Windows 8.1 Administration Storage, Security, & Networking
Pocket Consultant

The practical, portable guide for Windows administrators!
Portable and precise, this pocket-sized guide delivers ready answers for managing storage, security, and networking features in Windows 8.1. Zero in on core procedures and operations through quick-reference tables, instructions, and lists. You’ll get the focused information you need to save time and get the job done—whether at your desk or in the field.

Get fast facts to:
• Troubleshoot boot configuration and startup
• Administer Group Policy settings
• Manage file systems and drives
• Configure and manage storage
• Implement file sharing and auditing
• Manage data access and availability
• Administer BitLocker and TPM services
• Configure and troubleshoot TCP/IP networking
• Enable remote and mobile access

About the Author
William R. Stanek is a leading technology expert with 20+ years of experience in systems management and advanced programming. He is an award-winning author of more than 150 books, including Microsoft Exchange Server 2013 Pocket Consultant and two new Inside Out Titles for Windows Server 2012 R2. He is the series editor for the Pocket Consultant line of books.

Also Look For
Microsoft.com/msspress

U.S.A. $39.99
Canada $41.99
Recommended

Windows 8.1 Administration Essentials & Configuration
Pocket Consultant
William Stanek
ISBN 9780735682658

Microsoft Press
Celebrating 30 years!
Contents

Acknowledgments xi
Introduction xiii

Chapter 1 Managing firmware, boot configuration, and startup 1

Navigating and understanding firmware options ............ 1
  Firmware interface types and boot data 2
  Boot services, run-time services, and beyond 3
  UEFI 5

Navigating startup and power states ......................... 8
  Working with firmware interfaces 9
  Examining firmware interfaces 10
  Power states and power management 12

Diagnosing and resolving startup problems .................. 15
  Troubleshooting startup phase 1 17
  Troubleshooting startup phase 2 18
  Troubleshooting startup phase 3 19
  Troubleshooting startup phase 4 20
  Troubleshooting startup phase 5 21

Managing startup and boot configuration .................... 22
  Setting startup and recovery options 22
  Managing system boot configuration 23
  Using the BCD Editor 25

Managing the BCD store ........................................ 27
  Viewing BCD entries 28
  Creating and identifying the BCD store 31
  Importing and exporting the BCD store 31
  Creating and deleting BCD entries 32

What do you think of this book? We want to hear from you!
Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey
<table>
<thead>
<tr>
<th>Setting BCD entry values</th>
<th>33</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing Data Execution Prevention and Physical Address Extension options</td>
<td>38</td>
</tr>
<tr>
<td>Changing the operating system display order</td>
<td>39</td>
</tr>
<tr>
<td>Changing the default operating system entry</td>
<td>40</td>
</tr>
<tr>
<td>Changing the default timeout</td>
<td>40</td>
</tr>
<tr>
<td>Changing the boot sequence temporarily</td>
<td>41</td>
</tr>
</tbody>
</table>

## Chapter 2 Using TPM and BitLocker Drive Encryption 43

- Creating trusted platforms ........................................ 43
- TPM: the essentials .................................................. 44
- TPM: management and policies ...................................... 45
- Enabling TPM ................................................................ 48
- Initializing and preparing a TPM for first use .................. 50
- Turning an initialized TPM on or off .............................. 53
- Clearing the TPM ......................................................... 53
- Changing the TPM owner password .................................. 55

- BitLocker Drive Encryption: the essentials ....................... 56
- Understanding BitLocker Drive Encryption ...................... 56
- Hardware encryption, secure boot, and network unlock ....... 59
- Deploying BitLocker Drive Encryption .............................. 62

- Managing BitLocker Drive Encryption .............................. 66
- Preparing for BitLocker Drive Encryption ......................... 67
- Enabling BitLocker on nonsystem volumes ...................... 70
- Enabling BitLocker on USB flash drives ........................... 72
- Enabling BitLocker on system volumes ............................ 74
- Managing and troubleshooting BitLocker .......................... 78

## Chapter 3 Managing disk drives and file systems 81

- Disk management essentials .......................................... 82
- Using the This PC console ............................................. 85
- Using Disk Management ................................................ 87
- Using FSUtil and DiskPart .............................................. 89

- Improving disk performance ......................................... 90
- Understanding and using Windows ReadyBoost ................ 90
- Enabling and configuring Windows ReadyBoost ................. 91
- Understanding and using Windows ReadyDrive .................. 93
- Understanding and using Windows SuperFetch ................... 93
Working with basic and dynamic disks ........................................ 95
  Preparing basic and dynamic disks ........................................ 99
    Understanding drive designations .................................... 99
    Installing and initializing new physical disks ....................... 100
    Changing a disk’s partition table style ................................ 101
    Marking a partition as active ........................................... 101
    Converting a basic disk to a dynamic disk or vice versa ............ 103

Working with disks, partitions, and volumes ............................. 104
  Partitioning disks and preparing them for use ......................... 106
    Creating partitions, logical drives, and simple volumes ............ 106
    Creating spanned and striped volumes ................................ 109
    Shrinking or extending volumes ....................................... 111
    Formatting partitions and volumes .................................... 112
    Assigning, changing, or removing drive letters and paths ......... 113
    Assigning, changing, or deleting a volume label .................... 114
    Deleting partitions, volumes, and logical drives .................... 115
    Converting a volume to NTFS ......................................... 116
    Recovering a failed simple, spanned, or striped volume .......... 118
    Regenerating a striped set with parity ................................ 118

Using disk mirroring ............................................................. 119
  Creating mirrored volumes .............................................. 119
  Breaking a mirrored set ............................................... 120
  Removing a mirrored set ................................................... 120

Moving a dynamic disk to a new system .................................. 121

Using storage spaces .......................................................... 122
  Getting started with storage spaces .................................... 122
  Creating redundant data sets ............................................ 123

Working with storage pools .................................................. 124
  Creating a storage pool and allocating storage ....................... 124
  Adding drives to a storage space ...................................... 127
  Changing the storage configuration .................................... 128
  Deleting a storage space ............................................... 128
  Deleting a storage pool .................................................... 129
  Troubleshooting storage spaces ........................................... 129
Chapter 4  Configuring and maintaining storage ........................................ 131
  Working with removable storage devices ............................................ 131
  Working with data discs ................................................................. 133
    Disc burning: the essentials ......................................................... 133
    Mounting ISO images ............................................................... 134
    Burning ISO images to disc ....................................................... 134
    Burning mastered discs ............................................................. 135
    Burning discs with live file systems ............................................. 136
    Changing the default burning options ......................................... 137
  Managing disk compression and file encryption .................................. 137
    Compressing drives and data ....................................................... 138
    Encrypting drives and data ......................................................... 140
  Troubleshooting common disk problems .......................................... 144
    Repairing disk errors and inconsistencies ..................................... 150
    Checking for disk errors ............................................................ 151
    Defragmenting disks .................................................................. 154
    Resynchronizing and repairing a mirrored set ............................... 156
    Repairing a mirrored system volume to enable boot ....................... 157

