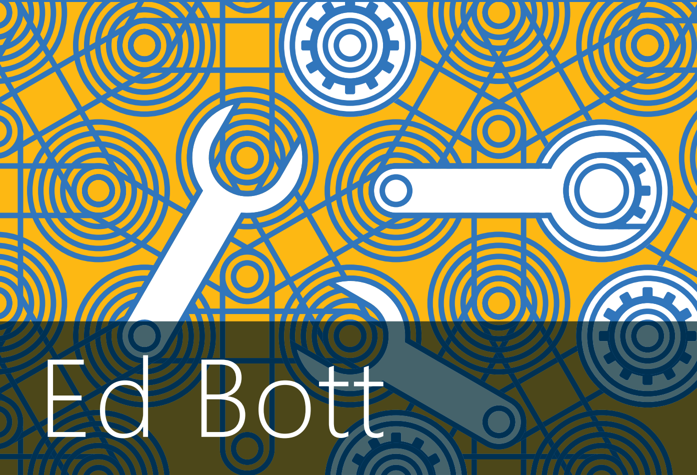
WINDOWS 10
IT PRO ESSENTIALS

Microsoft

Top 10 Tools



Ed Bott

PUBLISHED BY
Microsoft Press
A division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

ISBN: 978-1-5093-0278-9

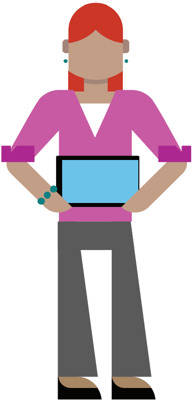
First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Support at mspinput@microsoft.com. Please tell us what you think of this book at http://aka.ms/tellpress.

This book is provided "as-is" and expresses the author's views and opinions. The views, opinions and information expressed in this book, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

Acquisitions Editor: Rosemary Caperton
Developmental Editor Rosemary Caperton
Editorial Production: Dianne Russell, Octal Publishing, Inc.
Copyeditor: Bob Russell, Octal Publishing, Inc.
Cover: Twist Creative • Seattle



Contents

Introduction

This book is about unsung heroes.

Over a quarter-century of talking to people about Microsoft Windows, I've learned that the greatest gains in productivity come from mastering the fundamentals. In many cases, that means learning about the capabilities of tools that you might have taken for granted.

After all those years, I'm still discovering new things about these unsung heroes, including tools and apps I use every day. Some of these tools have been part of Windows for decades, and yet most of us IT pros and expert Windows users tap only a fraction of their power.

As I've learned from watching Windows evolve over the past few years (and from digging into countless Windows 10 Insider Preview builds and sharing discoveries with colleagues and readers), many of those old, familiar programs are still evolving. With each new major release, I've found tiny but meaningful improvements in unexpected places.

Sharing that hard-won knowledge with you is one of two fundamental goals I set out to achieve in this book. My other goal is convincing you to take a closer look at how you use Windows. That means digging a little deeper into programs you probably use every day—File Explorer and Task Manager, for example. If I can help you replace old habits with faster and smarter ways to get things done, I've done my job.

I'm especially grateful to the developers and designers at Microsoft who are building Windows 10, for giving me a mountain of interesting material to work with. And I'd like to thank Microsoft Press, which gave me complete editorial independence for this project. Every word in this book comes from my personal experience. I am confident you'll find a few surprises here.

I encourage you to share your feedback about this book directly with me. Email your comments to me at feedback@realworldwindows.com.

Ed Bott
April 19, 2016

Acknowledgments

I'd like to thank the good folks at Microsoft Press—Anne Hamilton, Rob Linsky, and Rosemary Caperton—for their efforts at making this project happen. And a special thanks to Bob and Dianne Russell of Octal Publishing, who helped turn around this project and create the great-looking ebook you're reading right now.

Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

http://aka.ms/mspressfree

Check back often to see what is new!

Errata, updates, & book support

We’ve made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

http://aka.ms/Win10Tools/errata

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at mspinput@microsoft.com.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to http://support.microsoft.com.

We want to hear from you

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

http://aka.ms/tellpress

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

Stay in touch

Let’s keep the conversation going! We’re on Twitter: http://twitter.com/MicrosoftPress.

CHAPTER 1

Power tools for IT pros

I have a confession to make. The title of this book isn't, strictly speaking, accurate. It actually contains descriptions and hands-on advice for more than 10 apps, accessories, and utilities—many more, in fact.

I began with a list of several hundred software tools and accessories, all built by Microsoft and compatible with Microsoft Windows 10. Eventually, I narrowed the list to my top 10, giving each of the finalists its own turn in the spotlight in the remaining chapters of this book. But that winnowing process wasn't easy.

The sheer volume of Windows programs and accessories, including utilities such as Sysinternals Suite, says a lot about the power and complexity of Windows—a fact that every IT pro knows from firsthand experience. There’s a tool for nearly every task, and a large part of the process of becoming a Windows expert is knowing how to find the appropriate one when you need it.

This chapter provides an overview of many of the apps and accessories that are included in the box with Windows 10, along with a brief explanation of how and why I picked the top 10. It’s also an opportunity to highlight a few of my favorites that I couldn’t include elsewhere.

And, of course, it’s an opportunity for me to share some hard-won knowledge with my fellow IT pros, helping you to figure out the best way to make Windows 10 work for you. There’s rarely a right or wrong way to accomplish a particular goal, but there’s often a faster, smarter way, which is what I look for.

Some of these tools are for everybody—end users and experts alike—whereas some are strictly for professionals. A few are so specialized that you’ll only need them once in a blue moon.

Collectively, though, they make up a toolbox that can save you (and your company) time and money.

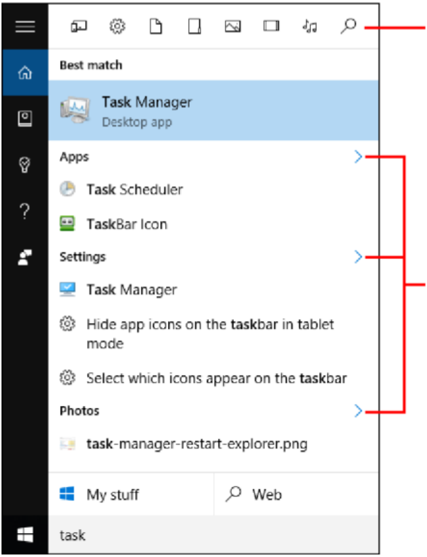
Finding the right tool for the job

Sometimes, accomplishing a task requires nothing more than adjusting a Windows setting by selecting a check box or moving a slider to the right position. Other times, you might need a stand-alone program.

Occasionally, those two options are related. The Settings app and classic Control Panel are filled with buttons and links that do nothing more than launch executable files, typically from the Windows\System32 folder on the system drive.

You could, for example, run the Color Management Control Panel tool (Colorcpl.exe) directly from that location, but experienced Windows users are more accustomed to opening Control Panel and navigating through Hardware And Sound to Display.

In Windows 10, it's even easier to just search for the setting or program you need. You can find nearly anything you want by using the search box on the Windows 10 taskbar, located to the right of the Start button. Because settings and built-in tools are indexed by keyword, you don’t need to know the exact name to find what you're looking for. Figure 1-1, for example, shows the results when I searched for the term “task,” all neatly categorized.

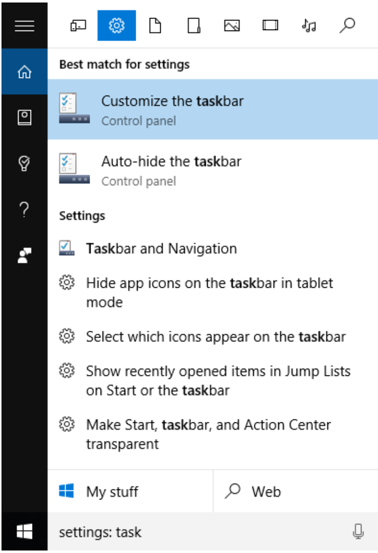

Best match
Task Manager
Desktop app
Apps
Task Scheduler
TaskBar Icon
Settings
Task Manager
Hide app icons on the taskbar in tablet mode
Select which icons appear on the taskbar
Photos
task-manager-restart-explorer.png
My stuff
Web
task

Refine search by choosing a category

Show more results from the current category

Figure 1-1: Most of the time, just searching for a related term is enough to find what you’re looking for.

With the help of a few subtle controls on those raw search results, you can filter your search to refine the list, eliminate the noise, and show more of the type of results you’re looking for. The controls on the search results list are so subtle that you might not even notice them. Click the arrow to the right of a heading (Apps or Settings, in Figure 1-1, for example) to show only results from that category. Or, click one of the icons at the top of the results list to show a group of categories that you can use to refine your search, as I’ve done in Figure 1-2.



Best match for settings

Customize the **task**bar
Control panel

Auto-hide the **task**bar
Control panel

Settings

Taskbar and Navigation

Hide app icons on the **task**bar in tablet mode

Select which icons appear on the **task**bar

Show recently opened items in Jump Lists on Start or the **task**bar

Make Start, **task**bar, and Action Center transparent

settings: task

Figure 1-2: Tap an icon at the top of the search results to refine your search. In this case, I've asked for just results in the Settings category.

By the way, Figure 1-2 also reveals a shortcut that is especially useful if you prefer using the keyboard rather than the mouse. Instead of using the hidden menu at the top to refine by categories, just type one of the text operators—**apps**, **settings**, or **files**, for example—followed by a colon and then the search term.

Here’s one final secret in this section: Get in the habit of using the Quick Links menu, which is available by right-clicking Start or by using the keyboard shortcut Windows logo key+X. Figure 1-3 shows that this menu contains several of the tools I feature in this book as well as the ability to quickly open a Command Prompt window with administrative rights. For Windows experts, it offers instant access to programs that you will use regularly.

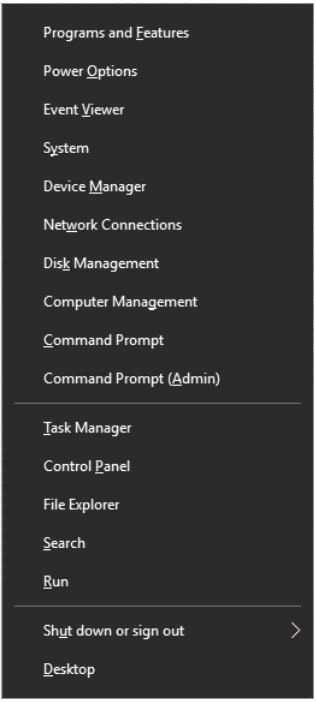


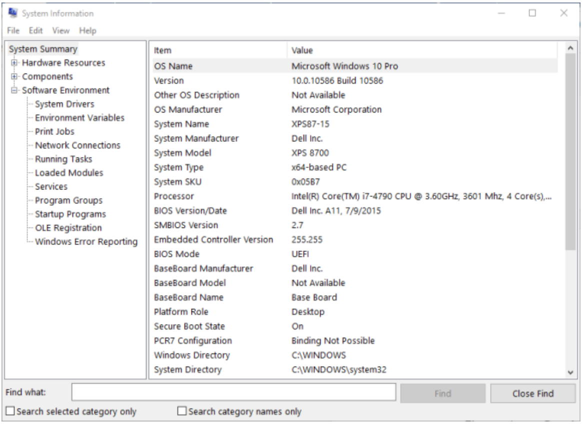
Figure 1-3: Every would-be Windows expert should memorize the keyboard shortcut Windows logo key+X, which opens the incredibly useful Quick Links menu shown here.

Everyday tasks and information

This book includes full chapters on File Explorer (a tool you probably use many times a day) and Event Viewer (which performs tasks on your behalf all day, even though most people rarely open it).

Elsewhere in Windows 10, you'll find simple dashboards that can provide information about the current configuration. For example, in the Search box, type **About** and then, from the results that appear, click About Your PC to see details such as the name of the PC on which you're running the command, the current Windows version, the system type (64-bit or 32-bit), the processor, and the amount of RAM that's installed on your device. Click System from the same results list to see some of the same details in classic Control Panel.

One related tool that deserves a quick shout-out is the System Information accessory, MsInfo32.exe. (Yes, that's the correct executable name, even if you're running a 64-bit Windows version.) Figure 1-4 shows the main page, which contains a wealth of information about the current system. One of the most important details it offers is one that you can’t easily find elsewhere: the current version of the system BIOS or UEFI firmware.



Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.10586 Build 10586
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	XPS87-15
System Manufacturer	Dell Inc.
System Model	XPS 8700
System Type	x64-based PC
System SKU	0x05B7
Processor	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz, 3601 Mhz, 4 Core(s),...
BIOS Version/Date	Dell Inc. A11, 7/9/2015
SMBIOS Version	2.7
Embedded Controller Version	255.255
BIOS Mode	UEFI
BaseBoard Manufacturer	Dell Inc.
BaseBoard Model	Not Available
BaseBoard Name	Base Board
Platform Role	Desktop
Secure Boot State	On
PCR7 Configuration	Binding Not Possible
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32

Figure 1-4: To open System Information, use the command Msinfo32. One normally hard-to-find detail it offers is the current BIOS (or UEFI firmware) version.

Tweaking Windows 10

Hundreds, perhaps even thousands, of customization and personalization options are available directly within Windows 10: the picture on your lock screen, your current time zone, and

User Account Control settings are just a few examples.

Over the past few years, Microsoft has been slowly but steadily migrating these options from the classic Control Panel to the new Settings app. The result of this work-in-progress is that you can find the check box or option you’re looking for in either place.

Both the Settings app and classic Control Panel have search boxes. But here’s a secret most people don’t know: the search box in the Settings app also returns results from Control Panel.

So, if you’re looking for a specific setting, try opening the Settings app; using the shortcut Windows logo key+I (that’s a capital “eye”) is the fastest way. In the search box, type your keyword (see Figure 1-5) to see a list of matching results. Options from the Settings app appear at the top of the list; options for Control Panel settings appear below those for the Settings app and are easily identified by the colorful icons.

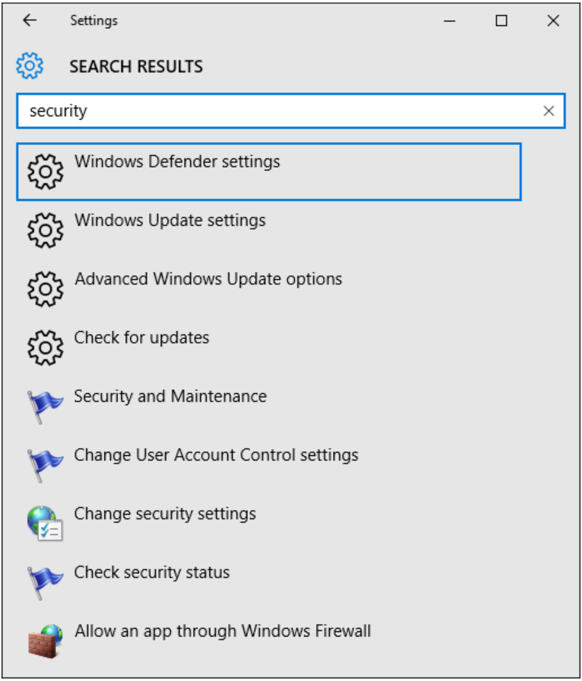
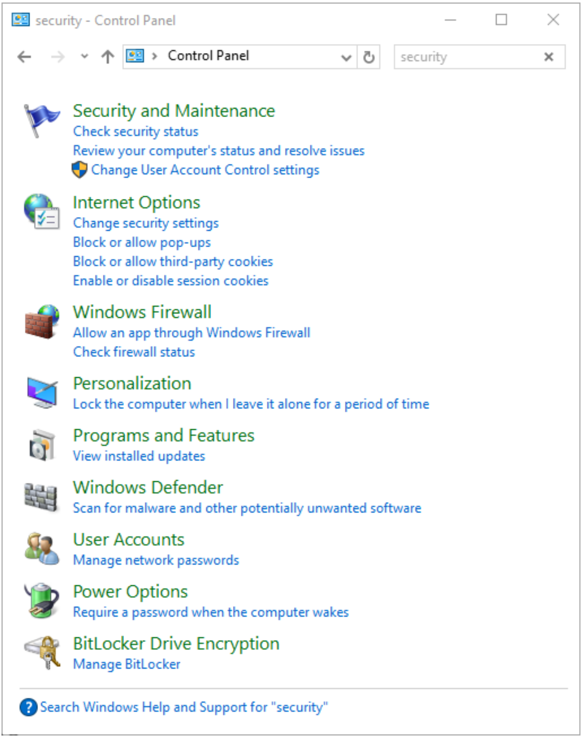


Figure 1-5: When you type a keyword in the search box at the top of the modern Settings app, the results include options from both Settings and classic Control Panel.

Note that the reverse is not true. If you open Control Panel and search for a term, your search returns results only for items that are in Control

Panel. You won’t see any options that have been migrated to the newer Settings app. Figure 1-6 shows the results using the same search term as in the previous figure, but from within Control Panel.



Security and Maintenance
Check security status
Review your computer's status and resolve issues
Change User Account Control settings

Internet Options
Change security settings
Block or allow pop-ups
Block or allow third-party cookies
Enable or disable session cookies

Windows Firewall
Allow an app through Windows Firewall
Check firewall status

Personalization
Lock the computer when I leave it alone for a period of time

Programs and Features
View installed updates

Windows Defender
Scan for malware and other potentially unwanted software

User Accounts
Manage network passwords

Power Options
Require a password when the computer wakes

BitLocker Drive Encryption
Manage BitLocker

Search Windows Help and Support for "security"

Figure 1-6: Searching for a keyword in Control Panel returns only results from Control Panel. Options that have migrated to the newer Settings app aren’t included.

Most of the tweaks you’ll make using any of these “official” options are likely to be saved in the Windows registry. For deployment purposes or to make tweaks that aren’t readily available in the Settings app and Control panel, you’ll most likely use Registry Editor (which I cover in detail in Chapter 3) or Windows PowerShell (Chapter 9). Organizations also have the option to tweak computer and user settings by using Group Policy, which I discuss later in this chapter.

Performance and troubleshooting tools

By far the largest group of Windows tools and accessories is intended to provide information about system performance as well as diagnostic tools that can help you to identify the cause of reliability problems. In this book, I include separate chapters for four professional-strength tools that fall into the following categories:

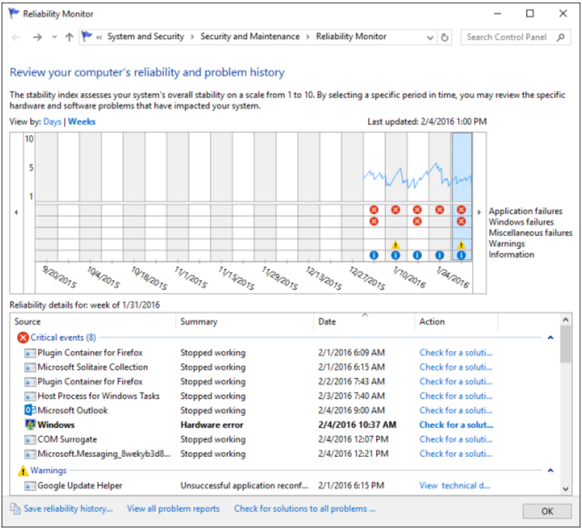
- **Event Viewer (Chapter 4)** There’s a log for nearly everything in Windows, which makes

Event Viewer indispensable and potentially overwhelming. I have some suggestions to zero-in on the exact information you need to solve a problem.

- **Task Manager and Resource Monitor (Chapter 5)** Anyone moving to Windows 10 from Windows 7 should be pleasantly surprised by the improvements in Task Manager. This chapter also includes details about Resource Monitor, a separate accessory that you can access on the **Performance** tab in Task Manager.
- **Sysinternals Suite (Chapter 7)** This amazing and powerful collection of utilities (nearly 80 in all) is regularly updated and available for you to download for free. My discussion includes three absolute essentials.
- **Diagnostic and Recovery Toolset (Chapter 8)** Among the top 10, this choice is unique in that it's not available to every Windows 10 user. But if your organization has a Volume Licensing contract with Software Assurance, or if you have access to a Visual Studio subscription, this collection of tools is a must-have troubleshooting resource.

A few other useful tools didn't make the cut but are worth a mention here.

You can think of Reliability Monitor, for example, as a highly filtered version of Event Viewer. It lists successful and failed software and driver installations as well as crashes, apps, and programs that stopped responding, and other errors, on a time-based scale. It can often provide important clues about the cause of sudden changes in system behavior. Figure 1-7 shows a typical display, with events presented in a weekly rather than daily view.



Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system.

View by: Days | **Weeks**

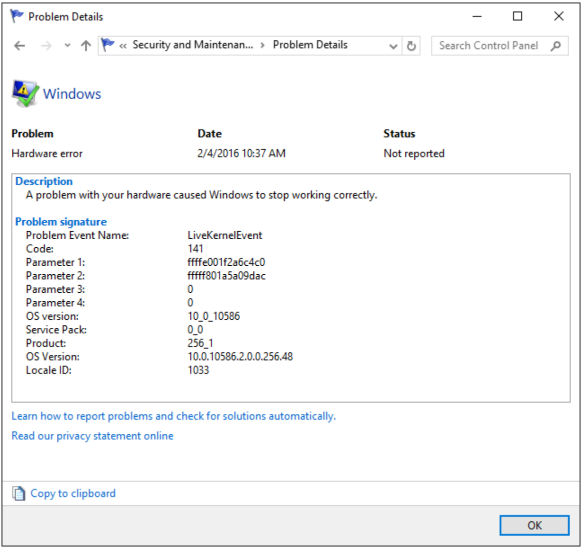
Last updated: 2/4/2016 1:00 PM

Reliability details for: week of 1/31/2016

Source	Summary	Date	Action
Critical events (8)			
Plugin Container for Firefox	Stopped working	2/1/2016 6:09 AM	Check for a soluti...
Microsoft Solitaire Collection	Stopped working	2/1/2016 6:15 AM	Check for a soluti...
Plugin Container for Firefox	Stopped working	2/2/2016 7:43 AM	Check for a soluti...
Host Process for Windows Tasks	Stopped working	2/3/2016 7:40 AM	Check for a soluti...
Microsoft Outlook	Stopped working	2/4/2016 9:00 AM	Check for a soluti...
Windows	**Hardware error**	**2/4/2016 10:37 AM**	**Check for a solut...**
COM Surrogate	Stopped working	2/4/2016 12:07 PM	Check for a soluti...
Microsoft.Messaging_8wekyb3d8...	Stopped working	2/4/2016 12:21 PM	Check for a soluti...
Warnings			
Google Update Helper	Unsuccessful application reconf...	2/1/2016 6:15 PM	View technical d...

Figure 1-7: Reliability Monitor can help pinpoint clusters of events that might provide clues to the cause of a sudden change in performance or an outbreak of crashes and nonresponsive apps.

Although it’s not immediately obvious, double-clicking any event listed at the bottom of Reliability Monitor opens a more detailed display of information, such as that shown in Figure 1-8. You can use error messages, codes, and other details to search for more information about the issue.



Problem	Date	Status
Hardware error	2/4/2016 10:37 AM	Not reported

Description

A problem with your hardware caused Windows to stop working correctly.

Problem signature

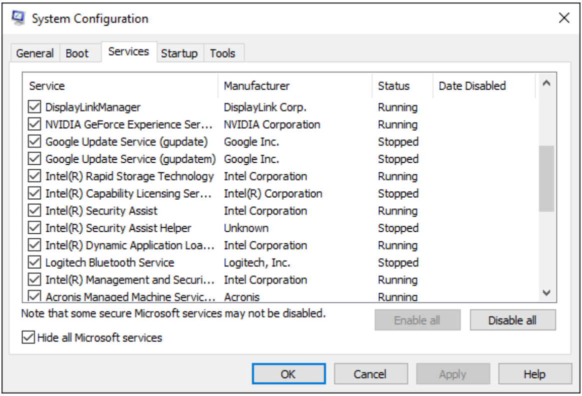
Problem Event Name:	LiveKernelEvent
Code:	141
Parameter 1:	ffffe001f2a6c4c0
Parameter 2:	fffff801a5a09dac
Parameter 3:	0
Parameter 4:	0
OS version:	10_0_10586
Service Pack:	0_0
Product:	256_1
OS Version:	10.0.10586.2.0.0.256.48
Locale ID:	1033

Learn how to report problems and check for solutions automatically.

Read our privacy statement online

Figure 1-8: Double-clicking an event in Reliability Monitor provides important clues that you can use when troubleshooting problems and performance issues.

Another tool that should be familiar to longtime Windows users, especially if you have had to troubleshoot problems with a user's PC, is System Configuration (MSConfig.exe). One especially useful capability is on the Services tab, shown in Figure 1-9, with which you can disable third-party services, either one at a time or in batches, and then restart to narrow-down the cause of a problem.



Service	Manufacturer	Status	Date Disabled
☑ DisplayLinkManager	DisplayLink Corp.	Running	
☑ NVIDIA GeForce Experience Ser…	NVIDIA Corporation	Running	
☑ Google Update Service (gupdate)	Google Inc.	Stopped	
☑ Google Update Service (gupdatem)	Google Inc.	Stopped	
☑ Intel(R) Rapid Storage Technology	Intel Corporation	Running	
☑ Intel(R) Capability Licensing Ser…	Intel(R) Corporation	Stopped	
☑ Intel(R) Security Assist	Intel Corporation	Running	
☑ Intel(R) Security Assist Helper	Unknown	Stopped	
☑ Intel(R) Dynamic Application Loa…	Intel Corporation	Running	
☑ Logitech Bluetooth Service	Logitech, Inc.	Stopped	
☑ Intel(R) Management and Securi…	Intel Corporation	Running	
☑ Acronis Managed Machine Servic…	Acronis	Running	

Note that some secure Microsoft services may not be disabled.

☑ Hide all Microsoft services

Figure 1-9: You can use the venerable System Configuration tool (also known as MSConfig) for basic troubleshooting tasks such as temporarily disabling services to narrow down the possible cause of a problem.

Here’s a power tip for using System Configuration: At the bottom of the Services tab, select the Hide All Microsoft Services check box, and then click Disable All and restart. If the problem no longer occurs, you’ve narrowed-down the cause to a third-party service.

Finally, there’s the Powercfg command, an odd beast that is extremely useful for isolating the cause of an overactive portable PC that isn’t getting the battery life you expect. Used with the /energy switch, it generates a profile of system activity over a period of 60 seconds and saves it as an HTML page in the current directory.

The versatile Microsoft Management Console

By itself, the Microsoft Management Console (MMC) is hopelessly boring and literally good for only one task, which is adding one or more snap-ins that provide in-depth management capabilities for a specific function or feature. You can save these as Microsoft Common Console Document files, which you can identify by the .msc extension.

MMC is the foundation for many preconfigured management tools that are available as .msc files in Windows 10. Perhaps the best known and richest is the Computer Management console, shown in Figure 1-10, which combines multiple snap-ins for easy access to a wide range of system settings.

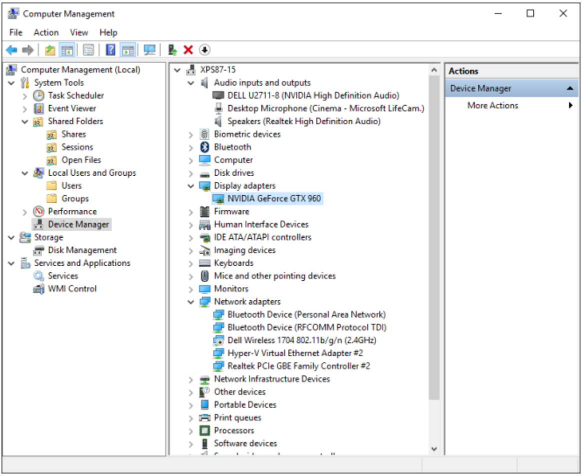
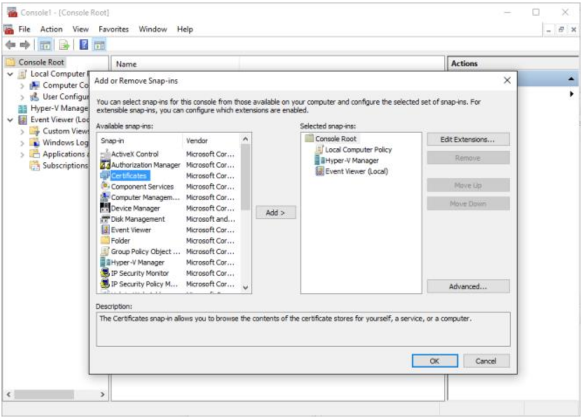


Figure 1-10: Computer Management is a built-in console that combines multiple snap-ins for one-stop access to common system management tools.

The MMC layout is consistent (if a bit old-fashioned looking) across all of its tools. MMC-based hardware configuration tools include Device Manager, which you can open in stand-alone mode or access from Computer Management, and Disk Management (which gets the spotlight in Chapter 6).

If you like the way Computer Management works—with a preconfigured collection of snap-ins—you can build your own custom console by running the MMC command and then adding snap-ins to the new, empty console window. Figure 1-11 shows the Add Or Remove Snap-Ins dialog box, which you can open on the File menu. From the list on the left, select a snap-in, and then click Add to include it in your custom console. Finally, save the result as an .msc file.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Hyper-V Manager	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...

Selected snap-ins:

Console Root
Local Computer Policy
Hyper-V Manager
Event Viewer (Local)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Figure 1-11: You can build a custom MMC console by using this list of snap-ins.

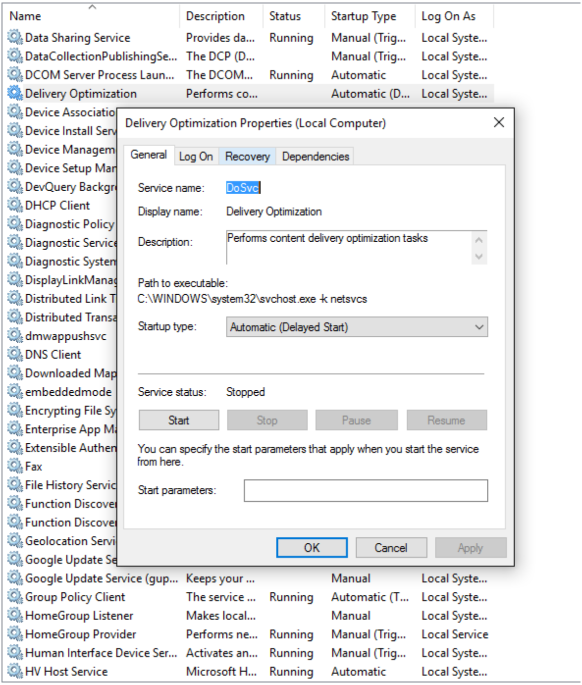
Table 1-1 lists all the snap-ins included with Windows 10 Pro. A description of each one is available at the bottom of the Add Or Remove Snap-Ins dialog box when you select it from the list on the left.

Table 1-1: Snap-ins available with Windows 10 Pro

Console name	File name
Authorization Manager	Azman.msc
Certificate Manager (local machine)	Certlm.msc
Certificate Manager (current user)	Certmgr.msc
Component Services	Comexp.msc
Computer Management	Compmgmt.msc
Device Manager	Devmgmt.msc
Disk Management	Diskmgmt.msc
Event Viewer	Eventvwr.msc
Shared Folders	Fsmgmt.msc
Local Group Policy Editor	Gpedit.msc
Local Users and Groups	Lusrmgr.msc
Performance Monitor	Perfmon.msc
Print Management	Printmanagement.msc
Resultant Set of Policy	Rsop.msc
Local Security Policy	Secpol.msc
Services	Services.msc

Task Scheduler	Taskschd.msc
Trusted Platform Module Manager	Tpm.msc
Hyper-V Manager	Virtmgmt.msc
Windows Firewall with Advanced Security	WF.msc
Windows Management Instrumentation	WmiMgmt.msc

One other feature common to every MMC-based console is the ability to open an item to view additional details about it as well as configuration options. In the Services snap-in, for example, you can double-click any entry in the list of available local services to set its startup type and start, stop, pause, or resume that service, as shown in Figure 1-12.



Name	Description	Status	Startup Type	Log On As
Data Sharing Service	Provides da...	Running	Manual (Trig...	Local Syste...
DataCollectionPublishingSe...	The DCP (D...		Manual (Trig...	Local Syste...
DCOM Server Process Laun...	The DCOM...	Running	Automatic	Local Syste...
Delivery Optimization	Performs co...		Automatic (D...	Local Syste...
Device Associatio				
Device Install Serv				
Device Managem				
Device Setup Mar				
DevQuery Backgr				
DHCP Client				
Diagnostic Policy				
Diagnostic Servic				
Diagnostic Systen				
DisplayLinkManag				
Distributed Link T				
Distributed Transa				
dmwappushsvc				
DNS Client				
Downloaded Map				
embeddedmode				
Encrypting File Sy				
Enterprise App Ma				
Extensible Authen				
Fax				
File History Servic				
Function Discover				
Function Discover				
Geolocation Servi				
Google Update Se				
Google Update Service (gup...	Keeps your ...		Manual	Local Syste...
Group Policy Client	The service ...	Running	Automatic (T...	Local Syste...
HomeGroup Listener	Makes local...		Manual	Local Syste...
HomeGroup Provider	Performs ne...	Running	Manual (Trig...	Local Service
Human Interface Device Ser...	Activates an...	Running	Manual (Trig...	Local Syste...
HV Host Service	Microsoft H...	Running	Automatic	Local Syste...

Delivery Optimization Properties (Local Computer)

Service name: DoSvc

Display name: Delivery Optimization

Description: Performs content delivery optimization tasks

Path to executable:
C:\WINDOWS\system32\svchost.exe -k netsvcs

Startup type: Automatic (Delayed Start)

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

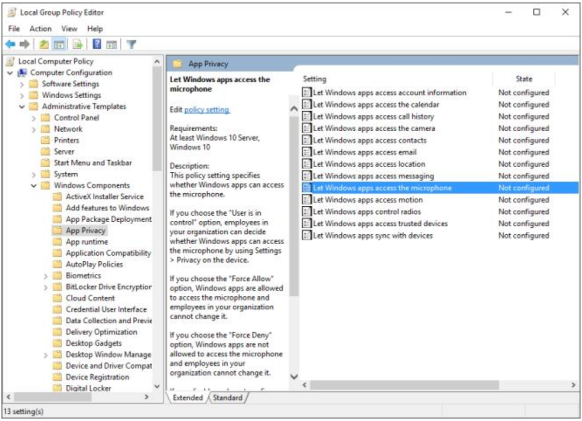
Start parameters:

Figure 1-12: You can use the details pane in the center of an MMC snap-in to see details about an item, such as the configuration options for this service.

Management and deployment tools

In homes and small businesses, you typically work on computers one at a time. In Windows domains, you can use Group Policy Objects to configure settings for users and machines. I discuss this option in Chapter 3.

Even if you’re on a small network, though, you can use the same policy editor to manage Local Computer Policy settings. To accomplish that task, open the oddly named Local Group Policy Editor (Gpedit.msc), which is available only in Windows 10 Pro, Enterprise, and Education editions. Many policies available here date back years, even decades, but each new Windows version typically includes its own new policies. Figure 1-13 shows a group of privacy settings that are new in Windows 10.



Let Windows apps access the microphone

Edit policy setting

Requirements:
At least Windows 10 Server, Windows 10

Description:
This policy setting specifies whether Windows apps can access the microphone.

If you choose the "User is in control" option, employees in your organization can decide whether Windows apps can access the microphone by using Settings > Privacy on the device.

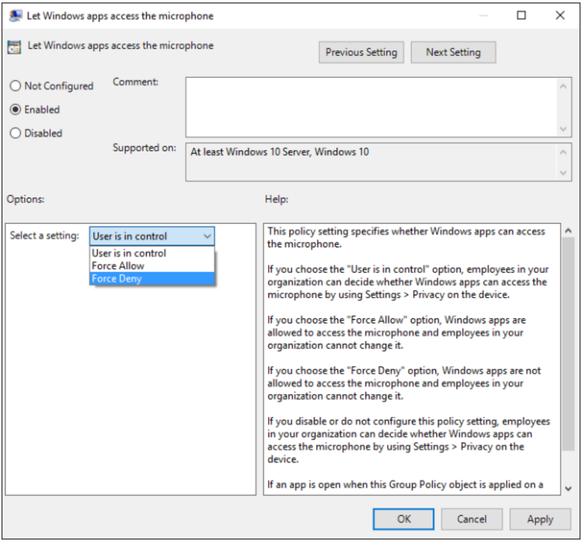
If you choose the "Force Allow" option, Windows apps are allowed to access the microphone and employees in your organization cannot change it.

If you choose the "Force Deny" option, Windows apps are not allowed to access the microphone and employees in your organization cannot change it.

Setting	State
Let Windows apps access account information	Not configured
Let Windows apps access the calendar	Not configured
Let Windows apps access call history	Not configured
Let Windows apps access the camera	Not configured
Let Windows apps access contacts	Not configured
Let Windows apps access email	Not configured
Let Windows apps access location	Not configured
Let Windows apps access messaging	Not configured
Let Windows apps access the microphone	Not configured
Let Windows apps access motion	Not configured
Let Windows apps control radios	Not configured
Let Windows apps access trusted devices	Not configured
Let Windows apps sync with devices	Not configured

Figure 1-13: Group Policy isn’t just for Windows domains: You can use local policies to define or restrict capabilities for users of an individual PC.

I could spend an entire book on the subject of Group Policy, but for now the single example in Figure 1-14 will have to suffice. Note that the policy is turned on for the local PC, which in turn makes available to you (as administrator) the three options in the Select A Setting section.



Let Windows apps access the microphone

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 10 Server, Windows 10

Options:

Select a setting: User is in control

User is in control
Force Allow
Force Deny

Help:

This policy setting specifies whether Windows apps can access the microphone.

If you choose the "User is in control" option, employees in your organization can decide whether Windows apps can access the microphone by using Settings > Privacy on the device.

If you choose the "Force Allow" option, Windows apps are allowed to access the microphone and employees in your organization cannot change it.

If you choose the "Force Deny" option, Windows apps are not allowed to access the microphone and employees in your organization cannot change it.

If you disable or do not configure this policy setting, employees in your organization can decide whether Windows apps can access the microphone by using Settings > Privacy on the device.

If an app is open when this Group Policy object is applied on a

Figure 1-14: To enforce a specific policy on a PC, you first must configure it. For some policies, as in this privacy setting, you can select from multiple options that a standard user can't override.

Powered by the cloud

Many of Microsoft's cloud services are designed to be platform-agnostic, with management from a web browser running on any operating system. As an administrator, for example, you can manage virtual machines and cloud services in Microsoft Azure from its web-based interface.

A few cloud services are tied directly to Windows 10, including the most recent client software for Microsoft's cloud-based file storage. This so-called next-generation sync client is capable of synchronizing OneDrive and OneDrive for Business files from a single PC and displaying the synchronized contents in File Explorer. I discuss this option more in Chapter 2.

Similarly, you can create a Windows 10 virtual machine in the Microsoft Azure cloud, or connect a work account to a Windows 10 PC by using Azure Active Directory. I discuss both options in Chapter 11.

CHAPTER 2

File Explorer

Of all the tools I cover in this book, File Explorer (formerly called Windows Explorer in Microsoft Windows 7 and earlier editions) is the one you no doubt use most often. And yet even many Windows experts only scratch the surface of this incredibly rich built-in app.

My basic principles for organizing files are simple:

- Consolidate your files into a handful of easy-to-access locations.
- Use keywords and descriptive filenames to make searches more effective.

- Master the powerful search tools in File Explorer.
- Have a backup plan.

Understanding how to make the most of File Explorer requires some background into how Windows itself organizes files. Some of these details are incredibly obvious, whereas others are subtle enough that even an experienced hand can miss them. So, in the interest of making sure we’re on the same page, allow me to start with a quick overview.

File Explorer essentials

File Explorer has its own button pinned to the taskbar by default. If you prefer not to take your hands off the keyboard, use its easy-to-remember keyboard shortcut, Windows logo key+E.

Figure 2-1 shows the default layout for File Explorer.

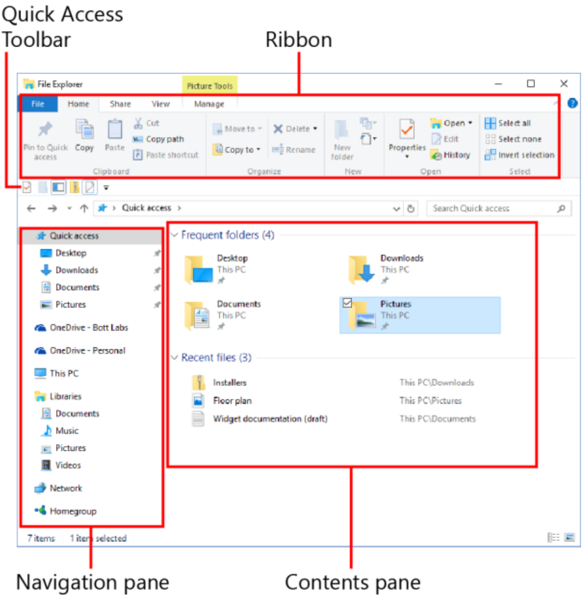
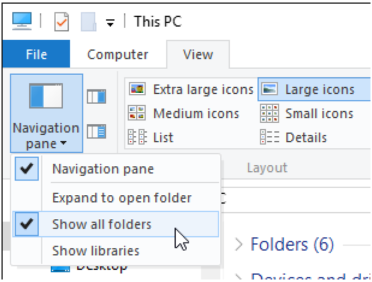


Figure 2-1: With a few tweaks, you can personalize the File Explorer layout to match your working style.

The ribbon that runs along the top of the File Explorer window resembles its counterpart in Microsoft Office applications, with a key distinction—you can't customize it. You can hide its contents, however, by double-clicking any of the tab headings. With the ribbon contents hidden, the headings resemble an old-fashioned menu bar and there’s more room for the contents pane.

The navigation pane on the left side is arranged into nodes that expand and collapse on demand. If you prefer the older, tree-style view with a single hierarchy, select This PC, and then, on the View tab, click Navigation Pane, and then select Show All Folders, as shown here:



With the Show All Folders option selected, the navigation pane looks like the example shown in Figure 2-2. (Note that I’ve collapsed the Quick Access menu to make the listing even more compact.)

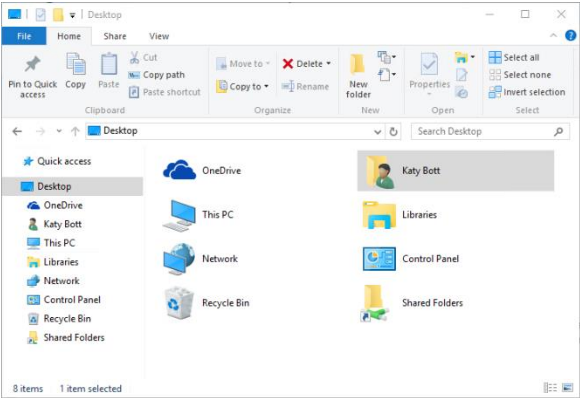
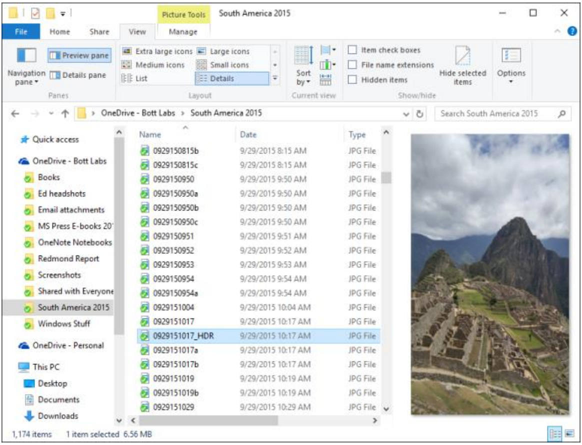


Figure 2-2: After selecting the Show All Folders option, the navigation pane shows only two nodes, Quick Access and Desktop.

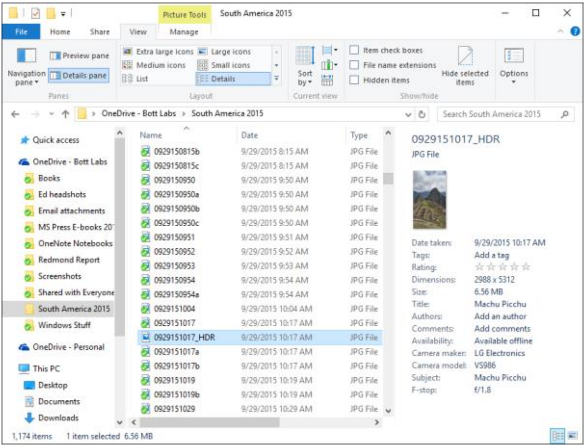
An optional element, hidden by default, is a pane that appears to the right of the contents pane. Depending on which option you select in the Panes group on the View tab, you see either a preview of the current selection or details about that selection. Figure 2-3 shows the preview pane for a high-resolution photo saved in JPEG format. Windows 10 contains filters with which you can preview most photo formats as well as Office documents, PDF files, and other common document formats.



Name	Date	Type
0929150815b	9/29/2015 8:15 AM	JPG File
0929150815c	9/29/2015 8:15 AM	JPG File
0929150950	9/29/2015 9:50 AM	JPG File
0929150950a	9/29/2015 9:50 AM	JPG File
0929150950b	9/29/2015 9:50 AM	JPG File
0929150950c	9/29/2015 9:50 AM	JPG File
0929150951	9/29/2015 9:51 AM	JPG File
0929150952	9/29/2015 9:52 AM	JPG File
0929150953	9/29/2015 9:53 AM	JPG File
0929150954	9/29/2015 9:54 AM	JPG File
0929150954a	9/29/2015 9:54 AM	JPG File
0929151004	9/29/2015 10:04 AM	JPG File
0929151017	9/29/2015 10:17 AM	JPG File
0929151017_HDR	9/29/2015 10:17 AM	JPG File
0929151017a	9/29/2015 10:17 AM	JPG File
0929151017b	9/29/2015 10:17 AM	JPG File
0929151019	9/29/2015 10:19 AM	JPG File
0929151019b	9/29/2015 10:19 AM	JPG File
0929151029	9/29/2015 10:29 AM	JPG File

Figure 2-3: Windows 10 contains filters that you can use to see a preview of the currently selected file in a pane to the right of the contents.

Figure 2-4 shows the Details pane for the same file.



Name	Date	Type
0929150815b	9/29/2015 8:15 AM	JPG File
0929150815c	9/29/2015 8:15 AM	JPG File
0929150950	9/29/2015 9:50 AM	JPG File
0929150950a	9/29/2015 9:50 AM	JPG File
0929150950b	9/29/2015 9:50 AM	JPG File
0929150950c	9/29/2015 9:50 AM	JPG File
0929150951	9/29/2015 9:51 AM	JPG File
0929150952	9/29/2015 9:52 AM	JPG File
0929150953	9/29/2015 9:53 AM	JPG File
0929150954	9/29/2015 9:54 AM	JPG File
0929150954a	9/29/2015 9:54 AM	JPG File
0929151004	9/29/2015 10:04 AM	JPG File
0929151017	9/29/2015 10:17 AM	JPG File
0929151017_HDR	9/29/2015 10:17 AM	JPG File
0929151017a	9/29/2015 10:17 AM	JPG File
0929151017b	9/29/2015 10:17 AM	JPG File
0929151019	9/29/2015 10:19 AM	JPG File
0929151019b	9/29/2015 10:19 AM	JPG File
0929151029	9/29/2015 10:29 AM	JPG File

0929151017_HDR
JPG File

Date taken:	9/29/2015 10:17 AM
Tags:	Add a tag
Rating:	☆☆☆☆☆
Dimensions:	2988 x 5312
Size:	6.56 MB
Title:	Machu Picchu
Authors:	Add an author
Comments:	Add comments
Availability:	Available offline
Camera maker:	LG Electronics
Camera model:	VS986
Subject:	Machu Picchu
F-stop:	f/1.8

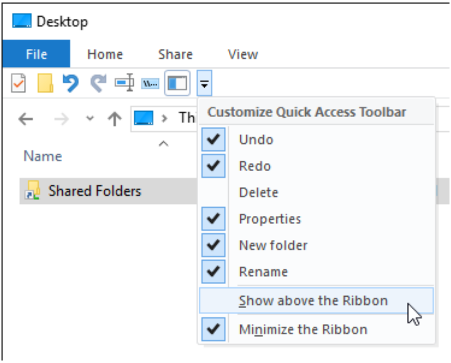
Figure 2-4: When the Details pane is visible, you can edit metadata for the current file; after you click in a field, Save and Cancel buttons appear at the bottom of the pane.

Change views quickly

Sometimes you want to see a table listing details about a file. Sometimes you want to see thumbnails of all files in a folder. In any File Explorer window, you can toggle between Details view and Large Thumbnails view by using the small, subtle buttons in the lower-right corner. Details view is especially useful when you want to filter the contents of a folder, as I explain later in this chapter.

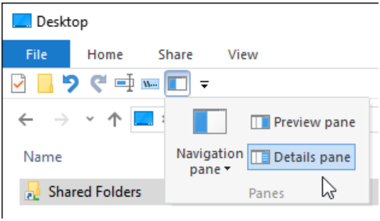
As I noted earlier, you can't customize the ribbon, but you can arrange the Quick Access Toolbar (QAT) to your heart's content.

By default, the QAT appears in the title bar, above the ribbon. Click the down arrow to its right and then click Show Below The Ribbon to move it. With the QAT in its new position, that option changes so that you can move it back above the ribbon, as shown here:



That same menu includes a short list of commonly used commands that you can add to the QAT. To add commands that are on the ribbon but not on that menu, right-click the command and then, on the shortcut menu that appears, choose Add To Quick Access Toolbar.

One of my favorite customization secrets involves a little-known fact about the QAT. You can add groups of commands to it, as well. For example, click the View tab, right-click the label at the bottom of the Panes group, and then choose Add To Quick Access Toolbar. Now, when you click that icon on the QAT, you can choose the Preview pane or the Details pane, as shown here:



Using Quick Access to organize files

The Quick Access node always appears at the top of the navigation pane. Its purpose is to give you a quick way to open frequently used files and folders. In addition, you can customize its contents by pinning locations here.

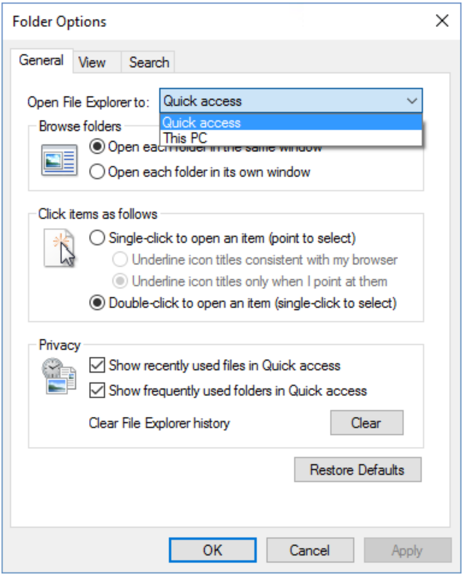
I consider this the most important real estate in File Explorer. As I mentioned at the beginning of this chapter, organizing files into a handful of locations is one of the first steps on the road to staying organized. After you have those locations established, you can pin shortcuts to each location here so that you can get to them quickly.

To pin a drive, folder, library, or other location to the Quick Access list, right-click that location and then, on the shortcut menu, choose Pin To Quick Access. To remove a pinned location, right-click its entry in the Quick Access list and then choose Unpin From Quick Access.

Space permitting, folders you've opened recently appear at the bottom of the Quick Access list. If you select the Quick Access heading, the Quick Access pane shows pinned and recent folders in a group at the top of the contents pane, with recently opened files beneath that group.

You can browse that list of recent files (and even pin a shortcut to the Quick Access pane) by going to %AppData%\Microsoft\Windows\Recent. You can get to the same location even more quickly by opening the Run box and entering **shell:recent**.

You'll find some extra Quick Access settings in the Folder Options dialog box, shown in Figure 2-5. At the very top is where you can specify whether you want new File Explorer windows to open in Quick Access or in This PC.



Open File Explorer to: Quick access

Browse folders

● Open each folder in the same window

○ Open each folder in its own window

Click items as follows

○ Single-click to open an item (point to select)

○ Underline icon titles consistent with my browser

● Underline icon titles only when I point at them

● Double-click to open an item (single-click to select)

Privacy

☑ Show recently used files in Quick access

☑ Show frequently used folders in Quick access

Clear File Explorer history

Figure 2-5: Clear either or both of the Privacy options at the bottom of the Folder Options dialog box to prevent recently opened files and folders from appearing in Quick Access.

If you don’t want recent files or folders to appear in Quick Access clear either or both of the options. Click Clear to empty the Recent folder and remove any shortcuts (except those you’ve pinned).

Using libraries and known folders

The longer you’ve been using a PC, the more at ease you’re likely to be with a hierarchy of folders that starts with drives and drive letters.

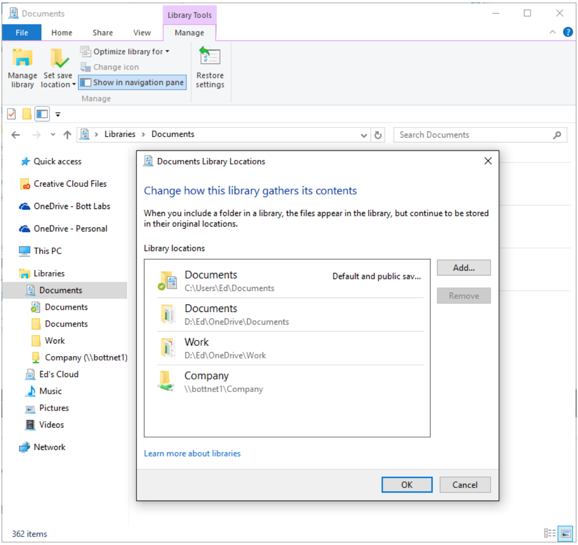
If you’re willing to break those old habits, though, you can be significantly more productive with File Explorer. The secret is to master the so-called *known folders* in your user profile—Documents, Downloads, Music, Pictures, Videos, and so on. And then, crucially, learn to use libraries, which represent an incredibly powerful way to pull together files from multiple locations into virtual folders that are easy to search and filter.

