually.

CHAPTER 13

Repairing Windows Startup Problems

In Chapter 8, I showed you how you can use the tools and utilities available in Windows 10 to troubleshoot startup problems. But what happens if Windows cannot be easily or automatically repaired? If you can't get your copy of Windows 10 to boot to the desktop, then you can't get any work done at all.

The normal response to a nonbootable copy of Windows is either you might reimage the PC, which will inevitably result in huge numbers of Windows updates and app updates needing to be installed… perhaps before you can begin work, or you might be faced with completely reinstalling Windows and ALL of your apps and updates, which can take you out of business for up to two full days.

The good news, however, is that you don't necessarily have to do either of these things, as you can affect manual repairs of the Windows boot system, and even rebuild it completely. Over the years, I've had more mail in my mailbox about this than any other subject, so I would expect this chapter to be the most thumbed of this whole book.

Manually Repairing Windows Startup

If Windows 10 won't start, there are different ways to repair the startup files. You can completely rebuild the boot system by creating new boot partitions, should these have become corrupt, and I'll show you how to do this later in this chapter, and I'll also talk you through the different boot partitions in detail. Microsoft does include a facility, however, that will rebuild the boot files on their existing "hidden" partition, and this is a good first step to try to get your PC working normally again.

To do this, you will need either the USB Recovery Drive I prompted you to create back in Chapter 1, and which I'm sure you have sitting somewhere nice and safe by now, or Windows 10 installation media such as a USB Flash Drive.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_13

Note If you do not have a USB Recovery Drive or installation media, you can download a Windows 10 ISO file, which you can burn to DVD, or create USB installation media at www.microsoft.com/software-download/windows10 by installing the Windows 10 Media Creation Tool on another PC.

If you start the nonbooting PC using Windows 10 installation media, at the *Install* screen, click the *Repair your computer* link in the bottom left corner of the install window. At the Recovery options screen, click *Troubleshoot*, then click *Advanced options*, and then click *Command Prompt*; see Figure 13-1.

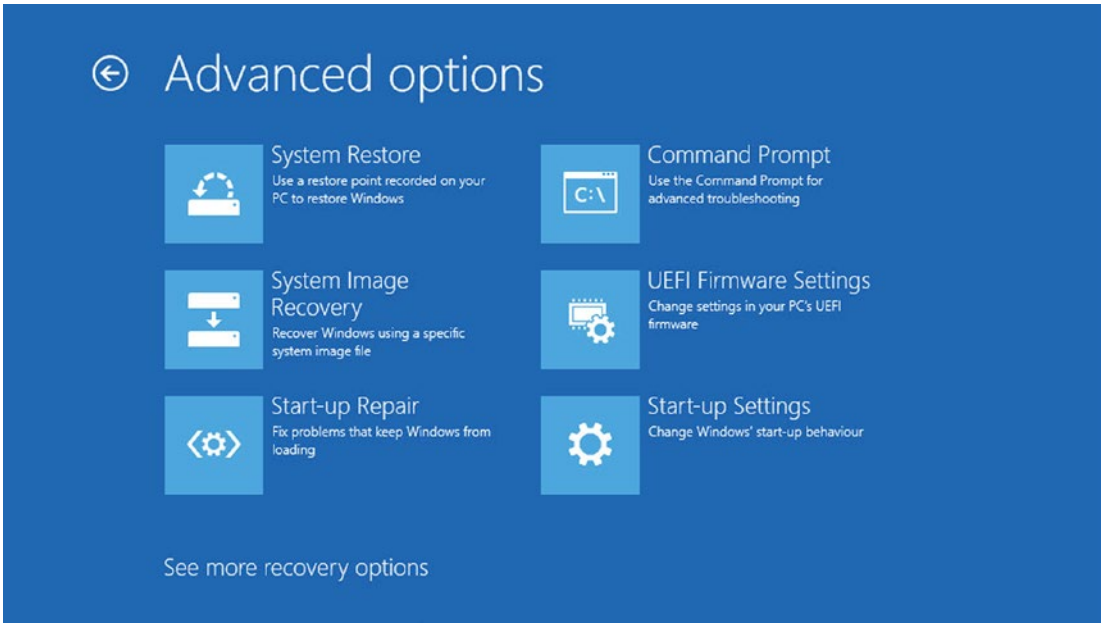


Figure 13-1. *You repair Windows startup from the Command Prompt*

Repairing BIOS Startup Files

When the Command Prompt window is open, the commands you type will be different if you have Windows 10 installed with BIOS or UEFI compatibility. If your copy of Windows 10 is installed with a BIOS system (in which you will have one *System Reserved* partition), type these commands:

1. **BcdEdit /export C:\BCD_Backup**, to create a backup of the current boot files (just in case) where C:\ represents the drive on which you want the backup stored. These can later be reimported in necessary with the **/import** switch.
2. **C:**, moves you to the boot drive as seen by the Command Prompt from a Recovery Drive or installation media.
3. **Cd boot**, navigates to the Windows boot folder.
4. **Attrib bcd -r -h -s**, changes permissions on the boot file so you can rebuild it.
5. **Ren C:\Boot\bcd C:\Boot\bcd.old**, renames the boot file so you can create a new one, but keeps it as a backup.
6. **Bootrec /RebuildBCD**, rebuilds the boot files.

Tip How can you tell if you have a BIOS or UEFI installation of Windows 10? If you can get to the desktop (such as when the PC working fine), open *Disk Management* from the Win+X menu. BIOS installations will have a System Reserved partition before the Windows installation on your hard disk. UEFI installations will have separate Recovery and EFI partitions listed. If you cannot access the desktop, first try the BIOS repair method. If the **Bootrec /RebuildBCD** command reports "`Total identified Windows installations: 0`", you will have a UEFI installation.

Repairing UEFI Startup Files

As I have mentioned, the process for repairing UEFI startup files is different than those for BIOS installations and so requires a different process for repair. At the Command Prompt, type the following commands:

1. **Diskpart**, to enter the Windows Disk partitioning and management tool.
2. **List disk**, to check the hard disks installed on your PC. Choose the correct hard disk (there may only be one) and note its number.

3. **Select disk=0**, where the number you type matches the disk on which Windows 10 is installed.
4. **List volume**, to see the partitions on the disk listed. You are looking for either a FAT32-formatted partition of around 99MB in size (see Figure 13-2) or a volume-labeled `BOOT`; note its number.

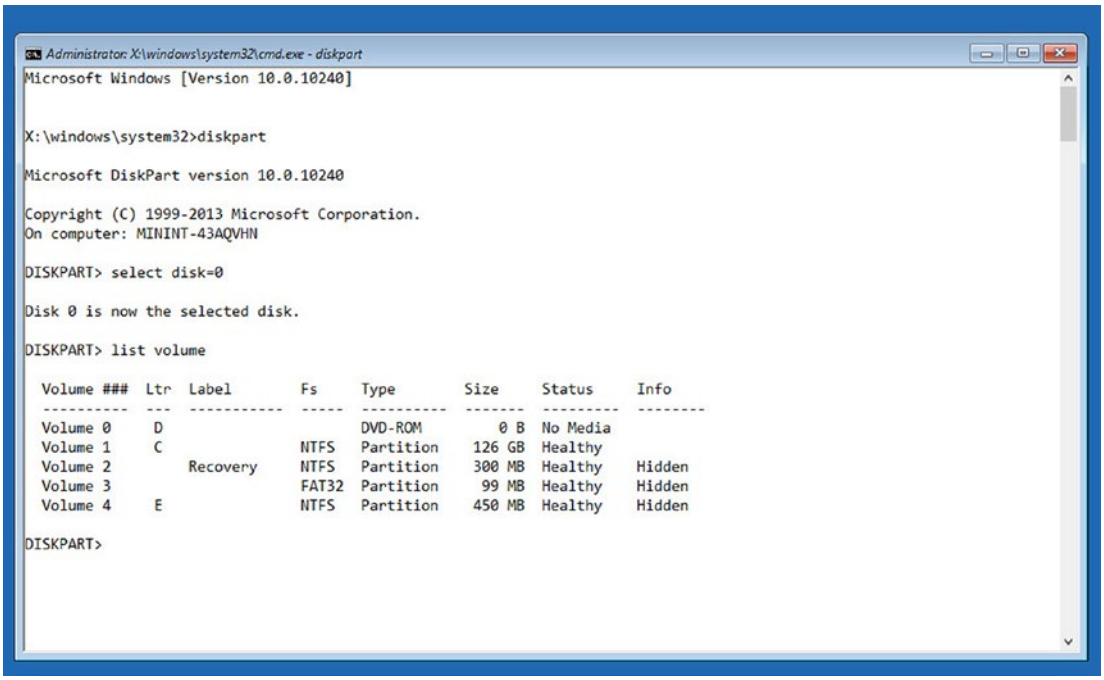


Figure 13-2. *You want a FAT32-formatted volume of around 99MB or a volume-labeled BOOT*

5. **Select volume=3**, where the number represents the number of the correct boot volume.
6. **Assign letter=F:**, to assign a drive letter to the selected volume.
7. **Exit**, to exit the Disk Partitioning tool.
8. **F:**, to select the boot partition, where the letter you type matches the drive letter you assigned the volume.
9. **Cd \EFI\Microsoft\Boot**, to access the boot folder (note: this could also be \Boot\ or \ESD\Windows\EFI\Microsoft\Boot\ depending on your system).

10. **Ren BCD BCD.old**, to rename the boot file so you can create a new one.
11. **Bootrec /RebuildBCD**, to rebuild the boot files (see the following note about the *BCDBoot* command, if this does not fix the problem).
12. When prompted to *Add [the discovered] Windows installation to the boot list*, type **Y**.

Additional Repair Commands for BIOS and UEFI

There are a few additional commands that you may want or need to run at this point to repair startup:

- **Bootrec /FixMBR**, creates a new Master Boot Record for the disk, and should be used if the MBR file is corrupt.
- **Bootrec /FixBoot**, writes a new boot sector to the disk, and should be used if the disk boot sector is corrupt.
- **Bootrec /ScanOS**, can be used if your Windows 10 installation is not found. This command searches for operating system installations and reports what it finds.
- **BcdBoot C:\Windows /s F: /f ALL**, used if the Bootrec /RebuildBCD command does not repair your boot files. This command creates completely new boot files by copying the necessary files from your Windows installation (which should be on `C:` at this point, but you can check in *Diskpart* by viewing the disks and volumes as I detailed earlier). The `/s` switch designates the boot drive and the letter you gave it, in this case `F:`, and the `/f` switch specifies the firmware type to create a boot system for. This can be `BIOS`, `UEFI`, or `ALL`.

Recreating or Moving the Boot Partition

Sometimes you need to completely rebuild the Windows boot partition from the ground up, and you might be surprised when this might be required. Let's take the example of when you install Windows 10 on your PC. In Figure 13-3, we can see the Windows installer asking where we want to put the OS, but there's only one physical disk, this being labeled as Disk 0.

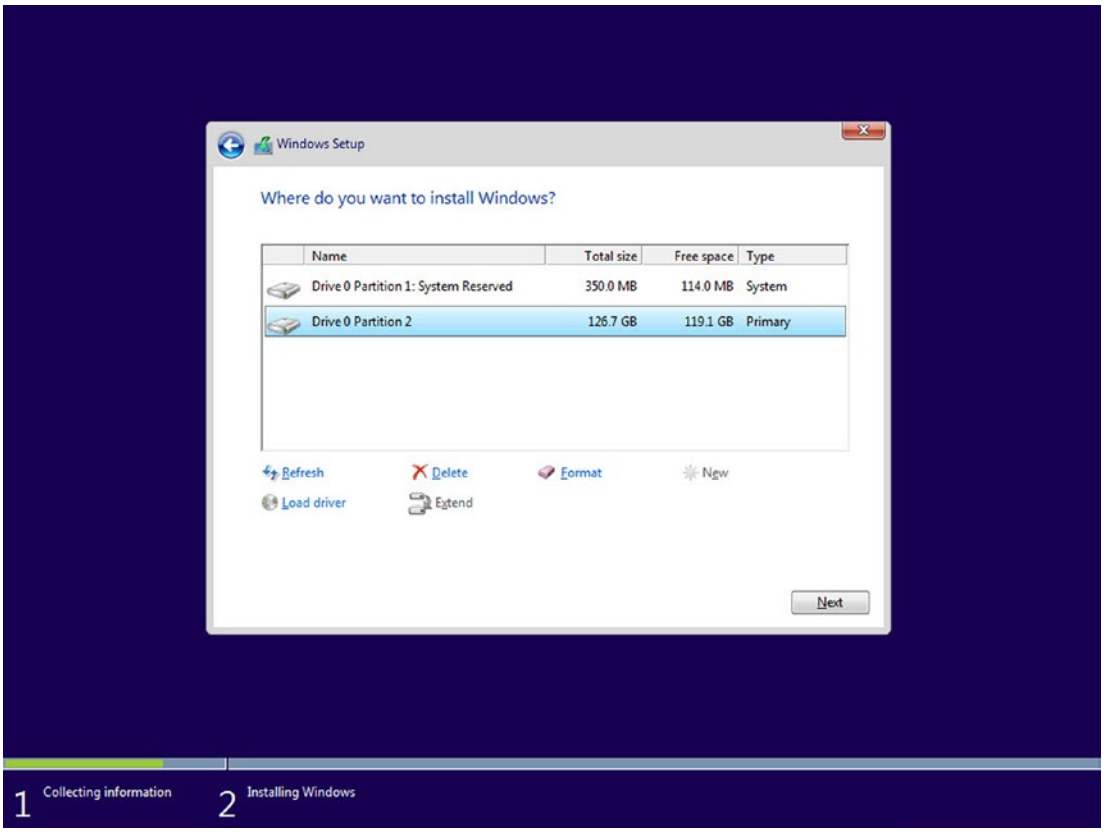


Figure 13-3. *Occasionally, the Windows installer puts the boot files on the wrong disk*

You might have more than one physical hard disk in your PC, however: Disk 1, Disk 2, and so on. Occasionally when you install Windows, the boot partitions will end up on the wrong physical disk. This is most likely because you want to install Windows 10 on a specific disk, but that disk isn't marked as Disk 0 by the BIOS or UEFI system on the motherboard.

Generally speaking, this isn't annoying, as if you just install Windows 10 and leave it, you won't even notice this has happened. If you want to create a System Image Backup of the installed OS though, one of two things will happen:

1. You will try to back up your Windows installation using the Windows 10 Image Backup utility, to be told that there is no available hard disk or partition on your PC on which the backup can be stored. This is because each partition is occupied by either Windows 10 or the boot files, and both need to be included in the backup.

2. Your backup will include the entire contents of the second disk because, unless that disk was completely blank, with no partitions at the time Windows 10 was installed, the boot files will be placed on the first partition on the disk. If this disk contains your files and folders, these will be included in the backup, rendering the backup useless. This is because when you come to restore the backup, you will also restore the contents of your files disk, as they were at the time the backup was made. This will completely wipe any files created or modified since.

There might be other circumstances too in which the boot system in Windows 10 becomes, to use a technical term, completely buggered. In most circumstances, however, it can still be rescued by following these instructions.

Caution Rebuilding the boot system in Windows 10 using the following method will render some parts of the recovery system, the Reset backup image, and the USB Recovery Drive creator tool completely useless. You will need to ensure you already have a System Image Backup and a USB Recovery Drive to repair Windows should anything untoward happen to it in the future.

Step 1a: Create a New Boot Partition (Command Prompt)

The first step involves creating a new partition on which the boot system can reside. You can do this from the Disk Management Console on the desktop, but I will show you how to action this from the Command Prompt when you start the PC from a USB Recovery Drive or Windows 10 installation media, as it's most likely that you're doing this because you can't start the PC. I will include side-instructions though on how to achieve this from the desktop. At the *Command Prompt (Admin)* (accessed using the method I described in the "Manually Repairing Windows Startup" section), type the following commands:

1. **Diskpart**, to enter the Disk Partitioning and Management tool.
2. **List Disk**, and make a note of the disk on which Windows 10 is installed.
3. **Select Disk=0**, where the number is the number of the disk on which Windows 10 resides.

4. **List Volume**, to list all the volumes and partitions on the disk.
5. **Select Volume=4**, where the number represents the final (or largest partition on the disk). I say largest because sometimes a UEFI install can place hidden partitions at the end of the disk.
6. **Shrink desired=500**, to shrink the partition by 500MB. This will create blank space at the end of the partition.
7. **Create Partition Primary Size=500**, to create a new partition in the available space.
8. **List Volume**, to check the number for the newly created partition; it will be listed as having a `RAW` file system.
9. **Select Volume=5**, where the number represents the number of the new partition.
10. **Format FS=NTFS LABEL="Boot" Quick**, to format the disk.
11. **Assign Letter=F**, to assign a drive letter to the partition temporarily. This should be a letter that is not currently showing as being in use in *List Volume* for any installed disk.
12. **Exit**, to leave the Diskpart tool.

Step 1b: Create a New Boot Partition (Disk Management Console)

If you can get to the desktop, perhaps because the boot folders were placed on the wrong disk during the installation of Windows 10, follow these instructions:

1. Press *Windows key* + *X* to open the Administration menu.
2. Click *Disk Management* to open the Disk Management Console. You can also open this by searching for diskmgmt.msc in the Start Menu.
3. Right-click the last or largest partition on the disk on which Windows 10 is installed (I say largest because sometimes, as in the example in Figure 13-4, the Windows installer places boot partitions at the end of the disk, not giving us space to create a new partition).

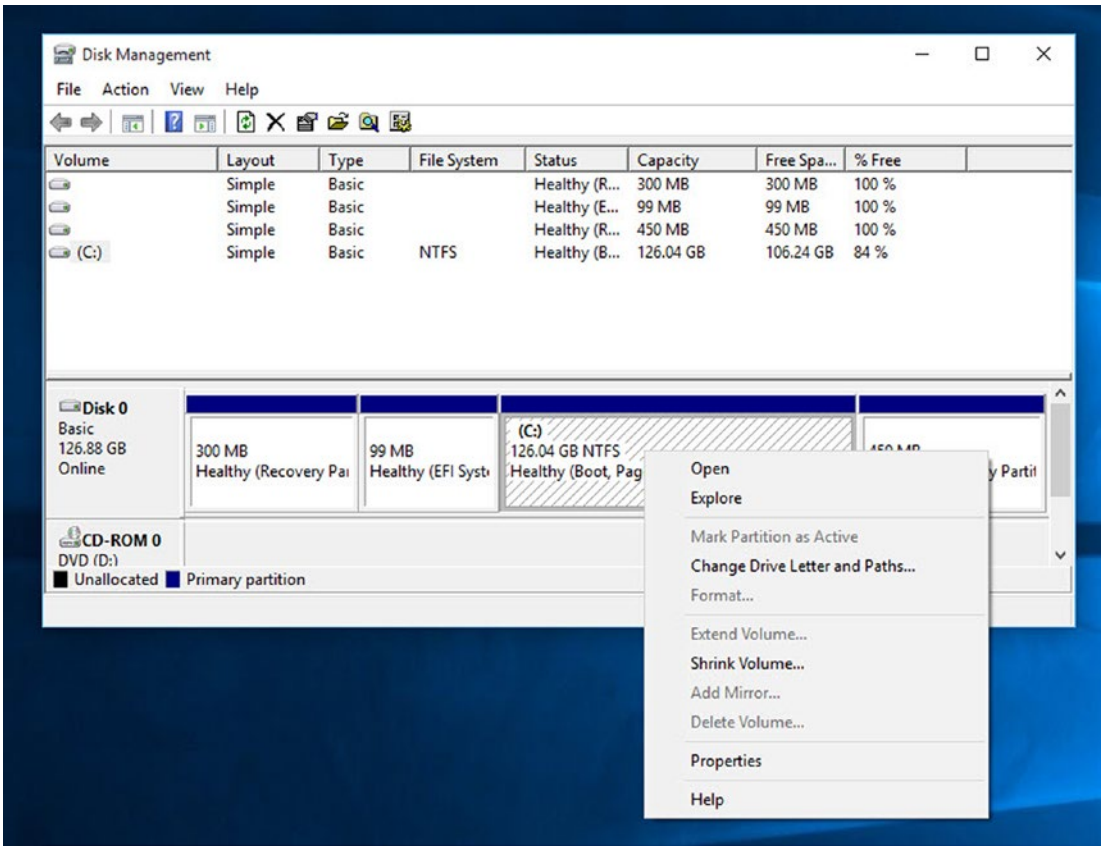


Figure 13-4. *You need to right-click the last or largest partition*

4. Click *Shrink Volume* in the menu that appears.
5. In the dialog that appears, set the *Enter the amount of space to shrink in MB* figure to 500 (see Figure 13-5), and click *Shrink*.

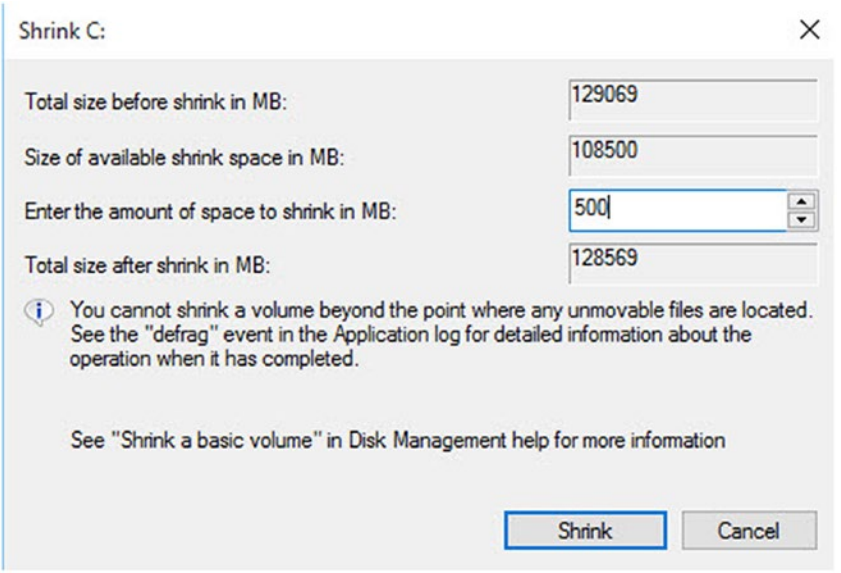


Figure 13-5. *You need to shrink the partition by 500MB*

6. In the blank partition space that is created, right-click and select *Create Simple Volume* from the menu that appears; see Figure 13-6.

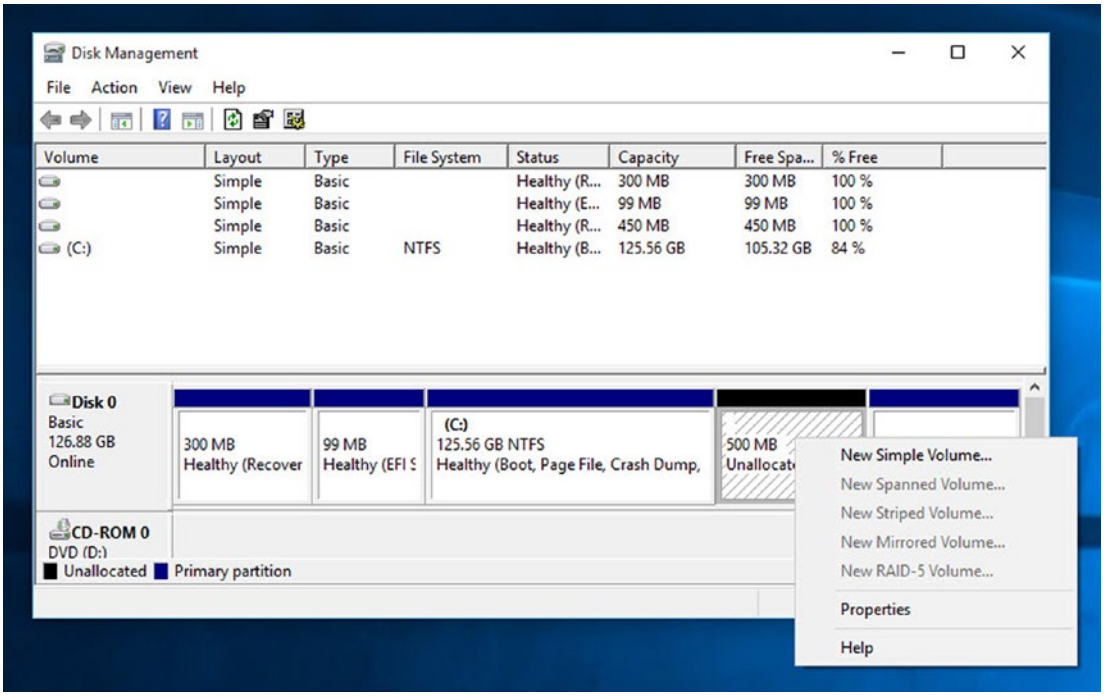


Figure 13-6. *You need to create a new partition in the available space*

7. In the dialog that appears, click through the options, assigning the maximum available amount of space, making sure it was a drive letter assigned (see Figure 13-7), and that it is formatted as NTFS with the volume name "Boot."

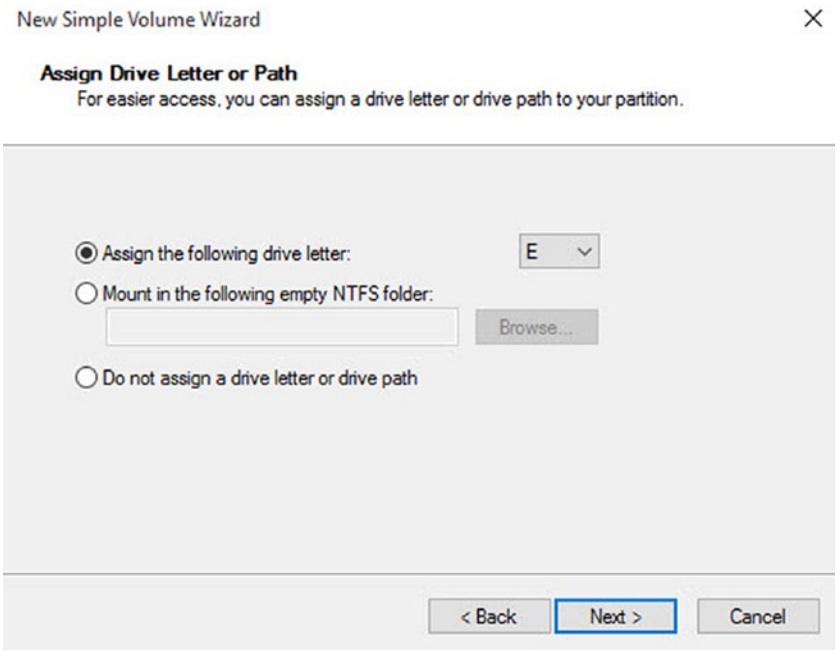


Figure 13-7. *The new partition should have a drive letter assigned*

Step 2: Create the New Boot Files

Once your new boot partition has been created, either from the desktop or the Command Prompt, you need to move the boot files across to it. To do this you must be at the Command Prompt. This can be done either from the Recovery environment or from the desktop. Should you be doing this from the desktop, run the Command Prompt as an *Administrator*; the option for this is in the Win+X menu. Next, type the following commands:

1. **BcdBoot C:\Windows /s E: /f ALL**, used if the Bootrec /RebuildBCD command does not repair your boot files. This command creates completely new boot files by copying the necessary files from your Windows installation (which should be on `C:` at this point, but you can check in *Diskpart* by viewing the

disks and volumes as I detailed earlier). The `/s` switch designates the boot drive and the letter you gave it, in this case `E:`, and the `/f` switch specifies the firmware type to create a boot system for. This can be `BIOS`, `UEFI`, or `ALL`. If you are not sure what partitions Windows 10 installed on, and which one you have created for your new boot system, use the *List Disk* and *List Volume* commands I detailed earlier.

2. **DiskPart**, to enter the Disk Partitioning tool.
3. **List Disk**, and make a note of the disk on which Windows 10 is installed.
4. **Select Disk=0**, where the number is the number of the disk on which your new boot partition resides.
5. **List Volume**, to list all the volumes and partitions on the disk.
6. **Select Volume=5**, where the number represents the partition you created for your new boot system.
7. **Active**, to mark the partition as active.
8. **Remove Letter=E**, to remove the drive letter from the partition.

Your new boot system has now been created. When you restart the PC, your old boot partitions will no longer be used. **Bear in mind the caution earlier, however, that performing this task will completely break some parts of the recovery environment, the Reset backup image, and the USB Recovery Drive creator utility**. If these are important to you, perhaps a better alternative is to physically unplug all but the hard disk on which you want Windows 10 installed and perform a clean install, wiping out all your existing partitions on the Windows drive first. I will show you how to do this in Chapter 30.

Setting Up and Managing Dual/Multiboot Systems

Dual and multiboot PCs are still commonplace both in the home and in businesses. There are many reasons why someone might want to configure their PC to boot from two different operating systems. This might be to maintain compatibility with older software that runs fine in an earlier version of Windows, but not in Windows 10. In the IT support

space, it might be to have a reference machine you can refer to (though a VM might be a better choice in this example). Some people like to have a dual-boot system to separate their work and home lives, or to have a dedicated OS for gaming.

Whatever the reason to set up a dual-boot system, it's not without its complications, especially with Windows 10. If you already have Windows 10 installed on your PC, and then want to also install an earlier version of Windows, then you can pretty much forget it, as the advances Microsoft has implemented with the boot loader will render your entire system unbootable should you try. If you want a different version of Windows, or Linux, installed on your PC, though, you should install them in this order:

1. Linux/Windows XP
2. Windows Vista
3. Windows 7
4. Windows 8.1
5. Windows 10

Caution I want to mention end-of-support dates for Windows operating systems, as all support for Windows XP ended in 2014. This means that there are no longer any security or stability updates for the OS and any vulnerabilities that still exist will never be patched. Windows XP therefore is a significant security risk unless it's completely sandboxed in a VM, and I'll show you how to do this in Chapter 20. Similarly, the end-of-support dates for other Windows versions were (depending on when you're reading this) Vista in April 2017, Windows 7 in January 2020, and Windows 8.1 in January 2023.

Secure Boot

Secure Boot, sometimes called Trusted Boot, is an Intel-designed system that's built into the UEFI firmware systems of modern motherboards. It's designed to prevent the execution of any code at the PC's startup that's not digitally signed and known to the system, such as rootkits and malware.

Microsoft mandated that all new PCs that were sold with Windows 8.1 or Windows 10 must come with Secure Boot available and enabled. This can cause a problem for people who want to dual-boot with older or non-Windows operating systems, as only

Windows 8.1 and Windows 10 support it. As such, Windows 7, Windows Vista, Windows XP, and any Linux distribution (at the time of writing this anyway) will simply fail to install on a system where Secure Boot is enabled.

When you are purchasing a new PC, or on an existing PC where you wish to install an older or non-Windows OS, you should check the UEFI firmware settings to see if Secure Boot can be disabled, as it often can. Not all UEFI systems support disabling of Secure Boot, however, especially on cheaper PCs.

Bitlocker and Dual-Boot Systems

Microsoft's full disk encryption feature, Bitlocker, notoriously hates dual and multiboot systems. If you use Bitlocker to encrypt your Windows drive or partition and/or any other partitions, every time you start your PC to Windows, you will be asked to enter your 48-character Bitlocker unlock key.

This can be bothersome, so the best solution if you wish to dual-boot your PC is simply not to use Bitlocker on your PC. There are other encryption methods you can use for your files though, such as the Encrypting File System (EFS), and I'll show you how to use this in Chapter 18.

Managing Boot Systems with BCDEdit

Sometimes you need to manually edit the boot menu system in Windows 10. This might be because you have multiple copies of Windows 10 installed in a dual-boot system, and they're all showing up in the startup menu with the same name. It also might be because you have a Linux installation that is configured incorrectly in the boot menu.

You can edit the boot menu both from the desktop and from a USB Recovery Drive or Windows 10 installation media by using the (Boot Configuration Data) BCDEdit command. This works in the Command Prompt. If you are opening the Command Prompt from the desktop, start it from the *Win+X* menu, and click *Command Prompt (Admin)*. If you are using the Command Prompt from boot media, start it in the way I described at the very beginning of this chapter.

When you type the command **BCDEdit** into a Command Prompt window, you will be presented with a list of all the operating systems currently installed on the PC that are listed in the Windows 10 boot system; see Figure 13-8.

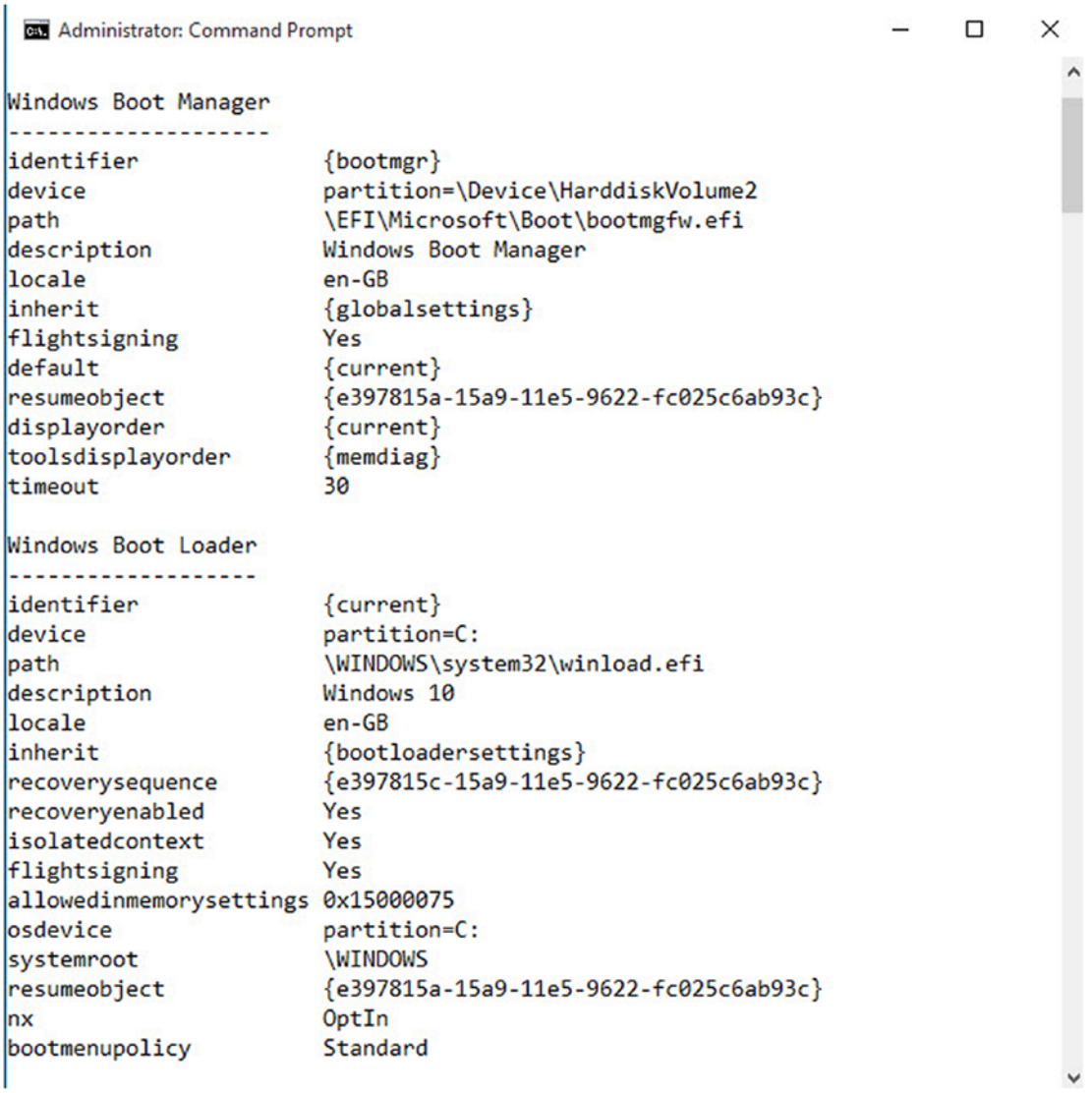


Figure 13-8. *BCDEdit is run from the Command Prompt as an Administrator*

The important object for each to note is its *{identifier}*; this might be a text string, but it could also be a hexadecimal code as in the {e397815a-15a9-11e5-9622-fc025c6ab93c} format seen in Figure 13-8. There are many switches you can use with BCDEdit to edit,

create, and delete entries from the Windows 10 boot menu. Of these, by far the most useful for troubleshooting are

- **bcdedit [/store filename] /bootdebug [id] { ON | OFF }** is used to enable or disable the debugger for the specified boot entry. The debug log is stored in the file specified in the command. This might be used in the format *bcdedit /store C:\BootDebugLog /bootdebug {current} ON*.
- **bcdedit [/store filename] /bootsequence id [...] [/addfirst | /addlast | /remove]** specifies the boot sequence for a one-time boot. This might be used in the format *bcdedit /bootsequence { e397815a-15a9-11e5-9622-fc025c6ab93c } {current} {ntldr}*.
- **bcdedit [/store filename] /copy id /d description** creates a copy of the specified boot entry. This might be used in the format bcdedit /copy { e397815a-15a9-11e5-9622-fc025c6ab93c } /d "Copy of Windows 10".
- **bcdedit [/store filename] /create [id] /d description [/application apptype | /inherit [apptype] | /inherit DEVICE | /device]** creates a new boot entry with the specified ID. The supported application types are *BOOTSECTOR, OSLOADER,* and *RESUME*, and the supported Inherit types are *BOOTMGR, BOOTSECTOR, FWBOOTMGR, MEMDIAG, NTLDR, ORLOADER,* and *RESUME*. This might be used in the format *bcdedit /create {ntldr} /d "Compatibility OS"*.
- **bcdedit [/store filename] /debug [id] { ON | OFF }** enables or disables the kernel debugger for the specified boot entry. This might be used in the format *bcdedit /debug ON*.
- **bcdedit [/store filename] /default id** sets the default boot entry for the PC. This might be used in the format *bcdedit /default { e397815a-15a9-11e5-9622-fc025c6ab93c }*.
- **bcdedit [/store filename] /delete id [/f] [/cleanup | /nocleanup]** deletes the specified boot entry and optionally cleans it from the display order. This might be used in the format *bcdedit /delete {cbd971bf-b7b8-4885-951a-fa03044f5d71} /cleanup*.

- **bcdedit [/store filename] /deletevalue [id] datatype** deletes an element or value from a boot entry. This might be used in the format *bcdedit /deletevalue {bootmgr} bootsequence.*
- **bcdedit [/store filename] /displayorder id [...] [/addfirst | /addlast | /remove]** sets the boot manager's display order. This might be used in the format *bcdedit /displayorder { e397815a-15a9-11e5-9622-fc025c6ab93c } /addlast.*
- **bcdedit [/store filename] /enum [type | id] [/v]** lists all the boot entries in the specified BCD store. This can be used with the enum types ACTIVE, ALL, BOOTAPP, BOOTMGR, FIRMWARE, INERIT, OSLOADER, and RESUME. It may be used in the format *bcdedit /enum OSLOADER.*
- **bcdedit /export filename** creates a backup copy of the BCD store to the specified file. It might be used in the format *bcdedit /export "C:\BCD Backup".*
- **bcdedit /import [/clean] filename** imports the contents of an exported BCD backup. It might be used in the same format as the export command. The /clean switch is used only on UEFI systems, and it forces the firmware to delete all its existing NVRAM boot entries that are used with Secure Boot.
- **bcdedit [/store filename] /set [id] datatype value [/addfirst | /addlast | /remove]** creates or modifies an element in a boot entry. It might be used in the format *bcdedit /set { e397815a-15a9-11e5-9622-fc025c6ab93c } path \windows\system32\winload.exe.*
- **bcdedit /sysstore partition** specifies the partition used for the BCD store. This switch is used only on UEFI systems, and might be used in the format *bcdedit /sysstore C:.*
- **bcdedit [/store filename] /timeout** timeout specifies how long the boot loader should wait at the OS loader menu before selecting the default entry. It might be used in the format *bcdedit /timeout 30*, where the number is a representation of seconds.

BCDEdit Identifiers

I've already detailed that the OS identifiers used in the Boot Configuration Data store come in the format {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}, but there are others available, such as {current} and {ntldr}, which I've used in the preceding examples. The full list of available identifiers is shown in Table 13-1.

Table 13-1. *Identifiers used by the BCDEdit Command*

Identifier	Description
{badmemory}	The global RAM defect list
{bootloadersettings}	Global settings to be inherited by all boot loader entries
{bootmgr}	The Windows Boot Manager
{current}	The currently running operating system
{dbgsettings}	The global debugger settings
{default}	An identifier for the default boot entry
{emssettings}	The global EMS settings
{fwbootmgr}	The firmware boot manager boot entry; stored in NVRAM on UEFI systems
{globalsettings}	Global settings that should be inherited by all boot entries
{memdiag}	The memory diagnostic utility
{ntldr}	The Windows legacy loader, NTLDR; used for versions of Windows released prior to Windows Vista
{ramdiskoptions}	Additional options required for RAM disks
{resumeloadersettings}	Global settings that should be inherited by all Windows resume-from-hibernation entries

BCDEdit Data Formats

Additionally, each BCDEdit command is used with data fields such as ID. These are shown in Table 13-2.

Table 13-2. *BCDEdit data formats*

Data Format	Description
boolean	A Boolean value that can be set to TRUE or FALSE. You can also use the values TRUE or FALSE, as well as 1 and 0, and YES and NO
device	A device data type that can be one of BOOT, PARTITION=drive, FILE=[parent]path, or RAMDISK=[parent]path,optionsid
enum	The data type that takes a value from a list
id	The identifier for a boot entry, known as its globally unique identifier {GUID}
integer	A 64-bit integer, 32-bit variables are not supported
list	A boot entry identifier list that contains one or more boot entry identifiers separated by spaces. This list type does not use quotation marks
string	A string variable. It should be surrounded by quotation marks ("") if it contains spaces

An excellent and full reference document for the BCDEdit command is available to download from the Microsoft website `http://pcs.tv/1MBUbPu`.

Examples of BCDEdit Use

This all seems fairly confusing, so I want to detail some real-world examples of how you might use the BCDEdit command with your Windows 10 PC:

- To change the default operating system, the one that appears first in the OS choices list and that will load automatically if no option is selected there, use the command **BCDEdit /default {id}**.
- If an operating system has the incorrect disk or partition associated with it, this can be rectified with the command **BCDEdit /set {id} device partition=X:**, where X: represents the disk or partition on which the operating system is installed. You must then also use the command **BCDEdit /set {id} osdevice partition=X:**.

- To manually add a legacy operating system that isn't appearing in the list, use these commands with the new custom ID {legacy}:

  a. **BCDEdit /create {legacy} /d "Legacy OS Name"**

  b. **BCDEdit /set {legacy} device partition=D:** or the letter of the partition where the legacy OS is installed

  c. **BCDEdit /set {legacy} path /ntldr**

  d. **BCDEdit /displayorder {legacy} /addlast**

- If you are adding a Linux installation to the boot menu, follow these instructions:

  Boot into Linux and launch a Terminal session with root privileges.

  Find which partition Linux is installed on with the command **fdisk -l** (lowercase "L"). The Linux installation will be on a partition labeled as /dev/sda1 or /dev/hda1.

  Install a GRUB (Grand Unified Boot Loader) boot manager on that partition with the command **grub-install /dev/sda1**.

  Copy the Linux boot sector with the command **dd if=/dev/sda1 of /tmp/linux.bin bs=512 count=1**.

  Copy the file linux.bin to a USB Flash Drive as a backup.

  Install Windows 10 on your PC.

  Press *Win+X* to open the Administration menu and run *Command Prompt (Admin).*

  Type **diskpart** to enter the disk management utility.

  Type **select disk=0**, which is more than likely where your boot partition is located.

  Type **list volume** and look for the active or System partition; see Figure 13-9.

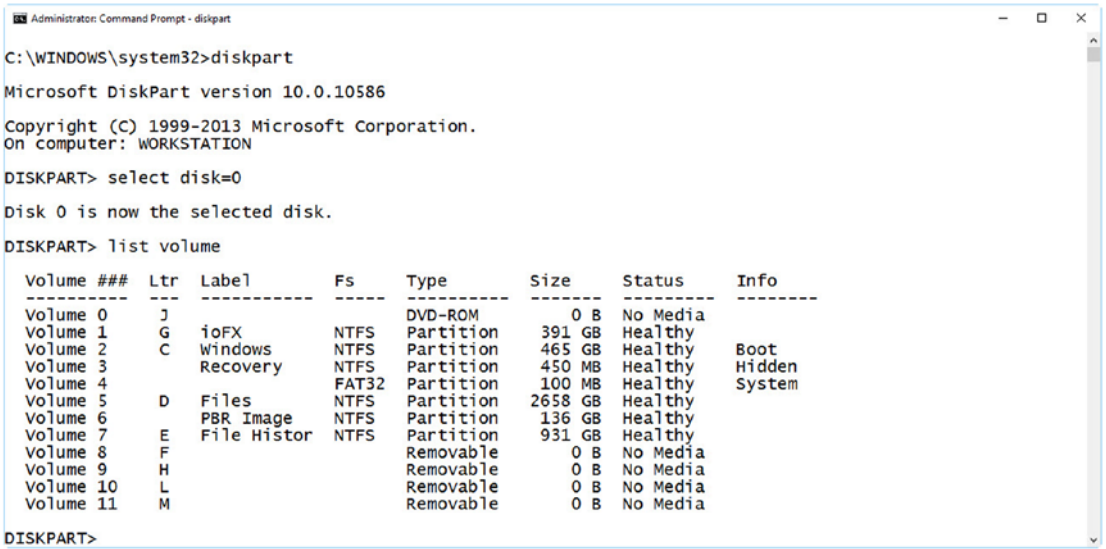


Figure 13-9. *You are looking for the System partition on your disk*

You need to temporarily assign a drive letter to the System partition. Type **assign letter=n** and use the next available drive letter.

Copy your *linux.bin* backup file from your USB Flash Drive to the root (active) partition.

Type **remove letter=n** to remove the drive letter.

Create a GRUB entry with the command **BCDEdit /create /d "GRUB" /application BOOTSECTOR**. This will return a unique ID: make a note of it. For the remainder of this example, I will call it {linuxid}.

Type **BCDEdit /set {linuxid} device boot**.

Type **BCDEdit /set {linuxid} PATH /linux.bin**.

Type **BCDEdit /displayorder {linuxid} /addlast**.

Effecting Repairs on the Boot Partition Structures

If the main boot partition becomes corrupt in Windows, you can, as I detailed earlier, create a new one and get your copy of Windows 10 working again. This will, however, break some crucial functionality such as some parts of the Recovery Environment, the Reset backup image, and the ability to create a USB Recovery Drive. But what happens if you want to preserve these, or if you are suffering from a general disk corruption?

Normally in these circumstances, you'd run a command such as the venerable `CHKDSK`, or a third-party disk utility. CHKDSK can be run from a Recovery Drive but isn't very comprehensive. If you can't get Windows 10 to start, however, this becomes very difficult. You could start the PC from a Windows To Go (WTG) drive, but these are designed to hide the underlying PC drives for security reasons. There are ways around this by giving yourself access in the Disk Management Console, but Windows 10 doesn't really come with useful disk partition management tools, and certainly doesn't come with repair tools. You would need these to already be installed on the WTG drive.

In these circumstances I recommend starting the PC from a Linux CD or DVD. It's noninvasive in that it can be run entirely from the removable disk, without needing to be installed, and many distributions (known as distros) come with useful disk and partition management tools.

I mentioned early in this chapter that BIOS and UEFI installations of Windows have different boot partition structures. BIOS systems use a single *System Reserved* partition; see Figure 13-10. This contains all the files needed to boot the operating system. This partition is commonly 100MB in size.

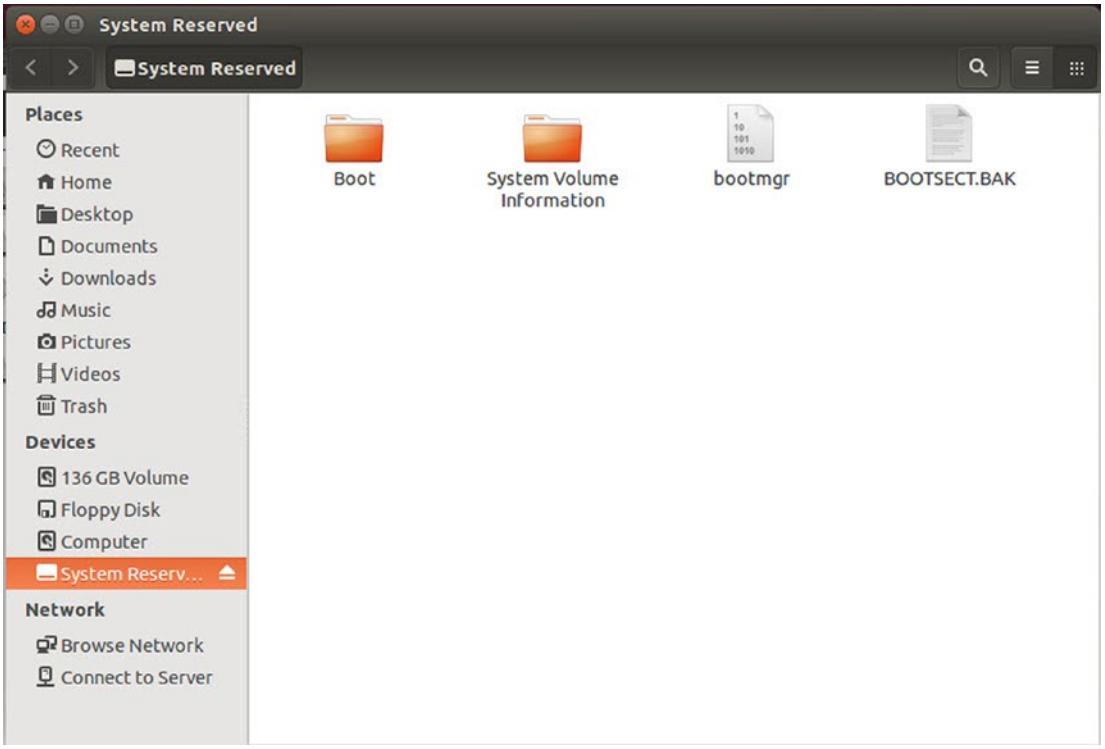


Figure 13-10. *BIOS PCs have a single System Reserved partition*

UEFI systems have a three-partition structure. The first of these is a 100MB *EFI System* partition, a 300MB *Recovery* partition that contains a copy of the WinRE Windows Recovery Environment file, and a third small, hidden partition that's used for storing the security tools used for features such as Bitlocker.

Note Some UEFI installations of older 32-bit Windows 10 versions have only a System Reserved partition. This will be because they are installed on a PC with a 32-bit processor and older motherboard that does not support all the features of the UEFI specification.

It's the *EFI System* partition (see Figure 13-11) that contains all the boot files for Windows 10. With both the *System Reserved* and *EFI System* partitions, you can, if you're extremely paranoid and have a tin foil hat, make backup copies of all the files in these partitions. It's not normally necessary, however.

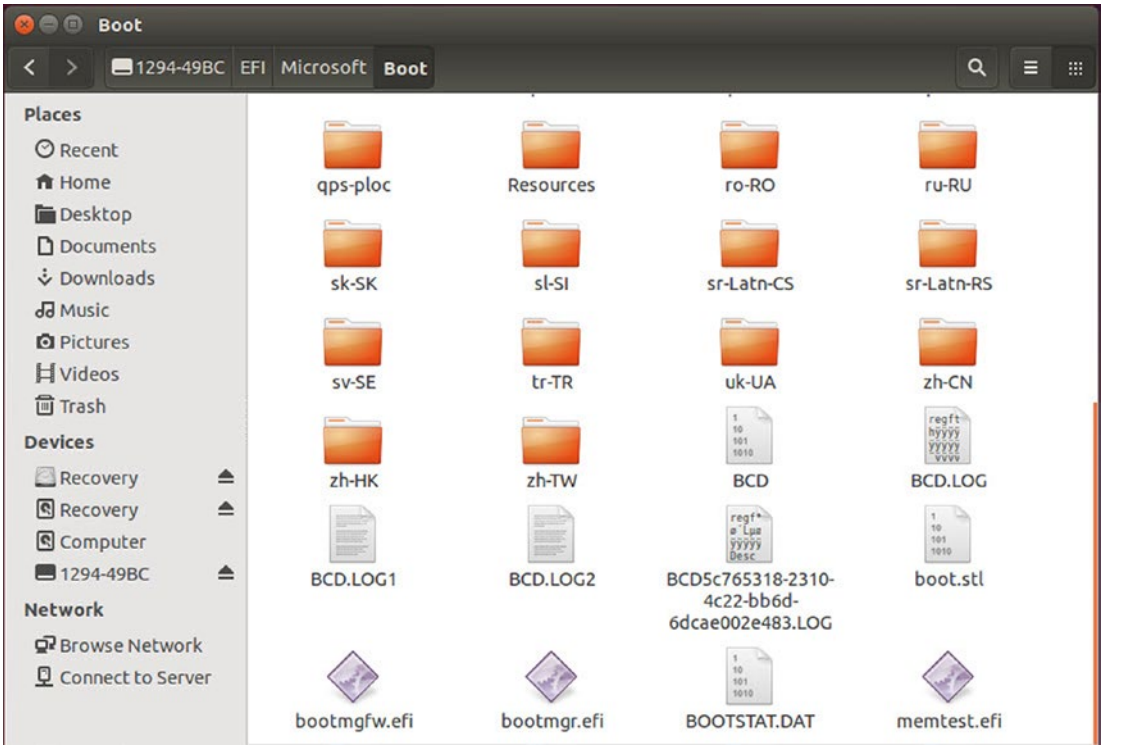


Figure 13-11. *UEFI systems have a three-partition structure, different from BIOS systems*

There are many Linux distros. I'm using Ubuntu here (`www.ubuntu.com`), but you could use another such as Linux Mint (`www.linuxmint.com`) or Red Hat (`www.redhat.com`); many come with disk and partition management tools such as GParted, seen in Figure 13-12. These can report on partitions and check them for errors, repairing those they find if possible. This can be a useful way to repair errors in the partition structure of your PC's hard disk.

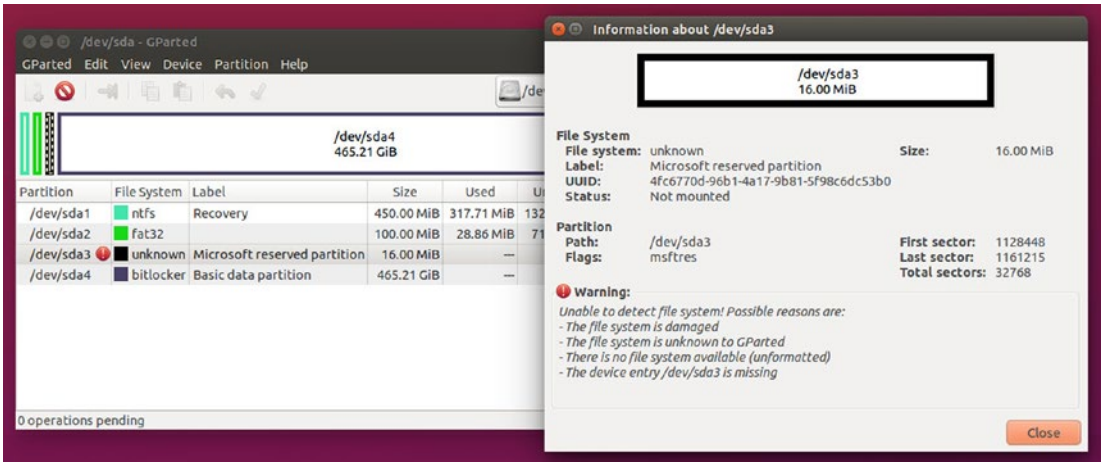


Figure 13-12. *You can get partition information and even repair partitions from Linux*

Summary

I really wanted to go all out to make this chapter as comprehensive as possible, simply because I know from the size of my mailbag how many people have problems with Windows startup, and just how easy it can really be to avoid a reinstall.

Startup isn't the only thing that can drive PC users "nutzoid," however. In the next chapter, I'll show you how to effect advanced repairs on your networking systems to maintain stable connections to your home devices, business servers, and the all-important Internet.

CHAPTER 14

Networks and Internet Connections

What use is a computer that doesn't have Internet access? It's odd to think that life wasn't always this way, though I do remember how frustrating it was that my early computers—be they a Sinclair ZX81, ZX Spectrum and QL, Psion Series 3, 3a, and 5 handhelds, or an Olivetti M240 8086-based PC—couldn't get access to each other let alone the wider world, and oh the problems I had using the earlier serial versions of Laplink. All this, of course, was before the World Wide Web (or even DARPANET as it was originally) was invented.

Now, it's impossible to think of a device that's not online, from tablets and watches to the refrigerator in your kitchen and even the radiators and air conditioners around your home. It boggles the mind really that I live on my own, but my router currently has 22 devices connecting to it, that's only the ones that are switched on, and I'm still planning on adding smart-home radiators and solar panels in the coming year. My washing machine is also able to connect to the Internet, though even I'm not daft enough to set that one up.

You'll be pleased to learn that this chapter is not a master class in how to connect your fridge to the Internet, I'm afraid you're on your own with that particular delight. What it is, though, is everything you need to know to troubleshoot and repair network connections to your company network and the wider world. Let's face facts: *nothing* is more annoying on PCs than not having an Internet connection, and we've reached the point with society that it can also be a significant barrier to productivity as well with so many company services, such as Microsoft 365, requiring online access.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_14

Checking the Status of a Network Connection

Troubleshooting any problem on a PC, especially one involving networking, is always a methodical process of elimination. Why do I say this? Well, a network problem isn't the same thing as a software compatibility issue as there are always external factors to consider as well. Let's take just one example to focus on, the humble Ethernet cable.

How many times have you, or someone else you know, pulled, tripped over, or damaged a network cable? For our laptops and tablets that now come equipped with fast Wi-Fi, that might be a thing of the past, but in a business environment, they are still de rigueur. If an Internet or network connection fails on a PC that's connected via Ethernet, my initial reaction is always to check the cabling first, to ensure that everything is plugged in securely and that the cable hasn't been pulled or snagged.

After that, it's a case of checking the Ethernet socket and/or the router or switch the cable is plugged into, to see if there's any problem or damage there. Third is to check any other PCs in the vicinity, connected via Ethernet or Wi-Fi (and smartphones count in this as well, though with their cellular connection it can sometimes be harder to tell for certain) if the problem is isolated to the single PC, or exists elsewhere on the network.

These three checks will quickly tell you if you need to go digging around in the PC's networking settings at all, and it's amazing how many times a network problem will be caused by an ISP (Internet Service Provider) issue or outage and people don't associate it with that. In a way it's the old story of the person calling IT support to report their computer won't switch on, and when asked to check the power cable says they can't see it because the power is out in the building, and it's all dark.

There's a quick and easy way to check the status of a network or Internet connection, and you can find it in the Network and Sharing Center (available through the Control Panel). At the top center of the window, you'll see details of your "active networks"; see Figure 14-1. To the right of each, and it's very likely there's only one listed, is a *Connections* link.

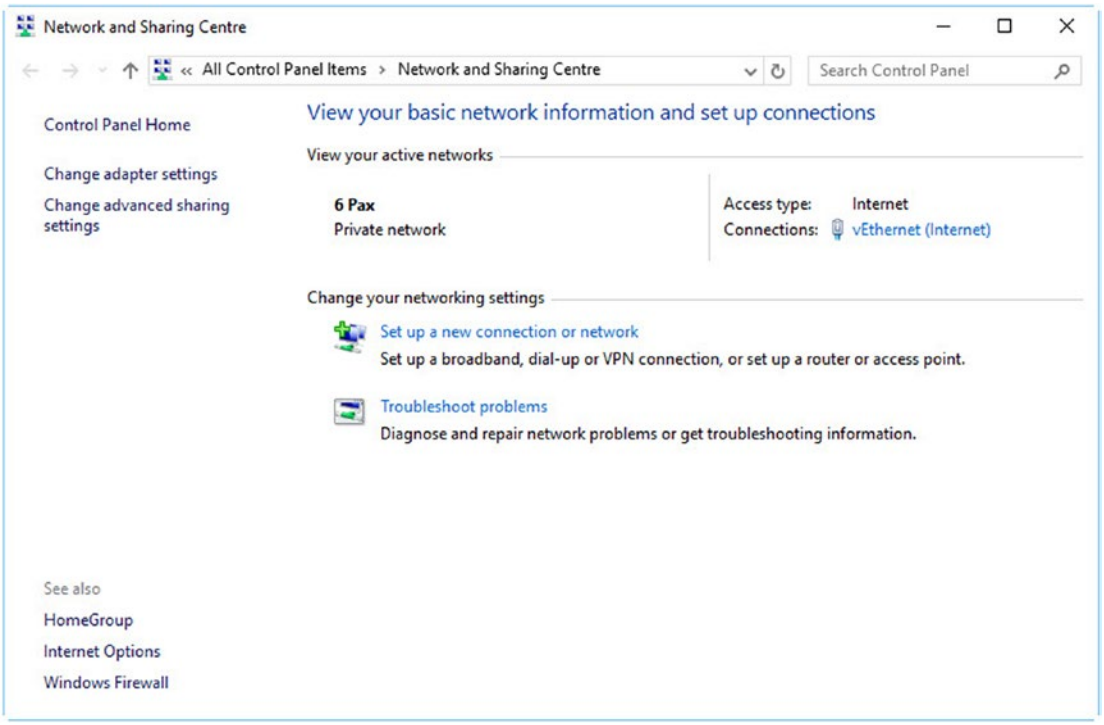


Figure 14-1. *You can check your network connection status in the Network and Sharing Center*

Clicking this connections link will display a status dialog for the network connection; see Figure 14-2. In the bottom half of this dialog is an Activity panel which will show you, in real time, the inbound and outbound packets of data. For a live connection, there will be an almost constant stream of small data packets, as the PC performs routine handshaking with the network. If there is no data passing through the network connection, or if the Sent and Received values register as zero, the network connection is definitely down.

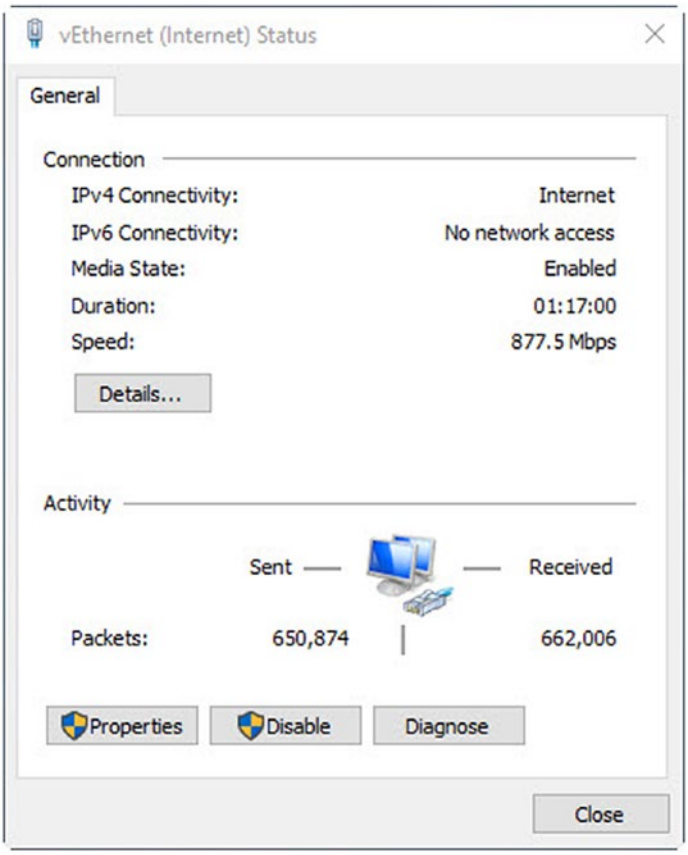


Figure 14-2. *The network status dialog will display real-time traffic information*

As with any detective work, troubleshooting and diagnosing problems with network connections requires some sleuthing. There is a huge amount of information available to you when it comes to networking, however.

From the Network Connection Status dialog, as detailed in Figure 14-2, click the *Details* button for data about your current connection. The dialog that will appear lists a great many useful details, including the name of the network adapter in use, your physical (MAC) address, your IPv4, and, if applicable, IPv6 address and details such as the default gateway, which is the address on your network of the router; see Figure 14-3. It may be that some of these details are incorrectly configured, and later in this chapter I'll show you how to fix them.

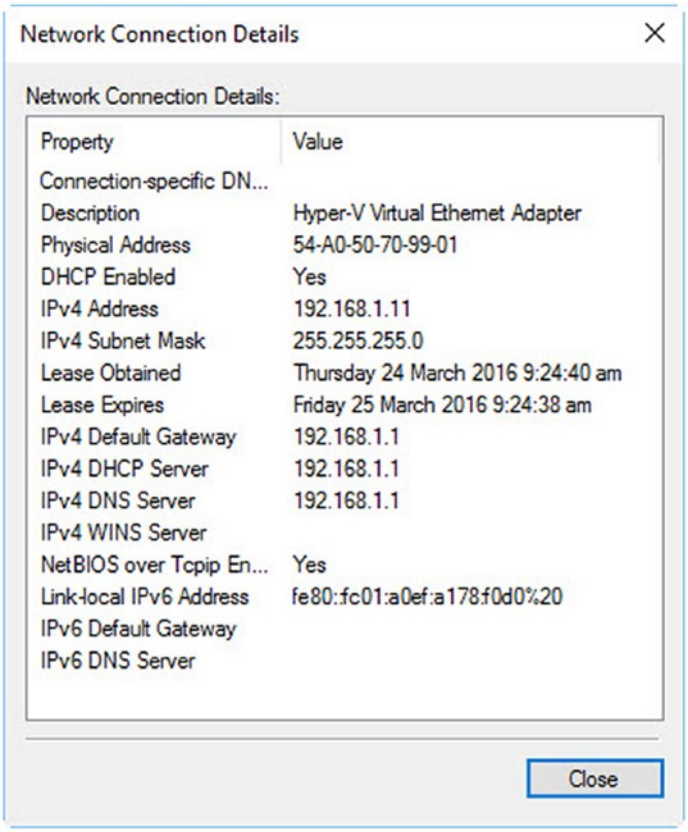


Figure 14-3. *You can get detailed information about the connection, including your IP address*

Back in the Network Connections Status dialog, click the *Properties* button to see which Windows and third-party services are available and enabled for the connection; see Figure 14-4. If you are having difficulty connecting to network shares or other PCs on the network, for example, you might find that the File and Printer Sharing service is not checked and thus not enabled for this connection.

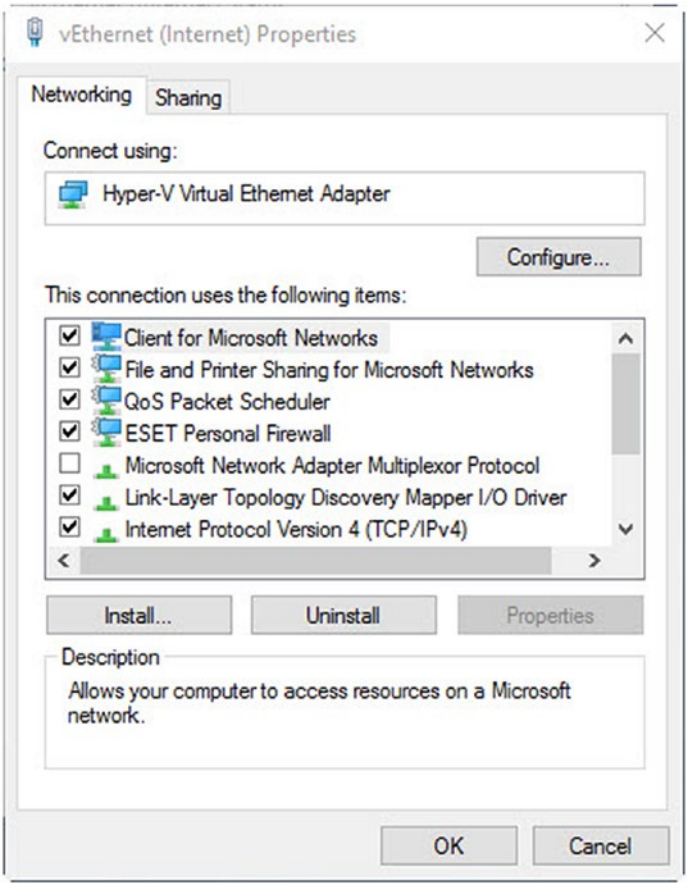


Figure 14-4. *You can check if appropriate Windows services are available for the connection*

You might also find that either the IPv4 or IPv6 connection isn't enabled. This could be because the PC, let's say it's a laptop or tablet, has been configured to work in a specific way on a secure company network, but when you connect to a network at home, as you're using the same network adapter, the settings you need are now incorrect.

Tip You can quickly fix some network problems at the Network Connection Status dialog by clicking the Diagnose button. This will run the automatic network troubleshooter, which will reset components to their default state, but one of the most popular methods for quickly repairing network connections, especially if there's a configuration problem, is to manually reset the TCP/IP networking stack in Windows. To do this, from the *Win+X* menu, open *Command Prompt (Admin)* and type the command `netsh int ip reset`.

In addition to the Network and Sharing Center, more networking controls have been included with the Windows 10 *Settings* panel, which is opened from its dedicated icon above the power button in the Start Menu. In Figure 14-5 you can see it's more aimed at a general user, with a button to display your *data usage*, but more advanced controls do exist here.

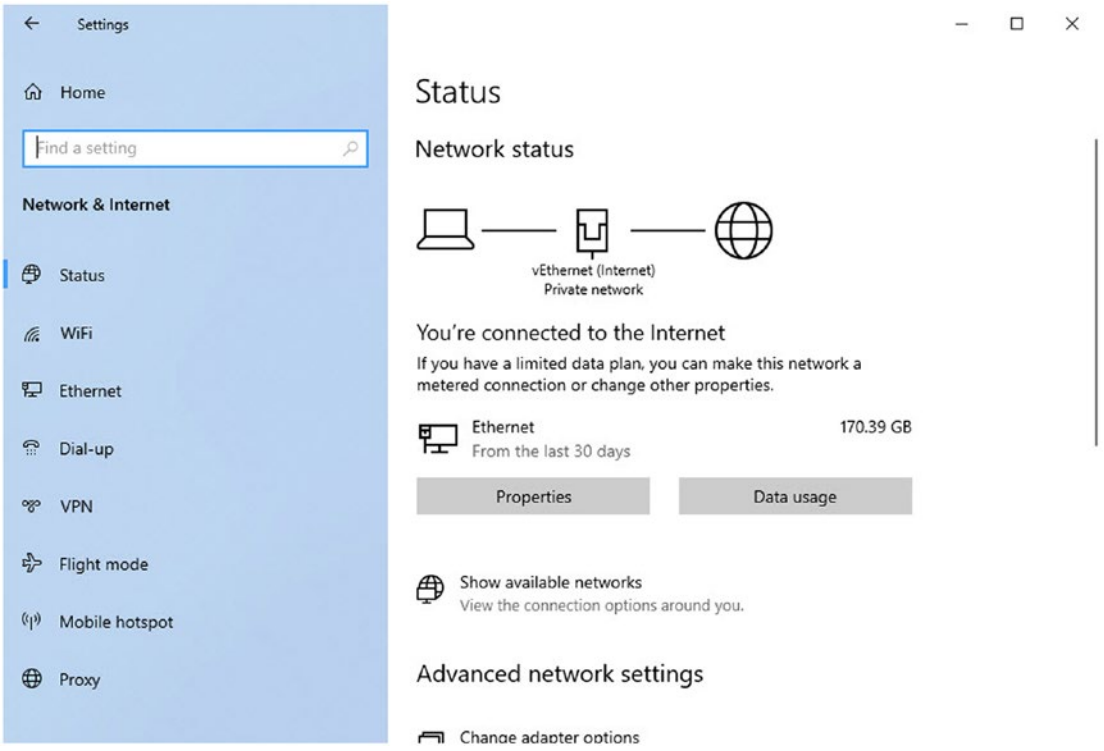


Figure 14-5. *You can find Network controls in the Settings panel*

Scrolling down the page and clicking the *View network and connection properties* provides the same information you can get from the Network and Sharing Center, but perhaps in a better organized and friendlier way; see Figure 14-6.

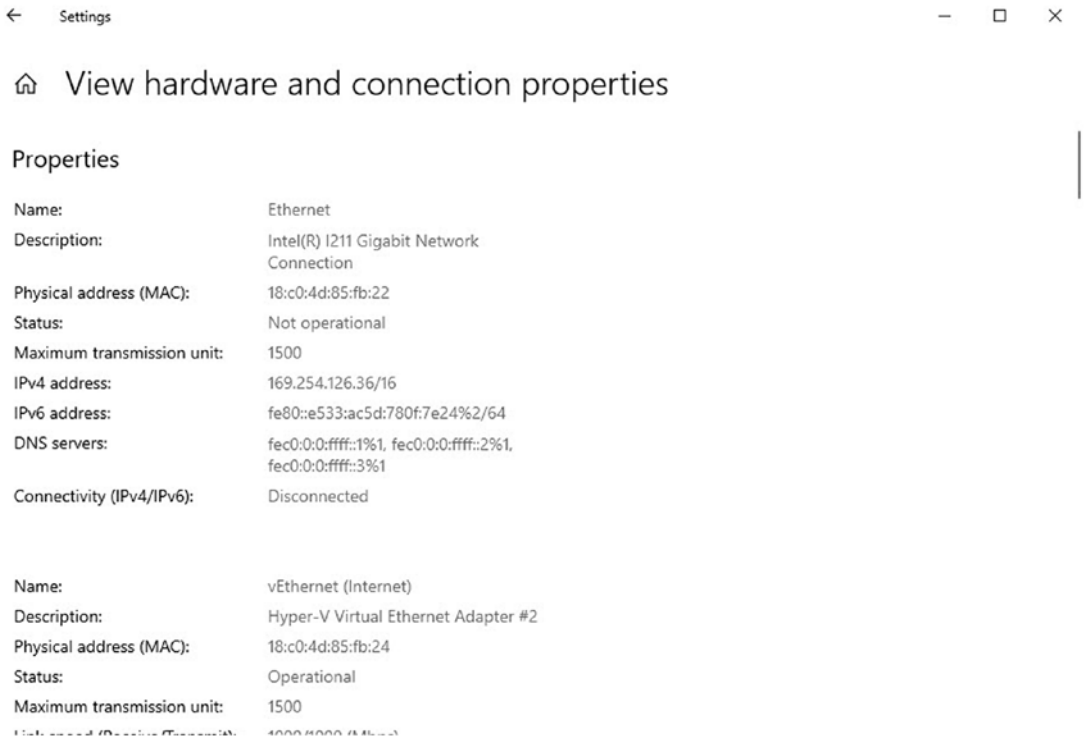


Figure 14-6. *You can get detailed network information from Settings*

Additionally, if you click the *Properties* button, you can get some limited control over the network settings, but at the time of writing (the Settings panel might have more functionality added at a later date), you can only change the connection to being *metered* (i.e., a cellular connection) and change the IP address between dynamically assigned (DHCP) and manually set; see Figure 14-7.

Figure 14-7. *The amount of control in Settings is still limited*

Displaying Information About Wi-Fi Networks

Jumping back to the more useful Network and Sharing Center, if the PC you are troubleshooting network problems for connects to the network by Wi-Fi, then opening the Network Connection Status panel will also reveal a *Wireless Properties* button; see Figure 14-8. Clicking this will reveal details such as the SSID name of the network (it's entirely possible the user is connected to the wrong network!), and if you click the security tab, you'll be able to see the security and encryption types that Windows 10 is using to connect to the network. You can check these against another working PC, or in the router settings, to ensure they are correct, as incorrect settings will cause a connection attempt to fail.

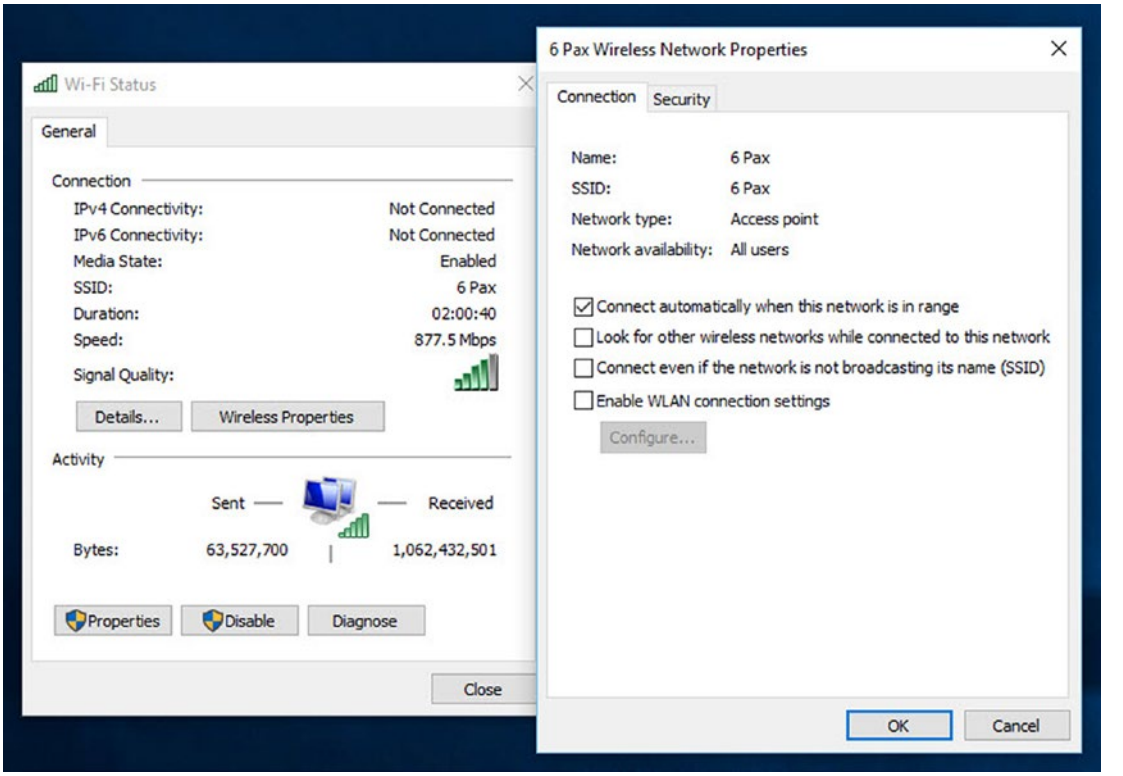


Figure 14-8. *Checking the details of a Wi-Fi connection additionally presents a Wireless Properties button*

Tip You can also discover the password for a Wi-Fi network in the Wireless Network Properties panel, under the Security tab, by checking the Show characters box for the Network Security Key. This will display the Wi-Fi password for the network to which you are currently connected.

Sometimes you want more advanced information about a wireless network, including perhaps even the password used to access a network to which you're not currently connected. The good news is that both are easily achievable. Simply open a *Command Prompt (Admin)* window to use the command **`netsh wlan show profiles name="network name" key=clear`**. Full details for the Wi-Fi network connection will then be displayed, including in the *Key Content field*, the password used to access that network; see Figure 14-9.

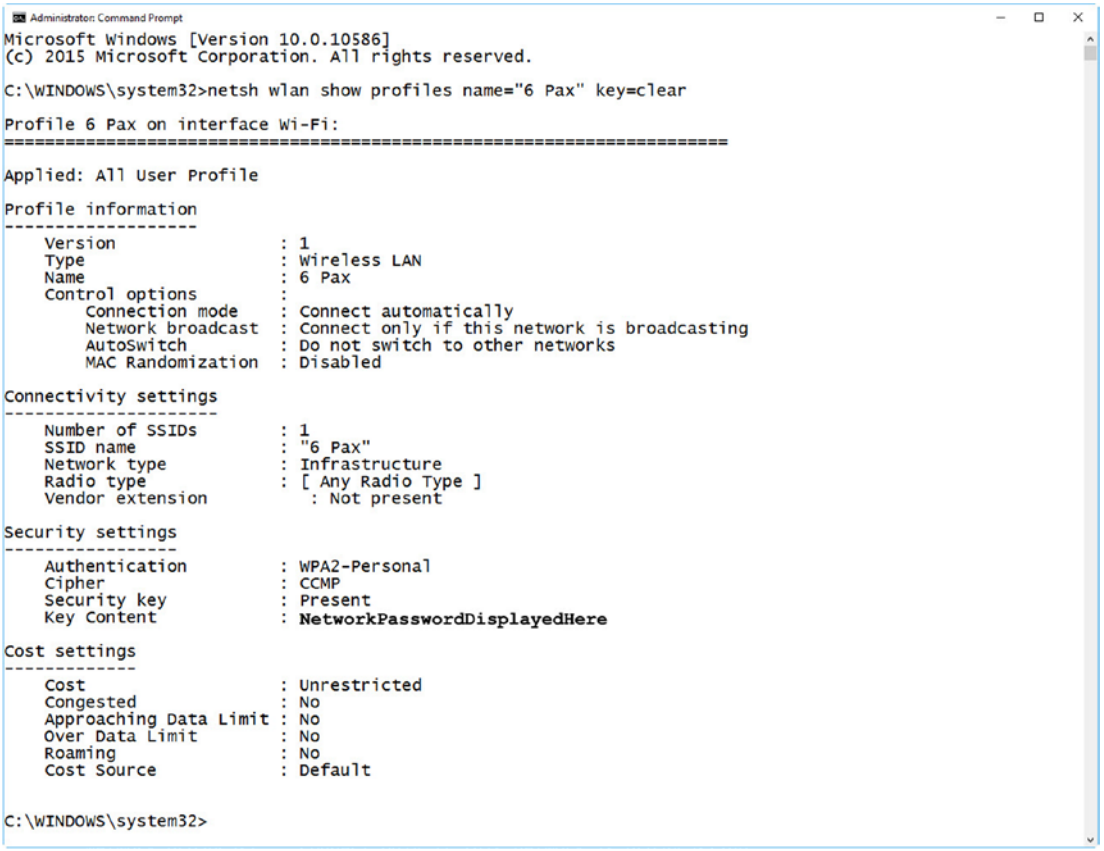


Figure 14-9. *You can discover a Wi-Fi network password with a simple command*

Additionally, using the **`netsh wlan show profiles`** command on its own will display a list of all the Wi-Fi network connection details stored on the PC; see Figure 14-10. You can use this to check if required network settings are in place, or if a network connection that should not be present is still there after a connection.

Figure 14-10. *You can display details of all the Wireless network details stored on the PC*

Prioritizing Wi-Fi Network Connections

Netsh is a hugely useful command, and I'll detail it in much more depth later in this chapter, but another of its most useful features is being able to set a connection priority order for Wi-Fi networks. By default, Windows 10 will automatically reconnect to the last network it was connected to, but your business or organization might have several Wi-Fi networks, and your own preference for which ones are used.

You can use the command `netsh wlan set profileorder name="network name" priority=1` and so on to manually set the connection order for a specific PC. Of course, all of this can be preconfigured as part of a PC's deployment using the scripting tools Microsoft provide for deployment and configuration.

Sometimes the settings for a Wi-Fi connection become corrupt, and you need to delete the profile and set it up again from scratch. This can be achieved within the Settings app, but can also be done from a *Command Prompt (Admin)* window with the command `netsh wlan delete profile name "network name"`.

Diagnosing Network Connection Problems

The Network and Sharing Center isn't the only place where you can find detailed information about the status of your network connection. The Task Manager, Resource Monitor, Performance Monitor, and Event Viewer can all provide detailed diagnostic and real-time data about the status of a network connection. I'll show you how to use these tools in depth in Chapter 25, except for the Event Viewer, which I detailed in Chapter 5.

I do want to focus a little more on the Event Viewer in this chapter, however, and show you how to get specific network status reports from it. Then, I'll show you how to get network-specific data from the Performance Monitor and Resource Monitor.

Getting Network Diagnostic Reports from the Event Viewer

If you *Create [a] Custom View* in the Event Viewer, you can choose from a variety of different networking logs of services from which to get reports; see Figure 14-11. These can include everything from "information," which will report, for example, when a successful connection is made or when there is a connection failure, to "warnings," "errors," and "critical [stops]."

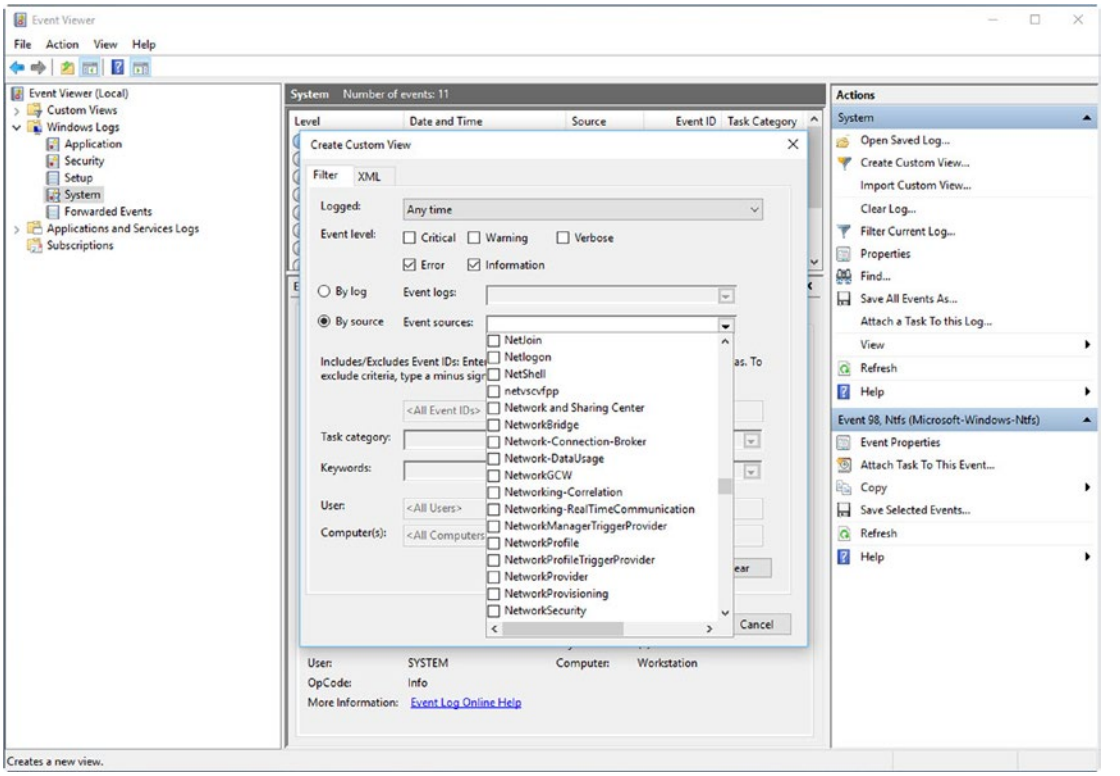


Figure 14-11. *You can receive reports of network errors in the Event Viewer*

Unless you are an experienced System Administrator, however, who *really* knows exactly what to seek for your specific problem, you can get connection reports from the Network-Connection-Broker, NetworkBridge (if you have used bridged connections), Network and Sharing Center, and more. To make things simpler, however, you can select reports "by log" and select "System [logs]" with the event ID **6100**; these will automatically include all the Network Diagnostics events filtered by the Event Level(s) you choose.

See the Status of Your Connection with the Performance Monitor

The Task Manager's Performance tab, which I'll detail more in Chapter 25, allows you to view your current overall network traffic. This can be broken down further, however, with the Performance Monitor, which I'll detail in full in Chapter 25. You can open the Performance Monitor from the Administrative Tools in the Control Panel, or by searching for it in the Start Menu or Cortana.

Clicking the green + icon at the top of the Performance Monitor window allows you to add counters that will be displayed in the main Performance Monitor view as a live bar graph. These include the number of bytes sent and received by the PC, including many other networking metrics; see Figure 14-12.

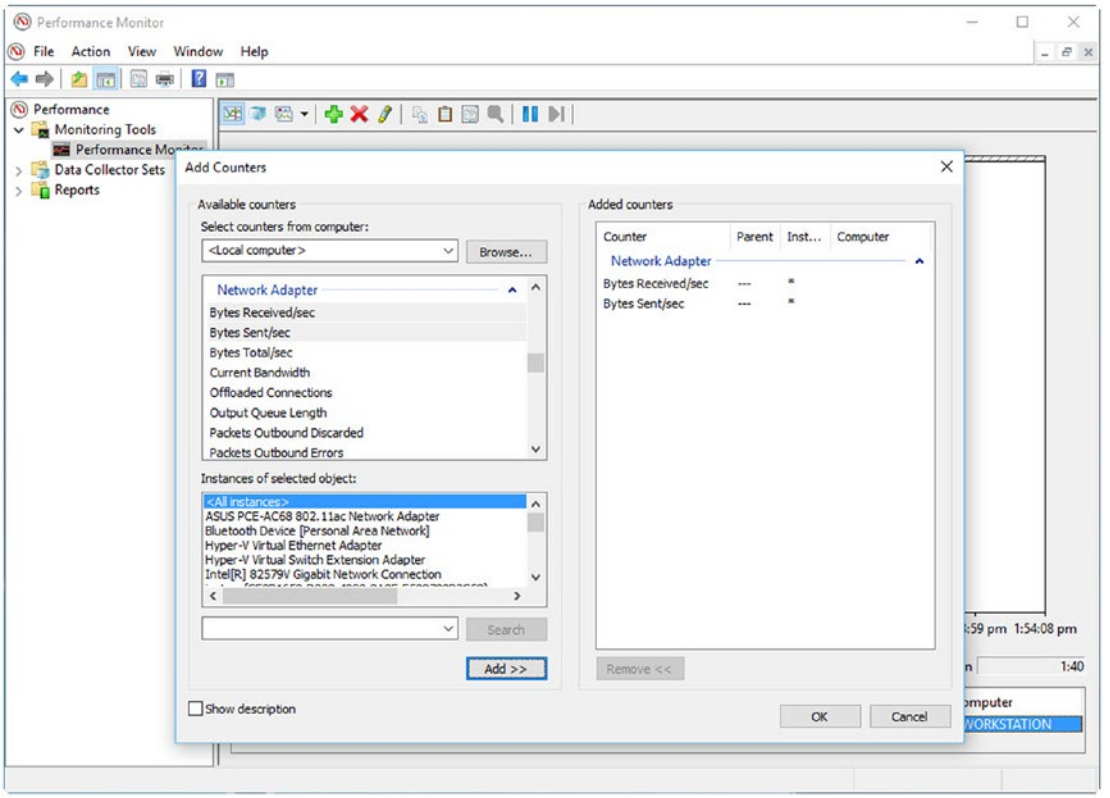


Figure 14-12. *You can get live network metrics from the Performance Monitor*

See What's Using Your Bandwidth with the Resource Monitor

Perhaps, though, you have a situation where you have a working and seemingly stable network connection, but nothing you try and do on that connection is working properly. Maybe activities are failing or timing out. In this circumstance, you need to know exactly what's using all your network bandwidth and why.

This is where the Resource Monitor comes in, which again I'll show you how to use in detail in Chapter 25. In short, however, it is split into four horizontal, collapsible panels. The Network panel, which is the one we're interested in here, shows you exactly what apps, services, and processes are using bandwidth, and exactly how much bandwidth they're using at any given time; see Figure 14-13.

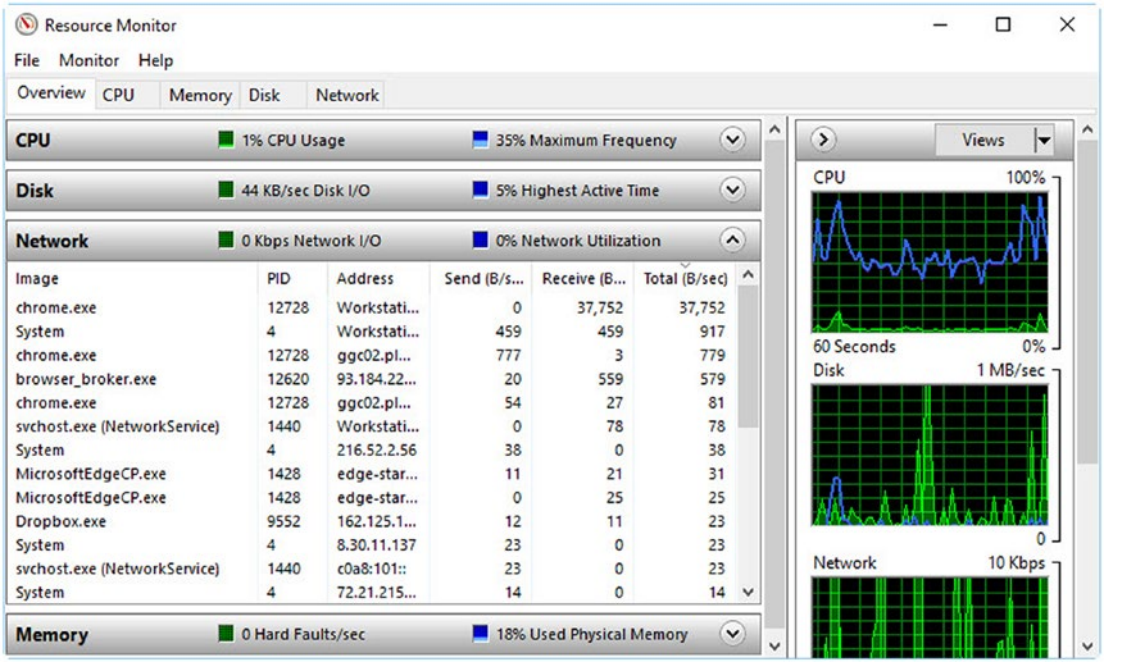


Figure 14-13. *The Resource Monitor can tell you what's using your bandwidth*

You may find that you have a runaway process, maybe an app updater, a poorly coded app, or perhaps even malware on the PC, which is consuming large amounts of network bandwidth, and maybe even swamping your Internet connection. In the preceding example, you can see that Chrome is using the most bandwidth (it's playing relaxing chillout music from YouTube, which I like to listen to while writing these books, should you be interested in such things), and we can see other apps such as Edge and Dropbox using bandwidth as well.

If there was anything here we didn't recognize, however, perhaps because it's a malware process, we can search for the name of the process online. You do this in Task Manager, under either the Process or Details tab, by right-clicking the process and selecting *Search online* from the menu that appears; see Figure 14-14.

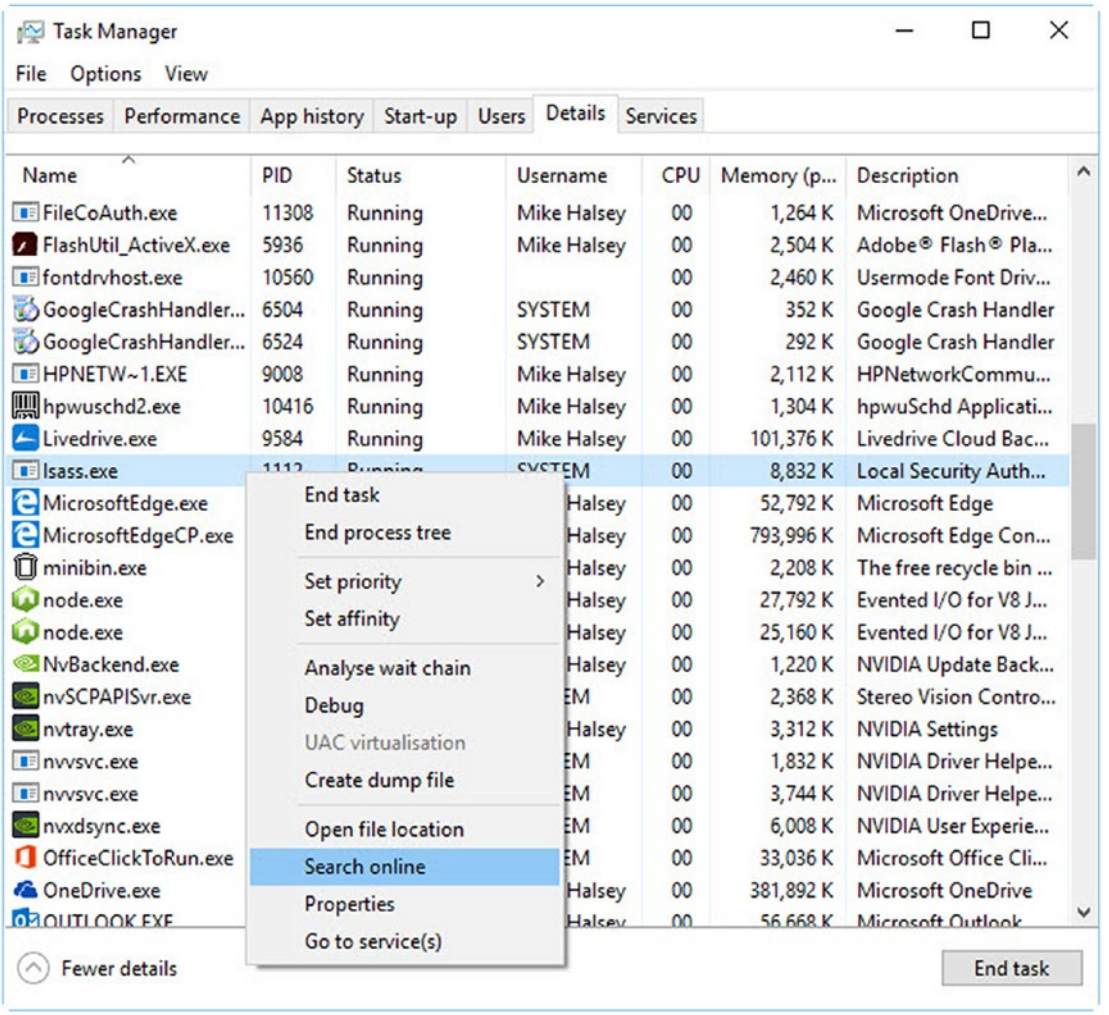


Figure 14-14. *Task Manager lets you search for process details online*

Troubleshooting in the Network and Sharing Center

The Network and Sharing Center, accessed from the Control Panel, isn't just a place for Windows to display information about your current network status, as it also contains useful configuration options you might need when troubleshooting a problem. In the top left of the Network and Sharing Center window are two links, *Change Adapter Settings* and *Change Advanced Sharing Settings*. We'll look at the second one of these first.

Occasionally, the sharing settings for a PC might be changed (perhaps by the user accidentally). These settings, however, don't just affect file and folder sharing, but they also affect discovery for other PCs, and network hardware, and for the discoverability of that PC by other hardware and systems on the network.

If you click the *Network* link in File Explorer, Windows 10 is extremely good at prompting you that Network Discovery is switched off, if it's unable to see any other PCs on the local network. Obviously, however, you won't get this message from other PCs that can't see the one on which Network Discovery is deactivated.

The Advanced Sharing Settings panel is split into three main collapsible sections: Private, Guest or Public, and All Networks; see Figure 14-15. Additionally, in a corporate environment, you may see an additional option here for your Business Network.

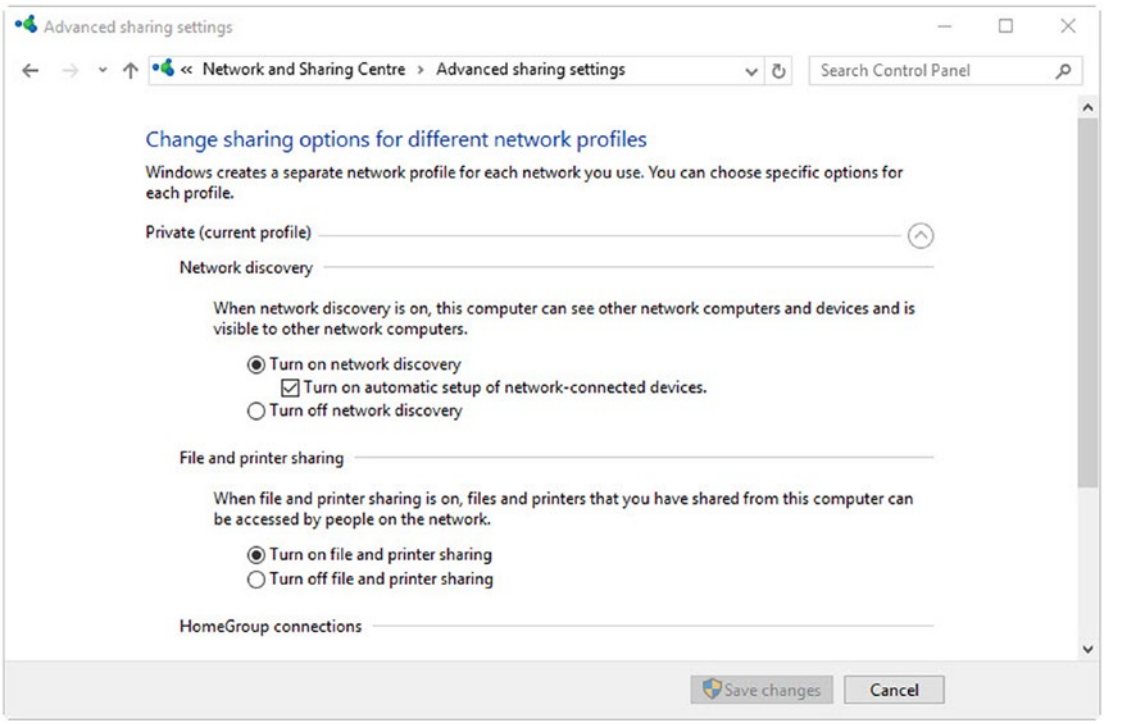


Figure 14-15. *The Advanced Sharing Settings control discoverability as well as sharing*

This is where the settings can occasionally become confusing for a user, because they might say, for example, that they can see all the network storage and devices on their laptop in the office, but not at the remote site they need to visit. This would be because

the worker has connected to the network at the remote site by assigning it a different network type. By this I mean that when you connect to a network in Windows 10, a dialog will appear near the top right of your screen asking if you want to be able to see other PCs on the network, and have them see you. This is exactly the sort of information dialog that people don't read, and where they'll just click one button or another. Consequently, it's all too easy to set the network as Public (can't see the network) when you had intended for it to be marked Private (can see PCs).

I'll show you how to change the network type shortly, but in the Advanced Sharing Settings panel, you can change the individual settings for Network Driver and File and Printer Sharing, for each individual network type by checking the appropriate options. Additionally, the Public network type includes file sharing encryption options. If file sharing is not working correctly on a PC, it may be either that this encryption is disabled (it's enabled by default) or that the setting is configured incorrectly for the security policies on the PC or on the network.

Changing a Network Type Between Private and Public

There are three ways to change a Wi-Fi network connection between Public and Private, and you might want to do this because, as has happened to me in a local pub, the landlord didn't want to give away the Wi-Fi password so typed it into my PC and then hit the *Yes* button when asked "Did [I] want to see other PCs…" before I could stop him. Clearly, this was a Public network, and I didn't want my laptop being seen by any other PCs that were also connected.

The simplest way, from a user perspective, is to go to the Settings app, open the *Network & Internet* section, and under the *WiFi* section, click the *Manage known networks* link. This will display a list of all the Wi-Fi networks that are known to the PC. You can click the *Properties* button for any network to display an option to change it from a public to a private network; see Figure 14-16.

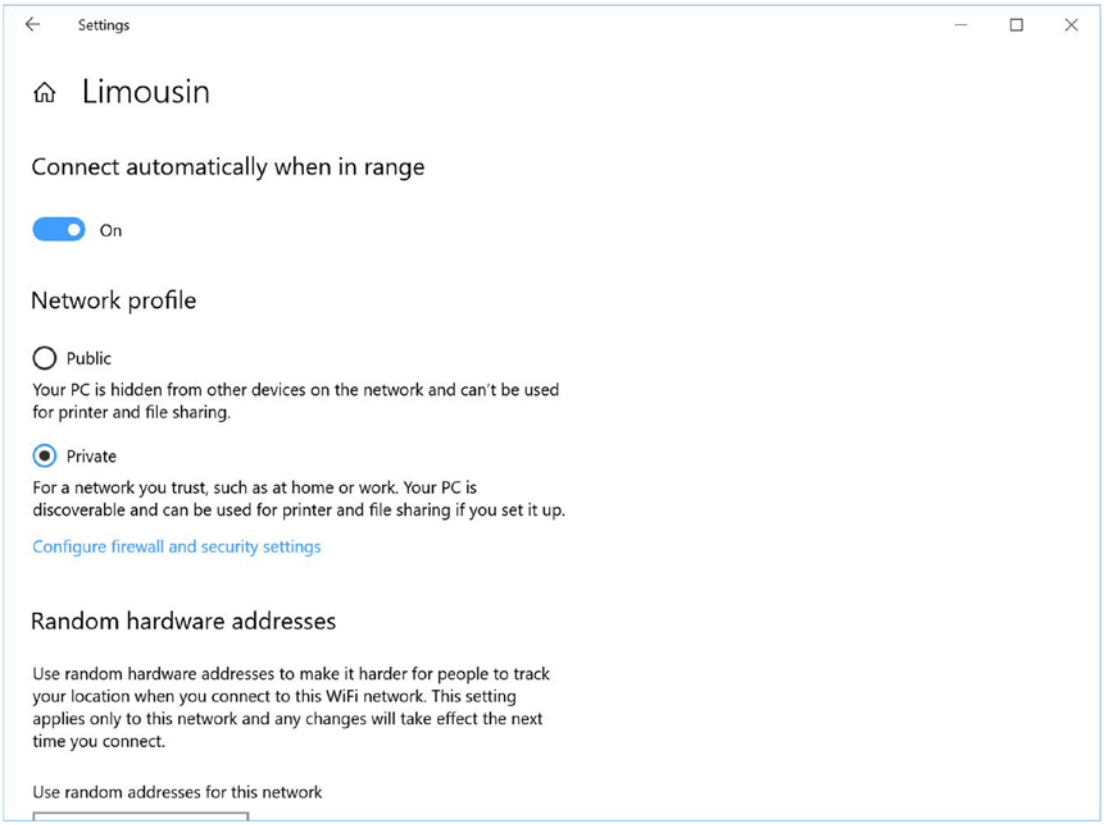


Figure 14-16. *You can change networks between public and private*

The other methods of changing the network type require Group Policy and the Registry Editor, and so you might want to perform this change yourself, onsite or via remote access. Both changes will require a restart to take effect, so Remote Access is a good option.

To change the network type using the Group Policy Editor, open Group Policy by searching for **gpedit** in the Start Menu and navigate to *Computer Configuration* ➤ *Windows Settings* ➤ *Security Settings* ➤ *Network List Manager Profiles*. This will display the name of the current Wi-Fi network, which you can double-click to open its properties. In the Properties dialog, click the *Network Location* tab, and then you can forcibly change the location type to either Public or Private; see Figure 14-17.

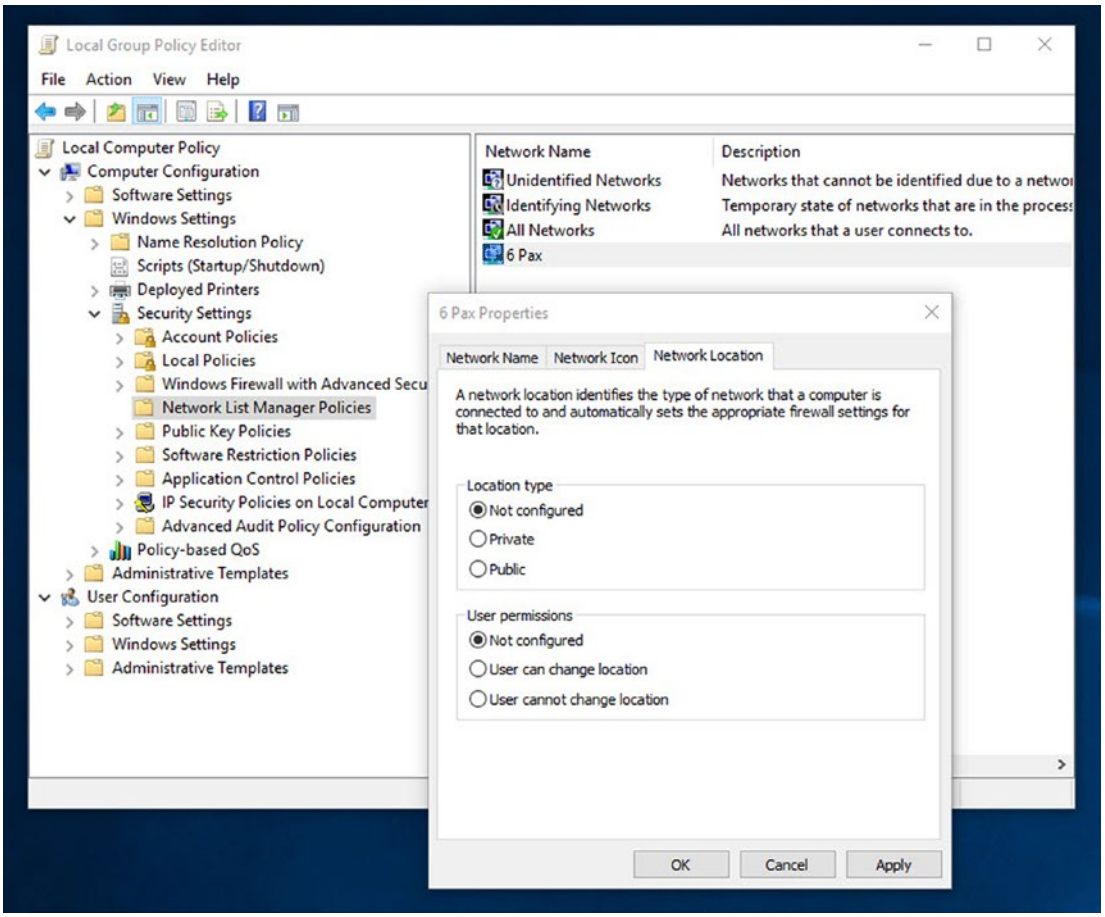


Figure 14-17. *You can change the network type in Group Policy*

If the PC is not running the Pro or Enterprise edition of Windows 10, you won't have access to the Group Policy Editor. The network type can still be changed, however, in the Registry Editor. I'll show you how to use the Registry Editor in full in Chapter 26, but you should always create a backup copy of the Registry before making any changes.

To open the Registry Editor, search for **regedit** at the Start Menu, and when the Registry Editor window opens, click the *File* menu and the *Export* option. This will export a full backup copy of the Registry that can later be restored using the *Import* option if need be. To change the network type, in the left panel of the Registry Editor, navigate to *HKEY_LOCAL_MACHINE* ➤ *Software* ➤ *Microsoft* ➤ *WindowsNT* ➤ *CurrentVersion* ➤ *NetworkList* ➤ *Profiles,* and look for the profile that has the *ProfileName* tag with the correct Network SSID; see Figure 14-18.

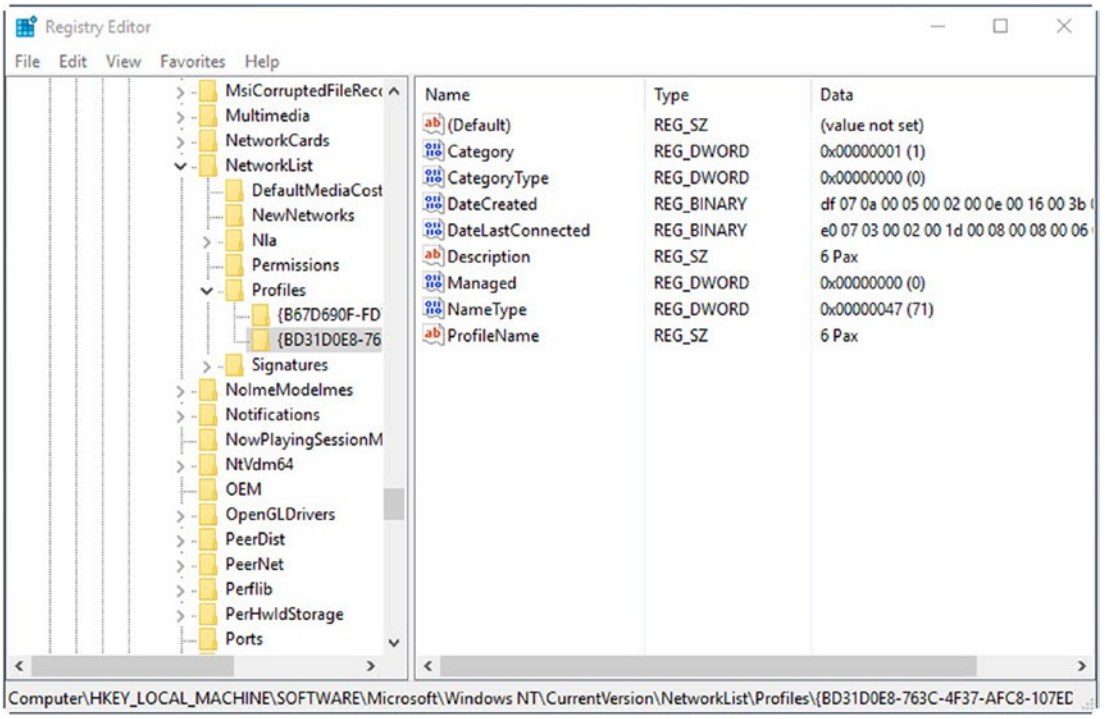


Figure 14-18. *You can change the network type in the Registry Editor*

To change the network type, double-click the *Category* value and change its value to **0** (zero) for a Public network, or **1** for a Private network. You will then, for both the Group Policy and Registry change, need to restart the PC for the change to become effective.

Setting Advanced Network Configuration Options

Sometimes you need to change advanced network configuration options on the PC, perhaps because the IPv4, IPv6, or Default Gateway settings are incorrect. In the Network and Sharing Center, click the *Change Adapter Settings* link (this is also available by clicking *Network Connections* in the Win+X menu), and double-click the network adapter you need to make changes to. In the dialog that appears, click the Properties button to open another dialog in which you can view, manage, and change the network properties for the adapter; see Figure 14-19.

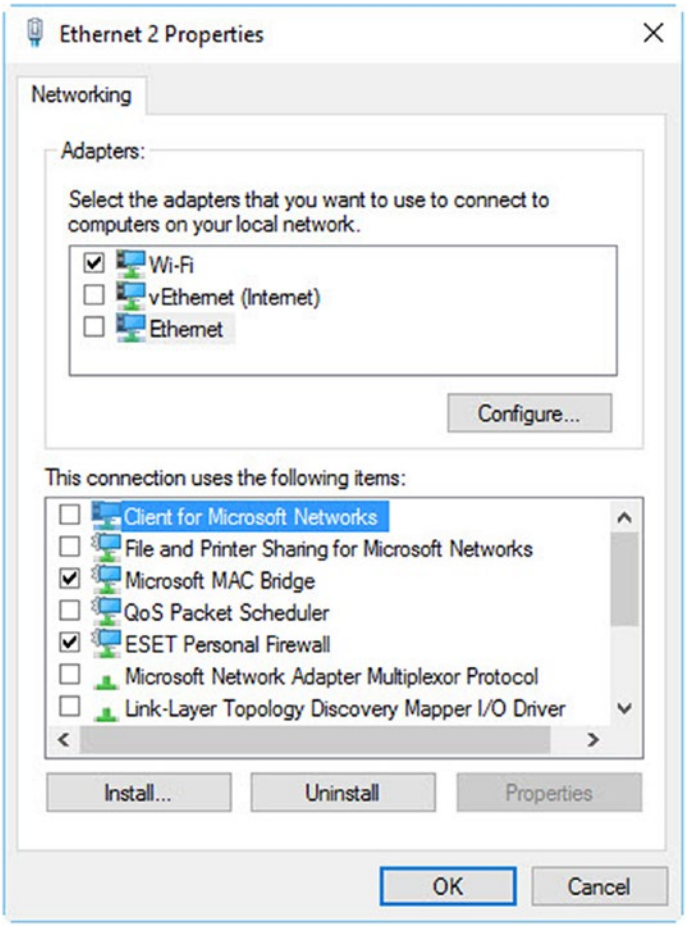


Figure 14-19. *The Network Adapter Properties dialog is where you configure network settings*

In the *This connection uses the following items* panel, you will see a list of the Microsoft and third-party network services used by the adapter. Some will be checked, and some won't. You might find that *Client for Microsoft Networks*, which is required for access to Domains and other Microsoft network systems, and *File and Printer Sharing* are not enabled. Should this be the case, as in Figure 14-20, it's not always necessary to enable them as, in this case, the PC uses Hyper-V with the virtual machines able to connect to the local network and the Internet. This Ethernet 2 connection is a virtual adapter, created by Hyper-V and bridged with the PC's main Wi-Fi adapter.

When it comes to configuring network options, however, it's the *Internet Protocol Version 4 (TCP/IPv4)* and *Internet Protocol Version 6 (TCP/IPv6)* options we'll want to configure, as these determine how the PC connects to the network.

If you highlight the IPv4 service and click its *Properties* button, you will be able to configure its IP address and DNS (Domain Name System) options; see Figure 14-17. By default, these are assigned automatically when the PC handshakes with the router. On your network, however, you might require each PC to have a static IP address, or to connect to the Internet that has a nonstandard DNS address.

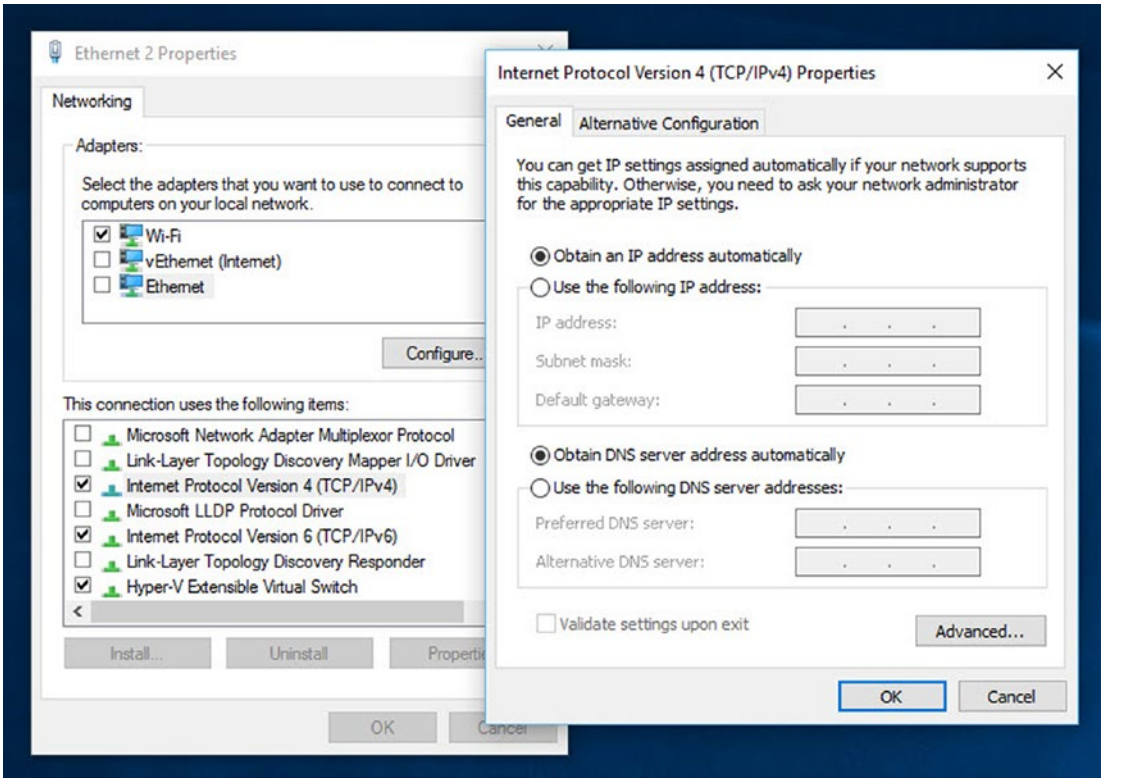


Figure 14-20. *You can set IP and DNS addresses for the IPv4 connection*

The Alternative Configuration tab also allows you to set separate IP and DNS settings for when the PC is connected to other networks, such as for a laptop or tablet that's used in multiple locations such as the office and the user's home.

Clicking the *Advanced* button also allows you to set additional options, such as multiple DNS addresses (if different DNS settings are used for different routers in business locations), or if a different default gateway (also related to the router configuration) needs to be set for the PC to be able to access the network, and its files and resources.

The IPv6 properties allow you to set very similar options except that there is no Alternative Configuration option (see Figure 14-21), and the Advanced options do not support the WINS (Windows Internet Name Service) protocol.

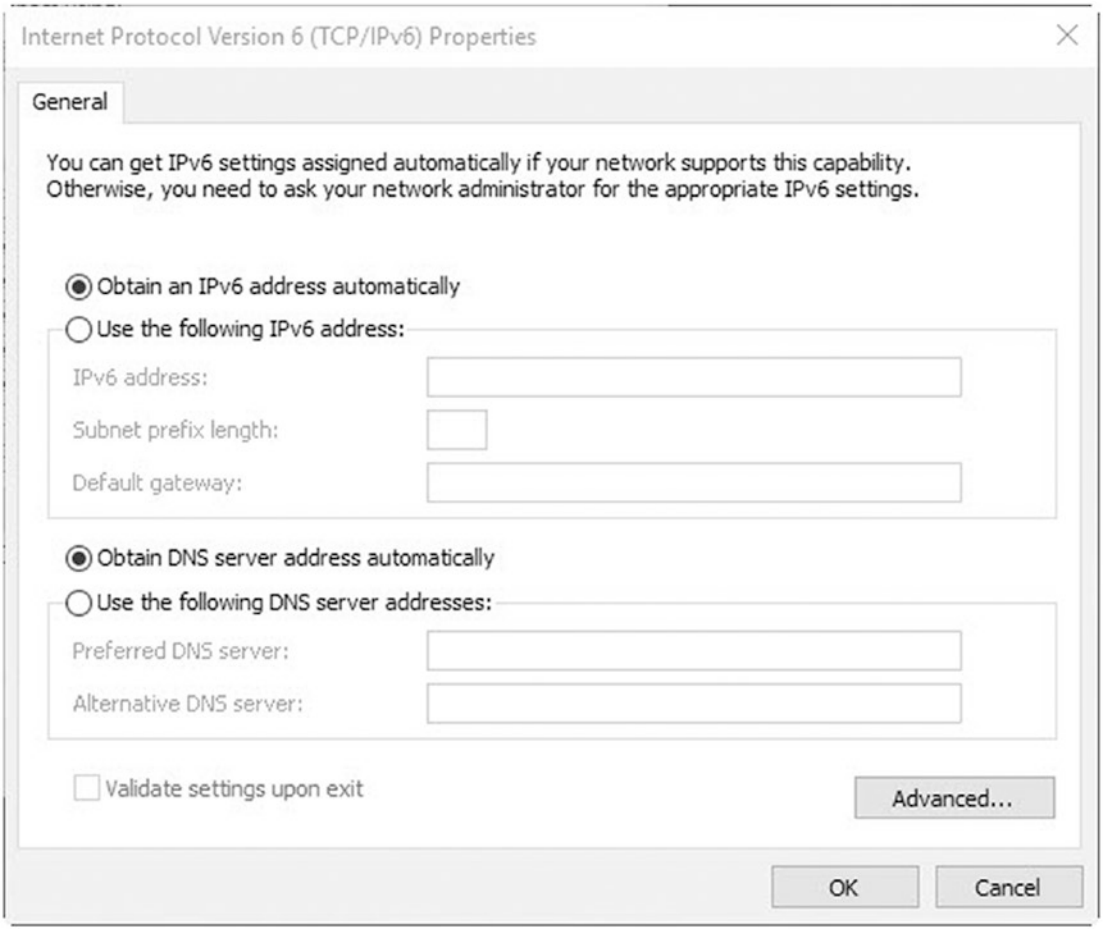


Figure 14-21. *The IPv6 settings do not offer an Alternative Configuration panel*

Note You might be wondering what the difference is between a DNS address and the default gateway when connecting to your network. In short, the default gateway is the network address of the main router (usually 192.168.0.1), though this may be set to a nonstandard address for reasons of security and network

stability. A DNS address is used by your ISP to enable a connection to the Internet. Again, for reasons of security, or sometimes because an ISP has a "walled-garden" approach to Internet connections, this might be a nonstandard setting you will need to configure manually.

HOSTS, LMHOSTS, and WINS

Hidden away not just in the recesses of Windows, but in every operating system from iOS to Android, is a little file called **hosts**. You will find it in the **`%windir%\System32\drivers\etc`** folder, and it is used to map hostnames (on your local network, intranet, or domain names) to specific IP addresses online or on your own network; see Figure 14-22.

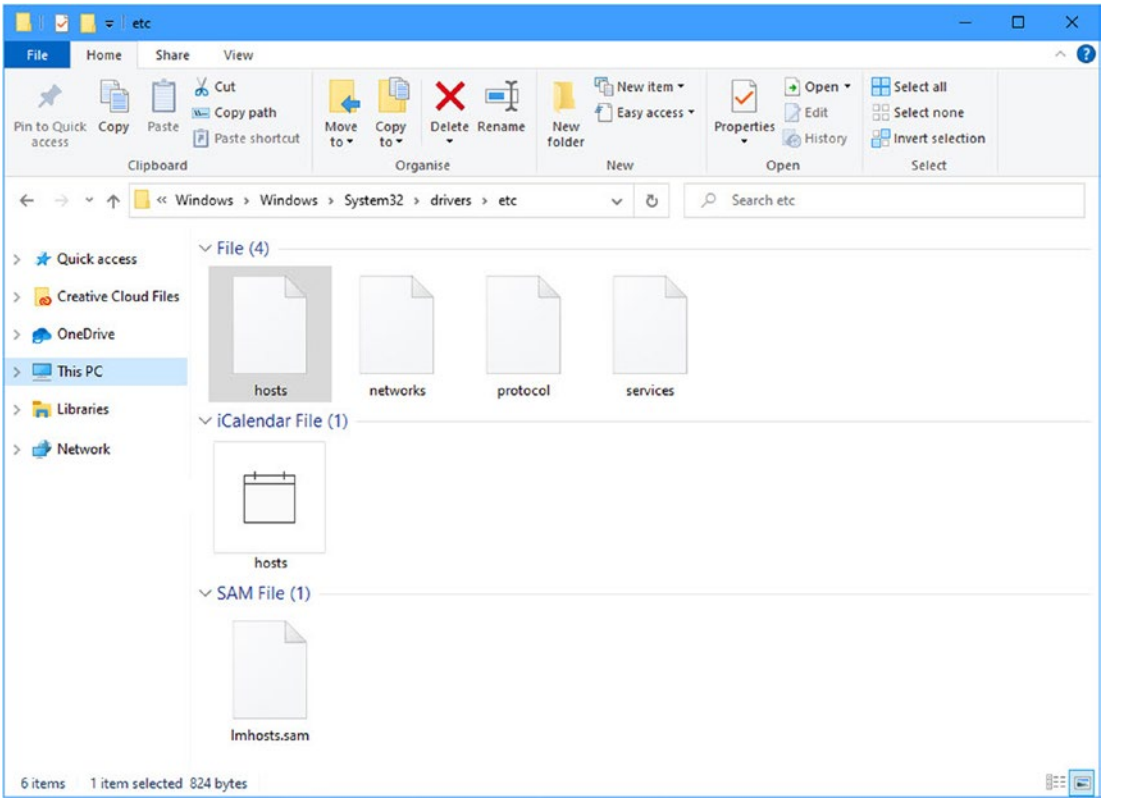


Figure 14-22. *The Hosts file is part of all operating systems*

Hosts file isn't commonly used on modern operating systems, as the Domain Name System (DNS) takes care of name resolution, the mapping it hostnames to IP addresses online, but for some legacy and mission-critical systems, you might find it useful for making sure that a specific local or Internet address always lands in the correct place. For example, it's a common trick to use the hosts file to point websites such as Facebook and Amazon to the IP address 0.0.0.0 to prevent people on the PC from being able to visit them. You can open the Hosts file with Notepad, as it's plain text, and here you can add specific entries to map a local or IP address with a specific host; see Figure 14-23.

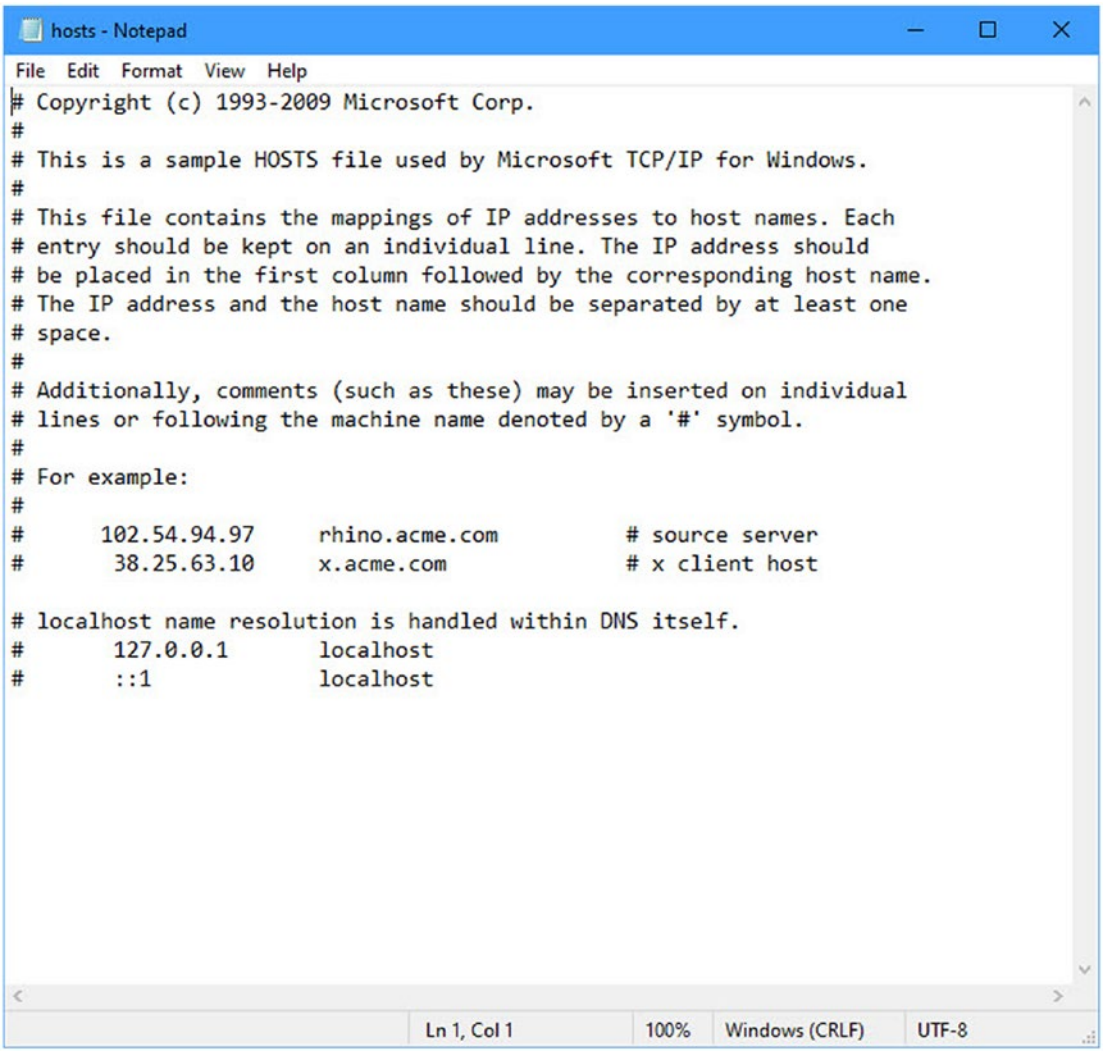


Figure 14-23. *The Hosts file is plain text and can be opened in Notepad*

Also in the same folder is the **LMHosts** file which, despite its different file suffix, can also be opened in Notepad. LMHosts (LAN Manager Hosts) can be useful if you need to connect to legacy operating systems on mission-critical PCs in your workplace, as it can resolve specific IP addresses to computernames using the older, and not used anymore, Microsoft NetBios system; see Figure 14-24.

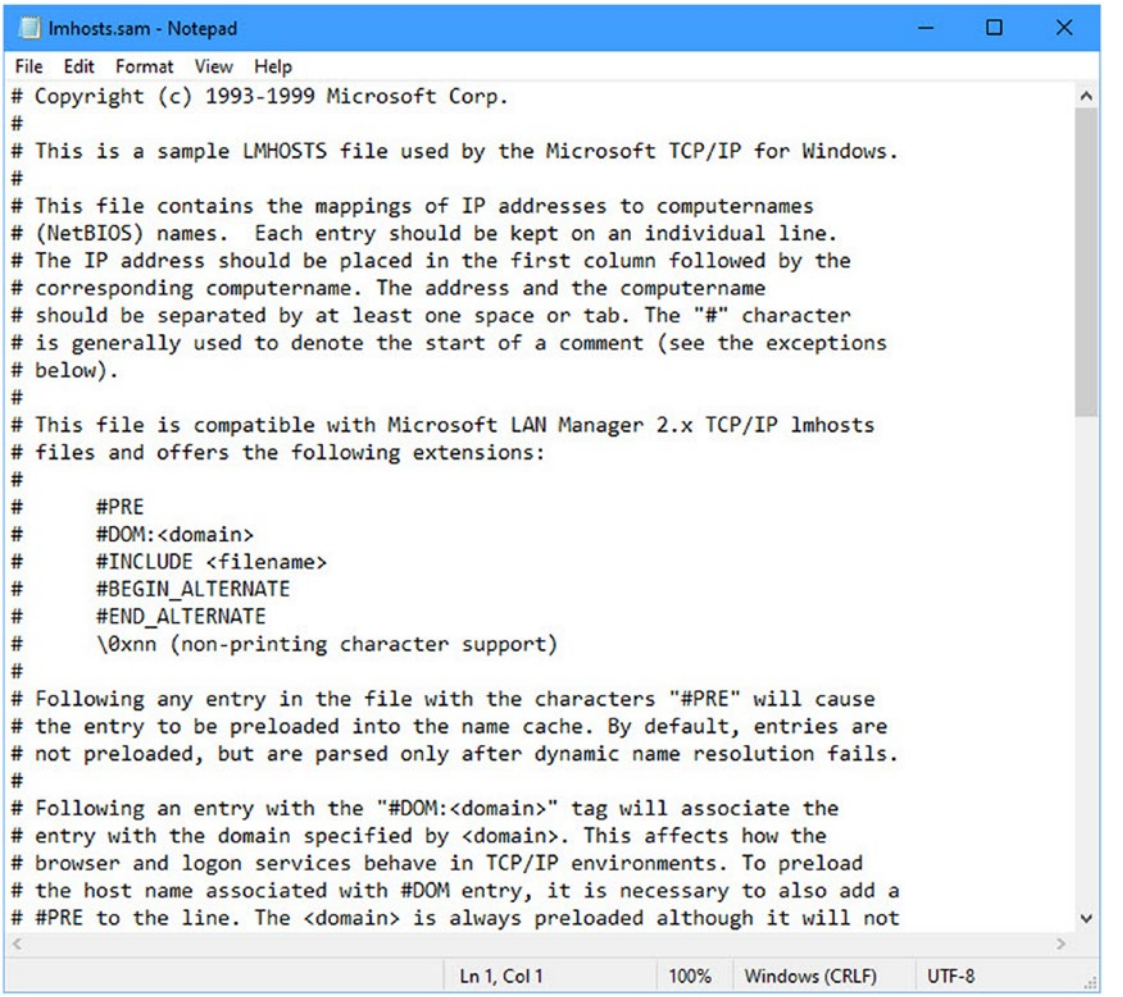


Figure 14-24. *The LMHosts file can also be opened in Notepad*

WINS (Windows Internet Name Service) was Microsoft's own answer to DNS and isn't used any more. It does still exist in Windows however for networks in case you need to connect to older Windows 95, Windows 98, or Windows Me PCs which are performing mission-critical tasks. You can access WINS for IPv4 networks (it's not supported for

IPv6) from the Network and Sharing Center by opening the network adapter status, clicking *Properties* and then selecting *Internet Protocol Version 4 (TCP/IPv4)*, clicking the *Properties* button in that panel, and in the next dialog, clicking the *Alternate Configuration* tab; see Figure 14-25. Microsoft has a resource online about WINS which you can find at `https://pcs.tv/2eRhWdn`.

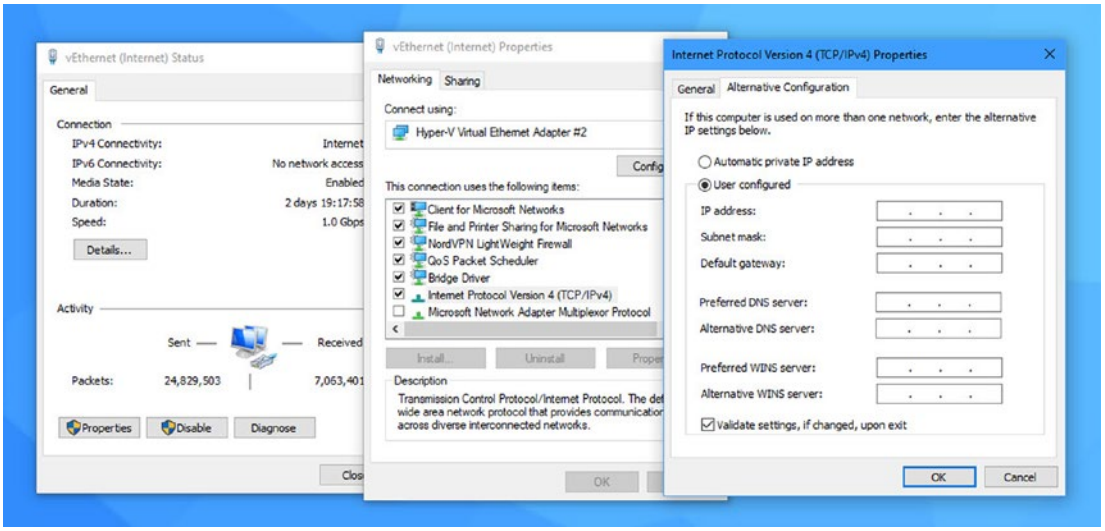


Figure 14-25. *You can configure WINS settings for IPv4 connections*

Troubleshooting TCP/IP Connections

There are several tools built into Windows 10 to help you troubleshoot and repair problems with TCP/IP connections, and these vary from very basis to highly configurable. I want to spend a little time looking at these tools.

Ping

Ping is one of the most basic commands when it comes to troubleshooting networking. Named after the "ping" sound sonar makes when used from a submarine in war movies, it works in a broadly similar way, sending out packets of data to a source and waiting to see how long it takes for a return signal to be received. Though I am not suggesting that if the connection to your NAS drive goes down, you proclaim across the office "You sunk my battleship!"

In its simplest form, you use it from a Command Prompt window in the format **ping 10.0.0.8** in the case of an IP address (see Figure 14-26), where I am pinging my own NAS drive (I wasn't worried), or **ping** `www.apress.com` to determine a connection to an Internet server.