Chapter 5  Configuring user and computer policies .................................. 159
  Group Policy essentials ................................................................. 159
    Accessing and using local group policies ...................................... 160
    Accessing and using site, domain, and OU policies ....................... 163
  Configuring policies ..................................................................... 165
    Viewing policies and templates .................................................. 166
    Enabling, disabling, and configuring policies ................................. 166
    Adding or removing templates .................................................... 167
  Working with file and data management policies ............................. 168
    Configuring disk quota policies .................................................. 168
    Configuring System Restore policies ......................................... 170
    Configuring Offline File policies ................................................. 171
    Configuring policy for Work Folders ............................................ 176
  Working with access and connectivity policies .................................. 177
    Configuring network policies ...................................................... 177
    Configuring Remote Assistance policies ...................................... 178
  Working with computer and user script policies .............................. 180
    Controlling script behavior through policy ................................... 180
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning computer startup and shutdown scripts</td>
<td>182</td>
</tr>
<tr>
<td>Assigning user logon and logoff scripts</td>
<td>183</td>
</tr>
<tr>
<td>Working with logon and startup policies</td>
<td>184</td>
</tr>
<tr>
<td>Setting policy-based startup programs</td>
<td>185</td>
</tr>
<tr>
<td>Disabling run lists through policy</td>
<td>185</td>
</tr>
<tr>
<td>Chapter 6  <strong>Optimizing file security</strong></td>
<td>187</td>
</tr>
<tr>
<td>File security and sharing options</td>
<td>187</td>
</tr>
<tr>
<td>Controlling access to files and folders with NTFS permissions</td>
<td>192</td>
</tr>
<tr>
<td>Understanding and using basic permissions</td>
<td>193</td>
</tr>
<tr>
<td>Assigning special permissions</td>
<td>198</td>
</tr>
<tr>
<td>Assigning claims-based permissions</td>
<td>202</td>
</tr>
<tr>
<td>File ownership and permission assignment</td>
<td>205</td>
</tr>
<tr>
<td>Applying permissions through inheritance</td>
<td>206</td>
</tr>
<tr>
<td>Inheritance essentials</td>
<td>206</td>
</tr>
<tr>
<td>Viewing inherited permissions</td>
<td>207</td>
</tr>
<tr>
<td>Stopping inheritance</td>
<td>208</td>
</tr>
<tr>
<td>Restoring inherited permissions</td>
<td>208</td>
</tr>
<tr>
<td>Determining the effective permissions and troubleshooting</td>
<td>209</td>
</tr>
<tr>
<td>Chapter 7  <strong>Managing file sharing and auditing</strong></td>
<td>213</td>
</tr>
<tr>
<td>Sharing files and folders over the network</td>
<td>213</td>
</tr>
<tr>
<td>Controlling access to network shares</td>
<td>214</td>
</tr>
<tr>
<td>Creating a shared resource</td>
<td>215</td>
</tr>
<tr>
<td>Creating and managing shared folders in Group Policy</td>
<td>219</td>
</tr>
<tr>
<td>Using and accessing shared resources</td>
<td>221</td>
</tr>
<tr>
<td>Using and accessing shared folders for administration</td>
<td>224</td>
</tr>
<tr>
<td>Troubleshooting file sharing</td>
<td>226</td>
</tr>
<tr>
<td>Using and configuring public folder sharing</td>
<td>227</td>
</tr>
<tr>
<td>Using public folder sharing</td>
<td>227</td>
</tr>
<tr>
<td>Configuring public folder sharing</td>
<td>228</td>
</tr>
<tr>
<td>Implementing synced sharing</td>
<td>229</td>
</tr>
<tr>
<td>Understanding work folders</td>
<td>229</td>
</tr>
<tr>
<td>Creating sync shares and enabling SMB access</td>
<td>231</td>
</tr>
<tr>
<td>Accessing Work Folders on clients</td>
<td>234</td>
</tr>
</tbody>
</table>
Auditing file and folder access ........................................... 235
   Enabling auditing for files and folders 235
   Configuring and tracking auditing 235

Chapter 8  Maintaining data access and availability  241

   Configuring File Explorer options ................................... 241
      Customizing File Explorer 241
      Configuring advanced File Explorer options 244

   Managing offline files .................................................. 248
      Understanding offline files 248
      Making files or folders available offline 249
      Managing offline file synchronization 252
      Configuring disk usage limits for offline files 257
      Managing encryption for offline files 258
      Making offline files unavailable 258

   Configuring disk quotas ............................................... 259
      Using disk quotas 259
      Enabling disk quotas on NTFS volumes 260
      Viewing disk quota entries 262
      Creating disk quota entries 262
      Updating and customizing disk quota entries 263
      Deleting disk quota entries 263
      Exporting and importing disk quota settings 264
      Disabling disk quotas 265

   Using branch caching ................................................... 266

Chapter 9  Configuring and troubleshooting TCP/IP networking  271

   Navigating Windows 8.1 networking features .................... 271
      Understanding network discovery and network categories 272
      Working with Network Explorer 273
      Working with Network And Sharing Center 275

   Installing networking components ................................... 276
      Working with TCP/IP and the Dual TCP/IP stack 276
      Installing network adapters 279
      Installing networking services and TCP/IP 280
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring network connections</td>
<td>281</td>
</tr>
<tr>
<td>Configuring static IP addresses</td>
<td>281</td>
</tr>
<tr>
<td>Configuring dynamic IP addresses and alternate IP addressing</td>
<td>283</td>
</tr>
<tr>
<td>Configuring multiple gateways</td>
<td>284</td>
</tr>
<tr>
<td>Configuring DNS resolution</td>
<td>286</td>
</tr>
<tr>
<td>Configuring WINS resolution</td>
<td>288</td>
</tr>
<tr>
<td>Managing network connections</td>
<td>290</td>
</tr>
<tr>
<td>Enabling and disabling network connections</td>
<td>290</td>
</tr>
<tr>
<td>Checking the status, speed, and activity for network connections</td>
<td>291</td>
</tr>
<tr>
<td>Viewing network configuration information</td>
<td>292</td>
</tr>
<tr>
<td>Renaming network connections</td>
<td>293</td>
</tr>
<tr>
<td>Troubleshooting and testing network settings</td>
<td>293</td>
</tr>
<tr>
<td>Diagnosing and resolving network connection problems</td>
<td>293</td>
</tr>
<tr>
<td>Diagnosing and resolving Internet connection problems</td>
<td>294</td>
</tr>
<tr>
<td>Performing basic network tests</td>
<td>295</td>
</tr>
<tr>
<td>Resolving IP addressing problems</td>
<td>296</td>
</tr>
<tr>
<td>Releasing and renewing DHCP settings</td>
<td>297</td>
</tr>
<tr>
<td>Registering and flushing DNS</td>
<td>298</td>
</tr>
<tr>
<td>Chapter 10 Managing mobile networking and remote access</td>
<td>301</td>
</tr>
<tr>
<td>Configuring networking for mobile devices</td>
<td>301</td>
</tr>
<tr>
<td>Working with mobility settings</td>
<td>302</td>
</tr>
<tr>
<td>Configuring dynamic IP addresses</td>
<td>304</td>
</tr>
<tr>
<td>Configuring alternate private IP addresses</td>
<td>305</td>
</tr>
<tr>
<td>Connecting to networked projectors</td>
<td>307</td>
</tr>
<tr>
<td>Understanding mobile networking and remote access</td>
<td>308</td>
</tr>
<tr>
<td>Creating connections for remote access</td>
<td>310</td>
</tr>
<tr>
<td>Creating a dial-up connection</td>
<td>311</td>
</tr>
<tr>
<td>Creating a broadband connection to the Internet</td>
<td>317</td>
</tr>
<tr>
<td>Creating a VPN connection</td>
<td>318</td>
</tr>
<tr>
<td>Joining a device to a workplace</td>
<td>320</td>
</tr>
<tr>
<td>Configuring connection properties</td>
<td>320</td>
</tr>
<tr>
<td>Configuring automatic or manual connections</td>
<td>321</td>
</tr>
<tr>
<td>Configuring proxy settings for mobile connections</td>
<td>322</td>
</tr>
</tbody>
</table>
Acknowledgments

To my readers—thank you for being there with me through many books and many years. It has been an honor and a privilege to be your pocket consultant.

To my wife—for many years, through many books, many millions of words, and many thousands of pages she's been there, providing support and encouragement and making every place we've lived a home.

To my kids—for helping me see the world in new ways, for having exceptional patience and boundless love, and for making every day an adventure.

To Anne, Karen, Martin, Lucinda, Juliana, and many others who’ve helped out in ways both large and small.

Special thanks to my son Will for not only installing and managing my extensive dev lab for all my books since Windows 8 Administration Pocket Consultant but for also performing check reads of all those books.

—William R. Stanek
Windows 8.1 Administration Pocket Consultant: Storage, Security, & Networking is designed to be a concise and compulsively usable resource for Windows administrators, developers, and programmers, and for anyone else who wants to use the storage, security, and networking features of Windows 8.1. This is the readable resource guide that you’ll want on your desk or in your pocket at all times. The book discusses everything you need to perform core tasks. Because the focus is on providing you with the maximum value in a pocket-sized guide, you don’t have to wade through hundreds of pages of extraneous information to find what you’re looking for. Instead, you’ll find exactly what you need to get the job done.