In a clean Windows 10 installation, libraries are hidden. If you don’t see the Libraries node in the navigation pane, click View, Navigation Pane, Show Libraries to make them visible.

The default selection of libraries basically duplicates the Documents, Music, Pictures, and Videos folders from your user profile. If you don’t plan to customize those libraries or create your own, you can keep them hidden. But I hope to convince you in this section that the benefits of using libraries are worth the trouble.

Adding folders to a library

To view and manage the folders that go into an existing library, select the library to make the Manage tab visible (it’s under the Library Tools heading), and then click Manage Library. Figure 2-6 shows the results for the Documents library on one of my Windows 10 PCs, with files drawn from four folders—the default Documents folder in my user profile, two separate synced OneDrive folders, and a shared folder called Company, located on a network file server.



Documents Library Locations

Change how this library gathers its contents

When you include a folder in a library, the files appear in the library, but continue to be stored in their original locations.

Library locations

Documents — Default and public sav...
C:\Users\Ed\Documents

Documents
D:\Ed\OneDrive\Documents

Work
D:\Ed\OneDrive\Work

Company
\\bottnet1\Company

Figure 2-6: This customized Documents library consists of four folders: three local folders on two different drives, along with a shared folder from a network server.

Expanding the Documents library in the navigation pane shows a separate entry for each folder that the library contains. You can use those links to browse through individual folders. More important, though, all of the folders in a library are automatically indexed, which means that you can search and filter contents from multiple sources as if they were in a single folder. In addition, all files in a library are backed up by File History, a feature I discuss later in this chapter.

To add a folder to an existing library, click the Manage Library button, click Add, and then browse to the location that you want to include. An easier way is to right-click the folder you want to add and then, on the shortcut menu, choose Include In Library. That option shows a list of existing libraries, as demonstrated in Figure 2-7.

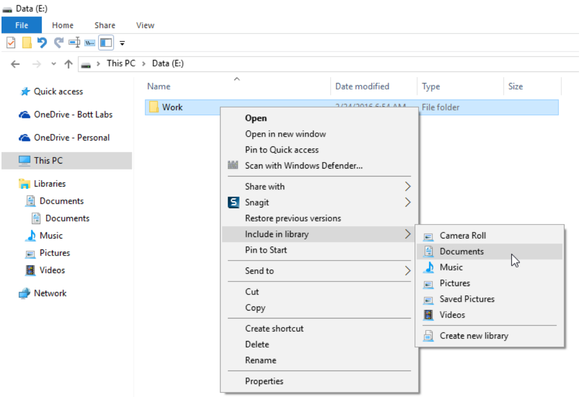


Figure 2-7: Right-click a folder and use this shortcut menu to add it to an existing library, or use the Create

New Library option at the bottom to start a library from scratch.

Eagle-eyed readers will no doubt note that the list of available libraries on that shortcut menu includes two that are not in the navigation pane. The Photos app created the Camera Roll and Saved Pictures libraries for its own use, and other apps can do the same.

To create your own custom library, use the Create New Library option at the bottom of that menu. Or as an alternative, click the Libraries heading in the navigation pane, right-click in the contents pane and choose New, and then choose Library. When you open the new library, click Include A Folder to browse for the first folder to include, or click Manage Library to add multiple folders.

I regularly use a custom library to keep track of content stored in multiple cloud services. I have both OneDrive and OneDrive for Business accounts, of course, but I also use third-party cloud services to work with clients and partners who prefer those services.

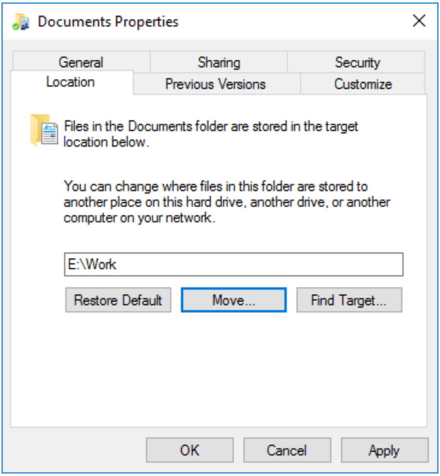
To keep track of all that cloud content, I created a custom library called Ed’s Cloud and added the local sync folder for each of those cloud services.

The resulting library gives me a unified view of all those cloud files, as well as the option to quickly find any file, even if I can’t remember in which service it’s stored.

Moving your data folders to a new location

On a related note, you can also move the known folders in your user profile—Documents, Downloads, Music, Pictures, and so on—to a different location. This is especially useful on a desktop PC with the option to add a second physical disk drive. Use a small, fast solid-state drive (SSD) as the system drive, and move data files to a conventional hard disk with greater capacity. The effects are most noticeable if your collection of digital music or photos is too large to fit comfortably on the system drive, where it’s normally located.

The process is simple. Open your user profile (easiest way is to enter %UserProfile% in the address bar), right-click the folder that you want to move, and then, on the shortcut menu, click the Location tab. That opens a dialog box like the one shown in Figure 2-8.



Files in the Documents folder are stored in the target location below.

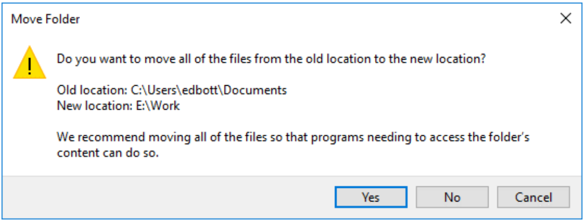
You can change where files in this folder are stored to another place on this hard drive, another drive, or another computer on your network.

E:\Work

Figure 2-8: To move a known folder (in this case, Documents) from your user profile to a new location, use the controls on the Location tab.

You can enter the path of the folder that you want to use or click Move to browse for a folder (with the option to create a new folder if necessary). Click Apply or OK to change the location.

When you do that, expect to see a dialog box like the one shown here:


Move Folder

Do you want to move all of the files from the old location to the new location?

Old location: C:\Users\edbott\Documents
New location: E:\Work

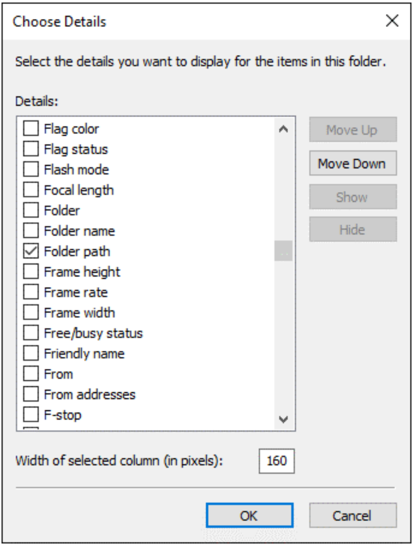
We recommend moving all of the files so that programs needing to access the folder's content can do so.

The correct answer is Yes, unless you want to keep an orphaned folder (and its contents) in your user profile.

Repeat this process for any other folders in your profile that you want to relocate.

It's OK to mix and match locations for these known folders. In fact, here's a tweak you can make that makes it possible for you to see the current location for all folders at a glance.

1. In the File Explorer address bar, open your user profile by typing **%userprofile%** and then pressing Enter.
2. Switch to Details view, if necessary.
3. Right-click any column heading and then, at the bottom of the shortcut menu that appears, choose More. That opens the Choose Details dialog box shown here:



Choose Details

Select the details you want to display for the items in this folder.

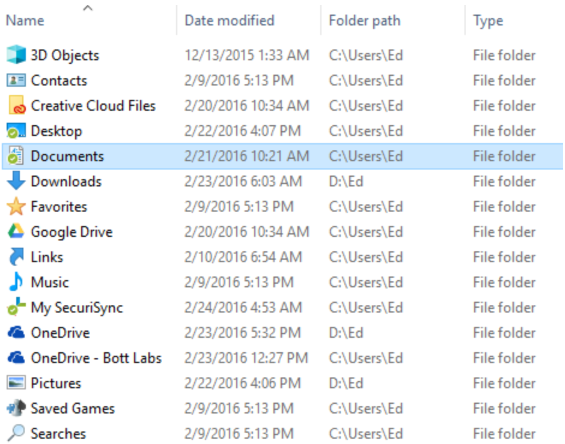
Details:

- □ Flag color
- □ Flag status
- □ Flash mode
- □ Focal length
- □ Folder
- □ Folder name
- ☑ Folder path
- □ Frame height
- □ Frame rate
- □ Frame width
- □ Free/busy status
- □ Friendly name
- □ From
- □ From addresses
- □ F-stop

Width of selected column (in pixels): 160

4. Select Folder Path from the list, and then click OK.

The contents of the File Explorer window should now look something like Figure 2-9. In this case, you can see at a glance that I have moved the Downloads and Pictures folder. (I've also chosen to put the synced copy of my OneDrive files on a separate drive, but making that change requires a different set of steps, as I explain later in this chapter.)



Name	Date modified	Folder path	Type
3D Objects	12/13/2015 1:33 AM	C:\Users\Ed	File folder
Contacts	2/9/2016 5:13 PM	C:\Users\Ed	File folder
Creative Cloud Files	2/20/2016 10:34 AM	C:\Users\Ed	File folder
Desktop	2/22/2016 4:07 PM	C:\Users\Ed	File folder
Documents	2/21/2016 10:21 AM	C:\Users\Ed	File folder
Downloads	2/23/2016 6:03 AM	D:\Ed	File folder
Favorites	2/9/2016 5:13 PM	C:\Users\Ed	File folder
Google Drive	2/20/2016 10:34 AM	C:\Users\Ed	File folder
Links	2/10/2016 6:54 AM	C:\Users\Ed	File folder
Music	2/9/2016 5:13 PM	C:\Users\Ed	File folder
My SecuriSync	2/24/2016 4:53 AM	C:\Users\Ed	File folder
OneDrive	2/23/2016 5:32 PM	D:\Ed	File folder
OneDrive - Bott Labs	2/23/2016 12:27 PM	C:\Users\Ed	File folder
Pictures	2/22/2016 4:06 PM	D:\Ed	File folder
Saved Games	2/9/2016 5:13 PM	C:\Users\Ed	File folder
Searches	2/9/2016 5:13 PM	C:\Users\Ed	File folder

Figure 2-9: With Folder Path added to the list of columns displayed in Details view, you can see at a glance where each of your user profile folders is located.

Search

If you’ve skimmed through this chapter so far, you might want to pay closer attention in this section. Mastering the search tools in File Explorer is the single most essential technique you can learn. The biggest increase in productivity comes when you realize that you can save files in a single folder and find them quickly with searches instead of meticulously organizing them in subfolders.

Every search in File Explorer consists of three parts:

- **Scope** This is where you’re searching. It can be a folder (with or without its subfolders), a library, or another search.
- **Filters** You use filters to restrict the search results by specifying dates, file types, tags, and other properties, typically by picking from a list or a calendar control.
- **Search terms** These are text strings that you type in the search box. Windows finds files and folders that contain the search terms in the file name or its contents.

You can, of course, search for files by using the search box on the taskbar. Type a search term and then click one of the small icons at the top of the results list to show documents, folders, pictures, music files, or videos that match those terms.

But for anything more than simple searches, the search box in File Explorer is the logical starting point.

Building a search by using the ribbon

Over the years, the tools for building a search in Windows have evolved impressively. With Windows 10, you can build a search by using a collection of point-and-click lists. In the upper-right corner of the File Explorer window, click in the search box to reveal the Search Tools ribbon, shown in Figure 2-10.

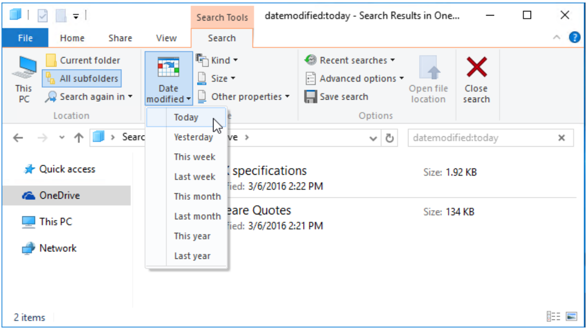


Figure 2-10: These search tools appear only after you click to position the insertion point in the search box. You can combine multiple criteria for moderately complex searches.

The choices you make using the Search Tools tab apply to the scope you have selected. In Figure 2-10, for example, OneDrive is selected in the navigation pane, and All Folders (the default) is selected in the Location group on the ribbon. Clicking Date Modified and selecting Today from the drop-down list shows me the two files that were added or changed in my OneDrive folder today.

If you're looking for notes you created after a meeting and you remember the meeting was last month, you can click Last Month from the Date Modified list. If the set of results is still too large to scan, you can apply additional filters or click in the search box and type a word or phrase that you know was in the file's name or its contents.

Three filters get top billing in the Refine group on the Search Tools tab:

- **Date Modified** This property is the most recent date a file or folder was saved, either when it was created or when it was last edited. For a downloaded program file, it shows the date you saved the file locally, not the date on which the developer created it.

- **Kind** This field shows predefined groups of file types, including those for some items that aren’t stored in Explorer. The most common choice to make here is Document, which includes text files, any file in an Office format, and PDF files. Try Music or Pictures if you’re looking for digital media files.
- **Size** This offers a range of sizes. If you’re trying to clear space on your system drive, choosing Huge (16 to 128 MB) or Gigantic (more than 128 MB) is a good way to locate large files that you can safely delete or archive on an external drive.

Clicking Other Properties on the Search Tools tab displays four additional filters with which you can refine the search results:

- **Type** This property uses the file type attribute. You can type a file name extension (pdf, xls, or docx, for example) or any part of the description (such as Excel, Word, image, text, or folder).
- **Name** Type a string of text here. The results list will show any file or folder that contains that exact string anywhere in its name.

- **Folder Path** Type a string of text here. The results list will show any file or folder that contains that exact string anywhere in its full path. For example, try typing **doc**; the results will include all files and folders in your Documents folder and any of its subfolders (because Documents is part of the path for those subfolders) as well as the contents of any other folder whose name contains those three letters.
- **Tags** Almost every data file contains this field, which is stored as metadata in the file itself. You can add one or more tags to any file by using the Details pane or the Details tab in its properties dialog box.

Use tags for pinpoint searches

Entering tags requires an extra step, but the effort can be worth it, especially for shared projects. The advantage of adding a tag like *Project X* or *2016 Taxes* to a group of files is that you can count on finding those files even if the tag text isn't in the file's name or contents. Because tags are saved as metadata, they can be used to identify files that are part of the group project.

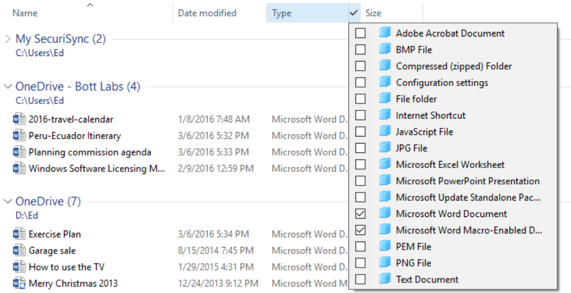
You can build a search by combining values from these different fields. So, you might choose This Week from the Date Modified list, and then Document from Kind. The result filters out any items that are older than the beginning of the current week as well as any extraneous files such as MP3 files and pictures.

You can't, however, choose more than one value from the drop-down list for a particular field. If you choose a value such as Last Week from Date Modified, it replaces whatever value you previously chose from that list. (There's a workaround, which I explain a bit later in this chapter, in the section "Creating complex searches.")

Using filters to find groups of files

Using the Search Tools tab on the ribbon is fine for occasional one-off searches, but it's often faster and more flexible to switch to Details view in File Explorer and use its built-in filtering options.

Figure 2-10, shows an example of how to filter files in a library by Type. Unlike the corresponding options on the Search Tools tab, you can choose multiple file types by selecting check boxes from the drop-down list associated with the Type column.



Name	Date modified	Type	Size
My SecuriSync (2) C:\Users\Ed			
OneDrive - Bott Labs (4) C:\Users\Ed			
2016-travel-calendar	1/8/2016 7:48 AM	Microsoft Word D.	
Peru-Ecuador Itinerary	3/6/2016 5:32 PM	Microsoft Word D.	
Planning commission agenda	3/6/2016 5:33 PM	Microsoft Word D.	
Windows Software Licensing M...	2/9/2016 12:59 PM	Microsoft Word D.	
OneDrive (7) D:\Ed			
Exercise Plan	3/6/2016 5:34 PM	Microsoft Word D.	
Garage sale	8/15/2014 7:45 PM	Microsoft Word D.	
How to use the TV	1/29/2015 4:31 PM	Microsoft Word D.	
Merry Christmas 2013	12/24/2013 9:12 PM	Microsoft Word M	

- □ Adobe Acrobat Document
- □ BMP File
- □ Compressed (zipped) Folder
- □ Configuration settings
- □ File folder
- □ Internet Shortcut
- □ JavaScript File
- □ JPG File
- □ Microsoft Excel Worksheet
- □ Microsoft PowerPoint Presentation
- □ Microsoft Update Standalone Pac...
- ☑ Microsoft Word Document
- ☑ Microsoft Word Macro-Enabled D...
- □ PEM File
- □ PNG File
- □ Text Document

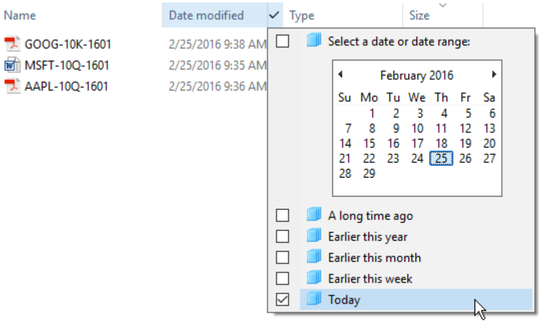
Figure 2-11: In Details view, click the right edge of any column heading to display a drop-down list built from that contents of that folder, and then select check boxes to show matching files.

It's worth noting that this technique filters only whatever is currently displayed in the contents pane, which is typically the contents of a folder or library. It doesn't search in subfolders.

Combine searches and filters

To expand a filtered Details view so that it includes all subfolders, click in the search box and then type the * wildcard character. This displays every file and folder in the current folder and all of its subfolders in a list. Now, you can switch to Details view and use the drop-down filter list on any column heading to refine the results.

The Date Modified filter is worth a closer look. As shown in Figure 2-12, it includes a calendar control that displays the current month and some predefined options below it.



Name	Date modified ✓	Type	Size
GOOG-10K-1601	2/25/2016 9:38 AM		
MSFT-10Q-1601	2/25/2016 9:35 AM		
AAPL-10Q-1601	2/25/2016 9:36 AM		

□ Select a date or date range:

February 2016

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29					

□ A long time ago

□ Earlier this year

□ Earlier this month

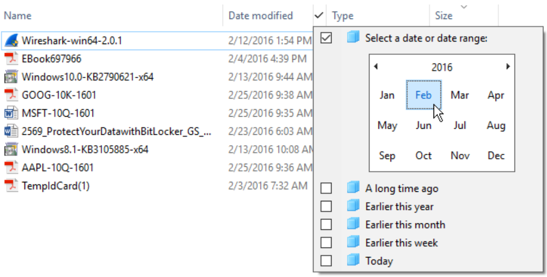
□ Earlier this week

☑ Today

Figure 2-12: This calendar control looks simple, but it provides far more options than you'd think.

The list of options at the bottom is dynamic, only showing choices that will return valid search results. This is different from the fixed menu on the Search Tools tab.

The calendar control is considerably more versatile than it looks at first glance. By default, it shows the current month. Click the month heading to change the control so that it shows all 12 months in the current year, as shown here:



Name	Date modified
Wireshark-win64-2.0.1	2/12/2016 1:54 PM
EBook697966	2/4/2016 4:39 PM
Windows10.0-KB2790621-x64	2/13/2016 9:44 AM
GOOG-10K-1601	2/25/2016 9:38 AM
MSFT-10Q-1601	2/25/2016 9:35 AM
2569_ProtectYourDatawithBitLocker_GS_...	2/23/2016 6:03 AM
Windows8.1-KB3105885-x64	2/13/2016 10:08 AM
AAPL-10Q-1601	2/25/2016 9:36 AM
TempldCard(1)	2/3/2016 7:32 AM

☑ Select a date or date range:

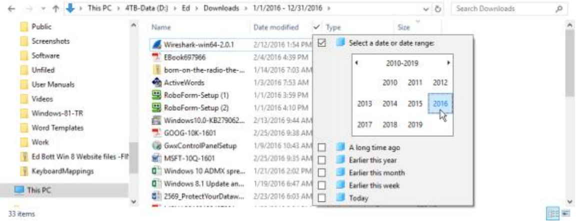
◂ 2016 ▸

Jan	Feb	Mar	Apr
May	Jun	Jul	Aug
Sep	Oct	Nov	Dec

□ A long time ago
□ Earlier this year
□ Earlier this month
□ Earlier this week
□ Today

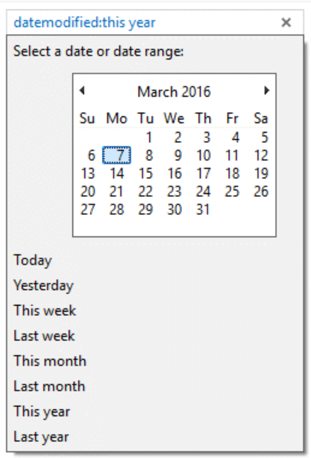
With this view open, you can Shift-click or click and drag to select multiple consecutive months in the same year. (Sorry, you can’t Ctrl+click to select nonadjacent months.)

Click the year heading to show all 10 years in the current decade, as shown here:



Again, you can click and drag to see files from two or more consecutive years. This is a handy trick if you’re looking through an archive that contains many years’ worth of files and folders.

If you like that calendar control, you can incorporate it into searches from the search box itself. To make it appear, click the search box and type **datemodified:** (don’t forget the colon). If there’s already a datemodified filter in the search box, click it to display the same calendar control, as shown here (note that you can select multiple options from the list below the calendar):



datemodified:this year

Select a date or date range:

March 2016

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

This calendar control works exactly the same as the one you display from the Date Modified heading in Details view. The fixed menu of options below it is different, however.

Creating complex searches

The search capabilities in Windows 10 are the direct descendants of features that date back more than a decade. Those original search tools relied on something called Advanced Query Syntax (AQS), which survives in a mostly undocumented form today.

You can see some vestiges of AQS when you build a search by using the Search Tools tab. Each entry you make from the ribbon adds a corresponding query to the search box.

You can distinguish a search operator from a search string because it appears in blue and is followed by a colon. If you follow that with an equal sign (=), you can enclose your search string in quotes to force an exact match.

If you're willing to tinker a bit, you can try manually building a search. For example, if you want to see only folders whose names begin with the letters A through E, in the search box, enter **type:="File folder" name:(>A AND <F)**.

You can also use two dots to mean "between" a pair of dates. So, **datemodified:12/1/2015 .. 1/31/2016** displays files created in either December 2015 or January 2016, a range you can't select via the calendar control.

You'll find a much more detailed discussion of these advanced queries in *Windows 10 Inside Out* (Microsoft Press, 2015).

Saving a search

I’ve saved the most powerful search trick of all for last: You can save a search and reuse it.

When you save a search, Windows writes your settings to an XML file, which is stored in the Searches folder within your user profile. This Saved Search format uses the .search-ms file name extension.

The beauty of saved searches is that relative dates such as This Week and Last Month are evaluated fresh each time you run the saved search, so the results should always be what you expect.

For example, suppose that you want to quickly see all of the synchronized OneDrive files you’ve added or edited in the past week or two. Here’s how to create that saved search:

1. Open your OneDrive folder by clicking its entry in the navigation pane.
2. Click the search box and type **datemodified:This Week OR datemodified:last week**.

3. On the ribbon's Search tab, click Save Search.

That's all you need to do. Windows automatically saved the current search scope and your date filters as an XML file in your %UserProfile%\Searches folder. Open that folder and double-click any saved search to rerun it.

Figure 2-13 shows my collection of saved searches. To make it easier to figure out what each search does, I've renamed the Saved Search files. (Right-click the saved search, choose Rename, and change the generic name to one that's more descriptive.)

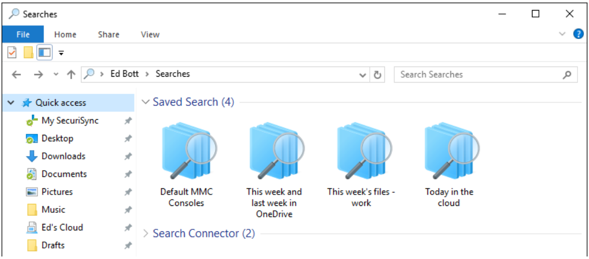


Figure 2-13: The Searches folder in your user profile contains all saved searches. In this example, I've changed the default names to more descriptive ones.

Use a saved search as a starting point

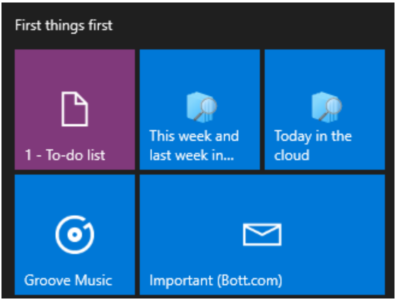
If you open a saved search, you can use its results as the scope for a new search. Any terms you type in the search box will return matching files and folders from the results of your saved search. So, if you have a saved search that shows all the files you saved to OneDrive this year, you can open that saved search and then type *invoice* or *budget* in the search box. This finds files that contain your search term in the name or the file itself, but only if they're in OneDrive and were modified this year.

The type of searches you can save is limited only by your imagination. You can define a nearly infinite number of combinations of locations, dates, file types, and other properties.

After you've built up a collection, here are two things you can do to make those saved searches easier to access:

- Pin a shortcut for the Searches folder to Quick Access. This way, you can quickly see all your saved searches and double-click any one to rerun that search.

- In the Searches folder, right-click any saved search and then, on the shortcut menu, choose Pin To Start, as I've done with two of my most useful searches in the example shown here:



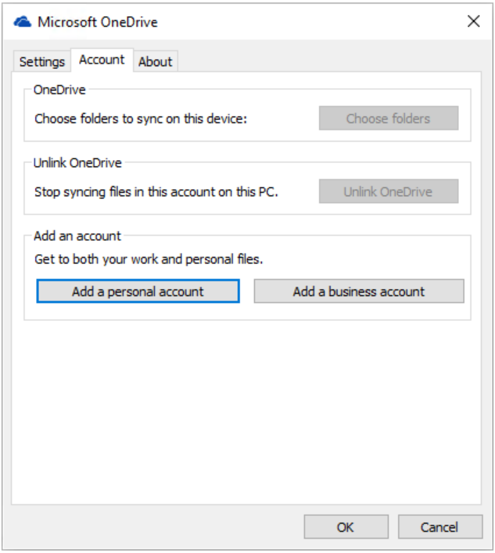
Syncing with OneDrive

One of the first things I do with any new PC is connect it to OneDrive, which gives me immediate access to the tens of thousands of documents, pictures, and other files I've stored there, not to mention my digital music collection.

OneDrive is no substitute for a solid backup routine, but it's an excellent part of that routine. If a drive suffers a hardware failure, I know that I don't need to worry about the files that were synced from OneDrive, because they're still safe in the cloud. There’s also a Recycle Bin on OneDrive, so even if I accidentally delete a file or folder, I can sign in to onedrive.com using my Microsoft account and restore it.

Because I have a Microsoft Office 365 Enterprise subscription I also have access to 1 TB of storage in OneDrive for Business, which is a separate cloud service. Until recently, those two services, despite the similar name, used separate sync clients. That’s no longer true. Microsoft has rolled out what it calls the Next-Generation Sync Client for Windows 10, which makes it possible for a single sync engine to work with OneDrive and OneDrive for Business accounts.

Figure 2-14 shows what the Next-Generation Sync Client looked like as of this writing. Because this cloud service and its associated sync client are constantly evolving, it’s possible that the version you see might look different.



Choose folders to sync on this device:

Stop syncing files in this account on this PC.

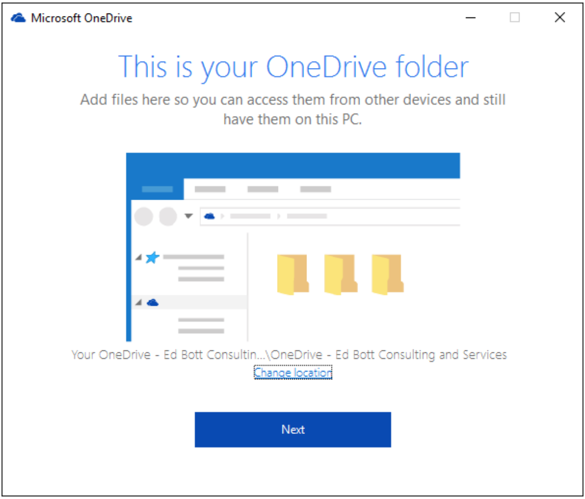
Get to both your work and personal files.

Figure 2-14: With the Next-Generation Sync Client, you can set up OneDrive personal accounts and OneDrive for Business accounts from a single starting point.

For now, at least, the sync client lets you add one personal account but multiple OneDrive for Business accounts. In either case, as part of the initial setup you get to do two things.

First, you get to choose the location for the local folder that will store your synced files. By default, this folder is stored in your user profile, on your system drive. For a personal OneDrive account, this folder is named simply OneDrive. For a OneDrive for Business account, the folder name includes the name of your business, as well.

In either case, you can see the suggested location and change it by clicking the Change Location link on this setup page. (Allow your mouse pointer to hover over the location to see its full path.)



Microsoft OneDrive

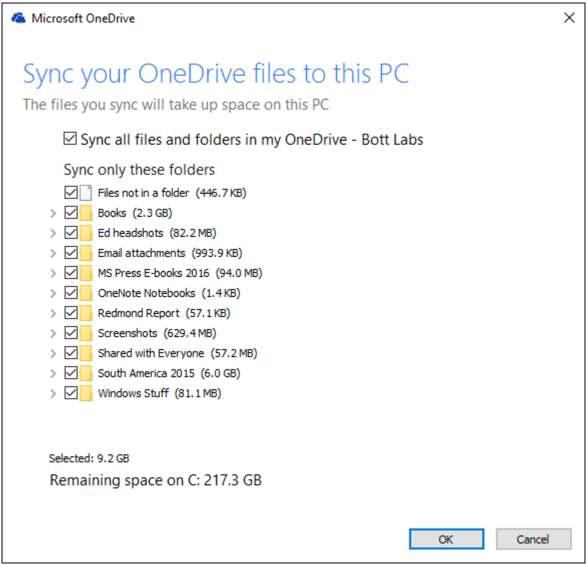
This is your OneDrive folder

Add files here so you can access them from other devices and still have them on this PC.

Your OneDrive - Ed Bott Consultin...\OneDrive - Ed Bott Consulting and Services

Make this choice carefully! If you change your mind later, there’s no easy way to relocate your synced files. Instead, you must unlink the folder, move the now-orphaned local files to the new location, and then set up sync again.

Second, you get to choose whether to sync all of your folders from the cloud to your local device or just choose some. Figure 2-15 shows these settings for a OneDrive for Business account, awaiting my approval or changes.



Microsoft OneDrive

Sync your OneDrive files to this PC

The files you sync will take up space on this PC

☑ Sync all files and folders in my OneDrive - Bott Labs

Sync only these folders

- ☑ Files not in a folder (446.7 KB)
- ☑ Books (2.3 GB)
- ☑ Ed headshots (82.2 MB)
- ☑ Email attachments (993.9 KB)
- ☑ MS Press E-books 2016 (94.0 MB)
- ☑ OneNote Notebooks (1.4 KB)
- ☑ Redmond Report (57.1 KB)
- ☑ Screenshots (629.4 MB)
- ☑ Shared with Everyone (57.2 MB)
- ☑ South America 2015 (6.0 GB)
- ☑ Windows Stuff (81.1 MB)

Selected: 9.2 GB

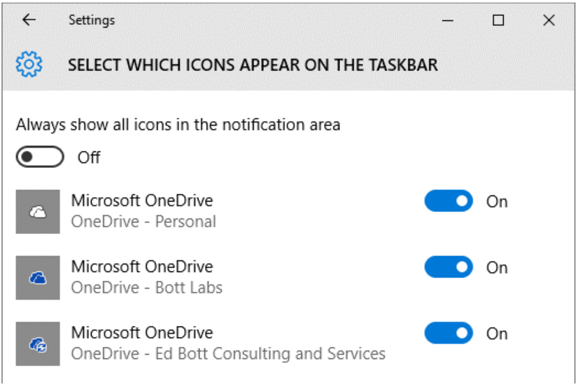
Remaining space on C: 217.3 GB

Figure 2-15: With either type of OneDrive account, personal or business, you get to choose which folders to sync to your local PC.

Your sync settings can be different for every device. On my desktop computer, for example, which has multiple terabytes of storage, I sync my entire OneDrive collection—several hundred gigabytes in all. On a Windows 10 tablet or laptop with limited storage, I sync only a few essential folders. As you can see from Figure 2-15, on the other hand, my OneDrive for Business account currently contains less than 10 GB of files, which means I can afford to be less selective with my sync decisions.

Each sync agent gets its own icon in the taskbar, a white cloud for your personal OneDrive account, a blue cloud for a OneDrive for Business account.

Use the Notifications page in the Settings app to show or hide the icons for any of your OneDrive accounts, as shown in Figure 2-16.



SELECT WHICH ICONS APPEAR ON THE TASKBAR

Always show all icons in the notification area

Off

Microsoft OneDrive
OneDrive - Personal — On

Microsoft OneDrive
OneDrive - Bott Labs — On

Microsoft OneDrive
OneDrive - Ed Bott Consulting and Services — On

Figure 2-16: Use the Windows 10 Settings app to show or hide icons for OneDrive accounts.

CHAPTER 3

Registry Editor

An unwritten law, passed down from generation to generation by Microsoft Windows support professionals, requires that I begin this chapter with the obligatory warning that editing the registry is potentially dangerous. Most mere mortals never need to know that Registry Editor even exists, much less open it. If you make an incorrect change in the registry, you can break your system. Proceed with caution.

Right, then. With that out of the way, please allow me to spend the rest of this chapter explaining why, on occasion, it's worth (carefully) ignoring that advice. The judicious use of Registry Editor is often the best and sometimes the only way to accomplish specific tasks that don't have an easily accessible entry point in the Windows user interface.

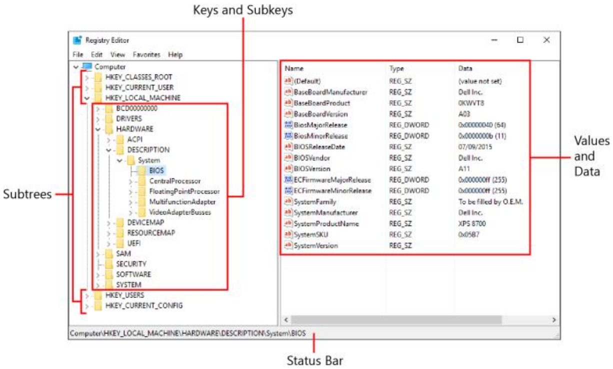
Despite the aura of magic and mystery surrounding the Windows registry, it's actually a simple database that contains all of the settings for a PC and for the currently signed-in user. Group Policy settings are stored in the registry, as are virtually every preference and configuration option in the Settings app and in Control Panel

There's a lot of mythology about the registry, which is probably an excellent starting point for this discussion.

How the registry works

Simply opening Registry Editor offers your first hints of its organization. Make sure you're signed in with an account in the Local Administrators group (Standard users can view the registry but not make changes), type **regedit** in the search box, and then click the matching command in the results list. You can open its file location and pin the shortcut to Start if you want; I don’t recommend pinning Registry Editor to the taskbar except for short-term tasks.

The basic structure of the registry has remained constant for decades. Figure 3-1 shows the hierarchy of the registry, with one of its five top-level subtrees expanded to show some of its keys and subkeys.



Name	Type	Data
(Default)	REG_SZ	(value not set)
BaseBoardManufacturer	REG_SZ	Dell Inc.
BaseBoardProduct	REG_SZ	0KWVT8
BaseBoardVersion	REG_SZ	A03
BiosMajorRelease	REG_DWORD	0x00000040 (64)
BiosMinorRelease	REG_DWORD	0x0000000b (11)
BIOSReleaseDate	REG_SZ	07/09/2015
BIOSVendor	REG_SZ	Dell Inc.
BIOSVersion	REG_SZ	A11
ECFirmwareMajorRelease	REG_DWORD	0x000000ff (255)
ECFirmwareMinorRelease	REG_DWORD	0x000000ff (255)
SystemFamily	REG_SZ	To be filled by O.E.M.
SystemManufacturer	REG_SZ	Dell Inc.
SystemProductName	REG_SZ	XPS 8700
SystemSKU	REG_SZ	0x05B7
SystemVersion	REG_SZ	

Computer\HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS

Figure 3-1: Opening Registry Editor shows the five subtrees, each beginning with HKEY, with values and data available for viewing and editing in the right pane.

This instance of Registry Editor is connected to the local computer, as evidenced by the heading at the top of the tree. (As I explain later in this chapter, you can connect to another PC over a network to edit its registry remotely.)

Beneath that top heading are five subtrees, each beginning with HKEY. In general, information about the local PC is saved in HKEY_LOCAL_MACHINE; settings for the user who is currently signed-in interactively are in HKEY_CURRENT_USER. In this and other books, you'll often see these two subtrees abbreviated, properly, as HKLM and HKCU.

Keys and subkeys in each of those subtrees are the equivalent of folders and subfolders. By itself, a key or subkey does nothing but supply a location where values can be stored.

In Figure 3-1, I've expanded the HKEY_LOCAL_MACHINE subtree to display several levels of keys and subkeys, with the BIOS subkey selected and its associated values listed on the right. You can see the full path to this subkey in the status bar at the bottom of the window.

Each value in the pane on the right represents a setting or configuration detail for the current PC or user. As I explain in the next section, you can view and (carefully) edit the data contained in those values to change a preference or setting.

In general, I recommend that you use built-in configuration tools—typically the Windows 10 Settings app, the Local Group Policy Editor (Gpedit.msc), or Control Panel, in particular—rather than editing the registry directly. Save the latter option for times when it's the only practical solution.

Don't use registry cleaners

In the Annals of Useless Software, there's a special category for registry cleaners. These tools are usually sold with extravagant promises of improved performance and reliability. And yet, the only objective tests I have seen show literally zero difference in performance after "cleaning" and "optimizing" the registry.

In fact, the entire premise behind registry cleaning is flawed. Yes, there are, no doubt, a few stray entries in your registry that were left behind when you uninstalled a program. But the idea that cleaning even a few dozen of those unneeded entries will make a measurable difference is absurd.

If you have a specific problem with removing a specific program, a registry cleaning utility might be able to identify keys that will help you to solve that specific problem. But that's a rare scenario. The more likely result of indiscriminately "cleaning" (in other words, deleting) registry entries is that you'll delete something you really need, causing a program or feature to fail.

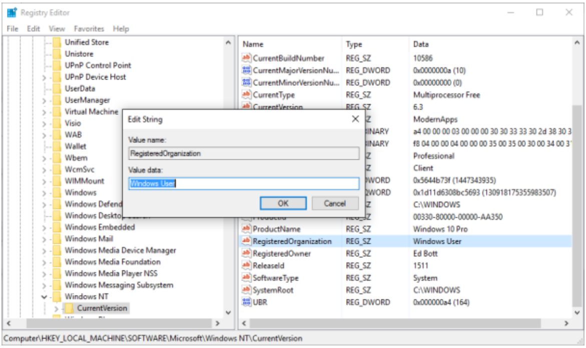
And if you don't believe me, maybe you'll believe Microsoft, which has published its support policy for registry cleaning utilities at support.microsoft.com/kb/2563254. The executive summary states the following:

"Microsoft does not support the use of registry cleaners. … Microsoft is not responsible for issues caused by using a registry cleaning utility. … Microsoft cannot guarantee that problems resulting from the use of a registry cleaning utility can be solved."

Editing the registry like a pro

For an example of a task that can't be accomplished by using built-in Windows tools, look no further than the Registered Owner and Registered Organization values associated with a copy of Windows 10. These values are occasionally used by third-party programs to populate default user information fields.

You can find those in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion key. In Figure 3-2, I’ve double-clicked the RegisteredOrganization value, opening a box in which I can change its data to something other than the default “Windows User” entry.



Value name: RegisteredOrganization

Value data: Windows User

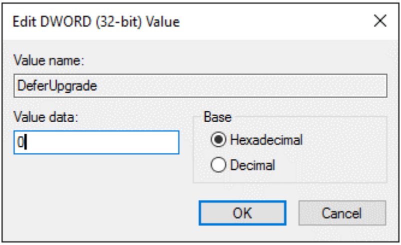
Name	Type	Data
CurrentBuildNumber	REG_SZ	10586
CurrentMajorVersionNu...	REG_DWORD	0x0000000a (10)
CurrentMinorVersionNu...	REG_DWORD	0x00000000 (0)
CurrentType	REG_SZ	Multiprocessor Free
CurrentVersion	REG_SZ	6.3
	Z	ModernApps
	INARY	a4 00 00 00 03 00 00 00 30 30 33 33 30 2d 38 30 3
	INARY	f8 04 00 00 04 00 00 00 35 00 35 00 30 00 34 00 3
	Z	Professional
	Z	Client
	WORD	0x5644b73f (1447343935)
	WORD	0x1d11d6308bc5693 (130918175355983507)
	Z	C:\WINDOWS
	Z	00330-80000-00000-AA350
ProductName	REG_SZ	Windows 10 Pro
RegisteredOrganization	REG_SZ	Windows User
RegisteredOwner	REG_SZ	Ed Bott
ReleaseId	REG_SZ	1511
SoftwareType	REG_SZ	System
SystemRoot	REG_SZ	C:\WINDOWS
UBR	REG_DWORD	0x000000a4 (164)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Figure 3-2: Editing a text string in a registry value is one of the simplest tasks in Registry Editor.

Because the data type in that value is REG_SZ (plain text), it’s a simple matter to type a replacement value and press Enter or click OK to save it.

For values that you can turn on or off, the data type is usually REG_DWORD, with a 0 for off and 1 for on. In the Settings app, for example, you'll find a Defer Upgrades check box under Update & Security > Windows Update > Advanced Options. Selecting or clearing that check box changes the associated value in HKLM\SOFTWARE\Microsoft\WindowsUpdate\UX\Settings. You could accomplish the same configuration setting by changing the registry value from 0 to 1, as shown here:



Edit DWORD (32-bit) Value

Value name: DeferUpgrade

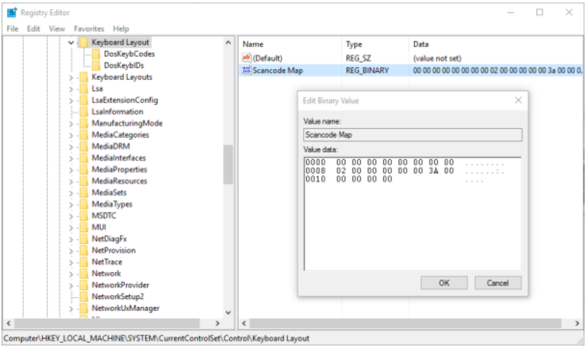
Value data: 0

Base: ● Hexadecimal ○ Decimal

Backup and restoring registry values

Some registry values don't really lend themselves to manual editing. Consider the example of the Caps Lock key on your keyboard. For many people (myself included), its actual function is completely useless, and its primary effect is to change text TO ALL CAPS when you accidentally hit it, resulting in muttered curses and some unnecessary editing.

The only way to change what happens when you press the Caps Lock key on a PC running Windows 10 is to make a change to the registry, specifically to the Scancode Map value in the subkey HKLM\SYSTEM\CurrentControlSet\Control\Keyboard Layout. Figure 3-2 shows the Keyboard Layout key selected. I've double-clicked the Scancode Map value and changed its data to a value that tells Windows to ignore the Caps Lock key. Note that its data is a binary value, with the data type REG_BINARY.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Scancode Map	REG_BINARY	00 00 00 00 00 00 00 00 02 00 00 00 00 00 3a 00 00 0.

Value name: Scancode Map

Value data:

```
0000   00  00  00  00  00  00  00  00    ........
0008   02  00  00  00  00  00  3A  00    ......:.
0010   00  00  00  00                    ....
```

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout

Figure 3-3: This slightly intimidating Registry Editor window is where you add the binary information to

change the keyboard scan codes to turn off the Caps Lock key.

After you change that value and restart your PC, that annoying Caps Lock key is effectively neutralized. Tapping it, deliberately or otherwise, does absolutely nothing.

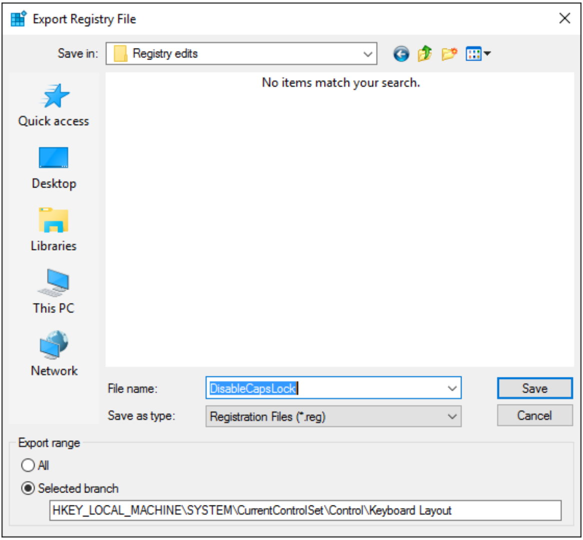
More on keyboard scancode maps

If that example whetted your interest, you might want to read this article from the superb howtogeek.com website, which explains how scancode maps work: http://bit.ly/scancode-maps.

That's an extreme but fitting example of a task that you can accomplish by using Registry Editor. But do you really want to manually type all of that binary code? Of course you don't. Which is why clever IT pros save that type of registry change so that they can apply it automatically, with just a click or two.

The secret is to create a simple text file that contains the necessary changes and save it in Registration Entries format, with a .reg file name extension. (This is the same technique you should use before you make a change that you might want to roll back, by the way.)

After you’ve made the changes in the registry, right-click the key or subkey whose changes you want to save and then, on the shortcut menu, choose Export. That opens the dialog box shown in Figure 3-3.



Save in: Registry edits

No items match your search.

File name: DisableCapsLock

Save as type: Registration Files (*.reg)

Export range

○ All

● Selected branch

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout

Figure 3-4: Use the Export option to save the current contents of a registry key before editing it. Afterward, you can use this tool to copy settings between PCs.

Note the Export Range selection at the bottom of that dialog box. It’s worth double-checking the Selected Branch box to be certain it displays the key or subkey you chose. (The only reason to select All is if you want to save the contents of the entire registry in a plain-text file so that you can compare before and after versions after installing a program or making a configuration change. Be warned: The resulting files are enormous. In that scenario, you're better off saving an individual subtree or two rather than the entire registry.)

Should you back up the registry?

In earlier Windows versions, making a backup copy of the registry was an essential step before most major configuration changes. With Windows 10, that step is unnecessary. The System Restore option is a more effective way to accomplish the same goal of rolling back unwanted changes, and in the case of major problems, the Reset option is faster and more likely to succeed. It is, however, prudent to back up individual keys and subkeys before making changes, just in case you need to restore the original settings.

After you save the exported file, you need to jump through one more hoop to make that file truly useful. The .reg file contains every value associated with the selected key and all its subkeys. This can result in a problem if you import that file on another PC: You're likely to change a bunch of settings you didn't really want to tamper with.