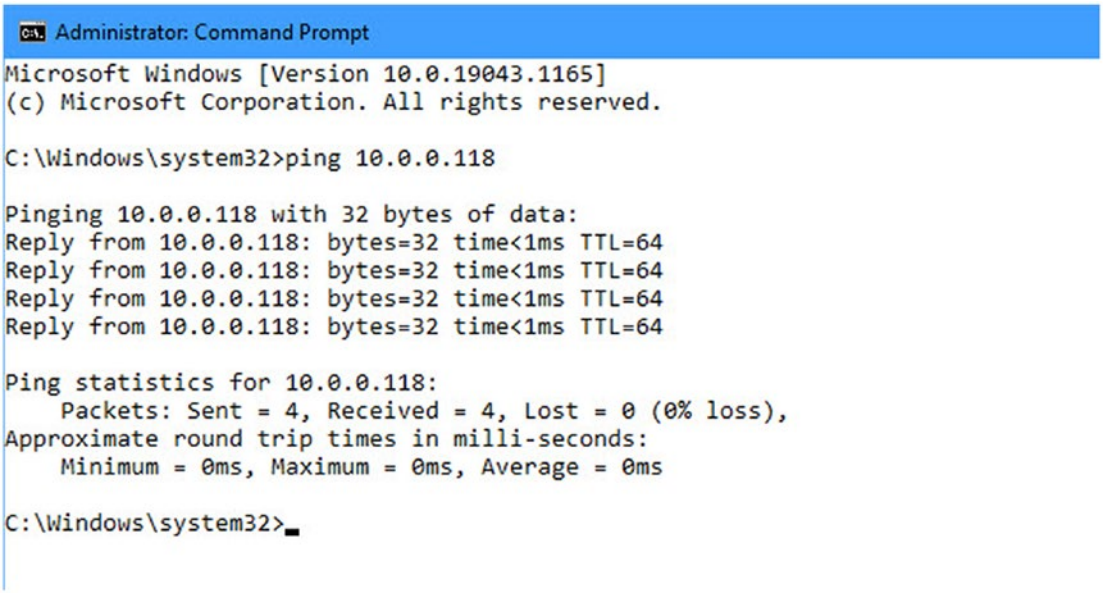


Figure 14-26. *Ping is used to determine the status of a network connection*

There are switches you can use with ping however you might find useful, and these can be found in Table 14-1.

Table 14-1. *Switches for use with ping*

Switch	Description
-t	Continue pinging the specified host until stopped. To interrupt and display statistics, press Ctrl + Enter or to interrupt and quiet press Ctrl + C
-a	Use reverse name resolution for a destination IP address, if successful ping will display the corresponding hostname
/n <count>	Set the number or echo requests to be sent (the default is 4)

(*continued*)

Table 14-1. (*continued*)

Switch	Description
/l <size>	Specifies the length in bytes of the data sent in echo requests, the default is 32; the maximum is 65527
/f	Specifies that the echo requests should not be fragmented by servers on path to the destination, useful for troubleshooting Maximum Transmission Unit (MTU) problems
/l <TTL>	Specifies the Time to Live (TTL) field in the IP header for echo requests
/v <TOS>	Specifies the Type of Service (TOS) field in the l{ header for echo requests (IPv4 only)
/r <count>	Used to record the route taken by the echo request (IPv4 only), you can specify the number of hops between the source and destination from 1 to 9
/s <count>	Specifies that the Internet Timestamp should be used to record time of arrival for each request and its reply, from a maximum of 1–4
/j <hostlist>	Specifies requests should use the Loose Source Route option in the IP header with the intermediate destinations specified (ipv4 only) with a maximum of nine addresses specified and separated by spaces
/k <hostlist>	Specifies requests should use the Strict Source Route option in the IP header with the intermediate destinations specified (ipv4 only) with a maximum of nine addresses specified and separated by spaces
/w <timeout>	Determines the amount of time in milliseconds to wait for a reply, the default is 4000 (4 seconds)
/R	Specified a round-trip path is traced (IPv6 only)
/S <Srcaddr>	Specifies the source address to use (IPv6 only)
/c <compartmnent>	Specifies a routing compartment identifier
/p	Ping a Hyper-V network Virtualization address
/4	Specifies that IPv4 be used to ping
/6	Specifies that IPv6 be used to ping

TraceRT

TraceRT (Trace Route) is very similar to ping in that its primary function is to test the connection to another local or remote server or computer. Where it differs is with the level of detail about the journey it provides. In Figure 14-27 you can see a typical tracert command, in which we can see the request first goes to my Netgear mesh router (10.0.0.1) and then my home Internet router (192.168.1.1) before heading out into the wider world and eventually ending at the server hosting the Apress website.

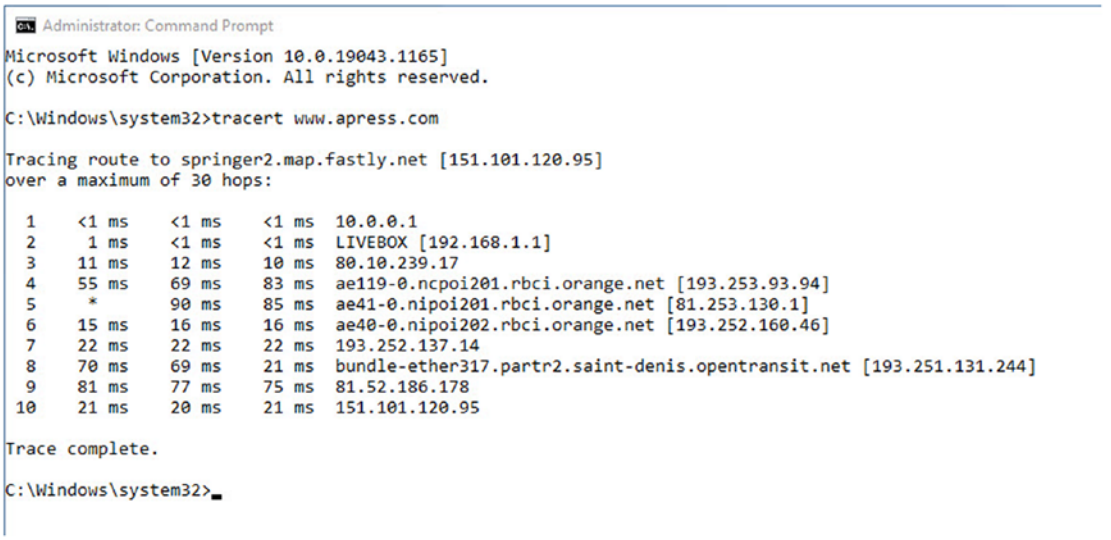


Figure 14-27. *TraceRT provides much more details than ping*

You can use TraceRT with a variety of switches to help refine the results you receive.

Table 14-2. *Switches used with the TraceRT command*

Switch	Description
/d	Stops the command from resolving the IP addresses of intermediate routers to their names; this can speed up results
/h <maxhops>	Specifies the maximum number of hops to the destination; the default is 30
/j <hostlist>	Specifies requests should use the Loose Source Route option in the IP header with the intermediate destinations specified (ipv4 only) with a maximum of nine addresses specified and separated by spaces

(*continued*)

Table 14-2. (*continued*)

Switch	Description
/w <timeout>	Determines the amount of time in milliseconds to wait for a reply; the default is 4000 (4 seconds)
/R	Specified a round-trip path is traced (IPv6 only)
/S <srcaddr>	Specifies the source address to use (IPv6 only)
/4	Specifies that IPv4 be used to ping
/6	Specifies that IPv6 be used to ping

IPConfig

If you suspect a network issue is being caused by a misconfiguration somewhere, the **ipconfig** command can help restore order, and there are plenty of useful switches you can use it with. Run from the Command Line, IPConfig (IP Configuration) will display information about the current network configuration, and can also be used to refresh and repair connection faults. You can read full documentation for it on the Microsoft website at this link `https://pcs.tv/32lxMnr`. It can be used with the following switches; see Table 14-3.

Table 14-3. *IPConfig command-line switches*

Switch	Description
/all	Displays full TCP/IP information for all network adapters in the PC, including virtual adapters created in software or by hypervisors, and dial-up connections
/displaydns	Displays the contents of the local DNS cache, including entries preloaded from the HOSTS file (see earlier in this chapter)
/flushdns	Flushes and resets the DNS cache, used to discard erroneous entries from the cache, as well as those which have been added dynamically and that may now be unresolvable
/registerdns	Start a dynamic re-registration for all the DNS names and IP addresses configured on the PC, can be used to troubleshoot a failed DNS registration or to repair a problem between the PC and the DNS server without having to restart the PC

(*continued*)

Table 14-3. (*continued*)

Switch	Description
/release <adapter>	Sends a DHCPRELEASE message to the DHCP server to release the current configuration and discard the IP address configuration for all adapters (if no adapter is specified) or a specific adapter
/release6 <adapter>	Sends a DHCPRELEASE message to the DHCPv6 server to release the current configuration and discard the IP address configuration for all adapters (if no adapter is specified) or a specific adapter
/renew <adapter>	Renews the DHCP configuration for the specified adapter, or for all adapters if none is specified. This can be very useful for resetting network connections without having to restart the PC, though it only works for adapters that are configured to obtain an IP address automatically
/renew6 <adapter>	Renews the DHCPv6 configuration for the specified adapter, or for all adapters if none is specified. This can be very useful for resetting network connections without having to restart the PC, though it only works for adapters that are configured to obtain an IP address automatically
/setclassid <adapter> [classID]	Configures the DHCP class ID for the specified adapter or all adapters if a wildcard (*) is used. If the classID is not specified, the current one is removed. This switch only works for adapters that are configured to obtain an IP address automatically
/showclassid <adapter>	Displays the current ClassID for a specified adapter, use an asterisk (*) to display information for all installed adapters. This switch only works for adapters that are configured to obtain an IP address automatically

Netsh

Network Shell (netsh) is a suite of commands that can be extremely useful for troubleshooting, configuring, and repairing network problems on both the local *and* remote computers. The tools include utilities for managing the Windows firewall, LAN and WLAN management, IP and Server configuration, Adapter configuration, and more besides. It could justify a short book on its own as an essential resource for any IT pro, but here I'm going to focus on its uses when it comes to troubleshooting and repairing problems. You can read about the netsh utility in depth on the Microsoft website at this link https://pcs.tv/2qYtYYX.

At the beginning of this chapter, I detailed how netsh can be used to retrieve forgotten passwords for Wi-Fi networks, and to set the connection priority for Wi-Fi networks, but there's much, much more it can do. Some of the most useful commands are the following.

Netsh wlan show settings will display the current global settings for Wi-Fi connections; see Figure 14-28. This includes whether blocked networks are visible (more on these in a moment) and whether automatic configuration is enabled.

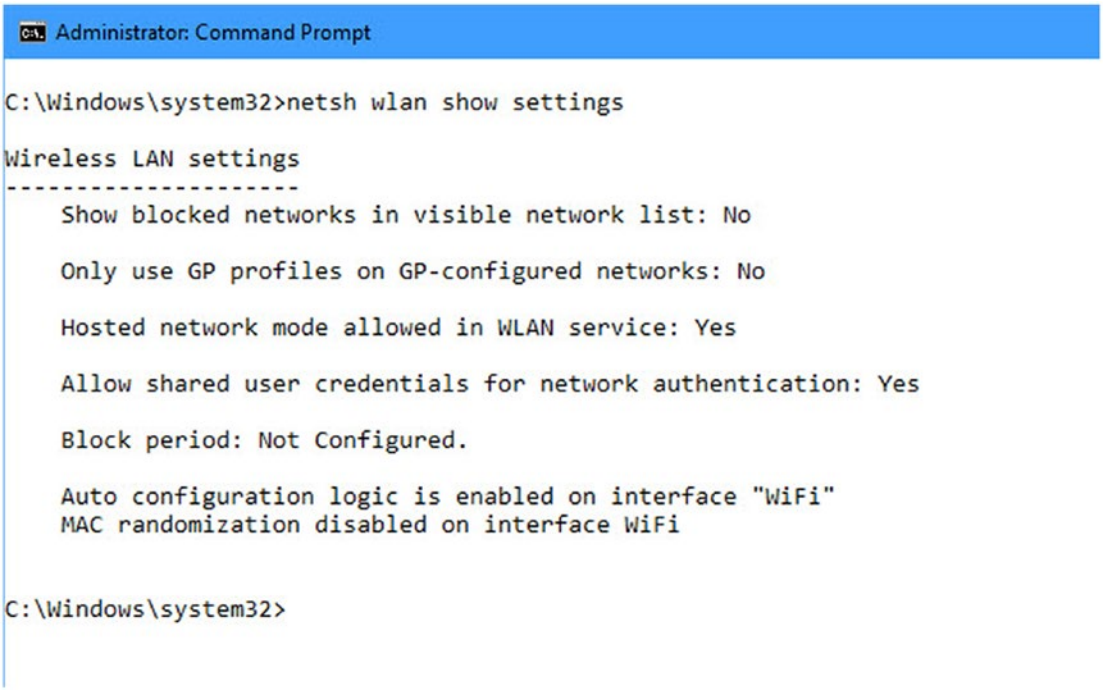


Figure 14-28. *You can display the current settings for WiFi connections*

Netsh show blocked networks is used to display a list of any currently blocked Wi-Fi networks, which you can set to be visible or invisible to the user in the Taskbar Wi-Fi connections popup with the command **netsh wlan set blockednetworks display={show|hide}**.

Netsh wlan add filter permission={allow|block|denyall} ssid="Network Name" networktype={infracturucture|adhoc} is used to block or allow access to a specific network. You might, for example, have a wireless network that is only used for testing, that needs to be without an access password because of the specific devices that connect to it, or that is used for security traffic that you do not want casual users connecting to it.

You can delete a filter you have already applied to a network with the command **Netsh wlan delete filter permission={allow|block|denyall} ssid="Network Name" networktype={infracturucture|adhoc}**.

Tip Perhaps one of the most useful netsh commands is **netsh int ip reset** which can be used to reset the TCP/IP stack without having to restart the PC. This command is most useful when the PC's connection to the network is dropped or is intermittent and can be used as a quick reset by a technician or the end user to try and resolve the issue.

If you enter the netsh scripting environment by just typing the command **netsh** at an Administrator Command Prompt, you can then use the syntax **netsh[-a AliasFile] [-c Context] [-r RemoteComputer] [-u [DomainName\ ] UserName] [-p Password | *] [{NetshCommand | -f ScriptFile}]**. This includes the following switches; see Table 14-4.

Table 14-4. *Switches to use with netsh scripting*

Switch	Description
-a <AliasFile>	Specifies that you should be returned to the netsh prompt after running your alias file, this being a text file containing one or more netsh commands
-c <Context>	Specifies that netsh enters the specified context. These are a group of commands specific to a networking server role or feature, and they extend netsh's functionality. You can obtain a list of contexts with the command **/?** within the netsh scripting environment, or on the link at the beginning of this section
-r <RemoteComputer>	Specifies a remote computer to connect to on the network
-u <[DomainName\] UserName>	Specifies the remote computer you wish to connect to with an optional Domain and User account name
-p <Password | *>	Specifies the password required for a remote computer that you used with the **-u** switch
{NetshCommand | -f <ScriptFile>}	Specifies the netsh command you want to run, with the **-f** switch being optionally used to exit netsh after the script you specify has completed

Microsoft provides some example batch and script files for netsh on their website, which you can find on this link, https://pcs.tv/3gbUet2.

Managing User Profiles

There are two types of user profile in Windows 10, local and domain. The latter is used where the user account is configured by a remote server administrator, such as that found with Azure AD. There are different ways to manage profiles in Windows 10. The first gives you the ability to switch a profile from being a roaming one to a local profile. You can find this in the *Control Panel* under *User Accounts* and then by clicking the *Configure advanced user profile properties* link; see Figure 14-29. Click the *Change Type* button to switch to a local profile.

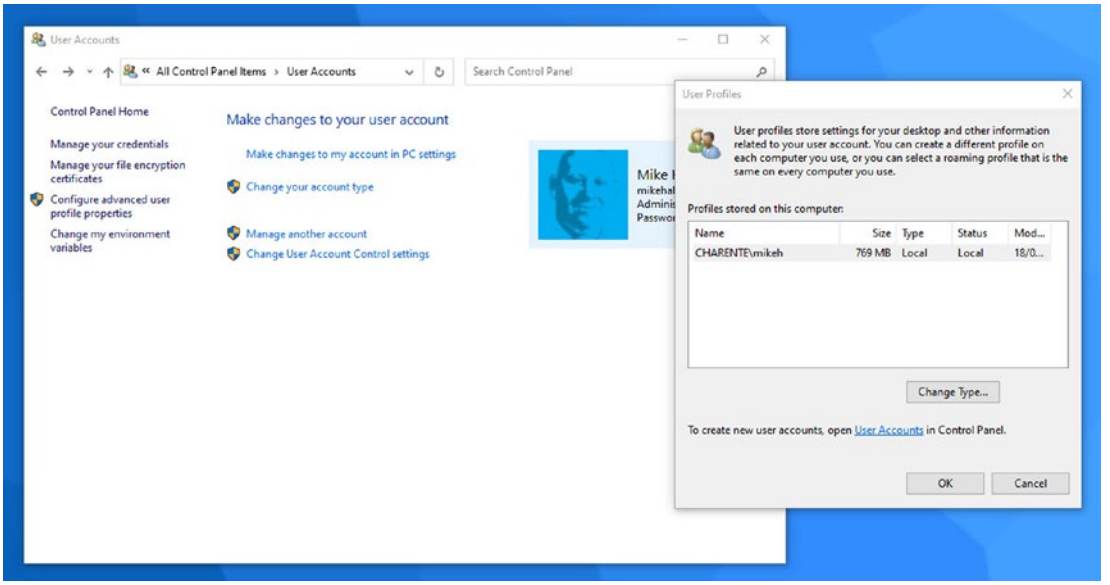


Figure 14-29. *You can switch user profiles between local and remote*

There are also many controls available in Group Policy; search for **gpedit** from the Start Menu in Windows 10 Pro and Enterprise (Group Policy is not available in Windows 10 Home) and navigate to Computer Configuration\Administrative Templates\System\User Profiles; see Figure 14-30.

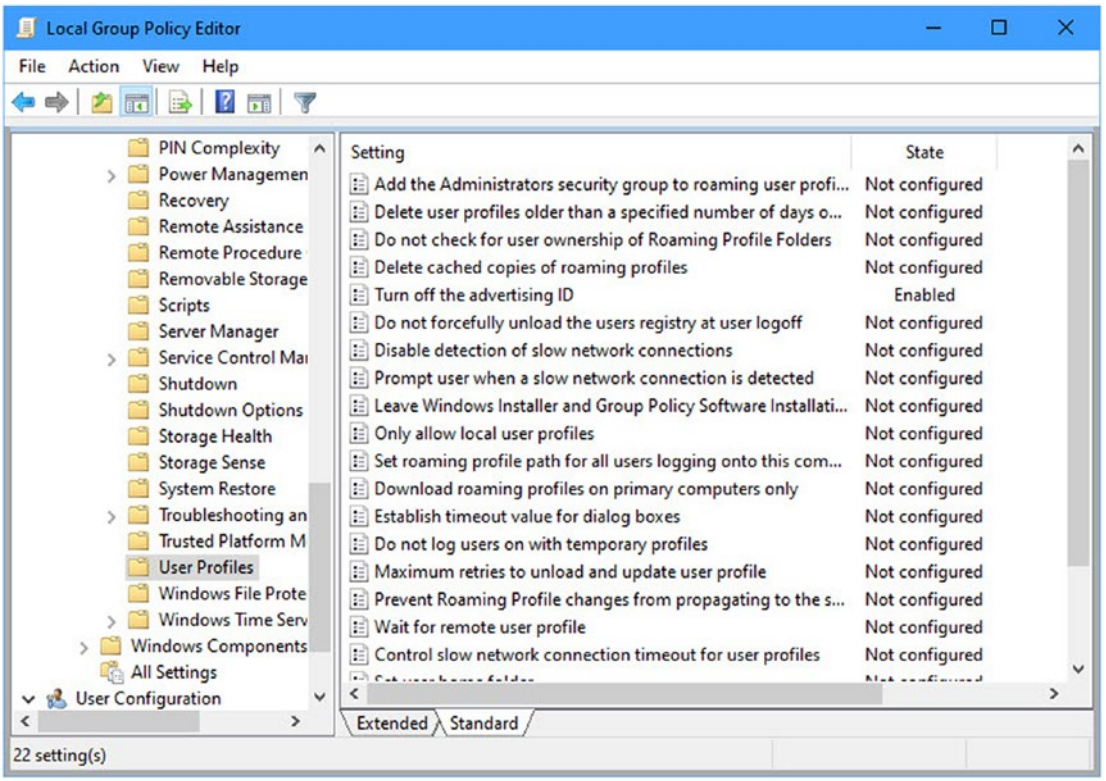


Figure 14-30. *Many user profile controls exist in Group Policy*

Some of the more useful policies include being able to delete cached copies of roaming profiles, delete profiles older than a specified number of days (useful for overall security this one), and set or change the folder path where roaming profiles are stored on the PC. Should any local or roaming profile settings become corrupt, you might find that checking group policy will help provide solutions.

You can also use PowerShell to manage user profiles and local user accounts, and there is extensive documentation on all of the available scripting tools available on the Microsoft website at this link `https://pcs.tv/3xYnWrG`. As you can imagine, PowerShell is hugely complex and detailed language, but the resources Microsoft provides are well written and straightforward to understand.

Summary

It's possible to get a huge amount of detailed information about the status of a network connection in Windows 10. Usually, connections manage themselves as router and switch hardware manufacturers, and ISPs are sensible enough to set their systems to configure connections automatically when they handshake with a new PC. Occasions where this doesn't happen might include secure environments, such as research or government offices, or corporations where there are multiple networks configured to handle extremely large numbers of PCs and network-connected devices.

As configurable as the network options are, there's one thing I have deliberately missed in this chapter, and that's how you can directly manipulate the settings for network driver hardware. Hardware driver configurations can appear an impenetrable business at times, with driver management a tricky task in some circumstances. In the next chapter, we'll look at how we can install, remove, and manage drivers, including how to manipulate individual properties of the driver to affect its behavior.

CHAPTER 15

Managing Device Drivers and PC Resources

Startup, networking, and drivers—where will the problems end on our PCs? It can indeed safely be said that one of the biggest headaches when it comes to getting PCs working reliably is hardware drivers. A large part of the problem is that Microsoft simply doesn't control drivers. Sure they have a certification program, and with Windows 10 every device driver must be digitally signed by Microsoft to ensure it's compatible with the OS and won't crash, but life is unfortunately more complex than that.

There's very little, other than warning dialogs, to prevent an administrator on a PC from installing an unsigned device driver, and indeed there are occasions when you may have to do exactly that, such as for older hardware or for bespoke hardware where the manufacturer weighs up the cost involved vs. the profits and overheads for a product that may only have a niche market, and concludes that the certification process is unaffordable. There's also no way to know how the driver will interact with other drivers and apps on the PC, given the limitless scope of the PC ecosystem, though in fairness there's usually no reason to assume it'll be written more poorly than any other driver.

It's not all bad news though as managing device drivers isn't as impenetrable as many people believe, and Microsoft has done a good job of managing compatibility with device drivers. In this chapter, we'll examine every aspect of driver management and look at how you can troubleshoot any driver problem.

Deciphering the Device Manager

The Device Manager is where all hardware, software, and virtualized devices on your PC are managed. It's often accessed from within the Control Panel, but it's most easily accessed from the *Windows key* + *X* Administration menu.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_15

When you open the Device Manager, you'll be presented with all the devices on your PC grouped by their main category type; see Figure 15-1. This means that all graphics cards, all disks, and all optical drives will be helpfully grouped together. It also means though that any unknown devices will also be grouped together.

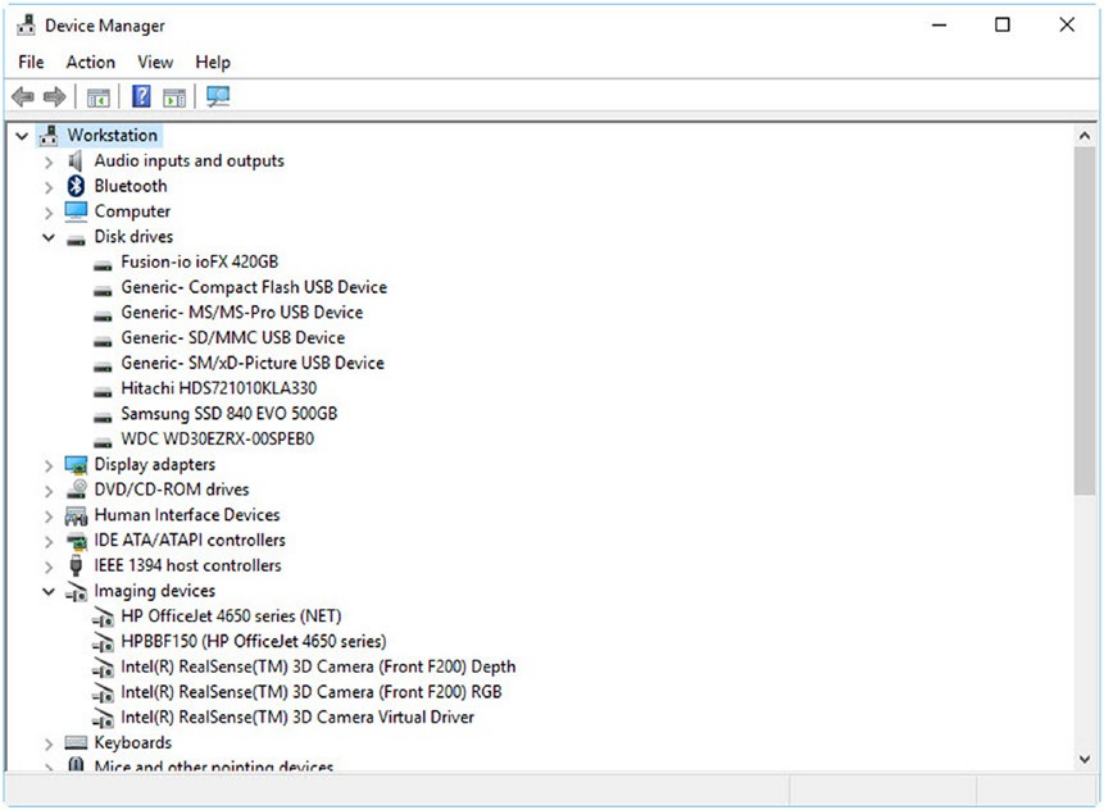


Figure 15-1. *The Device Manager's default view groups device by type*

The *View* menu at the top of the Device Manager window allows you to change the Device Manager so that it displays all your devices in different ways (see Figure 15-2):

- **Devices by Type** is the default view. It groups devices by their main device type category.
- **Devices by Connection** will group devices by how they are attached to the PC, with each device being listed under the device to which it is connected. This view can be useful for troubleshooting nested devices, such as USB devices that are connected to a hub.

- **Resources by Type** displays all allocated resources on the PC, grouped by the type of device that is using the resources. These include Direct Memory Access (DMA) channels, Input/Output ports (I/O Ports), Interrupt Requests (IRQs), and Memory Addresses.
- **Resources by Connection** displays all the allocated resources by their connection type.

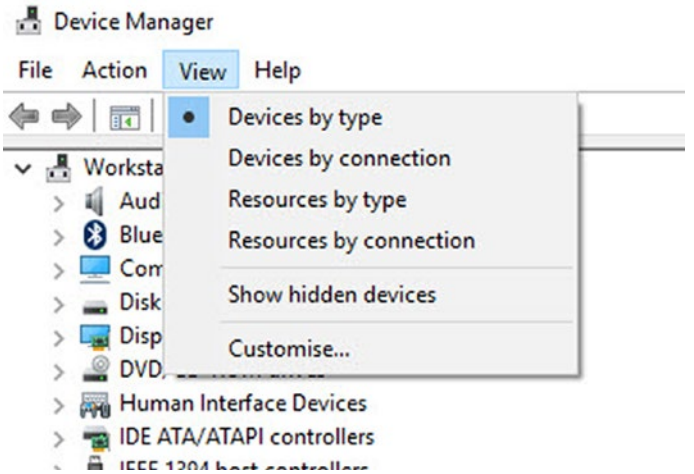


Figure 15-2. *Different views are available in the Device Manager*

Additionally, in the *View* menu is a *Show Hidden Devices* option. By default, the Device Manager shows connected Universal Plug and Play (UPnP) devices. Activating the Show Hidden Devices option will also display non-UPnP devices, such as legacy devices and UPnP devices that are installed but not currently connected to the PC.

Tip Not all hidden devices are displayed in the Device Manager when the Show Hidden Devices option is activated. There is a category called *Nonpresent Devices* which you should never have to view because they have been physically removed from the PC, but their Registry entries remain. This view is mostly used during driver development; however, should an error report a problem with a file or Registry entry that you cannot trace to a specific installed driver, you can view nonpresent devices by opening a *Command Prompt (Admin)* window and typing the command `SET DEVMGR_SHOW_NONPRESENT_DEVICES=1`. These devices will then appear grayed out in the Device Manager when the Show Hidden Devices option is selected.

Identifying and Installing Unknown Devices

When you install a device driver, you will be prompted by Windows 10 to look for the driver automatically, which will search the Driver Store, which comes as part of Windows 10, and will also search Windows Update for a driver if you have an Internet connection. Alternatively, you can install the driver manually by pointing the Device Manager at the specific installer file for the hardware.

Very often, however, the hardware is listed as being an *Unknown device*; see Figure 15-3. Sometimes, after a few Windows Update installs, these devices sort themselves out and are automatically installed. On other occasions, however, you can be left scratching your head, and wondering what the device could be.

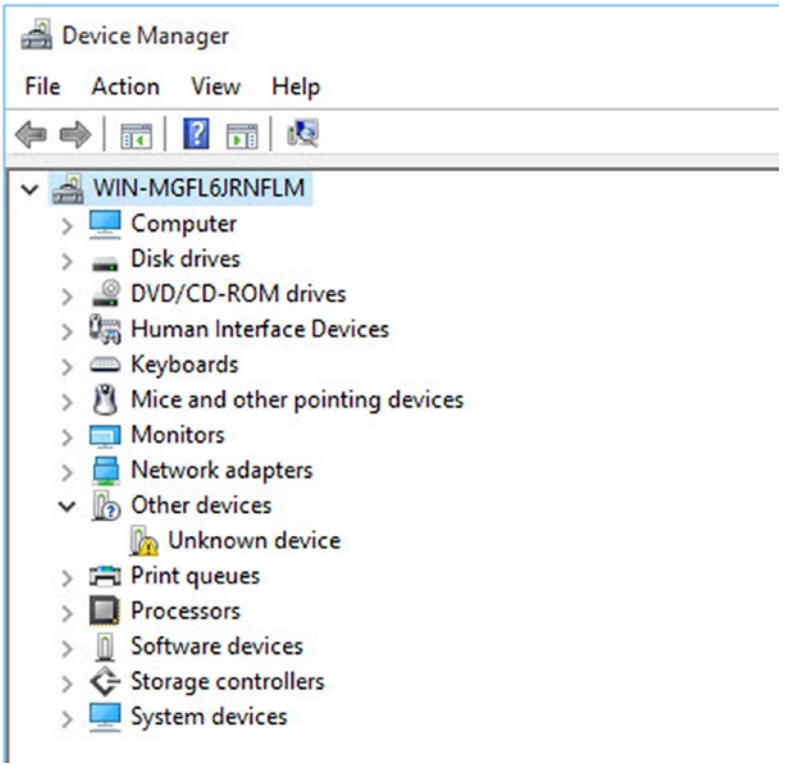


Figure 15-3. *Unknown devices appear grouped in an Other Devices category*

If Windows 10 cannot identify a driver, it's still possible to easily discover what it is as long as it's a Plug and Play device. Right-clicking the device and choosing *Properties* from the menu that appears will display detailed properties for that hardware. The *Details* tab in this dialog contains a drop-down options menu. Selecting *Hardware IDs* in this menu will display *VEN_* (Vendor) and *DEV_* (Device) codes that will be (almost always) unique to that device; see Figure 15-4. You can search for these VEN_ and DEV_ codes online to discover what the device is, so as to obtain the correct driver. In the example here it's an Nvidia GeForce GTX 980 graphics card with the codes VEN_10DE and DEV_13C0.

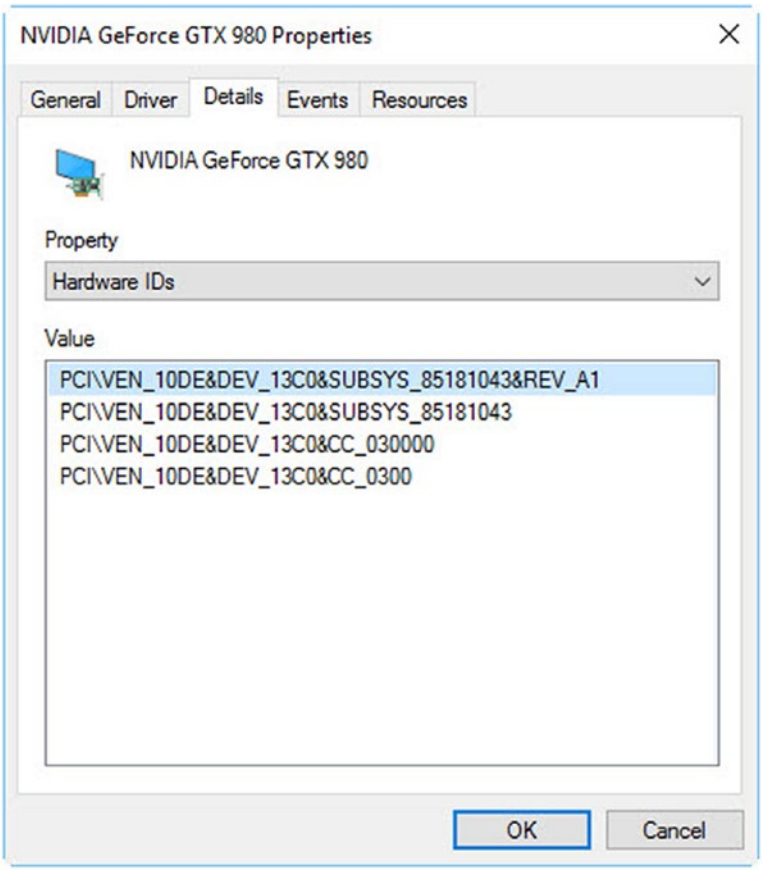


Figure 15-4. *You can identify unknown devices by their VEN_ and DEV_ codes*

Sometimes, you will be installing a legacy driver for a device that's displaying as Unknown, or something that you're certain will have a driver already shipped with Windows 10, or that has been installed previously on your PC. If you don't have access to the driver install media, you can search the Windows 10 Driver Store for the correct driver to install:

1. Right-click the device, and select *Update Driver Software* from the menu that appears.
2. At the wizard that opens, click *Browse my computer for driver software*; see Figure 15-5.

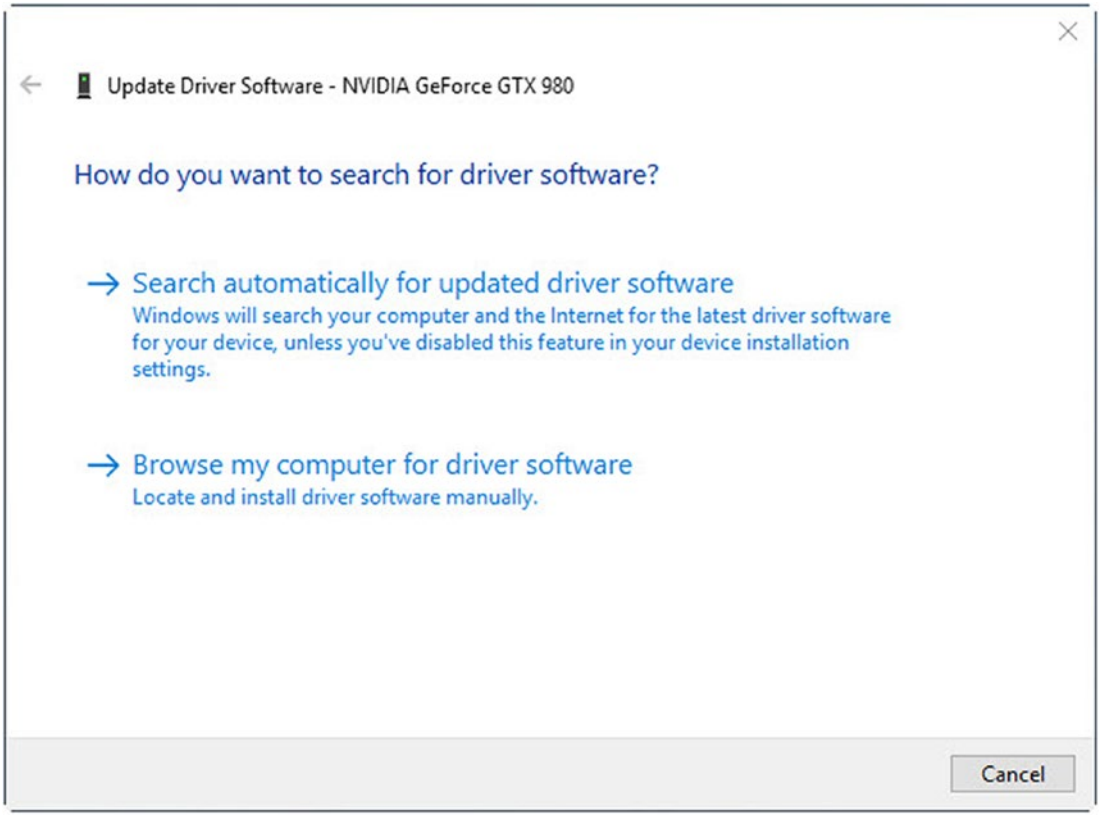


Figure 15-5. *Choose Browse my computer for driver software to install the driver manually*

3. At the next panel, instead of clicking the Browse button to search for the driver install file, click Let me pick from a list of devices on my computer; see Figure 15-6.

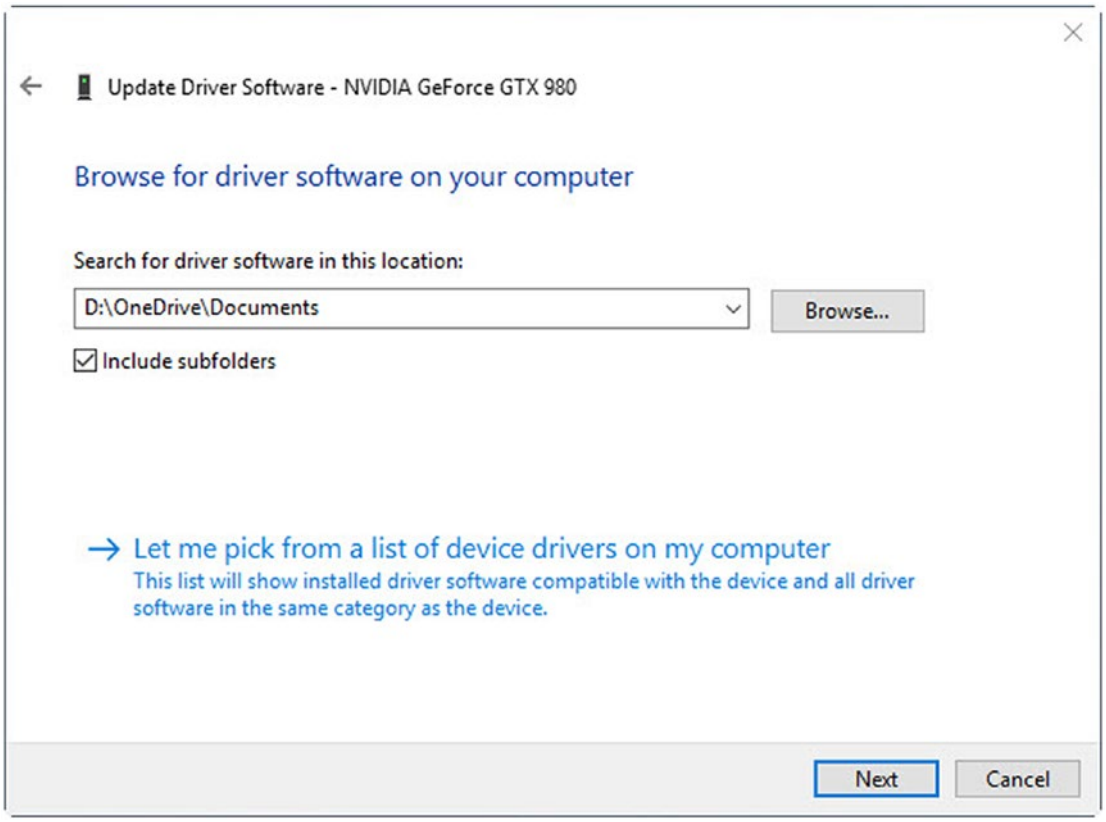


Figure 15-6. *You can choose Let me pick… to choose a driver from the Driver Store*

4. You will be shown a list of the drivers that Windows 10 identifies as being compatible with your hardware; see Figure 15-7. Occasionally though, and especially with an older device, you may wish to specifically search the Driver Store.

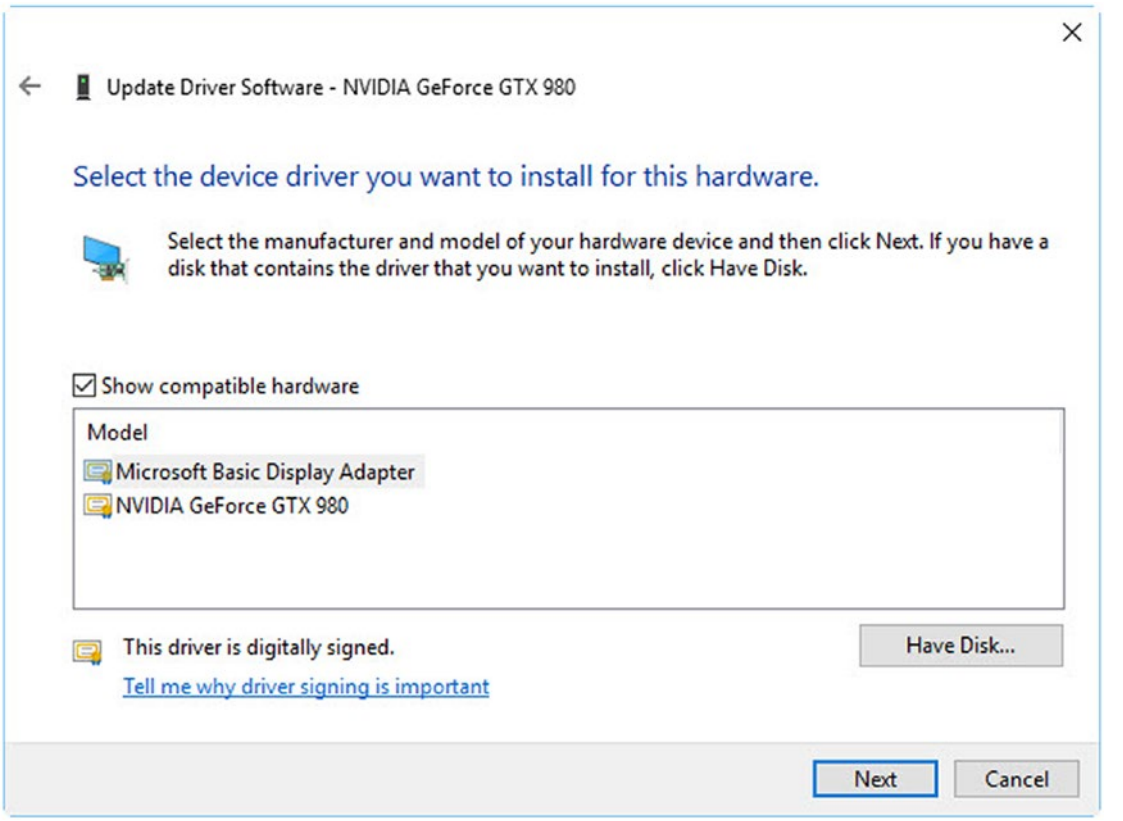


Figure 15-7. *Only drivers Windows feels are compatible will be shown*

5. Uncheck the Show compatible hardware option, and the contents of the Windows 10 Driver Store will become available to you; see Figure 15-8.

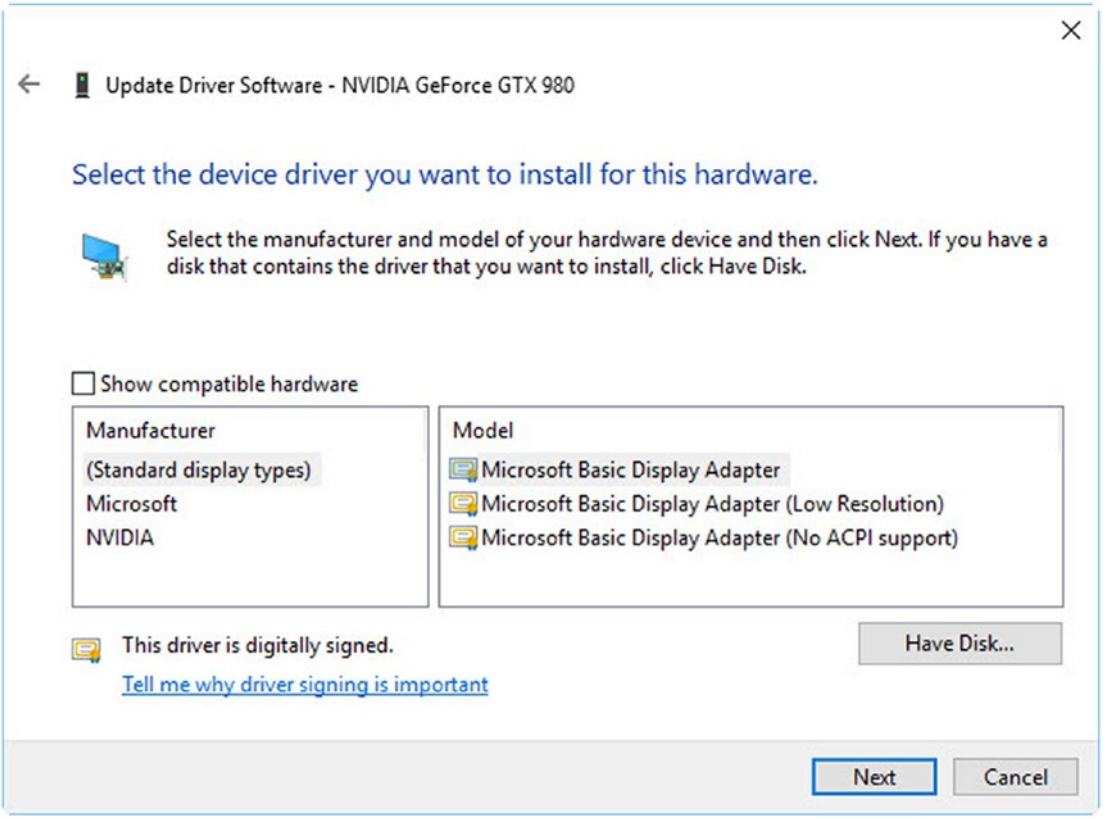


Figure 15-8. *You can display all drivers for that device type*

If the device type is unknown to Windows, a list of all available device categories in the Driver Store will be displayed; see Figure 15-9. Choose the correct category for the device, and compatible drivers for that category, as seen in steps 4 and 5, will be displayed.

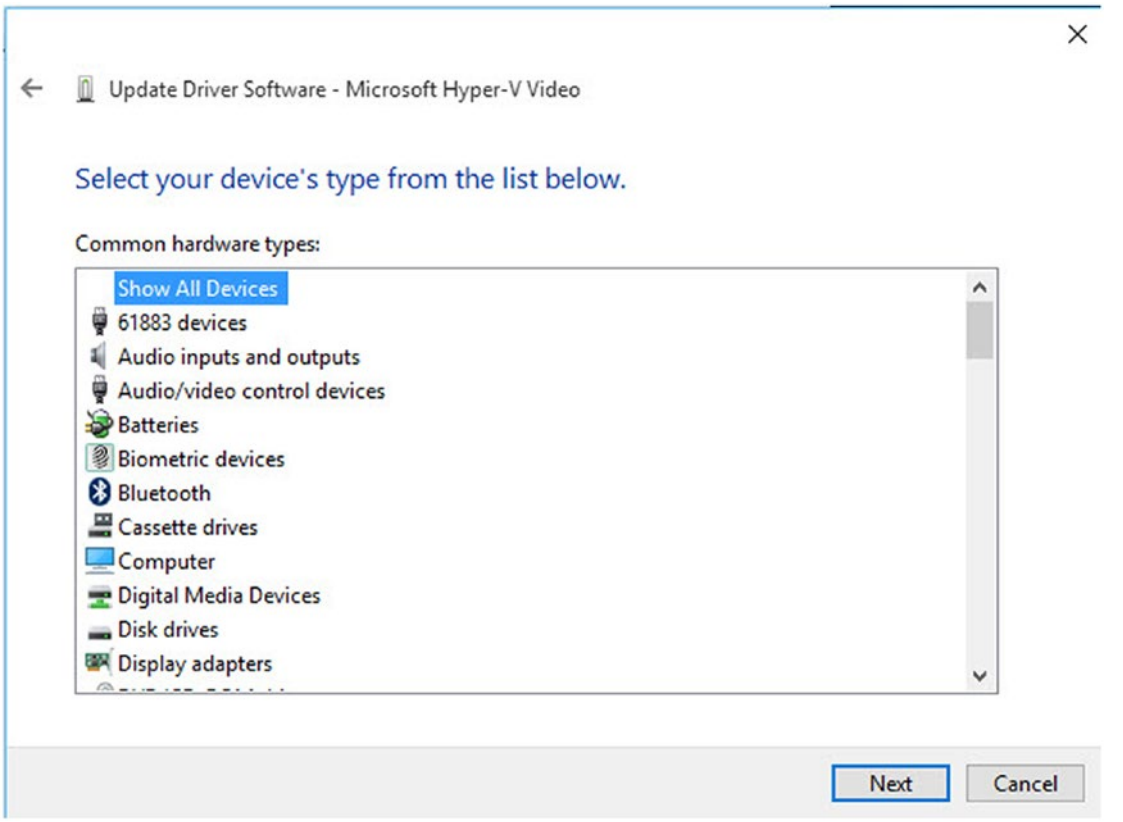


Figure 15-9. *Unknown devices will display all device types in the Driver Store*

Installing Legacy Hardware

Sometimes you will need to install non–Plug and Play devices such as older Serial or Parallel devices. These can still be regularly used in specialist scenarios such as medicine and engineering. To install a legacy driver, select *Add legacy hardware* from the Action menu in the Device Manager. You will be asked if you want Windows 10 to automatically search for and install the hardware or if you want to manually select it from a list; see Figure 15-10.

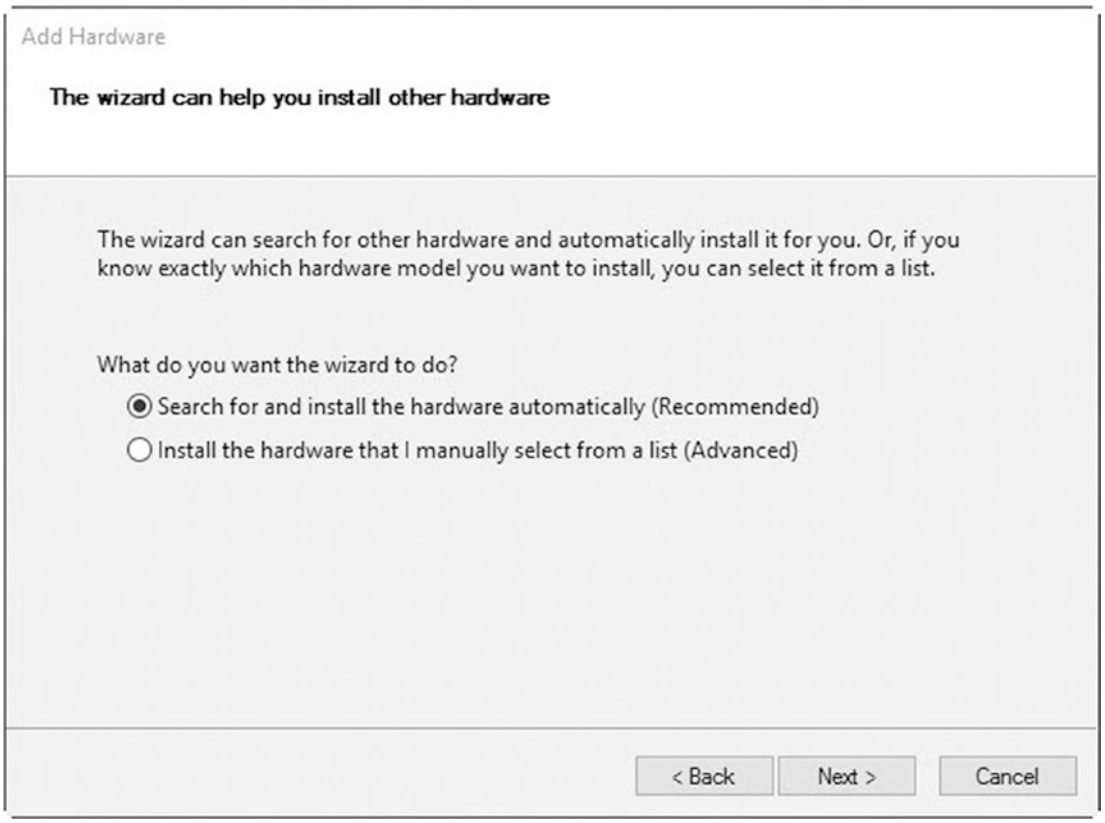


Figure 15-10. *Legacy hardware can sometimes be installed automatically*

If you choose to manually select your hardware from a list, you will be presented with a full list of all the main device types that are available in the Driver Store; see Figure 15-11.

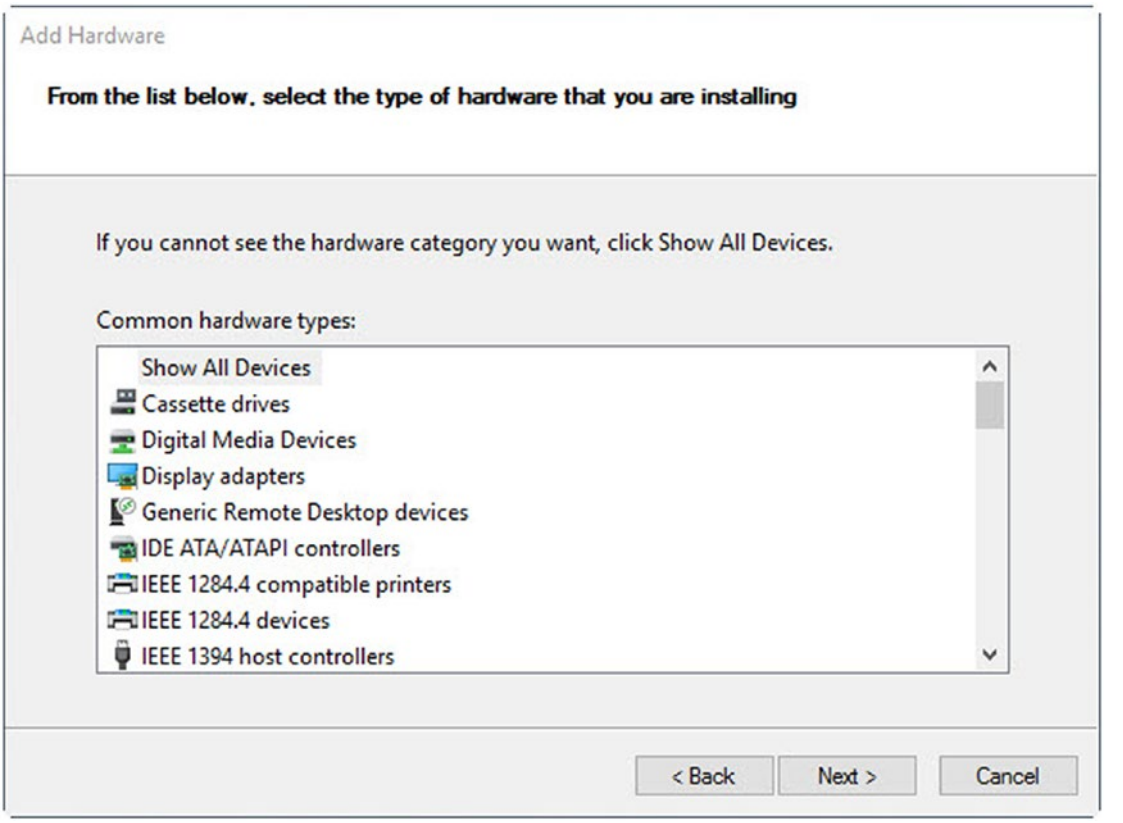


Figure 15-11. *You will be shown all the legacy device categories from the Driver Store*

What happens from here will vary depending on what device category you choose. If you are, for example, installing a modem, you will be first asked if you want the modem automatically detected, or you will be taken to a list of all the legacy and smartphone modem types that are known to Windows.

If on the other hand you're installing a printer, you will be asked which port on the computer it is connected to, or if Windows needs to create a virtual port for the connection; see Figure 15-12.

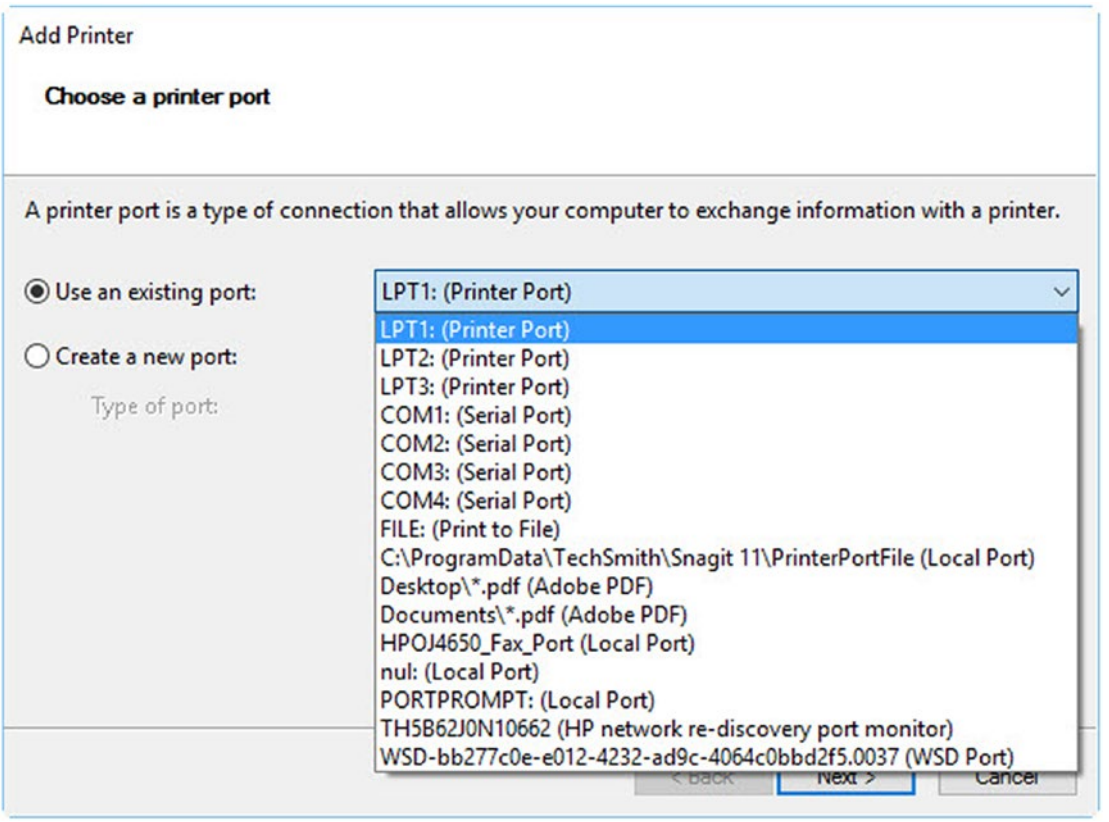


Figure 15-12. *Installing legacy printers will ask what port the printer is connected to*

But what happens if you have a specialist medical, engineering, or other device and you're not certain what category to choose for its installation? Point-of-sale (POS) hardware has several categories available in the legacy device installer wizard, but what about everything else? Generally speaking, the categories are sensibly laid out with titles such as Network infrastructure devices, Imaging devices, and Sensors. If you cannot gain access to the manual that came with the device, there are no VEN_ and DEV_ codes you'll be able to check, though a search online for the device name and model number may reveal full installation instructions, and perhaps even a current driver.

Note Parallel devices will connect to the *LPTx* ports on a PC, and Serial devices will connect to the *COMx* ports, where the x in these examples represents the port number.

Uninstalling and Deleting Device Drivers

When it comes to troubleshooting device drivers, they can provide a wealth of information, and there are several tools and techniques you can use to assist you. The first of these is driver updating and removal. You can right-click a driver in the Device Manager and select *Uninstall* from the menu that appears, but sometimes you will also get an option to *Delete the driver software for this device*; see Figure 15-13.

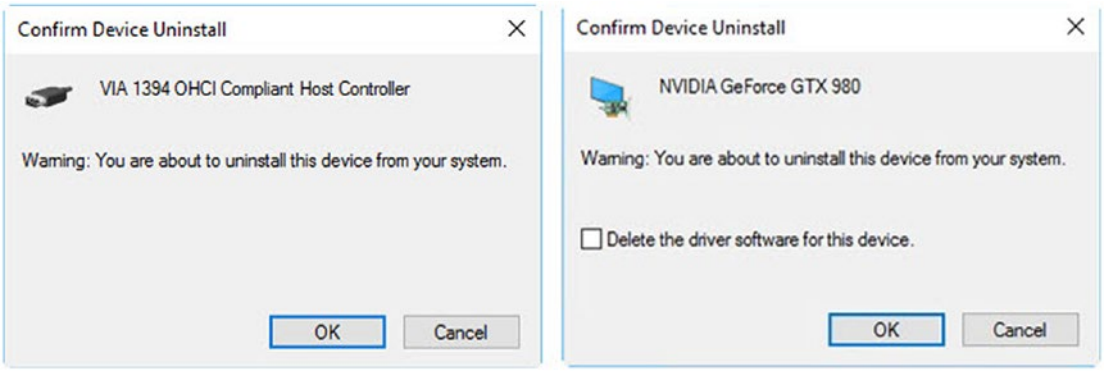


Figure 15-13. *Some drivers offer the option to delete the driver files from the hard disk*

Tip Sometimes a device isn't needed by the system and can be disabled. This can be achieved by right-clicking the device and selecting *Disable* from the context menu that appears.

You will be offered the *Delete the driver software…* option when the driver was not shipped with Windows 10, or when no other devices or Windows services rely on the driver or share a component with it. Checking this box will permanently delete the driver from the Driver Store. This means that when the device is reinstalled on the PC, the driver will need to be reloaded from Windows Update or reinstalled from the device installation media.

This can be very useful if a device that's causing problems is automatically being reinstalled on a restart or on a refresh of the Device Manager. If you need to install a different driver for a device, perhaps an earlier driver, and are being prevented from doing so, this may be because the faulty version of the driver is constantly being reinstalled.

Tip Sometimes you may wish to roll a driver back to the previously installed version and then block the new driver from installing. I will show you how to block driver installation shortly, but under the *Driver* tab in the Device Properties panel, you will find a *Roll Back Driver* button. If a previous driver is available for the device, this button will be available to click. Note that this system uses the Windows 10 System Restore feature and will not work if System Restore is disabled on the PC.

Blocking Device Driver and Device App Installation

Additionally, you might want to block all driver updates from Windows Update, or specific driver updates that you know are causing problems. Windows Update was changed in Windows 10 so as to deny users and administrators the option to block specific updates. I'll talk about Windows Update in full in Chapter 16, but it's still possible to block driver updates from Windows Update.

If you find that a driver is automatically downloading an app or apps from the manufacturer's website (such as an updater app) that is either causing a problem or that you don't want installed, you can block all of these downloads by opening *System* from Settings and then clicking the *Advanced System Settings* link which you'll find near the bottom of the page.

Under the Hardware tab in the System Properties window, click the *Advanced System Settings* link at the left of the window; then, in the dialog that appears, click the *Hardware* tab. This will display a *Device installation settings* button, which offers you the option of blocking all third-party apps that may be automatically downloaded by devices; see Figure 15-14.

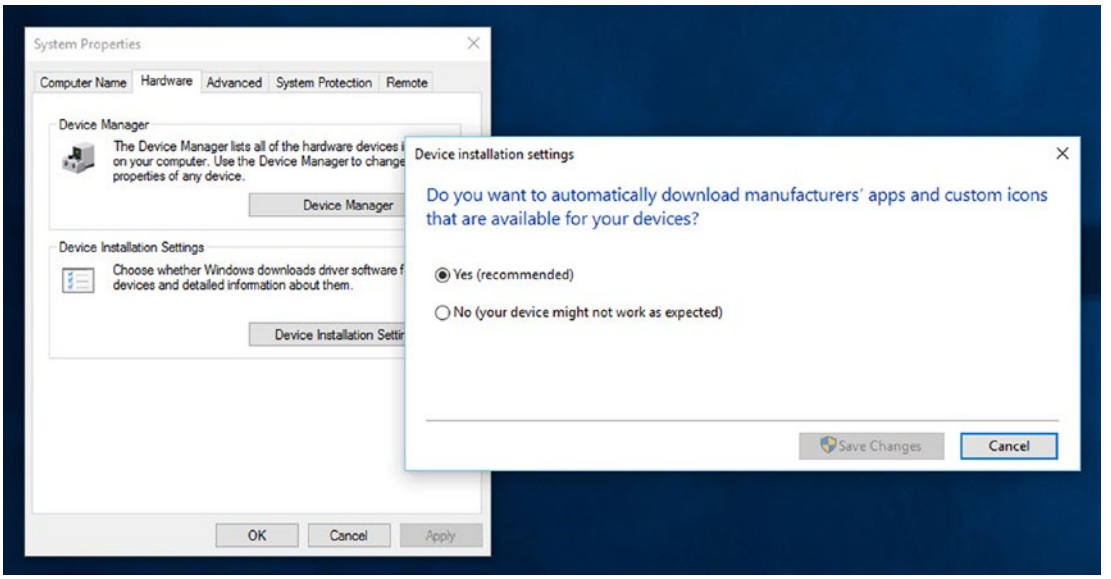


Figure 15-14. *You can block all app downloads that accompany some drivers*

Sometimes, however, you need to block a driver completely, because you know it is causing problems. Microsoft used to have a downloadable Troubleshooter called *Show/Hide Updates* (filename **wushowhide.diagcab**) but have removed this very handy tool from their website. Some third-party websites still host it, and I found it at MajorGeeks on the link `https://pcs.tv/3jfVTPd;` however, this comes as always with a caveat to use caution downloading anything from a third-party website, and you should always virus-scan any file you download before opening it.

That said, running this troubleshooter will enable you to block specific Windows Updates, including hardware drivers, from being downloaded and installed onto the PC; see Figure 15-15. Please note though that it only works on updates you have already downloaded and then later uninstalled.

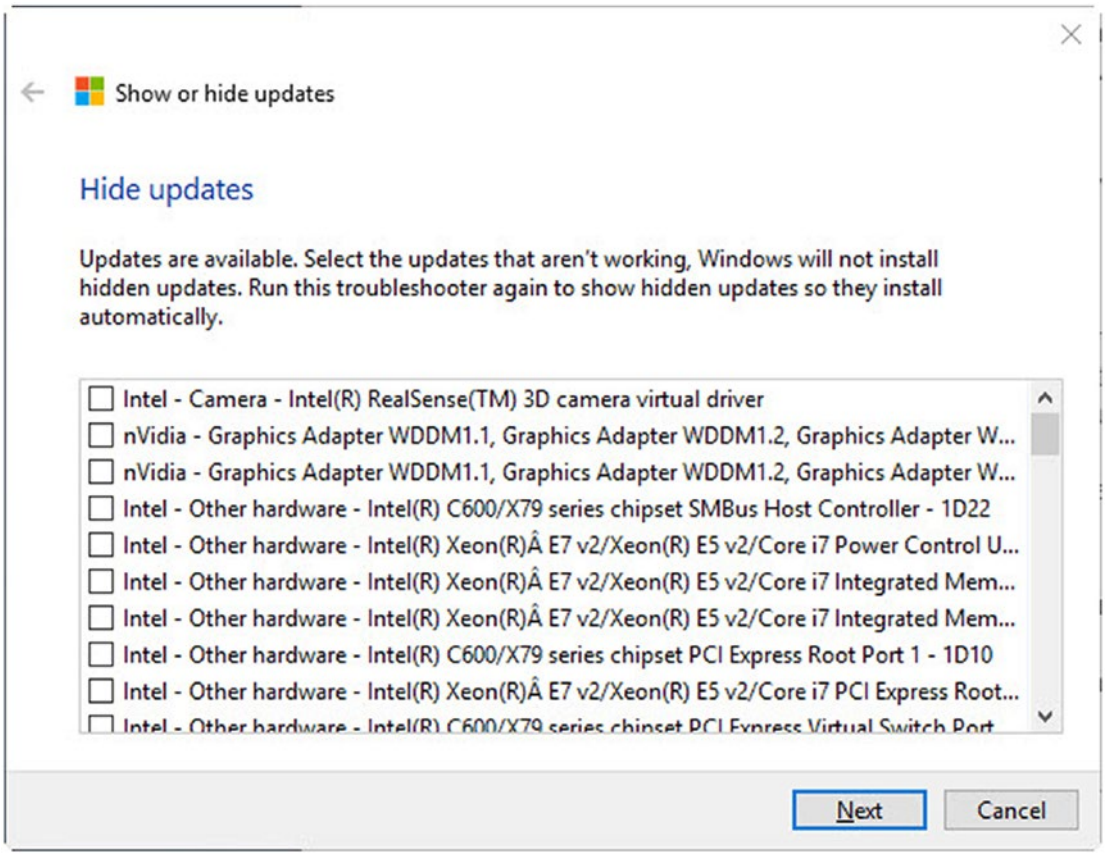


Figure 15-15. *Microsoft provides a troubleshooter that can block Windows Updates*

Another option available to you that can be useful if you have a mission-critical system that won't change over time, such as a Long-Term Servicing Channel (LTSC) PC system, is to block **all** driver updates and downloads from Windows Update. You can do this in the Group Policy Editor, search for **gpedit** in the Start Menu, and navigate to *Computer Configuration* ➤ *Administrative Templates* ➤ *Windows Components* ➤ *Windows Update*. Here you can enable the policy named *Do not include drivers with Windows Updates*; see Figure 15-16.

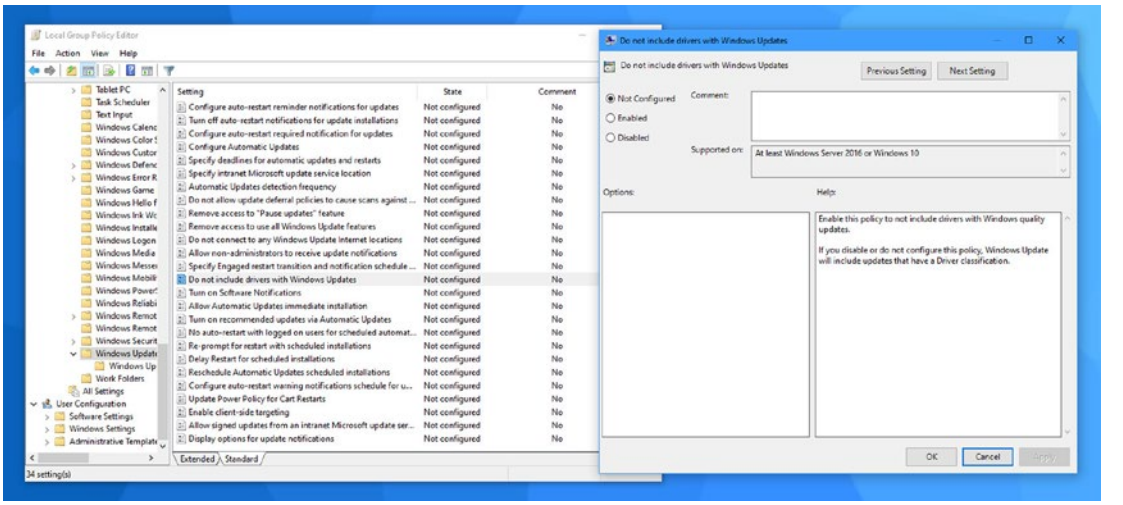


Figure 15-16. *You can tell Windows Update not to install drivers*

Finding Device Driver Details and Information

Sometimes you need to find advanced information about a driver, perhaps because you need to remove the driver files manually from a PC. A wealth of information is available for many drivers by right-clicking them in the Device Manager and selecting *Properties* from the menu that appears.

You might want to know exactly what files are installed on the PC as part of the driver installation (it's always more than one file), perhaps because you want to manually delete the files. Under the *Driver* tab in the Driver Properties dialog is a *Driver Details* button. Clicking this button will display another dialog listing all the files associated with the driver that are installed on the PC's hard disk. You can make a note of these files (sadly there's no copy button) for manual deletion; see Figure 15-17.

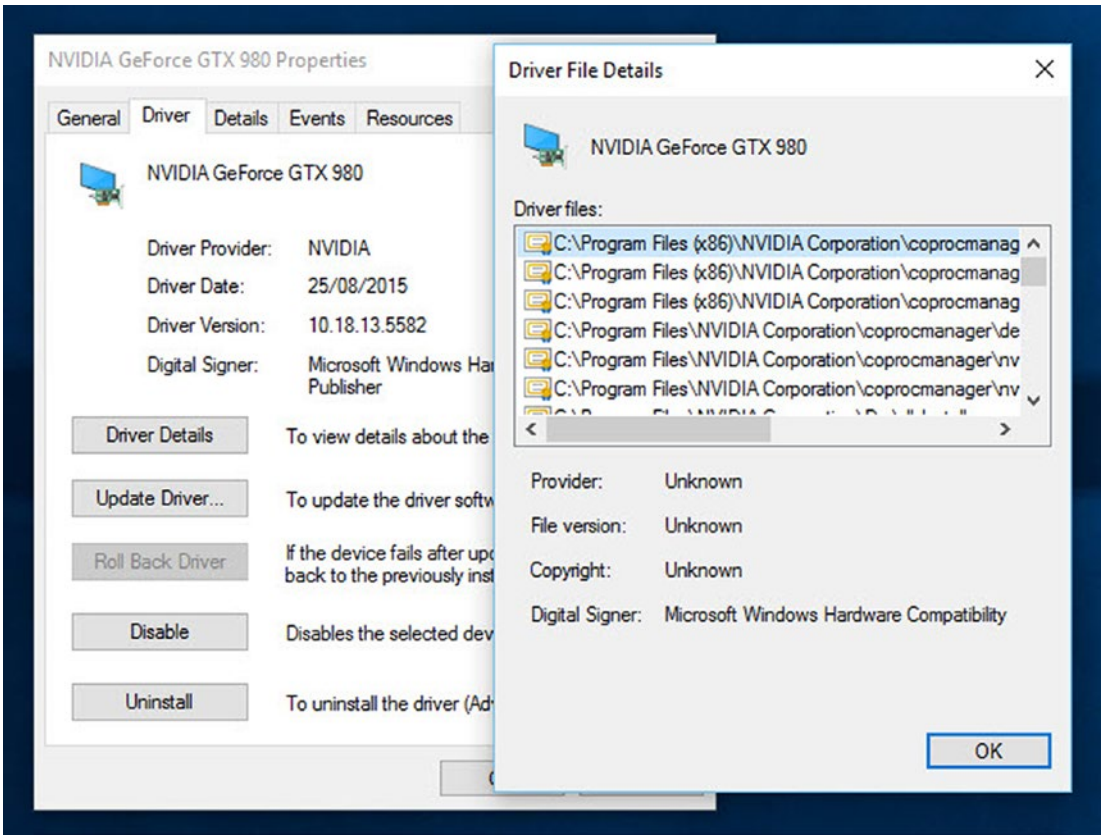


Figure 15-17. *You can see the full driver file list in the Device Properties*

Note Some driver files may be locked by Windows due to being currently "in use." You can start the PC in Safe Mode or Diagnostic Mode to manually delete the files, and I will detail how to start the PC in these modes in Chapter 19.

Additionally, the *Details* tab of the driver properties panel displays a drop-down menu with a wealth of useful information, and this is where you can find the DEV_ and VEN_ codes I detailed earlier in this chapter. The information in the drop-down menu will vary from one driver and device type to another, but one very useful piece of information that's common to all devices is its version number; see Figure 15-18.

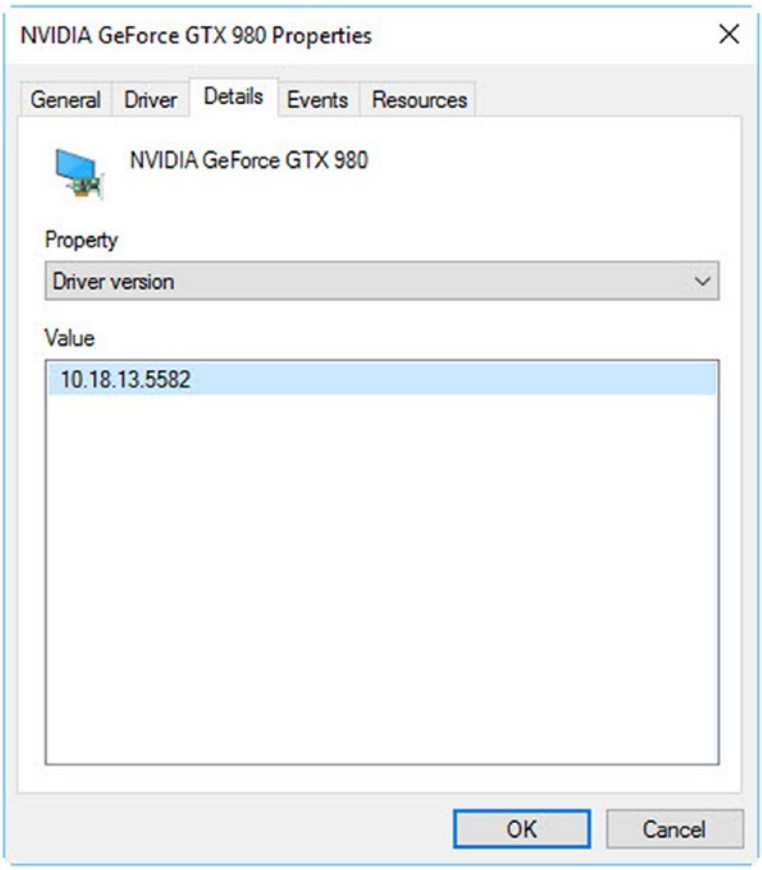


Figure 15-18. *You can get useful information about the driver such as its version number*

The version number of anything is crucial both to system administrators, who will want to exhaustively test new versions of apps and drivers before deploying them, and also when troubleshooting a problem. You can search online for the version number of a driver (or app) to see if a more recent version is available, or if the currently installed version is known to cause problems or, perhaps, was designed for an earlier version of Windows and shouldn't be installed at all.

Troubleshooting Device Drivers

At the end of the previous chapter, I mentioned that the properties for some devices can be changed and reconfigured, so as to alter or improve the behavior or performance of the driver. The context I gave was network drivers where some behaviors might need to be individually configured to create stable connections to secure or specialist network types.

In Figure 15-19 you can see a driver, a Wi-Fi networking driver in this case, which has configurable properties under an *Advanced* tab. The options available will vary from one device and driver to another. They will, however, be configurable so that you can, in the example of this 802.11ac Wi-Fi driver, disable some of the older Wi-Fi connection protocols should it be necessary for security or when the device may not be providing a stable connection with its default settings.

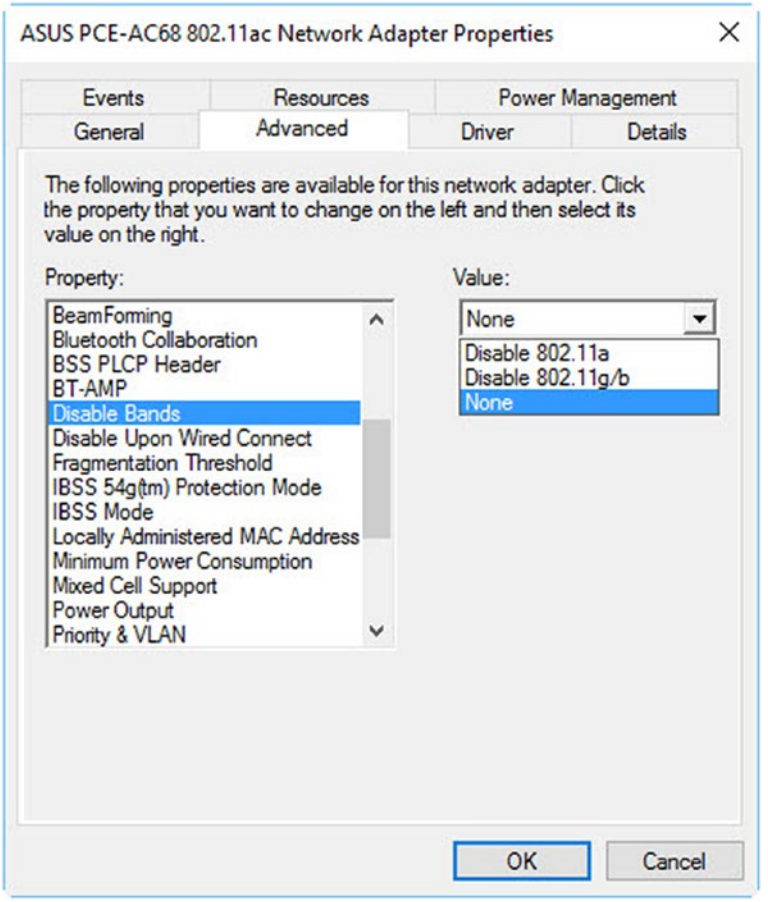


Figure 15-19. *Some drivers have configurable properties*

The *Resources* tab (see Figure 15-20) can provide information that's useful in determining if a device is conflicting with another device. It was common for earlier versions of Windows that IRQs or memory conflicts would take place, where the driver would be trying to address the same memory space as another device or app, or where it was trying to use the same processor interrupt channel as another device.

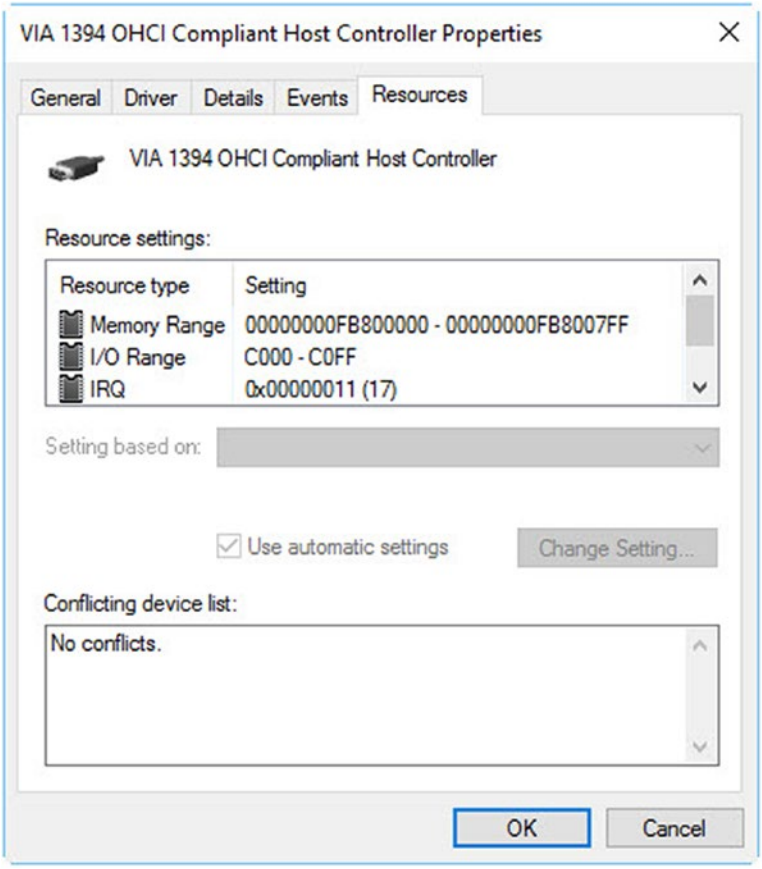


Figure 15-20. *The Resources tab can display information about memory, port, and IRQ usage*

Note Interrupts are communications channels assigned by the PC's processor to allow all apps, services, and devices to share processor time. Rather than have everything making requests of the processor all of the time, which would overload the processor's capacity, devices, apps, and services are assigned an IRQ. These IRQs are cycled by the processor, enabling everything to get an equal amount of processor time, without overloading the system.

Memory, IRQ, and I/O assignments are managed automatically by Windows 10, which uses a system called Side-by-Side. This permits multiple versions of files, drivers, and DLLs (Dynamic-Linked Libraries), which are used to provide services in Windows, to operate concurrently. I will look more at Side-by-Side files, which are found in the `\Windows\WinSXS` folder, in Chapter 27.

Because Windows 10 manages these aspects of driver operation, you will almost always find that the *Change Setting* options under the *Resources* tab are grayed out and unavailable. In some cases, with specific hardware (such as legacy hardware), you will find that you can manually assign IRQ and other resource channels for a driver. This can be useful if you find that a device is using the same IRQ as another device with which it is conflicting.

The Events tab is extremely useful when diagnosing problems with a device. It hooks into the Event Viewer, which I detailed in Chapter 5, to list all events for the driver; see Figure 15-21. These will include configuration and error events. Clicking an event will list further details, including an 0x000… format error code if relevant. Clicking the *View All Events* button will open the full Event Viewer with all of the events for the device listed. More detailed information on the events and errors can be obtained in the Event Viewer, and tasks can be attached to errors to alert the user or a support person about the crash.

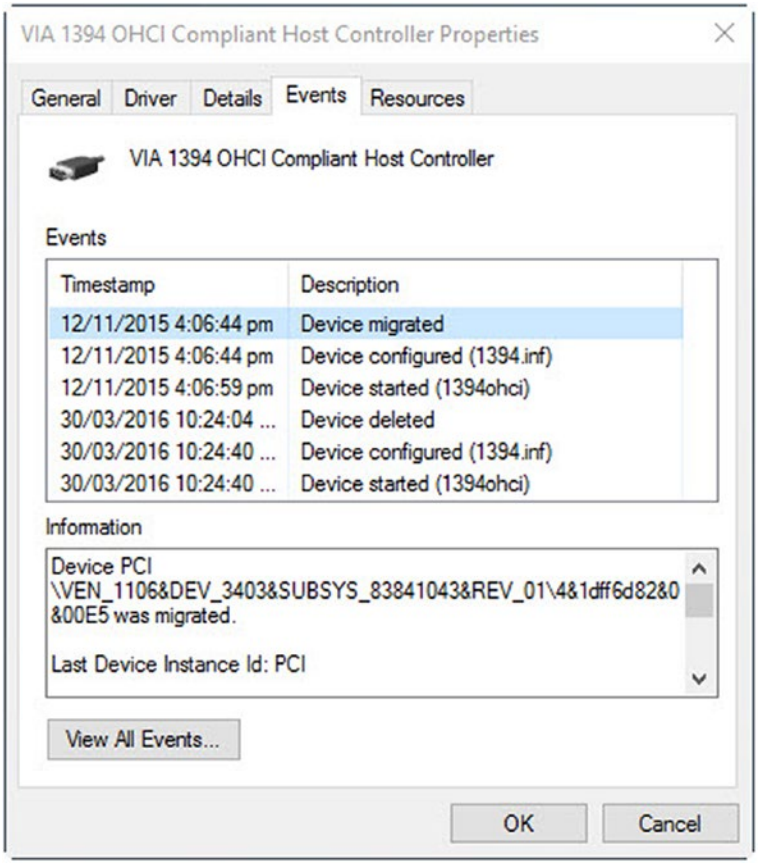


Figure 15-21. *The Events tab provides details of device crashes and other events*

Configuring Driver Parameters

Some drivers including network adapters allow you to configure advanced parameters, and fairly clearly these will vary from one device to the next. As an example, you might find that an employee is visiting a customer site where the available technology is quite old, and the automatic settings on their laptop means they're having difficulty connecting to the older network equipment.

Opening the *Advanced* tab from a driver properties (should the driver support additional configuration), you can tweak all manner of settings. In the example in Figure 15-22, you can see we can the Wi-Fi to use an older standard, to try to get it to connect, or to disable either the 2.4-GHz or 5-GHz bands completely if they cause a connection issue.

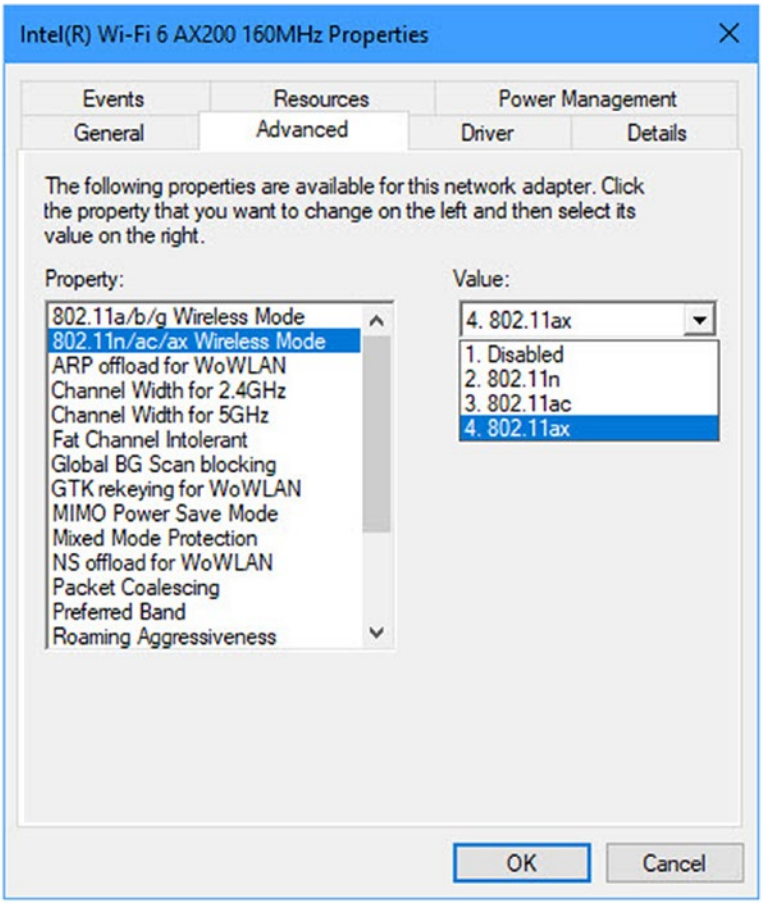


Figure 15-22. *You can configure advanced parameters for some drivers*

In fairness it's only in very specific and specialized circumstances you'll have to do this, such as enforcing specific security protocols for networking if you happen to visit the headquarters of the Illuminati (and if so, please email me to tell me where they are), but these configuration options do exist for a reason.

Backing Up and Restoring the Driver Store

If you're anything like me, you'll have a partition or disk in your system in which you keep important win32 app installers and hardware drivers. When the time comes to reinstall Windows 10 from scratch, which will most likely still need doing every so often for one reason or another, these are your quick way to get the system working. This is

especially so in light of the fact that Murphy's law dictates that you won't be able to get Internet access on the PC, at the very time you need to download the network drivers.

The Windows 10 Driver Store is located in the `C:\Windows\System32\DriverStore` folder on your PC. You can create a backup copy of this folder and, when time comes to reinstall, either copy it back to the fresh installation or tell Device Manager to search your backup copy of the folder when reinstalling drivers. Additionally, there is a `C:\Windows\System32\Drivers` folder that you may also want to back up, as it may contain device drivers required by your hardware.

If you are copying the folder back to its original location, you should only do this if the version of Windows 10 you are installing is the same as the one the backup copy of the DriverStore folder was copied from. The reason for this is that new and updated drivers for existing and new hardware types are released on a regular basis both through Windows Update and with updated releases of Windows 10.

Summary

Device drivers on a PC can be complex things to work with, especially when they're misbehaving. Some drivers, such as the graphics driver, are embedded so deeply within the operating system that troubleshooting and managing them can prove difficult. On these occasions, you'll likely need Windows 10's Safe or Diagnostic Modes, and I'll show you how to use these in Chapter 19.

In the last few chapters, we've dealt with the issues that plague PC users and system administrators the most, these being startup, networking and Internet connections, and device drivers. We've still got software and app compatibility to come in Chapter 17, but in the next chapter, we'll deal with the fourth most common plague for the PC, this being Windows Updates and edition upgrade installation.

CHAPTER 16

Windows Update and System Upgrades

Windows Update received a major shake-up with Windows 10, and not everybody welcomed the changes. The short version of the story is that whoever you are, wherever you work, it's not possible to opt out of stability and security patches for Windows 10… ever! If you are using Windows 10 Home or Pro, it's not possible for you to opt out of feature updates and upgrades either.

Why would Microsoft do such a thing? Well, I want to first deal with the tricky subject of Windows 10 Home (and Pro) users who cannot or do not defer updates. Generally speaking, Windows Updates never cause problems. Of course this isn't always the case, and there are a few isolated incidents where a Windows Update has needed to be pulled by Microsoft for causing problems. Third-party hardware drivers that are released through Windows Update are another matter entirely. Nothing is ever released through Windows Update until it's been extensively tested, but problem updates do occasionally sneak through. That, frankly, is why all of us have a job.

So, let's get back to the thorny issue of why Microsoft would do such a thing. When Windows 10 was released in July 2015, it was widely reported online that the move was made either because with Windows being free for the first 12 months, you would no longer own your own copy of the OS. Another theory held that Microsoft simply wanted to force everybody to be using Windows 10, or that the updates would at some point after the first year become chargeable. None of these reasons are true.

The truth is that when Satya Nadella took over as Microsoft CEO in 2014, he immediately took the company on a major slimming exercise. The company was bloated and inefficient. When it came to Windows, they had always had a policy of supporting each operating system for ten full years after its release, with the latter half of that being just security and stability updates. This, coupled with the ability of any Windows user to

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_16

either hide specific updates or opt out of updates altogether, meant that Microsoft was effectively supporting a massive number of different versions of each OS. The cost for providing this support would run into tens of millions of dollars every year, but all of it was essential to keep Windows desktop PCs safe, secure, and reliable.

With Windows 10 the decision was made to cut those costs massively, and the best way to do this was to ensure that all Windows users would be in the same place, all of the time. The only way to achieve this would be to mandate Windows Updates and remove the ability people had to opt out of receiving them. While this didn't turn out precisely as Microsoft had intended, as they're still supporting several different versions of Windows 10 concurrently, it's much more straightforward for them than it used to be.

To a large extent, this makes sense. If you compare the policy to that of other technology companies, Apple only support OS X versions for 18 months after their release, and the same goes with versions of their iOS operating system. Google on the other hand has a very different problem. They don't enforce or encourage OS updates in the way that Apple does, and so its OS ecosystem is extremely fragmented, with many versions of Android in use simultaneously. If you examine how we use those mobile operating systems, however, we're used to having updates to apps just appear overnight. We might open an app one evening to find that it looks and operates quite differently from the way it did when we used it only that morning. This has become the norm for apps, so could or should it become the norm for operating systems as well?

A word about the feature upgrades. It's true that the Windows 10 user interface (UI) will change over time. It's also true, however, that it won't change very much. The Start Menu won't be going anywhere (though it was given a significant overhaul with Windows 11), the Action Center will still operate the same way, and so on. All that will happen is that each part of the OS will gain additional functionality and be improved in usability over time.

So where does this leave you, the person having to deal with the fallout from all of this? Well, there are some workarounds and ways to configure Windows 10 to enable, and guarantee, safe and reliable service when updates do come a'callin'.

Deferring Updates in Windows 10

Let's jump right in then to deferring updates in Windows 10. As I've mentioned, if you are using Windows 10, then the system tries to strongly discourage you from deferring any updates, and even then there's a very limited time you can defer them for. Microsoft

specify "several months" in their help documentation because *feature packs* (by which they mean new and enhanced OS features) and *updates* (stability and bug fixes) are handled differently, with the latter only being delayable by a maximum period of only 1 month.

Windows 10 has two "servicing channels" which determine how and when updates are delivered. These are called the Semiannual Channel (SAC) and the Long-Term Servicing Channel (LTSC). I should point out that none of these will *ever* allow you to defer critical security updates. Microsoft is quite clear in their documentation about this fact. Full details about Microsoft's different servicing branches for Windows 10 can be found online at `https://pcs.tv/3BVcO1W`.

Semiannual Channel

The SAC is available as an option in all PC, laptop, and tablet editions of Windows 10. You can find it in Settings (there is no longer a Windows Update option in the Control Panel). Open *Update & Security*, and then click the *Advanced Options* link in the Windows Update section.

This will reveal Windows Update's limited configuration options. One of these is a drop-down menu where you can *Pause updates*; see Figure 16-1. Checking this will activate the CSAC deferment option and defer all Windows updates for a period of up to 32 days after their release.

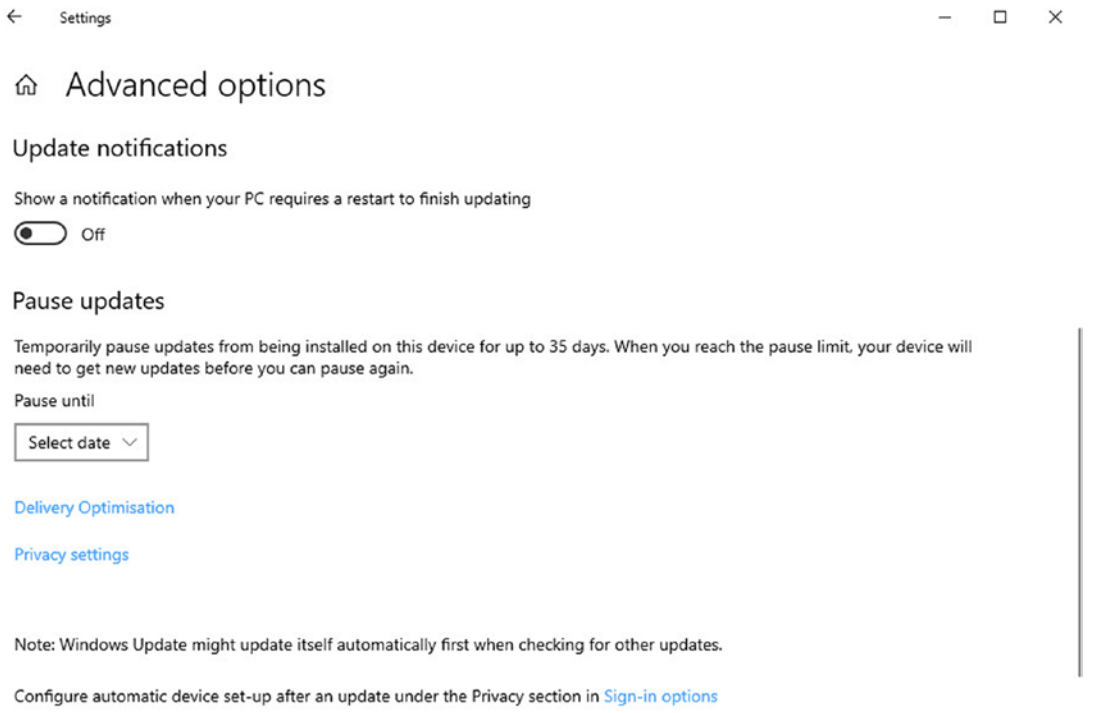


Figure 16-1. *The Defer Updates option can defer all but security updates for 3 months*

Long-Term Servicing Channel

The LTSC is available only for PCs running Windows 10 Enterprise that are managed by a Windows Server Administrator. Once activated, it is similar to how the SAC works, except that the Upgrades deferment option will extend to a maximum time of 10 years.

Something of note regarding the LTSC is that it's only really intended for mission-critical systems, where operation will not change over time, and where user interaction with the desktop will be minimal. Examples of this are automatic teller machines (ATMs), medical or engineering systems, or point-of-sale terminals. These are systems where the inbuilt apps in Windows 10 would be very unlikely to be needed or used.

Because Microsoft Store apps in Windows 10 are updated much more frequently, they are blocked from installation entirely on systems configured for LTSC. No Microsoft Store apps will be available or installable on LTSC-configured Windows 10 PCs. Win32 apps will still be installable.

Choosing How Updates Are Delivered

Another new feature in Windows 10 that pertains to how updates are delivered is that the OS now supports peer-to-peer update sharing. This works in three ways (see Figure 16-2):

1. Either it's off completely, in which case app updates only come directly to each PC through that PC's own Internet connection.
2. Updates provided by PCs on the local network are enabled. This means that a PC doesn't have to download part or all of an update from the Internet, which can reduce the Internet bandwidth used by multiple PCs connected to a home or work network.
3. Updates will be provided by PCs on the local network or on the Internet. This is the same as option 2, except that updates can be provided to the PC over the Internet by other Windows 10 PCs that also have all or part of the update. Each PC configured in this way will also share its Windows Updates with other Windows 10 PCs around the world.

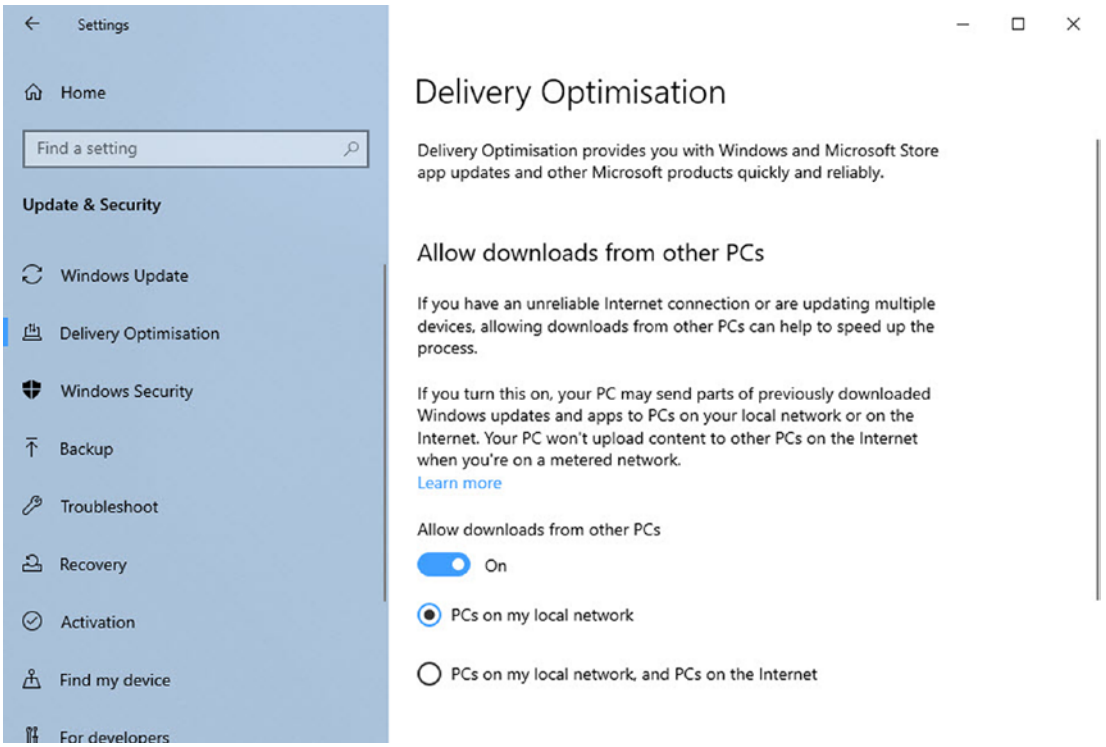


Figure 16-2. *Windows Updates can be delivered via a peer-to-peer system*

You may have a workplace with a large number of PCs and where bandwidth is at a premium, or very much needed for mission-critical work. If this is the case, there is a Group Policy setting you can use to force PCs to only get updates from other PCs on the network, and not from the Internet.

Open the Group Policy Editor by searching in the Start Menu for **gpedit,** and navigate to *Computer Configuration* ➤ *Administrative Templates* ➤ *Windows Components* ➤ *Windows Update*. Here you can enable the setting marked *Do not connect to any Windows Update Internet locations*; see Figure 16-3.

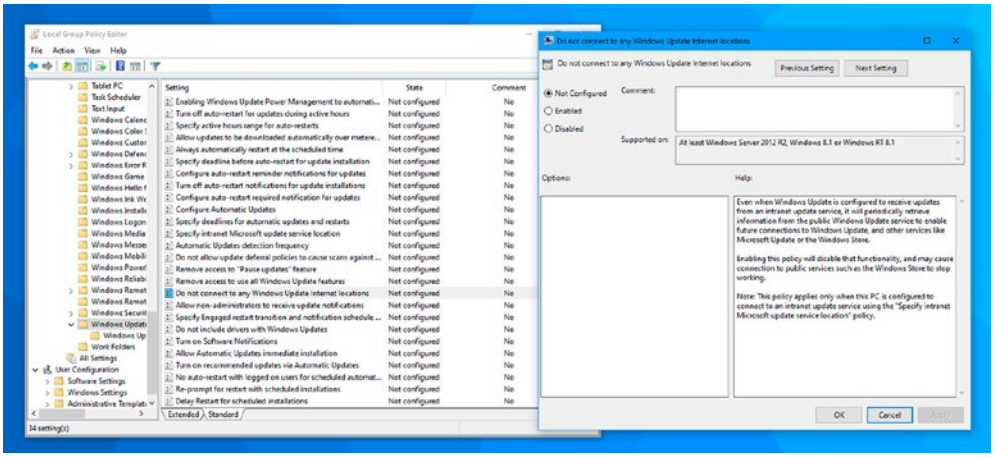


Figure 16-3. *You can force Windows to only get updates from other computers on your network*

Uninstalling and Blocking Updates

If a Windows Update needs to be removed from a PC, perhaps because it is conflicting with an app, is a faulty driver update, or is causing the PC to become unstable, this can be done from the *View update history* panel in the Windows Update Settings. Here you can click the *Uninstall updates* link, which will open a Programs and Features window where offending updates can be removed by right-clicking them; see Figure 16-4.

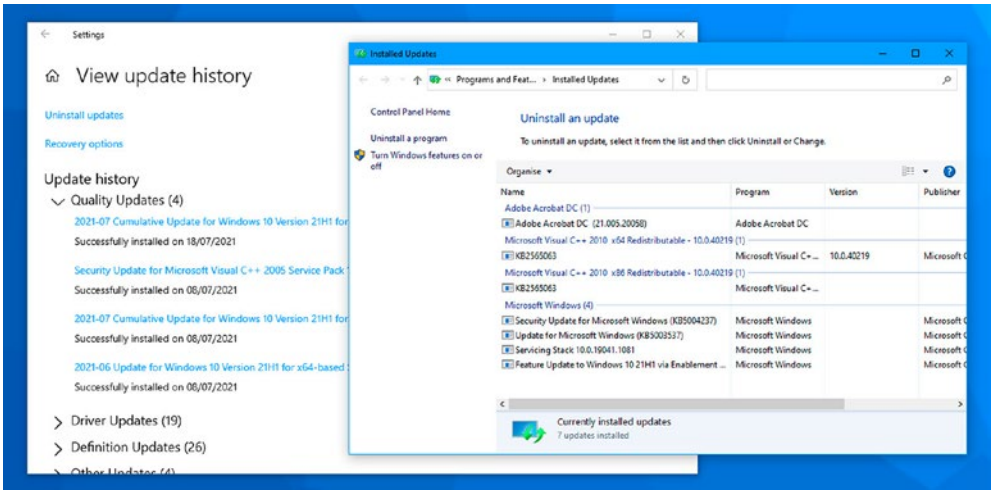


Figure 16-4. *Windows Updates can be uninstalled through the Settings app*

I mentioned in Chapter 15 a downloadable troubleshooter Microsoft used to provide called Show/Hide Updates. Microsoft has removed this useful tool from their website, but some third-party websites still host it. Called **wushowhide.diagcab**, I have found it hosted at MajorGeeks on the link `https://pcs.tv/3jfVTPd;` however, this comes as always with a caveat to use caution downloading anything from a third-party website, and you should always virus-scan any file you download before opening it.

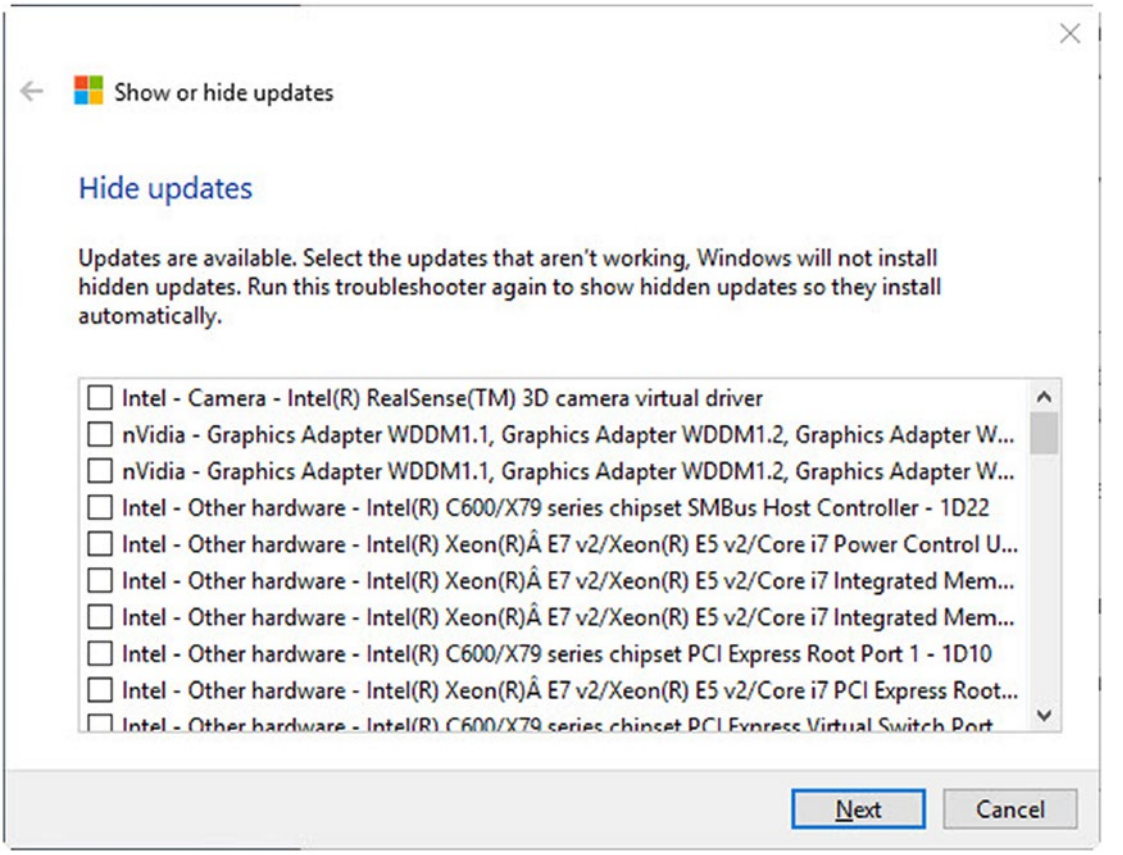


Figure 16-5. *Microsoft has released a tool that can block Windows Updates*

The Show or Hide Updates Troubleshooter works on a per-PC basis. Should you wish to block updates on PCs managed by Windows Server, you will have a tool available to you through the System Center Configuration Manager.

Tip The *Update & security* panel in the Settings app allows PC users to enroll in the Windows Insider program. This is a beta program for new Windows 10 features and releases, and it completely overrides the current Windows Update settings. The *Insider Preview Builds* option can be disabled in Group Policy in *Computer Configuration* ➤ *Administrative Templates* ➤ *Windows Components* ➤ *Data Collection and Preview Builds*.

Troubleshooting and Repairing Windows Update

So what happens should Windows Update become corrupt and stop working? This does occasionally happen, and you may find that updates will either flatly refuse to install or even refuse to download at all. In this circumstance it's straightforward to reset Windows Update, though you might need to restart your PC first if Windows Update has recently been in use.

To reset Windows Update, open the Services panel by searching for **services** in the Start Menu, and scroll down the list until you see *Windows Update* and *Windows Update Medic Service*. Right-click both of these and select *Stop* from the context menu that appears; see Figure 16-6. These services will restart automatically when you next reboot the PC.

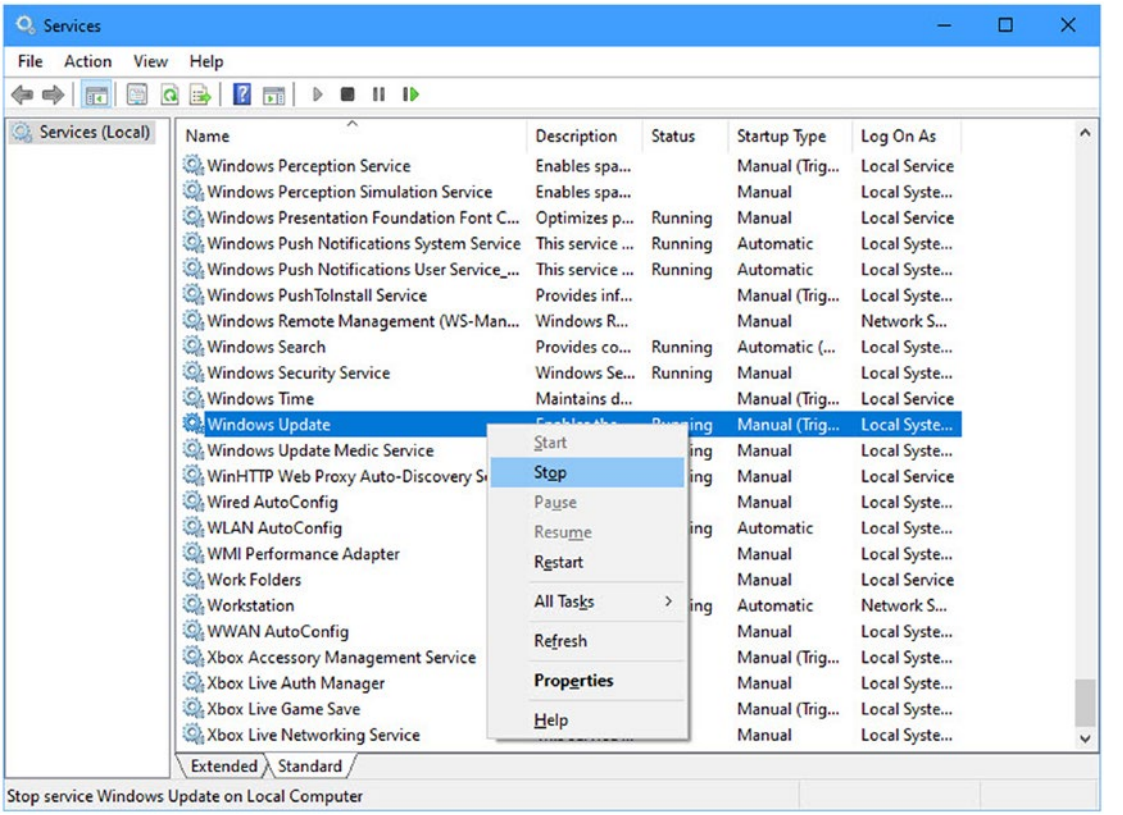


Figure 16-6. *You need to stop the Windows Update Services*

Next, open File Explorer and navigate to `C:\Windows\SoftwareDistribution`. This folder, seen in Figure 16-7, contains all the downloads and configuration options for Windows Update. You can completely delete the entire contents of the SoftwareDistribution folder if you want, and it won't harm the PC at all. Should you do this, however, Windows Update will be completely reset, which will include any updates you may have hidden. Perhaps a preferable option is to delete the Download folder (or its contents). This will delete any updates that have partially or completely downloaded, but that will be corrupt, preventing installation.

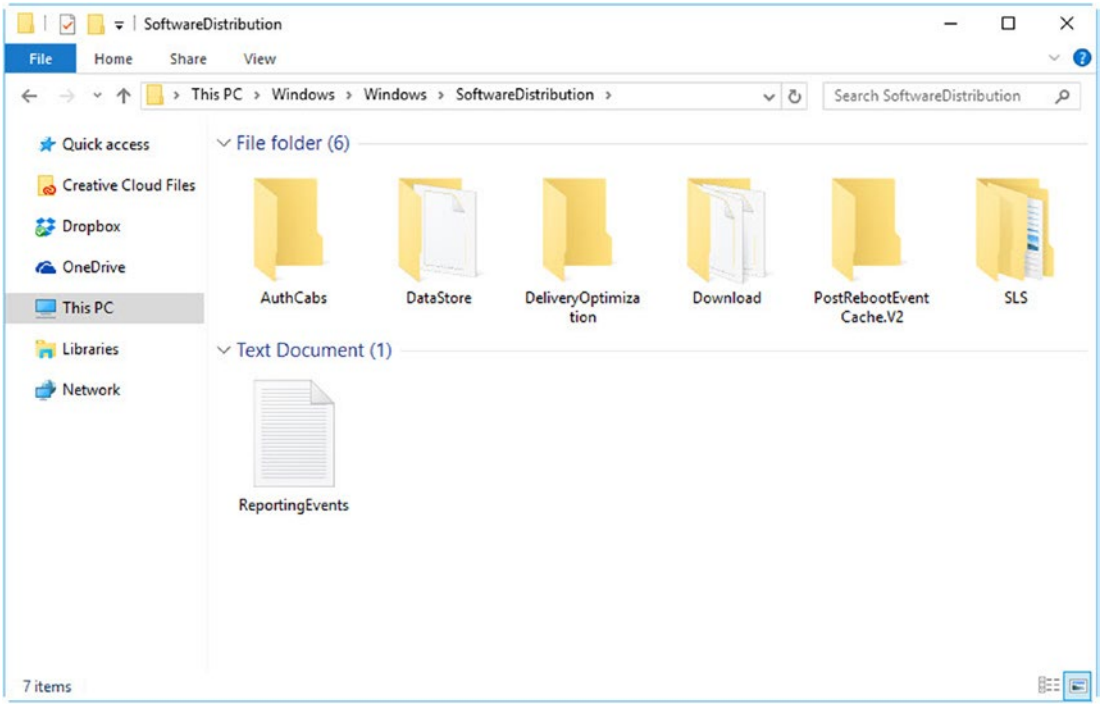


Figure 16-7. *The SoftwareDistribution folder contains Windows Updates downloads and config files*

Repairing the Windows Reset Image

In Chapter 2, I showed you how you can repair and reset Windows 10 by using its inbuilt Reset feature. This is different from a System Image Backup, which is a single disk image file containing a snapshot of the disk or partition on which Windows 10 is installed, complete with copies of the boot partitions, at the time the backup was made.

Reset doesn't have a single image file. It does work from a backup version of the main Kernel file, `install.wim` (the root operating system), which is hidden away in a backup partition. This file is very small though and isn't the full OS as installed on your PC. The rest of the files sit in the folders beneath the `\Windows` folder and are updated periodically by Windows Update.

The System Image Backup restore method is superior to the Reset feature in the following way: all of your installed Store and win32 apps, and all of your settings and configuration options, are kept intact. Where it fails is that you then have to download any and all updates to all those apps (and, crucially, to Windows 10) that have been

released since the snapshot was made. This can take a considerable amount of time, especially considering you'll likely still be using the same Windows 10 installation for 10 years… or more.

Reset uses the files that come from Windows Update to make sure that, when the PC is reimaged, it's also up to date (it won't update your apps, however). This can save considerable time in downloading the half a million Windows Updates that were released since you first installed Windows 10 on the PC.

"But," you might say, "what if it's a Windows Update that buggered my PC in the first place?" The Reset feature will only use Windows Updates that have already been installed on the PC for 30 days or more, the theory being that if you've been using them for the last 30 days, they'll be alright and won't cause any problems.

Occasionally, the core `install.wim` image backup file required to make Reset work can itself become corrupt. Microsoft has included a tool within Windows 10, however, that can check this Reset image and, if necessary, repair it. You run this from a *Command Prompt (Admin)* window from the desktop or the Recovery Environment, with the following commands:

- **DISM /Online /Cleanup-Image /CheckHealth** will verify if any corruption has been detected in the Reset Image files. It will not perform any repairs, however.
- **DISM /Online /Cleanup-Image /ScanHealth** will check for file corruption and will take much longer than the /CheckHealth switch. It will also not perform repairs.
- **DISM /Online /Cleanup-Image /RestoreHealth** will scan the Reset image files for any corruption, and repair any damage automatically, taking the repair files it needs from your installed copy of Windows 10 and also fresh copies of appropriate files from Windows Update.

If you have a situation where you are trying to repair the Reset image, but your Windows installation is itself corrupt, you can use an existing Windows 10 installer ISO file. It's best to get a fresh one (that's up to date with all the latest upgrades) from the Windows 10 Download page. You can find this online at `http://pcs.tv/1M2It5N`.

Download the Media Creation tool, and use it to create an ISO file (you may need to do this on another PC if your main Windows installation isn't working properly). Once the ISO file is created, you can burn it to a DVD by right-clicking it, or if it's downloaded to the PC that needs repair, double-click it to mount it.

Now use the command **DISM /Online /Cleanup-Image /RestoreHealth /Source:D:\sources\install.wim**, where `D:` might need to be replaced by the drive containing the install DVD or mounted disk image. The repair operation will try to use Windows Update to ensure the Reset image is repaired correctly. If you do not wish for Windows Update to be used, perhaps because you are on a metered Internet connection, you can also use the **/LimitAccess** switch to prevent the tool from accessing Windows Update.

Summary

It's very clear that Windows Update in Windows 10 is a very different beast from anything seen in earlier Windows versions. That isn't to say it's not configurable, and that it's not possible to block problematic updates. The hooks that Windows Update has into the Reset system can also be of enormous benefit.

In the next chapter, we'll look at the last of the big five problem areas, already having covered startup, network and Internet connections, device drivers, and Windows Update; I'll show you how to maintain *compatibility* with the older win32 apps, websites, and intranets we all still need to use in our working lives.

CHAPTER 17

Maintaining App and Website Compatibility

Having a stable, reliable, and robust PC, with a good network and Internet connection that's fully updated and configured as you need it, isn't going to help you much if you can't use the apps or access the websites or intranet sites that you need. Apps are everything. From the smallest utility that sits in your system tray to a major suite such as Adobe Creative Cloud, or a custom app that was written specifically for your business, if you can't use the apps you need, you can't get anything done at all.

It doesn't stop there either. Your business may rely on websites or an intranet site that was designed and programmed some years ago, but which needs to be maintained and kept in use. This site may rely on specific web browser plug-ins or web standards that were de rigueur at the time.

It's easy for the world to say it's moved on, and that technology and standards have moved on. If your business relies on older technologies, which would be prohibitively expensive to rewrite, at least in the short term, you have to find ways to get everything working that you need.

The good news is that Windows 10 is a very legacy-friendly operating system, both supporting win32 apps that would run happily on Windows 7 and having good compatibility solutions for those that didn't. There are also compatibility settings for websites and intranets for both the Microsoft Edge and Internet Explorer 11 (IE11) (which remains in the OS for all users).

Maintaining compatibility is everything. I mentioned in the previous chapter that even Windows Store apps aren't immune to compatibility problems. Should an Enterprise PC be placed on the Long-Term Servicing Channel (LTSC), in which only security and stability updates are delivered for 10 years, you might find that after a

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_17

while your custom or even the standard Microsoft Store apps stop working. This will be because, as the app framework evolves and apps are updated, they will require new OS features that will be rolled out over the years but that won't be included in the LTSC updates.

Maintaining Compatibility with Win32 Apps

Let's begin with win32 apps, otherwise known as the desktop apps we've all been using since the days of Windows 95 (technically we were using them in Windows 1, but the win32 framework changed considerably with the move to Windows 95, and the onward march to the modern Windows NT kernel).

Windows 10 is quite good at detecting problems with win32 apps, and it will alert you if it detects that an app didn't start, run, or close properly. It's possible to have Windows 10 assist in making apps compatible, however, or to set compatibility manually on a per-app basis.

There are four ways to get to the app compatibility settings in Windows 10:

1. From an app that's pinned to the Taskbar, right-click it and then right-click the app name again in the jumplist that appears. From the context menu that appears, select its *Properties*; see Figure 17-1.

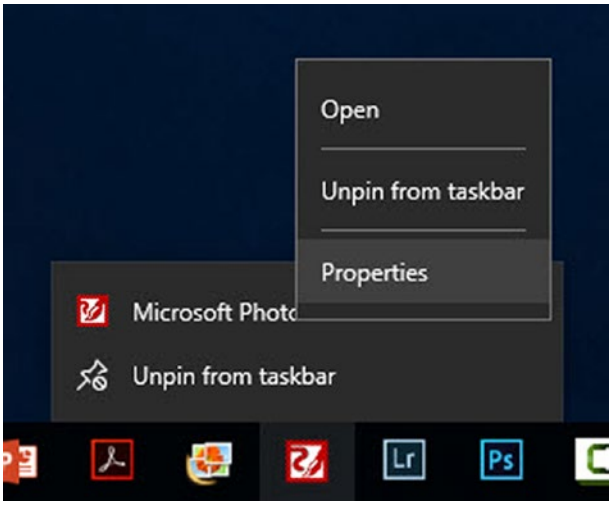


Figure 17-1. *You can access an app's properties panel from the Taskbar*

2. From the Start Menu, right-click the app, and from the menu that appears, click More and then click Open File Location; see Figure 17-2. In the window that appears, right-click the app (which should already be highlighted), and select *Properties* from the menu that appears.

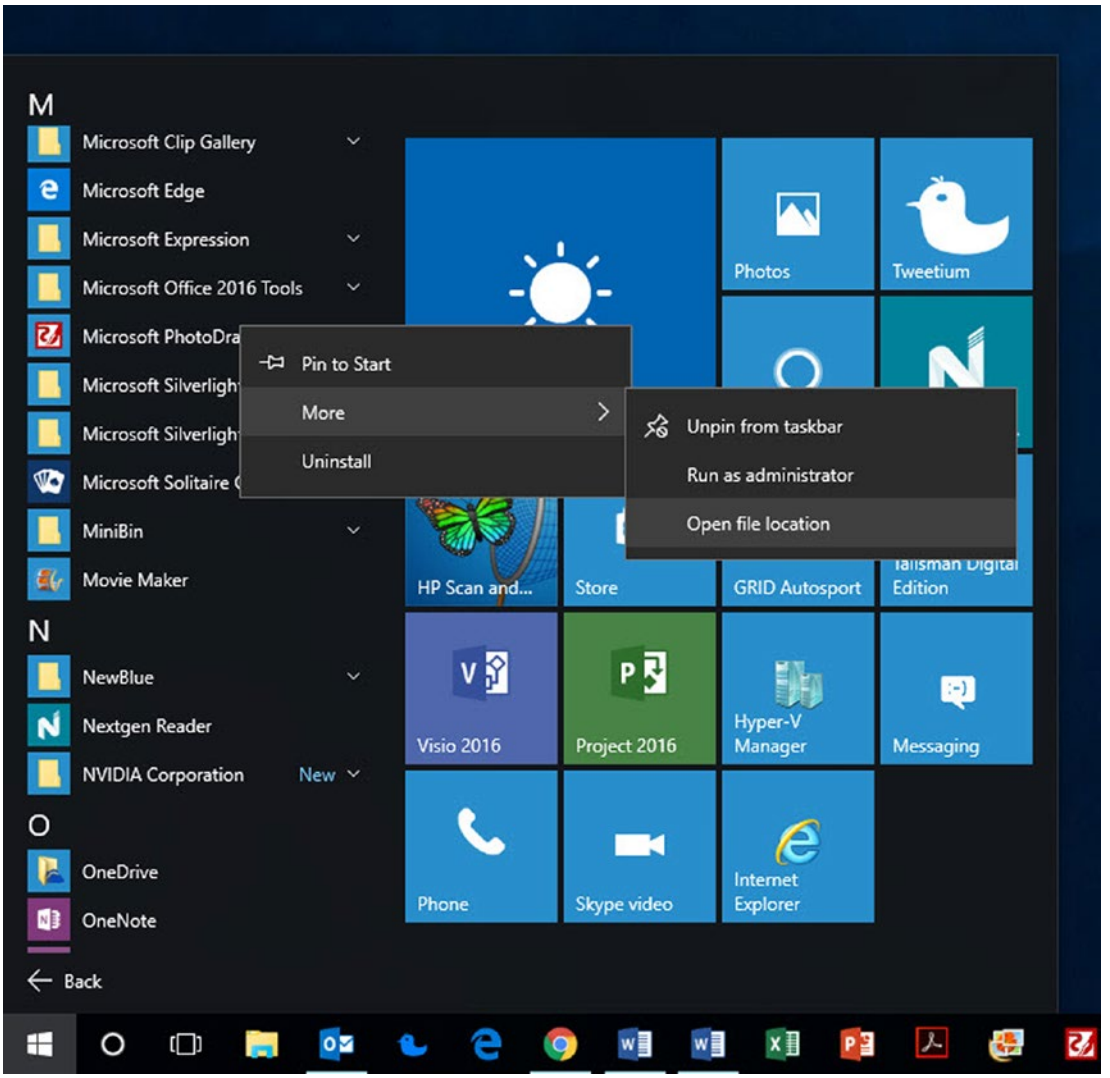


Figure 17-2. *You can access an app's properties panel from the Start Menu*

3. Open the installation folder for the app, if you know what it is. In the example I'm using here of Microsoft PhotoDraw 2000 (which I still use almost every day as it's brilliant!), it's `C:\Program Files (x86)\Microsoft Office\Office`. Then right-click the app launcher, and select *Properties* from the menu that appears.

4. If you are having trouble installing a win32 app, right-click the installer file, and select Properties from the menu that appears.

When the App properties panel appears, click the Compatibility tab, and it is here that you have several options and courses of action available to you; see Figure 17-3. At the top of this dialog will appear a button to *Run [the] compatibility troubleshooter*.

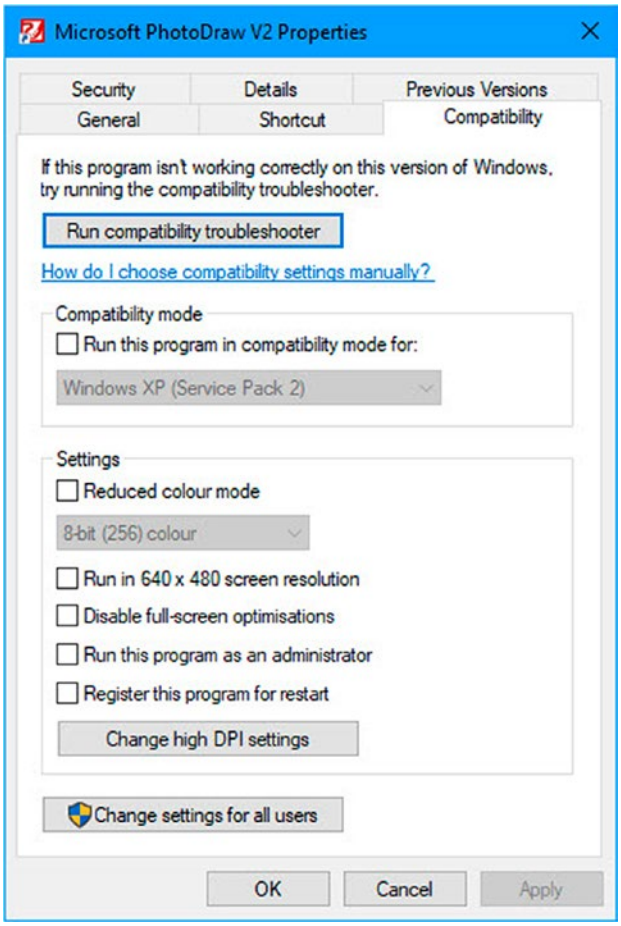


Figure 17-3. *The Compatibility tab in the App properties panel lets you manage compatibility*

Running the compatibility troubleshooter app will display a wizard that will present you with a series of options to describe the problems you experience; see Figure 17-4. These include "The program worked in an earlier version of Windows but won't install or run now." Selecting one or more of these description options will enable the troubleshooter to set app compatibility automatically. You will then be asked to run or install the app to check if the settings worked. If they don't, the troubleshooter will offer you additional options.

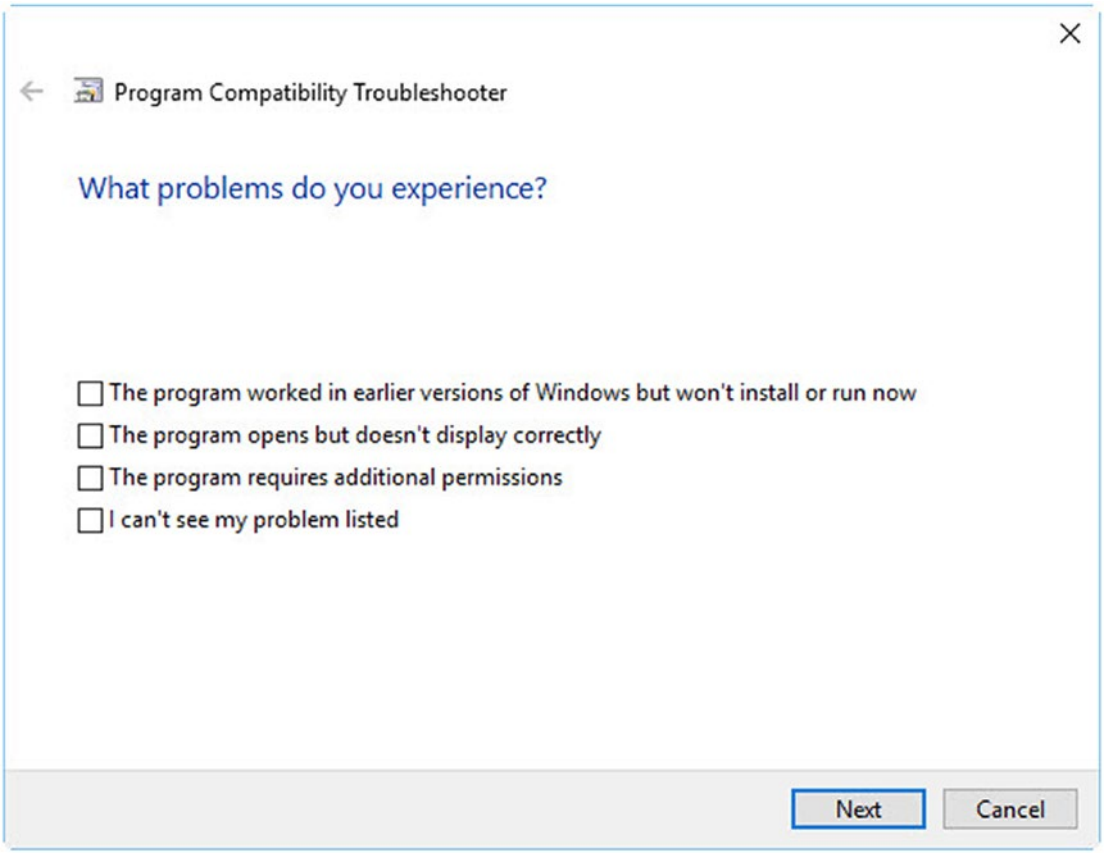


Figure 17-4. *The App compatibility troubleshooter can set compatibility automatically*

If you want or need to set app compatibility manually, there are several options available to you. The first is a drop-down menu that lists every Windows version going back to Windows 95 (20 years before Windows 10 was released); see Figure 17-5. Remember I said that the app framework before Windows 95 was very different, and I'll come to this shortly.

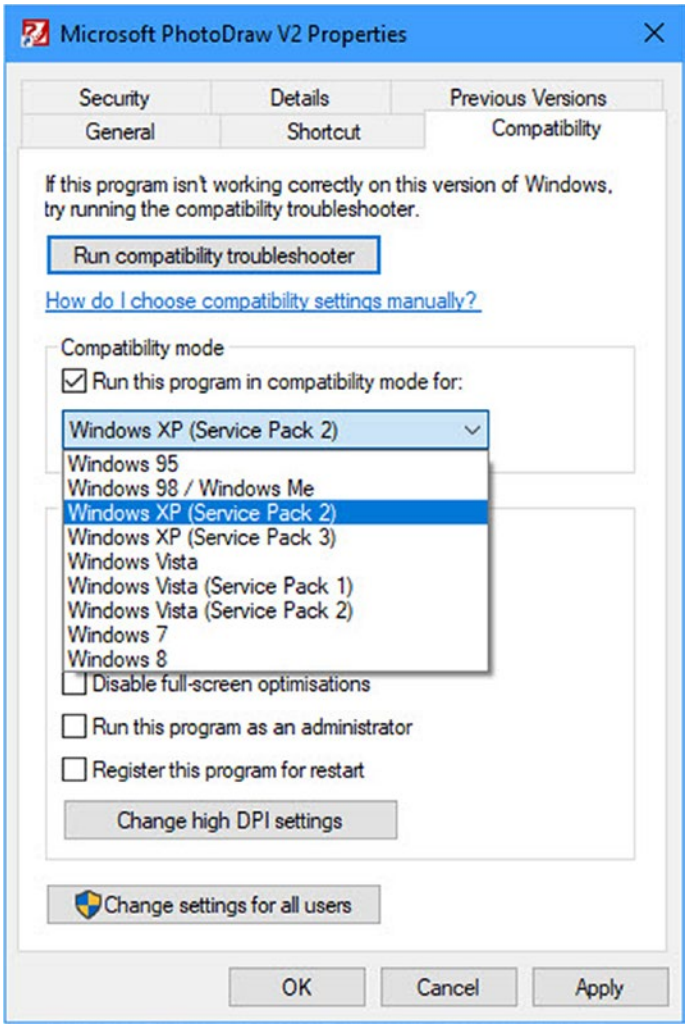


Figure 17-5. *You can choose an OS version the app ran in before*

Now, I want to stress an important caveat at this point, as simply setting *Run this program in compatibility mode for [an older OS version]* won't fix every problem. This is because, as Windows has evolved over the years, many features and services in the OS have changed or been dropped altogether.

I'm using Microsoft PhotoDraw 2000 v2 for this demonstration, which was released when Windows 98 and ME were the current desktop operating systems in use. PhotoDraw has an incompatibility today in that none of the 3D modeling features in the app will work. This is because they rely on Direct3D, which has changed so considerably

since its first release in 1996 that it's completely incompatible with PhotoDraw today. This is okay for me, as I can live without the 3D features, but it's a good example of how Windows has changed and evolved with technology.

So what happens if you have a *really* old app that you still want or need to use? You might have an app that you still need to use, but that was written back in the days before high-DPI displays and User Account Control, 20 years ago or more. Below the Windows version selection drop-down menu are five additional options; see Figure 17-6.