In short, the book is designed to be the one resource you consult whenever you have questions regarding storage, security, and networking in Windows 8.1. To this end, the book concentrates on configuration options, frequently used tasks, documented examples, and options that are representative but not necessarily inclusive. One of the goals is to keep the content so concise that the book remains compact and easy to navigate while ensuring that the book is packed with as much information as possible—making it a valuable resource.

Anyone transitioning to Windows 8.1 from Windows 8 might be surprised at just how much has been updated, because changes both subtle and substantial have been made throughout the operating system. For anyone transitioning from Windows 7 or earlier, the extensive user interface (UI) changes will be among the most substantial revisions to the operating system. Like Windows 8, Windows 8.1 supports a touch UI, in addition to the traditional mouse and keyboard. When you are working with touch-enabled computers, you can manipulate on-screen elements in ways that weren’t possible previously. You can do any of the following:

- **Tap** Tap an item by touching it with your finger. A tap or double-tap of elements on the screen generally is the equivalent of a mouse click or double-click.
- **Press and hold** Press your finger down and leave it there for a few seconds. Pressing and holding elements on the screen generally is the equivalent of a right-click.
- **Swipe to select** Slide an item a short distance in the opposite direction compared to how the page scrolls. This selects the item and might also bring up related commands. If press and hold doesn’t display commands and options for an item, try using swipe to select instead.
- **Swipe from edge (slide in from edge)** Starting from the edge of the screen, swipe or slide in. Sliding in from the right edge displays the charms. Sliding in from the left edge shows open apps and allows you to switch between them easily. Sliding in from the top or bottom edge shows commands for the active element.
- **Pinch**  Touch an item with two or more fingers, and then move the fingers toward each other. Pinching zooms out.

- **Stretch**  Touch an item with two or more fingers, and then move the fingers away from each other. Stretching zooms in.

You also are able to enter text by using the on-screen keyboard. Although the UI changes are substantial, they aren’t the most significant changes to the operating system. The most significant changes are below the surface, affecting the underlying architecture and providing many new features. Some of these features are revolutionary in that they forever change the way we use Windows.

### Who is this book for?

The focus of *Windows 8.1 Administration Pocket Consultant: Storage, Security, & Networking* is on the Standard, Professional, and Enterprise editions of Windows 8.1. The book is designed for the following readers:

- Accomplished users who are looking to configure and maintain Windows 8.1
- Current Windows system administrators and support staff
- Administrators upgrading to Windows 8.1 from earlier releases of Windows
- Administrators transferring from other platforms

To pack in as much information as possible, I had to assume that you have basic networking skills and a basic understanding of Windows operating systems. As a result, I don’t devote entire chapters to understanding Windows basics, Windows architecture, or Windows networks. I do, however, cover firmware management, boot configuration data, Trusted Platform Module (TPM), BitLocker Drive Encryption, Storage Spaces, Work Folders, and much more. The book also goes into depth on troubleshooting, and I’ve tried to ensure that each chapter, where appropriate, has troubleshooting guidelines and discussions to accompany the main text. From the start, troubleshooting advice is integrated into the book, instead of being captured in a single, catchall troubleshooting chapter inserted as an afterthought. I hope that after you read these chapters and dig into the details, you’ll be able to improve the overall experience of your users and reduce problems.

### How is this book organized?

Rome wasn’t built in a day, nor was this book intended to be read in a day, in a week, or even in a month. Ideally, you’ll read this book at your own pace, a little each day as you work your way through. This book is organized into 10 chapters. The chapters are arranged in a logical order, taking you from boot configuration and startup to drive encryption, storage configuration, data access, and networking optimization.

Ease of reference is an essential part of this hands-on guide. This book has an expanded table of contents and an extensive index for finding answers to problems quickly. Many other quick-reference features have also been added to the book,
including quick step-by-step procedures, lists, tables with fast facts, and extensive cross references.

Although designed and written to stand on its own, this book can also be used with Windows 8.1 Administration Pocket Consultant: Essentials & Configuration by William R. Stanek (Microsoft Press, 2013). The latter book focuses on deployment, installation, configuration, optimization, maintenance, and much more.

Conventions used in this book

I’ve used a variety of elements to help keep the text clear and easy to follow. You’ll find code listings in monospace type, except when I tell you to actually enter a command. In that case, the command appears in bold type, as does any text that the user is supposed to enter. When I introduce and define a new term, I put it in italics.

Other conventions include the following:

- **Best Practices**  To examine the best technique to use when working with advanced configuration and maintenance concepts
- **Caution**  To warn you about potential problems
- **Important**  To highlight important concepts and issues
- **More Info**  To provide more information on a subject
- **Note**  To provide additional details on a particular point that needs emphasis
- **Real World**  To provide real-world advice when discussing advanced topics
- **Security Alert**  To point out important security issues
- **Tip**  To offer helpful hints or additional information

I truly hope you find that Windows 8.1 Administration Pocket Consultant: Storage, Security, & Networking provides everything that you need to perform the essential tasks on Windows 8.1 systems as quickly and efficiently as possible. You are welcome to send your thoughts to me at williamstanek@aol.com. Thank you.

Other resources

No single magic bullet for learning everything you’ll ever need to know about Windows 8.1 exists. Even though some books are offered as all-in-one guides, there’s just no way one book can do it all. With this in mind, I hope you use this book as it is intended to be used—as a concise and easy-to-use resource. It covers everything you need to perform essential storage, networking, and security tasks, but it is by no means exhaustive.

Your current knowledge will largely determine your success with this or any other Windows resource or book. As you encounter new topics, take the time to practice what you’ve learned and read about. Seek out further information as necessary to get the practical hands-on know-how and knowledge you need.
For topics this book doesn't cover, you might want to look to *Windows 8.1 Administration Pocket Consultant: Essentials & Configuration*. I also recommend that you regularly visit the Microsoft website for Windows (microsoft.com/windows/) and support.microsoft.com to stay current with the latest changes. To help you get the most out of this book, you can visit my corresponding website at pocket-consultant.com. This site contains information about Windows 8.1 and updates to the book.

**Errata and book support**

We’ve made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed at:

http://aka.ms/Win81APC_SSN/errata

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at:

msinput@microsoft.com

Please note that product support for Microsoft software is not offered through the addresses above.

**We want to hear from you**

At Microsoft Press, your satisfaction is our top priority, and your feedback is 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.
As surprising as it might seem, when a computer fails to start or experiences a Stop error that crashes the operating system, the most basic element involved in starting a computer and loading an operating system—the firmware—is often overlooked as a possible cause. This happens because most people dig in and begin troubleshooting Windows without looking at the firmware. The trouble with this approach is that many computer problems originate in firmware, either because the firmware itself is flawed or because the firmware has been improperly configured. To distinguish between problems in firmware and problems in the operating system, you need to understand how the startup process works and what occurs during each of its phases. You also need to understand firmware itself. Primed with a solid understanding of these subjects, you’ll be better prepared to diagnose and resolve related problems.

Navigating and understanding firmware options

The startup process involves firmware, firmware interfaces, and an operating system. During startup, firmware is the first code that runs. Firmware performs basic initialization of the computer and provides the services that enable a computer to start loading an operating system.

Platform firmware is implemented in motherboards and chipsets. All computers—whether tablets, desktops, or laptops—have motherboard chipsets, and there are many different types. Although older motherboard chipsets might not be updatable, most newer ones have updatable firmware. Chipset firmware is separate and different from the computer’s underlying firmware interface.
Windows for the ARM processor architecture, also called Windows On ARM (or WOA), is designed with platform firmware that is also implemented in a motherboard chipset. With WOA, though, the board is a series of silicon layers packaged together in a very small form factor called a System on a Chip (SoC). At the time of this writing, there are two variants of Windows On ARM: Windows RT, which was originally designed for tablets, and Windows Phone operating system, which was originally designed for smartphones. Though Windows RT has nearly the same UI as Windows 8.1, the Windows Phone operating system has a UI that has substantial differences from Windows 8.1.