The solution is to open the .reg file in a text editor, manually delete the settings for keys you don't want to change, and then save the edited file. The result is a file that looks like this:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
\Keyboard Layout]

"Scancode
Map"=hex:00,00,00,00,00,00,00,00,02,00,00,00,00,00,3
a,00,00,00,00,00
```

Note that the key or subkey is enclosed in brackets. For an explanation of the syntax of .reg files (including the use of the hyphen to delete registry keys and values), go to https://support.microsoft.com/en-us/kb/310516.

To import your saved setting into the registry of another PC running Windows 10, all you need to do is copy the file to a USB flash drive or a shared network folder and then double-click it from the target PC. Doing so results in a confirmation prompt and a success message. To make the change silently, type **Regedit.exe /s *saved_file***, where *saved_file* is the full path to the .reg file you created.

When you import settings from a .reg file, Windows processes the file's contents in order, starting at the top of the file. If the first key on the list doesn't already exist, Windows creates that key and then adds any values you specify. If you want to create a new subkey with another subkey below it, be sure to enter the lines in the correct order.

Data items must be enclosed in quotation marks and are immediately followed by an equal sign and then the value you want to add. If a data item in your file doesn't exist in the registry, the .reg file adds it along with the specified value. If the specified data item does exist, the value in your .reg file overwrites the existing value.

Finally, you have the option to use the Reg command in a Command Prompt window or in a batch file or script. From an elevated Command Prompt, use this command:

```
reg add
"HKLM\SYSTEM\CurrentControlSet\Control\Keyboard
Layout" /v "Scancode Map" /t REG_BINARY
```

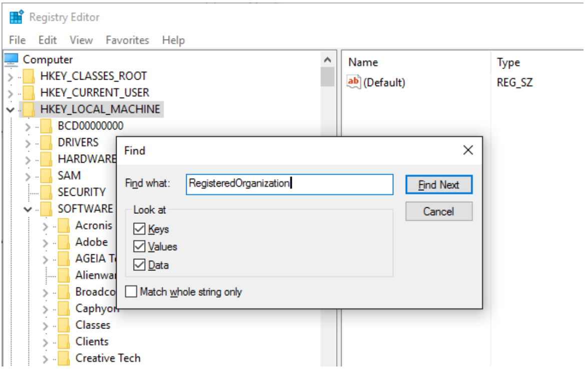
```
/d "00 00 00 00 00 00 00 00 02 00 00 00 00 00 3a 00
00 00 00 00"
```

Type **reg /?** to see the full list of eligible arguments for the reg command (query, add, export, import, and so on). Each of those variants has its own syntax help. Try **reg add /?** to make sense of the switches in the command above.

Finding keys, values, and data

If you know the exact subkey that contains the value you're looking for, you can navigate through the tree on the left to find it, expanding keys to see the full list of subkeys beneath them.

When you're not sure of the location, use Registry Editor's built-in Find function, which is available on the Edit menu. You can also use the keyboard shortcut Ctrl+F. Either option opens the dialog box shown in Figure 3-5.



Find what: RegisteredOrganization

Look at

☑ Keys

☑ Values

☑ Data

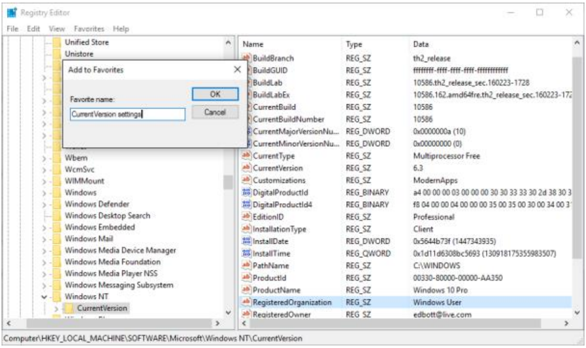
☐ Match whole string only

Figure 3-5: Press Ctrl+F to open the Find dialog box and search for a setting in the registry.

If you know the exact string you're looking for, type it here and, optionally, use the three check boxes to narrow your search to find matches only in keys, values, or data. Press Enter or click Find Next to locate the next matching instance below your current selection.

You don't need to reopen the Find dialog box to repeat the search. Instead, press F3 to find the next matching entry in the list. Keep pressing F3 until you locate the entry you're looking for.

If you regularly revisit the same keys in the registry, you should get to know the Favorites option on the Registry Editor menu. Select a key or subkey, click Favorite, and then click Add To Favorites. That opens the dialog box shown in Figure 3-6. By default, this box contains the name of the selected key or subkey, but you can change it to a more descriptive name.



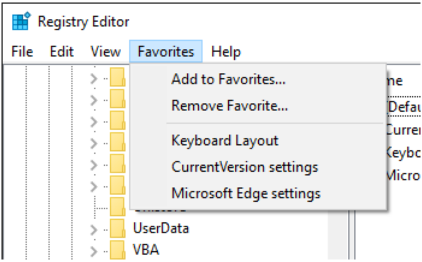
Favorite name: CurrentVersion settings

Name	Type	Data
BuildBranch	REG_SZ	th2_release
BuildGUID	REG_SZ	ffffffff-ffff-ffff-ffff-ffffffffffff
BuildLab	REG_SZ	10586.th2_release_sec.160223-1728
BuildLabEx	REG_SZ	10586.162.amd64fre.th2_release_sec.160223-172
CurrentBuild	REG_SZ	10586
CurrentBuildNumber	REG_SZ	10586
CurrentMajorVersionNu...	REG_DWORD	0x0000000a (10)
CurrentMinorVersionNu...	REG_DWORD	0x00000000 (0)
CurrentType	REG_SZ	Multiprocessor Free
CurrentVersion	REG_SZ	6.3
Customizations	REG_SZ	ModernApps
DigitalProductId	REG_BINARY	a4 00 00 00 03 00 00 00 30 30 33 33 30 2d 38 30 3
DigitalProductId4	REG_BINARY	f8 04 00 00 04 00 00 00 35 00 35 00 30 00 34 00 3
EditionID	REG_SZ	Professional
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0x5644b73f (1447343935)
InstallTime	REG_QWORD	0x1d11d6308bc5693 (130918175355983507)
PathName	REG_SZ	C:\WINDOWS
ProductId	REG_SZ	00330-80000-00000-AA350
ProductName	REG_SZ	Windows 10 Pro
RegisteredOrganization	REG_SZ	Windows User
RegisteredOwner	REG_SZ	edbott@live.com

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Figure 3-6: After selecting a key or subkey from the tree on the left, use the Add To Favorites menu to save a pointer to that key on the Favorites menu.

After you add one or more items in this fashion, they appear at the bottom of the Favorites menu, as shown here:



To remove a saved Favorite, click Favorites, point to Remove Favorite, and then, in the Remove Favorites dialog box, select a saved item from the list.

Copy your favorite registry settings

Here's a secret that even most Windows experts don't know about. Your Registry Editor Favorites are saved, naturally, in the registry—specifically in the subkey HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\Regedit\Favorites. After customizing the Favorites menu, right-click that key and export its contents to a .reg file, as I described in the previous section. You can now use that file to export your Favorites from one machine to another.

Using the command line

As I illustrated in the example earlier in this chapter, all versions of Windows include a built-in command called Reg with which you can perform operations on registry subkeys and values. It's especially useful for IT pros who want to put together scripts to query and change registry values on a network.

Documenting this powerful command could easily fill a chapter of its own, but if you're curious, check out the official reference at http://bit.ly/reg-command.

Editing the registry by using Local Group Policy Editor

You can configure many user preferences and system settings by using Group Policy. On a domain network, that typically involves an administrator creating templates that are applied to a domain-joined PC when it connects to the network.

But those same policies are available on any PC running Windows 10 Professional or Enterprise, using the Local Group Policy Editor. The result gives the administrator of such a PC access to many settings that aren’t otherwise available. To start this useful tool, run Gpedit.msc. Figure 3-7 shows the Local Group Policy Editor in action.

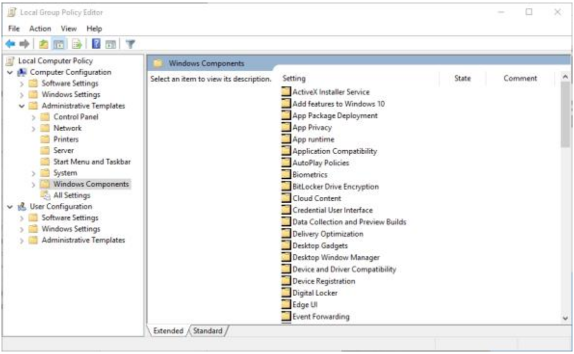
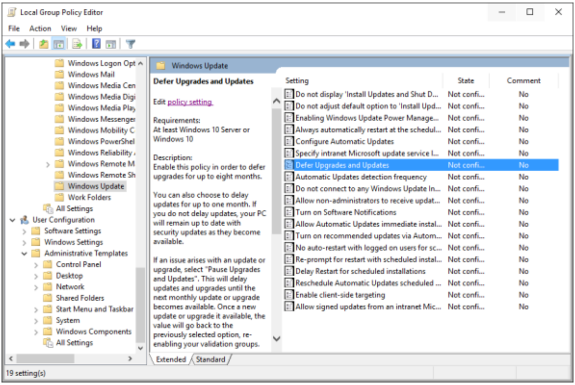


Figure 3-7: Local Group Policy Editor typically offers more options than the Settings app and other end-user-focused controls.

This built-in app has a hierarchical organization, as displayed in the tree on the left, that’s similar to that of Registry Editor. The two main branches correspond roughly to HKLM and KKCU. Policies in the Computer Configuration branch typically apply to the PC, independent of users, whereas those in the User Configuration branch typically apply after a user signs in.

Earlier in this chapter, I pointed out the Defer Upgrades option, which you can set by selecting a check box in the Settings app or by editing the registry. Using Group Policy offers significantly more options than a single check box. This policy and its associated setting are found in Computer Configuration > Administrative Templates > Windows Components > Windows Update. Figure 3-7 shows the relevant policy, one of 19 settings available under this heading (note that not all of them apply to Windows 10).



Defer Upgrades and Updates

Edit policy setting

Requirements:
At least Windows 10 Server or Windows 10

Description:
Enable this policy in order to defer upgrades for up to eight months.

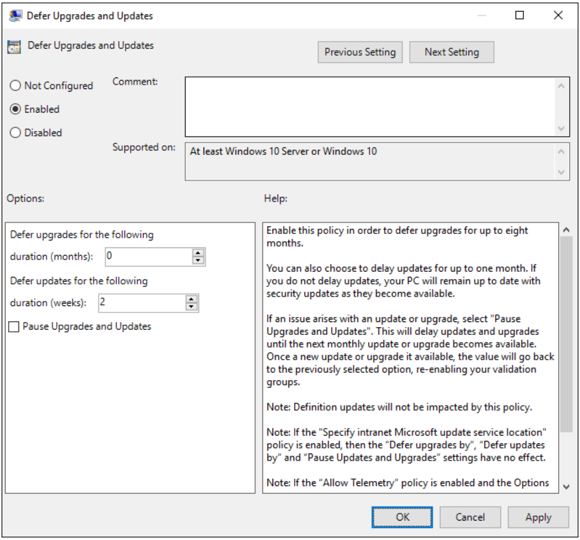
You can also choose to delay updates for up to one month. If you do not delay updates, your PC will remain up to date with security updates as they become available.

If an issue arises with an update or upgrade, select "Pause Upgrades and Updates". This will delay updates and upgrades until the next monthly update or upgrade becomes available. Once a new update or upgrade it available, the value will go back to the previously selected option, re-enabling your validation groups.

Setting	State	Comment
Do not display 'Install Updates and Shut D...	Not confi...	No
Do not adjust default option to 'Install Upd...	Not confi...	No
Enabling Windows Update Power Manage...	Not confi...	No
Always automatically restart at the schedul...	Not confi...	No
Configure Automatic Updates	Not confi...	No
Specify intranet Microsoft update service l...	Not confi...	No
Defer Upgrades and Updates	Not confi...	No
Automatic Updates detection frequency	Not confi...	No
Do not connect to any Windows Update In...	Not confi...	No
Allow non-administrators to receive updat...	Not confi...	No
Turn on Software Notifications	Not confi...	No
Allow Automatic Updates immediate instal...	Not confi...	No
Turn on recommended updates via Autom...	Not confi...	No
No auto-restart with logged on users for sc...	Not confi...	No
Re-prompt for restart with scheduled instal...	Not confi...	No
Delay Restart for scheduled installations	Not confi...	No
Reschedule Automatic Updates scheduled ...	Not confi...	No
Enable client-side targeting	Not confi...	No
Allow signed updates from an intranet Mic...	Not confi...	No

Figure 3-8: The explanatory text to the left of the list of available policies typically offers a thorough explanation of what the selected policy does.

Selecting that policy from the list on the right in Local Group Policy Editor displays a surprisingly detailed block of help text to the left of the entry itself, explaining what the policy does and how to configure it. Double-click the policy to open a window in which you can configure it, as shown in Figure 3-9.



○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows 10 Server or Windows 10

Options:

Defer upgrades for the following duration (months): 0

Defer updates for the following duration (weeks): 2

□ Pause Upgrades and Updates

Help:

Enable this policy in order to defer upgrades for up to eight months.

You can also choose to delay updates for up to one month. If you do not delay updates, your PC will remain up to date with security updates as they become available.

If an issue arises with an update or upgrade, select "Pause Upgrades and Updates". This will delay updates and upgrades until the next monthly update or upgrade becomes available. Once a new update or upgrade it available, the value will go back to the previously selected option, re-enabling your validation groups.

Note: Definition updates will not be impacted by this policy.

Note: If the "Specify intranet Microsoft update service location" policy is enabled, then the "Defer upgrades by", "Defer updates by" and "Pause Updates and Upgrades" settings have no effect.

Note: If the "Allow Telemetry" policy is enabled and the Options

Figure 3-9: Select Enabled from the options at the top of this policy setting window to make more detailed settings available below.

Although the explanatory text never uses the phrase, this is an important piece of the Windows Update for Business feature. As with many features that are intended for business users, the primary deployment tool is Group Policy, and it allows for far more options than are available in the Settings app. Although its design is for enterprise networks, you can freely use it on your own PC, with exactly the same effect.

Editing the registry on a remote PC

By default, opening Registry Editor connects to the registry on the local PC. With a little advance work, you can connect to a remote PC for some simple registry editing tasks. The Connect Network Registry option is available on Registry Editor's File menu, but before you can make it work, you need to do a bit of advance configuration.

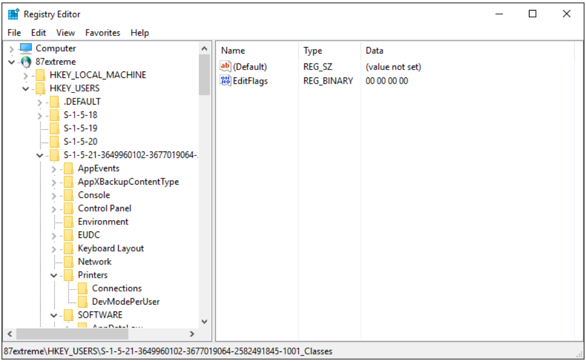
First, you must turn on the Remote Registry service on the remote PC whose registry you want to edit. To do that, in the search box on the taskbar, type **services** and then click Services from the results list. In the Services console (Services.msc), double-click the Remote Registry service and change the Startup entry from Disabled to Manual or Automatic, and then click Start.

To edit the remote registry (as opposed to just viewing it), you must be signed in as an administrator on your local computer.

Finally, you need to be able to supply administrative credentials for the remote PC.

With those details out of the way, on the File menu, choose Connect Network Registry. Type the name of the remote computer to which you want to connect, and then enter the credentials for an administrator's account on the remote PC when prompted.

The result, shown in Figure 3-10, is a new top-level branch in the tree pane, with two subtrees beneath it.



Name	Type	Data
(Default)	REG_SZ	(value not set)
EditFlags	REG_BINARY	00 00 00 00

87extreme\HKEY_USERS\S-1-5-21-3649960102-3677019064-2582491845-1001_Classes

Figure 3-10: Connecting to a remote registry requires some configuration changes and offers only limited access to the remote PC.

Your capabilities in this mode are severely limited compared to those you have available when you sign in interactively to the remote PC. In general, on a home or small office network, you'll probably have better results using Remote Desktop Protocol to connect to the remote PC and then run Registry Editor in the Remote Desktop session.

CHAPTER 4

Event Viewer

If something happens in Windows, chances are there's a record of it on your system drive. Like its predecessors, Windows 10 keeps copious logs of its activity, primarily for use by IT pros and support technicians troubleshooting problems or trying to understand the workings of a feature.

To view the contents of those logs, Windows 10 includes the latest version of the built-in Event Viewer app. Most people only ever scratch the surface of this amazingly powerful troubleshooting tool. It's most commonly used for tracking down problems on a single PC, but

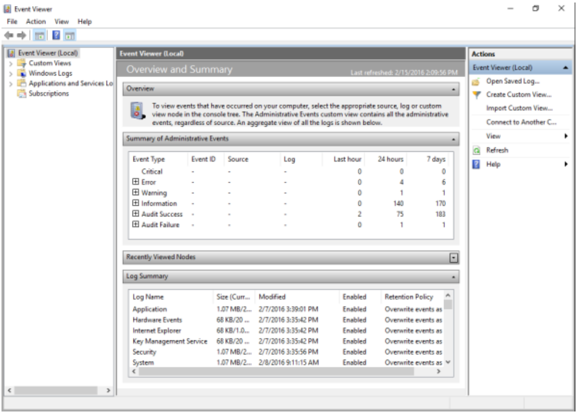
IT pros can connect to a remote computer easily for troubleshooting without leaving the help desk. Finding information in event logs can take some digging, and interpreting those events properly can be challenging, as well.

In this chapter, my goal is to help you unlock the hidden power of Event Viewer.

An overview of Event Viewer

Although you can start Event Viewer by digging around in Control Panel, the easiest way to open this console is to type **event** in the search box and then, from the top of the search results list, click the Event Viewer shortcut. You can also right-click Start (or press Windows logo key+X) and then select Event Viewer from the Quick Links menu. If you prefer the full command name, enter **eventvwr.exe** or **eventvwr.msc** in the Run box or at any command prompt.

If the .msc filename extension doesn’t make it clear that this app uses a Microsoft Management Console (MMC) snap-in, the main window should erase all doubt. (For more on MMC apps, see Chapter 1.) The default view, shown in Figure 4-1, offers the familiar three-pane arrangement, with a tree-based navigation control in the pane on the left, actions on the right, and a useful summary of recent events in the center.



To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
Critical	-	-	-	0	0	0
⊞ Error	-	-	-	0	4	6
⊞ Warning	-	-	-	0	1	1
⊞ Information	-	-	-	0	140	170
⊞ Audit Success	-	-	-	2	75	183
⊞ Audit Failure	-	-	-	0	1	1

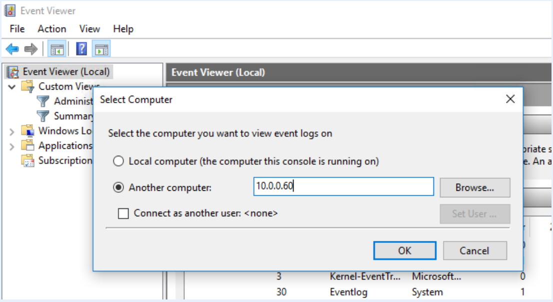
Log Name	Size (Curr...	Modified	Enabled	Retention Policy
Application	1.07 MB/2...	2/7/2016 3:39:01 PM	Enabled	Overwrite events as
Hardware Events	68 KB/20 ...	2/7/2016 3:35:42 PM	Enabled	Overwrite events as
Internet Explorer	68 KB/1.0...	2/7/2016 3:35:42 PM	Enabled	Overwrite events as
Key Management Service	68 KB/20 ...	2/7/2016 3:35:42 PM	Enabled	Overwrite events as
Security	1.07 MB/2...	2/7/2016 3:35:56 PM	Enabled	Overwrite events as
System	1.07 MB/2...	2/8/2016 9:11:15 AM	Enabled	Overwrite events as

Figure 4-1: This Overview And Summary page is the starting point for Event Viewer, offering a view of recent events in a collapsible list, categorized by severity.

When you open Event Viewer, the navigation pane on the left is collapsed and the Event Viewer (Local) node at the top is selected. This gives you a summary view of administrative events in the center.

View event logs on a remote computer

Like many of its siblings in the Windows administrative tools family, Event Viewer can connect to a remote computer so that an administrator can view and manage event logs without leaving the help desk. Choose Action, Connect To Another Computer to open the dialog box shown here, where you can type a computer name or IP address. (You can also use the Wevtutil command-line tool for this function.) For step-by-step instructions, see the TechNet article “Work with Event Logs on Remote Computer,” at https://technet.microsoft.com/library/cc766438.aspx.



Select Computer

Select the computer you want to view event logs on

○ Local computer (the computer this console is running on)

● Another computer: 10.0.0.60

☐ Connect as another user: <none>

Even if a system appears to be running flawlessly, it’s worth checking the summary of administrative events every so often. The log entries shown here are divided into six categories, listed in decreasing order of severity:

- **Critical** This type of event indicates a failure in an application or a part of the operating system that cannot be automatically recovered. STOP errors (aka the Blue Screen of Death) appear here. Any event that appears in this category deserves thorough troubleshooting.
- **Error** Problems listed here typically affect the functionality of an app or a part of the operating system from which recovery might be possible. Some errors are harmless and can be safely ignored, but others indicate failures in hardware drivers or peripherals that are worth investigating.
- **Warning** These events are typically not serious but can be indications of transient issues (such as a lack of a network connection) or configuration problems.
- **Information** Entries in this category are usually status reports. You'll find reports of successful installations from the Windows Update client here, for example. Typically, no

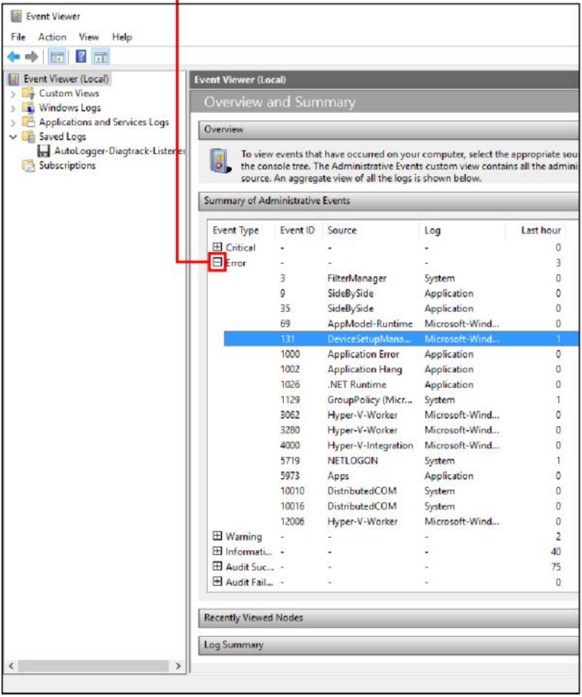
action is necessary in response to these events.

- **Audit Success** and **Audit Failure** These entries come from the security logs and indicate that the exercise of a user right has succeeded or failed. These are of little interest for the kind of troubleshooting I discuss in this chapter, although they might be of interest to a security professional looking for unusual activity from a user account.

Windows draws events from multiple logs: Windows logs (Application, Security, and System), which collect events from the entire operating system; Setup logs; and Applications and Services logs that store events from a single application or operating system component.

The summary combines the most important of these events into a unified view, where you can collapse or expand each of the sections to see more details. In Figure 4-2, for example, I've clicked the plus sign to the left of the Error heading to expand it and display the full list of events in this category. (Expanding the list turns that box into a minus sign, which you can then click to collapse the category again.)

Click to
expand/collapse
a category



To view events that have occurred on your computer, select the appropriate sou
the console tree. The Administrative Events custom view contains all the admini
source. An aggregate view of all the logs is shown below.

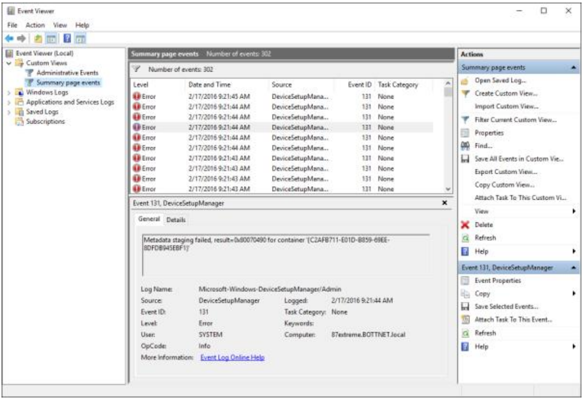
Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour
⊞ Critical	-	-	-	0
⊟ Error	-	-	-	3
	3	FilterManager	System	0
	9	SideBySide	Application	0
	35	SideBySide	Application	0
	69	AppModel-Runtime	Microsoft-Wind...	0
	131	DeviceSetupMana...	Microsoft-Wind...	1
	1000	Application Error	Application	0
	1002	Application Hang	Application	0
	1026	.NET Runtime	Application	0
	1129	GroupPolicy (Micr...	System	1
	3062	Hyper-V-Worker	Microsoft-Wind...	0
	3280	Hyper-V-Worker	Microsoft-Wind...	0
	4000	Hyper-V-Integration	Microsoft-Wind...	0
	5719	NETLOGON	System	1
	5973	Apps	Application	0
	10010	DistributedCOM	System	0
	10016	DistributedCOM	System	0
	12006	Hyper-V-Worker	Microsoft-Wind...	0
⊞ Warning	-	-	-	2
⊞ Informati...	-	-	-	40
⊞ Audit Suc...	-	-	-	75
⊞ Audit Fail...	-	-	-	0

Figure 4-2: You can expand any category in the summary of administrative events to see a detailed breakdown of errors, sorted by Event ID.

Each row in the Summary Of Administrative Events section lists key information about that grouping: the Event ID (a numeric code that you can use to search for technical details and troubleshooting advice), the source of the event, and which log it comes from. The three columns to the right break down the total to show the number of times an event in that category occurred in the past hour, the past 24 hours and the past week.

Double-click any row to open a summary of all the events in that category. Summary Page Events is a predefined custom view that is generated automatically and contains much more granular information (including date and time stamps) about each event in the list. Figure 4-3, for example, shows the full list of events generated by DeviceSetupManager after starting a Windows 10 PC.



Summary page events Number of events: 302

Number of events: 302

Level	Date and Time	Source	Event ID	Task Category
Error	2/17/2016 9:21:45 AM	DeviceSetupMana...	131	None
Error	2/17/2016 9:21:44 AM	DeviceSetupMana...	131	None
Error	2/17/2016 9:21:44 AM	DeviceSetupMana...	131	None
Error	2/17/2016 9:21:44 AM	DeviceSetupMana...	131	None
Error	2/17/2016 9:21:44 AM	DeviceSetupMana...	131	None
Error	2/17/2016 9:21:44 AM	DeviceSetupMana...	131	None
Error	2/17/2016 9:21:43 AM	DeviceSetupMana...	131	None
Error	2/17/2016 9:21:43 AM	DeviceSetupMana...	131	None
Error	2/17/2016 9:21:43 AM	DeviceSetupMana...	131	None
Error	2/17/2016 9:21:43 AM	DeviceSetupMana...	131	None

Event 131, DeviceSetupManager

General Details

Metadata staging failed, result=0x80070490 for container '{C2AFB711-E01D-8859-69EE-8DFDB945EBF1}'

Log Name:	Microsoft-Windows-DeviceSetupManager/Admin		
Source:	DeviceSetupManager	Logged:	2/17/2016 9:21:44 AM
Event ID:	131	Task Category:	None
Level:	Error	Keywords:	
User:	SYSTEM	Computer:	87extreme.BOTTNET.local
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 4-3: Double-clicking any entry in the administrative summary generates a detailed list like this one, chock-full of information you can use to determine whether an error needs more attention.

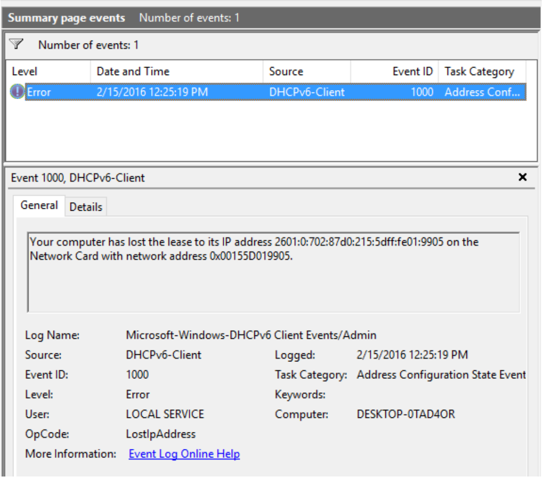
In this example, it's clear that the source of this event, DeviceSetupManager, is not performing as expected. All of the errors visible in that list occurred within seconds of one another. Is this something to be concerned about? As you can see in Figure 4-3, selecting an entry from the list displays its details in the preview pane at the bottom of the Event Viewer window. Use the arrow keys to scroll up and down through the list to quickly get a picture of what these errors have in common.

I was able to use the data from this list—specifically Event ID 131 from the source DeviceSetupManager—to search for further details and confirm that the errors, although annoying in their frequency, were not serious and were probably caused by a problem at the other end of the network, outside of my control.

Don’t lose sleep over harmless errors

Spend enough time using Event Viewer and you’ll discover that its listings are filled with error messages that don’t indicate actual problems. Sometimes the “errors” are simply the result of an app that doesn’t provide Windows with event codes for status messages. As a result, a simple confirmation of, say, a licensing check can turn into an error because Windows can’t find a description to match the event ID. It’s tempting to treat every batch of Event Viewer messages as a mystery to be solved, but for the sake of productivity it’s often just as helpful to know when to ignore those events.

Figure 4-4 shows a different error, from a different source, the DHCPv6 Client. In this case (involving a client computer I was reconfiguring) the error details helped me determine the problem, which was caused by a misconfigured DHCP server on the local network.



Level	Date and Time	Source	Event ID	Task Category
Error	2/15/2016 12:25:19 PM	DHCPv6-Client	1000	Address Conf...

Event 1000, DHCPv6-Client

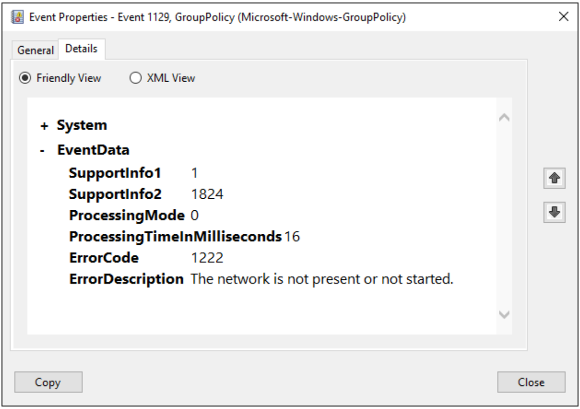
Your computer has lost the lease to its IP address 2601:0:702:87d0:215:5dff:fe01:9905 on the Network Card with network address 0x00155D019905.

Log Name: Microsoft-Windows-DHCPv6 Client Events/Admin
Source: DHCPv6-Client
Logged: 2/15/2016 12:25:19 PM
Event ID: 1000
Task Category: Address Configuration State Event
Level: Error
Keywords:
User: LOCAL SERVICE
Computer: DESKTOP-0TAD4OR
OpCode: LostIpAddress
More Information: Event Log Online Help

Figure 4-4: The preview pane beneath the summary of events shows details for the currently selected event. The General tab usually includes a readable summary of the event.

In that preview pane, you can see two tabs. The General tab provides a (usually) readable description of the error or informational message. Click the Details tab to choose from two additional views—one showing details in a list format, the other displaying the same details in XML format.

You can double-click any event to see it in its own window, with the same choice of General and Details tabs, as shown in Figure 4-5. (When you view an event in a window, use the up and down arrows on the right to scroll between entries; use the Copy button at the bottom to save the full set of event properties to the Windows Clipboard.)


Event Properties - Event 1129, GroupPolicy (Microsoft-Windows-GroupPolicy)
General
Details
Copy
Close

● Friendly View ○ XML View

+ System

- EventData

SupportInfo1 1
SupportInfo2 1824
ProcessingMode 0
ProcessingTimeInMilliseconds 16
ErrorCode 1222
ErrorDescription The network is not present or not started.

Figure 4-5: Opening an event in its own window provides the same views as in the preview pane. The Copy button saves the event details to the Clipboard.

Changing the view

The navigation pane on the left side of Event Viewer contains several nodes, all of them collapsed initially. Expanded, this default collection should look something like what you see in Figure 4-6.

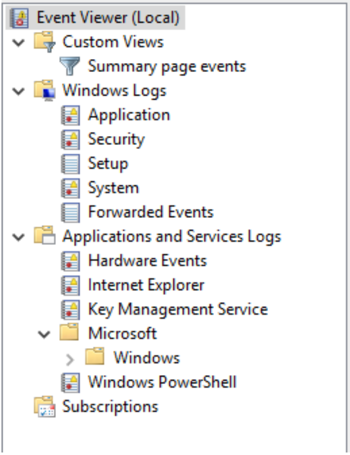


Figure 4-6: You can expand the navigation pane in Event Viewer to see the full contents of a group of event logs. Expand the Windows heading (near the bottom of the list) to see hundreds of special-purpose logs.

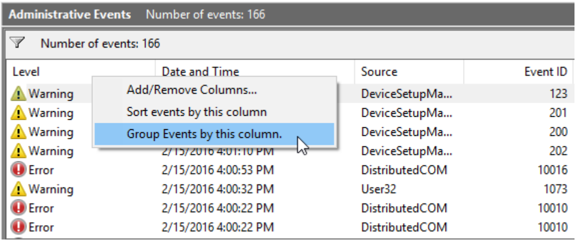
I described the entries under the Windows Logs heading earlier in this chapter, and I'll discuss the

Custom Views heading later. Third-party applications can add entries under the Applications And Services Logs heading to keep track of their own events. By selecting an option on the View menu, it’s possible to expand this list to include Analytic and Debug logs, but these logs are dense, technical, and not of much use for ordinary troubleshooting.

You might notice in Figure 4-6 that I didn’t expand the Windows heading (under Microsoft in the Applications And Services Logs group). That’s because doing so unveils a truly enormous list, containing hundreds of logs covering discrete parts of the Windows operating system. (Even MSPaint has its own event log!) It would probably take several pages just to list all those entries, much less describe them in useful detail.

And for the most part you can safely ignore virtually all of those logs, many of which are turned off and thus will remain empty throughout the useful life of your PC unless you choose to turn them on. You will find some interesting entries in the bunch—the Operational log under Diagnostics-Performance, for example, records an event for every startup and shutdown that takes longer than normal, and is worth looking through if you’re looking for ideas on how to speed up either operation. (The Log Summary at the bottom of the overview page is a more useful place, listing only logs that have had recent activity.)

Unlike the opening summary view, a listing of events in an individual log isn't categorized; instead, it's listed by date. As with other such tabular listings in Windows 10, you can click any column heading to sort by a specific column. You can also group the listing by any heading you choose. Right-click any heading to show a Group By menu. Right-click Level and then select Group Events By This Column, as shown in the graphic that follows, to move events categorized as Error to their own group, below Critical items but above the Warning group.



Administrative Events Number of events: 166

Number of events: 166

Level	Date and Time	Source	Event ID
Warning		DeviceSetupMa...	123
Warning		DeviceSetupMa...	201
Warning		DeviceSetupMa...	200
Warning	2/15/2016 4:01:10 PM	DeviceSetupMa...	202
Error	2/15/2016 4:00:53 PM	DistributedCOM	10016
Warning	2/15/2016 4:00:32 PM	User32	1073
Error	2/15/2016 4:00:22 PM	DistributedCOM	10010
Error	2/15/2016 4:00:22 PM	DistributedCOM	10010

As I mentioned earlier, the default sort order is by the Date And Time column. You might choose to sort by Event ID if you're simply scanning through a list looking for potential issues. You don’t need to open a menu to do that; just double-click the Event ID column heading.

You can also change the width or placement of columns by dragging the headings. (The process is similar to how you customize File Explorer’s Details view, as explained in Chapter 2.)

The standard view of an event log includes five columns. For some specialized tasks you might want to add or remove columns. If you’ve saved logs from multiple computers, for example, you might want to add the Computer column so that you can see at a glance which computer generated a given event. To do that, right-click any column heading and select Add/Remove Columns. That opens the dialog box shown in Figure 4-7, where you can select a column from the left side and click Add. (To reverse the change, select a column name from the right side and click Remove, or use Restore Defaults to get rid of all your customizations.)

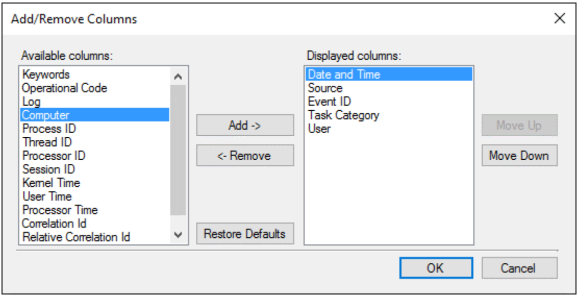


Figure 4-7: As with File Explorer, you can add columns to the display in Event Viewer by using this dialog box.

The Actions pane on the right side is context-sensitive, so options visible there depend on what is currently selected. Actions in the top section apply to the currently open log or view; if one or more events are selected, actions for those events are available in the bottom. Figure 4-8 shows a typical assortment of actions, including options to copy the selected events as a table (essentially a text-based version of what you see in the listing) or as text.

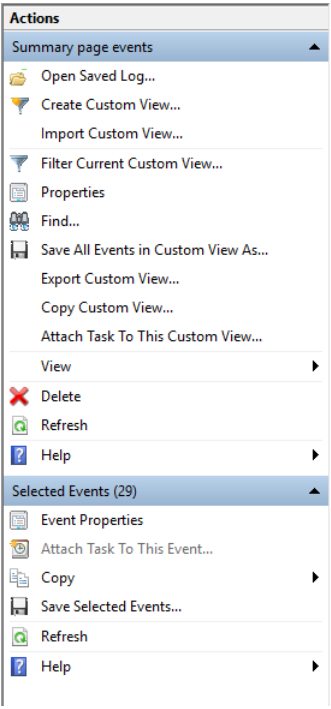


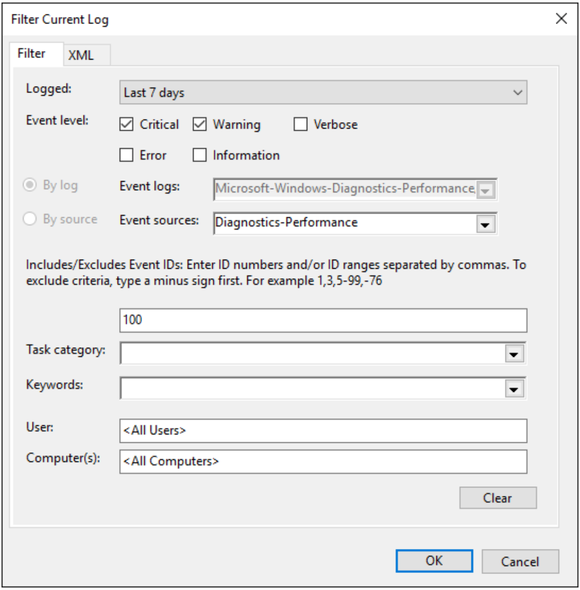
Figure 4-8: The contents of the Actions pane are context-sensitive, with the bottom group visible only if one or more events are selected.

Filtering event logs

The sheer volume of information contained in Windows event logs can be overwhelming. Creating a filter makes it possible for you to zero in on the information you need.

Filters can be a quick way to remove “noise” from an event log. For information that you want to be able to check on quickly, you can save a filter as a custom view.

To create a filter for the current log, click Filter Current Log in the Actions pane. If you’re in a custom view, the corresponding option is Filter Current Custom View. (But note that you can’t filter the built-in custom views, including Summary Page Events.) Figure 4-9 shows a filter I put together. As you can see, it shows only events from the Diagnostics-Performance log, recorded in the last seven days, categorized as Critical or Warning, and having Event ID 100.



Logged: Last 7 days

Event level: ☑ Critical ☑ Warning □ Verbose □ Error □ Information

● By log Event logs: Microsoft-Windows-Diagnostics-Performance

○ By source Event sources: Diagnostics-Performance

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

100

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

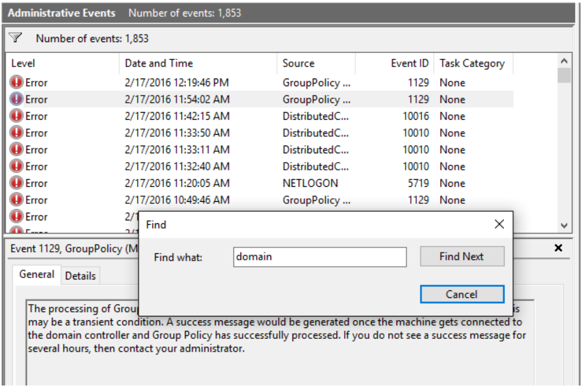
Figure 4-9: This filter zeroes in on events with a specific ID and event level in a specific time period, pinpointing information from a lengthy list that includes hundreds of unrelated entries.

Why Event ID 100? Because that’s the ID for Windows startup times. Event ID 101 is associated with application start times and 200 identifies Windows shutdown times. Using this filter. I can quickly check how long it took

Windows to complete its startup activities for each start in the past week.

To reuse a filter without going through the tedious steps of re-creating its settings, save it as a custom view. I explain how to do that in the next section.

With Event Viewer, you also can find words or values in the current log or view. In the Actions pane, click Find or use the intuitive Ctrl+F keyboard shortcut to open the simple Find box shown in Figure 4-10. Type any text to find the next event containing that text in any field.



Administrative Events Number of events: 1,853

Number of events: 1,853

Level	Date and Time	Source	Event ID	Task Category
Error	2/17/2016 12:19:46 PM	GroupPolicy ...	1129	None
Error	2/17/2016 11:54:02 AM	GroupPolicy ...	1129	None
Error	2/17/2016 11:42:15 AM	DistributedC...	10016	None
Error	2/17/2016 11:33:50 AM	DistributedC...	10010	None
Error	2/17/2016 11:33:11 AM	DistributedC...	10010	None
Error	2/17/2016 11:32:40 AM	DistributedC...	10010	None
Error	2/17/2016 11:20:05 AM	NETLOGON	5719	None
Error	2/17/2016 10:49:46 AM	GroupPolicy ...	1129	None
Error	2/1			

Event 1129, GroupPolicy (M

The processing of Grou is
may be a transient condition. A success message would be generated once the machine gets connected to the domain controller and Group Policy has successfully processed. If you do not see a success message for several hours, then contact your administrator.

Find

Find what: domain

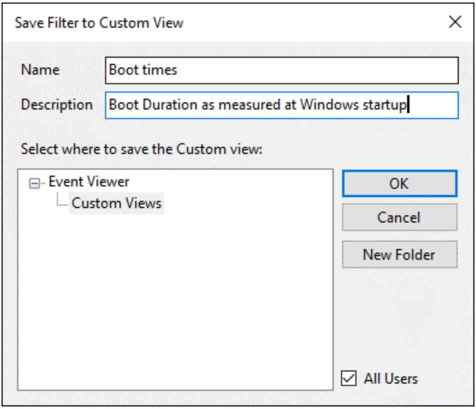
Figure 4-10: Type some text in the Find What box and click Find Next to locate the next event containing

that text in any field, including the source and description.

Creating custom views

Filters are great for finding patterns in an event log. But the process of creating a filter can be a little tedious. For any filter you plan on using again, save your settings as a custom view.

After applying a filter to the current log or custom view, in the Actions pane, click Save Filter To Custom View. That opens a dialog box like the one shown in Figure 4-11, where you can type a name and a description. (This example uses the filter settings I showed earlier in Figure 4-9.)



Save Filter to Custom View

Name: Boot times

Description: Boot Duration as measured at Windows startup

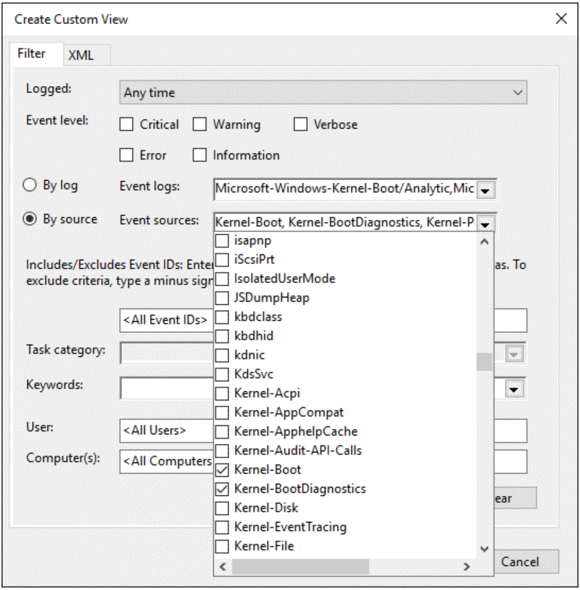
Select where to save the Custom view:

☑ All Users

Figure 4-11: When you save a filter as a custom view, it appears in the Custom Views node. You can add subfolders if you have a large number of saved views.

By default, any custom views you create in Event Viewer are available for all users of the current PC. If you want to reserve a custom view for your use only, clear the All Users check box.

When you start a filter by viewing an existing log or opening a previously saved custom view, its scope is automatically set in the By Log field and can’t be changed. For more flexibility, in the Actions pane, click Create Custom View and create a custom view completely from scratch. With this option, you can choose By Source, as shown in Figure 4-12, with a full list of available sources that includes those that don’t yet have any events recorded. In every other meaningful respect, the filtering options are the same.



Create Custom View

Logged: Any time

Event level: □ Critical □ Warning □ Verbose
□ Error □ Information

○ By log Event logs: Microsoft-Windows-Kernel-Boot/Analytic,Mic

● By source Event sources: Kernel-Boot, Kernel-BootDiagnostics, Kernel-P

□ isapnp
□ iScsiPrt
□ IsolatedUserMode
□ JSDumpHeap
□ kbdclass
□ kbdhid
□ kdnic
□ KdsSvc
□ Kernel-Acpi
□ Kernel-AppCompat
□ Kernel-ApphelpCache
□ Kernel-Audit-API-Calls
☑ Kernel-Boot
☑ Kernel-BootDiagnostics
□ Kernel-Disk
□ Kernel-EventTracing
□ Kernel-File

Includes/Excludes Event IDs: Ente as. To
exclude criteria, type a minus sign

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers

Figure 4-12: When you create a custom view from scratch, you can use the By Source option to specify sources that don’t currently have events recorded.

If you’ve gone to the trouble of creating custom views on one PC, it’s easy to save those views in XML format and import them on a different

Windows 10 device. In the Actions pane, click Export Custom View and save the settings as an XML file. On the destination PC, open Event Viewer and, again in the Actions pane, click Import Custom View, specifying the file you saved earlier.

Copy (and then customize) the Administrative Events view

Although you can't apply a filter to the built-in Administrative Events view (the source of information for the Overview And Summary page), you can make a copy of that view and then filter your copy. In the Navigation pane, in the Custom Views group, choose Administrative Events (if it's not visible, you need to restart Event Viewer using the Run As Administrator option). Then, in the Actions pane, click Copy Custom View. Give your copy a unique name, and then select your newly created copy from the Custom Views list. You can now apply filters and save the results as a custom view.

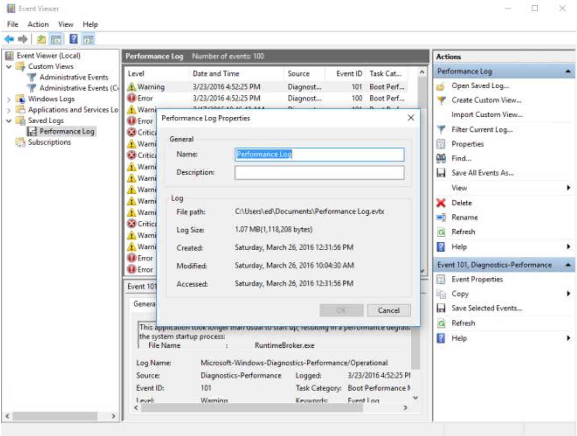
Saving an event log

By using filters and custom views, you can see an up-to-date picture of what Event Viewer has recorded recently. But every event log has a built-in size limit, which means that older events might be discarded. For long-term evaluations, you might want to save the actual content of a particular log or view so that you can review its contents at a later date.

The Save commands are all in the Actions pane.

- To save the full contents of the current log, choose Save All Events As.
- To save the full contents of the current custom view, choose Save All Events In Custom View As.
- To save only the currently selected events from a log or custom view, choose Save Selected Events (from the bottom group in the Actions pane).

The default file type for all of these actions is Event File, with the file name extension .evtx. When you save a file in this format, you can open it with Event Viewer, where its contents appear under the Saved Logs heading. When you open the file, you're prompted to give it a name. You can change that name (and see when the file was created), by right-clicking the entry under the Saved Logs heading, as shown in Figure 4-13.



Level	Date and Time	Source	Event ID	Task Cat...
Warning	3/23/2016 4:52:25 PM	Diagnost...	101	Boot Perf...
Error	3/23/2016 4:52:25 PM	Diagnost...	100	Boot Perf...

Performance Log Properties

General

Name: Performance Log

Description:

Log

File path: C:\Users\ed\Documents\Performance Log.evtx

Log Size: 1.07 MB(1,118,208 bytes)

Created: Saturday, March 26, 2016 12:31:56 PM

Modified: Saturday, March 26, 2016 10:04:30 AM

Accessed: Saturday, March 26, 2016 12:31:56 PM

OK Cancel

Event 101

General

This application took longer than usual to start up, resulting in a performance degrad the system startup process:
File Name : RuntimeBroker.exe

Log Name: Microsoft-Windows-Diagnostics-Performance/Operational
Source: Diagnostics-Performance Logged: 3/23/2016 4:52:25 PI
Event ID: 101 Task Category: Boot Performance I
Level: Warning Keywords: Event Log

Figure 4-13: You can save the contents of any log file or custom view and open that snapshot later. Right-click the entry under Saved Logs and then click Properties to see these details.

The shortcut menu for any custom view or saved log includes a Delete option with which you can remove the entry from the navigation pane. In the case of a custom view, using this option removes the saved settings completely; for a saved log, the .evtx file remains wherever you left it, so you can reopen it whenever you want.

If you've applied a filter to a log or custom view, you can clear it by using the Clear Filter command in the Actions pane.

When you're viewing a log (as opposed to a custom view), you'll see some additional commands in the Actions pane. Clear Log removes all saved entries from the current log. Exercise this command with caution, especially when viewing system-wide logs. Disable Log is available for individual logs under Applications And Services (including third-party additions and those under the Microsoft / Windows heading). In general, there's no need to ever click this.

Now that you’ve read the book...

Tell us what you think!

Was it useful?
Did it teach you what you wanted to learn?
Was there room for improvement?

Let us know at http://aka.ms/tellpress

Your feedback goes directly to the staff at Microsoft Press, and we read every one of your responses. Thanks in advance!

Microsoft

CHAPTER 5

Task Manager

The original Task Manager did exactly what its name suggested, and not much more. Job one for this venerable Windows tool is the occasionally necessary dirty work of closing a program that has stopped responding to normal input.

But Task Manager in Windows 10 does considerably more, providing a veritable Swiss Army knife of features and functions. Yes, you can check details about running tasks and end a process that's stopped responding. But by expanding Task Manager to its full, multitabbed glory, you can see far more details about how your system's resources are being used, including details for each individual process. Do you need to know why your laptop fan is running nonstop? Task Manager is a good place to start.

In this chapter, I also introduce a related system app, Resource Monitor, which is one click away from the Performance tab in Task Manager and offers even more precise performance monitoring options.

Mastering Task Manager

To open Task Manager, right-click any empty space on the taskbar that isn’t occupied by a pinned shortcut and then, on the shortcut menu that appears, click Task Manager. You can also press Ctrl+Alt+Delete to reveal a similar option.

But the easiest route to Task Manager is a keyboard shortcut that’s unfamiliar to most Windows users: Press Ctrl+Shift+Esc. On a standard keyboard layout, those three keys are arranged in a column at the left edge, making the combination easy to remember.

By default, Task Manager’s view is minimalist, as shown in Figure 5-1.

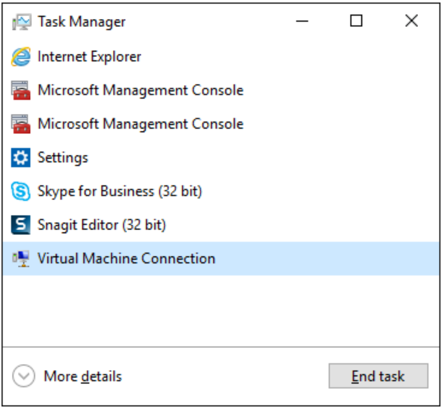
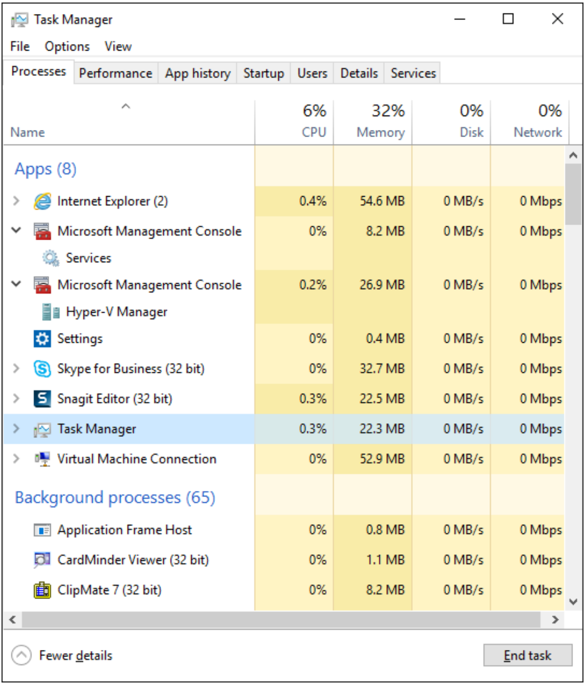

Task Manager
Internet Explorer
Microsoft Management Console
Microsoft Management Console
Settings
Skype for Business (32 bit)
Snagit Editor (32 bit)
Virtual Machine Connection
More details
End task

Figure 5-1: The default view of Task Manager shows only apps and desktop programs started by the current user, along with the option to end a task that isn’t responding.

Click More Details to expand Task Manager into a far more interesting display, with seven tabs. As Figure 5-2 shows, the Processes tab includes the same collection of processes as the default view (which you can return to by clicking Fewer Details), but it also supplies details about child windows as well as four columns of information about system resource usage.



	6%	32%	0%	0%
Name	CPU	Memory	Disk	Network
Apps (8)				
Internet Explorer (2)	0.4%	54.6 MB	0 MB/s	0 Mbps
Microsoft Management Console	0%	8.2 MB	0 MB/s	0 Mbps
Services				
Microsoft Management Console	0.2%	26.9 MB	0 MB/s	0 Mbps
Hyper-V Manager				
Settings	0%	0.4 MB	0 MB/s	0 Mbps
Skype for Business (32 bit)	0%	32.7 MB	0 MB/s	0 Mbps
Snagit Editor (32 bit)	0.3%	22.5 MB	0 MB/s	0 Mbps
Task Manager	0.3%	22.3 MB	0 MB/s	0 Mbps
Virtual Machine Connection	0%	52.9 MB	0 MB/s	0 Mbps
Background processes (65)				
Application Frame Host	0%	0.8 MB	0 MB/s	0 Mbps
CardMinder Viewer (32 bit)	0%	1.1 MB	0 MB/s	0 Mbps
ClipMate 7 (32 bit)	0%	8.2 MB	0 MB/s	0 Mbps

Figure 5-2: After clicking More Details, the Task Manager view expands dramatically.

The End Task button remains, but the display of information is significantly expanded.

The most noticeable addition to the Processes tab is the group of four columns to the right of the list of processes; these columns provide an overview of total system resource usage—CPU, memory, disk, and network—in the column headings. The details to the right of each process show the corresponding activity for that process.

You'll find additional details about running processes, as well. Instead of including just desktop programs and apps, the list is expanded into three groups: Apps, Background Processes, and Windows Processes.

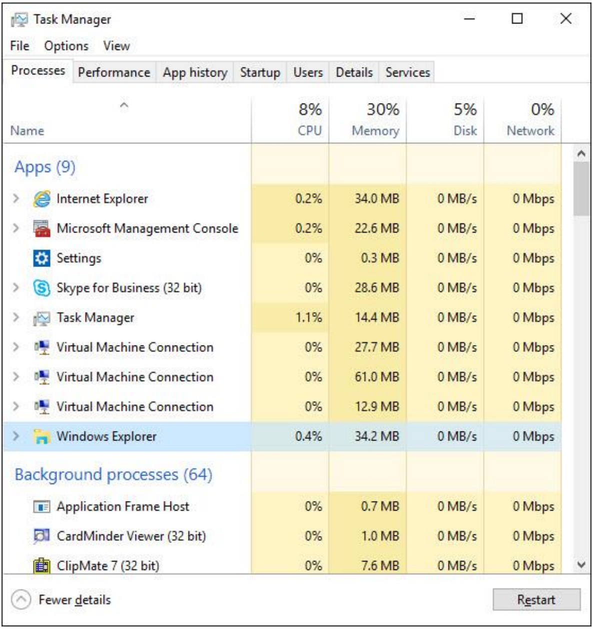
So, what can you do with these expanded listings?

- Click any of the four resource-based headings to sort the list by that column, in descending order. This way, you can see which processes are using the most CPU. (Click again to re-sort in ascending order.) Click the Name heading to restore the sort order by process.
- Click View > Update Speed to choose a faster (High) or slower (Low) rate of polling for system resource usage. Click Pause to temporarily freeze the values so that you can examine them without experiencing sudden changes. Click Refresh Now to update the paused display and show the current values.

- On the View menu, clear the Group By Type check box to see an alphabetical listing of processes without the three groupings.
- Choose any item in the list and click End Task to forcibly stop that process. This action is effective for ending a nonresponsive app (with the inevitable risk that you'll lose unsaved data, of course). Note that you can't forcibly close most individual entries under the Windows Processes heading; for example, if you try to end the Desktop Window Manager task, you'll be prompted to abandon any unsaved data and shut down Windows completely.

One task, Explorer.exe, receives special treatment on the Processes tab. This process, typically listed as Windows Explorer, serves multiple functions. If any File Explorer windows are open, this process is listed under the Apps group. If no File Explorer windows are open, you'll find it under Windows Processes.

In either case, selecting Windows Explorer results in a subtle change to the Task Manager window. The End Task button changes to Restart. Clicking that button (shown in the graphic that follows) forcibly closes any File Explorer windows and restarts the Windows shell.

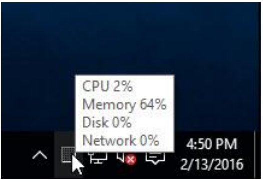


Name	8% CPU	30% Memory	5% Disk	0% Network
Apps (9)				
Internet Explorer	0.2%	34.0 MB	0 MB/s	0 Mbps
Microsoft Management Console	0.2%	22.6 MB	0 MB/s	0 Mbps
Settings	0%	0.3 MB	0 MB/s	0 Mbps
Skype for Business (32 bit)	0%	28.6 MB	0 MB/s	0 Mbps
Task Manager	1.1%	14.4 MB	0 MB/s	0 Mbps
Virtual Machine Connection	0%	27.7 MB	0 MB/s	0 Mbps
Virtual Machine Connection	0%	61.0 MB	0 MB/s	0 Mbps
Virtual Machine Connection	0%	12.9 MB	0 MB/s	0 Mbps
Windows Explorer	0.4%	34.2 MB	0 MB/s	0 Mbps
Background processes (64)				
Application Frame Host	0%	0.7 MB	0 MB/s	0 Mbps
CardMinder Viewer (32 bit)	0%	1.0 MB	0 MB/s	0 Mbps
ClipMate 7 (32 bit)	0%	7.6 MB	0 MB/s	0 Mbps

This feature is especially useful if, for whatever reason, the Windows shell is no longer responding to mouse clicks or keyboard input. Because Task Manager runs at a higher priority than the shell, you can use the Ctrl+Shift+Esc process to force the Windows shell to restart.

By default, the Task Manager button is visible on the taskbar even when you minimize it. To allow Task Manager to run without cluttering the taskbar, click Options > Hide When Minimized. (This same menu also offers the Always On Top option; this displays Task Manager above all other windows, which is useful for real-time performance monitoring.)

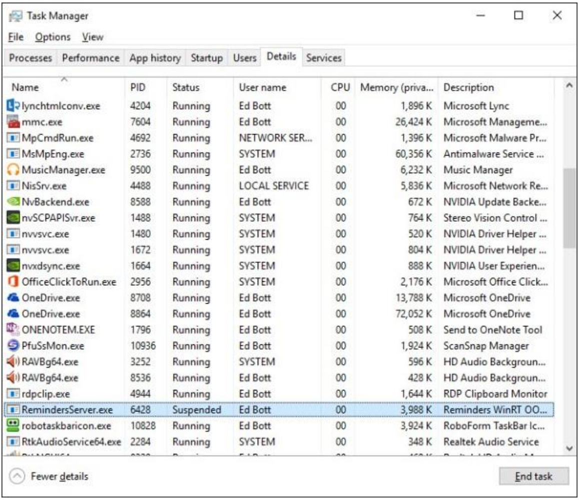
Whenever Task Manager is running, even if you've hidden its taskbar icon, you can see overall details about system resource usage in a graph displayed as an icon in the notification area. Move the mouse pointer over that icon to see details, as shown here:


CPU 2%
Memory 64%
Disk 0%
Network 0%

Digging into the Details tab

The Details tab includes the exact same list of processes that you'll find on the Processes tab, in a more compact tabular format. You can jump to the Details tab directly and scroll through its listings; you can also get to it by right-clicking an entry on the Processes tab and then clicking Go To Details.

As Figure 5-3 shows, the default layout includes seven columns, offering several details you won't find on the Processes tab.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Name	PID	Status	User name	CPU	Memory (priva...	Description
lynchtmlconv.exe	4204	Running	Ed Bott	00	1,896 K	Microsoft Lync
mmc.exe	7604	Running	Ed Bott	00	26,424 K	Microsoft Manageme...
MpCmdRun.exe	4692	Running	NETWORK SER...	00	1,396 K	Microsoft Malware Pr...
MsMpEng.exe	2736	Running	SYSTEM	00	60,356 K	Antimalware Service ...
MusicManager.exe	9500	Running	Ed Bott	00	6,232 K	Music Manager
NisSrv.exe	4488	Running	LOCAL SERVICE	00	5,836 K	Microsoft Network Re...
NvBackend.exe	8588	Running	Ed Bott	00	672 K	NVIDIA Update Backe...
nvSCPAPISvr.exe	1488	Running	SYSTEM	00	764 K	Stereo Vision Control ...
nvvsvc.exe	1480	Running	SYSTEM	00	520 K	NVIDIA Driver Helper ...
nvvsvc.exe	1672	Running	SYSTEM	00	804 K	NVIDIA Driver Helper ...
nvxdsync.exe	1664	Running	SYSTEM	00	888 K	NVIDIA User Experien...
OfficeClickToRun.exe	2956	Running	SYSTEM	00	2,176 K	Microsoft Office Click...
OneDrive.exe	8708	Running	Ed Bott	00	13,788 K	Microsoft OneDrive
OneDrive.exe	8864	Running	Ed Bott	00	72,052 K	Microsoft OneDrive
ONENOTEM.EXE	1796	Running	Ed Bott	00	508 K	Send to OneNote Tool
PfuSsMon.exe	10936	Running	Ed Bott	00	1,924 K	ScanSnap Manager
RAVBg64.exe	3252	Running	SYSTEM	00	596 K	HD Audio Backgroun...
RAVBg64.exe	8536	Running	Ed Bott	00	428 K	HD Audio Backgroun...
rdpclip.exe	4944	Running	Ed Bott	00	1,644 K	RDP Clipboard Monitor
RemindersServer.exe	6428	Suspended	Ed Bott	00	3,988 K	Reminders WinRT OO...
robotaskbaricon.exe	10828	Running	Ed Bott	00	3,924 K	RoboForm TaskBar Ic...
RtkAudioService64.exe	2284	Running	SYSTEM	00	348 K	Realtek Audio Service

Figure 5-3: The Details tab offers much more information about each running process, including the Process ID (PID), which is useful in other troubleshooting tools.

Here’s what to look for in those seven default columns:

- **Name** This column, which cannot be removed from the table layout, shows the name of the executable file associated with the process. In the case of local services, the executable name is Svchost.exe, and it’s normal for multiple instances to appear here. (More on that in the next section.)
- **PID** The Process ID is a number that uniquely identifies an individual process. It’s invaluable for looking up information on the Services tab and in other tools such as Resource Monitor or the command-line Tasklist.exe.
- **Status** As its name implies, this shows the current status of a process. Most Windows processes and desktop apps and services will show Running. Windows 10 apps that are running in the background might show a status of Suspended.
- **User Name** Programs that you run interactively or that start up when you sign in show under your user name in this column. Processes (typically services) that

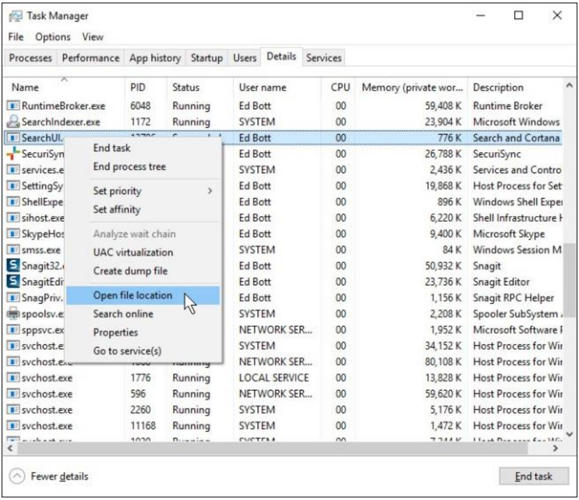
run with higher privileges show which built-in account they're using.

- **CPU** This column is the same as what's displayed under the Processes tab and is governed by the same update pace as those measurements.
- **Memory (Private Working Set)** This column duplicates the information in the matching column on the Processes tab, except that values are displayed in kilobytes instead of megabytes.
- **Description** The text in this column is supplied as metadata (File Description) by the developer of the executable file. It is identical to what appears in the Name column on the Processes tab. To see additional information about a process, including version numbers and date/time stamps, right-click its entry here and then, on the shortcut menu that appears, click Properties, and then click the Details tab.

Why is the System Idle Process using so much of the CPU?

There is one entry that's visible on the Details tab but isn't shown on the Processes tab. The System Idle Process always has a PID of 0 and, despite the name, isn't actually a process at all. Instead, it measures clock cycles when the CPU is not in use by any other processes and thus is idle. Every so often, I hear from readers who checked Task Manager and were alarmed that the System Idle Process was using 90 percent or more of the CPU. This is actually not a cause for concern. In fact, that value indicates how much of the CPU's resources are *not* in use and thus are available for other programs to use. The higher that value, the less strain your CPU is experiencing.

Right-click any process name to see a shortcut menu of additional options, as shown in Figure 5-4.



Name	PID	Status	User name	CPU	Memory (private wor...	Description
RuntimeBroker.exe	6048	Running	Ed Bott	00	59,408 K	Runtime Broker
SearchIndexer.exe	1172	Running	SYSTEM	00	23,904 K	Microsoft Windows
SearchUI.			Ed Bott	00	776 K	Search and Cortana
SecuriSyn			Ed Bott	00	26,788 K	SecuriSync
services.e			SYSTEM	00	2,436 K	Services and Contro
SettingSy			Ed Bott	00	19,868 K	Host Process for Set
ShellExpe			Ed Bott	00	896 K	Windows Shell Expe
sihost.exe			Ed Bott	00	6,220 K	Shell Infrastructure H
SkypeHos			Ed Bott	00	9,400 K	Microsoft Skype
smss.exe			SYSTEM	00	84 K	Windows Session M
Snagit32.			Ed Bott	00	50,932 K	Snagit
SnagitEdi			Ed Bott	00	23,736 K	Snagit Editor
SnagPriv.			Ed Bott	00	1,156 K	Snagit RPC Helper
spoolsv.e			SYSTEM	00	2,208 K	Spooler SubSystem
sppsvc.ex			NETWORK SER...	00	1,952 K	Microsoft Software
svchost.e			SYSTEM	00	34,152 K	Host Process for Wi
svchost.e			NETWORK SER...	00	80,108 K	Host Process for Wi
svchost.exe	1776	Running	LOCAL SERVICE	00	13,828 K	Host Process for Wi
svchost.exe	596	Running	NETWORK SER...	00	59,620 K	Host Process for Wi
svchost.exe	2260	Running	SYSTEM	00	5,176 K	Host Process for Wi
svchost.exe	11168	Running	SYSTEM	00	1,472 K	Host Process for Wi

Figure 5-4: For any process on the Details tab, you can right-click to find the associated file in File Explorer. Other options give you the ability to search for information or inspect properties of the file.

The first option on that menu, End Task, duplicates the button in the lower-right corner. The remaining options in the top three groups are rarely used; you can use the bottom four options to further investigate an unknown process or one that appears to be misbehaving.

Be skeptical of online sources

The Search Online option sends the values from the Name and Description fields to Bing, using your default browser. The results of that search can be wildly uneven, especially for system processes whose names have been repurposed by malware authors. In general, you should prefer information from an official source such as TechNet or MSDN. Some community resources are consistently reliable. My favorites include Stack Overflow (stackoverflow.com) and Bleeping Computer (bleepingcomputer.com). Information in community forums, including official threads at answers.microsoft.com, can be wildly variable. Don't assume that an assertion from a knowledgeable-sounding forum contributor is necessarily accurate.

As with the similar tabular arrangement in File Explorer's Details view, you can change the layout by using a few common tricks:

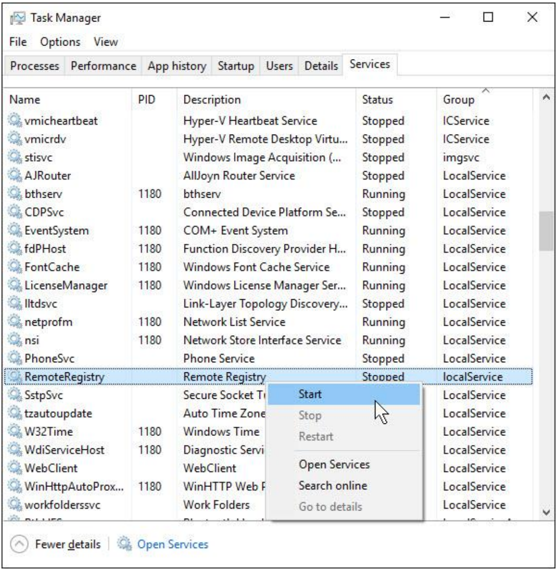
- Drag column headings left or right to rearrange their order.
- Click any heading to sort by that heading. Clicking the CPU or Memory heading, for example, moves processes that are using more of those resources to the top of the

list. Likewise, you can click the User Name heading to group processes that are under the control of the System account or are running in the context of specific local services.

- Right-click any column heading and then choose Select Columns to add or remove columns from the table. The Command Line heading, for example, shows the exact command used to start a process. Here are some other columns worth adding: Platform distinguishes 32-bit and 64-bit processes; Elevated shows processes that are running with administrative privileges; GDI Objects hints at how much of a load a specific process is putting on your graphics processing unit (GPU).
- Right-click any column heading (except Name) and then click Hide Column to remove it from the table.

Investigating services

On the Processes tab, you can expand any Service Host entry to see the individual services running in the context of that process. Opening the Services tab provides a view of all services, running or stopped, with a few extra details you won’t find on the Processes tab. The additional information in this tabular view includes the Process ID for running services as well as the service name (this is useful if you want to use the sc command to manage a service from a command line or script) and the group of which it’s part. As Figure 5-5 shows, you can right-click any listed process to start or stop it.



Name	PID	Description	Status	Group
vmicheartbeat		Hyper-V Heartbeat Service	Stopped	ICService
vmicrdv		Hyper-V Remote Desktop Virtu...	Stopped	ICService
stisvc		Windows Image Acquisition (...	Stopped	imgsvc
AJRouter		AllJoyn Router Service	Stopped	LocalService
bthserv	1180	bthserv	Running	LocalService
CDPSvc		Connected Device Platform Se...	Stopped	LocalService
EventSystem	1180	COM+ Event System	Running	LocalService
fdPHost	1180	Function Discovery Provider H...	Running	LocalService
FontCache	1180	Windows Font Cache Service	Running	LocalService
LicenseManager	1180	Windows License Manager Ser...	Running	LocalService
lltdsvc		Link-Layer Topology Discovery...	Stopped	LocalService
netprofm	1180	Network List Service	Running	LocalService
nsi	1180	Network Store Interface Service	Running	LocalService
PhoneSvc		Phone Service	Stopped	LocalService
RemoteRegistry		Remote Registry	Stopped	localService
SstpSvc		Secure Socket Tı		LocalService
tzautoupdate		Auto Time Zone		LocalService
W32Time	1180	Windows Time		LocalService
WdiServiceHost	1180	Diagnostic Servi		LocalService
WebClient		WebClient		LocalService
WinHttpAutoProx...	1180	WinHTTP Web P		LocalService
workfolderssvc		Work Folders		LocalService

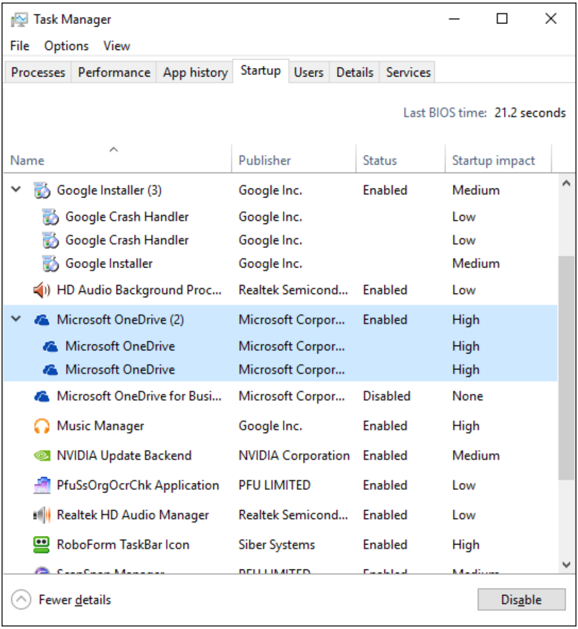
Figure 5-5: The Services tab in Task Manager offers only basic controls for starting, stopping, and restarting services. Click Open Services to use the more powerful Services console.

If you need to pause or resume a service or change its startup behavior, open the Services console (Services.msc) by using the command on that shortcut menu.

Managing startup apps and monitoring resource usage

Apps and services that start automatically when you turn on a PC or sign in to a user account are a mixed blessing. Yes, they’re convenient, but they can also degrade performance. And sometimes there’s just no valid reason for a third-party program to automatically start itself without your consent.

Previous versions of Windows provided crude controls in the System Configuration tool (MSConfig.exe) that you could use to manage many (but not all) of these programs and services. Now, these options, slightly expanded, are available on the Startup tab in Task Manager, as shown in Figure 5-6.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
Disable

Last BIOS time: 21.2 seconds

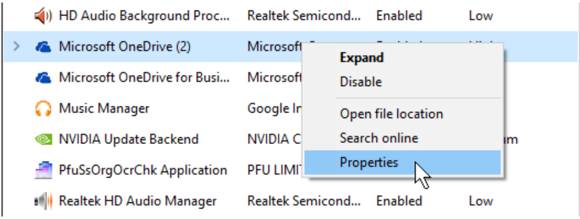
Name	Publisher	Status	Startup impact
Google Installer (3)	Google Inc.	Enabled	Medium
Google Crash Handler	Google Inc.		Low
Google Crash Handler	Google Inc.		Low
Google Installer	Google Inc.		Medium
HD Audio Background Proc...	Realtek Semicond...	Enabled	Low
Microsoft OneDrive (2)	Microsoft Corpor...	Enabled	High
Microsoft OneDrive	Microsoft Corpor...		High
Microsoft OneDrive	Microsoft Corpor...		High
Microsoft OneDrive for Busi...	Microsoft Corpor...	Disabled	None
Music Manager	Google Inc.	Enabled	High
NVIDIA Update Backend	NVIDIA Corporation	Enabled	Medium
PfuSsOrgOcrChk Application	PFU LIMITED	Enabled	Low
Realtek HD Audio Manager	Realtek Semicond...	Enabled	Low
RoboForm TaskBar Icon	Siber Systems	Enabled	High
ScanSnap Manager	PFU LIMITED	Enabled	Medium

Figure 5-6: Use the Disable button to temporarily stop a process from starting automatically.

The Startup Impact column shows a vague estimate of how much drain a particular process puts on your system when it starts. Also unexpectedly useful is a detail that you won’t easily find anywhere else: the Last BIOS Time. On a device with UEFI firmware, expect this value to be less than 5 seconds. Older designs with a conventional BIOS typically take more than 20 seconds to start up.

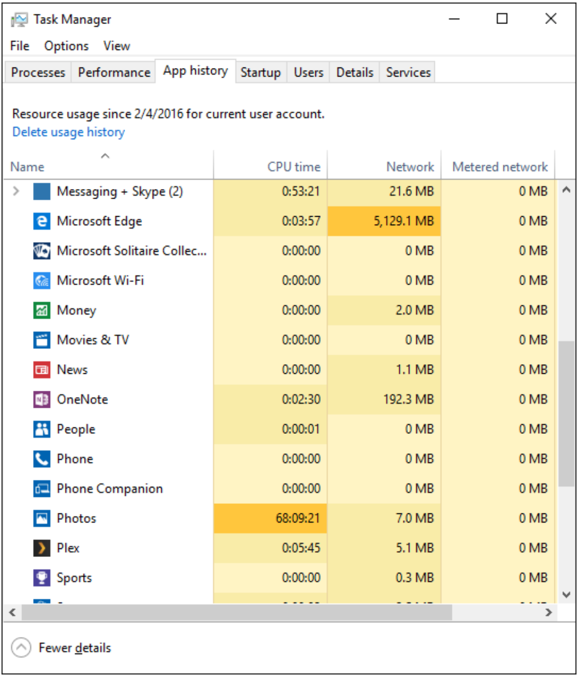
> Although the Windows 10 version of the Startup tab is more capable than earlier versions, it’s not comprehensive. For pinpoint control over programs and services that start automatically, use AutoRuns, one of the free Sysinternals tools. Chapter 7, “Sysinternals Suite,” provides more details about all of these free tools.

For more details about any item in the startup list, you can right-click that item and then, on the shortcut menu, click Properties (see the graphic that follows). Next, click the Details tab to inspect information about the program, including its developer and version number.



HD Audio Background Proc...	Realtek Semicond...	Enabled	Low
Microsoft OneDrive (2)	Microsoft		
Microsoft OneDrive for Busi...	Microsoft		
Music Manager	Google In		
NVIDIA Update Backend	NVIDIA C		m
PfuSsOrgOcrChk Application	PFU LIMI		
Realtek HD Audio Manager	Realtek Semicond...	Enabled	Low

The App History tab shows color-coded values for system resource usage by the current user account and the System account, as shown in Figure 5-7.



Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details

Resource usage since 2/4/2016 for current user account.

Delete usage history

Name	CPU time	Network	Metered network
Messaging + Skype (2)	0:53:21	21.6 MB	0 MB
Microsoft Edge	0:03:57	5,129.1 MB	0 MB
Microsoft Solitaire Collec...	0:00:00	0 MB	0 MB
Microsoft Wi-Fi	0:00:00	0 MB	0 MB
Money	0:00:00	2.0 MB	0 MB
Movies & TV	0:00:00	0 MB	0 MB
News	0:00:00	1.1 MB	0 MB
OneNote	0:02:30	192.3 MB	0 MB
People	0:00:01	0 MB	0 MB
Phone	0:00:00	0 MB	0 MB
Phone Companion	0:00:00	0 MB	0 MB
Photos	68:09:21	7.0 MB	0 MB
Plex	0:05:45	5.1 MB	0 MB
Sports	0:00:00	0.3 MB	0 MB

Figure 5-7: The darker color gradients in the App History listing indicate apps that are using higher levels of a particular resource.

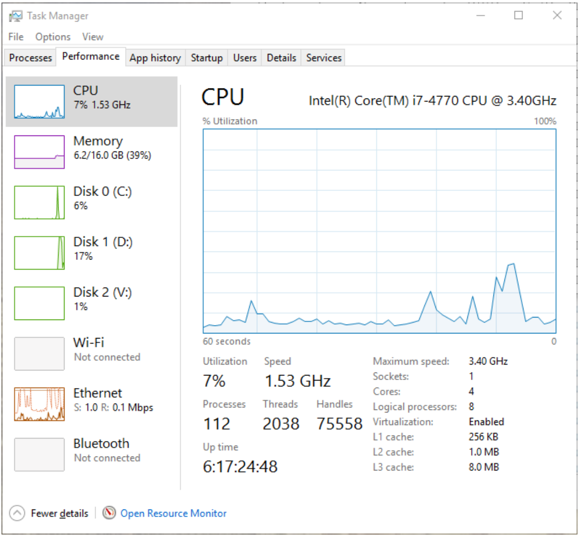
At first glance, this tab might seem useful only for satisfying idle curiosity, but with a few tweaks you can turn its details into actionable information. For example, if you're on a Wi-Fi network that's not marked as metered but where you need to carefully monitor your data usage, try this:

1. Click Options and then click Show History For All Processes. That expands the list to include Windows desktop apps and services.
2. Click Delete Usage History to zero out all of the values.
3. Click the Network heading to sort the list by the amount of data used, in descending order.

Task Manager monitors CPU and network usage in the background regardless of whether it's open. Every so often, you can check the values on this tab to see if any apps are using more data than you expected. If so, you can adjust settings quickly to avoid bumping into a data cap or paying charges for exceeding your limit.

Monitoring performance in real time

You'll find an amazing amount of information on the Performance tab in Task Manager. It's one of the first places I look when I'm trying to chase down a performance issue. Figure 5-8 shows the default interface, which displays many performance details at a glance; but, as I explain in this section, you can find some additional details that are normally hidden, if you know where to look.



Utilization 7%

Speed 1.53 GHz

Processes 112

Threads 2038

Handles 75558

Up time 6:17:24:48

Maximum speed:	3.40 GHz
Sockets:	1
Cores:	4
Logical processors:	8
Virtualization:	Enabled
L1 cache:	256 KB
L2 cache:	1.0 MB
L3 cache:	8.0 MB

Figure 5-8: Each thumbnail in the left pane of the Performance tab is a live graph of that metric. Click a thumbnail to see a larger version with additional details in the pane on the right.

The list of available thumbnails on the left side includes CPU and Memory graphs at the top. The remaining lineup varies depending on your installed hardware. The desktop PC shown in Figure 5-8, for example, is stuffed with storage and networking options, with separate performance graphs for each of three individual physical disks and three network adapters.

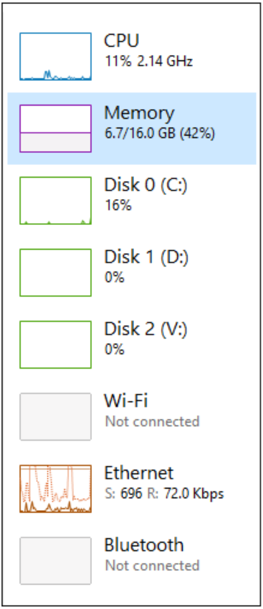
How is the CPU chart useful? Say you’re trying to figure out whether a new device has enough horsepower to handle demanding photo and video editing tasks. Open Task Manager, display the CPU graph on the Performance tab, and then start a CPU-intensive task such as transcoding a video or converting a large batch of raw image files to compressed format.

You can use options on the View menu to change the update speed (or pause it completely) and to keep the Task Manager window on top as you perform a series of tests for which you want to see the response in real time.

Save and share performance details

Would you like to save a snapshot of current performance details for later review? Use the Copy shortcut (Ctrl+C) to save the details displayed below the graph for the current selection. You can then paste those numbers from the Clipboard into a document or an email message. To freeze the display of information at the current moment, click View > Update Speed > Paused. You then can go through each panel in turn, copying its details for the record.

If you just want the overview and don’t need to see the details for the current selection, double-click anywhere on the left side of the Performance tab. That’s a shortcut for right-clicking in the column of thumbnails and choosing Summary View (shown at left in the graphic that follows). For an even more minimal display, right-click and then choose the Hide Graphs option (shown on the right).



CPU
11% 2.14 GHz

Memory
6.7/16.0 GB (42%)

Disk 0 (C:)
16%

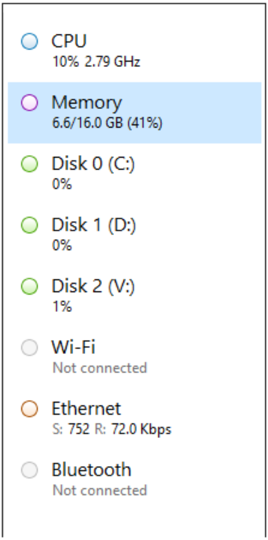
Disk 1 (D:)
0%

Disk 2 (V:)
0%

Wi-Fi
Not connected

Ethernet
S: 696 R: 72.0 Kbps

Bluetooth
Not connected



CPU
10% 2.79 GHz

Memory
6.6/16.0 GB (41%)

Disk 0 (C:)
0%

Disk 1 (D:)
0%

Disk 2 (V:)
1%

Wi-Fi
Not connected

Ethernet
S: 752 R: 72.0 Kbps

Bluetooth
Not connected

Or perhaps you're more interested in simply seeing the real-time performance graph for CPU usage, minus the title bar, menus, the technical details at the bottom, and the column of thumbnails on the left. In that case, double-click the right side of the Performance tab to hide everything except the large real-time graphs. (That's a shortcut for the Graph Summary View option, available when you right-click anywhere on the right side of the tab.) Double-click again to restore the missing details.

Each performance graph has its own set of display options. On the CPU graph, for example, you can right-click to see individual graphs for each logical processor instead of a single graph for overall utilization. Figure 5-9 shows this option in action.

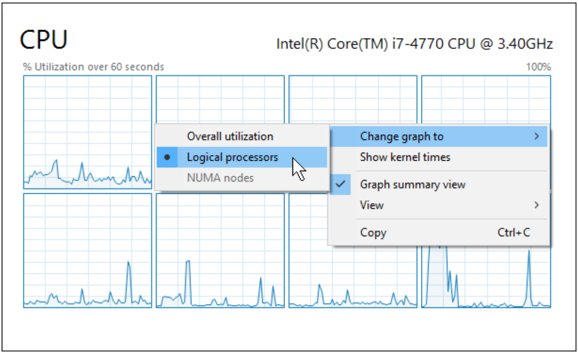
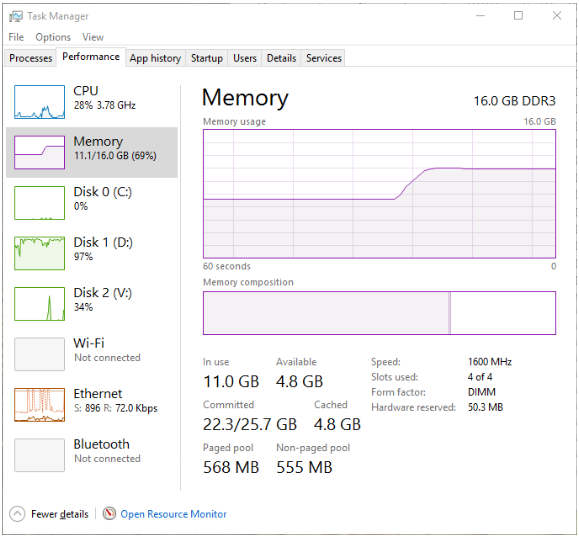


Figure 5-9: You can fine-tune the real-time graph for any of the metrics on the Performance tab. This display, for example, shows eight individual graphs for a quad-core processor with hyper-threading turned on.

The Memory graph is probably the least volatile of the options shown on the Performance tab. Figure 5-10 shows the display shortly after I opened a Hyper-V virtual machine. Notice the spike in memory usage.



CPU
28% 3.78 GHz

Memory
11.1/16.0 GB (69%)

Disk 0 (C:)
0%

Disk 1 (D:)
97%

Disk 2 (V:)
34%

Wi-Fi
Not connected

Ethernet
S: 896 R: 72.0 Kbps

Bluetooth
Not connected

Memory — 16.0 GB DDR3

Memory usage — 16.0 GB

Memory composition

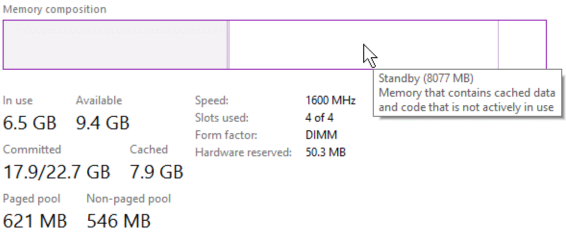
In use	11.0 GB
Available	4.8 GB
Committed	22.3/25.7 GB
Cached	4.8 GB
Paged pool	568 MB
Non-paged pool	555 MB
Speed:	1600 MHz
Slots used:	4 of 4
Form factor:	DIMM
Hardware reserved:	50.3 MB

Figure 5-10: Unlike the other measurements on the Performance tab, you’re unlikely to see wild swings in memory usage; instead, you can expect gradual changes as you open and close programs and large data files.

Several important details appear below the memory graphs, including the most important detail: how much memory is available for use by programs, drivers, and the operating system itself. If you're working on an unfamiliar PC, look to the right of the Available value to see details about the physical RAM, such as speed and form factor. The Slots Used value indicates whether it's possible to expand physical memory without replacing existing modules.

The smaller Memory Composition graph, below the main Memory Usage graph, shows a breakdown by category: In Use, Modified, Standby, and Free. You can move the mouse pointer over one of the blocks to see the amount of memory in that category as well as a Screen tip that defines the category.

This example shows the result after I closed several virtual machines, moving their memory to the Standby category, where it remains cached until the system needs that memory for another task:



Memory composition

Standby (8077 MB)
Memory that contains cached data
and code that is not actively in use

In use
6.5 GB

Available
9.4 GB

Committed
17.9/22.7 GB

Cached
7.9 GB

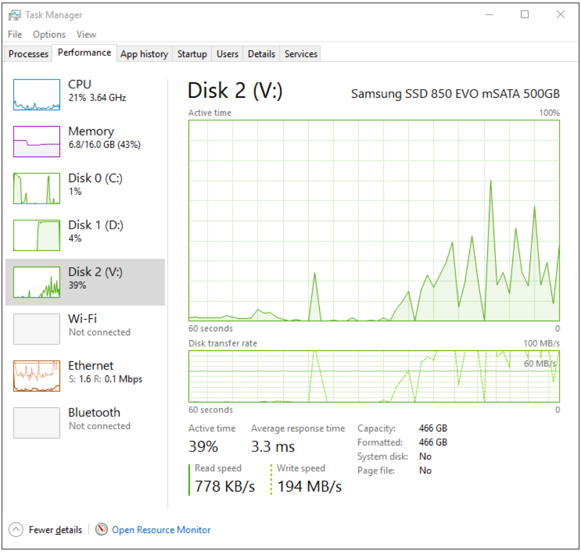
Paged pool
621 MB

Non-paged pool
546 MB

Speed: 1600 MHz
Slots used: 4 of 4
Form factor: DIMM
Hardware reserved: 50.3 MB

On a desktop or laptop PC, the scale of the CPU and Memory graphs never changes. Each graph represents 100 percent of the available CPU or installed memory, respectively, and the placement of the lines indicates what percent of the total is in use at any update.

Figure 5-11 illustrates how each physical disk is represented by a graph on the Performance tab. As with CPU and Memory, the top graph shows what percent of the disk’s total capacity is in use at any given time. In the Disk Transfer Rate graph below the main graph, the scale changes dynamically so that you can see relative changes in activity. For example, on a system that’s not actively performing any strenuous disk activity, the scale might range from 0 to 100 KBps, but if you begin transferring a large file, the scale might change to 100 MBps to reflect the actual workload. (Actual values are determined by the speed of your storage device and storage controller.)



CPU
21% 3.64 GHz

Memory
6.8/16.0 GB (43%)

Disk 0 (C:)
1%

Disk 1 (D:)
4%

Disk 2 (V:)
39%

Wi-Fi
Not connected

Ethernet
S: 1.6 R: 0.1 Mbps

Bluetooth
Not connected

Disk 2 (V:) Samsung SSD 850 EVO mSATA 500GB

Active time
39%

Average response time
3.3 ms

Read speed
778 KB/s

Write speed
194 MB/s

Capacity: 466 GB
Formatted: 466 GB
System disk: No
Page file: No

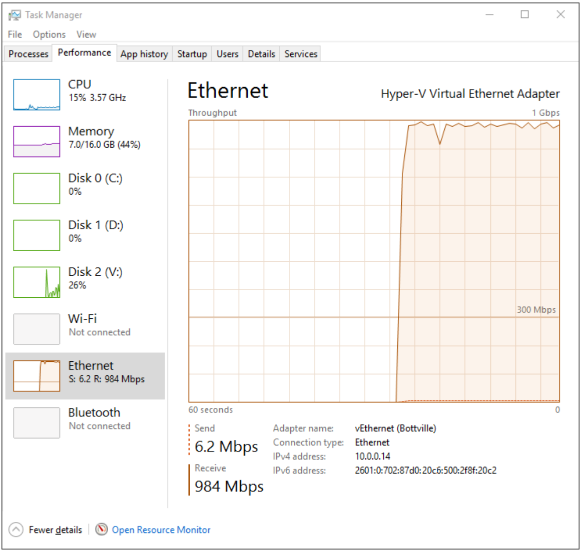
Figure 5-11: The top graph for a physical storage device shows what percentage of its ability to read and write information is in use; the bottom graph shows actual throughput speeds.

The full-sized chart for a network adapter is the only one on the Performance tab that isn't fixed at 100 percent. Instead, as with the smaller disk chart, the scale changes dynamically as network throughput increases or decreases.

Figure 5-12, for example, shows a Gigabit Ethernet adapter in a Hyper-V virtual machine as it goes from no measurable activity to nearly the full capacity of the adapter.

Get your internal IP addresses quickly

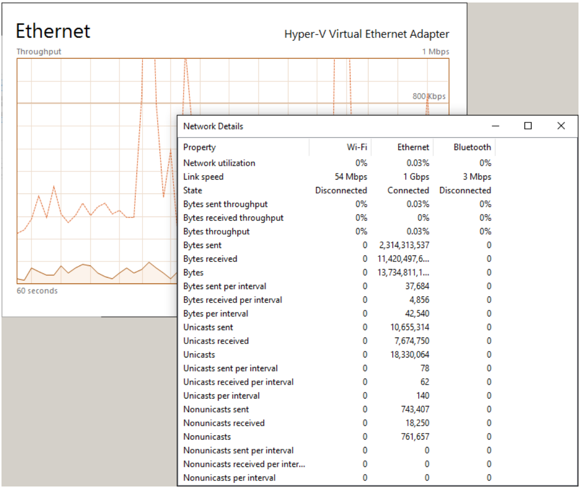
Although there are several ways to find your IP addresses (IPv4 and IPv6), Task Manager is one of the quickest. The details section, located just below the main Network graph on the Performance tab, shows the IP addresses assigned to that adapter. Press Ctrl+C to copy those values to the Clipboard for use elsewhere.



Adapter name: vEthernet (Bottville)
Connection type: Ethernet
IPv4 address: 10.0.0.14
IPv6 address: 2601:0:702:87d0:20c6:500:2f8f:20c2

Figure 5-12: This large incoming file transfer is nearly saturating a Gigabit Ethernet adapter. On a less active connection, the scale changes to make network activity more obvious.

The Network graph is the only one on the Performance tab that offers extremely detailed real-time measurements. Right-click the Throughput chart and then, on the shortcut menu, click View Network Details to see a continuously updating table like the one shown in Figure 5-13.



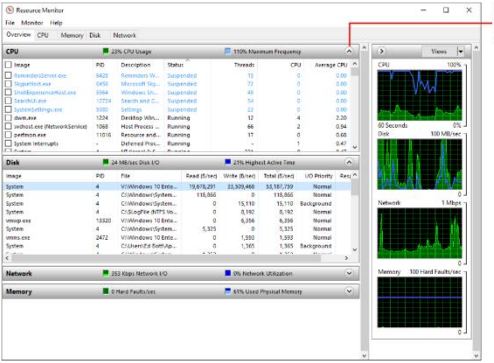
Property	Wi-Fi	Ethernet	Bluetooth
Network utilization	0%	0.03%	0%
Link speed	54 Mbps	1 Gbps	3 Mbps
State	Disconnected	Connected	Disconnected
Bytes sent throughput	0%	0.03%	0%
Bytes received throughput	0%	0%	0%
Bytes throughput	0%	0.03%	0%
Bytes sent	0	2,314,313,537	0
Bytes received	0	11,420,497,6...	0
Bytes	0	13,734,811,1...	0
Bytes sent per interval	0	37,684	0
Bytes received per interval	0	4,856	0
Bytes per interval	0	42,540	0
Unicasts sent	0	10,655,314	0
Unicasts received	0	7,674,750	0
Unicasts	0	18,330,064	0
Unicasts sent per interval	0	78	0
Unicasts received per interval	0	62	0
Unicasts per interval	0	140	0
Nonunicasts sent	0	743,407	0
Nonunicasts received	0	18,250	0
Nonunicasts	0	761,657	0
Nonunicasts sent per interval	0	0	0
Nonunicasts received per inter...	0	0	0
Nonunicasts per interval	0	0	0

Figure 5-13: This well-hidden Network Details table shows continuously updated throughput for all available network adapters, with byte-sized accuracy.

Digging deeper by using Resource Monitor

The Performance tab in Task Manager is useful for watching overall resource usage in real time, but it’s not capable of helping you understand exactly what a given process is doing with system resources.

To get that level of detail, at the bottom of the Performance tab, click Open Resource Monitor. Figure 5-14 shows the Overview tab of Resource Monitor. Thumbnail graphs on the right side show CPU, disk, network, and memory usage in a continuously updated display, while the main window shows four sections with detail for each of those categories.



CPU 🟩 23% CPU Usage 🟦 110% Maximum Frequency

□ Image	PID	Description	Status	Threads	CPU	Average CPU
□ RemindersServer.exe	6428	Reminders W...	Suspended	15	0	0.00
□ SkypeHost.exe	6456	Microsoft Sky...	Suspended	72	0	0.00
□ ShellExperienceHost.exe	5964	Windows Sh...	Suspended	45	0	0.00
□ SearchUI.exe	12724	Search and C...	Suspended	54	0	0.00
□ SystemSettings.exe	9080	Settings	Suspended	23	0	0.00
□ dwm.exe	1224	Desktop Win...	Running	12	4	2.20
□ svchost.exe (NetworkService)	1068	Host Process ...	Running	66	2	0.94
□ perfmon.exe	11016	Resource and...	Running	17	0	0.68
□ System Interrupts	-	Deferred Proc...	Running	-	1	0.47

Disk 🟩 24 MB/sec Disk I/O 🟦 21% Highest Active Time

Image	PID	File	Read (B/sec)	Write (B/sec)	Total (B/sec)	I/O Priority	Res
System	4	V:\Windows 10 Ente...	19,678,291	33,509,468	53,187,759	Normal	
System	4	C:\Windows\System...	118,866	0	118,866	Normal	
System	4	C:\Windows\System...	0	15,110	15,110	Background	
System	4	C:\$LogFile (NTFS Vo...	0	8,192	8,192	Normal	
vmwp.exe	13320	V:\Windows 10 Ente...	0	6,356	6,356	Normal	
System	4	C:\Windows\System...	5,325	0	5,325	Normal	
vmms.exe	2472	V:\Windows 10 Ente...	0	1,593	1,593	Normal	
System	4	C:\Users\Ed Bott\Ap...	0	1,365	1,365	Background	

Network 🟩 353 Kbps Network I/O 🟦 0% Network Utilization

Memory 🟩 0 Hard Faults/sec 🟦 61% Used Physical Memory

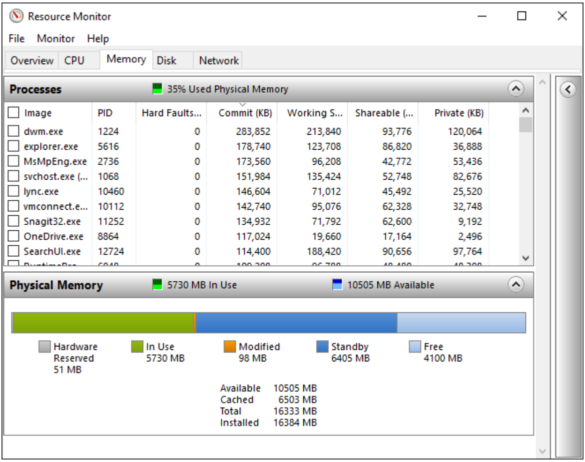
Click to expand or collapse a section

Figure 5-14: The Overview tab in Resource Monitor shows CPU, disk, network, and memory usage at a glance, with the option to filter the display by process.

The Overview tab offers an all-in-one view of system resource usage. Separate tabs to its right give you the ability to zero in on CPU, Disk, Network, and Memory activity, respectively. All of the tabs display activity in a tabular format;

you can drag column headings left or right to change their order, drag a column heading's right edge to change the column's width, and click a heading to sort by that column.

The Memory tab offers a unique map-style view of memory usage. Figure 5-15 shows the color-coded bar chart that represents how much memory is in use and how much is available for use. When you move your mouse pointer over a segment, a Screen tip appears that gives you a definition of the category.



Processes 🟩 35% Used Physical Memory

□ Image	PID	Hard Faults...	Commit (KB)	Working S...	Shareable (...	Private (KB)
□ dwm.exe	1224	0	283,852	213,840	93,776	120,064
□ explorer.exe	5616	0	178,740	123,708	86,820	36,888
□ MsMpEng.exe	2736	0	173,560	96,208	42,772	53,436
□ svchost.exe (...	1068	0	151,984	135,424	52,748	82,676
□ lync.exe	10460	0	146,604	71,012	45,492	25,520
□ vmconnect.e...	10112	0	142,740	95,076	62,328	32,748
□ Snagit32.exe	11252	0	134,932	71,792	62,600	9,192
□ OneDrive.exe	8864	0	117,024	19,660	17,164	2,496
□ SearchUI.exe	12724	0	114,400	188,420	90,656	97,764

Physical Memory 🟩 5730 MB In Use 🟦 10505 MB Available

Hardware Reserved	In Use	Modified	Standby	Free
51 MB	5730 MB	98 MB	6405 MB	4100 MB

Available	10505 MB
Cached	6503 MB
Total	16333 MB
Installed	16384 MB

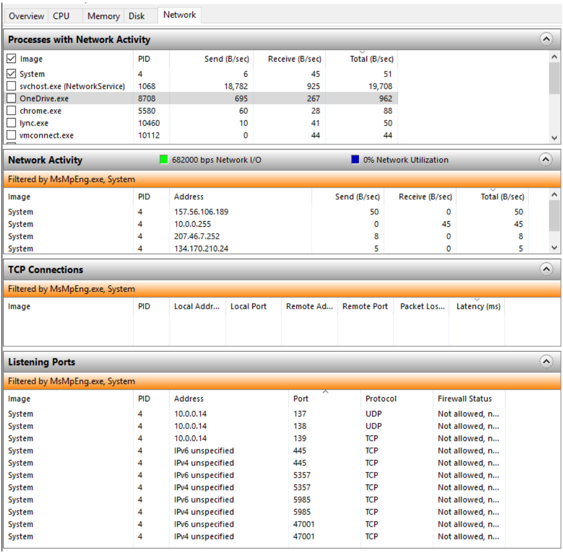
Figure 5-15: The Memory tab, unlike its counterparts, contains a color-coded map showing how much

physical memory is in use and how much is in Standby (cached but not actively in use), and the amount that’s Free.

The most important skill to learn with Resource Monitor is how to filter the results to show just the activity you want to examine.

Note the check boxes alongside each entry in the top section of any tab. Select any of these check boxes to pin the associated process to the top of the list and filter the results below to show only activity for that process. If you select additional processes, the lower sections show activity for all the selected processes.

When you pin one or more processes to the list on one tab, your selection remains pinned as you move to other tabs, even if one or more processes end their activity. In the example shown in Figure 5-16, for example, I selected MsMpEng.exe (the Windows Defender engine) and the System process (PID 4) on the Overview tab. Switching to the Network tab shows detailed network activity, including the IP addresses of active connections.



Processes with Network Activity

☑ Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
☑ System	4	6	45	51
□ svchost.exe (NetworkService)	1068	18,782	925	19,708
□ OneDrive.exe	8708	695	267	962
□ chrome.exe	5580	60	28	88
□ lync.exe	10460	10	41	50
□ vmconnect.exe	10112	0	44	44

Network Activity 🟩 682000 bps Network I/O 🟦 0% Network Utilization

Filtered by MsMpEng.exe, System

Image	PID	Address	Send (B/sec)	Receive (B/sec)	Total (B/sec)
System	4	157.56.106.189	50	0	50
System	4	10.0.0.255	0	45	45
System	4	207.46.7.252	8	0	8
System	4	134.170.210.24	5	0	5

TCP Connections

Filtered by MsMpEng.exe, System

Image	PID	Local Addr...	Local Port	Remote Ad...	Remote Port	Packet Los...	Latency (ms)

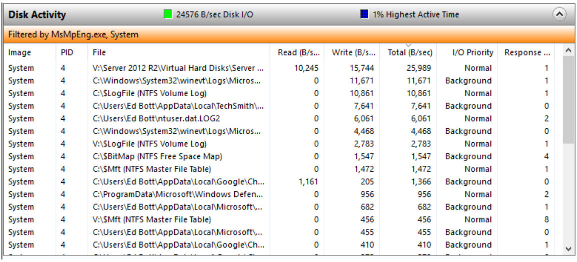
Listening Ports

Filtered by MsMpEng.exe, System

Image	PID	Address	Port	Protocol	Firewall Status
System	4	10.0.0.14	137	UDP	Not allowed, n...
System	4	10.0.0.14	138	UDP	Not allowed, n...
System	4	10.0.0.14	139	TCP	Not allowed, n...
System	4	IPv6 unspecified	445	TCP	Not allowed, n...
System	4	IPv4 unspecified	445	TCP	Not allowed, n...
System	4	IPv6 unspecified	5357	TCP	Not allowed, n...
System	4	IPv4 unspecified	5357	TCP	Not allowed, n...
System	4	IPv6 unspecified	5985	TCP	Not allowed, n...
System	4	IPv4 unspecified	5985	TCP	Not allowed, n...
System	4	IPv6 unspecified	47001	TCP	Not allowed, n...
System	4	IPv4 unspecified	47001	TCP	Not allowed, n...

Figure 5-16: Selecting a check box in the list at the top of any tab filters the display of information below, showing only details from the selected processes.

With that filter in place, you can switch to a different tab and see exactly what the selected processes are doing. The example that follows shows a filtered view of disk activity, with full paths to files with which the System process is interacting. This sort of detail is exceptionally valuable if you're trying to determine, for example, where a third-party program is saving update files or settings.



Disk Activity 🟩 24576 B/sec Disk I/O 🟦 1% Highest Active Time

Filtered by MsMpEng.exe, System

Image	PID	File	Read (B/s...	Write (B/s...	Total (B/sec)	I/O Priority	Response ...
System	4	V:\Server 2012 R2\Virtual Hard Disks\Server ...	10,245	15,744	25,989	Normal	1
System	4	C:\Windows\System32\winevt\Logs\Micros...	0	11,671	11,671	Background	1
System	4	C:\$LogFile (NTFS Volume Log)	0	10,861	10,861	Normal	1
System	4	C:\Users\Ed Bott\AppData\Local\TechSmith\...	0	7,641	7,641	Background	0
System	4	C:\Users\Ed Bott\ntuser.dat.LOG2	0	6,061	6,061	Normal	2
System	4	C:\Windows\System32\winevt\Logs\Micros...	0	4,468	4,468	Background	0
System	4	V:\$LogFile (NTFS Volume Log)	0	2,783	2,783	Normal	1
System	4	C:\$BitMap (NTFS Free Space Map)	0	1,547	1,547	Background	4
System	4	C:\$Mft (NTFS Master File Table)	0	1,472	1,472	Normal	1
System	4	C:\Users\Ed Bott\AppData\Local\Google\Ch...	1,161	205	1,366	Background	0
System	4	C:\ProgramData\Microsoft\Windows Defen...	0	956	956	Normal	2
System	4	C:\Users\Ed Bott\AppData\Local\Microsoft\...	0	682	682	Background	1
System	4	V:\$Mft (NTFS Master File Table)	0	456	456	Normal	8
System	4	C:\Users\Ed Bott\AppData\Local\Microsoft\...	0	455	455	Background	0
System	4	C:\Users\Ed Bott\AppData\Local\Google\Ch...	0	410	410	Background	1

CHAPTER 6

Disk Management

Storage is a core feature of any computing platform, and you don't earn the "IT pro" badge until you master the fine art of managing those bits and bytes. For this task, Windows 10 uses many of the same tools as its predecessors, most notably the Disk Management console.

Even if you're familiar with the fundamentals of Disk Management, I suspect you'll learn some tricks from this chapter. You also might find a few surprising improvements in Windows 10. My favorite? You can shrink a volume, even your system drive, to create space for a new volume. If you ever tried this feature in earlier versions of

Windows, you were undoubtedly tripped up by weird limitations that made the feature virtually unusable (and completely frustrating).

Disk Management is the most important built-in tool in the storage category, but there are a few others, as well. In this chapter, I talk a bit about the command-line DiskPart tool, and I also introduce a few other obscure but occasionally useful built-in apps.

This chapter also discusses BitLocker Drive Encryption, an essential feature that protects business and personal data on both system drives and removable media.

Note For this chapter, I assume that you're already familiar with the basics of managing storage in Windows, such as the difference between NTFS and FAT32 as well as the parts that are independent of Windows: what makes a solid-state drive (SSD) different from a conventional hard drive, for example, as well as how to physically connect a new internal or external drive; If you need a refresher course on this big topic, my coauthors and I devote a full chapter to it in *Windows 10 Inside Out* (Microsoft Press, 2015).

How Windows 10 manages storage

Every Windows 10 device, without exception, has a primary storage device that contains Windows system files and is the default location for programs and data files.

Depending on the hardware design, you can attach other storage devices—internal, external, or virtual—to expand your storage capacity and perform backups. You manage all these storage devices by using the Disk Management console and other tools.

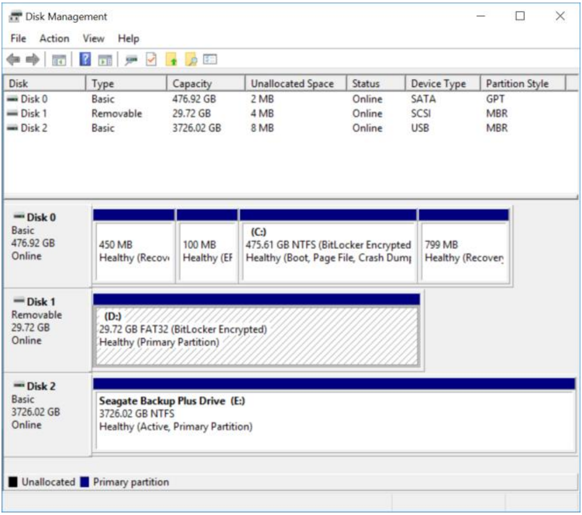
The word *disk*, of course, is a throwback to a bygone era, when every bit of storage ended up on a spinning disk of some sort. Hard disks are still alive and well, although floppy drives have nearly disappeared. CD and DVD drives (writeable and otherwise) are an endangered species. Most modern storage media are disk-free devices that use fast and quiet flash memory: SSDs and portable USB drives, for example, as well as flash-based memory cards (including those that use the MicroSD format that you frequently find in tablets and smartphones). Devices such as phones and portable music players can appear as storage devices when connected to a Windows 10 PC via USB.

In Windows 10, a disk is typically divided into volumes (a term sometimes used interchangeably with partitions). On most desktop and portable PCs, you'll use simple volumes on basic disks. (With Disk Management, you can turn basic disks into dynamic disks and combine physical disks into spanned, striped, mirrored or RAID-5 volumes. If you don't know what that last sentence meant, you probably don't need any of those features.)

Although some Windows 10 features try to hide drive letters (File Explorer libraries, for example), they're never far away. As for file systems, there are very good reasons why your system drive and secondary data drives (internal or external), should use NTFS. For smaller removable storage devices, there are occasionally reasons to use the FAT32 or ExFAT standards, instead.

Disk Management

The star of this chapter is yet another essential tool designed as a snap-in for the Microsoft Management Console. Figure 6-1 shows the layout of a laptop with a 480 GB SSD configured as the system drive and two removable storage devices: a 32 GB card in a MicroSD slot and a 4 TB external drive attached using a USB 3.0 port.



Disk	Type	Capacity	Unallocated Space	Status	Device Type	Partition Style
Disk 0	Basic	476.92 GB	2 MB	Online	SATA	GPT
Disk 1	Removable	29.72 GB	4 MB	Online	SCSI	MBR
Disk 2	Basic	3726.02 GB	8 MB	Online	USB	MBR

Disk 0
Basic
476.92 GB
Online

450 MB
Healthy (Recov

100 MB
Healthy (EF

(C:)
475.61 GB NTFS (BitLocker Encrypted
Healthy (Boot, Page File, Crash Dump

799 MB
Healthy (Recover

Disk 1
Removable
29.72 GB
Online

(D:)
29.72 GB FAT32 (BitLocker Encrypted)
Healthy (Primary Partition)

Disk 2
Basic
3726.02 GB
Online

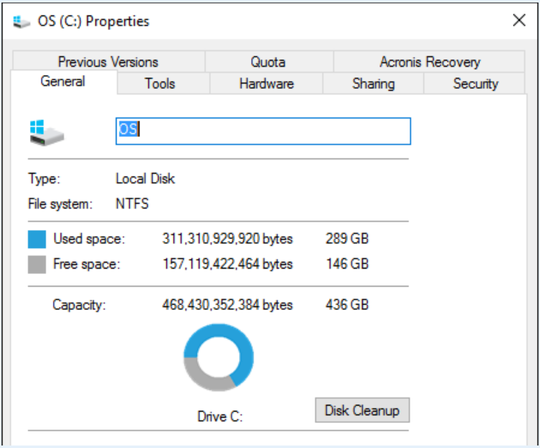
Seagate Backup Plus Drive (E:)
3726.02 GB NTFS
Healthy (Active, Primary Partition)

■ Unallocated ■ Primary partition

Figure 6-1: The graphical view in Disk Management, shown in the bottom pane here, displays details for each attached storage device, with disk details on the left, volumes (not shown to scale) on the right.

Why do storage capacities in Windows 10 always appear smaller than advertised?

If you compare the capacities listed in the previous paragraph to the actual values shown in the graphical pane in Figure 6-1, you'll probably notice that the actual values are smaller than the advertised capacities. You can see the same disparity if you right-click a volume in Disk Management or in File Explorer and then choose Properties. Why has the 480 GB SSD shown here shrunk to a mere 436 GB?

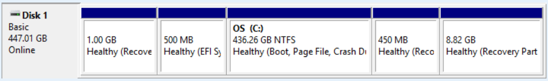


OS (C:) Properties

OS

Type:	Local Disk	
File system:	NTFS	
🟦 Used space:	311,310,929,920 bytes	289 GB
⬜ Free space:	157,119,422,464 bytes	146 GB
Capacity:	468,430,352,384 bytes	436 GB

Some of the missing space is actually in use. As you can see in the details in the screenshot that follows, Disk Management shows the drive’s full capacity as 447.01 GB, with 10.75 GB used for two Windows 10 recovery partitions, an EFI System partition, and the OEM-supplied recovery partition.



Disk 1
Basic
447.01 GB
Online

1.00 GB
Healthy (Recove

500 MB
Healthy (EFI Sy

OS (C:)
436.26 GB NTFS
Healthy (Boot, Page File, Crash Du

450 MB
Healthy (Reco

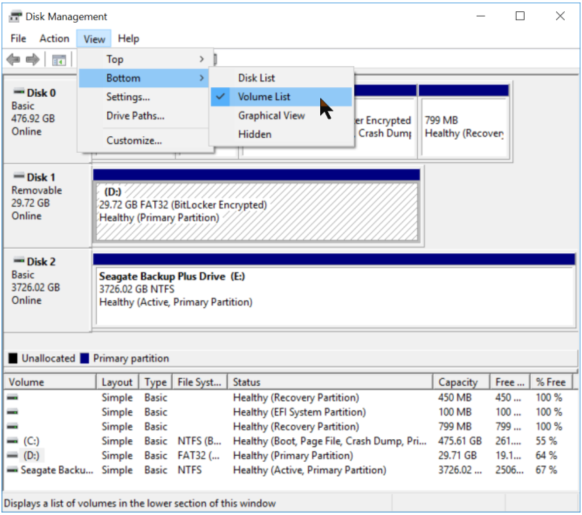
8.82 GB
Healthy (Recovery Part

The remainder of the disparity is simply a difference in arithmetic. Advertised storage capacities are almost always calculated with a GB equaling 1 billion bytes. Inside Windows 10, however, a GB is actually 1024 MB, each of which in turn is 1024 KB, with each KB made up of 1024 bytes. Multiply 447.01 GB (the amount shown in Disk Management) by 1024, then by 1024 again, and then by 1024 one more time, and you end up with nearly exactly 480 billion bytes.

The default layout of Disk Management has two panes, with a list of volumes at the top and a graphical view showing the layout of volumes on a disk below it.

Use the choices on the View menu (see Figure 6-2) to change this arrangement of information.

Here, I've moved the volume list to the bottom pane and changed the top pane to show the graphic view.



Disk 0
Basic
476.92 GB
Online

er Encrypted
Crash Dum

799 MB
Healthy (Recover

Disk 1
Removable
29.72 GB
Online

(D:)
29.72 GB FAT32 (BitLocker Encrypted)
Healthy (Primary Partition)

Disk 2
Basic
3726.02 GB
Online

Seagate Backup Plus Drive (E:)
3726.02 GB NTFS
Healthy (Active, Primary Partition)

Volume	Layout	Type	File Syst...	Status	Capacity	Free ...	% Free
	Simple	Basic		Healthy (Recovery Partition)	450 MB	450 ...	100 %
	Simple	Basic		Healthy (EFI System Partition)	100 MB	100 ...	100 %
	Simple	Basic		Healthy (Recovery Partition)	799 MB	799 ...	100 %
(C:)	Simple	Basic	NTFS (B...	Healthy (Boot, Page File, Crash Dump, Pri...	475.61 GB	261....	55 %
(D:)	Simple	Basic	FAT32 (...	Healthy (Primary Partition)	29.71 GB	19.1...	64 %
Seagate Backu...	Simple	Basic	NTFS	Healthy (Active, Primary Partition)	3726.02 ...	2506...	67 %

Displays a list of volumes in the lower section of this window

Figure 6-2: Use these options on the View menu to change the Disk Management layout, including hiding the bottom pane, if you prefer.

You can use the choices on the Top menu to specify whether you want to see the Disk List, Volume List, or Graphical View when you open Disk Management. The same choices are available for the Bottom menu, along with a fourth option: Specify Hidden for the bottom pane and you can work with a single view in the top pane only.

You can right-click just about any object on this screen to get information about it or to manage its configuration. After connecting a new, never-before-formatted disk, for example, you might be prompted to initialize it. If you skip that option, you can return to it by right-clicking the entry for a disk (on the left side of the graphical view).

You can right-click a volume or a block of unallocated space to create a new volume, delete an existing volume, shrink or extend an existing volume, or change drive letters. Figure 6-3 shows these options for a data volume on a large conventional hard drive.

> **Note** Don’t choose the Format option unless your goal is to erase all of the data on the selected volume.)

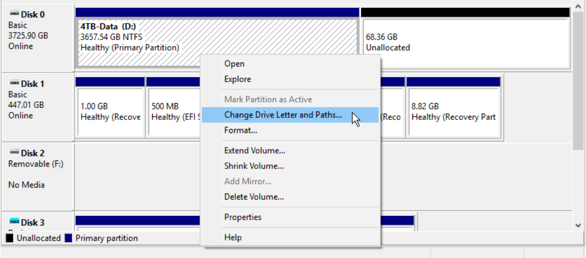


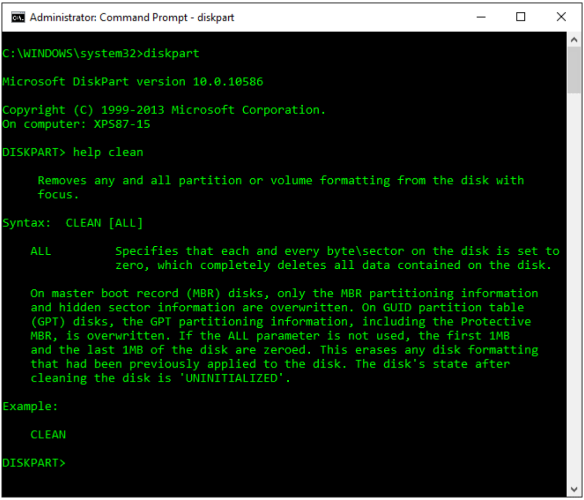
Figure 6-3: Right-click any volume in Disk Management to open this shortcut menu, which contains a wide range of options, some of them destructive.

I cover all these options later in this chapter.

Diskpart

Almost everything that you can do in the Disk Management console you can also accomplish from an elevated Command Prompt window, using the DiskPart tool.

DiskPart is slightly different from most other command-line tools in Windows 10, in that it doesn’t operate by executing with switches. Instead, running the **diskpart** command starts a new environment with its own prompt. From the DISKPART> prompt, type **help** to see a full list of available commands. Type **help** **<*command_name*>** to get instructions for the use of that command. Figure 6-4 shows this help text for the Clean command.

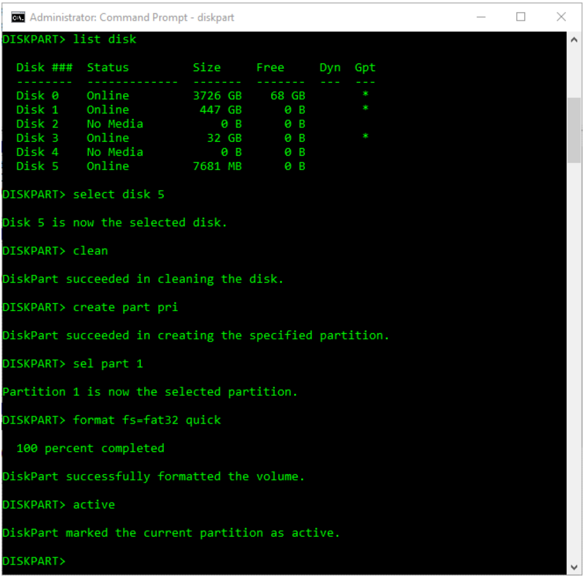