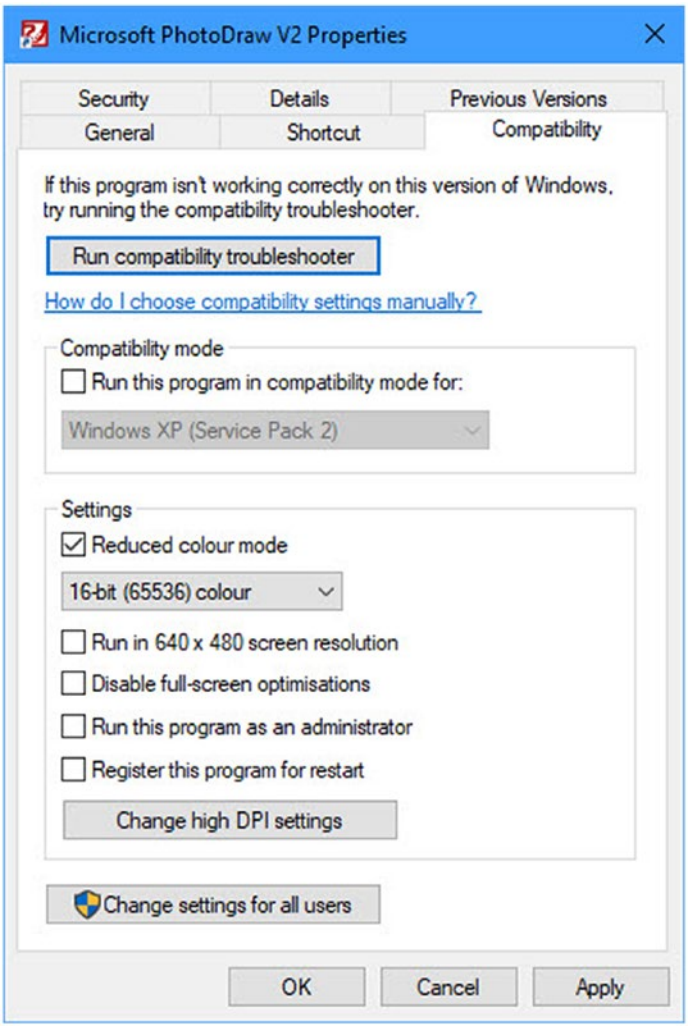


Figure 17-6. *You can set compatibility for 20-plus-year-old apps in Windows 10*

- **Reduced color mode** will force the app to run in either 8-bit, 256-color, or 16-bit, 65,535-color mode. This maintains compatibility for apps that do not render correctly, because they were designed for old VGA (Video Graphics Adapter) screens that typically used a 640-by 480-pixel resolution (I'm writing this on a 4K display that has 27 times the resolution of VGA, and can't imagine having a desktop that small any more).
- **Run in 640 × 480 screen resolution** will force the app to stay within a confine of a VGA-size window. This is used if the app doesn't display properly when resized on your screen or run in a regular Windows 10 window.
- **Disable display scaling on high-DPI screens** is used because on high-DPI screens (such as my own 4K display), it's common to tell Windows 10 to scale the desktop by 125%, 150%, or even 200%. This makes text and other items on screen larger, but it can also break the rendering of apps that were designed before this feature came about. Checking this option will force Windows to ignore desktop scaling for that app.
- **Run this program as an administrator** is a tricky one that I'd like to spend a bit more time on, so let's do just that…
- **Register this program for restart** will automatically restart the program if it has been open for at least 60 seconds before crashing or becoming unresponsive.

Caution Some legacy apps on Windows, and by this I mean apps that were written for Windows 95, Windows 98, Windows ME, Windows 2000, and Windows XP, were written in such as way as to exploit the fact that the default user of a PC was an Administrator who could do anything they wanted, at any time. This presented a major security risk, thus bringing about the introduction of User Account Control in Windows Vista. Because users could change any setting, delete any file, or modify any configuration option, so could malware (and it often did). It's now considered "sloppy" coding when apps relied on this functionality, and often this was a workaround meaning developers didn't have to code their apps properly. Should a legacy app require Administrative rights in order to work, this presents a security risk to your PC. Any malware that attacks the app can take advantage of its Admin rights to make any change it wants to your system, such as injecting more malware or a rootkit virus. Should an app need to be run as an Administrator, it should, ideally, be completely sandboxed in a virtual machine, and I will show you how to do this in Chapter 20.

It is very common on new PCs and laptops to use Windows 10's desktop scaling features to compensate for 4K and even 5K screen resolutions where, if just left at 100% scaling, icons and text could look absolutely tiny. Some older programs simply cannot cope with this desktop scaling and can go completely loopy when faced with it.

If you click the *Change high DPI settings* button however, you can set specific options or overrides for DPI scaling for the app, though the compatibility settings to alert you that your app might appear blurry (just like my head after last night's wine; Ed) and need additional configuration on the *Open advanced scaling settings* link; see Figure 17-7.

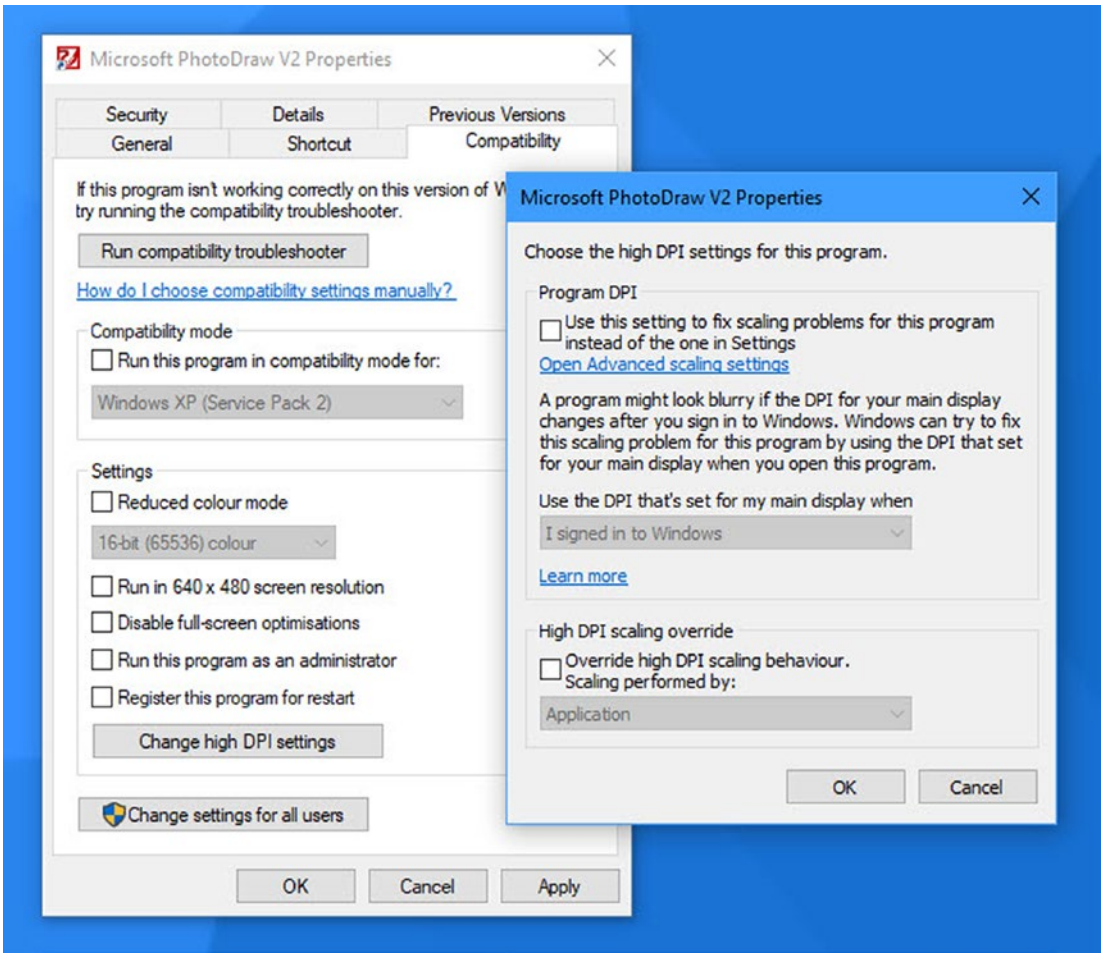


Figure 17-7. *There are specific settings if you use desktop scaling on high DPI displays*

Managing Website and Intranet Compatibility

Just as we use apps on our PC to accomplish tasks at home and in the workplace, web apps and intranets are also essential to our daily lives. You might use the Gmail website to read and manage your email, or Microsoft 365 to manage and collaborate on documents with colleagues. While these web services and web apps are regularly updated to ensure they work with the latest browsers, if you need to use an older website or intranet site for your business, things can be trickier. The good news, though, is that both Microsoft Edge and IE come with advanced tools for managing and maintaining website compatibility, and the better news is that these tools work the same way in both browsers.

Compatibility in Internet Explorer

In IE11, you can set and manage compatibility with websites and intranet sites using the *F12 Developer Tools*. These are accessed in the same way in both browsers, by selecting F12 Developer Tools from the browser Settings menu (see Figure 17-8), or (oddly enough) by pressing the F12 key on your keyboard (i.e., if you have an F12 key).

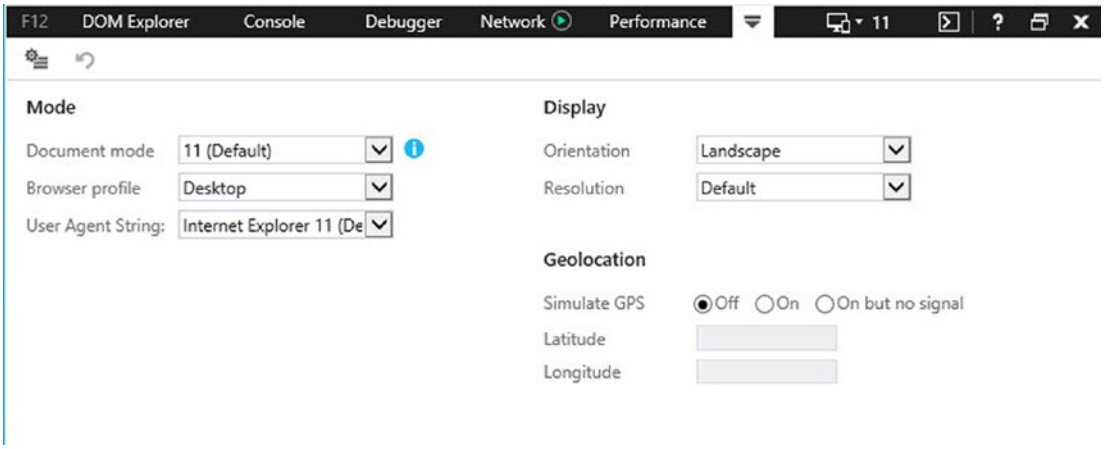


Figure 17-8. *The F12 Developer Tools are available in both Edge and IE11*

The following compatibility settings are available both Edge and IE:

- **Browser Profile** lets you choose if the web or intranet site is designed primarily for a desktop or smartphone display.
- **User Agent String** will present a long list of browsers. You can choose which one the website or intranet site worked well with; see Figure 17-9. These include every version of IE going back to IE8 (in Edge) and IE6 (in IE11), Mozilla Firefox, Google Chrome, and Apple Safari.

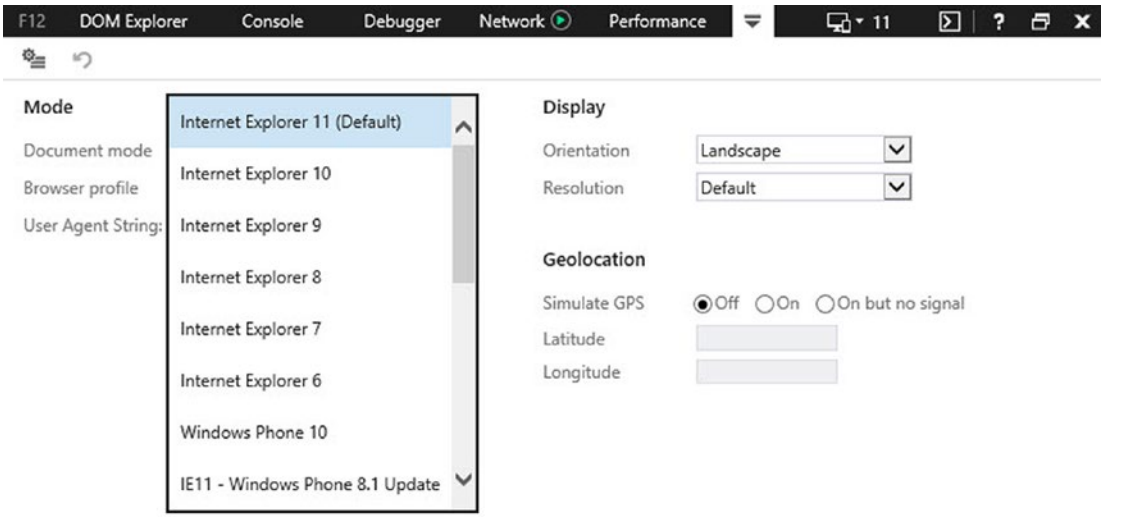


Figure 17-9. *You can choose which browser the website or intranet site worked in before*

Tip The F12 Developer Tools in IE11 additionally support compatibility modes for IE versions 7 and 6. IE6 was around for many years, and many intranets still exist that were written for it, though the browser itself wasn't what we'd now call either "standards compliant" or "secure."

- **Orientation** allows you to set a default portrait or landscape orientation for the site. This can be used if the site does not render properly in the browser, or if the layout doesn't properly fit the browser window.
- ***Resolution*** is again used if the web or intranet site does not render properly in the browser window, because it was designed for a specific screen resolution on older PCs. You can set resolutions between 2560 × 1440 and 800 × 480 pixels (see Figure 17-10), or you can set Custom options if a web or intranet site requires, say, a 640 × 480 maximum resolution to function correctly.

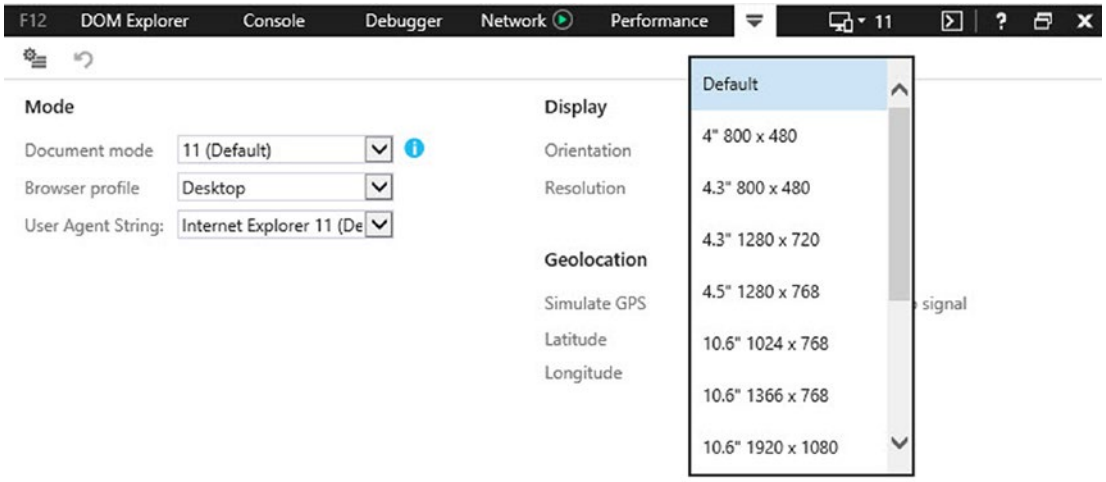


Figure 17-10. *You can force the website or intranet site to be constrained in a specific maximum resolution*

- **Geolocation** is used only if the website or intranet site requires the use of GPS or Windows geolocation features, but either your PC does not support them or they have been disabled in Group Policy. You can fix a latitude and longitude that will be given to the website by the browser.

Compatibility in Microsoft Edge

Microsoft Edge doesn't have the fine control available in Internet Explorer; however, it's arguable now that the number of websites and, especially in the days of Microsoft 365 and Azure, intranet sites that require compatibility settings will be absolutely miniscule (though yours will be one of them I'm certain as you've not skipped over this chapter).

What it does have though is an Internet Explorer compatibility mode. You access this in the browser settings in the *Default browser* options. Here you can set Internet Explorer compatibility for all websites and intranet sites, or just ones where the browser detects an incompatibility; see Figure 17-11. Should your website or intranet not be detected, you can add it manually to the options.

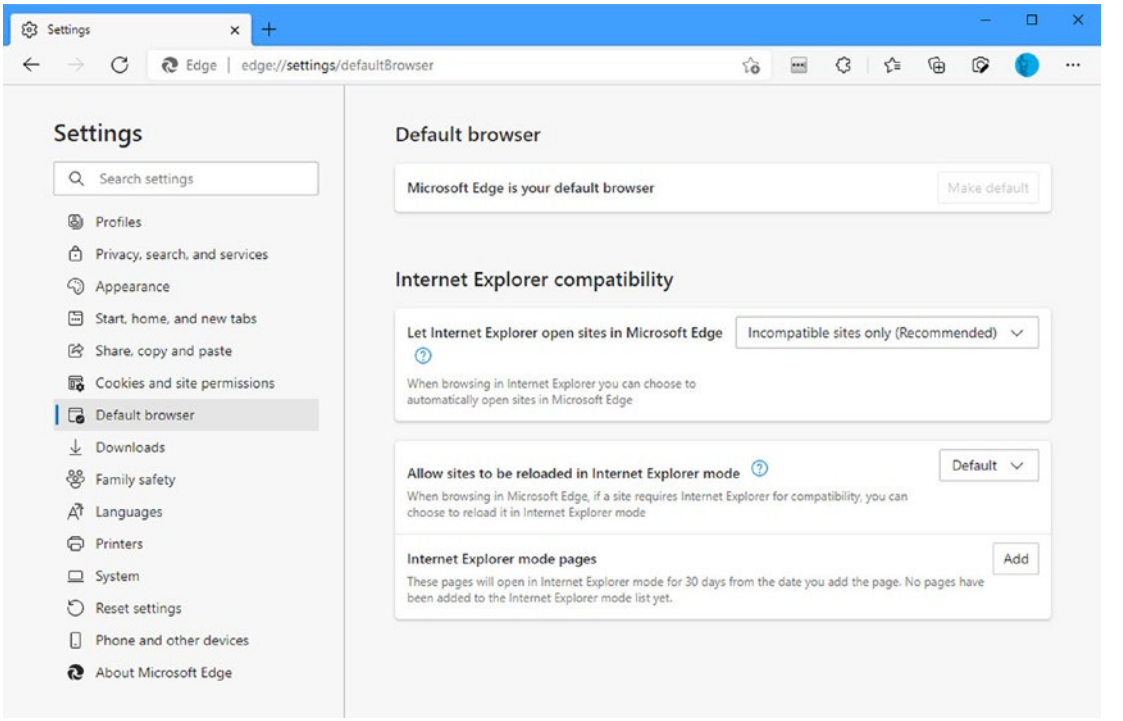


Figure 17-11. *Microsoft Edge comes with an Internet Explorer compatibility mode*

Managing Security in IE

Earlier in this chapter, I talked about how some older apps require Administrator rights in order to function correctly. This presents a significant security risk to any PC, because if malware can successfully attack the app, then it can pretty much do whatever it likes on your computer. Web browsers aren't immune to this, as while both Google Chrome and Microsoft Edge have some formidable sandboxing technologies built into them, IE… well… doesn't. As a result, it is *the* most attacked web browser in the whole history of the Internet, helped I'm sure by the runaway popularity of IE6, which, at one point, held 99% of the browser market, putting competitor Netscape (which I always really liked) out of business completely.

IE comes bundled with all editions of Windows 10. It's initially hidden, but you can search for it in the Start Menu after which time it will always appear in the Start Menu. You manage privacy and security in the Internet Options panel, which is available from the Settings menu in IE11 itself, but is also available from the Control Panel, and controllable through Group Policy.

Note Do you *really* need to use IE? Certainly for compatibility for legacy intranet and other sites, there's a strong case for doing so, but for everything else? The recommendation of this particular author is only to use IE11 for the tasks that it absolutely *must* be used for, and that a modern, secure browser such as Edge is used for everything else.

Security in IE11 is managed through, oddly enough, the Security tab in the Internet Options (also called Internet Properties) panel; see Figure 17-12. At the top of the panel are four "zones" for which you can set security permissions.

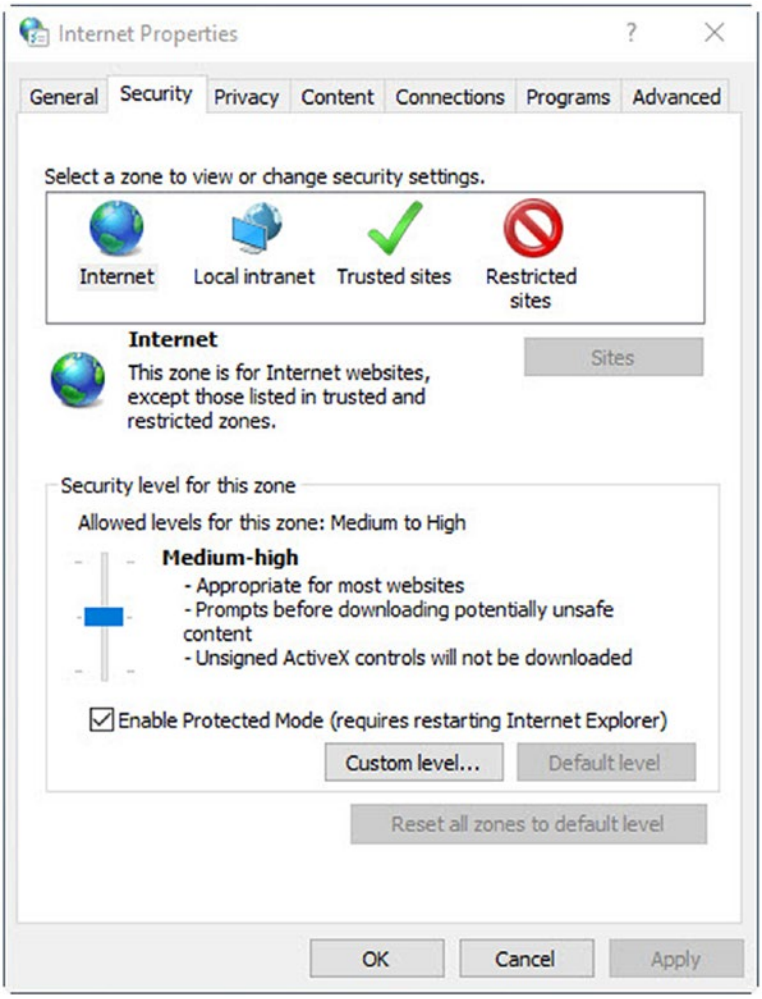


Figure 17-12. *IE11 security is managed in Internet Options*

- **Internet** is for, funnily enough, websites and anything not on your local network. Clicking the *Custom level* button allows you to approve and deny access for specific web technologies, such as ActiveX, which is notoriously attacked by malware. There is also a security-level slider control you can use to automatically set Medium, Medium-High, and High levels of security for the browser. If you use IE11 only to access certain websites, try setting the security level to high, and disabling all web technologies, reenabling them only as necessary to ensure your websites work correctly in the browser.
- **Local intranet** is for intranet sites run from your company network. It too has a security slider, which ranges here from Low to High, and a *Custom level* button in which you can disable specific web technologies. Additionally, there is a *Sites* button which you can click to permit only specific intranet sites. This feature can prevent malware from connecting to any website by spoofing the site as an intranet instead.
- **Trusted sites** are web and intranet sites that you definitely trust not to harm your PC or let in malware. If you only use IE11 for your intranet and a limited number of websites, it is good to add them to the trusted sites list.
- **Restricted sites** are web and intranet sites that you specifically do *not* want IE11 connecting to. Unfortunately, there isn't an option to "block everything except sites on the Trusted list"; instead, you need to specifically add websites you wish to block. This makes it less useful than other web filtering systems.

The *Privacy* tab is where you control (guess what) in IE11. It may sound frivolous, given that pretty much none of us have any privacy online these days, but it's very important to businesses. This is because cookies, which are small files that websites and intranets store on our PCs and that often contain login details, can also be used to track our activities with the site online.

A website may use its own cookies for innocuous purposes, perhaps as in the preceding example, to automatically sign you in each time you visit it. Sites can also place third-party cookies on your PC. Generally speaking, these almost always come

from advertisers, through advertisements displayed on the page. Very occasionally, though, an advert can deliver malware, and then any cookies placed could be monitoring your site usage in such a way you would not wish to permit.

You can click the *Sites* button to specify websites which must always or never be allowed to use cookies, but as with the Restricted sites list, this isn't a catch-all solution. You can instead click the *Advanced* button to define specific policies on the PC for accepting or blocking both first- and third-party cookies; see Figure 17-13.

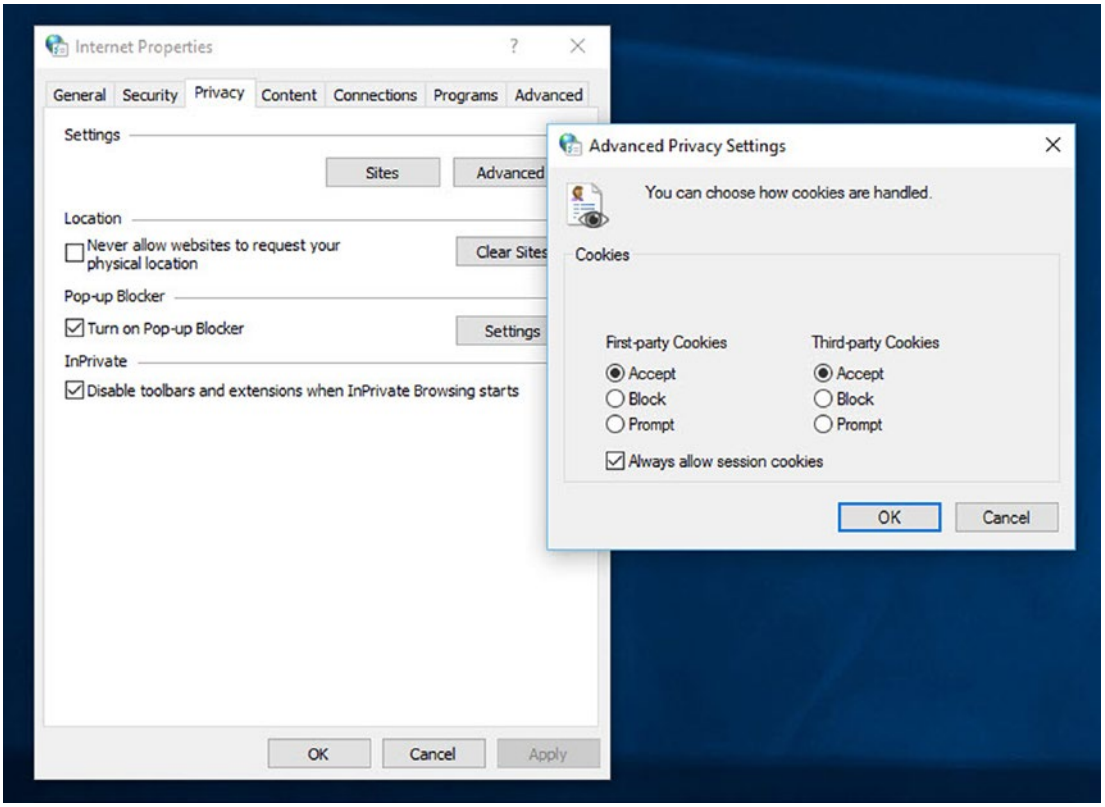


Figure 17-13. *The Privacy controls allow you to block cookies*

The *Content* tab is where you can manage IE11 features such as form, username, and password autocomplete. You can also manage security certificates through this tab, however. Secure websites, VPNs, Remote Desktop software, security tools, and intranet sites will have a security certificate, and here those certificates can be viewed, imported, or exported to other PCs (perhaps from a central server store) and wiped from the PC; see Figure 17-14.

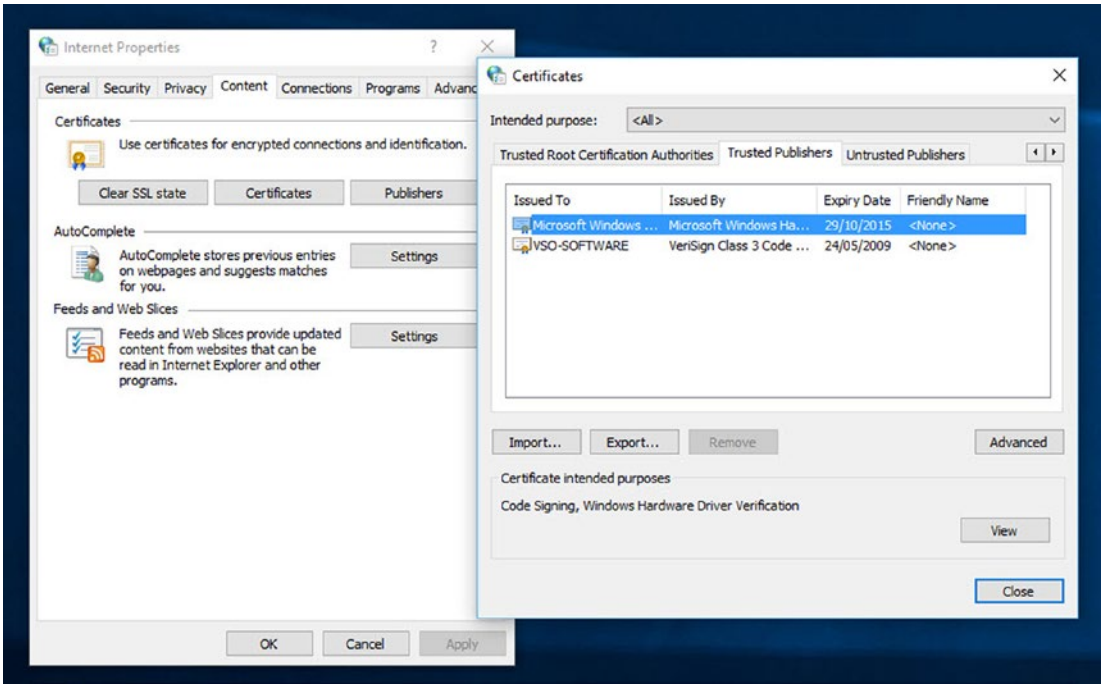


Figure 17-14. *The Content tab is where you can control security certificates for web and intranet sites*

Back at the General tab are controls for managing the files (cookies, passwords, usernames, web history, etc.) that build up during a session using IE11. You can manually delete these files by clicking the *Delete* button in the *Browsing History* section, or you can check the *Delete browsing history on exit*, to automatically delete the files each time IE is closed. If you click the *Settings* button, you can choose exactly what it is that is deleted, as not everything is deleted by default; see Figure 17-15.

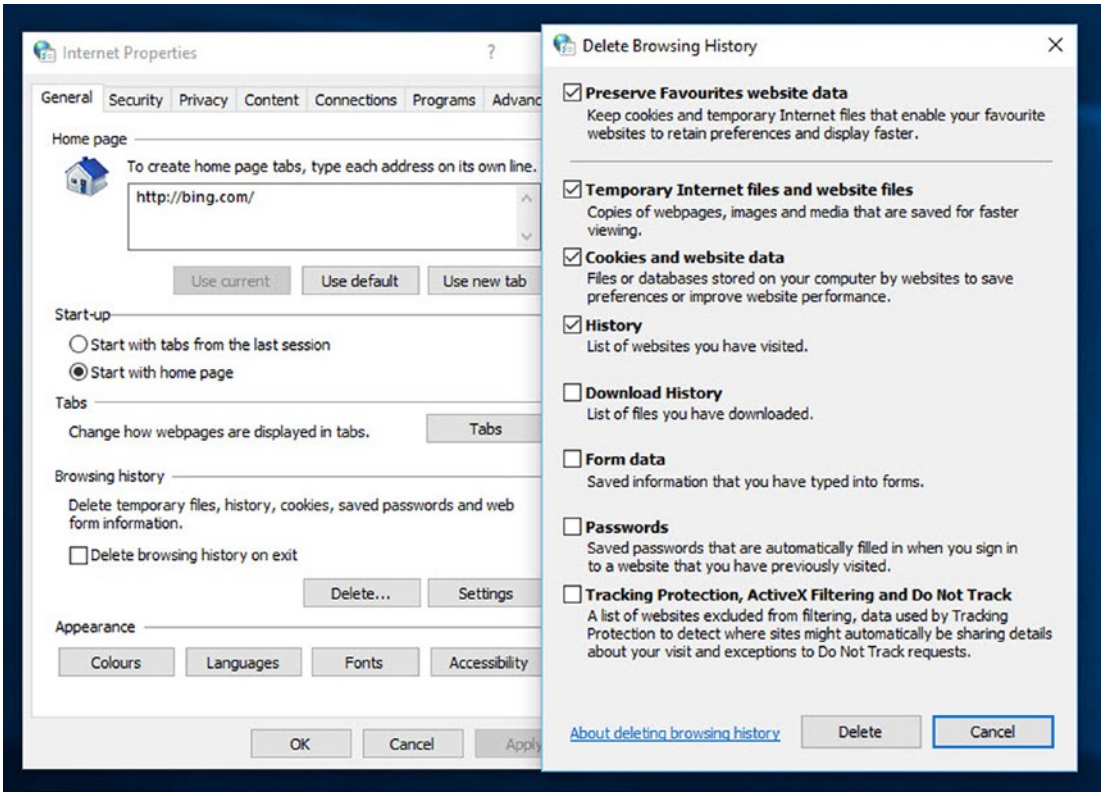


Figure 17-15. *You can manage the browsing history files in IE11*

Resetting IE

Despite all the controls available in IE11, and the Advanced tab containing yet more browsing and security options for the browser, you might find occasionally that IE11 fails to start or work reliably. Should this happen you can be faced with a problem, as you can't uninstall or reinstall the browser, nor will there ever be a newer version released you can upgrade to, as Microsoft has stated that IE11 will be the final version.

It is possible, however, to completely reset IE, which does have the same effect as completely reinstalling it (i.e., unless some core files have become corrupt), in which case a reset or reimage might be required. Under the *Advanced* tab in the Internet Options is a *Reset* button. Click this and you will be told that IE11 will be completely reset, and you'll also be given the option to delete all of your personal files, as a corruption with the browser might also be causing problems with them; see Figure 17-16. I would point out, however, that resetting IE11 will not affect your stored website Favorites, as these are stored elsewhere in your users folder.

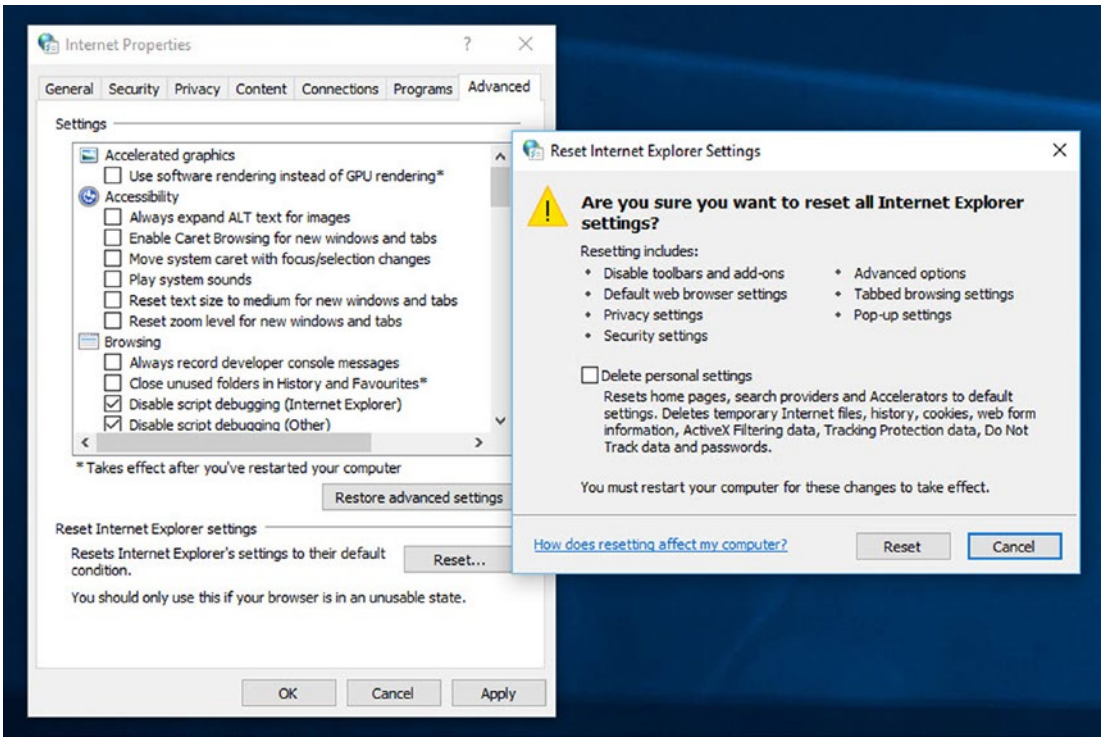


Figure 17-16. *You can completely reset IE11*

Managing Security in Edge

There are fewer security options in Microsoft Edge, but it's easily arguable that less configuration is required as the Chromium core the web browser is based on, and the additional work Microsoft have done to the core features of Edge, make it extremely secure to begin with.

Navigate in the Edge settings to *Privacy, security, and services*, and you'll find a few options; see Figure 17-17. These mostly revolve around the additional security services already baked into Windows 10 such as SmartScreen. It could be however that an older site is being blocked by SmartScreen or that a website or intranet plug-in is being blocked. You can control those settings here.

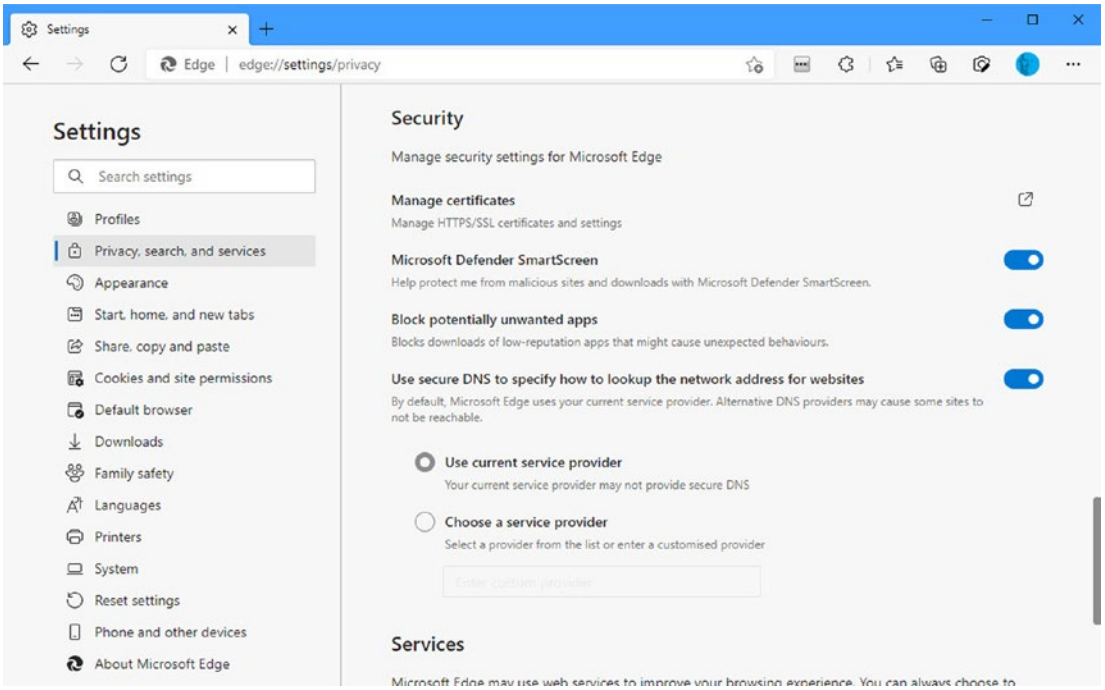


Figure 17-17. *There are security settings available in Edge*

Perhaps the most useful security setting here is to be able to manage and import security certificates. Your business may rely on them to authenticate a laptop or desktop PC with a secure server (perhaps you even work at the CIA, MI6, or Mossad?). Click the flyout icon to the right of the *Manage certificates* section to open a dialog in which you can view, import, and export certificates; see Figure 17-18.

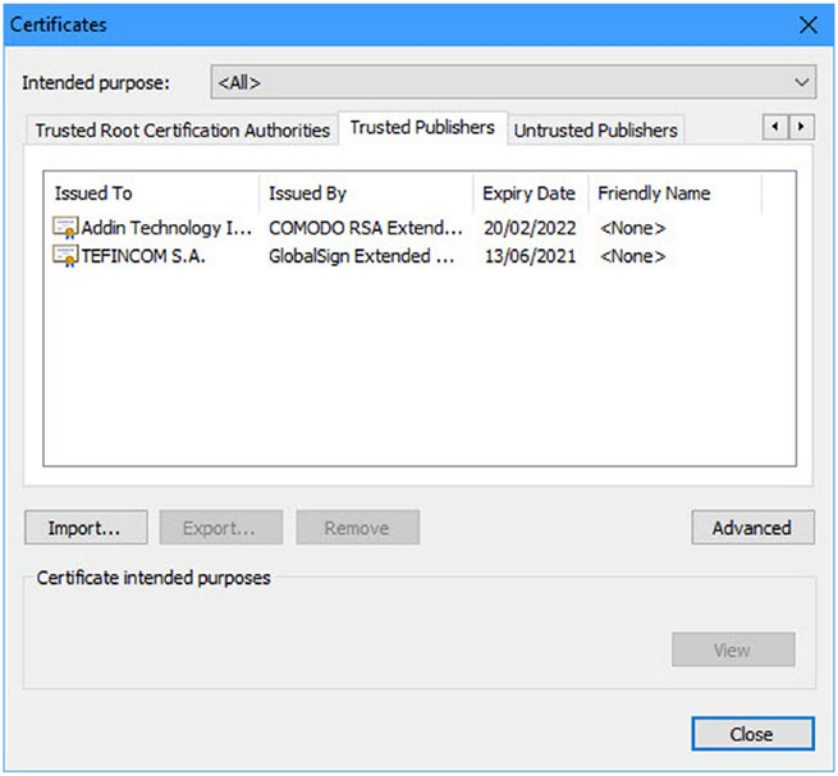


Figure 17-18. *You can manage security certificates in Edge*

Setting Your Default Web Browser

I mentioned earlier in this chapter that it can be wise to use IE only to connect to the legacy web and intranet sites that you need it for, and to use a more secure browser, such as Edge, for everything else. There are three ways to make sure that Edge (or another browser such as Google Chrome) is your default browser.

You can open the Settings app and navigate to *Apps* ➤ *Default Apps*, where the default web browser can be selected; see Figure 17-19.

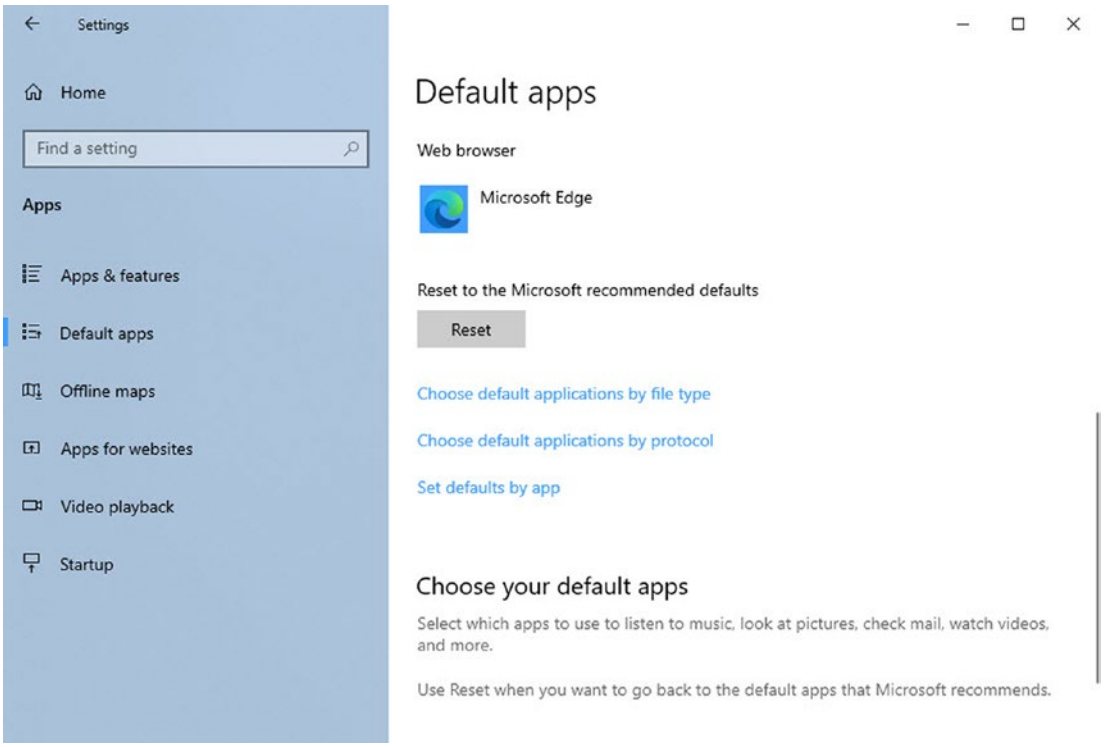


Figure 17-19. *You can set your default browser in the Settings app*

The default browser can also be set directly from within the Internet Options panel, though here you can only choose between IE and Edge; see Figure 17-20. Navigate to the *Programs* tab, and you will see an *Opening Internet Explorer* drop-down menu at the top of the dialog. Note that this menu will be grayed out if IE is not currently set as the default browser.

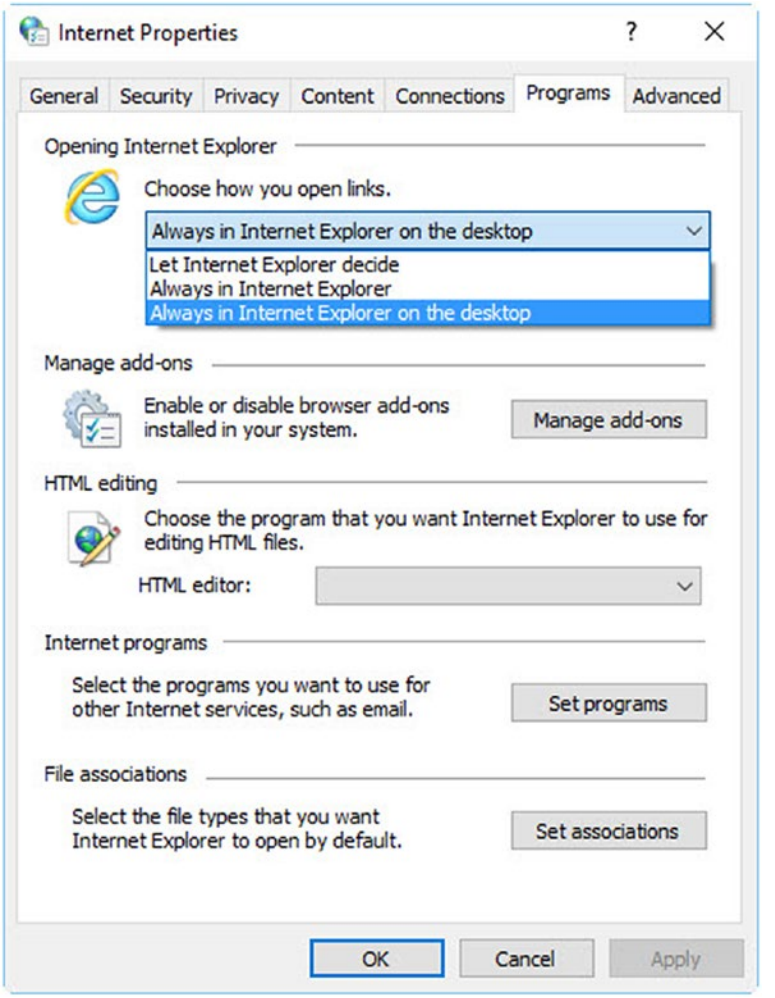


Figure 17-20. *You can also set the default browser from within the Internet Options*

In Microsoft Edge, open the browser's settings, and navigate to the *Default browser* section. Here you can set Edge as the default browser for the PC; see Figure 17-21.

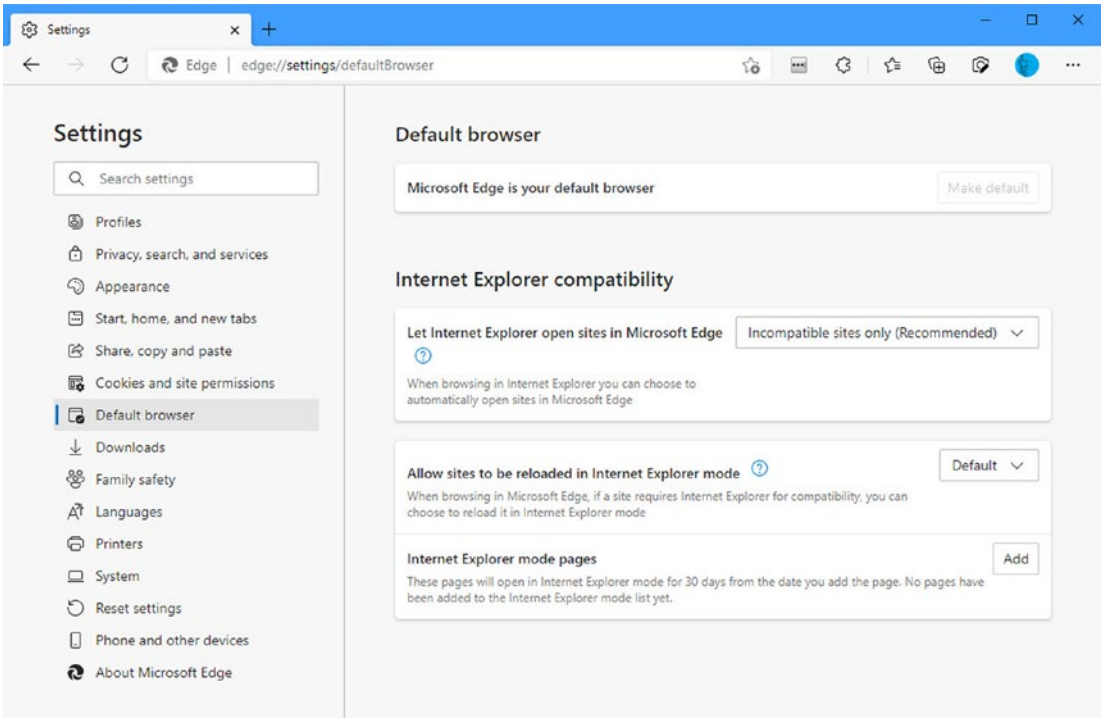


Figure 17-21. *You can set Edge as the default browser in the browser settings*

Using and Managing Progressive Web Apps

Progressive Web Apps (PWAs) are an idea that came out of Google, based on work and ideas that had previously come from Apple and Mozilla, to create websites that could be run natively on any smartphone or PC as though they were an app installed on the device itself. Indeed, it's very common now for PWAs to appear in app stores, and you will find them available in the Microsoft Store in Windows 10.

Indeed, the term PWA has almost become irrelevant as Microsoft Edge, along with just about every other modern browser, will allow you to install absolutely *any* website as an app (see Figure 17-22) where my own website, which is definitely not a PWA, can be installed and even have an icon pinned to the Start Menu or Taskbar.

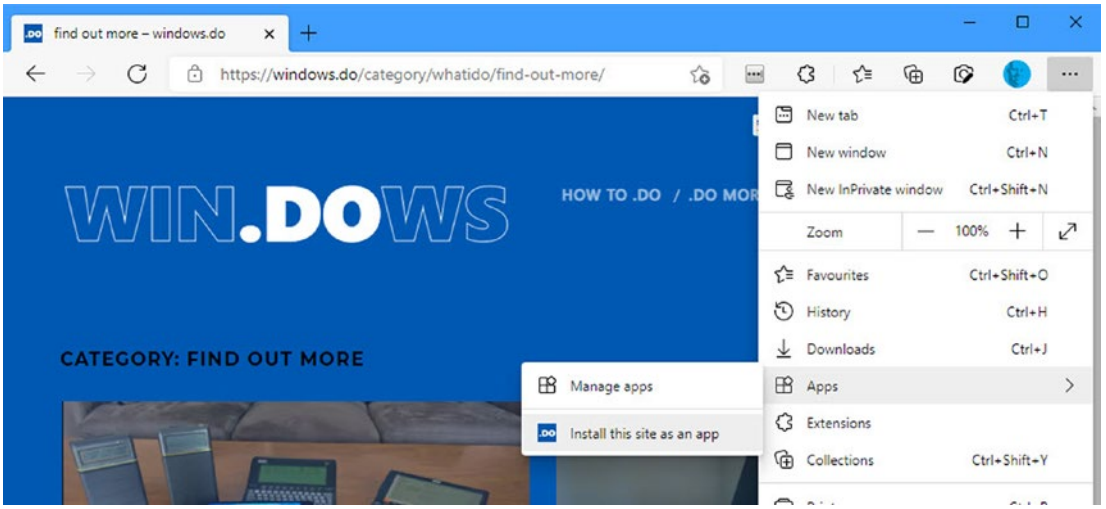


Figure 17-22. *Any website can be installed as an app*

The true definition of a Progressive Web App however is that it can be fully and properly used when the PC is offline without an Internet connection. Installing `Windows.do` as an app won't do you any good if you aren't online, as it simply won't do anything. Proper PWAs cache their code and, optionally, content so they can still work offline. This is most useful with email apps such as Outlook.com or Gmail.com, or with cloud-based productivity software like Office.com; see Figure 17-23. Indeed to the casual observer, they've have no idea they were using a PWA as they appear in their own window on the desktop and look just like any other app.

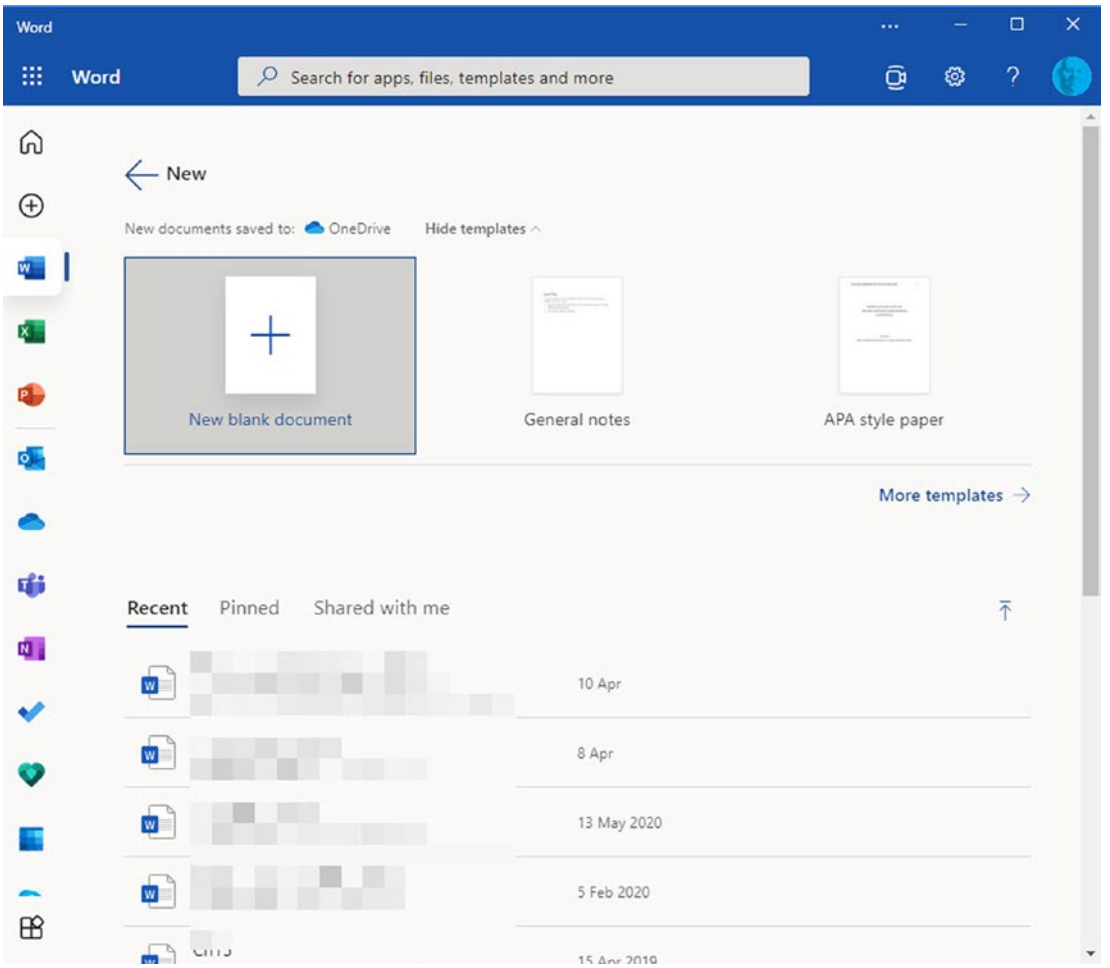


Figure 17-23. *PWAs can be very useful for productivity and business*

You install a PWA in Edge (Internet Explorer does not support this feature) from the main menu, the three dots in the top right corner, and in the *Apps* section click *Install this site as an app*; see Figure 17-24. The app will then install and open in its own window which will appear in the Start Menu automatically and that can also be pinned to the Taskbar.

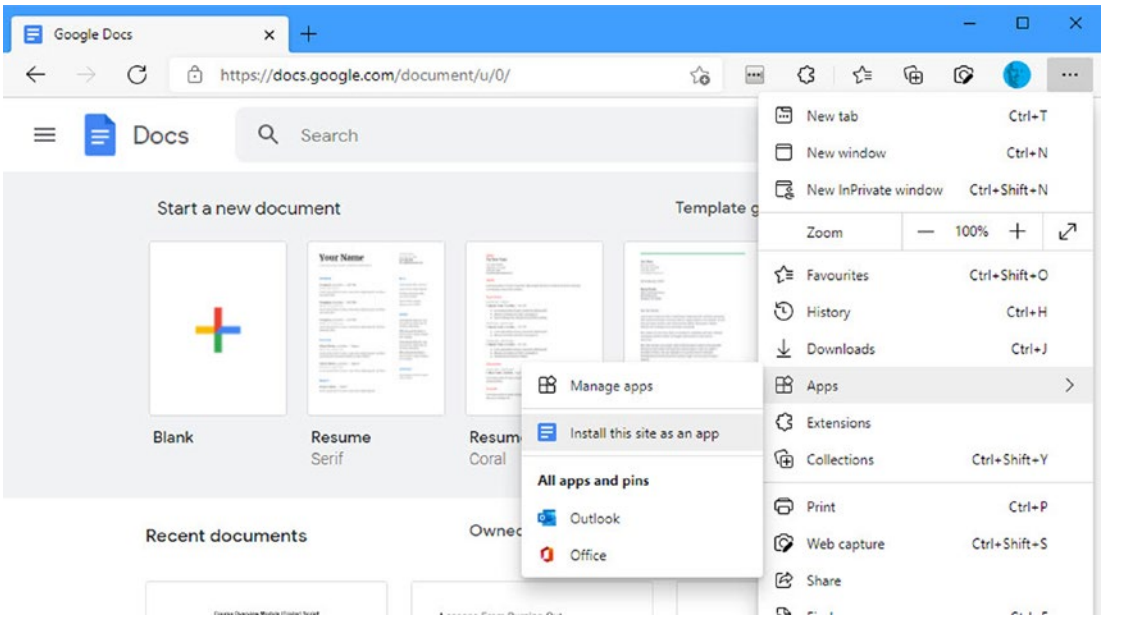


Figure 17-24. *You install a PWA from within the browser*

To check what PWAs you have installed, or to remove a PWA, from the same menu, select *Manage apps*. This will display a page where you will see a list of your installed PWAs, each having a remove cross to its right; see Figure 17-25.

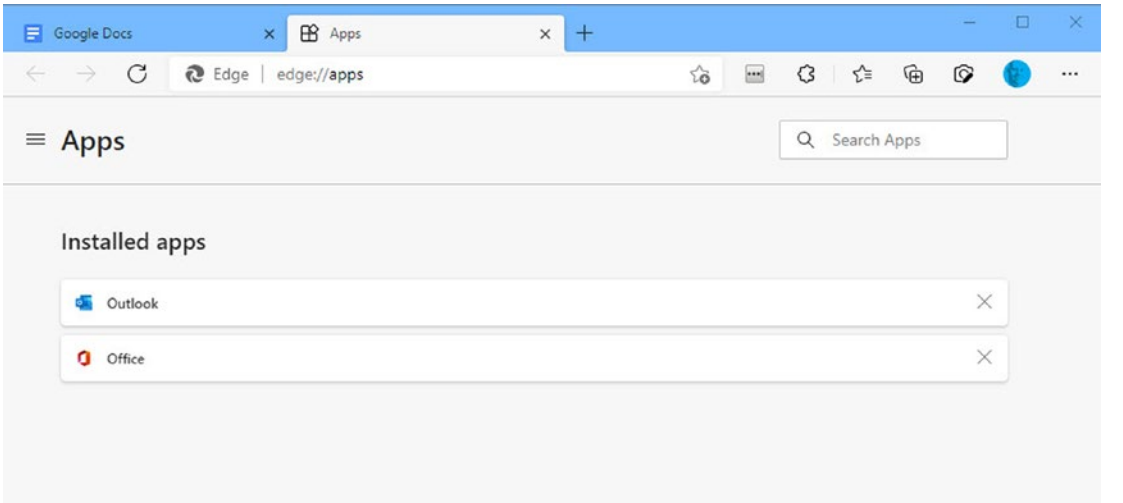


Figure 17-25. *You can easily remove PWAs*

Program Compatibility Assistant Service

For some years now, Windows has included a service that runs quietly in the background and detects, or tries to detect, when a program compatibility occurs. If you search for **services** in the Start Menu and open the Services applet, you will see *Program Compatibility Assistant Service* in the list; see Figure 17-26.

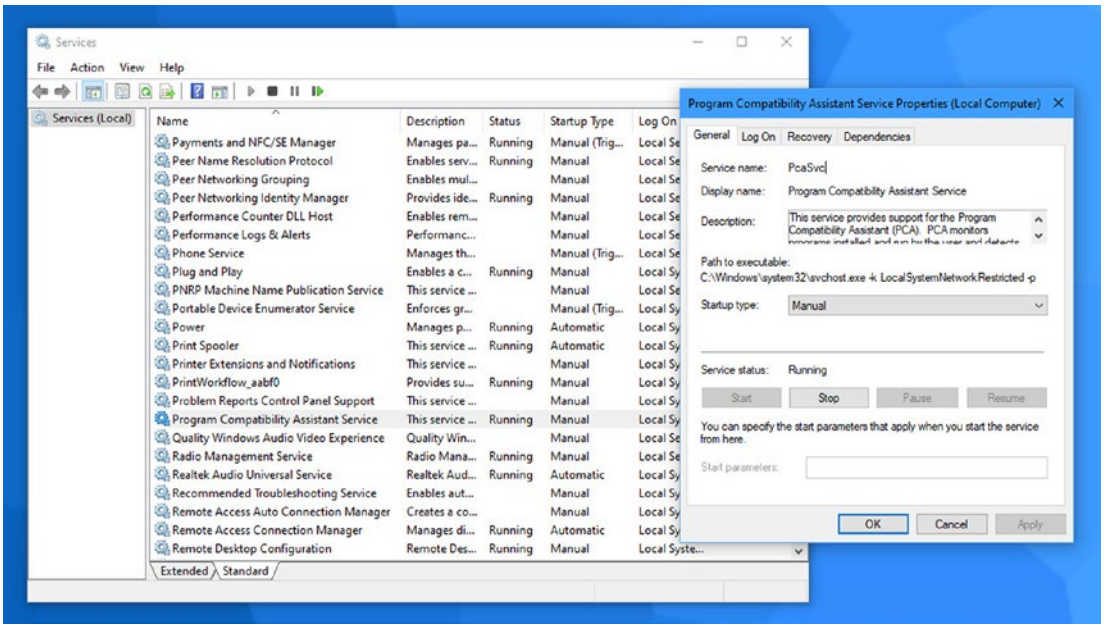


Figure 17-26. *The Program Compatibility Assistant Service is part of Windows*

This service is set to run automatically each time when Windows starts, and you may have seen a dialog pop up now and again over the years, particularly for program installers, asking you want to run it with compatibility settings. This is the Assistant Service in action. If you are having compatibility issues, you might want to check if the service is running properly.

The Microsoft Assessment and Deployment Toolkit

If you manage a large enterprise IT environment, you will no doubt be aware of the Microsoft Assessment and Deployment Toolkit (ADK) for Windows 10, but in fact anybody can download it from the Microsoft website on this link https://pcs.tv/3fcOFdf. There are two tools in the ADK that are useful for diagnosing and mitigating issues with older incompatible software:

- **Windows Assessment Toolkit** can be used to assess installed apps on a PC to determine their compatibility with Windows 10, and to implement fixes as appropriate to help software to work effectively, you can read more at this link https://pcs.tv/3xgZGAu.
- **Application Virtualization (AppV)** is a feature of Windows 10 Enterprise used to enable you to run apps in virtualized containers, isolating them from the rest of the operating system. You can read more at https://pcs.tv/3ydE9tV.

Windows 365 and Windows Sandbox

I want to end this chapter with one of, at the time of writing, Microsoft's newest services, Windows 365, and a hidden feature built into Windows 10. Windows 365 is a subscription service for businesses that allows for the streaming of full desktops to end users anywhere in the world, and on whatever device.

Potentially however this rebadged and repackaged Azure Virtual Desktop is a very useful way to have end users able to access older apps that can be fiddly to configure or that perhaps present a security risk if set up or used in the wrong way. You can read more about the Windows 365 service at https://pcs.tv/3lisFSp.

The other service is Windows Sandbox, and this is already built into the Pro and Enterprise versions of Windows 10. It's part of the Hyper-V virtualization system and is deactivated by default. Search in the Start Menu for **turn windows features on or off,** and you can get to a dialog in which you can activate it; see Figure 17-27.

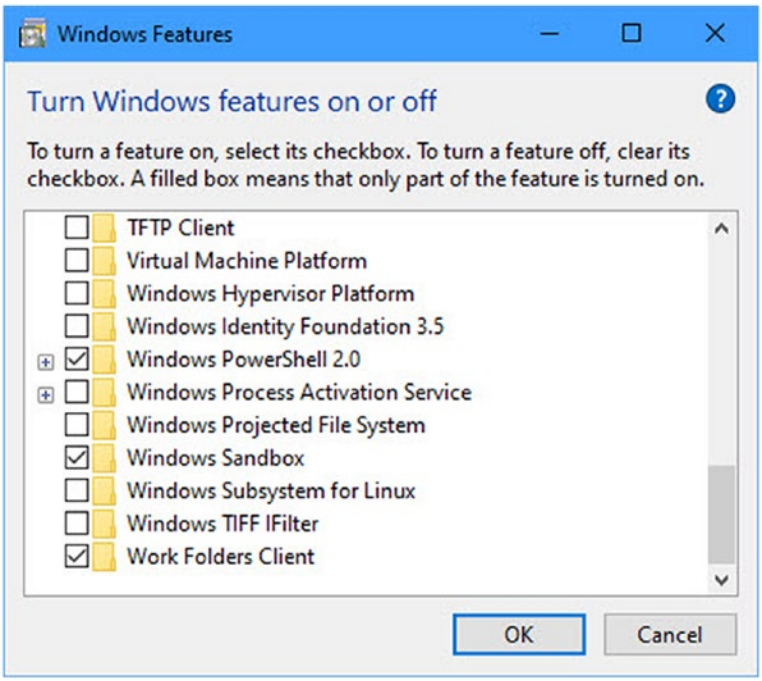


Figure 17-27. *Windows Sandbox comes in the Pro and Enterprise editions of Windows 10*

When you run Windows Sandbox, you are presented with a completely clean installation of Windows (effectively it uses a copy of your own installation and virtualizes it) in which no software, drivers, or indeed anything is installed; see Figure 17-28.

Figure 17-28. *Windows Sandbox is useful for testing apps*

If you want to test an app in Windows 10 that you think could cause stability or security issues, then here is the place to do so, as the Sandbox is completely isolated from the rest of your installed operating system, and when you close the Sandbox window afterward, the session is completely deleted, with no trace left on the PC.

Summary

Windows is, and always has been, the most compatible operating system in history. You can still run DOS programs that were written in the early 1980s in Windows 10 through the Command Prompt, and hundreds, perhaps even thousands, of apps that are over 20 years old will still install and work fine on your PC, though perhaps with a bit of compatibility tweaking.

Using any legacy app, website, or intranet on your system, though, will always present a potential security risk, so in the next chapter, I'm going to focus on that entirely and show you how to ensure that your PC, your files, and your personal information are kept safe, secure, and (as and where appropriate) encrypted and away from prying eyes.

CHAPTER 18

Managing Security and Privacy

How would you feel if your laptop or PC were stolen, with your files and data on board, including online and business logins and passwords, financial details, and personal photos? Worse, how would you feel if you didn't have a password on your PC, or if that password were easily guessable? Now imagine how your employer would feel if it were your company laptop or tablet that were stolen, complete with confidential customer details and information on current and future projects?

It might be annoying or even humiliating to lose a personal device containing autologins to social networks, and some photos you'd rather the rest of the world not see. In the business space however, the use and storage of data are strictly regulated in most countries around the world. People's data is personal to them, and you have a responsibility to look after it and keep it safe.

In many countries, the fines and penalties for losing unencrypted customer, employee, and other personal data can be steep enough to shut down a small business for good. So, what are the best practices for managing privacy and encryption on PCs, but also, how can you regain access to that encrypted data if you find yourself locked out?

The Last *Pass*Word in Security?

Do you remember the days when you had a simple password that was just four to six characters long, and that this was perfectly good enough for the things you did on the Internet? Well, this was long before the days of Amazon and online banking, and where the risks of criminals getting access to your online accounts were small.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_18

These days the risks are enormous, as our entire lives are lived and managed online. Everything from banking to government benefits, food shopping to family memories plays out in either an app or a web browser. I want to spend a little time going through the various options available in Windows 10 as it's important for the security and reliability of your PC(s).

To App or Not to App, That Is the Question

"There's an app for that" as the saying goes, and you'd be quite correct as seemingly every business has at least one app these days. We've been using computers now since the early 1980s (even longer for some of you). In my own home office, I have my own computer museum of devices I've owned and love over the years. This includes a variety of Psion handheld PDAs (personal digital assistants), some computers from Clive Sinclair in the United Kingdom that I grew up with, and even an original working IBM 5150 PC.

All of these computers hold a special place in my heart, and, at the risk of showing my age (early 50s if you want to know) some of us ~~older~~ more discerning, people can be resistant to change. After all, why change something when it's worked so well in the past. Just yesterday evening I was sitting on my terrace with a good friend discussing, over a nice bottle of wine, the importance of him activating Two-Factor Authentication on his online accounts.

The thing was that he already thought he had done so, because he said he gets a text message from Microsoft telling him when there's a login to his account, and giving him the location of the login. I had to explain, which took a little time and convincing, that this information wouldn't stop a criminal in Ukraine (to give just one example as there has been a lot of online criminal activity in the few years preceding my writing this book) from getting access to his account and receiving a text from Microsoft wouldn't help him if he'd just gone to bed for the night.

So, what has this to do with apps you ask? Well, apps offer a level of security that simply isn't possible in a web browser. Let me list the reasons why I think you should use an app for everything if you at all can:

1. Apps don't run in a browser, and so aren't susceptible to any of the vulnerabilities you can find lurking in browser code.
2. The app can only be accessed on a device that is either in your personal possession or close at hand. This is as opposed to a web browser which can be accessed from anywhere on the planet at any time.

3. The app can offer sign-in methods not available in a web browser such as face and fingerprint unlock, a simple four- to eight-digit code, or by automatically unlocking via a proximity setting with a Bluetooth device, such as a fitness tracker. This of course is unlike a web browser.

Microsoft has made great strides in making their services passwordless, but the real benefit is that you can take advantage of this to create superlong and supersecure passwords that you simply never need to remember, and certainly don't need to use in an app once it's been set up for the first time.

As an example, I will never use a web browser to access my various bank accounts if there is an app available (which isn't always the case for savings and investment accounts). For everyday banking I will only use apps.

Memory, Aging, and Neurological Conditions

My father, before he passed away, suffered from dementia. In fact, dementia is an all-too common condition, and my closest friend also has a father with the condition. Dementia isn't the only thing however that can cause people to become forgetful, have difficulty using online services and apps, or just have trouble using smartphones. I've already mentioned that many of us computer users are not as young as we used to be. I was telling a friend only the other day that aging is relative, in that when you're over the hill, you pick up speed.

How is this important to us? Well Microsoft's OneDrive service is just one that offers a *Personal Vault*; see Figure 18-1. This is a secure folder in your cloud storage that requires Two-Factor Authentication to access, and we'll talk about how you set that up in a little while.

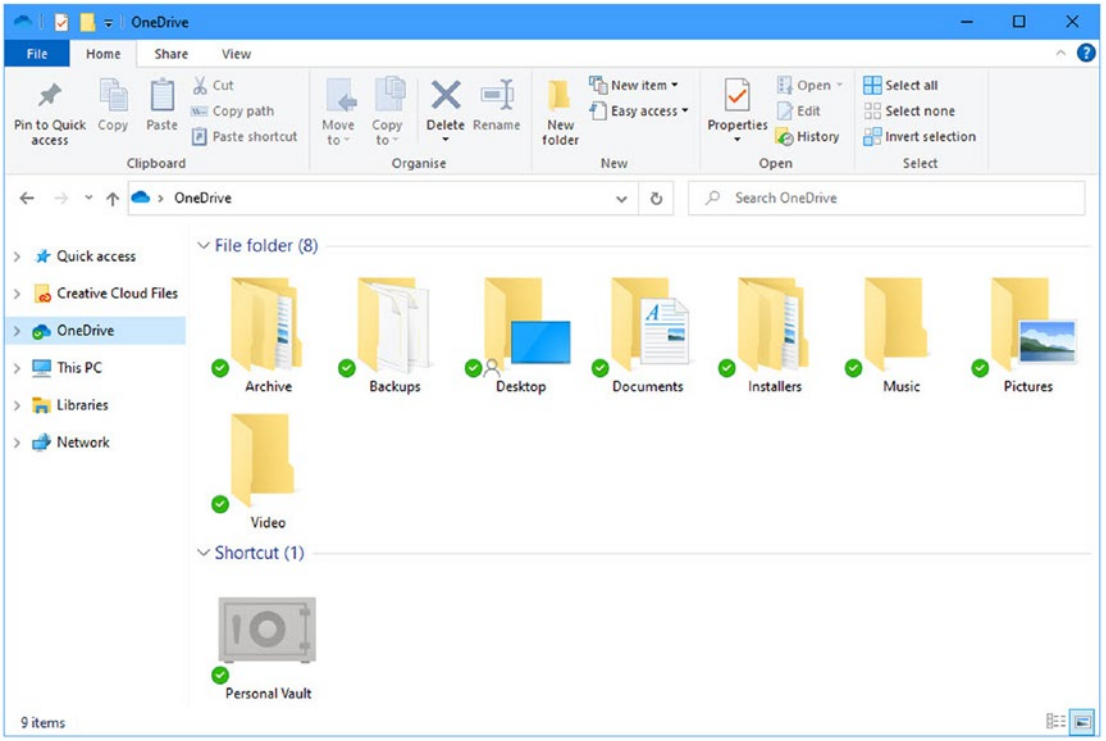


Figure 18-1. *OneDrive comes with a Personal Vault*

This presents its own challenges, and I raise it because with your own security, and the online security of your family, friends, and colleagues is a balancing act where you have to judge how to get the best security without it becoming too difficult to access things should you need to.

Let me give you an example. You have a parent with dementia. All of their important digital documents are set up either in OneDrive's Personal Vault or in a different vault offered by a password manager service such as LastPass. These are locked behind a master password and Two-Factor Authentication. Something happens and your parent is admitted to hospital. You need access to one of the documents in their vault and know their password, but you're currently on business hundreds of kilometers from your parents' home, and that's if you live close to them at all.

Immediately you're stuck. Your parent is unlikely to have access to their phone and is unlikely to be in a position to authenticate your access, and as they have dementia, they could very likely not be aware of the need to do so for much of the time.

You have to balance and judge the security methods I will detail in this chapter with all of this in mind. This is no different for employees of a company when you are deciding on security policy. You might use a corporate password manager and use it as an opportunity to enforce a minimum password criterion of 34 characters, containing upper- and lower-case letters, numbers, and symbol; see Figure 18-2.

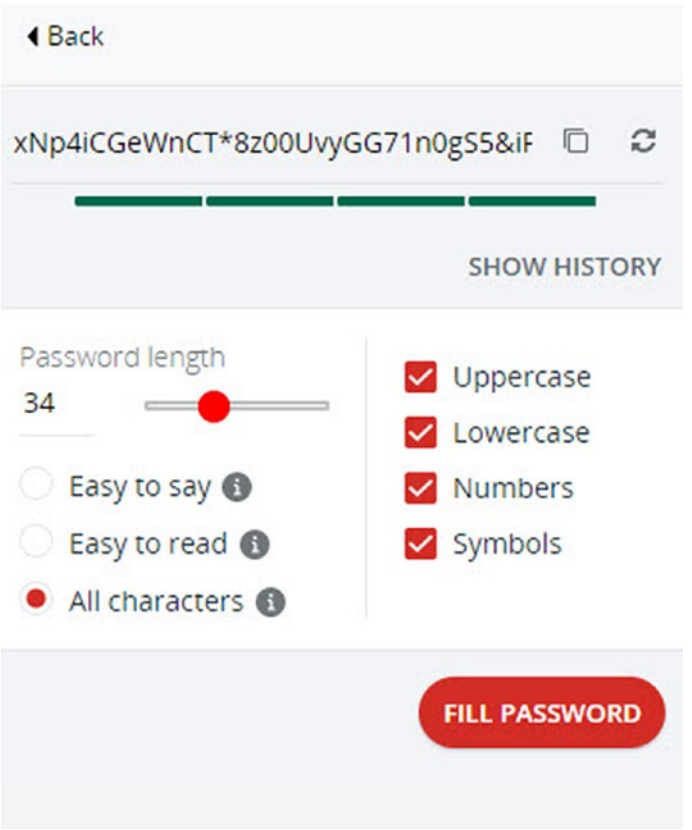


Figure 18-2. *Password managers can be used to enforce very strict password rules for business*

You're doing this on the basis that all of the desktop PCs and laptops you provide for the company employees and directors include one or more biometric devices, whether a fingerprint scanner or a facial-recognition camera. "Great" you say, "problem solved, and now everything is supersecure." But is it?

It's difficult enough for a young, fit, and perfectly healthy person to remember a secure password, let alone one that's utterly random. All you need is for one employee who can't remember passwords to spend a day working from their own PC at home and the whole system falls back to passwords scribbled on a piece of paper and stuffed in a bag with their laptop.

These are all considerations you have to make when deciding security policies, and I wanted to highlight them before proceeding further. The good news however is that the option of a balanced approach, using a mixture of the available methods, is likely the best solution for most people, and most businesses.

Creating a Strong P455w()rd?

Let's begin with passwords. If you're a system administrator or an IT pro, you used to be able to use the **netplwiz** (which you can search for in the Start Menu) to disable the forcing of password entry for the PC at sign-in. In later versions of Windows 10, in order to enforce better security, this option was removed; see Figure 18-3.

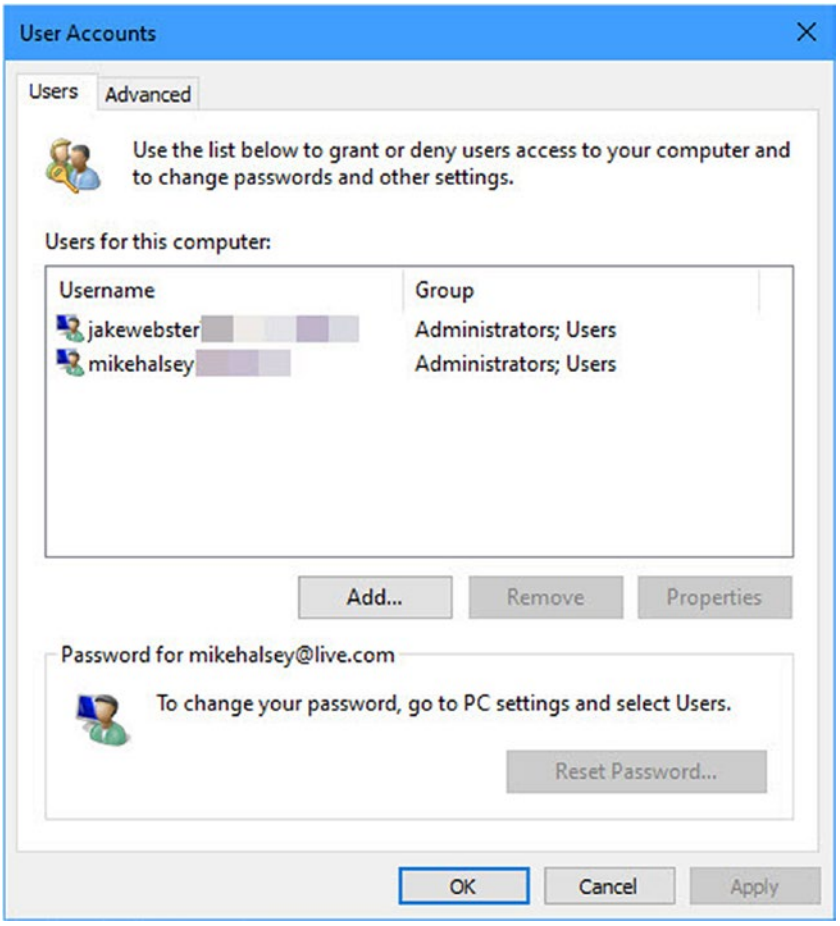


Figure 18-3. *Requiring a password at sign-in can be disabled*

You may have previously done this on some of your PCs; I used to, but only on a Surface Go that never left the house, and on which I don't store any files (to be honest I only used it to watch video and TV while I'm playing Elite: Dangerous on my gaming PC). Was this secure? Well only if you use a local account on the machine to separate it from your OneDrive files, Microsoft email, and the like, which I did. If the Surface Go was stolen by a burglar, it couldn't be used to access any of my personal files or information.

This is a fairly expensive way to watch TV, however, and I've been weaning myself away from television since. For all of my other machines, I am horrendously paranoid. I simply will not buy a PC, laptop, tablet, or desktop that doesn't come with a TPM (Trusted Platform Module) encryption chip, and while I'm a big fan of Windows Hello, because Windows Hello requires a PIN be set up, which is considerably less secure than

my superstrong password, I simply won't use a PIN on anything that leaves the house unless it contains letters and symbols and matches my secure password. Finally, and for good measure, on the desktops that do have a PIN and Windows Hello set up, they are securely tethered to a solid wall by use of a land anchor.

So how do you set up a good password? I have a video online that will guide nontechnical users through the process of setting one up, and you can find it online at http://pcs.tv/1B1NOja. There are some simple rules you can follow, however, to help make your password supersecure:

- Use a phrase as the basis of your password, perhaps a line from a song or poem or a quote.
- Choose a format for changing characters in the password, perhaps capitalizing the second, third, and last letters, or changing the first or second vowel into a number or symbol.
- Substitute numbers or symbols for letters. The following are examples of how you can do this.
  - 3, £, or # instead of E
  - $ or 5 instead of S
  - () or 0 (zero) instead of O
  - & or @ instead of A
  - 8 instead of B
  - 1, |, or [instead of L or I
  - / instead of 7
- Append to the beginning, middle, or end, of the password some unique characters to represent the service or website for which that password is to be used. This will make the password unique to that one place:
  - eBa, or e8@ for eBay
  - Ama, @m@ for Amazon
  - D()m for the company domain

You will then have passwords that are extremely strong, fairly straightforward to remember, and utterly unique in every instance. In the following examples, you will see each password is more secure than the last, and they all follow an easy-to-remember pattern:

- imagine
- Imagine
- ImagineAllThePeople
- imAginealLthEpeOple
- 1mAg1n3&lLthEp3Opl3
- 1mAg1n3&lLthEp3Opl3g()Ogl3

You can test the strength of your own password at the website HowSecureIsMyPassword.net, available at `http://pcs.tv/howsecpwd`. In the examples I've given, the first is a dictionary word and will be guessable by a hacker almost instantly. The last, which has been uniquely modified for Google sign-in, would be almost completely uncrackable, and anybody who wanted to do so would need intelligence about how you create your passwords to aid them in the process.

It's not impossible to remember complex passwords either. Let's take the last example, **1mAg1n3&lLthEp3Opl3g()Ogl3**. The code here is that the vowels are changed to numbers or symbols, and always the same number or symbol, and the third letter of each word is capitalized; it's no more complicated than that.

Caution If you are required to change your password regularly, perhaps every 90 days, please avoid incrementing the password by adding a number or letter on the end of it, 1, 2, and so on. This makes the password easy to guess if people discover the core password.

None of this is a substitute for using a good password manager app however, and most can be used across Windows, Mac OS, Linux, Android, and iOS. My own choice is LastPass, but there are many more including Dashlane, 1Password, and more. Many offer business subscriptions, some come with secure cloud storage, and some have family protection features. I chose LastPass because they allow me to share my subscription with friends.

Using Two-Factor Authentication

Two-Factor Authentication (TFA) is now widely used across the Web, from signing into email and shopping services to banking and online payments. It can work in different ways. Sometimes you'll receive an SMS text message with a code to type into a website; sometimes you'll install an Authenticator app on your smartphone that will provide you with a code. Alternatively, some services can send you an email with a secure code, though this can be less secure if you have email set up in Outlook or another app on the same PC you're using to try and do something that requires authentication online.

Two-Factor Authentication is an absolute necessity for anybody that uses online services from email to banking, and all the major companies including Microsoft, Apple, Google, Amazon, and Netflix offer it. If you use a Microsoft Account, you can activate and manage TFA at `http://account.microsoft.com` where in the *Security* settings, you will find TFA options that include backup email addresses, phone numbers, authenticator app usage, and more to help you access your account securely; see Figure 18-4.

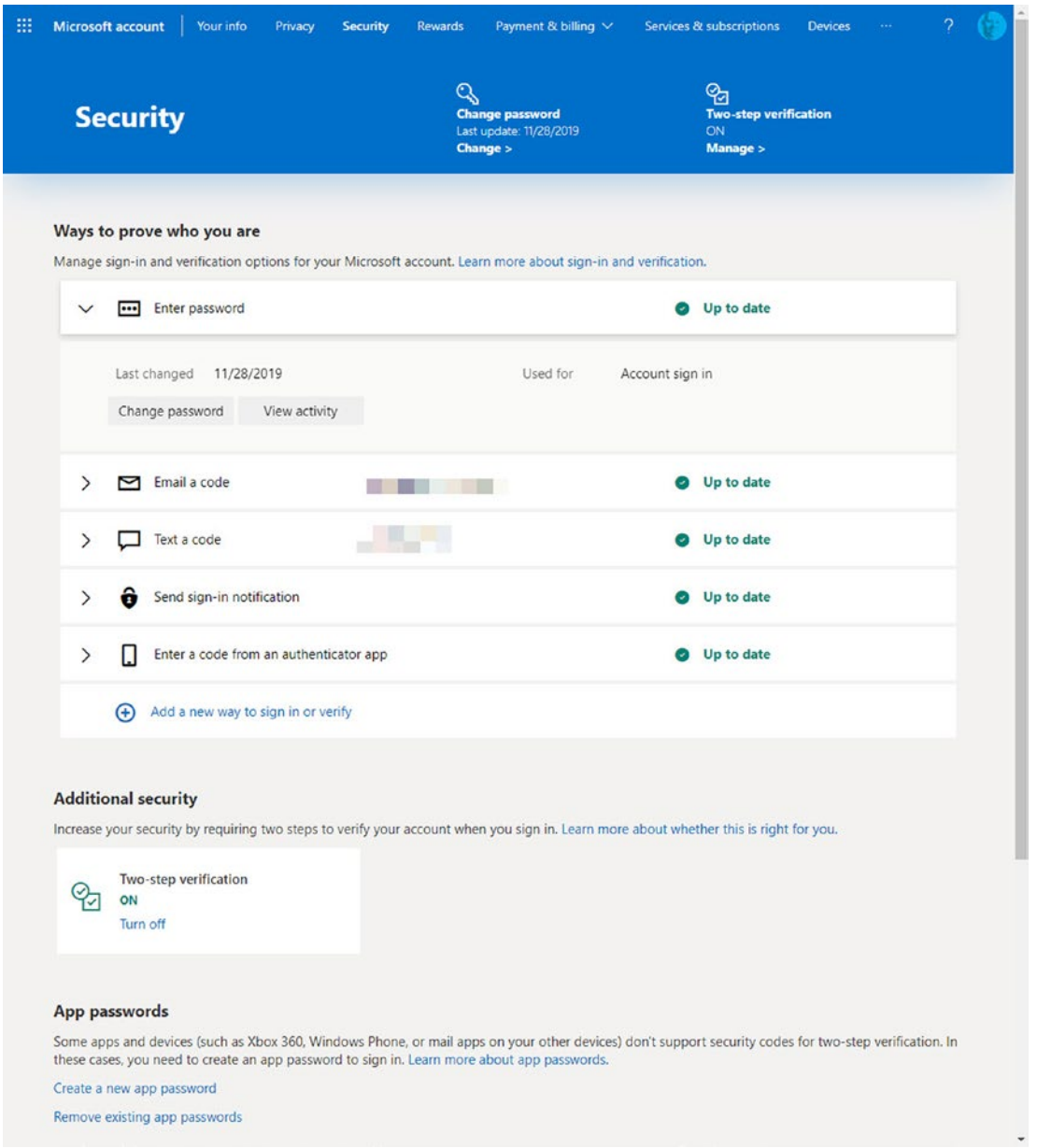


Figure 18-4. *You can activate TFA for a Microsoft Account online*

You can find the Microsoft Authenticator app for both Android and iOS in their respective app stores, but if you prefer to use a different authenticator app that will work perfectly fine, just as you can use the Microsoft Authenticator app for Google services

should you wish. When you set up a new app, you will be shown a QR code which you can scan from the authenticator app you have installed on your smartphone; see Figure 18-5.

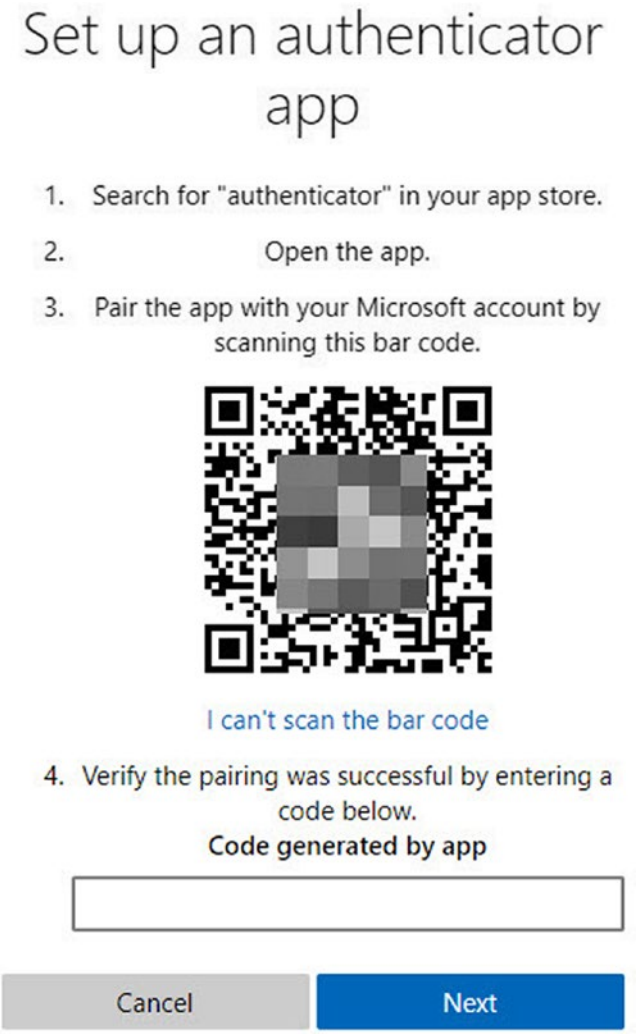


Figure 18-5. *You scan a QR code to set up an authenticator app*

Microsoft's Azure has its own TFA settings you can configure, and there is extensive documentation on the Microsoft website that is updated regularly. You can find it at this link `https://pcs.tv/3CibRRA`.

Windows Hello

Windows Hello is the umbrella name for Microsoft's biometric security features. These include facial recognition, fingerprint scanning, USB security keys, and security smartcards. You access the Windows Hello options in *Settings* ➤ *Accounts* ➤ *Sign-in options*; see Figure 18-6.

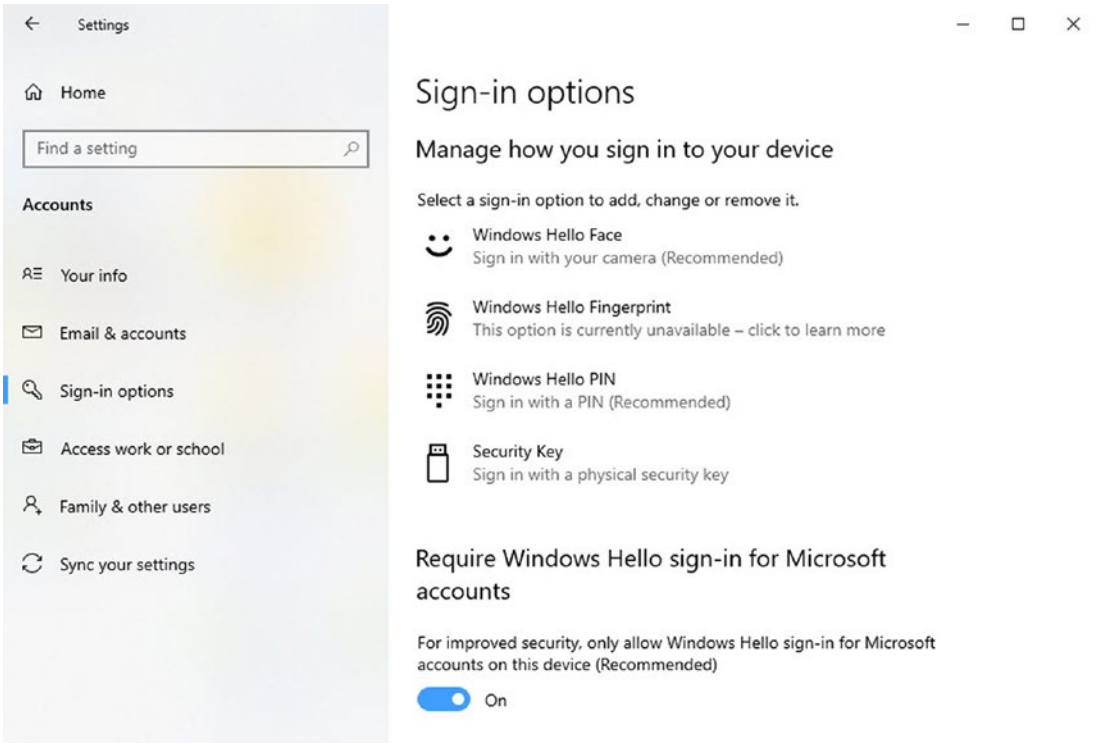


Figure 18-6. *Windows Hello offers a variety of security features*

One thing of note however is that Windows Hello requires the computer to have a Trusted Platform Module (TPM) chip. This is a special dedicated chip on the motherboard that is used to store encryption keys. When Windows 8.1 was released back in 2013, Microsoft mandated that all new PCs sold to the public had to include a TPM.

This is fine for every PC purchased after this time for the home, but not all business PCs will have been subject to the same restrictions as they weren't sold "with Windows 8.1" and would have come without an operating system. To compensate for this, many motherboard manufacturers include a *Firmware TPM (fTPM)* option in their UEFI settings; see Figure 18-7.

Figure 18-7. *Many modern UEFI systems come with a Firmware TPM option*

fTPMs are handled in a secure area of the PC's CPU and simulate the working of a hardware TPM chip. This is a great solution for many, especially given the global TPM chip shortage caused by the announcement of Windows 11, but it's not without its problems.

To give you just one example, because the TPM configuration and security keys are held in and stored by the UEFI firmware itself, if you update, flash, or reset your UEFI firmware at any time, you will completely wipe your keys. In this regard it is nowhere near as useful as a full hardware TPM but can be a good solution for some computers.

A hardware TPM however will appear as an option you can enable in your UEFI firmware if you have one installed on the PC; see Figure 18-8. This will enable you to use security features such as Windows Hello and Bitlocker drive encryption without any problems as the security keys are stored in the chip itself.

Figure 18-8. *If you have a TPM chip on your motherboard, you can enable it in the UEFI firmware*

With the TPM or fTPM enabled, you can activate Windows Hello for your PC, assuming of course that you have either a Windows Hello compatible infrared webcam or a compatible fingerprint scanner. The Sign-in options Settings will tell you what can and cannot be activated on the individual PC.

Note Some people are wary of biometric logins because they don't like the idea of their personal fingerprint, facial, or iris data being stored by companies like Microsoft in the cloud. The important thing to remember with *all* biometric systems, and this includes the biometrics found on Apple devices and in Google Android, is that the data is only ever stored locally on the device in a securely encrypted chip, and it is *never* transmitted over the Internet or stored in the cloud.

Managing Safety and Privacy for Children

Nothing is more important than the safety and security of children, or so I'm told as I haven't got any myself, which is why I have to time to write big books such as this. What is much more important however is the security of our PCs, especially ones for home workers where their children might want to have a play. Nothing can be worse than

someone who does not understand what they're doing getting Administrator access and changing or installing random things on a PC. I don't as I said have children of my own to set up with the family options in Windows 10, but I do have a dog, a rescue border collie called Evan, so for the purposes of this section, I've set him up with his own user account on my PC.

You'll see in Figure 18-9 that I've set up an account for my border collie Evan in the family section of the *Accounts* page in *Settings*. Adding the child (or dog in this case, but we'll call him a child as he really is just a big kid) lets you choose if the account is for a child or an adult, and then makes settings for that child available in Family Safety in your Microsoft account.

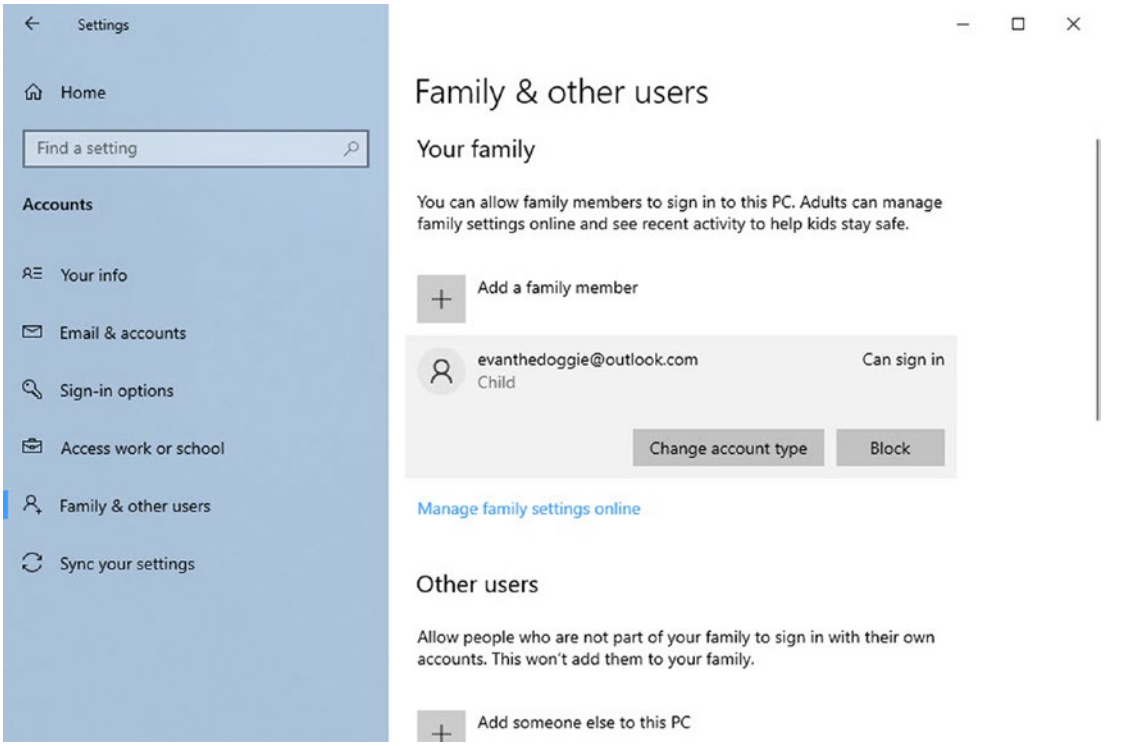


Figure 18-9. *You add child accounts as family members*

Note The Family Safety feature in Windows 10 requires that the parent(s) and children all sign into the PC(s) with Microsoft accounts.

Clicking the *Manage family settings online* link in the Family Accounts panel will take you to the Family Safety page of your Microsoft account online. Here you will see a list of your children, and you can click each one to display details of their activities online (which I'm assuming for Jed was watching cat videos), and you can optionally have a weekly status report emailed to you for each child; see Figure 18-10.

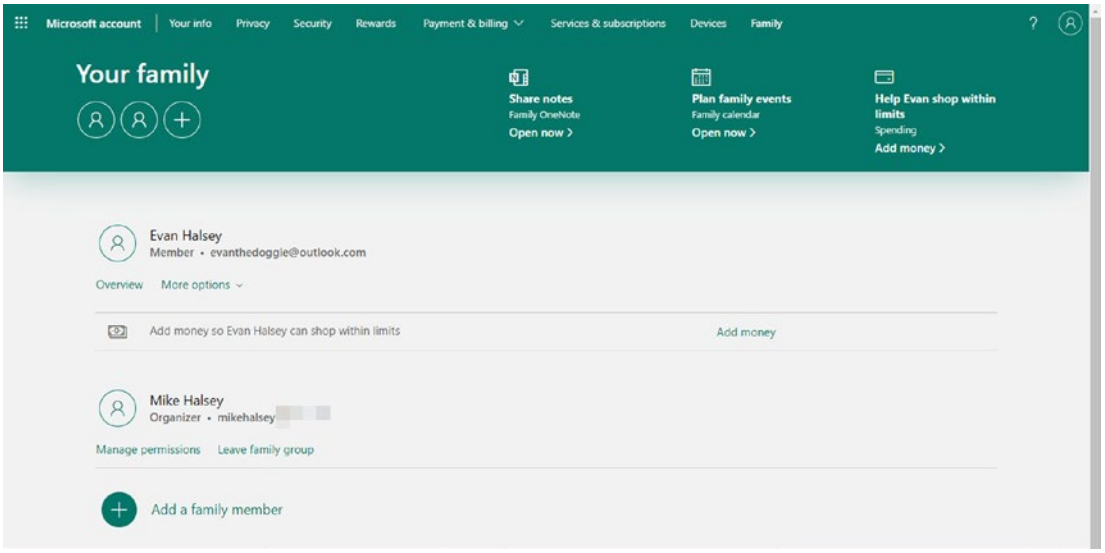


Figure 18-10. *You can get weekly activity reports from Family Safety*

The Family Safety dashboard provides controls that you can activate and configure for each child. These include web filtering, time permissions, and game ratings; see Figure 18-11. Clicking one will allow you to set permissions for that child.

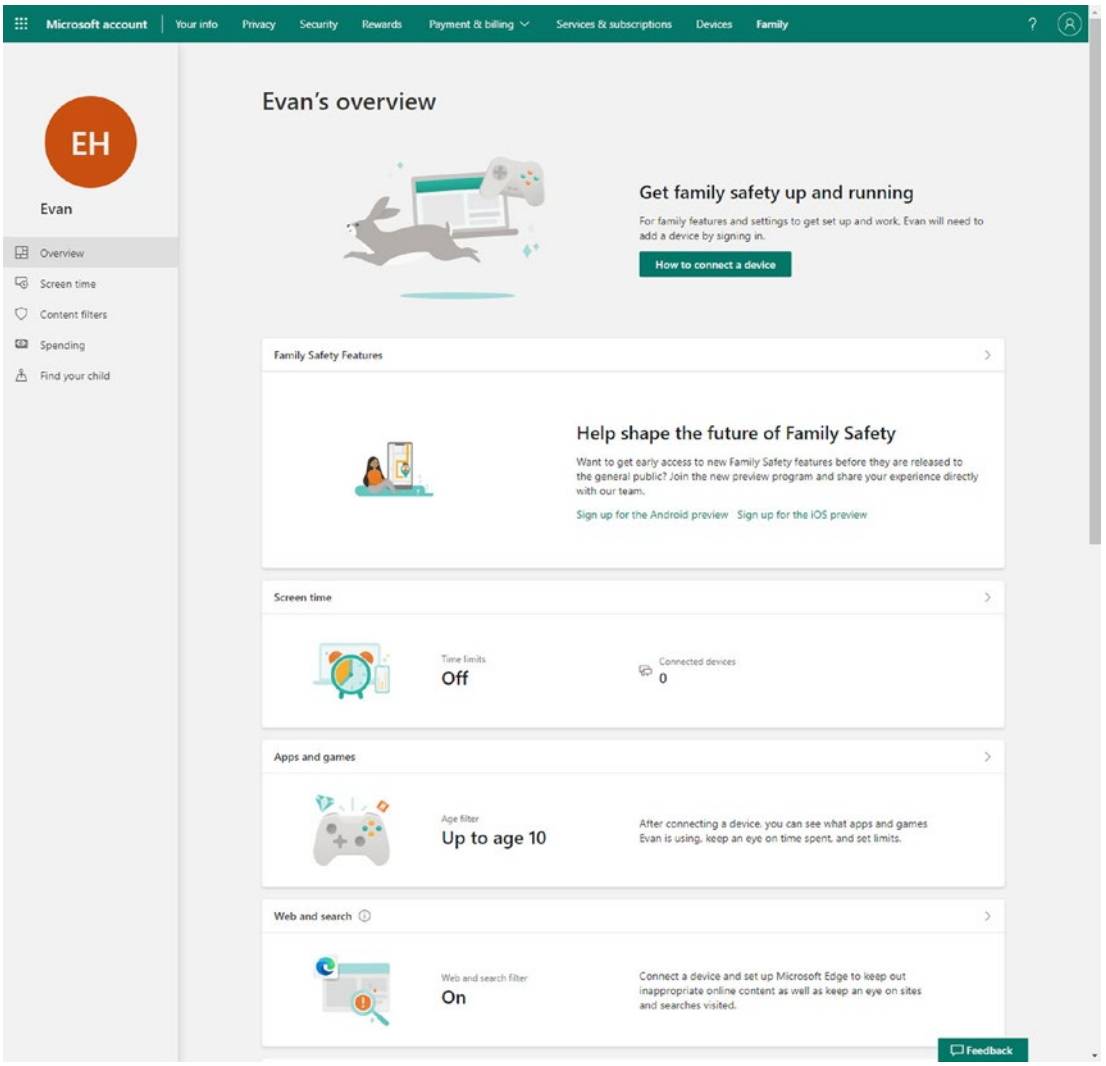


Figure 18-11. *There are different settings available in Family Safety*

When you have activated the web filtering, you will see that to make the system easy to use, Microsoft has a single-switch approach; see Figure 18-12. This activates global web filtering based on the age of the child. The filters are provided not only by Microsoft but also child protection companies and organizations around the world, and they're very extensive.

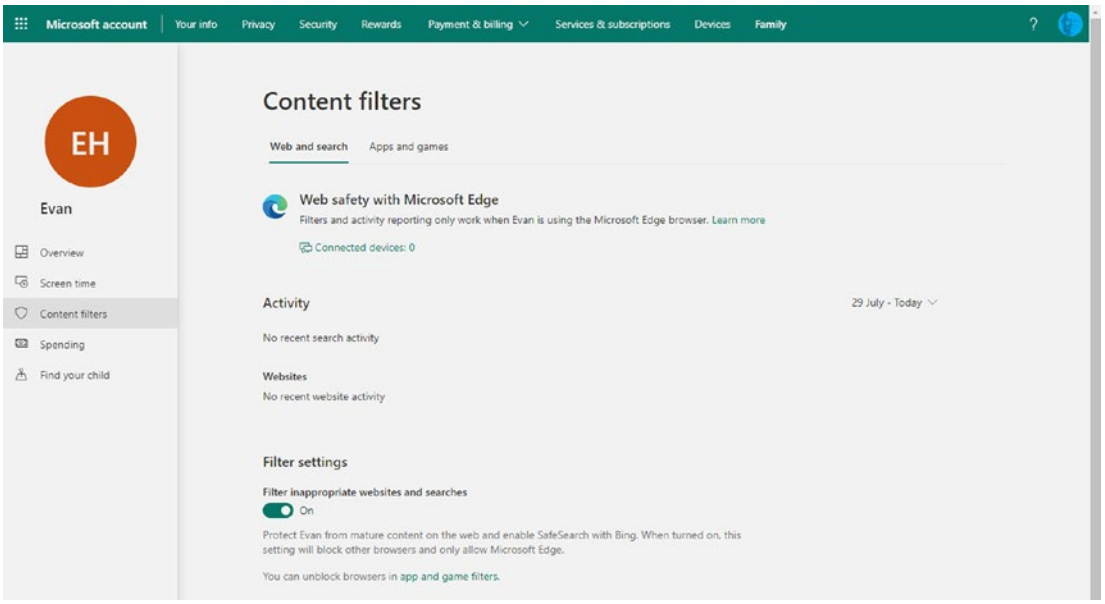


Figure 18-12. *You can use website filtering for children*

You might find, however, that the system could still block some websites that your child requires for school, or that some websites are permitted when you would rather your child not see them, perhaps on religious grounds. You can add websites to your personal white and black lists from the Family Safety, web filtering panel; see Figure 18-13.

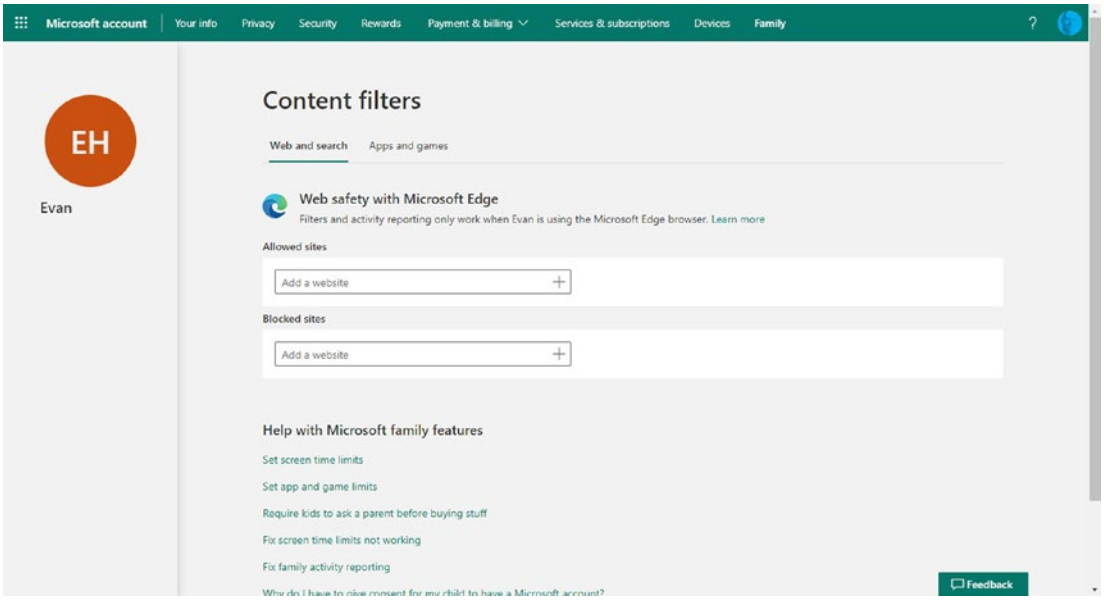


Figure 18-13. *You can add specific sites to your white or black list*

The times controls allow you to set how often, or for how many hours a day, your child is allowed to use their PC. This might be that you don't want them using the PC after 7 p.m., but you might allow them to continue until 9 p.m. on a Friday or Saturday night. Should there be a circumstance such as a school holiday, during which you could be more flexible on the times, overrides are also available.

When it comes to games, it's important to note that this system is not a catchall for every game. It only really works with games provided through the Windows Store. You can choose the age of the child from a drop-down menu to choose what games they should be allowed to play on their PCs; see Figure 18-14.

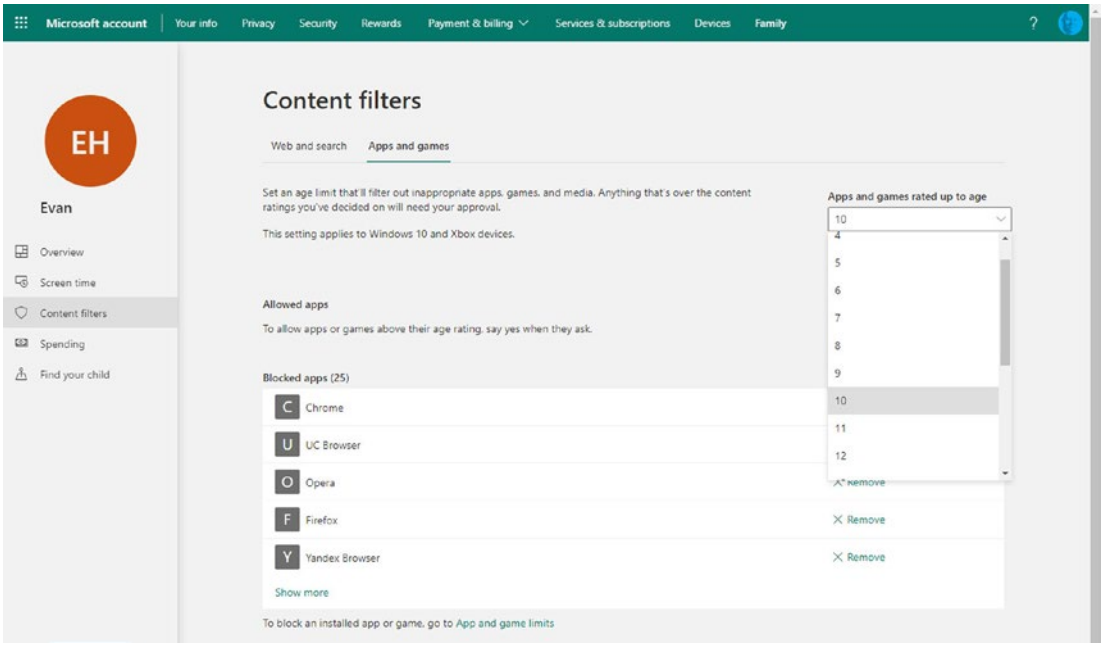


Figure 18-14. *Game ratings are available for children*

The Windows Security Center

Microsoft have been evolving and expanding their security options steadily over the years. From the first inclusion of a firewall with Windows XP Service Pack 2 to the inclusion of User Account Control (UAC) in Vista and integrated antivirus (AV) software in Windows 8, it should hardly come as a surprise that Microsoft included more security features in Windows 10 when it launched and has been adding even more in the years since.

I know what you're about to say here, that it's essential to install a third-party antimalware package because the one included with Windows 10 is woeful. Hold fire on that though, as the Windows antimalware service is as good now as many of the headline AV alternatives. To find out how they stack up as you read this, head over to `www.av-comparatives.org` for their latest figures. Figure 18-15 contains data from the `www.av-test.org` website that shows just how far Microsoft has progressed in the last few years.

Figure 18-15. *Microsoft's antivirus software is not the dead weight it used to be*

I'm not trying to convince you to use the inbuilt software, but it does come with some useful features you might want to know about.

Ransomware Protection

There is ransomware protection baked into Windows 10, though it's only available if you use Microsoft's antivirus offering (which seems a bit mean; Ed). You can access the security settings either from *Settings* ➤ *Update & Security* ➤ *Windows* Security or by clicking the shield icon that appears in the Taskbar system tray. Figure 18-16 shows the ransomware protection, which is called *Controlled Folder Access*.

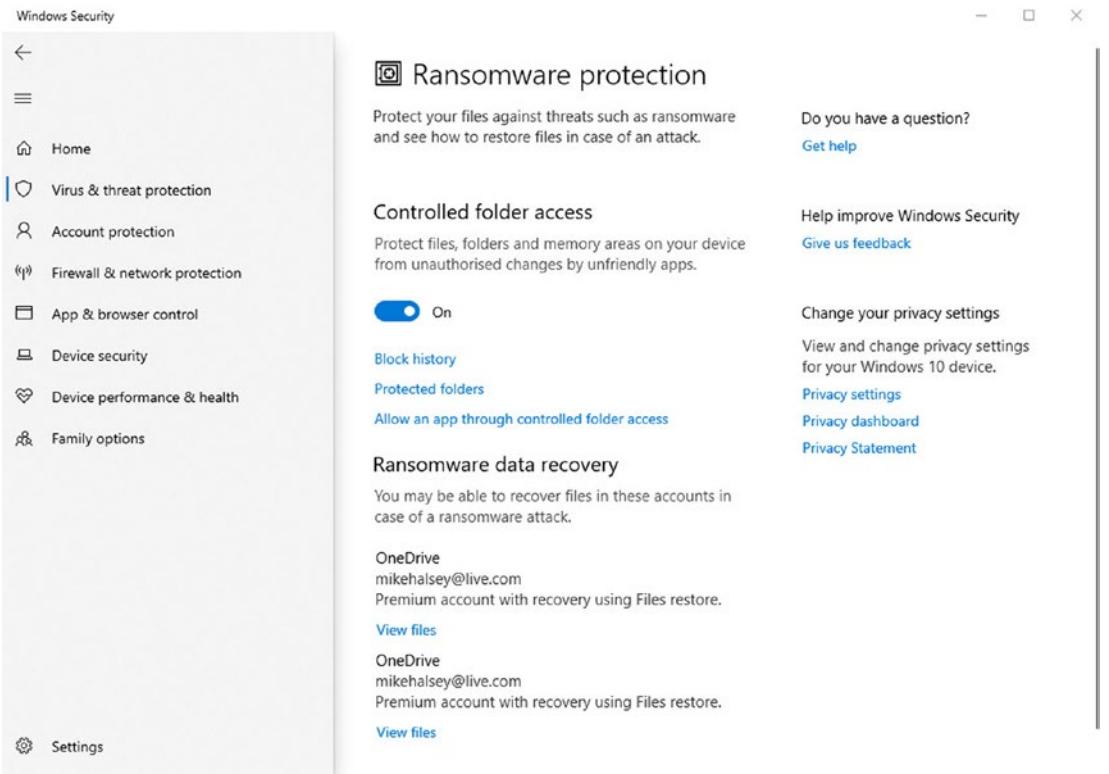


Figure 18-16. *There is ransomware protection baked into Windows 10*

What Controlled Folder Access does is monitor a set of predetermined user folders (or whole drives) and prevents any read/write operations from software that it doesn't recognize as safe. By default, it will protect the Shell User Folders (Documents, Pictures, etc.), but you can click the *Protected folders* link to add more folders and drives.

Controlled Folder Access can be very effective, as it will stop ransomware from encrypting your files stone dead, it's not without its problems however, and these primarily come from older win32 software and programs like backup applications. These are often blocked by the system, though you will get a notification when it occurs that takes you to a page where you can change the settings for the specific app.

Clicking the *Allow an app through controlled folder access* link however will allow you to manually change the settings for any app that does or that you suspect might be blocked; see Figure 18-17.

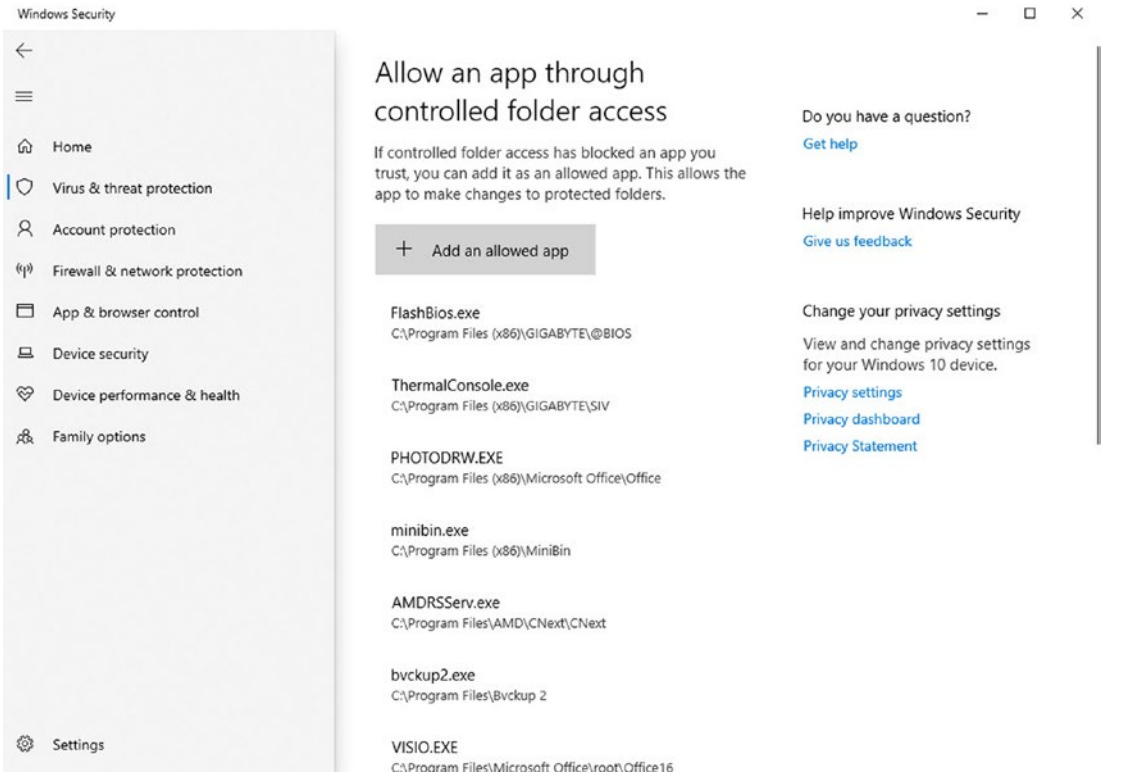


Figure 18-17. *You can allow apps through Controlled Folder Access*

App and Browser Control

App & Browser Control is also a feature of the Windows 10 security system; see Figure 18-18. Here you will see some features that have been ported from Microsoft's business and enterprise security products over the years.

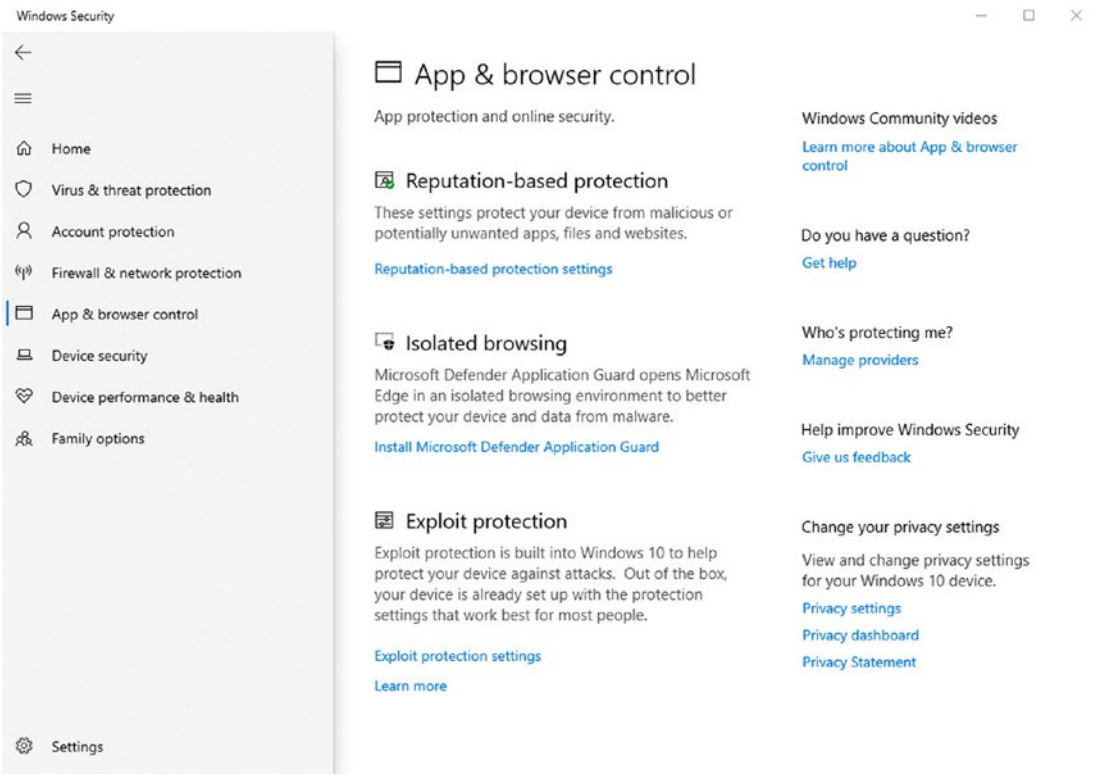


Figure 18-18. *App & browser control offers highly effective security settings*

Reputation-based protection uses data from Microsoft to determine if an app is safe to download and install. This uses the *SmartScreen* protections that checks files as you download them. *Isolated browsing* is a feature of Microsoft Defender Application Guard that can enable you to use the Edge web browser in a completely containerized environment, shielding it completely from the host operating system.

Exploit protection is a series of systems used to protect against zero-day exploits in your software or the operating system. A zero-day exploit is one that's being actively used by criminals and hackers, but that is currently unknown to security and app vendors. There are a series of different options (see Figure 18-19) that are all on by default and should only *ever* be disabled if they're really interfering with something critical on the PC.

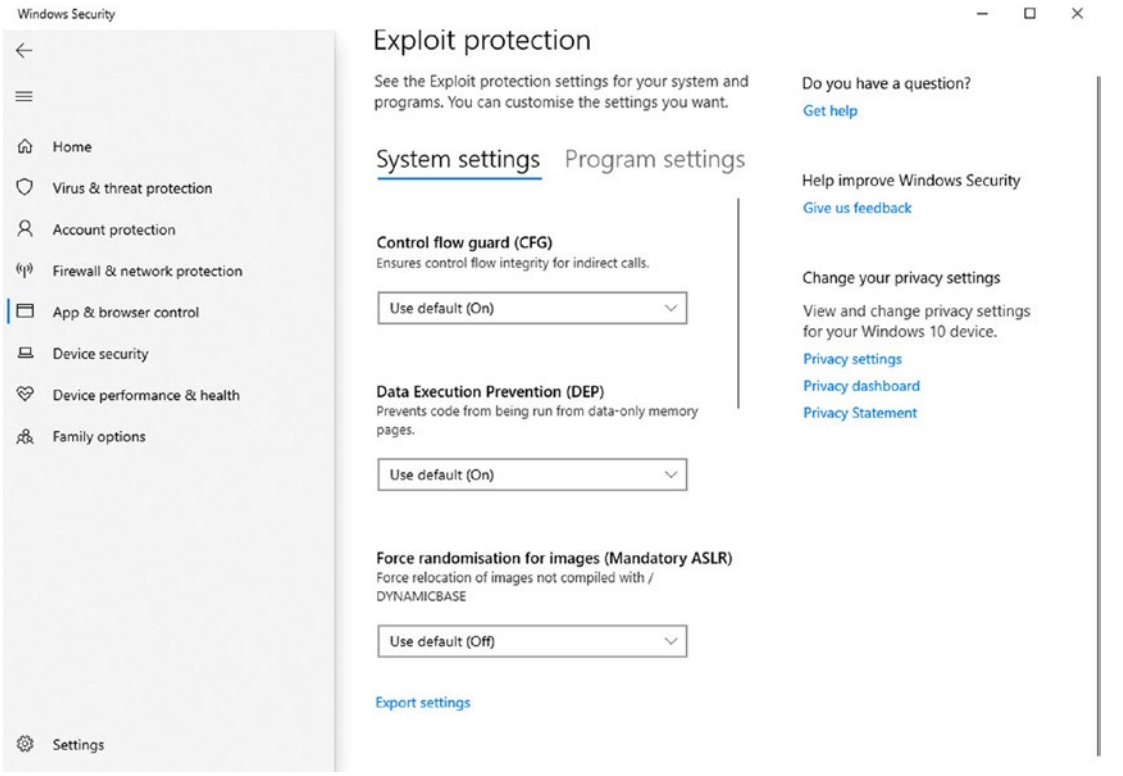


Figure 18-19. *Exploit protection contains a wide variety of options that should be left activated*

Core Isolation

Core isolation is a feature that requires support in the PC's CPU. It is a feature ported from the Enterprise editions of Windows 10 that uses hardware-based virtualization (on processors that support it, which is pretty much everything these days) to run critical system and security processes in a secure area of memory, isolating it from the main memory used by the PC; see Figure 18-20.

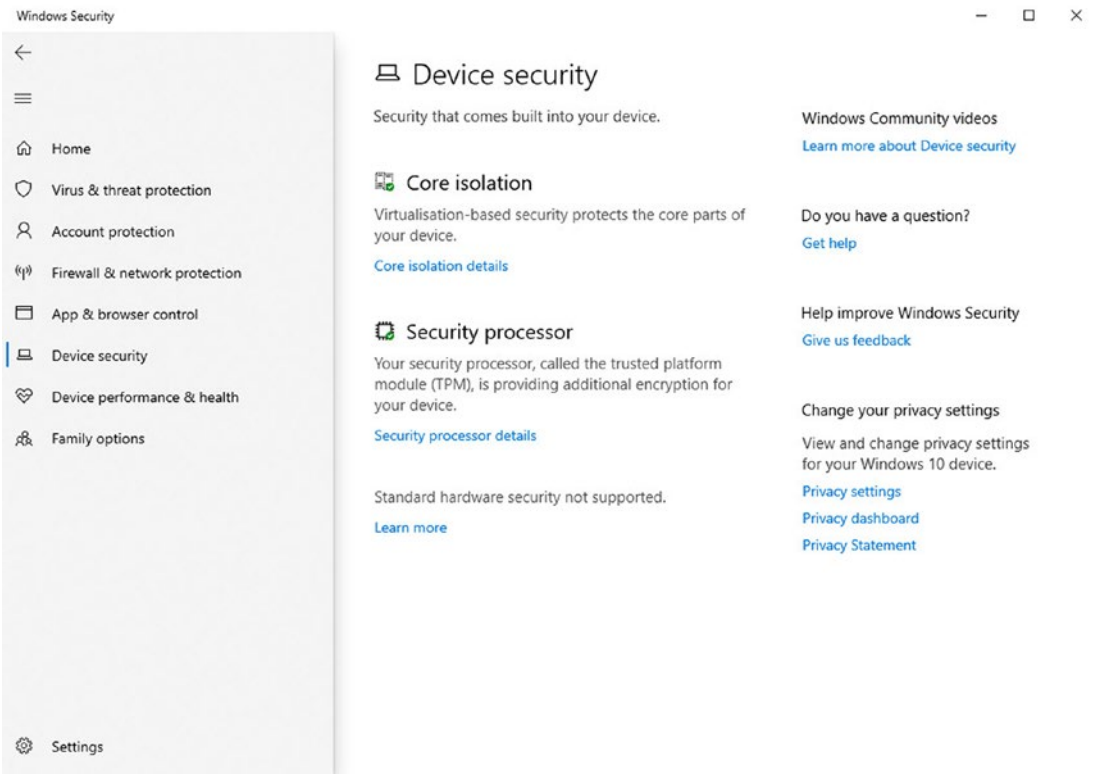


Figure 18-20. *Core isolation is a highly useful and effective security system*

Memory Integrity is a subfeature of core isolation that runs the code-integrity service in Windows inside a hypervisor. This is a service that checks software and device drivers for their digital signature. Malware can attempt to inject code into high-security processes on the PC, such as driver installs and upgrades, and Memory Integrity can prevent this. This feature is not automatically enabled on Windows 10 PCs however, but you can easily activate it.

Using the Credential Manager

Username and password management is crucial for any computer use these days, especially given the need for supersecure passwords, as I detailed at the beginning of this chapter. You can create superstrong, perhaps even completely random, passwords, but how can you manage them or remember them if you've forgotten one?

You might use a third-party password manager, but these do have problems associated with them. The first, and probably the biggest, certainly when it comes to businesses, is that they almost always only manage Internet usernames and passwords. The second, however, is that because all your password information is stored with these services in the cloud, they are a target for hackers and criminal gangs. Indeed, in recent years we've seen data breaches from these services.

I'm a big fan of not using third-party software to replace something that's already part of Windows anyway, and the good news is that the Windows 10 *Credential Manager* (search for it in the Start Menu) is a great tool for managing local, network, and Internet security.

It's separated into two parts, your Web Credentials and your Windows Credentials; see Figure 18-21. The former will keep a list of all your Internet usernames and passwords and synchronize them between Windows 10 devices (this includes PCs and smartphones) using a Microsoft account or another account type that supports syncing, such as a Domain. You will see a list of all the websites and web services for which details are stored and can display a password on entering your PC account password, or by using Windows Hello.

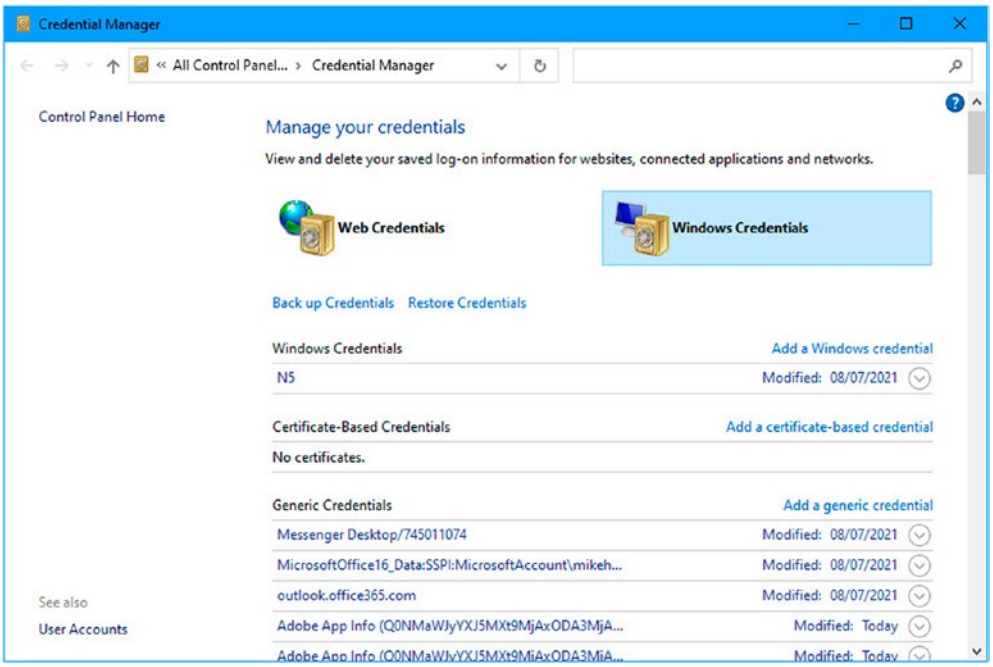


Figure 18-21. *The Credential Manager allows you to store and retrieve passwords and usernames*

When it comes to Windows Credentials, which include network sign-ins, these can be both backed up and restored from PCs, and credentials can be manually added by a user or administrator. It's also possible to add credentials that rely on a specific security certificate, and I'll show you how to manage security certificates later in this chapter.

Managing Encryption in Windows 10

There are three main types of encryption in Windows 10. These are the Encrypting File System (EFS), which is a file- and folder-based encryption system; Bitlocker and Bitlocker To Go, which are full-volume (partition or disk) encryption systems; and the full disk encryption system, which is an easier-to-manage version of Bitlocker, which is implemented on smartphones and consumer-grade tablets.

Each has its uses, and I'll show you how to use and manage them shortly. Why would you want to use encryption, however? In both the personal and business spaces, there are compelling reasons, especially given that we store much of our lives on our PCs these days. This doesn't include family, vacation, and personal photos and work or private documents, but our PCs do store, as I've just detailed, sign-in details for our shopping, banking, and other websites.

In the business space, it's even more important, as on our PCs we often carry commercially sensitive documentation, or client or customer data. Any data on anybody that you hold, be they customers, clients, or members of your own staff, will be subject to strict data protection regulations, the fines for breaches of which can be enough to put a small company out of business for good.

It's important then to choose the right type of encryption for your needs. Each one has its uses, but EFS and Bitlocker are both very different from one another.

Caution Is any type of encryption completely secure? While EFS and Bitlocker provide extremely strong encryption for your files and data, it's true to say that no form of encryption is completely secure. As has been proven with high-profile cases involving the FBI and other security agencies, if somebody is truly determined to gain access to your data, it's likely they'll find a way to do it eventually. Also, many companies exist to recover data that has been lost or is on damaged computers. This will include the ability to decrypt files and drives as and where necessary.

Why do I mention this? As customer and staff details are covered by data protection regulations around the world, should you operate in a high-security environment such as research, finance, or where large amounts of data on individuals are stored, it's always wise to minimize the surface for attack. This can involve laptops and tablets having on them only the data they *absolutely need* at any one time or having all access to secure data provided only through an encrypted VPN.

Using the EFS

As I mentioned earlier in this section, the EFS is a file- and folder-based encryption system. Activating it creates a security key that can be transferred from one PC or user account to another, which means it does have an advantage over Bitlocker, where the disk or volume is encrypted, meaning that when files are copied into a nonencrypted space, such as another PC, or when attached to an email, they will be decrypted.

EFS does need to be managed carefully, however, as this complete encryption can have its downsides. The first is that it is supported only on NTFS-formatted drives. This means that when transporting EFS-encrypted files, you might find that their encryption becomes scrambled, and the files will become corrupt. When transporting encrypted files on an ExFAT or other Microsoft file system, you should be fine. I have encountered an issue with a third-party network-attached storage (NAS) drive, however, where its proprietary file system completely scrambled my backup of encrypted files, much to my own annoyance.

You can activate EFS on any file(s) or folders you have selected in File Explorer. Just right-click your selection, and click *Properties* from the menu that appears. In the Properties dialog, click the *Advanced* button in the Attributes section of the General tab, and a dialog will appear displaying a checkbox option to Encrypt contents to secure data; see Figure 18-22.