**NOTE** WOA presents a special case for firmware, boot configuration, and startup. Although I’ve tried to integrate some WOA discussion into this chapter, not everything I discuss in this chapter will apply to WOA. Further, it is important to point out that I refer to WOA throughout this chapter rather than discussing either Windows RT or Windows Phone operating system specifically. In the future, Windows Phone operating system might be merged into Windows RT (or a new variant might be created by merging aspects of both).

### Firmware interface types and boot data

Every computer has firmware, yet it’s the interface between that firmware and the operating system that handles the startup process. The way a firmware interface works and the tasks it performs depend on the type of firmware interface. Currently, the prevalent firmware interfaces are:

- Basic input/output system (BIOS)
- Extensible Firmware Interface (EFI)
- Unified Extensible Firmware Interface (UEFI)

A computer’s BIOS, EFI, or UEFI provides the hardware-level interface between hardware components and software. Like chipsets themselves, BIOS, EFI, and UEFI can be updated. Most technical documentation refers to a computer’s firmware interface simply as firmware. For example, documentation might specify to make “such and such a change in firmware” or to “check firmware.” Technically, you make the change in the firmware interface, and the firmware interface makes the change in firmware.

UEFI is both a type of firmware interface and an industry standard. UEFI, as a firmware interface, is modular and does not necessarily serve the same purpose or provide the same functionality as BIOS or EFI. UEFI, as a standard, is designed to provide extensible and testable interfaces. For WOA, UEFI is the lowest layer of the system and, as with other chip architectures, UEFI provides the services necessary to load the operating system. WOA also supports Trusted Platform Module (TPM) for trusted boot and hardware-based drive encryption.

It’s also important to understand that BIOS, EFI, and UEFI work in distinctly different ways. BIOS is based on x86, 16-bit, real-mode architecture and was originally designed to get a computer started after the computer was powered on. This is why BIOS performs firmware-to-operating-system interfacing and platform initialization.
Regardless of the firmware interface type, Windows 8.1 uses a pre–operating system boot environment. The boot environment is an extensible abstraction layer that makes it possible for the operating system to work with multiple types of firmware interfaces without requiring the operating system to be specifically written to work with these firmware interfaces. Within the boot environment, startup is controlled by using the parameters in the Boot Configuration Data (BCD) store.

All computers running current Windows operating systems have a BCD store. The BCD store is contained in a file called the BCD registry. The location of this registry depends on the computer’s firmware, as follows:

- On BIOS-based operating systems, the BCD registry file is stored in the \Boot\Bcd directory of the active partition.
- On EFI-based operating systems, the BCD registry file is stored on the EFI system partition.

Entries in the BCD store identify the boot manager to use during startup and the specific boot applications available. The default boot manager is Windows Boot Manager. Windows Boot Manager controls the boot experience and enables you to choose which boot application is to run. Boot applications load a specific operating system or operating system version. For example, the boot application for Windows 8.1 is the Windows Boot Loader, which enables you to boot BIOS-based and EFI-based computers in much the same way.

Typically, you can press F8 or F12 during startup of the operating system to access the Advanced Boot Options menu, and then use this menu to select one of several advanced startup modes, including Safe Mode, Enable Boot Logging, and Disable Driver Signature Enforcement. These advanced modes temporarily modify the way the operating system starts to help you diagnose and resolve problems; however, they don’t make permanent changes to the boot configuration or to the BCD store.

**Boot services, run-time services, and beyond**

BIOS manages the preboot data flow between the operating system and attached devices, such as the video adapter, keyboard, mouse, and hard drive. When BIOS initializes a computer, it first determines whether all attached devices are available and functioning, and then it begins to load the operating system.

Over the years, these basic features of BIOS were expanded to encompass the following:

- **Boot services** Refers to the collection of interfaces and protocols that are present in the boot environment. The services at a minimum provide an operating system loader with access to platform capabilities required to complete the operating system boot. These services are also available to drivers and applications that need access to platform capabilities. Boot services are terminated after the operating system takes control of the computer.

- **Run-time services** Refers to the interfaces that provide access to underlying platform-specific hardware, such as timers, that might be useful during operating system run time. These services are available during the boot process but also persist after the operating system loader terminates boot services.
- **Advanced Configuration and Power Interface (ACPI)** Refers to a table-based interface to the system board that enables the operating system to implement operating system–directed power management and system configuration.

- **Services for system management BIOS (SMBIOS)** Refers to a table-based interface that is required by the Wired for Management Baseline (WMB) specification and used to relate platform-specific management information to the operating system or to an operating system–based management agent.

Generally, computers with BIOS use hard drives that have master boot record (MBR) partitions. To break free of the 16-bit roots of BIOS, Intel developed EFI as a firmware implementation for its 64-bit Itanium-based processors. EFI is based on x64, 64-bit, real-mode architecture. As with BIOS, EFI performs firmware-to-operating-system interfacing, platform initialization, and other functions. With the introduction of EFI, Intel also provided a new table architecture for hard drives, called the GUID partition table (GPT).

MBR is now considered a legacy partitioning scheme, with GPT as the preferred partitioning scheme. A legacy MBR is located at the first logical block on a disk that is not using the GPT disk layout. The first 512 bytes on an MBR disk have the following layout:

- The MBR begins with a 424-byte boot code, which is used to select an MBR partition record and load the first logical block of that partition. The boot code on the MBR is not executed by UEFI.
- The boot code is followed by a 4-byte unique MBR disk signature, which can be used by the operating system to identify the disk and distinguish the disk from other disks on the system. The unique signature is written by the operating system and not used by UEFI.
- A 2-byte separator follows the disk signature. At byte offset 446, there is an array of four MBR partition records, with each record being 16 bytes in length. Block 510 contains 0x55 and block 511 contains 0xAA. Block 512 is reserved.

The four partition records each define the first and last logical blocks that a particular partition uses on a disk:

- Each 16-byte MBR partition record begins with a 1-byte boot indicator. For example, a value of 0x80 identifies a bootable legacy partition. Any other value indicates that this is not a bootable legacy partition. This value is not used by UEFI.
- The boot indicator is followed by a 3-byte address identifying the start of the partition. At byte offset 4, there’s a 1-byte value that indicates the operating system type, which is followed by a 3-byte value that identifies the end of the partition. These values are not used by UEFI.
- At byte offset 8, there’s a 4-byte value indicating the first logical block of the partition, and this is followed by a 4-byte value indicating the size of the partition in units of logical blocks. Both of these values are used by UEFI.
**NOTE** If an MBR partition has an operating system type value of 0xEF, firmware must add the UEFI system partition GUID to the handle for the MBR partition. This enables boot applications, operating system loaders, drivers, and other lower-level tools to locate the UEFI system partition, which must physically reside on the disk.

A protective MBR may be located at the first logical block on a disk that is using the GPT disk layout. The protective MBR precedes the GUID Partition Table header and is used to maintain compatibility with tools that do not understand GPT partition structures. The purpose of the protective MBR is to protect the GPT partitions from boot applications, operating system loaders, drivers, and other lower-level tools that don’t understand the GPT partitioning scheme. The protective MBR does this by defining a fake partition covering the entire disk. When a disk has a protective MBR, the first 512 bytes on the disk have the following layout:

- The protective MBR begins with a 424-byte boot code, which is not executed by UEFI.
- The boot code is followed by a 4-byte disk signature, which is set to zero and not used by UEFI.
- A 2-byte separator follows the disk signature. This separator is set to zero and not used by UEFI.
- At byte offset 446, there is an array of four MBR partition records, with each record being 16 bytes in length. Only the first partition record—the protective partition record—is used. The other partition records are set to zero.
- Block 510 contains 0x55, and block 511 contains 0xAA. Block 512 is reserved.

The protective partition record reserves the entire space on the disk after the first 512 bytes for the GPT disk layout. The protective partition record begins with a 1-byte boot indicator that is set to 0x00, which indicates a non-bootable partition. The boot indicator is followed by a 3-byte address identifying the start of the partition at 0x000200, which is the first usable block on the disk.