```
C:\WINDOWS\system32>diskpart

Microsoft DiskPart version 10.0.10586

Copyright (C) 1999-2013 Microsoft Corporation.
On computer: XPS87-15

DISKPART> help clean

     Removes any and all partition or volume formatting from the disk with
     focus.

Syntax:  CLEAN [ALL]

    ALL         Specifies that each and every byte\sector on the disk is set to
                zero, which completely deletes all data contained on the disk.

    On master boot record (MBR) disks, only the MBR partitioning information
    and hidden sector information are overwritten. On GUID partition table
    (GPT) disks, the GPT partitioning information, including the Protective
    MBR, is overwritten. If the ALL parameter is not used, the first 1MB
    and the last 1MB of the disk are zeroed. This erases any disk formatting
    that had been previously applied to the disk. The disk's state after
    cleaning the disk is 'UNINITIALIZED'.

Example:

    CLEAN

DISKPART>
```

Figure 6-4: A DiskPart session has its own custom prompt and a peculiar syntax. Use the Help command to get instructions for a particular command.

The way DiskPart works can be a bit confusing. To clean a disk, for example, you first must select the disk by number. After creating one or more partitions, you need to select a partition, again by number, to use the **format** command. After every selection and action, DiskPart gives you a confirmation message.

Figure 6-5 shows the string of commands I needed to type to erase an 8 GB USB drive, create a new primary partition, format it as FAT32 (so that it will boot on a UEFI-based system), and then make the volume active so that it will start. Note that the sequence begins with the **list disk** command; this way I can identify the number of the disk that I need to select.



```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online         3726 GB    68 GB        *
  Disk 1    Online          447 GB     0 B         *
  Disk 2    No Media          0 B      0 B
  Disk 3    Online           32 GB     0 B         *
  Disk 4    No Media          0 B      0 B
  Disk 5    Online         7681 MB     0 B

DISKPART> select disk 5

Disk 5 is now the selected disk.

DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART> create part pri

DiskPart succeeded in creating the specified partition.

DISKPART> sel part 1

Partition 1 is now the selected partition.

DISKPART> format fs=fat32 quick

  100 percent completed

DiskPart successfully formatted the volume.

DISKPART> active

DiskPart marked the current partition as active.

DISKPART>
```

Figure 6-5: Every command in this sequence is followed by a confirmation message from DiskPart. Be very careful to select the correct drive number before using the Clean and Format commands to wipe it.

Eagle-eyed readers will note that I abbreviated some commands in that sequence. DiskPart will recognize a command as long as you type at least three characters, so **cre par pri** and **create part pri** have the same effect as **create primary partition**.

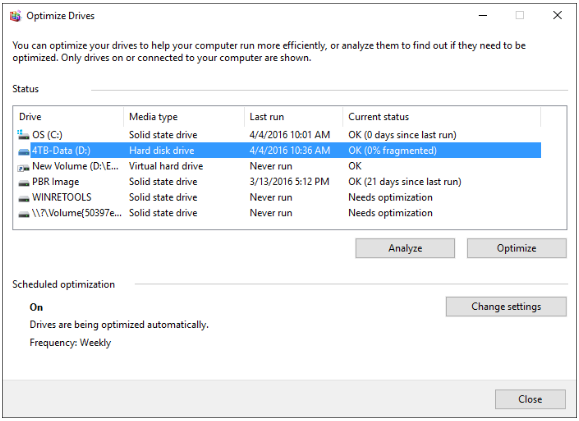
To end the DiskPart session, use the **exit** command.

Other useful storage-related tools

There are plenty of tools that help you to perform specific tasks on storage devices in Windows 10. One option that will be vaguely familiar to longtime Windows users is the Microsoft Drive Optimizer (dfrgui.exe), which appears under Administrative Tools as Defragment And Optimize Drives.

Once upon a time, defragmenting a hard disk was a time-consuming but thoroughly necessary maintenance task. Solid-state drives, which store data using a completely different set of technologies from conventional hard disks, don't need regular "defragging" but do occasionally need to shuffle large files and mark the pages of memory used by deleted files for cleanup.

Figure 6-6 shows the Drive Optimizer in action. Note that volumes located on a solid-state drive are properly identified under the Media Type heading. If you select the OS volume and click Optimize, you’ll see a series of progress messages as the operation takes place (very quickly) under the Current Status heading: “73% trimmed,” for example.



You can optimize your drives to help your computer run more efficiently, or analyze them to find out if they need to be optimized. Only drives on or connected to your computer are shown.

Status

Drive	Media type	Last run	Current status
OS (C:)	Solid state drive	4/4/2016 10:01 AM	OK (0 days since last run)
4TB-Data (D:)	Hard disk drive	4/4/2016 10:36 AM	OK (0% fragmented)
New Volume (D:\E...	Virtual hard drive	Never run	OK
PBR Image	Solid state drive	3/13/2016 5:12 PM	OK (21 days since last run)
WINRETOOLS	Solid state drive	Never run	Needs optimization
\\?\Volume{50397e...	Solid state drive	Never run	Needs optimization

Scheduled optimization

On

Drives are being optimized automatically.

Frequency: Weekly

Figure 6-6: The Microsoft Drive Optimizer tool can distinguish between hard disks, which need defragmenting, and SSDs, which just need to run the Trim command.

Another fascinating tool is Storage Spaces. You can use this feature to combine multiple drives into a single virtual volume, managed by Windows 10. This capability is most useful on server hardware, on which you can easily add multiple drives and combine them to create a massive amount of storage. You'll find a more detailed discussion of Storage Spaces in *Windows 10 Inside Out*.

Common Disk Management tasks

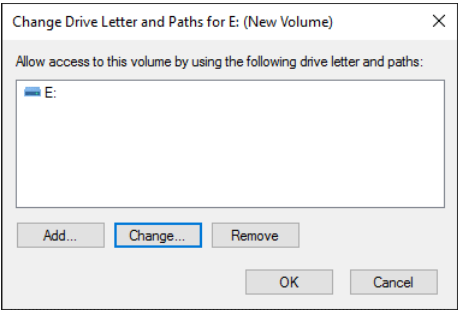
As I mentioned earlier, to get information about a disk or a volume, right-click its listing in Disk Management and then, on the shortcut menu that opens, choose Properties. The resulting dialog box shows free space and used space, in the exact same format you would see if you had checked the disk properties from This PC in File Explorer. That properties dialog box contains a big button that runs the Disk Cleanup tool, with more buttons on a separate Tools tab for other tasks.

This section contains a rapid-fire list of other things you can do from within Disk Management.

Change a drive letter

Unless you performed actual magic spells at setup time (and if so, I tip my hat to your wizardry), your system drive is assigned the letter C. I do not recommend changing that drive letter. For all other drives, including secondary data drives and removable media drives, Windows 10 automatically assigns drive letters starting with D and going all the way up to Z.

You might prefer to change the drive letter assigned to a particular device. Maybe you regularly switch between two desktop systems and want to avoid confusion by assigning the same letter to the DVD drive and external File History drives on each one. Or maybe you just like seeing X: in File Explorer. Whatever the reason, you need only to right-click the volume from Disk Management and then, on the shortcut menu, choose Change Drive Letters And Paths.



Change Drive Letter and Paths for E: (New Volume)

Allow access to this volume by using the following drive letter and paths:

E:

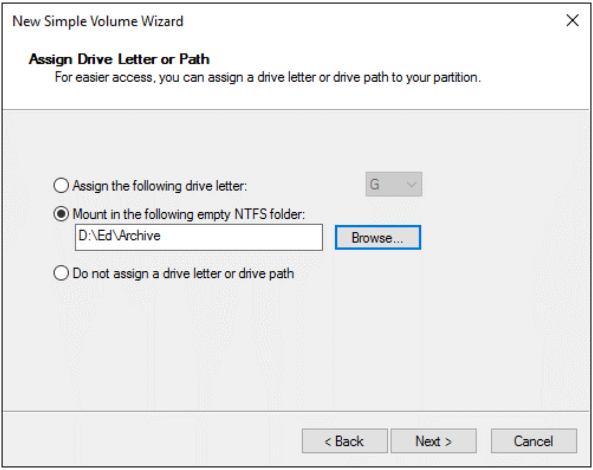
Figure 6-7: Click Change to display a list of available letters to use in place of the current drive letter. To free a drive letter for use on another device, click Remove.

Click Change to choose from a list of unassigned drive letters. (If you want to assign a drive letter that is already in use, you need to right-click the volume currently using that letter and then choose Remove to make the drive letter available.)

Map a new disk to a folder

Using one little-known trick, you can add a new volume (formatted as NTFS) to a system and then assign its storage to an existing folder. Maybe the system drive on your desktop PC is getting full, and you've added a new, larger hard disk to the system. You've created a new, empty subfolder in your user profile called Archive, and you'd like anything you place in that folder to be stored on the newly added drive. Easy.

In Disk Management, right-click the empty space on the disk you just added and then, on the shortcut menu, choose New Simple Volume. Follow the wizard's steps and, after specifying the size of the volume, you should see the page shown in Figure 6-8. Choose Mount In The Following Empty NTFS Folder, click the Browse button to specify the folder that you want to map to this location, and then finish the wizard.



New Simple Volume Wizard

Assign Drive Letter or Path

For easier access, you can assign a drive letter or drive path to your partition.

○ Assign the following drive letter: G

● Mount in the following empty NTFS folder: D:\Ed\Archive

○ Do not assign a drive letter or drive path

Figure 6-8: Instead of (or in addition to) assigning a drive letter, you can mount a new volume so that its contents appear in a folder on an existing drive.

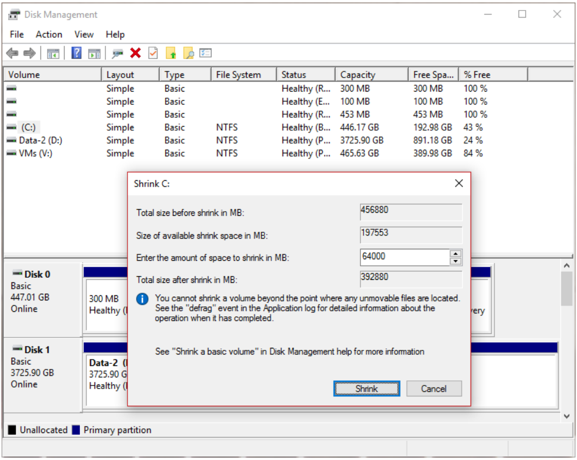
If you've already created the volume, this same option is available: right-click, choose Change Drive Letters And Paths, and then click Add.

Shrink a volume

Why would you want to remove storage space from a perfectly good drive? I can think of several good reasons. You have only one physical disk, but you want to install a second copy of Windows (or another operating system) in a dual-boot configuration. Or you've upgraded your primary system drive to a gigantic multi-terabyte hard drive and you want to create a separate logical drive for keeping your data separate from the operating system. (That makes image backups easier and also makes it possible to reset Windows 10 without worrying about loss of data.)

In either case, assuming that you have sufficient unused space on the physical disk, you should be able to shrink the current volume and then create a new volume on the newly freed empty space.

To begin, right-click the existing volume in Disk Management and then choose Shrink Volume. That opens a dialog box like the one shown in Figure 6-9. In this example, Disk Management told me that I had more than 190 GB of free space to use for shrinking, but for this example I really only need a 64 GB drive, so I clicked Enter The Amount Of Space To Shrink In MB and changed the value to 64000.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
	Simple	Basic		Healthy (R...	300 MB	300 MB	100 %
	Simple	Basic		Healthy (E...	100 MB	100 MB	100 %
	Simple	Basic		Healthy (R...	453 MB	453 MB	100 %
(C:)	Simple	Basic	NTFS	Healthy (B...	446.17 GB	192.98 GB	43 %
Data-2 (D:)	Simple	Basic	NTFS	Healthy (P...	3725.90 GB	891.18 GB	24 %
VMs (V:)	Simple	Basic	NTFS	Healthy (P...	465.63 GB	389.98 GB	84 %

Shrink C:

Total size before shrink in MB: 456880

Size of available shrink space in MB: 197553

Enter the amount of space to shrink in MB: 64000

Total size after shrink in MB: 392880

You cannot shrink a volume beyond the point where any unmovable files are located. See the "defrag" event in the Application log for detailed information about the operation when it has completed.

See "Shrink a basic volume" in Disk Management help for more information

Disk 0
Basic
447.01 GB
Online

300 MB
Healthy (

Disk 1
Basic
3725.90 GB
Online

Data-2 (I
3725.90 G
Healthy (

Figure 6-9: If you have sufficient free space, you can shrink an existing volume, creating unallocated space that you can turn into a separate volume with its own drive letter.

Click Shrink to begin the process of consolidating the existing data and adding empty space to the right of the existing volume.

Now, this all might seem pretty ho-hum. But if you ever tried using this feature in earlier versions of Windows, you probably remember being frustrated to discover that you could actually use only a small fraction of the free space on a volume, thanks to unmovable system files. That limitation appears to be gone as of Windows 10, and you can use the entire free space if you want,

From that unallocated space, you can right-click to create a new simple volume, or start from Windows installation media and specify the freshly freed-up space as the destination for the new installation. If your second installation is also running Windows 10, the installer automatically creates a nifty boot menu on which you can choose which copy you want to run.

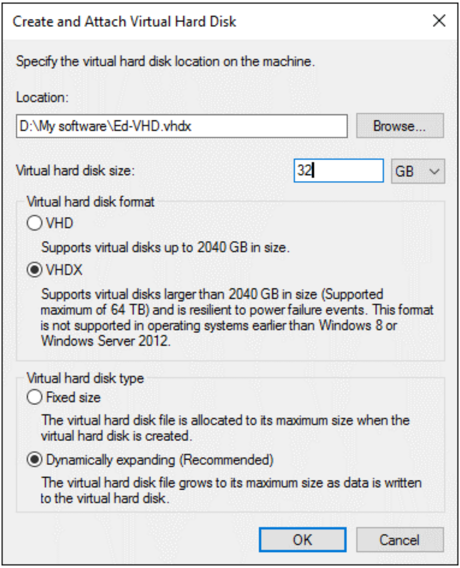
Create a virtual hard disk and attach it as a drive

You can use one genuinely obscure but useful feature in Disk Management to create a Virtual

Hard Disk (VHD) file and double-click to mount it as if it were a separate physical drive, with its own drive letter. One good use of this feature is to create an instant data drive that you can move between virtual machines in Hyper-V (see Chapter 10 for more details on setting up and using Hyper-V).

You can stuff a VHD with as many files as it will hold and move it between physical PCs, as well. So, if you have a collection of downloaded software, document templates, corporate resources, or anything that you frequently want to move between devices, consider a VHD.

To create one, from Disk Management, click Action, Create VHD. That opens a dialog box like the one shown in Figure 6-10, where you can specify the format of your VHD. The choices are pretty straightforward: Specify where you want the VHD file to be saved, and give the file a descriptive name; specify a virtual hard disk format (VHD if you need compatibility with Windows 7, VHDX if you'll only ever need to mount it on a physical or virtual PC running Windows 10, Windows 8.1, or Windows Server 2012 or later).



Create and Attach Virtual Hard Disk

Specify the virtual hard disk location on the machine.

Location:

D:\My software\Ed-VHD.vhdx

Virtual hard disk size: 32 GB

Virtual hard disk format

○ VHD

Supports virtual disks up to 2040 GB in size.

● VHDX

Supports virtual disks larger than 2040 GB in size (Supported maximum of 64 TB) and is resilient to power failure events. This format is not supported in operating systems earlier than Windows 8 or Windows Server 2012.

Virtual hard disk type

○ Fixed size

The virtual hard disk file is allocated to its maximum size when the virtual hard disk is created.

● Dynamically expanding (Recommended)

The virtual hard disk file grows to its maximum size as data is written to the virtual hard disk.

Figure 6-10: Caption

In general, I recommend choosing the Dynamically Expanding option, which allows the VHD file to be only as large as the data you've stored on it, making it easy to move between PCs. After the VHD is created, Disk Management automatically adds it, assigning the next available drive letter. You can detach the VHD by selecting it in Disk Management and using the corresponding option on the Action menu.

Wipe a drive clean

One task that Disk Management does not do particularly well is wiping a drive clean when you're getting ready to give away, sell, or transfer a PC. Formatting a drive leaves behind data that third-party disk utility software can recover in whole or in part. The solution is to open an elevated Command Prompt window and use the Cipher tool with the /W (for Wipe) switch. That erases all blank space on the drive, replacing it with zeroes and making the drive's contents unrecoverable.

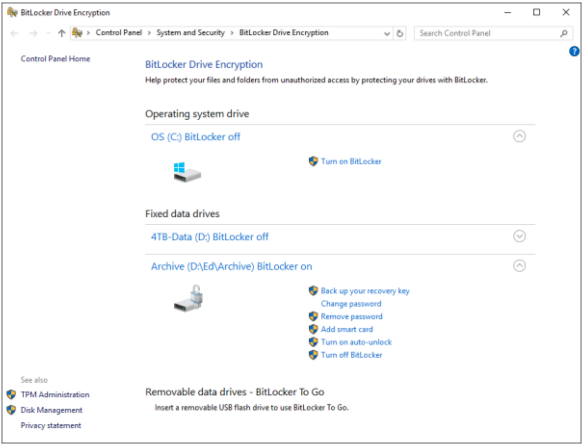
BitLocker Drive Encryption

One of the most important storage capabilities in Windows 10 is its support for enterprise-grade data security using the BitLocker Drive Encryption technology. This feature is available in Windows 10 Pro, Enterprise, and Education editions and should be a must on any device that you take outside of your home or locked office when you travel.

BitLocker Drive Encryption uses AES 256-bit encryption that renders the contents of your system drive (and other drives if you so choose) unreadable except to someone who can successfully sign in with your credentials. If you've chosen a sufficiently strong password, that's excellent protection against someone stealing your portable device, booting from removable media, and then using disk tools to rummage through your secrets. If your organization uses smartcards, BitLocker can require that you unlock the drive with a smart card and a PIN, making it impossible for a thief to gain access even if he has your password.

To use BitLocker to encrypt your system drive, your PC must have a Trusted Platform Module (TPM) chip, which is standard these days on most portable PCs sold for business use. (It's possible to use Group Policy to turn on BitLocker without a TPM, but I recommend against it.) You can use BitLocker on nonsystem drives and removable drives even without a TPM.

To use any of these forms of encryption, sign in with an administrator account, type **encryption** in the taskbar search box, and then click the Manage BitLocker shortcut. That opens a dialog box like the one shown in Figure 6-11.



BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

OS (C:) BitLocker off

Fixed data drives

4TB-Data (D:) BitLocker off

Archive (D:\Ed\Archive) BitLocker on

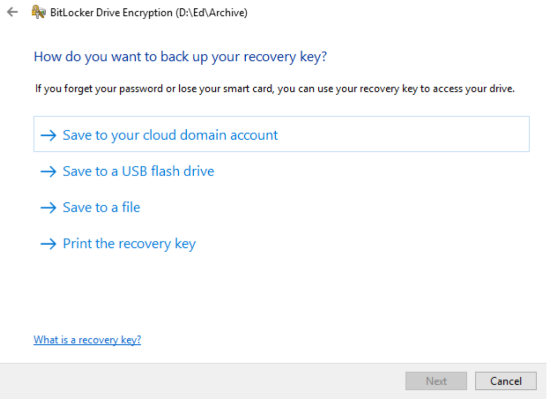
Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

Figure 6-11: You can use BitLocker Drive Encryption to protect data on the system drive, on data drives, and on removable drives.

Assuming that you have the proper hardware support for BitLocker Drive Encryption, the wizard is straightforward enough, and I don't need to walk you through its fine points. However, here are a few details worth noting:

- You'll be prompted to save your recovery key. By default, this key is saved to either your Microsoft account or to a domain account (as shown in the illustration that follows), if you have one. As an alternative, you can choose to save this key to a local file or to a USB flash drive (protect it well!) or you can print it. Regardless of the option you choose, this step is a must; I have seen routine system updates that have configured BitLocker encryption so that it won't unlock with user credentials, because the system mistakenly determined that the drive had been compromised. Without access to this recovery key, your data will be gone forever in that event. Seriously, forever.



BitLocker Drive Encryption (D:\Ed\Archive)

How do you want to back up your recovery key?

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to your cloud domain account

→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key

What is a recovery key?

- You can speed up the encryption process by choosing to encrypt only used space on a drive. Choose this option if you're setting up a new PC and you are certain that none of your business or personal data is in the erased space on the drive.

- Windows 10 version 1511 introduced a new, tougher encryption mode (XTS-AES). Use this option if you are certain that the encrypted drive will only be used on a device running the latest version of Windows 10. For removable drives that might need to be read on an older device, choose the Compatible Mode option.

Encrypting a removable drive, such as a USB flash drive, is a bit easier. The data on the drive is encrypted with a password or smart card, and you can set the drive so that it unlocks automatically when you sign in with your user account. That precaution prevents you from data loss if you leave a USB flash drive behind when leaving a trade show but makes the process of reading data from that drive easy when you're signed in properly.

CHAPTER 7

Sysinternals Suite

Two decades ago, before Mark Russinovich became the guiding technical force behind Microsoft Azure, he and Bryce Cogswell founded a company called Winternals Software. Over the years, they developed a library of powerful tools for digging deep into the internals of what was then the flagship Microsoft operating system for business customers, Windows NT.

Microsoft acquired the company (and wisely hired both of its founders) in 2006. Amazingly, the tools in the Sysinternals Suite continue to be updated regularly today, a decade later. Equally astonishing: They're also completely free.

You'll find more than 70 apps and command-line tools in the full Sysinternals Utilities collection, along with their associated help files. A handful are absolute essentials for IT pros and Windows power users, but you're likely to discover a personal favorite if you dig deep enough.

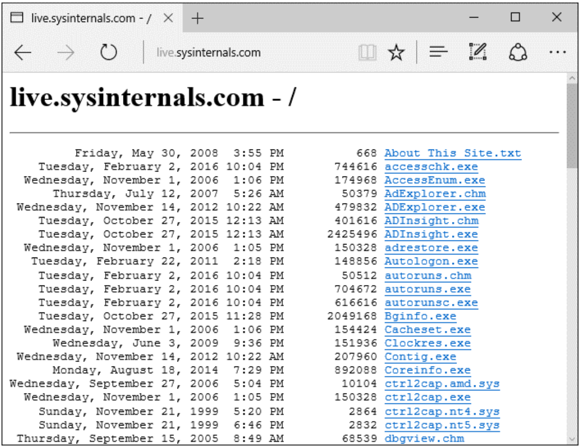
In this chapter, I focus first on the three Sysinternals superstars: Autoruns, Process Explorer, and Process Monitor. Each of these tools is a worthy upgrade to a corresponding built-in Windows app. Next, I look at a few personal favorites from the collection, including PsTools and TcpView, with additional guidance on what else you might find useful.

An overview of the Sysinternals utilities

You can, of course, visit the Windows Sysinternals page at https://technet.microsoft.com/sysinternals and use the alphabetical Utilities Index to cherry-pick just the tools you want. For a slightly more granular approach, try the six individual category lists: File And Disk, Networking, Process, Security, System Information, and Miscellaneous.

But it's much easier to download the entire Sysinternals Suite (https://technet.microsoft.com/sysinternals/bb842062) and unzip it to its own folder.

As a handy alternative to save drive space and ensure that you have the most up-to-date version of the tool you plan to use, use the Sysinternals Live service. You'll find a full listing of all tools and support files at https://live.sysinternals.com, as shown in Figure 7-1. If you know the name of the tool you want to use, you can type its path into Windows Explorer or a command prompt as https://live.sysinternals.com/<*toolname*> or \\live.sysinternals.com\tools\<*toolname*>. (Hint: Save your favorites as web shortcuts for fast access without a lot of typing.)



live.sysinternals.com - /