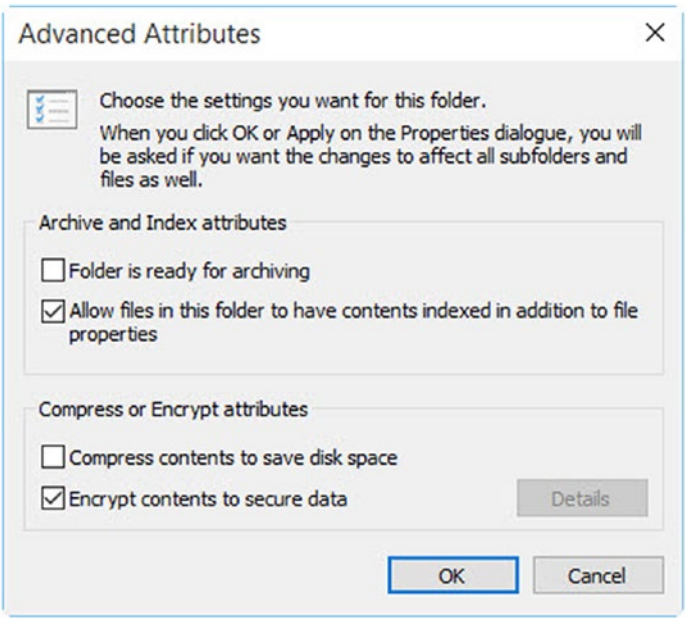


Figure 18-22. *You encrypt files and folders in EFS with a checkbox option*

Once the files/folders have been encrypted, a system tray alert will prompt you to back up your encryption key. Rather foolishly, it gives you the options to both do this later, or to not do it at all (why?). You really do need to back up your encryption key immediately… just in case either disaster strikes or you get distracted by cat videos and forget.

You are asked where you want the encryption key to be stored. This should be a safe repository where it's out of reach of thieves (or is at least where they're not likely to look for it). The two places you should never store your EFS encryption key are on your Windows drive (because if disaster strikes and you need to reinstall Windows 10, you will lose it) and in a folder that's encrypted with EFS (because you could lose access to the key). In fact, I'd go so far as to advise that you don't keep only one copy of the key, and don't keep it on the same physical hard disk as the encrypted files. A disk failure could mean that backups made of those files could then be irrecoverable.

Caution Do not save your EFS certificate to a folder that is encrypted by EFS, or you will be unable to decrypt the folder later as you will lose access to the key.

Should you at a later time need to create a backup copy of your encryption key (damn those cat videos), you can do this by searching for **encryption** in the Start Menu and selecting *Manage file encryption certificates* from the search results. This will display a wizard that will allow you to create backup copies of your certificate(s); see Figure 18-23.

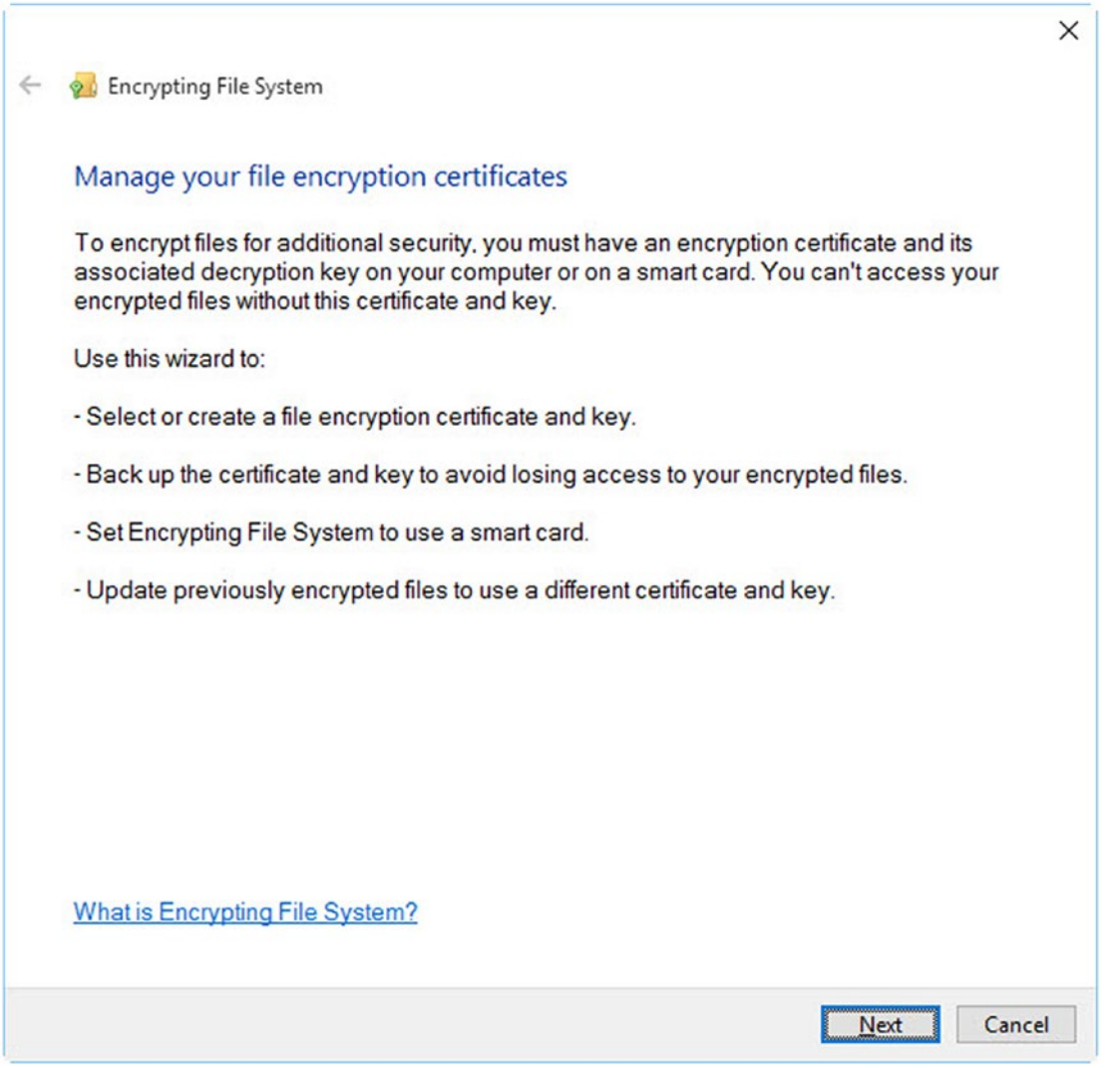


Figure 18-23. *You can back up and restore EFS certificates*

If you need to import your EFS certificate, perhaps because you've reinstalled Windows, or transferred encrypted files to a different user on the PC, or a different PC, you can double-click the certificate file to import it to the currently signed-in user account on the PC.

Note EFS certificates are locked to individual user accounts. Should another user, with her own separate account on the PC, or on a different PC, need to access the files, she can import the certificate to her own account by double-clicking the key file.

Managing EFS Encryption with Cipher.exe

Windows 10 includes a command-line tool called *Cipher.exe*, which can be used to manage EFS encryption on PCs. It needs to be run from a *Command Prompt (Admin)* window and can be used with the following switches and syntax:

- `/e` encrypts files and folders in the format `Cipher /e D:\Secret`.
- `/d` decrypts files and folders using the same syntax as `/e`.
- `/s` tells EFS to encrypt or decrypt all subfolders as well, used in the format `/s:D:\Secret`.
- `/a` performs the operation on ALL files and folders.
- `/f` forces the operation on all files (use with care as it will also reencrypt encrypted files).
- `/q` Quiet mode does not report activity.
- `/h` displays files with hidden or system variables, as these are not encrypted by default.
- `/k` creates a new file encryption key.
- `/u` updates the user's current encryption key.
- `/n` prevents the user's current encryption key from being updated (again, use with care).

- `/r:PathnameNoExtension` creates a new recovery certificate and private key.
- `/w:Pathname` deletes data from unused portions of a volume (can be used to wipe free space on a disk).
- `/x[:PathName] PathNameNoExtension` creates a backup of certificates and private keys for the currently signed-in user.

Managing Device Encryption

Only the Pro and Enterprise versions of Windows 10 support the Bitlocker drive and volume encryption technology, which I'll detail in full, shortly. Microsoft mandated with Windows 8.1, however, that all devices with screens larger than 8 inches should be equipped with a TPM security chip.

This means that some but not all Windows 10 devices will support a feature called Device Encryption. This is effectively Bitlocker with a friendly face, and it's a way to help ensure that consumers, and nontechnical PC owners, can carry tablets and laptops around with them while keeping their personal and sensitive files and data protected.

Caution Device Encryption will encrypt only the drive on which Windows 10 is installed. If you have partitioned your device, any additional volumes you create will not be encrypted by Device Encryption.

When I say that not all devices will come with Device Encryption, not every Windows 10 PC supports it. Typically, any device with a screen of between 8 and 11 inches that comes with both a TPM and supports Connected Standby will support Device Encryption. For devices with screens larger than this, Device Encryption will be unavailable.

Caution It's worth noting that devices with screens of 11 inches or more, and that have Windows 10 Home installed, will not have Device Encryption available as an option in the Settings app. You will also not be able to encrypt these PCs with Bitlocker, as Bitlocker is supported only in the Pro and Enterprise editions of Windows 10. If you are purchasing a laptop or tablet with a screen of 11 inches or larger (10 inches to be on the safe side) and want to guarantee you can encrypt your drive, it's best to factor the upgrade to Windows 10 Pro into the cost of the device.

To activate Device Encryption, open the Settings app and navigate to *System*, and then to *About*. This will display if your device supports it, a Device Encryption option; see Figure 18-24.

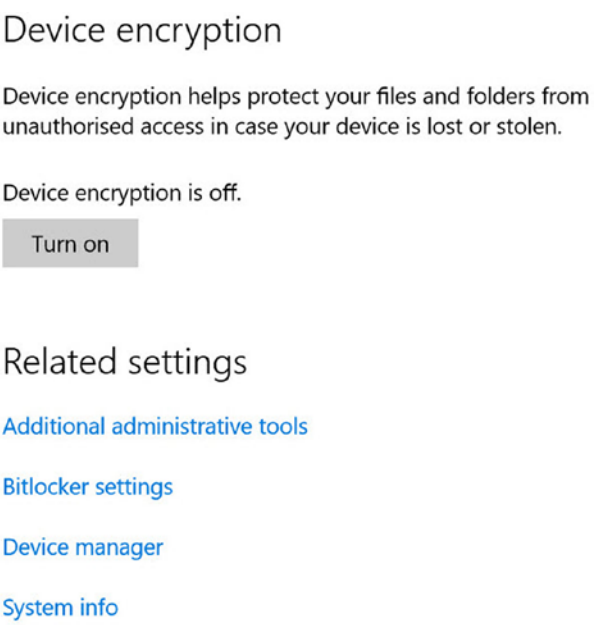


Figure 18-24. *You can manage Device Encryption in the Settings app*

So, what happens with your decryption key, as it's all well and good encrypting your device, but if something goes wrong, such as the PC not starting properly, and all of a sudden you find yourself locked out and asked to enter your decryption key: where do you find it?

If you have signed into the device using a Microsoft account, you will find your Device Encryption key online at https://onedrive.live.com/recoverykey. I find it useful to keep a link to this in the browser on my smartphone, just in case. If you use Bitlocker with a company Domain, the recovery key is stored in Active Directory.

You can manually back up your encryption key, however, should you want a copy on a USB Flash Drive, or if you have signed into the PC using a local account. In the Start Menu, search for **device encryption,** and choose the option to *Back up your recovery key* when it appears. This will display a wizard that allows you to create a backup of the key.

Caution Do not store the backup copy of your recovery key on a drive encrypted by Device Encryption or Bitlocker (or EFS for that matter), as you will be unable to recover the key later should you become locked out of the drive.

Encrypting Your PC with Bitlocker

On PCs running Windows 10 Pro or Enterprise, you will have an option to use the Bitlocker drive and volume encryption system to encrypt the contents of your PC. Bitlocker can be found in the Control Panel, and while it doesn't require that a TPM chip be installed on the PC, there are very compelling reasons to have one.

Bitlocker encrypts full disks and partitions on your PC. You can individually select which drives are encrypted, though you must have the partition on which Windows 10 installed encrypted, if you want to encrypt any other drives, or have those drives autounlock when the PC starts. Before you start encrypting drives, however, you need to activate the TPM, as this is the chip on which Windows 10 stores its encryption keys. The TPM ensures that if a drive that's encrypted is removed from the PC, it cannot be decrypted. This is because the TPM is part of the motherboard on the PC and cannot be removed.[1]

[1] Some desktop PCs come with the TPM as a removable module, usually purchased separately from the motherboard itself. In these circumstances, the TPM can be moved to a different PC containing a compatible module slot (usually with a motherboard from the same manufacturer) and should unlock any encrypted drives that are moved with it once it has been enabled in the BIOS or UEFI firmware.

Managing a TPM on Your PC and in Windows 10

The TPM chip on a PC must be activated in the BIOS or UEFI firmware. Should you want to use Bitlocker on your TPM-equipped PC, but you're receiving the message that a TPM chip isn't installed, it's because you need to go into the firmware on your PC and activate it.

You manage your TPM by opening the *Bitlocker* options in the Control Panel, or by searching for Bitlocker in the Start Menu (it is also available by searching for **tpm.msc**). When the Bitlocker panel is open on your screen, click the TPM Administration link in the bottom left of the window.

The TPM Management screen is the standard Microsoft Management Console fare with three vertical panels; see Figure 18-25. Here there are options in the right panel to prepare the TPM (basically to turn it on), turn it off, and more. If you prepare the TPM and begin using it to encrypt drives, an owner password is created automatically and stored in the chip itself. Should a problem arise, and you find yourself locked out of a drive, you can use the *Reset TPM lockout* option to automatically reset your Bitlocker access permissions. You might want to set the password manually however (though there's no need to do so), and you can do this by selecting the *Change Owner Password* option.

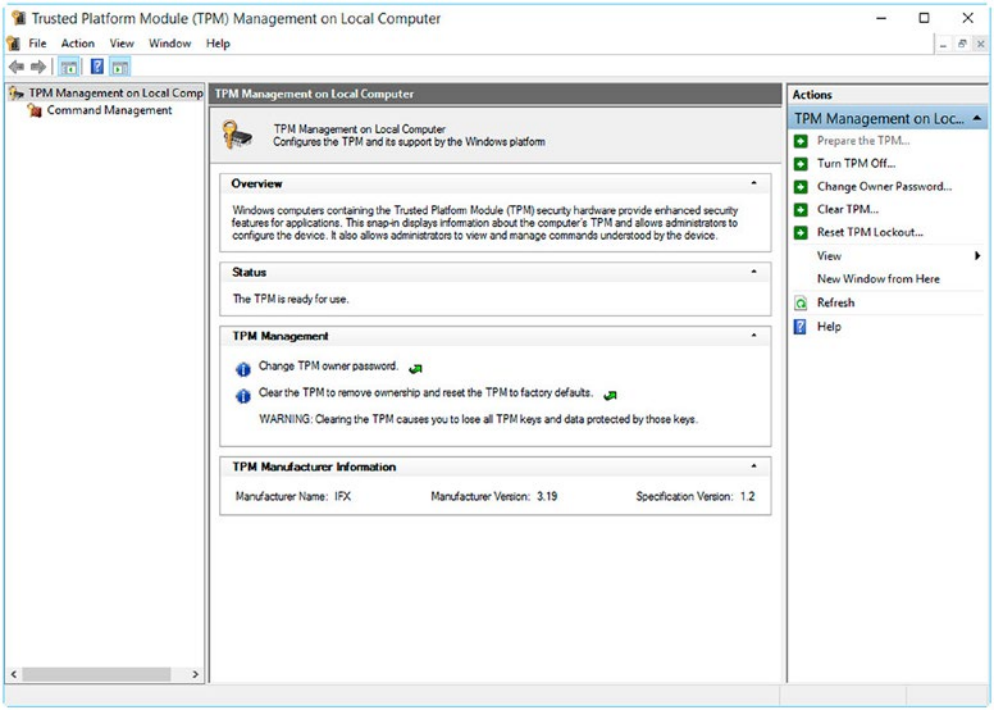


Figure 18-25. *You administer your TPM from within Windows 10*

The *Clear TPM* option can be useful if you are performing a full, clean reinstallation of Windows 10 and are not keeping any drives or partitions that have been encrypted with Bitlocker. This will delete any and all encryption keys from the TPM chip. These can build up over time as you encrypt, decrypt, and reencrypt drives, and there's only a finite amount of storage available in the chip.

Using Bitlocker Without a TPM

It's possible to use Bitlocker on your PC without having a TPM chip installed, though I don't recommend it. Instead, you will need to have a USB Flash Drive that contains the Bitlocker key plugged into the PC every time the computer starts. While this might seem like a great way to ensure nobody can use the PC or access your data when you're away from it, a USB Flash Drive is not the same thing as a security smartcard.

The problem arises because a USB Flash Drive has a normal file system, like any drive on your PC, and this file system can become corrupt. With USB Flash Drives, an operation as simple as unplugging the drive from the PC while it's being read can cause a corruption, and as such, you really can't rely on a Flash Drive to remain stable for such a critical role as providing TPM access to a PC.

That said, should you *really* want to use Bitlocker on your PC without a TPM, you can activate the option in the Group Policy editor (search for **gpedit** in the Start Menu) and navigate to *Computer Configuration* ➤ *Administrative Templates* ➤ *Windows Components* ➤ *Bitlocker Drive Encryption* ➤ *Operating System Drives*; see Figure 18-26.

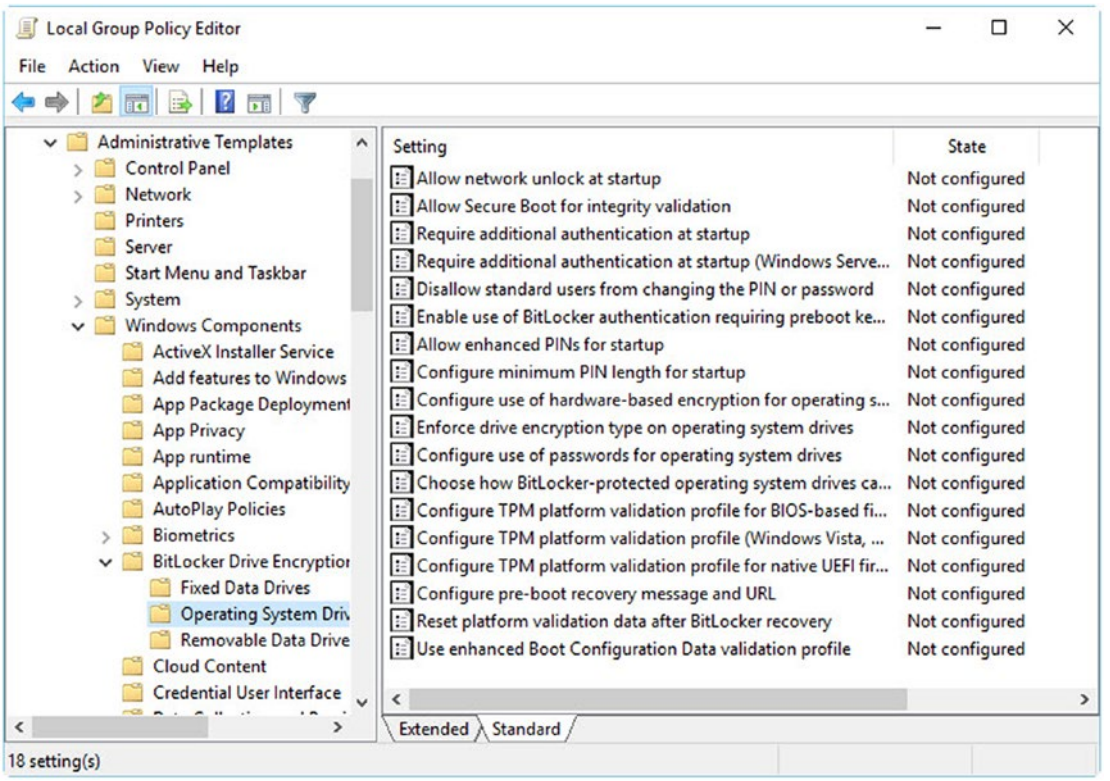


Figure 18-26. *You can configure the PC to use Bitlocker without a TPM in Group Policy*

Double-click the *Require additional authentication at Startup* option and enable the policy. You will be given a verbose description of what enabling the policy will do, and presented with a check box, which will already be checked, to require a startup key on a USB Flash Drive; see Figure 18-27. Once the policy is enabled, restart the PC to allow Bitlocker to be used without a TPM.

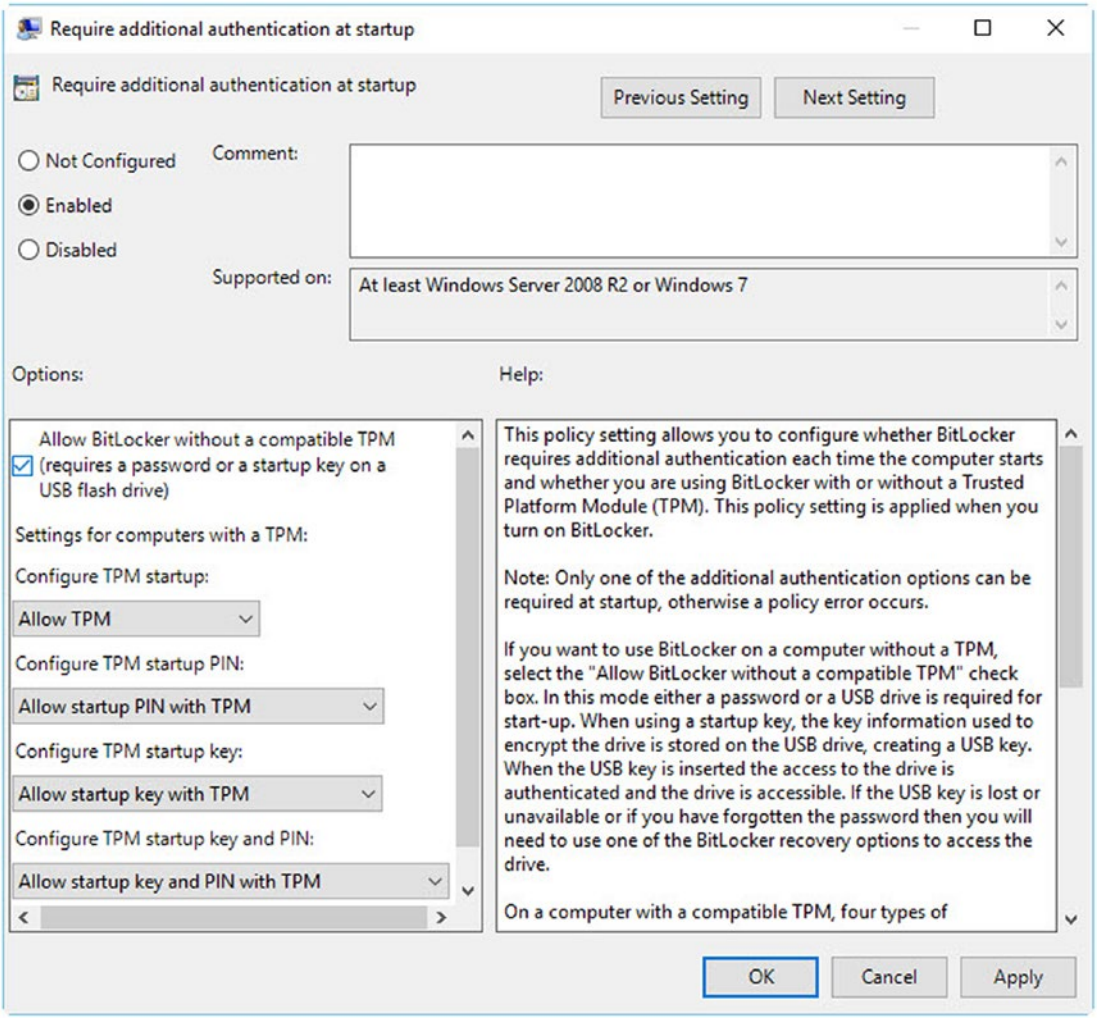


Figure 18-27. *The Group Policy editor will inform you what the policy change will do*

Managing Bitlocker Encryption on Your PC

You manage Bitlocker encryption from the main Bitlocker panel, accessible in the Control Panel, but also by searching for **Bitlocker** in the Start Menu. You will see collapsible panels for each of your installed hard disks (and partitioned volumes); see Figure 18-28.

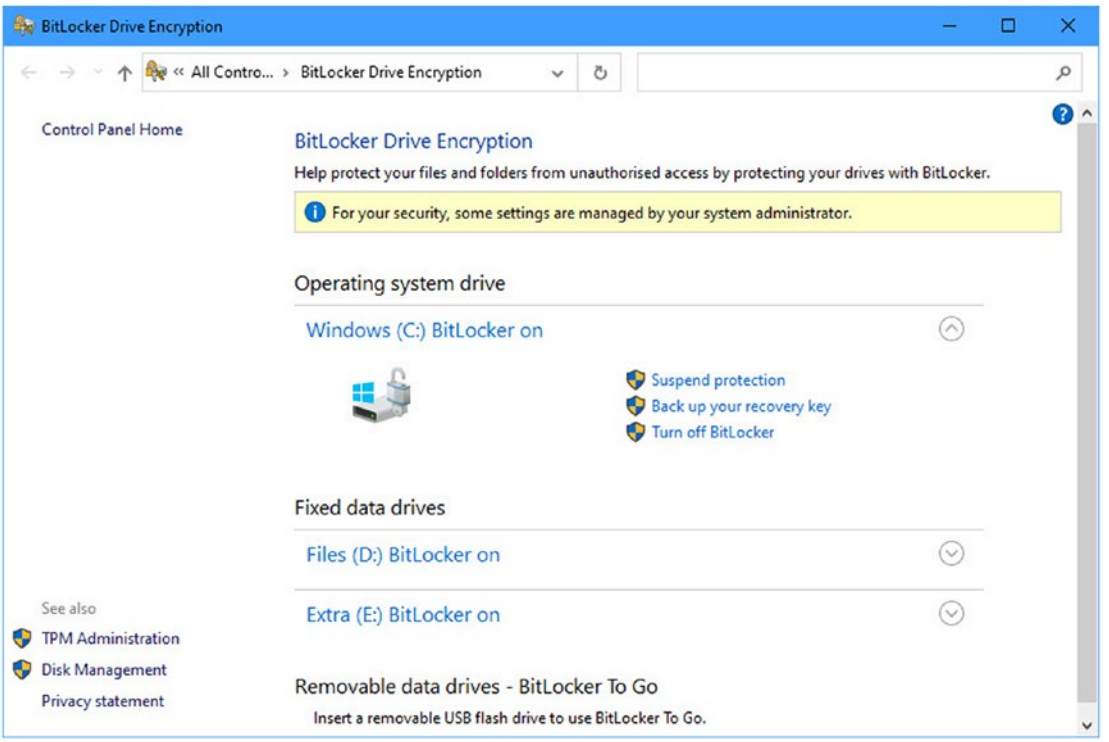


Figure 18-28. *The Bitlocker panel displays collapsible panels for all your disks and partitions*

Expanding a drive's panel will present various options for managing Bitlocker on that particular drive. These include options for encrypting and reencrypting the drive (fairly obviously), as well as creating a backup copy of your recovery key, adding a password or smartcard to unlock the drive, or activating or deactivating autounlock of the drive. You can also temporarily suspend protection, which can be useful if you are trying to undertake intensive file management tasks, while the system is encrypting your drive for the first time.

Caution If you are updating the BIOS or UEFI firmware on your PC from the desktop, you should suspend Bitlocker protection. This is because on some firmware, Bitlocker will see what it thinks is "new" hardware and require input of your recovery key on the next restart.

That really is all there is to configuring Bitlocker, as it's designed as what I like to call a "fart-and-forget" system. You can carry on working while Bitlocker encrypts your drives, and even shut down the PC or put it to sleep. Bitlocker will simply resume encryption when you start the PC and sign in to your account again.

Managing Your Bitlocker Recovery Key

When you encrypt a drive using Bitlocker, you will be prompted to create a backup copy of your encryption key, and, unlike EFS, the process simply won't progress until you've done so; see Figure 18-29. If you have signed into your PC using a Microsoft account, you will be prompted to save a copy of the recovery key directly to the cloud. This can be very useful should you find yourself locked out of the machine; simply point a browser on any device at `https://onedrive.live.com/recoverykey` and sign in to view the 48-character unlock code.

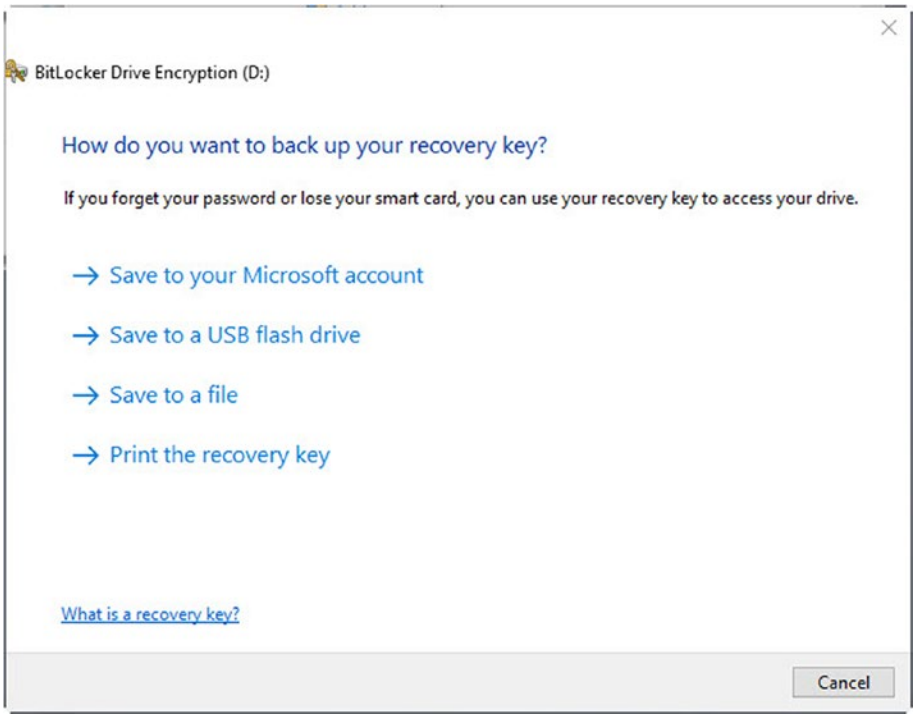


Figure 18-29. *You can back up your recovery key in various ways*

Additionally, there are options to save the recovery key to a USB Flash Drive (you'll need to plug one in at this point obviously), save it to a file, or print it. It should be noted that for your Windows 10 drive, the option to save the key to a USB Flash Drive doesn't appear. This is a little odd, but you can choose the *Save to a file* option instead, and merely point to an attached USB Flash Drive on the PC instead.

Caution Do not store the backup copy of your Bitlocker recovery key on a drive encrypted by Device Encryption or Bitlocker (or a folder encrypted with EFS), as you will be unable to recover the key later should you become locked out of the drive. Also, if you choose to carry a USB Flash Drive with the recovery key with you when you travel, do not keep it in the same bag as your laptop or tablet, which will prevent them from being stolen together should a thief strike.

Using Bitlocker To Go

Bitlocker To Go is a tool that allows you to encrypt removable drives such as USB Flash Drives and external hard disks (and no, please don't encrypt the drive that contains your Bitlocker and EFS recovery keys, as that's just asking for trouble).

You can encrypt removable drives through the main Bitlocker panel, where they will appear listed below the hard disks and partitions in your PC. One crucial difference is that the unlock key for a removable drive is never stored in the TPM (which also means you can use Bitlocker To Go on PCs that don't have a TPM). The reason for this is that the drives are, by their very definition, mobile and can be used on any PC. Thus, the only options available when you encrypt a removable drive are either to set a password or to use a smartcard; see Figure 18-30. Additionally, you cannot set a drive encrypted with Bitlocker To Go to automatically unlock, as that would rather defeat the point of it being encrypted in the first place.

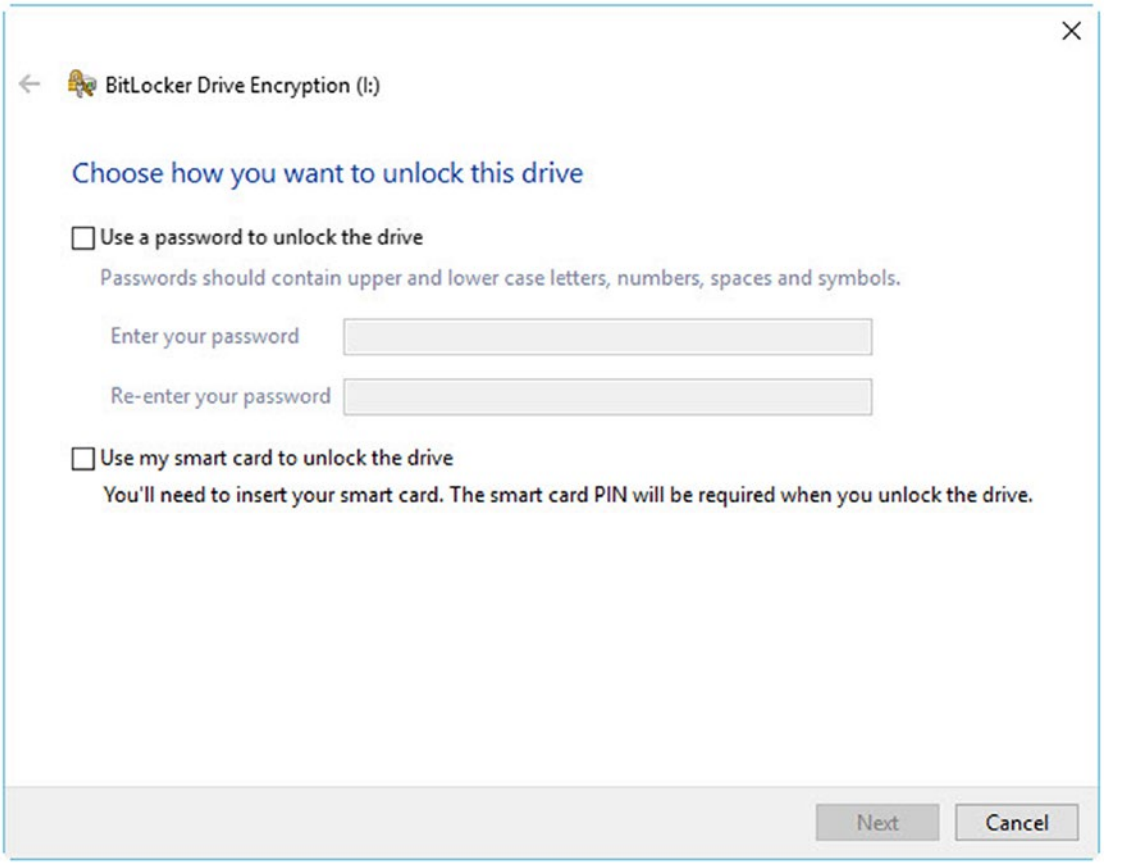


Figure 18-30. *Bitlocker To Go will not store the unlock code in your TPM*

Tip While we're on the subject of removable drives, there are two Group Policy options you can set in Windows 10 Pro or Enterprise that can significantly enhance the security of your systems. The first of these can be found in *Computer Configuration* ➤ *Administrative Templates* ➤ *Windows Components* ➤ *AutoPlay Policies*, where you can block USB and other removable media from automatically starting and opening files and apps when inserted into the PC. This is a common way for malware to spread, and so disabling AutoPlay can be a great boost to security.

You can also help guard against data theft. In *Computer Configuration* ➤ *Administrative Templates* ➤ *System* ➤ *Removable Storage Access*, you can block all manner of removable storage completely on the PC, including USB Flash Drives, CDs, DVDs and Blu-ray disks, floppy drives, and more besides.

Summary

The security and encryption facilities in Windows 10 are both extensive and easy to use. They should, however, always be used with care, and some basic rules should be followed. The primary rule is always to make sure you have a backup copy of your recovery or encryption key. You should always make sure that you never store this key in a folder or on a drive that is, itself, encrypted, as you may not be able to recover it when you need to.

Encryption is a great way to prevent thieves and unwanted eyes from getting access to your files and data. This is in the same way that we use antivirus software to prevent the spread of malware to our PCs, a subject we'll be looking at in depth in the very next chapter, including how we can troubleshoot and remove malware after a PC has become infected.

CHAPTER 19

Troubleshooting Viruses and Malware

Probably the worst fate to befall a PC is for it to become infected with malware. Long gone are the days when viruses were fairly innocuous things; the first one I got on a PC played "Yankee Doodle Dandy" to me every day at five o'clock but did nothing other than that. Nowadays viruses, malware, and ransomware exist to make money, real money, for the criminal gangs that create them. Why is this? Simply put, a few years ago, many criminals around the world discovered that, rather than rob banks and steal jewelry, they could make much more money sitting at home by infecting our computers.

Windows 10 includes some excellent security systems, such as SmartScreen and the ransomware protection that are both part of Windows 10, and which I detailed in Chapter 18, which can identify malicious files when downloaded from the Internet and block changes to files and folders being made on your PC, and User Account Control (UAC), which can help defend against software that wants to be installed, or run as an administrator.

The weak point with our PCs, however, is the soft, squidgy thing that sits at the keyboard (you might be aware of the IT support term PEBKAC, which stands for "Problem Exists Between Keyboard and Chair"), and it's always the user who will be exploited. How will this happen? Malware will attempt to exploit both our natural tendency not to read things properly on our screens, and just click "Okay" anyway, and also the lack of technical knowledge that most PC users have.

How to Defend Against Malware

This does seem like an important place to begin, as it's always the user who is the point of entry for malware on a PC (unless the security on a PC is pretty nonexistent, it's extremely difficult for a PC to become infected any other way). If you are a system

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_19

administrator, it's very likely that you'll have your systems locked down as best as you can. This will mean you will have up-to-date antimalware software installed, the apps installed on the PC, and your copy of Windows will always be kept patched and up to date, you won't have anything installed that could pose a security risk, and your users won't be administrators, so they won't be able to install malware themselves.

This, of course, is a rose-tinted view of the world, and while it might be the case in large corporations, it certainly isn't the case for many small businesses and almost every home user, where the PCs in use are much more likely to be individual, stand-alone units. It's crucial then with so many more people working from home and using their own computers to access company systems and data to educate PC users in how to identify possible malware attacks, so that they can be defended against.

Note Because of the interconnectedness of computer systems across the Internet, an end user accessing your organization's systems using MacOS, iOS, or Android is no more secure than someone using Windows 10 or Windows 11 on a PC. There are plenty of malware threats to Apple Mac computers every year, and both iOS and Android are known to have had malware injected into apps and games, no matter how vigilant Apple and Google are at policing their app stores. Additionally, there's little to stop an iOS or Android user from uploading a document or file containing malware to your organization's file share, from which it can be opened by other users. Thus, it is important to employ mobile device management on *all* computers that connect to your systems, and I detail how you can do this in Chapters 21 and 23.

Malware on PCs spreads in the following ways:

- App downloads from the Internet–these can appear as legitimate versions of the app you're really looking for, a cool new game, or perhaps a codec that's required to play video on a website you've visited.
- Infected websites that will encourage you to install a codec or plug-in that contains a malware payload. This is usually a website that purports to offer something compelling or cool, such as a cartoonize yourself app, or the latest video of a naked celebrity.

- Some malware is injected into legitimate files, but that are hosted on websites other than the original download source, such as a hardware driver or Windows installation ISO file hosted on a generic driver website.
- Malware that's injected into legitimate websites using vulnerabilities in the site code to permit changes to the site, which can include links to autodownload malware, or to display full-screen warnings that your PC is already infected, and you have to download the fix that's offered.
- Macros in infected office documents, such as Word, Excel, and PowerPoint.
- Infected downloadable files from file-sharing (Torrent) websites. These are commonly modified versions of existing files, such as pirated software.
- Viruses that are transferred from one PC to another, by sending themselves as a "Look at me" file via email, or by infecting USB Flash Drives or other removable media.
- "Worm" malware that tunnels its way across your network using zero-day vulnerabilities in Windows, your network hardware, or software that has yet to be patched.
- Malware injected into apps that gets through scanners in the Microsoft, Apple, and Google app stores.
- Malware accidentally or intentionally injected into your network by autorunning USB Flash Drives (this is one for NSA conspiracy theorists).

It's actually very easy to defend against malware from your organization's systems, and you should make sure that the following three rules are included with any training you provide for people:

1. NEVER install or click Okay on anything unless you specifically set out to do so beforehand.

2. NEVER download anything unless you trust the source website implicitly, or unless it's from an official Microsoft, Google, or Apple App Store, and even then, don't install anything because you're being nagged to do so.
3. NEVER perform any action on your PC simply because a website wants you to do so.

Tip A good way to keep up to date with the types of malware threats in the wild, and with the tools you can use to defend against them and remove them, is the Microsoft Malware Protection Center, https://pcs.tv/37BBUVH, which is a great resource for articles and downloads and support for system administrators.

What Is This Malware Stuff Anyway?

Malware comes in many different forms these days, each with its own purpose, some of which is to affect your files and your PC, and some of which is to affect other systems:

- **Viruses** will affect the local PC and are increasingly rare, as their purpose is only to make it difficult to use the PC. This might include infecting the BIOS or UEFI firmware system so as to make the PC unbootable.
- **Back doors** will use your PC as a route into your network, to try to allow a hacker to steal sensitive data such as customer or staff details, or credit card details. They are also used for industrial and state-sponsored espionage.
- **Keyloggers** will record what you type on your keyboard and the websites you visit, in order to try to harvest usernames and passwords for shopping or other sites where your credit card information is stored, or your online banking (on-screen keyboards are good to protect against this).

- **Trojans** are malware payloads that look, to all intents and purposes, like a perfectly legitimate file or app. They could even be the app installer or file you are looking for but embedded within the code will be a malware payload.
- **Bots** are not to be confused with the chatbots just about every company uses online these days to seemingly make it easier to interact with that company online (which they don't). This malware will use your Internet bandwidth to link your PC into a network of infected PCs that will collectively perform actions such as Distributed Denial-of-Service (DDoS) attacks on major companies' websites and servers.
- **Rootkits** will attempt to inject themselves into the Windows 10 kernel and boot files, so as to bypass any security on the PC and load unfettered at startup. They then have full administrative access to the PC.
- **Worms** propagate across your network by exploiting zero-day (unpatched) vulnerabilities in your operating system, network hardware, or software.
- **Macros** are malware programs that are embedded inside document types that permit code to be run, such as spreadsheets and other office documents.
- **Ransomware** is a particularly nasty form of malware that will encrypt any and all files found on your PC or network stores, demanding money for a decryption key, which will itself also likely contain malware.

Defending PCs Against Malware

Throughout this book, I'm detailing the security tools available in Windows 10 that can defend a PC against malware. I just want to run through them here though, to reiterate what each of the tools is, and why they're all important:

- **UAC** is the security subsystem in Windows 10. UAC will alert the user whenever they attempt to make a change to a PC that could affect other users on the system. Administrators will get an elevated OK/Cancel prompt, and standard users and children will be required to enter an Administrator password.

- **Windows Virus & Threat Protection** is the free antimalware package that's included with Windows 10. These days it's pretty good, and in tests of security suites can hold its own against the popular third-party packages.
- **Windows Firewall** is actually a really good firewall defense and doesn't need to be replaced by a third-party firewall package, with most third-party security suites not including a firewall as a result.
- **Windows Advanced Firewall** offers configurable rules for apps, ports, and services, and is useful for people who need more control over their firewall, such as some businesses and gamers.
- **Windows SmartScreen** checks all files and apps downloaded from the Internet against white and black lists of known files held and maintained by Microsoft and many third-party security companies. If it detects a file known to contain malware, it will block it, and it will alert you if it cannot recognize a file that might contain malicious code.
- **Ransomware Protection** is available in the Windows Security Center, but it is not on by default as it can interfere with some perfectly legitimate file operations and needs to be configured. It is not available however if you are using a third-party security suite.
- **Secure Boot** is a firmware system designed to prevent rootkits from gaining access to the boot system on your PC, and from infecting the UEFI system. It is incompatible with Windows operating systems before Windows 8.1 and some Linux distros, and needs to be disabled to get incompatible dual-boot systems to run. Not all PCs support Secure Boot. Any PC sold with Windows 8.1 or later will support it, but older PCs may not, motherboards you purchase online may not, and PCs with the older BIOS firmware definitely will not.
- **Windows Defender Advanced Threat Protection (ATP)** is a system released by Microsoft for corporations, as an optional extra for PCs, to analyze their networks for malware or other unwanted activity, though some of its features have been integrated into Windows 10 and I detailed these in Chapter 18.

It's worth noting that each and every one of these security systems can be disabled. If you have a dual-boot PC, for example, running Windows 7 or some Linux distros alongside Windows 10, Secure Boot will have to be disabled, as it would prevent those other operating systems from starting. UAC, Windows Defender, the Windows Firewall, and SmartScreen can all be disabled in Windows 10, though if you don't have installed alternatives, Defender and the Firewall will nag you to switch them back on. In fact, it's far too easy to disable some security features. SmartScreen, for example, can be disabled through a simple on/off switch in the Edge browser that doesn't, in my own opinion, explain how important the feature is at all; see Figure 19-1.

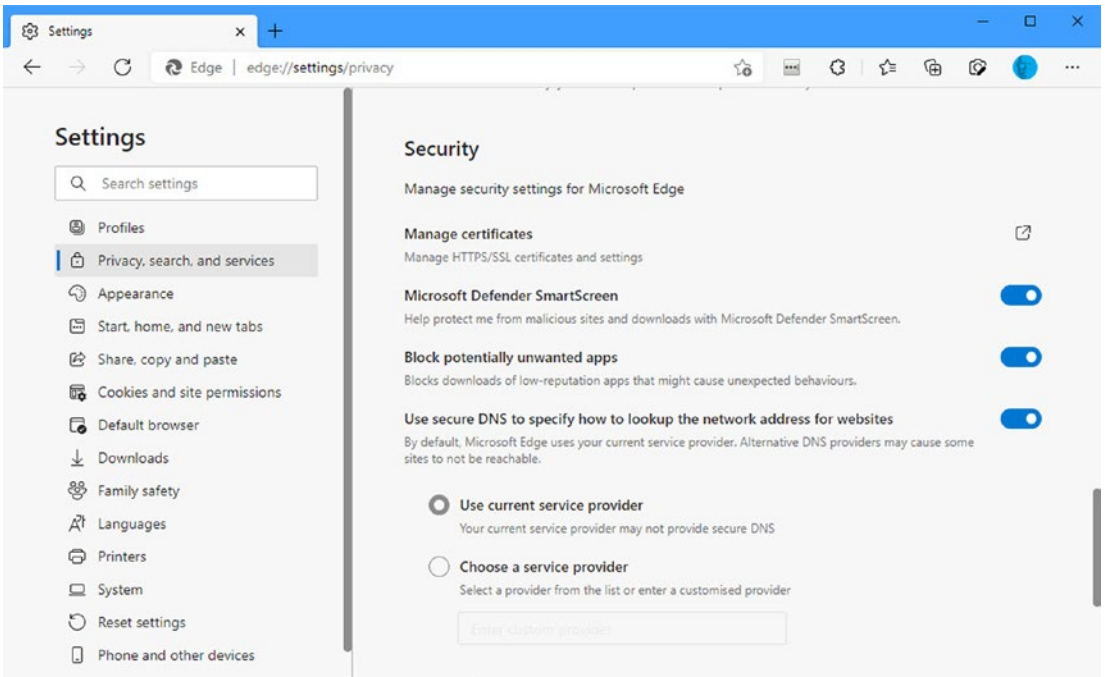


Figure 19-1. *SmartScreen is all too easy to disable in the Edge browser*

It is for this reason that only users of a PC who actually MUST be administrators should be so, and every other user should be a standard user. The weak link in a PC's security will always be the soft, squidgy thing sitting at the keyboard. Criminals are extremely good at tricking people into clicking and authorizing things they shouldn't, or to entering secure details on a website that's fake, but even with this being the case, having lax security can let a hacker or malware into your system everywhere from a coffee shop to CIA headquarters.

Defending Your Files Against Ransomware

Ransomware is a very different beast from malware, and in many ways it's considerably more dangerous should your PCs become infected. Ransomware will encrypt all of your files and documents, and then demand a ransom (the clue was in the name) for the decryption key. This key is itself likely to be loaded with more malware, and so the cycle will continue.

The ransom demanded for the unlock code for your files is usually several hundred dollars though stories have leaked about some companies playing out millions of dollars, and although it's known that many people, including businesses, do pay the ransom, it's also something that many other people, and especially small businesses, simply wouldn't be able to afford. No organization is in the clear either it comes to ransomware, as while small businesses can be particularly vulnerable, even huge organizations such as the UK's National Health Service (NHS) have been affected.

So how do you protect your PCs from ransomware? It might seem that the obvious way is to keep your files and documents that are normally stored in your Shell User Folders (Documents, Pictures, Music, and Video) in a different location on your hard disk. This does make them slightly more awkward to access, but crucially it offers no guarantee of protection, as ransomware is highly likely to scan your whole hard disk, network shares, and all other available storage, and encrypt every known document type it finds.

Tip Windows 10 does include a ransomware protection feature, but it is only available if you use Windows 10's inbuilt antivirus and antimalware tools. I detailed it in full in Chapter 18.

The trick to defending your files against ransomware is incremental backups. We used to create these all the time, perhaps once a month onto a few CDs or DVDs, or once a week through backup software onto an external hard disk. These days, with Windows features such as OneDrive sync, and other cloud services like Dropbox, and Google Drive, we've gotten used to instantaneous sync. The problem this creates is that every time a file changes (such as being encrypted), it will be reuploaded to your cloud storage.

Some cloud systems will allow you to set a sync schedule, such as backing up files every 48 hours, though it's possible that in the case of a ransomware infection, you'll need longer than this. For this reason, I strongly suggest using dedicated backup software with an external USB hard disk or secure network location which should be set to reauthenticate the connection each time. The backup can be set to run all the time, or on a schedule of up to a week or two (meaning you'd only ever lose 1 or 2 weeks' worth of file updates). The advantage though is that you can physically unplug a hard disk from your system, meaning that no malware or ransomware can ever get onto it. This is opposed to network-attached USB hard disks and network-attached storage (NAS) drives, which will be viewable through your PC all the time and thus also viewable by the ransomware.

Versioning support, which is offered by many backup systems and services, can also be very useful, as it allows you to roll back to previous versions of (i.e., nonencrypted) files. Where this falls down is that the people who create ransomware know this too, so versioning does not create a guarantee of file security. Only a segregated backup strategy is any guarantee that if you are infected by ransomware, and need to completely wipe and reimage the PC, you can recover all of your files.

Manually Removing Malware from a PC

Sometimes you will need manual file access to a PC to remove malware. This is because the "fix" might come in the form of detailed instructions from a security website (please only use the websites from the well-known security providers such as Symantec and Kaspersky for this). In this case, how do you get that file access without having the malware run automatically? Well, there are various options available to you for this.

Microsoft Defender Offline Scan

Windows 10 includes an offline virus and malware scanner and removal tool. You can access this from the Start Manu by searching for *Windows Security* (also available by clicking the *Shield* icon in the Taskbar notification area) and then clicking *Virus & threat protection* and scrolling down the page to select *Microsoft Defender Offline scan*; see Figure 19-2. You will be prompted to restart the PC, and then the antimalware scan will be run from within the startup environment, hopefully before any malware has loaded into memory.

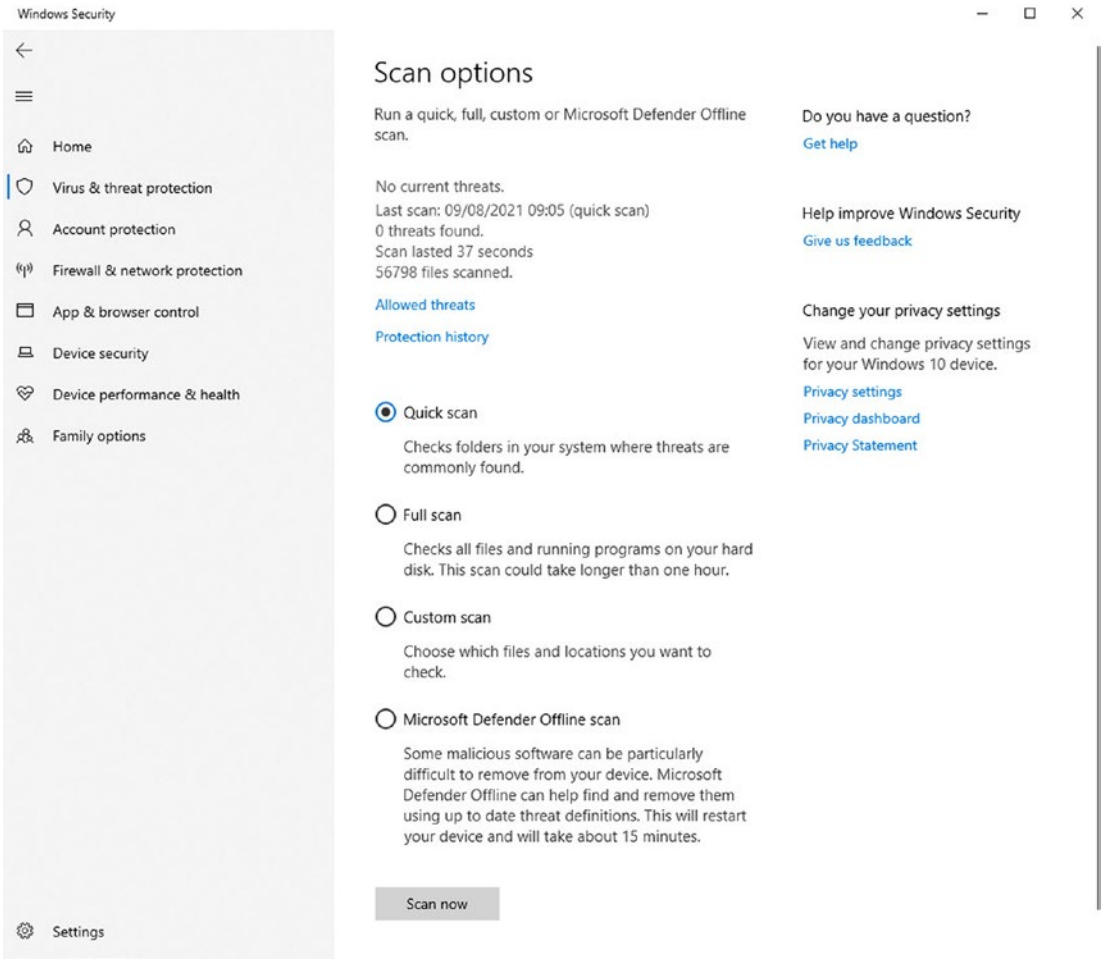


Figure 19-2. *You can run an offline virus and malware scan in Windows 10*

Using Safe Mode and Diagnostic Mode

Malware, once it gets its hooks into your PC, can be extremely difficult to remove. It buries itself in the Windows services that are automatically loaded at the PC's startup, or within the OS kernel itself. Malware will commonly run a series of codependent services on the PC. This means that when you shut one down, other malware services will recognize that it's no longer running and automatically restart it. Antimalware software can shut down all the offending services simultaneously, but this requires the malware to be identified by your antivirus software.

Should you need to remove malware manually, it can be extremely tricky but is still possible. Some malware is relatively straightforward to remove and can be done from within Safe Mode or Diagnostic Mode in Windows 10. Safe Mode and Diagnostic Mode (also known as Diagnostic Startup) are similar, but also very different from one another.

Starting Your PC in Safe Mode

You're probably already familiar with Safe Mode. This is a reduced functionality mode in which only essential Windows services, and no third-party services or apps, are loaded. There are various ways to get to Safe Mode in Windows 10. If you restart your PC while holding down the Shift key, the system will restart into the Recovery options menu. Once here, click *Troubleshoot*, then *Advanced options*, and then *Startup Settings*. This will restart the PC and present a version of the legacy Windows boot menu; see Figure 19-3.

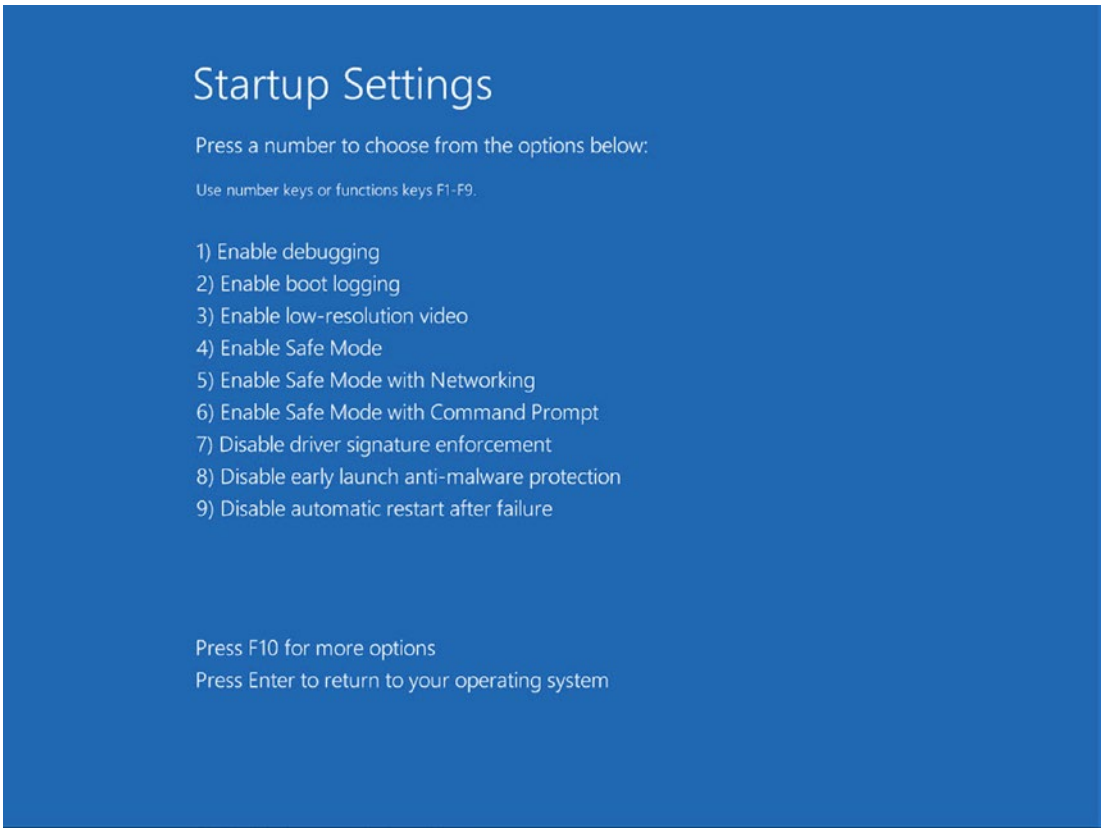


Figure 19-3. *The Startup settings menu allows you to invoke Safe Mode*

There are three Safe Mode options at this menu: *Safe Mode*, *Safe Mode with Networking*, and *Safe Mode with Command Prompt*. Safe Mode is the default option. This will load the basic, essential Windows services only with a desktop interface and basic graphics, but with all networking features disabled. Choosing this option can be useful when removing malware, as you are isolating the machine, and not allowing the malware to see other PCs or devices on your network or to gain access to the Internet.

Safe Mode with Networking will also boot the minimal Windows services, but will also load the networking drivers, giving the PC both local network and Internet access. You can use this if you do not have another PC on which to download a malware removal tool, and where the download of the tool is blocked by the malware on the regular desktop.

Safe Mode with Command Prompt starts Windows 10 in a Command Prompt–only environment, with no desktop interface. If you are proficient with command-line tools and utilities and prefer to work in this way, it is a good option for troubleshooting and malware removal; I will detail useful command-line tools for troubleshooting in Chapter 27.

The other way to invoke Safe Mode is through the System Configuration panel. You can best access this by searching for **msconfig** in the Start Menu. This displays a utility from where, in Windows 7 and earlier, you managed the startup apps on your PC (a process that's since been moved to the Task Manager). It's also from where you can invoke Safe Mode and Diagnostic Startup.

Caution When you activate Safe Mode or Diagnostic Startup using MSConfig, the PC will then **always** start in that mode, until you open MSConfig again and select the *Normal startup* option.

Safe Mode can be invoked from the *Boot* tab; see Figure 19-4. There are various options available to you that mirror those available from the Recovery Environment menu.

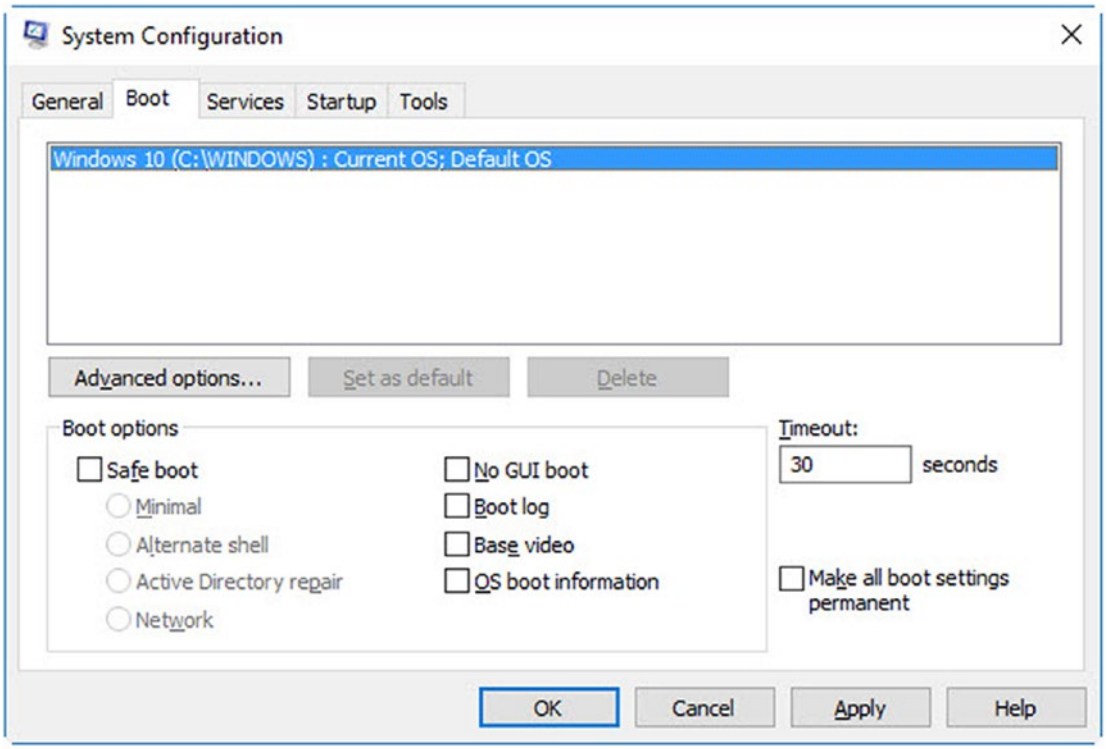


Figure 19-4. *You can start Safe Mode from MSConfig*

- **Safe boot–Minimal** will start the PC in the standard Safe Mode, with no networking support.
- **Safe boot–Alternate shell** will start the PC with a Command Prompt–only interface.
- **Safe boot–Active Directory repair** is an additional option that will also load the Active Directory services, in addition to networking services.
- **Safe boot–Network** loads the OS in Safe Mode with networking services also loaded.

Additionally, there are four checkbox options also available:

- **No GUI boot** will load the OS without displaying the Windows loading screen. This can be used when you are troubleshooting display problems.

- **Boot log** saves a log of what starts and is loaded to the file `C:\Windows\Ntblog.txt`.
- **Base video** forces Safe Mode to use only the standard VGA video drivers that come with Windows. This can be useful for troubleshooting display driver issues.
- **OS boot information** can be used in conjunction with the No GUI boot option. It will display a list onscreen of services and Windows components that are loaded and run, as they are invoked. You may be familiar with Safe Mode displaying this information by default in versions up to Windows XP.

Note You may have noticed a check box to *Make all boot settings permanent*. This isn't because you're paranoid enough to always want to start your PC in Safe Mode. It's instead because the four checkbox items I detailed, from No GUI boot to OS boot information, can be invoked independently of Safe Mode. Checking the Make all boot settings permanent option will write these to the boot system for your OS.

Starting Your PC in Diagnostic Mode

Diagnostic Mode is different from Safe Mode in that it's not quite as limiting. In Safe Mode, nothing except the base services and drivers are loaded when the OS starts. This leaves you with (possibly) no networking, very limited graphical functionality and, crucially, with some of the Control Panel applets disabled; see Figure 19-5.

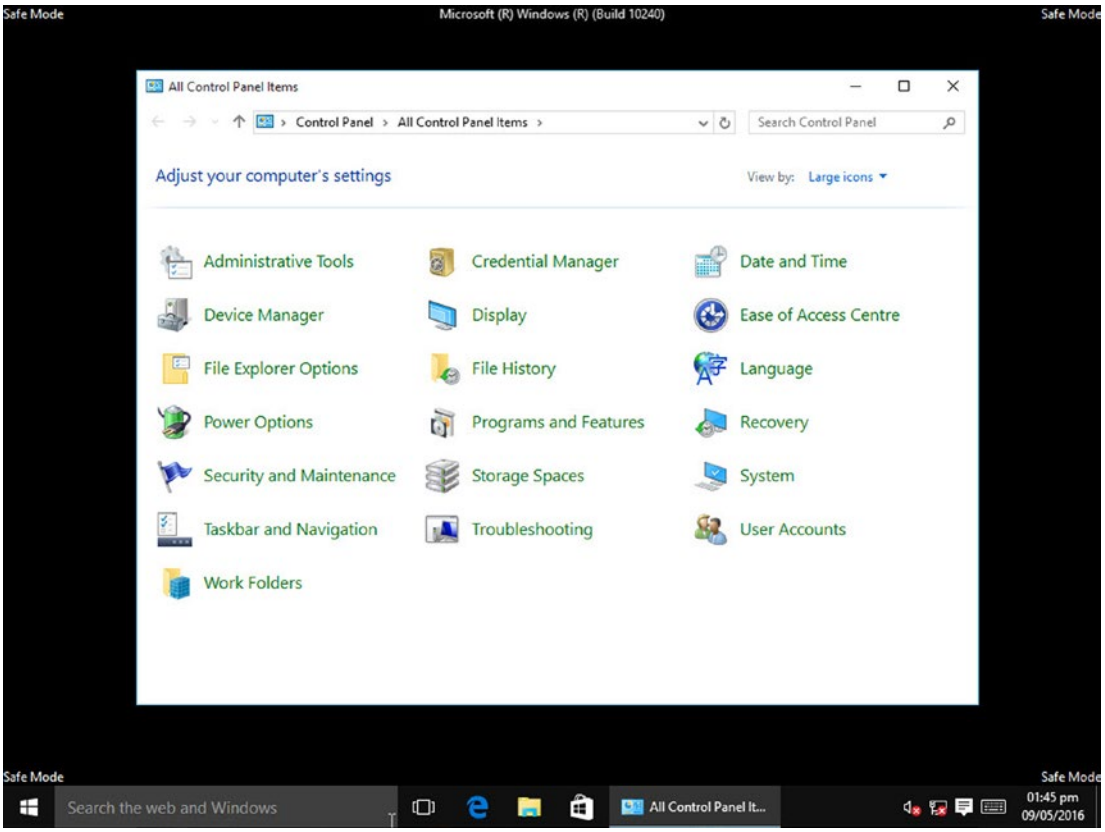


Figure 19-5. *Not all Control Panel applets are available in Safe Mode*

You may find this limiting and might, for example, need to access a feature such as the Windows Firewall when manually removing malware from the PC. For this you can use Diagnostic Startup. This is different from Safe Mode in that more is loaded when the PC starts, including the full Control Panel. The startup items include the graphics drivers, so you have a full desktop experience. It will mean, however, that some Windows or third-party services are loaded (your graphics subsystem will likely be a third-party service) that would not be loaded in Safe Mode, and these might be infected.

You can invoke Diagnostic Startup from **MSConfig**, by choosing its option under the *General* tab; see Figure 19-6. Again, remember that when you want the PC to return to normal startup, you will need to open MSConfig again, and check the *Normal startup* option.

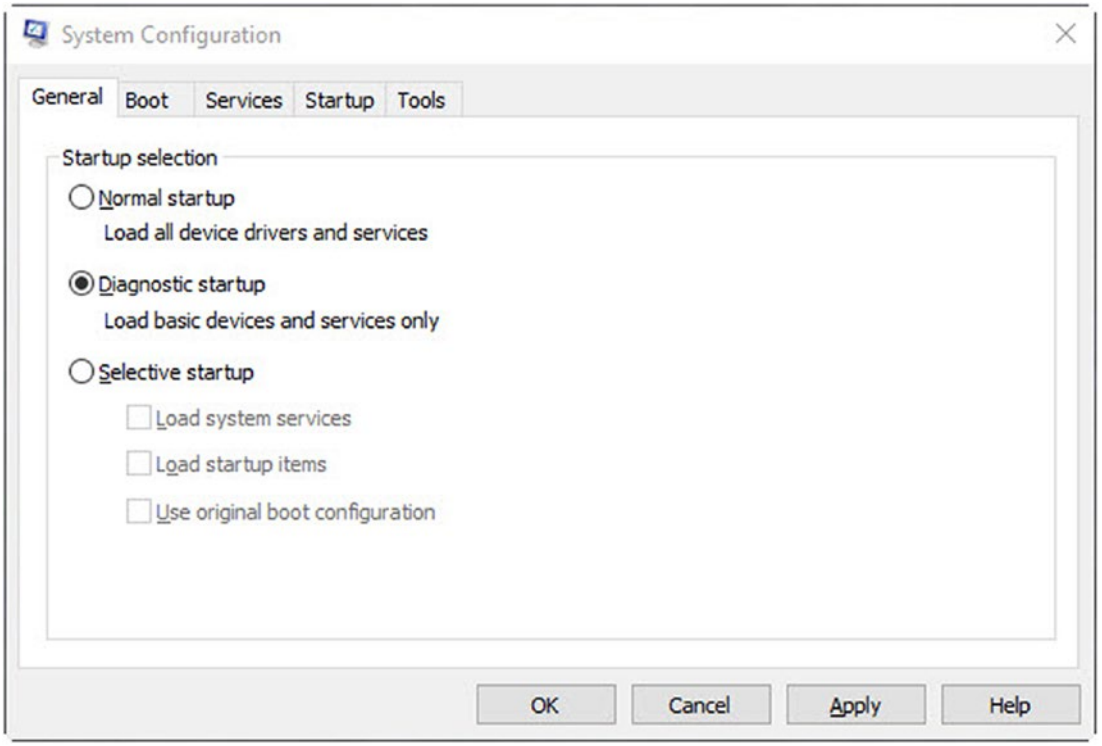


Figure 19-6. *You invoke Diagnostic Mode startup from MSConfig*

Checking Loaded Services in Safe or Diagnostic Mode

Once you have started your PC into Safe or Diagnostic Mode, you can use the MSConfig tool to check which services have been loaded, and which ones are set to load when the PC starts normally from the *Services* tab; see Figure 19-7.

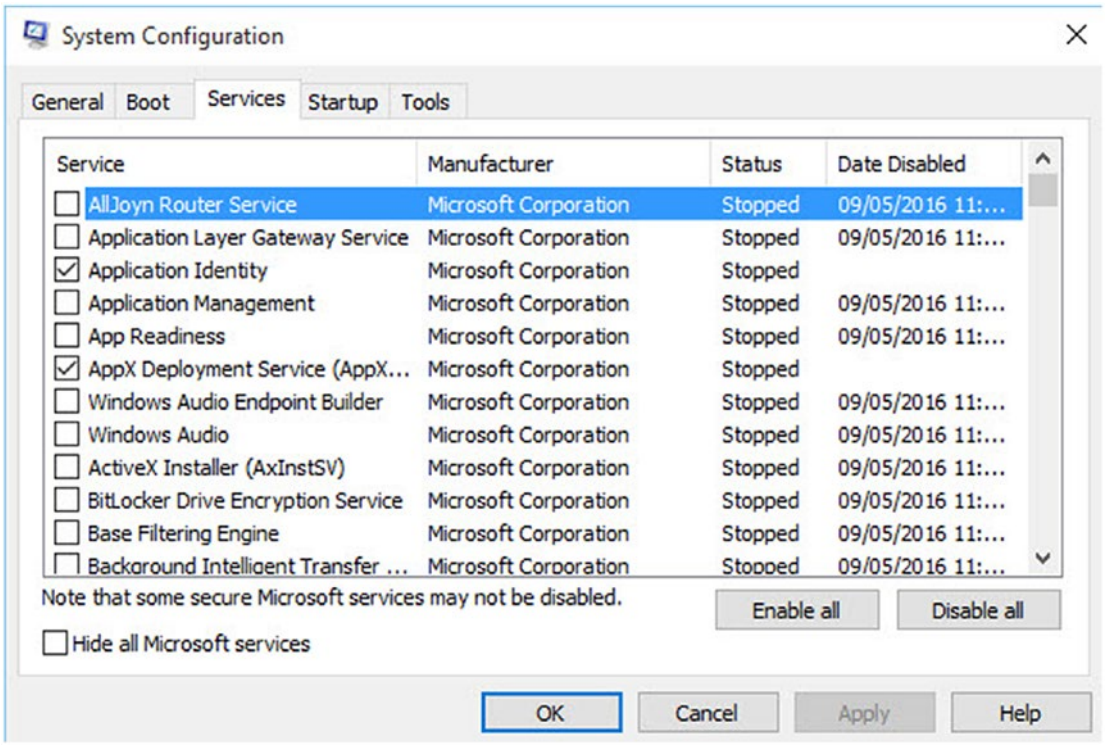


Figure 19-7. *You can manage malware services in Safe and Diagnostic Modes*

This can be much better than referring to the main Service panel, which I will detail in full in Chapter 21. In the MSConfig panel, only the services that are set to load at normal startup are included. There is also a helpful *Hide all Microsoft services* check box, which will change the view to only display third-party services. Note however it may be a Microsoft Service that has become infected.

Using the Registry Editor to Remove Malware

If you have malware on your PC, then it will certainly have embedded itself in the Windows Registry. I will show you how to use the Registry Editor in depth in Chapter 26, but it can be run by searching for **regedit** in the Start Menu. You can also run the Registry Editor from the Command Prompt when you start the PC into the Recovery Environment, or from a Recovery Drive.

All Registry manipulation should be undertaken with great care, which is why there is an entire chapter to this book devoted to the subject. I do strongly urge you to read Chapter 26 before undertaking modifications to the Windows Registry, as making the wrong change can cause the PC to be unbootable.

Caution If you can identify all the Registry entries associated with malware and delete them, including startup entries, this will still leave the malware files themselves on the hard disk, with a risk they could become reactivated accidentally.

Using a Portable OS to Manually Remove Malware

While Safe Mode and Diagnostic Modes can be useful and effective ways of removing malware, most malware embeds itself so deeply into the Windows OS that you'd never get rid of it completely if the core Windows kernel files are loaded at all. Under these circumstances, it used to be common for people to remove the hard disk from a PC, plug into a different PC, and remove the virus then while the hard disk was effectively dormant. This method should be used when you have to follow detailed instructions to remove malware manually from a PC.

Note Booting your PC from a portable OS will not allow access to any disks or partitions that are encrypted with Bitlocker.

This was fine when most PCs were big towers, or laptops with removable hard disks. Nowadays, though, with ultrabooks and tablets that have nonremovable storage, this method simply isn't possible. It can be replicated, though, by booting the PC from a portable OS. This could be a downloadable disk Image (ISO) file of a Linux distro, such as Ubuntu or Mint. You can download a Linux distro on a noninfected PC and burn it to a CD or USB Flash Drive. Starting the infected PC from this will provide file access to the hard disks on the infected machine.

Forensic Investigation and Remove of Malware

While there are ways to start Windows into a less-vulnerable environment, let's be honest, Safe Mode will only be good for getting rid of a bit of spyware. For the real malware, you're in trouble unless you know what you're doing. If you need to forensically investigate and remove a malware threat from a PC, there are six steps you need to go through and some specialist tools.

Step 1: Isolate the PC

The very first thing you should do with an infected PC is to isolate it. This will mean disconnecting it from your network and the Internet. If the PC is only connected via an Ethernet cable, then unplugging it will suffice, but if the PC connects via Wi-Fi, then just disconnecting it from the network may not be enough as the malware could reestablish the connection without you knowing.

It's essential then to delete the stored password for any Wi-Fi network the PC could conceivably connect to while it's still infected. There are two ways to do this. In the Wi-Fi connection flyout from the System Tray, you can right-click (tap and hold) on a network to display options that include telling Windows to *Forget [the network]*; see Figure 19-8.

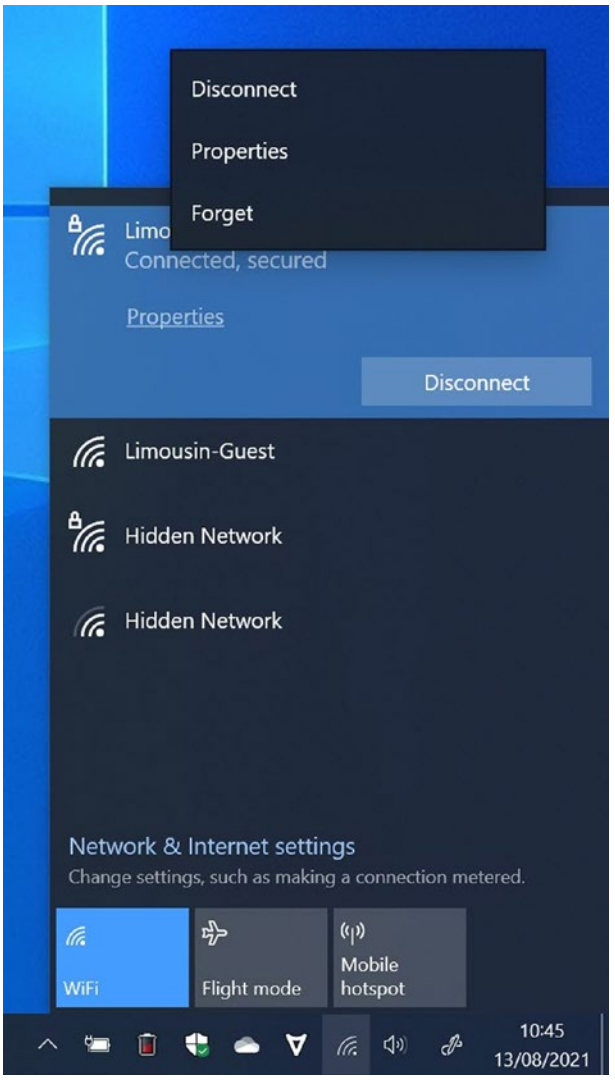


Figure 19-8. *You should delete Wi-Fi passwords on the PC*

Another method is to be found in *Settings*. Open *Network & Internet* and then *WiFi*, and you'll see a link for *Manage known networks*; see Figure 19-9.

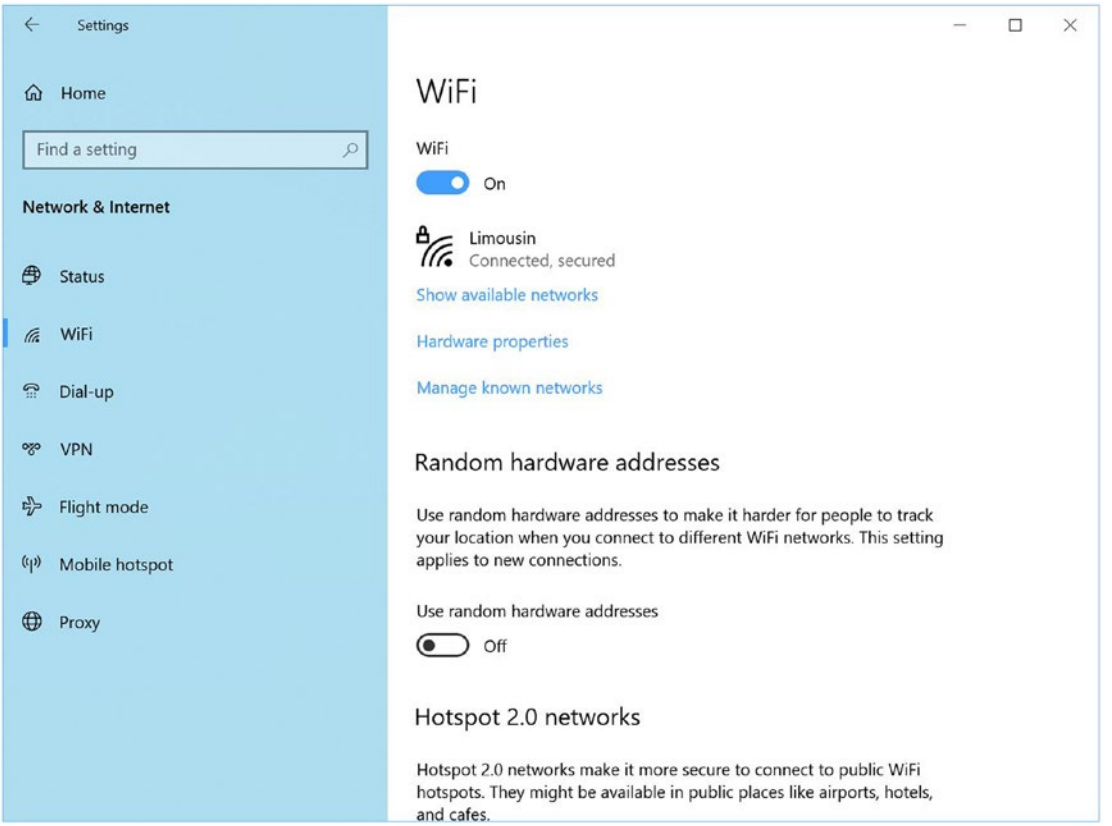


Figure 19-9. *You can delete Wi-Fi passwords in Settings*

When you click this link, a list will appear of all the networks that Windows PC is storing the passwords and access details for. You can click the ones in current proximity to the PC and select *Forget*; see Figure 19-10.

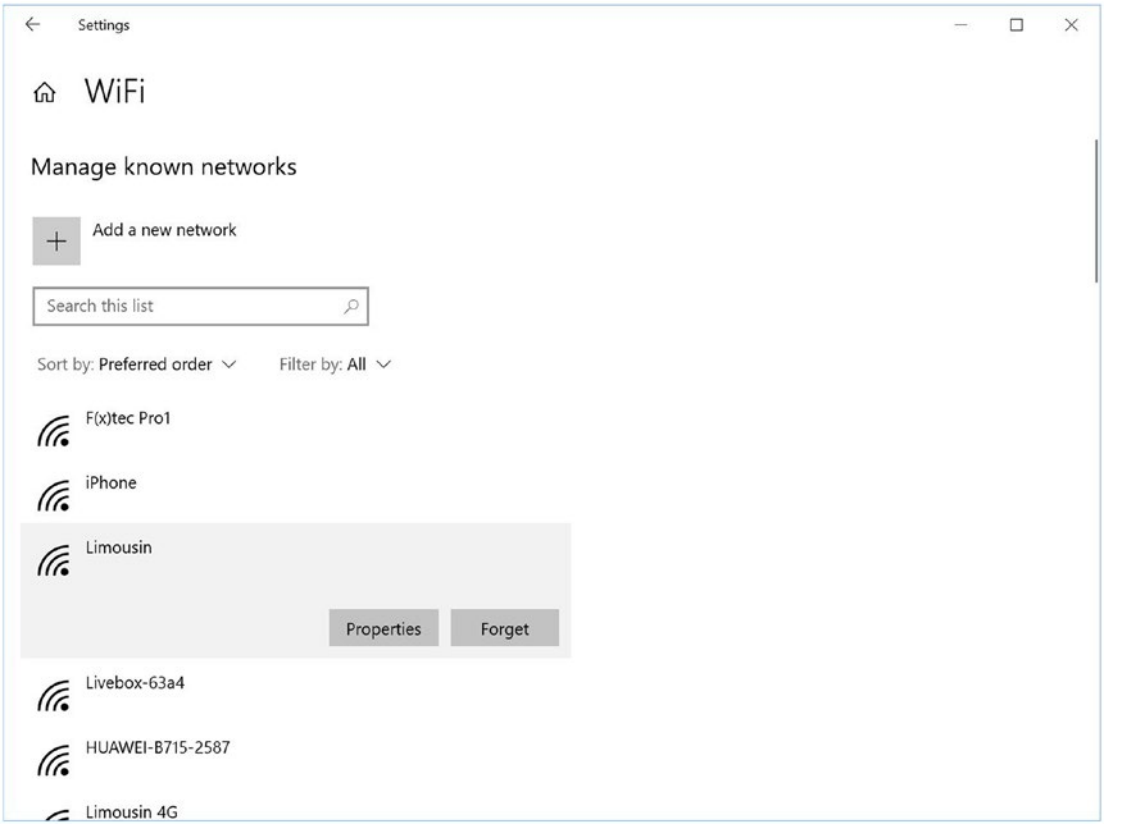


Figure 19-10. *Click the names of the local Wi-Fi networks and then click Forget*

Note If you have open Wi-Fi networks in the vicinity that do not require a password for access, you still have three options available to you. The first is to physically move the PC to a place where it can't see or access those networks. Additionally, some laptops come with a physical switch to deactivate all radio features including Wi-Fi and Bluetooth. Lastly, if you have access to the router for that network, you should be able to block the laptop from the network in the router settings until you have the matter resolved.

The reason for isolating the PC from the Internet especially is that many viruses know when they're being attacked and can automatically redownload themselves if they have a live Internet connection. This is definitely something you want to avoid.

Step 2: Identify the Malware Processes

Some but not all malware will appear as a running process in Task Manager. Sorting the wheat from the chaff here can be extremely difficult but will be simpler if you shut down everything you don't need (Safe Mode is good for this). Open Task Manager from the *Win+X* menu, and click the *Details* tab.

In Figure 19-11 we can see a list of running processes on a PC, in this case a virtual machine that I have deliberately infected with malware (at least a demonstration virus as even I'm not that daft). In this case the "malware" has been clearly labeled so we can see it as *WinlogonMalwareForm*, and you will see that it has a process name of *~DLEE4.tmp.exe*.

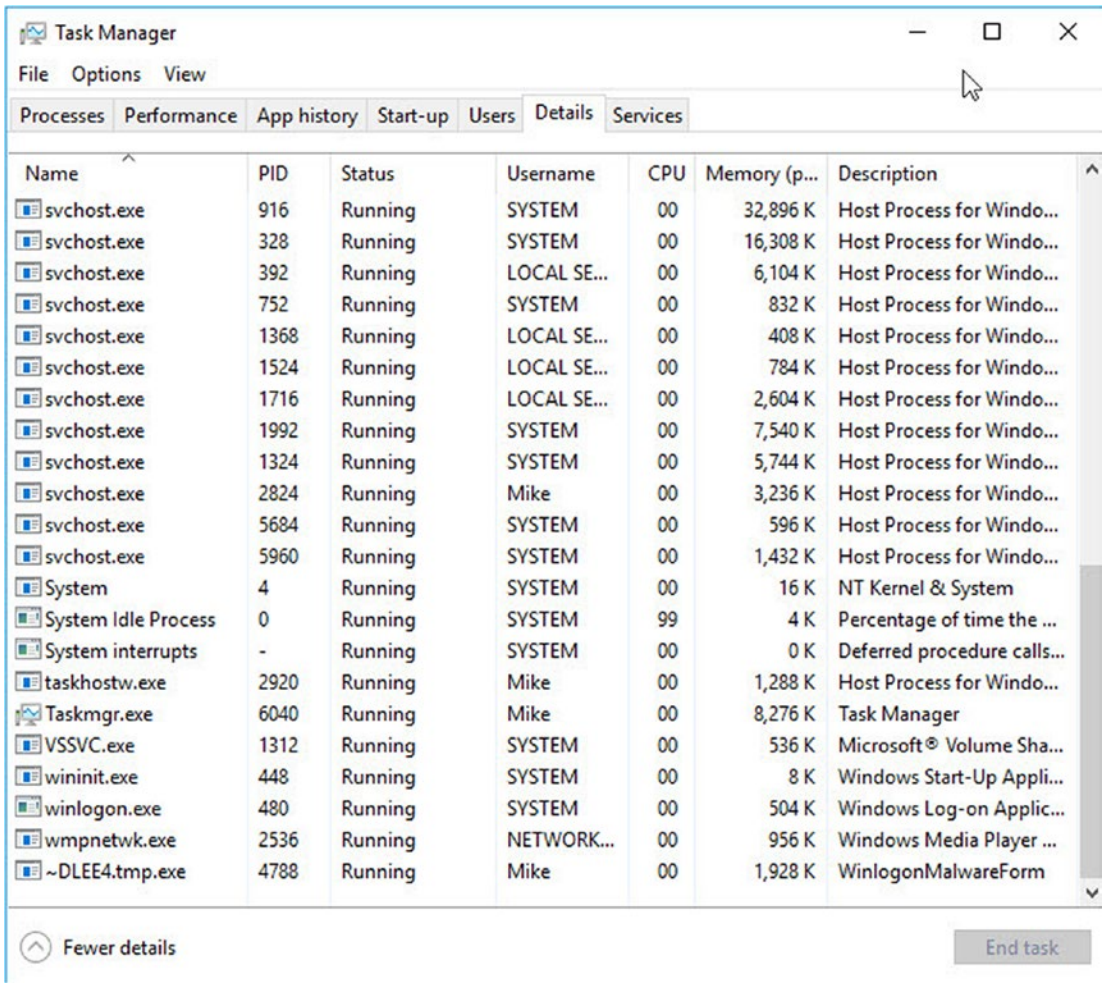


Figure 19-11. *Some malware will appear as running tasks in Task Manager*

When I say that some malware processes can be very difficult to identify, it's often because legitimate software companies can give their own processes really dumb names. On my own PC, I currently have a process running call *ijplmsvc.exe* which looks to me as just a random jumble of letters. If this happens to you, you can search for the process **on your phone or a separate PC,** and in this case it turns out to be something that I neither need nor want, so I'll be getting rid of it, for a Canon printer on my home network. It's the imaginatively named **I**nk **J**et **P**IXMA **LM** Survey Program **S**er**v**i**c**e, which is unhelpfully sending information about my printer usage to Canon without my knowledge… naughty, naughty Canon!

Regardless of my own privacy concerns at this time, the fewer processes you have running in the background, the easier it will become to spot a malware executable. There is perhaps a simpler and easier way to spot malware processes however, and this is by using the *Process Explorer* tool in the Microsoft Sysinternals Suite, which you can download from `https://pcs.tv/374QuDt`. In Figure 19-12 we can see Process Explorer running and the malware executable visible.

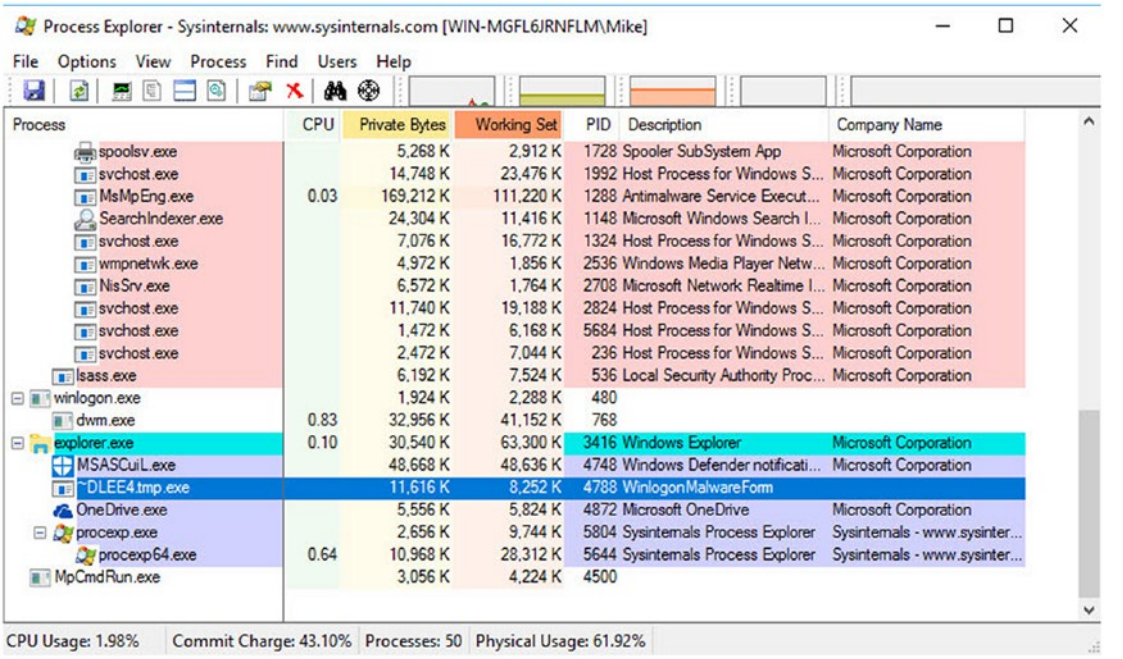


Figure 19-12. *Process Explorer is part of the Microsoft Sysinternals suite of tools*

One of the first things you will notice is that all the different running processes on the PC are color-coded. This is for a good reason and to help you to differentiate one type of process from the others:

- **Purple** processes, which in our case include the malware, are files that may be compressed (also called packed) which for legitimate applications can help them to use less memory, but in the case of malware can also help to hide the code from your antimalware scanner. Looking at the purple-colored files should be your first step.
- **Red** processes are ones that are currently existing (being stopped).
- **Green** processes have been freshly run (also known as spawned).
- **Light blue** processes are those run by the same account that started Process Explorer.
- **Dark blue** processes are ones that have currently been selected by yourself in Process Explorer.
- **Pink** processes are running Services on the PC, such as the common *svchost.exe* which is a Windows system process that can host one or more other services where they share a process to reduce overall resource usage on a PC.

Malware and SVCHOST.EXE

Some malware will try to imitate svchost.exe as you will always see a lot of these instances of this service running on a PC; see Figure 19-13. Process Explorer however will still highlight nonservice processes in purple. Look for a [+] icon to the left of an svchost.exe process in the Process Explorer processes list to see any subprocesses which could be malware.

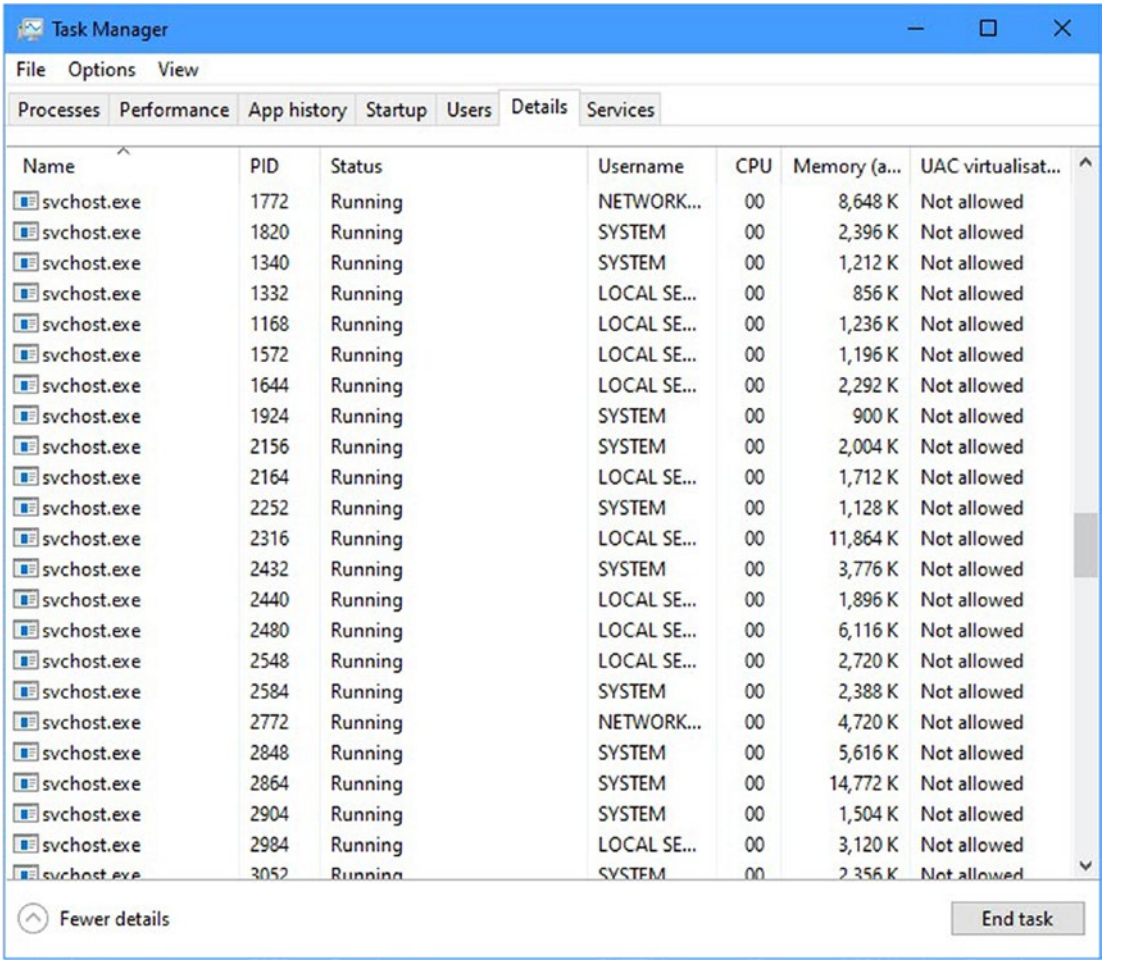


Figure 19-13. *Malware can often pretend to be an instance of svchost.exe*

Another thing you can do in Process Explorer is turn on the column to display the user account the processes are running under. Right-click the column headings and click *Select columns*. Then in the dialog that appears, click *UserName* and then click *OK*.

All genuine svchost.exe processes will be running under one of these three usernames, **NT AUTHORITY\SYSTEM**, **LOCAL SERVICE,** or **NETWORK SERVICE**. An instance of svchost running under a different username will be malware.

A third way to check if an svchost.exe process is genuine is to right-click it in Process Explorer and examine its *Properties*. In the *Command line* field, genuine Windows processes will always start with `C:\Windows\System32\svchost.exe -k`; see Figure 19-14.

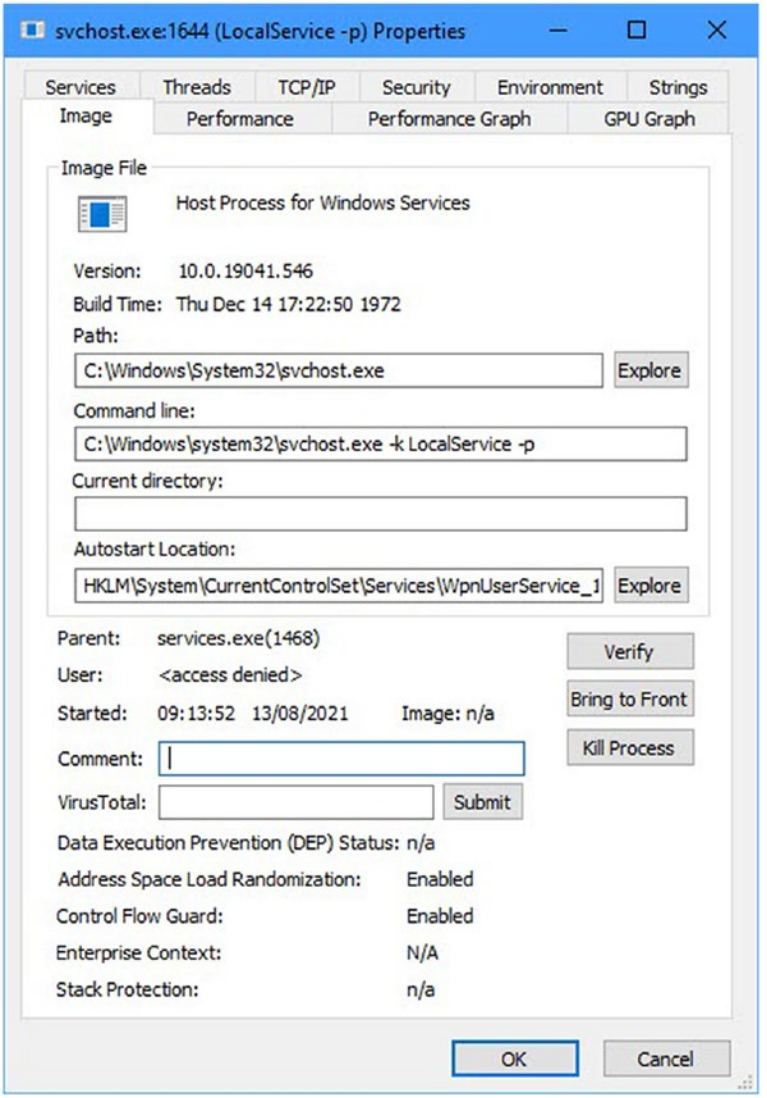


Figure 19-14. *You can check if an Svchost process is genuine by its Command line parameter*

Step 3: Deactivate the Malware

We are now ready to try and deactivate the malware. If we right-click it and examine its *Properties*, we will see that this particular piece of malware is being run from the *C:\Windows\Temp* folder; see Figure 19-15. You will need to make a note of both the *Path* and *Autostart Location* parameters.

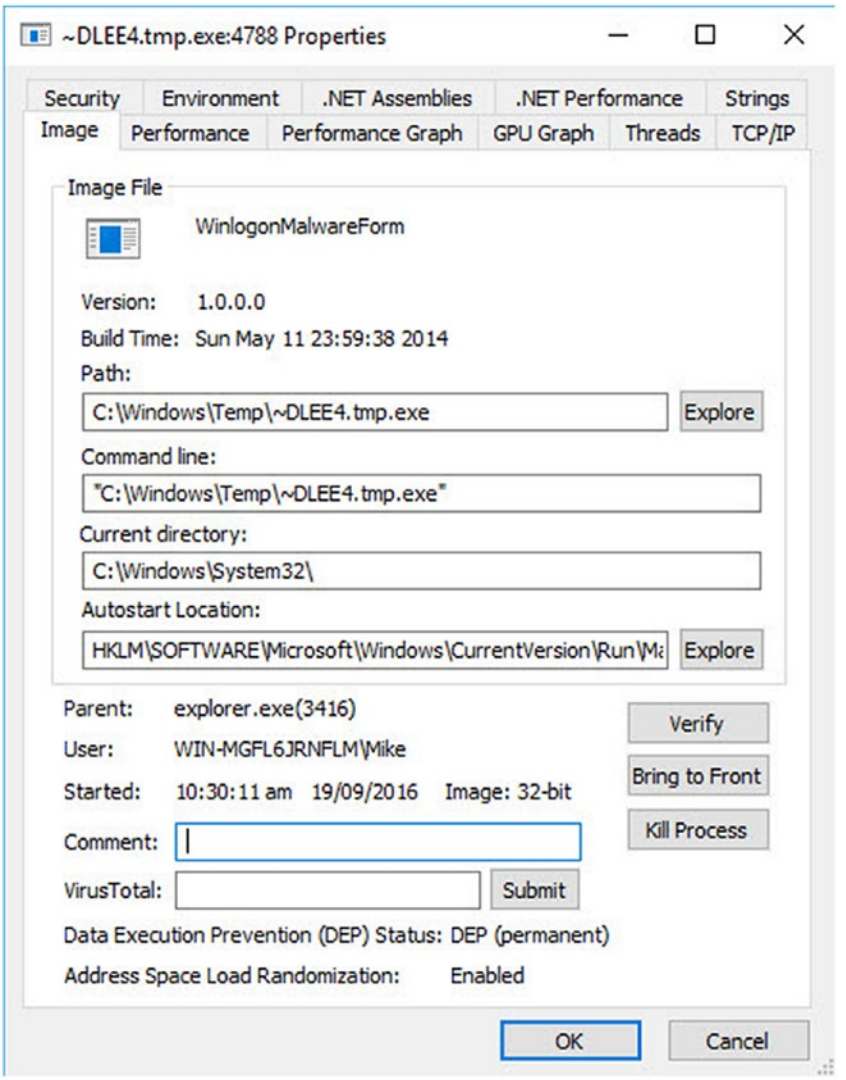


Figure 19-15. *Check the Path and Autostart parameters to find the malware file*

Open the Registry Editor by clicking the *Explore* button next to the *Autostart location* field, and you will be taken directly to that key in the Windows Registry; you should *Delete* this key from the Registry; see Figure 19-16.

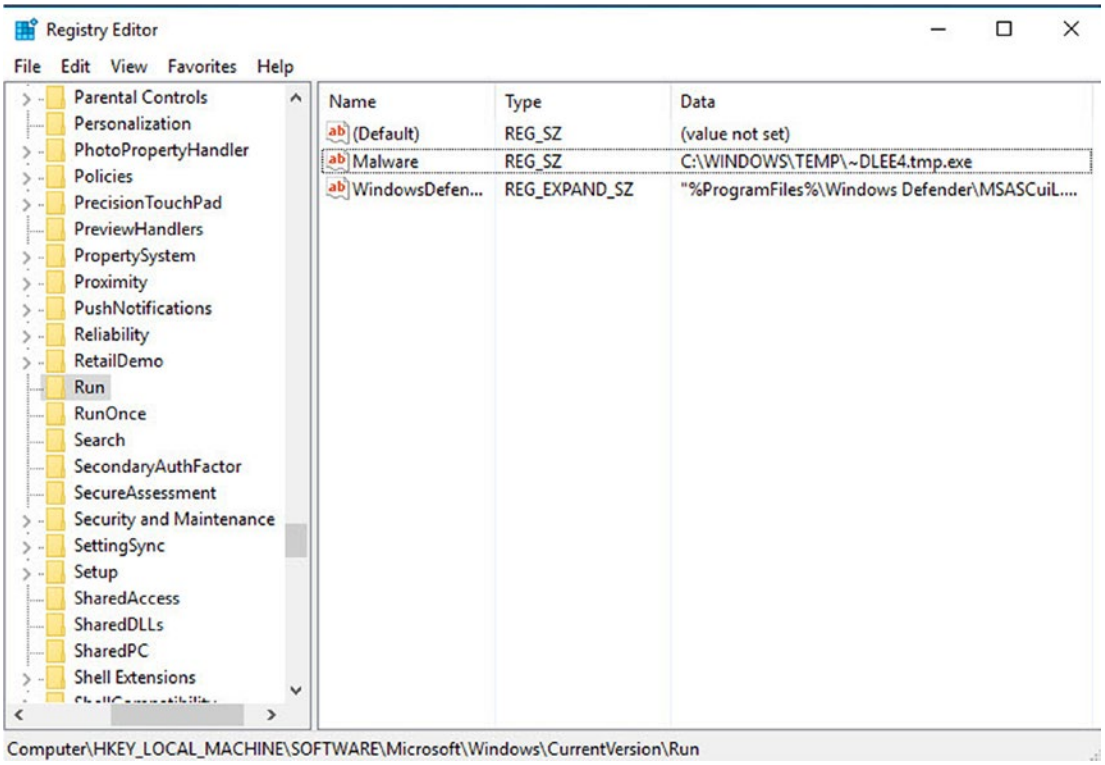


Figure 19-16. *You need to delete the Startup Registry key for the malware*

Now we return to Process Explorer and shut down the malware process. Most malware processes though will have a secondary process checking to see if it is being shut down, as a defense mechanism. Instead of killing the process then, you can *right-click* the process name and *Suspend* it; see Figure 19-17. This will prevent other malware processes from seeing you are killing the infection.

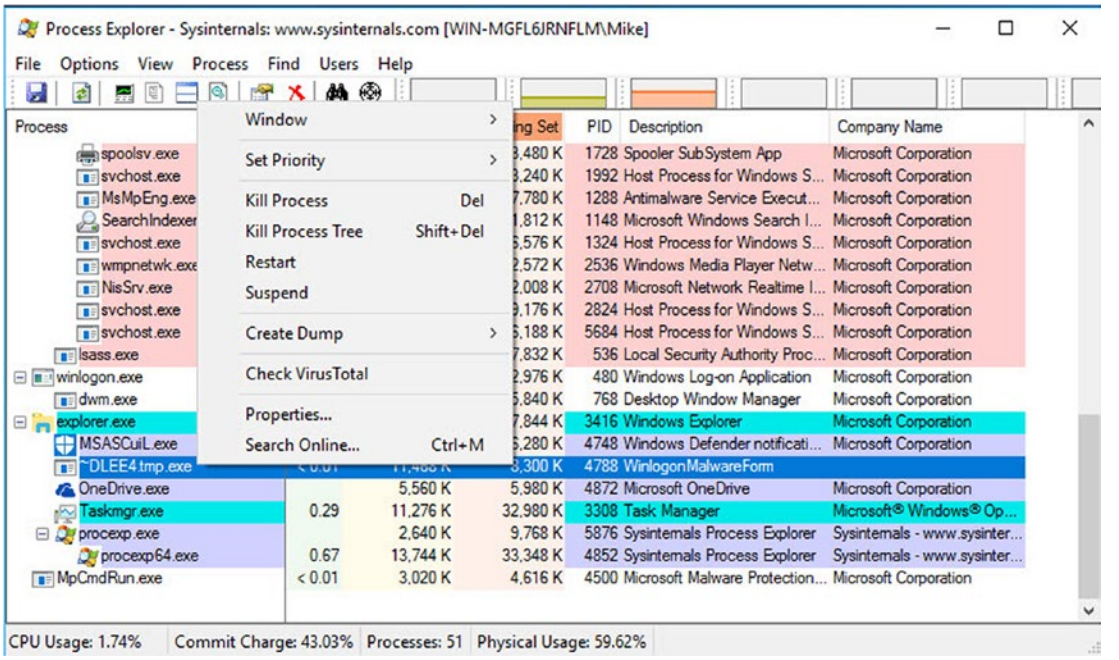


Figure 19-17. *You need to suspend malware processes, not kill them*

Step 4: Test the Results

With the malware possibly disabled, you should restart the PC and then run *Process Explorer* again as an Administrator to see if the malware process is still running. In this case we need to use another Sysinternals tool called *Autoruns* to see if the malware is still running. Under the *logon* tab, see if the malware process is listed. If it is, uncheck it here to disable it; see Figure 19-18.

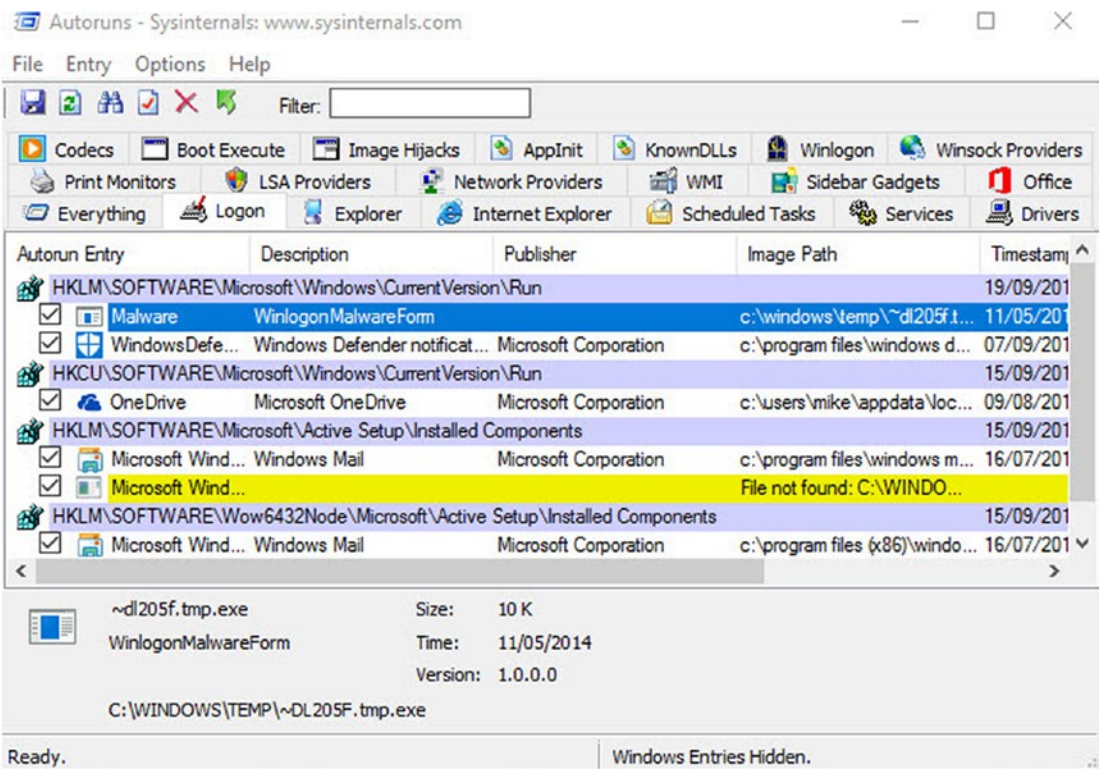


Figure 19-18. *You can use the Autoruns tool to see if the malware is still running*

This malware has automatically recreated itself at sign-on, which means there must be something else happening on the PC, so we need to go hunting again. This means that, still in Autoruns, we need to look tab-to-tab for any processes that are not digitally signed; these will be highlighted in *pink*.

When we look under the *Winlogon* tab, we can see a *SampleCredentialProvider* dll that is highlighted because it's not digitally signed; see Figure 19-19. It might look legitimate, being stored in the `C:\Windows\System32` folder having a perfectly normal-sounding name *winlogondll.dll*, but this will be our malware process. We should disable this for now (just in case we're wrong) as we can always reenable it later if we need to. Make a note of the Registry key through the DLL name and folder location.

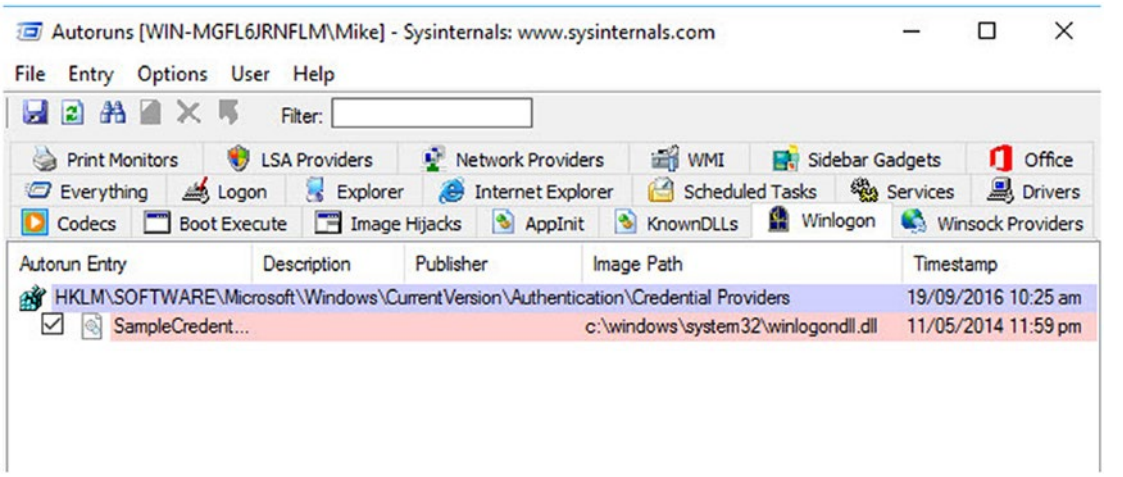


Figure 19-19. *Nondigitally signed processes show in Autoruns in pink*

Step 5: Retest the PC

Now we need to restart the PC again and check once more in Process Explorer for our malware. We can see in Figure 19-20 that we have successfully deactivated it and it is no longer running on the PC.

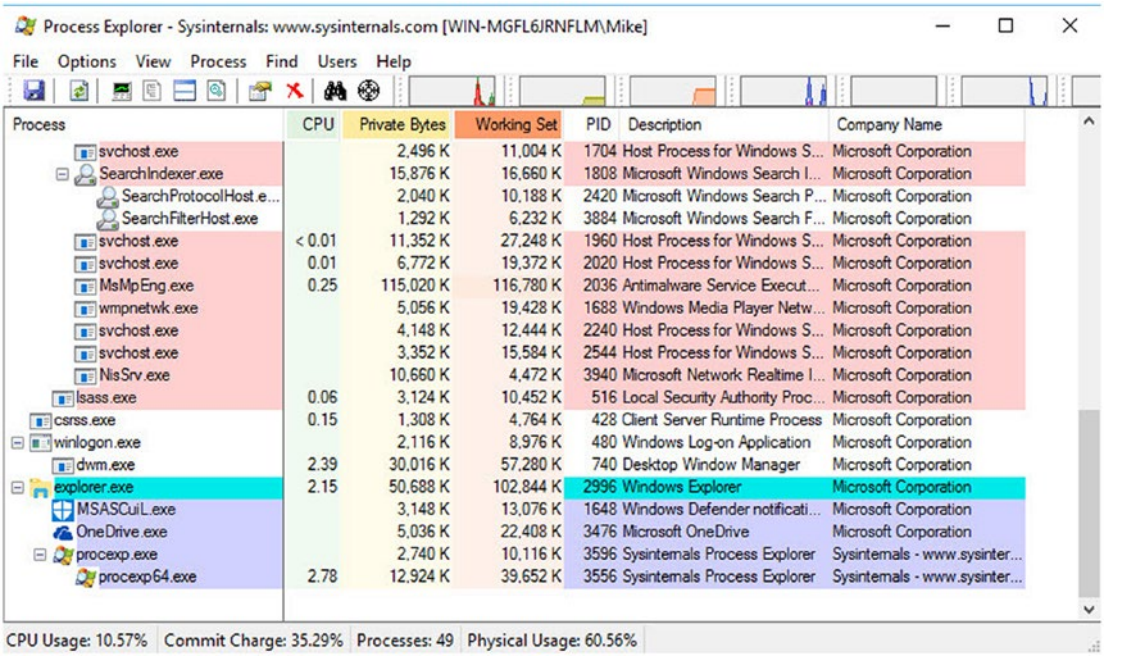


Figure 19-20. *We can see that the malware is no longer running on the PC*

Step 6: Clean Up the Malware

The final step in the process is to remove all of the malware files and Registry keys that we found. We know that the malware file was in the `C:\Windows\Temp` folder and called **~DLEE4.tmp.exe**, that the malware DLL file was in `C:\Windows\System32` and was called **winlogondll.dll**, and that there were a couple of Registry keys associated with the malware too. In Figure 19-21 we can see the Startup Registry key that autoruns highlighted for us, and also the malware files itself.

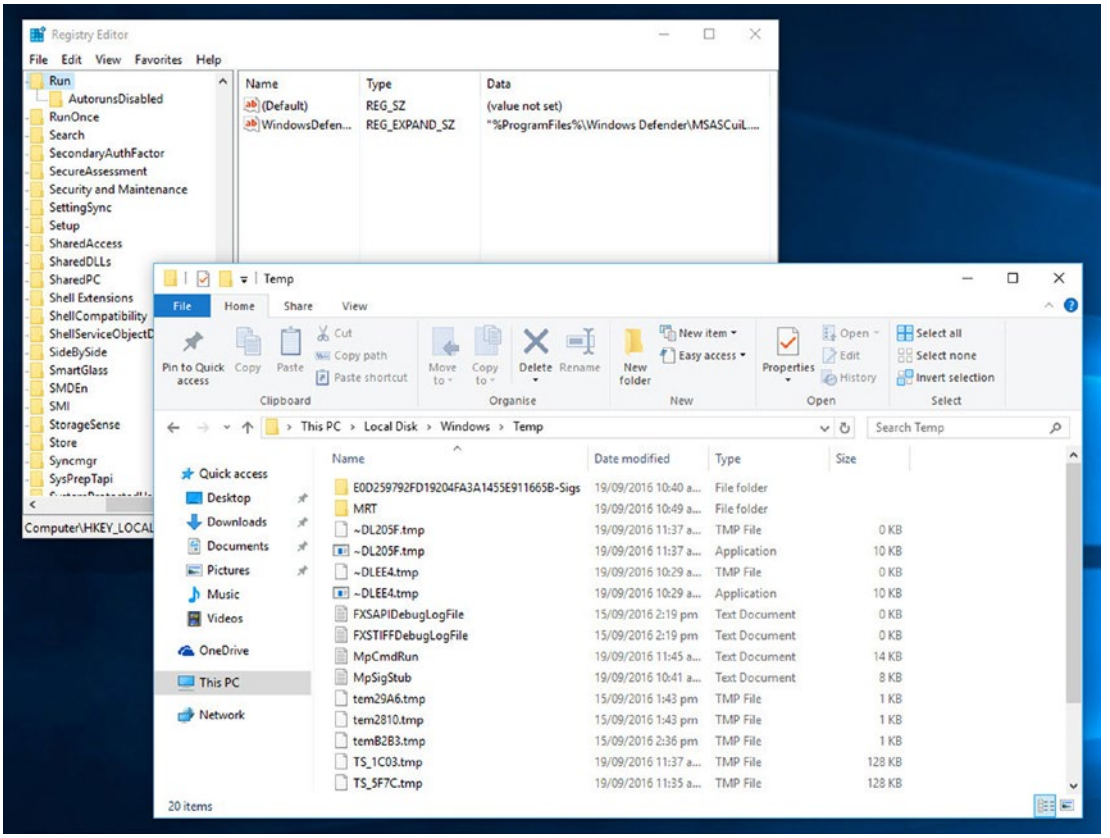


Figure 19-21. *The final step is to delete all trace of the malware*

The process of removing actual malware from a PC is likely to be more involved than in this demonstration, as there will very likely be multiple processes running on the PC. It will therefore take some time, and you probably be prepared to clear your diary for the day when you set out to remove the infection, as it will require your full concentration.

Rootkit Removal

Removing a rootkit from a PC can be much more complicated as these things embed themselves in the boot partitions of the PC. There are always things you can do however for which you will need a portable OS, which can best be obtained by downloading a Linux distro that can be run from a DVD or USB Flash Drive. In this example I'm using **www.ubuntu.com**, but you could also use **www.linuxmint.com** or **www.redhat.com**, and these are provided to enable people to evaluate a version of Linux without having to install it first.

Start the PC from the removable media, and run the *GParted* tool so you can see and access the hidden boot and system partitions on the host PC. In Figure 19-22 you will see a clean *System Reserved* partition which is what would be seen on a PC with an older BIOS firmware, or an EFI firmware PC set to BIOS compatibility mode. Please make sure you put things back as they were when you've finished.

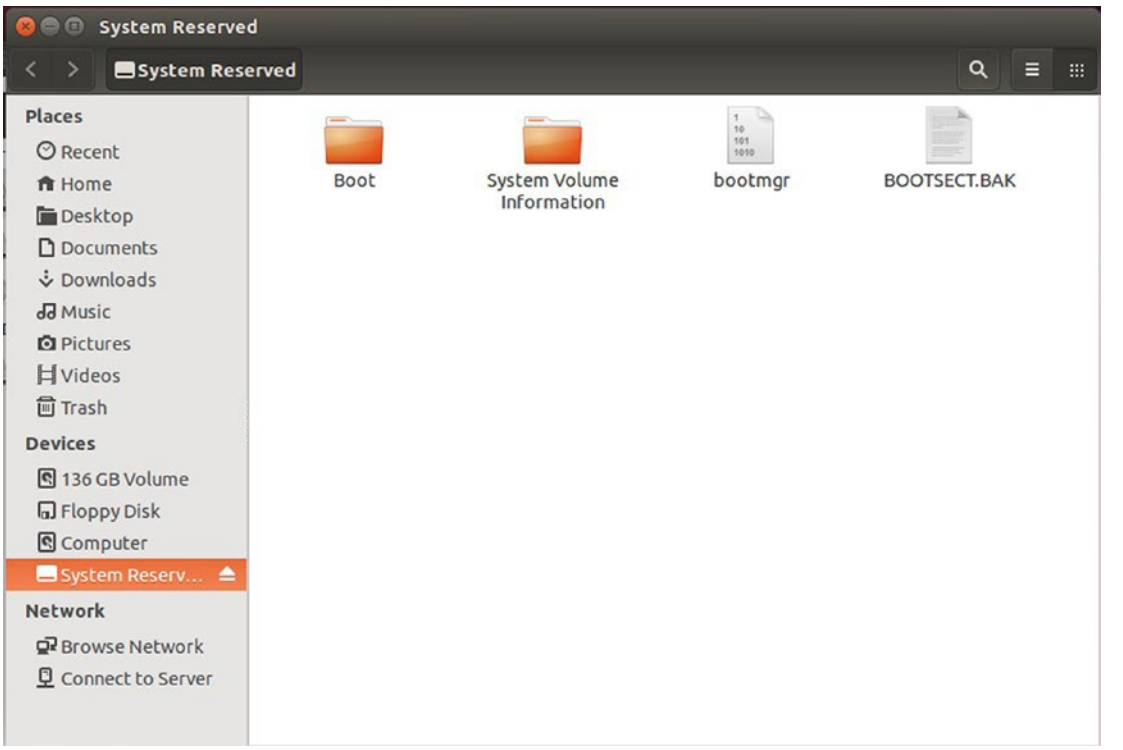


Figure 19-22. *You can remove rootkits using a portable OS*

Figure 19-23 on the other hand shows the contents of a clean UFEI *Boot* partition, which is more complex and includes more tools and security features.

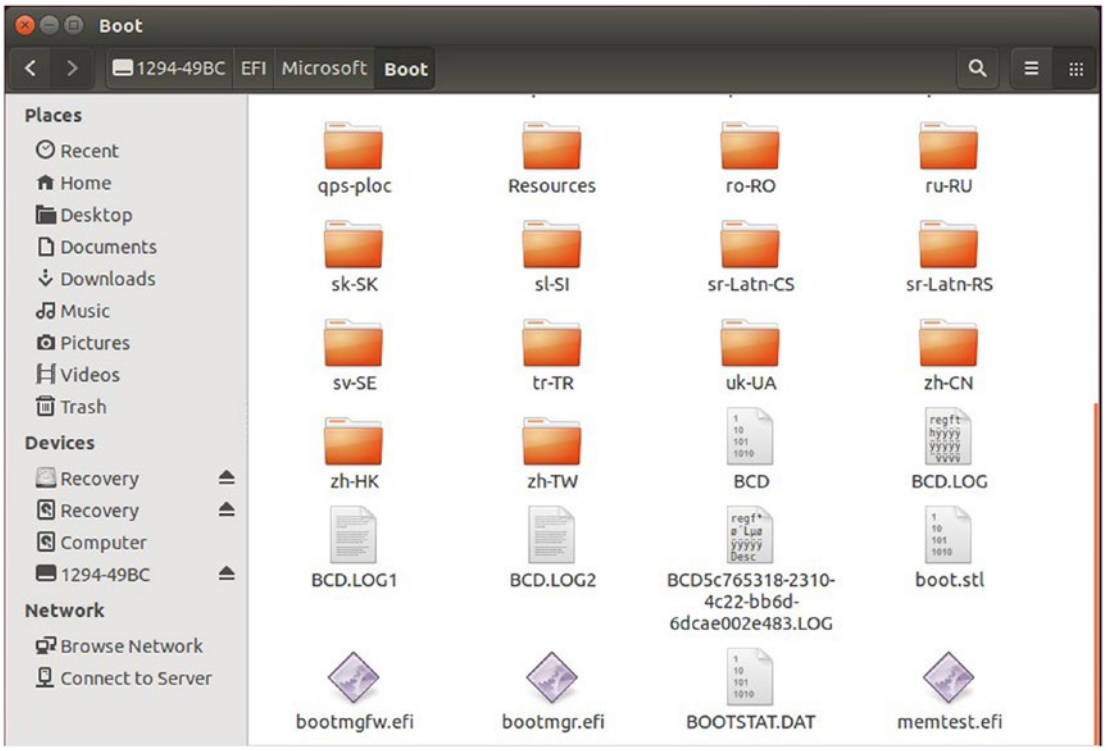


Figure 19-23. *A UEFI Boot partition contains more files than a BIOS partition*

You will need to find the name of the rootkit virus through research and then look online for detailed instructions on how to remove it safely, as they are all different. Deleting the wrong file in the boot system can make your PC completely unable to start.

Using BCEEdit

If you have had a rootkit infection, it is prudent to check the Windows BCD (Boot Configuration Database) files after removing the malware to get rid of the code that loaded the virus when Windows started. You can do this from the desktop by opening a Command Prompt window as an administrator and typing **BCDEdit**; see Figure 19-24.

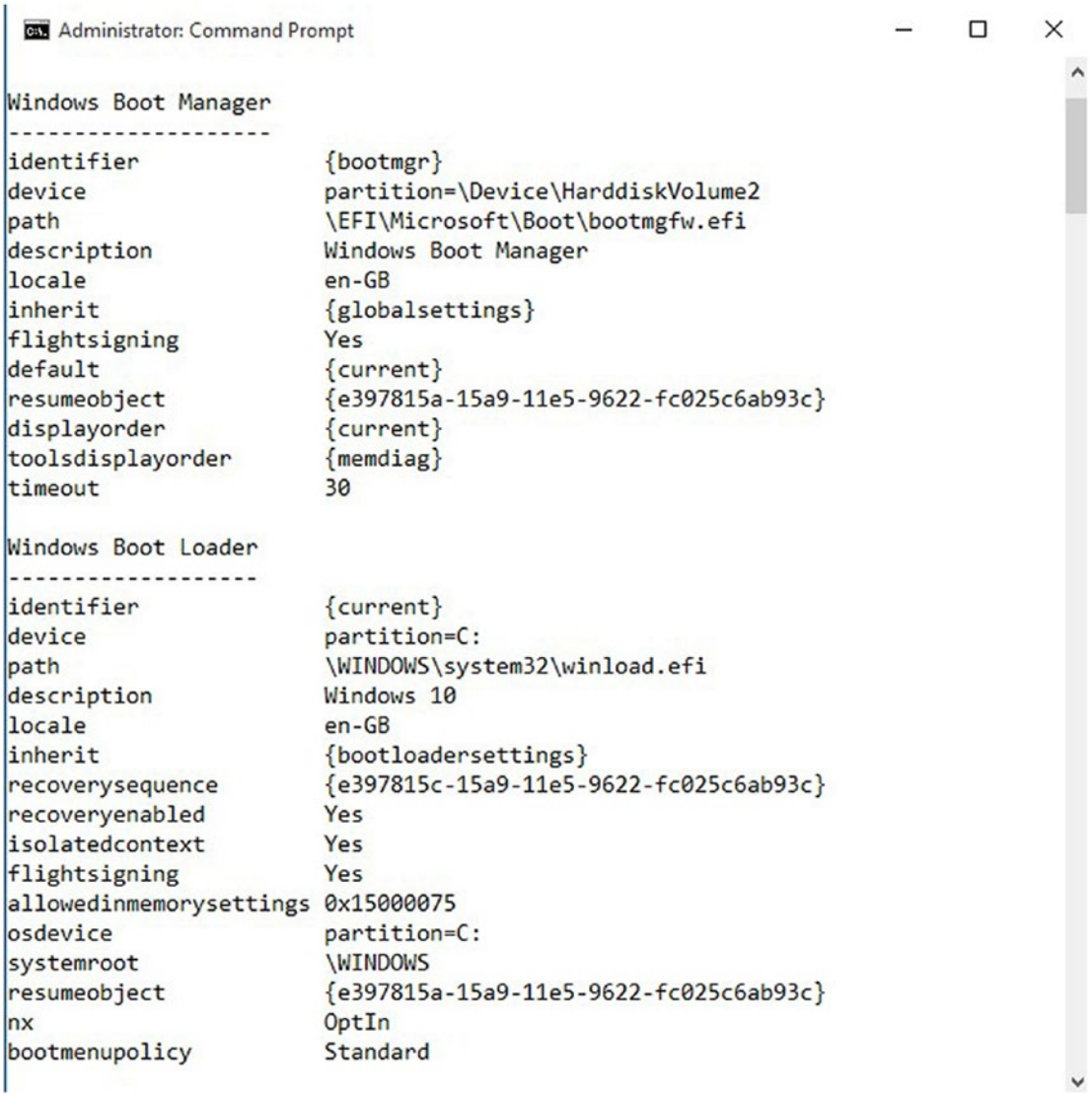


Figure 19-24. *BCDEdit is the command used to manage the Boot Configuration Database*

Check through the database to see if there are any referenced to the rootkit malware. If you find any, you can use the command **BCDEdit /Delete {identifier} /Cleanup**. Additionally, you may find this rootkit has replaced your existing Windows bootloader; if this has happened, type the command **BCDEdit /Default {identifier}** to set the correct bootloader for the PC.

Using Third-Party Tools to Remove Malware

By far the best and most recommended way to remove malware from a PC, when your installed antivirus software can't do the job on its own, is to use a third-party tool. There are plenty to choose from, and here I'll detail some of the very best and why you can trust them to do the job.

It's important to note that these tools need to be up to date, so you should always download (from a noninfected PC) the most current and up-to-date version of the tool before using it. This is because the malware your PC is infected with might be new, and the removal utility will only be built into the latest versions of these tools.

Microsoft DaRT

If you are in a business using the Enterprise edition of Windows 10, you will have access to Microsoft's Diagnostics and Recovery Toolset (DaRT). This allows you to create recovery media for a PC that includes the following tools:

- **Computer Management console** is the same as on the host Windows 10 PC and allows you to view that PC's event logs, scheduled tasks, local users and user groups, device drivers, autorunning applications, and both Microsoft and third-party services.
- **Crash Analyzer** helps you determine the cause of crashed on the host PC, by examining the contents of the crash memory dump file(s) and having them interpreted for you.
- **Defender** is an offline version of the Windows antivirus package. This can be used to scan a PC for malware and remove it safely without the malware becoming active.
- **Disk Commander** provides tools to help you repair and recover corrupt disks and partitions.
- **Disk Wipe** can be used to delete all data from a hard disk, when you need to wipe a disk completely to eradicate a virus infection, before a reimage.

- **Explorer** is a full version of File Explorer that lets you examine and manipulate the files on the host PC. This can be used when you need to manually remove files as part of malware removal.
- **File Restore** is a file "undeletion" tool to help you recover files that were deleted accidentally, or that were too large for the PC's Recycle Bin.
- **File Search** is a general-purpose search tool for locating specific files or file types on the host PC.
- **Hotfix Uninstall** can be used to remove Windows Updates that can be causing the PC to become unstable.
- **Locksmith** lets you change and manage user account passwords for any account on the PC. This can be used if malware has locked you out of your own, or the Administrator account.
- **Registry Editor** allows you to access the Registry on the host PC and manually remove any keys placed there by malware.
- **SFC Scan**, the System File Repair Wizard, checks all the Windows OS files on the host PC to determine if any have been changed or have become corrupt. It can then be used with up-to-date installation media to replace any modified or damaged files with the proper ones.
- **Solution Wizard** is a tool that can be used if you are not sure which of the DaRT tools is best to fix your specific problem. It asks a series of questions and will suggest the best way to fix your problem.
- **TCP/IP Config** can be used to manipulate the network settings on the host PC, so that you can access local network resources or the Internet to apply fixes.

ESET Online (and Offline) Scanner

Several companies, including some of those listed in this section, provide online scanners that can scan your PC for viruses through your web browser. ESET provides a scanner that can also be downloaded to use on your PC as well. This can be useful if you suspect your current antivirus software has missed a virus:

`http://www.eset.com/us/online-scanner/`

Norton Bootable Recovery Tool

Many of the following tools all fall into broadly the same category as Windows Defender Offline. Norton is the same in that it allows you to create a bootable DVD or USB Flash Drive that can be used to scan for and remove malware:

`https://norton.com/nbrt`

Sophos Bootable Antivirus

By this point, you might have guessed that the choice of which tool you download and use depends on your personal preference for antivirus vendor. It also needs to work, and not all of these tools will be up to date with the very newest viruses, however. The Sophos tool can only be used to create a bootable CD or DVD, and so it is less suitable for ultrabooks and tablets:

`https://www.sophos.com/en-us/support/knowledgebase/52011.aspx`

Kaspersky Rescue Disk

Kaspersky Rescue Disk is designed to create a bootable CD or DVD from which to remove malware, though instructions do exist on the website for how you can create a bootable USB Flash Drive:

`https://support.kaspersky.com/viruses/rescuedisk`

Kaspersky Ransomware Decryptor

A suite of free utilities that, while they can't defend against ransomware, will help you remove ransomware from an already infected PC, and decrypt any files the ransomware has encrypted. You can download it at

`https://noransom.kaspersky.com.`

AVG Rootkit Scanner and Remover

The AVG Rootkit Remover is a tool that you download to an infected PC to scan for malware. If an infection is found, the tool will ask you to restart the PC so that removal and cleanup can take place:

`https://www.avg.com/en/signal/rootkit-scanner-tool`

F-Secure Online Scanner

It can be used to scan for and remove malware on your PC from a direct download, without having to install a package that could become infected with malware:

`https://www.f-secure.com/en/home/free-tools/online-scanner`

McAfee Free Tools

Security firm McAfee provides a selection of free security tools, which include the following tools:

- **GetSusp** will scan for undetected malware on a PC and can be used if you suspect you may have undetected malware on a PC: `https://www.mcafee.com/enterprise/en-us/downloads/free-tools/getsusp.html`
- **RootkitRemover** is a stand-alone utility for detecting and removing complex rootkit attacks: `https://pcs.tv/3CE2ewy`
- **Stinger** is used to remove a specific list of supported viruses and is updated regularly with the latest and most common virus definitions: `https://www.mcafee.com/enterprise/en-gb/downloads/free-tools/stinger.html`

D7II

If money is no object, then subscribing to an annual license for D7II can pay dividends. It's a complex suite to use and should not be used unless you're proficient in maintaining and configuring PCs, but it includes a powerful antimalware suite that includes tools from Kaspersky, Bitdefender, Sophos, McAfee, and more on the unfortunately named domain *foolishit* (funny; Ed):

`https://www.foolishit.com/d7ii/`

RKill

RKill can be used to terminate the running processes that malware is using to keep itself active on a PC. This can be useful if your standard antivirus software is unable to clean the infection. Run RKill first to stop the offending processes, and then use your existing antivirus software to clean the infection as per normal:

`http://www.bleepingcomputer.com/download/rkill/`

Junkware/Adware Removal Tools

Sometimes you can have software on your PC called junkware or adware. This isn't actually a virus, but it can be really annoying and slow down your PC. Several companies provide free software for removing junkware including

- Malwarebytes **Adware Cleaner**, `https://www.malwarebytes.com/adwcleaner`
- Adlice **RogueKiller**, `http://www.adlice.com/software/roguekiller/`
- Xplode **AdwCleaner**, available by searching online

Microsoft Sysinternals Suite

Several packages in Microsoft's excellent Sysinternals suite can be used to detect and remove malware from a PC, including AutoRuns, Process Explorer, and Rootkit Revealer. I will detail these and other Sysinternals tools in full in Chapter 22.

Researching Virus Removal Online

Earlier in this chapter, I wrote about how you can use Windows utilities such as the Safe and Diagnostic Modes, or a portable OS, to manually remove viruses and other malware from a PC. This will be necessary if the tools I've detailed in the preceding section can't remove malware from your system. You need to be very careful when removing viruses manually, as you will need to access both the Windows Registry and the Services panel and disabling or changing the wrong thing can cause your PC to become unstable or unresponsive.

How do you go about finding the information you need to remove a virus manually in the first place, though? This can be tricky as the Internet is a vast resource full of people who think they're experts in everything, but who most certainly are not. When researching a virus, it'll be because one of two things has happened. Either your antivirus software has identified a virus, and given you its name, but can't remove it, or it could be because you know someone else who has recently had a virus called "X" which now also appears to be on your PC as well. Suffice to say, it'll always be because you already know what the malware is called.

Generally speaking, stick to the list of vendors I've listed here, companies such as Microsoft, Symantec, Sophos, McAfee, Bitdefender, and the like. They will often post manual removal instructions for malware should it be necessary, perhaps because they've not been able to update their own tools yet. DO NOT trust any other source unless you can be absolutely certain of its credibility.