At byte offset 4, there’s a 1-byte value set to 0xEE to indicate the operating system type as GPT Protective. This is followed by a 3-byte value that identifies the last usable block on the disk, which is the end of the partition (or 0xFFFFFFFF if it is not possible to represent this value).

At byte offset 8, there is a 4-byte value set to 0x00000001, which identifies the logical block address of the GPT partition header. This is followed by a 4-byte value indicating size of the disk minus one block (or 0xFFFFFFFF if the size of the disk is too large to be represented).

**UEFI**

As Intel began developing EFI, Intel developers and others around the world began to recognize the need to break the tie between firmware and processor architecture. This led to the development of UEFI. The UEFI 2.4 specification was finalized in April 2013. The UEFI specifications define a model for the interface between operating systems and platform firmware. The interface consists of data tables that contain platform-related information, in addition to boot and run-time service calls that
are available to the operating system and its loader. The interface is independent of
the processor architecture. Because UEFI abstracts the processor architecture, UEFI
works with computers that have x86, x64, ARM, or an alternative architecture. As
with EFI, computers with UEFI generally use hard drives that have GPT partitions.
However, UEFI doesn’t replace all the functionality in either BIOS or EFI and can, in
fact, be wrapped around BIOS or EFI.

**REAL WORLD** UEFI 2.4 is an incremental enhancement of UEFI 2.31, which was
released in April 2011. UEFI 2.4 adds support for NIC iSCSI and FCoE boot capabili-
ties and current boot mode. UEFI 2.4 also has improvements to prevent conflicts with
Secure Boot and enables hashes of certificates to be used for revocation and timestamp
support. Secure boot and other advanced security features are discussed in Chapter 2,
“Using TPM and BitLocker Drive encryption.”

In UEFI, the system abstraction layer (SAL) is the firmware that abstracts platform
implementation differences and provides the basic interface to all higher-level soft-
ware. UEFI defines boot services and run-time services.

UEFI boot services include:

- Event, timer, and task priority services that create, wait for, signal, check, and
close events; set timers; and raise or restore the priority of tasks.
- Memory allocation services that allocate or free memory pages, get memory
maps, and allocate or free pooled memory.
- Driver model boot services that handle protocol interfaces for devices, open
and close protocol streams, and connect or disconnect from controllers.
- Image services that load, start, and unload images.
- Miscellaneous services that set watchdog timers, copy and set memory,
install configuration tables, and perform cyclic redundancy checking (CRC)
calculations.

UEFI run-time services include:

- Variable services that get, set, and query variables.
- Time services that get and set time and get and set wakeup time.
- Virtual memory services that set virtual address mapping and convert
memory pointers.
- Miscellaneous services that reset the computer, return counters, and pass
information to the firmware.

UEFI defines architecture-independent models for EFI-loaded images, device
paths, device drivers, driver signing, and secure boot. It also defines the following:

- Console support, which enables simple text and graphics output.
- Human Interface Infrastructure support, which describes the basic mecha-
nisms for managing user input and provides definitions for related protocols,
functions, and type definitions that can help abstract user input.
- Media support, which enables I/O access to file systems, files, and media devices.
- Peripheral Component Interconnect (PCI), small computer system interface (SCSI), and Internet small computer system interface (iSCSI) bus support, which enables I/O access across a PCI, SCSI, or iSCSI bus, in addition to SCSI or iSCSI boot.
- USB support, which enables I/O access over USB host controllers, USB buses, and USB devices.
- Compression support, which provides algorithms for compressing and decompressing data.
- ACPI table support, which enables installation or removal of an ACPI table.
- EFI byte code virtual machine support, which enables loading and executing EFI device drivers.
- Network protocol support, which defines the Simple Network Protocol (SNP), Preboot Execution Environment (PXE), and Boot Integrity Services (BIS) protocols. SNP provides a packet-level interface to network adapters. PXE is used for network access and network booting. BIS is used to check the digital signature of a data block against a digital certificate for the purpose of checking integrity and authorization. PXE uses BIS to check downloaded network boot images before executing them.
- Managed network protocol support, which defines the Managed Network Service Binding Protocol (MNSBP) and the Managed Network Protocol (MNP). These services enable multiple event-driven drivers and applications to access and use network interfaces simultaneously. MNSBP is used to locate communication devices that are supported by an MNP drive and manage instances of protocol drivers. MNP is used by drivers and applications to perform raw asynchronous network-packet I/O.
- Network addressing protocol support, which defines the following protocols: Address Resolution Protocol Service Binding Protocol (ARPSBP), Address Resolution Protocol (ARP), DHCPv4, DHCPv4 service binding, DHCPv6, and DHCPv6 service binding.
- Miscellaneous network protocol support, which defines the following protocols: virtual LAN configuration, EAP and EAP management, TCPv4, TCPv4 service binding, TCPv6, TCPv6 service binding, IPv4, IPv4 service binding and configuration, IPv6, IPv6 service binding and configuration, IP5ec and IPSec2 configuration, FTPv4, FTPv4 service binding, UDPv4, UDPv4 service binding, UDPv6, UDPv6 service binding, Multicast TFTPv4, and Multicast TFTPv6.

**NOTE**  With WOA, ACPI is used for plug and play enumeration of devices (such as touch controllers, displays, and so on) during boot and for power management of devices outside of the SoC. Otherwise, there is no device tree or ability to discover what is connected to a SoC or determine how the SoC is connected.
To be clear, UEFI is not designed to replace either BIOS or EFI. Although UEFI uses a different interface for boot services and run-time services, some platform firmware must perform the functions that BIOS and EFI need for system configuration and setup because UEFI does not do this. For this reason, UEFI is often implemented on top of traditional BIOS and EFI, in which case UEFI takes the place of the initialization entry points into BIOS or EFI.

Navigating startup and power states

When a computer is first started, the firmware interface activates all the hardware required by the computer to initialize and load the operating system, including:

- Motherboard chipsets
- Processors and processor caches
- System memory
- Graphics and audio controllers
- Internal drives
- Internal expansion cards

After the firmware interface completes this process, it transfers control of the computer to the operating system. The firmware interface implementation determines what happens next:

- With BIOS-based computers running current Windows operating systems, Windows Boot Manager and Windows Boot Loader are used to boot into the operating system. Windows Boot Manager initializes the operating system by starting the Windows Boot Loader, which in turn starts the operating system by using information in the BCD store. Through the BCD parameters, you can add options that control the way the operating system starts, the way computer components are used, and the way operating system features are used.

- With Itanium-based computers, Ia64ldr.efi, Diskpart.efi, and Nvrboot.efi are used to boot into the operating system. Ia64ldr.efi handles the task of loading the operating system, whereas Diskpart.efi identifies the boot partitions. Through Nvrboot.efi, you set the parameters that enable startup.

- With other EFI-based computers, Bootmgfw.efi manages the boot process and passes control to the Windows Boot Loader. Through Bcdedit.exe, you set the parameters that enable startup.

- With UEFI, UEFI boot services provide an abstraction layer. Currently, this abstraction layer is wrapped around BIOS or EFI. A computer with BIOS in its underlying architecture uses a BIOS-based approach to booting into the operating system. A computer with EFI in its underlying architecture uses an EFI-based approach to booting into the operating system.

- With WOA, UEFI boot services provide an abstraction layer. Windows Boot Manager initializes the operating system by starting the Windows Boot Loader, which in turn starts the operating system by using information in the BCD store. Information needed to configure the device is stored in tables.
Working with firmware interfaces

When you power on most computers, you can access the firmware interface by pressing the key designated for Setup in the initial display. For example, you might press F2 or Delete during the first few seconds of startup to enter the firmware interface. Firmware interfaces have control options that make it possible for you to adjust the functionality of hardware. You can use these controls to do the following:

- Adjust LCD brightness (on laptop computers).
- Adjust the hard drive noise level.
- Adjust the number of cores the processor is using and their speed.
- Change the boot sequence.
- Change the complementary metal oxide semiconductor (CMOS) date and time.
- Restore the firmware interface to the default configuration.
- Turn on or off modular add-on devices.