```
         Friday, May 30, 2008  3:55 PM          668 About This Site.txt
    Tuesday, February 2, 2016 10:04 PM       744616 accesschk.exe
  Wednesday, November 1, 2006  1:06 PM       174968 AccessEnum.exe
       Thursday, July 12, 2007  5:26 AM        50379 AdExplorer.chm
 Wednesday, November 14, 2012 10:22 AM       479832 ADExplorer.exe
    Tuesday, October 27, 2015 12:13 AM       401616 ADInsight.chm
    Tuesday, October 27, 2015 12:13 AM      2425496 ADInsight.exe
  Wednesday, November 1, 2006  1:05 PM       150328 adrestore.exe
   Tuesday, February 22, 2011  2:18 PM       148856 Autologon.exe
    Tuesday, February 2, 2016 10:04 PM        50512 autoruns.chm
    Tuesday, February 2, 2016 10:04 PM       704672 autoruns.exe
    Tuesday, February 2, 2016 10:04 PM       616616 autorunsc.exe
    Tuesday, October 27, 2015 11:28 PM      2049168 Bginfo.exe
  Wednesday, November 1, 2006  1:06 PM       154424 Cacheset.exe
      Wednesday, June 3, 2009  9:36 PM       151936 Clockres.exe
 Wednesday, November 14, 2012 10:22 AM       207960 Contig.exe
      Monday, August 18, 2014  7:29 PM       892088 Coreinfo.exe
Wednesday, September 27, 2006  5:04 PM        10104 ctrl2cap.amd.sys
  Wednesday, November 1, 2006  1:05 PM       150328 ctrl2cap.exe
    Sunday, November 21, 1999  5:20 PM         2864 ctrl2cap.nt4.sys
    Sunday, November 21, 1999  6:46 PM         2832 ctrl2cap.nt5.sys
 Thursday, September 15, 2005  8:49 AM        68539 dbgview.chm
```

Figure 7-1: The Sysinternals Live service offers click-to-run access to the latest version of every tool in the collection.

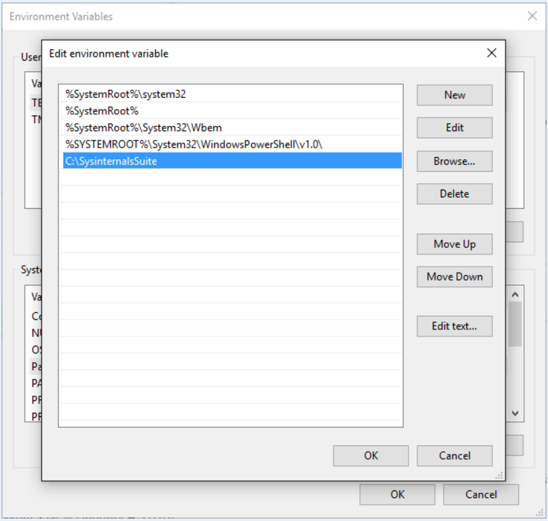
Some Sysinternals tools are fully fleshed-out programs with a distinctive graphical interface. Others are intended to be run interactively at a command line or as part of a script.

Set up Sysinternals Suite to run from anywhere

Consider this tip a twofer. If you've downloaded the entire Sysinternals Suite, you'd probably like to run its commands from anywhere: the

Run dialog box, a Command Prompt window, the search box. If you add the Sysinternals folder to the Path environment variable, you can do just that. Which gives me a chance to show off the much-improved Windows 10 interface for editing this and other environment variables.

To get started, type **environment** in the search box, and then, from the results list, click Edit The System Environment Variables. In the Environmental Variables dialog box, click Environment Variables, select Path, and then click Edit. That displays a dialog box like the one that follows. If you ever tried to edit the Path variable in a previous Windows version, I hope you appreciate how much simpler this dialog box is compared to its predecessors.



%SystemRoot%\system32
%SystemRoot%
%SystemRoot%\System32\Wbem
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\
C:\SysinternalsSuite

Because I extracted the files to a folder called SysinternalsSuite in the root of the C drive, all I had to do was click New, browse to find that folder, and click to fill in its full path. Do the same using the full path to wherever you saved the files, and then click OK twice to save your changes. You can now type any Sysinternals command—Autoruns, for example—to start that tool without specifying its full location.

Not all of the options in the Sysinternals Suite are created equal. Some were clearly written for another era and have little relevance in a world where you’re running the latest version of Windows on the desktop with modern server versions on your network. In addition, some tools, although still perfectly useful, have been superseded by built-in features. With the Desktops program, for example, you can create up to four virtual desktops and assign hotkeys to each one. The addition of virtual desktops as a built-in feature in Windows 10 makes the Sysinternals alternative far less necessary.

The best clue to help you figure which programs deserve an early look is the Date Created field. In File Explorer, switch to list view, add the Date Created field, and then sort by that field. You’ll find some date and time stamps in this list dating back to 1999, and many others that go back to 2006 or earlier. By contrast, the most useful Sysinternals programs are updated regularly and appear at the top of the list.

Autoruns

Over the years, Windows has steadily improved the ways it helps you manage which programs start automatically when you turn on your system and sign in. The latest addition to the

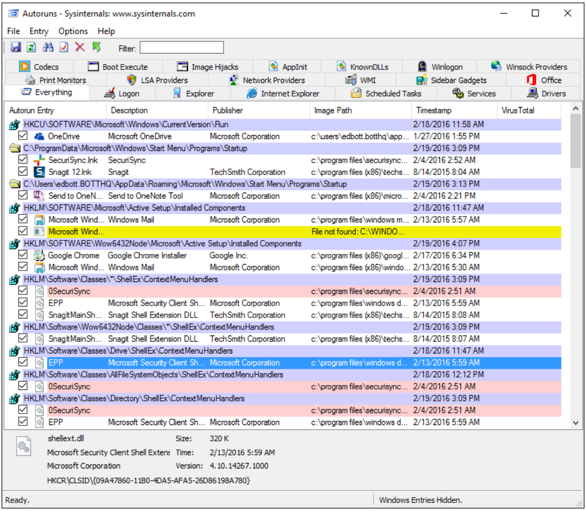
Windows toolset is the Startup tab in Task Manager, which I describe in Chapter 5.

But that built-in tool doesn’t begin to compare to Autoruns, which legitimately bills itself as “the most comprehensive autostart viewer and manager available for Windows.”

Unlike Task Manager, which limits its list to the most common locations, Autoruns shows you the full list of places in the registry, in scheduled tasks, and anywhere else where applications can configure themselves to run automatically, without your approval or interaction. Using Task Manager, you can temporarily turn off any entry listed on the Startup tab. Autoruns also makes it possible for you to delete that entry permanently, without having to muck around in the registry.

Sometimes—maybe even most of the time—these entries represent useful things, including tasks that check for security updates and perform essential synchronization tasks. But some entries are just resource hogs that run at startup so a third-party program can appear to load a few milliseconds faster.

Figure 7-2 shows the contents of the Everything tab, which pulls those many sources together into a display whose contents might qualify as overwhelming.



Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2/18/2016 11:58 AM	
☑ OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\edbott.botthq\app...	1/27/2016 1:55 PM	
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				2/19/2016 3:09 PM	
☑ SecuriSync.lnk	SecuriSync		c:\program files\securisync...	2/4/2016 2:52 AM	
☑ Snagit 12.lnk	Snagit	TechSmith Corporation	c:\program files (x86)\techs...	8/14/2015 8:04 AM	
C:\Users\edbott.BOTTHQ\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				2/19/2016 3:13 PM	
☑ Send to OneN...	Send to OneNote Tool	Microsoft Corporation	c:\program files (x86)\micro...	2/4/2016 2:21 PM	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2/18/2016 11:47 AM	
☑ Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files\windows m...	2/13/2016 5:57 AM	
☑ Microsoft Wind...			File not found: C:\WINDO...		
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2/19/2016 4:07 PM	
☑ Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\googl...	2/17/2016 6:34 PM	
☑ Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files (x86)\windo...	2/13/2016 5:30 AM	
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers				2/19/2016 3:09 PM	
☑ 0SecuriSync			c:\program files\securisync...	2/4/2016 2:51 AM	
☑ EPP	Microsoft Security Client Sh...	Microsoft Corporation	c:\program files\windows d...	2/13/2016 5:59 AM	
☑ SnagItMainSh...	Snagit Shell Extension DLL	TechSmith Corporation	c:\program files (x86)\techs...	8/14/2015 8:08 AM	
HKLM\Software\Wow6432Node\Classes\*\ShellEx\ContextMenuHandlers				2/19/2016 3:09 PM	
☑ SnagItMainSh...	Snagit Shell Extension DLL	TechSmith Corporation	c:\program files (x86)\techs...	8/14/2015 8:07 AM	
HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				2/18/2016 11:47 AM	
☑ EPP	Microsoft Security Client Sh...	Microsoft Corporation	c:\program files\windows d...	2/13/2016 5:59 AM	
HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers				2/18/2016 12:12 PM	
☑ 0SecuriSync			c:\program files\securisync...	2/4/2016 2:51 AM	
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers				2/19/2016 3:09 PM	
☑ 0SecuriSync			c:\program files\securisync...	2/4/2016 2:51 AM	
☑ EPP	Microsoft Security Client Sh...	Microsoft Corporation	c:\program files\windows d...	2/13/2016 5:59 AM	

shellext.dll	Size:	320 K
Microsoft Security Client Shell Exten:	Time:	2/13/2016 5:59 AM
Microsoft Corporation	Version:	4.10.14267.1000
HKCR\CLSID\{09A47860-11B0-4DA5-AFA5-26D86198A780}		

Ready. | Windows Entries Hidden.

Figure 7-2: The Everything tab shows every file, driver, service, scheduled task, and other items configured to start automatically, either when you turn on the device or when you sign in.

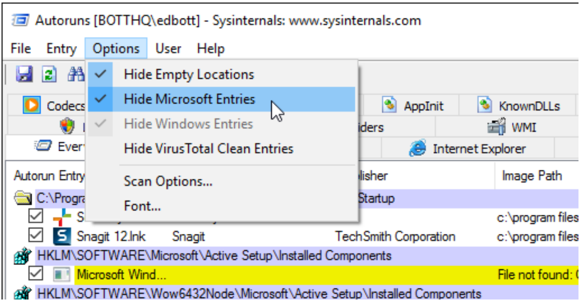
Each row includes the name of the autostart entry, the Description and Publisher fields for executable files and DLLs, the path to the file that runs when the item starts, and an icon for that file. Clear the check box to the left of any item to temporarily turn off the entry. The pane at the bottom displays details about the current selection, including its full command line.

What do the Autoruns color codes mean?

The color coding in Autoruns listings might baffle you at first, especially because they don't appear to be documented anywhere. Each heading, which identifies a location under which autostart entries are stored, is shaded a light purple. The currently selected row is highlighted in dark blue. Rows highlighted in red are associated with files for which the Description and Publisher fields are blank; yellow shading means that the autostart entry points to a file that can't be found.

If you're certain that a yellow row is only there because a program didn't clean up properly after itself, you can delete it by using Autoruns. For rows that are red, you can select the row, right-click the entry, and then, on the shortcut menu, choose Verify Image. If the code-signing certificate from the file's digital signature is trusted by a root certificate authority on the computer, the text in the Publisher column changes to "(Verified)" followed by the publisher name from the code-signing certificate. If the file is unsigned or the verification fails for any other reason, the text changes to "(Not verified)."

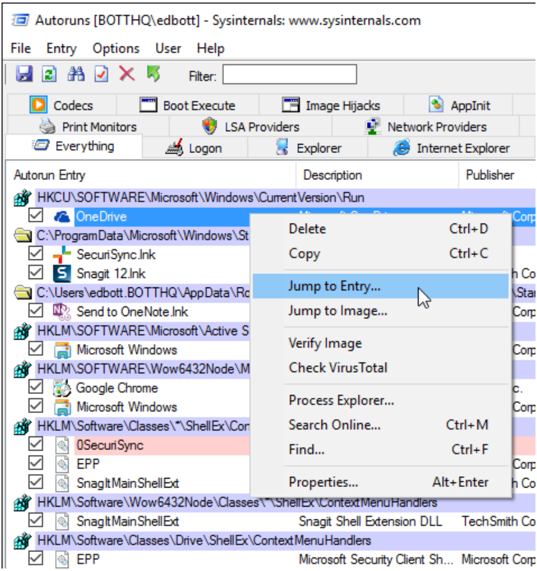
As I mentioned earlier, the Autoruns list can be overwhelming. One way to reduce the noise level is to click the Options menu and select Hide Microsoft Entries, as shown in Figure 7-3. This option makes it easier to spot potentially problematic third-party programs, including malware.



C:\Progr | Startup
☑ S | c:\program files
☑ Snagit 12.lnk | Snagit | TechSmith Corporation | c:\program files
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
☑ Microsoft Wind... | File not found: (
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components

Figure 7-3: When searching for a potentially problematic third-party program, use this option to hide Microsoft entries and reduce the number of entries you have to scan.

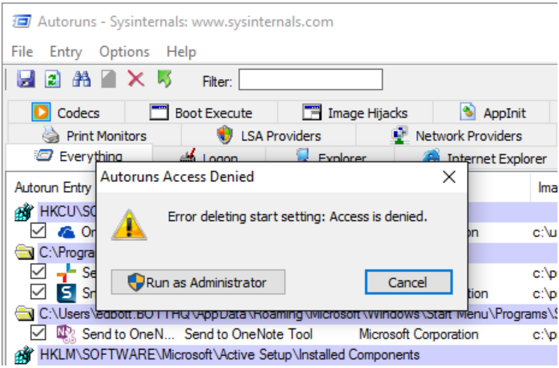
Right-click any entry on any tab in Autoruns to see a list of options for that item, as shown in Figure 7-4. Jump To Entry, for example, takes you to the folder or registry key where the item is located; Jump To Image opens File Explorer and selects the file that is set to start automatically.



Autorun Entry	Description	Publisher
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		
☑ OneDrive		Corp
C:\ProgramData\Microsoft\Windows\St		
☑ SecuriSync.lnk		
☑ Snagit 12.lnk		h Co
C:\Users\edbott.BOTTHQ\AppData\Ro		\Sta
☑ Send to OneNote.lnk		Corp
HKLM\SOFTWARE\Microsoft\Active S		
☑ Microsoft Windows		Corp
HKLM\SOFTWARE\Wow6432Node\M		
☑ Google Chrome		c.
☑ Microsoft Windows		Corp
HKLM\Software\Classes\*\ShellEx\Cor		
☑ 0SecuriSync		
☑ EPP		Corp
☑ SnagItMainShellExt		h Co
HKLM\Software\Wow6432Node\Classes\*\ShellEx\ContextMenuHandlers		
☑ SnagItMainShellExt	Snagit Shell Extension DLL	TechSmith Co
HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers		
☑ EPP	Microsoft Security Client Sh...	Microsoft Corp

Figure 7-4: If you see an unfamiliar entry in the Autoruns list, right-click to see these options and investigate it further.

Several options in this list require administrative privileges, including the option to delete an entry from the registry. If you started Autoruns without elevating, you'll see an Access Denied dialog box, like the one shown in the image that follows. Click Run As Administrator to restart Autoruns and try again.


Autoruns - Sysinternals: www.sysinternals.com
File
Entry
Options
Help
Filter:
Codecs
Boot Execute
Image Hijacks
AppInit
Print Monitors
LSA Providers
Network Providers
Everything
Logon
Explorer
Internet Explorer
Autorun Entry
Ima
Autoruns Access Denied
Run as Administrator
Cancel

Error deleting start setting: Access is denied.

HKCU\SO
C:\Progra
C:\Users\edbott.BOTTHQ\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\S
Send to OneN... Send to OneNote Tool Microsoft Corporation c:\p
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components

In general, the most prudent way to troubleshoot with Autoruns is to turn off an item by clearing the check box to its left. After you're satisfied that making that change has no long-term negative side effects, you can delete it permanently.

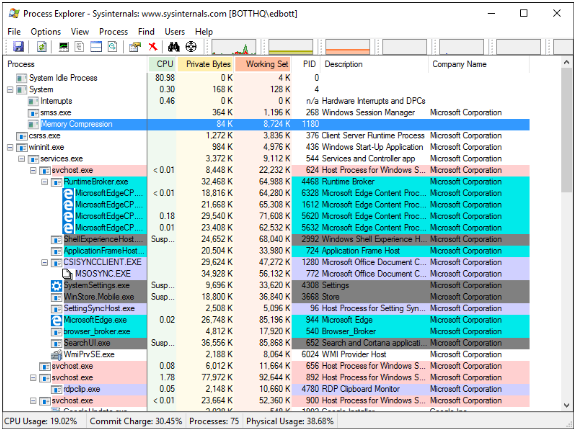
Process Explorer

When you want to know exactly what's happening on your PC right now, Process Explorer should be your first stop. At its heart, Process Explorer is a more complex version of the Windows 10 Task Manager, displaying real-time information about running processes, including which account owns a specific process; what files, registry keys, and other objects the process has open; and which DLLs the process has loaded. Process Explorer also provides a snapshot of system performance and resource usage.

Replace Task Manager

You say you prefer the more information-dense Process Explorer display to the clean but sparse Task Manager display? There's a setting for that. Specifically, in Process Explorer, click the Options menu and then select Replace Task Manager (you'll need to provide administrator's credentials to make this change). With this setting selected, pressing Ctrl+Shift+Esc opens the Sysinternals tool instead of the Windows Task Manager.

As the example in Figure 7-5 makes clear, Process Explorer is extremely active. It uses color coding to identify each process by type and uses animation to call attention to processes as they start and end.


Process Explorer - Sysinternals: www.sysinternals.com [BOTTHQ\edbott]
File
Options
View
Process
Find
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	80.98	0 K	4 K	0		
System	0.30	168 K	128 K	4		
Interrupts	0.46	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		364 K	1,196 K	268	Windows Session Manager	Microsoft Corporation
Memory Compression		84 K	8,724 K	1180		
csrss.exe		1,272 K	3,836 K	376	Client Server Runtime Process	Microsoft Corporation
wininit.exe		984 K	4,976 K	436	Windows Start-Up Application	Microsoft Corporation
services.exe		3,372 K	9,112 K	544	Services and Controller app	Microsoft Corporation
svchost.exe	< 0.01	8,448 K	22,232 K	624	Host Process for Windows S...	Microsoft Corporation
RuntimeBroker.exe		32,468 K	64,988 K	4468	Runtime Broker	Microsoft Corporation
MicrosoftEdgeCP....	< 0.01	18,816 K	64,280 K	6328	Microsoft Edge Content Proc...	Microsoft Corporation
MicrosoftEdgeCP....		21,668 K	65,308 K	1612	Microsoft Edge Content Proc...	Microsoft Corporation
MicrosoftEdgeCP....	0.18	29,540 K	71,608 K	5620	Microsoft Edge Content Proc...	Microsoft Corporation
MicrosoftEdgeCP....	0.01	23,408 K	62,532 K	5632	Microsoft Edge Content Proc...	Microsoft Corporation
ShellExperienceHost....	Susp...	24,652 K	68,040 K	2992	Windows Shell Experience H...	Microsoft Corporation
ApplicationFrameHost...		20,504 K	33,980 K	724	Application Frame Host	Microsoft Corporation
CSISYNCCLIENT.EXE		29,624 K	47,272 K	1280	Microsoft Office Document C...	Microsoft Corporation
MSOSYNC.EXE		34,928 K	56,132 K	772	Microsoft Office Document C...	Microsoft Corporation
SystemSettings.exe	Susp...	9,696 K	33,620 K	4308	Settings	Microsoft Corporation
WinStore.Mobile.exe	Susp...	18,800 K	36,840 K	3668	Store	Microsoft Corporation
SettingSyncHost.exe		2,508 K	5,096 K	96	Host Process for Setting Syn...	Microsoft Corporation
MicrosoftEdge.exe	0.02	26,748 K	85,196 K	944	Microsoft Edge	Microsoft Corporation
browser_broker.exe		4,812 K	17,920 K	540	Browser_Broker	Microsoft Corporation
SearchUI.exe	Susp...	36,556 K	85,868 K	652	Search and Cortana applicati...	Microsoft Corporation
WmiPrvSE.exe		2,188 K	8,064 K	6024	WMI Provider Host	Microsoft Corporation
svchost.exe	0.08	6,012 K	11,664 K	656	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1.78	77,972 K	92,644 K	892	Host Process for Windows S...	Microsoft Corporation
rdpclip.exe	0.05	2,148 K	10,660 K	4780	RDP Clipboard Monitor	Microsoft Corporation
svchost.exe	< 0.01	23,664 K	52,360 K	900	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 19.02% Commit Charge: 30.45% Processes: 75 Physical Usage: 38.68%

Figure 7-5: The default Process Explorer view groups processes by parent-child relationships and uses color coding to identify different types of processes.

You can customize Process Explorer's color coding by clicking Options and then selecting Configure Colors. The default settings are as follows:

- Green indicates new objects, and deep red highlights deleted objects. Both of these colors appear only briefly as processes start and end.
- Light blue identifies "own processes," which run under the same account that was used

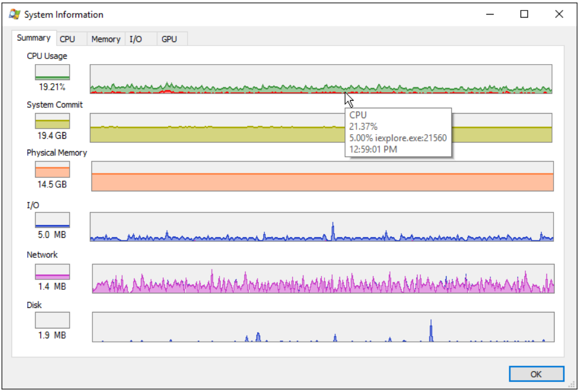
to start Process Explorer. Note that these processes might be running in a different security context than the user account under which they were started.

- Pink rows highlight processes that contain one or more Windows services. When you point to one of these rows, a screen tip appears, showing the names of individual services running in that process, which can be useful for determining what an instance of Svchost.exe is responsible for.
- Violet (or very deep purple) indicates a “packed” (encrypted or compressed) executable program. This might indicate potential malware, especially if associated with an unknown process.
- Turquoise indicates immersive processes, which are associated with Windows Store apps.
- Dark gray identifies a suspended process. Typically these are Windows Store apps that you previously opened but are no longer using. Some Windows Store apps are specifically written to continue running in the background. Groove Music, for example,

will keep playing tunes even if you switch the focus to another program.

You can identify Windows jobs and .NET processes by their color coding, although these attributes are not displayed under default settings.

Tiny graphs along the top of the Process Explorer window display system Information in real time. To see all performance charts in a single window, press Ctrl+I (as in Information) or, on the menu bar click View and then select System Information. Figure 7-6 shows this display in action.



CPU Usage 19.21%
System Commit 19.4 GB
Physical Memory 14.5 GB
I/O 5.0 MB
Network 1.4 MB
Disk 1.9 MB

CPU
21.37%
5.00% iexplore.exe:21560
12:59:01 PM

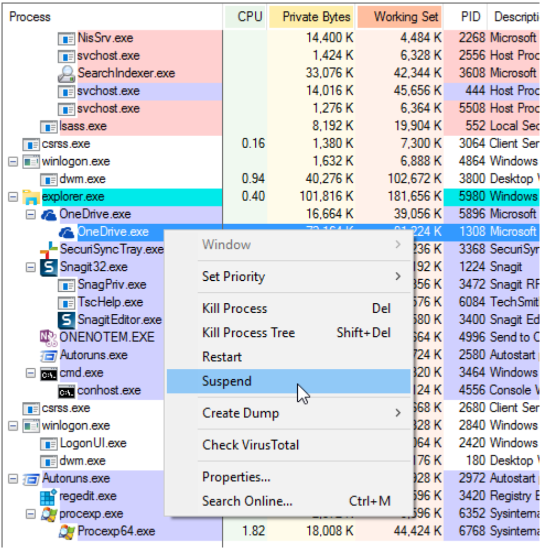
Figure 7-6: The System Information window shows real-time performance graphs for the current system,

with screen tips that provide details when you point at a particular spot.

Note If you don’t see all of the charts in Figure 7-6, restart Process Explorer as an administrator.

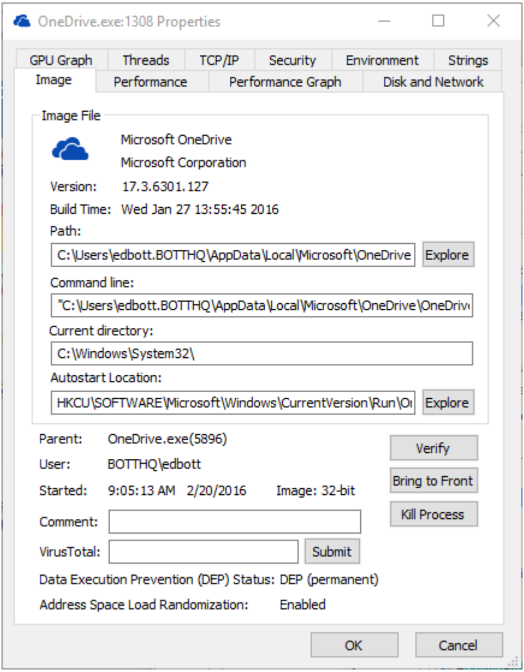
Each of the individual tabs—CPU, Memory, I/O, and GPU—contains additional details about that particular batch of resources. The GPU tab in particular adds details that you won’t find on the Performance tab in Task Manager.

The real power of Process Explorer becomes apparent when you right-click an individual process to reveal the menu of available options, as shown in the image that follows. I describe these in more detail in the remainder of this section.



Process	CPU	Private Bytes	Working Set	PID	Descripti
NisSrv.exe		14,400 K	4,484 K	2268	Microsoft
svchost.exe		1,424 K	6,328 K	2556	Host Proc
SearchIndexer.exe		33,076 K	42,344 K	3608	Microsoft
svchost.exe		14,016 K	45,656 K	444	Host Proc
svchost.exe		1,276 K	6,364 K	5508	Host Proc
lsass.exe		8,192 K	19,904 K	552	Local Sec
csrss.exe	0.16	1,380 K	7,300 K	3064	Client Ser
winlogon.exe		1,632 K	6,888 K	4864	Windows
dwm.exe	0.94	40,276 K	102,672 K	3800	Desktop
explorer.exe	0.40	101,816 K	181,656 K	5980	Windows
OneDrive.exe		16,664 K	39,056 K	5896	Microsoft
OneDrive.exe			224 K	1308	Microsoft
SecuriSyncTray.exe			36 K	3368	SecuriSyr
Snagit32.exe			192 K	1224	Snagit
SnagPriv.exe			56 K	3472	Snagit RF
TscHelp.exe			576 K	6084	TechSmit
SnagitEditor.exe			580 K	3400	Snagit Ed
ONENOTEM.EXE			64 K	4996	Send to C
Autoruns.exe			724 K	2580	Autostart
cmd.exe			320 K	3464	Windows
conhost.exe			124 K	4556	Console
csrss.exe			68 K	2680	Client Ser
winlogon.exe			328 K	2840	Windows
LogonUI.exe			64 K	2420	Windows
dwm.exe			176 K	180	Desktop
Autoruns.exe			928 K	2972	Autostart
regedit.exe			96 K	3420	Registry E
procexp.exe			96 K	6352	Sysinterna
Procexp64.exe	1.82	18,008 K	44,424 K	6768	Sysinterna

The first place to look, especially when you want to find out exactly what a process is, is the properties dialog box, which shows significantly more information than you'll find in its File Explorer counterpart. Figure 7-7, for example, shows the Image tab for the file OneDrive.exe.

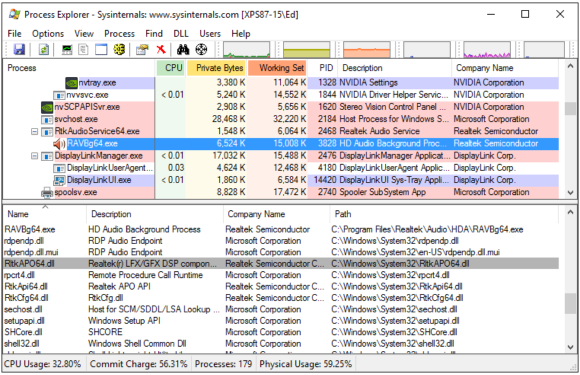


Microsoft OneDrive
Microsoft Corporation
Version: 17.3.6301.127
Build Time: Wed Jan 27 13:55:45 2016
Path: C:\Users\edbott.BOTTHQ\AppData\Local\Microsoft\OneDrive
Command line: "C:\Users\edbott.BOTTHQ\AppData\Local\Microsoft\OneDrive\OneDriv
Current directory: C:\Windows\System32\
Autostart Location: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\O
Parent: OneDrive.exe(5896)
User: BOTTHQ\edbott
Started: 9:05:13 AM 2/20/2016 Image: 32-bit
Comment:
VirusTotal:
Data Execution Prevention (DEP) Status: DEP (permanent)
Address Space Load Randomization: Enabled

Figure 7-7: Details available for a running process include version information and whether it starts automatically.

From that properties dialog box or from the process list itself, you can submit the hash for a file to the VirusTotal service to find out whether that hash has been identified as possible malware by any of the 50-plus antivirus engines that VirusTotal monitors.

The lower pane of the Process Explorer window is normally hidden. You can make it visible by using the keyboard shortcut Ctrl+L (or, on the View menu, choose Show Lower Pane). This pane shows one of two views for the current process: DLLs or handles. You can switch between the two views by using the keyboard shortcuts Ctrl+D and Ctrl+H, respectively. Figure 7-8 shows the lower pane in DLLs view.


Process Explorer - Sysinternals: www.sysinternals.com [XPS87-15\Ed]
File
Options
View
Process
Find
DLL
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
nvtray.exe		3,380 K	11,064 K	1328	NVIDIA Settings	NVIDIA Corporation
nvvsvc.exe	< 0.01	5,240 K	14,552 K	1844	NVIDIA Driver Helper Servic...	NVIDIA Corporation
nvSCPAPISvr.exe		2,908 K	5,656 K	1620	Stereo Vision Control Panel ...	NVIDIA Corporation
svchost.exe		28,468 K	32,220 K	2184	Host Process for Windows S...	Microsoft Corporation
⊟ RtkAudioService64.exe		1,548 K	6,064 K	2468	Realtek Audio Service	Realtek Semiconductor
RAVBg64.exe		6,524 K	15,008 K	3828	HD Audio Background Proc...	Realtek Semiconductor
⊟ DisplayLinkManager.exe	< 0.01	17,032 K	15,488 K	2476	DisplayLinkManager Applicat...	DisplayLink Corp.
DisplayLinkUserAgent...	0.03	4,624 K	12,468 K	4180	DisplayLinkUserAgent Applic...	DisplayLink Corp.
DisplayLinkUI.exe	< 0.01	1,860 K	6,584 K	14420	DisplayLinkUI Sys-Tray Appli...	DisplayLink Corp.
spoolsv.exe		8,828 K	17,472 K	2740	Spooler SubSystem App	Microsoft Corporation

Name	Description	Company Name	Path
RAVBg64.exe	HD Audio Background Process	Realtek Semiconductor	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe
rdpendp.dll	RDP Audio Endpoint	Microsoft Corporation	C:\Windows\System32\rdpendp.dll
rdpendp.dll.mui	RDP Audio Endpoint	Microsoft Corporation	C:\Windows\System32\en-US\rdpendp.dll.mui
RltkAPO64.dll	Realtek(r) LFX/GFX DSP compon...	Realtek Semiconductor C...	C:\Windows\System32\RltkAPO64.dll
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\Windows\System32\rpcrt4.dll
RtkApi64.dll	Realtek APO API	Realtek Semiconductor C...	C:\Windows\System32\RtkApi64.dll
RtkCfg64.dll	RtkCfg.dll	Realtek Semiconductor C...	C:\Windows\System32\RtkCfg64.dll
sechost.dll	Host for SCM/SDDL/LSA Lookup ...	Microsoft Corporation	C:\Windows\System32\sechost.dll
setupapi.dll	Windows Setup API	Microsoft Corporation	C:\Windows\System32\setupapi.dll
SHCore.dll	SHCORE	Microsoft Corporation	C:\Windows\System32\SHCore.dll
shell32.dll	Windows Shell Common Dll	Microsoft Corporation	C:\Windows\System32\shell32.dll

CPU Usage: 32.80% | Commit Charge: 56.31% | Processes: 179 | Physical Usage: 59.25%

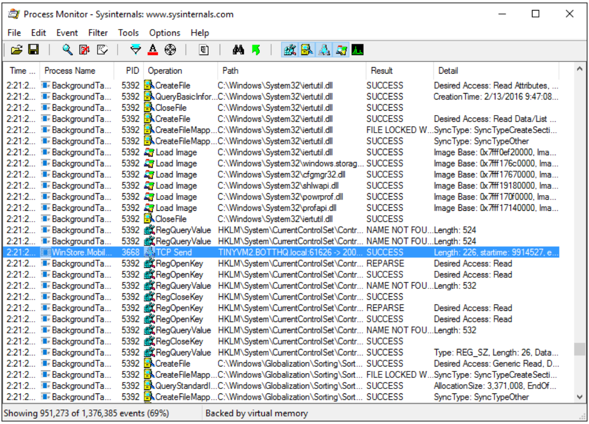
Figure 7-8: The lower pane can show either a list of DLLs associated with the selected process (as shown here) or a list of handles

Process Monitor

The last of the three Sysinternals superstars is Process Monitor, also known as Procmon. When running, it keeps track of all activity involving the file system, the registry, the network, processes, threads, and DLLs, in real time.

A Procmon trace can collect an enormous amount of activity—millions of distinct operations in a matter of seconds—which you can then filter to eliminate noise and zero in on the potential cause of a problem. Because you can save Procmon traces in log files, it's relatively easy to capture activity on a system that's acting up and then analyze the captured data on another system.

To get a sense of the level of detail captured by Procmon, see the listing in Figure 7-9, which represents system activity for a period measured in a small fraction of a second.



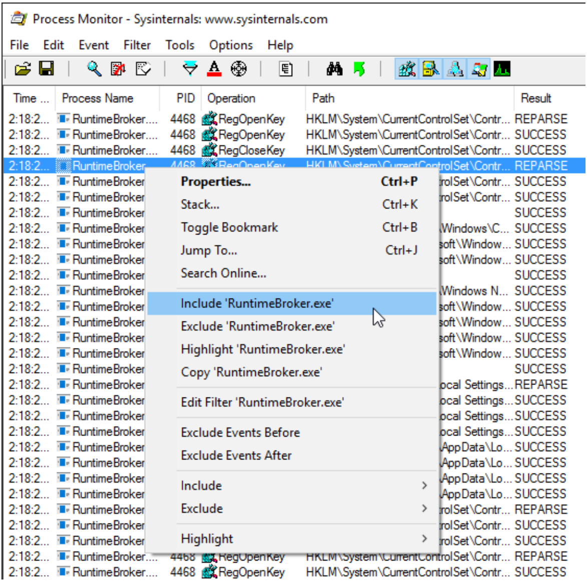
Time ...	Process Name	PID	Operation	Path	Result	Detail
2:21:2...	BackgroundTa...	5392	CreateFile	C:\Windows\System32\iertutil.dll	SUCCESS	Desired Access: Read Attributes, ...
2:21:2...	BackgroundTa...	5392	QueryBasicInfor...	C:\Windows\System32\iertutil.dll	SUCCESS	CreationTime: 2/13/2016 9:47:08...
2:21:2...	BackgroundTa...	5392	CloseFile	C:\Windows\System32\iertutil.dll	SUCCESS	
2:21:2...	BackgroundTa...	5392	CreateFile	C:\Windows\System32\iertutil.dll	SUCCESS	Desired Access: Read Data/List ...
2:21:2...	BackgroundTa...	5392	CreateFileMapp...	C:\Windows\System32\iertutil.dll	FILE LOCKED W...	SyncType: SyncTypeCreateSecti...
2:21:2...	BackgroundTa...	5392	CreateFileMapp...	C:\Windows\System32\iertutil.dll	SUCCESS	SyncType: SyncTypeOther
2:21:2...	BackgroundTa...	5392	Load Image	C:\Windows\System32\iertutil.dll	SUCCESS	Image Base: 0x7fff0ef20000, Ima...
2:21:2...	BackgroundTa...	5392	Load Image	C:\Windows\System32\windows.storag...	SUCCESS	Image Base: 0x7fff176c0000, Ima...
2:21:2...	BackgroundTa...	5392	Load Image	C:\Windows\System32\cfgmgr32.dll	SUCCESS	Image Base: 0x7fff17670000, Ima...
2:21:2...	BackgroundTa...	5392	Load Image	C:\Windows\System32\shlwapi.dll	SUCCESS	Image Base: 0x7fff19180000, Ima...
2:21:2...	BackgroundTa...	5392	Load Image	C:\Windows\System32\powrprof.dll	SUCCESS	Image Base: 0x7fff170f0000, Ima...
2:21:2...	BackgroundTa...	5392	Load Image	C:\Windows\System32\profapi.dll	SUCCESS	Image Base: 0x7fff17140000, Ima...
2:21:2...	BackgroundTa...	5392	CloseFile	C:\Windows\System32\iertutil.dll	SUCCESS	
2:21:2...	BackgroundTa...	5392	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOU...	Length: 524
2:21:2...	BackgroundTa...	5392	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOU...	Length: 524
2:21:2...	WinStore.Mobil...	3668	TCP Send	TINYVM2.BOTTHQ.local:61626 -> 200...	SUCCESS	Length: 226, startime: 9914527, e...
2:21:2...	BackgroundTa...	5392	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Read
2:21:2...	BackgroundTa...	5392	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read
2:21:2...	BackgroundTa...	5392	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOU...	Length: 532
2:21:2...	BackgroundTa...	5392	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
2:21:2...	BackgroundTa...	5392	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Read
2:21:2...	BackgroundTa...	5392	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read
2:21:2...	BackgroundTa...	5392	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOU...	Length: 532
2:21:2...	BackgroundTa...	5392	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
2:21:2...	BackgroundTa...	5392	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Length: 26, Data...
2:21:2...	BackgroundTa...	5392	CreateFile	C:\Windows\Globalization\Sorting\Sort...	SUCCESS	Desired Access: Generic Read, D...
2:21:2...	BackgroundTa...	5392	CreateFileMapp...	C:\Windows\Globalization\Sorting\Sort...	FILE LOCKED W...	SyncType: SyncTypeCreateSecti...
2:21:2...	BackgroundTa...	5392	QueryStandardI...	C:\Windows\Globalization\Sorting\Sort...	SUCCESS	AllocationSize: 3,371,008, EndOf...
2:21:2...	BackgroundTa...	5392	CreateFileMapp...	C:\Windows\Globalization\Sorting\Sort...	SUCCESS	SyncType: SyncTypeOther

Showing 951,273 of 1,376,385 events (69%) Backed by virtual memory

Figure 7-9: Process Monitor records every event from every process running during a trace, which can result in millions of discrete events, as shown in the status bar.

Although Procmon collects everything it observes, the default settings include a filter that hides raw details from the file system and from Procmon itself. You can fine-tune the filter on the fly by right-clicking a specific entry in a specific column and then, on the shortcut menu, choosing from among the options.

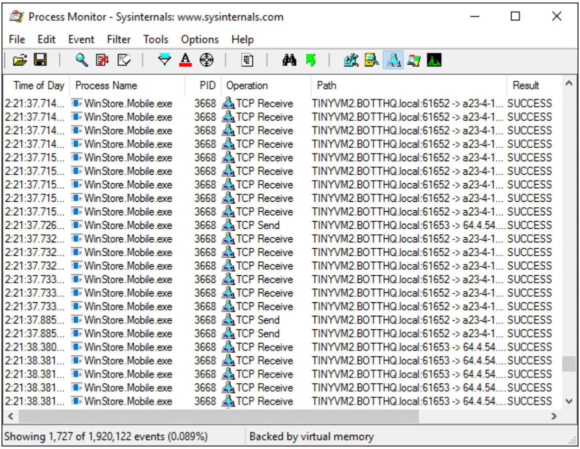
In Figure 7-10, for example, I right-clicked Runtimebroker.exe in the Process Name column. I can now choose to include that process in the current filter, effectively displaying only entries from that process, or exclude it so that matching results are hidden. I can also choose to highlight matching entries without hiding those that don’t match.



Time ...	Process Name	PID	Operation	Path	Result
2:18:2...	RuntimeBroker....	4468	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE
2:18:2...	RuntimeBroker....	4468	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
2:18:2...	RuntimeBroker....	4468	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
2:18:2...	RuntimeBroker	4468	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE
2:18:2...	RuntimeBroker			rolSet\Contr...	SUCCESS
2:18:2...	RuntimeBroker			rolSet\Contr...	SUCCESS
2:18:2...	RuntimeBroker				SUCCESS
2:18:2...	RuntimeBroker			Windows\C...	SUCCESS
2:18:2...	RuntimeBroker			soft\Window...	SUCCESS
2:18:2...	RuntimeBroker			soft\Window...	SUCCESS
2:18:2...	RuntimeBroker				SUCCESS
2:18:2...	RuntimeBroker			Windows N...	SUCCESS
2:18:2...	RuntimeBroker			soft\Window...	SUCCESS
2:18:2...	RuntimeBroker			soft\Window...	SUCCESS
2:18:2...	RuntimeBroker			soft\Window...	SUCCESS
2:18:2...	RuntimeBroker			soft\Window...	SUCCESS
2:18:2...	RuntimeBroker				SUCCESS
2:18:2...	RuntimeBroker			ocal Settings...	REPARSE
2:18:2...	RuntimeBroker			ocal Settings...	SUCCESS
2:18:2...	RuntimeBroker			ocal Settings...	SUCCESS
2:18:2...	RuntimeBroker			ocal Settings...	SUCCESS
2:18:2...	RuntimeBroker			AppData\Lo...	SUCCESS
2:18:2...	RuntimeBroker			AppData\Lo...	SUCCESS
2:18:2...	RuntimeBroker			AppData\Lo...	SUCCESS
2:18:2...	RuntimeBroker			AppData\Lo...	SUCCESS
2:18:2...	RuntimeBroker			rolSet\Contr...	REPARSE
2:18:2...	RuntimeBroker			rolSet\Contr...	SUCCESS
2:18:2...	RuntimeBroker			rolSet\Contr...	SUCCESS
2:18:2...	RuntimeBroker....	4468	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE
2:18:2...	RuntimeBroker....	4468	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS

Figure 7-10: Right-click an item in any column to see this menu of options for filtering events containing matching entries.

Look at the status bar along the bottom of the Procmon window to see whether a filter has been applied to the captured data and, if so, how much of an impact it has had. In Figure 7-11, for example, the filtered list shows fewer than 1 in 1000 events, making it possible to scroll through the data—or filter it further—in search of patterns or clues.



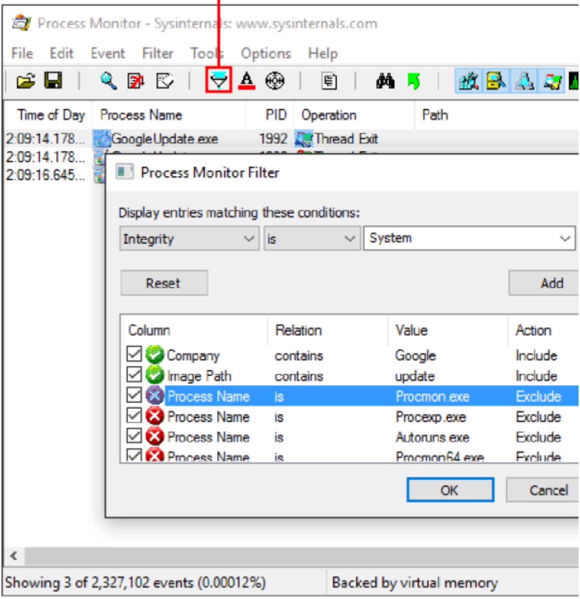
Time of Day	Process Name	PID	Operation	Path	Result
2:21:37.714...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.714...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.714...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.714...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.715...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.715...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.715...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.715...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.715...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.726...	WinStore.Mobile.exe	3668	TCP Send	TINYVM2.BOTTHQ.local:61653 -> 64.4.54....	SUCCESS
2:21:37.732...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.732...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.732...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.733...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.733...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.733...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.885...	WinStore.Mobile.exe	3668	TCP Send	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:37.885...	WinStore.Mobile.exe	3668	TCP Send	TINYVM2.BOTTHQ.local:61652 -> a23-4-1...	SUCCESS
2:21:38.380...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61653 -> 64.4.54....	SUCCESS
2:21:38.381...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61653 -> 64.4.54....	SUCCESS
2:21:38.381...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61653 -> 64.4.54....	SUCCESS
2:21:38.381...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61653 -> 64.4.54....	SUCCESS
2:21:38.381...	WinStore.Mobile.exe	3668	TCP Receive	TINYVM2.BOTTHQ.local:61653 -> 64.4.54....	SUCCESS

Showing 1,727 of 1,920,122 events (0.089%)   Backed by virtual memory

Figure 7-11: See the status bar at the bottom of the Process Monitor window for an idea of how effective your filter is.

You can also create or modify a filter by using the Process Monitor Filter dialog box, which offers a point-and-click convenience, as demonstrated in Figure 7-12. To access the Process Monitor Filter dialog box, on the menu bar, click Filter. You can set conditions that define which events to include or exclude and then click Add, or select an existing filter and click Remove. Click Apply to see the effect of the new filter immediately.

Click to modify the current filter



Time of Day	Process Name	PID	Operation	Path
2:09:14.178...	GoogleUpdate.exe	1992	Thread Exit	
2:09:14.178...				
2:09:16.645...				

Display entries matching these conditions:

Integrity | is | System

Column	Relation	Value	Action
☑ Company	contains	Google	Include
☑ Image Path	contains	update	Include
☑ Process Name	is	Procmon.exe	Exclude
☑ Process Name	is	Procexp.exe	Exclude
☑ Process Name	is	Autoruns.exe	Exclude
☑ Process Name	is	Procmon64.exe	Exclude

Showing 3 of 2,327,102 events (0.00012%) | Backed by virtual memory

Figure 7-12: Clicking the Filter button opens the Process Monitor Filter dialog box, where you can add criteria by using drop-down lists. Remember to click Apply before exiting.

More Sysinternals tools

This chapter doesn’t have enough pages to do justice to the “other” programs in the Sysinternals tools collection. So, consider this section a bit of a sampler, offering hints that might encourage you to poke around for your own enlightenment.

PsTools

The PsTools group includes command-line utilities for working with processes running on local or remote computers, running processes remotely, rebooting computers, and dumping event logs, among other tasks. Each of the commands begins, naturally, with the letters *Ps*. (The name is derived from the Ps utility, which is short for “process status” and provides similar capabilities on UNIX systems.)

Because of changes in network authentication, remote access is most effective on domain-joined systems and unlikely to be worth the trouble on simple workgroups. Most of the tools require administrative rights, as well. The following list provides a terse description of the capabilities of the PsTools commands.

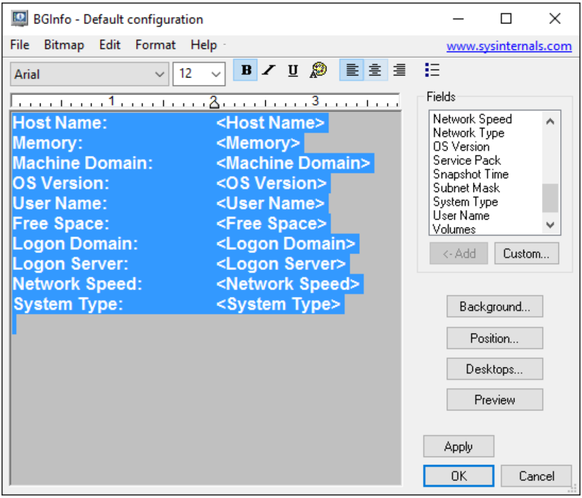
- **PsExec** Runs processes with limited-user rights
- **PsFile** Lists files that are opened remotely
- **PsGetSid** Displays the SID of a computer or a user
- **PsInfo** Obtains information about a system
- **PsKill** Terminates local or remote processes
- **PsList** Shows information about processes and threads
- **PsLoggedOn** Shows users signed in to a system
- **PsLogList** Dumps event log records
- **PsPasswd** Gives administrators the ability to change passwords for user accounts
- **PsPing** Measures network performance
- **PsService** Views and controls services
- **PsShutdown** Shuts down, logs off, or changes the power state of a system

- **PsSuspend** Suspends and resumes processes

BgInfo

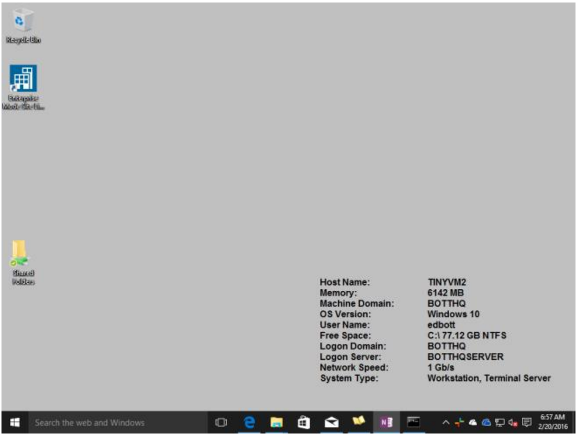
If you've configured a bunch of virtual machines (VMs) for testing purposes and you're having trouble telling them apart, this small but useful program can help. It automatically generates desktop backgrounds that include details about the system, including its IP address, computer name, domain name, and more.

Figure 7-13 shows the basic configuration for one of these backgrounds. Figure 7-14 shows the resulting text as it appears on the desktop background.