When it comes to your local PC repair shop (be they a sole trader or a national company), in all the years I've worked in IT, I have almost NEVER heard of any of these types of vendors removing malware correctly. The normal response is to wipe the PC, probably losing some of your files in the process, and maybe even charging you for a new Windows license for the reinstall. Find a techie friend or colleague if you're not certain, and use the tools I've listed in this chapter.

Summary

Virus and malware infection is a problem, a big one. Knowing what tools are available to help you remove malware is the most important step, however, and how you can manually remove any remaining files associated with the malware is a very useful skill to acquire. Armed with the information in this chapter (some of which will inevitably change over time, as some packages are changed), you can be a great IT support person.

One useful way to reduce the risks involved with malware infection is to always run your PC in a virtualized environment. In the next chapter, we'll look at exactly this: how you can use the Virtualization client that comes in the Pro and Enterprise editions of Windows 10 to run virtual machines that you can both access from your desktop and start your PC from.

CHAPTER 20

Using Virtualization to Protect PCs

Much of the work involved in troubleshooting and repairing PCs comes in the form of either finding quick solutions to problems or finding ways to mitigate problems entirely. Virtualization, which is the process of running an operating system and apps inside a software container, actually provides ways to achieve both of these aims, and in Windows 10, it also offers some compelling ways for IT departments to be able to quickly adapt to changing workflows.

Windows 10 actually comes with two virtualization clients, the best known is Hyper-V, and this comes preinstalled in the Pro and Enterprise editions of Windows 10. You might find that it's hidden from view and unobtainable from the Start Menu, however, in which case you'll need to enable it. To do this, open the *Win + X* administration menu, and click *Programs and Features*. Next, in the window that appears, click the *Turn Windows features on or off* link.

This will display an options dialog in which you may see that the check box next to Hyper-V is unchecked; see Figure 20-1. Check the box to enable the Hyper-V Virtualization client.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_20

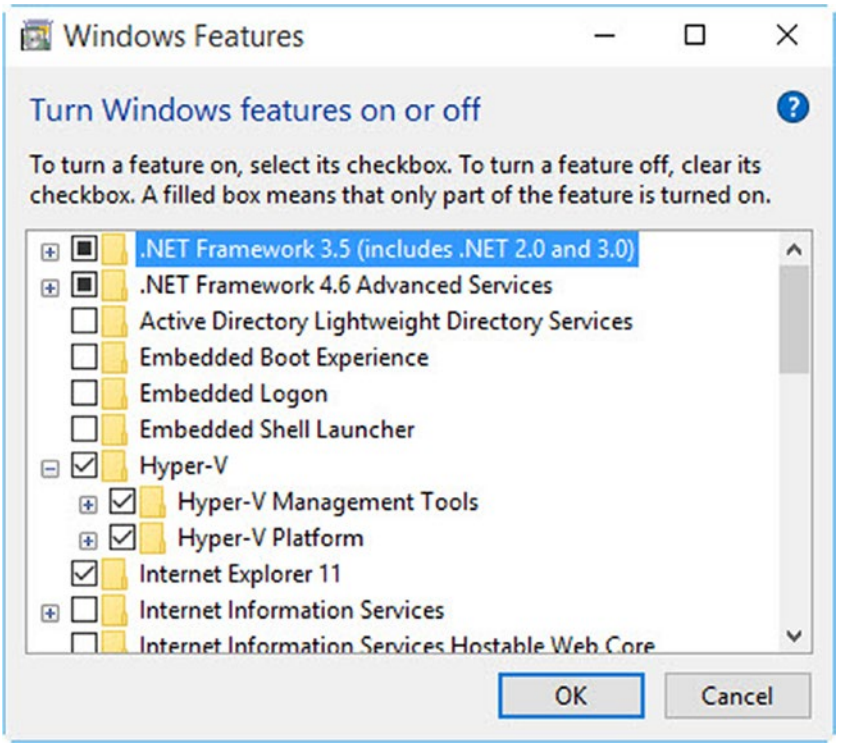


Figure 20-1. *You might need to enable Hyper-V in Windows 10*

If you are using a newer AMD processor on your PC, then you might not be able to install and use the Hyper-V Platform. This is because a feature required to support virtualization, called Secure Virtual Machine (SVM), is often disabled in the UEFI firmware for newer AMD Ryzen processors. It's simple and straightforward though to enable it; in your UEFI settings, check in the CPU options for *SVM Mode* and enable this; see Figure 20-2. After restarting the PC, you will be able to install the full features of Hyper-V.

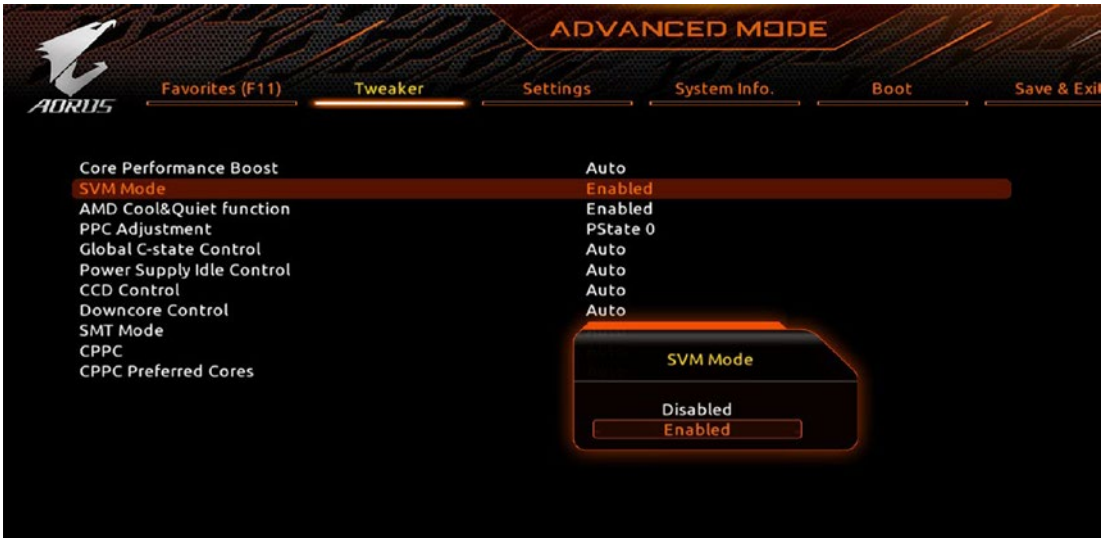


Figure 20-2. *You might need to enable SVM on some AMD motherboards for Hyper-V to function*

So what is it that Hyper-V can do for me, I hear you ask. Virtualization has many different uses. App developers, for example, might have several Virtual Machines (VMs) open on their desktop, each running a different version of the Windows OS, so they can test their app in all the different OS versions, without needing multiple PCs. System administrators might use a VM of the standard company Windows installation, in which they can test new updates, patches, and apps for stability and security.

When it comes to troubleshooting, however, there are several uses for VMs. These include being able to create a quick restore system, in which a PC can boot into a VM, or having a system where, using VMs, a PC can quickly be repurposed for different tasks. Perhaps most useful, however, is that virtualization can be used to completely sandbox older operating system versions, such as Windows XP, which are completely out of support, but that might still be required for mission-critical tasks in the workplace.

Creating and Managing VMs in Hyper-V

VMs in Windows 10 are created, added, and managed in the Hyper-V Manager; search for this in the Start Menu. This is a standard Microsoft Management Console fare, with a panel on the left where the master systems (in this case, your PC) are listed, a panel on the right containing context-sensitive menu options, and a central panel with information about any VMs that have been created or imported; see Figure 20-3.

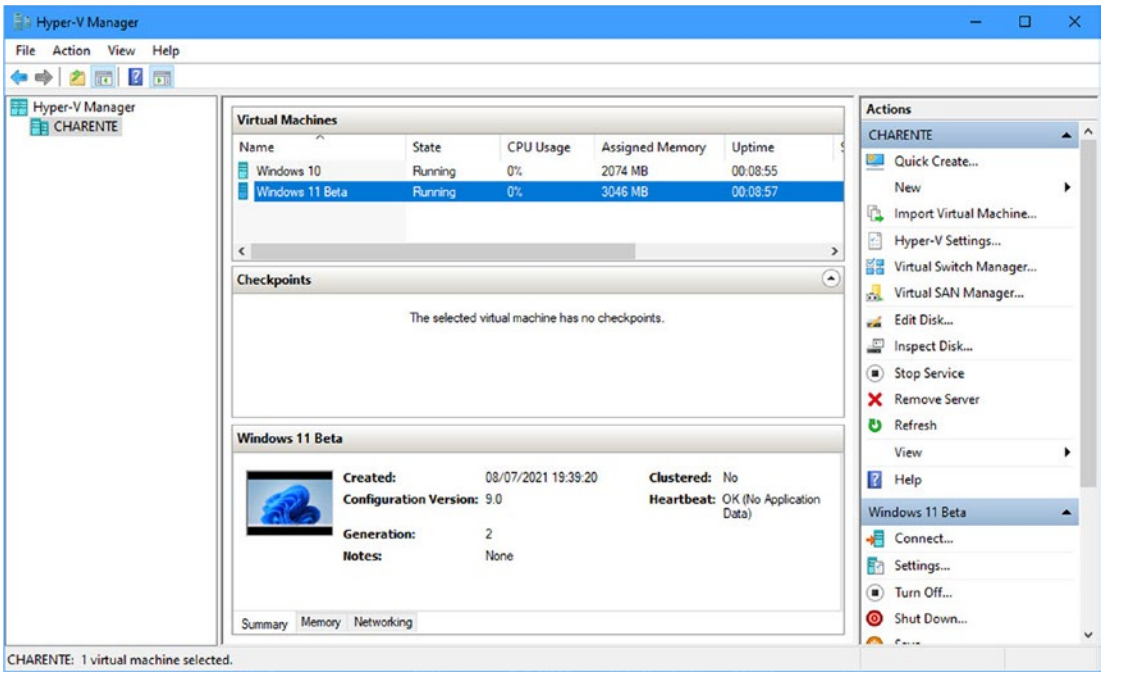


Figure 20-3. *The Hyper-V Manager in Windows 10*

There are two ways to create a virtual machine in Hyper-V. The first is the *Quick Create* link in the top right of the window. This is primarily intended for developers and enables quick installation of a preconfigured Windows 10 or Ubuntu Linux development environment; see Figure 20-4.

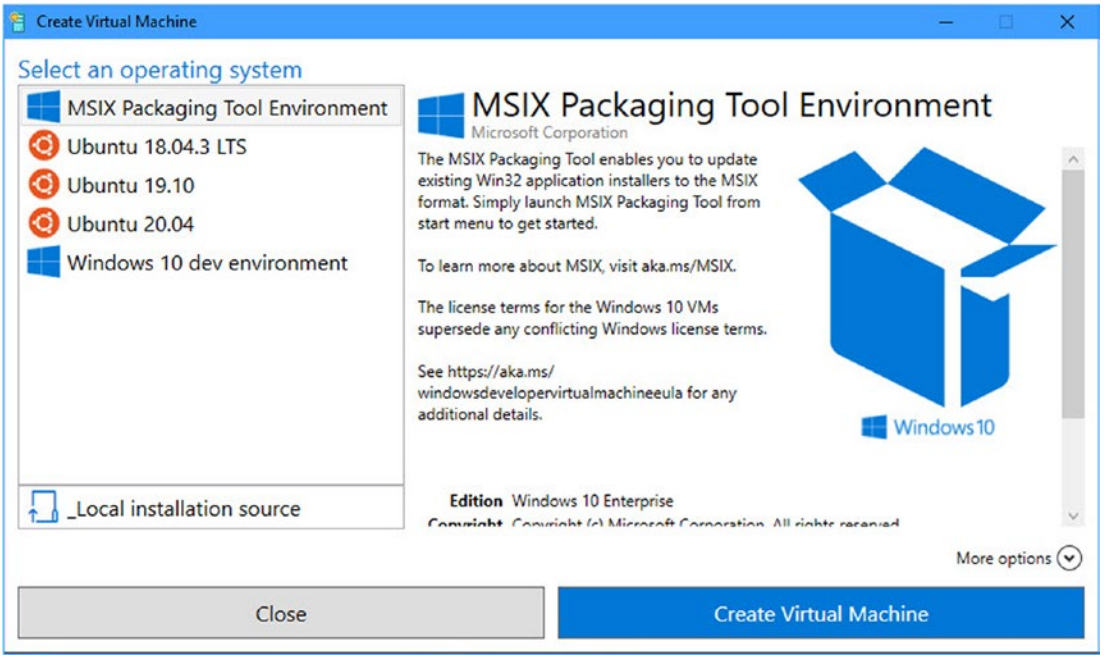


Figure 20-4. *You can install some development environments easily in Hyper-V*

The main way to create or import an existing VM into Hyper-V is by clicking the *New… Virtual Machine* or *Import Virtual Machine* links in the top of the right panel. This will run through a wizard that will ask how you want to set up your VM, with questions such as its storage location and more.

I want to deal with some of the more important questions that arise in this wizard interface. The first of these is which *generation* of VM you wish to create; see Figure 20-5. If you need to create a VM running Windows XP, for example, you won't be able to use the newer Generation 2–type VM. This is because the Generation 2 type, which offers additional functionality such as UEFI support, Secure Boot, Boot from a SCSI virtual hard disk (VHD), and faster boot and operation times, also requires a 64-bit OS. The 64-bit version of Windows XP was short-lived and poorly supported.

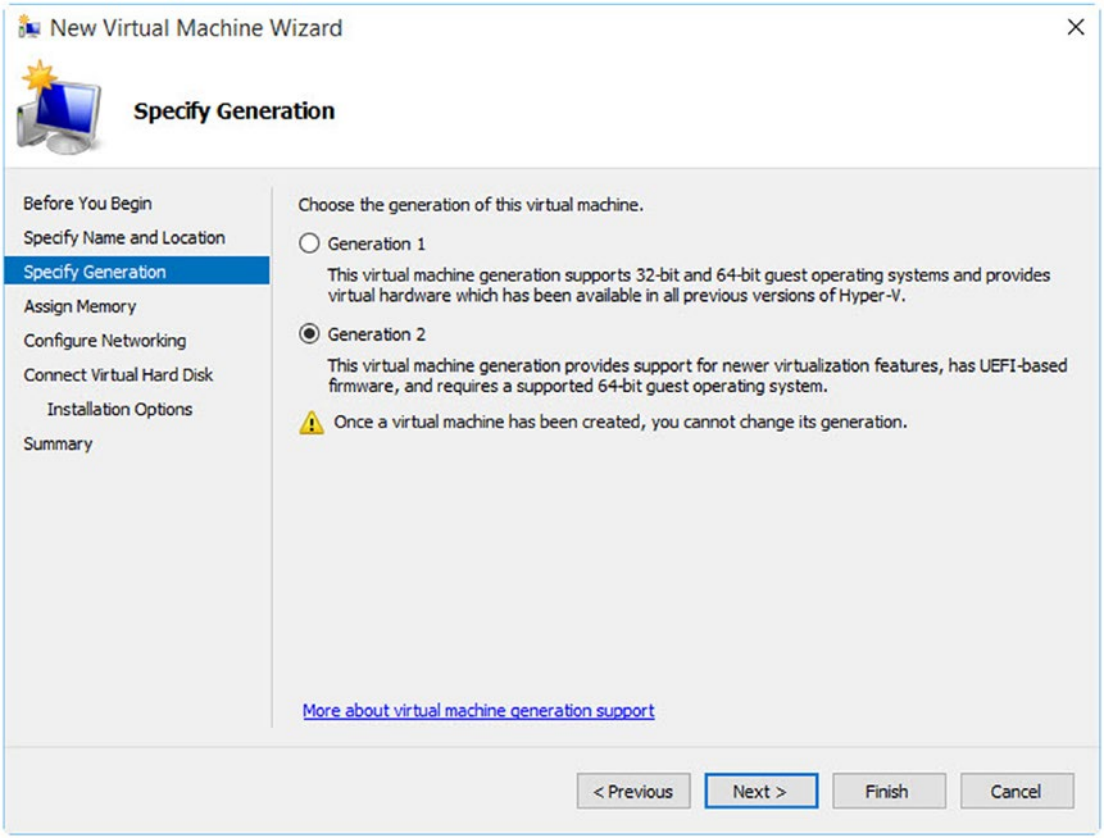


Figure 20-5. *You can choose from different generations of VM type*

The next option is how much memory to assign to the VM, and whether to use Dynamic Memory; see Figure 20-6. When a VM starts, it will consume all of the memory you give it. This is memory shared with the host OS on the PC, and you might only have so much you want to spare. Hyper-V's Dynamic Memory feature allows the host OS to reclaim unused memory when the VM isn't using it. This can help improve the overall performance of the host PC, especially if it is running multiple VMs.

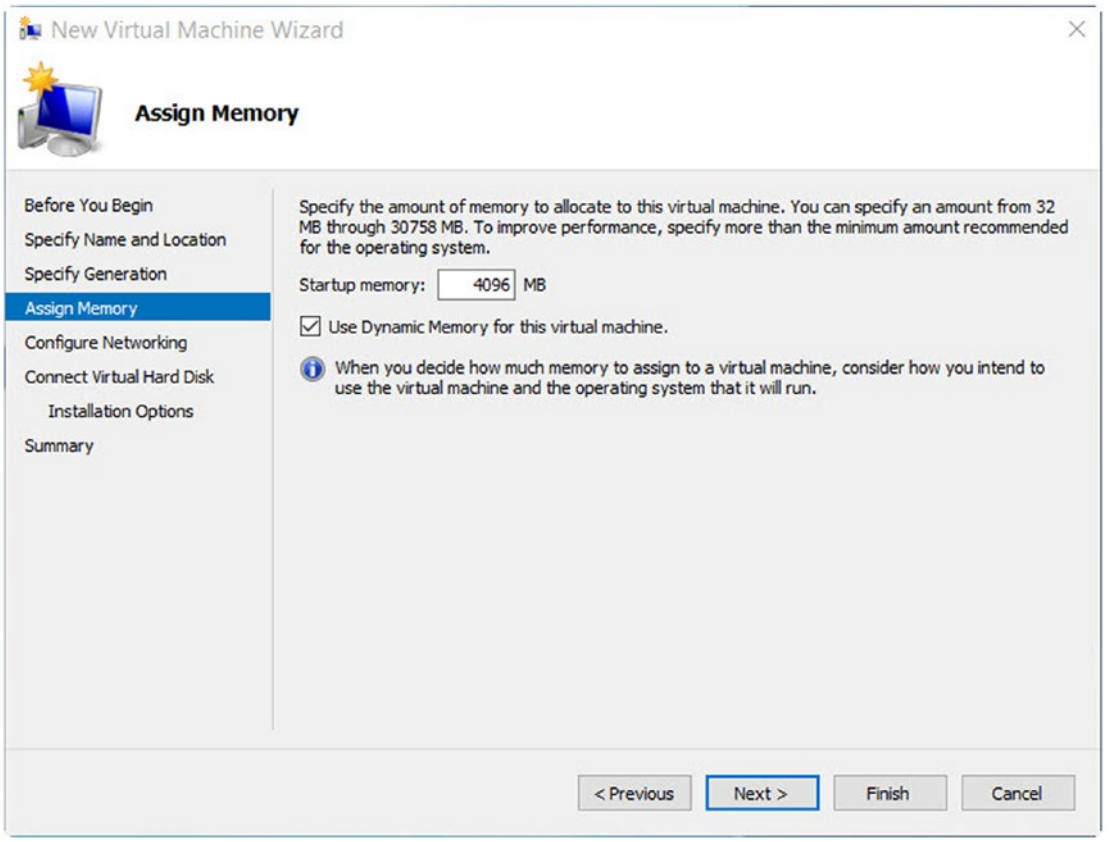


Figure 20-6. *You can choose to assign Dynamic Memory to a VM*

Managing Networks in Hyper-V

Next up is the network connection assigned to the VM; see Figure 20-7. Network connections are created separately to the VM itself, as you might have one network connection that's shared by multiple VMs. Creating the correct network connection, however, is crucial, especially if you want to maintain strict security on your systems, or if you are running a vulnerable OS, such as one that is out of support, like Windows XP.

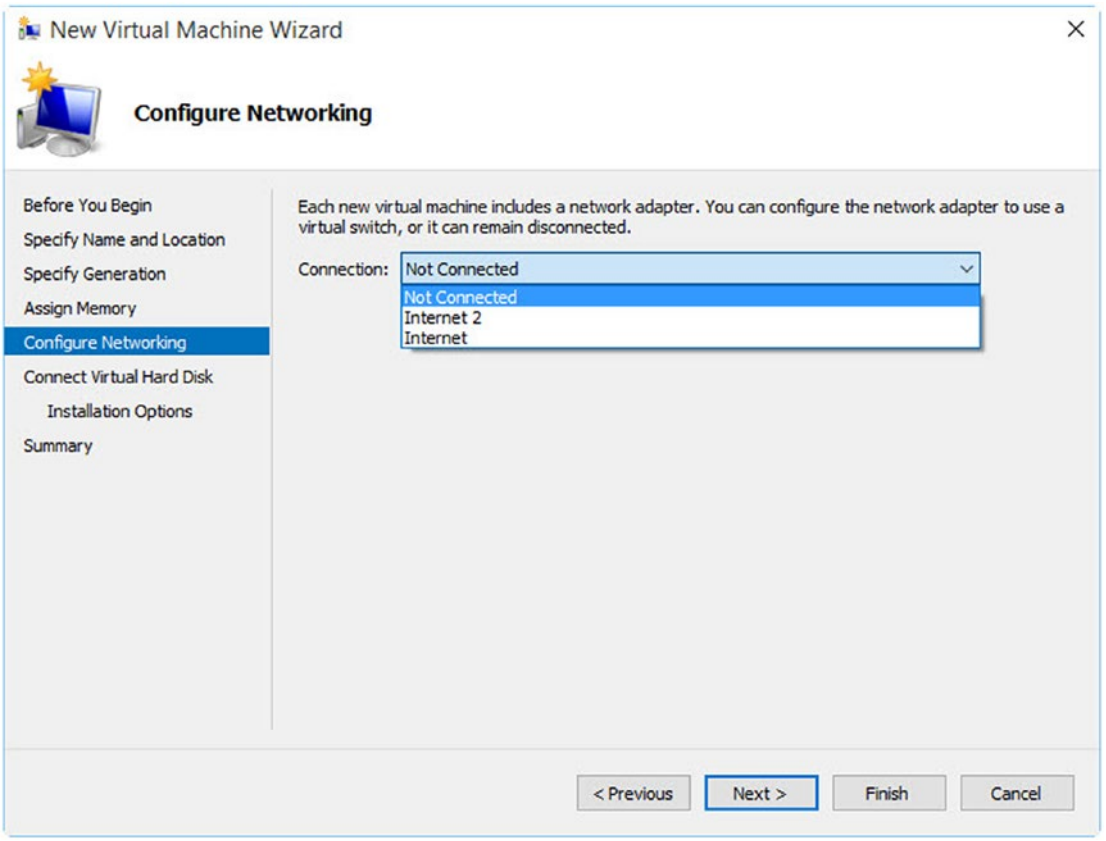


Figure 20-7. *You can assign different network types to VMs*

There are three different network connection types that you can create within Hyper-V (see Figure 20-8), and it's extremely important to maintaining good security that you choose the correct one:

- **External** networks can see everything that your physical network adapter can. This includes other machines and devices on the network, but also it means they can get full access to the Internet, if your PC also has Internet access.
- **Internal** networks are ones that are constrained to the host PC and the VMs that run on it. This means that the VM will be able to see all other locally running VMs, and also the storage resources on the local PC.

- **Private** networks are to be used if you really do need to sandbox a VM, as they provide the best security. A VM connected to a private network will only be able to see other VMs running on the PC, and nothing else.

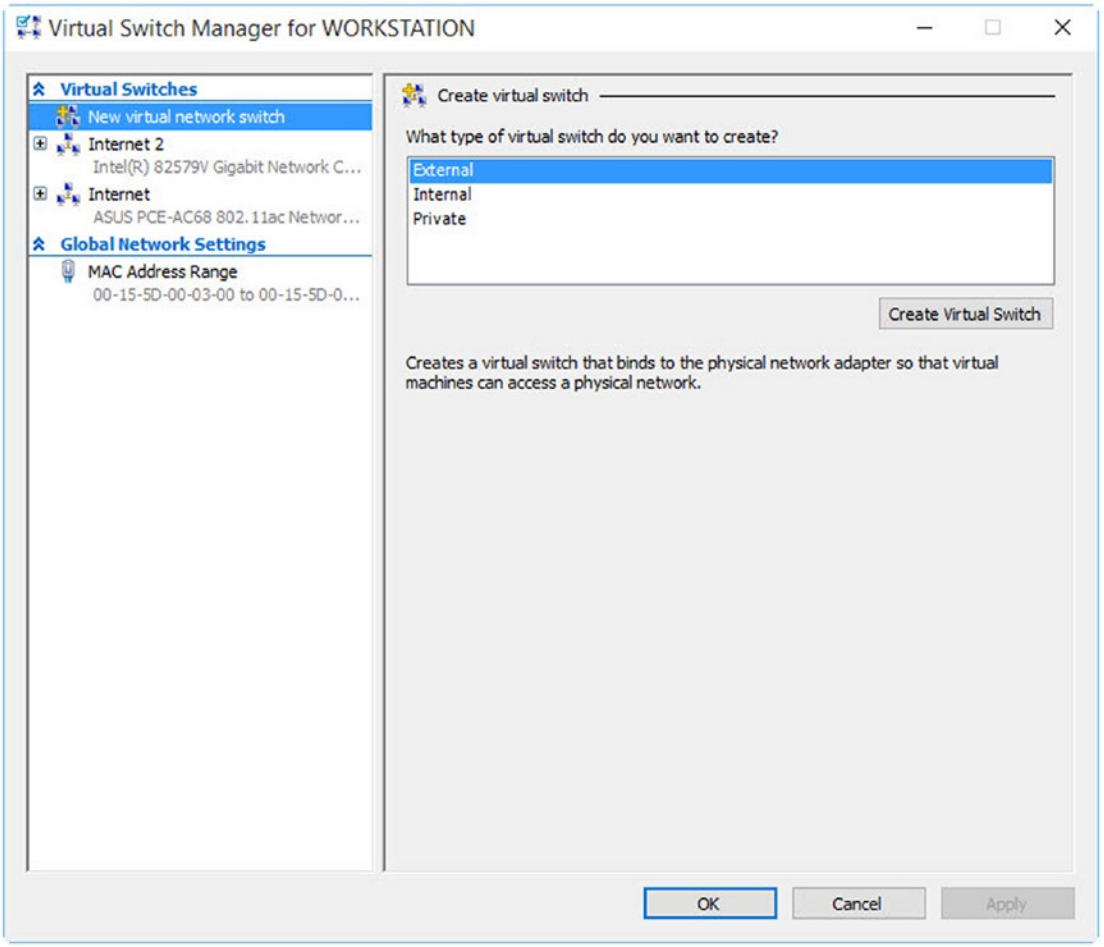


Figure 20-8. *There are three different types of network connection you can create*

Tip If you have more than one physical network adapter in your PC, perhaps two-gigabit Ethernet, or Ethernet and Wi-Fi, you can connect the virtual switch to the adapter you're not using for your own Internet access. This will give the VM access to PCs and VMs connected to that second network, which you can isolate for its own purposes, for instance, to create a secure network of PCs internally in your company.

That said, there's nothing to say that a VM has to be connected to a network at all. By far the best way to sandbox a VM is to not have it connected to a virtual network at all. You may find that the legacy apps you need to run on the VM don't require Internet access. It may be a payroll system where all the data is stored locally, for example, and where there is no need for any type of network connection. You can disable the network connection at any time however, which enables you to fully update and secure the VM before isolating it from the Internet and/or your network.

Creating Backups of VMs in Hyper-V

One very useful feature of Hyper-V is the ability to create checkpoints for VMs. These work like System Restore on your PC, in that they are a snapshot of the state of that VM, at the time to checkpoint was created. They can be used to test different scenarios in the VM because you can safely roll back the changes using the checkpoint afterward, if the change has resulted in an unexpected or unwanted result.

You can create and manage checkpoints in the central panel in the Hyper-V manager by selecting the appropriate VM, whereby checkpoint options will appear in the bottom right of the window; see Figure 20-9.

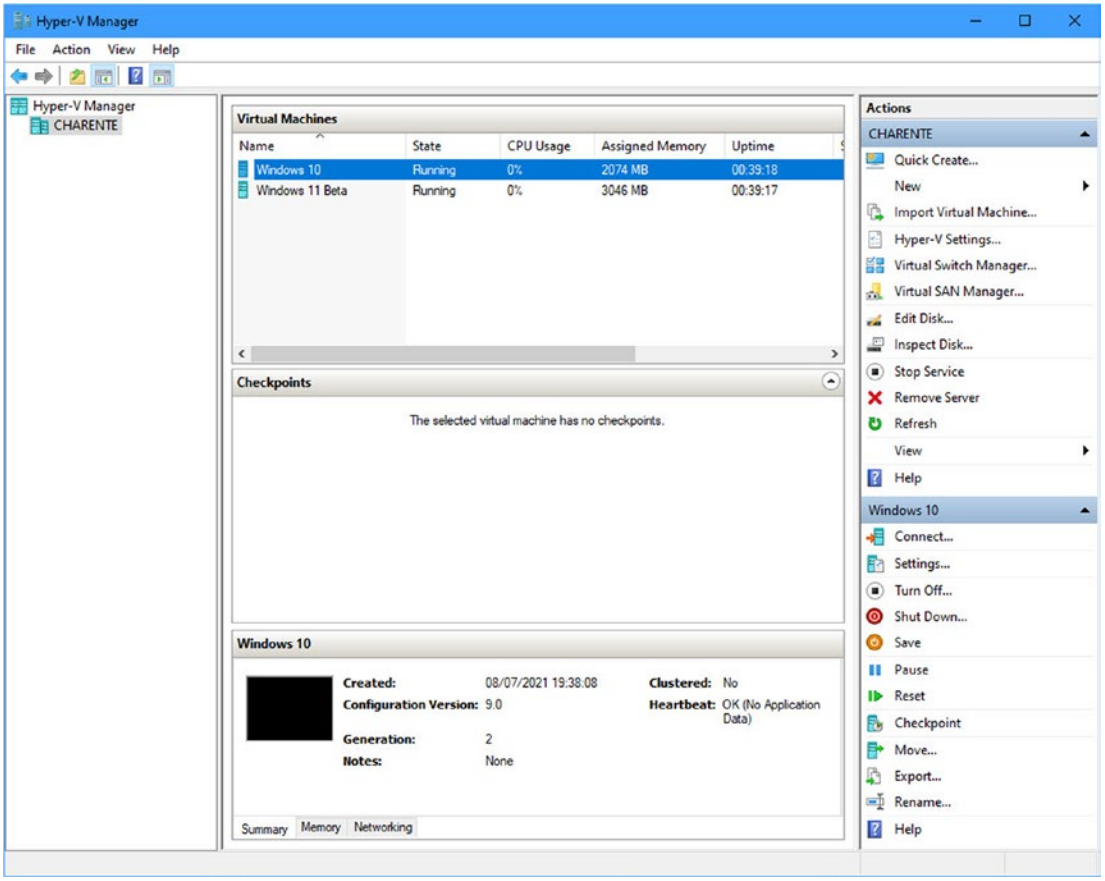


Figure 20-9. *You can create checkpoints so you can test changes to VMs*

Tip Selecting a VM in the Hyper-V Management window will present an Export option in the bottom right of the window. You can use this to create a backup copy of the VM, so that it can also be used on other PCs, or so that it can be easily copied back to the PC should there be a problem with the VM later.

Managing Hyper-V from PowerShell

Many system administrators won't want to have to open the Hyper-V client interface to manage virtual machines, so you'll no doubt be pleased to hear that you can manage VMs directly from within PowerShell. Open **powershell** from the Start Menu. When in the PowerShell interface, type `Get-Command -Module hyper-V | Out-GridView` to display a list of all the available commands for managing Hyper-V and VMs; see Figure 20-10.

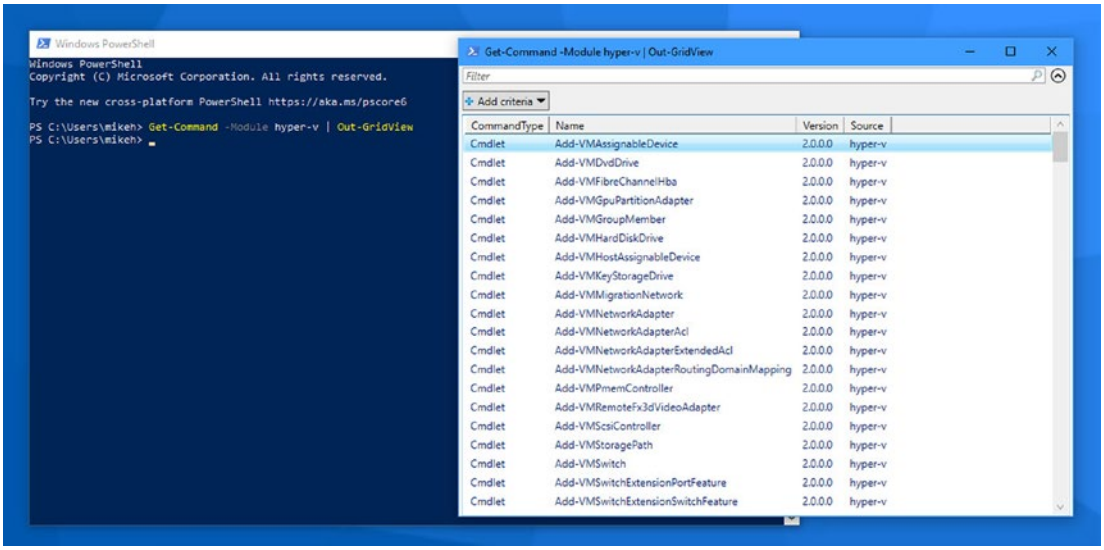


Figure 20-10. *You can manage Hyper-V directly from PowerShell*

If you are new to PowerShell, and Chapter 27 covers how to troubleshoot Windows 10 using scripting, then help is on hand as the command `Get-Help Het-VM` will show you how to structure your PowerShell commands, and what secondary and optional parameters are available for you to use. Some more of the most useful PowerShell commands for managing Hyper-V include:

Get-VM displays a list of virtual machines, used in the format `Get-VM | where {$_.State -eq 'Running'}` or `Get-VM | where {$_.State -eq 'Off'}`.

Start-VM to start and shut down virtual machines, often used in the format `Get-VM | where {$_.State -eq 'Off'} | Start-VM` to start all currently switched off VMs or `Get-VM | where {$_.State -eq 'Running'} | Stop-VM` to stop all running VMs.

Get-VM -Name <VM Name> | Checkpoint-VM -SnapshotName <snapshot long name> to create a snapshot for a chosen VM.

You can find a full and comprehensive list of all PowerShell commands related to Hyper-V on the Microsoft website at this link https://pcs.tv/3iomcDi although I can also recommend Pro Microsoft Hyper-V (Apress, 2019), the latest edition of which can be found at this link https://pcs.tv/3xpRWfC.

Booting and Repurposing Your PC from a VM

At the beginning of this chapter, I said that you can make PCs more robust through the use of VMs. One of the methods for doing this is to boot your PC from a VM. When you do this using a VM created in Hyper-V, you won't even know you're not using the host operating system, as the VM will have full access to the PC's hardware, and will run quickly and effectively.

There are several advantages to booting a PC into a VM. The first is that, from a system administrator's point of view, you will always have a working, safe, secure underlying OS that you can start the PC into if something goes wrong with the VM. Repairing the VM for the user can then become a simple task of copying a fresh copy of the VM from across your company network (you may even store VM images on the PC itself). This can be significantly faster than reimaging a PC, and has the only drawback that you may need more than one product license for the copy of Windows on the PC.

Note Each operating system and software package you install into a VM needs to have its own license and, if necessary for that product, its own product key. Some versions of Windows are not licensed for use inside a VM. You can find out more about licensing for your particular copies of Windows and other Microsoft software at www.microsoft.com/About/Legal/IntellectualProperty/UseTerms.

Booting your PC from a VM can provide the additional benefit of being able to quickly repurpose the machine. Let's say, for example, you are a business with a limited amount of laptops, and you need to take one that's been used by a sales representative and repurpose it, so that a designer can use it instead.

Rather than having to place a base Windows image onto the laptop, and then sideload all of the apps that a designer in your company needs, you can create a VM in advance that has this preconfigured. This is pretty much the same as creating multiple installation images of Windows 10 for your company, but VMs can be easier to manage and configure.

Resetting and Removing Hyper-V Network Connections

One of the potential issues with Hyper-V is the complexity of the virtual networking system, and a quick search online will reveal countless problems with the virtual network switch dropping and completely losing network and Internet connections. When you create a virtual switch in Hyper-V, you might get one or two virtual network adapters being added to your Windows 10 networking system, or as in the case of my own PC, you might end up with a lot of them; see Figure 20-11.

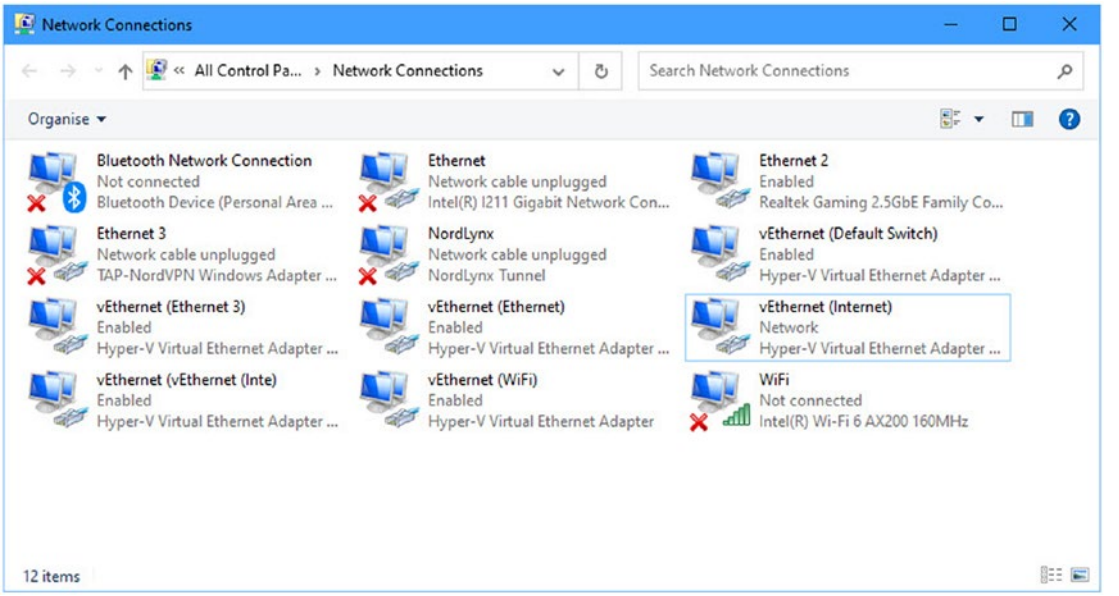


Figure 20-11. *The Hyper-V networking system can be… complicated*

One of the issues with Hyper-V network switches is that they're really difficult to uninstall if something goes wrong. Simply removing the virtual switches in the Hyper-V controls often won't remove them from the Network and Sharing Center. This is where you have to shut down some services to get them removed.

At any given time, there will be one or more Hyper-V services running on your PC, and in order to be able to delete the virtual switches from the *Network and Sharing Center*, you will first need to disable these services. Search in the Start Menu for **services,** and then from the Services applet, scroll down the list until you find the ones related to Hyper-V. You can right-click any running service to *Stop* it, at which point you should then be able to delete the switches, restart the PC, and create new switches in the Hyper-V console; see Figure 20-12.

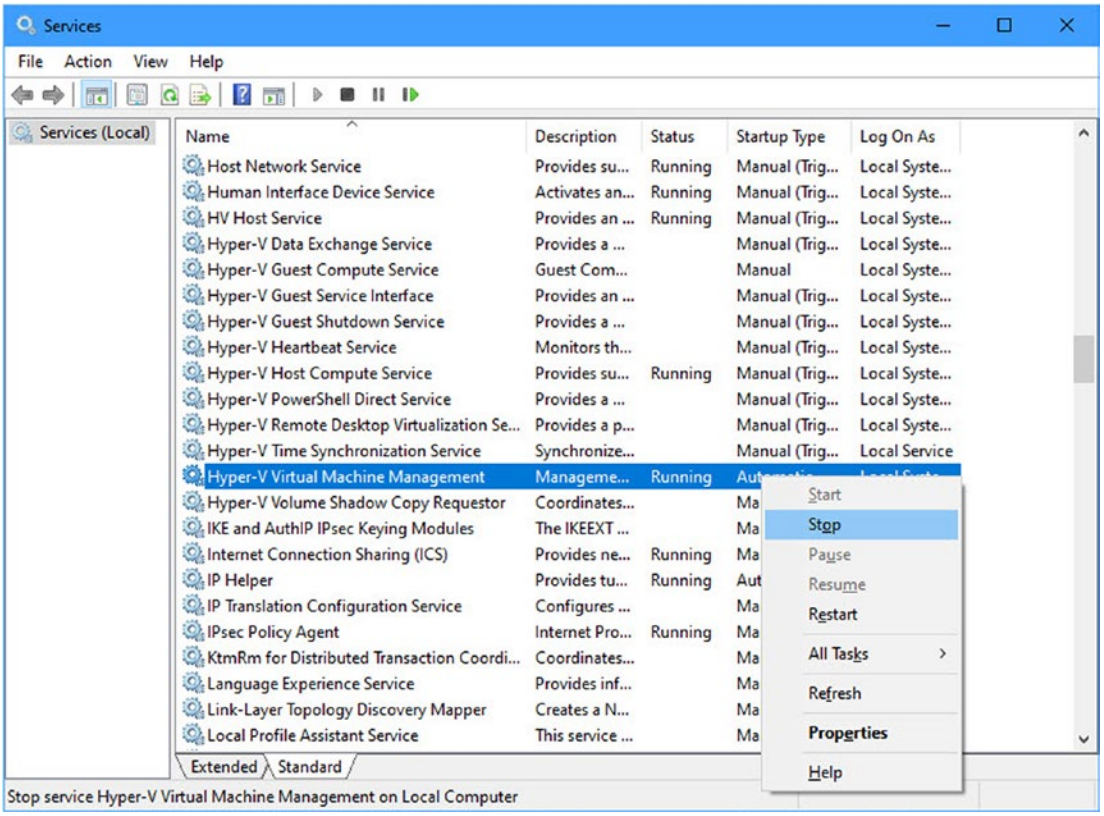


Figure 20-12. *You have to shut down Hyper-V services to delete virtual switches from Windows*

Creating a VHD

To boot your PC from a VM, you will need a VHD, and while you can create this when you install Windows, you can also create it in advance. You do this from the *Disk Management Console* (available from the *Win+X* menu). From the *Action* menu, click the *Create VHD* option; see Figure 20-13.

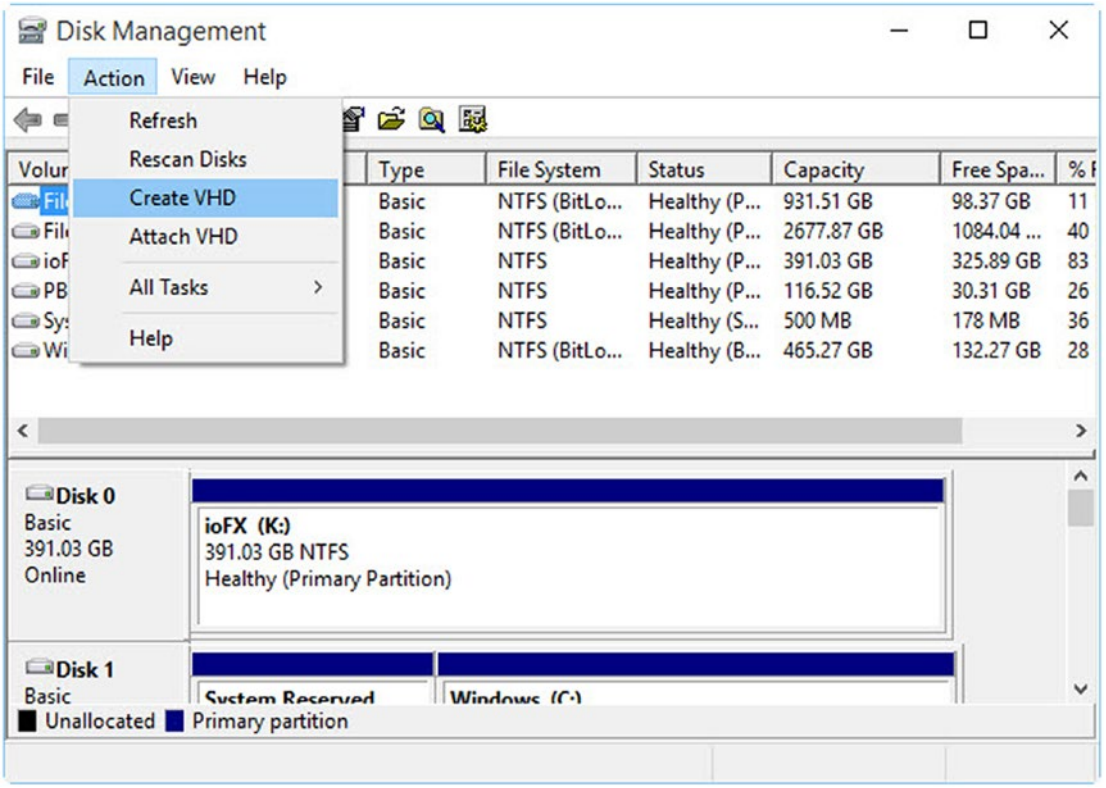


Figure 20-13. *You can create VHD from the Disk Management Console*

In the dialog that appears, you need to choose a storage location for the VHD, the type of VHD container you want to use (both types are described well), and if the VHD is to be a fixed size or if it should expand dynamically; see Figure 20-14. The latter option should be kept as fixed, because once you boot the PC from the VHD, it won't be able to expand dynamically anyway, as it won't be managed by the host OS.

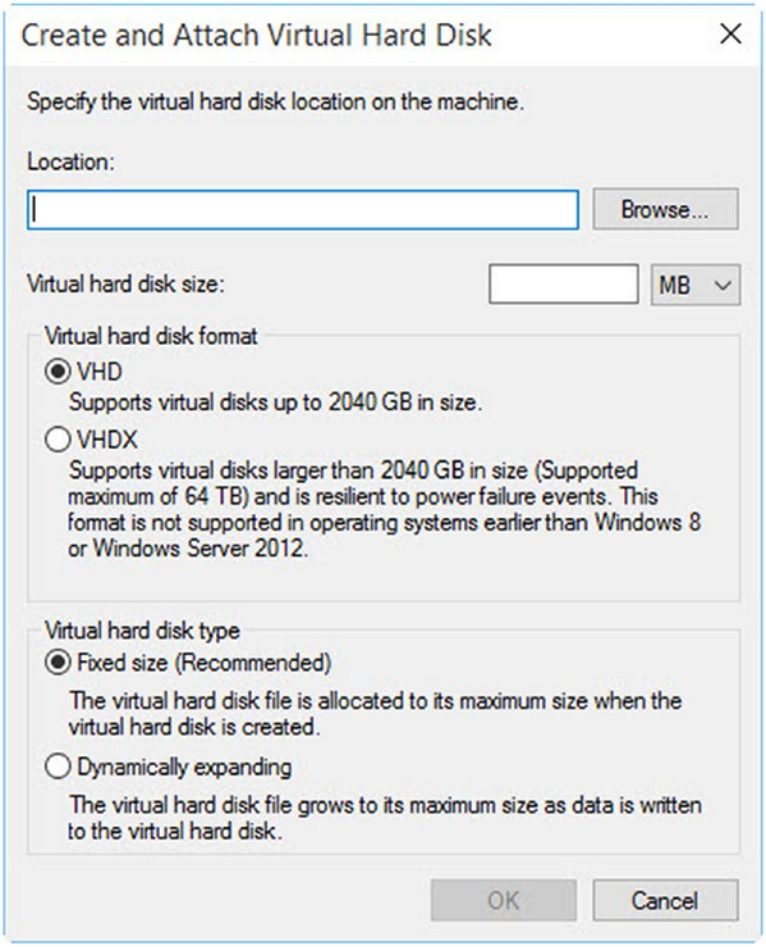


Figure 20-14. *You need to choose parameters for the VHD*

Tip You can also create VHDs in Hyper-V by using the *New* ➤ *VHD* option in the top right of the window.

Adding a VHD to the Boot Menu

To boot the PC from the VM, so that you can install an operating system into it, start your PC using your Windows installation media (DVD or USB Flash Drive):

1. Press **Shift+F10** at the installation screen to open a Command window.

2. Type **diskpart** and press Enter.
3. To use an existing VHD, type **Select vdisk file=C:\Path1\Path2\disk.vhd**, substituting the path and disk names for the location on the disk of the VHD and its name.
4. If you don't have an existing VHD and need to create one, type **Create vdisk file=C:\Path1\Path2\disk.vhd maximum=20000 type=fixed**, again substituting the path and disk names with where you want the VHD to be created and what you want it to be called (the path folders must already exist). Also, substitute the number of megabytes and create either a fixed or a dynamic disk.
5. If you have just created a new VHD, type **Select vdisk file=C:\Path1\Path2\disk. vhd,** and press Enter to attach the VHD if you have just created one, as per step 2.
6. Type **attach vdisk** and press Enter.
7. Type **exit** and press Enter.
8. Type **exit** again and press Enter.
9. Click **Install Custom: Install Windows Only (Advanced)**.
10. Locate the newly attached VHD in the hard disk pane in which you want to install Windows. This is Disk 1 if you have only one hard disk in your computer. You can identify it by its size. Click **Next** when you are ready to install Windows onto the VHD.

The next step is to add the VHD to the PC's boot menu:

1. Press **Win+X** to open the administration menu.
2. Click **Command Prompt** (Admin).
3. Type **bcdedit /v** in the Command window.
4. Press Enter.
5. Locate the VHD you installed, and make a note of its globally unique identifier (GUID) code. It is a long string of numbers and letters in the Identifier section for the OS (see Figure 20-15).

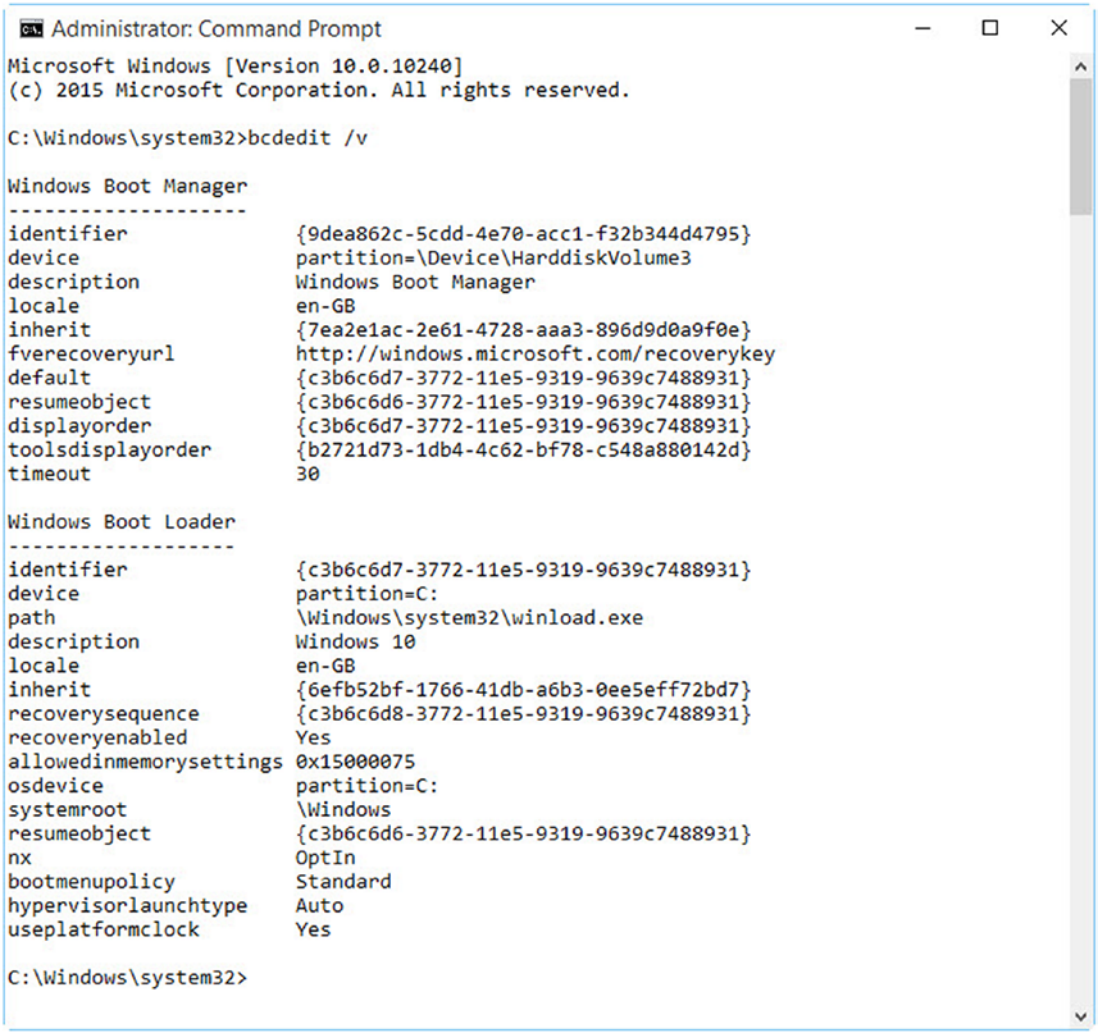


Figure 20-15. *You will need the GUID (Identifier) of the VM*

6. Type **bcdedit /set {GUID} description "OS Name,"** substituting the actual GUID for the OS for the letters GUID and assigning the OS its proper name. Press **Enter**.

7. Optionally, you might want this VHD to be the OS that loads by default. Set this by typing **bcdedit / default {GUID}**. Press **Enter**.

The VM has now been added to the boot menu on the PC and will start as though it were a regular OS, installed on the main hard disk. This is better because as long as you keep the file name of the VHD and its storage path the same, you can swap it out with another VM and quickly repurpose or repair the PC.

Windows Sandbox

The sandbox is where you get to go and play, at least in the literal sense, as just as things were when you were young, playing in the sandbox came with zero consequences and usually a lot of fun. Windows Sandbox might not offer as much fun as a proper sandbox, with a spade and bucket, but it's a great place in which to try out new things.

In short, Windows Sandbox is a feature of the Pro and Enterprise versions of Windows that uses Hyper-V to create an instant, completely contained, and completely disposable Windows environment in which you can try new things, such as software compatibility and configuration options, with no danger of affecting the host OS.

You have to enable Windows Sandbox, so in the Start Menu, search for **turn windows features on or off,** and then in the dialog that appears, you will see Windows Sandbox near the bottom of the list; see Figure 20-16.

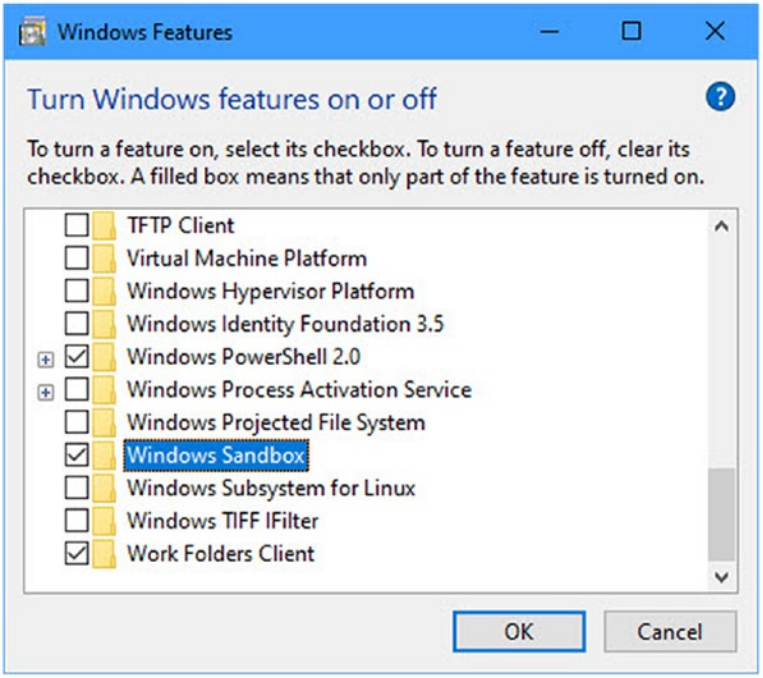


Figure 20-16. *You have to enable Windows Sandbox before you can use it*

With Windows Sandbox enabled, it will become available in the Start Menu. Running it will present you with a stripped-down version of your Windows 10 installation. I say stripped-down as not all features of the OS will be available; remember that Sandbox is intended as a testing and diagnostic tool; see Figure 20-17.

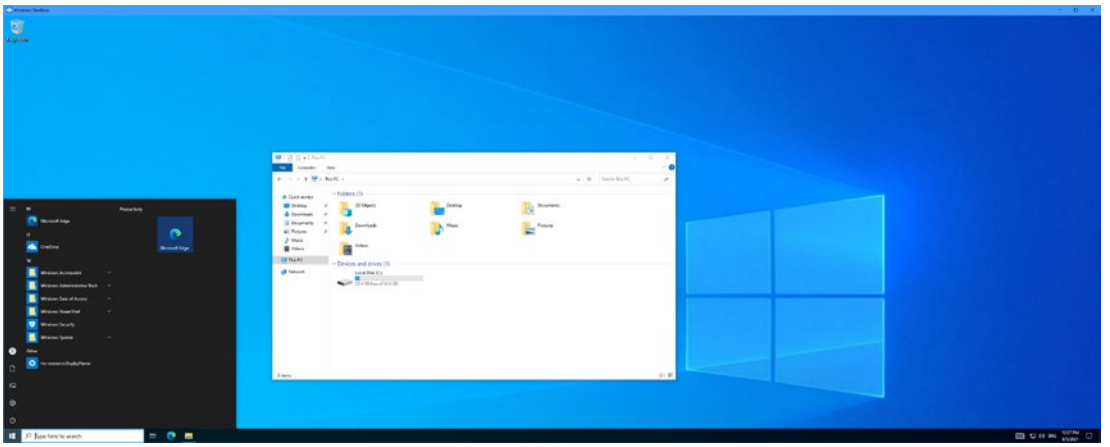


Figure 20-17. *Windows Sandbox appears as a VM window on your desktop*

When you close Windows Sandbox, you will see a message saying that what happened in Vegas will stay in Vegas and that everything you have done in the sandbox will be permanently deleted. If you need to check compatibility with an update, app, or device, then this really is the perfect environment in which to do so.

Windows 365 and Cloud PC

Another option if you run software that requires fiddly configuration, or that could present security or stability problems on a local PC, is Microsoft's Windows 365 service. This is a repackaged and rebadged version of Azure Virtual Desktop, and it allows you to have a real host PC in the cloud that can stream to any device you choose, including desktop and laptop PCs, and even to an iPad or Android tablet; see Figure 20-18.

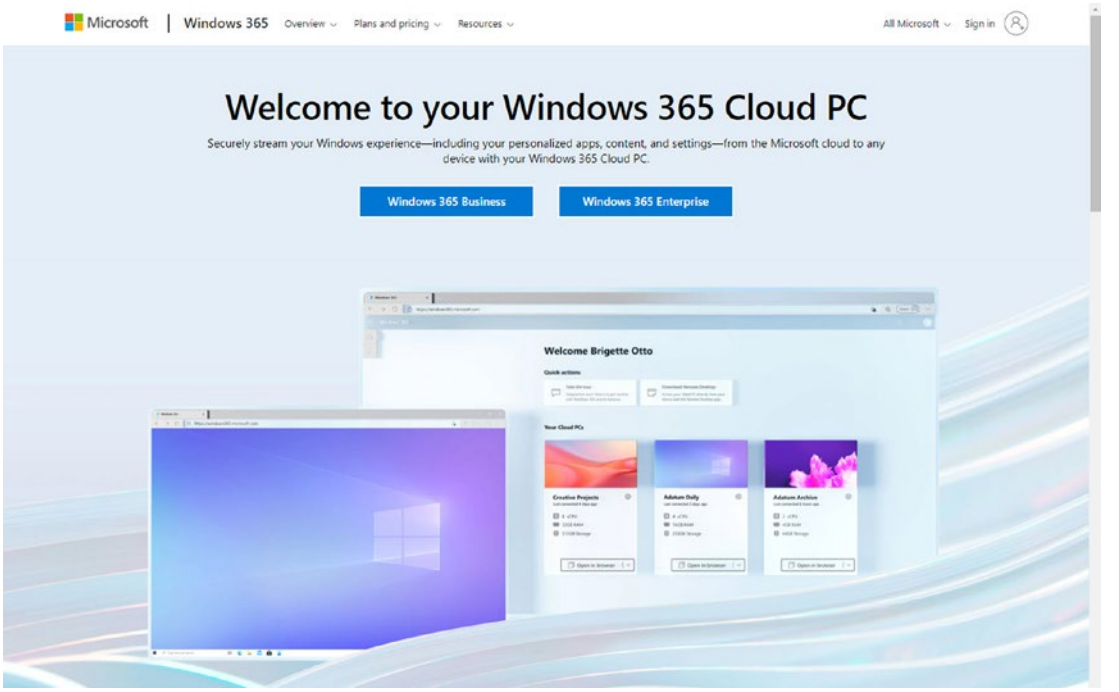


Figure 20-18. *Microsoft's Windows 365 service acts as a full PC in the clouds*

While not cheap, Windows 365 can provide some stability and security for apps and software that are a little more bespoke and difficult to configure. It can also be a very helpful backup option to help workers get working again quickly if their main PC or laptop encounters a problem and needs to be serviced and/or repaired.

Summary

VMs can be a very useful way to protect the host OS on a PC, and to ensure that repair can be implemented quickly and without fuss. It's also useful when it comes to setting up PCs, as you won't need additional tools such as the Assessment and Deployment Toolkit and System Center Configuration Manager, which are sometimes available only to Enterprise customers and can also be complicated to understand and use.

The ultimate aim of any PC administrator though is to try, as much as is humanly possible, to make the PC completely bomb-proof, so that no matter what disaster might befall it, you can be up and running again quickly. This is precisely the subject we'll be tackling in the next chapter.

PART III

Mastering Windows 10 Troubleshooting

CHAPTER 21

Bomb-Proofing Your PC

It's fair to say that nothing ever goes wrong with a PC unless there's a human involved in some way. Machines are simply not capable of going wrong on their own, as it's going to be performing an operation, making a change, applying an update, or just not understanding correct use that can lead to anything from a minor issue to full-scale failure. Let's face it, just taking something out of the box can be enough for some people.

As an IT pro, however, it's not just your job to keep systems operational and functional all of the time; it's going to be your passion as well. Sure, you probably love delving into the OS and fixing problems every bit as much as I do, but it's still a pain in the butt when you have to do it.

The ultimate aim, therefore, isn't just to make a PC system as resilient, robust, and reliable as possible but to actually make it completely bomb-proof. I do genuinely mean bomb-proof too, as you want to be certain that if the very worst eventually did indeed occur, you could pick up quickly and carry on working with as little fuss and as minimal downtime as possible.

The global pandemic of 2020 showed us just how unprepared we can be when disaster strikes. Personally I think we were fortunate that big tech companies, and even small startups, were moving our entire system of work to the cloud. Microsoft in particular had been busy spending the previous few years building systems and services such as Azure Virtual Desktop and Teams that made the transition to working from home considerably simpler. Just imagine if the pandemic had happened a decade earlier!

Note I talked about Microsoft's *Windows 365* service in Chapter 20, and this can be a useful tool to employ in the event of a disaster, or perhaps another global pandemic. It means that any worker who is suddenly unable to access their work PC can almost immediately continue so long as they have access to any other computer, from a Linux laptop to an iPad.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_21

So while being prepared for the unexpected on our PCs is as crucial as it was when I wrote the first edition of this book back in 2015, we are now very more aware of the need. So what does this mean for you? Well for starters it means properly securing your PCs to avoid a local disaster from occurring. I have already written about some of the new tools available, such as Windows 10's built-in ransomware protection (Chapter 18) and Windows 365, but there's still more you can do on a per-machine basis to avoid disaster occurring in the first place, or to at least help mitigate against it should that happen.

Creating a Robust Backup Strategy

The most important part of making any PC system bomb-proof is to create a robust and reliable backup strategy. Take major tech corporations such as Microsoft and Google, for example. These companies store and keep much if not all of our data safe for us. Almost all of my own files are synced with OneDrive, and you may have a similar system in place for your personal or company files with Microsoft, Google, Amazon, Dropbox, or any one of the multitude of cloud service providers.

Each and every one of these companies, if they're clever and the big players certainly are, will store at least two copies of your data in separate geographic locations. This means that if there's a disaster at one data center, the other will remain intact, and you will still have access to all your files while the first data center is repaired, or even rebuilt.

For people who have a robust backup strategy in place, a similar approach will be adopted. This may just involve cloud storage, but it could also include offline storage as well. Remember that cloud restore can be slow, and if you want to be back up and running quickly, having hundreds of gigabytes, or even terabytes of data in the cloud, will take some considerable time to restore, even on the fastest fiber connection, and not all of your workforce will benefit from such a thing; as I write this, I'm still waiting for fiber to be installed where I live and work, and am making do with a 3.5Mbps ADSL line.

You may store an offline backup of your data at your premises, and perhaps (and I do recommend this) a mirrored copy of that backup at a separate, and again secure, location. This can be achieved in several ways. You may have backup software on your PCs that will create backups both to your local storage and to the remote storage via the Internet. You may alternatively have a network-attached storage (NAS) drive which can automatically mirror the data it holds to the remote location. Should a catastrophe occur, you can then take one of these local backups and use them to restore all of your data quickly.

When it comes to the PCs themselves, you can store your installation image files, and all files necessary to quickly set up new PCs, as a part of your backup process. You may even have virtual machines configured that can be quickly deployed to new PCs as bootable operating environments (see Chapter 20 on how to create these) or that can be run on a remote server and accessed via Remote Desktop Services (RDS).

You might have noticed that I'm placing emphasis here on having more than one backup, and you'd be correct. No matter who you are, your files and data will be the most important things to you, from photos of your dog to documents about your business projects. I use a multitier backup strategy, of a cloud backup to OneDrive, and backup to a NAS drive locally as well, in addition to which copies of my OneDrive files are mirrored onto my laptop and a second PC in the house… I take no chances!

With these strategies in place, you will find that, should the building in which your offices are based suddenly fall over and land in a pile of dust (let's face it, it's been known to happen) or should another global pandemic strike, your employees will be able to keep working, from home if necessary and on their own machines, with file access you can provide to them, and with full access to all the apps and services they need to get the job done.

Managing the Work from Home, Workforce

If you're a system's administrator, and unless you're fairly new to the role, you will have already been supporting a workforce, perhaps a very large one, that's been working from home. Many people would have had their own work laptop to use, but many more would have only had their home computer. I say home computer and not PC because while many will have their own Windows laptops, and the overwhelming majority of those should be running Windows 10, others may have a Mac, or an iPad or Android tablet with a Bluetooth keyboard.

The good news is that if you're using Microsoft 365 in your company, then connecting to Azure AD from any of these devices is straightforward, and both Microsoft and Apple have provided handy guides that you can find on the links below:

- **Join a Windows 10 PC to Azure AD**–https://pcs.tv/3yvWvGB.
- **Join an Android tablet to Azure AD**–https://pcs.tv/3rYXr3V.
- **Join an iPad to Azure AD**–https://pcs.tv/3jxkH5h.
- **Join an Apple Mac to Azure AD**–https://pcs.tv/3s9ZWRb.

Let's have a closer look at Windows 10 though, as its simplicity itself to connect an Azure AD account. In *Settings* click *Accounts* and then *Access work or school*. Here you will see a simple *Connect* button, and it's so easy to connect that any employee ought to be able to do this on their own; see Figure 21-1. Your employee(s) will want to click the *Join this device to Azure Active Directory* link, and then they can sign in using the work email address and password you have specified for them.

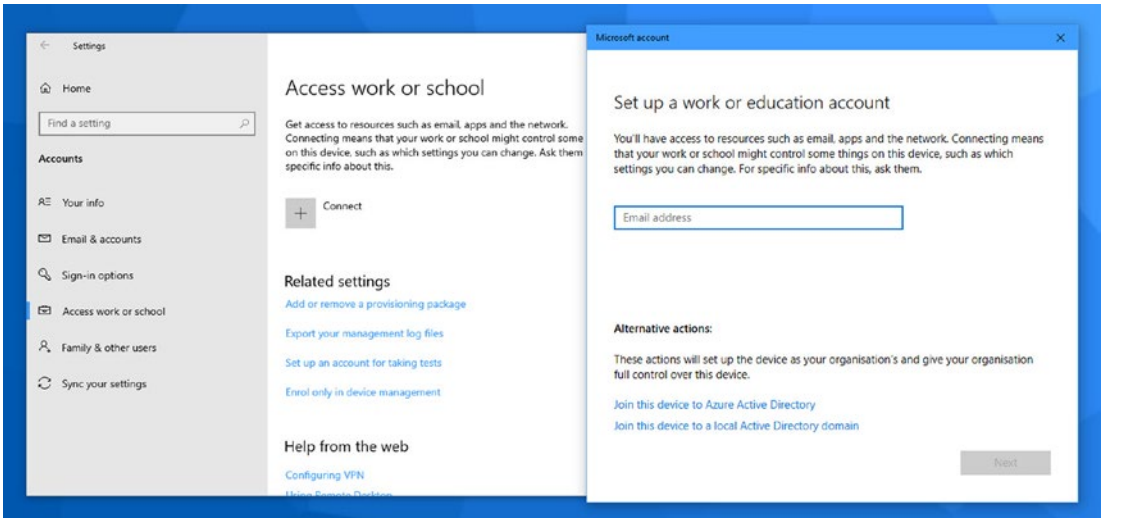


Figure 21-1. *You can easily connect a Windows 10 PC to Azure AD*

There are other links in the *Access work or school* settings that you will need to configure, or ask the employee to configure. Chief among these is to click *Add or remove a provisioning package*. This feature has been created by Microsoft to allow you to configure users' own PCs without needing to reimage them. A provisioning package is a file you will need to provide to the employee, either as a download or on a USB Flash Drive. When they add the package (see Figure 21-2), Windows will automatically search any removable media for appropriate files, and alert the user if nothing is found. Microsoft has extensive documentation about creating and deploying Provisioning Packages that you can find on this link `https://pcs.tv/3Cn1CuX`.

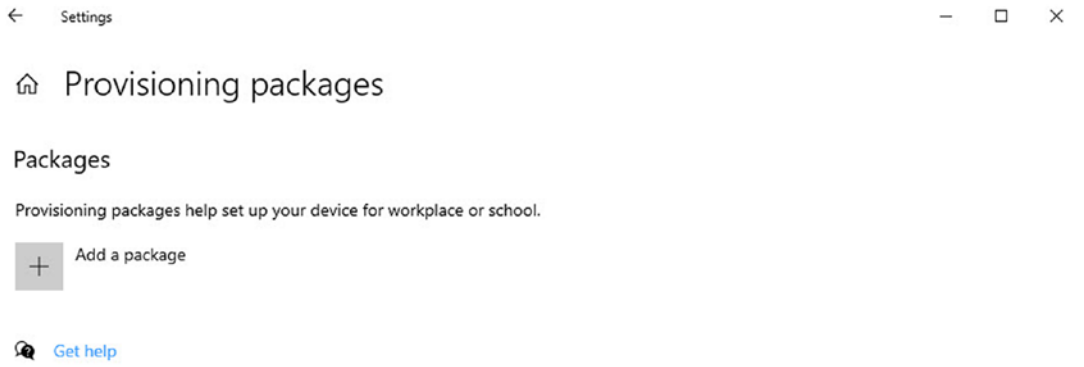


Figure 21-2. *Provisioning Packages let you configure a users' own PC easily*

If, however, you're happy that the employee already has the software they need on their PC, for example, they can do everything in a web browser, or they already have Microsoft Office installed, you can ask them to click the *Enrol only in device management* link; see Figure 21-3.

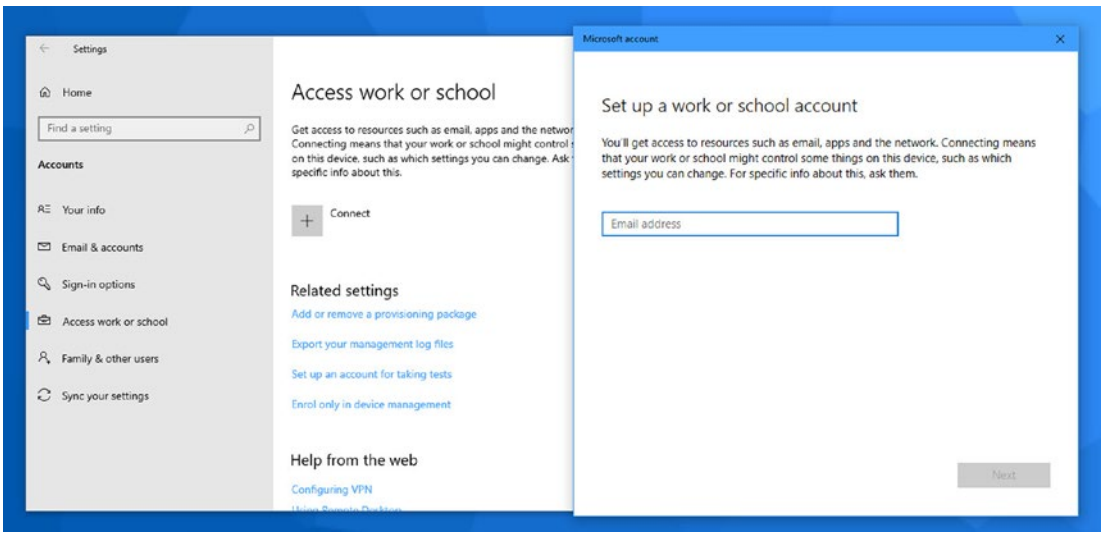


Figure 21-3. *You can optionally enrol PCs in device management*

Device management offers useful control from the enterprise perspective while not completely taking over the user's own PC and treating it as corporate property. These useful features include being able to specify a minimum security level for the PC, including that it must have up-to-date antimalware definitions installed to access company servers and files and that specific group policies are in place. You can read Microsoft's documentation about device management on this link https://pcs.tv/3Cn2TCf.

Lock Down Your PCs with Group Policy

Not all security is about making sure your business can get up and running again quickly after a disaster. Internal security is every bit as important, especially in these days of data theft and whistleblowers (though I should say if you're doing something wrong and somebody might whistleblow on you, a change in behavior might be a better option).

It's all too easy these days for an employee to slip a tiny USB Flash Drive into a PC and copy huge amounts of data. This data might even include the personal details of employees, customers, or suppliers, all of which will be governed by strict data protection laws, and don't even get me started on criminals and government agencies around the world trying to trick or lure employees to give them access to your data and servers. So how do you prevent data loss in this manner?

Tip Okay, I'll get started. Education is the name of the game when it comes to preventing third parties from tricking their way into your systems. It's worth making sure that everybody at the company, and this extends from first-line workers to directors, understands that if Eleanor from IT calls them saying she's trying to resolve an issue and just needs them to reconfirm their password, then it's definitely a scam. It's also a good idea to create an atmosphere of trust and openness, in which any employee can feel free to tell you if they think something unusual is going on, as if it really is *you* need to know about it.

If you are using the Pro or Enterprise editions of Windows 10, you will have access to the Group Policy Editor (search for **gpedit** in the Start Menu). Group Policy allows you to lock down many aspects of the OS and your PC, but the first I want to detail is how to block removable storage.

In the *Computer Configuration* ➤ *Administrative Templates* ➤ *System* ➤ *Removable Storage Access* section are options to completely block all types of removable storage, from CDs and DVDs to floppy drives, tape drives, and USB Flash Drives (listed as removable disks); see Figure 21-4.

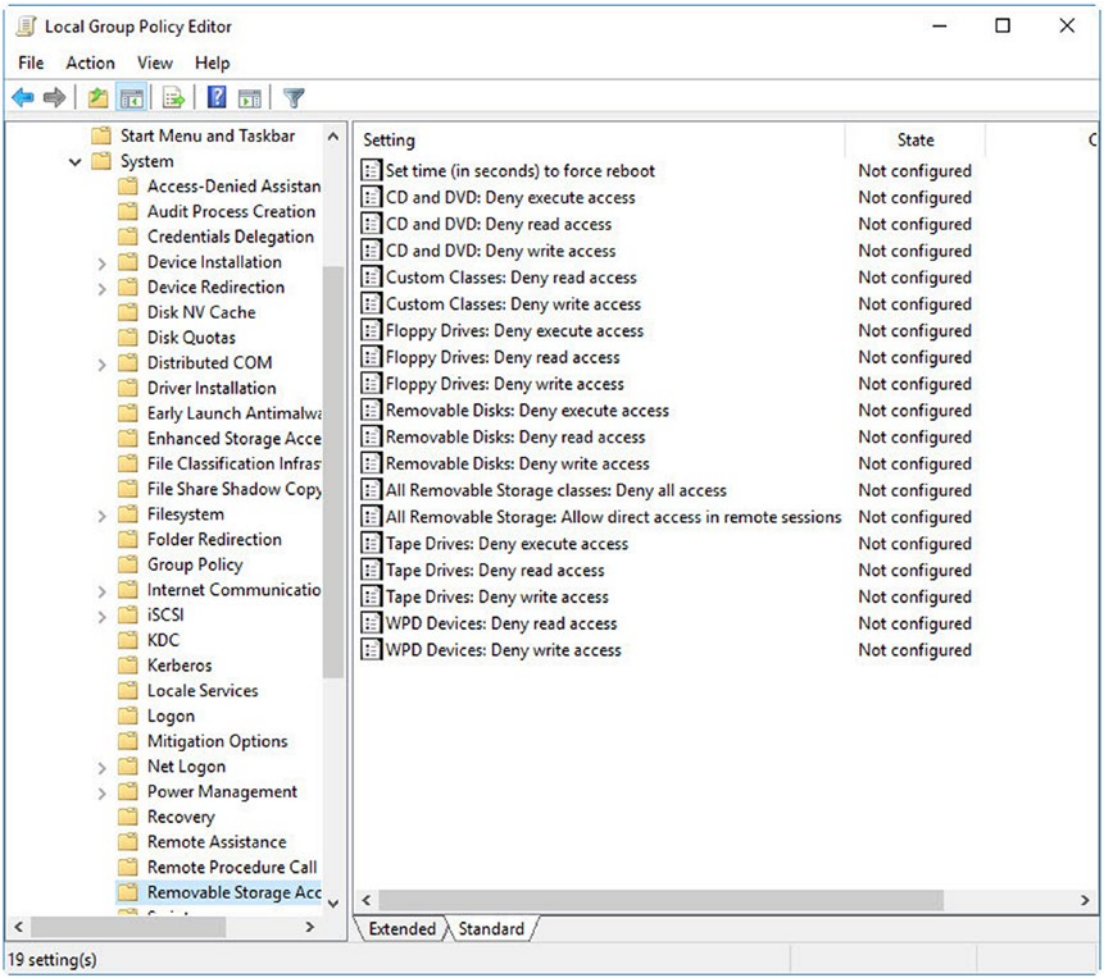


Figure 21-4. *You can manage removable storage in Group Policy*

You can even control access in such a way as to allow people to read files from removable media, but not to write data to the media or to be able to execute (run) apps from the media, which is a good way for malware to spread.

Other ways you can secure your PCs in Group Policy include being able to restrict hardware device installation and updating (as these can sometimes be updated to use nonsigned or unstable drivers). This can be found in *Computer Configuration* ➤ *Administrative Templates* ➤ *System* ➤ *Device Installation*, and can prevent unauthorized hardware being installed on your PCs.

There are other settings available in Group Policy that can be used to secure your PCs. Including the two I've already mentioned in this list, these are

- **Computer Configuration ➤ Windows Settings ➤ Security Settings ➤ Account Policies**–where you can enforce password policies for the PC.
- **Computer Configuration ➤ Windows Settings ➤ Security Settings ➤ User Rights Management**–where you can control additional sign-in and user permissions.
- **[Computer Configuration / User Configuration] ➤ Windows Settings ➤ Security Settings ➤ Security Options–**which contains security settings that don't fall into the previous two categories.
- **Computer Configuration ➤ Administrative Templates ➤ System ➤ Device Installation**–to prevent the installation of unauthorized hardware.
- **[Computer Configuration / User Configuration] ➤ Administrative Templates ➤ System ➤ Logon**–for setting security and password rules for users.
- **Computer Configuration ➤ Administrative Templates ➤ System ➤ Remote Assistance**–where you can specify if Remote Assistance can be used, and also restrict connections to newer, more secure versions of Windows.
- **[Computer Configuration / User Configuration] ➤ Administrative Templates ➤ System ➤ Removable Storage Access**–for denying read, write, and execute rights for removable and USB Flash media.

- **[Computer Configuration / User Configuration] ➤ Administrative Templates ➤ System ➤ User Profiles**–where you can specify security rules for caching and deleting user profiles.
- **[Computer Configuration / User Configuration] ➤ Administrative Templates ➤ Windows Components ➤ AutoPlay Policies**–if you allow removable media on your PCs, you can disable autoplay, which can restrict the ability of malware to infect the PC.
- **Computer Configuration ➤ Administrative Templates ➤ Windows Components ➤ Biometrics**–to control the use of biometric sign-in on the PC.
- **Computer Configuration ➤ Administrative Templates ➤ Windows Components ➤ Bitlocker Drive Encryption**–to enforce encryption policies on the PC.
- **Computer Configuration ➤ Administrative Templates ➤ Windows Components ➤ Data Collection and Preview Builds**–used to manage what usage data is sent to Microsoft, and to prevent the user from installing prerelease builds of Windows 10.
- **Computer Configuration ➤ Administrative Templates ➤ Windows Components ➤ Device and Driver Compatibility**–used to enforce the signed-driver policy.
- **[Computer Configuration / User Configuration] ➤ Administrative Templates ➤ Windows Components ➤ Remote Desktop Services**–where you can control all aspects of Remote Desktop and its security.
- **Computer Configuration ➤ Administrative Templates ➤ Windows Components ➤ Security Center**–where you can activate the Windows (legacy) Security Center for domain-attached PCs.
- **Computer Configuration ➤ Administrative Templates ➤ Windows Components ➤ Smart Card**–where you can control smartcard sign-in and security policies.

Managing Windows Services

Services are Microsoft and third-party applets that run in the background and either perform essential tasks to keep the OS running, such as managing user sign in, or provide features that will be shared by other apps or devices on the PC, like Plug and Play or the Print Spooler.

You access the Services panel in Windows 10 by searching for **services** in the Start Menu, and it will display a list of all the services currently installed on the PC, with sortable (clickable) column headings, so that you can, for example, arrange the list by the services that are currently running; see Figure 21-5.

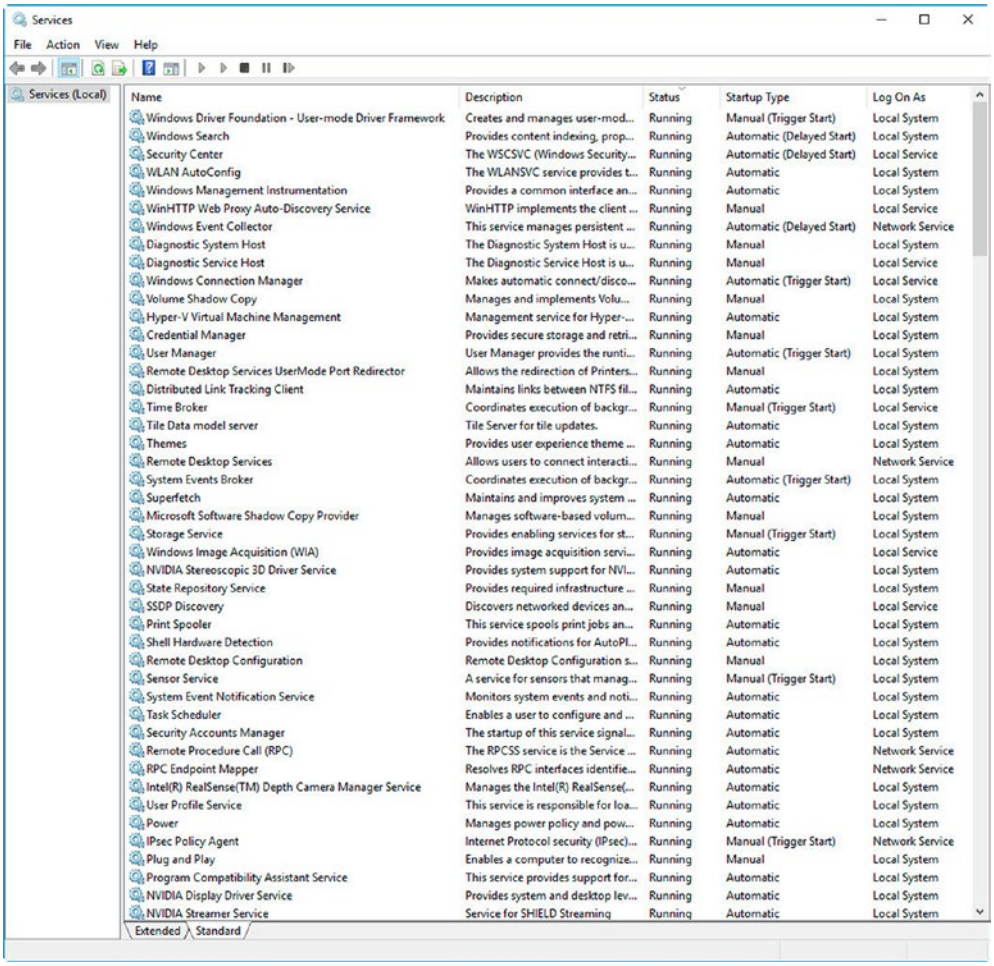


Figure 21-5. *You can view and control all the Microsoft and third-party Windows services*

You will see that each service has a full description, and this can be very useful in determining exactly what a service is for, and what apps or Windows features might need to use it. After all, you don't want to disable a service that might be required, or that could even prove essential in the smooth operation of the PC.

Each service will have one of four startup types assigned to it: *Disabled*, *Manual* (where the service is run only when invoked by an app or process), *Automatic* (where it will run on startup), and *Delayed Start* (where it loads only after everything else associated with startup has finished loading). You can display the properties inspector for a service by double-clicking it. This will display a dialog in which you can get information about and change settings for the service, such as its startup type; see Figure 21-6.

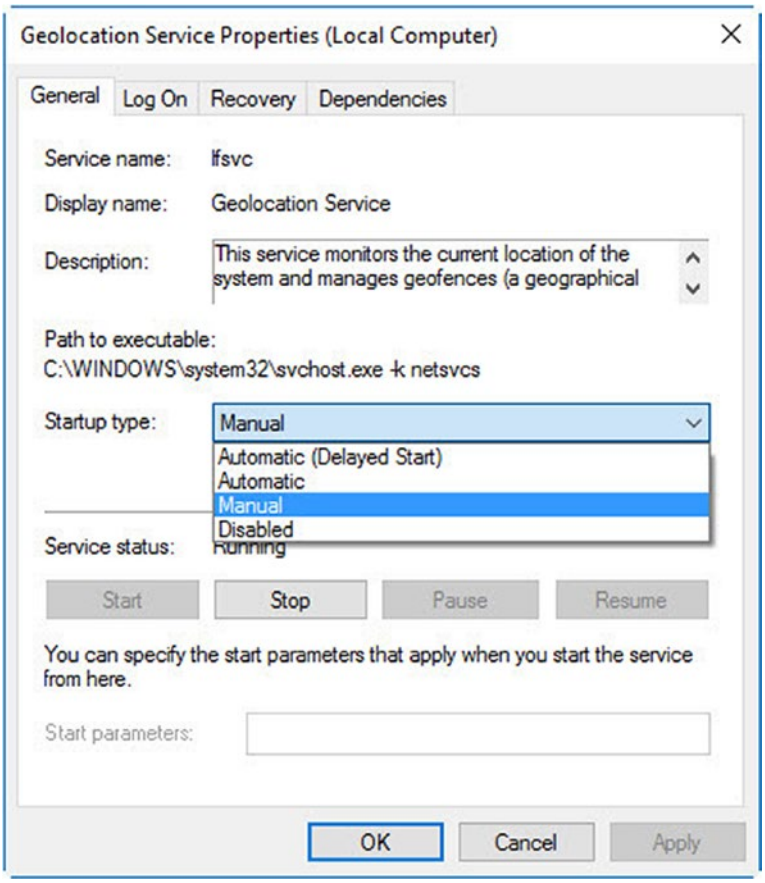


Figure 21-6. *You can control individual services by double-clicking them*

There is useful information available in each services properties panel. For example, under the *Dependencies* tab, you can see if this service relies on any other services to operate. This is useful if you are considering disabling services, as you might find that something you need to run depends on the service you wish to disable being active; see Figure 21-7.

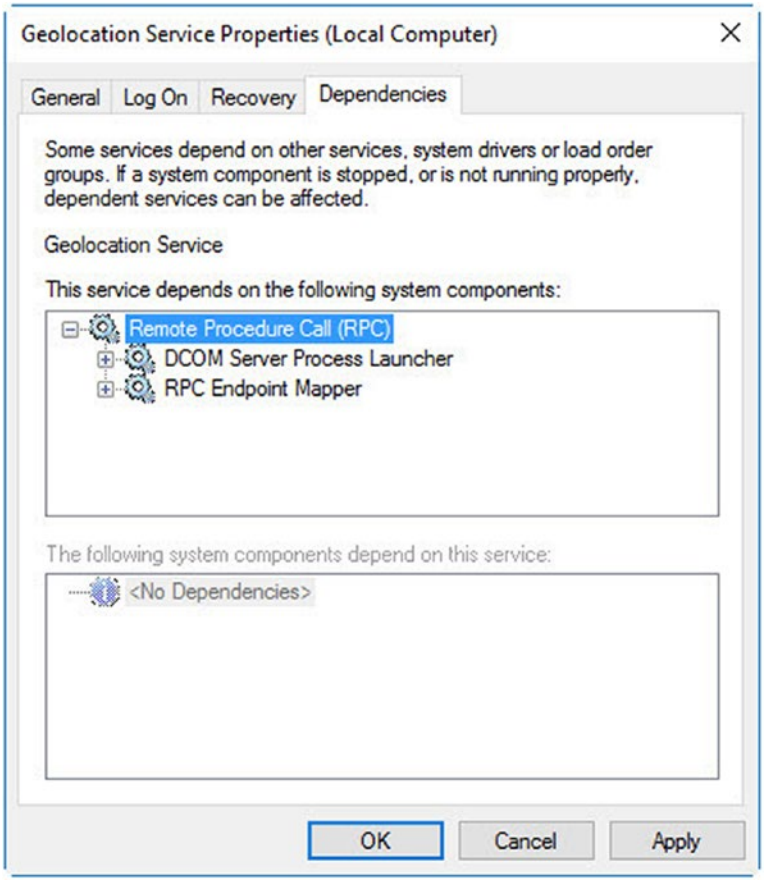


Figure 21-7. *You can check if a service has any dependent services before you disable it*

Additionally, the *Recovery* tab contains options for what Windows should do if a service fails or crashes; see Figure 21-8. This includes restarting the service, running a specific program (perhaps a dedicated troubleshooter), or restarting the PC. You can choose different actions for the first, second, and each subsequent service failure.

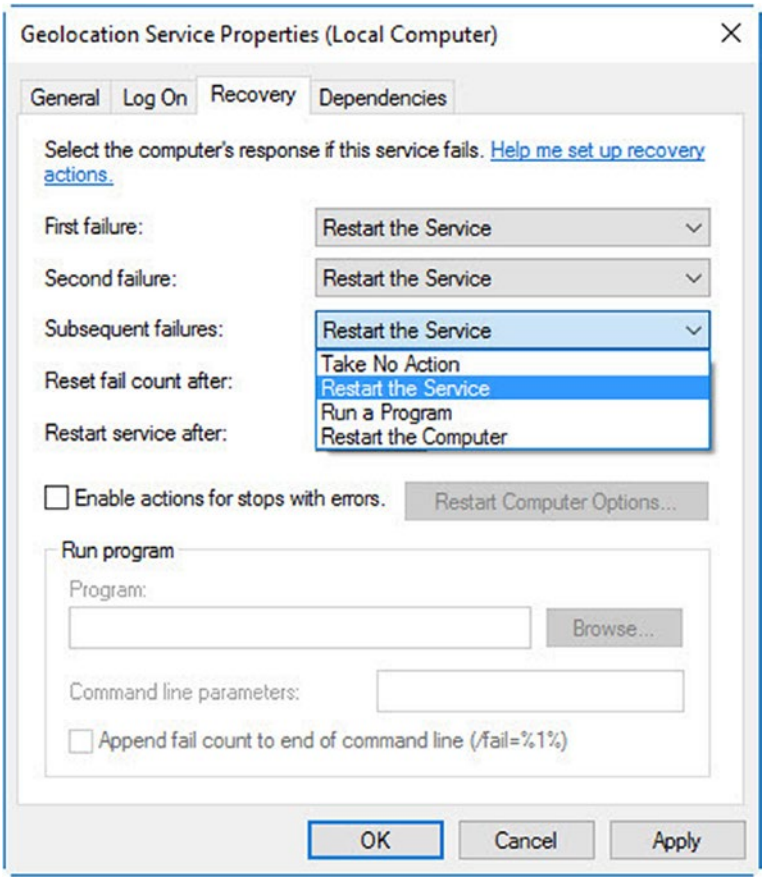


Figure 21-8. *You can set troubleshooting options for services*

Over the last few versions of Windows, Microsoft has become extremely good at enabling only the services your PC actually *needs*, in order to be able to start and operate quickly and effectively. There are services, however, that might be enabled that you won't need, and can stop. Why would you want to disable services though? Well, done properly, a PC with less services running will be faster and more robust and reliable overall:

- **Third-party management and update services from companies such as AMD, Apple, Adobe, Dropbox, Google, Nvidia, and Skype**– You might want to leave the update services enabled from third-party companies, as they can install critical security updates for apps installed on your PC. There might be additional services, however, that are not necessary.

- **Auto Time Zone Updater** will not be necessary for static desktop PCs.
- **Bitlocker Drive Encryption Service** will not be necessary for PCs on which you choose not to use Bitlocker, or Bitlocker To Go.
- **Bluetooth Handsfree Service/Bluetooth Support Service** will not be necessary on PCs where you do not intend to use Bluetooth devices.
- **Downloaded Maps Manager** is not necessary on PCs where you will not be using the maps app.
- **Encrypting File System (EFS)** is not necessary on PCs where you do not intend to use EFS.
- **Fax** is not necessary if you will not be sending or receiving faxes from the PC.
- **File History Service** is necessary only if you will be using the File History backup feature.
- **Geolocation Service** is not needed if you do not wish to use the geolocation features of Windows 10 on the PC.
- **HomeGroup Listener/HomeGroup Provider** can be disabled if you do not wish to use the HomeGroup feature in Windows 10.
- **Hyper-V Services**–Many can be disabled if you do not wish to use virtualization on the PC.
- **Phone Service/Telephony** is useful only for telephony features on the PC.
- **Print Spooler** can be disabled if the PC is to be used only for tasks that will not involve printing.
- **Remote Access/Remote Desktop Services** can be disabled to boost security if you do not want to permit Remote Desktop and Remote Assistance on the PC.
- **Smartcard Services** can be disabled if you will not be using smartcard authentication with the PC.

- **Touch Keyboard and Handwriting Panel Service** can be disabled on nontouch PCs.
- **Windows Image Acquisition (WIA)** only provides services for the importing of photos and video from attached cameras.
- **Windows Media Player Network Sharing Service** supports media playback features such as Play-To.
- **Windows Mobile Hotspot Service** can be disabled on static desktop PCs.
- **Windows Search** is extremely useful as it manages and maintains the full search capabilities of the OS. However, if you disable it, you can sometimes boost the battery life of a laptop or tablet by up to 30%.
- **Windows Store Service (WSService)** can be disabled if you do not intend to use the Windows Store.
- **Work Folders** can be disabled if you will not be using the Work Folders BYOD feature.
- **Xbox Services** can be disabled if you do not want to use the gaming or Xbox streaming features of Windows 10.

Manage Your Local Security Policy

You can manage security policies for the PC, such as user permissions and sign-in controls, through the Local Security Policy panel; search for **secpol** in the Start Menu. This contains policies that are also found in Group Policy, but it keeps all the security policies together and in one place, so they are easy to navigate; see Figure 21-9.

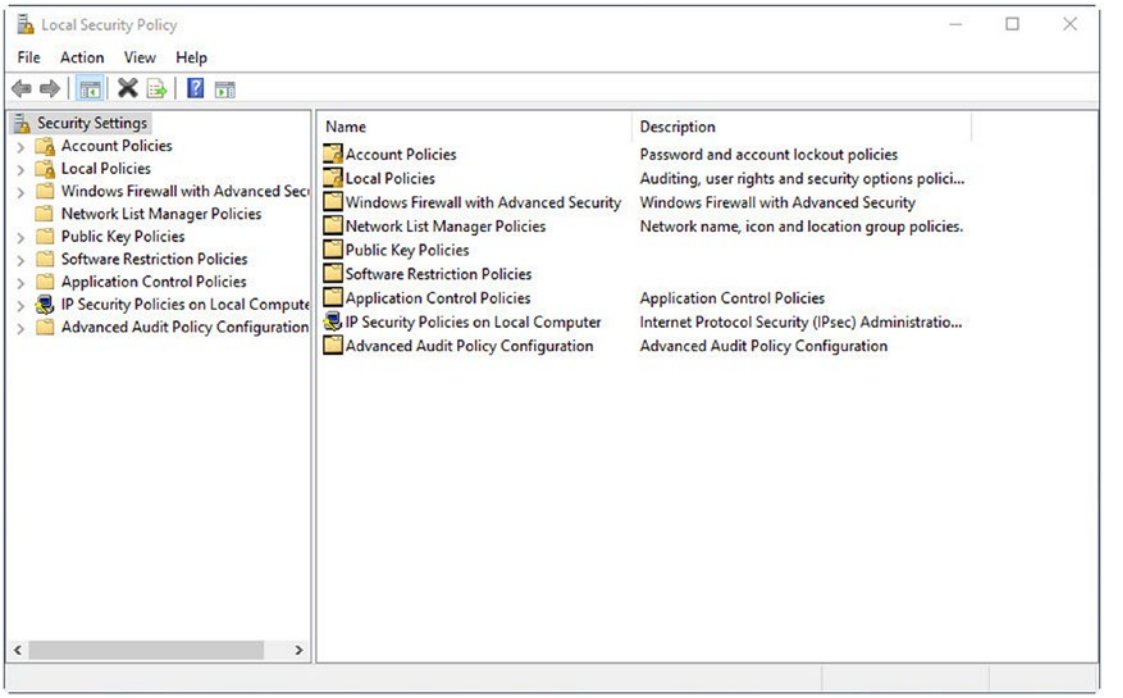


Figure 21-9. *You can manage a multitude of security policies in Windows 10*

It can be well worth spending some time examining the different options available to you. The Password Policy section, for example, can enforce minimum standards of complexity for the PC that must be met when users create or change their password. These policies can also specify that passwords must be changed on a regular basis.

If you are unsure about what any security policy does or means, double-clicking it will open its properties dialog, in which you will find an *Explain* tab. This will provide a full, plain text description of the policy and what it does; see Figure 21-10.

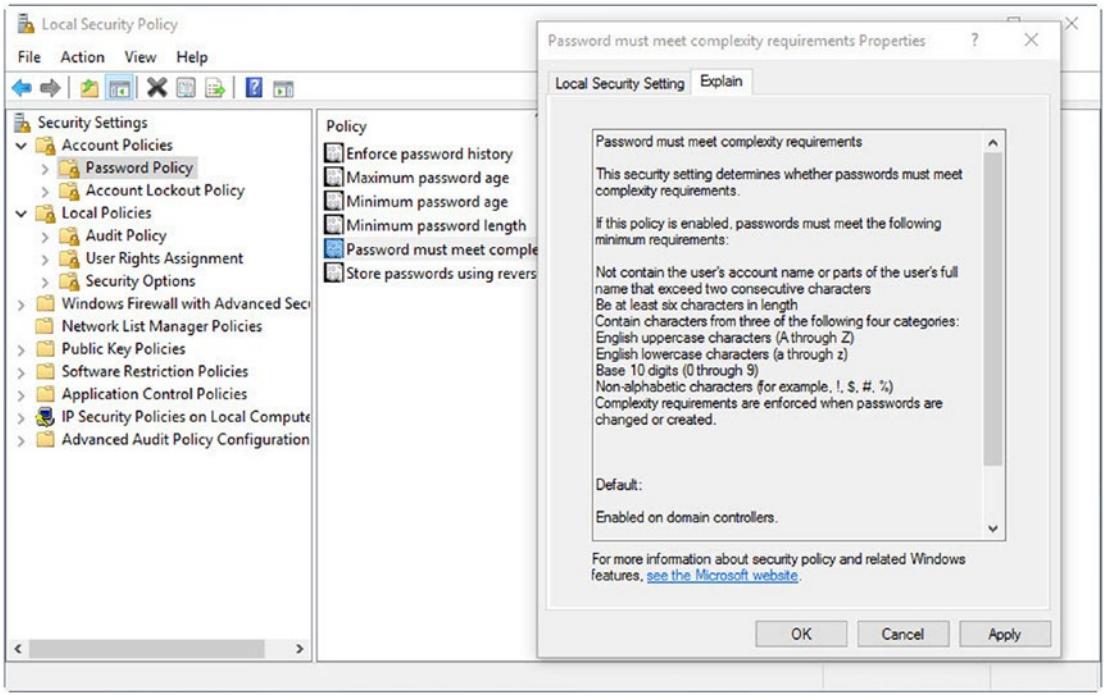


Figure 21-10. *Each policy has an Explain tab with a detailed description*

Managing Advanced Firewall Policy

When it comes to maintaining good security on our PCs, nothing is more important than a firewall. The Windows Firewall is extremely good, and there's almost never any need to replace it with a third-party option. It's boosted further by the inclusion of a *Windows Firewall with Advanced Security* panel, which you can open by searching for **firewall** in the Start Menu.

The Advanced Firewall is standard Microsoft Management Console fare, with the usual three-column layout; see Figure 21-11. In the top left of the window, you will see options to create Inbound, Outbound, and Connection Security rules. The right column contains context-sensitive options that will change depending on what is highlighted and what you are doing.

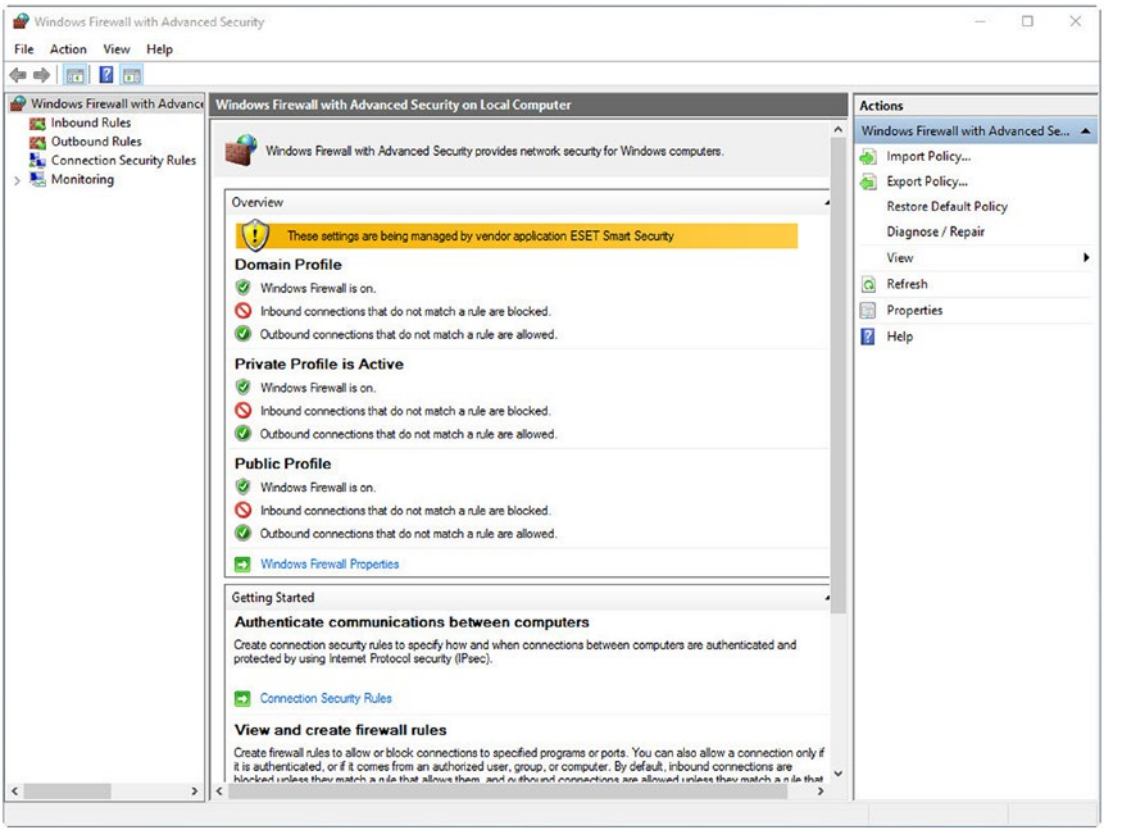


Figure 21-11. *The Advanced Firewall panel in Windows 10*

Clicking the Inbound or Outbound rules section will display a list of all the rules that are currently created, with details of whether the rules are enabled or not. You will also see a *New Rule* link appear in the top right of the window. You can click this to create new Firewall rules for the PC. There are four different types of rules you can create; see Figure 21-12.

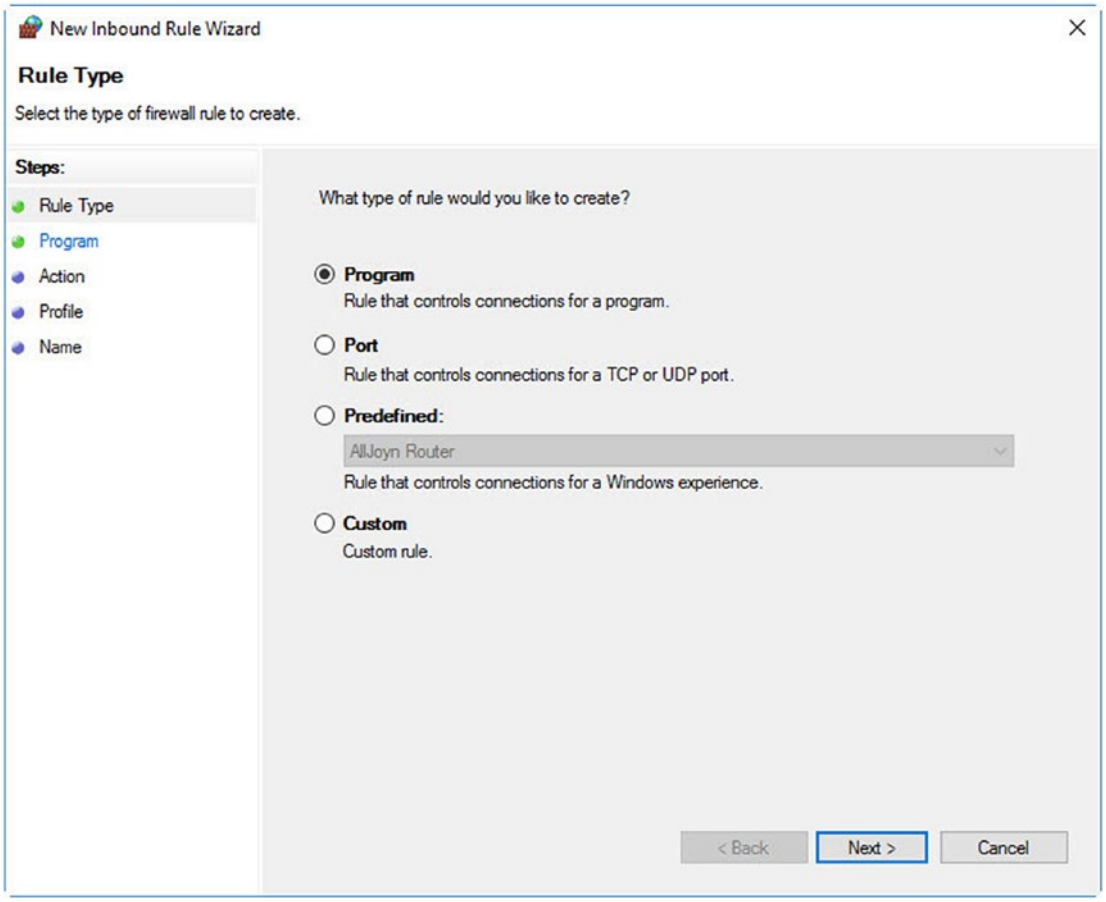


Figure 21-12. *You can create new rules in the Firewall*

- **Program** rules are those associated with a specific win32 app on your PC; Store apps are not managed here. You may find that you have a specific app on your PC which is being blocked by the firewall or that you wish to block. You can allow or deny access to the app here.
- **Port** is for allowing or denying access to specific communication ports on the PC. You may, for example, have a Virtual Private Network (VPN) solution that requires specific ports to be open and accessible on the PC, or you may specifically want to block ports used by file-sharing torrent apps.

- **Predefined** rules are ones that have already been configured by Microsoft to cover a wide range of business scenarios. These include rules that cover the BranchCache and Hyper-V features of the OS, along with Remote Access and Media Playback.
- **Custom** rules are defined in a very similar way to Program rules, but they also allow you to define rules that include specific Microsoft or third-party services.

You can examine and change the properties for any Firewall rule by double-clicking it to display its properties panel; see Figure 21-13. There is a wealth of information and a great many configuration options here for the firewall, including a plain text description of what the rule is, and what it is used for.

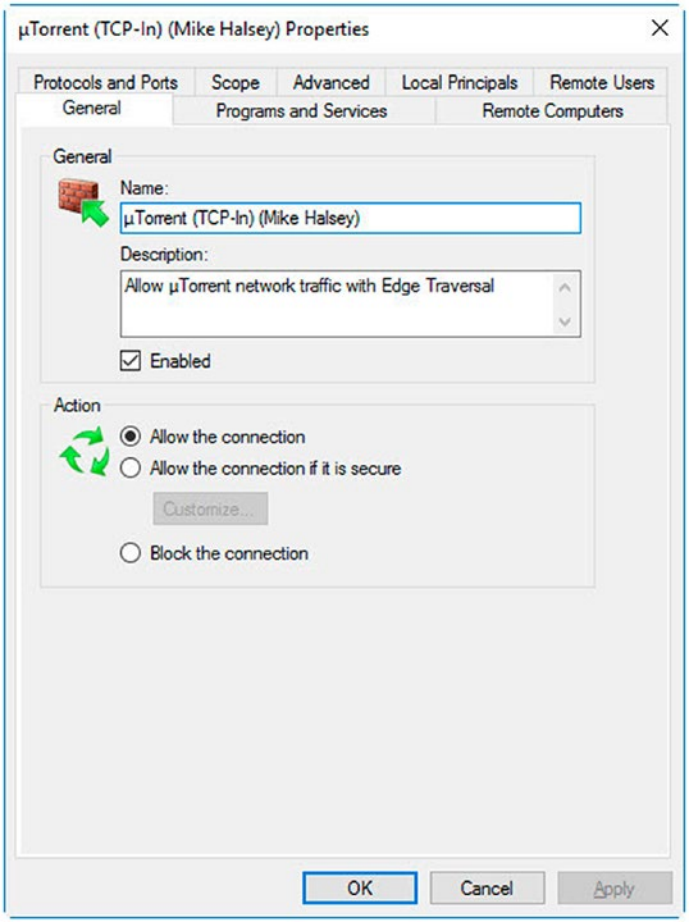


Figure 21-13. *You can change the properties for any rule*

In the rule properties panel, you can view and manage the following aspects of the rule:

- **Action** is used to allow or block the connection, or to only allow it if you have a secure network connection, such as a VPN.
- **Programs and Services** lets you define which apps, Application Packages (which include Store apps), and Services the rule applies to.
- **Remote Computers** allows you to define rules that will allow remote connections only from specific PCs, or that will not apply if a specific PC is connected. These can be useful for managing strong security during Remote Desktop sessions.
- **Protocols and Ports** is where you can set the communications protocol type (such as TCP, IPv6, etc.) and communications ports to which the rule applies.
- **Scope** allows you to limit access through the rule to specific IP addresses or an IP address range.
- **Advanced** is where you can specify if the rule applies to each of domain, private, and public network connection types, and where other options that don't fall into other categories reside.
- **Local Principals/Remote Users** are similar to the Remote Computers options, except that it allows you to restrict access to specific local and remote users.

The Connection Security rules are to determine security policies when using network and Internet connections that need to be tightly controlled; see Figure 21-14. These include Tunnel (VPN) connections, direct server-to-server communications, and where authentication between the different computers can be overridden.

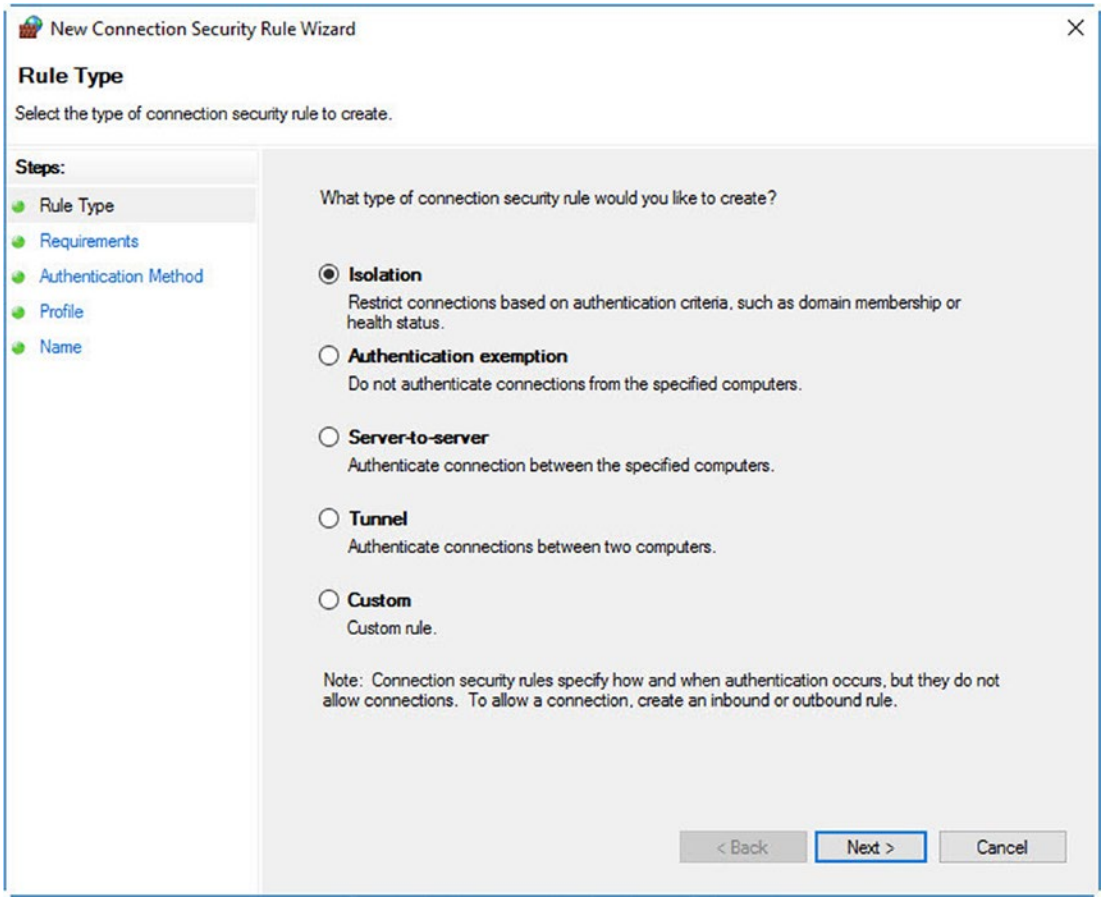


Figure 21-14. *You can set Connection Security rules*

Summary

Creating a bomb-proof PC system isn't limited to what I have described in this chapter, as you will also need to ensure you have a full system image backup of your PC that can be restored if required, and that you keep copies of your Windows image (ISO) installation file and all hardware drivers for your PCs safe and in multiple locations to cover you in the case of data loss.

Following this advice and setting appropriate levels of security, however, can really help you to prevent problems that can compromise your PCs and your network from occurring in the first instance. Remember that everything is connected to everything else, and thus, if your PC can see other PCs and storage systems on the network, it is a potential weak point of entry to those other systems.

Sometimes, however, we need much more detailed information when we're diagnosing and repairing PC problems. In the next chapter, we'll look in depth at the excellent Microsoft Sysinternals suite, and the programs it includes that can aid with troubleshooting a Windows 10 PC.

CHAPTER 22

Microsoft Sysinternals Suite

Nothing says you're an IT pro better than a good knowledge of Microsoft's Sysinternals suite. First developed by Bryce Cogswell and Mark Russinovich in 1996, it was bought 10 years later by Microsoft, for whom Russinovich now works as a senior technical fellow and sits as part of Microsoft's TechNet website. You can find Sysinternals on the Microsoft website at https://docs.microsoft.com/sysinternals/.

It consists of a suite of stand-alone apps that perform various configuration, diagnostic, and repair tasks within the Windows OS, some of which have almost become legendary. Rather than let the tools sit and stagnate, Sysinternals is an active Microsoft project, being updated on a regular basis with upgrades and new tools.

There are currently, as I write this, a massive 73 tools and utilities available as part of Sysinternals, plus additional copies for the ARM version of Windows 10 and for Windows 10 IoT (Internet of Things) Nano Server. I won't write about how to use them all here, as that would be a book on its own, but instead I'll focus on the tools available that can be specifically used to diagnose, troubleshoot, and repair problems with PCs.

Some of the tools I will highlight in detail. This is because these will be tools that can directly benefit troubleshooting. Others I will just reference as they are primarily configuration tools yet can be useful when troubleshooting problems. This may mean I don't include all the commands available for a tool, but all of this information is available on the Sysinternals website.

File and Disk Utilities

The file and disk utilities within Sysinternals will provide a wide range of functions, from helping configure PCs systems to helping you view and check the configuration options you have already made.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_22

AccessChk and AccessChk64

The first tool to detail falls into the "useful for checking if permissions are configured correctly" category. AccessChk is run from the command line and can be used to check what access specific users or user groups have to files, directories, Registry keys, Services, and more. Full details of its command-line syntax can be found on the Sysinternals website; see Figure 22-1.

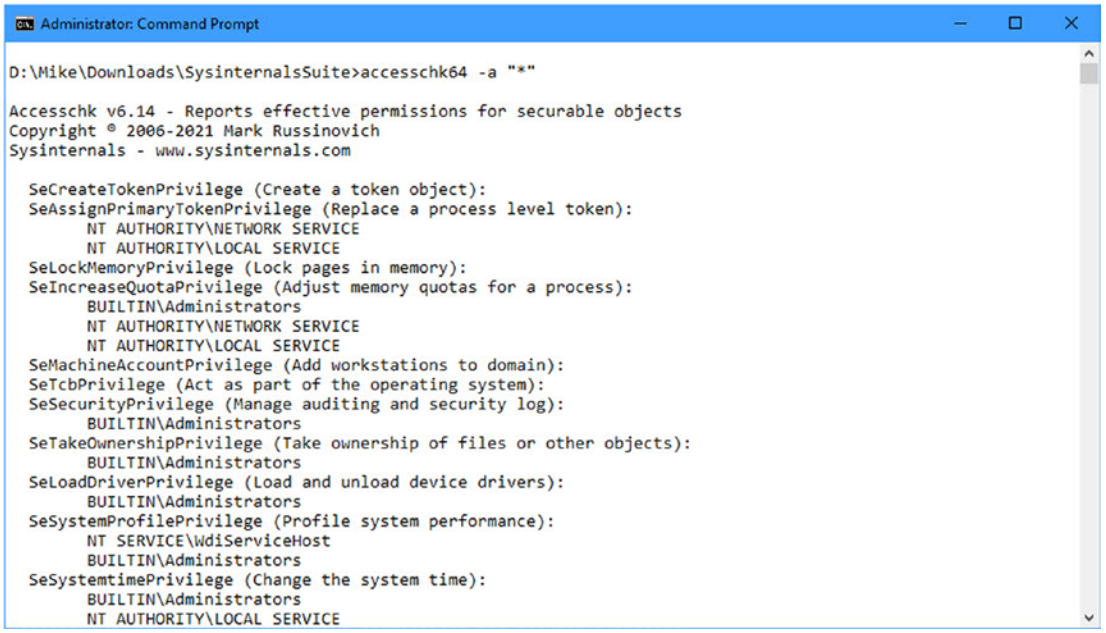


Figure 22-1. *AccessChk is used to display rights for services, processes, and accounts*

- **AccessChk[64] -a "*"** can be used to check the rights given to Windows system accounts.
- **AccessChk[64] -c "*"** will display the access rights for Windows services.
- **AccessChk[64] -h "*"** will display all the rights for printer shares on the PC.

AccessEnum

AccessEnum is a graphical utility that will allow you to view a tree view of files, directories, and Registry keys, detailing what users have read and write permissions, and what users might be denied access. It is a tool that is simple to use: you simply point it at the drive or Registry location you wish to view permissions for and click the Scan button; see Figure 22-2. The *Save* button allows you to save the results as a plain text (*.TXT) file.

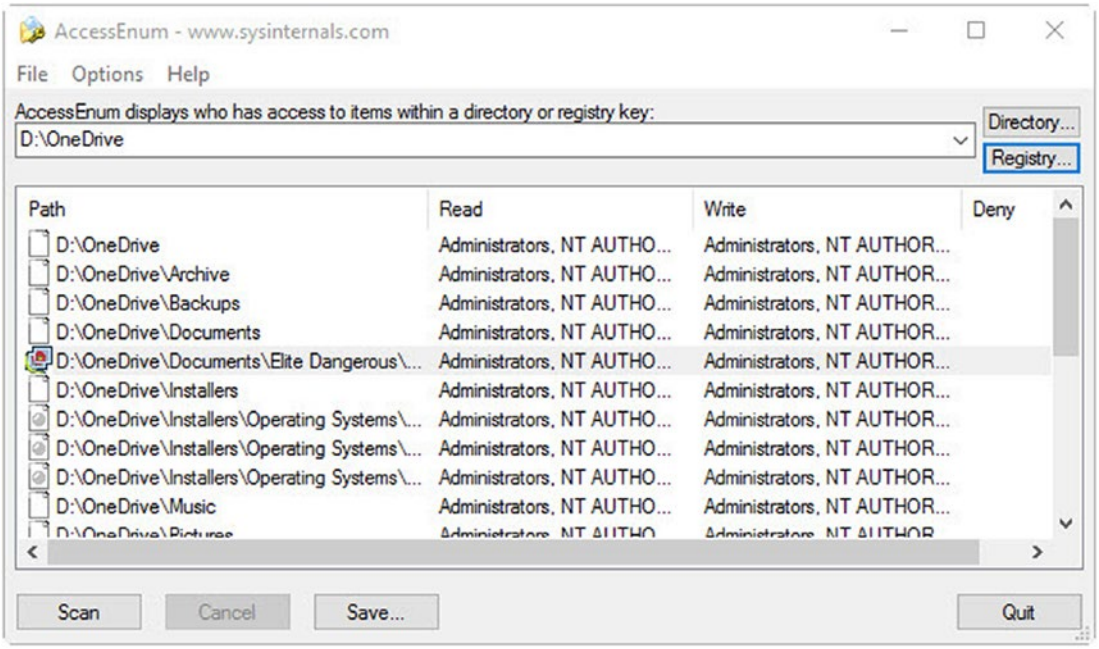


Figure 22-2. *The AccessEnum utility*

Contig

This is another Command-Line tool, and the switches are available on the Sysinternals website. While Windows 10 includes a full disk defragmentation tool, the Contig tool picks up where the defragmentation tool ends by providing file-level defragmentation. This is important because defragmenting a drive won't always defragment every file on that drive, and you may occasionally find a file being reported as corrupt where this tool may be able to help.

Disk2Vhd

Sometimes you might have a hard disk in a PC that needs deep diagnosis, or perhaps a very careful recovery of files and data. Disk2Vhd can create a virtual hard disk snapshot of any hard disk or partition on the PC, even a live system. This then resides as a file that can be examined or worked on later on another PC; moreover, the file will work with Hyper-V; see Figure 22-3.

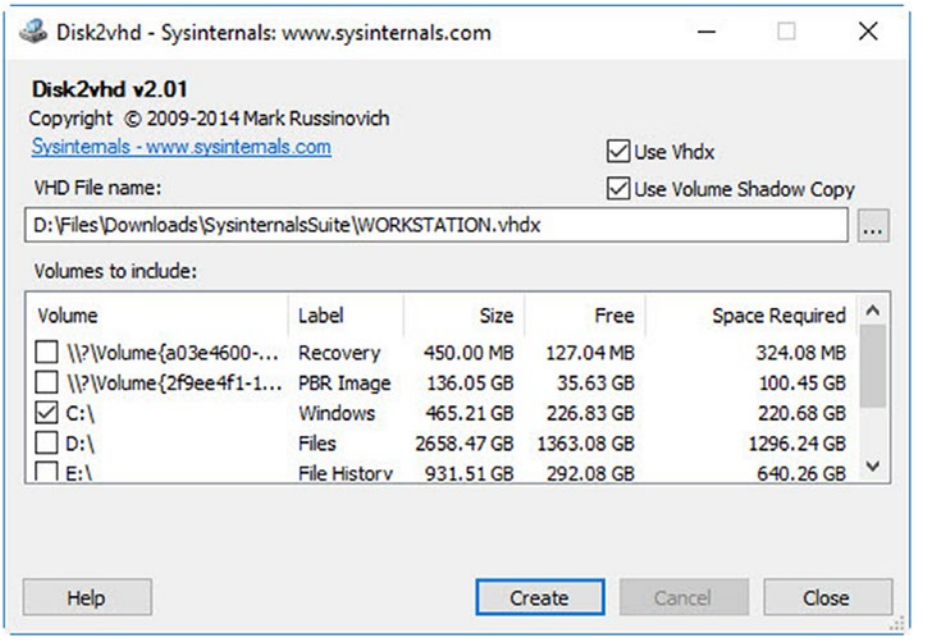


Figure 22-3. *Disk2Vhd can create VHDs from disks and partitions*

Disk2Vhd can also be useful if you have an older PC system, for example, Windows 7, that still needs to be run because of the critical processes it is for, and you want to move it to run inside of a virtual machine in Hyper-V instead of on its own PC.

DiskExt

Another Command-Line utility, this one will list the physical disks that partitions in the PC are located on, and where on those disks the partitions are located. This can be useful when diagnosing partition and RAID issues, and for checking if a partition, such as the Windows boot partition, is located on the correct disk; see Figure 22-4.

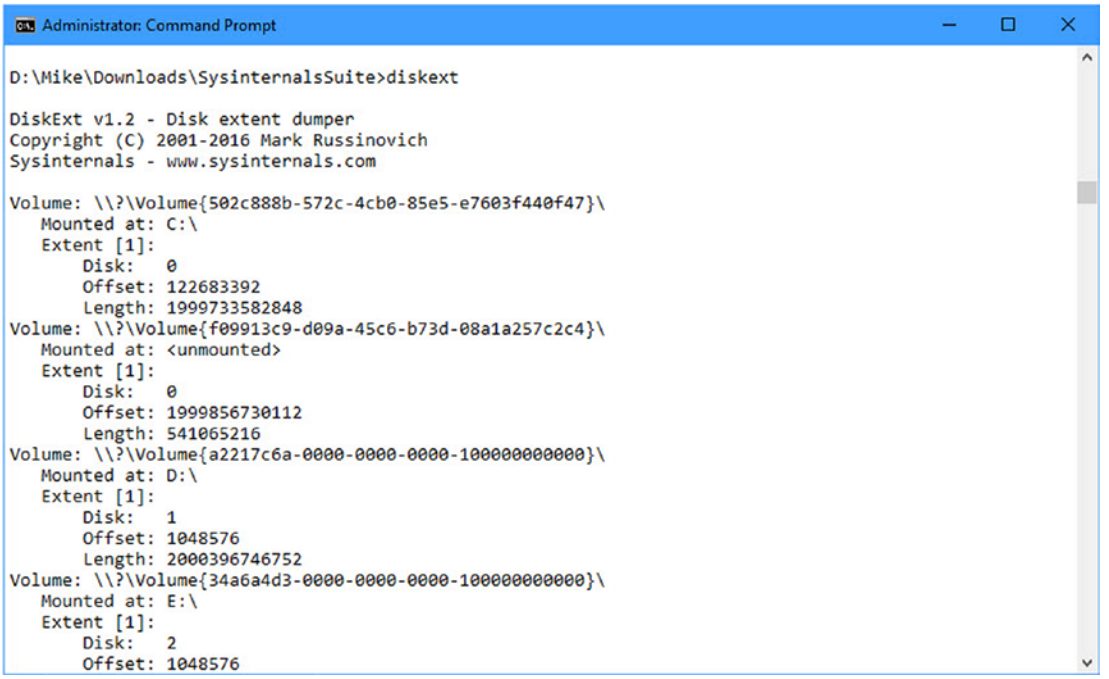
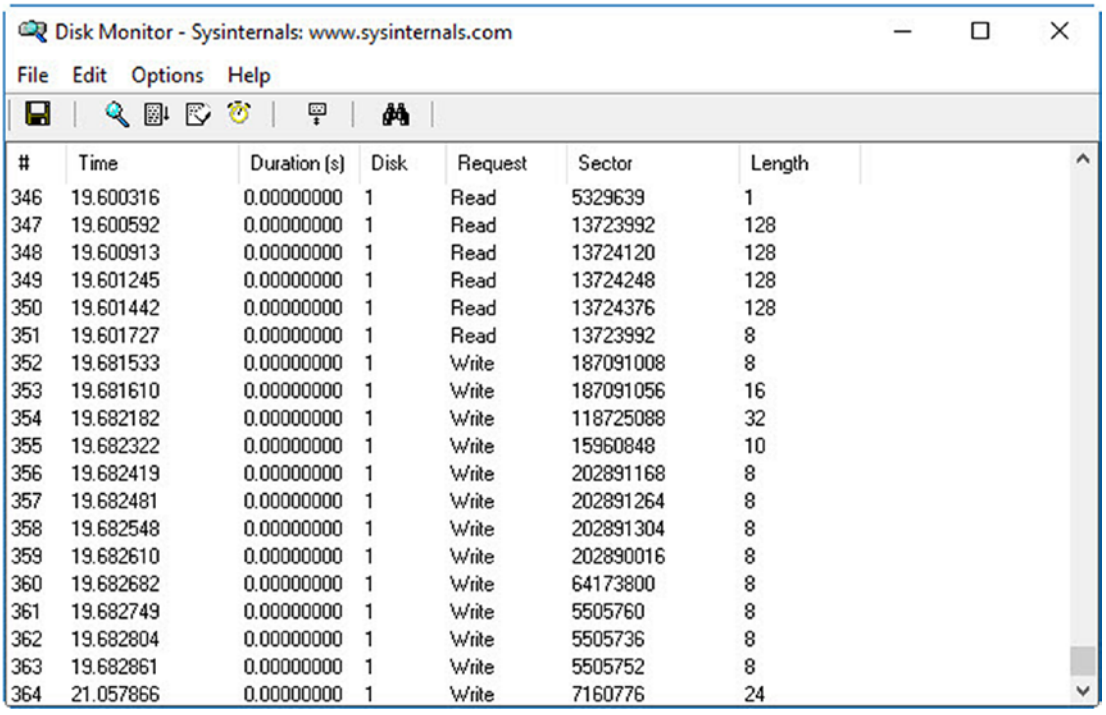


Figure 22-4. *Diskext can tell you what physical disks and partitions reside on*

Diskmon

Diskmon is the first of the majorly useful troubleshooting and diagnostic tools. Diskmon provides a live report of every read and write activity that takes place on your hard disk; see Figure 22-5. This can be useful in many circumstances. For example, you may be concerned that something on the PC is accessing disk space that it should not, such as malware. Alternatively, you may be trying to determine if a fault when accessing or saving a file resides in a bad sector on the hard disk or is a problem with the file or data itself. If there are failures to read and write files and data, these will be displayed as either multiple repeated attempts by Windows or an extended read or write duration.



#	Time	Duration (s)	Disk	Request	Sector	Length
346	19.600316	0.00000000	1	Read	5329639	1
347	19.600592	0.00000000	1	Read	13723992	128
348	19.600913	0.00000000	1	Read	13724120	128
349	19.601245	0.00000000	1	Read	13724248	128
350	19.601442	0.00000000	1	Read	13724376	128
351	19.601727	0.00000000	1	Read	13723992	8
352	19.681533	0.00000000	1	Write	187091008	8
353	19.681610	0.00000000	1	Write	187091056	16
354	19.682182	0.00000000	1	Write	118725088	32
355	19.682322	0.00000000	1	Write	15960848	10
356	19.682419	0.00000000	1	Write	202891168	8
357	19.682481	0.00000000	1	Write	202891264	8
358	19.682548	0.00000000	1	Write	202891304	8
359	19.682610	0.00000000	1	Write	202890016	8
360	19.682682	0.00000000	1	Write	64173800	8
361	19.682749	0.00000000	1	Write	5505760	8
362	19.682804	0.00000000	1	Write	5505736	8
363	19.682861	0.00000000	1	Write	5505752	8
364	21.057866	0.00000000	1	Write	7160776	24

Figure 22-5. *Diskmon reports on all hard disk activity*

DiskView

Perhaps slightly less useful for troubleshooting, but interesting all the same, DiskView can tell you where on your disk a file is physically located. This can be useful if you are diagnosing a corrupt or damaged disk or solid-state drive.

DU (Disk Usage)

This Command-Line utility will report the disk usage for any folder and/or its subfolders on a disk. This can be useful for interrogating drives where space is at a premium, and you are attempting to determine what is eating up space on the disk. Use the switches **-v** to display a verbose list of the sizes of all subfolders, and **-ct** to export the data as a tab-delimited CSV text file.

EFSDump

The Encrypting File System (EFS), which I detailed in Chapter 18, isn't like Bitlocker in that when you sign into the PC, you have access to your files. File access needs to be granted on a per-user basis through implementation of an unlock key. The EFSDump utility can display which users have access to EFS-encrypted files on a PC.

FindLinks

The FindLinks Command-Line tool will report on any hard links and the file index for a specified file. This may come in useful, for example, when finding links to a malware file on a PC; see Figure 22-6.

Figure 22-6. *FindLinks reports any hard links to a file*

MoveFile and PendMoves

These two utilities are very similar to one another and can be used to move or delete files that are currently locked because they are in use. MovieFile is used to specify files that should be moved or deleted when the next reboot takes place, and PendMoves is used to see what operations are scheduled. They are Command-Line utilities for which you use the syntax **movefile [source] [destination]** to move a file, or **movefile [source] “”** to delete the file at the next restart. Use **pendmoves** on its own to see any scheduled operations.

NTFSInfo

NTFSInfo is another Command-Line utility that can display details about an NTFS-formatted disk or partition. This includes technical information such as the allocation unit size, the location and details of key NTFS files, and information about the Master File Table; see Figure 22-7.

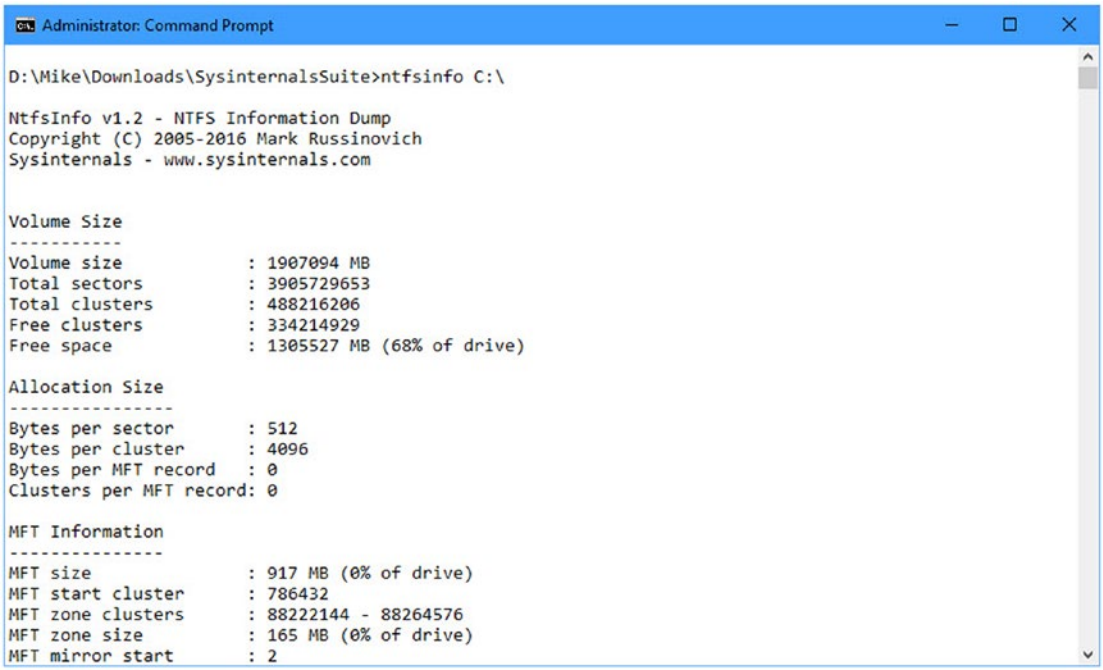


Figure 22-7. *NTFSInfo displays information about NTFS volumes on a PC*

PsFile

This is another Command-Line utility, and another utility that can provide information about files that are locked because they are open by other computers on the network. Use it on its own to see if any files are open, or with the switches **psfile [\\RemoteComputer [-u Username [-p Password]]]** to specify a specific user and remote computer, and with the switches **psfile [\\RemoteComputer [-u Username [-p Password]]] [[id | path]** [**-c]]** to close a remotely locked file.

SDelete

SDelete is included here only because it's a useful tool to know about. It's a Command-Line utility that can be used to securely delete files on a PC. It was created to assist with deleting EFS-encrypted files, where space is not quickly overwritten afterward by new data. Use with the switches **-c** to force the cleaning of free space, and **[-p passes]** to specify the number of overwrite passes.

ShareEnum

ShareEnum can be used to identify all file shares available on a network. This tool can be useful for helping diagnose problems with network file shares on a PC, to determine if the PC can actually see the share, or if it is a misconfigured app or firewall setting that is blocking access.

Sigcheck

The sigcheck utility will report on the file version number, timestamp, digital signature, and certificate details of any file on the PC. It is a Command-Line utility that can be useful if you believe that a specific system or other file has become corrupt or has been tampered with.