Firmware interfaces have the ability to report basic configuration details, including information about the following:

- AC adapter capacity (on laptop computers)
- Battery charge and health (on laptop computers)
- LCD type and native resolution (on laptop computers)
- Firmware version
- Memory
- Processors
- Storage devices
- Video chipsets

Most firmware interfaces allow you to create supervisor, user, and/or general passwords that are not accessible from the operating system. If a supervisor password is set, you need to provide the password before you can modify the firmware configuration. If a user password is set, you need to enter the password during startup before the computer will load the operating system. If you forget these passwords, you might not be able to operate the computer or change firmware settings until you clear the forgotten passwords, which generally also clears any customization you have made to the firmware interface.

A firmware interface update can often resolve problems or add features to the computer's firmware interface. If you are not experiencing problems on a computer and are not aware of any additional features in the firmware interface that are needed, you might not need to update a computer to the latest version of the firmware interface. An additional cautionary note is that if a firmware interface update is not performed properly, it can harm the computer and prevent it from starting.
examining firmware interfaces

The information and configuration options available in the firmware interface depend on the computer with which you are working, the type of firmware interface, and the version of the firmware interface. Most desktop computers have more configuration options than do laptop computers.

As configured on my laptop computer, the firmware interface provides several menu pages offering information and controls, including Main, Advanced, Security, and Boot. The Main page provides basic information about the computer’s configuration, including:

- System time and date.
- System memory size.
- Extended memory size.
- Memory speed, such as 1,333 MHz.
- CPU type, such as Intel Core i5-2430.
- CPU speed, such as 2.40 GHz.
- CPU cache levels for L1 cache, L2 cache, and L3 cache.
- Hard drive type and model, such as WDC WD5000BPVT-75HXZ 500 GB.
- Optical disk type and model, such as PLDS DVD +/- RW DU 8A-(S1) ATAPI.
- System BIOS version, such as A02.
- AC adapter type, such as 65 W.
- Serial tag number.
- Asset tag number.
- Product name.

On the Main page, you can set the system date and time by using the options provided. The Advanced page provides additional configuration information and enables you to manage important settings. On the Advanced page, you can view or set the following:

- Intel Multiple Monitor status as Enabled or Disabled. When this setting is enabled, the computer’s integrated graphic card and add-in graphic card might be able to work together in the operating system. When it is disabled, only one graphic card (either the integrated card or a plug-in card) can be used in the operating system.
- Intel SpeedStep status as Enabled or Disabled. When this setting is enabled, the CPU can operate in multiple performance states. When it is disabled, the computer is prevented from adjusting the processor’s performance.
- Intel Virtualization status as Enabled or Disabled. When this setting is enabled, a virtual machine monitor can use hardware virtualization capabilities.
- Intel Turbo Boost status as Enabled or Disabled. When this setting is enabled, processor cores can run faster than the base operating frequency if they’re operating below temperature, current, and power limits.
- USB PowerShare status as Enabled or Disabled. When this setting is enabled, users can use the USB PowerShare port to charge external devices by using the stored system battery power even if the computer is turned off.
- USB Emulation status as Enabled or Disabled. When this setting is enabled, firmware can handle USB devices during the POST process (which occurs before the operating system starts).
- USB Wake Support status as Enabled or Disabled. When this setting is enabled, USB devices can wake the computer.

The Security page enables you to view and set supervisor, user, and hard drive passwords. The status information tells you the current state for each password, such as:
- Supervisor Password Is: Clear
- User Password Is: Clear
- Hard Disk Password Status: Clear

The following additional configuration options enable you to manage passwords:
- **Set Supervisor Password** Controls access to the firmware interface
- **Set User Password** Controls access to the computer
- **Set Hard Disk Password** Controls access to the computer’s hard drive

To set a password, select the option, and then press Enter. When prompted, type the new password, and then type the new password again to confirm it. Press Enter to continue.

On the Boot page, the Boot Priority Order enables you to view and manage the priority order for boot devices. A sample boot priority order listing from a Dell desktop computer is as follows:

1. Hard drive
2. USB hard drive
3. CD/DVD
4. USB CD/DVD
5. USB Floppy
6. Network

When you power on the computer, the computer tries to boot using the device listed first. If that fails, the computer tries the second device, and so on. You can use the Up Arrow and Down Arrow keys to select a device, and then use the plus sign (+) or the hyphen (-) to move the device up or down in the list.

The Exit page enables you to exit the firmware interface and resume startup of the computer. As with most firmware interfaces, you have a few options:
- **Exit Saving Changes** Exits the firmware interface and saves your changes
- **Exit Discarding Changes** Exits the firmware interface and discards your changes
- **Discard Changes** Discards your changes without exiting the firmware interface
- **Save Changes** Saves your changes without exiting the firmware interface
Regardless of the menu page with which you are working, you have a set of options that are standard in most firmware interfaces:

- Press F1 to get help.
- Press the Up Arrow or Down Arrow key to select an item.
- Press Enter to select the current option on a submenu.
- Press the Left Arrow or Right Arrow key to select a menu page.
- Press + or - to change values.
- Press F9 to apply setup defaults (you must confirm when prompted).
- Press Esc to exit (and then select an option to save or discard changes).
- Press Enter to apply or execute a command.
- Press F10 to save changes and exit the firmware interface. (When prompted to confirm, Yes is selected. Press Enter to save changes and exit. Press the spacebar to select No, and then press Enter to remain in the firmware interface.)

As you can tell, the configuration options here aren’t very extensive. In contrast, desktop computers can have a dizzying array of options and suboptions. When you are working with a desktop computer, you’ll likely find options that serve similar purposes. However, because few standards and conventions exist among firmware interface manufacturers, the options might have different labels and values.

**power states and power management**

To better understand the hardware aspects related to boot issues, let’s dig in and take a look at ACPI. A computer’s motherboard chipset, firmware, and operating system must support ACPI for the related advanced power state features to work. ACPI-aware components track the power state of the computer. An ACPI-aware operating system can generate a request that the system be switched into a different ACPI mode, and the firmware interface responds by enabling the requested ACPI mode.

As shown in Table 1-1, there are six different power states, ranging from S0 (the system is completely on and fully operational) to S5 (the system is completely off). The states S1, S2, S3, and S4 are referred to as sleep states, in which the system appears off because of low power consumption but retains enough of the hardware context to return to the working state without a system reboot.

Motherboard chipsets support specific power states. For example, one motherboard might support the S0, S1, S4, and S5 states but not the S2 and S3 states. In Windows operating systems, the sleep power transition refers to switching off the system to a sleep or a hibernate mode, and the wake power transition refers to switching on the system from a sleep or a hibernate mode. The sleep and hibernate modes enable users to switch systems off and on much faster than the regular shutdown and startup processes.
Thus, a computer is waking up when the computer is transitioning from the Off state (S5) or any sleep state (S1–S4) to the On state (S0). The computer is turning off (going to sleep) when the computer is transitioning from the On state (S0) to the Off state (S5) or one of the sleep states (S1–S4). A computer cannot enter one sleep state directly from another; it must enter the On state before entering a different sleep state.

TABLE 1-1 Power states for ACPI in firmware and hardware

<table>
<thead>
<tr>
<th>STATE</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0</td>
<td>On state</td>
<td>The system is completely operational, fully powered, and completely retains the context (such as the volatile registers, memory caches, and RAM).</td>
</tr>
<tr>
<td>S1</td>
<td>Sleep state</td>
<td>The system consumes less power than the S0 state. All hardware and processor contexts are maintained.</td>
</tr>
<tr>
<td>S2</td>
<td>Sleep state</td>
<td>The system consumes less power than the S1 state. The processor loses power, and processor context and contents of the cache are lost.</td>
</tr>
<tr>
<td>S3</td>
<td>Sleep state</td>
<td>The system consumes less power than the S2 state. Processor and hardware contexts, cache contents, and chipset context are lost. The system memory is retained.</td>
</tr>
<tr>
<td>S4</td>
<td>Hibernate state</td>
<td>The system consumes the least power compared to all other sleep states. The system is almost at the Off state. The context data is written to the hard drive, and no context is retained. The system can restart from the context data stored on the disk.</td>
</tr>
<tr>
<td>S5</td>
<td>Off state</td>
<td>The system is in a shutdown state and retains no context. The system requires a full reboot to start.</td>
</tr>
</tbody>
</table>

When you are working with firmware, you can go to the Advanced/Power Management screen or a similar screen to manage ACPI and related settings. Power settings you might find include the following:

- **Restore AC Power Loss or AC Recovery** Determines the mode of operation if a power loss occurs, for which you’ll get settings such as Stay Off, Last State, and Power On. Stay Off (or Power Off) means the system will remain off after power is restored. Last State restores the system to the state it was in before power failed. Power On means the system will turn on after power is restored.