```
Host Name:        <Host Name>
Memory:           <Memory>
Machine Domain:   <Machine Domain>
OS Version:       <OS Version>
User Name:        <User Name>
Free Space:       <Free Space>
Logon Domain:     <Logon Domain>
Logon Server:     <Logon Server>
Network Speed:    <Network Speed>
System Type:      <System Type>
```

Figure 7-13: Using the BGInfo program, you can automatically display information about the current system on its desktop background, making it easier to identify a remote desktop connection or a running VM.



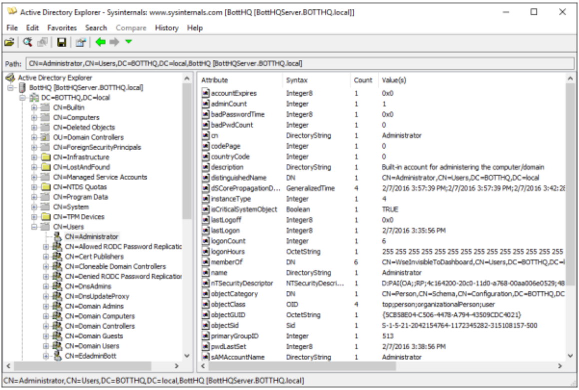
```
Host Name:          TINYVM2
Memory:             6142 MB
Machine Domain:     BOTTHQ
OS Version:         Windows 10
User Name:          edbott
Free Space:         C:\ 77.12 GB NTFS
Logon Domain:       BOTTHQ
Logon Server:       BOTTHQSERVER
Network Speed:      1 Gb/s
System Type:        Workstation, Terminal Server
```

Figure 7-14: The information on this desktop background was drawn from the system itself using the BGInfo program.

Active Directory Explorer

If you work as an administrator in a Windows domain, Active Directory Explorer offers an advanced viewer and editor for working with directory services, including an Active Directory database or Active Directory Lightweight Directory Services.

Like other, similar management tools, it uses a two-pane design, with the Active Directory object tree on the left and attributes for the current selection on the right, as in the example in Figure 7-15. To begin, connect to a directory using administrative credentials; you can view, edit, add, and remove items, and the tool also supports search functionality.



Path: CN=Administrator,CN=Users,DC=BOTTHQ,DC=local,BottHQ [BottHQServer.BOTTHQ.local]

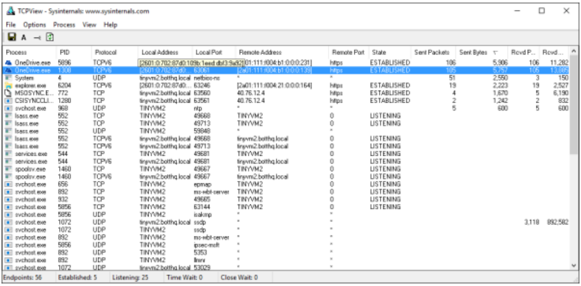
Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	Built-in account for administering the computer/domain
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=BOTTHQ,DC=local
dSCorePropagationD...	GeneralizedTime	4	2/7/2016 3:57:39 PM;2/7/2016 3:57:39 PM;2/7/2016 3:42:2
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	2/7/2016 3:35:56 PM
logonCount	Integer	1	6
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	6	CN=WseInvisibleToDashboard,CN=Users,DC=BOTTHQ,DC=l
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescri...	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;48
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=BOTTHQ,DC
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{5CB58E04-C506-4478-A794-43509CDC4021}
objectSid	Sid	1	S-1-5-21-2042154764-1172345282-315108157-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	2/7/2016 3:38:56 PM
sAMAccountName	DirectoryString	1	Administrator

CN=Administrator,CN=Users,DC=BOTTHQ,DC=local,BottHQ [BottHQServer.BOTTHQ.local]

Figure 7-15: You might prefer this lightweight Active Directory management tool over the official alternative included with Windows Server editions.

TCPView

Windows includes several built-in command-line tools, most notably Netstat, for viewing the status of network connections. TCPView is significantly easier to use and gives you details about TCP and UDP connections between local ports and remote addresses. Figure 7-16 shows this tool in action. Note that by pointing to a connection, you to see full details in a screen tip.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd P...	Rcvd ...
OneDrive.exe	5896	TCPV6	[2601:0:702:87d0:109b:1eed:dbf3:9a92]		01:111:f004:b1:0:0:0:231]	https	ESTABLISHED	106	5,906	106	11,282
OneDrive.exe	1308	TCPV6	[2601:0:702:87d0:...	63061	[2a01:111:f004:b1:0:0:0:139]	https	ESTABLISHED	105	5,757	105	13,005
System	4	UDP	tinyvm2.botthq.local	netbios-ns	*	*		51	2,550	3	150
explorer.exe	6204	TCPV6	[2601:0:702:87d0:...	63246	[2a01:111:f004:21:0:0:0:164]	https	ESTABLISHED	19	2,223	19	2,527
MSOSYNC.E...	772	TCP	tinyvm2.botthq.local	63560	40.76.12.4	https	ESTABLISHED	4	1,670	5	6,190
CSISYNCCLI...	1280	TCP	tinyvm2.botthq.local	63561	40.76.12.4	https	ESTABLISHED	2	1,242	2	832
svchost.exe	968	UDP	TINYVM2	ntp	*	*		5	600	5	600
lsass.exe	552	TCP	TINYVM2	49668	TINYVM2	0	LISTENING				
lsass.exe	552	TCP	TINYVM2	49713	TINYVM2	0	LISTENING				
lsass.exe	552	UDP	TINYVM2	59848	*	*					
lsass.exe	552	TCPV6	tinyvm2.botthq.local	49668	tinyvm2.botthq.local	0	LISTENING				
lsass.exe	552	TCPV6	tinyvm2.botthq.local	49713	tinyvm2.botthq.local	0	LISTENING				
services.exe	544	TCP	TINYVM2	49681	TINYVM2	0	LISTENING				
services.exe	544	TCPV6	tinyvm2.botthq.local	49681	tinyvm2.botthq.local	0	LISTENING				
spoolsv.exe	1460	TCP	TINYVM2	49667	TINYVM2	0	LISTENING				
spoolsv.exe	1460	TCPV6	tinyvm2.botthq.local	49667	tinyvm2.botthq.local	0	LISTENING				
svchost.exe	656	TCP	TINYVM2	epmap	TINYVM2	0	LISTENING				
svchost.exe	892	TCP	TINYVM2	ms-wbt-server	TINYVM2	0	LISTENING				
svchost.exe	932	TCP	TINYVM2	49665	TINYVM2	0	LISTENING				
svchost.exe	5856	TCP	TINYVM2	63144	TINYVM2	0	LISTENING				
svchost.exe	5856	UDP	TINYVM2	isakmp	*	*					
svchost.exe	1072	UDP	tinyvm2.botthq.local	ssdp	*	*				3,118	892,582
svchost.exe	1072	UDP	TINYVM2	ssdp	*	*					
svchost.exe	892	UDP	TINYVM2	ms-wbt-server	*	*					
svchost.exe	5856	UDP	TINYVM2	ipsec-msft	*	*					
svchost.exe	892	UDP	TINYVM2	5353	*	*					
svchost.exe	892	UDP	TINYVM2	llmnr	*	*					
svchost.exe	1072	UDP	tinyvm2.botthq.local	53029	*	*					

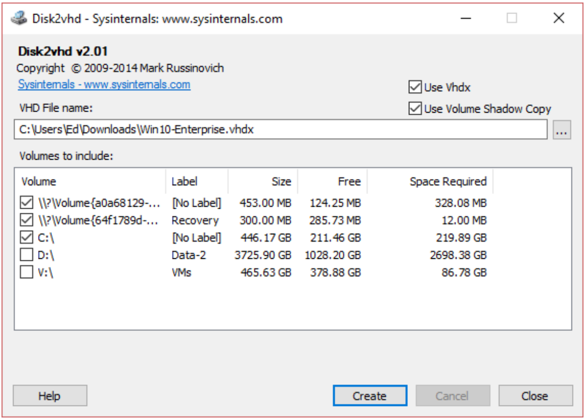
Endpoints: 56 | Established: 5 | Listening: 25 | Time Wait: 0 | Close Wait: 0

Figure 7-16: TCPView gives you a single list of all current and recent TCP and UDP connections.

> **Note** You also have the option to right-click and close any connection immediately.

Disk2vhd

Although its function might seem esoteric, Disk2vhd serves a genuine need, making it relatively easy to move a physical system into a VM. That's especially handy for virtualizing the workload of a server so that it can run in Hyper-V instead of on physical hardware.



Disk2vhd v2.01
Copyright © 2009-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

☑ Use Vhdx
☑ Use Volume Shadow Copy

VHD File name: C:\Users\Ed\Downloads\Win10-Enterprise.vhdx

Volumes to include:

Volume	Label	Size	Free	Space Required
☑ \\?\Volume{a0a68129-…	[No Label]	453.00 MB	124.25 MB	328.08 MB
☑ \\?\Volume{64f1789d-…	Recovery	300.00 MB	285.73 MB	12.00 MB
☑ C:\	[No Label]	446.17 GB	211.46 GB	219.89 GB
☐ D:\	Data-2	3725.90 GB	1028.20 GB	2698.38 GB
☐ V:\	VMs	465.63 GB	378.88 GB	86.78 GB

Figure 7-17: Use Disk2vhd to convert a physical machine into a Virtual Hard Drive file that you can attach to a Hyper-V VM.

And more

Still curious? Here are a few remaining Sysinternals tools that you might find useful.

- AccessEnum and ShareEnum are security tools that show who has access to directories, files, registry keys, and file shares on your systems. They're useful for spotting misconfigurations that could allow an attacker in.

- DiskView provides a graphical look at how drive space is being used on a given storage device.
- Whois gives you a way to enter a domain name and see who is listed as the owner of that address.
- Autologon makes it possible for you to automatically enter saved credentials at startup, skipping the sign-in screen. It should, of course, only be used in physically secure environments.
- Zoomit is used by elite presenters at Microsoft to zoom in to a portion of the demo screen so that the audience can get a good look at it. You also can use it to write on a presentation screen.

And no chapter covering Sysinternals would be complete without a mention of the infamous Bluescreen Screen Saver, which is not included with the Sysinternals Suite; you must download it separately. As the name suggests, it mimics a STOP error (aka Blue Screen of Death) as part of a normal screen saver. If you're tempted to install it on a colleague's workstation as a prank, be prepared to pay the price later.

CHAPTER 8

Diagnostics and Recovery Toolset

Most of the tools I highlight in this book are included with Windows or can be downloaded for free. The Microsoft Diagnostics and Recovery Toolset, better known as DaRT, is a noteworthy exception.

DaRT is packaged as a bootable Emergency Recovery Disk, and its feature list is packed with indispensable diagnosis and repair capabilities any IT pro will appreciate. It can repair PCs that won't start up and help fix a variety of problems that can otherwise render a PC unusable. But its killer feature is the prosaically named Crash Analyzer, which reliably uncovers the cause of frustrating STOP errors—aka the Blue Screen of Death (BSOD).

DaRT traces its ancestry back to Emergency Repair Disk Commander, a product of Winternals Software that was split off from that company’s Sysinternal Utilities when Microsoft acquired the company in 2006. (I highlighted the free Sysinternal Utilities in Chapter 7.) DaRT, in sharp contrast, is not free.

To legally acquire and use this impressive collection of recovery and troubleshooting tools, you need the Microsoft Desktop Optimization Pack (MDOP), which is available as a benefit for Microsoft Windows Volume Licensing customers who have purchased a Software Assurance subscription. MDOP is also available for evaluation as part of most Visual Studio (MSDN) subscriptions.

In this chapter, I assume that you have already downloaded MDOP 2015, in x86 or x64 format, from https://technet.microsoft.com/mdop.aspx.

What DaRT does

DaRT 10, the most recent release, is compatible with Windows 10 and Windows Server 2012 R2.

More details online

This chapter offers an introduction to DaRT. For detailed DaRT 10 documentation, see this page on TechNet: http://go.microsoft.com/fwlink/?LinkID=613764 . The DaRT 10 Release Notes are here: http://go.microsoft.com/fwlink/?LinkID=613765 .

When you start a PC using the DaRT recovery media (typically on a DVD or USB flash drive), choose the Troubleshoot option to reach the screen shown in Figure 8-1.

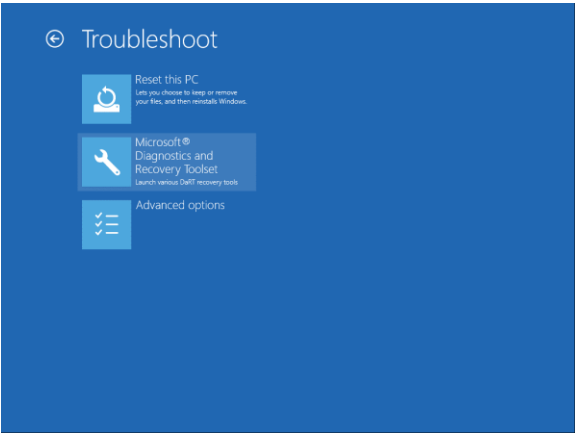
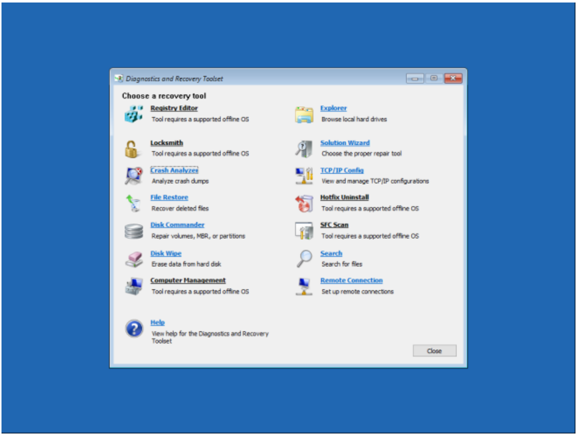

Troubleshoot
Reset this PC
Lets you choose to keep or remove your files, and then reinstalls Windows.
Microsoft® Diagnostics and Recovery Toolset
Launch various DaRT recovery tools
Advanced options

Figure 8-1: The bootable DaRT recovery media adds this option to the standard Windows 10 troubleshooting menu.

Choosing the Microsoft Diagnostics And Recovery Toolset option opens a dialog box in which you can connect to a network. This is followed by the wide-ranging menu in the Diagnostics And Recovery Toolset dialog box, as shown in Figure 8-2.



Diagnostics and Recovery Toolset

Choose a recovery tool

Registry Editor
Tool requires a supported offline OS

Locksmith
Tool requires a supported offline OS

Crash Analyzer
Analyze crash dumps

File Restore
Recover deleted files

Disk Commander
Repair volumes, MBR, or partitions

Disk Wipe
Erase data from hard disk

Computer Management
Tool requires a supported offline OS

Explorer
Browse local hard drives

Solution Wizard
Choose the proper repair tool

TCP/IP Config
View and manage TCP/IP configurations

Hotfix Uninstall
Tool requires a supported offline OS

SFC Scan
Tool requires a supported offline OS

Search
Search for files

Remote Connection
Set up remote connections

Help
View help for the Diagnostics and Recovery Toolset

Figure 8-2: Starting from the DaRT recovery media displays this menu of diagnostic and repair options. Note that you must run the Solution Wizard to turn on some tools on the list.

Using the TCP/IP Config option, you can tweak network addresses, if needed, and with the Remote Connection tool, you can make a system available for a help desk to access using the DaRT Remote Viewer tool.

Finding and recovering files

If a PC running Windows 10 refuses to start properly, one of your first priorities before you begin troubleshooting is to recover important data files from that machine. The Explorer tool, shown in Figure 8-3, offers basic file management capabilities with which you can copy files to another drive or a network share before you take a radical step like resetting or reimaging the PC.

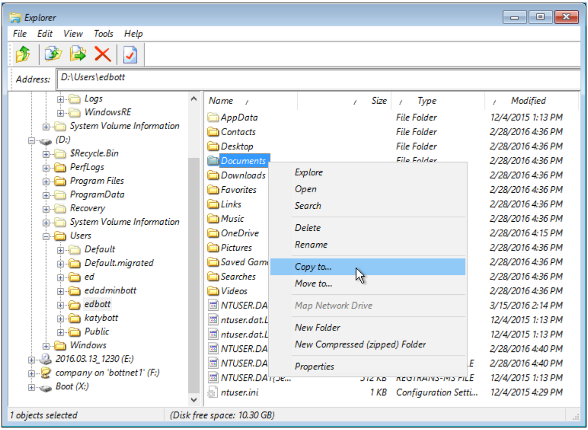


Figure 8-3: DaRT's Explorer tool doesn't have the bells and whistles that you'll find in the Windows 10 File Explorer, but it's extremely useful for recovering files from a PC that won't boot.

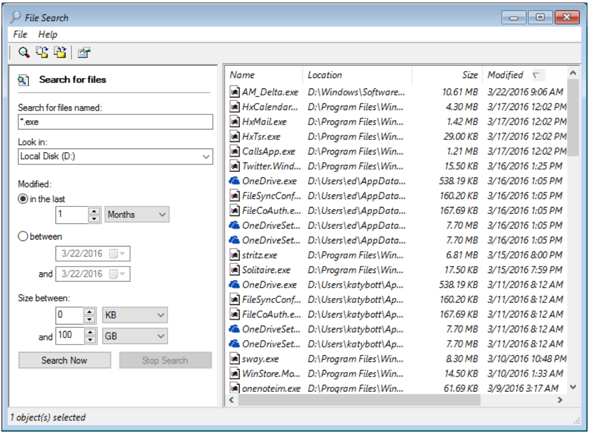
To connect to a network drive, click the Tools menu, choose Map Network Drive, and then type the details for the network computer and shared folder in UNC syntax *(\\computer\share)*, providing a user name and password with access to that share. The mapped drive appears in the navigation pane with a drive letter that you can specify during setup. Right-click any drive in the navigation pane to see its capacity, used space, and free space.

Note that you might need to provide the recovery key for a volume that is encrypted using BitLocker Drive Encryption.

Another indispensable file tool is Search, shown in Figure 8-4. You can search for files by date, size, or both, using wildcards to narrow the list to those with a particular string in the file name or a specific extension.

Be careful with drive letters!

When you start a Windows 10 PC using DaRT 10 recovery media, the letters assigned to available volumes don’t necessarily match those that are assigned when you start Windows 10 normally. You might find, for example, that, the DaRT recovery disk lists the small System Reserved partition (which has no drive letter in Windows 10) as drive C. In that configuration, the system drive, which contains Windows files and user profiles for each account on the machine, is listed as drive D instead of its normal C. Be extremely careful when using the disk tools included with DaRT 10 so that you don’t inadvertently wipe out valuable data or system files.



Search for files

Search for files named: *.exe

Look in: Local Disk (D:)

Modified:

● in the last 1 Months

○ between 3/22/2016 and 3/22/2016

Size between: 0 KB and 100 GB

Name	Location	Size	Modified
AM_Delta.exe	D:\Windows\Software...	10.61 MB	3/22/2016 9:06 AM
HxCalendar...	D:\Program Files\Win...	4.30 MB	3/17/2016 12:02 PM
HxMail.exe	D:\Program Files\Win...	1.42 MB	3/17/2016 12:02 PM
HxTsr.exe	D:\Program Files\Win...	29.00 KB	3/17/2016 12:02 PM
CallsApp.exe	D:\Program Files\Win...	1.21 MB	3/17/2016 12:02 PM
Twitter.Wind...	D:\Program Files\Win...	15.50 KB	3/16/2016 1:25 PM
OneDrive.exe	D:\Users\ed\AppData...	538.19 KB	3/16/2016 1:05 PM
FileSyncConf...	D:\Users\ed\AppData...	160.20 KB	3/16/2016 1:05 PM
FileCoAuth.e...	D:\Users\ed\AppData...	167.69 KB	3/16/2016 1:05 PM
OneDriveSet...	D:\Users\ed\AppData...	7.70 MB	3/16/2016 1:05 PM
OneDriveSet...	D:\Users\ed\AppData...	7.70 MB	3/16/2016 1:05 PM
stritz.exe	D:\Program Files\Win...	6.81 MB	3/15/2016 8:00 PM
Solitaire.exe	D:\Program Files\Win...	17.50 KB	3/15/2016 7:59 PM
OneDrive.exe	D:\Users\katybott\Ap...	538.19 KB	3/11/2016 8:12 AM
FileSyncConf...	D:\Users\katybott\Ap...	160.20 KB	3/11/2016 8:12 AM
FileCoAuth.e...	D:\Users\katybott\Ap...	167.69 KB	3/11/2016 8:12 AM
OneDriveSet...	D:\Users\katybott\Ap...	7.70 MB	3/11/2016 8:12 AM
OneDriveSet...	D:\Users\katybott\Ap...	7.70 MB	3/11/2016 8:12 AM
sway.exe	D:\Program Files\Win...	8.30 MB	3/10/2016 10:48 PM
WinStore.Mo...	D:\Program Files\Win...	14.50 KB	3/10/2016 1:33 AM
onenoteim.exe	D:\Program Files\Win...	61.69 KB	3/9/2016 3:17 AM

1 object(s) selected

Figure 8-4: You can use DaRT to search for files on any accessible volume. Click headings in the results pane to sort by that value.

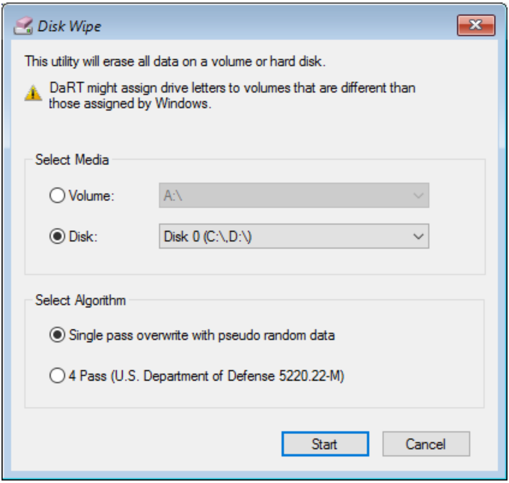
> **Note** You cannot use the Search tool to copy files to an external drive or network location.

A third tool, File Restore, includes a search interface that's similar to the one shown in Figure 8-4, except that it lists files that can be recovered from the Recycle Bin on the destination PC.

Working with disks

Using Disk Commander, you can repair certain types of drive errors that can prevent a system from starting properly. For example, you can restore the Master Boot Record or GPT header. You can also back up and restore partition information.

The Disk Wipe utility offers the capability to securely erase information on a logical volume or an entire drive—an excellent precaution if you’re removing a device from service or transferring it to a third party and you want to be sure that any confidential information is protected from recovery using low-level disk tools.



This utility will erase all data on a volume or hard disk.

DaRT might assign drive letters to volumes that are different than those assigned by Windows.

Select Media

○ Volume: A:\

● Disk: Disk 0 (C:\,D:\)

Select Algorithm

● Single pass overwrite with pseudo random data

○ 4 Pass (U.S. Department of Defense 5220.22-M)

Figure 8-5: You can use the Disk Wipe utility to securely erase and overwrite the contents of a drive so that it can't be recovered using drive editing tools.

Advanced recovery tools

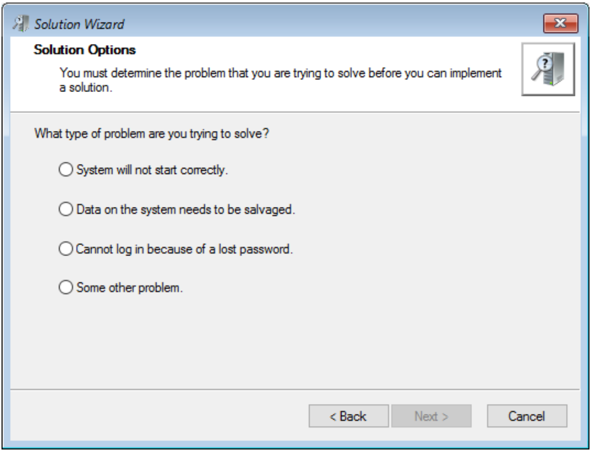
In the DaRT welcome screen shown earlier in Figure 8-2, you might have noticed that five of the options were unavailable, with a message beneath each one noting that the tool "requires a supported offline OS."

These tools include the following:

- **Computer Management** With this grab bag of administrative tools, you can view event logs, work with drives, and manage systems and drivers, among other things.
- **Registry Editor** Use this tool to access and change the registry of the local PC. You can add, remove, or edit keys and values, either interactively or by using .reg files.
- **Locksmith** Using this powerful tool, you can change the password for any local account, including the local Administrator account. (It doesn’t work with domain accounts.) You don’t have to know the current password.
- **Hotfix Uninstall** If you need to remove an update that is causing a system to fail at startup, this is your best option.
- **SFC Scan** Use this tool to check system files and repair them if necessary. It starts the System File Repair Wizard.

The supported way to gain access to these tools is by using the Microsoft Deployment Toolkit.

If you’re not sure which tool to use, try the Solution Wizard option, which runs through a brief but thorough interview that begins with the step shown in Figure 8-6.



Solution Options

You must determine the problem that you are trying to solve before you can implement a solution.

What type of problem are you trying to solve?

○ System will not start correctly.

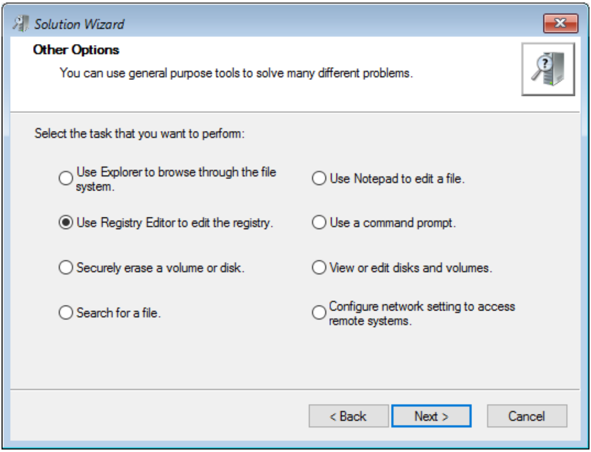
○ Data on the system needs to be salvaged.

○ Cannot log in because of a lost password.

○ Some other problem.

Figure 8-6: When you run the DaRT Recovery Image Solution Wizard, it conducts a quick interview that helps narrow down the correct tool to use.

If you can’t narrow down the problem to a specific symptom with its own tool, you’ll eventually end up at the Other Options page shown in Figure 8-7, where you can specify the exact tool that you want to use.



Solution Wizard

Other Options

You can use general purpose tools to solve many different problems.

Select the task that you want to perform:

- ○ Use Explorer to browse through the file system.
- ○ Use Notepad to edit a file.
- ● Use Registry Editor to edit the registry.
- ○ Use a command prompt.
- ○ Securely erase a volume or disk.
- ○ View or edit disks and volumes.
- ○ Search for a file.
- ○ Configure network setting to access remote systems.

Figure 8-7: On the Other Options page in the Solution Wizard, you can choose specific tools to solve specific problems.

The one option I didn't mention, Crash Analyzer, gets its own section later in this chapter.

Getting started with DaRT

As I mentioned earlier in this chapter, I assume that you or your organization is properly licensed to use DaRT 10 as part of MDOP 2015. In the case of MSDN subscriptions, that license is for test and evaluation purposes and not for production use.

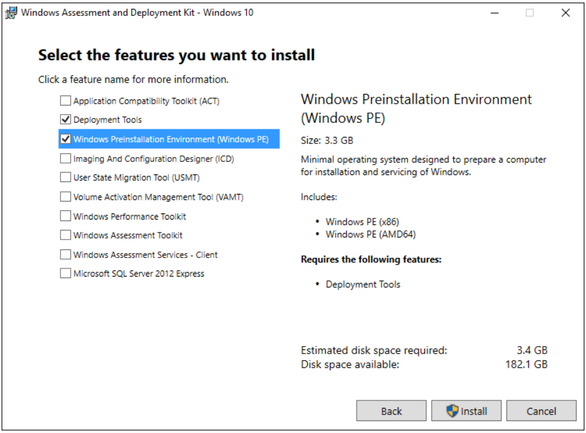
MDOP (available from the Volume Licensing Service Center or from MSDN's Subscription Downloads site) arrives as a disk image, in .iso format. Double-click it to mount the image as a virtual drive, and then extract the DaRT 10 subfolder to a local drive. From that location, choose the language and platform type (x86 or x64) to locate the correct installer for your system.

Running that setup file creates a new Microsoft DaRT 10 program group containing three shortcuts: Crash Analyzer, DaRT Recovery Image, and DaRT Remote Connection Viewer

Although the DaRT tools are self-contained, you need two additional pieces of software to create a recovery image that makes available all of advanced features in DaRT.

First, download the Windows Assessment and Deployment Kit (ADK) for Windows 10. With this option, you can install the Windows 10 Deployment Tools and the Windows Preinstallation Environment (WinPE), which is an essential part of the DaRT recovery image. You'll find the ADK at https://msdn.microsoft.com/windows/hardware/dn913721.aspx.

Run its setup program and clear the check boxes for features until only the two options shown in Figure 8-8 are on the list. Click Install to complete the installation.



Windows Assessment and Deployment Kit - Windows 10

Select the features you want to install

Click a feature name for more information.

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

Windows Preinstallation Environment (Windows PE)

Size: 3.3 GB

Minimal operating system designed to prepare a computer for installation and servicing of Windows.

Includes:

- Windows PE (x86)
- Windows PE (AMD64)

Requires the following features:

- Deployment Tools

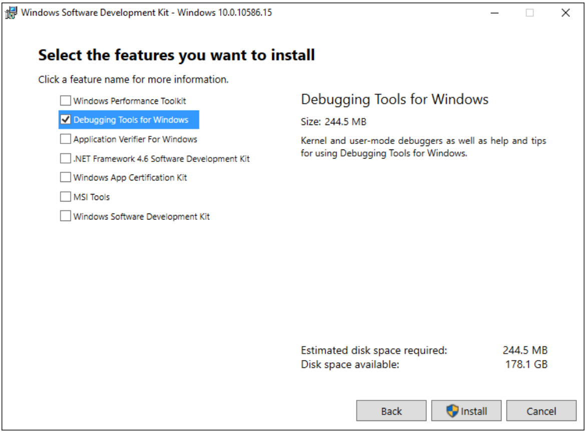
Estimated disk space required: 3.4 GB
Disk space available: 182.1 GB

Figure 8-8: To create a DaRT recovery image, you must first install the Windows Assessment and Deployment Toolkit with these options selected.

In addition, assuming that you plan to use the Crash Analyzer tool, you must install the Windows Debugging Tools. They're available as part of the Windows 10 Software Development

Kit (SDK) at https://dev.windows.com/downloads/windows-10-sdk.

Although the SDK itself is large, the Windows Debugging Tools themselves are relatively compact. This is the only piece of the SDK you absolutely need to install, as shown in Figure 8-9.



Windows Software Development Kit - Windows 10.0.10586.15

Select the features you want to install

Click a feature name for more information.

- □ Windows Performance Toolkit
- ☑ Debugging Tools for Windows
- □ Application Verifier For Windows
- □ .NET Framework 4.6 Software Development Kit
- □ Windows App Certification Kit
- □ MSI Tools
- □ Windows Software Development Kit

Debugging Tools for Windows

Size: 244.5 MB

Kernel and user-mode debuggers as well as help and tips for using Debugging Tools for Windows.

Estimated disk space required:	244.5 MB
Disk space available:	178.1 GB

Figure 8-9: If you plan to use the Crash Analyzer to identify the cause of STOP errors (the dreaded BSOD), install this part of the Windows 10 SDK.

You'll also need Windows 10 installation media to create the recovery image. If you have downloaded the Windows 10 installer files in ISO format, you can double-click that disk image to mount it as a virtual drive before running the wizard that creates the recovery image.

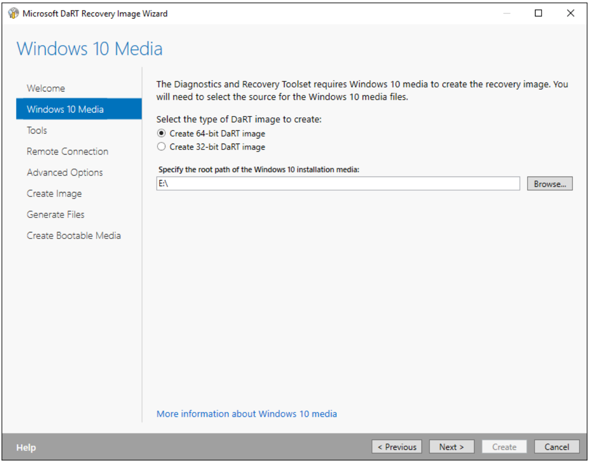
Later, when you run the Crash Analyzer, you'll need debugging symbols for the PC you're working with. However, you don't need those to create the initial recovery image.

With those prerequisites out of the way, you're ready to create a recovery image.

Creating a recovery image

Having the DaRT tools at your fingertips when you need them requires some advance preparation. The DaRT Recovery Image Wizard is a straightforward tool, which creates a bootable Windows image in ISO format. You can start up from that ISO file directly by attaching it to a virtual machine; to boot from a physical device, you need to create startup media.

After clicking past the Welcome message, you're prompted to select the type of DaRT image you want to create, x64 or x86. You'll need corresponding Windows 10 installation media, which can be in the form of a USB drive, a DVD, or a mounted ISO image file (you can also specify the location of a subfolder containing the full set of installation files). Enter the path of the physical or virtual drive containing the installer files, as shown in Figure 8-10, and then click Next to continue.



Windows 10 Media

The Diagnostics and Recovery Toolset requires Windows 10 media to create the recovery image. You will need to select the source for the Windows 10 media files.

Select the type of DaRT image to create:

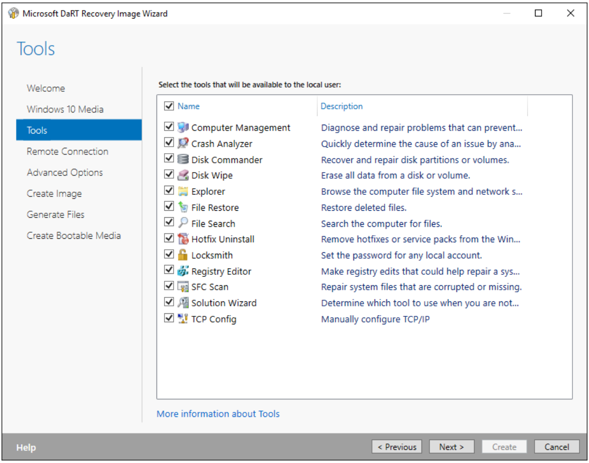
● Create 64-bit DaRT image

○ Create 32-bit DaRT image

Specify the root path of the Windows 10 installation media: E:\

Figure 8-10: Creating a DaRT recovery image requires Windows 10 installation media.

On the next page, you specify which tools are available for the recovery image. By default, the entire collection is selected, as shown in Figure 8-11. You might want to remove specific tools from the list when creating devices for other people to use. Disk Commander and Disk Wipe, for example, are potentially destructive tools.



Select the tools that will be available to the local user:

☑ Name	Description
☑ Computer Management	Diagnose and repair problems that can prevent...
☑ Crash Analyzer	Quickly determine the cause of an issue by ana...
☑ Disk Commander	Recover and repair disk partitions or volumes.
☑ Disk Wipe	Erase all data from a disk or volume.
☑ Explorer	Browse the computer file system and network s...
☑ File Restore	Restore deleted files.
☑ File Search	Search the computer for files.
☑ Hotfix Uninstall	Remove hotfixes or service packs from the Win...
☑ Locksmith	Set the password for any local account.
☑ Registry Editor	Make registry edits that could help repair a sys...
☑ SFC Scan	Repair system files that are corrupted or missing.
☑ Solution Wizard	Determine which tool to use when you are not...
☑ TCP Config	Manually configure TCP/IP

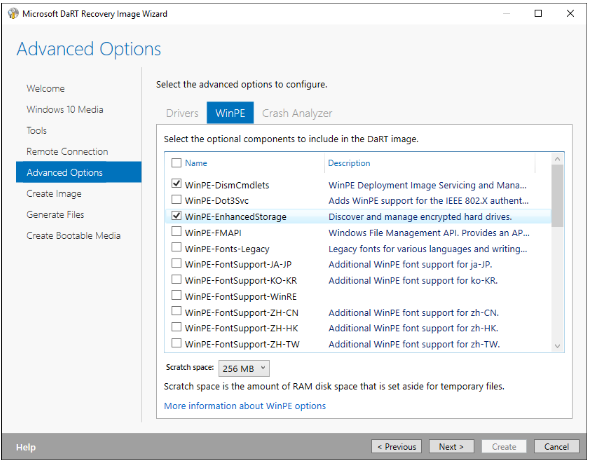
More information about Tools

Figure 8-11: When creating a recovery image, you can select which tools to include.

On the next wizard page, you specify whether to allow remote connections to the device from which you just started. With this option turned on, you can also specify a standard port to use, instead of allowing Windows to choose a port dynamically. Use this option to simplify the process of configuring the Windows Firewall on the machine you plan to use to do remote troubleshooting and repairs.

The Advanced Options step includes three tabs. With the first, Drivers, you can include specific hardware drivers in the recovery image. Use this option if you know you'll be using the recovery image on hardware that requires network or storage drivers that are not part of the standard Windows 10 installation files.

On the WinPE tab, shown in Figure 8-12, you can include specialized tools for working with systems. In this example, I've included the Deployment Image Servicing and Management PowerShell cmdlets and tools for working with drives that include hardware encryption. For common troubleshooting tasks, you can safely skip these options.



Advanced Options

Select the advanced options to configure.

Select the optional components to include in the DaRT image.

☐ Name	Description
☑ WinPE-DismCmdlets	WinPE Deployment Image Servicing and Mana...
☐ WinPE-Dot3Svc	Adds WinPE support for the IEEE 802.X authent...
☑ WinPE-EnhancedStorage	Discover and manage encrypted hard drives.
☐ WinPE-FMAPI	Windows File Management API. Provides an AP...
☐ WinPE-Fonts-Legacy	Legacy fonts for various languages and writing...
☐ WinPE-FontSupport-JA-JP	Additional WinPE font support for ja-JP.
☐ WinPE-FontSupport-KO-KR	Additional WinPE font support for ko-KR.
☐ WinPE-FontSupport-WinRE	
☐ WinPE-FontSupport-ZH-CN	Additional WinPE font support for zh-CN.
☐ WinPE-FontSupport-ZH-HK	Additional WinPE font support for zh-HK.
☐ WinPE-FontSupport-ZH-TW	Additional WinPE font support for zh-TW.

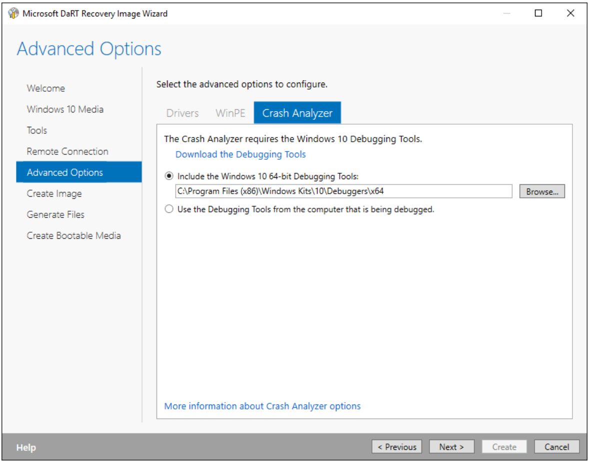
Scratch space: 256 MB

Scratch space is the amount of RAM disk space that is set aside for temporary files.

More information about WinPE options

Figure 8-12: These optional WinPE components aren’t necessary for most garden-variety troubleshooting tasks.

On the Crash Analyzer tab (see Figure 8-13), you can include debugging tools directly in the recovery image and as part of any startup media you create by using that image.



Advanced Options

Select the advanced options to configure.

The Crash Analyzer requires the Windows 10 Debugging Tools.

Download the Debugging Tools

● Include the Windows 10 64-bit Debugging Tools:

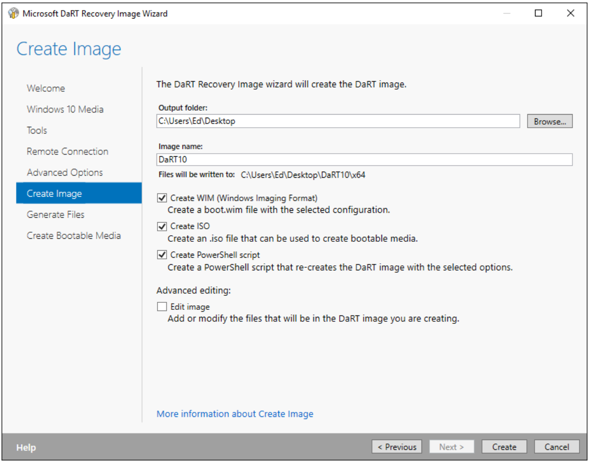
C:\Program Files (x86)\Windows Kits\10\Debuggers\x64

○ Use the Debugging Tools from the computer that is being debugged.

More information about Crash Analyzer options

Figure 8-13: Using DaRT's Crash Analyzer requires the Windows 10 Debugging Tools. If they're not included here, you'll need to install them on the destination machine.

Figure 8-14 shows the Create Image wizard page, where you can, consolidate all of the preceding options into a Windows 10 image file. Here, you specify an output folder, give the image a descriptive name, and then choose which formats you want to create.



The DaRT Recovery Image wizard will create the DaRT image.

Output folder: C:\Users\Ed\Desktop

Image name: DaRT10

Files will be written to: C:\Users\Ed\Desktop\DaRT10\x64

☑ Create WIM (Windows Imaging Format)
Create a boot.wim file with the selected configuration.

☑ Create ISO
Create an .iso file that can be used to create bootable media.

☑ Create PowerShell script
Create a PowerShell script that re-creates the DaRT image with the selected options.

Advanced editing:

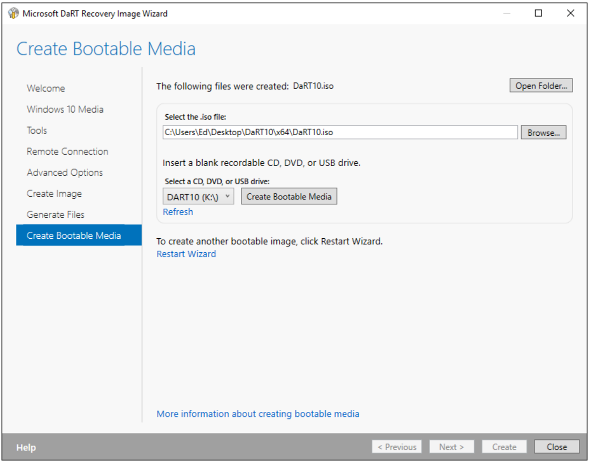
□ Edit image
Add or modify the files that will be in the DaRT image you are creating.

Figure 8-14: The essential option here is the one to create an ISO file, which you can then use to create bootable media for on-site troubleshooting.

The Windows Imaging Format (WIM) format is most useful if you're planning to add DaRT as part of a custom recovery partition on systems you image using deployment tools. The more common option is the one in the middle, which creates a standard ISO image that you can use to create bootable media.

After you complete that task, use the final page of the wizard, Create Bootable Media, to copy the files you just created to a USB flash drive or

DVD. Figure 8-15 shows this action with a USB flash drive available in drive K.


Microsoft DaRT Recovery Image Wizard

Create Bootable Media

The following files were created: DaRT10.iso

Select the .iso file: C:\Users\Ed\Desktop\DaRT10\x64\DaRT10.iso

Insert a blank recordable CD, DVD, or USB drive.

Select a CD, DVD, or USB drive: DART10 (K:\)

To create another bootable image, click Restart Wizard.

Figure 8-15: Immediately after creating the ISO recovery image, copy it to bootable media, label the drive, and then save it with other troubleshooting tools.

The DaRT recovery drive doesn't need to be large. Windows 10 installation media typically requires an 8 GB drive, but the DaRT recovery image takes only a tiny fraction of that space. In fact, it's small enough to fit on a writable CD.

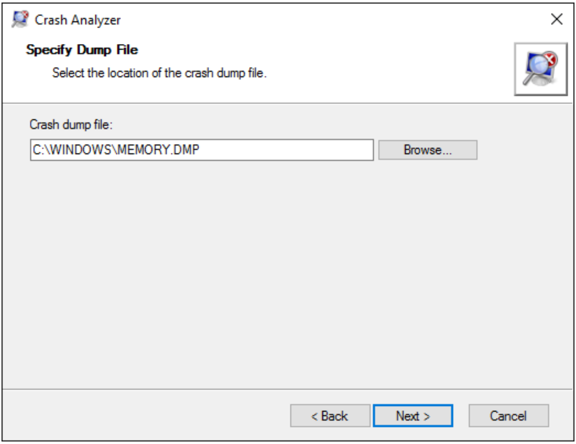
One caution: Creating the bootable recovery media will format the drive and erase any files on it.

Using Crash Analyzer

Tracking down the cause of a STOP error (typically known by the more colorful moniker Blue Screen of Death, or BSOD) can be frustrating. By design, STOP errors do exactly what the name says: Shut the system down, forcefully and without warning, when a serious error compromises the integrity of the operating system.

For most STOP errors, Windows is able to save a dump of the memory state at the time that the system encountered the error. DaRT's Crash Analyzer can inspect that dump file and provide important clues about the cause of the crash.

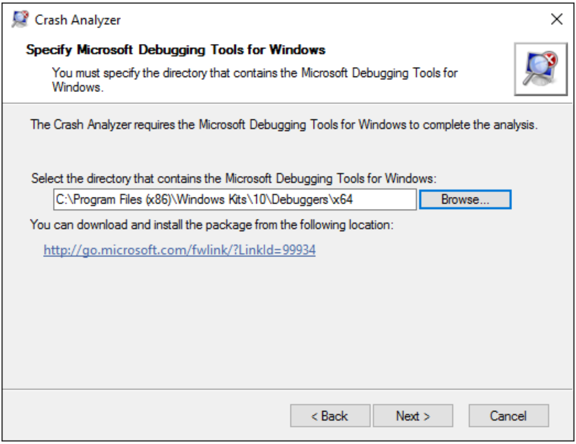
The Memory.dmp file is saved by default in the system folder (C:\Windows). If DaRT is installed on the machine that experienced the error (or if you've started from the DaRT Recovery Image), you can run Crash Analyzer directly and point it to the Memory.dmp file in that location, as I've done here.



C:\WINDOWS\MEMORY.DMP

Otherwise, consider copying the dump file (which can be very large) to removable media or to a network store, and then specifying that file in Crash Analyzer.

As noted earlier, you must have the Windows Debugging Tools installed on the machine on which you’re running Crash Analyzer. The first time you run the tool, you are prompted to enter the location of those files, as shown in Figure 8-16.



Specify Microsoft Debugging Tools for Windows

You must specify the directory that contains the Microsoft Debugging Tools for Windows.

The Crash Analyzer requires the Microsoft Debugging Tools for Windows to complete the analysis.

Select the directory that contains the Microsoft Debugging Tools for Windows:

C:\Program Files (x86)\Windows Kits\10\Debuggers\x64

You can download and install the package from the following location:

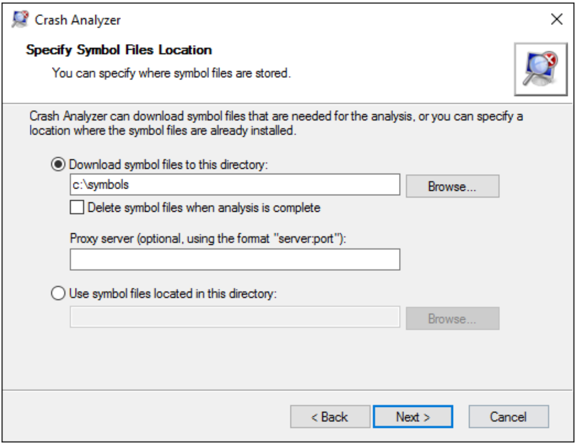
http://go.microsoft.com/fwlink/?LinkId=99934

Figure 8-16: You have to specify a location for the Debugging Tools for Windows when you first run Crash Analyzer. Note that the 64-bit tools are located in the Program Files (x86) folder.

If you’re momentarily confused when you go looking for those debugging tools, you’re probably not alone. Both the x86 and x64 versions of these tools are located in a nested subfolder of the Program Files (x86) folder. So, even if you’re using a 64-bit version of Windows, that’s where you should look.

Next, you need to supply symbols files that match the version of Windows that created the dump file. As you can see in Figure 8-17, Crash

Analyzer offers to download those symbols for you and store them in the C:\Symbols folder.


Crash Analyzer

Specify Symbol Files Location

You can specify where symbol files are stored.

Crash Analyzer can download symbol files that are needed for the analysis, or you can specify a location where the symbol files are already installed.

● Download symbol files to this directory:

c:\symbols

□ Delete symbol files when analysis is complete

Proxy server (optional, using the format "server:port"):

○ Use symbol files located in this directory:

Figure 8-17: Properly analyzing a dump file requires that you have access to symbol files for the Windows version that created that file.

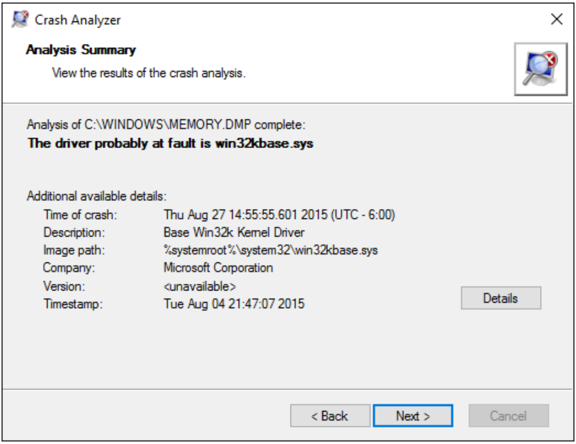
Download all the symbols

If you routinely troubleshoot systems running a broad range of Windows operating systems, you can download the full set of symbols for every supported desktop and server version of Windows from the Microsoft Symbol Server.

You can also download individual symbol sets as needed. For full details, see this page at Microsoft's Hardware Dev Center: https://msdn.microsoft.com/windows/hardware/gg463028.aspx.

When you use Crash Analyzer in the future, you can specify the location of the symbol files you previously downloaded, assuming that they're the ones that match the dump file in question.

With those steps out of the way, let the analysis begin. Figure 8-18 shows the results for one STOP error I encountered on a Windows 10 PC recently.



Analysis Summary

View the results of the crash analysis.

Analysis of C:\WINDOWS\MEMORY.DMP complete:

The driver probably at fault is win32kbase.sys

Additional available details:

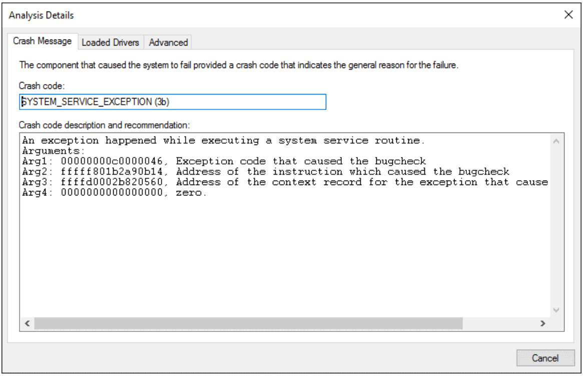
Time of crash:	Thu Aug 27 14:55:55.601 2015 (UTC - 6:00)
Description:	Base Win32k Kernel Driver
Image path:	%systemroot%\system32\win32kbase.sys
Company:	Microsoft Corporation
Version:	<unavailable>
Timestamp:	Tue Aug 04 21:47:07 2015

Figure 8-18: After completing its work, Crash Analyzer identifies the most likely cause of the STOP error.

In this case, Crash Analyzer revealed a Windows 10 system file as the cause of the crash. That doesn’t mean this file is defective; it means only that it was where the operation that caused the crash occurred. For a one-time event (as this was), you can probably ignore the error. But if Crash Analyzer identifies a third-party driver as the cause of a crash, you might want to look more closely at that driver and look for an update.

If you inadvertently supply the wrong symbol files, Crash Analyzer will dutifully analyze the dump file anyway and then return a message that pinpoints the errant driver as ntoskrnl.wrong.symbols.exe.

Crash Analyzer's output includes more than just that summary. Click the Details button to see the Analysis Details page. On the Crash Message tab, shown in Figure 8-19, you can see the STOP error code and the four arguments included with it. These details are available in Event Viewer but are more convenient to examine and save here.



The component that caused the system to fail provided a crash code that indicates the general reason for the failure.

Crash code:

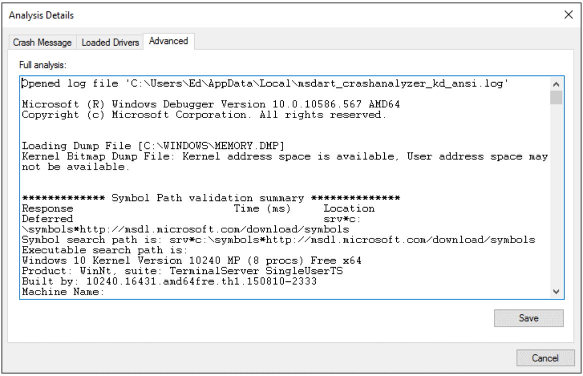
SYSTEM_SERVICE_EXCEPTION (3b)

Crash code description and recommendation:

```
An exception happened while executing a system service routine.
Arguments:
Arg1: 00000000c0000046, Exception code that caused the bugcheck
Arg2: fffff801b2a90b14, Address of the instruction which caused the bugcheck
Arg3: ffffd0002b820560, Address of the context record for the exception that cause
Arg4: 0000000000000000, zero.
```

Figure 8-19: The Crash Message page shows the STOP error code, which can be a useful starting point when searching for possible solutions to a rash of crashes.

The Advanced tab offers exhaustive output from Crash Analyzer, as shown in Figure 8-20. Click Save to preserve a copy for use when filing a bug report or corresponding with support personnel at Microsoft or a third-party vendor.



```
Opened log file 'C:\Users\Ed\AppData\Local\msdart_crashanalyzer_kd_ansi.log'

Microsoft (R) Windows Debugger Version 10.0.10586.567 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.


Loading Dump File [C:\WINDOWS\MEMORY.DMP]
Kernel Bitmap Dump File: Kernel address space is available, User address space may
not be available.


************* Symbol Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       srv*c:
\symbols*http://msdl.microsoft.com/download/symbols
Symbol search path is: srv*c:\symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 10 Kernel Version 10240 MP (8 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 10240.16431.amd64fre.th1.150810-2333
Machine Name:
```

Figure 8-20: The Advanced tab contains a full log of all the findings from Crash Analyzer. Click Save if you need to share these details as part of a bug report.

CHAPTER 9

Windows PowerShell and the Command Prompt

Everything old is new again.

Windows users of a certain age remember the MS-DOS command line, perhaps not so fondly. But even after 20 years of trying to ditch its command-line past, Windows 10 still rewards those who understand the benefits of using a command line for some common tasks.

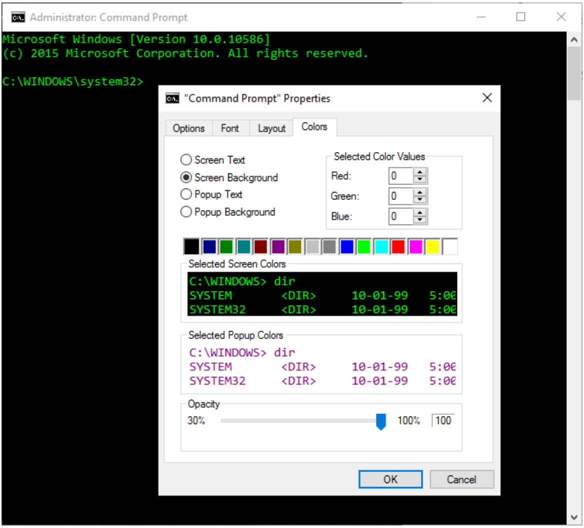
As system administrators have known all along, sometimes typing a command is just faster than using a graphical interface, and that's even truer for scripts that can carry out entire sequences of commands. Windows 10 includes a new-age command-based environment called Windows PowerShell, which offers tremendous power to those who are willing to invest a little time learning its ways.

But let's begin with…

The good ol' Command Prompt

The Windows Command Processor, Cmd.exe, is only superficially similar to its ancient forebear, MS-DOS. On a 64-bit Windows 10 system, Cmd.exe is a 64-bit native Windows process. The easiest way to open a Command Prompt is via the Quick Links menu (right-click Start or use the keyboard shortcut Windows key+X). That menu includes two Command Prompt options: one that runs under your user account and the other that runs as an Administrator.

You can also type **Cmd** in the search box and then click Command Prompt in the results list, or right-click that entry and then, on the shortcut menu, choose Open As Administrator to open an elevated Command Prompt window. The only visible difference between the two ways of starting this environment is the Administrator prefix, which appears in the title bar in an elevated Command Prompt session. You can see that subtle change in Figure 9-1, where I’ve also opened the customization properties for the Command Prompt window by right-clicking the icon at the left of the title bar and then choosing Properties.



```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

○ Screen Text
● Screen Background
○ Popup Text
○ Popup Background

Selected Color Values
Red: 0
Green: 0
Blue: 0

Selected Screen Colors

```
C:\WINDOWS> dir
SYSTEM          <DIR>        10-01-99    5:0€
SYSTEM32        <DIR>        10-01-99    5:0€
```

Selected Popup Colors

```
C:\WINDOWS> dir
SYSTEM          <DIR>        10-01-99    5:0€
SYSTEM32        <DIR>        10-01-99    5:0€
```

Opacity
30% 100% 100

Figure 9-1: Use the Colors tab to change the Command Prompt color scheme to this retro green-on-black combination. (Look at the file dates in the preview!)

Go from File Explorer to a Command Prompt with two clicks

You’re in File Explorer. You want to open a Command Prompt window in the current folder. Fortunately, there’s a shortcut for that:

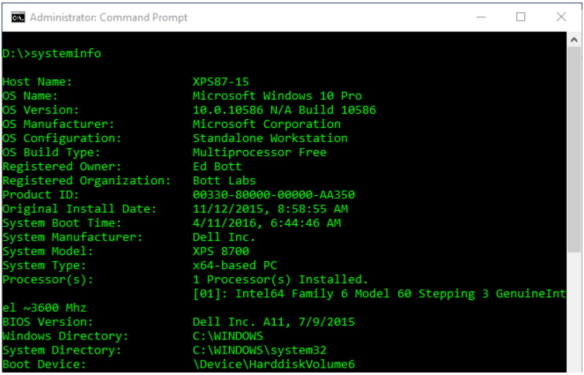
Hold down the Shift key as you right-click any empty space in the folder (make sure no files are selected) and then, on the shortcut menu, click Open Command Window Here.

If you’re not sure what you can do in a Windows 10 Command Prompt window, try typing **help**. That returns a list of 84 commands, with a brief description for each one. Want full syntax for a command? In the Command Prompt window, type the command name followed by the **/?** switch.

The command line is useful for some file management tasks, with syntax that hasn’t changed much since the days of MS-DOS. Thanks to wildcard characters, you can change the extension on a group of files in a folder, for example, using the command **ren *.htm *.html**. That job is nearly impossible in File Explorer.

But there are also a handful of commands you probably don’t know that can come in extremely handy. The following list contains a few commands I use regularly:

- **Systeminfo** This handy command spits out a lengthy description of the current system, including the host name, the Windows version and original installation date, domain or workgroup membership, networking details, and much more. Figure 9-2 shows a small portion of the output you can expect. Follow the command with the > symbol, followed by the full path of a destination file, to save the results in a file that you can consult later.

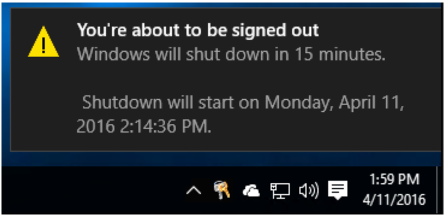


```
D:\>systeminfo

Host Name:                 XPS87-15
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.10586 N/A Build 10586
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Ed Bott
Registered Organization:   Bott Labs
Product ID:                00330-80000-00000-AA350
Original Install Date:     11/12/2015, 8:58:55 AM
System Boot Time:          4/11/2016, 6:44:46 AM
System Manufacturer:       Dell Inc.
System Model:              XPS 8700
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 60 Stepping 3 GenuineInt
el ~3600 Mhz
BIOS Version:              Dell Inc. A11, 7/9/2015
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume6
```

Figure 9-2: The output for the Systeminfo command contains many more details than the snippet shown here. Redirect the output to a text file to save the information for future reference.

- **Driverquery** If you’re curious about which drivers are installed on a given system (local or remote), this command is your friend. Use the **/FO CSV** switch to specify that you want the output in comma-separated values (CSV) format; redirect that output to a file and you can open it in Excel for more detailed analysis.

- **Icacls** This oddly named command allows you to manipulate permissions (access control lists, or ACLs) on files and folders. If you're unable to delete or rename a file or folder because of permissions, this command can help.
- **Shutdown** Sometimes, the Power menu doesn't contain the options you really need. This command, with its many switches (**/r** for restart and **/s** for shutdown, to name just two), can cover those different scenarios. Using the **/t** switch, you can specify how long to wait (in seconds) before executing the command. (The default is 30 seconds.) If you have a few tasks to finish up before lunch and want your PC to restart in 15 minutes, use the command **shutdown /r /t 900**. That produces a notification like the one shown in the image that follows. If you change your mind, use **shutdown /a** to cancel the planned shutdown or restart.



You're about to be signed out
Windows will shut down in 15 minutes.

Shutdown will start on Monday, April 11, 2016 2:14:36 PM.

- **Sc** With this, you can query, start, pause, stop, and configure services using the Service Control Manager. Its syntax is daunting but its capabilities are extremely powerful.
- **Tasklist** and **Taskkill** Using these matching commands, you can generate a list of running tasks and then forcibly end any process on that list. Taskkill is a blunt weapon but effective when you need it.

For faster navigation in a Command Prompt window, it's worth noting how the arrow keys work. Use the up and down arrows to scroll through and recall recent commands. Use the right arrow to repeat the previous command one character at a time, which can save you some typing if you need to reissue a command with a different parameter or switch. Finally, after recalling or entering a command but before pressing Enter, use the left and right arrows to move through the command and make changes as needed. When editing a command, press the Insert key to toggle between overtype mode (in which whatever you type replaces the existing contents of the command line) and insert mode, which adds whatever you type without disturbing the current command.

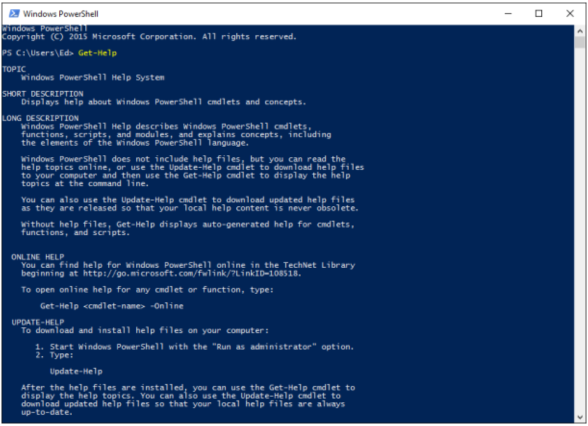
Introducing Windows PowerShell

The Windows 10 Command Prompt can trace its ancestry back more than three decades. Windows PowerShell is distinctly more modern, with version 1.0 arriving on the scene a mere decade ago.

PowerShell is an incredibly rich environment built for system administrators to automate tasks and configurations. Instead of a limited number of commands, Windows PowerShell offers *cmdlets*, which work with the file system, the registry, certificate stores, and just about anything in Windows (desktop and server editions) that you can manage. Cmdlets are available in core modules that are included with every edition of Windows 10. And, of course, the real goal for many of these cmdlets is for you to be able to combine them into scripts. If you're an administrator, you can use these scripts to perform repetitive management tasks quickly and effectively.

If you're not a system administrator, the sheer scope of Windows PowerShell can be extremely intimidating. But some tasks, including managing Microsoft Azure and Office 365, are ideally suited for Windows PowerShell commands. In this section, I just want to introduce the basics of Windows PowerShell so that you feel comfortable when you're required to dive into the deep end.

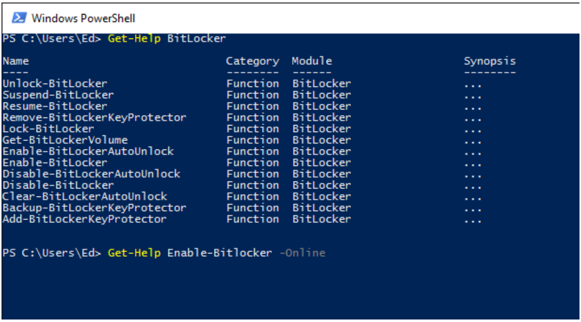
Windows PowerShell includes its own command-line environment, with a distinctive blue background that sets it apart from the Windows 10 Command Prompt. As Figure 9-3 illustrates, one of the first things any Windows PowerShell neophyte should do is to issue the Get-Help cmdlet, which includes a link to online help and detailed instructions for using the Update-Help cmdlet.



```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\Ed> Get-Help

TOPIC
    Windows PowerShell Help System

SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.

LONG DESCRIPTION
    Windows PowerShell Help describes Windows PowerShell cmdlets,
    functions, scripts, and modules, and explains concepts, including
    the elements of the Windows PowerShell language.

    Windows PowerShell does not include help files, but you can read the
    help topics online, or use the Update-Help cmdlet to download help files
    to your computer and then use the Get-Help cmdlet to display the help
    topics at the command line.

    You can also use the Update-Help cmdlet to download updated help files
    as they are released so that your local help content is never obsolete.

    Without help files, Get-Help displays auto-generated help for cmdlets,
    functions, and scripts.


  ONLINE HELP
    You can find help for Windows PowerShell online in the TechNet Library
    beginning at http://go.microsoft.com/fwlink/?LinkID=108518.

    To open online help for any cmdlet or function, type:

        Get-Help <cmdlet-name> -Online

  UPDATE-HELP
    To download and install help files on your computer:

       1. Start Windows PowerShell with the "Run as administrator" option.
       2. Type:

          Update-Help

    After the help files are installed, you can use the Get-Help cmdlet to
    display the help topics. You can also use the Update-Help cmdlet to
    download updated help files so that your local help files are always
    up-to-date.
```

Figure 9-3: Use the Get-Help cmdlet to get started in the interactive Windows PowerShell command-line environment.

Add a word to the end of Get-Help and you can find cmdlets that include that term. If you know there's a cmdlet for managing BitLocker but you can't remember exactly which one you need, try **Get-Help Bitlocker** to display this list. And you can jump directly to the online reference for a specific cmdlet by using the syntax **Get-Help <cmdlet> -Online**.

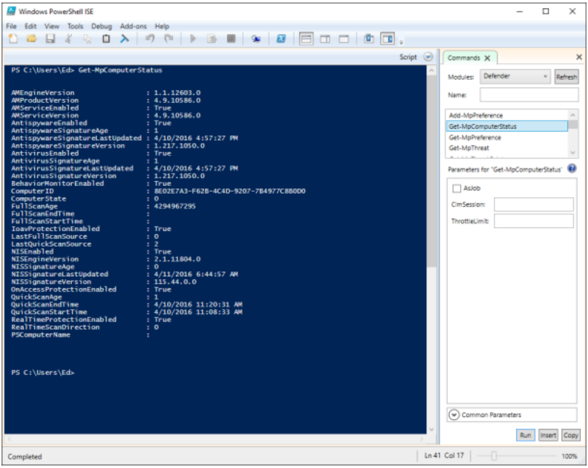


```
PS C:\Users\Ed> Get-Help BitLocker

Name                              Category  Module                    Synopsis
----                              --------  ------                    --------
Unlock-BitLocker                  Function  BitLocker                 ...
Suspend-BitLocker                 Function  BitLocker                 ...
Resume-BitLocker                  Function  BitLocker                 ...
Remove-BitLockerKeyProtector      Function  BitLocker                 ...
Lock-BitLocker                    Function  BitLocker                 ...
Get-BitLockerVolume               Function  BitLocker                 ...
Enable-BitLockerAutoUnlock        Function  BitLocker                 ...
Enable-BitLocker                  Function  BitLocker                 ...
Disable-BitLockerAutoUnlock       Function  BitLocker                 ...
Disable-BitLocker                 Function  BitLocker                 ...
Clear-BitLockerAutoUnlock         Function  BitLocker                 ...
Backup-BitLockerKeyProtector      Function  BitLocker                 ...
Add-BitLockerKeyProtector         Function  BitLocker                 ...

PS C:\Users\Ed> Get-Help Enable-Bitlocker -Online
```

Although Windows PowerShell cmdlets follow consistent capitalization, you don't need to worry about case. And if you're not sure of the exact name of a cmdlet, you can press the Tab key and use IntelliSense to offer suggestions. For example, type **get-p** and then press Tab to see the first matching cmdlet, Get-Package. Keep pressing Tab to cycle through Get-PackageProvider, Get-PackageSource, Get-Partition, and so on.

If you need more help, consider using the Windows PowerShell Integrated Scripting Environment (ISE), which offers a point-and-click graphical interface that takes a lot of the guesswork out of typing cmdlets. Figure 9-4 shows the Windows PowerShell ISE with the Commands window open on the right, with the

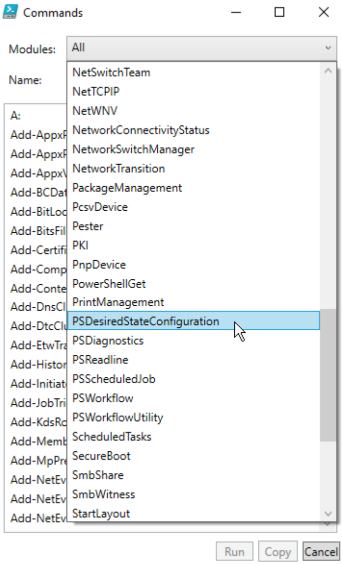
Get-MpComputerStatus cmdlet from the Defender module visible. I didn’t need to type a cmdlet; I just selected it from the list and then clicked Run.



```
PS C:\Users\Ed> Get-MpComputerStatus


AMEngineVersion                 : 1.1.12603.0
AMProductVersion                : 4.9.10586.0
AMServiceEnabled                : True
AMServiceVersion                : 4.9.10586.0
AntispywareEnabled              : True
AntispywareSignatureAge         : 1
AntispywareSignatureLastUpdated : 4/10/2016 4:57:27 PM
AntispywareSignatureVersion     : 1.217.1050.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 1
AntivirusSignatureLastUpdated   : 4/10/2016 4:57:27 PM
AntivirusSignatureVersion       : 1.217.1050.0
BehaviorMonitorEnabled          : True
ComputerID                      : 8E02E7A3-F62B-4C4D-9207-7B4977C8B0D0
ComputerState                   : 0
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : True
NISEngineVersion                : 2.1.11804.0
NISSignatureAge                 : 0
NISSignatureLastUpdated         : 4/11/2016 6:44:57 AM
NISSignatureVersion             : 115.44.0.0
OnAccessProtectionEnabled       : True
QuickScanAge                    : 1
QuickScanEndTime                : 4/10/2016 11:20:31 AM
QuickScanStartTime              : 4/10/2016 11:08:33 AM
RealTimeProtectionEnabled       : True
RealTimeScanDirection           : 0
PSComputerName                  :



PS C:\Users\Ed>
```

Figure 9-4: Using the Windows PowerShell ISE, you can dock a Commands window alongside the shell so that you can browse through the cmdlets in a module, and then click Run or Insert.

If you prefer a floating window instead of the docked pane, on the toolbar, click the Show Command Window button (second from the right). As Figure 9-5 shows, you can choose from the full selection of modules here, as well.



Modules: All

Figure 9-5: Although the Windows PowerShell ISE is tailor-made for creating Windows PowerShell scripts, its Commands add-on serves as a useful training tool.

CHAPTER 10

Hyper-V

My office has become considerably less cluttered in recent years, thanks to a Windows 10 feature called Hyper-V. Where there once was a workbench full of PCs in all shapes and sizes, using power and generating heat and noise, now those PCs are virtual.

Hyper-V adds virtualization capabilities to desktop versions of Windows 10 Pro and Enterprise editions, using the same industrial-strength hypervisor found in Windows Server editions. If you need a PC for testing purposes, you can build one, virtually, with just a few clicks. If you’ve never used Hyper-V, you’re in for a pleasant surprise.

The benefits of virtualization are profound. Consider these scenarios:

- You want to evaluate a new software program without the risk messing up your production system.
- You regularly train users or demonstrate features of a program or service and need a predictable demonstration environment that you can reset before each session.
- A program you rely on requires an earlier Windows version to run properly.
- You want to experiment with an alternative operating system, such as Linux.
- You need to access your corporate network using an environment that's completely separate from your personal files and email accounts.
- For test purposes, you need access to a Windows server.

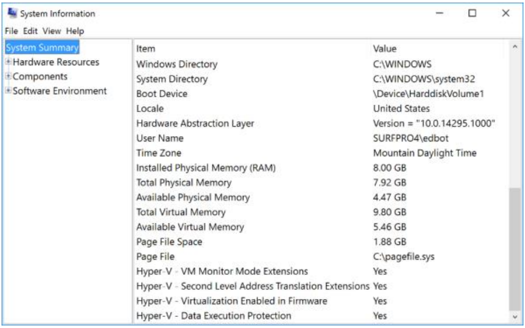
You can do all those things with Hyper-V, running on your own PC. To accomplish those tasks, you'll use two built-in tools, Hyper-V Manager and Virtual Machine Connection.

Hyper-V is not turned on by default, so that’s our first step.

Getting started with Hyper-V

Your first step is to check the system you want to use as the host for your virtual machines (VMs), to make sure it supports Hyper-V. You need a 64-bit version of Windows 10 Pro or Enterprise, of course, with sufficient resources (especially memory) to allocate to the VMs. I don’t recommend turning on Hyper-V on a PC unless it has at least 8 GB of RAM, and that minimum configuration requires that you manage memory carefully.

Most important, the CPU that powers your PC must support a handful of features that are crucial for the operation of the hypervisor. Most modern PCs designed for business use support these features. You can check whether your PC is compatible by using the built-in System Information app. In the search box, type **Msinfo32**, click the System Information entry at the top of the results list, and scroll to the bottom of the System Summary page, as shown in Figure 10-1.



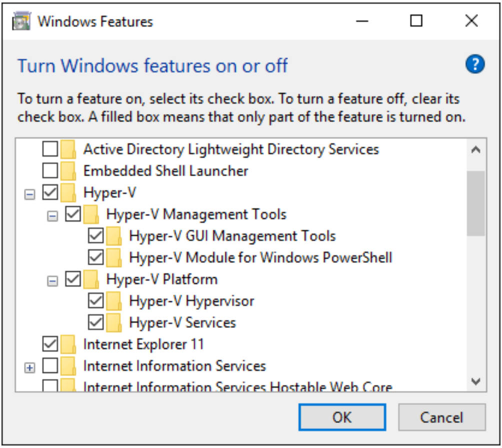
Item	Value
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "10.0.14295.1000"
User Name	SURFPRO4\edbot
Time Zone	Mountain Daylight Time
Installed Physical Memory (RAM)	8.00 GB
Total Physical Memory	7.92 GB
Available Physical Memory	4.47 GB
Total Virtual Memory	9.80 GB
Available Virtual Memory	5.46 GB
Page File Space	1.88 GB
Page File	C:\pagefile.sys
Hyper-V - VM Monitor Mode Extensions	Yes
Hyper-V - Second Level Address Translation Extensions	Yes
Hyper-V - Virtualization Enabled in Firmware	Yes
Hyper-V - Data Execution Protection	Yes

Figure 10-1: If you see “Yes” next to the four values at the bottom of this list, your system is capable of running Hyper-V.

(If the last entry in that list begins “A hypervisor has been detected…” Hyper-V is already turned on and you can move to the next step.)

These hardware requirements aren’t negotiable: A PC that doesn’t support these required features can’t run Hyper-V. In some cases, CPU capabilities required by Hyper-V might be turned off in firmware. If the Virtualization Enabled In Firmware setting says No, you’ll need to check the documentation for your system to determine how to access the BIOS or firmware settings and make available the required virtualization support.

If you have a green light, the next step is to turn Hyper-V on. In the search box, type **features** and then, in the results list, click Turn Windows Features On Or Off. That opens the Windows Features dialog box, shown in Figure 10-2. Make sure that all the Hyper-V options are selected and click OK.



Turn Windows features on or off

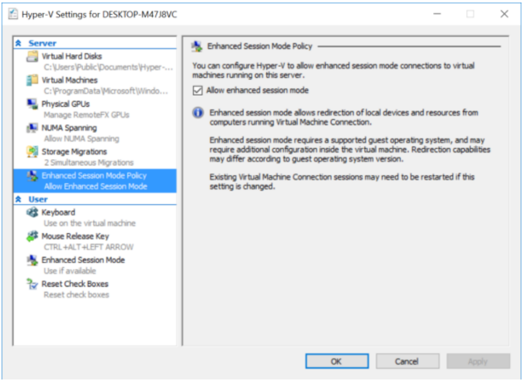
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ Active Directory Lightweight Directory Services
- □ Embedded Shell Launcher
- ⊟ ☑ Hyper-V
  - ⊟ ☑ Hyper-V Management Tools
    - ☑ Hyper-V GUI Management Tools
    - ☑ Hyper-V Module for Windows PowerShell
  - ⊟ ☑ Hyper-V Platform
    - ☑ Hyper-V Hypervisor
    - ☑ Hyper-V Services
- ☑ Internet Explorer 11
- ⊞ □ Internet Information Services
- □ Internet Information Services Hostable Web Core

Figure 10-2: Hyper-V isn't on by default. Use this dialog box to turn on the necessary features.

(You can also turn on and configure Hyper-V by using Windows PowerShell commands, but this option is simpler for a single PC.)

After restarting your PC, it’s a good idea to configure some virtualization settings. Open the newly installed Hyper-V Manager app (this is also a good time to pin that app to the Start menu and, optionally, the taskbar), and then, in the Actions pane on the right, click Hyper-V Settings. Figure 10-3 shows the available settings, which are arranged into two groups.



Hyper-V Settings for DESKTOP-M47J8VC

Server
- Virtual Hard Disks: C:\Users\Public\Documents\Hyper-...
- Virtual Machines: C:\ProgramData\Microsoft\Windo...
- Physical GPUs: Manage RemoteFX GPUs
- NUMA Spanning: Allow NUMA Spanning
- Storage Migrations: 2 Simultaneous Migrations
- Enhanced Session Mode Policy: Allow Enhanced Session Mode

User
- Keyboard: Use on the virtual machine
- Mouse Release Key: CTRL+ALT+LEFT ARROW
- Enhanced Session Mode: Use if available
- Reset Check Boxes: Reset check boxes

Enhanced Session Mode Policy

You can configure Hyper-V to allow enhanced session mode connections to virtual machines running on this server.

☑ Allow enhanced session mode

Enhanced session mode allows redirection of local devices and resources from computers running Virtual Machine Connection.

Enhanced session mode requires a supported guest operating system, and may require additional configuration inside the virtual machine. Redirection capabilities may differ according to guest operating system version.

Existing Virtual Machine Connection sessions may need to be restarted if this setting is changed.

Figure 10-3: It’s worth checking these Hyper-V settings before you create your first VM.

I recommend looking at the following three settings under the Server heading:

- **Virtual Hard Disks** This setting specifies the folder where virtual hard drives (VHDs) will be stored. By default, this location is on the system drive, in the Documents folder for the Public user account. That makes it possible for all users to access VHDs. If you're setting up Hyper-V on a desktop PC with multiple hard drives, you might want to change this location to a folder on the largest drive.

- **Virtual Machines** This setting specifies the folder where Hyper-V configuration and saved-state files will be stored. By default, this location is on the system drive, in a subfolder within the ProgramData folder. Although the configuration files for each VM are relatively small, the files for saving the state of a VM can become large. If space on the system drive is limited and you have a large, reasonably fast data drive, consider changing this location.
- **Enhanced Session Mode Policy** By default, this option is on, and I recommend you leave it on. (I explain how enhanced sessions work later in this chapter.)