Networking Utilities

When it comes to troubleshooting problems on a PC, networking is right up at the top of the list of problem areas. This is because if we can't get access to our network files and resources, access to the Internet or, heaven forbid… social media, the world comes to an abrupt and shuddering halt. For anybody not interested at that point in something called the "front door," the Sysinternals suite includes some useful network troubleshooting tools.

ADExplorer

Active Directory Explorer (ADExplorer) allows you to easily view and edit an Active Directory database, including additional functionality not normally available including making a copy of the database and comparing two AD databases side by side.

ADInsight

ADInsight is a Lightweight Directory Access Protocol (LDAP) real-time monitoring tool that you can use to troubleshoot Active Directory client applications. You can use it to view processes and events that applications make to the Wldap32.dll library.

ADRestore

ADRestore exists to help you undelete "tombstoned" Active Directory objects in a domain. The utility enumerates the deleted objects in a domain and allows to restore the ones you choose.

PsTools

Rather than being a utility, PsTools is actually an extra suite of utilities for administering PC systems remotely. It includes utilities that can remotely execute apps, display information about files and users, kill processes detailed information about processes, and shutdown and restart the PC. Full details of the tools available and their switches can be found on the Sysinternals website.

PsExec

This command is used to execute processes on a remote PC. Use this in the format P**sExec** \\RemotePC **"C:\\long app name.exe"**.

PsFile

PsFile, also detailed earlier in this chapter, will display a list of files that are currently open on a remote PC. Use it in the format **PsFile [\\RemotePC [-u OptionalUsername [-p UsePassword]]] [[id | PathAndNameOfFile] [-c** ToCloseFile**]**.

PsGetSid

This tool is used to display the Security Identifier (SID) of a remote computer or user. Use it in the format **psgetsid [\\RemotePC[,RemotePC[,...] | @file\] [-u OptionalUsername [-p UserPassword]]] [account|SID]**.

PsInfo

PsInfo can display information about a remote computer. You can use this with the switch **Re**motePC for a specific PC, or * to run it on all networked PCs. You can also use it with these switches to get detailed information on **[-h]** installed hotfixes, **[-s]** installed applications **[-d]** disk information, and use **[-c]** to export the data as a CSV file.

PsPing

PsPing does exactly what you might expect it to: it displays detailed ping information to test network connections. It is a Command-Line utility that is much more configurable than Windows 10's standard `Ping` command. PsPing is used with one of the four main switches and then a series of subswitches to test for ICMP (the main protocol used by routers for reporting errors), TCP, latency, and bandwidth. Full details of the switches are available on the Sysinternals website.

PsKill

If you need to kill a running process on a remote PC, then PsKill is the tool to use. Use it in the format **pskill [-] [-t] [\\RemotePC [-OptionalUsername [-p UserPassword]]] <processname | process id>** where **[-]** displays a list of supported options, and **[-t]** kills not just the process but all its dependent processes as well.

PsList

PsList will display detailed information about the processes running on a remote PC. Use with the switches **[-d]** to display additional details, **[-m]** to show memory usage information, and **[-t]** to show process trees.

PsLoggedOn

This tool will display details of each user currently logged on (signed in) to a remote PC. This can be used with the switch **[-l]** to only show accounts logged into the PC locally, and not across the network.

PsLogList

This is used to create a dump of event lot records from a remote PC. There are quite a few switches and commands for this utility which you can see in Table 22-1. You use it in the format psloglist [-] **[\\RemotePC[,RemotePC[,...] | @file [-u OptionalUsername [-p UserPassword]]] [-s [-t delimiter]] [-m #|-n #|-h #|-d #|-w][-c][-x][-r][-a mm/dd/yy] [-b mm/dd/yy][-f filter] [-i ID[,ID[,...] | -e ID[,ID[,...]]] [-o event source[,event source] [,..]]] [-q event source[,event source][,..]]] [-l event log file]** <**eventlog**>.

Table 22-1. *Available switches for PsLogList*

Switch	Description
@file	Execute the command on each of the PCs specified
-a	Export the records timestamped after a specified date
-b	Export the records timestamped before a specified date
-c	Clear the event log after displaying its contents
-d	Only display records from previous *n* days
-e	Exclude events with the specified ID or IDs (up to 10)
-f	Filter event types with a string (e.g., [**-f w]** to filter warnings)
-h	Only display records from previous *n* hours
-i	Show only events with the specified ID or IDs (up to 10)
-l	Exports records from the specified event log file
-m	Only display records from previous *n* minutes
-n	Only display the number of most recent entries (e.g., **[-n 6])**
-o	Show only records from the specified event source
-p	Specifies optional password for username. You will be prompted for a password if you omit this
-q	Omit records from the specified event source or sources
-r	SDump log from least recent to most recent
-s	Displays Event Log records one-per-line, with comma-delimited fields

(*continued*)

Table 22-1. (*continued*)

Switch	Description
-t	Changes the delimiter to a specified character
-u	Specifies an optional username for login to remote computer
-w	Tells PsLogList to wait for new events, exporting them as they generate (on the local PC only)
-x	Dump extended data
@file	Execute the command specified on each of the PCs specified

PsPasswd

This security tool can be used to change account passwords on a remote PC. Use it in the format **pspasswd [[\\RemotePC[,RemotePC[,..] | @file [-u Username [-p Password]]] Username [NewPassword]**.

PsService

It lets you view and control services on a remote PC. Use it in the format **psservice [\\RemotePC [-u OptionalUsername] [-p UserPassword]] <command> <options>** where the options include those listed in Table 22-2.

Table 22-2. *Switches for the PsService command*

Switch	Description
query	Displays the status of a specified service
config	Displays the configuration of a specified service
setconfig	Sets the start type for a specified service (disabled, auto, on-demand)
start	Starts the specified service
stop	Stops the specified service
restart	Stops and then restarts a specified service
pause	Pauses the specified service

(*continued*)

Table 22-1. (*continued*)

Switch	Description
cont	Resumes a paused specified service
depend	Lists all of the services that are dependent on the one specified
security	Dumps the specified service's security descriptor
find	Searches the network for the specified service

PsShutdown

PsShutdown can be used to either shut down or restart a remote PC. This can be used with the following useful switches **[-f]** to force all applications to close immediately rather than giving them time to close on their own; **[-l]** to lock the remote PC; **[-m]** to display a message to appear on the screen for anybody using the PC when the shutdown countdown commences, which can be set with the **[-t xx]** switch, the default being 20 seconds; **[-r]** to restart the PC; and **[-c]** to allow the shutdown to be aborted by somebody still using the remote PC.

PsSuspend

If you need to suspend a process on a remote PC, then this tool will do the job. Use it in the format **pssuspend [-] [-r] [\\RemotePC [-u OptionalUsername] [-p UserPassword]] <process name | process id>** where **[-r]** resumes the suspended processes after they have been previously suspended.

TCPView

The TCPView utility provides information about the endpoint network connections from your PC, including the remote or IP address of the destination and the port used by the PC to make the connection; see Figure 22-8. Using this utility, you can see every running process and service that has an active network connection, and the destination they are connected to.

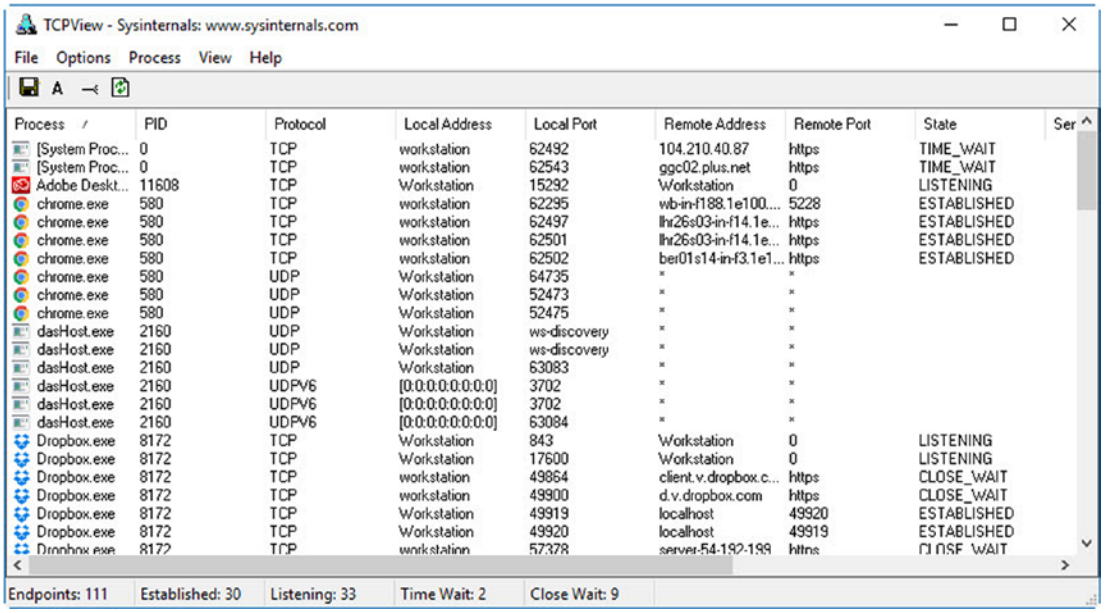


Figure 22-8. *TCPView provides useful endpoint information*

You can marry this information with the data you have on IP address ranges within your company, or company VPN, to check for misconfigured network connections, or to see where malware or rogue apps might be making connections. You can also save the data as a file to read later or to send to a support technician.

There is also a Command-Line version of this tool available in Sysinternals, called **TCPVcon** which is used in the format **TcpVcon [-a] [-c] [-n] [process name or PID]** where **[-a]** displays all endpoints, **[-n]** doesn't resolve addresses, and **[-c]** outputs the results as a CSV file.

WhoIs

WhoIs is useful for providing information on who owns and maintains domain names or IP addresses to which your PC is connecting. For example, in running TCPView, I spotted that Google Chrome on my PC was connecting to the IP address `216.58.198.206` and wanted to see what company was at the end of this address. A quick search using WhoIs reveals that the connection was being made by the browser to the company MarkMonitor, which is known to be trustworthy; see Figure 22-9.

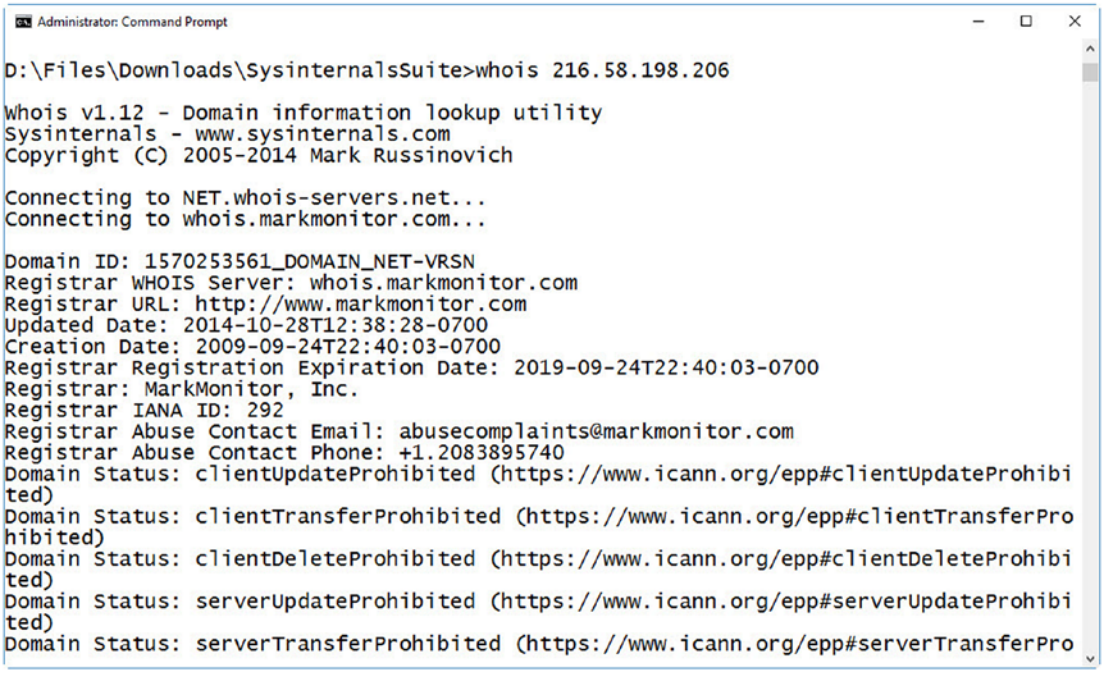


Figure 22-9. *WhoIs can provide information on IP addresses you connect to*

Process Utilities

Knowing what's going on inside your PC at any one time is essential to effective troubleshooting. Perhaps you have a hung process you need to root out, or malware that restarts every time you shut it down, because there's a dependent process running in the background that has yet to be identified. The process utilities in the Sysinternals suite are powerful, flexible, and almost always completely indispensable.

AutoRuns

There are a few utilities in Sysinternals that can be considered "the daddy," and AutoRuns is most definitely one of them. Seen in Figure 22-10, it goes far beyond the startup apps list that Windows 10 includes in the Task Manager, to show absolutely everything that starts when you switch on your PC.

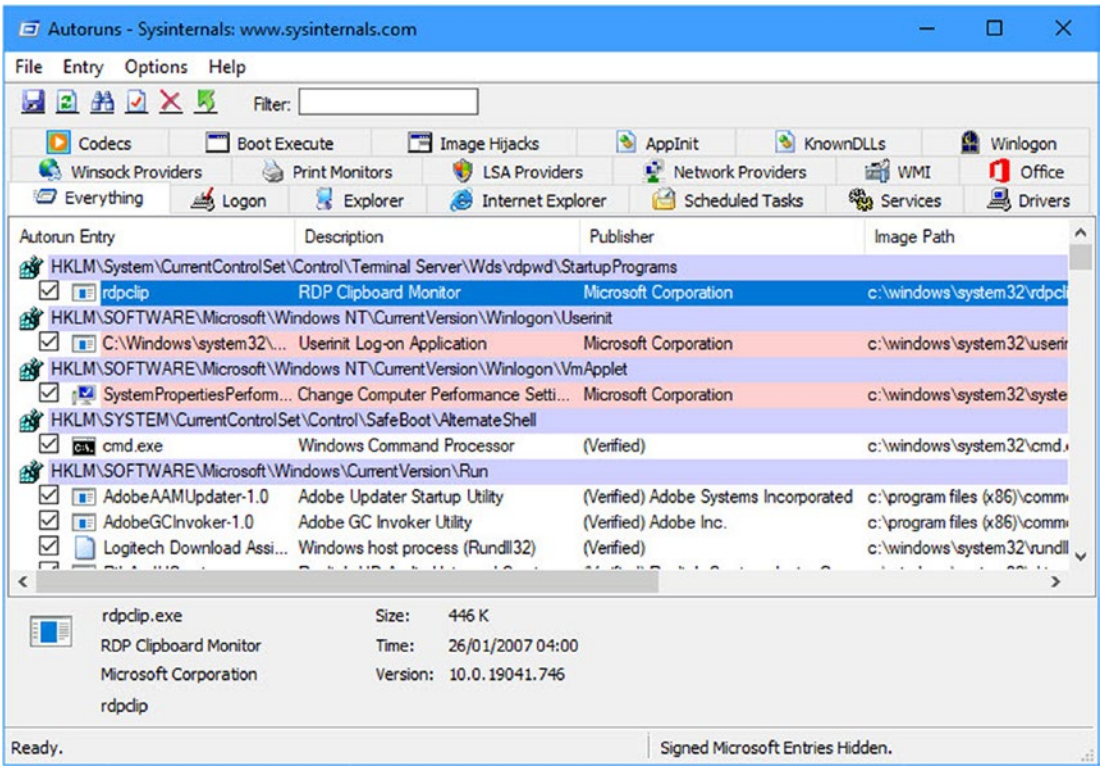


Figure 22-10. *The AutoRuns utility; the daddy of startup managers*

The information available in AutoRuns is at the far end of detailed, and every single item comes with a handy check box, enabling you to quickly disable anything that's causing a problem, or that you don't want running on the system. Remember that you can use AutoRuns to reenable anything afterward.

The list of things that you might want to disable using AutoRuns is extensive and includes (but is by no means limited to) malware, unwanted or problematic audio and video codecs, software that hasn't been uninstalled properly or for which the startup entries remain on the system, crapware (the term used to define all the useless apps and utilities that come bundled with new PCs), Registry keys that are associated with startup items, apps that hijack Windows functions such as ISO disk image handling or screen capture, dynamic link libraries (DLLs) that the system can no longer find, web browser plug-ins, tasks that have been set to run automatically at startup, third-party and other Windows Services, faulty drivers or drivers that cannot be found or that were incorrectly uninstalled, Registry keys that lead nowhere and that are causing errors, etc.; the list just goes on. AutoRuns is just an amazing little utility.

The Options menu allows you to hide and unhide both known Microsoft and Windows entries, if you just want to see what third-party software is doing at startup on the PC. Additionally, many items in Autoruns are color-coded as follows:

- **Yellow** where a startup entry exists, but Autoruns cannot find the installed program on your PC.
- **Green** where the entry was added recently since the last time you used Autoruns.
- **Pink** where no known publisher information exists, either because the entry is not digitally signed or because no publisher information has been included with the process.
- **Purple** is the Registry address of the entry.

Handle

Earlier in this chapter, I showed you some Sysinternals utilities for dealing with locked files. Handle is a Command-Line utility that can provide details of which app has opened and locked a particular file or director on your PC. Use it in the format **Handle <filename>** with additional switches, which are detailed on the Sysinternals website being useful, such as **[-u]** to show the username of the person with the open file.

ListDLLs

DLLs are files that are an essential part of Windows 10, or provided by third-party software companies, which enable apps to share functions on the PC. Back in the days of DOS, every running program had to provide its own way of managing everything, and I remember the excellent WordPerfect 5.1 word processor coming with a battery of disks that contained its own printer drivers.

DLLs took all this pain away, but knowing what's running can be impossible without the use of a utility such as ListDLLs. This is a Command-Line utility (with switches available on the Sysinternals website) that can list all the DLLs that have been loaded by an app or process, or to list all the processes that are accessing a particular DLL. Should you find, for example, that an app, process, or DLL is crashing, you can use this tool to see if the DLLs in use have any other dependencies which may be causing the problem.

You can use it in the format **ListDLLs [processname]** to see what DLLs are in use by a specific process, or in the format **ListDLLs [-d DLLname]** to see what running processes are using a specific DLL. Other useful switches, which are available on the Sysinternals website, include **[-u]** which will display only unsigned DLLs and **[-v]** which will display DLL version information.

Portmon

If you are using a PC system to which Serial or Parallel devices are attached, and they're still more common than you might think, then the Portmon utility can display all the activities for those ports. This includes successful and failed communications and the process using each port. This information can be useful in tracking down communication problems between the PC and attached devices.

ProcDump

ProcDump is a Command-Line utility with two uses. The first of these is for monitoring an app for CPU processor spikes and reporting when a spike occurs. If you have an app that is periodically, or even regularly, using huge amounts of processor time, then ProcDump can provide valuable information about what it's doing at the time.

The second use for ProcDump is to monitor apps when they are hung. Sometimes you may encounter an app for which the window appears to temporarily crash. This is because the app is doing or trying to do something in the background and cannot proceed until that task is complete. In this circumstance, ProcDump can provide information on what is occurring with that app at the time. Full details of the very many switches available to use with ProcDump are available on the Sysinternals website.

In its basic format however, use it as **ProcDump winword.exe** (see Figure 22-11), and it will produce its output in a .DMP file. This can be read using Microsoft Visual Studio, the Windows Driver Kit (WDK), or Windows Software Development kit (SDK), but a search online will reveal other free .dmp file readers.

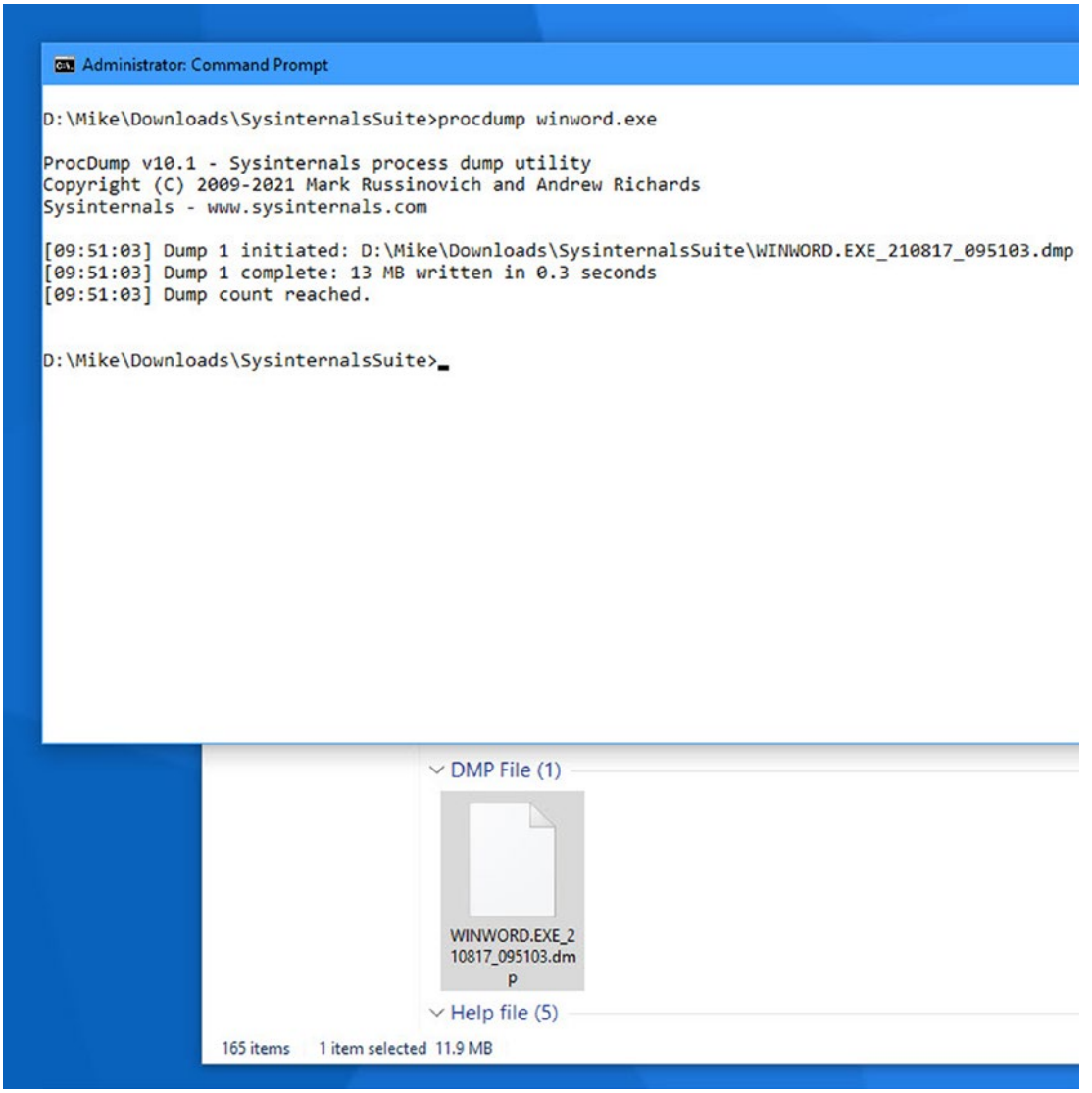


Figure 22-11. *ProcDump will tell you what a hung process is doing*

Process Explorer

I mentioned earlier that Sysinternals had more than one "daddy" in its arsenal, and Process Explorer is another. It's great if you really want to know what's going on in your PC; what app has opened a particular file or folder; what DLLs are being used by an app; how much CPU time an app is taking; how much memory it's using; what network

bandwidth it's using; whether it's being run in a secure, virtualized environment, or not; what permissions each user or user group has over the app; if there is a DLL version problem with an app; and more besides. All of this can be gained from a simple and easy-to-understand interface; see Figure 22-12.

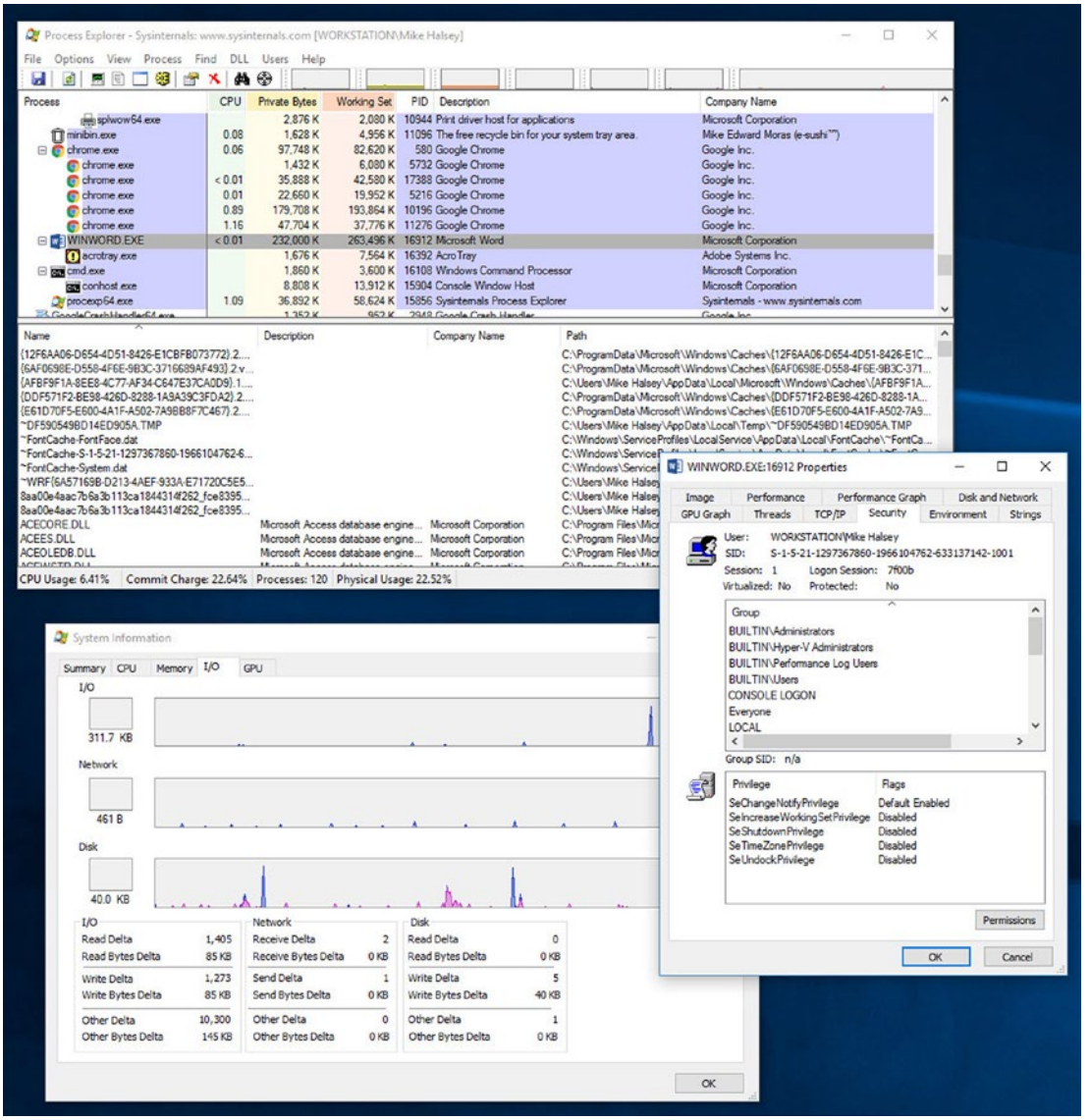


Figure 22-12. *Process Explorer provides more information on running apps than you can believe*

From Process Explorer you can kill processes, or entire process trees, which include all the dependencies for a process. You can suspend processes so problems can be investigated without the process actually being shut down, restart them, find information about installed DLLs, submit suspect app samples for virus testing, disconnect and send messages to other users who are using resources on the PC, and also find all the Registry entries associated with a process or app on the PC.

Tip Sometimes Process Explorer can fail to run, reporting an "*Unable to extract 64-bit image. Run Process Explorer from a writeable directory*" error. Should you encounter this, navigate to your AppData\Local\Temp folder by typing **%tmp%** into the Start menu or the breadcrumb bar in File Explorer, right-click the `procexp64` app, and run it as an Administrator from there.

Different processes in Process Explorer are color-coded to help you identify them more easily. These color-codings work as follows:

- **Purple** processes, which in our case include the malware, are files that may be compressed (also called packed) which for legitimate applications can help them to use less memory, but in the case of malware can also help to hide the code from your antimalware scanner. Looking at the purple-colored files should be your first step.
- **Red** processes are ones that are currently existing (being stopped).
- **Green** processes have been freshly run (also known as spawned).
- **Light blue** processes are those run by the same account that started Process Explorer.
- **Dark blue** processes are ones that have currently been selected by yourself in Process Explorer.
- **Pink** processes are running Services on the PC, such as the common *svchost.exe* which is a Windows system process that can host one or more other services where they share a process to reduce overall resource usage on a PC.

Process Monitor

If there are any other utilities in the Sysinternals suite that stand head and shoulders above the rest, and that are constantly used and referenced by system administrators and IT pros, then Process Monitor will definitely be one; see Figure 22-13.

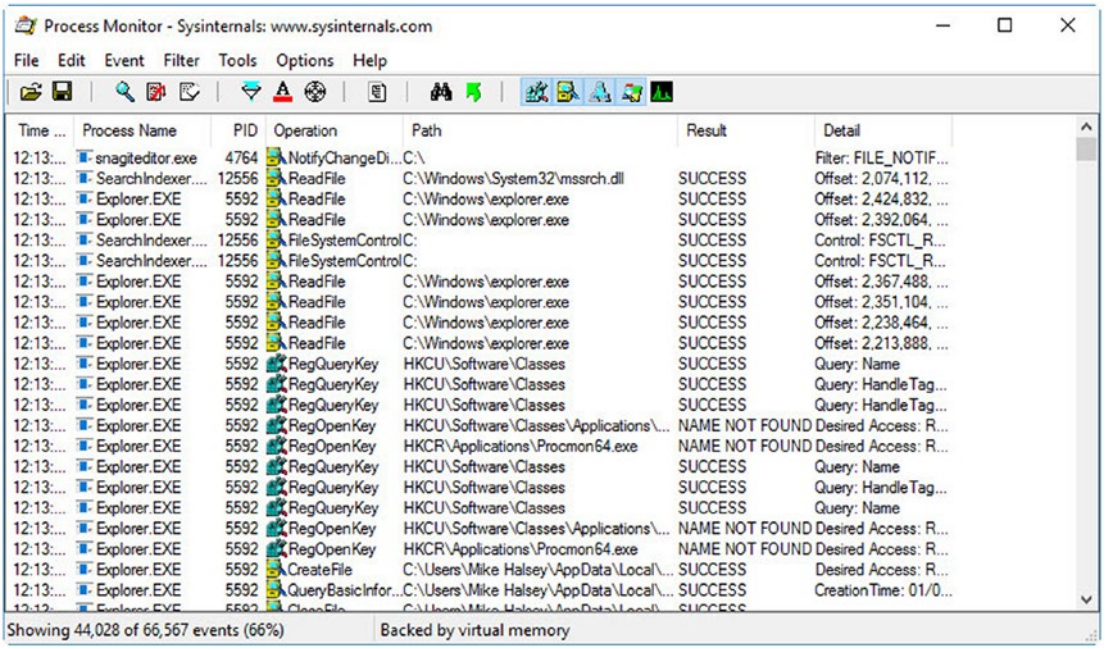


Figure 22-13. *Process Monitor details everything running on the PC*

This wonderful little utility is so incredibly useful when diagnosing and troubleshooting many types of problems on a PC, including hung apps and app dependencies, malware infections, misconfigured software, deleted files and Registry keys, and more besides.

Process Monitor details, in real time, every running process and service on the PC, with information about every operation they are performing, every Registry key they have open or have access to, and whether the actions they are taking are successful or are reporting an error.

Perhaps you are looking for the dependencies for malware that has infected a PC. You can use Process Monitor to identify all of the Services, DLLs, and Registry keys associated with the core malware app. You can also use Process Monitor to check the dependencies for any running app on the PC, to see what files and keys are associated

with it. All of this information can come in handy when diagnosing problems with apps and Windows features, because you can see at a glance what's happening, if the tasks performed have been successful or not, or if essential Registry keys, DLLs, or Services are missing or reporting an error.

Additionally, you can filter the view to narrow the information displayed to a subset of the full available information. If a file is locked on the PC and unable to be deleted, moved, copied, or even opened, you can also see what process is currently using and has locked the file, so that the process can be closed or terminated. Perhaps most usefully, you can set Process Monitor to record every operation at boot time, and this data can then be exported to be read later in a variety of formats, including CSV and XML files.

ShellRunas

ShellRunas is another Command-Line utility, but one that allows you to launch an app or process under the sign-in credentials of a user other than the one who is already signed into the PC. Use it in the format **ShellRunAs /reg** to add this functionality to the *right-click* context menu in File Explorer with more switches available on the Sysinternals website.

VMMap

PCs don't just hold running apps and processes in memory; they also save some memory to disk in the form of virtual memory, also known as the Paging File in Windows. VMMap allows you to view the physical and virtual memory usage of a specific process; see Figure 22-14. If an app or process is hogging memory, this utility can provide detailed information on how much memory and what memory types are being used.

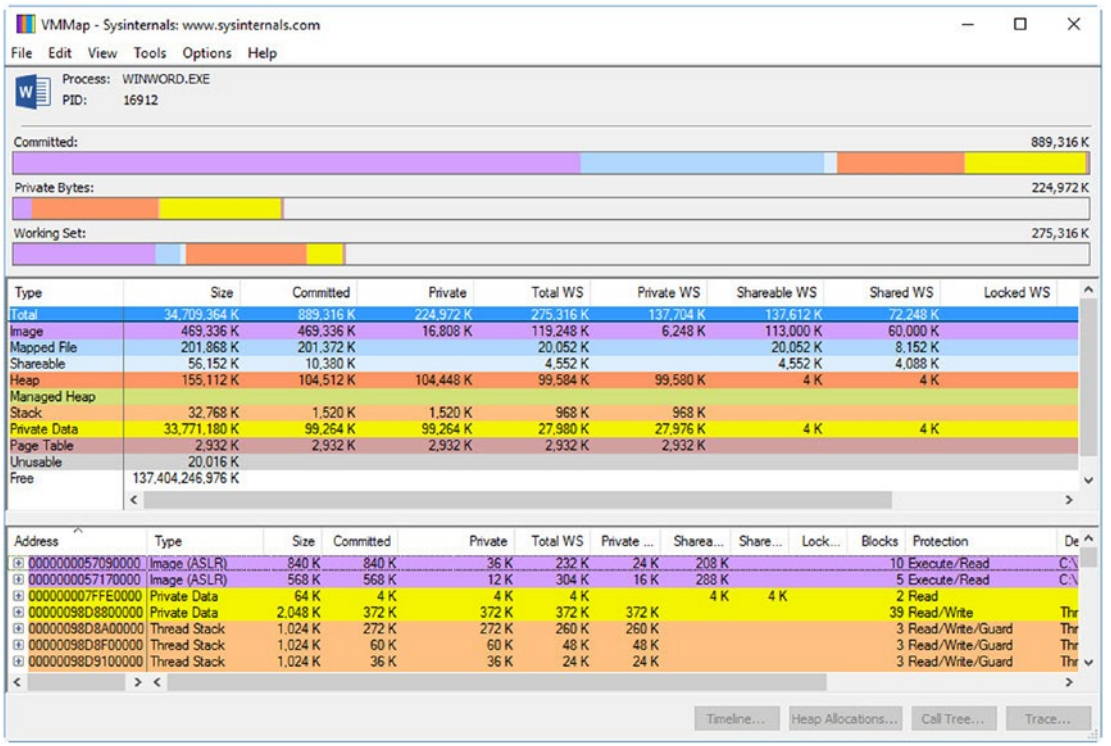


Figure 22-14. *VMMap allows you to view the memory usage for a particular process*

Security Utilities

Security is crucial to maintaining stable and reliable PCs, and to avoid data loss and malware infection. Some of the security tools available in Sysinternals, such as AccessChk and AccessEnum, have already been detailed in this chapter, but others can prove useful.

LogonSessions

LogonSessions is a Command-Line utility that will detail all of the current user sessions running on the PC. It can be used in the format **LogonSessions -ct** to automatically output the data as a tab-delimited CSV file, or it can be used with the **[-p]** switch to also list all the processes running in a logon session. Full details and syntax can be found on the Sysinternals website.

Sysmon/Sysmon64

If you suspect that a PC has been infected with malware, then Sysmon can probably help. This tool runs as a service and driver very early in the Windows boot cycle, and checks for process creation, process change, and network connection activity that could be the result of a malware or other type of infection. Once Sysmon is loaded on a PC, it runs silently in the background and reports its findings through the Event Viewer. You can find the full syntax for this Command-Line utility on the Sysinternals website, and you can view a Microsoft video on how the utility works at **http://pcs.tv/1TLl8TX**.

System Information Utilities

Many of the utilities that provide information about your system in the Sysinternals suite, such as LogonSessions and Process Explorer, have already been detailed in this chapter. There are a few, however, that don't also fall into one of the other categories. Not all of them are applicable to troubleshooting, but the following ones are.

Handle

Handle is a Command-Line utility that can report which program has a specific file or directory open. It provides all the data about a specific profess or app, and its full syntax and switches can be seen on the Sysinternals website. It can be used in a variety of ways, including **Handle windows\system** to display which processes are using files in the `C:\Windows\System32` folder; see Figure 22-15.

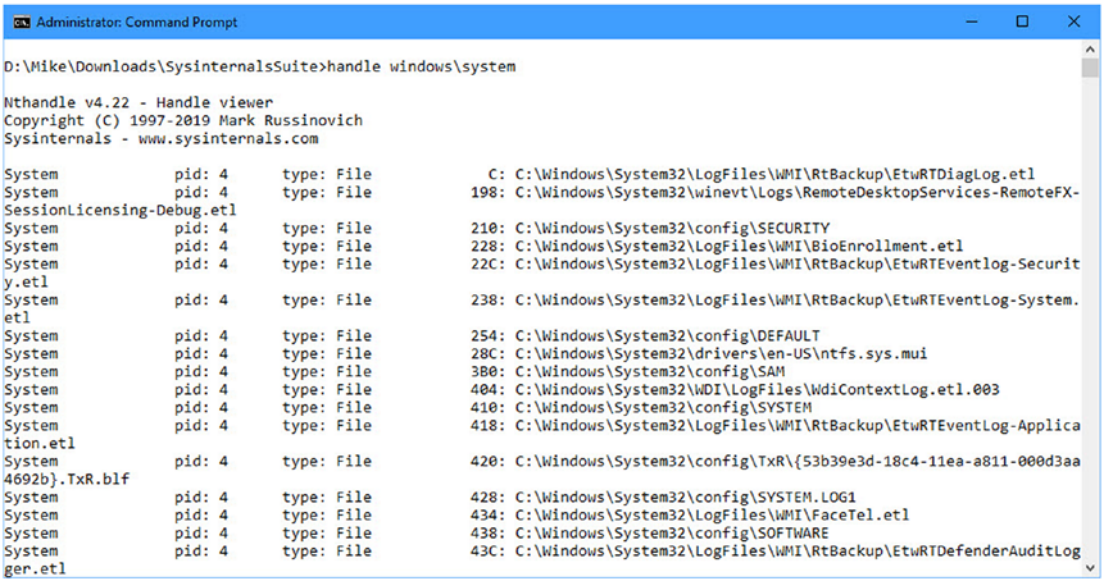


Figure 22-15. *Handle can display which processes are using which files in the System32 folder*

LiveKd

LiveKd is a Command-Line debugging tool for the Windows kernel files. It can be used on the main PC or on a Hyper-V virtual machine running on the PC and should be installed into the `\Program Files\Microsoft\Debugging Tools` directory. These tools, and full details on how to use LiveKd, can be found on the Sysinternals website.

LoadOrder

The LoadOrder utility can be used to view the order in which device drivers are loaded when a PC starts; see Figure 22-16. If a driver is failing at startup, you can see if it is loading early enough in the boot process, so any dependencies load afterward. LoadOrder can also be used to detect unwanted drivers or malware infections.

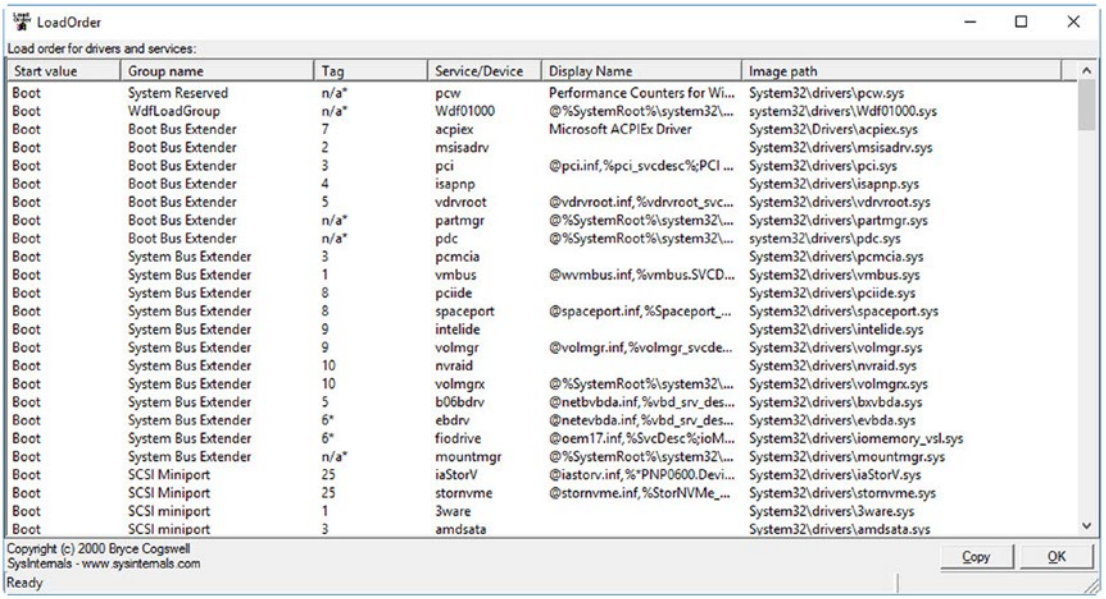


Figure 22-16. *LoadOrder displays the order in which drivers are loaded at startup*

RAMMap

This utility provides detailed graphical and technical data on memory usage on the PC; see Figure 22-17. This includes details of all apps and process memory usage, but also details of file memory usage. You can use RAMMap to see how memory is being allocated in Windows 10, so that you can analyze memory usage on the PC.

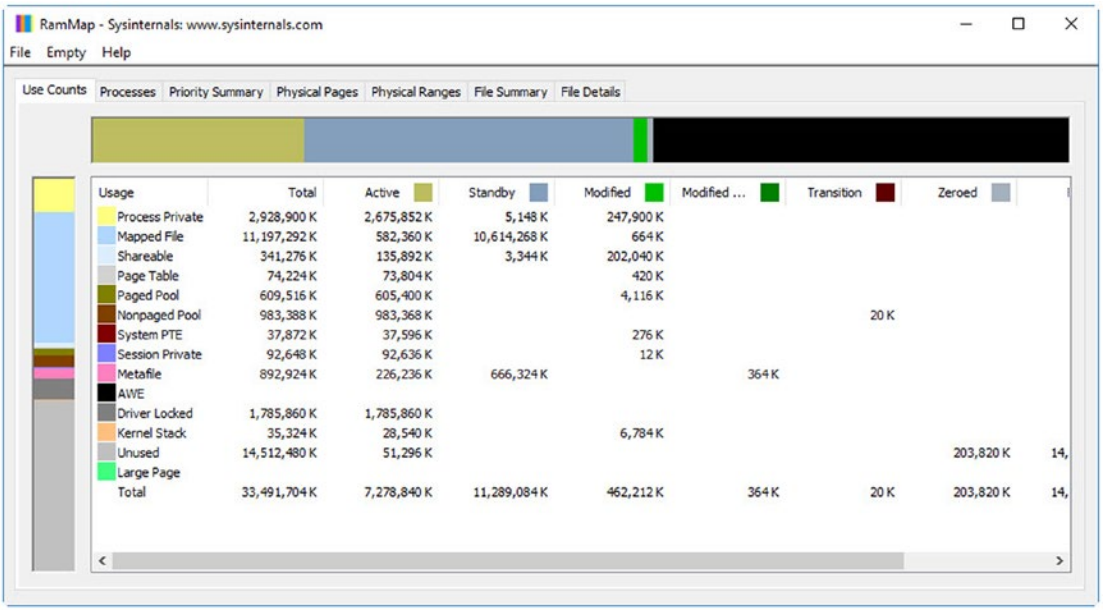


Figure 22-17. *RAMMap provides technical data on memory usage*

RAMMap provides the following useful information in its tabs across the top of the screen:

- **Use counts** is a summary of memory use by type and paging list.
- **Processes** shows memory usage by running process.
- **Priority Summary** shows prioritized standby list sizes.
- **Physical Pages** is per-page use for physical memory.
- **Physical Ranges** shows physical memory addresses that are in use.
- **File Summary** displays memory usage by file.
- **File Details** shows individual physical pages by open file.

Miscellaneous Utilities

There are a few other Sysinternals utilities that don't fall into any of the main categories, but that are useful, nonetheless. Not all of the miscellaneous Sysinternals tools are relevant to troubleshooting, but those that are follow.

RegDelNull

If you find yourself unable to delete a Registry key that you need to get rid of, perhaps to clean up an app that's not uninstalled properly, or to remove malware, and you're unable to delete the key, RegDelNull might be able to help. This Command-Line tool is used in the format **RegDelNull <RegistryKeyPath> [-s]** to delete keys that have embedded-null characters, and that are otherwise undeletable, perhaps due to a Registry corruption. The **[-s]** switch forces the command to include all subkeys in the deletion. More information is available on the Sysinternals website.

Registry Usage

This Command-Line tool provides details on the Registry space usage for the key you specify. Its full syntax and the switches you can use with it can be found on the Sysinternals website.

RegJump

RegJump is a very handy little Command-Line utility to use, and is made even more useful in Windows 10, now that the Command Line fully supports cut and paste. It will force the Registry Editor to open at the key you specify, saving time having to scroll through the Registry Editor, opening paths as you go. It can be used in the format **RegJump <RegistryPathName>**, or in the format **regjump -c**, which will automatically copy the Registry Address from the Windows clipboard.

Summary

Microsoft's Sysinternals suite is so useful, and so packed full of utilities, that I could never have hoped to fit all the information on how to use it for troubleshooting into anything smaller than its own book. There are many additional tools and utilities that I've not included here, but that are useful for administrating PCs. Again, you can download the Sysinternals tools and get full documentation from the Microsoft website at `https://technet.microsoft.com/Sysinternals`.

Now seems like a good time though to bring the focus back to the best way to protect PCs so that complex tools like Sysinternals don't need to be used, or where their use can be minimized. In the next chapter then, we'll look at best practices for setting up, maintaining, and using PCs in the workplace.

CHAPTER 23

Best Practice in the Workplace

Much of the preventative work you can do, to help make sure problems with PCs don't occur, or at least occur infrequently, comes down to best practice methodology. In the business space, this is doubly important as, whether you have six or six thousand PCs to support, troubleshooting and repair are complex and time-consuming processes. Either you've got to invest time in diagnosing the cause of a problem so that you can implement a fix or you reimage a machine and the user then has to wait some time for all the most recent updates and patches to be installed.

But what is best practice when it comes to making sure your PCs work in a worry- and trouble-free way? Simply put, it's a common-sense approach to your work that not only helps you get things done more quickly and effectively when deploying and maintaining PCs but that can also help the user. Indeed, some of the ideas and suggestions I'll put forward in this chapter (and you'll also have your own ideas) can save battery power, keep users working longer, and help them to be more productive in the mix.

Education, Information, Cooperation!

I've said previously in this book that nothing ever happens on a PC without a human being involved, as these machines simply can't go wrong on their own (unless Boston Dynamics becomes involved, when they'll likely make a PC able to take itself out of the box). It is therefore completely crucial that the people using your computers know what the deal is as regards using the equipment safely and properly.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_23

What this doesn't mean is coming down all Genghis Khan on them (not that Genghis Khan had a lot of IT issues to deal with) and being very strict about the long list of things they must never do. You'll find that many of the problems that occur simply aren't the fault of the end user. Let's take the example of malware, ransomware, and data theft.

Malware and ransomware are as much an exercise in social engineering these days as it is technical expertise, or knowing how to bring down a server's security with a brute force attack. Criminals want access to our data and systems. This is becoming such a problem that even government agencies around the world have gotten in on the act with reports of companies as diverse as Boeing, Microsoft, and oil pipelines being hacked in, apparently, state-sponsored attacks.

These people can use a variety of methods to try and access your systems, from Distributed Denial-of-Service (DDoS) Attacks to seeking out flaws in your security, or in the software you're running and exploiting them. By far one of the most favored ways however is to try and coerce an employee into giving them the access they require. It's quick, cheap, and highly effective.

Criminals will often obtain the names, email addresses, and phone numbers of employees that they think can get them system access, and then call them pretending to be from IT sorting out some issue or other. They'll be very happy, chatty, and friendly, and ask the user to disclose their system password to help in the issue resolution. Once they have the password however, and unless you have a Two-Factor Authentication system in place, they'll be able to sign into the system as that user and begin creating havoc.

This isn't the end user's fault as it's exactly the same types of technique used by social media and advertising forms to get us to disclose personal information online that can be harvested for advertisers. It's also the same technique used by criminal groups on Facebook and other social networks to trick us into disclosing answers to common security questions. You might think it's innocent for a Facebook page to get people to share a meme asking what your favorite food was as a child, or where you really want to go on vacation next, but when they begin asking the name of your first pet, or where you went to school, they've got you.

Education Theory

This is where educating your workforce, and indeed your family and friends, becomes your first and very best line of defense against disaster. Never forget that while you're the IT expert, the people using your computers, or indeed their own computers and smartphones, very often have little or no technical expertise. This is okay though as these people will be expert in the gardening, cooking, creative arts, or other things you haven't got a clue about (call me on all three; Ed).

The first part of educating your workforce in best practice, and this is for both security and the usage of computers and equipment, is to **never make assumptions** about what they know, and what they understand. Always go into any training with clear and concise explanations, using the simplest terminology that you can, which detail the reasons **why** something is, **why** it's important, and **why** you need *them* to do it for you.

The next thing you need to do is what's called checking learning (you can probably tell at this point that I have a teaching degree). This is done in a variety of ways, and the reason is to make sure that each and every person in the room has understood what you're telling them. You can go around the room and ask each person a different question about the subject, to see if they give the correct response. Alternatively, and this is a way that won't make people feel like you're putting them "on the spot," which can be stressful for some people, is to have a short questionnaire with a series of quick-fire questions they can answer, and that you can later check.

If anybody is flagged as not having understood, you can send them resource materials, or invite them in a few weeks later for a refresher session. In the meantime it's always a good idea to encourage the attendees to discuss the matter with each other later. This does two things; it helps keep the subject fresh in their minds, and it uses peer support where those who understand some aspects of the subject better than others can then pass on their knowledge of the subject to those that don't.

Finally, and this is by far the **most** important thing, though it can be uncomfortable to hear. If the people you are educating are not taking in the subject and understand it, it is **never** their fault, it's yours. There's no shame in this and nobody should feel bad. I studied 4 years at university to learn how to do this, and why it is so important. If you find that people aren't learning, don't resort to dumbing things down, try instead using less technical language and jargon, or include more real-world examples so people can visualize what it is you're talking about.

Creating Community Involvement

With all this done, you will hopefully have a workforce that feels valued, and an important part of the processes of security and creating robust systems. They should understand that, for as annoying it is that their children play havoc with their iPad when they need it to buy their mother's birthday present online, the same can be true of a bored employee customizing the look and feel of their PC during a boring coffee break. They should also understand that any unsolicited phone calls, emails, or private messages they may receive are definitely not coming from you (unless you currently do this in which case, please stop it). This is the same as them knowing that their bank will never ask for their PIN number.

The end result is a workforce that feels as though it's part of the solution, and not just there to be blamed when things go wrong. An atmosphere of openness, transparency, and honesty in which people are never chastised for saying something they think is sensible or valid, but that just turns out to be incorrect or unnecessary, is a great environment to have, as you'll quickly find that while more people will come to you with questions, those questions can alert you to bigger problems coming down the line.

Managing Power and Batteries

Education being as important as it is, there are still many things you can do in Windows 10 itself to make life simpler for yourself, and the battery seems like a great place to begin, as effective power management can help boost not just battery life on laptops and tablets but the security on all PCs. Why do I say this? Well, it's because some of Windows 10's security features are tied in with the power management settings.

The power management settings can be found by opening the Power Options from the *Win+X* menu. You will see options for the screen and sleep, both for when plugged in (see Figure 23-1) and, if you are using a laptop, also when using battery.

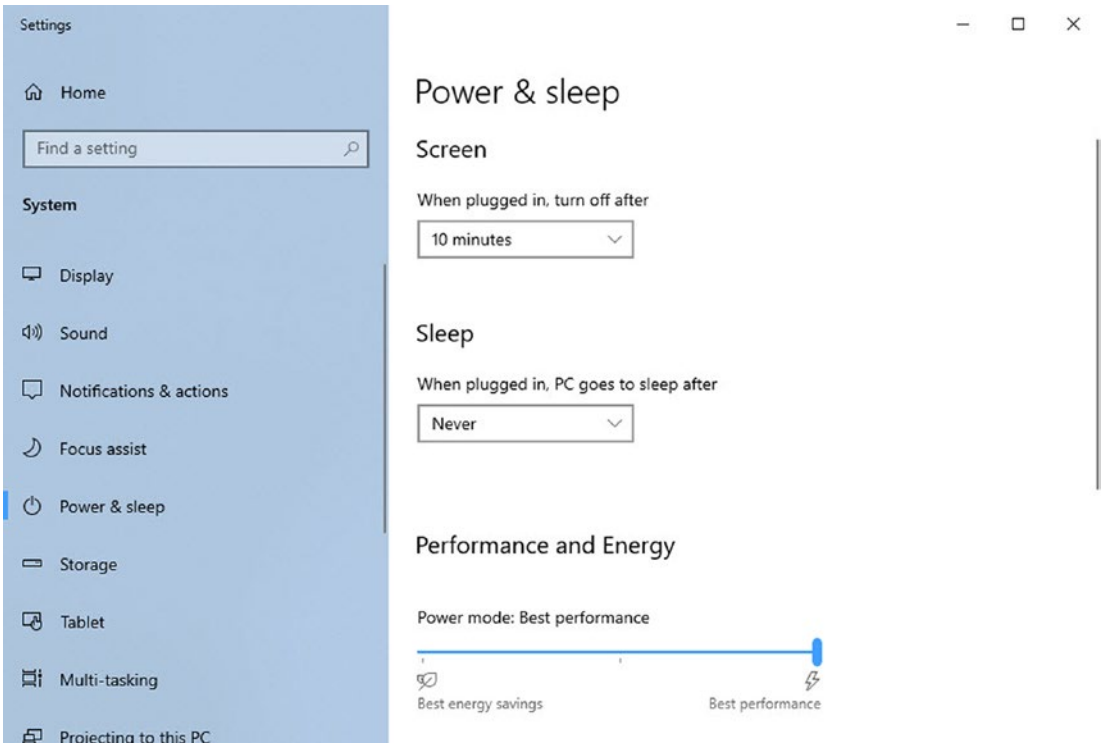


Figure 23-1. *You can disable password entry on wake-up if necessary*

Below these options is an *additional power settings* link which opens the *Control Panel* options. This is where you will get much finer control. You will see in the Control Panel options your different available power plans (see Figure 23-2), along with various links on the left of the panel to configure those options and other power settings.

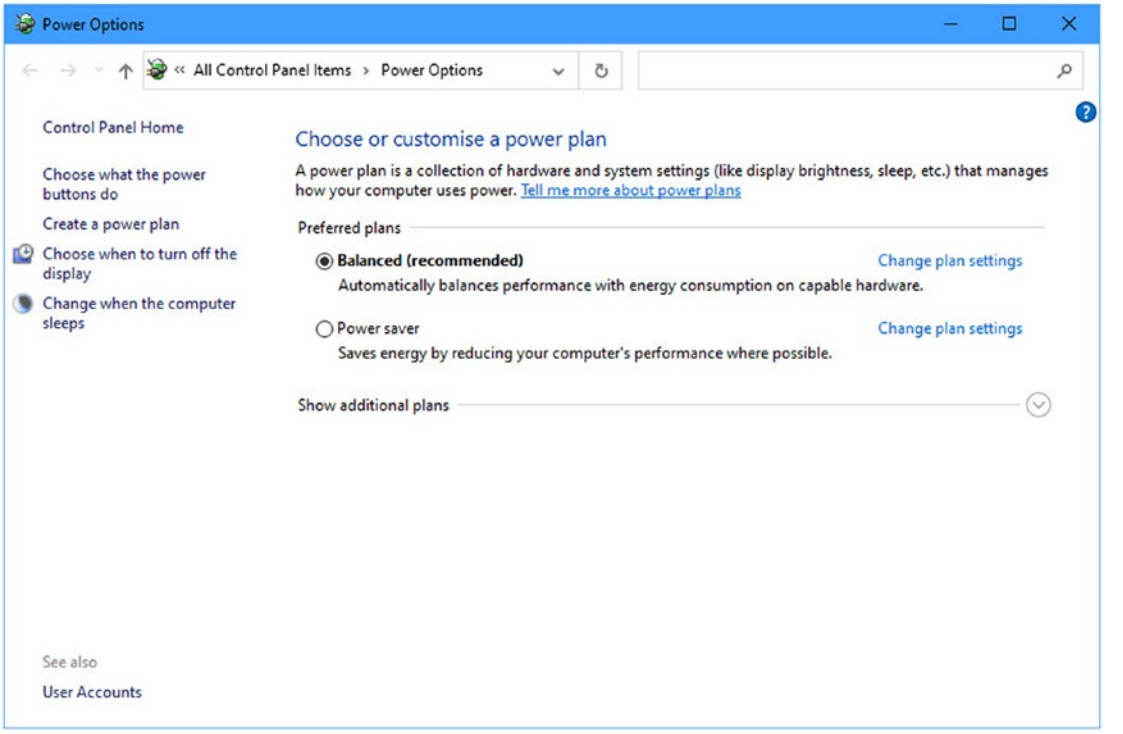


Figure 23-2. *The Control Panel power settings are still in Windows 10*

Tip If the user of a laptop or tablet doesn't need to use the file search feature of Windows 10, disabling the *Windows Search* service can sometimes boost battery life by up to 30%.

One of the most useful settings is the *Change what the power buttons do* link. Changing the behavior of the power buttons on the PC can reap benefits as well. Additionally, clicking the *Change settings that are currently unavailable* link if necessary will allow you to change the Fast Startup, Sleep, Hibernate, and Lock features of the PC; see Figure 23-3. Why might you want to do this? There are both technical and practical reasons for doing so.

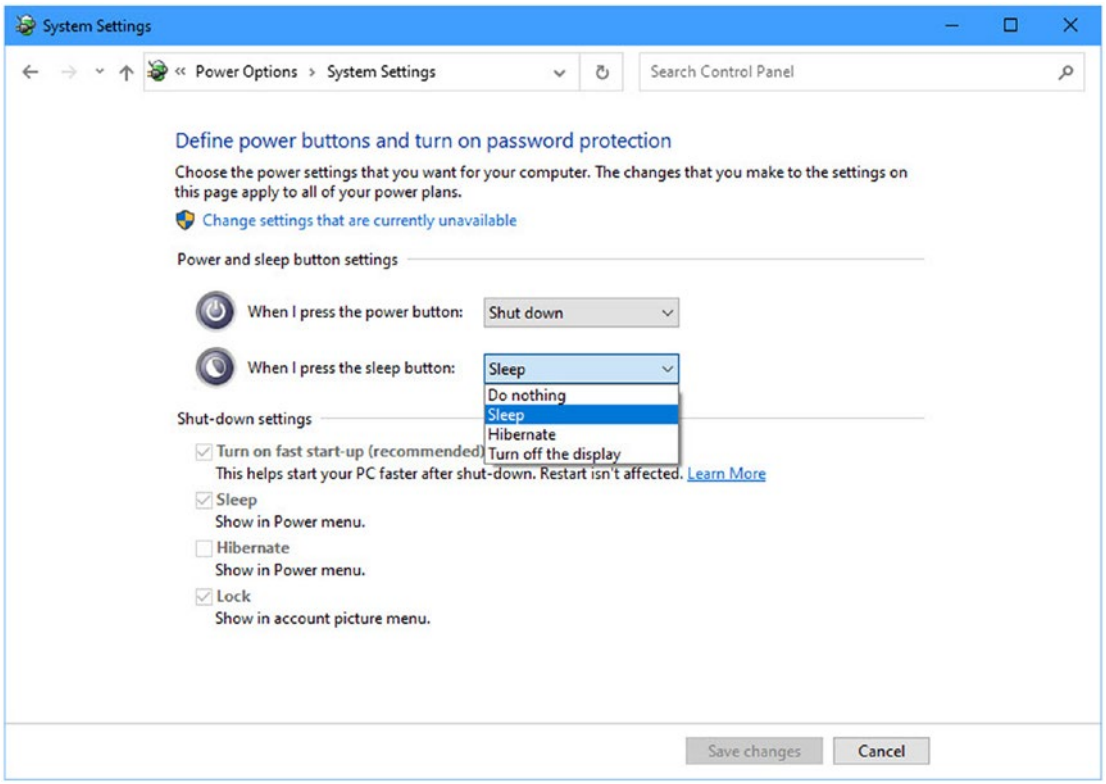


Figure 23-3. *You can change the behavior of the power buttons*

The practical reasons include the fact that modern PCs consume almost no electricity in sleep mode, and after a couple of hours in sleep, the PC will hibernate automatically, in which it will use no power at all. In these states, startup is considerably quicker than starting the PC from cold, and the effect on your power or battery usage is minimal because both Windows 10 and modern PCs are incredibly power-efficient.

Fast Startup uses a hibernation feature to save the current Windows kernel state (the core OS) that's held in memory to disk when you shut down the PC. This means the PC can resume from a "cold start" more quickly. In reality this has been known to cause issues when troubleshooting some problems, so you can either disable Fast Startup either here or just force a full shutdown that will not save the memory contents by holding down the *Shift* key when you press *Shutdown* from the Start Menu.

On a more technical level, there are some PCs that simply don't like various sleep and hibernate states in Windows 10. You'll know this from trial and error, but symptoms can include a signal not being returned to a connected monitor, so you don't get a picture, the PC effectively hanging when you try to wake it, or a PC not really going to sleep at all.

Tip Having one app, be it a store app or a win32 app, open full screen uses less power than having multiple apps open in separate windows on the desktop. This is because the PC's graphics processor has less to draw, and less work to do. Encouraging people to use their apps full screen, perhaps by switching the device into Tablet Mode, and switching between them as necessary, can extend the battery life of a laptop or tablet.

Newer PCs, that is to say ones that have been released in the Windows 8.1/Windows 10 timeframe, will usually support a feature called Hybrid Sleep, which is designed primarily for desktop PCs, and is a combination of the sleep and hibernate states. It saves the current working state of the PC to both memory and the hard disk, enabling you to carry on working quickly from sleep, or from a hibernate state, should there be a power failure. This is just now known as *Sleep* and is why the *Hibernate* option in Windows 10 is hidden by default.

Tip Microsoft Store apps consume less power than traditional win32 desktop apps. This is because they are suspended when not in focus (i.e., not in the foreground and selected on the desktop). In this suspended state, they use no processor time at all. If you have people in your business who use, for example, Microsoft Office, encourage them to switch to the Store versions of Word, Excel, PowerPoint, and OneNote to save power on their laptop or tablet, extending its battery life, while also providing most, if not all, of the functionality they need.

Sleeping Browser Tabs

Microsoft Edge supports a feature called *Sleeping tabs* where any open tabs in the web browser can be suspended (meaning they stop consuming power as they're not doing anything) after a certain amount of time. You can configure this option for your PCs in the Edge browser by opening *Settings* and navigating to the *System* options; see Figure 23-4.

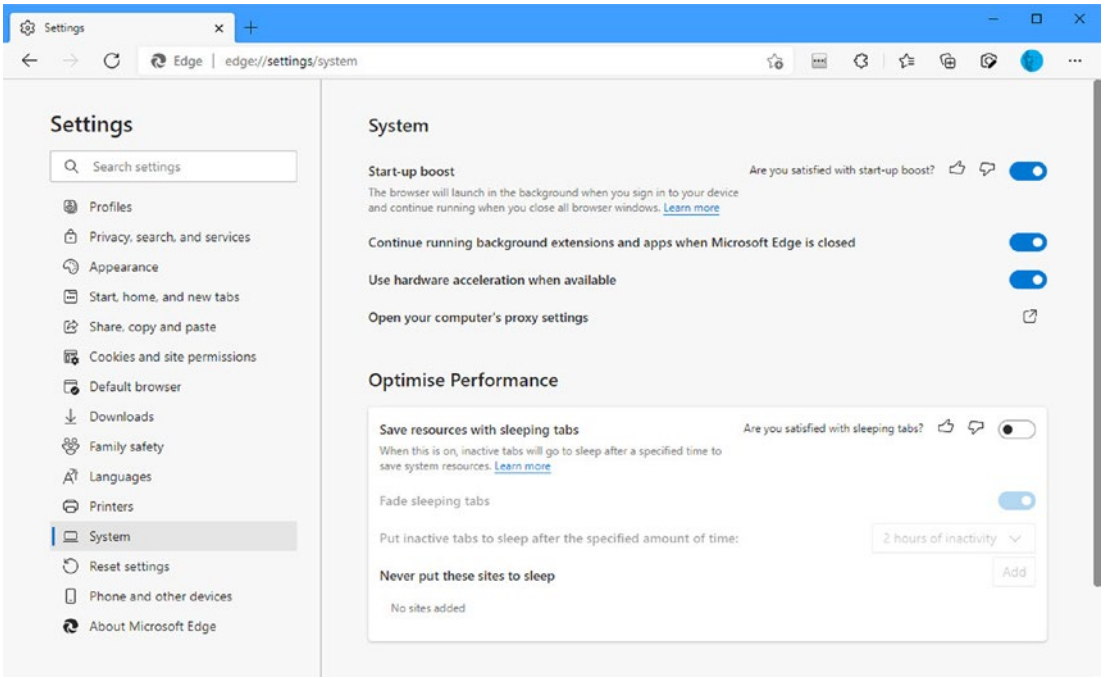


Figure 23-4. *You can configure Edge to put open tabs to sleep, saving power*

Managing Users and BYOD PCs

Nothing will break something on a PC faster than letting someone actually use the thing. Unfortunately, much as we would like people to stop using and therefore breaking our PCs, it's not very practical, and they wouldn't get much work done. Managing users in an effective way, then, is essential to best practice and minimizing problems from occurring.

This is complicated slightly in the workplace because of the rise and rise of BYOD, known as Bring Your Own Device (and sometimes Bring Your Own Disaster). People love using own laptops and tablets in the workplace, perhaps because the ones provided by the company are so crummy, or perhaps because it allows them to work more freely at home.

The problems associated with BYOD however are many and bountiful. They include not being able to control the antivirus software, or Windows Updates on the PC, not being able to control the basic security of the PC, and not being able to control who else gets access to it and gets to use it. All of these are a nightmare for system administrators.

Device Management

Windows 8 was the first Microsoft operating system to feature BYOD support. These come in the form of Azure Active Directory sign-in, and Work folders (a more modern and manageable version of ActiveSync for files). Device Management is by far the most useful, however. Managed from a Windows Server system, MDM allows system administrators to specify minimum standards for Windows Updates, security settings, and malware protection. Additionally, should an employee with an enrolled PC leave the company, the administrators can remotely wipe any company files and data stored on the PC.

Device Management is configured from the Settings app, in the Accounts section by clicking the *Enrol only in device management* link (see Figure 23-5), and it's a simple process that can be done by the users themselves. It doesn't affect the basic operation of their PCs, but it can prevent them from accessing the company network or files, if they do not meet, and keep up with the minimum security requirements.

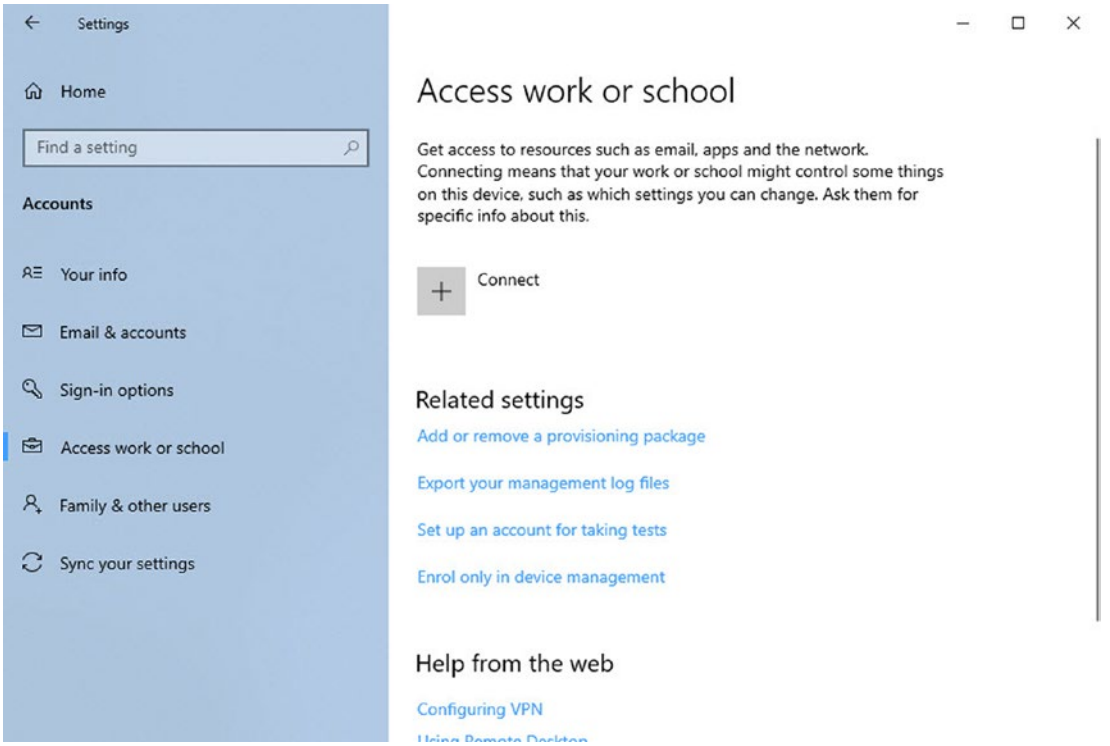


Figure 23-5. *MDM allows administrators control over BYOD PCs*

Group Policy

There are other ways to manage users as well. In Chapter 21 I showed you how you can effectively bomb-proof your PCs using Group Policy. There's much that can be done with Group Policy to prevent users from putting PCs into a state where problems will occur. These can include blocking the installation of anything other than approved apps, and even specific versions of apps.

You can also prevent users from making any configuration changes to the PC, such as changing its power, desktop, or network settings, and you can stop users from installing Windows Updates, if you have a policy of carefully checking for compatibility and other issues before rolling these out.

Backups' Best Practice

The way we back up our files and data has changed dramatically in the last few years. Do you remember the days when you'd buy a big stack of blank CDs or DVDs, and then spend several hours every month burning copies of all your files to them, only to find that when you needed to copy a file back, the disk had become corrupt and wouldn't work? I certainly do!

These days we're far more likely to rely on network-attached storage (NAS) or cloud backups, as they are seamless, constant, and nonintrusive in our lives. I love that the files on my PCs both are backed up and synchronized with Microsoft's OneDrive service; after all, what's not to like?

Sadly, though, maintaining your backups only in this way is also a recipe for disaster, as the world and its threats have moved on. Now, especially with the threat of ransomware, we need to be smarter about how we schedule, and where we put, our backups.

Now, what I'm going to write here is my own recommendation. You might use some or all of it, or you might have your own ideas. I'm not going to say that my way is best practice, though it's certainly good practice. It's based upon the three core principles of being prepared, staying ready to restore quickly, and maintaining a consistently high level of paranoia. My own backup strategy works as follows:

- **Backup #1**–Full file backup to Microsoft's OneDrive cloud service. This creates a reliable offsite backup in case of an event such as fire or theft while also allowing me to synchronize my files between my PC, laptop, tablet, and other devices.
- **Backup #2**–Synchronization of my OneDrive files to another PC and my laptop, so that I can continue working if I have a problem that renders my main desktop PC unusable for a time.
- **Backup #3**–Local backup performed to a NAS drive that occurs when changes are made to files as a reliable and quick to access backup.
- **Backup #4**–This is something I have yet to implement but will require a second NAS. My home consists of two buildings as many French properties do, and I'll take advantage of it. I have the main house, and a smaller outhouse known as a gîte, which is where my office is. Having a second NAS in a different location is my protection

against ransomware (though I have ransomware protection turned on, which I detailed in Chapter 18). With a backup performed on a schedule every week or three, you can only lose the most recent work should you need to reformat the hard disk and recover your files.

Like I said, I'm pretty paranoid! Our files are our lives and often our livelihoods as well. It's one thing for Granny Clark to dig an old photo album out of the drawer to show you photos of you when you were a baby, but quite another thing for all your precious photos to be wiped out by an accident, malware attack, or user error.

Caution I want to deal for a moment with the issue of offsite backups. These are crucial for any individual or business as they keep you covered in the event of a fire, theft, flood, alien attack, war, asteroid strike, supervolcano eruption, or the cat peeing on the computer. There are data protection issues tied to offsite backups for business, however. Data protection regulations will differ around the world, but generally they will require any data you store on employees, customers, suppliers, and members of the public to be secure and safe at all times. It might be tempting for a small business, for example, to mirror their workplace backup to a NAS drive in somebody's home. The simple act of doing this, however, could put the business in breach of data protection law should the NAS drive later be stolen. You should always check local data protection legislation before deciding where to store your offsite backups.

Deployment and Recovery Best Practice

If you're deploying Windows 10 across a medium- to large-size organization using volume licensing, then you'll already be using the Windows Assessment and Deployment Toolkit (ADK). This affords you full control over deployment images, drivers, installed apps, and more besides. For small businesses, however, perhaps with just a few PCs, each machine must be installed individually. You can read extensive documentation about the Windows 10 ADK in this link `https://pcs.tv/3fCrbi3`.

Generally speaking, each PC will have come with Windows 10 preinstalled, or will have been upgraded from Windows 7 or Windows 8.1. Windows 10 is a very stable and robust OS that should operate for years on the same hardware with few problems. There are still things you should do however to make sure that if you need to reimage or redeploy the OS, you can do this quickly, easily, and without any barriers. These, then, are my top tips to aid deployment and recovery in a non–volume-licensing business environment, or in the home:

1. Keep a copy of all the drivers for your hardware in at least one safe place. I keep a copy of all drivers in cloud storage so they can be synced to devices for installation, or easily copied to a USB Flash Drive.

2. Optionally, you can also keep a copy of the `C:\Windows\System32\DriverStore` folder after installation, as this will contain drivers that can be searched for by the Device Manager. However, do not immediately merge this folder with the DriverStore folder after reinstallation, as some drivers may rely on system updates that may not be installed.

3. Install Windows 10 from fresh media (DVD or USB) created using the official Media Creation Tool, `www.microsoft.com/software-download/windows10`. This ensures you are installing the most recent build of the OS, and therefore reduces the time needed after installation to install updates and patches. This can also be downloaded to create a DVD you can use with the System File Checker; see Chapter 4.

4. **Create a USB Recovery Drive**. Yes, you just knew I was going to come back to this, but it really is the single most important thing you can do with any Windows 10 PC. Label the drive, and keep it in a safe place where you can easily find it. I detailed how to create a Recovery Drive in Chapter 2.

5. Make a backup image of your Windows 10 installation to a separate internal hard disk or partition. I create special backup partitions on all my PCs for this purpose, containing a clean installation that has all apps and drivers installed. You can find out how to create a System Image Backup in Chapter 2.

6. Always leave a spare, general-purpose machine available on standby when you're going on vacation. You can guarantee that somebody important in the business will have a major PC crisis the moment you go away. Keeping a spare, patched, and up-to-date machine on standby will enable this individual to carry on working, so as not to ruin your once-in-a-lifetime trip to the Bahamas.

Managing External and Network Hardware

The best way for any external or network hardware to cause problems is for it to become damaged, and the best way for it to become damaged is for somebody to bash into it, trip over it, or snag it. This is especially true of cabling, which can be severely damaged if pulled, not to mention what can happen to the hardware on the other end of the cable, which is also pulled.

This type of damage can result in broken plugs and sockets, ripped cables, cracked cases when hardware hits the floor… you get the idea. It's extremely easy to avoid too because the cable tie is the system administrator's best friend. These small pieces of plastic can secure any bunch of cables together, on their own or to anything else. If your desks have cable management built in, do use it; it'll save you a lot of headaches, and please, please, keep anything that people don't actively need access to away from them. They'll definitely find a way to break it if you leave it out or lying around.

Summary

Best practice really is just common sense and is very easy to both practice and instill into others. The end users of PCs won't exercise common sense, however, because they just want to get stuff done quickly and enjoy themselves with the minimum amount of effort, so you can't rely on them to help and will have to do things yourself.

I mentioned BYOD earlier in this chapter and how you can use best practice to manage BYOD devices. In the next chapter, we'll look at this in more detail, and I'll show you how BYOD devices can be managed and configured in workplace environments.

CHAPTER 24

Managing BYOD Hardware

BYOD, or Bring Your Own Device, sprang up on the popularity of the iPad. Corporate executives would get a shiny-new tablet for Christmas or for their birthday and then proclaim to the IT department that it was wonderful and that everybody should be allowed to use them.

It's fine in theory that all computers should be able to work well together; after all, they just communicate in 1's and 0's (zeros). As you'll know, however, not only do all devices *not* communicate with each other nicely sometimes, but the risks involved in letting people use their own computers at work are enough to cause many sleepless nights for an IT pro.

Then, the pandemic hit, and what was often seen as either a novelty or a hindrance in the workplace suddenly became an essential part of everyday life. Everybody that could work from home *was* working from home, and the whole world of being an IT professional in business of all sizes was almost instantly turned on its head. If this includes you, then I don't envy the work you had to do, and in such a short period of time, to make sure everybody that needed to be able to work from home could actually do so, as it was an enormous challenge for every business.

Managing these remote devices however, especially when they weren't owned by the company, becomes a great challenge in itself. You simply have no idea, or control over, where the computers came from, how old they might be, what hardware and software are installed, and what other family members might be using them. Let's not forget children were often using the same computers for home schooling, and they were an essential tool for helping families and friends that were separated for many, many months stay in touch and stay sane.

Fortunately, Microsoft had already stepped into the fray with Intune; you can read all about this at `https://pcs.tv/3jB9ctF`, and I can't even begin to guess how the world in 2020 and 2021 would have played out if companies such as Microsoft and Google hadn't already put these suites of cloud services in place. Intune is a suite of tools that

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_24

allows you to manage BYOD devices running the Windows, iOS, and Android operating systems. This includes smartphones and tablets and is a service often referred to as Mobile Device Management (MDM).

Why is a tool such as MDM important? Simply put, as an IT pro, you will have no control over the security and patching of devices not directly owned and maintained by your company. For all you know, the person wanting to use their Android smartphone or tablet is running an extremely old, and no longer supported, version of the OS; the person wanting to use their own Windows laptop might have let the 30-day trial of antivirus software lapse after they purchased it, thinking that they're still protected; or the person with the lovely new iPad might let their children, and all of their children's friends, play with it in the evenings. In short, BYOD is at the very least a headache and at most a nightmare.

There's a whole book in how you use MDM to manage iOS, Android, and Windows devices, and sadly I've not enough pages in this chapter to show you how to manage everything here, but I'll show you what BYOD functions exist within Windows 10 and how you and the owners of BYOD PCs can use them to help them use their own device at work, and to also give you the peace of mind and reassurance that you all need.

Managing VPNs and Secure Connections

Before we jump into all the BYOD stuff, though, I want to begin by looking at how you can get secure connections from mobile devices to your company using a Virtual Private Network (VPN). VPNs are secure, encrypted data connections that give you peace of mind when an employee is connecting to your company network from a remote location over an Internet connection. VPNs are managed in Windows 10 from the *Network & Internet* section of the Settings panel; see Figure 24-1.

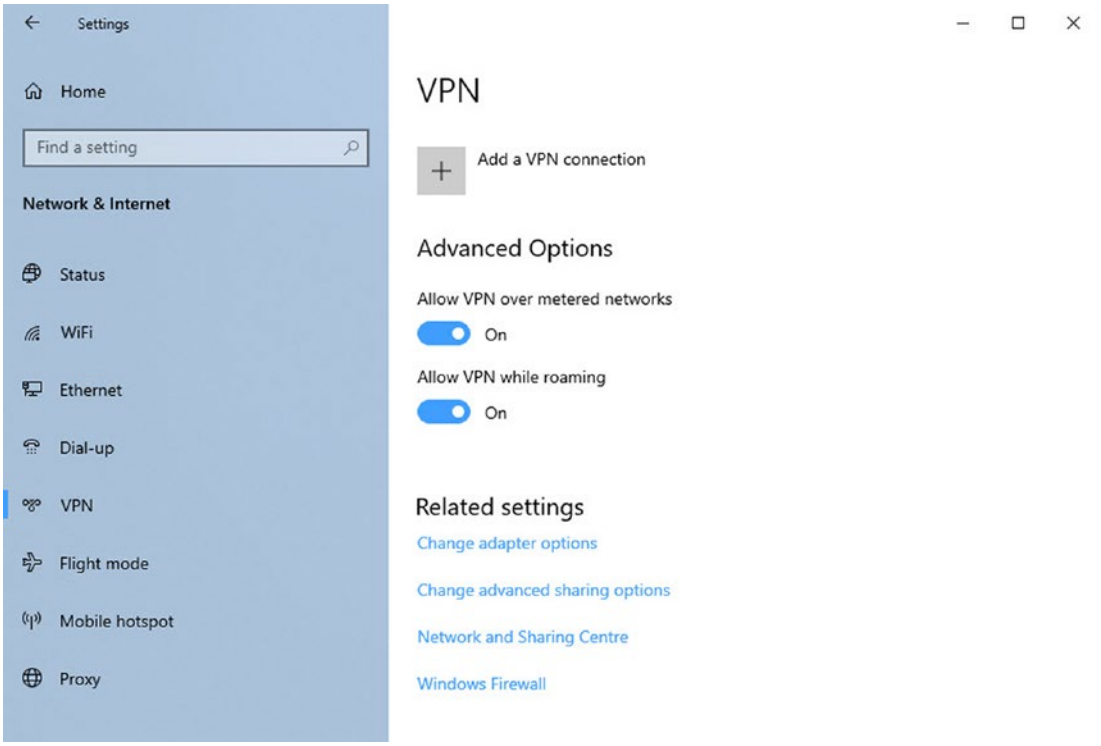


Figure 24-1. *VPNs are managed in the Settings panel*

Microsoft has configured the Settings app in such a way as to make it easy and straightforward for anybody, of any technical ability, to configure the settings there. You can see in Figure 24-2 the information that you will need to provide to an employee so that they can configure their own PC to connect to your VPN.

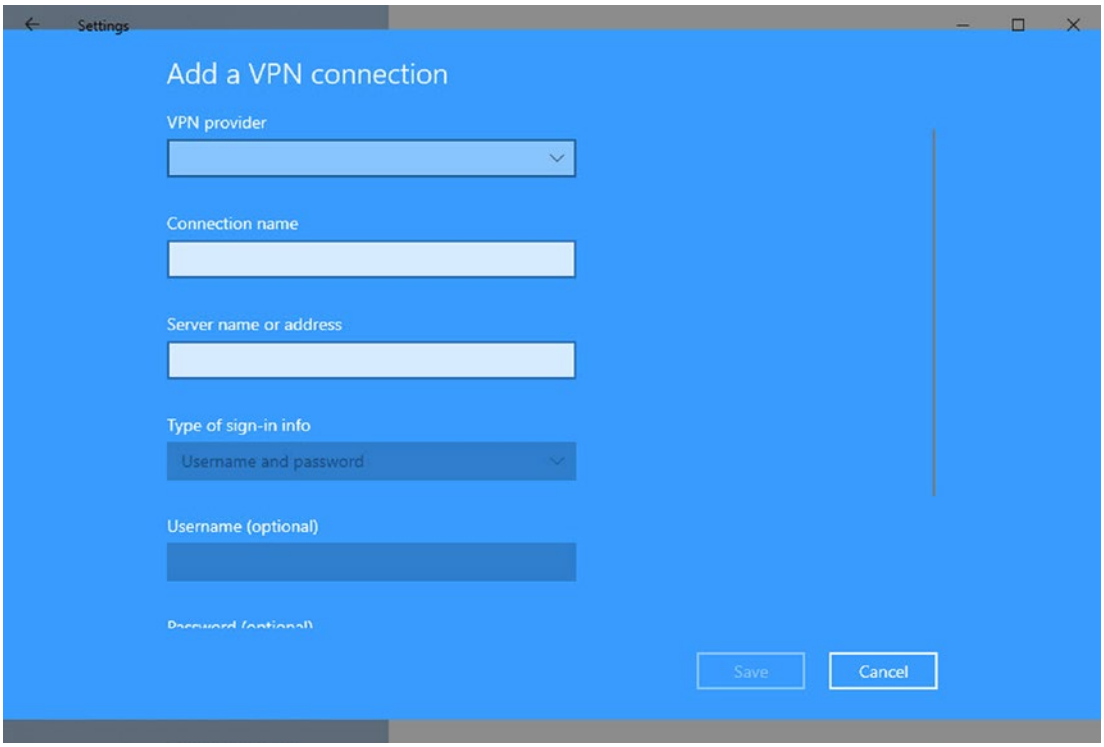


Figure 24-2. *It is easy to set up new VPN connections*

The *VPN Provider* option will use the *Windows (built-in)* default option unless you use a third-party VPN provider, for which there will no doubt be software the user will need to install on their PC first. You will then need to provide the connection name, server name or address, the VPN connection type, and details of how the user connects to the VPN, be this a username and password or a smart card.

Once the VPN is configured, the user can then connect to it from the Network & Internet panel, where *Connect*, *Advanced Options* (effectively editing the settings), and *Remove* options will be available to them.

Workplace Join

Whether the user is connecting their own PC to your company network remotely over a VPN or directly in your workplace over your own Wi-Fi or wired network, there are additional options available for managing these BYOD devices.

Tip A good security measure in the workplace is to maintain a separate Wi-Fi network for BYOD devices. This will still enable them to access workplace resources that you have connected via a switch, but can limit the surface area for attack should a device's security become compromised.

Workplace Join ties in directly with MDM, and Workplace Join can be configured to not permit connections unless the user also enrolls their device into MDM. They can do this in the Settings app, so again it's easy for them to do and understand, in the *Accounts ➤ Access work or school* section; see Figure 24-3.

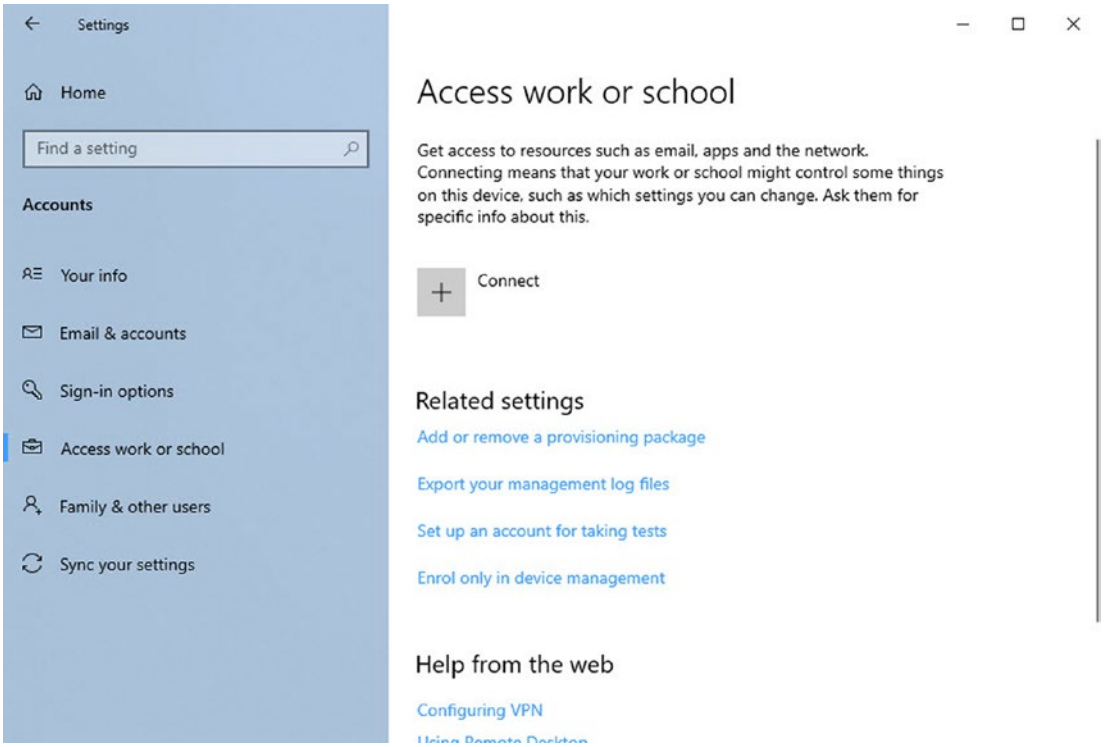


Figure 24-3. *MDM and Workplace Join are managed from the Accounts settings*

Let's spend a minute looking at what MDM allows you to do with a PC. The benefits include being able to specify minimum levels of threat protection for the device. For example, you can specify that devices for which updates and malware security are not

up to date will not be permitted to connect to the network. All of this is manageable yourself, however, through Microsoft's Intune service, where you can see the current status of all BYOD (and other) PCs and push updates and apps to them as appropriate.

MDM also gives you permissions on apps. You can't stop the owner of the device from installing whatever apps they want—it is their device after all—but you can specify which ones they can use when connected to your network, and which versions of those apps can be used as well. This means that, for example, they could be prevented from using a browser where Flash is installed, or from using an older and insecure version of Adobe Acrobat Reader or Microsoft Office.

Lastly, MDM gives you authority to wipe all apps and documents related to the business from the device remotely and at any time. This means you can completely revoke a person's access should they leave the company, or for another reason, such as the PC being lost or stolen, without having to have the user or the device onsite. You specify what needs to be wiped, and the next time that device is online, the instruction will be passed. You will then be able to monitor the status of the management using Intune.

You can read more about what happens when you join a device to your organization's network on this link https://pcs.tv/3yvWvGB, and below are additional help and tutorial links from both Apple and Microsoft on how to connect MacOS, iOS, and Android devices to your systems:

- **Join a Windows 10 PC to Azure AD**–https://pcs.tv/3yvWvGB.
- **Join an Android tablet to Azure AD**–https://pcs.tv/3rYXr3V.
- **Join an iPad to Azure AD**–https://pcs.tv/3jxkH5h.
- **Join an Apple Mac to Azure AD**–https://pcs.tv/3s9ZWRb.

Managing Provisioning and Device Enrollment

There are two links in the *Access work or school* settings that you will want to take note of when connecting a BYOD PC to your company or organization's network and services. The first is called *Add or remove a provisioning package*. This is a file, normally delivered to a BYOD worker via a download or on a USB Flash Drive that tells their device what software to install from the company's Azure AD systems, and how security and services should be configured. Windows 10 will look at removable media (a USB Flash Drive or SD Card) for a Provisioning package (see Figure 24-4) and will tell the user if one cannot be found.

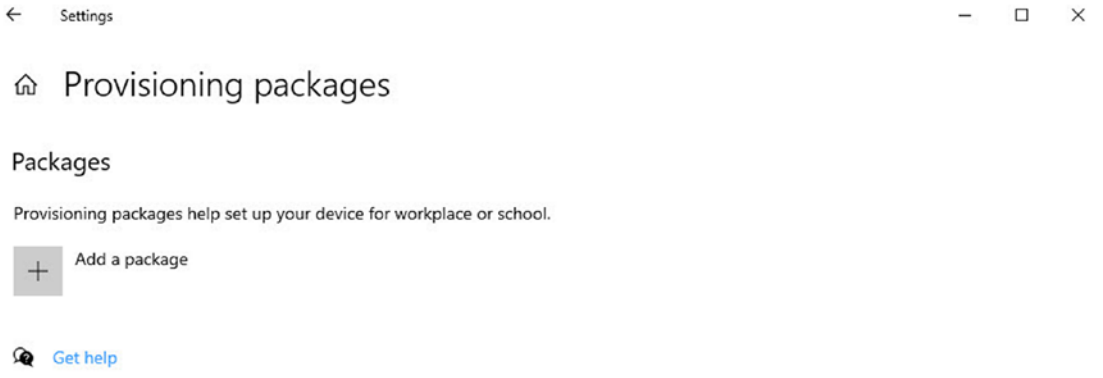


Figure 24-4. *You can remotely configure a BYOD computer using Provisioning*

Microsoft have a large amount of documentation online about how Provisioning works, and how you can best configure it for the needs you're your company or organization. You can read more on this link `https://pcs.tv/3iDbZDr`.

Sometimes though you won't want to provision a computer as, to give an example, the remote worker only needs to access services in a web browser and they have Edge or Chrome installed, or because they use Microsoft Office software such as Word, Excel, and PowerPoint, and they already have access to these as part of a Microsoft 365 Home or Personal subscription. In this circumstance there is an option to *Enrol [the computer] only in device management*; see Figure 24-5. This is a subset of provisioning that helps make sure the connection made between the computer and your company servers is secure. It allows you to specify a minimum security level for the remote computer, including that it must have up-to-date antimalware definitions installed, and be enrolled in appropriate operating system update services.

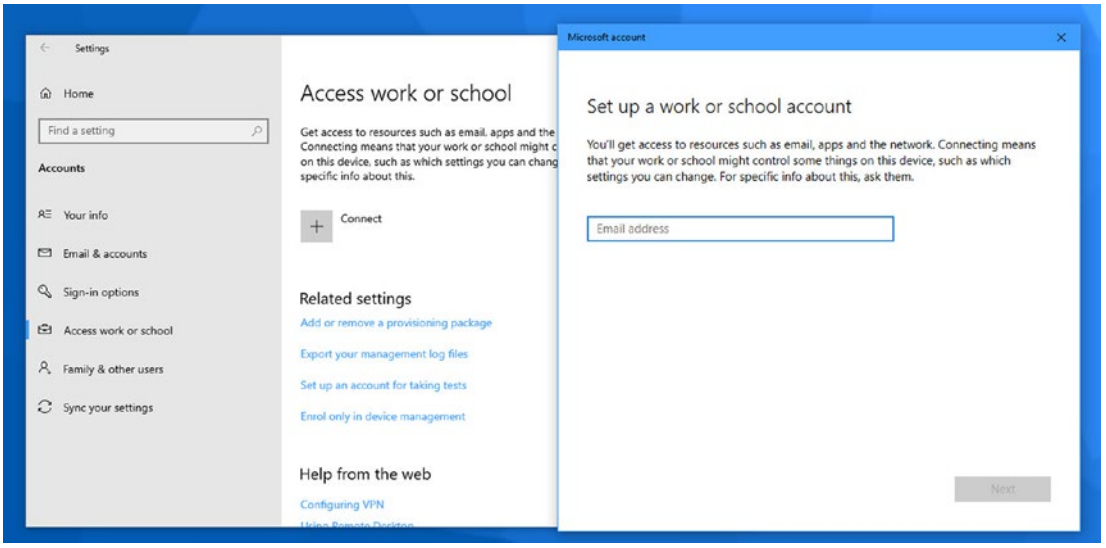


Figure 24-5. *Device Management allows you to specify minimum security for a remote computer*

Device Management also allows the IT department to remotely wipe all company data and settings from the remote computer should the employee leave the company, or not need to use that device with company systems in the future. You can read more about Device Management on the Microsoft website at this link `https://pcs.tv/3Cn2TCf`.

Connecting to an Exchange Account

The device owner can connect to your Workplace simply by clicking the *Access work or school account* link. This will drop them into the main Accounts options where they need to click the *(+) Add an account* button. This will present various options to add Microsoft, Google, or other email account types. You can also add business accounts by clicking *Email & app accounts* and then clicking *Add an account*, which will allow them to set up Exchange account types; see Figure 24-6.

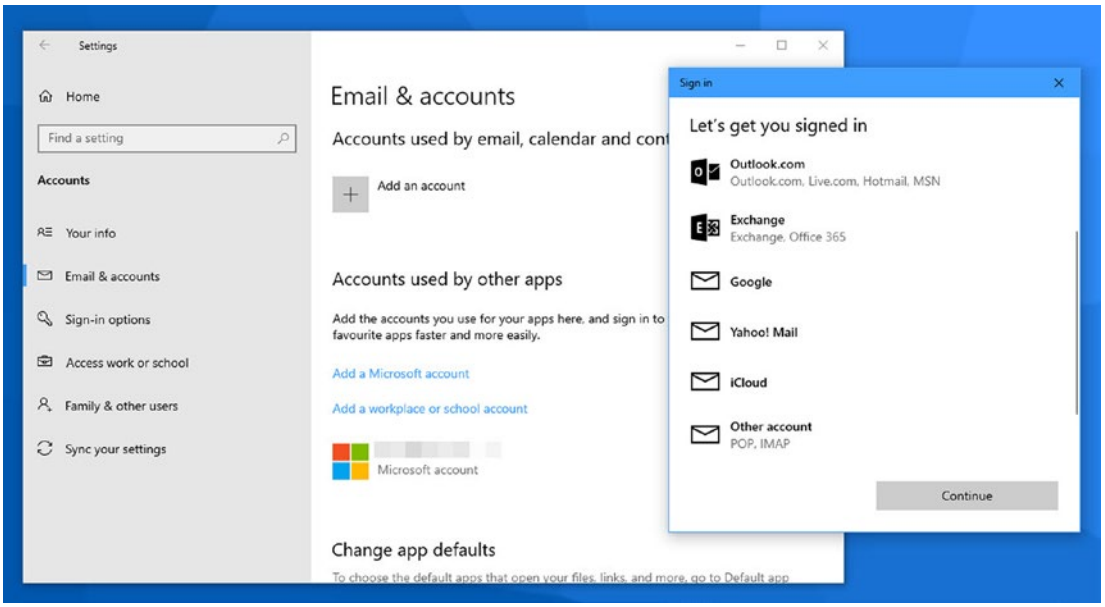


Figure 24-6. *You can add business accounts in the main Accounts settings*

Connecting to Microsoft 365 or Microsoft Azure

If you use Microsoft 365 or Microsoft Azure, you will need to point the user at the *Accounts* ➤ *About Access work or school* panel in the Settings app. Here they can click the *Connect* button, and then one of the two links at the bottom of the dialog that appears, to enroll their device in the company's services; see Figure 24-7. This will automatically enroll the device in MDM and allow you to manage it remotely.

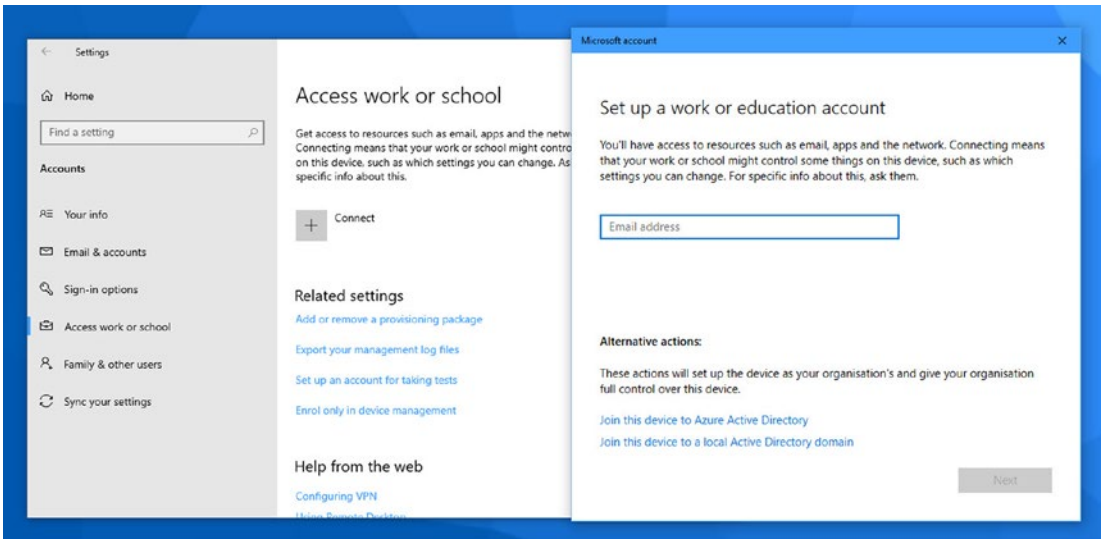


Figure 24-7. *You can easily enroll a PC in Office 365 or Azure*

Additionally, at the bottom of the *Set up a work or education account* dialog are two links to *join this device to Azure Active Directory* and, for computers that are already connected to the company network, *Join this device to a local Azure Active Directory domain*.

Work Folders

You might be familiar with Microsoft's ActiveSync technology. This has been around since the heady days of Windows 95, and it allowed PC users to store files from the workplace directly on their device, be that a laptop or a phone running Windows Mobile or Windows CE (officially the abbreviation for Consumer Electronics by Microsoft, but always known by myself as Crap Edition). ActiveSync worked effectively for many years, but it was designed for a bygone time before we had fast Internet, or even the Internet come to that.

In Windows 10 there is no ActiveSync, but there is a feature called Work Folders which performs the same task, but in a more modern way. Work Folders can be managed from the Control Panel, and you can most easily find it by searching for it in the Start Menu. It's a simple affair, as you can see in Figure 24-8; there's only one item to click in its Control Panel settings.

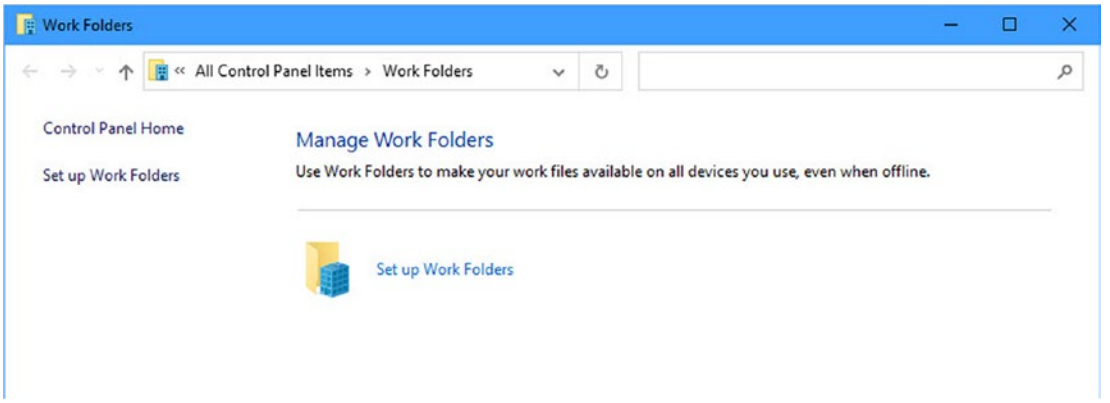


Figure 24-8. *Work Folders are easy to configure in Windows 10*

To configure Work Folders, enter the username or URL of the Work Folder access, which needs to be configured in Windows Server. A folder is configured at `C:\Users\[Username]\Work Folders`, where any synced files will be stored. These are automatically encrypted by Windows 10, and the user is not allowed to change the location of this store folder. The user also cannot decrypt the files.

Work Folders are designed to automatically sync on the PC and stay up to date. Should a user feel, however, that a sync has not taken place and that they do not have the latest version of their files, they can click the *Sync Now* option that will appear in the Work Folders settings in the Control Panel. That really is all there is to Work Folders. They are an alternative to ActiveSync, and, just as with all other BYOD features in Windows 10, they also work with the iOS and Android operating systems.

Summary

As I mentioned at the beginning of this chapter, all MDM features in Windows 10 are managed by Windows Intune, which can also manage devices running Apple's iOS and Google's Android operating systems. Intune allows you to make sure that the security, patching, and apps on the device are both up to date and approved by yourself and your company; you can read more about it at `www.microsoft.com/server-cloud/enterprise-mobility`.

We're heading into the home stretch now with this troubleshooting book, and that's all now for best practice. In the next chapter, we'll begin to look at how we can really dig deep within Windows 10 and get advanced and detailed technical information about the OS, your PC, your installed apps and updates, and what different types of diagnostic and system information are available to you.

CHAPTER 25

Getting Advanced Information

In Chapter 22, I detailed the Microsoft Sysinternals suite, and it's clear from using utilities such as AutoRuns just how much there is going on inside a PC at any one time. It's not just the drivers for the hardware you can see on your desk that are installed but the many dozens more for all the hardware on your motherboard that you can't. This is coupled with audio and video codecs, support utilities, Windows and third-party services, etc.; the list is pretty endless.

When you're troubleshooting a problem with your PC, then how do you go about getting the detailed diagnostic and support information that you need? Back in Chapter 5, I detailed the Event Viewer and showed how powerful and useful it is to get information about errors and events. Believe me, though, the Event Viewer is just one place from which you can get useful and detailed information. There are others. Many others!

The Task Manager

If you still think of the Task Manager in Windows just as the place where you can close running and hung apps, then think again. Sure, in its simplest form, the default when Windows 10 is installed, it's just that, a list of running apps with an End Task button; see Figure 25-1. Click that More details icon however, and a whole new world opens its doors to you.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_25

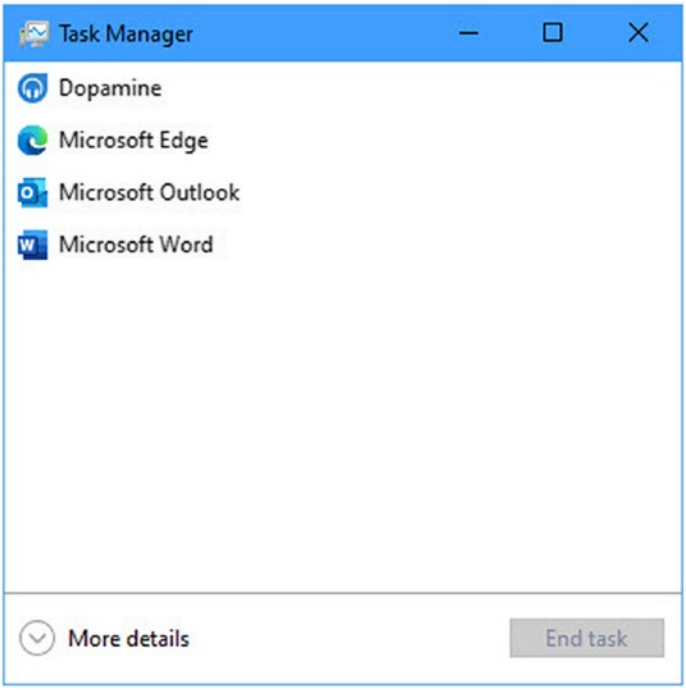


Figure 25-1. *The "default" Task Manager is a simple affair*

With the full Task Manager view open, a wealth of useful information is displayed across several tabbed panels; see Figure 25-2. The default view, the *Processes* tab, provides live information about the processor, memory, disk, and network usage of running apps and services.

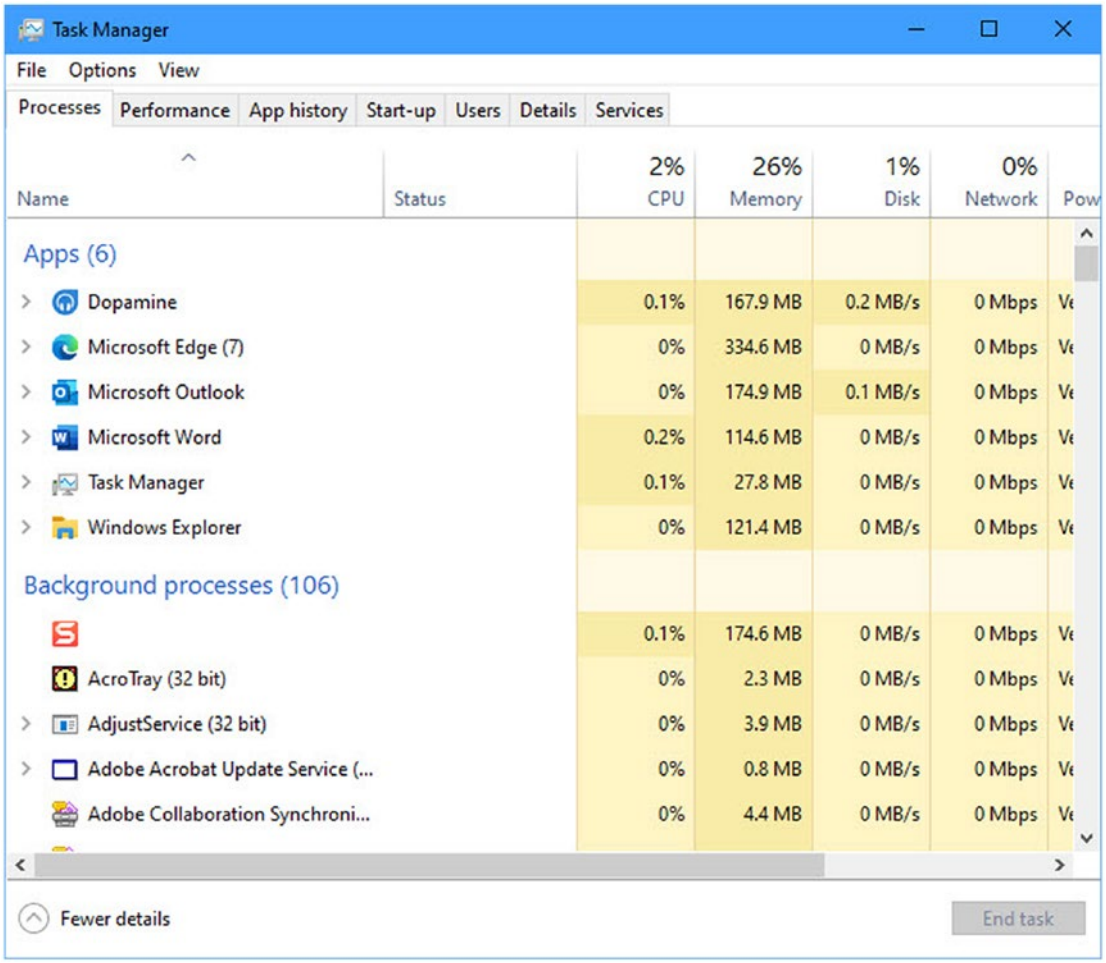


Figure 25-2. *The full Task Manager is packed with useful information*

The information the Processes tab provides is heat-mapped, enabling you to see at a glance if an app is hogging too much processor time or memory, as an example. Hung apps will also be detailed, and another useful feature when it comes to managing hung apps is that if any app has a dependency, for example, it has multiple processes (sometimes called threads) running, an arrow will appear to its left. Click this, and you will be able to see if you will also terminate any other processes by forcing the closure of the hung app.

The *App history* tab can sometimes be useful, but only if you use a lot of Store apps. As well as reporting on processor and network usage (note this is local as well as Internet usage), it can very helpfully report on whether apps are using metered data (which can be expensive when you're on a roaming data connection), and how much data they have used to update their live tiles; see Figure 25-3.

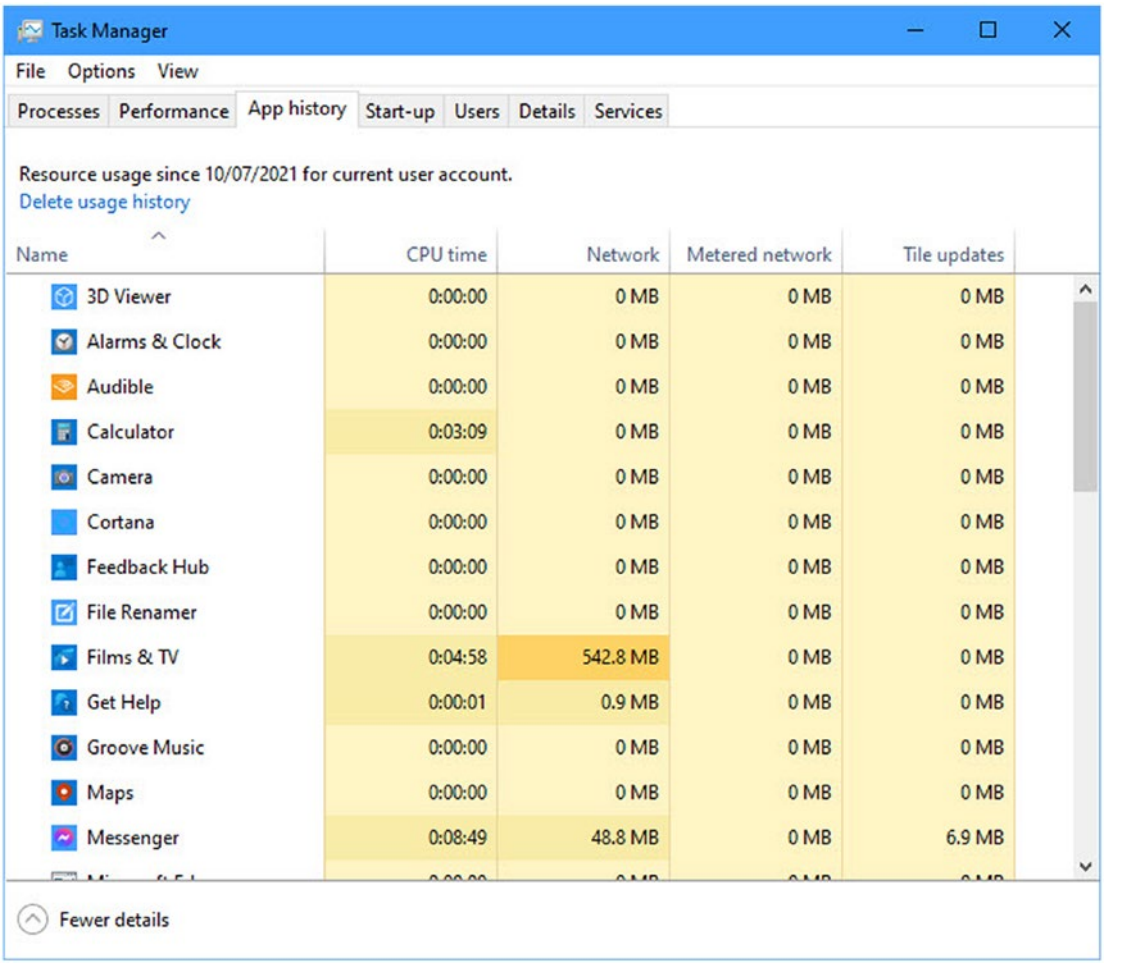


Figure 25-3. *The App History tab provides information about Store apps*

It's entirely possible, however, that you might be a Task Manager purist, and not fancy this "trimmed-down" traffic-light approach. If you were a fan of the Task Manager as it appeared in Windows XP and Windows 7, then the *Details* tab is for you. This lists all running apps and processes, complete with detailed descriptions of what each is,

their CPU and memory usage, and more besides; see Figure 25-4. In many ways, this provides more information than the Processes tab, as it lists background processes which may hang or fail on the PC. The *Services* tab also lists all Microsoft and third-party services that are running on the PC.

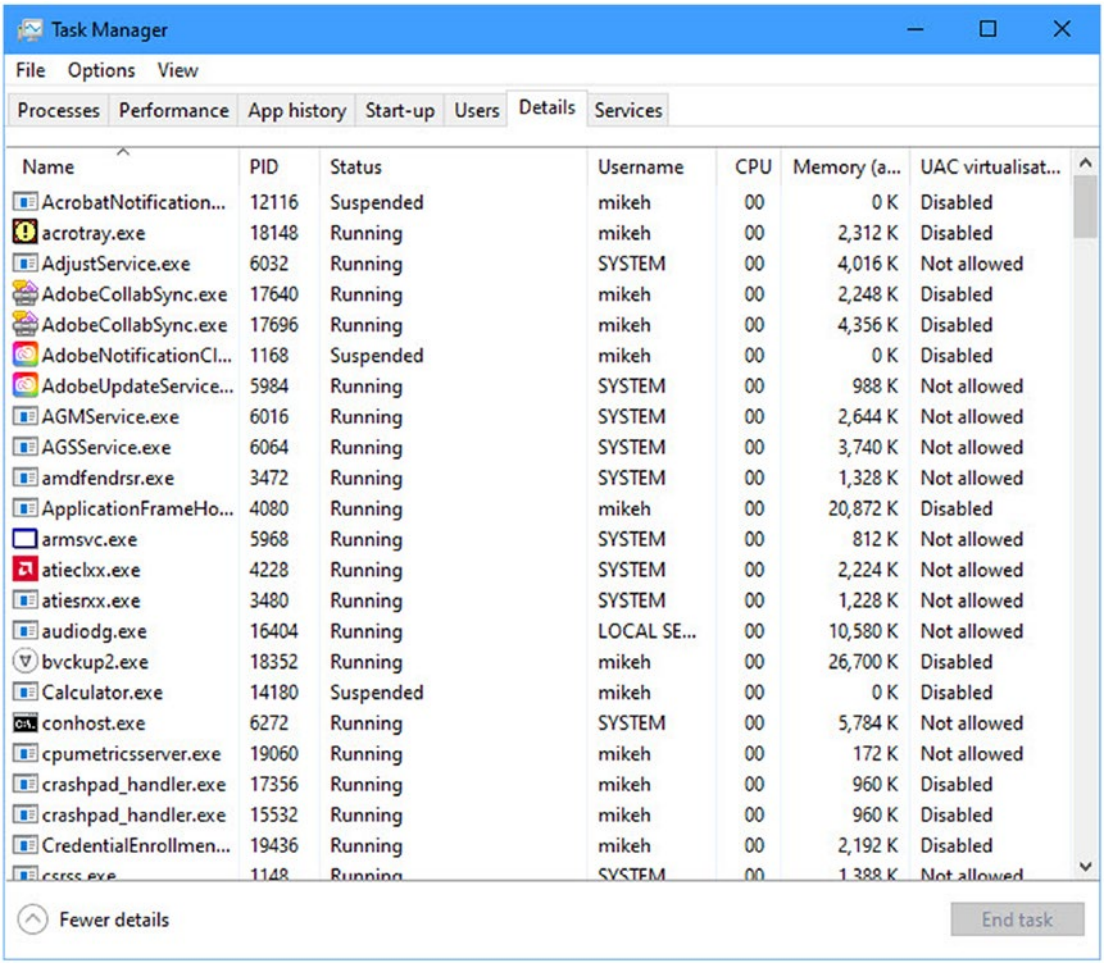


Figure 25-4. *The Details tab is a wealth of "What's going on" info*

The Task Manager's party-trick, however, is what it can do in providing live status and information panels, which you can sit on your screen; see Figure 25-5. If you right-click a graph under the *Performance* tab, you can view live data about the PC's processor, memory, hard disk (separated by disk), network (separated by connection) usage, and graphics processor (GPU). These can be presented as graphs or numeric metrics, and processor information can also be viewed on a core-by-core basis.

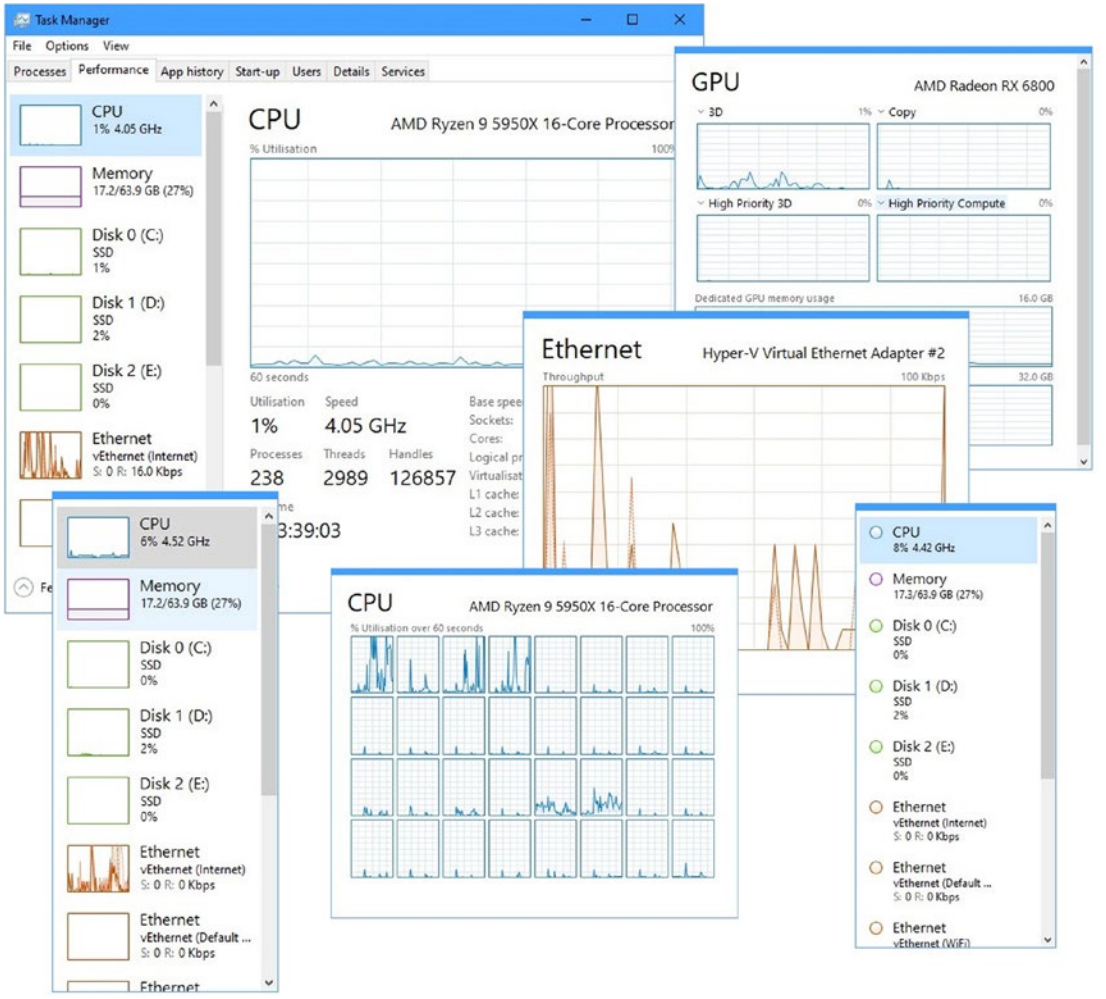


Figure 25-5. *Meet the Task Manager's party-trick, live system status panels*

If you need to monitor live information about your PC, such as the processor, memory, or network usage, then the Task Manager is by far the simplest and least intrusive way to do it. Then, last but by no means least, the *Start-up* tab is where you can manage the apps that run at startup on the PC; see Figure 25-6.

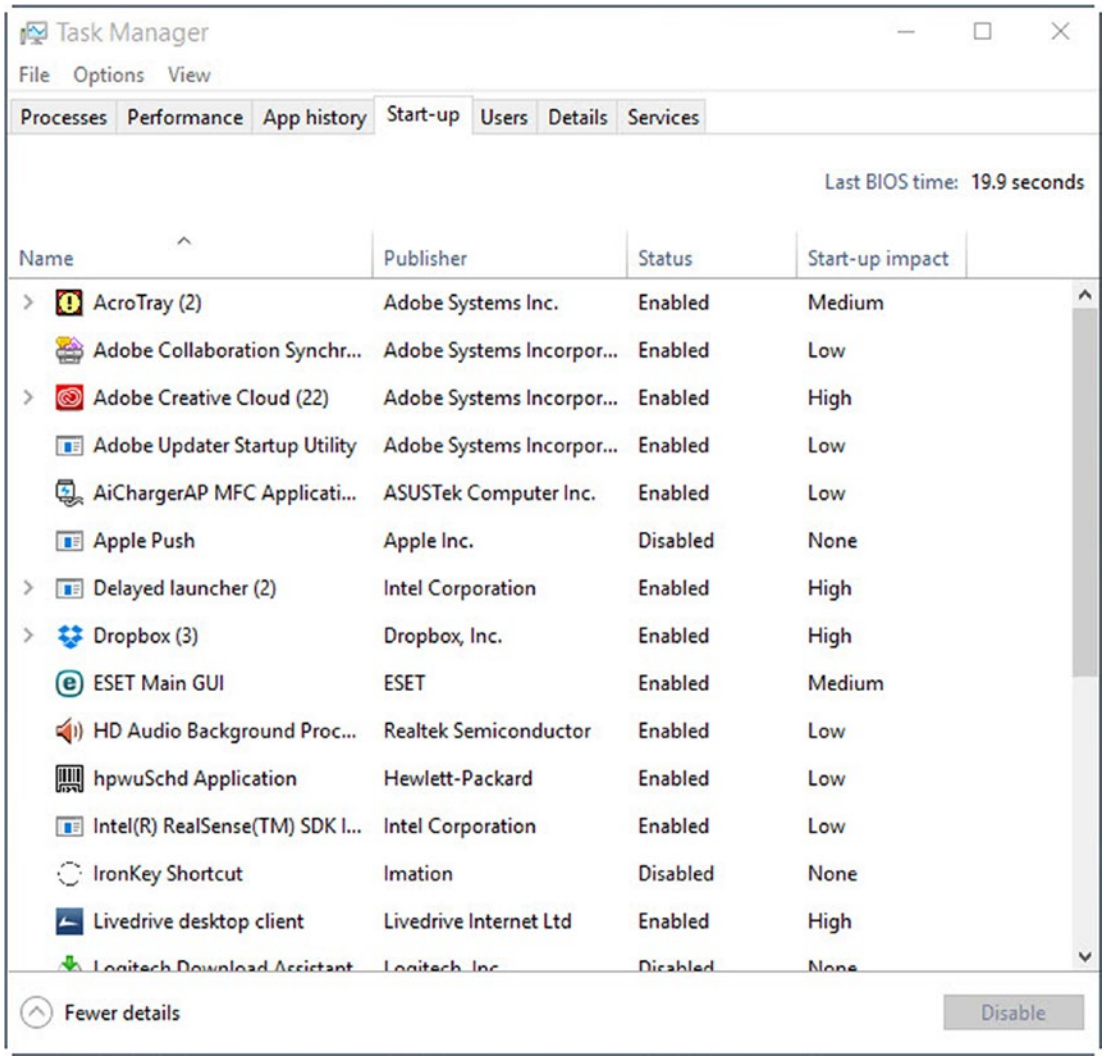


Figure 25-6. *You can manage your startup apps from the Task Manager*

The Performance Monitor

If you need to monitor more live metrics on your PC than the Task Manager can display, then the Performance Monitor is where you want to head. Everything that it's possible to monitor in Windows or on your PC can be displayed by live metrics in the Performance Monitor, from Bitlocker throughput to telephony connections.

The Performance Monitor displays a constantly updating graph above a series of checkbox options. By default, the processor time is displayed, but you can add any other metric to the graph by clicking the green *(+) Plus* icon on the toolbar. This will present a

list of all the available metrics on your PC; see Figure 25-7. Select the metrics you want to add to the graph, and click the *Add* button. Once metrics are added, they can be removed by pressing the *(X) Remove* icon, or by unchecking them below the graph.

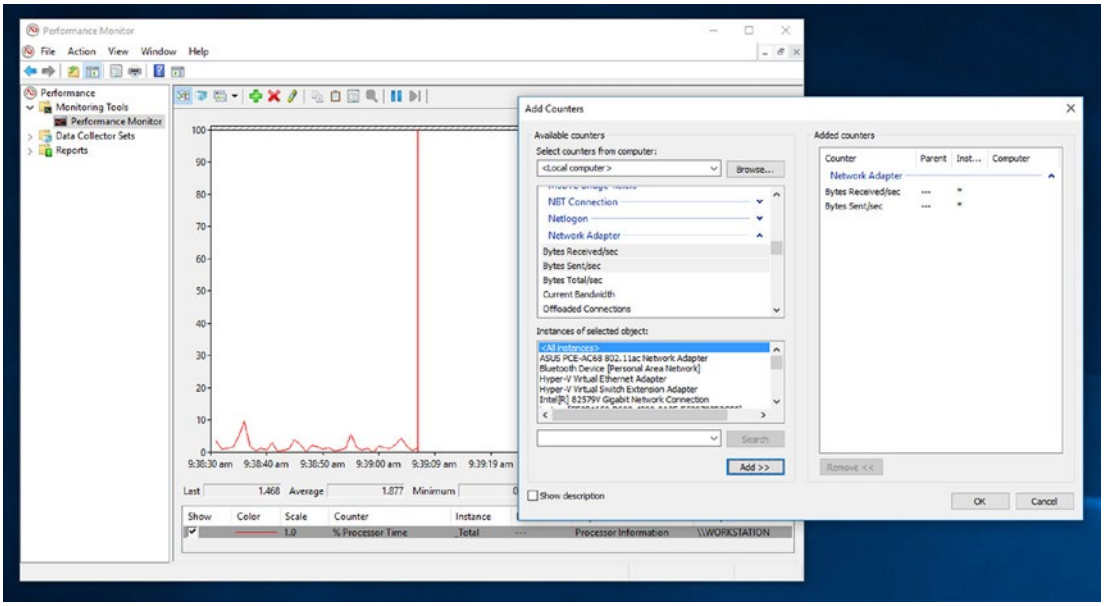


Figure 25-7. *The Performance Monitor can display hundreds of live metrics*

Tip If you have several metrics displayed in your graph but want to highlight one, select it in the panel below the graph, and then click the *Highlight* icon in the toolbar.

Data Collector Sets

Sometimes you need to collect data on the operation of the PC to read later, as you will be unable to read the data live and when it happens. You can achieve this through the creation of Data Collector Sets. You can set these to monitor any available metric, which includes events for Windows features, Registry key changes, and general performance. These collector sets can be viewed later in the Performance Monitor.

You create a new Data Collector Set by clicking the *Data Collector Sets* ➤ *User Defined* link in the left panel of the Performance Monitor, and then right-clicking a blank space in the main panel and selecting *New* from the context menu that appears.

You will be asked if you want to create a Data Collector Set from a predefined template or manually. If you choose manual, you will be given full control over the data collected from everything available to you; see Figure 25-8.

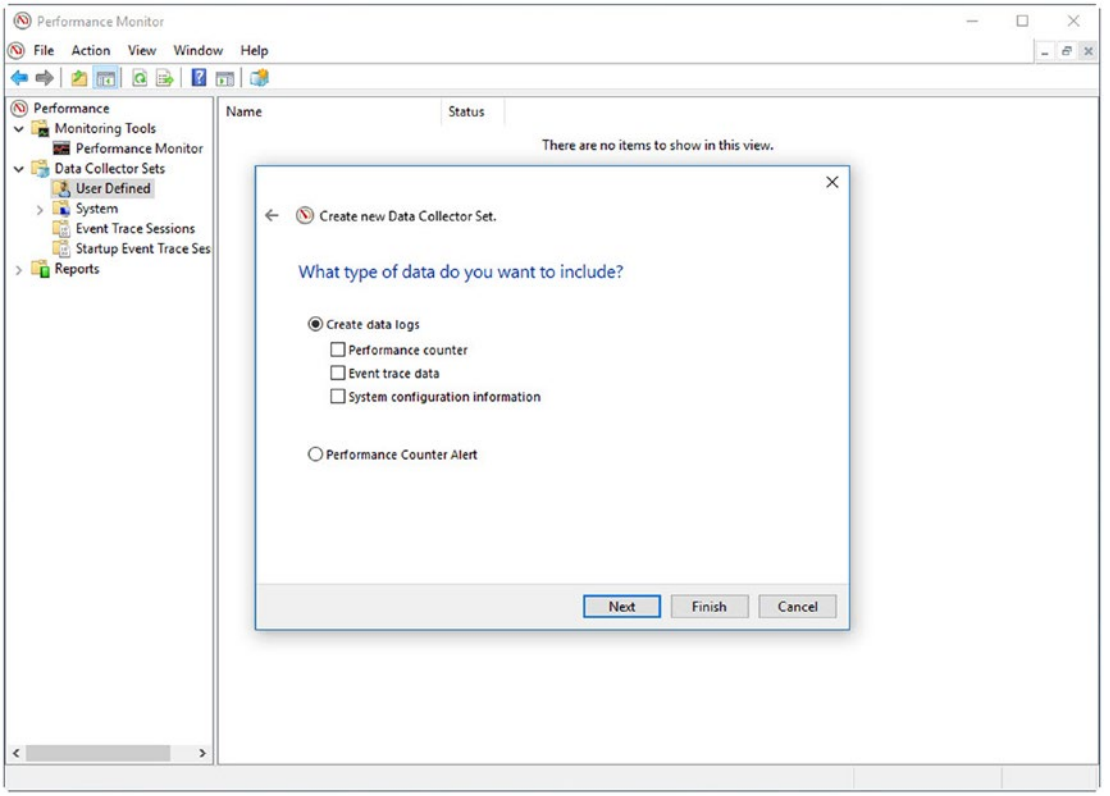


Figure 25-8. *You can create custom Data Collector Sets*

To view the data collected, you can at any time right-click the Data Collector Set to display its report. This will display in a new Reports section, which will display in the bottom left side of the window.

The Resource Monitor

Another way to view live information, and more detailed information than can often be provided by the Performance Monitor, is to use the Windows 10 Resource Monitor. This consists of a series of collapsible panels and tabs, and allows you to look at detailed breakdowns of what is happening at any one time with the PC's CPU, memory, disk, and network usage; see Figure 25-9.

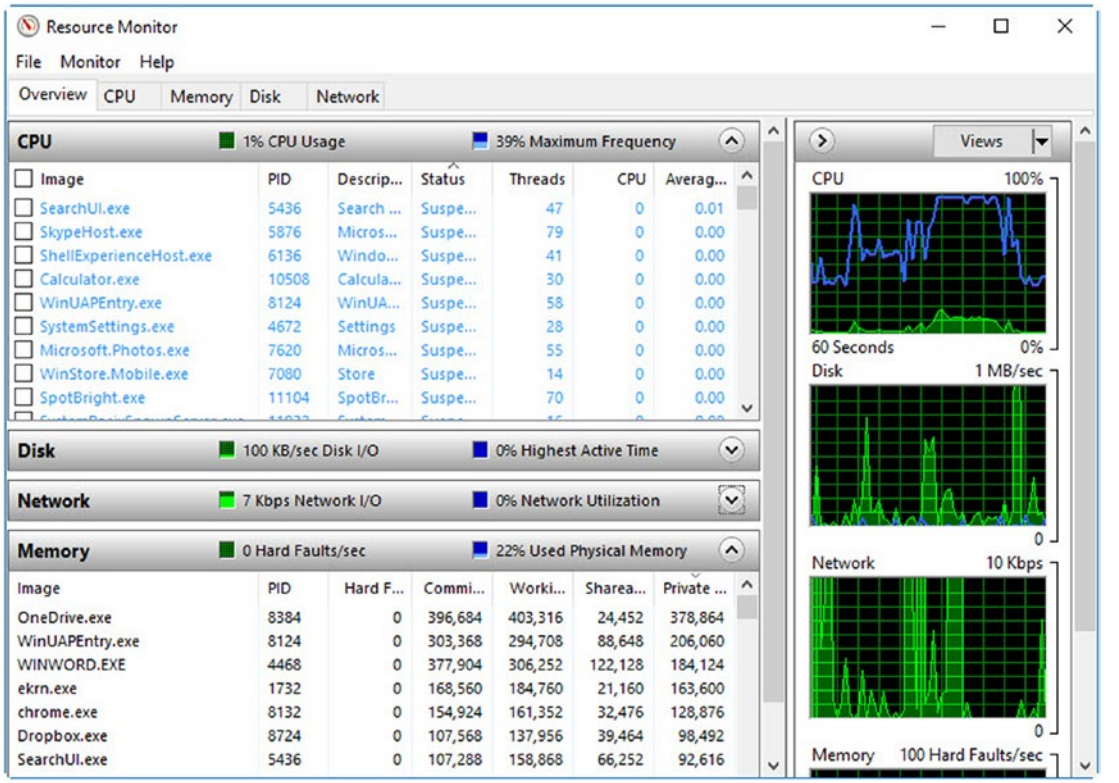


Figure 25-9. *The Resource Monitor displays very detailed metrics*

The Overview tab will give you details of all running processes: their memory, disk, and network usage. You can break this information down further, however, with the tabs along the top of the window. The CPU tab, for example, lists all running processes and services, along with their CPU usage.

Perhaps the two most useful tabs, however, are disk and network usage. The disk usage tab will show you every live disk activity, along with the read and write operations, and how much data is being read and written, by each specific app that is using the disk. You can use this if you suspect that a particular app is being a disk hog on your PC.

The Network tab is a fantastic tool for monitoring network issues and snarl-ups. Let's say, for example, that you suspect that the OneDrive sync engine isn't doing anything when it should. You can see in the Network tab exactly how much network bandwidth it is using. Alternatively, you suspect that an app is communicating with a system it shouldn't, perhaps because of a macro or another type of malware infection. The network tab can provide the IP address of the remote server. It can also provide details of the communication port(s) that an app is using, or trying to use. If you have an app, or perhaps a game, that's not communicating with the Internet properly, you can see which port it is using, and then check in the Advanced Firewall if that port is blocked for the app.

The Computer Management Console

Throughout this book I've detailed how you can use Windows 10 features such as the Event Viewer and Performance Monitor to get useful information about the Windows operating system and the status of your PC. The Computer Management Console, available from *Win+X menu*, provides access to some of these tools, as well as access to the Disk Management Console and the Device Manager.

Perhaps more useful, however, is the instant information it can give you on the status of folder shares and user and user group permissions. It allows you to view at a glance all of the folder and drive shares currently configured on the PC, useful if you suspect that a share is misconfigured or if another PC is unable to connect to it; see Figure 25-10.