- **Wake On LAN From S4/S5 or Auto Power On** Determines the action taken when the system power is off and a PCI Power Management wake event occurs. You’ll notice settings like Power On or Power Off. You might also notice Enabled or Disabled.

- **ACPI Suspend State or Suspend Mode** Sets the suspend mode. Typically, you’re able to set S1 state or S3 state as the suspend mode.
NOTE In this list, I provide two standard labels for each setting because your computer hardware might not have these exact labels. The firmware variant with which you are working determines the actual labels that are associated with boot, power, and other settings.

Because Intel and AMD also have other technologies to help reduce startup and resume times, you might also find power settings, such as these for Intel:

- Enhanced Intel SpeedStep Technology (EIST), which can be either disabled or enabled
- Intel Quick Resume Technology Driver (QRTD), which can be either disabled or enabled

EIST (also known as SpeedStep) enables the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. When EIST or a similar technology is enabled and in use, you'll find two different processor speeds on the System page in Control Panel. The first speed listed is the specified speed of the processor. The second speed is the current operating speed, which should be less than the first speed. If EIST is off, both processor speeds will be equal. Advanced Settings for Processor Power Management under Power Options can also affect how this technology works. Generally speaking, you should not use this technology with Windows 8.1 (although you might want to use this technology with Windows Vista).

QRTD makes it possible for an Intel Viiv technology-based computer to behave like a consumer electronic device, with instant on/off after an initial boot. Intel QRTD manages this behavior through the Quick Resume mode function of the Intel Viiv chipset. Pressing the power button on the computer or a remote control puts the computer in the Quick Sleep mode, and you can switch the computer to the Quick Resume mode by moving the mouse, pressing an on/off key on the keyboard (if available), or pressing the Sleep button on the remote control. Quick Sleep mode is different from standard sleep mode. In Quick Sleep mode, the computer’s video card stops sending data to the display, the sound is muted, and the monitor light-emitting diode (LED) indicates a lowered power state on the monitor, but the power continues to be supplied to vital components on the system, such as the processor, fans, and so on. This technology was originally designed for legacy Windows operating systems and generally should not be used with Windows 8.1. (On older hardware, you might need to disable this feature in firmware to enable Windows 8.1 to properly sleep and resume.)

After you look at the computer’s power settings in firmware, you should also review the computer’s boot settings in firmware. Often, you can configure the following boot settings:

- **Boot Drive Order** Determines the boot order for boot devices.
- **Boot To Hard Disk Drive** Determines whether the computer can boot to hard drives. Can be set to Disabled or Enabled.
- **Boot To Removable Devices** Determines whether the computer can boot to removable media. Can be set to Disabled or Enabled.
- **Boot To Network**  Determines whether the computer can perform a network boot. Can be set to Disabled or Enabled.

- **USB Boot**  Determines whether the computer can boot to USB flash devices. Can be set to Disabled or Enabled.

On some computers, you might have a list of bootable devices and be able to select which to boot.

As for power settings, your computer might not have the exact labels shown here, but the labels should be similar. You need to optimize these settings for the way you plan to use the computer. When you use BitLocker Drive Encryption, you should enable Boot To Removable Devices, USB Boot, or both to ensure that the computer can detect the USB flash drive with the encryption key during the boot process.

### Diagnosing and resolving startup problems

To diagnose and resolve startup problems, you need to understand the sequence of events that occur after you press the power button on a computer. When you press the power button, the following happens:

1. The firmware interface performs system configuration, also known as power-on self test (POST).
2. The firmware interface performs setup of the computer, also known as initialization of the computer.
3. The firmware interface passes control to the operating system loader, also known as the boot manager.
4. The boot manager starts the boot loader. The boot loader uses the firmware interface boot services to complete the operating system boot and load the operating system. Loading the operating system involves:
   a. Loading (but not running) the operating system kernel (typically, Ntoskrnl.exe).
   b. Loading (but not running) the hardware abstraction layer (HAL) (typically, Hal.dll).
   c. Loading the HKEY_LOCAL_MACHINE\SYSTEM registry hive into memory (from %SystemRoot%\System32\Config\System).
   d. Scanning the HKEY_LOCAL_MACHINE\SYSTEM\Services key for device drivers and then loading (but not initializing) the drivers that are configured for the boot class into memory. Drivers are also services (which means both device drivers and system services are prepared).
   e. Enabling memory paging.

5. The boot loader passes control to the operating system kernel.
6. The kernel and the HAL initialize the Windows executive, which in turn processes the configuration information stored in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet hive, and then starts device drivers and system services.
7. The kernel starts the Session Manager (Smss.exe), which in turn:
   a. Initializes the system environment by creating system environment variables.
   b. Starts the Win32 subsystem (Csrss.exe). Here, Windows switches the display output from text mode to graphics mode.
   c. Starts the Windows Logon Manager (Winlogon.exe), which in turn starts the Services Control Manager (Services.exe) and the Local Security Authority (Lsass.exe) and waits for a user to log on.
   d. Creates additional paging files that are required.
   e. As necessary, performs delayed renaming of in-use files that were updated in the previous session.

8. The Windows Logon Manager waits for a user to log on. The logon user interface and the default credential provider collect the user name and password and pass this information to the Local Security Authority for authentication.

9. The Windows Logon Manager runs Userinit.exe and the File Explorer shell. Userinit.exe initializes the user environment by creating user environment variables, running startup programs, and performing other essential tasks.

   This sequence of events is for a cold start of a computer from power on through logon. The sequence of events varies if the computer is resuming from sleep, standby, or hibernation. The sequence of events also varies if you are starting an operating system other than Windows or a Windows operating system other than Windows Vista or later.

   **REAL WORLD**  With WOA, the sequence of events is similar but slightly different. Here, UEFI provides the services necessary for loading the operating system. Windows Boot Manager initializes the operating system by starting the Windows Boot Loader, which in turn starts the operating system by using information in the BCD store. The boot loader passes control to the operating system kernel. The kernel and the HAL initialize the Windows executive. Information needed to configure WOA is stored in tables so the operating system can read the table and configure WOA. In order to load device drivers and continue boot, the Windows executive initializes the simple peripheral buses (a series of low-power serial buses) and then the device drivers that support connections to those buses. The kernel can then start the Session Manager, which in turn brings up the rest of the system.

   Sometimes you can identify the source of a startup problem by pinpointing where the startup process breaks. Table 1-2 lists the various startup phases and provides a possible cause of problems in each phase. The phase numbers are meant only to aid in the subsequent discussion.
TABLE 1-2 Troubleshooting startup

<table>
<thead>
<tr>
<th>PHASE</th>
<th>PHASE TITLE</th>
<th>POSSIBLE CAUSE OF PROBLEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>System configuration, power-on self-test</td>
<td>Hardware failure or missing device</td>
</tr>
<tr>
<td>2</td>
<td>Setup, initial startup</td>
<td>Firmware configuration, the disk subsystem, or the file system</td>
</tr>
<tr>
<td>3</td>
<td>Operating system loader, boot manager</td>
<td>BCD data, improper operating system selection for loading, or invalid boot loader</td>
</tr>
<tr>
<td>4</td>
<td>Kernel, HAL, Windows executive</td>
<td>Driver or service configuration or service dependencies</td>
</tr>
<tr>
<td>5</td>
<td>Session Manager</td>
<td>Graphics display mode, system environment, or component configuration</td>
</tr>
</tbody>
</table>

Troubleshooting startup phase 1

When you turn on a computer from a cold state, system configuration (power-on self test) occurs first. During this phase, the firmware performs initial checks of hardware, verifies that required devices are present, and reads the system configuration settings from nonvolatile memory on the motherboard. Although nonvolatile memory could be Electronically Erasable Programmable Read-Only Memory (EEPROM), flash, or battery-backed RAM, it is more typically flash memory that remains even after you shut down and unplug the computer.