Under the User heading, look at these settings:

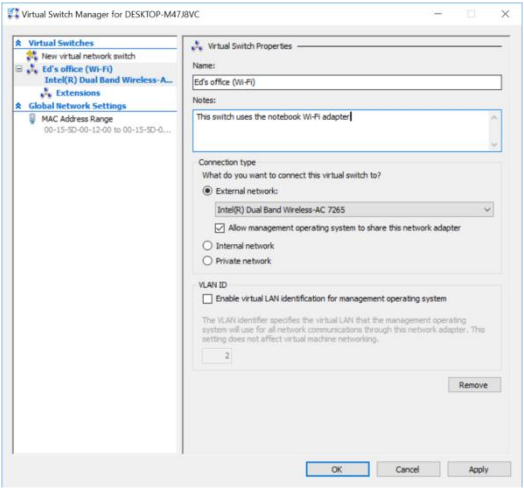
- **Keyboard** When a VM is running, you effectively have two PCs competing for the attention of system shortcuts like Alt+Tab.

The default setting sends Windows keyboard combinations to the VM when you're using it. You might prefer the third option on this page, which allows the VM to use those keystrokes only in full-screen mode.

- **Mouse release key** With certain operating systems running in VMs, you need to click in the Virtual Machine Connection window to use the mouse, and the mouse stops when it reaches the edge of the window. For those occasions, you can choose one of four special keyboard combinations to let the mouse back into the host PC environment.
- **Enhanced Session Mode** This is the user equivalent of the setting under the Server heading. I recommend leaving it turned on.

Click OK to save any changes you make to these settings.

Your next step should be to create a virtual switch. This option allows the virtual network adapter in a VM to share the physical network on your host PC. To begin the setup process, open Hyper-V Manager, display the Actions pane, and then click Virtual Switch Manager. That opens a dialog box like the one shown in Figure 10-4. Click New Virtual Network Switch to walk through the simple process of selecting the network adapter to share and giving the virtual switch a name, as I've done in Figure 10-4.


Virtual Switch Manager for DESKTOP-M47J8VC
Virtual Switches
New virtual network switch
Ed's office (Wi-Fi)
Intel(R) Dual Band Wireless-A...
Extensions
Global Network Settings
MAC Address Range
00-15-5D-00-12-00 to 00-15-5D-0...
Virtual Switch Properties

Name:
Ed's office (Wi-Fi)

Notes:
This switch uses the notebook Wi-Fi adapter

Connection type
What do you want to connect this virtual switch to?

● External network:
Intel(R) Dual Band Wireless-AC 7265
☑ Allow management operating system to share this network adapter

○ Internal network
○ Private network

VLAN ID
□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

Figure 10-4: Before a VM can connect to the Internet, you need to set up a virtual switch.

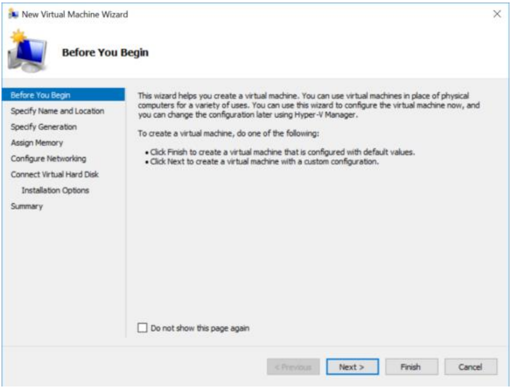
The three options here are interesting. External Network is generally the right choice. It assumes that you want to use your VM as if it were just another PC, sharing the host PC's network adapter to allow full Internet access and connections to other devices on the same network as the host PC.

The two remaining options don't allow access to the host PC's network adapter at all. Choose Internal Network if you want network access to the host PC on your local network; choose the Private Network option to isolate the VM completely from network communications. These two configurations are appropriate for security research and are mostly useful in situations for which you don't need Internet access and you want to avoid the risk that a threat within a VM can compromise the host PC or other devices on your network.

With those settings taken care of, you're now ready to create your first VM.

Creating a virtual machine

Hyper-V Manager provides an easy-to-use wizard to help you create a VM. In the Actions pane, click New > Virtual Machine to open that wizard to the introductory page shown in Figure 10-5. The New Virtual Machine Wizard is so simple, in fact, that you don't even need to click Next; you can create a VM using default settings with a single click of the Finish button.



This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

Figure 10-5: All of the steps in this wizard are optional. When you click Finish, your new VM uses default settings for any steps you skipped.

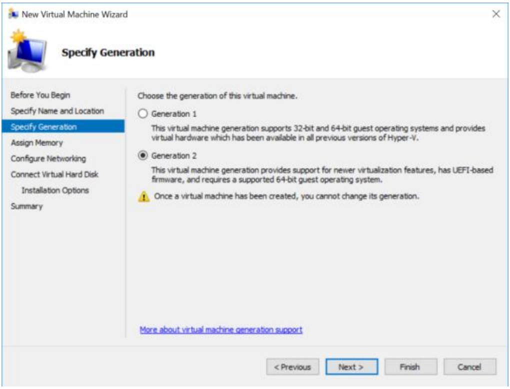
If you go for that simple solution, you'll probably need to manually adjust a few settings for the newly created VM. In particular, you'll want to change the name of the VM from the generic "New Virtual Machine" to something more descriptive. You'll also want to check the amount of RAM assigned—the default is only 1024 MB, which isn't adequate for installing Windows 10. You'll also need to connect the VM's network to the virtual switch you created earlier.

You can make all those changes from the Hyper-V Manager app (which I describe later in this chapter). But given all that, it might be easier for you to just run through the wizard and get everything configured properly from the start.

Setting up that VM involves configuring a full selection of virtualized hardware, including a virtual BIOS or UEFI firmware, virtual memory, VHDs, virtual network adapters, virtual DVD drives, and even virtual floppy disks (if you can find a reason to use one of those). Here's what you'll find in each step of the New Virtual Machine Wizard:

- **Specify Name And Location** Give the VM a descriptive name, which will appear in Hyper-V Manager and will be used as the default name for any new VHDs you create. You can also specify an alternate location for the VM here, although I recommend against that option for most installations.
- **Specify Generation** If you're planning to run a 64-bit version of Windows 8.1, Windows 10, or Windows Server 2012 R2 or later, choose the Generation 2 option, which supports the Secure Boot feature. For older operating systems or a 32-bit VM, choose Generation 1. Consider this option carefully, though, because as the warning text shown

in Figure 10-6 makes clear, you can't change this configuration later.



Choose the generation of this virtual machine.

○ Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

● Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

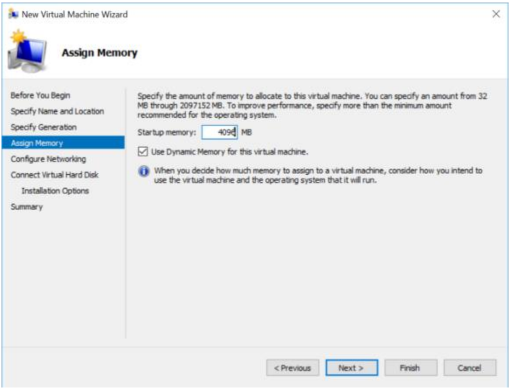
⚠ Once a virtual machine has been created, you cannot change its generation.

More about virtual machine generation support

Figure 10-6: Select the Generation 2 option to activate Secure Boot on a VM running 64-bit Windows 10 or a recent release of Windows Server.

- **Assign Memory** Choosing the right value here involves a balancing act. Memory assigned to a VM is not available for the host PC when that VM is running. On a desktop PC with at least 16 GB of available RAM, you can be generous with memory for a VM. In Figure 10-7, for example, I've configured the VM to start with a full 4 GB of virtual memory, which ensures that a Windows 10 VM will run well. On a notebook with only 8

GB of RAM, you need to manage memory far more carefully. The Dynamic Memory option is extremely useful for those configurations, taking memory away from your host PC only as the VM needs it.



Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 2097152 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 4096 MB

☑ Use Dynamic Memory for this virtual machine.

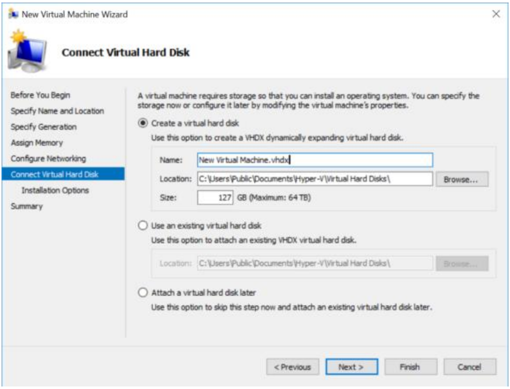
When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

Figure 10-7: Use the Dynamic Memory option when you want your host PC to give away physical memory only when a VM truly needs it.

Disable Dynamic Memory temporarily for installation

When installing an operating system on a VM, you might find that the Dynamic Memory option causes the Windows Setup program to fail, thinking that the memory in the VM is lower than the minimum requirements. The solution is to turn off Dynamic Memory and set the Startup Memory option to an amount that the installer will accept. After the setup is complete, return to the settings for the VM and turn on Dynamic Memory again.

- **Configure Networking** From the drop-down list, choose the virtual network switch you created earlier. If you skipped that step and there's no available virtual switch, don't worry. Create the VM without specifying a network, and then create the virtual switch and add it later.
- **Connect Virtual Hard Disk** A VHD acts exactly like a physical drive as far as your VM is concerned. In reality, though, the VHD is a file stored on the host PC's hard drive. The default option creates a dynamically expanding VHD—a single file that is initially small and grows only as needed. You can increase or decrease its size to fit, and replace the generic name with one that's more descriptive.



Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

● Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: New Virtual Machine.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse...

Size: 127 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

Use this option to attach an existing VHDX virtual hard disk.

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse...

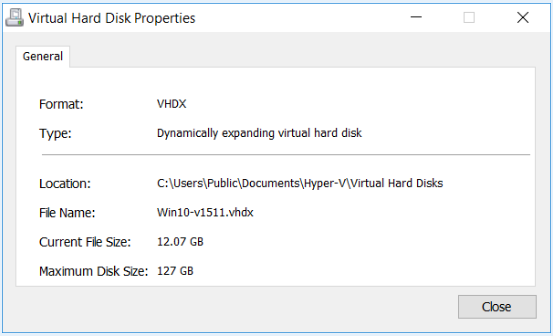
○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

Figure 10-8: The default value unhelpfully assigns the name New Virtual Machine to the VHD file you create here. I recommend changing it to one that's more descriptive.

Make your VHD large enough

For a VM running Windows 10, I've found that the default size of 127 GB is generally acceptable. If you're worried because free space on your host PC is tight, relax. The "dynamically expanding" nature of this file means that it initially occupies only a fraction of that space, even after you finish installing an operating system. For a clean installation of 64-bit Windows 10 using 4096 MB of virtual memory, for example, the VHD uses only about 12 GB of physical drive space on the host PC, as shown here:



Format: VHDX

Type: Dynamically expanding virtual hard disk

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

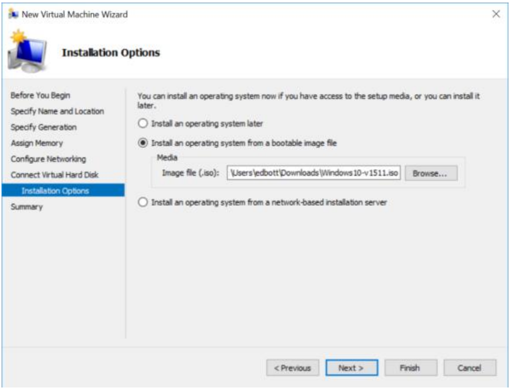
File Name: Win10-v1511.vhdx

Current File Size: 12.07 GB

Maximum Disk Size: 127 GB

It's easy to increase the size of a VHD after the fact. First, shut down any VM that's using the VHD file. Then, from Hyper-V Manager, in the Actions pane, click Edit Disk, choose the Edit Disk option, and then select the VHD file you want to adjust. Follow the wizard's prompts and use the Expand option to increase the drive size. Note that you'll have use the Disk Management console (which I describe in Chapter 6) in the VM to expand the system volume to use the newly created virtual drive space.

- **Installation Options** In most cases, you'll want to install an operating system immediately after finishing the previous steps. The best way to accomplish this task is by attaching a bootable disk image file (in ISO format), which then appears to the VM as a DVD that you can use to start setup. In Figure 10-9, I've attached an ISO file that I downloaded to the host PC by using the Windows 10 Media Creation Tool.



You can install an operating system now if you have access to the setup media, or you can install it later.

○ Install an operating system later

● Install an operating system from a bootable image file

Media

Image file (.iso): \Users\edbott\Downloads\Windows10-v1511.iso

○ Install an operating system from a network-based installation server

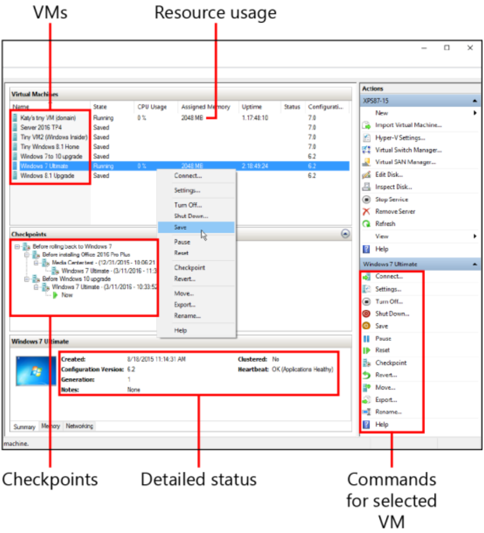
Figure 10-9: The simplest way to install an operating system on a new VM is to attach a disk image file, which then appears as a startup virtual DVD.

You can now click Finish and begin installing your operating system on the new VM.

Working with virtual machines

I couldn’t imagine doing what I do for a living without Hyper-V. If you’re a trainer, a software developer, or an IT pro who needs to support multiple platforms, you probably need more than one VM to handle different test environments.

Figure 10-10 offers a glimpse of what Hyper-V Manager looks like on my main system, a desktop PC with a powerful CPU, 32 GB of RAM, and plenty of spare disk space. As you can see, I’ve set up seven different VMs so that I can replicate a variety of computing environments, running multiple Windows versions, with and without being joined to a Windows domain.



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
Katy's tiny VM (domain)	Running	0 %	2048 MB	1.17:48:10		7.0
Server 2016 TP4	Saved					7.0
Tiny VM2 (Windows Insider)	Saved					7.0
Tiny Windows 8.1 Home	Saved					7.0
Windows 7to 10 upgrade	Saved					6.2
Windows 7 Ultimate	Running	0 %	2048 MB	2.18:49:24		6.2
Windows 8.1 Upgrade	Saved					6.2

Windows 7 Ultimate

Created: 8/18/2015 11:14:31 AM
Configuration Version: 6.2
Generation: 1
Notes: None
Clustered: No
Heartbeat: OK (Applications Healthy)

Figure 10-10: On a PC with sufficient resources, you can run multiple VMs simultaneously, monitoring them from Hyper-V Manager. Right-click a VM or use the same set of commands in the Actions pane (lower right)

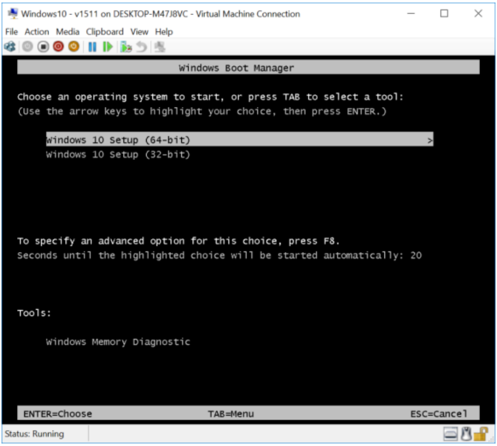
From Hyper-V Manager, you can start any VM by right-clicking its entry in the Virtual Machines list (or using the identical commands in the group at the bottom of the Actions pane) and then, on the shortcut menu that opens, click Start. When you do that, the VM starts and runs silently. So, for example, if you need access to an instance of the latest preview release of Windows Server 2016, you can start its VM and let it run in the background without interacting directly with it. It has its own network address, so it behaves exactly as if it were a physical machine located on your local area network.

The commands for a running VM are slightly different. Instead of the single Start command, you have three options:

- **Turn Off** This has the same effect on a VM as pressing the power switch on a physical PC. In general, you should avoid this option unless a VM has stopped responding and you need to forcibly end it, or you're planning to roll the VM back to a previous state and you don't care about its current state.
- **Shut Down** This sends the Windows shutdown command to the current VM, which facilitates a more graceful end to the session but could still result in data loss if any running apps have unsaved changes.
- **Save** This is usually the most common option for a VM that you plan to continue using. It's more or less the same as the Hibernate option on a physical PC, saving

the current state of the VM and releasing all resources it had been using. Restarting a saved VM returns it to the exact state it was in when you saved it. (On rare occasions, you might encounter problems with a saved VM. If that happens, try selecting the VM and clicking Delete Saved State from the Actions pane.)

To work with a VM, you need to connect to it, using the Connect command in Hyper-V Manager (or simply double-clicking the name of the VM). That opens the Virtual Machine Connection app, with the VM running in a window. Figure 10-11 shows the VM I set up in the previous section, booting from a virtual DVD to start Windows 10 setup.


Windows10 - v1511 on DESKTOP-M47J8VC - Virtual Machine Connection
File Action Media Clipboard View Help
Status: Running

```
                          Windows Boot Manager

Choose an operating system to start, or press TAB to select a tool:
(Use the arrow keys to highlight your choice, then press ENTER.)

    Windows 10 Setup (64-bit)                                 >
    Windows 10 Setup (32-bit)

To specify an advanced option for this choice, press F8.
Seconds until the highlighted choice will be started automatically: 20

Tools:

    Windows Memory Diagnostic

ENTER=Choose                  TAB=Menu                   ESC=Cancel
```

Figure 10-11: Using the Virtual Machine Connection app, you can interact directly with a VM, which can boot from a virtual DVD, giving you an opportunity to set up an operating system—in this case, a fresh copy of Windows 10.

The toolbar in the Virtual Machine Connection window includes several of the commands from the Actions pane. If you double-click a saved VM, for example, you can click the green Start button; for a running VM, available buttons on the toolbar include Turn Off, Shut Down, and Save.

The biggest limitation of a VM is that you have no direct access to hardware, as you do with a physical PC. As a result, from a basic session in a

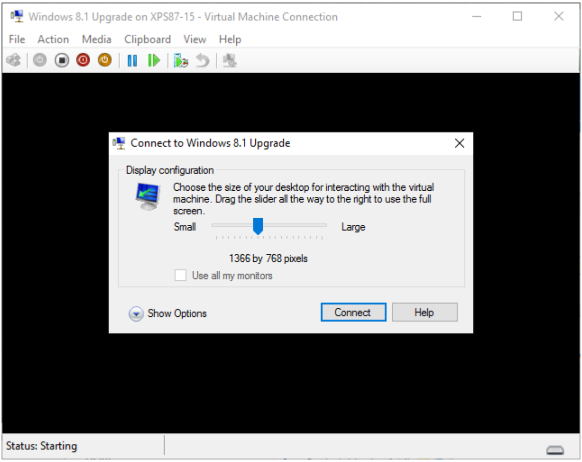
Virtual Machine Connection window, you can’t connect to a USB device such as a printer or scanner. Your display resolution options are limited to those supported by the Microsoft Hyper-V video display adapter. There’s no virtual sound hardware, so you’ll see a red X over the speaker icon in the notification area of the taskbar.

The solution is to run the VM in an enhanced session, which integrates Remote Desktop Protocol with the Virtual Machine Connection app to make available many of those missing features. In an enhanced session, you can choose a display configuration that matches the host hardware, including the ability to run multiple monitors. You can connect to printers and storage devices on the host PC and reroute audio through the host PC, as well.

Enhanced sessions support the use of the Clipboard to copy and paste files and folders between the VM and the host PC (in a basic session, you can use the Clipboard option on the Virtual Machine Connection app menu to type copied text from the host PC into the VM, but that’s about it).

Finally, if your organization uses smart cards for authentication, you can include that additional security in an enhanced session.

If the guest OS running in your VM supports incoming Remote Desktop sessions (in general, this requires a Pro, Business, or Enterprise edition of Windows), you can run an enhanced session. A configuration dialog box like the one depicted in Figure 10-12 should appear when you connect to a supported VM. If you’re currently in a basic session, click View > Enhanced Session from the Virtual Machine Connection app menu, or use the Enhanced Session button at the far right of the toolbar in that app.


Windows 8.1 Upgrade on XPS87-15 - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Connect to Windows 8.1 Upgrade
Small
Large
Show Options
Connect
Help

Display configuration

Choose the size of your desktop for interacting with the virtual machine. Drag the slider all the way to the right to use the full screen.

1366 by 768 pixels

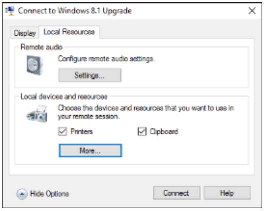
□ Use all my monitors

Status: Starting

Figure 10-12: When starting an enhanced session, you can choose the display resolution. Move this slider all the way to the right to use the full screen.

If your host PC is set up with multiple monitors, you can configure the VM to use them in an enhanced session by selecting the Use All My Monitors check box.

Click the Show Options dialog box to make a second tab, Local Resources, visible. As shown here, the default settings turn on remote audio and support for printers and the Clipboard. Click the More button to make local drives visible in File Explorer within the VM.



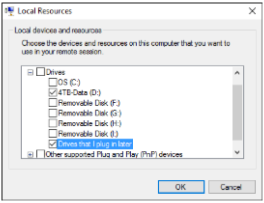
Remote audio

Configure remote audio settings.

Local devices and resources

Choose the devices and resources that you want to use in your remote session.

☑ Printers ☑ Clipboard



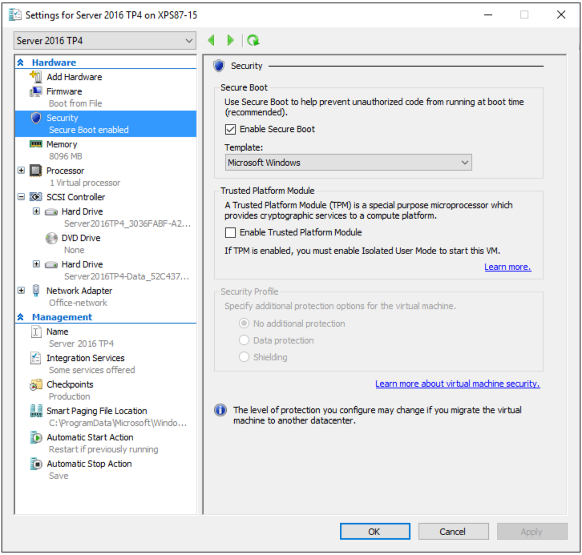
Local devices and resources

Choose the devices and resources on this computer that you want to use in your remote session.

- ☐ Drives
  - ☐ OS (C:)
  - ☑ 4TB-Data (D:)
  - ☐ Removable Disk (F:)
  - ☐ Removable Disk (G:)
  - ☐ Removable Disk (H:)
  - ☐ Removable Disk (I:)
  - ☑ Drives that I plug in later
- ☐ Other supported Plug and Play (PnP) devices

Managing virtual machines

In some respects, VMs behave exactly like their physical counterparts. But VMs have decided advantages over physical hardware for some activities. Would you like to increase the amount of memory available in your VM or add a second drive? You don’t need a screwdriver. Just shut down the VM cleanly first (don’t use the Save option), and then select the VM in Hyper-V Manager. At the bottom of the Actions pane, under the heading that matches the name of the VM, click Settings to open a dialog box like the one shown in Figure 10-13.



Settings for Server 2016 TP4 on XPS87-15

Hardware
- Add Hardware
- Firmware: Boot from File
- Security: Secure Boot enabled
- Memory: 8096 MB
- Processor: 1 Virtual processor
- SCSI Controller
  - Hard Drive: Server2016TP4_3036FABF-A2...
  - DVD Drive: None
  - Hard Drive: Server2016TP4-Data_52C437...
- Network Adapter: Office-network

Management
- Name: Server 2016 TP4
- Integration Services: Some services offered
- Checkpoints: Production
- Smart Paging File Location: C:\ProgramData\Microsoft\Windo...
- Automatic Start Action: Restart if previously running
- Automatic Stop Action: Save

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

☑ Enable Secure Boot

Template: Microsoft Windows

Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

□ Enable Trusted Platform Module

If TPM is enabled, you must enable Isolated User Mode to start this VM.

Learn more.

Security Profile

Specify additional protection options for the virtual machine.

● No additional protection

○ Data protection

○ Shielding

Learn more about virtual machine security.

The level of protection you configure may change if you migrate the virtual machine to another datacenter.

Figure 10-13: Many of the settings for a VM, including the Secure Boot and virtual TPM options, can only be adjusted after it's created.

In this example, you can tell that this is a Generation 2 VM because of the existence of a Firmware (not BIOS) option in the Navigation pane, with a Secure Boot option below it that is not available in a Generation 1 machine.

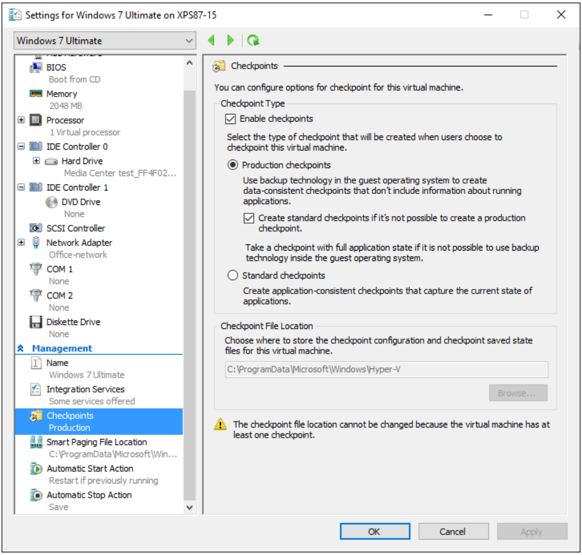
From the Hardware group of options, you can click Firmware to change the startup order (by default, a virtual DVD boots before hard drives); click Memory to adjust the amount of virtual RAM and turn on or turn off Dynamic Memory; and change the network type.

Under the Management heading you'll find options to change the name of the VM (you can also rename a VM from its listing in Hyper-V Manager) and, from the bottom of the list, to change the Automatic Start and Automatic Stop actions. For example, if you have a virtual server that you want available whenever your PC is turned on, click Automatic Start Action and select Always Start The Virtual Machine Automatically.

One huge advantage of a VM over a physical PC is the ability to create checkpoints. Using checkpoints, you can save the current state of a VM so that you can roll back to that state (Hyper-V uses the term *revert*) after you complete some testing.

Imagine, for example, that you're evaluating two competing software packages to see which one you want to use for a specific task. It's possible that the first program you install will change settings (such as file associations) that in turn affect the operation of the program you install afterward. By setting a checkpoint before you install the first program, you can perform your evaluation and then revert to the clean configuration after the test is complete. That action makes the playing field level for both programs.

Hyper-V in Windows 10 supports two types of checkpoints: production and standard. You can choose the checkpoint type (or turn off checkpoints completely) on the Settings page shown in Figure 10-14. In general, production checkpoints are preferable to standard checkpoints, which save the entire state of the machine and can result in some unwanted behaviors.



Settings for Windows 7 Ultimate on XPS87-15

Windows 7 Ultimate

- BIOS
  Boot from CD
- Memory
  2048 MB
- ⊞ Processor
  1 Virtual processor
- ⊟ IDE Controller 0
  - ⊞ Hard Drive
    Media Center test_FF4F02...
- ⊟ IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- ⊞ Network Adapter
  Office-network
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management

- Name
  Windows 7 Ultimate
- Integration Services
  Some services offered
- Checkpoints
  Production
- Smart Paging File Location
  C:\ProgramData\Microsoft\Win...
- Automatic Start Action
  Restart if previously running
- Automatic Stop Action
  Save

Checkpoints

You can configure options for checkpoint for this virtual machine.

Checkpoint Type

☑ Enable checkpoints

Select the type of checkpoint that will be created when users choose to checkpoint this virtual machine.

● Production checkpoints

Use backup technology in the guest operating system to create data-consistent checkpoints that don't include information about running applications.

☑ Create standard checkpoints if it's not possible to create a production checkpoint.

Take a checkpoint with full application state if it is not possible to use backup technology inside the guest operating system.

○ Standard checkpoints

Create application-consistent checkpoints that capture the current state of applications.

Checkpoint File Location

Choose where to store the checkpoint configuration and checkpoint saved state files for this virtual machine.

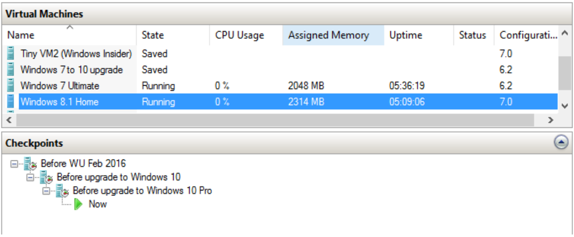
C:\ProgramData\Microsoft\Windows\Hyper-V

⚠ The checkpoint file location cannot be changed because the virtual machine has at least one checkpoint.

Figure 10-14: Checkpoints are turned on by default, and I can't think of a reason why you would want to turn them off. You can use them to roll back to a known good state, making it easy to experiment with a VM.

To set a checkpoint from a VM running in a window (a basic or enhanced session), on the Virtual Machine Connection app menu, choose Action and then Checkpoint. From Hyper-V Manager, right-click the VM name and then, on the shortcut menu, choose Checkpoint.

Each checkpoint is indented from the one above it, making it possible for you to snap multiple checkpoints and then revert to whichever one you want, as shown here:



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
Tiny VM2 (Windows Insider)	Saved					7.0
Windows 7 to 10 upgrade	Saved					6.2
Windows 7 Ultimate	Running	0 %	2048 MB	05:36:19		6.2
Windows 8.1 Home	Running	0 %	2314 MB	05:09:06		7.0

Checkpoints

- Before WU Feb 2016
  - Before upgrade to Windows 10
    - Before upgrade to Windows 10 Pro
      - Now

To roll back to a previously created checkpoint, select that checkpoint from the list in Hyper-V Manager, right-click, and then choose Apply. The operation is very quick.

Reverting to an earlier checkpoint doesn't affect later checkpoints. You can roll back to a previous configuration and then apply a checkpoint you saved later.

Checkpoints consume disk space, of course. After your testing is complete, you can safely delete a checkpoint (or an entire checkpoint tree) by selecting its entry in the Checkpoints list and then using commands in the Actions pane or on the right-click shortcut menu.

CHAPTER 11

Microsoft Azure

If you think you need new hardware to evaluate the latest versions of Windows, think again. Maybe you can find the resources you need in the cloud instead.

That’s the promise underlying Microsoft Azure, which offers subscription-based cloud services for developers and IT pros to build, test, and deploy websites, mobile apps, and computing resources. Azure offers an incredibly wide range of services, with new capabilities appearing regularly.

In this chapter, I focus on Azure's virtualization and networking features. First up is the option to create cloud-based virtual machines (VMs) running Windows 10 and Windows Server, which are ideal for IT pros who need an environment to test software and evaluate networks. I also cover Microsoft's cloud-based Azure Active Directory (Azure AD) service, which integrates exceptionally with Windows 10, regardless of whether you're already part of a Windows domain.

Let's begin with the basics of Azure subscriptions.

Getting started with Microsoft Azure

There's no charge to sign up for a pay-as-you-go Azure account, and many services are completely free. But before you rush to sign up at https://azure.com, check your existing portfolio of Microsoft services. You might already have access to some Azure services.

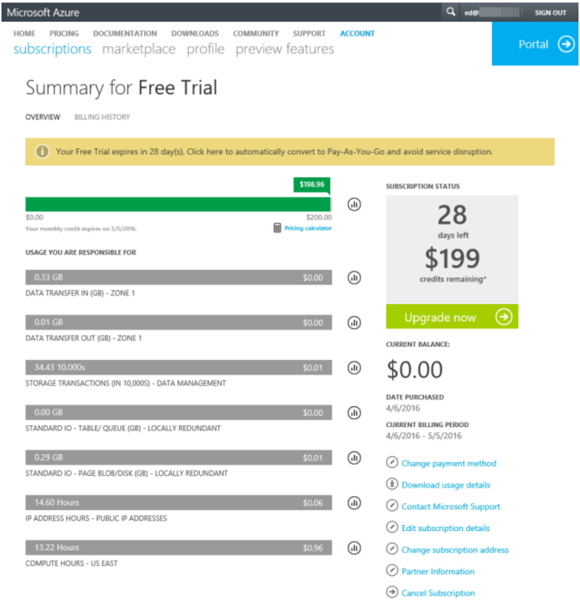
Every Microsoft Visual Studio subscription includes a monthly credit for Azure services (the exact amount varies by subscription level). Registered members of the Microsoft Partner Network can receive Azure credit as part of the Microsoft Action Pack, and startups that sign up for the BizSpark program get a generous allotment of free Azure credit. Organizations that subscribe to Microsoft online services—including Business or Enterprise editions of Microsoft Office 365, Microsoft Intune, and Microsoft Dynamics CRM Online—automatically have Azure AD services as part of their subscription.

If you’re not already part of one of those programs, use your Microsoft account to sign up for a free Azure account. Currently, a new subscription includes $200 of credit for you to use in the first month as you learn the ins and outs of the service. When that runs out, you can switch to a pay-as-you-go account; with Azure, you can set a spending limit and arrange billing alerts to ensure that you don’t receive any unwelcome surprises.

Two additional Azure subscription options are available:

- Twelve-month prepaid plans provide discounts for Azure services in exchange for an up-front monetary commitment. Unused dollars expire at the end of the year.
- Volume licensing customers can purchase Azure services using Microsoft's Open Volume Licensing program.

Two web pages are worth saving as Favorites. The first, https://account.windowsazure.com, displays a summary of your current subscription with meticulous billing details and links to common account management tasks.
Figure 11-1 shows the status of a newly created account.



Microsoft Azure ed@[redacted] SIGN OUT

HOME PRICING DOCUMENTATION DOWNLOADS COMMUNITY SUPPORT ACCOUNT

subscriptions marketplace profile preview features

Portal

Summary for **Free Trial**

OVERVIEW BILLING HISTORY

Your Free Trial expires in 28 day(s). Click here to automatically convert to Pay-As-You-Go and avoid service disruption.

$198.96

$0.00 $200.00

Your monthly credit expires on 5/5/2016.

Pricing calculator

USAGE YOU ARE RESPONSIBLE FOR

Usage	Amount	Item
0.33 GB	$0.00	DATA TRANSFER IN (GB) - ZONE 1
0.01 GB	$0.00	DATA TRANSFER OUT (GB) - ZONE 1
34.43 10,000s	$0.01	STORAGE TRANSACTIONS (IN 10,000S) - DATA MANAGEMENT
0.00 GB	$0.00	STANDARD IO - TABLE/ QUEUE (GB) - LOCALLY REDUNDANT
0.29 GB	$0.01	STANDARD IO - PAGE BLOB/DISK (GB) - LOCALLY REDUNDANT
14.60 Hours	$0.06	IP ADDRESS HOURS - PUBLIC IP ADDRESSES
13.22 Hours	$0.96	COMPUTE HOURS - US EAST

SUBSCRIPTION STATUS

28
days left

$199
credits remaining*

Upgrade now

CURRENT BALANCE:
$0.00

DATE PURCHASED
4/6/2016

CURRENT BILLING PERIOD
4/6/2016 - 5/5/2016

Change payment method

Download usage details

Contact Microsoft Support

Edit subscription details

Change subscription address

Partner Information

Cancel Subscription

Figure 11-1: A new Azure account comes with an allowance of free credit for the first month so that you can experiment with services without worrying about unwelcome financial surprises.

The upper-right corner of that page includes a link to the Azure Portal, which is where you go to create and use cloud-based services. (To visit that page directly, go to https://portal.azure.com.) Figure 11-2 shows a customized dashboard for an Azure account with two active subscriptions.

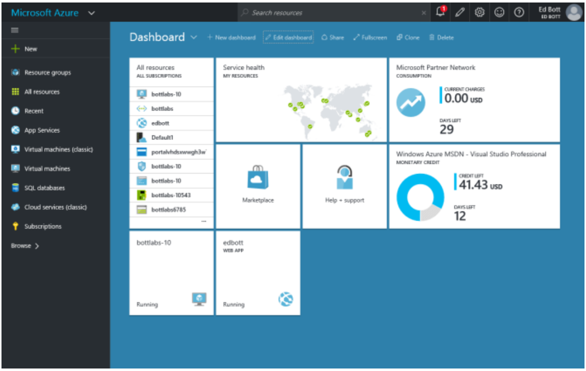


Figure 11-2: You can pin shortcuts to the Azure Portal dashboard, for an at-a-glance summary of each subscription’s status as well as quick access to resources such as VMs and websites.

The link in the upper-right corner of that dashboard leads to account settings.

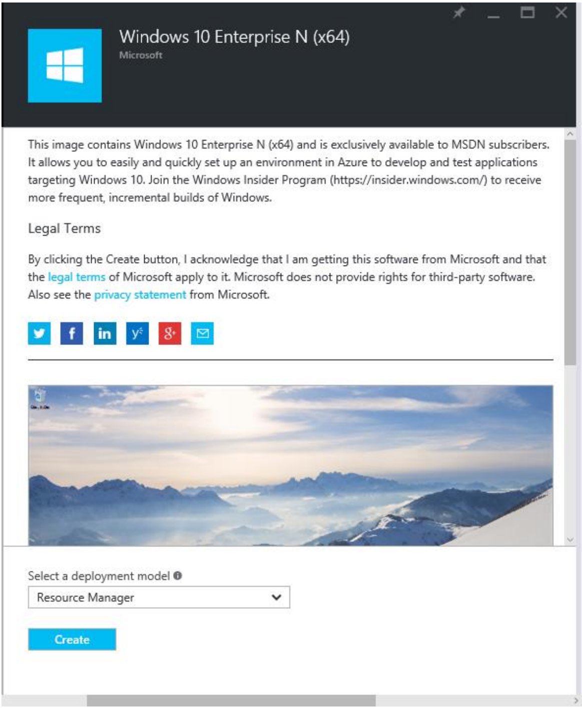
Note that the portal shown in Figure 11-2 is relatively new. As of this writing, an older portal is still required for some services, including Azure AD. Over time, those services will be moved to the new portal.

Running a virtual machine in the cloud

In Chapter 10, I introduced Hyper-V, the built-in virtualization platform in Windows 10. Running a local VM has performance advantages, but it also requires dedicated resources that your local PC might not have to spare, including memory and drive space.

Setting up a VM in the Azure cloud requires no local resources. You connect to the VM by using the Remote Desktop client built in to all editions of Windows 10, and you pay only while the VM is running.

From the Azure portal, in the navigation pane on the left, click Virtual Machines and then click Add to see a listing of the dizzying array of available, ready-made VMs. At the top of the listings, click the search box and type a search term to narrow the list. For MSDN subscribers, a Windows 10 Enterprise N (x64) option is available. Click that option to see the description shown in Figure 11-3.



Windows 10 Enterprise N (x64)

Microsoft

This image contains Windows 10 Enterprise N (x64) and is exclusively available to MSDN subscribers. It allows you to easily and quickly set up an environment in Azure to develop and test applications targeting Windows 10. Join the Windows Insider Program (https://insider.windows.com/) to receive more frequent, incremental builds of Windows.

Legal Terms

By clicking the Create button, I acknowledge that I am getting this software from Microsoft and that the legal terms of Microsoft apply to it. Microsoft does not provide rights for third-party software. Also see the privacy statement from Microsoft.

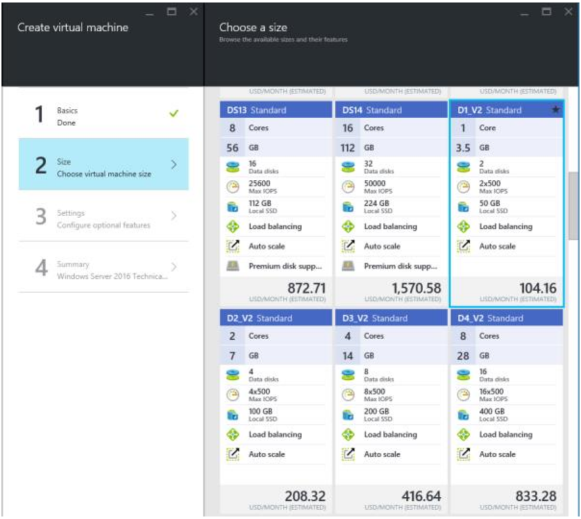
Select a deployment model: Resource Manager

Figure 11-3: You can configure ready-made VMs like this one in minutes. The Resource Manager deployment model removes most of the intricacy of setup.

The Select A Deployment Model box at the bottom of that description is set to Resource

Manager, which greatly simplifies the otherwise tedious process of defining cloud-based storage, virtual networks, and other infrastructure for the VM. The alternative is the Classic model, with which you can build your own VM. For a description of how the Classic model works, see the article "Create a custom virtual machine running Windows."

Creating a new VM requires some basic setup steps, including creating a default administrator account and, notably, choosing the size of the VM. The cost of an Azure VM is directly dependent on the resources you assign to it, and Azure gives you dozens of predefined combinations of CPU cores, memory, and drive storage, with estimates of the monthly charges below each option, as shown in Figure 11-4.



Create virtual machine

1 Basics
Done ✓

2 Size
Choose virtual machine size

3 Settings
Configure optional features

4 Summary
Windows Server 2016 Technica...

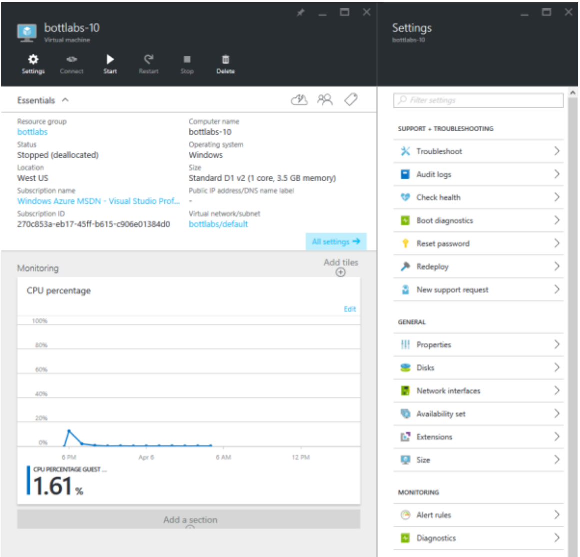
Choose a size
Browse the available sizes and their features

DS13 Standard	DS14 Standard	D1_V2 Standard
8 Cores	16 Cores	1 Core
56 GB	112 GB	3.5 GB
16 Data disks	32 Data disks	2 Data disks
25600 Max IOPS	50000 Max IOPS	2x500 Max IOPS
112 GB Local SSD	224 GB Local SSD	50 GB Local SSD
Load balancing	Load balancing	Load balancing
Auto scale	Auto scale	Auto scale
Premium disk supp...	Premium disk supp...	
872.71 USD/MONTH (ESTIMATED)	1,570.58 USD/MONTH (ESTIMATED)	104.16 USD/MONTH (ESTIMATED)

D2_V2 Standard	D3_V2 Standard	D4_V2 Standard
2 Cores	4 Cores	8 Cores
7 GB	14 GB	28 GB
4 Data disks	8 Data disks	16 Data disks
4x500 Max IOPS	8x500 Max IOPS	16x500 Max IOPS
100 GB Local SSD	200 GB Local SSD	400 GB Local SSD
Load balancing	Load balancing	Load balancing
Auto scale	Auto scale	Auto scale
208.32 USD/MONTH (ESTIMATED)	416.64 USD/MONTH (ESTIMATED)	833.28 USD/MONTH (ESTIMATED)

Figure 11-4: As part of the process of configuring an Azure VM, you must choose a size. The more resources you assign to the VM, the greater the cost.

After creating a VM, you'll find it listed in the dashboard under the Virtual Machines heading. Figure 11-5 shows the settings for a Windows 10 VM. Note that the machine is currently stopped and is thus not costing a penny.



Resource group
bottlabs

Status
Stopped (deallocated)

Location
West US

Subscription name
Windows Azure MSDN - Visual Studio Prof...

Subscription ID
270c853a-eb17-45ff-b615-c906e01384d0

Computer name
bottlabs-10

Operating system
Windows

Size
Standard D1 v2 (1 core, 3.5 GB memory)

Public IP address/DNS name label
-

Virtual network/subnet
bottlabs/default

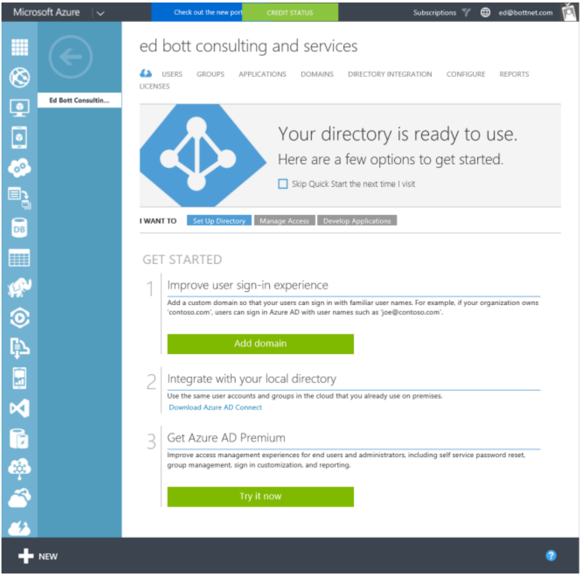
Figure 11-5: This VM, running Windows 10, is configured but not running. Click Start to power on the VM, and then click Connect to download a Remote Desktop Connection settings file.

To connect to this VM, you need to visit the Azure dashboard and click Start. Then, click the Connect button to download a Remote Desktop connection profile that makes it possible for you to run the VM as if it were a local machine.

For a virtual server, of course, you'll probably want to keep the VM running full time, so the monthly estimate of costs is accurate. For a virtual Windows 10 workstation that you only need for occasional testing, you can shut it down after your work is complete, keeping its cost to a bare minimum.

Azure Active Directory

As I mentioned earlier, Microsoft's business-focused cloud services, including Business and Enterprise editions of Office 365, use Azure AD for authentication. You can manage that directory within the Azure Portal, although doing so today requires the older Azure Management Portal (https://manage.windowsazure.com). Figure 11-6 shows the Quick Start page for a directory associated with an Office 365 Enterprise (E3) account.



ed bott consulting and services

Your directory is ready to use.

Here are a few options to get started.

☐ Skip Quick Start the next time I visit

GET STARTED

1 Improve user sign-in experience

Add a custom domain so that your users can sign in with familiar user names. For example, if your organization owns 'contoso.com', users can sign in Azure AD with user names such as 'joe@contoso.com'.

2 Integrate with your local directory

Use the same user accounts and groups in the cloud that you already use on premises.

Download Azure AD Connect

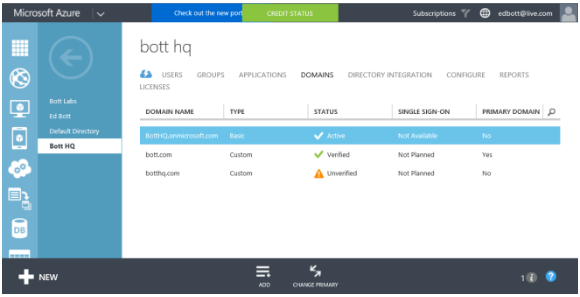
3 Get Azure AD Premium

Improve access management experiences for end users and administrators, including self service password reset, group management, sign in customization, and reporting.

Figure 11-6: Using this Quick Start page for a new Azure AD installation, you can associate a custom domain with the directory, to integrate with your own existing domain, and to add premium features.

Every Office 365 (business and Enterprise) and Azure subscription includes support for Azure AD at the Free level. This level supports synchronization with a local directory plus single sign-on (SSO) capabilities for up to 10 apps per user. Premium features are available (for a monthly charge per licensed user) allowing for unlimited SSO apps and advanced features such as multifactor authentication.

Each Azure subscription includes a default domain, which is based on the Azure identifier you specify when signing up. Figure 11-7 shows the default domain for a test account, botthq.onmicrosoft.com, with two custom domains added. Note that every custom domain you add must be verified, typically by adding a DNS record.

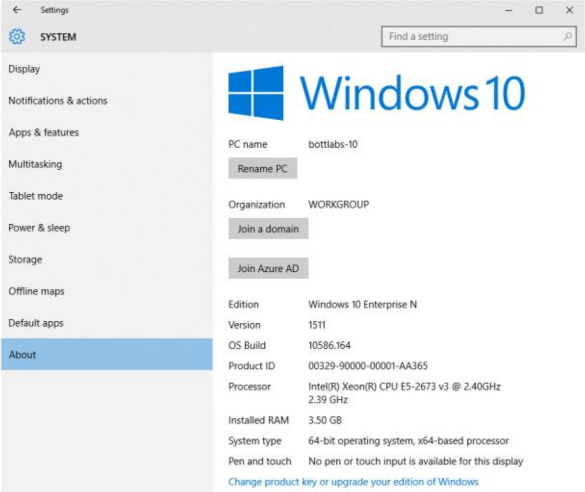


DOMAIN NAME	TYPE	STATUS	SINGLE SIGN-ON	PRIMARY DOMAIN
BottHQ.onmicrosoft.com	Basic	✓ Active	Not Available	No
bott.com	Custom	✓ Verified	Not Planned	Yes
botthq.com	Custom	⚠ Unverified	Not Planned	No

Figure 11-7: The default Azure AD domain, botthq.onmicrosoft.com in this example, is only a starting point. The real benefits of the cloud-based directory appear when you attach one or more custom domains.

If you’ve set up Azure AD, you can connect an account from that directory to a new Windows 10 installation during the initial setup of

Windows 10. In that configuration, the Azure AD account becomes the primary sign-in for the device. You can also connect a Windows 10 device after it's been set up using a local account or a Microsoft account. To accomplish this task, use the Join Azure AD feature, found in the About Your PC page in the Settings app (to get there, open Settings, click or tap System, and then click About). Figure 11-8 shows this option available for use.



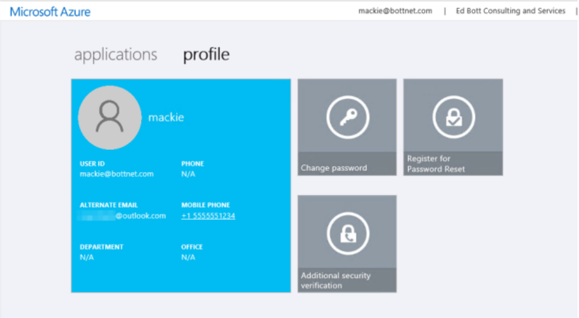
PC name bottlabs-10

Organization WORKGROUP

Edition Windows 10 Enterprise N
Version 1511
OS Build 10586.164
Product ID 00329-90000-00001-AA365
Processor Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz 2.39 GHz
Installed RAM 3.50 GB
System type 64-bit operating system, x64-based processor
Pen and touch No pen or touch input is available for this display

Figure 11-8: Click Join Azure AD to connect a PC to your organization's directory in the Azure cloud.

After connecting a Windows 10 PC to Azure AD, you can access your account by signing in using your Azure AD credentials at https://account.activedirectory.windowsazure.com (you can also use the much friendlier address https://myapps.microsoft.com). As Figure 11-9 shows, on the Profile page, you can request a password reset and manage multifactor authentication settings. The Applications tab includes any apps that have been set up by your administrator for SSO.



Microsoft Azure
mackie@bottnet.com | Ed Bott Consulting and Services
applications
profile
mackie
Change password
Register for Password Reset
Additional security verification

USER ID: mackie@bottnet.com

PHONE: N/A

ALTERNATE EMAIL: [redacted]@outlook.com

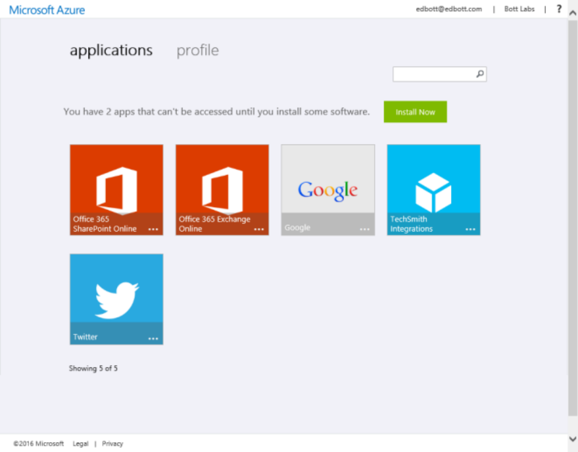
MOBILE PHONE: +1 5555551234

DEPARTMENT: N/A

OFFICE: N/A

Figure 11-9: The Azure AD user portal lists your details as they appear in the directory. Click Additional Security Verification to manage multifactor authentication settings.

The Applications tab contains shortcuts to applications that have been configured by the network administrator for SSO. Note that—for now at least—using these features requires a browser that supports the Access Panel Extension. This extension is available for Internet Explorer, Firefox, and Chrome, but is not supported in Windows 10 version 1511 for Microsoft Edge.



You have 2 apps that can't be accessed until you install some software.

Microsoft Azure
edbott@edbott.com | Bott Labs | ?
applications
profile
Install Now
Office 365 SharePoint Online
Office 365 Exchange Online
Google
Google
TechSmith Integrations
Twitter
Showing 5 of 5
©2016 Microsoft Legal | Privacy

Figure 11-10: The Azure AD Access Panel lists apps that are available for SSO. For some third-party apps, you might need to install a browser extension.

About the author

Ed Bott is an award-winning technology journalist and author who has been writing about Microsoft technologies for more than two decades. He is the author of more than 25 books on Microsoft Windows and Office, including *Windows 10 Inside Out* (Microsoft Press, 2015) and writes regularly about technology for The Ed Bott Report at ZDNet.