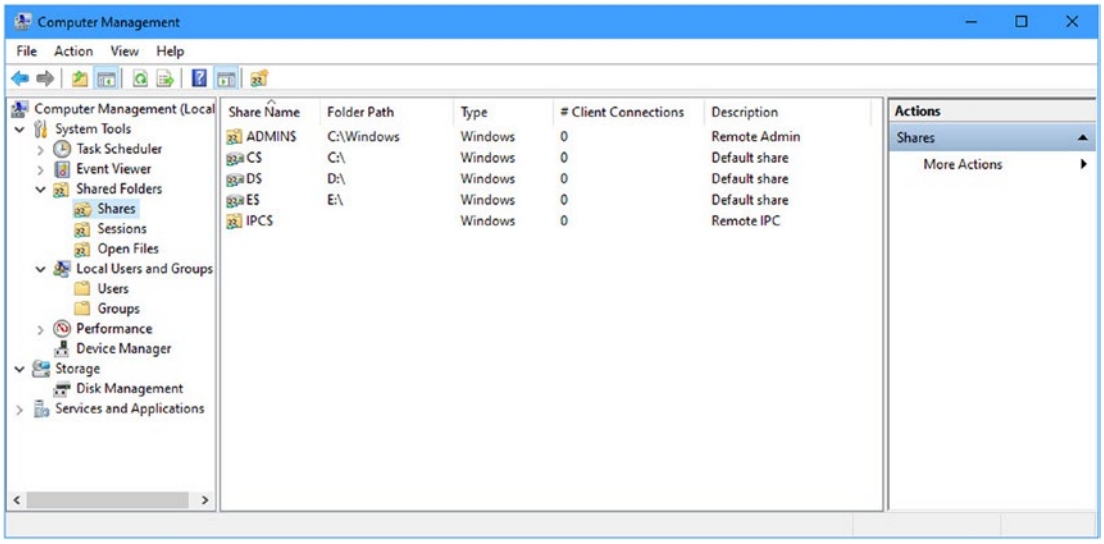


Figure 25-10. *The Computer Management Console provides quick access to useful tools and information*

Additionally, the Computer Management Console will display the details of any currently open folder or drive shares, with details of the PC and user connected to the share. You can also see what files are being shared, so you can get a huge amount of information about the current status of those shares. This can be useful if a user is trying to perform an action with a file or folder but permission is denied because the file is locked. Rather than just restarting the PC to unlock the file, you can first check here to see if the file or folder you need to work with is being accessed or used by another user, on another PC.

The User Groups section will detail all of the different groups of users that are configured on the PC, such as Administrator and Standard user, and you can see at a glance who is assigned to each group. You can also change the groups that a specific user is a member of. You can't change individual permissions from here, such as read, write, and modify permissions for users, but other features such as disabling an account temporarily or permanently are available.

System Information

Have you ever wanted to know absolutely **everything** about a PC? I don't mean what type of processor is installed, and how much memory, but what drivers are installed for the graphics card, what the MAC (physical) address of the PC's network adapter is, or what hardware devices are sharing interrupt requests (IRQ), ports, or memory addresses. I thought you might.

The System Information panel, available through the Administrative Tools window, is your one-stop shop for everything you could ever want to know about a PC; see Figure 25-11. This includes what hardware is installed, with the version numbers of the drivers; what apps are installed, again with version numbers; what print jobs are stuck in the queue; and the port addresses of the printers they're sent to. It can also tell you the full root of all the apps that begin at the PC's startup and what network protocols are configured on the PC.

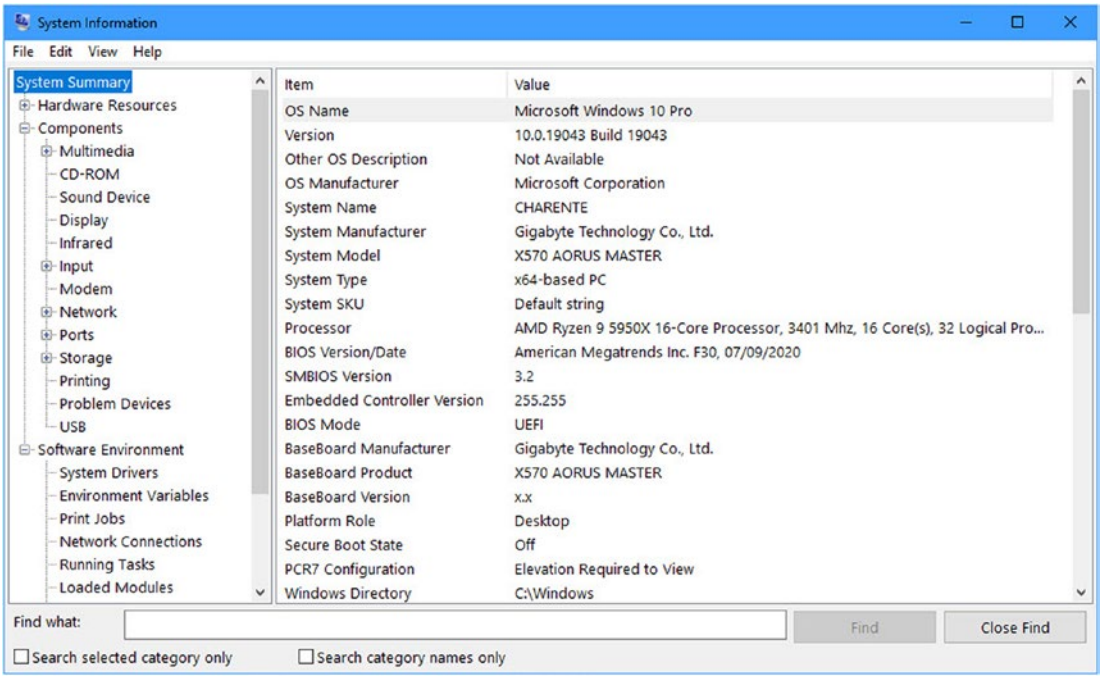


Figure 25-11. *The System Information panel is your one-stop shop for PC info*

What's even better about the System Information panel is that all of this information can be exported and emailed to a support person, or read on another PC. From the *File* menu, click *Save* or *Export,* and you will be able to create a text file containing everything you need to know about the PC. Save will create a file that can be opened in the System Information panel on a different PC, using the *Open* option, while Export will create a plain text (.TXT) file containing the information.

You can also use the System Information panel to obtain information about other computers on your network that you have administrator access into. From the *View* menu, click the *Remote Computer* option, where you will then be able to type the name or address of the remote PC.

DXDiag

Sometimes you may suspect you have a problem with your audio or video on a PC, but how do you go about diagnosing the issue? Microsoft has for years now included the DirectX Diagnostic tool (DXDiag) in Windows, and with Windows 10 it's still present and can be found by searching for **dxdiag** in the Start Menu. You can use this tool to get detailed information about the status of your audio and video equipment, check that your hardware and software drivers are digitally signed, and export that information in a text file format for other people to read.

The Display tab, for example, will provide information on whether features such as 3D and graphics acceleration are enabled on the device; see Figure 25-12.

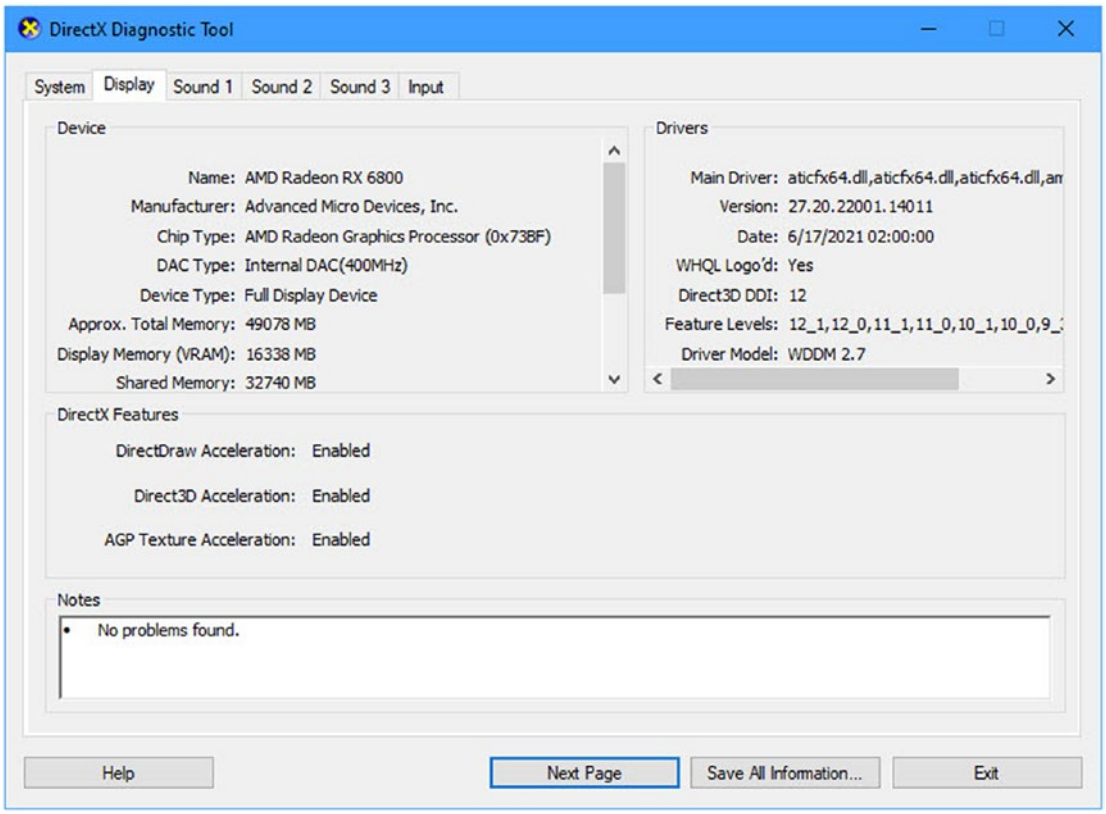


Figure 25-12. *DXDiag provides information on your audio and video equipment*

DXDiag will automatically check for problems with your audio and video hardware and report on any that it finds. You also get useful information such as the version numbers of any installed hardware. This means you can check the driver information from your PC against the manufacturer's website, and their forums, to see if there are any known problems.

Summary

There is a massive amount of information you can get from Windows 10 about the current and past status of your PC, and the tools detailed in this chapter should not be underestimated. Indeed, being able to create Data Collector Sets in the Performance Monitor and have them monitor from any one of hundreds of different metrics and collate that information into a report you can read at a later time is incredibly powerful.

Another part of the Windows OS that's incredibly powerful but also unbelievably complex is the Registry. In the next chapter, I'll give you a full tour of the Windows Registry and show you what each of its different parts is for, how you can work with it safely, and how to create backups and restore those backups at a later point in time.

CHAPTER 26

The Registry in Depth

The Registry is at the heart of everything that happens on your PC. Indeed, absolutely nothing *can* happen, including drivers and services being loaded at startup, to configuration changes and app usage, without the Registry being referenced, or without a Registry change being made. It is, quite simply, the brain of the PC.

Back in the days of Windows 3.1, you might remember, each program you installed had its own `.ini` file. This was a plain text document in which you would set configuration options for the program, such as the folder the program was installed in. Windows 95 did away with all of this manual nonsense and introduced the Registry, where all of the configuration links, settings, and options were handled automatically by both Windows and the program.

The Registry files are no longer plain text. They are binary format files that are not readable in a text editor. This is different from the `.reg` files, which are exportable and importable into the Registry and are in plain text format; see Figure 26-1.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_26

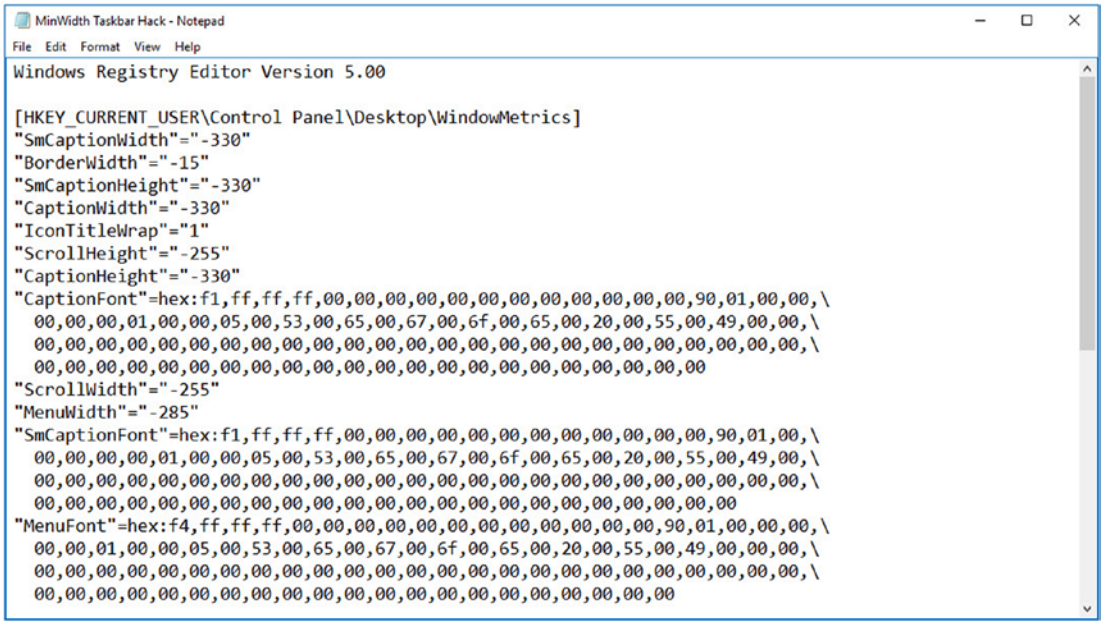


Figure 26-1. *A .REG file opened in Notepad*

As you can imagine then, the Registry is a huge, complex, and confusing database. If something goes wrong with it, such as a configuration change being made that causes something to become unstable, then just finding what you're looking for can be a monumental challenge in itself. Indeed, the Registry is so complex that I wrote, with fellow MVP Andrew Bettany, a whole book on it, which you can buy from Apress in the same Windows Troubleshooting range as the book you're reading now. It's *Windows Registry Troubleshooting* (Apress, 2015). For now, though, I'll give you all the information you need to get up to speed on what the Registry is, and how it works.

Registry Files

The Windows Registry isn't one big database that's stored in a hidden location on your PC. In fact, it's a collection of files scattered across various locations on your hard disk. The core Registry files on the PC are to be found in the `%systemroot%\System 32\Config\` folder; see Figure 26-2. They consist of the following files.

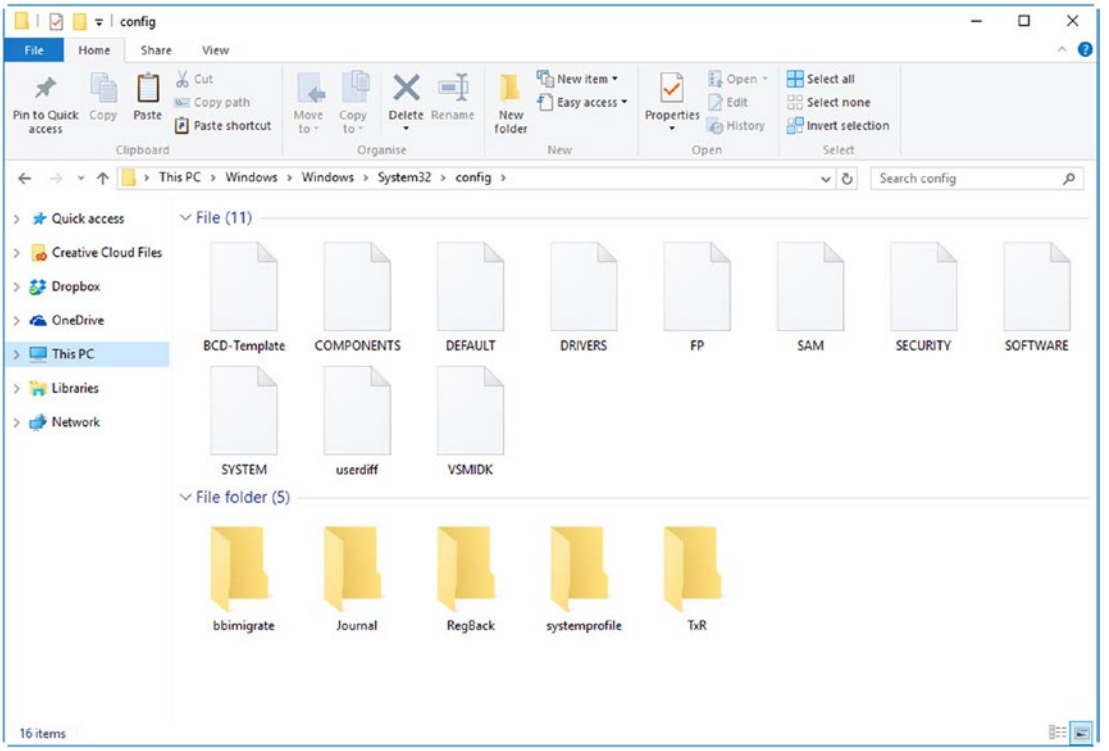


Figure 26-2. *The Core Registry files on the PC are hidden in the System 32 folder*

- `SAM` (Security Accounts Manager)
- `SECURITY`
- `SOFTWARE`
- `SYSTEM`
- `DEFAULT`
- `userdiff` (used only when the OS is being upgraded)

In addition to these, each individual user account on the PC has its own Registry files, which contain their person configuration and app options:

- `%userprofile%\ntuser.dat`
- `%userprofile%\AppData\Local\Microsoft\Windows\UsrClass.dat`

The `ntuser.dat` file is the one that contains the user's customization, app installation, and configuration options. The `UsrClass.dat` file contains additional settings for the user, such as user-specific file associations.

Registry Keys and Values

When you open the Windows Registry Editor, which is the only way to work with the Registry in the OS, you'll see that the Registry is arranged into a folder structure; see Figure 26-3. I'll show you how to use the Registry Editor later in this chapter, though you open it by searching for *regedit* at the Start Menu. For now, I want to walk you through the different Registry sections and key types.

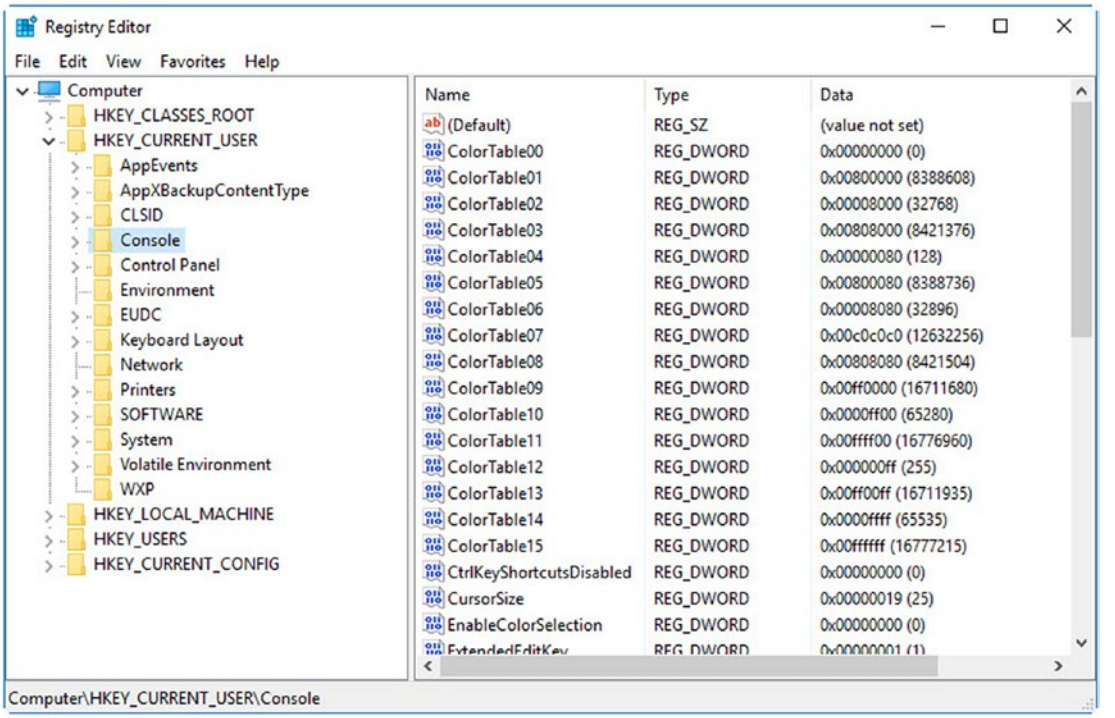


Figure 26-3. *The Windows Registry Editor*

HKEY_CLASSES_ROOT (HKCR)

This section of the Registry is where registered app information is stored. This includes file associations. Should a key be added or updated in HKCR that is also duplicated in the HKEY_CURRENT_USER\Software\Classes section of the Registry, the HKCU key will be used as the master, as it is specific to the individual user's preferences.

HKEY_CURRENT_USER (HKCU)

This Registry section is where the configuration options for the currently signed-in user are located. This includes the disk locations for user folders, control panel settings, and app installation and configuration settings. This section is loaded from the `%userprofile%` folder Registry files.

HKEY_LOCAL_MACHINE (HKLM)

If you're going to be making a change to the Registry, then it's most likely going to be in HKLM. This is where all the settings for Windows, drivers, and app installations are to be found, that is, all the settings and options that are generic for all users of the PC. It is split into several subsections that relate to some of the Registry files I detailed earlier.

SAM

The Security Accounts Manager will commonly appear to be empty unless the viewing user has appropriate security permissions. This Registry section contains the security information for any domains that the PC connects to.

SECURITY

The Security section also appears empty for most users, again unless the viewing user has appropriate permissions. It is used when connecting to a domain and is linked to the security database stored in the Server Registry Hive. This contains all the security policies specified on the server that are applicable to the currently signed-in user and installed apps on the PC.

SYSTEM

The System section contains the keys that are relevant to the Windows installation, configuration, devices, and any drives attached to the PC.

SOFTWARE

As you might guess, this section is where the keys and configuration settings for all installed win32 apps are to be found. This section is organized into subfolders labeled by the vendor name for the app.

Other Sections

There are other subsections in HKLM, including `DRIVERS` and `HARDWARE`. These are created when the user signs into the PC and discarded on sign-out.

HKEY_USERS (HKU)

The HKU section contains settings and options for the currently signed-in user. It cannot be used to access settings for any other user on the PC unless you sign out and sign in as that other user.

HKEY_CURRENT_CONFIG (HKCC)

The last section, HKCC, contains information that is gathered at the PC's startup and that is relevant only to the current working session for the PC. It is created automatically and discarded when the PC is shut down.

HKEY_PERFORMANCE_DATA

Okay, so there really is another Registry section, but it's hidden from the user and nonviewable in the Registry Editor. This contains performance data provided by the Windows kernel, drivers, apps, and services. It relates only to the current operating session of the PC and is discarded when the PC is switched off.

Registry Value Types

Within these five main Registry categories, there are a series of different types of values:

- REG_BINARY keys store raw binary data.
- REG_DWORD are variable-length 32-bit integers.
- DWORDS are commonly used to define parameters for strings, settings, drivers, and configuration options.
- REG_SZ are field-length string values.
- REG_EXPAND are expandable length string values, also used to contain environment variables.
- REG_MULTI_SZ are multiple string arrays that can contain a list of values, normally separated by a comma or space.
- REG_RESOURCE_LIST is a list of resources in a nested array; these are used by device drivers.
- REG_RESOURCE_REQUIREMENTS_LIST is an array list of hardware resources that is used by device drivers.
- REG_FULL_RESOURCE_DESCRIPTOR are nested arrays used to store resource lists for physical hardware.
- REG_LINK are symbolic links to other Registry keys. They specify both the root and target key.
- REG_NONE is data that does not have a specific type.
- REG_QWORD are variable-length 64-bit integers. These are not found in 32-bit editions of Windows 10.

Where You Will Find Important Registry Settings

Having access to the Registry and being able to create, modify, and delete individual keys is one thing, but locating what you're actually looking for in such a large database can seem daunting. There are a few common areas however that you will find yourself in where the most important and relevant Registry keys will always be found:

- **HKEY_CURRENT_USER ➤ Control Panel**–is where you will find Control Panel Registry values related to input, accessibility, and desktop appearance.
- **HKEY_CURRENT_USER ➤ Software**–is the location for installed apps (normally win32) settings and configuration.
- **HKEY_CURRENT_USER ➤ Software ➤ Microsoft ➤ Windows ➤ CurrentVersion**–is where you will find settings related to Windows.

HKEY_CURRENT_USER ➤ Software ➤ Microsoft ➤ Windows ➤ CurrentVersion ➤ Explorer–is the location for desktop configuration options for the current user including the all-important *User Shell Folders*. Additionally, there are a series of Registry keys that store information about all your installed software. You can find all of these keys at

- HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
- HKU\<User SID>\Software\Microsoft\Windows\CurrentVersion\Uninstall
- HKU\<User SID>\Software\Microsoft\Installer\Products
- HKLM\Software\Classes\Installer\Products

The Registry Editor

You can view, manage, and edit the Registry using the Windows 10 Registry Editor, opened by searching in the Start Menu for *regedit*. This is an editor that loads all of the separate Registry files into a single place, where all the keys and subkeys are sorted and arranged in plain English (well, as plain as you can be when you're a technical repository, anyway).

In the left panel of the Registry Editor is a collapsible panel of all the Registry files, showing their full folder (hierarchical) structure. The right panel will display all the keys at the currently selected hierarchy point. Additionally, there are traditional pull-down menus that allow you to perform various actions, such as adding, deleting, and renaming keys and folders; see Figure 26-4.

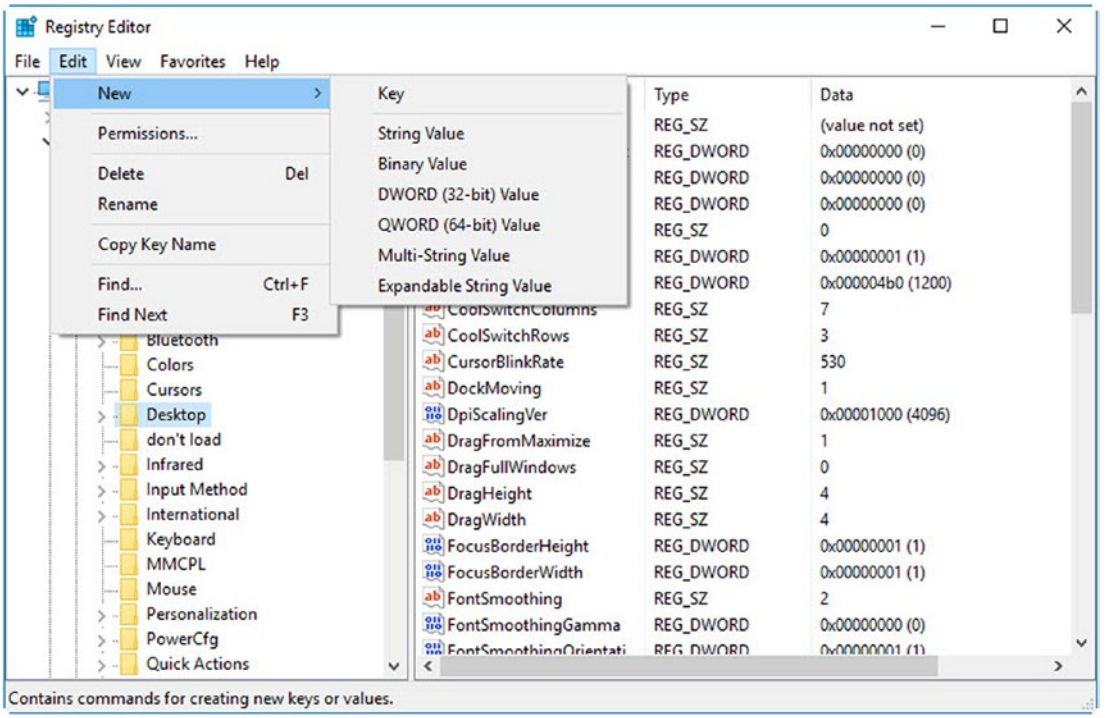


Figure 26-4. *You work with the Registry in the Registry Editor*

Backing Up and Restoring the Registry

Before you begin modifying, creating, or deleting Registry keys, you should always make a backup copy of the Registry, you know, in case something goes horrifically wrong. You can back up and reimport the Registry from the *File* menu; see Figure 26-5. This saves a copy of the Entire Registry in a plain text .reg file to any folder or drive you specify on your PC.

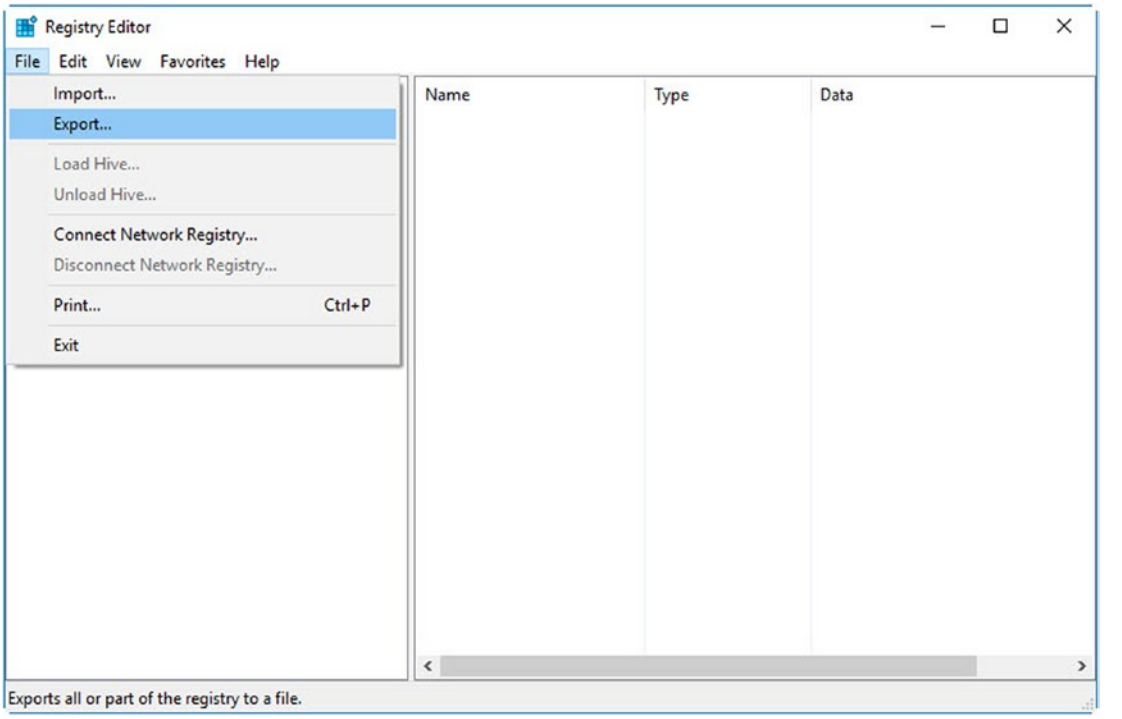


Figure 26-5. *You should always create a Registry backup when working on keys*

Tip You can also make backup copies of any particular key by right-clicking it, in the left panel of the Registry, and selecting *Export* from the options that appear.

Creating and Modifying Registry Keys

You can create new Registry keys and values by right-clicking the appropriate part of the Registry; see Figure 26-6. This allows you to create any type of key or value you require including both master and subkey types.

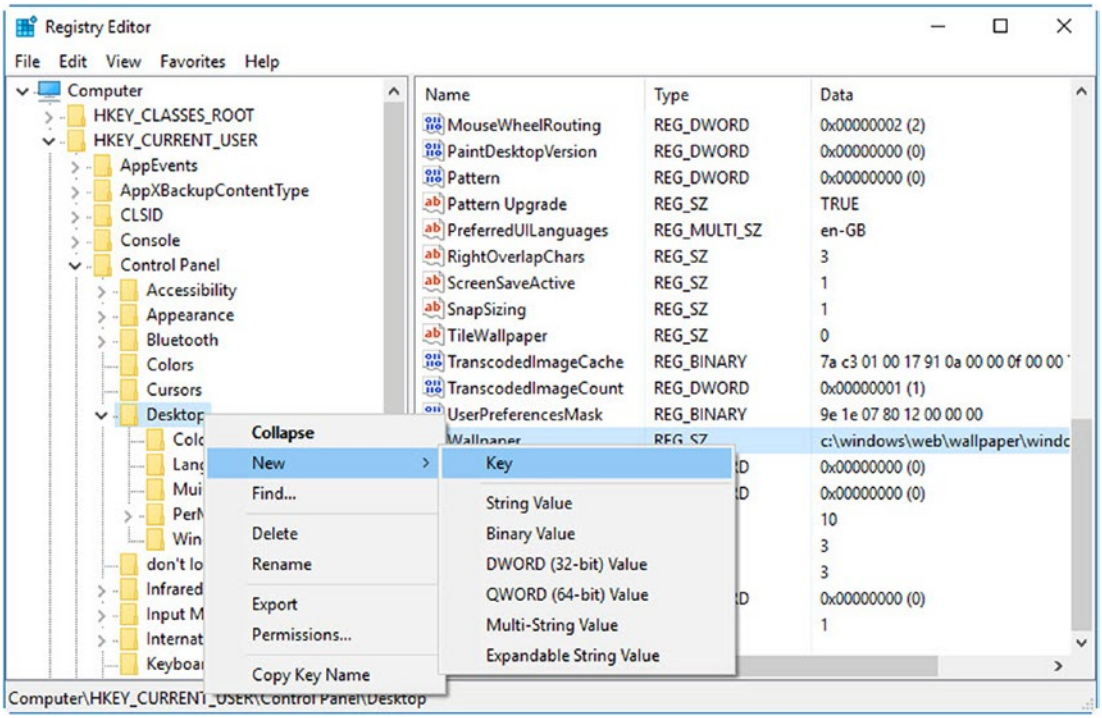


Figure 26-6. *You can create new keys in the Registry*

To edit a Registry key, right-click the key or value you want to edit, and several options will become available to you; see Figure 26-7. It's the main *Modify* option you'll need most of the time.

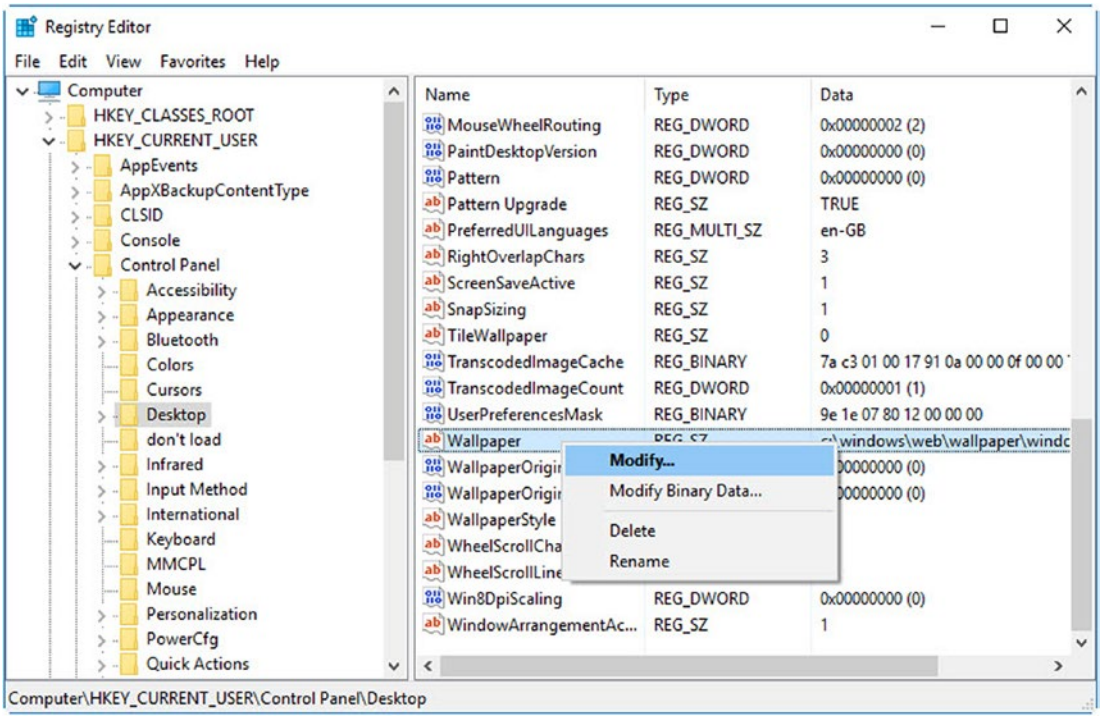


Figure 26-7. *You modify Registry values on a right-click*

Using REG.EXE and REGINI.EXE

If you're a command-line purist, you can use the `reg.exe` command to edit the Windows Registry; see Figure 26-8. You should always be very careful as you can't actually "see" the Registry when you're working on it in this way. There are many subcommands and switches when using `reg.exe`, and the full switch details can be found both in my *Windows Registry Troubleshooting book* (Apress, 2015) and on the Microsoft website at `technet.microsoft.com/library/cc732643(v=ws.11).aspx`.

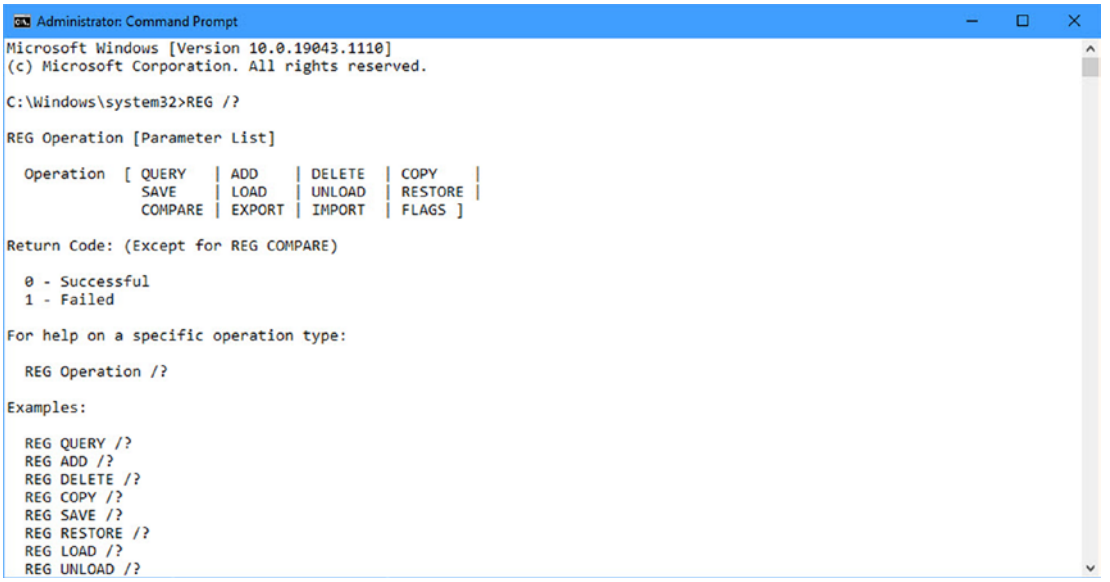


Figure 26-8. *You can edit the Registry from the Command Prompt*

You use REG.EXE in the format `REG /?` which will display a list of all the commands available. Using each of these with the `/?` Switch, for example, `REG ADD /?`, will display for command format further. REGINI.EXE is used in a similar way to REG.EXE but works with scrips written in plain text (.TXT) files. Again you can use it with the `/?` Switch to get information on how the command is used.

Note By default, Reg.exe works to match the version of Windows that is installed, be this 32 bits or 64 bits. To work specifically with other key types, you can use REG.EXE with the /reg:32 and /reg:64 switches.

Editing the Registry Using PowerShell

Most system administrators like to use Microsoft's PowerShell scripting tool for managing Windows installations, and you'll be pleased to hear that many dozens of commands exist to help you manage the Registry on a local and remote PC. You can find a full and complete list on Microsoft's website at the following link `http://pcs.tv/1x9NW1M`.

Tip To make sure PowerShell works as you expect it to, you need to check the command execution policy. You can do this in the PowerShell interface with the command **Get-ExecutionPolicy**, and you may find it is set to Restricted. You should then use the command **Set-ExecutionPolicy Unrestricted** so that your commands will run.

Useful commands you can use with PowerShell for managing the Registry include `Get-PSDrive` to display the list of disks in the PC that PowerShell has permission to interact with. PowerShell has access to only two user Registry files, `HKEY_CURRENT_USER` and `HKEY_LOCAL_MACHINE`, so it cannot be used to manage security or software keys. You can navigate to these Registry files with the command `CD HKCU:` and `CD HKLM:` and then use the command `DIR` to display information about them.

Editing the Registry from the Recovery Console

Sometimes you either can't get the PC to boot to the desktop or perhaps need to make a low-level Registry change that isn't permitted or available when you are in the desktop environment. If you start the PC into the Recovery Console however, which is most easily achieved by holding down the *Shift* key when selecting *Restart* from the Start Menu, you can still access the Registry Editor and Reg.exe.

When in the Recovery Console, select *Troubleshoot* ➤ *Advanced Options* ➤ *Command Prompt*, and after the PC restarts, you will see a Command window, automatically elevated with Administrator privileges, in which you can type **regedit** to start the Registry Editor, or in which you can use the *Reg.exe* command; see Figure 26-9.

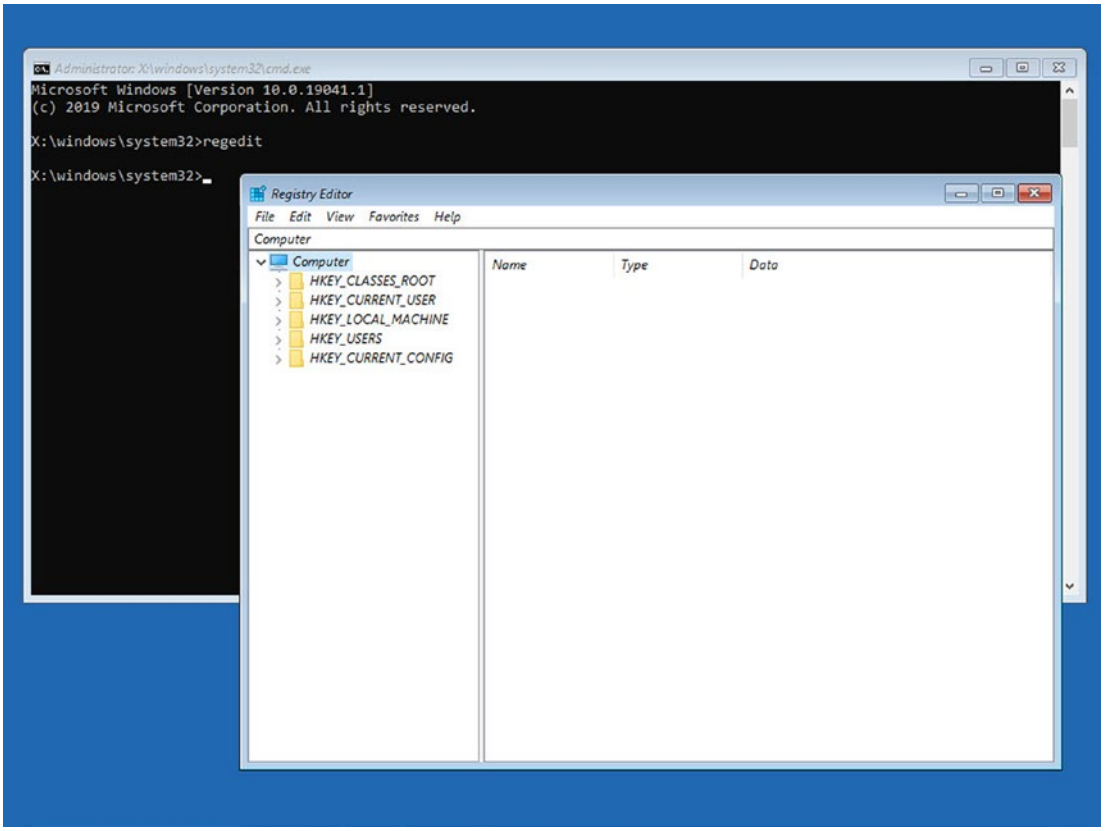


Figure 26-9. *You can edit the Registry from the Recovery Console*

Editing Other Users' Registry Databases

I mentioned earlier that it's only possible to view and modify the Registry of the currently signed-in user. In the normal Regedit view, this is true; however, it is also possible to view the HKU and HKLM registries of other users on a PC, and indeed across a network. To open the Registry files of another user on the PC, follow these instructions:

1. Sign into the PC as an Administrator.
2. Search for *regedit* at the Start Menu or in Cortana to run the Registry Editor.
3. Select the HKEY_USERS branch in the Registry Editor.
4. From the *File* menu, select *Load Hive;* see Figure 26-10.

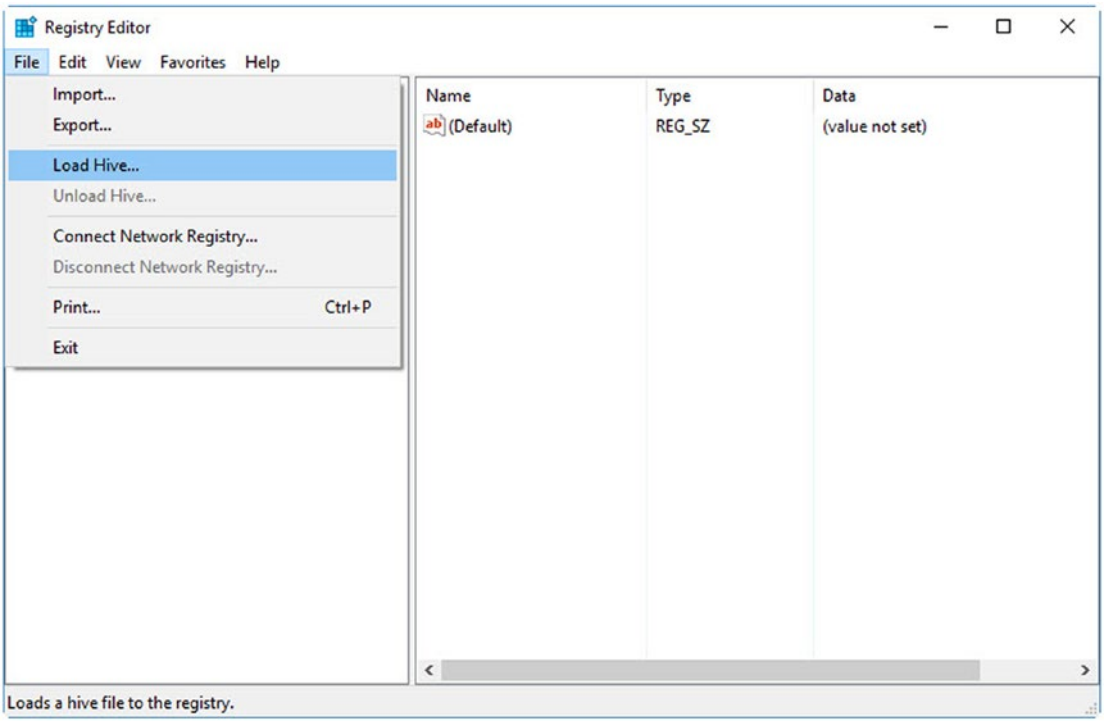


Figure 26-10. *You can connect to other users' Registries on the PC*

5. Browse to the user's profile directory on the hard disk, and select the `NTuser.dat` file.
6. When prompted for a key name, enter the user's username as a reference label.

You will now be able to view and edit the Registry files for that specific user in the Registry Editor. Note that you will need to set File Explorer to show both *Hidden* and *System* files to display the `NTuser.dat` file. You should also make sure that when you are finished with the remote Registry file, you should highlight it in the Registry Editor, and from the *file* menu, select *Unload Hive*.

There are several steps to go through. These are detailed in full in my *Windows Registry Troubleshooting* (Apress, 2015) book, though I will summarize them here:

1. In the Group Policy Editor, you need to allow *inbound remote administration exception* connections policy. You do this in Computer Configuration ➤ Administrative Templates ➤ Network ➤ Network Connections ➤ Firewall, and then in either the Standard Profile or Domain Profile sections.
2. Also in the Advanced Firewall, open TCP ports 135 and 445.
3. Activate the *Remote Registry* service in the *services* panel on the PC you wish to access remotely.
4. Open the Registry Editor, and from the *File* menu, select *Connect Network Registry*.
5. Enter the name of the PC and user you wish to connect to.

You will now see the PC listed in the Registry Editor, and two new branches will appear, `HKLU` and `HKU`. Once you have made the changes you need to make, be sure to disconnect the Registry Editor from the remote PC using the option in the *File* menu.

Tip If the PC won't boot, you can run the Registry Editor from a USB Recovery Drive. You do this by entering the Command Prompt option and typing regedit, from which the Registry Editor will appear. You will then be able to connect to different user's Registry files on the PC using the method I detailed earlier.

Connecting to the Registry of Another PC

It is also possible to connect to the Registry of another PC on your network. From the *File* menu in the Registry Editor, select the *Connect Network Registry* option; see Figure 26-11. This will allow you to select any PC on your network, and any user on that PC to connect to; remember that each individual user has their own set of Registry files.

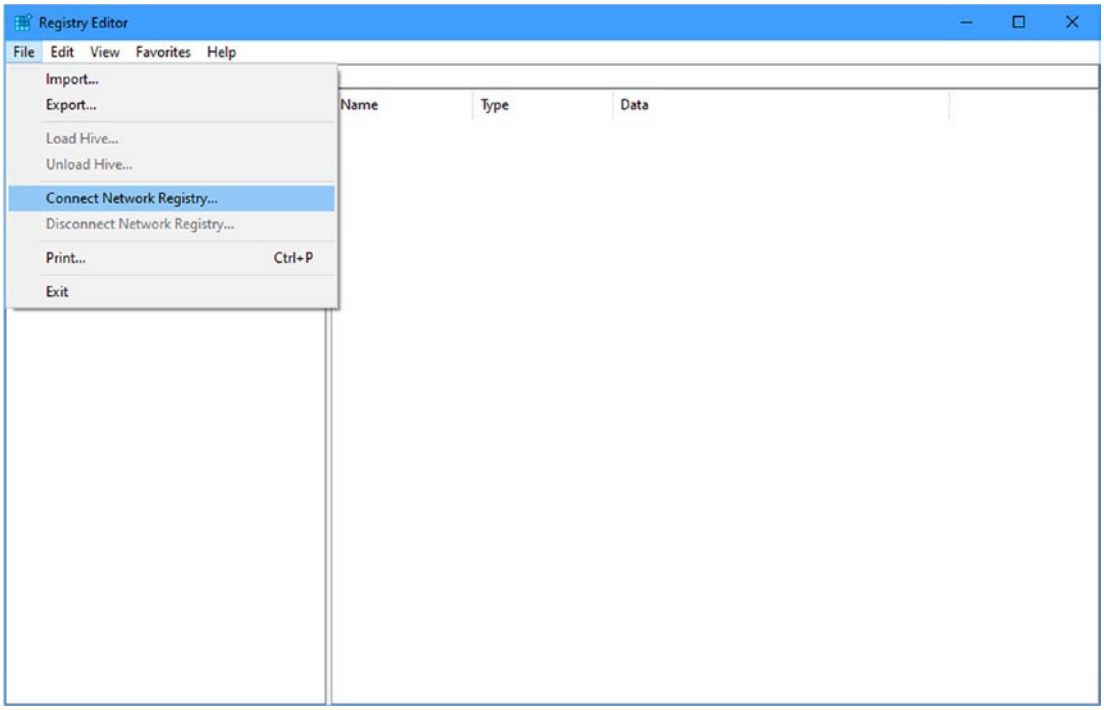


Figure 26-11. *You can connect to the Registries of other network-connected PCs*

Enabling Remote Administration on PCs

To be able to connect to a remote PC however, there are three things you must do first, the first of these is to enable the *Remote Administration* service. You can access this in the *Group Policy Editor*, search in the Start Menu for **gpedit,** and navigate to *Computer Configuration* ➤ *Administrative Templates* ➤ *Network* ➤ *Network Connections* ➤ *Windows Defender Firewall* and then either the Standard or Domain profile as is appropriate for your setup. Once here, look for the *Windows Defender Firewall: Allow inbound remote administration* rule, and enable it on all the PCs you want remote access to; see Figure 26-12.

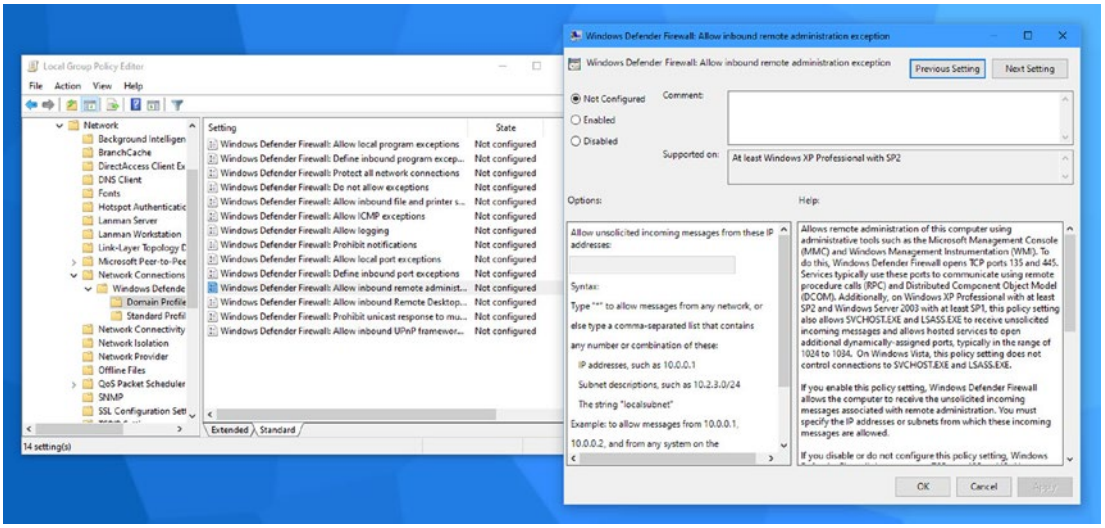


Figure 26-12. *You have to enable the remote administration policy*

Tip You can also enable or disable the Remote Administration policy from the Command Prompt by using the command `netsh firewall set service type = remoteadmin mode = [mode]` where `[mode]` is either `enable` or `disable`.

Next you need to open ports 135 and 445 in the Windows Firewall. Search in the Start Menu for **firewall,** and open the *Windows Defender Firewall with Advanced Security* option. Click *inbound rules,* and from the option in the top right of the window, create a new rule in which you can allow access through these two ports; see Figure 26-13.

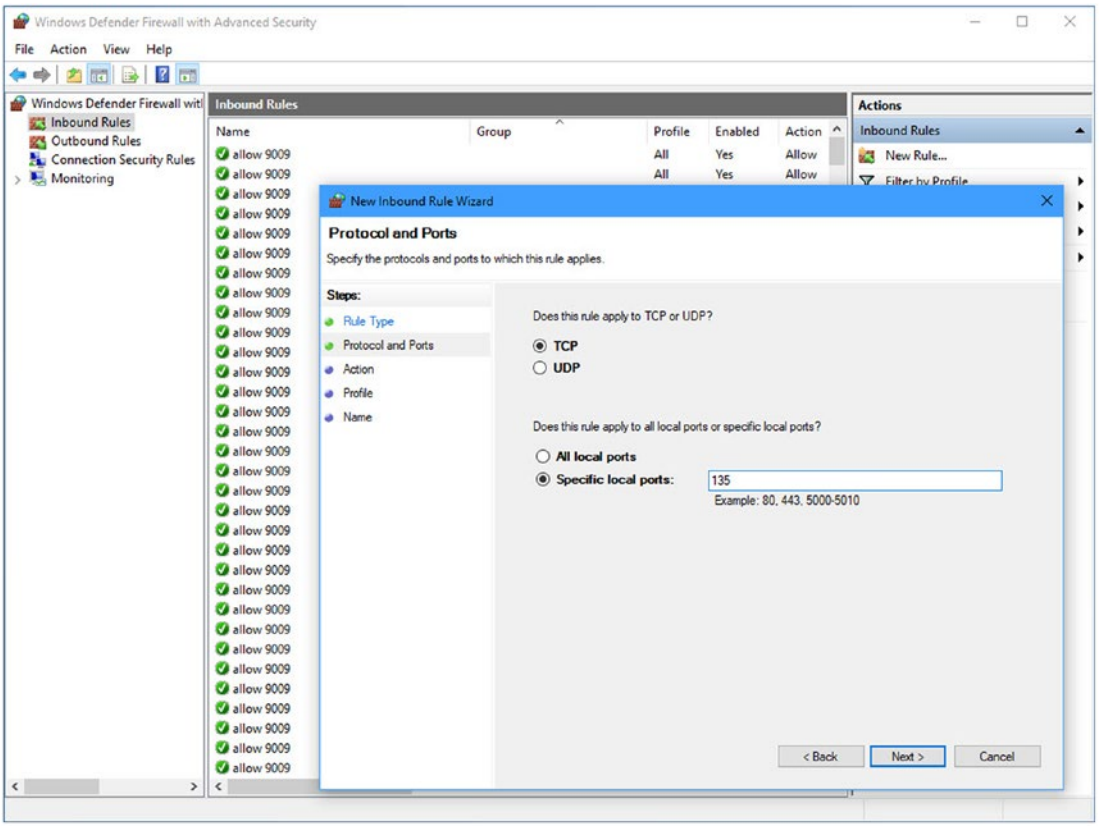


Figure 26-13. *You have to open two ports for the firewall*

The last thing to do is to enable the Remote Registry service. Search in the Start Menu for *services*, and when you have the Services panel open, scroll down the list until you get to *Remote Registry*. You need to set the status of this service to *Automatic* and then to *Start* it; see Figure 26-14.

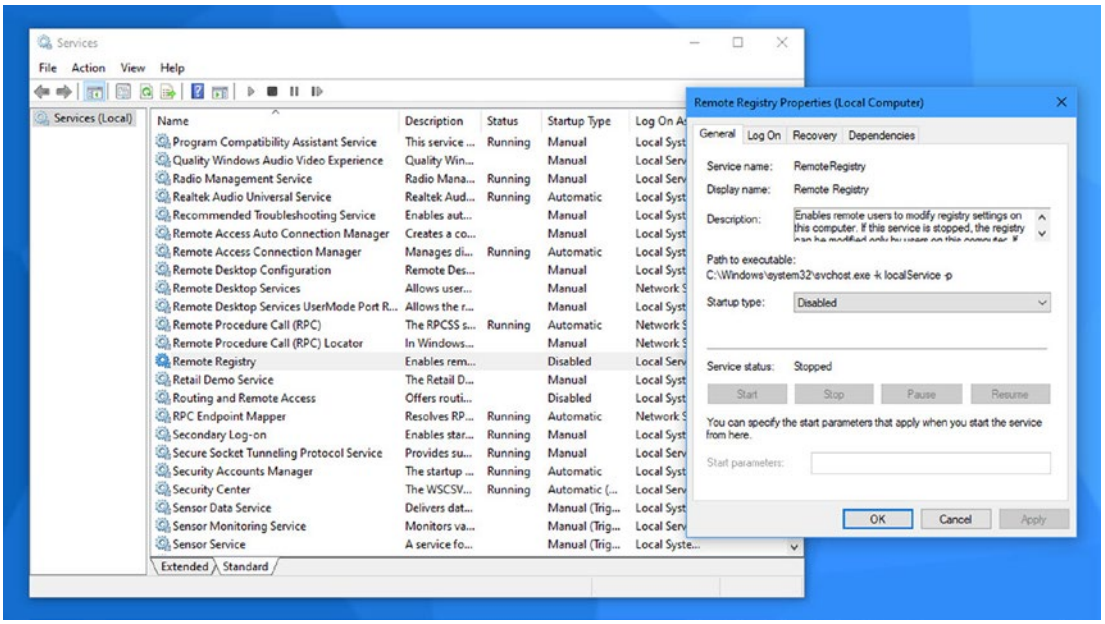


Figure 26-14. *You need to enable the Remote Registry service*

Tip You can also enable the Remote Registry service from the Command Prompt by typing `sc start RemoteRegistry` or by typing `sc config RemoteRegistry start = auto` to have the service start automatically every time Windows boots.

Third-Party Registry Utilities

I mentioned at the beginning of this chapter that the Windows Registry Editor is the only way to view and manage the Registry in Windows, and strictly just within Windows 10, it is. However, some useful third-party utilities exist that can also help, especially if the PC is unbootable. These all work in various ways, but the best tools available are

- **PCRegEdit**–found by searching online
- **Hiren's Boot CD**–`www.hiren.info/pages/bootcd`
- **Lazesoft Recovery Suite Home**, Recovery CD–`www.lazesoft.com/lazesoft-recovery-suite-free.html`

- **UBCD4Win**–ubcd4win.org
- **Microsoft Desktop Optimization Pack** (DaRT)–available through Software Assurance

Comparing Different Registry Files

In addition to third-party Registry editors and utilities, there are also third-party tools you can use to compare two Registry files. You might want to do this to compare the Registry files of a PC containing software or a hardware driver that is causing problems and cannot be cleanly uninstalled, with the Registry files on a similar PC on which this is not installed. Some of the tools you can use for this include

- **InstallWatch Pro** http://installwatch-pro.en.lo4d.com/
- **Process Monitor (Windows Sysinternals)** http://technet.microsoft.com/sysinternals/bb896645.aspx
- **Regshot** www.aplusfreeware.com/categories/util/registry.html
- **Tiny Watcher** http://kubicle.dcmembers.com/watcher/
- **Total Commander** http://ghisler.com/
- **What Changed** www.majorgeeks.com/files/details/what_changed.html
- **WinDiff** www.grigsoft.com/download-windiff.htm
- **WinMerge** http://winmerge.org

Summary

The Windows Registry is a very complex and utterly crucial part of the operating system. You should really only be editing it if you are following specific instructions from a hardware or software vendor, or from Microsoft itself, and you should absolutely know what it is you are doing. Making the wrong change in your Registry can not just result in hardware or apps misbehaving, but it can also render the entire Windows installation unusable.

You'll see that both the Command Prompt and PowerShell can be used to work with and edit the Registry. In fact, there's a great deal more that you can do with scripting to help you troubleshoot and repair problems in Windows 10, and in the next chapter, we'll look at how to get started with scripting tools, and what some of the more useful tools and commands are.

CHAPTER 27

Using Scripting Tools for Troubleshooting

One of the many problems IT pros can face with deployment and management of large numbers of computers is configuring each PC as you need it to be, with network configurations, Windows Update settings, Security and Firewall policies, Group Policy, security, malware, and so on. This is why Microsoft created the PowerShell scripting language in 2006. As I write this, it is now in its seventh version and has become a powerful and fully featured language in its own right.

Let's not discount the venerable Command Line however, as there are still things you can use this for where PowerShell simply cannot do the job; for example, it's still not possible to run PowerShell from the Windows Recovery Environment, but the Command Line is there for when you need it.

You can even plug additional scripting environments into Windows 10 by using the Windows Subsystem for Linux (WSL) such as Bash (which is one of the rarest things in tech as it's not actually an acronym for something).[1]

Throughout this book I've already detailed the most useful scripts and commands for configuring, managing, diagnosing, and troubleshooting problems for networking (Chapters 9 and 14), startup (Chapter 13), and the Windows Registry (Chapter 26), and we're still to cover file and folder management (Chapter 28).

[1] By far my favorite tech acronym is TWAIN, which is a now rarely used shorthand to describe scanners and a few other peripheral device types. TWAIN actually stands for "Technology Without An Interesting Name" and is by far the funniest tech acronym I've ever heard. As an aside you might find it amusing that the first webcam was invented by students at Cambridge University in 1991, so they could keep an eye on a coffee pot which was at the end of a long hallway from where they sat and was always empty whenever they went for to refill their cup.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_27

I'm not going to treat this chapter as a full an in-depth resource for the Command Line and PowerShell however, as there are whole books for that and a visit to www.Apress.com will reveal a large library of PowerShell guides as well as expert guides to using Bash. But there's little point in giving you useful scripts and commands to use without also giving you details on the best and most effective ways to use them.

In this chapter then we'll look at how you can use commands and scripting, what tools are available to help make this easier for you, and also some additional commands that come in very handy for troubleshooting.

The Windows Command Line

The Command Line has been in Windows since 4 years before Windows was first released, as it was the main and only interface for Microsoft MS-DOS. Let's not forget that DOS stands for Disk Operating System, as it was considered a full OS at the time. Indeed, DOS remained the operating system that Windows ran on top of for many years, and it wasn't until Windows 95 that DOS was hidden from the user, and finally relegated to a subfeature with Windows NT 4 in 1996.

The Command Line is still in Windows 10, though it's been deprecated further with Windows 11 because of the inclusion of the Windows Terminal (more in this later in this chapter). It remains highly useful though if for no reason than it's still the only scripting environment available in the Windows Recovery Environment (WinRE while we're getting all excited about acronyms).

The most obvious way to access the Command Line is to search for **command** in the Start Menu, where it's still referred to as *Command Prompt* (line being a term that better describes its terminal interface) where you can run it with Administrative privileges by right-clicking it. You can also access it from the *Win+X* pop-up menu from the Taskbar, but you need to enable it. This can be done in *Settings* from *Personalisation* and then *Taskbar* and deselecting the snappily titled option *Replace Command Prompt with Windows PowerShell in the menu when I right-click the start button or press Windows logo key + X*; see Figure 27-1.

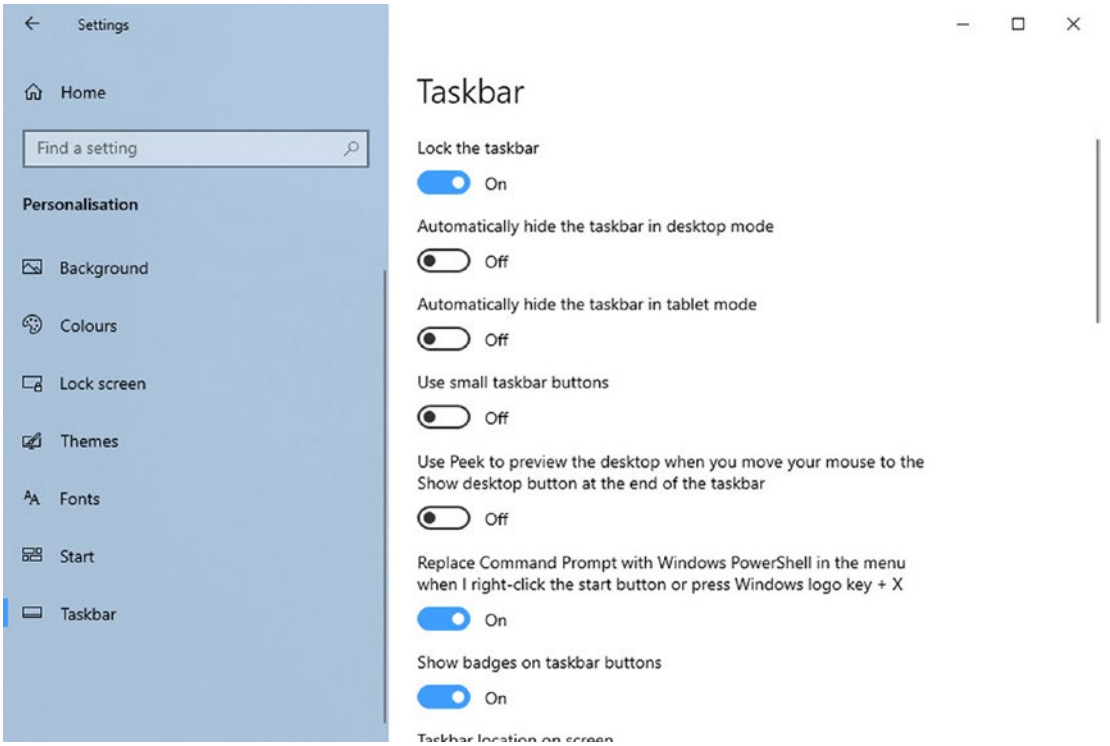


Figure 27-1. *You can enable Command Prompt in the Win+X menu*

Additionally, as I've already mentioned, the Command Prompt can also be accessed from the Windows Recovery Console. This can be especially useful if you're trying to perform an action that is locked by the operating system, perhaps because a file is open, or a system folder is locked and inaccessible. You can start Windows 10 into the Recovery Console in four ways:

- Hold the *Shift* key when selecting Restart from the Start Menu or lock screen.
- Start the PC from a USB Recovery Drive.
- Start the PC into the Recovery Options menu (see the following for how to do this), and select *Troubleshoot* ➤ *Advanced Options* ➤ *Startup Settings* ➤ *Restart* and then *6–Enable Safe Mode with Command Prompt*.
- Press and hold the power button for 4 seconds while Windows is starting. Do this three times, and the OS will think there's a problem and launch recovery, thought this really is the last resort option

When you're in the Recovery Environment, click *Troubleshoot* and then *Advanced options*, and then you will see *Command Prompt*; see Figure 27-2. The PC will restart, and you'll be faced with a Command Prompt interface.

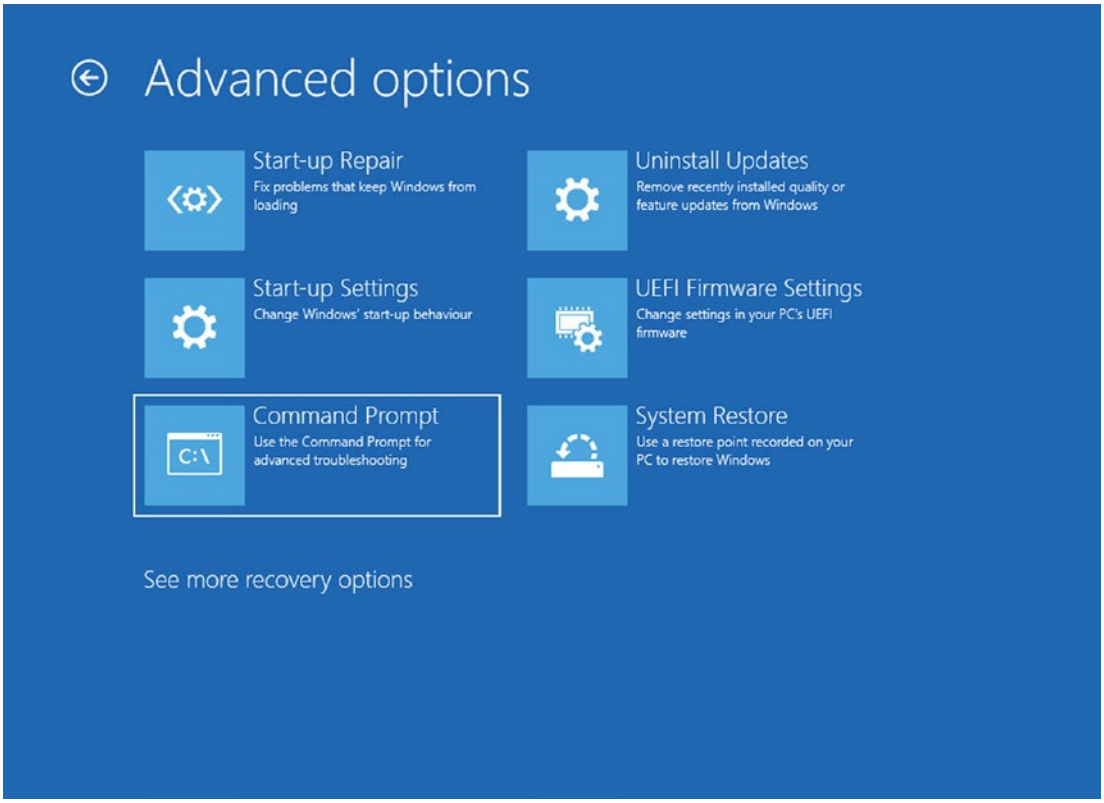


Figure 27-2. *You can access Command Prompt from the Recovery Options*

Microsoft have expanded the Command Prompt over the last few years and added new functionality including full cut and paste interoperability with the Windows desktop; see Figure 27-3.

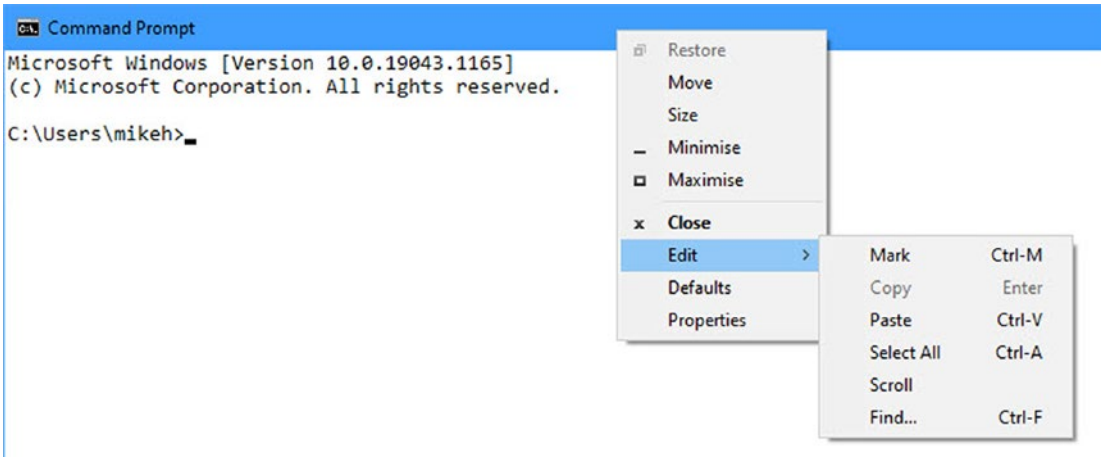


Figure 27-3. *Command Prompt now has full cut and paste functionality*

Additionally, if you right-click the command bar at the top of the window, often called the Title Bar, a menu will appear including two useful options. *Defaults* will reset all Command Prompt options to the way they were when Windows 10 was installed, and *Properties* allows you to reconfigure certain aspects of the Command Prompt window; see Figure 27-4.

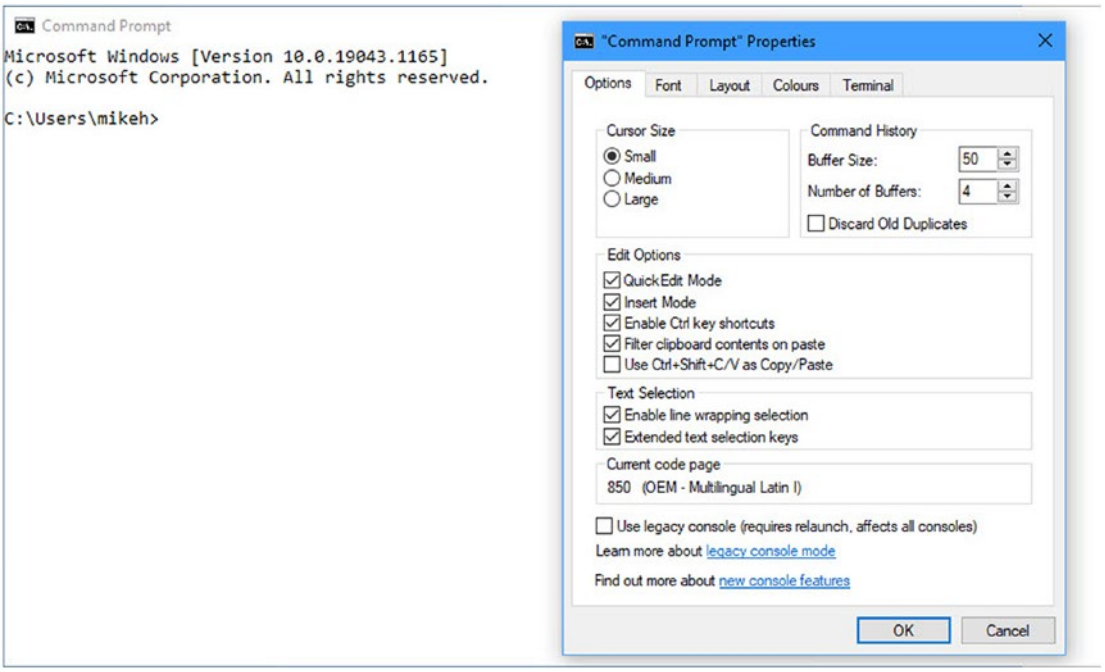


Figure 27-4. *You can reconfigure some aspects of a Command Prompt window*

The available options include being able to change the color scheme (which you can see has been very helpful to me in producing screenshots for this book) to keeping a command history (use the up arrow key on your keyboard to access previous commands). There are additionally useful things you can do with the Command Prompt interface:

- If a task is taking too long or has hung or you want to stop it, press **Ctrl + C**.
- Use the function keys to extend the Command Prompt functionality:
  - **F1** will paste the command last executed, but do it one character at a time.
  - **F2** will paste the last executed command but will ask you which character you want to paste up to.
  - **F3** pastes all of the last executed command commands (also achieved with the up cursor arrow on your keyboard).
  - **F4** asks which character ahead of the cursor you want to delete text up to.
  - **F5** cycles through the previously executed commands (also achieved with the up/down cursor arrows on your keyboard).
  - **F6** pastes the end of file character **^Z** to the Command Line.
  - **F7** displays a navigable list of previously used commands you can access with the up/down cursor keys on your keyboard, and Enter to select.
  - **Alt + F7** deletes the stored commands buffer.
  - **F8** displays all the commands that are stored in the memory buffer that start with characters in the current command.
  - **F9** prompts you for a history buffer number and then displays the command associated with the number you type.
- **Up, Down, Left Right cursor keys** to move the insertion point one character.
- **Ctrl + Left/Right** move the insertion point by one word or command.

- **Home/End** move the insertion point to the beginning or end of the line.
- **Esc** clears the current command from the display.
- You can save the output of the current display to a file using the suffix command ➤ **textfilename**, for example, the command **systeminfo ➤ C:\filename.txt** will export useful information about the PC as a Notepad document; see Figure 27-5.

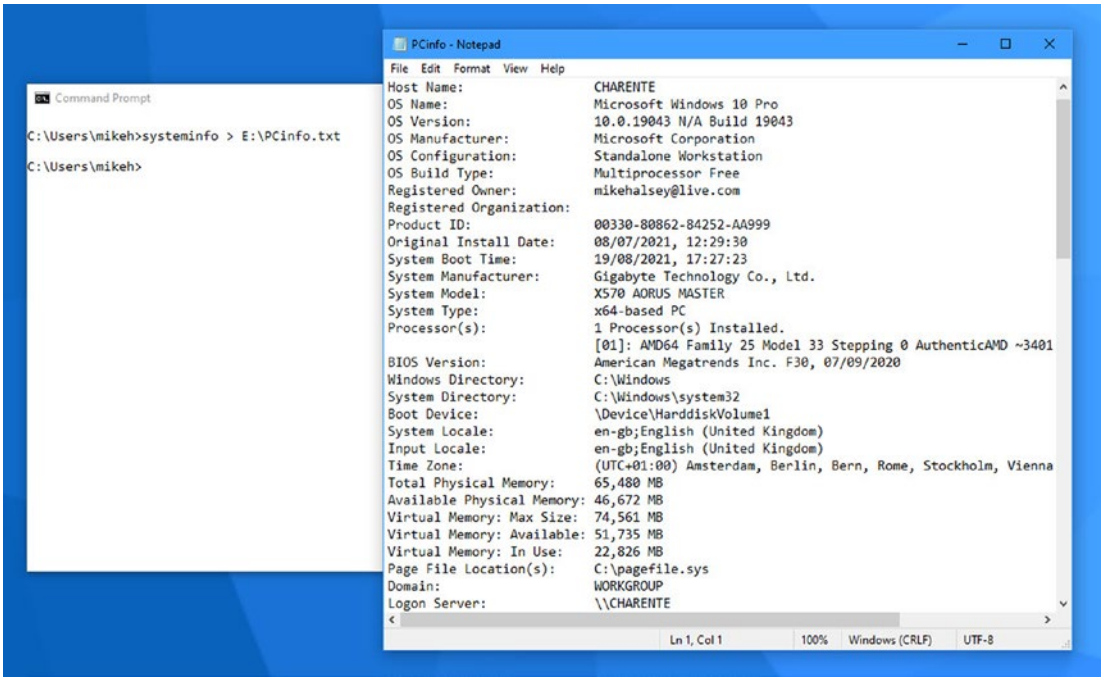


Figure 27-5. *You can export data from the Command Prompt as a text file*

- You can copy the output of the current command to the clipboard with the command suffix **| clip**.
- You can run multiple commands simultaneously by separating them on the same line with the symbols **&&**.
- You can also run the Command Prompt as an Administrator without having to use the mouse. Search for **cmd** from the Start Menu, and then press **Ctrl + Shift + Enter**.

Troubleshooting Using PowerShell

As I mentioned at the beginning of this chapter, Windows PowerShell was first introduced to make the deployment and management of Windows PCs easier in an Enterprise environment. Since that time in 2006, PowerShell has grown and been expanded considerably, so much so that you can now run PowerShell as a plug-in scripting environment for both Linux and MacOS. You can find the installers for these on GitHub at the following link `https://github.com/PowerShell/PowerShell`.

There are two PowerShell environments in Windows 10, the main PowerShell terminal, which is best accessed by pressing **Win + X**, though you can search for in the Start Menu, and the PowerShell Integrated Scripting Environment (ISE); see Figure 27-6.

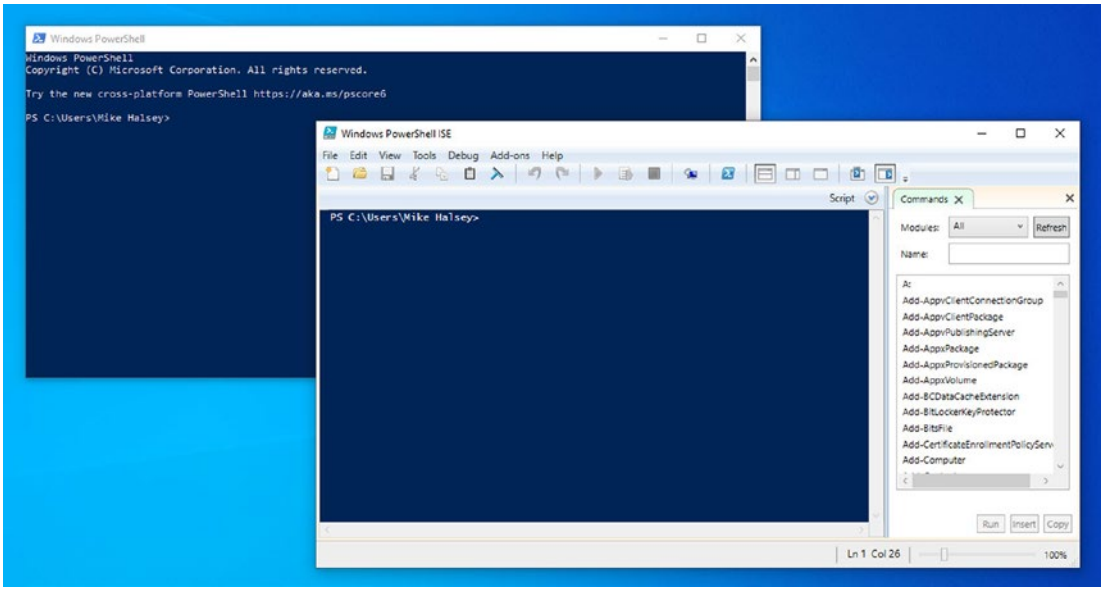


Figure 27-6. *There are two PowerShell scripting environments built into Windows 10*

These are different in that while the main PowerShell terminal is used for typing general commands in the way you do in the Command Prompt, or for loading prewritten PowerShell scripts (in the way you can with DOS Batch (.bat) files. The ISE on the other hand has been designed as an environment in which you can write, test, and debug complex scripts.

There are useful features in the PowerShell ISE including being able to test run just a part of a script. To achieve this, select the code you wish to run, and either click the *Run Script* button or press *F5*. You can also run the PowerShell ISE from the Command Line by using the command **PowerShell_Ise.exe** optionally with the switch **<file>** to open an existing script.

PowerShell is a complete scripting language and can be used for any management task in Windows. There are over 200 commands available which, as I mentioned at the beginning of this chapter, is too many to cover in this book. Fear not however as there are plenty of high-quality tutorial books about using PowerShell, from beginner to advanced, on the Apress website at `https://www.apress.com/search?query=powershell`.

Right-clicking the title bar in a PowerShell window and then clicking *Properties* in the menu that appears will display the same customization options you get for the Command Prompt; see Figure 27-7. These include being able to change the color scheme, but bear in mind that some commands and variables will be automatically color-coded in PowerShell and may become difficult to read if you change the foreground and background colors too much.

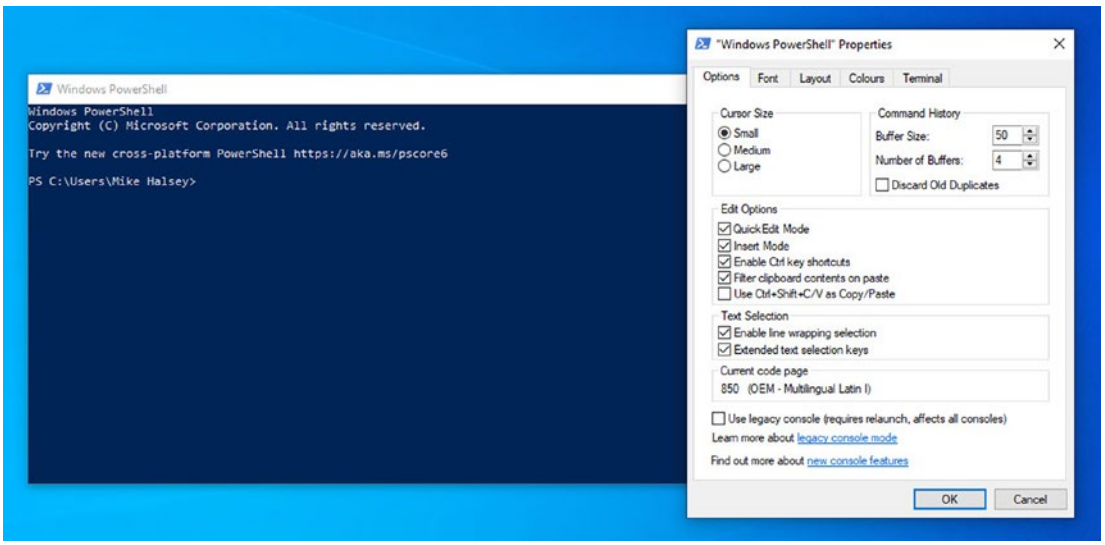


Figure 27-7. *You can customize the appearance and some functions of the PowerShell environment*

In addition to the books available on PowerShell from Apress, Microsoft have their own extensive online resource available at https://docs.microsoft.com/powershell/ with all the up-to-date information, tutorials, and guides you will need to get up to speed and find out how to complete the tasks you need to do.

Using the Event Log with PowerShell

In Chapter 5 I showed you the Windows 10 Event Viewer, and how it stores details of everything that happens in the operating system, from successful sign-ins to critical errors. While the Event Viewer panel is very useful, if you prefer to script, you can also get your information using PowerShell, and this is definitely the way you will need to query the Event Logs of remote computers on your network.

This is most useful when you're looking for event information for events you already know of, for instance you have the Event ID code. You can use PowerShell to obtain additional information using the format **`Get-EventLog -LogName System | Where-Object {$_.Eventid -eq 1074}`** which will display shutdown events on the PC.

There are additional switches you can use including **`-Newest X`**, where X represents the number of most recent events you wish to view information about. In Figure 27-8 we have used the command **`Get-EventLog -LogName System -Newest 10`** to display the ten most recent events on my own PC, which include four *warnings*.

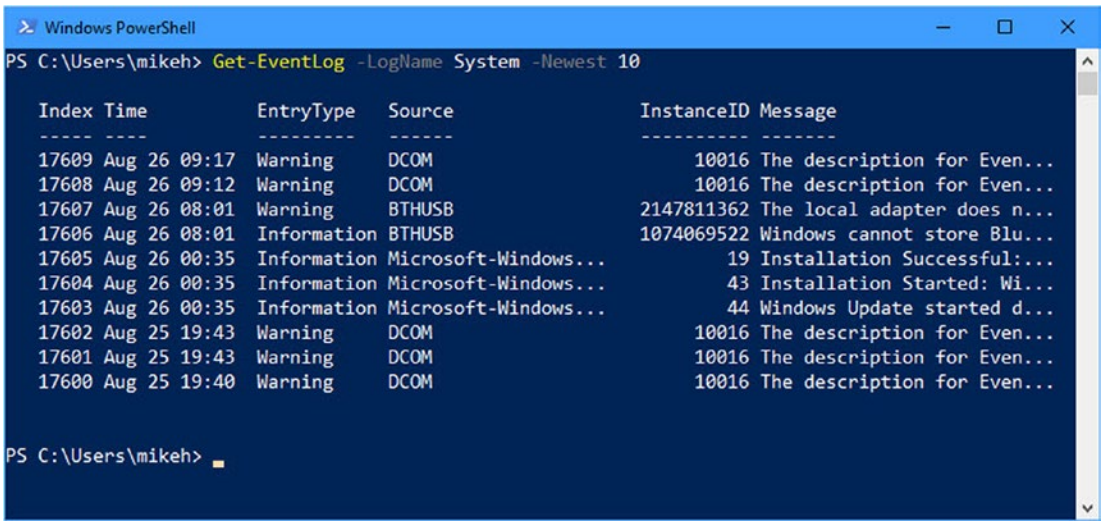


Figure 27-8. *Powershell is useful for displaying Event Log data*

Additional switches allow you to display more data for each event. You can use any of these to display the information you require: **`Get-EventLog -LogName System -Newest 10 | Select-Object -Property Index, TimeGenerated, TimeWritten, EventType, Source, CategoryNumber, Message`**.

Useful additional commands are

- **Get-EventLog -List** to view event logs on the local PC
- **Get-EventLog -LogName System -EntryType Error** to see all error events for a specific log
- **Get-EventLog -ComputerName <PCName> -LogName System** to gather logs from a remote PC
- **Get-EventLog -LogName System -ComputerName <PC1>, <PC2>, <PC3>** to gather event data from multiple PCs

You can read more about the Get-EventLog command on the Microsoft Docs website at this link https://pcs.tv/2WtF4J5.

The **`Get-WinEvent`** command works in a similar way to Get-EventLog but displays information differently. You can find detailed information on how it is used at the Microsoft Docs website on the following link https://pcs.tv/3kHFkfN.

While the Get-EventLog command is useful, displaying this data in the PowerShell window is far from ideal. You can export the results as a CSV file however that can be opened and read in Excel. For this you will use the additional command **`| Export-Csv -Path "Path and File Name`**". For example, in Figure 27-9, I have used the command **`Get-EventLog -LogName System -Newest 10 | Export-Csv -Path "E:\systemlog.csv`**" to export a file with details of the ten most recent system events.

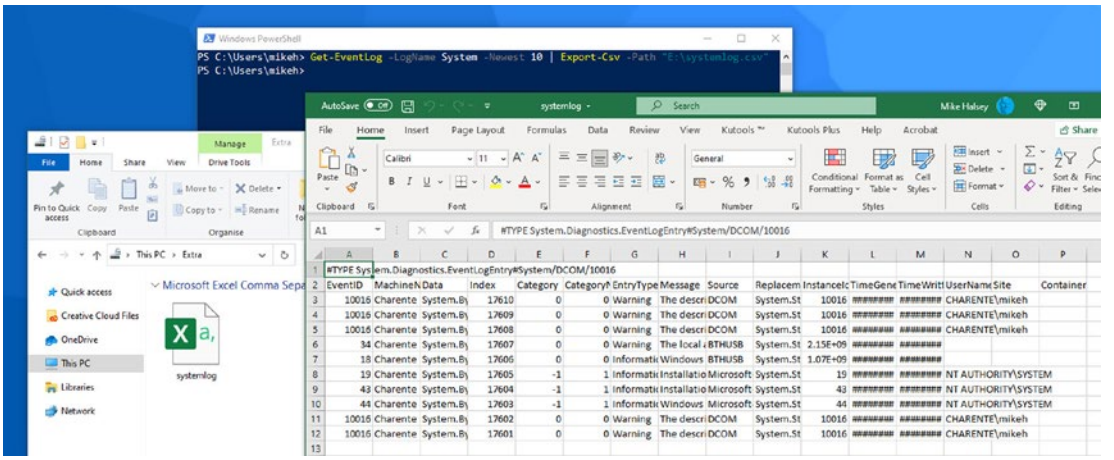


Figure 27-9. *You can export Event Log data as CSV files for Excel*

Gathering Disk and File Information

Just as with Event Logs, it is possible to gather detailed information about all aspects of a PC, local or remote, from disk partitioning to file access security. The **`Get-Disk`** and **`Get-PhysicalDisk`** commands report information about the disks in a PC, and the data can be exported to both CSV and HTML files with the additional commands **`| ConvertTo-Html -Title 'Disk Information' | Set-Content E:\DiskReport.htm`** and **`| Export-Csv -NoTypeInformation -Path E:\DiskReport.csv`**.

While these commands will provide details of physical disks, they won't report on partition structures. For this we use the **`Get-WmiObject`** command in the format **`Get-WinObject -Class Win32_LogicalDisk`** with the optional command **`| ft -AutoSize`**; see Figure 27-10.

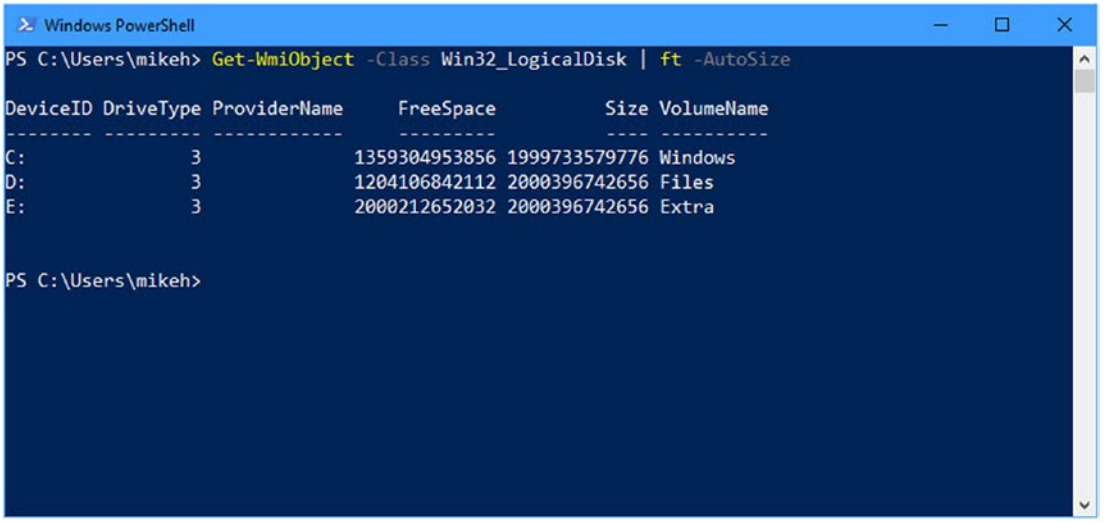


Figure 27-10. *You can display partition information with the Get-WmiObject command*

Just seeing information about the disks and partitions however will only get you so far. It is the disk's files, shares, and permissions that you will most commonly need to see information about. Let's start with file and folder shares. These can be viewed with the command **`Get-WmiObject -List -Namespace ROOT\CIMV2 | Where-Object Name -Match 'share' | Sort-Object Name`**.

This command will display all shared resources on the PC. This includes disks, printers, devices, folders, and files. It is possible to narrow this information down however, and also obtain additional information on when shares were created and the maximum number of users permitted to access the share, and to modify share parameters for both local and networked computers. You can read about the *Win32_Share* command on the Microsoft Docs website at the following link `https://pcs.tv/3sQoY4M`.

In the same way you can view information about shares, you can also get information about file, folder, and disk permissions. The command **`Get-Acl -Path C:\Windows`**, for example, can be used to see the *Owner* and *Access* permissions for the Windows folder on the local PC.

If we want more detailed information however, we can use the format **`Get-Acl -Path D:\Mike\OneDrive\Documents | Select-Object -ExpandProperty Access | Format-Table -AutoSize`**, as seen in Figure 27-11.

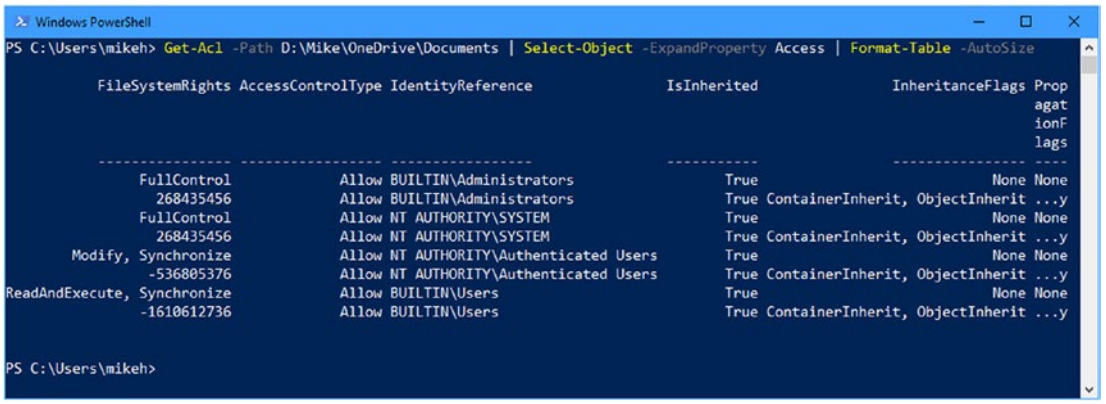


Figure 27-11. *You can get detailed information about ownership and access permissions*

You'll be viewing this information because some permission or inheritance will be misconfigured and you'll need to rectify it. For this we can use the **`FileSystemAccessRule`** command which you can read about on the Microsoft Docs website at `https://pcs.tv/38hBofE` and the **`Set-Acl`** command, which again you can read about on the Microsoft Docs website at `https://pcs.tv/2XYsK3Y`.

Set-Acl can be used in a variety of ways and on many things from files to Registry keys. You can, for example, copy the security permissions from one file to another using the commands:

```
$FirstFile = Get-Acl -Path "D:\MasterFiles.txt"
Set-Acl -Path "D:\SubordinateFile.txt" -AclObject $FirstFile
```

If you need to apple permissions to multiple files, you can do this with the command:

```
$NewAcl = Get-Acl MasterFile.txt
Get-ChildItem -Path "D:\Folder" -Recurse -Include "*.txt" -Force |
Set-Acl -AclObject $NewAcl
```

There are additional scripts available on the Microsoft Docs website I linked above for enabling and disabling inheritance and granting full access permissions for files and folders.

Gathering Hardware and Software Information

There is all manner of hardware reporting that can be gathered using PowerShell, from the command **`Get-CimInstance -ClassName Win32_BIOS`** which can be used to display information about the BIOS on a PC. It can also be used with the switches **`| Export-Csv -NoTypeInformation -Path D:\BiosReport.csv`** to save the information to a file you can then open in Excel to the **`-ComputerName <PCName>`** to connect and gather data on other PCs on the network. Separate the different PC names with a comma and space. You can read more about the Win32_BIOS command on the Microsoft Docs website at https://pcs.tv/38cPzTg.

The command **`Get-CimInstance -ClassName Win32_ComputerSystem | Format-List -Property *`** displays information about the PC (see Figure 27-12), which includes technical information about the hardware. Again, and as with all the commands listed here, it can be used with the switches **`-ComputerName <PCName>`** and **`| Export-Csv`** to gather information on multiple computers on the network, and to export the results to a file.

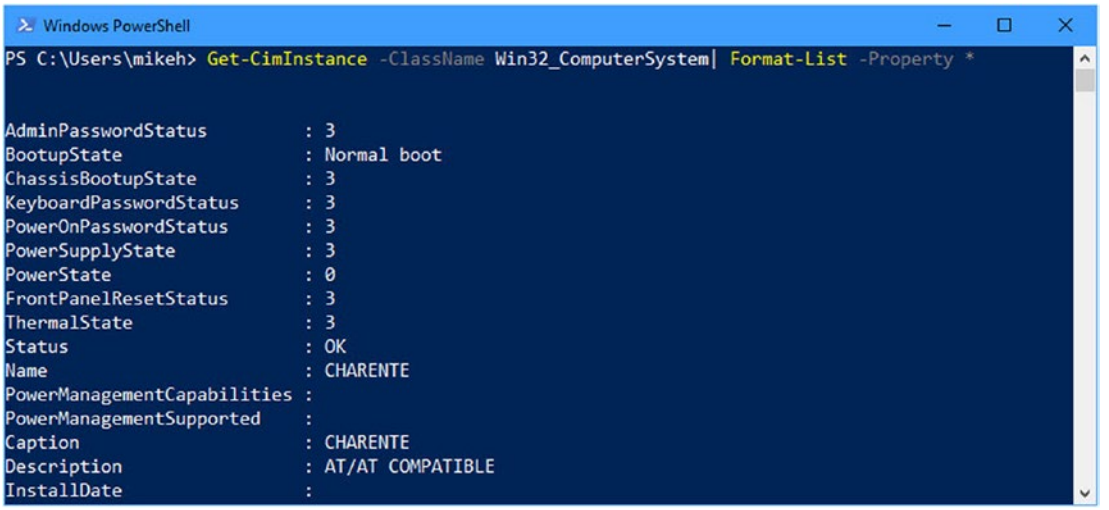


Figure 27-12. *You can view detailed information about a PC's hardware in PowerShell*

If you need information about the processor(s) in one or more PCs, you can use the commands **`Get-CimInstance -ClassName Win32_Processor | Format-List -Property *`** and **`Get-CimClass -Namespace Root\CimV2 -ClassName win32*processor*`**.

When it comes to software, it can be useful to see what applications are installed on PCs across the network. For this you can use the command **`Get-CimInstance -ClassName Win32_Product | Format-List`**. This displays a list of all the applications installed on the local PC; see Figure 27-13. When used with the **`-ComputerName <PCName>`** and **`| Export-Csv`** switches however, it comes into its own for diagnosing issues caused by different versions of software causing problems on specific computers.

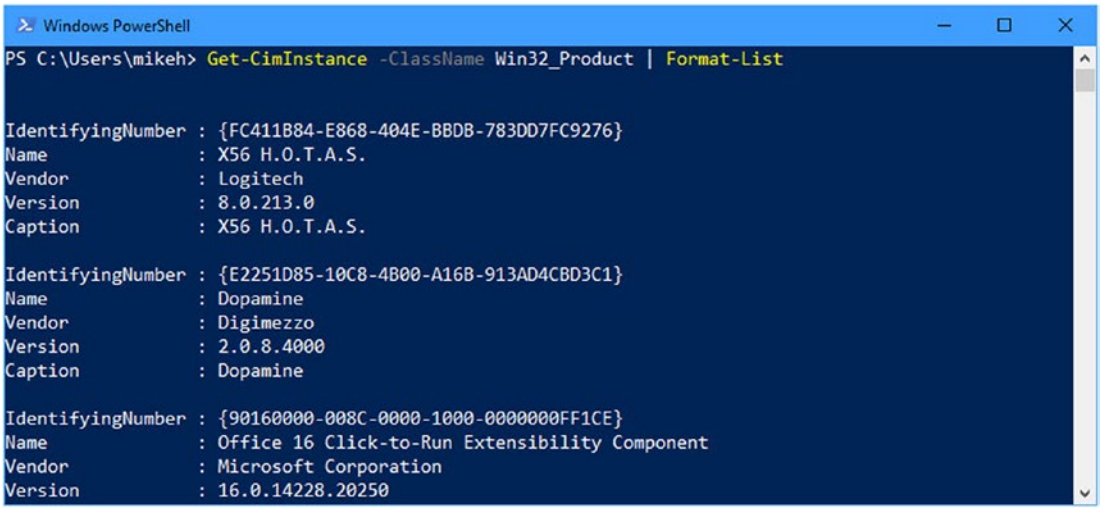


Figure 27-13. *You can view installed software information including version numbers*

In Chapter 26 I talked about the Windows Registry. There are five Registry keys in which information about installed applications can be found:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall
- HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
- HKU\<User SID>\Software\Microsoft\Windows\CurrentVersion\Uninstall
- HKU\<User SID>\Software\Microsoft\Installer\Products
- HKLM\Software\Classes\Installer\Products

You can use the **Get-Item** and **Get-ItemProperty** commands to interrogate the Registry with commands such as **Get-ItemProperty -Path Registry::HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion** to display information about Registry keys, but it gets fairly technical when you want to modify, delete, or add additional keys. Given how just a small incorrect change in the Registry can make a PC completely unbootable, I shall at this juncture point you toward Microsoft PowerShell Registry reference guide at the Microsoft Docs website, https://pcs.tv/2WqVCRW, and suggest you settle in for quite a technical read.

Managing Processes and Services

You can find out information about running processes on a local or remote PC(s) with the **Get-Process** command. There are various options and subcommands you can use this with to drill down into specific processes on the PC to get data about them, and you can read about these subcommands on the Microsoft Docs website at the following link https://pcs.tv/2Wnbzbr.

Windows and third-party services can be interrogated the same way with the **Get-Service** command. You can use this command on its own to see the status of all installed Services, or in one of the following formats:

- **Get-Service "net*"** to list services that begin with set characters but continue using a wildcard.
- **Get-Service -Displayname "*network*"** to display services that have a specific word or term in their descriptive name.
- **Get-Service -Name "net*" -Exclude "Netlogon"** to search for services but to exclude specific ones from the results.
- **Get-Service | Where-Object {$_.Status -eq "Running"}** to obtain a list of current running Services. This can also be used with the subcommands, **"Stopped"** and **"Suspended"**.

You can read more about how to manage Services using PowerShell on the Microsoft Docs website at the following link https://pcs.tv/3kszYFO.

Tip Some very useful commands for managing Processes and Services on a PC include **Stop-Process, Start-Process, Stop-Service, Start-Service,** and, perhaps one of the most useful, especially with troublesome third-party services, **Suspend-Service** and **Restart-Service**. More information on how these useful and simple commands work can be found on the Microsoft Docs website at https://pcs.tv/3ynX9Fp.

Managing Windows Update

As you can imagine, it's straightforward to manage Windows Update from PowerShell. Actually, this was always going to be a no-brainer, as system administrators need to configure and update computers across the network, which includes managing updates.

One of the reasons for this is some businesses, especially those using older-bespoke software, can find new updates causing that software to become unresponsive or buggy, which is why every system administrator, maybe yourself as well, tests each update provided by Microsoft before deploying them.

Sometimes you need to know what updates have been installed on the Windows 10 PCs across your network; this can be done with the **`Get-HotFix {-ComputerName <PCName>, <PCName2>, <PCName3>} | Sort-Object InstalledOn`** command; see Figure 27-14. This will display the "KB" number for each, which is Microsoft's standard way to identify particular fixes and updates.

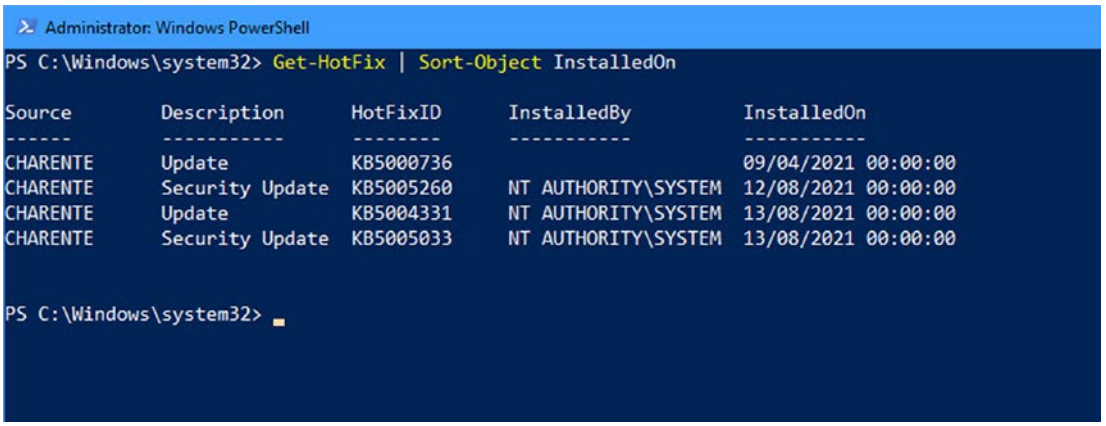


Figure 27-14. *You can check which updates have recently been installed on a local or remote PC*

If you want more detailed information about what updates have been installed on a PC or PCs over time, use the command **`Get-WindowsUpdateLog`**, which will export the full event logs from Windows Update, including error and failure events, and write them to a *WindowsUpdate.txt* file placed on your desktop; see Figure 27-15.

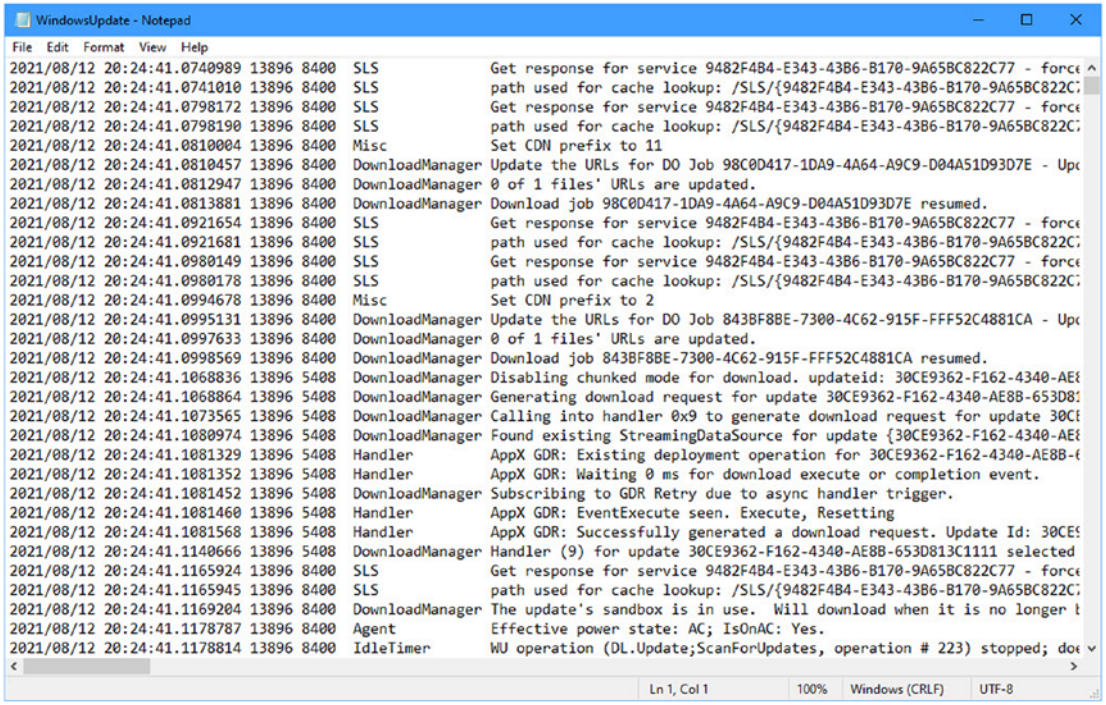


Figure 27-15. *You can view full event logs for Windows Update with PowerShell*

More information on the PowerShell commands you can use with Windows Update on PCs across a network can be found on the Microsoft Docs website at the following link, `https://pcs.tv/3mHleEP`.

Windows Terminal

New to Windows 10 is the *Windows Terminal*. This isn't installed with Windows 10 by default (though it could be added in a future update and does come per-installed in Windows 11). For now, it can be installed from the *Microsoft Store* or from Microsoft's GitHub site on this link `https://github.com/Microsoft/Terminal`.

The Windows Terminal is the logical next evolutionary step for the Command Prompt and PowerShell scripting environments. You can use to have open multiple instances of a PowerShell environment, a Command Prompt environment, and also Azure Cloud Shell; see Figure 27-16.

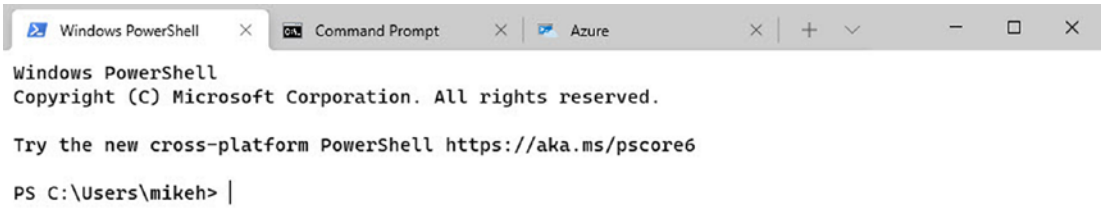


Figure 27-16. *Windows Terminal is a powerful and useful scripting environment*

Windows Terminal has a straightforward interface with a tabbed experience similar to a web browser. To the right of these tabs is a down arrow that you can click to display options, including opening the *Settings* for the environment. In Settings you have many options from how the Windows Terminal looks and behaves, to your personal preferences for word delimiters, keyboard shortcut keys, and more; see Figure 27-17.

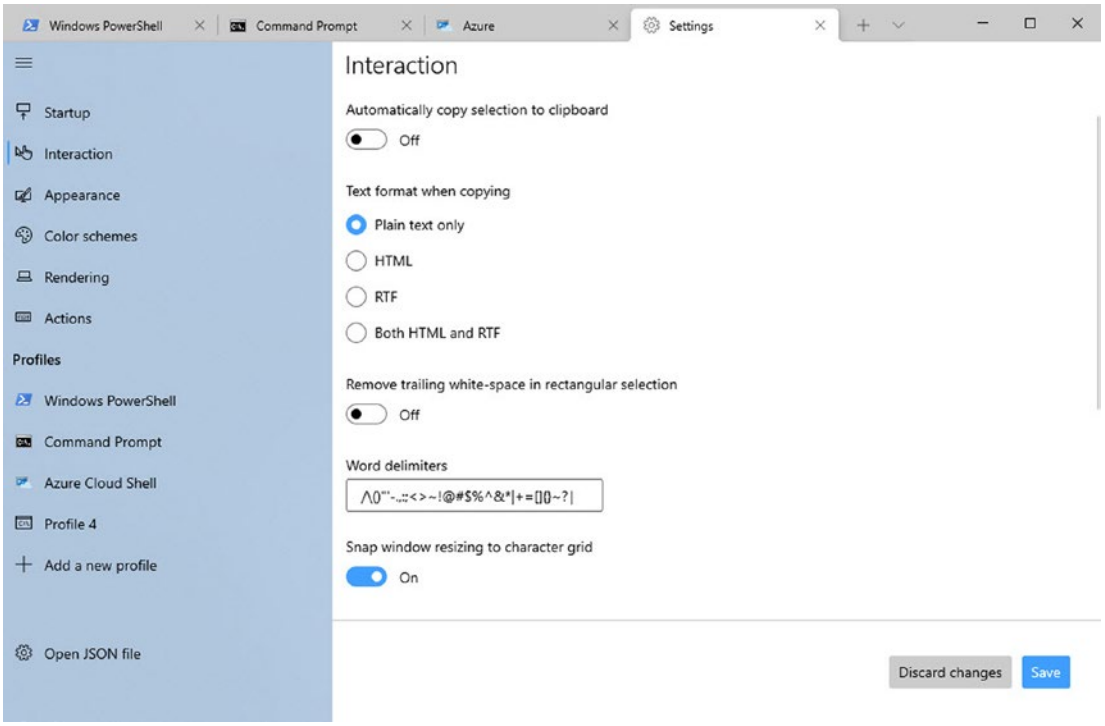


Figure 27-17. *Windows Terminal is highly configurable*

You can also add additional third-party scripting environments to the Windows Terminal such as Bash. This is achieved from the Windows Terminal Settings, click the *Add a new profile* link, but as you're probably all about scripting by this point anyway, you might prefer to configure the Settings.JSON file for Windows Terminal instead.

This can be most easily accessed from *Settings* ➤ *Open JSON file*, and it will open in a Notepad window; see Figure 27-18. This is where all of the configuration settings and options for Windows Terminal are stored, so anything you need or want to do to change settings or add profiles can be done here.

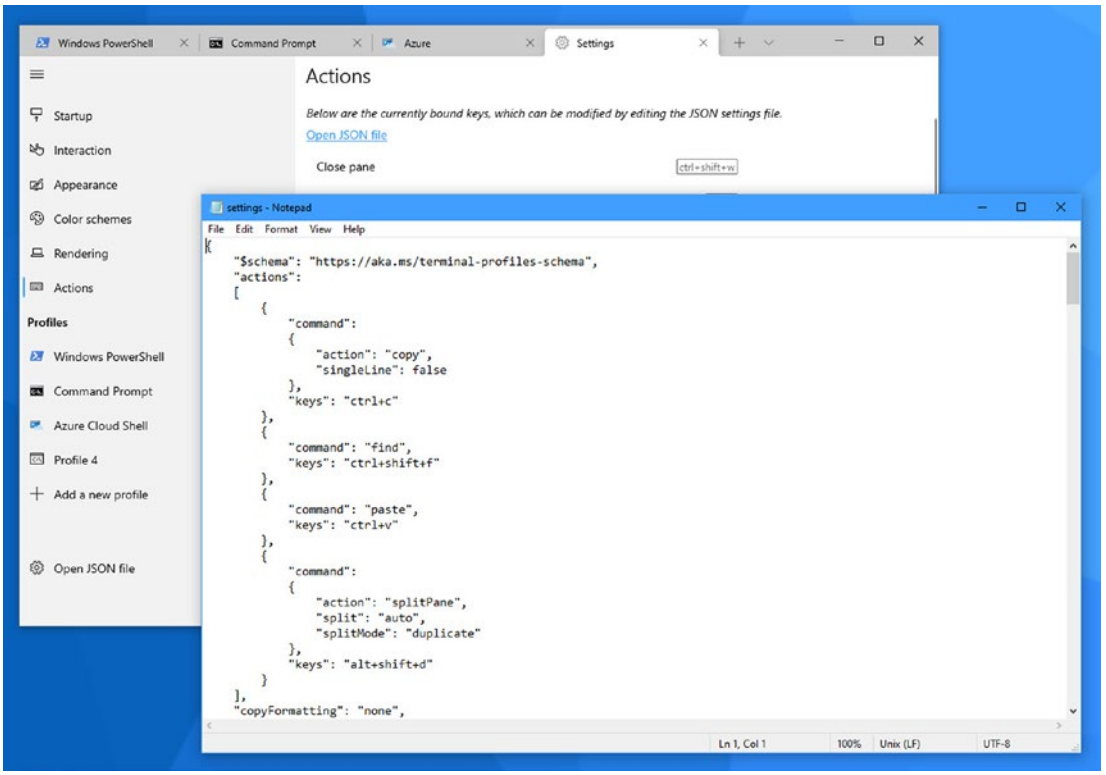


Figure 27-18. *You can manually configure Windows Terminal with its JSON file*

In operation there is nothing you can do in a standard Command Prompt or PowerShell window that you can't do in Windows Terminal, though there are some extra additions and standout new features, such as using the **Windows key + ` (in the top left corner of your keyboard)** opens the Windows Terminal in the top portion of your computer screen.

You can also cut, copy, and paste text between different tabs, but some of the icing on the cake comes from being able to add custom background images and icons, and make use of DOS-style terminal fonts. Microsoft's Terminal developers have a great blog online about how the terminal can be customized to your own preferences at the following link `https://pcs.tv/2WzjKBM`.

Summary

PowerShell has truly changed the landscape for administering Windows PC systems, and Microsoft's documentation, which can be found online at https://docs.microsoft.com/powershell/, is extraordinarily extensive. I can also recommend the book *Troubleshooting Windows Server with PowerShell* (Apress, 2016) which applies equally to Windows 10 given that Windows Server and Windows 10 are built on the same core architecture.

Earlier in this chapter, I wrote about how you can use PowerShell to manage disk and file permissions. In the next chapter, we'll look at the Windows file system, and Shell User Folders in significantly more depth, including how to manage permissions, what inheritance means, and how you can take ownership of files, folders, and even whole drives after a reinstallation or a PC rebuild.

CHAPTER 28

Windows 10 File Structure in Depth

I just counted how many files are currently sitting on my C: drive, where Windows 10 is installed on my PC. This doesn't count my documents, pictures, music, and video, which I store elsewhere to ensure file security, but there are well over half a million files in almost one hundred and thirty thousand folders sitting on the drive.

Now, I have some big app suites installed, such as the full Adobe Creative Suite, Microsoft Office, and several large games including Elite: Dangerous (Cmdr Travers if you do to) that I play regularly. These will install huge volumes of files on the PC, and then there's temporary files, configuration files, preferences files, etc.; the list goes on.

So how do we go about making sense of this file system from a troubleshooting point of view? What is the SysWOW64 folder, and what's so special about the WinSXS folder that it has to be more than 9GB in size? In this chapter I'll guide you through this file system maze and look at what every major part of the operating system is for, and where it can be found.

The Windows 10 File and Folder Structure

You probably don't need me to tell you that the Windows 10 OS is stored in the `C:\Windows` folder on your hard disk and that user files are stored in the `C:\Users` folder. Things are never quite that simple though, and if you're troubleshooting the boot files for the OS, Windows Update, or System Restore, where would you look?

Many of these folders and their files are hidden from view, under two levels of protection called hidden and system files. You can unhide either or both of these file types in File Explorer by clicking the *View* tab, and then the *Options* button. In the dialog that appears, click the *View* tab, and then you can change the options for *Show hidden files, folders and drives,* and *Hide protected operating system files (recommended)*; see Figure 28-1.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_28

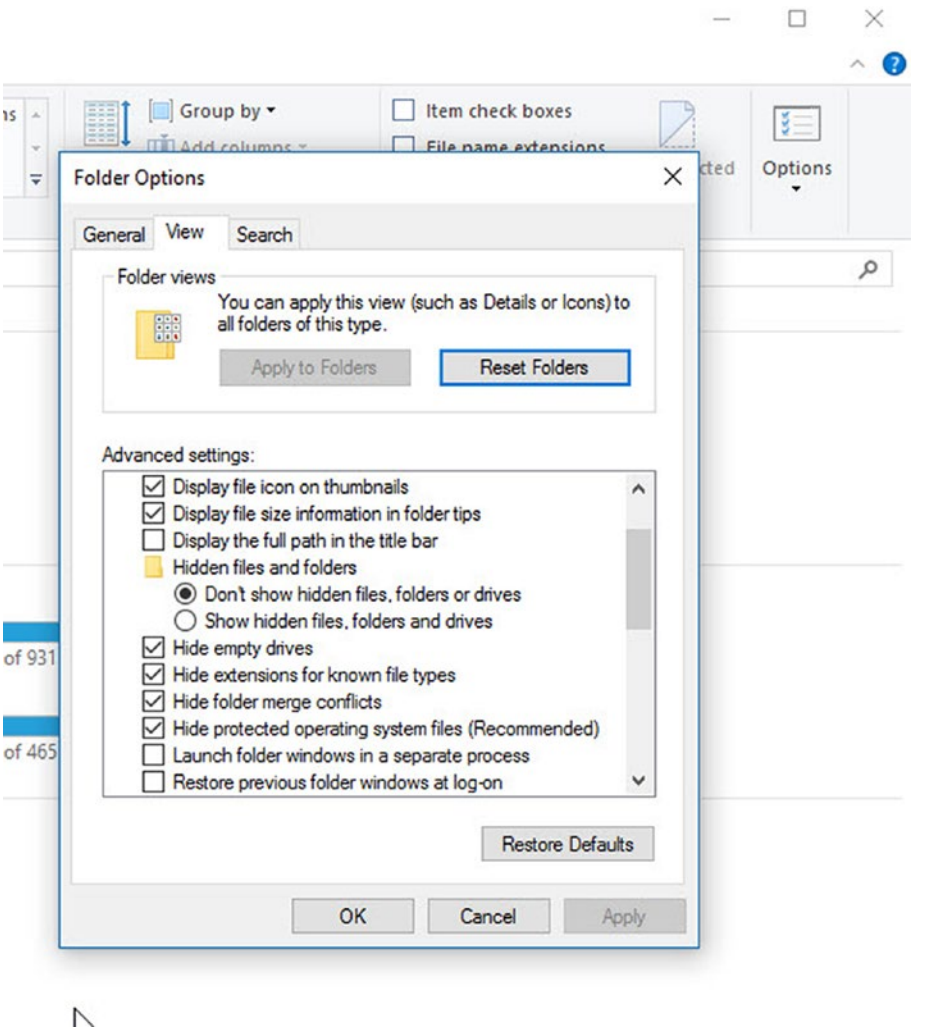


Figure 28-1. *You can display both hidden and system files in File Explorer*

But when you're then looking at the contents of the hard disk on which Windows is installed, and indeed every other disk, you might not recognize what some of the files and folders you see are for.

Root Windows Folders

- **MSOCache**—will be seen only on systems with Microsoft Office 2007 or a later version installed. It contains installation files for the Office suite that are used if the installed apps need to be repaired; it is not needed for the most recent editions of Office.

- **ProgramData**—contains win32 app data that applies to all users on the PC. This includes configuration and other files necessary for the apps to run. It can be a very large folder but should never be deleted.
- **System Volume Information**—seen on all of your hard disks and is used by the System Restore and File History features. It contains archived and encrypted versions of critical system files, such as the Registry and files that change on app installations. It does this with versioning control, so that System Restore can roll back to previous versions if needed. It is also used in a limited way by the File History feature for version control of your documents.

Win32 and Store App Folders

- **Program Files** and **Program Files (x86)** are the folders in which win32 desktop apps are installed. The Program Files (x86) folder is seen only on 64-bit Windows 10 installations, and it is where 32-bit software is installed, though some 64-bit software does end up being installed here, presumably because of decisions made by the publishers including Adobe.
- **Program Files\WindowsApps** is the install location for all Store apps. This folder is heavily protected by the OS, to the point where even the local Administrator account cannot gain access to it (more of this please Microsoft!).

Windows Operating System Folders

- **Windows\AppPatch**—contains application compatibility files.
- **Windows\Boot**—contains files necessary for starting the OS; I detailed these in Chapter 13.
- **Windows\CSC**—contains offline files and documents, used for caching.
- **Windows\Cursors**—contains cursor and icon files for the OS.

- **Windows\Debug**—contains Windows error logs. I'll talk more about the log files shortly.
- **Windows\Fonts**—where all the installed typefaces on your PC are installed.
- **Windows\Globalization**—where language packs, dictionary files, and other files relating to location are stored.
- **Windows\IME**—contains Language files used by the OS and apps, also IME (x86) on 32-bit systems.
- **Windows\ImmersiveControlPanel**—contains the files that constitute the Settings panel.
- **Windows\INF**—contains device driver installation files.
- **Windows\Media**—contains audio and video files that are used by the OS, such as sound packs.
- **Windows\Prefetch**—the system Windows uses to load commonly used files before you open them. The OS tries to anticipate what you want to use and open. Sometimes, this cache can become corrupt, and if so, it is safe to delete the contents of this folder.
- **Windows\Resources**—contains ease-of-access themes, accessibility themes, and other themes for Windows.
- **Windows\Security**—contains security files and logs used by Management Console snap-ins.
- **Windows\SoftwareDistribution**—the folder used by Windows Update. Should you find that Windows Update is unable to download or install any updates, you can completely delete the contents of this folder. I detailed the process of how to do this in Chapter 16.
- **Windows\System**—exists to maintain compatibility with legacy apps that do not look for the `System32` folder.
- **Windows\System32**—the main repository of all files that constitute the Windows operating system.

- **Windows\System32\Config**—contains the main Registry files used by the OS. Additional Registry files can be found in the `%userprofile%` and `%userprofile%\AppData\Local\Microsoft\Windows` folders.
- **Windows\System32\Drivers**—contains installed driver files.
- **Windows\System32\Divers\etc**—contains configuration text files such as the Hosts file, which can be used to modify the mapping of hostnames to IP addresses.
- **Windows\System32\GroupPolicy**—contains Group Policy script and template files.
- **Windows\System32\icsxml**—contains files used by the Universal Plug and Play feature for hardware.
- **Windows\System32\Microsoft**—contains cryptography files.
- **Windows\System32\oobe**—contains files that are used by the Windows Out-of-Box Experience when setting up new users on the PC.
- **Windows\System32\ras**—contains Remote Access encryption files for Windows server connections.
- **Windows\System32\Recovery**—contains files used by the Windows Reset feature.
- **Windows\System32\restore**—contains files used by the System Restore feature.
- **Windows\System32\spool**—contains files associated with your installed printers and the print spool queue.
- **Windows\SysWOW64**—used to store files necessary to maintain app and driver compatibility between 32- and 64-bit code.
- **Windows\Tasks**—contains scheduled task files.

- **Windows\WinSxS**—called the Windows Side-by-Side folder. It contains multiple copies of dynamic link libraries (DLLs) and other files that are crucial to your app and OS operation, but where different versions of the same file may be required to be loaded by different apps simultaneously. This folder can grow to an enormous size but is crucial to the operation of Windows 10.
- **Windows\Web**—contains images used by the lock screen and for Windows wallpapers.

User Account Folders

- **Users\[UserName]\AppData\Local**—known also by the shortcut `%localappdata%`, this folder contains the data and settings that are necessary for installed apps, and for your user profile to operate correctly. Internet temporary files are also stored in this folder.
- **Users\[UserName]\AppData\LocalLow**—contains data that cannot be moved, and has lower-level access on your PC, such as when a web browser is used in privacy mode.
- **Users\[UserName]\AppData\Roaming**—can be accessed by the shortcut `%appdata%`. It contains data and settings that can be moved with your user account, such as when you are connected to a Domain.

Windows Log Folders

- **PerfLogs**—where custom Data Collector Sets that are created in the Performance Monitor are stored. See Chapter 25 for details on how to create these, and what they are.
- **Windows\Debug**—where log files that are created when an app or service crashes, or when certain audit processes are performed, such as installing Windows Updates. These logs are stored in plain text format and can be read in Notepad.

- **Windows\Logs**—the main log folder for the Windows OS. It contains many log files such as WindowsUpdate.log. These files are sometimes stored as Extensible Markup Language (XML) files that can be opened in a web browser. Many files, however, are stored as Event Trace Log (ETL) files. You can read these files in the *Event Viewer* by clicking the *Action* menu and then the *Open saved log* option.
- **Windows\Minidump**—contains crash reports that are created by applications and Blue Screens of Death (BSOD). They have the file extension `.dmp`. You cannot read these files in Notepad and will need the Windows Driver Kit (WDK) or Windows Software Development Kit (SDK), both of which are available as part of Microsoft Visual Studio.
- **Users\[UserName]\AppData\Local\CrashDumps**—contains crash dump files that are pertinent to the specific user account. They can also be accessed through the address `%LOCALAPPDATA%\CrashDumps`.

Windows Temporary File Folders

- **Users\[UserName]\AppData\Local\Temp**—the main temporary file storage, stored on a per-user basis. It is used for multiple purposes, including downloaded files and web pages that are viewed in your browser. You can most easily access it by navigating to `%temp%`.
- **Users\[UserName]\AppData\Local\Microsoft\Windows\INetCache**—used for storing temporary Internet files.
- **Users\[UserName]\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low**—another Internet files temporary folder.
- **Windows\Temp**—a protected temporary file store used by the OS and apps.

Windows File Types

- **Bootmgr**—a critical file required at PC startup.
- **Desktop.ini**—a file found in every folder on your PC. It contains configuration data about how that folder and its contents should be viewed in File Explorer.
- **DLL** files—Dynamic link library files that contain code shared by many different apps and services. These apps and services can call upon DLLs to perform tasks that may be required by different apps, such as managing the print queue and displaying window furniture.
- **EXE** files—win32 apps that can be run on a double-click of the mouse.
- **Hiberfil.sys**—the Hibernation file that stores the PC's memory state.
- **INF** files—device driver installation files.
- **INI** files—configuration and option files for apps and Windows features.
- **Thumbs.db**—contains thumbnail images of files and documents within a folder. You may also have some `ehThumbs.db` files, which were used by Windows Media Center.
- **Pagefile.sys** and **Swapfile.sys**—used by the virtual memory feature in Windows 10.
- **SYS** files—contain system settings used by the OS and both software and hardware drivers on the PC.

Managing the Shell User Folders

You might find that you want to change the locations of some of the Shell User Folders on your PC. For example, I mentioned earlier in this chapter that I store my files and documents on a separate partition to my Windows installation. This ensures the files are not affected if I suffer a major problem with the OS and have to reinstall it.

There are different ways to manage the Shell User Folders, but we'll start with the temporary files folder, as this seems like a natural jumping-off point. If you open **Advanced system settings** from the Start Menu, you will be presented with the system properties panel. Then, clicking the *Environment variables* button in the bottom right corner of the dialog will display a dialog in which you can change the location, should you wish, of the Windows Temporary folder; see Figure 28-2.

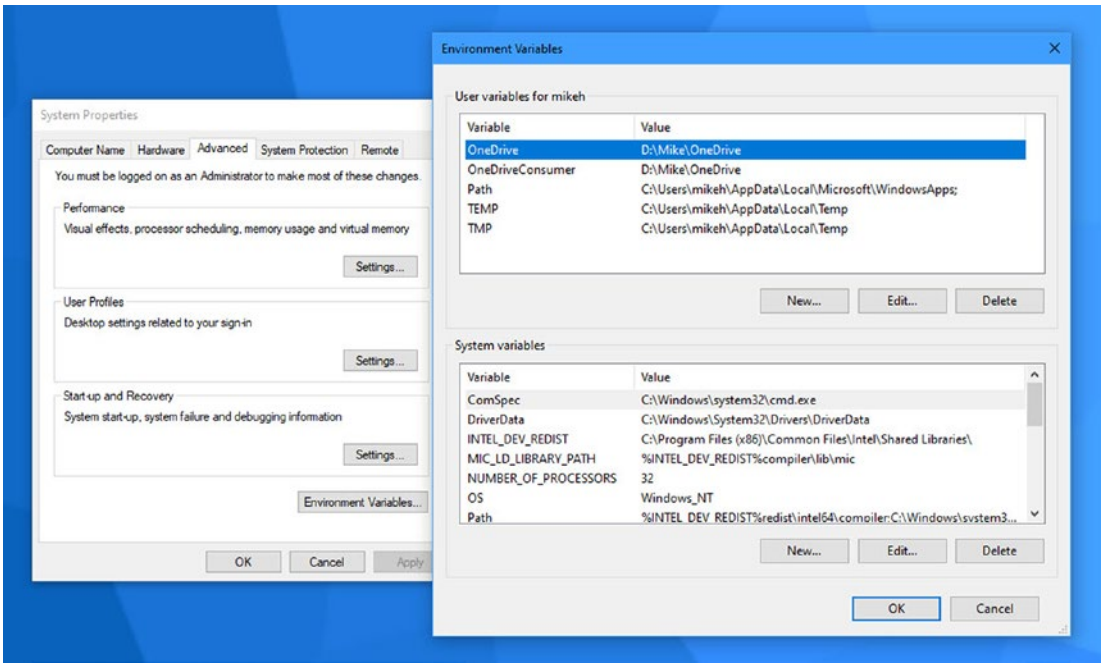


Figure 28-2. *You can change the location of the Temporary folder*

There are several ways to move the Shell User Folders, documents, pictures, music, video, and so on:

1. The easiest is to cut and paste the folders from their current location to the new location where you want them to be. Windows 10 will then automatically update all the pointers for you.

2. You can also right-click a folder (this must be done individually) and select its *Properties*. Then, click the *Location* tab in the dialog that appears where you can either click *Move*, to move the folder and its contents to a new location, or *Restore Default* if something has gone wrong with it, and it needs to be reset; see Figure 28-3.

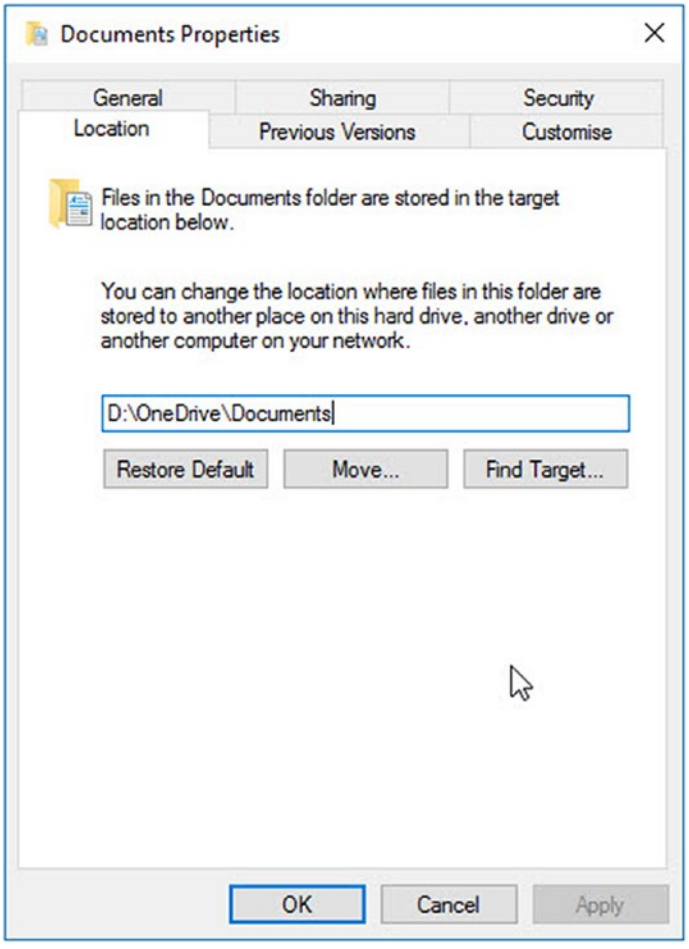


Figure 28-3. *You can move your user document folders in File Explorer*

If you want full and complete control over all the Shell User Folders, however, perhaps because the locations of one or more have become corrupt, you can find them in the Registry; see Figure 28-4. There are two Registry locations to visit:

- `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`
- `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`

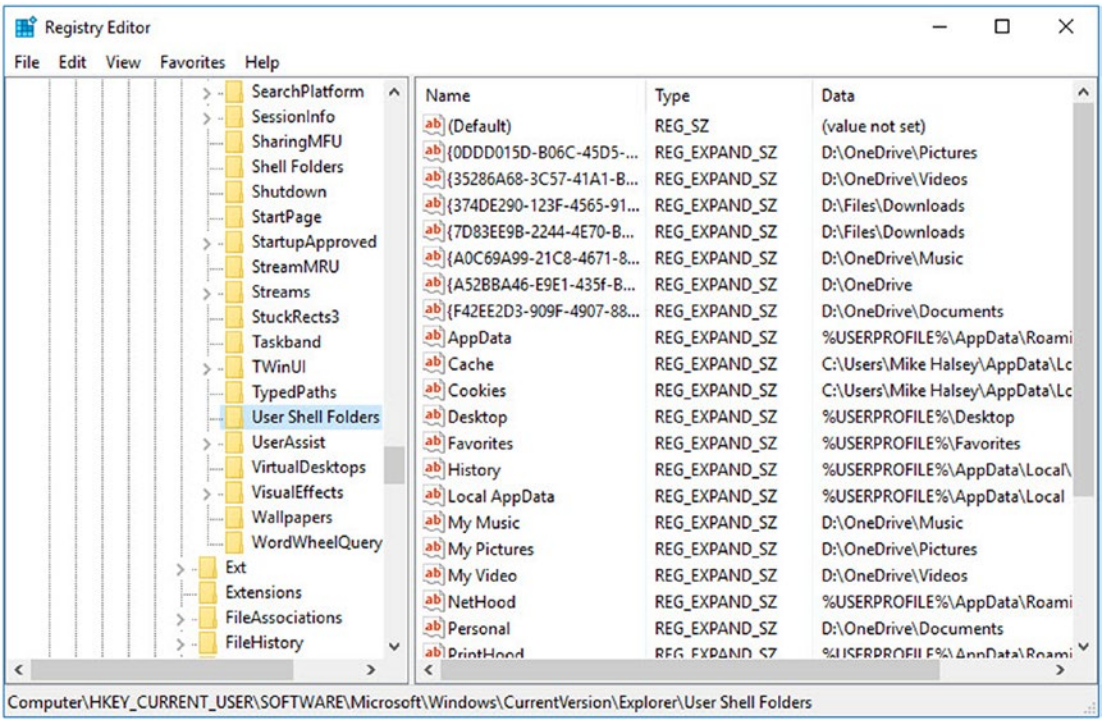


Figure 28-4. *You have full control over the Shell User Folders in the Registry*

Creating and Managing Symbolic Links

Symbolic links are a means of creating an easily accessible file or folder on a PC, perhaps on the desktop or in your Documents folder, which actually links through to a harder-to-find or network folder location. The symbolic link effectively acts as a shortcut to an alternative files or folder location. You use the **mklink** command from an Administrative Command Prompt window to create a symbolic link.

As an example, on my network-attached storage (NAS) drive, I have a folder containing virtual machine files. This has the network address `\\N5\n5\Virtual Machines`. I want to create a symbolic link on my main files drive (E:), so in an elevated Command Prompt, I type the command `MKLINK /D E:\VMs "\\N5\n5\Virtual Machines"`, and the folder E:\VMs then appears in File Explorer; see Figure 28-5.

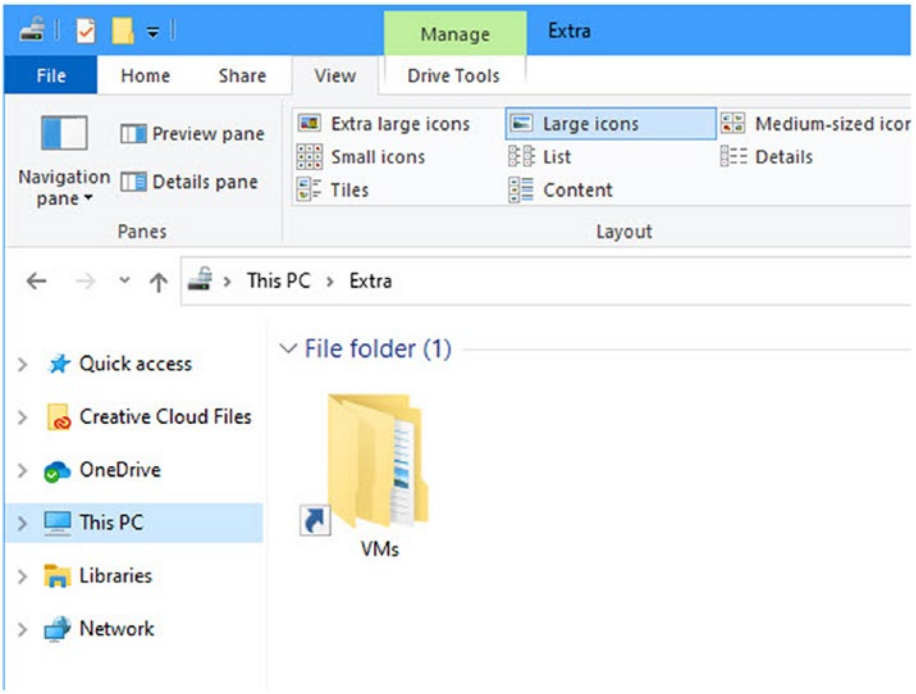


Figure 28-5. *You can create symbolic links to files and folders*

The **MKLINK** command is used with the following syntax. `MKLINK [[/D] | [/H] [/J]] Link Target` where

- **/D** creates a link to a directory.
- **/H** creates a hard link which makes it look as though the file or folder actually exists in the target destination, and can be useful for times where software is having compatibility issues with standard soft links.
- **/J** is used to create a directory junction, which is a hard link that acts like a hard disk, partition, or disk volume.
- **Link** is the new symbolic link location and name.
- **Target** is the file or folder you want to link from.

Note with the Link and Target parameters, you should include them in "double quotes" if the link name contains a space character. When it comes to deleting a symbolic link, you can delete it as though you are deleting any file or folder, but be careful not to delete its contents, as you will also delete the source contents.

File Management from the Command Line

Windows 10 comes with several Command-Line tools and utilities for managing and maintaining the files on your PC. Some of these date back to the early days of Windows, but that doesn't mean they're not still useful.

ChkDsk

The Check Disk (ChkDsk) tool has existed since the early days of Microsoft DOS in 1980, but it's still useful. It will check the integrity of files, folders, and data on a specified drive and attempt to fix errors if it can. In its simplest term, it is used in the format **CHKDSK C:** from an Administrator Command Prompt, but there are additional switches you can use:

- **/F** is used to get ChkDsk to fix any disk errors it finds if it can.
- **/V** uses verbose logging, where the name of every file and folder checked is displayed.
- **/R** locates bad sectors on a hard disk and attempts to recover unreadable information.
- **/X** forces the volume to dismount first, which can be useful if the disk is locked by an application, preventing ChkDsk from working.
- **/I** performs a less vigorous check only of data index entries, and reduces the time taken to perform the check.
- **/C** does not check cycles in the folder structure, and reduces the time taken to perform a check.
- **/L[:<size>]** changes the log file size to that size you specify; if you omit [:<size>], /L then displays the size of the log file.
- **/B** clears the list of bad clusters on a disk and then rescans the disk for errors; this also includes the functionality of /R.
- **/Scan** runs an online scan of the volume.
- **/Forceofflinefix** must be used with /Scan and bypasses all online repairs; all defects found are then queued for offline repair which we will cover shortly.

- /**Perf** must be used with /Scan and uses more system resources to complete the scan as quickly as possible.
- /**Spotfix** repairs the volume at the next reboot.
- /**Sdcleanup** runs a memory cleanup for unwanted security descriptor data.
- /**Offlinescanandfix** runs an offline scan and fix on the volume.
- /**Freeorphanedchains** frees any orphaned cluster chains instead of recovering their contents.
- /**Markclean** marks the volumes as clean if no problems are detected.

SFC

The System File Checker, used in an Administrator Command Prompt window with the command **SFC**, will check the core operating system files for corruption and attempt to repair them if it can. This is a very, very useful tool that is used with the following switches:

- /**SCANNOW** scans all protected OS files and repairs problems when possible.
- /**VERIFYONLY** scans all the OS files but does not attempt repairs if it finds a problem; instead, it will report any problems found.
- /**SCANFILE=<file>** can be used to verify the integrity of a specific OS file and repair it if possible.
- /**VERIFYFILE=<file>** scans a specific file but does not attempt to repair it.
- /**OFFBOOTDIR=<offline boot directory>** will attempt to scan and repair an offline boot directory; this is useful if you are running SFC from the Recovery Console.
- /**OFFWINDIR=<offline Windows directory>** will scan an offline Windows directory, again useful if you are running SFC from the Recovery Console.
- /**OFFLOGFILE=<log file path>** will create a log file for offline scanning and repair.

DISM

The Deployment Image Servicing Management (DISM) tool is also run from an Administrator Command Prompt and is normally used to help system administrator prepare and service Windows deployment images for installation.

However, you can also use DISM at any time in the format **DISM /Online /Cleanup-image /Restorehealth** to launch its ScanHealth feature. This will scan the Windows installation and attempt to repair any problems it finds.

If you get the message *cannot find source* files, you can use the command with the additional switch **/source:WIM:[X:]\Sources\Install.wim /LimitAccess** where X: is the location of a mounted Windows installation image. Note this must be exactly the same as the version installed on the PC.

Disk Partitions and Formats

It's worth talking a little about Disk Partition and formatting types as you will possibly have to diagnose problems on external, server, and perhaps even legacy drives. Windows 10, as you can imagine, is a very legacy-focused operating system so is compatible with "just about" every piece of software and hardware dating back to the early days of DOS, so where various disk and partition options are available to you. I detail all of these in considerable detail in my book *Windows File System Troubleshooting (Apress, 2015)*, but there are some things to note.

MBR and GPT Partitions

Windows has two partition types available in Windows 10. MBR (Master Boot Record) is a legacy system, while GPT (Globally Unique Identifier Partition Table) was introduced with Windows Vista and Server 2008. There are important differences between the two when determining which you should use for drives on your PC, and Table 28-1 details these differences.

Table 28-1. *Comparison of MBR and GPT partition systems*

MBR	GPT
4 partitions per disk maximum	128 partitions per disk maximum
Less reliable on modern drives	Designed for modern drives
2 terabyte (TB) maximum partition size	Support for disks up to 18 exabyte (EB)
Legacy flat database structure	Improved data structure with parity and integrity checking
No built-in redundancy	Creates primary and backup partition tables
Bootable from BIOS, or legacy BIOS mode on EFI firmware systems	Bootable only from an EFI firmware interface
Available to all removable media types	Not available for removable media
MBR disk can be converted to GPT disk	Conversion to MBR only available with all partitions removed

Windows File Systems

Each different partition structure can support a variety of different file systems, though some aren't directly available in the Windows 10 Disk Management tool, for reasons I shall explain. The supported file systems in Windows 10 include CDFS (for compact disks and DVDs), UDF (Universal Disk Format), FAT12, FAT16, FAT32, exFAT, NTFS, and ReFS for Windows Server. Some of these are useful in different circumstances, but not all are easily usable in Windows 10; see Table 28-2.

Table 28-2. *The different file systems available in Windows 10 for formatting*

File System	Characteristics
FAT (FAT16)	First introduced in 1981 and supported by DOS, OS/2. Linux, and Windows 3.1 onward Only available through the **Format** command at the Command Prompt. Use with the switches `Format X: /FS:FAT`
FAT32	Supported by Windows 95 SP2 and later, file size limit of 4GB, volume size limit of 32GB Only available through the **Format** command at the Command Prompt. Use with the switches `Format X: /FS:FAT32` Used for taking UEFI screenshots in supported firmware

(*continued*)

Table 28-2. (*continued*)

File System	Characteristics
exFAT	64-bit support with extended file allocation table, introduced with Windows Vista and designed specifically for Flash Storage Devices Volume size limit of 256TB and supports more than 1000 files per directory Widely supported, can be used from Format option in File Explorer or from the Disk Management Console Has no native file encryption or compression, does not support Bitlocker To Go In-place conversion from exFAT to NTFS drives using the command `CONVERT F: /fs:NTFS`
NTFS	*New Technology File System*. Default file system in Windows since Vista, supports Bitlocker drive encryption and 64-bit file tables with redundancy Volume sizes up to 256TB with file sizes up to 16TB Proprietary so not supported by all non-Windows devices and operating systems Can be used from Format option in File Explorer or from the Disk Management Console
ReFS	*Resilient File* System. First introduced with Windows Server 2012, designed for data storage with a relational database-type file system Has dependability, redundancy, and stability baked into the design Has no support for compression or encryption. Not available for use on bootable drives Only available through the **Format** command at the Command Prompt. Use with the switches `Format X: /FS:ReFS`

Troubleshooting File and Folder Permissions

File and folder permissions can cause all manner of problems on a PC, from the permissions on a file, folder, or even a whole hard disk becoming corrupt to the permissions being set incorrectly after a reinstall or when a disk is transferred from one PC to another. You can find full and technical information about this in my book *Windows File System Troubleshooting (Apress, 2015)*, but we will look here at what you need for troubleshooting and repairing problems, starting with the different permission types (Table 28-3).

Table 28-3. *NTFS file and folder permission types*

Basic Permission	Description: When Applied to a Folder	Description: When Applied to a File
Full Control	Allows for creation, reading, modification, and deletion of folders and the contents of subfolders and for applications to be run	Allows for the creation, reading, modification, and deletion of files and for applications to be run
Modify	Allows for the creation, reading, and modification of folder contents and for them to be run, but not for the subfolders or contents to be deleted	Allows for the creation, reading, and modification of file contents, and for applications to be run, but not for the files to be deleted
Read & Execute	Allows the contents of a folder to be accessed and applications to be run	Allows files to be viewed and applications to be run
List Folder Contents	Allows the contents of the folder to be viewed	N/A
Read	Allows content to be accessed	Allowed file contents to be accessed but not for applications to be run
Write	Allows adding of files and subfolders	Allows a user to modify, but not to delete a file

Permissions for files and folders can be viewed and modified in the *Properties* dialog for the file(s) or folders, which you can open by right-clicking the item and selecting *Properties* from the menu that appears. Under the *Security* tab, you will see the currently set permissions for different users and user groups on the PC; see Figure 28-6.

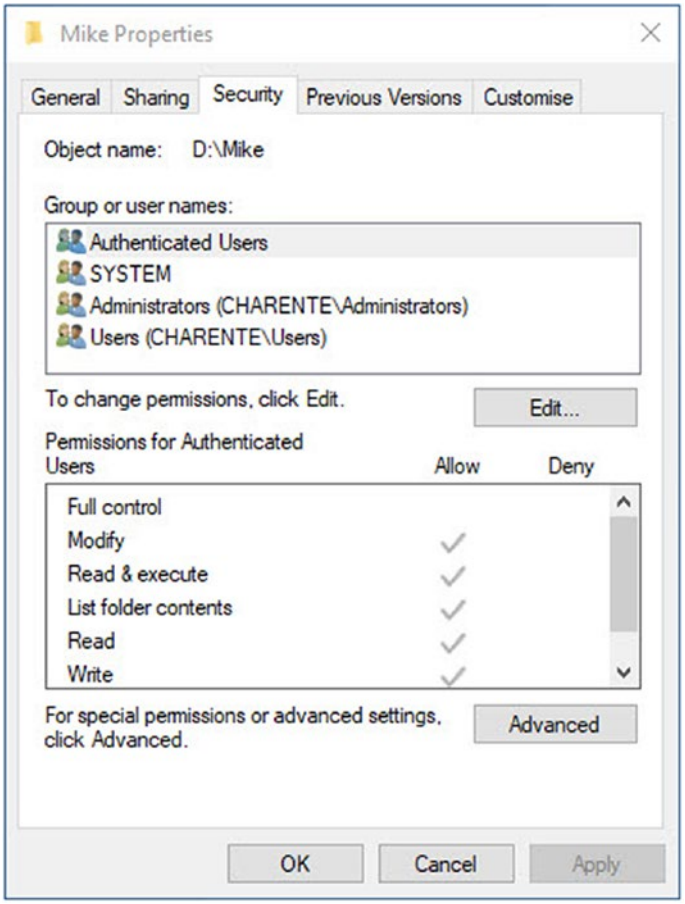


Figure 28-6. *You access File and Folder permissions from within File Explorer*

Here I am looking at a root folder on my secondary hard disk (D:) in which I store all of the files for one specific user account. I can see that Authenticated users have all permissions up to Modify, but when I click on Administrators, I will see that they have *full control*, while standard users only have *Read & execute* permissions.

Sometimes these permissions can be set incorrectly, and you need to perform an action known as *taking control* of the files, folders, or even a whole drive. This can be achieved by clicking the *edit* button, and a new dialog will appear in which you can change the permissions for the selected object(s); see Figure 28-7.

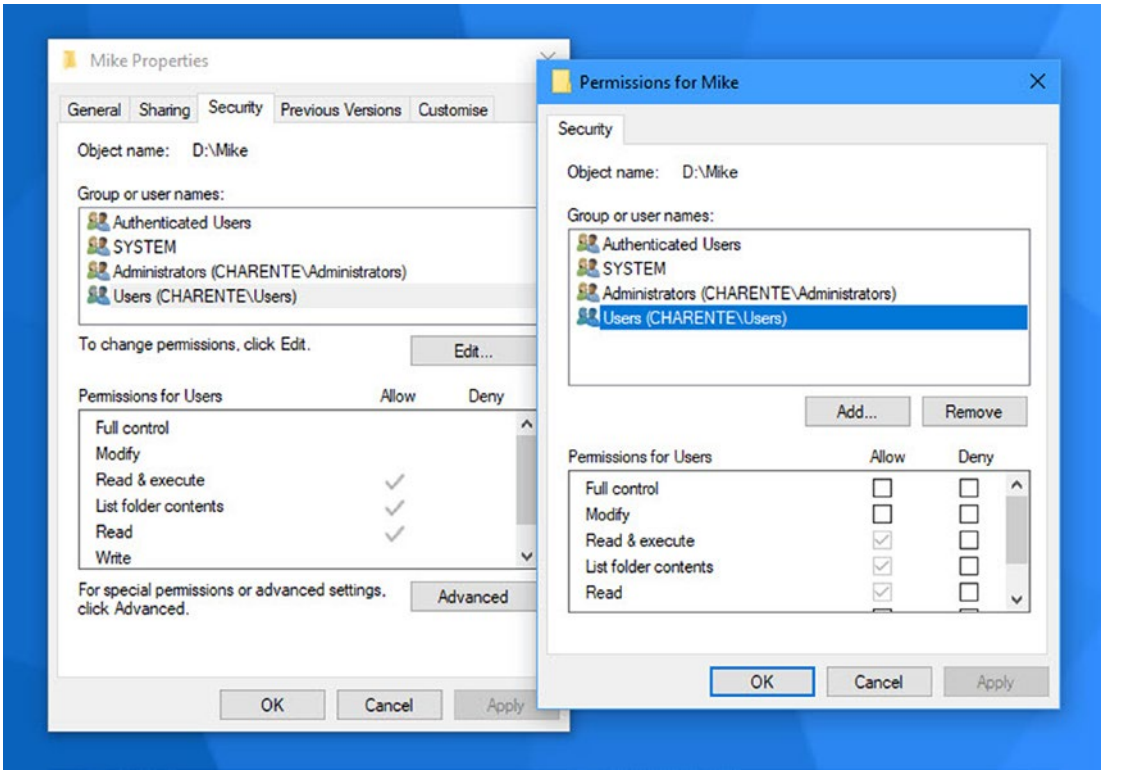


Figure 28-7. *You can change permissions for files and folders for individual users or groups of users*

Checking the permissions boxes you want for the selected user or groups of users and clicking the *Apply* button is often enough to set the permissions correctly. Sometimes however the user or user group you need to set permissions for will not appear in the group. In this circumstance you can click the *Add* button to add the specific user or group of users to what is technically termed the *Access Control List* (ACL); see Figure 28-8.

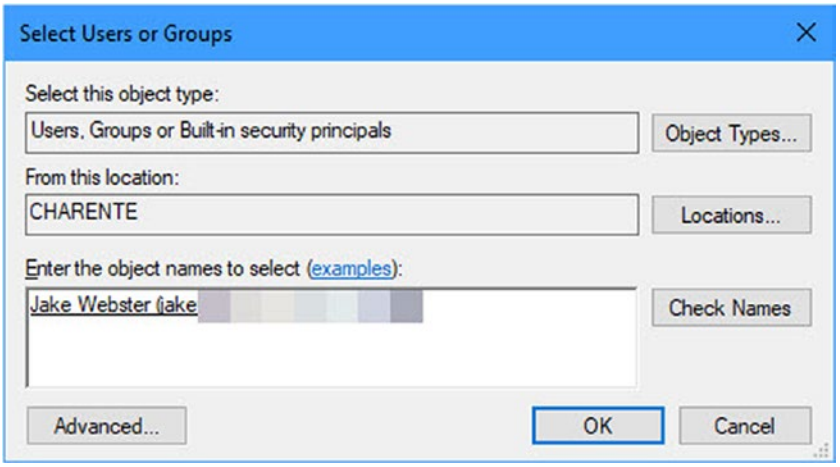


Figure 28-8. *You can add users and groups to the Access Control List*

Note here that you need to search for them using the account name they were set up on the PC with, which is commonly their email address for Microsoft Accounts and Azure AD accounts. Searching for their "display name" won't display the user.

Understanding Permission Inheritance

One of the problems faced with taking ownership of files and folders is that of permission inheritance. This is when files and folders (we'll call them objects here) get their permissions handed down from files and folders further up the folder chain. In the previous example, I was examining the permissions of a root folder on the hard disk.

You may find however that the permissions you need to change on a specific file and folder are being handed down to it, and effectively controlled, by a folder closer to the root of the drive. This can cause all manner of problems with people losing access to their all-important files and folders.

In the *Security* details tab of the file or folder *Properties* dialog, click the *Advanced* button to display more permissions details and options; see Figure 28-9.

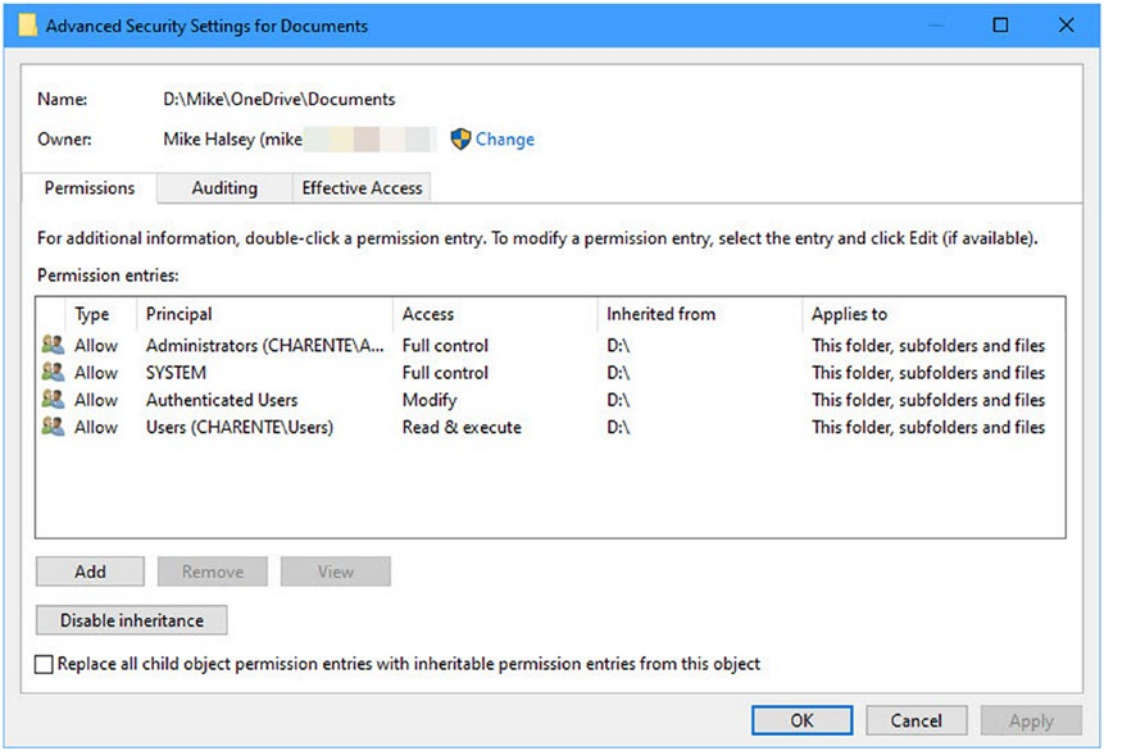


Figure 28-9. *You can view Inheritance details in the Advanced dialog*

In the main panel, you will see an *Inherited from* column. This tells you which drive or folder contains the "master" permissions for the current object. If there is no inheritance, for example, on a drive itself, then inheritance would be listed as "None."

Let's say then that you need to change the permissions on the currently selected object without the inherited permissions constantly screwing everything up for you. You can achieve this by disabling inheritance for the object. Click the *Disable inheritance* button, and a dialog will appear asking if you want to *Convert inherited permissions into explicit permissions…* or *Remove all inherited permissions…*; see Figure 28-10.

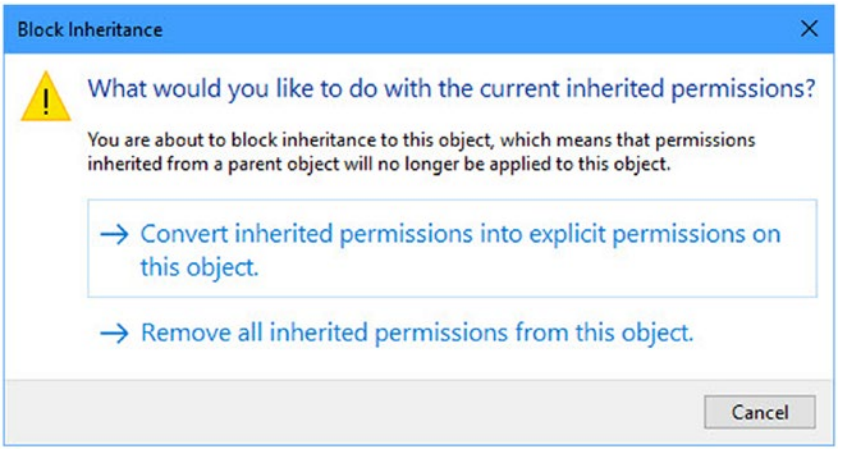


Figure 28-10. *You can disable the inheritance of permissions on an object*

Caution Be very careful with removing all permissions on the object as you will end up with that object having no permissions on it at all. You should always immediately add *Full Control* permissions back for SYSTEM; otherwise, you will end up with an object that cannot be read, accessed, or even deleted by Windows.

It is always a good idea to have inherited permissions simply to aid good file and folder management and administration. Thus, if you are moving the object to a new location or drive, or just tidying up a permissions mess, when you have set the permissions correctly on the folder or drive, they were inherited from, you can *[Re] Enable Inheritance* in the same way.

Checking the Effective Access for a User or User Group

If you need to check the access a specific user or user group has on an object, this can be done from the *Effective Access* tab in the *Advanced Security Settings* dialog. Select the user or user group you want to check, and then click the *View effective access* button; see Figure 28-11.

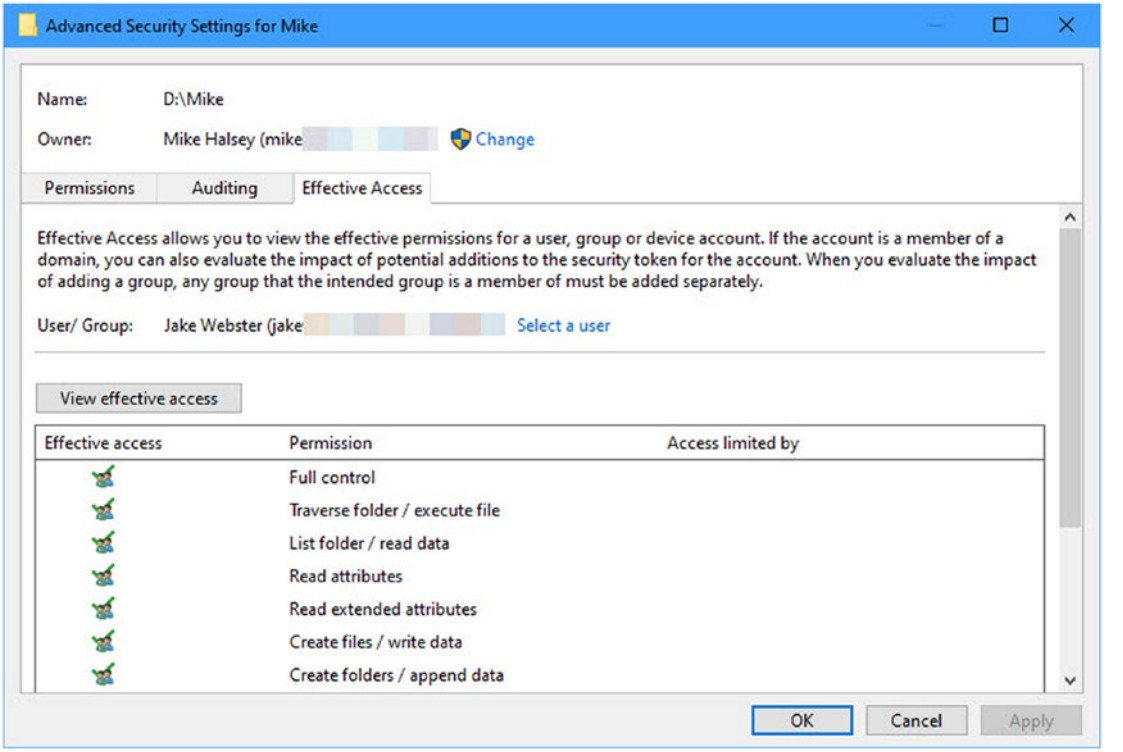


Figure 28-11. *The Effective Access tab lets you check permissions for users and user groups*

Taking Ownership of Files and Folders

Let's say you have performed a clean reinstallation of Windows 10, or perhaps you have moved a hard disk from an old PC to a new one. You suddenly find that you don't have control over the hard disk or any of its files and folders because you don't have the necessary permissions, them having been set for a user account that doesn't currently exist with the same identifications as it did before.

You can change the ownership of any drive, file, or folder in the *Advanced Security Settings* dialog by clicking the *Change owner* link next to the *Owner:* identifier; see Figure 28-12. This will display a dialog where you can choose a new owner or owner group for the object.

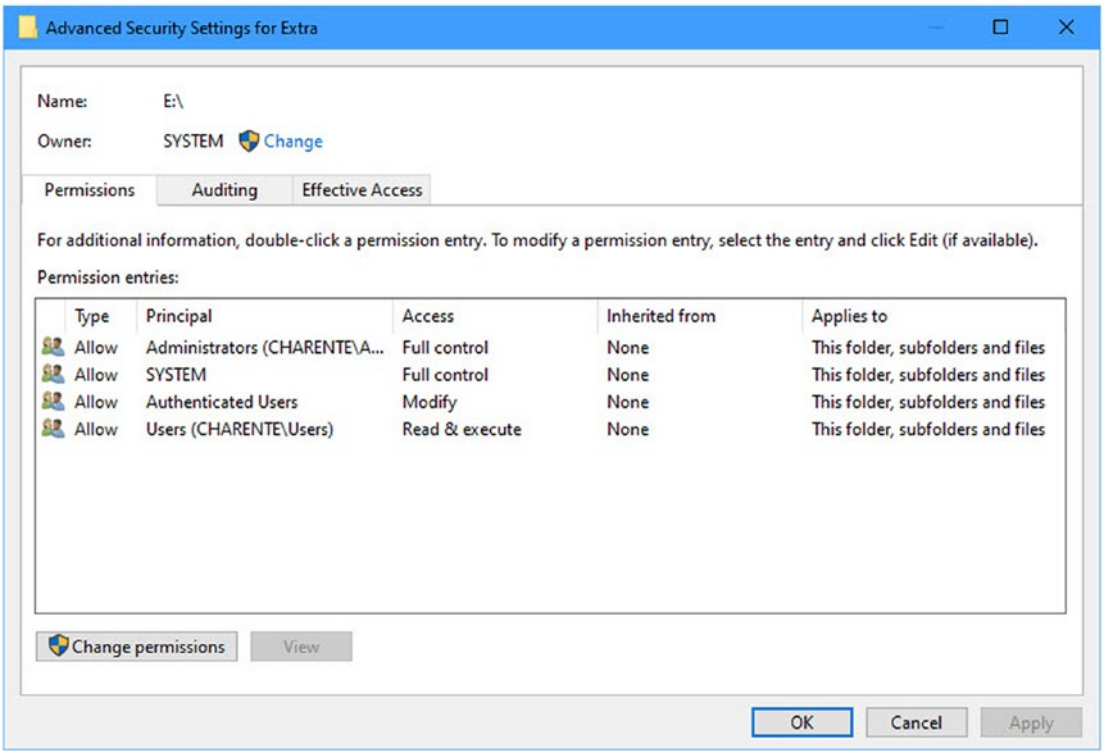


Figure 28-12. *You can change the owner of a file, folder, or disk*

Just like disabling inheritance, this should be done with great care. If you check the ownership of your folders and drives on your own PC, you will see that while individual users of user groups have ownership of the folders, the hard disks are done differently. The Windows drive itself will have *TrustedInstaller* as the owner, and any additional hard disk or partition will have the own set to *SYSTEM*. This should be maintained so that Windows on your PC can access the drive and get the permissions it needs for file and folder operations and encryption management.

Using Scripting to Handle Access Control Lists

If you prefer to use scripting to manage your Windows installations, you can use both the Command Prompt and PowerShell to control ACLs. The **icacls.exe** commend is the former, and it can be used to control all permissions on disks, folders, and files in Windows. You can read full information about the switches used with the icacls command at the Microsoft website on this link `https://pcs.tv/3CwKJ18`.

If PowerShell is more your bag, then two powerful cmdlets will let you manage permissions for any object on a PC. These are `Get-Acl` and `Set-Acl`. You can use these to manage permissions; see Figure 28-13. You can read technical details on how these two commands work on the Microsoft website at this link `https://pcs.tv/3lKn8UO`.

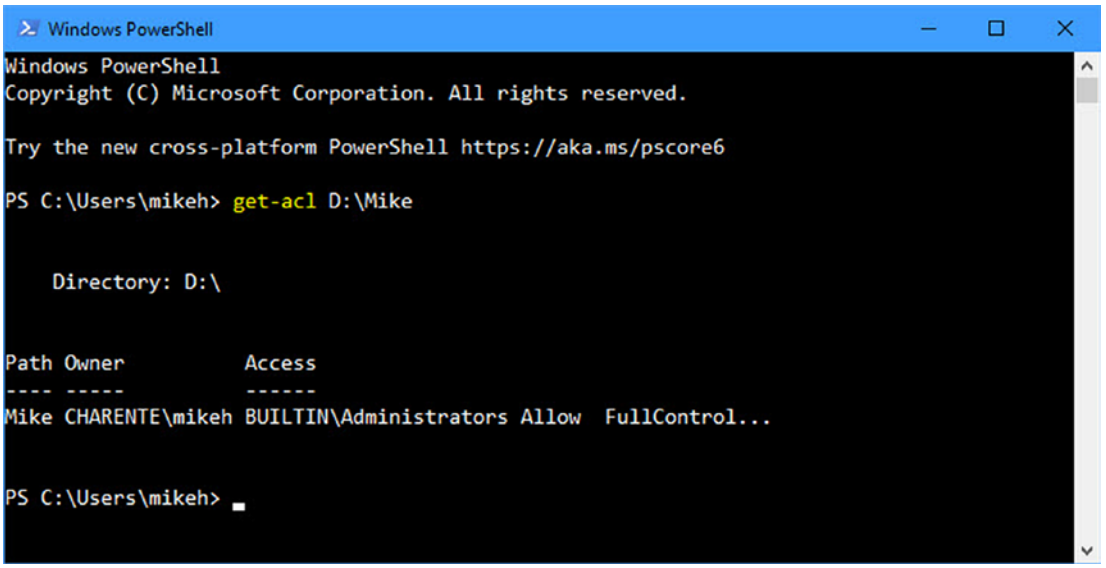


Figure 28-13. *You can manage Access Control Lists in PowerShell*

Troubleshooting File and Folder Sharing

Shared folders and drives on PCs are nothing new, though in these days of cloud storage, collaboration features in Office and drives in the multiterabytes of size, there's not much use for it. Sometimes though it can come in very useful such as sharing an optical drive on a PC with a laptop that needs to read from a CD but doesn't have a drive of its own.

The best and easiest way to troubleshoot problems with folder and drive sharing is, on the PC the object is being shared from, to right-click it, and select *Properties* from the menu that appears. Then, under the *Sharing* tab of the next dialog, click the *Advanced sharing* button; see Figure 28-14.

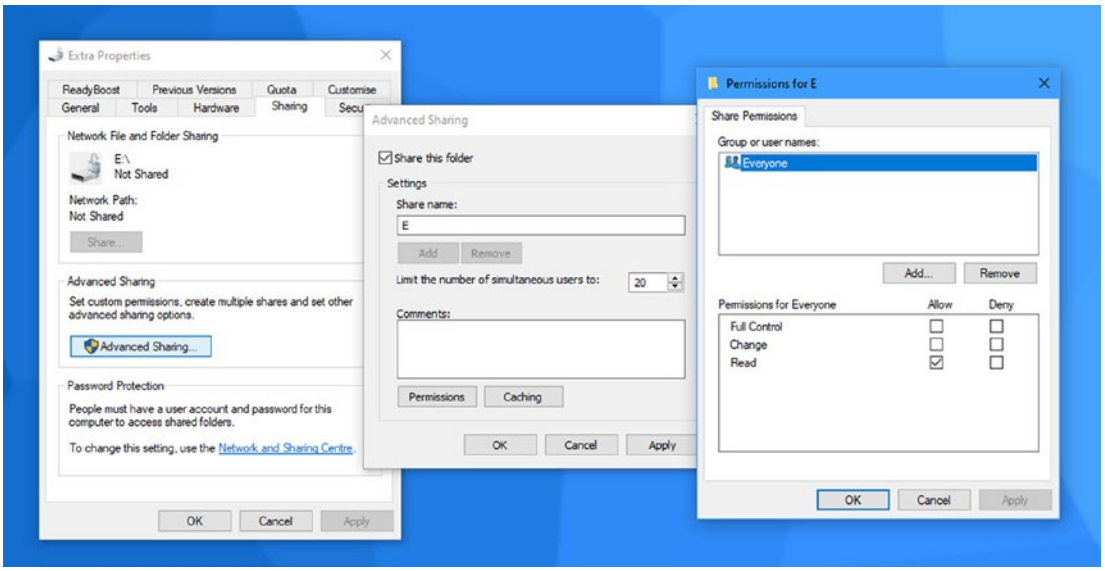


Figure 28-14. *You can easily troubleshoot sharing and sharing permissions in Windows*

Here you can check if the share is active and what the share name is. It is possible the share name has changed, or the user trying to access the share has been given the wrong name and can't find it. Clicking the *Permissions* button will then allow you to check if the user or user group the object is being shared with has the correct permissions set. If they do not, either you can click the user or group in the *Group or user names* list, change the permissions, and click *Apply* or you can click the *Add* button to add a specific user or a wider user group to the ACL for the shared object.

Summary

So, there you have it, an in-depth breakdown of what's what and why it's there in the Windows file system. The Windows OS is indeed a horrifically complicated beast when it comes to its file structure. Knowing what the look for, where to find it, or even what the hell something is can be a very frustrating and difficult process.

While we're on the subject of difficult problems, this gives me a good segue into the next chapter, where I'll be showing you how you can use the Internet to research the more difficult troubleshooting problems you might encounter. This includes where you can look online, what to look out for, how to avoid getting the wrong advice, and what tools are available that can help you in your work.

CHAPTER 29

Researching Difficult Problems

Throughout this book I've detailed the tools and utilities available to you, both within Windows 10 and externally from Microsoft and third parties, to help provide information and diagnose and repair problems. This is all fine for straightforward issues where it's clear what the cause of the problem is, and how you can repair it. What happens, though, when the cause of a problem is less clear, when there's some obscure error message that could have one of several causes, or when finding the actual solution to the problem is like searching for the proverbial needle in a haystack?

Troubleshooting is a very similar task to detective work, I've always said. The most famous detective quote comes from Sherlock Holmes: "Once you have eliminated the impossible, whatever remains, however improbable, must be the truth." This process of elimination is crucial in speedily determining the cause and discovering the correct solution for a problem, and let's face it and to slip in another well-used quote, "time is of the essence," when you're busy and need to get people working again. First, though, you need to be armed with the correct information.

Reading the Windows Log Files

Having accurate information is essential in troubleshooting any type of problem. Way back in Chapter 5, I detailed the Event Viewer, and how you can get extremely detailed information about events, errors, and crashes. Sometimes however, you also need direct access to crash logs. I detailed the locations of these in Chapter 27, but let's look at how you read them, and how you make sense of them.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_29

Log Text Files

The `Windows\Debug` log files contain audit (installation, deletion, update, etc.) operation details and app crash details in plain text file formats; see Figure 29-1. The files you will find in this folder will vary and are entirely dependent on what's been happening on the specific machine. In the following image, we can see that there are logs for the `wiaservc.dll` file.

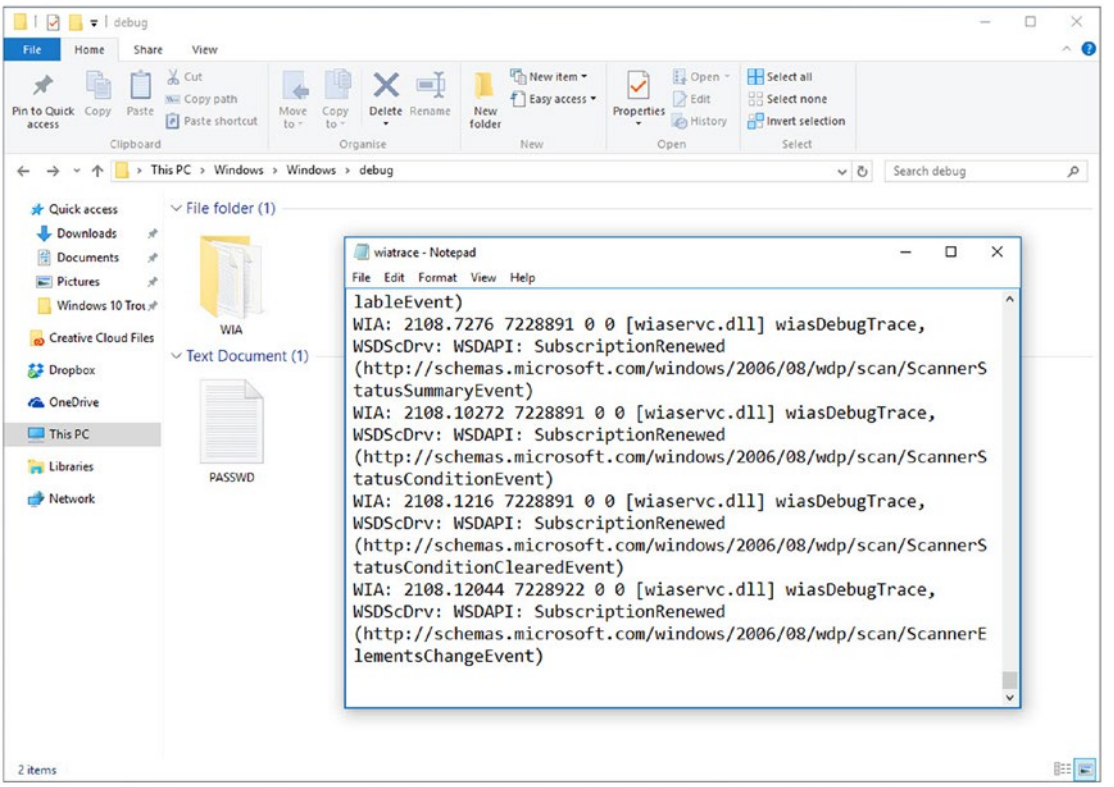


Figure 29-1. *The Windows\debug log files are stored in plain text format*

A search online, and I'll show you how to do this efficiently later in this chapter, reveals that this is the Windows driver associated with "still image devices." It makes sense that there would be event logs for this service, as I have been unplugging my printer (with its integrated scanner) fairly often recently, so I can plug a desk fan into its power outlet instead.

You will see in the text file though there is also a more verbose description of the events in the form of website links. You can copy and paste these into your browser to see more detailed information on the Microsoft website.

Reading .xml and .etl Files

The `Windows\Logs` folder is where the main Windows 10 logs are stored. They are separated into subfolders, most of which are sensibly named, such as RecoveryDrive and SystemRestore; see Figure 29-2. The log files are stored either as plain text (`.txt`) files, which can be opened in Notepad; as Extensible Markup Language (`.xml`) files, which can be opened and read in a web browser, such as Edge or Chrome; or as Event Trace Log (`.etl`) files.

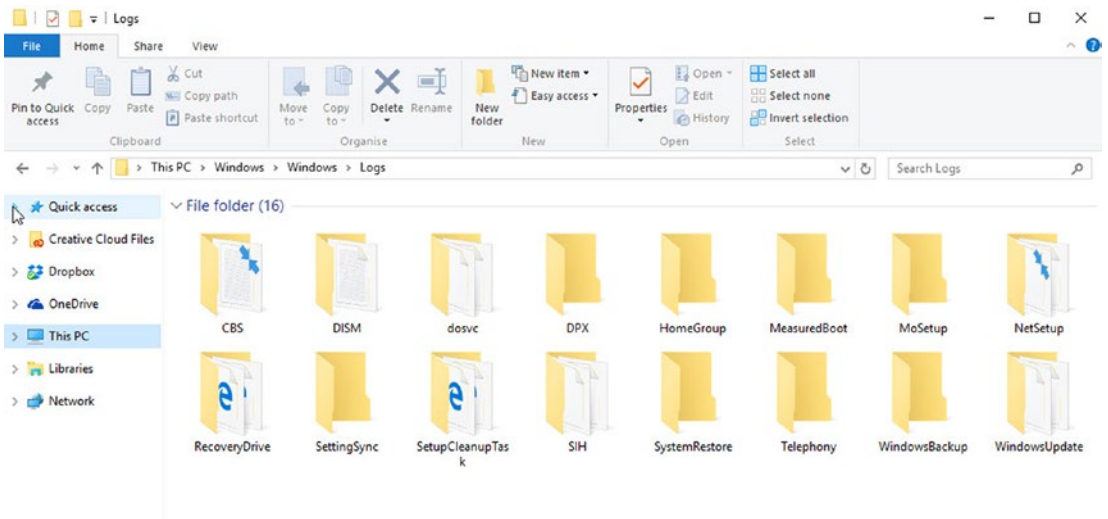


Figure 29-2. *The Windows\Logs folder contains the main Windows Logs*

Event Trace Log files are opened in the Event Viewer. They should all be available in the Event Viewer anyway, if I'm honest, though you may wish to open a file from another PC, perhaps one that's been emailed to you. To open an .etl file, in the Event Viewer, click the *Action* menu, and then click the *Open saved log* option; see Figure 29-3.

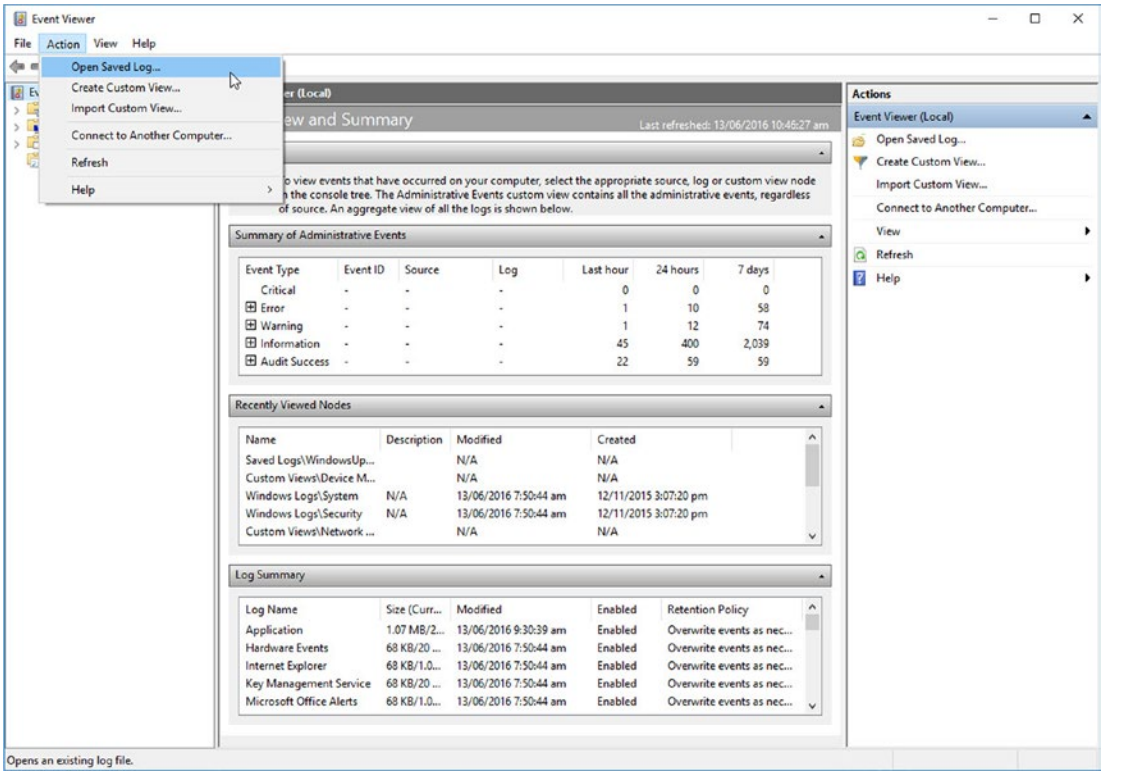


Figure 29-3. *You can open .etl files in the Event Viewer*

Once the `.etl` file has been opened in the Event Viewer, you will see it appear in the left panel in a new Saved Logs section; see Figure 29-4. You can now view it as you would any other event log. In the event logs, you're looking for several things that can guide you toward identifying and finding a solution to the problem. These can include a verbose description of the error, which can be extremely helpful, and also additional information such as Windows error codes (in the format 0x00...), driver, application, and also DLL file names.

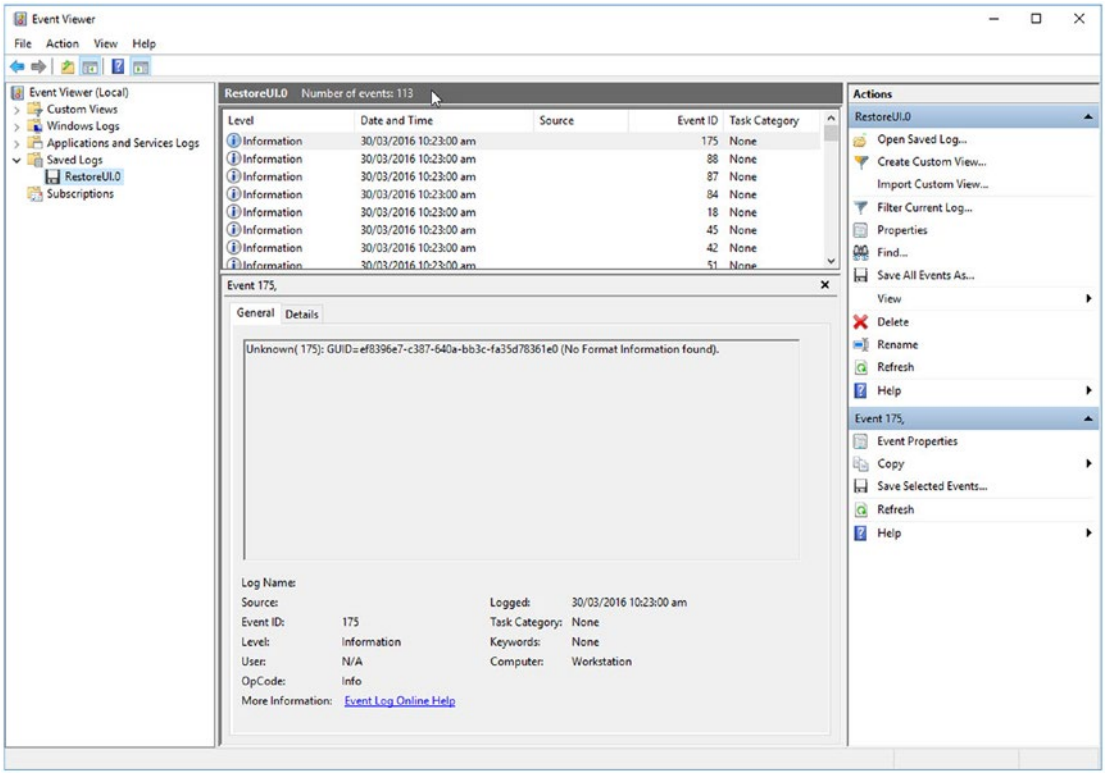


Figure 29-4. *The opened .etl file will appear in the Saved Logs section*

Reading .dmp files

The `Windows\MiniDump` folder is where you will find critical error log files, such as those associated with a Blue Screen of Death (BSOD). These files are stored in the slightly less friendly sounding `.dmp` format and cannot be opened natively in Windows 10. There are several ways to open them, however. If you have access to Microsoft Visual Studio, you can download the Windows Driver Kit (WDK) or Windows Software Development kit (SDK). Both of these will allow you to open, and read, the contents of the `.dmp` file.

Perhaps a preferable option for many people will be the third-party utility *BlueScreenView*. You can download this from `www.nirsoft.net/utils/blue_screen_view.html`, and it will automatically display the contents of all the `.dmp` files located in your `Windows\MiniDump` folder; see Figure 29-5.

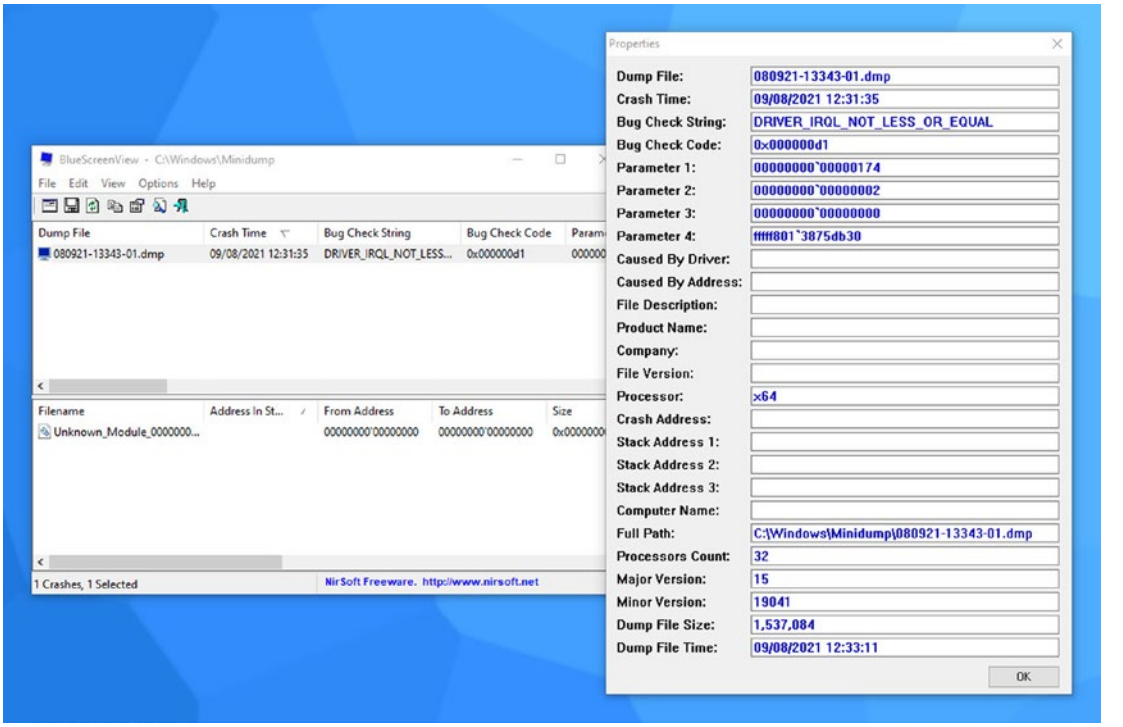


Figure 29-5. *BlueScreenView is a handy freeware utility for reading .dmp files*

So, what is it you're looking for within a .dmp file that can tell you why a Blue Screen occurred? There are plenty of pieces of useful information to be contained in the log, including the verbose text of the *Bug Check String* and the Windows standard error code in *Bug Check Code*. These can be searched for online to discover the cause of the problem, and hopefully a solution.

You can see in Figure 29-5 a critical error that occurred completely out of the blue on my own PC just the other day. The description is `DRIVER_IRQL_NOT_LESS_OR_EQUAL`, and the Windows error code is `0x000000d1`. A quick search online reveals useful information about this error, which dates back several versions of Windows. It could be caused by a variety of things including an incompatible or corrupt device driver or an Interrupt Request (IRQ) conflict. While the latter is extremely rare in Windows 10 since the introduction of the Windows Side-by-Side (WinSxS) folder, it's a legacy problem that can appear occasionally, and for many drivers you can check in their *Resources* tab in the Properties inspector for the driver, to see what IRQs they use and if any conflicts exist; see Figure 29-6.

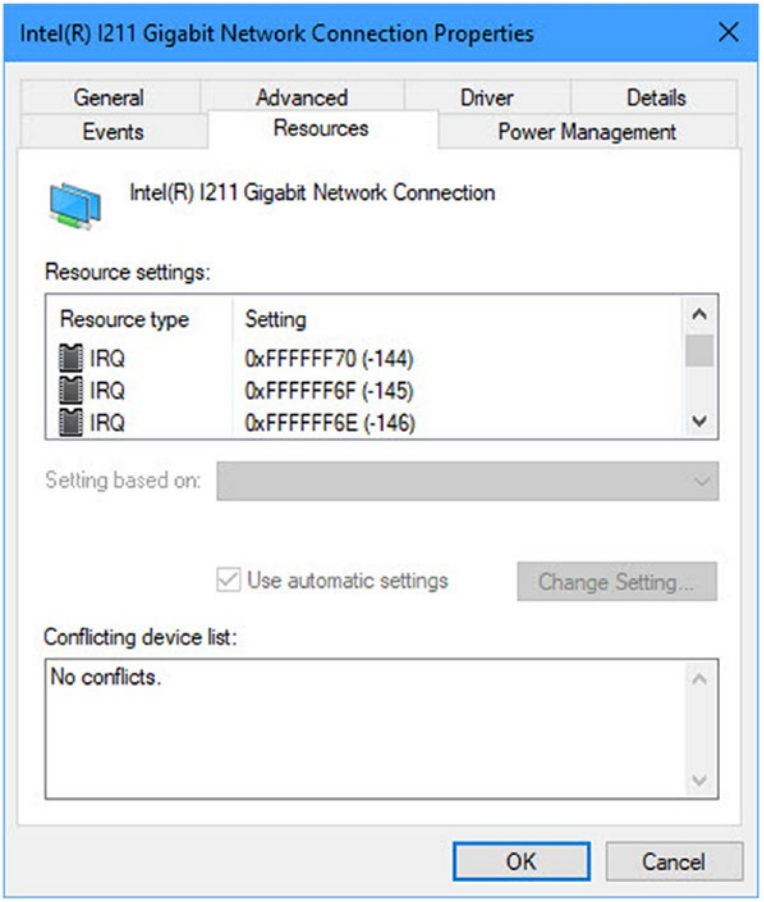


Figure 29-6. *You can check individual drivers for IRQ conflicts*

In this case the advice from many websites online would be to check Device Manager and Windows Update for updated drivers or download them manually if they're available from places such as your motherboard or graphics card manufacturer (who often bundle a utility with new PCs to handle this very task), and to see if an update to your BIOS is also available. All of these are good advice, and they're exactly what I'd look to do myself.

Searching the Internet for Solutions

The Internet is brilliant, the Internet is amazing, the Internet is all-powerful (okay, maybe not that last one), but certainly the Internet is a fantastic tool for researching the causes of and the solutions to problems on our PCs. Sadly, the Internet is also full of bad advice, misinformation, incomplete answers, sites that are simply after your money, and… let's face it, malware.

Knowing how to use the Internet to effectively search for and find solutions to problems can be a challenge in itself. Anybody can type a search query into Google or Bing and click the first link that appears in the search results. Is this going to provide the best result, the correct solution, or something less helpful, such as a website that's just trying to sell you something?

An example of this is that there are usually several, or even many, different problems that can result in the same error code. You may have to spend some time digging or try a few different things before you get the fix you need.

Tip You can make your Internet searches more effective by using search operators such as + (plus) before a word to force the inclusion of that in all the results, – (minus) before a word to specifically exclude that word from searches, and "…" (double quotes) around a search phrase to prevent the search returning results that contain each word you type individually. You can find Google search operators listed at `support.google.com/websearch/answer/2466433` and Bing search operators at `https://help.bing.microsoft.com/apex/index/18/en-US/10002`.

I want to start with a warning. Well, I don't want to, but it's very important. When you're searching for solutions to problems, and especially when you're searching for hardware drivers (using either the hardware device name or the VEN_ and DEV_ codes), there are a great many websites that will present you with their own installer, such as that seen in Figure 29-7, that I found when I searched for an Asus network card driver.

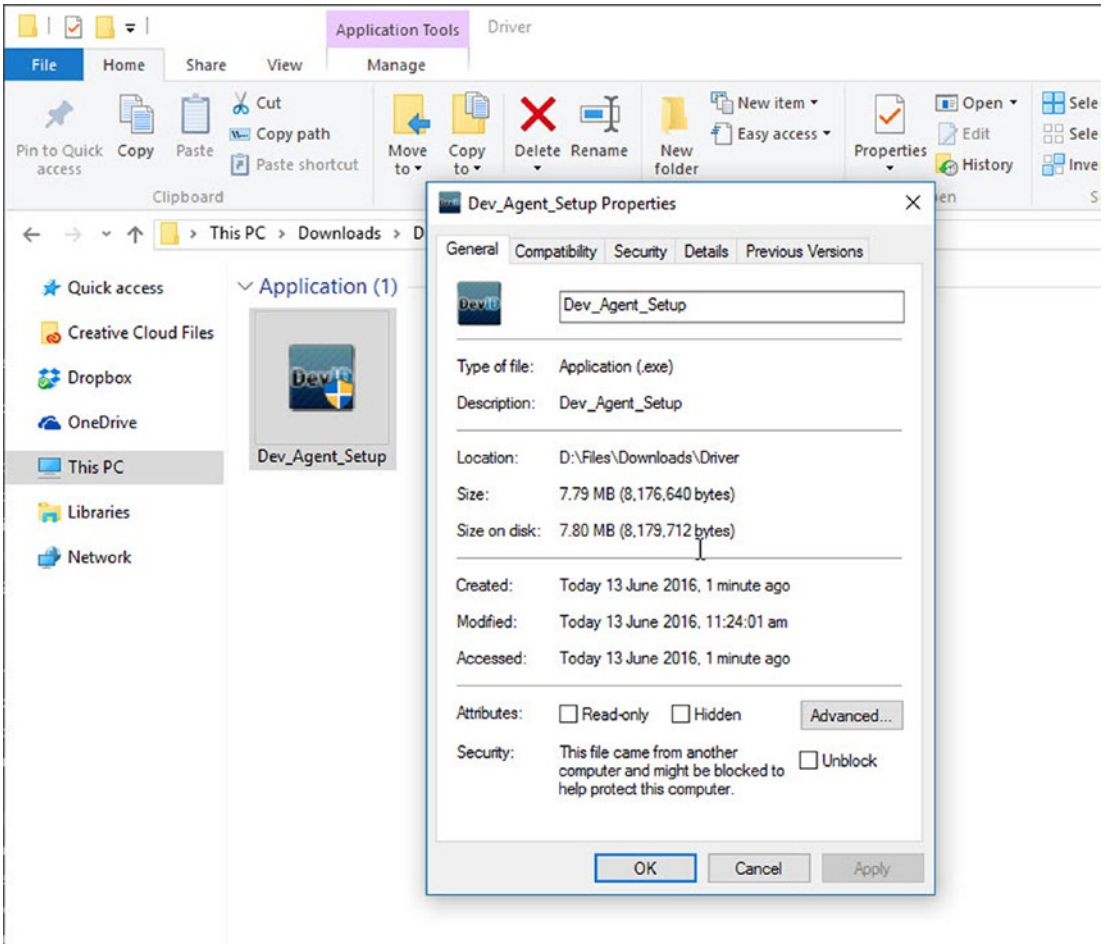


Figure 29-7. *Many "driver download" sites want you to install an unknown payload*

There is absolutely no way to know what is in these files until you click them and give them Administrator permission to install. **DO NOT EVER DO THIS** as once the installer has administrative rights, it can install whatever the hell it wants on your PC, from browser plugins and unwanted apps to malware. I would also stress that you **MUST NEVER USE** paid-for driver download services. Drivers are always freely available online; you will not ever need to pay for them.

So, what websites can you trust to provide quality information? Here's my rundown of the best, and those I would recommend.

Microsoft Docs

Microsoft Docs, found online at `docs.microsoft.com`, should always be your first port of call for researching anything for any Microsoft product. Throughout this book, where I've had to refer you to in-depth guides for Command-Line utilities, or PowerShell scripts, it's always been to Microsoft Docs.

Microsoft actively push their staff, contributors, Most Valuable Professional (MVP) awardees such as myself, developers, and more toward providing content for Microsoft Docs, and it's now by far the most comprehensive information and support resource for *all* of the company's products and services; see Figure 29-8.

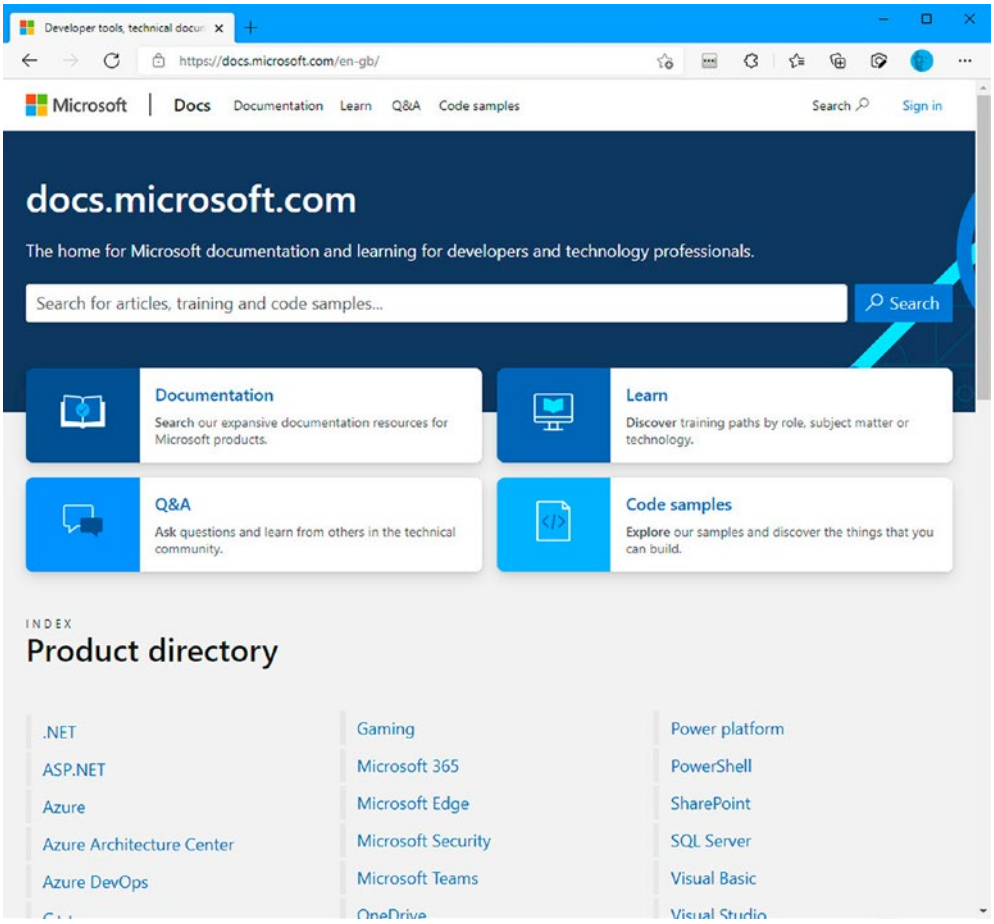


Figure 29-8. *Microsoft Docs is the main resource for help and information on the company's products*

Answers.Microsoft.com

The Microsoft Answers site is always a great resource, not the least of which is that Microsoft has its own support staff to answer questions and provide support. This is a great example, however, of how you should not always trust the quality of the advice you are receiving. Figure 29-9 shows three "badges" that are automatically assigned to different types of forum participants.

Of these, only two can be trusted absolutely for their professionalism; can you tell which one can't? Obviously, the one labeled "*Microsoft Support Engineer"* will be a dedicated support person, employed directly by Microsoft.

Figure 29-9. *The Microsoft Answers website tells you how qualified the person giving support is*

Of the other two, you can always trust the advice of an *MVP*. MVPs, such as myself, are technical experts that have been awarded with the MVP (Most Valuable Professional) badge to mark the significant contributions they have made in helping Microsoft's user communities worldwide.

An *Insider,* however, is anybody who has signed up to be a member of the Windows Insider (beta) program. Anybody can join the Windows Insider program, as it's open to the general public. As such, some answers given by insiders can be inaccurate.

Support.Microsoft.com

This is another dedicated Microsoft support site, with the help across all of the company's products. There are also community forums here, in which you can search for your problem to see if anybody else has encountered it as well. Windows 10 also comes with a *Get Help* app (see Figure 29-10), which you can find in the Start Menu.

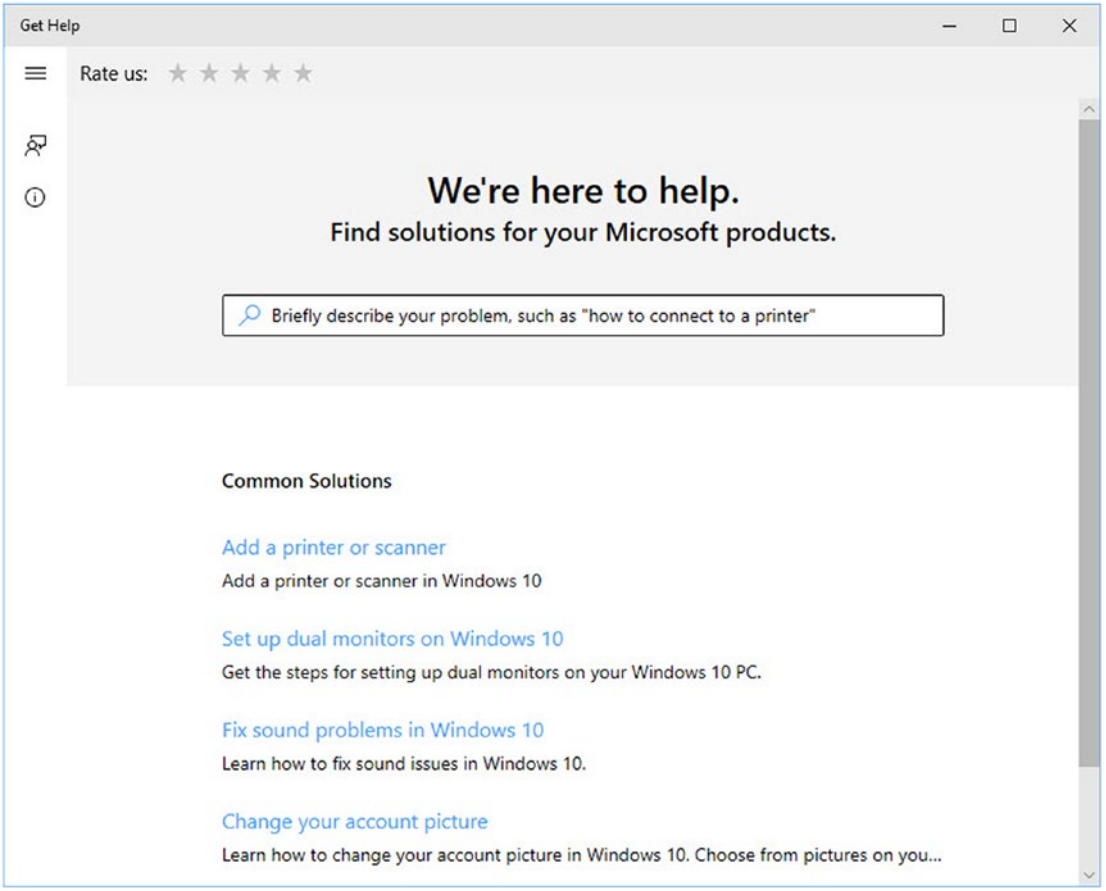


Figure 29-10. *Windows 10 comes with a Support app*

Other Microsoft and Third-Party Support Sites

There are a great many excellent-quality support websites provided by third parties. The best of these are

- Annoyances.org—`www.annoyances.org`
- Computing.net—`www.computing.net`
- **How To Geek**—`www.howtogeek.com`
- **Microsoft Download Center**—`www.microsoft.com/download`
- **Ten Forums**—`www.tenforums.com`
- **Tom's Hardware**—`www.tomshardware.co.uk`

Tip Twitter is a great resource if you are having trouble with a PC. Occasionally a problem will hit with a driver or Windows update that will affect a great many people. You can get instant reaction, and sometimes instant help, by monitoring Twitter for search terms or hashtags.

Hardware Driver and Support Sites

I always recommend that you download hardware drivers directly from the manufacturer's website. These websites will also have forums in which you can post questions and get answers directly from technical staff at the company:

- **Acer**—www.acer.com/support
- **Asus**—www.asus.com/support
- **AMD**—support.amd.com
- **Dell**—www.dell.com/support
- **HP**—support.hp.com
- **Intel**—downloadcenter.intel.com
- **Lenovo**—support.lenovo.com
- **Microsoft Surface Support**—www.microsoft.com/surface/support
- **Nvidia**—www.nvidia.com/page/support.html
- **Samsung**—www.samsung.com/support

Third-Party Support Tools

Additionally, there are many excellent third-party help, information, and support tools that are favored by IT pros; these are in addition to the Microsoft Sysinternals suite that I detailed in Chapter 22:

- **Aida64**—www.aida64.com
- **CCleaner**—www.piriform.com/ccleaner

- **Disk Digger**—www.diskdigger.org
- **GRC**—www.grc.com
- **Hiren's Boot CD**—www.hiren.info/pages/bootcd
- **Sandra Utilities**—www.sisoftware.eu
- **TeamViewer**—www.teamviewer.com
- **Ultimate Boot CD**—www.ultimatebootcd.com
- **WhoCrashed**—www.resplendence.com/whocrashed

Summary

It's certainly true that because the Internet is the ultimate democratic outlet, it's also full of errors and misinformation, as well as unwanted and malicious drive-by downloads. You should always be careful from where you source information and what you trust. Certainly, you should never download a driver that comes in its own container from the website that hosts it, as you have absolutely no idea what else might be in that package.

Researching difficult problems, however, is only half of the story, and in the next chapter, I'll show you how you can go about fixing them. This can include working safely with hardware, fixing the seemingly unfixable, and connecting the dots to see if the cause of your problem lies outside of the PC itself.

CHAPTER 30

Troubleshooting Difficult Problems

Troubleshooting is a process of elimination, detective work to join up the dots, making connections between different aspects of the OS, hardware, apps, and other factors, and coming to conclusions based on technical knowledge and expertise. This book can give you the technical knowledge you need to diagnose and repair problems. What do you do, though, in terms of the actual detective work?

Well, you might be surprised that this can be taught as well. (You can tell I'm a teacher, can't you?) Troubleshooting requires that you look at your PC holistically. It might appear, for straightforward faults, that a problem is being caused by a graphics driver, or that a nonbootable PC might have a faulty power supply. What do you do with the more complex problems, however, perhaps those that only occur occasionally or under certain circumstances?

"Mike Halsey's Holistic Troubleshooting Agency"

Back in 1987, acclaimed science fiction author Douglas Adams—he of the famous *Hitchhiker's Guide to the Galaxy* (Pan, 1979), some Monty Python contributions, and fondly remembered episodes of Doctor Who—released a novel called *Dirk Gently's Holistic Detective Agency*. The protagonist, the aforementioned Dirk Gently, believed in the "fundamental interconnectedness of all things," and used this principle to solve all manner of difficult and dangerous cases, from messy divorces to missing cats.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_30

Silly an idea as this might be for a novel (though no sillier than Adams' other novels; Ed), it's a sound principle to begin with when troubleshooting PC problems. To give an example of this, let's look at a typical PC system (it can be any type of PC), and how interconnected and interdependent it is on other services and devices. Our typical PC is connected to, at some point or another, each of the following:

- Keyboard
- Mouse
- Internal or external monitor
- Internal hard disk
- External hard disk/NAS drive
- Power cable(s)
- Monitor cable(s)
- Network cable(s)
- Wireless dongle/aerial
- USB hub (and cables)
- Router/switch
- Telephone socket/cable socket/satellite dish
- Telephony/cable network
- Telephone exchange
- Satellite
- Data center (with all the PCs, cabling, routers, etc. that entails)
- Company server (with all the routers, switches, storage, and cabling that entails)

…to be honest I could continue this list ad infinitum, but you probably get the point that when troubleshooting a problem on a PC, you might not see that problem contained within the apps, drivers, and OS structure that we're typically used to.

Gauging Both Internal and External Factors

I'll give you a couple of hypothetical scenarios. In the first, a PC user has called tech support to report a problem. "It's only intermittent," he says, only happening very occasionally. "Right!" you might proclaim, knowing that it's probably something he's doing, or something that's going on at that specific time. It could be a problem that only occurs when he runs the payroll software on the PC (so a software error or database connection failure), when he uses the printer (a driver, configuration, cable, or hardware fault), or about once a month on a Tuesday (could it be linked to Microsoft's Patch Tuesday update cycle for Windows?).

In scenario two, a worker in a busy office has a problem on their PC that's caused her to have to stop work. She details the issue she's having on her PC, but completely fails to mention that three other people in her office are also having trouble with their PCs that morning. Those are different problems though, so she didn't think it was worth mentioning. When you look at these problems separately, though (Azure AD not connecting, VPN connection dropping, NAS storage problem, and a PC that is hanging on a black screen at startup), it's reasonable to assume that none of the problems are local to the PCs themselves, but that all of them exist elsewhere on the company network (a PC hanging on a black screen at startup can sometimes be fixed by temporarily unplugging its Ethernet cable).

There is also all manner of external factors which can cause problems with PCs:

- Dust/pet hair collecting in vents and fans, or when a laptop/tablet is somewhere such as a construction site or the beach.
- Extreme heat/cold (though modern hardware is extremely resilient to these).
- Thick brick or stone walls (these can block Wi-Fi and other radio signals and frequently annoy people from the United States who visit Europe).
- Using the PC at a different location (another office or outside of the company).
- Poor cable routing (can lead to snagged and damaged plugs and cables).

- Insufficient amounts of available power, or an unreliable electricity supply, can cause PCs to fail to start, restart periodically, or to shut down occasionally.
- Human beings (who really are capable of being complete idiots).

Indeed, one of my all-time favorite phrases from the aforementioned Douglas Adams is "the problem people face in trying to make something completely foolproof, is that they frequently underestimate the ingenuity of complete fools."

Tip Some problems can be caused by the use of poor-quality cabling. Unshielded twisted pair (UTP) cables are commonly used for networking, as they're cheap. Good-quality shielded cables, however, can prevent many of the problems associated with UTP cables, such as picking up interference from television, radio and cellular signals, microwave ovens, and powerful motors.

It's the same when looking for problems internally on the PC as well. I had a problem on my own workstation PC at one point where the machine was completely and very suddenly failing to start. There was nothing happening when I turned the PC on, short of the power light coming on and a faint whirr of some fans. On the face of it, you might think, as I initially did, that the power supply had failed or that it just wasn't producing enough power any more to get the PC going. As it turned out, however, the graphics card had failed and was causing the entire system to hang in the BIOS. Because I had no picture though, I couldn't see the error it was producing.

Another example, this one from a personal friend and former Microsoft MVP awardee Dustin Harper, is that he was troubleshooting a PC that kept switching itself off after a few seconds. It transpired that the PC had been dropped, and the power button was pushing inward, remaining depressed. Releasing the power button rectified the problem.

Using Troubleshooting Tools Together

There are a lot of Windows, Microsoft, and third-party troubleshooting and diagnostic tools available for Windows 10 and that I've detailed throughout this book. Sometimes, though, you might find that just looking in the Event Viewer, or checking what's going on in the Resource Monitor, isn't enough. You might need to use more than one of these tools, perhaps even three or four, together at one time.

Using tools in concert with one another such as this can help you get a clearer picture of what's going on. Let's say you have a network problem. It might be caused by a driver, configuration, cable, or other issues, but the PC is pinging the network and the connection keeps dropping. With the Task Manager open, you can see the overall network usage; with the Resource Monitor, you can see exactly what apps are trying to use the network connection; and with the Event Viewer, you can set up a Data Collector Set to record warnings, events, and errors on everything those specific and running services apps are doing.

None of the diagnostic and troubleshooting tools I've detailed should always be used in isolation. You might see a rogue process in the Resource Monitor and not know what it is. The Task Manager's *Details* and *Services* tabs allow you to right-click a process name and search online for details of what it might be; see Figure 30-1. In the *Details* tab, you can also open its file location on the hard disk. You can then perhaps use Process Monitor to check the startup and other status of the app or process.

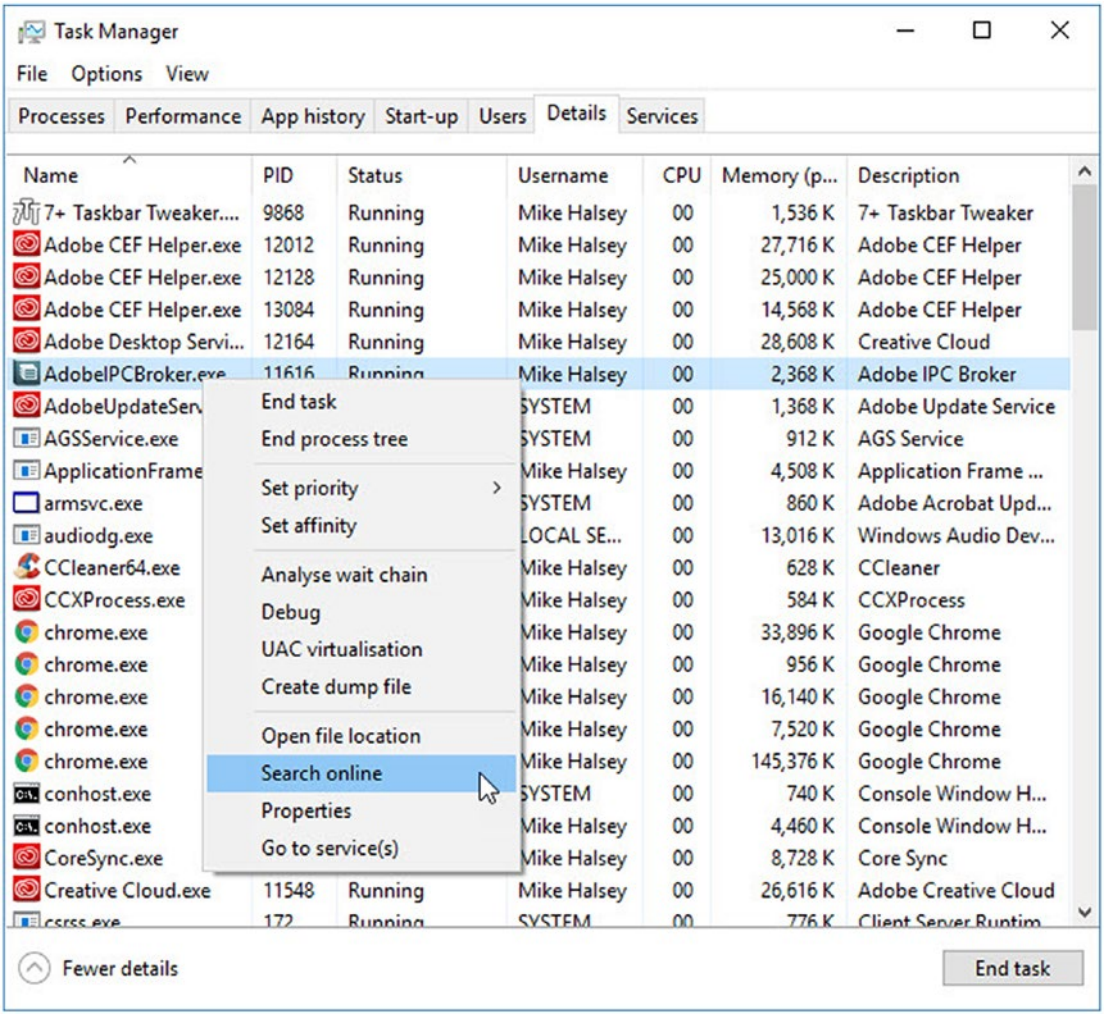


Figure 30-1. *You can search online for details about an app or process*

Troubleshooting and Repairing Hardware

When it comes to troubleshooting and repairing hardware, there are several important considerations. The first of these is safe working, not for you (though you don't want a PC landing on your foot because the table leg is wonky). If you are working on any electronics or electrical equipment, you should also follow these simple rules:

1. Disconnect the equipment from wall power.
2. Remove any trailing or dangling cables.
3. Use an antistatic wristband; see Figure 30-2.

Figure 30-2. *An antistatic wristband can protect delicate electronics*

The latter is very important, as modern electronics can have components that run on microvolts and components just a few nanometers across. Any static electricity you have on your person, which can be picked up from nylon carpets, clothing, metal surfaces, or Christmas jumpers (if you've ever rubbed a balloon on one), can have a profoundly damaging effect on hardware.

There are also the obvious rules to follow for putting the hardware on a safe and stable surface, keeping any unnecessary tools and equipment out of the way, and keeping the equipment away from water or any other liquids.

Note Many laptops and tablets these days are seemingly unrepairable, being sealed thin units with no obvious way into the case. iFixIt, found at `www.ifixit.com`, has repair guides for many of these devices, and they also sell dedicated repair toolkits that can include custom tools required for some devices from companies such as Apple. You should note, however, that opening these devices will void any manufacturer's warranty. One thing that is very helpful if you are looking to purchase new PCs and technology is that iFixIt also provides *Repairability Scores* for tech.

Minimal Boot Configuration and Jumpstarting PCs

I mentioned earlier in this chapter that I had a problem on my own workstation PC a while back, where the PC wouldn't start at all. The lights would come on and the fans would spin up, but nothing else happened.

Initially, I thought it might be the power supply that was at fault. Power supplies fail more than any other piece of hardware due to the heat they build up, their fan(s), and how much work they have to do. It turned out, however, that it was the graphics card, actually one of two in an SLI configuration, which had blown up and was causing the system to hang on the BIOS.

I didn't have a picture on my monitor (as the motherboard didn't have its own graphics output), so I couldn't see that the BIOS was hanging but was able to figure out the problems caused by using a minimal boot configuration. So, what is this, and how does it work?

Minimal boot configuration means stripping a PC's hardware down to the absolute basics and seeing what works and what doesn't. Disconnecting all the optical and hard disk drives, except the one on which Windows 10 is installed, removing all but one memory card, and removing the graphics card (if your motherboard has onboard graphics) and any PCI expansion cards can result in a PC that requires considerably less power to operate. This can be a good way to test both the power supply, which can produce less power as it gets older, just like a motor engine, and also individual components.

You can then try each memory card in turn (remembering to power down the PC when you switch components, obviously), different graphics cards, and expansion cards, and maybe even swap out the power supply for another.

Note Jumpstarting a PC is the process of using the power supply from one PC to temporarily replace the PSU in another. You will probably need to physically unscrew the power supply from the "loan" PC, but then might only need to plug in its motherboard plugs to the PC you wish to test.

It was using this minimal boot configuration that I was able to quickly diagnose the problem with my workstation and trace it to one specific graphics card, which had spectacularly failed.

Summary

Using joined-up thinking and looking at problems holistically can really help when troubleshooting PC problems. If you've been doing PC troubleshooting and repair for many years, as I have, it's all too easy to think of the PC as a stand-alone device. That really isn't the case anymore, however, as the ecosystem into which our PCs plug themselves is both extensive and complex.

We're going to finish this book, though, by going back to the stand-alone principle and looking at installation of the OS. This will include how to troubleshoot problems in upgrading a PC to Windows 10 from Windows 8.1 or even Windows 7 if you're still using it, and how to nondestructively reinstall the OS, so that in the event of a disaster, you can save all of the files and documents of the user on the system.

CHAPTER 31

Installation and Restore

When Windows 10 first launched into its "free for a year" offer, there were plenty of horror stories of people getting unstable systems after upgrading from Windows 7 and Windows 8.1, or from people who couldn't get the new OS installed at all.

The upgrade process to Windows 10 is actually the slickest and most reliable of any Windows upgrade process in the past, though it might sometimes be difficult to believe such a thing. Of the upgrade problems that people had, the faults, I'm sorry to say, were with the end users and the hardware and software makers. If you have a completely clean installation of Windows 7 or Windows 8.1 and upgrade it to Windows 10, you'll get a completely clean and fully working installation.

Sadly, hardware driver writers are almost always very slow to update their drivers when changes made to the underlying OS require such updates. The same is true too of many software houses. Then, you get the end user who wants to use really old versions of software. In many cases this is perfectly understandable and justifiable. I still use Microsoft PhotoDraw 2000 v2, as I've never found anything as powerful yet easy to use, and many people still like to use Microsoft Money. Then, there are a great many third-party apps that are out of support.

Many apps are still in support, however, and I know of people who are still using early versions of CCleaner as they just don't like having to update software all the time. Again, this is understandable to a certain extent, and it's great that the Windows Store updates apps silently and automatically in the background.

So in short, I'm not defending Microsoft's practices during this first free upgrade year, as many of the tactics employed to get people to upgrade bordered on underhand trickery. Upgrade failures with Windows 10 are very rarely the fault, or completely the fault though of Microsoft.

This doesn't mean that problems don't occur, and I want to spend some time in this last chapter looking at how these problems can be fixed, and to show you how to nondestructively refresh or reinstall Windows 10 if there isn't an image backup already available on the PC.

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2_31

Troubleshooting the Windows 10 Upgrade

It's common when upgrading a PC to Windows 10, to do this by downloading the Windows 10 Upgrade Tool, which is available to download from `www.microsoft.com/software-download/windows10`. This will allow you to purchase an upgrade license, if necessary, and upgrade in place from Windows 7 or Windows 8.1 to Windows 10.

What happens occasionally is that the upgrade process hangs completely, reporting a "can't install Windows 10" or similar error. By this time, it's already downloaded 3GB of Windows 10 files, and if you try to run the tool again, you're still presented with the same error, as it might not be able to download the files again afresh. There is a simple fix for this, however. This tool creates a `$WINDOWS.~BT` folder and can also create a `$Windows.~WS` folder in the root of your `C:` drive (see Figure 31-1), and it is to this folder that the downloaded files are placed. You may also or instead see a `Windows10 Upgrade` folder. If you are having trouble with the Upgrade Tools, you can delete these folders and begin your download of Windows 10 again.

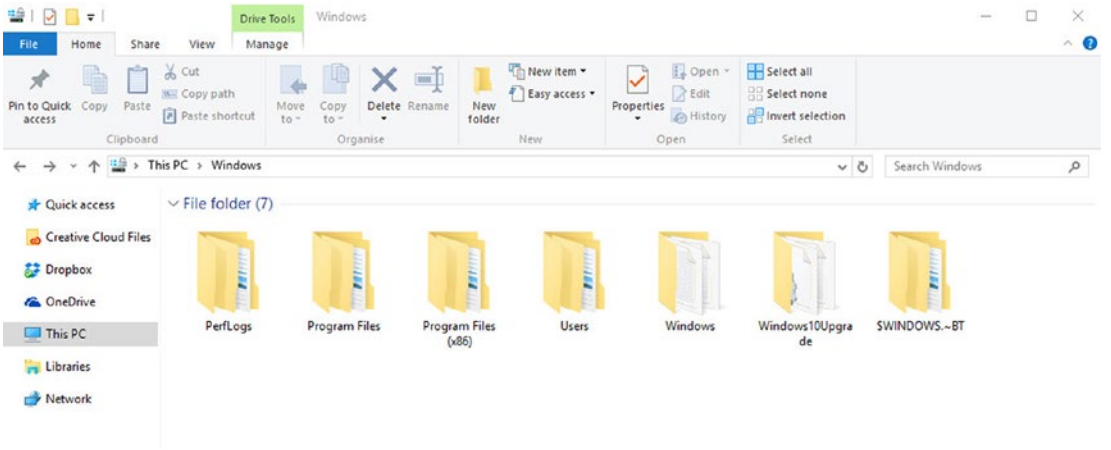


Figure 31-1. *The Windows 10 Upgrade Tool creates a $WINDOWS.~BT folder*

Tip If you are upgrading a PC with only a very small amount of storage, and the Disk Cleanup Wizard is not freeing up enough space for the Windows 10 download, you can use the Upgrade Tool with an external USB Flash Drive, though you may also need an on-the-go (OTG) cable to connect this to the PC. The installation files will be downloaded to this USB drive, but bear in mind that your backup copy

of Windows 7 or Windows 8.1 will also be placed on the USB drive. This means that you should not delete the contents of the Flash Drive until you are absolutely certain that there are no problems with Windows 10 on that device and that you will not need to roll back to your previous OS.

Installing Windows 10

Not everybody wants to upgrade their PC systems to Windows 10, however. Many people, including myself, see the benefits in performing a clean installation of the OS. There's also the plain fact that you might have been using Windows 10 for some years already (the chances of that given that you're reading this book are fairly high), and will need to reinstall it at some point. This might be because you've encountered a massive problem with the OS that can be solved only by a complete reinstall.

Obtaining Up-to-Date Installation Media

One of the problems with every version of Windows is that you would install the OS from your original installation CD or DVD, and then you'd have months, perhaps even years, of updates and patches to install. This could take days, and if you only had a Windows 8 disk, you'd then also had to perform the major upgrade to Windows 8.1. All of this was a real pain.

With Windows 10 ~~being the last major version of the OS~~ (well we thought this would be the case but "Ta Daa," you can look forward to buying my new book *Windows 11 Troubleshooting (Apress 2022)*, Microsoft sought to address this, and at the same time address the fact that so many people never kept or would lose their installation DVD. There's also the fact that if you upgraded in place from Windows 7 or Windows 8.1 during the first year in which Windows 10 was free, you wouldn't get physical installation media anyway.

The Windows 10 Media Creation Tool, available to download from `www.microsoft.com/software-download/windows10`, will let you create a USB Flash Drive or an ISO file that can then be burned to a DVD, from which you can install Windows 10; see Figure 31-2. The best part is that because this tool downloads Windows 10 from Microsoft's servers, it will *always* download the latest build. This means you'll never have more than a few months of Windows updates to install afterward, if at all.

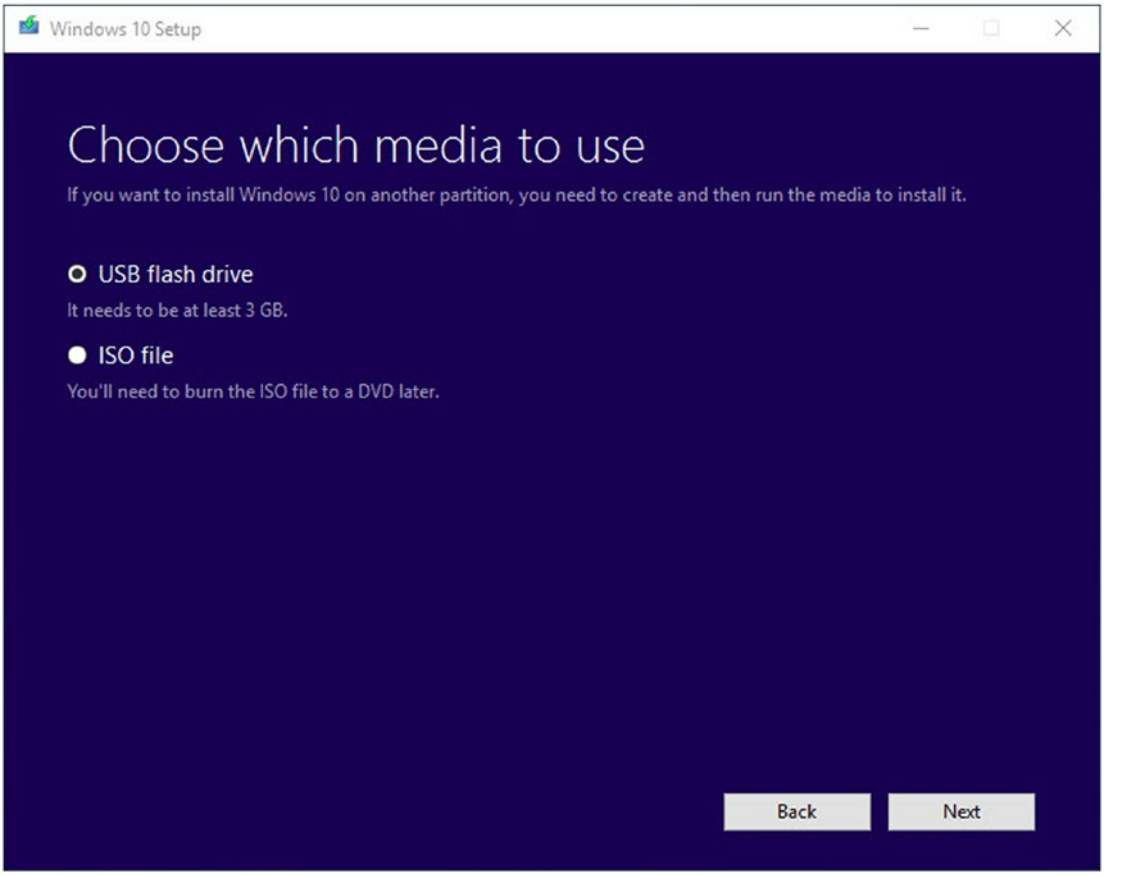


Figure 31-2. *You can create installation media of the latest Windows 10 build at any time*

Note Where does the Windows 10 Media Creation Tool stand with original equipment manufacturer (OEM) versions of Windows 10? With all previous versions of Windows, the product key you had on your PC could be locked to an edition of Windows you bought from a company such as HP, Dell, Lenovo, and so on, and you couldn't install a "regular" copy of Windows with that product key if something went disastrously wrong.

With Windows 10, you will be able to use the Media Creation Tool with **all** Windows 10 installations. This is because Windows 10 installations are product key agnostic. Provided a copy of Windows 10 has been previously activated on that PC, you will always be able to reinstall Windows 10 on the same hardware.

Creating Customized Installation Media

What if you're in a business environment, however, and need a customized version of the Windows 10 installation media? There are many reasons why you might want to do this. At its most basic, you might have bought a job lot of PCs for the business, all with the same hardware, and you want to embed the appropriate hardware drivers, and perhaps a series of core apps, into the Windows installation media, to reduce the overall installation time and Internet bandwidth usage.

You might additionally be on the Enterprise branches for Windows Update, or the Long-Term Servicing Channel, in which you get feature updates months or even years after they're rolled out to all other Windows PCs.

Neither of these scenarios can be used with the Windows 10 Media Creation Tool, which will always include all the latest feature packs rolled into the installer. So what can you do to create custom media?

With Windows 10, Microsoft has actually made it very difficult to create custom installation media, in which you have injected drivers and apps. These are called "slipstreamed" installers. You will either need access to an online portal such as `my.visualstudio.com`, where Microsoft keep downloadable copies of previous ISOs for Windows versions, the Windows 10 Installation and Deployment Toolkit, or will need to follow incredibly complex and difficult instructions using the DISM (Deployment Image Servicing and Management) tool that's built into the OS.

Fortunately, third parties have stepped in with various solutions that allow you to create custom installation media. Here I want to talk about just one, a very powerful tool called NTLite (`www.ntlite.com`). This utility (see Figure 31-3), of which there is a free version, can be used to perform a wide variety of tasks.

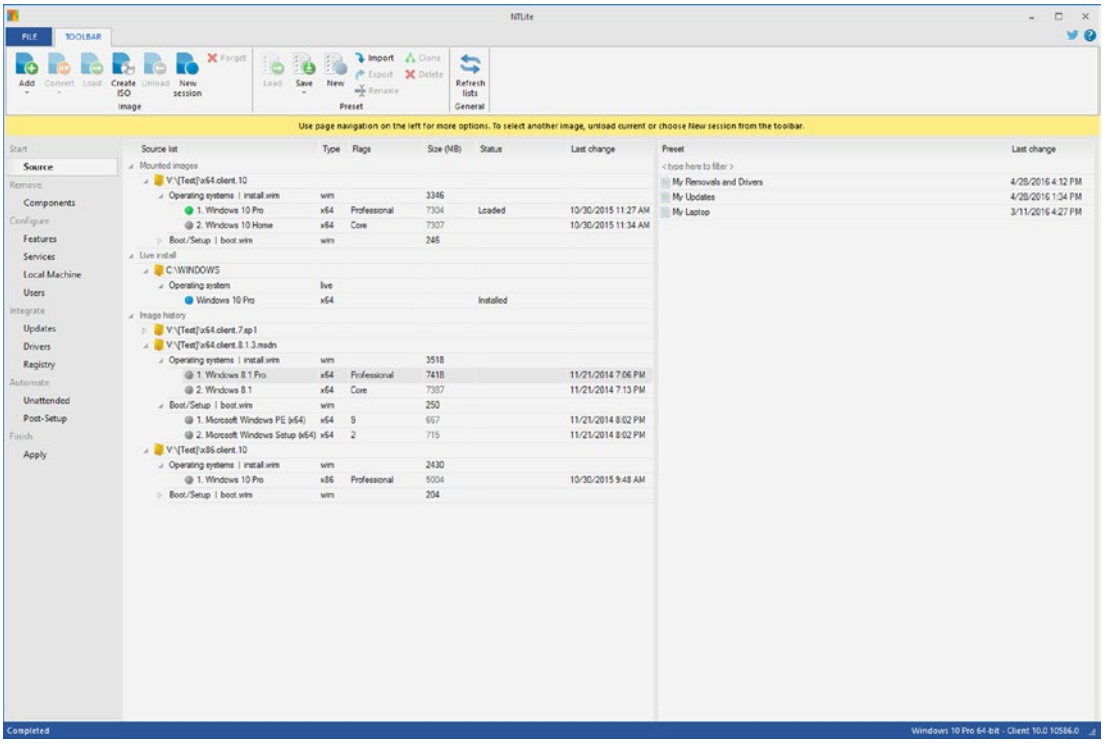


Figure 31-3. *NTLite allows you to easily create slipstreamed media*

NTLite will let you add drivers, Windows updates, language packs, and apps to your installation media. Additionally, however, you can use it to remove specific Windows components, tweak the OS, configure disk partitions in advance of installation (useful if you want to separate files and documents, or have a separate image backup partition), automate the installation process, and more besides.

Nondestructively Reinstalling Windows 10

Let's say then that you've encountered a problem that is so bad you have no choice but to completely reinstall Windows 10 on the PC. The user(s) on the PC, however, will likely have files and documents on the same partition as the corrupt OS installation (if those haven't already been moved to or been stored on a separate partition or hard disk, or are stored in a cloud service such as OneDrive or Azure AD) that will need to be kept. So how do you perform a nondestructive reinstallation of the OS?

It might seem obvious that you can use your installation media to *Upgrade* Windows 10 on the PC. You can do this by starting the Windows 10 installer from the desktop. If you can't get to the desktop, though, you can seem a bit stuck.

Never fear, however, as there is an easy solution. Start your PC from your Windows 10 installation media, be this a USB Flash Drive or DVD, and click *Install* as per normal. When asked if you want to upgrade or perform a custom installation, you won't be allowed to click the *Upgrade* option (this can be selected only by starting the installer from the desktop). Instead, click *Custom: install Windows only (advanced)* option (see Figure 31-4), and when asked on what disk or partition you want to install Windows 10, choose the partition on which it's already installed.

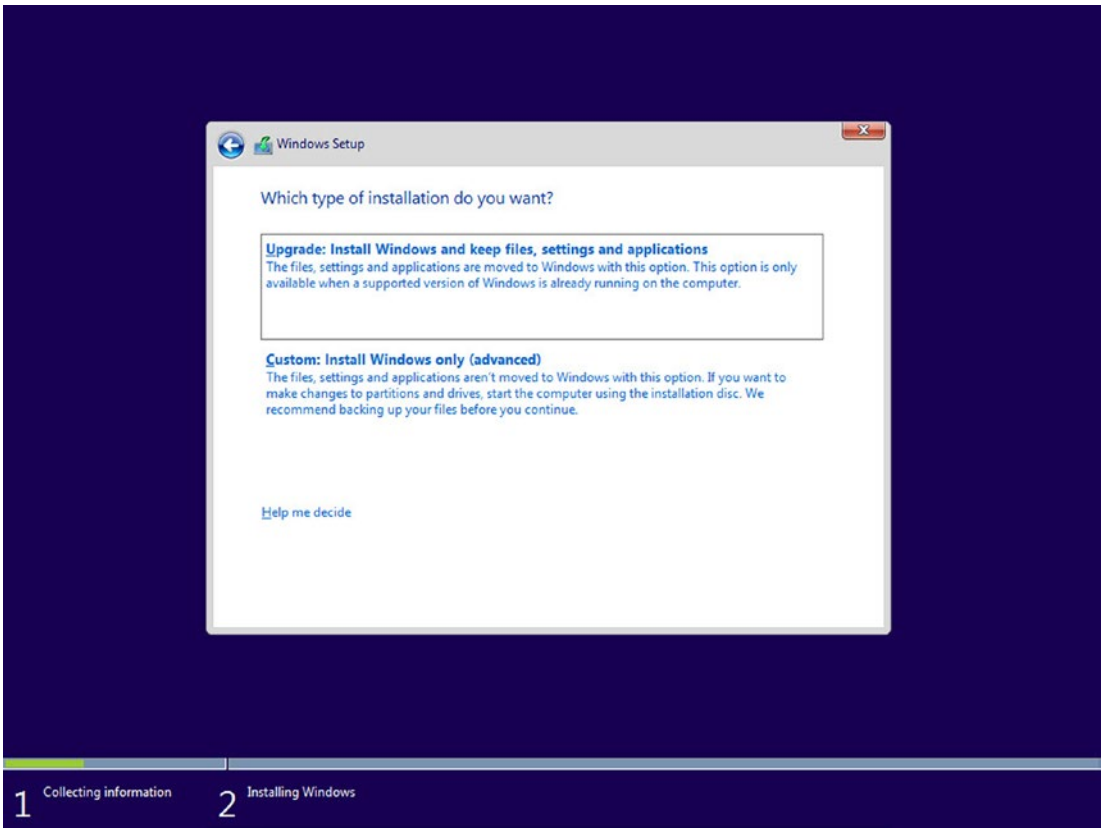


Figure 31-4. *Do not upgrade Windows if you need a nondestructive installation*

The difference now is that, if we were performing a clean installation of the OS, we'd open the disk tools options in the installer and format the partition, or perhaps even delete the partition and create a fresh one. To nondestructively reinstall the OS, though, **do not** format or delete the partition. When you click *Next,* you will then be told that the installer has found a previous copy of Windows, which it will move to a `Windows.old` folder; see Figure 31-5.

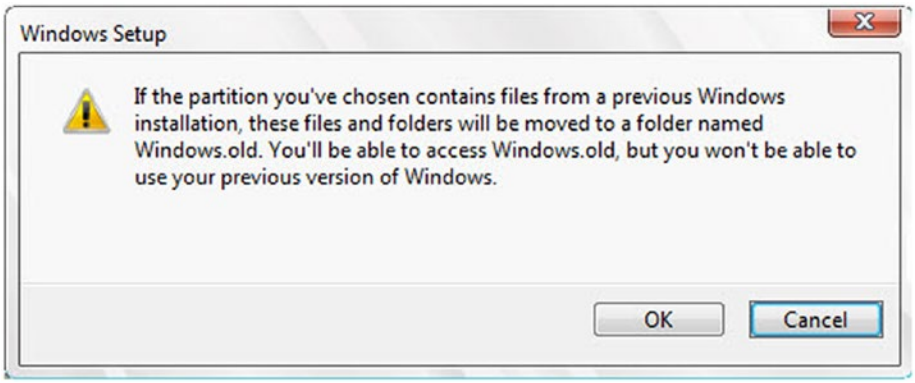


Figure 31-5. *You will be informed that a Windows.old folder will be created*

Once the Windows 10 reinstallation is complete, you will have a fresh install into which you will need to reinstall drivers, apps, updates, and so on, but you will also have this `Windows.old` folder, in which there will be a `Users` folder containing all the files and documents stored on the PC previously, as well as anything else you might have kept there, such as downloaded files, installers, driver backups, and more besides.

Note In addition to the Windows 10 Media Creation Tool, Microsoft has also released a *Windows 10 Refresh Tool*, which can be downloaded from `http://pcs.tv/23dD1AM`. This tool works similarly to the Media Creation Tool, but is intended to help you reinstall Windows 10 nondestructively on PCs where the currently installed version is unrecoverable.

Reset and Fresh Start

Windows 10 also includes two tools (that really are kind of the same thing but are found in completely different places, for some bizarre reason) which can be used to reinstall Windows on a PC. Reset can be found in *Settings* under *Update & Security* and *Recovery*. It will ask if you want to *keep [my] files* or *Remove everything*, with the former being a nondestructive reinstallation of Windows; see Figure 31-6

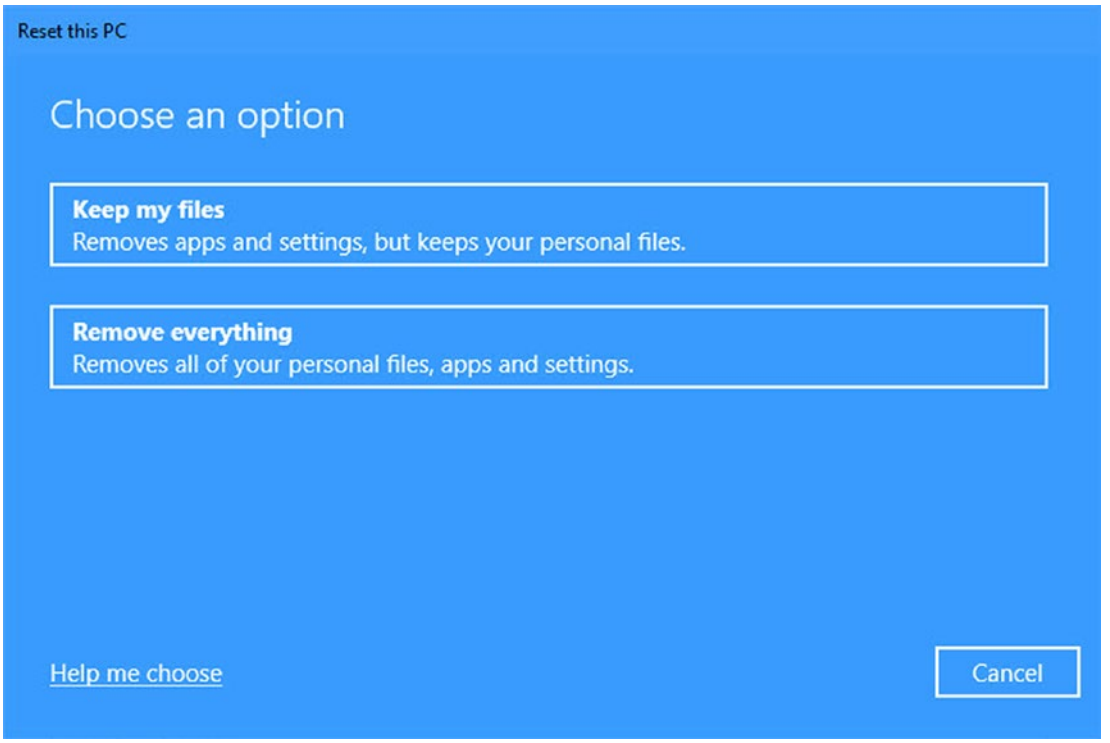


Figure 31-6. *You can Reset your Windows 10 PC*

The other option isn't in Settings at all, but can be found in *Windows Security*; search for this in the Start Menu or click the shield icon in the Taskbar notification center. Navigate to *Drive performance & health*, and you'll find an option called *Fresh Start* which, on the face of it, does exactly the same thing as Reset, in that it will nondestructively reinstall Windows while keeping all your files intact; see Figure 31-7.

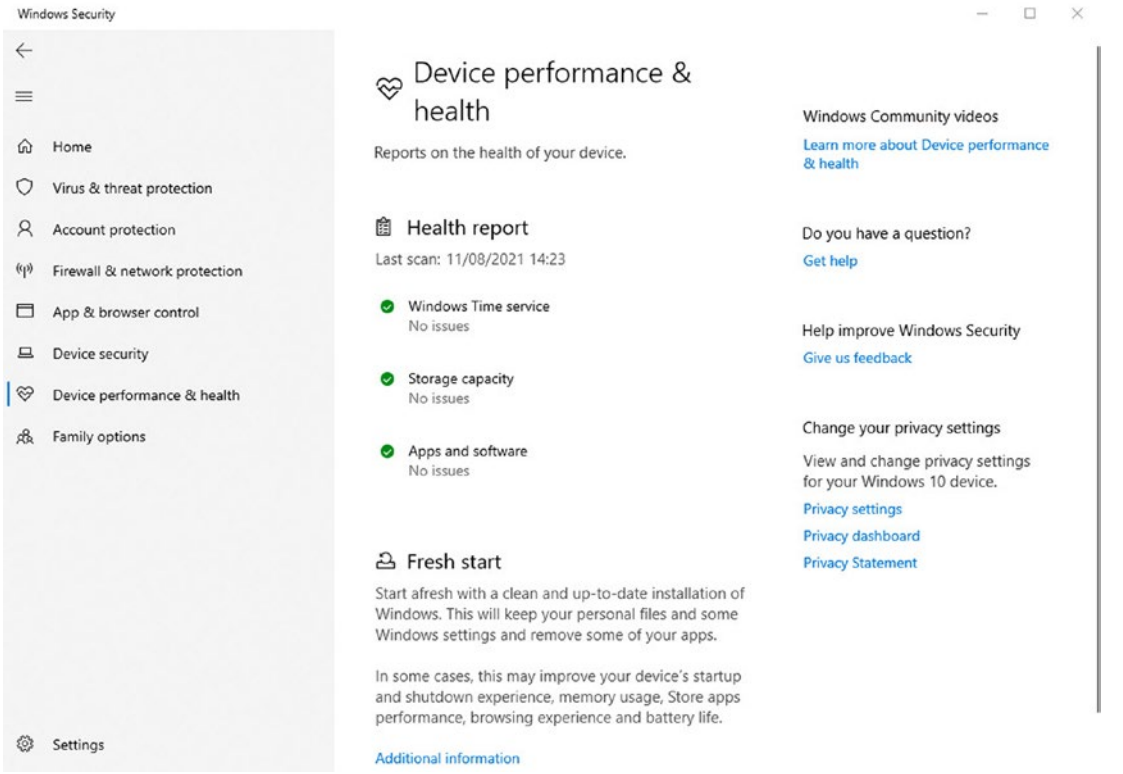


Figure 31-7. *Fresh Start is just like Reset, only completely different*

So what exactly is the difference between Reset and Fresh Start? Actually it's very simple and logical (though why both these options aren't available in the same damn tool astonishes me). Refresh uses the current Windows installation, complete with all updates that are more than 30 days old (to guarantee stability) to reinstall the OS, while the Fresh Start tool will download a new installation ISO from the Microsoft website automatically and reinstall from that instead.

This gives both options one advantage over the other. Reset will be quicker overall, as the install image already resides on your PC, but Fresh Start is most useful in scenarios where you have an underlying problem with the Windows installation itself.

Windows 10 SysPrep

It's worth spending a short time looking at the SysPrep tool in Windows 10, what it is, and how you can use it. When you install Windows 10 on a PC, you will be presented with the Out-of-Box Experience (OOBE). This will ask you for your Microsoft account details, present you with privacy and other options, and install the core Store apps.

SysPrep can be invoked either at the very beginning of the OOBE experience, by pressing *Ctrl+Shift+F3*, or after the OOBE experience from the `C:\Windows\System32\sysprep` folder. Once activated SysPrep will present itself on the desktop; see Figure 31-8. You will now be able to install drivers, make configuration changes, and install apps that will apply to **all** users on the PC. Note that you cannot use SysPrep to make changes on a per-user basis, nor will it allow you to create user accounts.

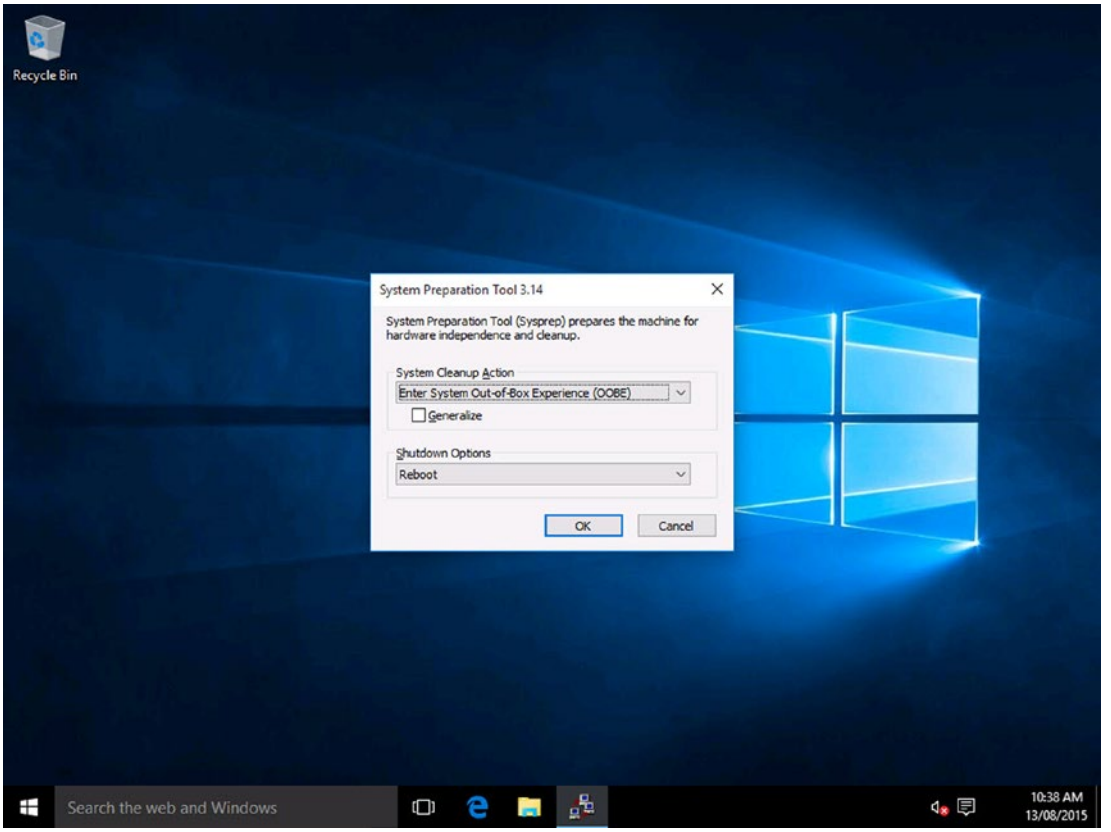


Figure 31-8. *SysPrep allows you to make changes to an OS without changing the OOBE*

It's important to leave the SysPrep window open on the PC when you are configuring Windows 10. Should you have to restart the PC at any time, you will need to invoke SysPrep again if you have not restarted the PC through the SysPrep tool itself. When you're finished, you can use the SysPrep window to shut down the PC. The next time it starts, the user who is receiving the PC will get the full OOBE experience. SysPrep can be a great tool to use then if you are preparing PCs that are purchased by or are to be given as a gift to other people. It can also be used with third-party imaging software, such as Symantec Ghost, for making image backups that can then be rolled out across other machines in a small- to medium-sized business. Note that the Windows Image Backup system won't operate in SysPrep.

Summary

I always like to end on a happy note, and the thought of giving a PC to somebody as a present is a very happy one indeed. You'll probably be asked to support that PC, however, but throughout this book, I have shown you everything you need to know about diagnosing and repairing problems on PCs. More importantly, I've shown you how to mitigate and prevent problems from occurring in the first instance. I sincerely hope you've found this book helpful, educational, informative, and authoritative.

More help is available through other books in this *Windows and Windows Server Troubleshooting Series*, which you can purchase online at `http://pcs.tv/1UADAyk`. These include specialist books dedicated to the Windows Registry, File System, Installation and Updating, Software and Hardware Compatibility, Malware, and Viruses, Networking, and Group Policy, through to advanced server topics including Troubleshooting Windows Using PowerShell, and Troubleshooting BYOD and Mobile Device Management.

By the time you read this book, we will also have seen the launch of Windows 11, and naturally I will be writing a *Windows 11 Troubleshooting* book for Apress to be published in 2022, so be certain to keep an eye out for it as there are a great many changes to the newer version of the operating system.

For now, I'd like to thank you for reading. This book has really been a labor of love. I hope you've got as much from it as I have put into it, and now that you know how to troubleshoot and repair any type of problem on a PC, I sincerely hope you never need to.

Index

A

Access Control List (ACL), 748, 749
AccessEnum, 609
Actions panel, 136
Activation key, 269
Active Directory
    Explorer (ADExplorer), 615
ADInsight, 616
ADRestore, 616
Advanced query syntax (AQS), 86
Advanced Threat Protection (ATP), 520
Adware, 555
Antimalware software, 210, 516, 524
App & Browser Control, 492
Assessment and Deployment
    Toolkit (ADK), 466, 649
Attach Task, 147
Automated Troubleshooters, 127, 128
Automatic teller machines (ATMs), 426
AVG Rootkit Remover, 554
Azure Active Directory (Azure AD), 85
Azure Virtual Desktop, 583

B

Backups, 650, 651
Basic Input, Output System (BIOS),
    157, 159
  reset, 161, 162
BCDEdit
  administrator, 345, 346
  data format, 348, 349
  examples, 349–351
  identifiers, 348
  Win+X menu, 344
Bitlocker, 286, 287
  encryption, 508, 509
  recovery key, 510
Bitlocker To Go, 511, 512
Blue Screens of Death (BSOD), 48, 210,
    255, 290–292, 735, 761
Bluetooth, 177, 178, 265, 266
Bomb proofing, PC
  firewall policy, 599–601, 603
  group policy, lockdown PCs, 588–591
  local security policy, 597–599
  robust backup strategy, 584, 585
  Windows services, 592–597
  work from home, 585–587
Bomb-proof PC system, 604
Boot Configuration Database (BCD), 549
Boot partition, recreating/moving
  command prompt, 337, 338
  create boot files, 341, 342
  disk management console,
    338, 340, 341
  effective repairs, 352–355
  installer, 336
Bring Your Own Device (BYOD), 85, 653

C

Cabling, 9
Category/Views panel, 135

© Mike Halsey 2022
M. Halsey, *Windows 10 Troubleshooting*, https://doi.org/10.1007/978-1-4842-7471-2

Check Disk (ChkDsk) tool, 741
Cloud systems, 523
Command-line tool, 501, 609, 706, 741
Command Prompt, 204, 210, 212, 707–711
Communications device, 267
Community involvement, 640
Compatibility, 124
Compatibility Troubleshooter, 122
Computer Management Console, 675, 676
Controlled Folder Access, 491
Control Panel, 91, 92
  paging file, 94
  remote connections, 94
  virtual memory, 92
Core isolation, 494
Credential Manager, 496
Custom views, 142, 144, 154

D

Debug, 119
Defragmentation, 114
Delivery Optimization, 88
Deployment Image Servicing Management (DISM) tool, 743
Details tab, 669
Device drivers
  backup/restore, 421
  blocking app installation, 411, 413
  configuring driver parameters, 420, 421
  device manager, 397–399
  finding details/information, 414–416
  identifying/installing unknown devices, 400–405, 407
  legacy hardware, 406, 408, 409
  troubleshooting, 417–420, 422
  uninstalling/deleting, 410
Device Encryption, 502–504
  bitlocker, 504
  TPM, 505
  without TPM, 506, 507
Device Management, 397, 660
Diagnostic Mode, 528, 530, 531
Diagnostics and Recovery Toolset (DaRT), 551
Diagnostic tools, 774
Direct Memory Access (DMA), 399
DirectX Diagnostic tool (DXDiag), 678, 679
Disk cleanup, 97
Disk Cleanup Wizard, 105, 106, 109
Disk Management tool, 744
Diskmon, 611
Disk Partition, 743
Distributed Denial-of-Service (DDoS), 159, 519, 638
Domain Name System (DNS), 219, 380, 383
Drive data cables, 200
Dual and multiboot PCs
  bitlocker/dual-boot systems, 344
  definition, 342
  secure boot, 343
DVI cable, 170
Dynamic link libraries (DLLs), 734

E

Ease of Access settings, 86
Edge browser, 109, 110, 245, 521
  IE compatibility mode, 245, 246
  installation, 249, 250
  reset, 247, 248
  settings, 246, 247
Education theory, 639
Electrical equipment, 776

Encrypting File System (EFS), 344, 497–499, 501, 596, 613
Ethernet network, 233
Event information, 149
Event logs, 139
Event occurrence, 151
Event Trace Log (ETL), 735
Event Viewer, 137, 138, 142
Expansion/graphics cards, 169
Exploit protection, 493, 494
Extensible Markup Language (XML), 735
External factors, 773
External/network hardware, 651
External storage, 79

F

Family Safety dashboard, 37, 486, 487
Fast Start-up, 285
File and folder permissions, 745–748
File backup, 66, 68
File Explorer window, 69, 730
  user document, 738
File History, 66–68, 71
File permissions, 262
File store, 261
FileSystemAccessRule command, 718
File type, 257, 258, 736
Flash Drive, 42
Folder and drive sharing, 754, 755
Fragmentation, 114

G

Get-PhysicalDisk commands, 716
Get-Process command, 721
Get-Service command, 721
Get-WinEvent command, 715
Get-WmiObject command, 716
Globally Unique Identifier Partition Table (GPT), 743
Graphics processor (GPU), 669

H

Hard disk, 114, 168
Hardware devices, 173
Hardware drivers, 769
HKEY_CURRENT_CONFIG (HKCC), 686
HKEY_LOCAL_MACHINE (HKLM)
  SAM, 685
  security, 685
  software, 686
  system, 686
HKEY_USERS (HKU), 686
Hyper-V Manager, 561
  networks, 565–567
  PowerShell, 570
  reset network, 572, 573
  VHD, 573–575
    boot menu, 575
    GUID, 577
  VM backups, 568, 569
  VM booting, 571
  Windows 10, 562–564

I

Improper shutdown, 199
Inherited permissions, 750, 751
Input/Output ports (I/O Ports), 399
Internet, 764, 765
  Microsoft Answers site, 767
  Microsoft Docs, 766

Internet Explorer 11 (IE11), 237, 437
caches/database, 242
delete files, 243
disable, 238–240
reset, 243, 244
temporary files, 240, 241
Internet Explorer (IE), 107, 108
clean temporary files, 110
IE11, 109
reset, 111, 112
Internet of Things (IOT), 607
Internet Protocol (IP), 219
Interrupt requests (IRQ), 399, 677, 762
ipconfig command, 389
IT systems, 13

J

Junkware, 555

K

Kaspersky Ransomware Decryptor, 553
Kaspersky Rescue Disk, 553
Keyboards, 170

L

Lightweight Directory Access Protocol (LDAP), 616
LiveKd, 633
LoadOrder utility, 633
Location information, 255, 256
Log file, 203, 205
LogonSessions, 631
Long-Term Servicing Branch, 125
Long-Term Servicing Channel (LTSC), 88, 413, 425, 437

M

Maintaining app/website compatibility
ADK, 466
assistant service, 465
default web browser, 458–461
DPI, 445, 446
IE
IE11 security, 451–453, 455
Microsoft Edge, 450, 456, 458
resetting, 455
Windows 10, 450
internet explorer, 447, 449
Microsoft edge, 449, 450
properties panel, 440
PWAs, 461, 463, 464
3D modeling features, 442
troubleshooter, 441
win32 apps, 438, 442
Windows 10, 443, 444
Windows 365/Windows sandbox, 466, 468
Malware, 516, 638
back doors, 518
bots, 519
forensic, 533
BCD, 549, 550
clean up, 547
color-coded, 539
deactivate, 541–544
identify process, 537
isolate PC, 533
retest PC, 546
rootkit removal, 548, 549
svchost.exe, 540, 541
test results, 544, 545
tools, 538
wi-fi passwords, 534–536

keyloggers, 518
macros, 519
manual, 523
offline virus, 523, 524
PC, 516, 517
portable OS, 532
ransomware, 519
rootkits, 519
third-party tools
D7II, 555
DaRT, 551, 552
ESET online/offline, 552
F-secure online scanner, 554
McAfee, 554
Norton tool, 553
online virus remover, 556
RKill, 555
Sophos tool, 553
trojans, 519
UAC, 519
viruses, 518
Malware attack, 649
Managing privacy
app, 470, 471
children, 483, 484
complex password, 477
create password, 474, 475
password rules, 469, 473, 476, 477
Managing users/BYOD PCs
device management, 646, 647
Group Policy, 647
Master Boot Record (MBR), 743
McAfee tool, 554
Memory, 168
Memory Integrity, 495
Micro SD card, 80
Microsoft 365, 130
Microsoft Answers website, 129, 767
Microsoft Docs, 766
Microsoft Edge, 645
Microsoft Management Console (MMC), 133
Microsoft's Sysinternals suite
files/disk utilities
AccessChk and AccessChk64, 608
AccessEnum, 609
Contig, 609
Disk2Vhd, 610
DiskExt, 610, 611
Diskmon, 611, 612
DiskView, 612
DU, 612
EFSDump, 613
FindLinks, 613
MovieFile/PendMove, 613
NTFSInfo, 614
PsFile, 614
SDelete, 615
ShareEnum, 615
signcheck, 615
network utilities, 615
process utilities
AutoRuns, 622, 623
definition, 622
handle, 624
ListDLLs, 624
Portmon, 625
ProcDump, 625, 626
process explorer, 626–628
process monitor, 629
ShellRunas, 630
VMMap, 630
RegDelNull, 636
registry usage, 636
RegJump, 636
security utilities, 631, 632
system information, 632–634

Minimal boot configuration, 778
mklink command, 739
MKLINK command, 740
Mobile Device Management (MDM), 85, 654
Motherboard, 166
MSOCache, 730
Murphy's law, 295

N

National Health Service (NHS), 522
Network and Sharing Center, 213
  connections, 223
  IPv6 settings, 220
  network adapters, 222, 223
  network connections, 216–218
  network reset, 227, 228
  network services, 221
  router, 228–230
  Wi-fi, 225, 226
  Windows 10, 214, 227
Network-attached storage (NAS), 52, 231, 263, 523, 584, 648, 739
Network bandwidth, 215
Network connection, 215
  checking status
    connection, 361, 362
    control settings, 365
    Etherner, 358
    prioritize Wi-Fi, 368
    properties button, 364
    real time traffic information, 360
    setting panel, 363
    sharing center, 359
    troubleshooting, 358
    Wi-Fi, 365–368
  diagnosing problems
    Event Viewer, 369, 370
    performance monitor, 370, 371
    resource monitor, bandwidth, 371–373
  hosts/LMHOSTS/WINS, 382–385
  Network and Sharing Center
    advanced network configuration options, 378–381
    control panel, 373
    discoverability, 374
    file explorer, 374
    public/private, changing network type, 375–378
  TCP/IP, 385
  user profiles, 393, 394
Networking utilities
  PsTools, 616–620
  TCPView, 620, 621
  WhoIs, 621
Network problems, 213
Network Shell (netsh), 390
Network storage, 52
Nonpresent devices, 399
Norton tool, 553
NTFSInfo, 614

O

Obsessive-compulsive disorder (OCD), 9
OneDrive, 71, 72, 74, 130
OneDrive sync engine, 675
On-the-go (OTG), 44
Original equipment manufacturer (OEM), 784
Out-of-Box Experience (OOBE), 791
Overclocking, 162, 163
Owner group, 752, 753

P

Paging file, 94
Partition information, 717
PC hardware, 5
PC monitors, 288, 289
Peer Name Resolution Protocol (PNRP), 313
Performance Monitor, 671, 672
  Data Collector Set, 673
  Resource Monitor, 674, 675
Permission inheritance, 749
Personal digital assistants (PDA), 470
Ping, 385
Point-of-sale (POS), 409
Power management, 640, 642–644
PowerShell, 712, 713
  disk/file information, 716–718
  event log, 714, 716
  hardware/software information, 719–721
  services, 721
  Windows Update, 722, 723
PowerShell scripting tool, 693, 694
Power supplies, 164
  jump-start, 165
  PC problems, 164, 165
Printers
  individual, 194
  install, 180
  IP address, 185–187
  network, 182, 189
  policies, 192, 193
  queue window, 195, 196
  shared, 190
  types, 180, 181
  web-type, 188
Problem Steps Recorder
  definition, 296
  game bar, 300–303
  pause record/add comment buttons, 296
  quick assist, 303, 304, 306, 307
  screenshots, 298, 299
  stop recording, 297
  technical details, 300
  toolbar, 296
ProcDump, 625
ProgramData, 731
Progressive Web Apps (PWAs), 4, 461
Protocol types, 259
Provisioning package, 658

Q

Quick diagnosis, 199

R

Ransomware, 522, 638, 648
Ransomware protection, 490, 491, 520
Read-Only Memory (ROM), 157
Rear panel sockets, 167
Recovery Console, 694, 695, 707
Recovery Drive, 42, 44
Recovery Options menu, 207, 208
  antimalware, 210
  automatic restart, 210
  boot logging, 209
  Command Prompt, 208
  debug, 209
  low-resolution video, 210
  safe mode, 210
  startup settings, 209
  System Restore, 208
  UEFI, 208

reg.exe command, 692
REG file, 682
Registry backup, 690
  create, 690–692
Registry corruption, 269
Registry databases, 695–697
Registry Editor, 531, 532, 684, 688, 689
  connect to PC, 697, 698
  HKCR, 685
  HKCU, 685
  HKLM, 685
  remote PC, 698–701
  third-party utilities, 701
Registry files, 681–683
Registry keys, 688
Registry Value Types, 687
RegJump, 636
Remote Desktop Services (RDS), 585
Repairing hardware, 776
Repairing windows startup
  BIOS startup files, 332, 333
  BIOS/UEFI, 335
  command prompt, 332
  UEFI startup files, 333–335
  USB flash drive, 331
Repair method, 199
Reputation-based protection, 493
Resource Monitor, 216
RKill, 555

S

Safe Mode, 525, 526
SDelete, 615
Secure Boot, 343, 520
Secure Virtual Machine (SVM), 560
Security Accounts Manager (SAM), 685
Security and Maintenance Center, 13–15
  automatic maintenance, 19
  feedback and privacy, 20
  View reliability history, 16–18
Security permissions, 265
Security systems
  App and Browser Control, 26–28
  defender antimalware, 21–23
  device security, 30, 31
  firewall, 23, 24, 26
  UAC, 28, 29
Semi-Annual Channel (SAC), 88, 425
Serial/Parallel printer, 183
Set affinity, 118
Set priority, 118
Settings panel, 77
  accounts, 84
  activation, 91
  add/remove printer, 78
  apps, 84
  backup, 90
  default app, 80, 81
  developers, 91
  devices
    AutoPlay, 83
    printers/scanners, 83
  gaming, 85
  information about PC, 82
  network/internet, 84
  personalization, 84
  phone app, 83
  privacy, 86
  recovery, 90
  search, 86
  storage, 79
  time/language, 85
  troubleshooters, 90
  VPN, 84
  Windows Security, 90

ShareEnum, 615
ShellRunas, 630
Shell User Folders, 96, 97, 736, 737
Sign-in methods, 33
  password manager, 36, 37
Sleeping tabs, 645
Small-form-factor (SFF), 164
Software Development kit (SDK), 735, 761
Solid State Drive (SSD), 92, 157
Sophos tool, 553
Startup apps, 101, 275
  power settings, 283
  sleep/resume, 280, 282
  sleep state, 284, 285
  Task Manager, 276
  Windows 10 hangs, 277
  Windows 10 shuts, 278
Startup Repair system, 201
Store apps, 668
Support app, 768
Surface-mount technology, 166
Symbolic link, 739, 740
Sysinternals tools, 555
Sysmon, 632
SysPrep tool, 791, 792
System File Checker (SFC), 125, 126, 742
System Image Backup
  configure, 62, 63
  create, 50–52, 54
  installation media, 63
  restore, 55–57
  UAC, 58–60
System Image Backup restore method, 433
System Information panel, 677
System Recovery menu, 201
System Volume Information, 731

T

Task Manager, 116, 121, 665–667, 670
TCP/IP connections
  ipconfig, 389, 390
  netsh, 390–392
  ping, 385
  TraceRT, 388
temporary file storage, 735
Third-party hardware drivers, 423
Third-Party Support Sites, 768
Third-Party Support Tools, 769
Thunderbolt devices, 288
Touchscreen laptop device, 287
Trace Route (TraceRT), 388
Troubleshooting, 771
3D features, 121
Trusted Platform Module (TPM), 481–483
Twitter hashtags, 8
Two-Factor Authentication (TFA), 471, 472, 478, 479

U

UEFI system, 45
Unified Extensible Firmware Interface (UEFI), 157
  reset, 161, 162
Uninterruptible Power Supplies (UPS), 200
Universal Disk Format (UDF), 744
Universal Plug and Play (UPnP) devices, 399
Universal Serial Bus (USB), 173
  Windows 10, 175
  work reliably, 174
Universal Web Apps (UWP), 247
Upgrade Tool, 782

USB cables, 167
USB Flash Drive, 43, 48, 64, 65, 260, 289, 658
USB Type-C, 288
User Account Control (UAC), 11, 28, 58, 119, 159, 248, 489, 515
User Account Folders, 734
User account management, 31
  administrators *vs.* standard users, 32
  local accounts *vs.* Microsoft accounts, 32, 33
User accounts, 38, 39
User group, 751, 752
User interface (UI), 424

V

Versioning, 523
VGA cable, 170
Virtual hard disk (VHD), 563
Virtualization, 559
Virtual Machines (VMs), 135, 561
Virtual memory, 93
Virtual Private Network (VPN), 601, 654
  settings panel, 655
  set up, 656
Vista and integrated antivirus (AV), 489

W, X, Y, Z

WhoIs, 621
Wi-Fi dongles, 174
Wi-Fi passwords, 233, 234
Wi-Fi signal, 231, 232
Win32 apps
  compatibility setting, 438
  definition, 438
  properties panel, 438, 439
win32 desktop apps, 731
Windows 10, 8, 270
  backup, 45
  charging cables, 10
  hardware problem, 9
  networking problems, 11
  nonbootable PC, 48
  OS installation, 12
  reset, 45, 46
  software/app problems, 10
  startup problems, 12
Windows 10, install
  customized media, 785, 786
  media, 783, 784
Windows 10, reinstall, 786, 787
  nondestructive installation, 787, 788
  reset/fresh start, 789, 790
Windows 365 service, 579, 580
Windows Advanced Firewall, 319, 520
Windows\Debug log files
  .dmp files, 761, 762
  text files, 758
  .xml/.etl files, 759–761
Windows Defender, 520
Windows Driver Kit (WDK), 625, 735, 761
Windows Event Collector (wecsvc), 145
Windows Event Viewer, 133
Windows Firewall, 520
Windows Hello, 481
Windows Image Acquisition (WIA), 597
Windows licensing, 269
Windows Media Center, 270
Windows Operating System Folders, 731, 732
Windows partition, 99
Windows Recovery Environment, 706
Windows remote assistance
  advanced options, 309

desktop feature, 321, 322, 324–328
Microsoft Account, 307
PC, 308
sending/responding, 309–318
third-party remote support apps, 307, 329
usolicited offers, sending, 318, 319, 321
Windows Remote Management (winRM), 145
Windows Sandbox, 578
Windows Security Center, 489, 490
Windows Server system, 13
Windows Side-by-Side (WinSxS), 762
Windows SmartScreen, 26, 520
Windows Software Development kit (SDK), 625
Windows Store app, 112
Windows Store Service (WSService), 597
Windows Subsystem for Linux (WSL), 705, 706
Windows Terminal, 723, 724, 726
Windows To Go (WTG), 352
Windows update, 87, 271, 272
log, 735
Microsoft, 424
power loss, 273
reset image, 433–435
search engine, 274
technology, 424
troubleshooting/repairing, 431–433
uninstalling/blocking, 429, 430
updates delivered, 427–429
Windows 10
definition, 425
LTSC, 426
SAC, 425, 426
Windows Virtual Desktop (WVD), 4
Windows Virus & Threat Protection, 520
Windows Vista system, 5
Work Folders, 662, 663
Workplace Join, 657, 658
Device Management, 660
exchange account, 660, 661
Microsoft 365/Microsoft Azure, 661, 662
Provisioning package, 658, 659
WSReset app, 114
wushowhide.diagcab, 430