After the motherboard firmware performs its tests and reads its settings, add-on devices that have their own firmware, such as video cards and host controller cards, perform their tests and load their settings. If startup fails in this phase, the computer likely has a hardware failure. A required device, such as a keyboard, mouse, or hard drive, could also be missing. In most cases, the firmware interface displays an error message that indicates the problem. If video isn’t working, the firmware interface might indicate the problem by emitting a series of beeps.

You can resolve a problem with a keyboard, mouse, or display by checking the device’s connection to the computer. If another device is causing a problem, you might be able to resolve the problem by changing the device configuration in the firmware interface, or you might need to replace the device.
Troubleshooting startup phase 2

After system configuration is complete, the computer enters the setup, or initial startup, phase. Firmware interface settings determine the devices the computer uses to start the operating system. The boot order and the boot enabled or disabled state of each device affects startup. As discussed previously, the computer tries to boot by using the device listed first. If that fails, the computer tries the second boot device, and so on. If none of the configured devices are bootable, you’ll get an error similar to the following:

Non-system disk or disk error
Replace and press any key when ready to continue

Here, you’ll want to check the boot order and be sure it is set correctly. If you are trying to boot from DVD media, check that the media is present and that DVD booting is enabled. If you are trying to boot from a hard drive, make sure booting from a hard drive is enabled and listed prior to any USB or other removable media you’ve inserted. If you’ve recently installed a hard drive, power off and unplug the computer, and then verify that all cables are connected correctly and that any jumpers are configured correctly.

Because configuring boot options in firmware isn’t necessarily intuitive, I’ll provide examples from a cross-section of computers by various vendors. On an HP notebook computer, the boot settings are found on the Boot Options and Boot Order submenus on the System Configuration page. The Boot Options sub-menu has these options:

- **F10 And F12 Delay (sec)**  Sets the amount of time for the user to press F10 or F12 at startup. On this notebook, F10 and F12 access boot options and advanced boot options, respectively.
- **DVD Boot**  Enables or disables DVD boot during startup.
- **Floppy Boot**  Enables or disables the floppy boot during startup.
- **Internal Network Adapter Boot**  Enables or disables networking booting during startup.

Use the Up Arrow and Down Arrow keys to select an option, and then press Enter to view and set the option.

On the Boot Order submenu, the boot order is listed as the following:

1. USB Floppy
2. ATAPI CD/DVD ROM Drive
3. Notebook Hard Drive
4. USB Diskette On Key
5. USB Hard Drive
6. Network Adapter (only if Internal Network Adapter Boot is enabled)

Here, you use the Up Arrow and Down Arrow keys to select a device, and then press F5 or F6 to move the device up or down in the list. It is important to note that this computer (like many newer computers) distinguishes between USB flash keys (referred to as **USB diskettes on keys**) and USB drives (referred to as **USB hard drives**). Computer users won’t really perceive a difference between the two.
On a Dell Inspiron laptop, you manage boot settings on the Boot page. The boot order is listed as:

1. Hard drive
2. USB hard drive
3. CD/DVD
4. USB CD/DVD
5. USB Floppy
6. Network

You use the Up Arrow and Down Arrow keys to navigate the boot priority list. Press Enter to select a priority level for editing and then to select the device that should have that priority. Select Disabled to temporarily disable that boot priority level.

More desktop computers are being shipped with hardware redundant array of independent disks (RAID) controller cards. On a Dell computer I have, the SATA Operation option of the Drives submenu is used to enable or disable the hardware RAID controller card. Typically, RAID controller cards for desktop computers support RAID 0 and RAID 1. RAID 0 offers no data protection and just stretches a logical disk volume across multiple physical disks. RAID 1 offers data protection by mirroring the disks. When disks are mirrored, two physical disks appear as one disk, and each disk has identical copies of any data.

**REAL WORLD** A computer with a hardware RAID controller might not boot if one of the drives required for RAID operations is removed from the computer without first disabling the hardware RAID. If the remaining drive is bootable, disable RAID in BIOS, and then restart the computer to enable booting of the operating system.

### Troubleshooting startup phase 3

After setup, the firmware interface passes control to the boot manager. The boot manager in turn starts the boot loader.

On computers using BIOS, the computer reads information from the master boot record (MBR), which usually is the first sector of data on the disk. The MBR contains boot instructions and a partition table that identifies disk partitions. The active partition, also known as the boot partition, also has boot code in its first sector of data. The data provides information about the file system on the partition and enables the firmware to locate and start the Bootmgr stub program in the root directory of the boot partition. Bootmgr switches the process into 32-bit or 64-bit protected mode from real mode and loads the 32-bit or 64-bit Windows Boot Manager (found within the stub file itself), as appropriate. Windows Boot Manager locates and starts the Windows Boot Loader (Winload).

Problems can occur if the active boot partition does not exist or if any boot sector data is missing or corrupt. Errors you might get include:

- **Error loading operating system**
- **Invalid partition table**
In many cases, you can restore proper operations by using the Startup Repair tool.

In contrast, computers using EFI have a built-in boot manager. When you install Windows, Windows adds an entry to the EFI boot manager called Windows Boot Manager, which points to the boot manager’s executable file on the EFI system partition (\Efi\Microsoft\Boot\Bootmgfw.efi). The boot manager then passes control to the Windows Boot Loader.

Problems can occur if you install a different operating system or change the EFI boot manager settings. In many cases, you’ll be able to restore proper operations by using the Startup Repair tool or by changing EFI boot manager settings.

**Troubleshooting startup phase 4**

The boot loader uses the firmware interface boot services to complete operating system boot. The boot loader loads the operating system kernel (Ntoskrnl.exe), and then loads the hardware abstraction layer (HAL), Hal.dll. Next, the boot loader loads the HKEY_LOCAL_MACHINE\SYSTEM registry hive into memory (from %SystemRoot%\System32\Config\System), and then it scans the HKEY_LOCAL_MACHINE\SYSTEM\Services key for device drivers. The boot loader scans this registry hive to find drivers that are configured for the boot class and loads them into memory.

After the boot loader passes control to the operating system kernel, the kernel and the HAL initialize the Windows executive, which in turn processes the configuration information stored in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet hive and then starts device drivers and system services. Drivers and services are started according to their start-type value. This value is set on the Start subkey under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Name, where Name is the name of the device or service. Valid values are 0 (identifies a boot driver), 1 (identifies a system driver), 2 (identifies an auto-load driver or service), 3 (identifies a load-on-demand driver or service), 4 (identifies a disabled and not-started driver or service), and 5 (identifies a delayed-start service). Drivers are started in the following order: boot, system, auto load, load on demand, and delayed start.

Most problems in this phase have to do with invalid driver and service configurations. Some drivers and services are dependent on other components and services. If dependent components or services are not available or are not configured properly, this also could cause startup problems.

During startup, subkeys of HKEY_LOCAL_MACHINE\SYSTEM are used to configure devices and services. The Select subkey has several values used in this regard:

- The Current value is a pointer to the ControlSet subkey containing the current configuration definitions for all devices and services.
- The Default value is a pointer to the ControlSet subkey containing the configuration definition the computer uses at the next startup, if no error occurs and you don’t use an alternate configuration.
The Failed value is a pointer to the ControlSet subkey containing a configuration definition that failed to load Windows.

The LastKnownGood value is a pointer to the ControlSet subkey containing the configuration definition that was used for the last successful logon.

During normal startup, the computer uses the Default control set. Generally, if no error has occurred during startup or you haven't selected the last known good configuration, the Default, Current, and LastKnownGood values all point to the same ControlSet subkey, such as ControlSet001. If startup fails and you access the last known good configuration by using the Advanced Boot options, the Failed entry is updated to point to the configuration definition that failed to load. If startup succeeds and you haven’t accessed the last known good configuration, the value of LastKnownGood is updated to point to the current configuration definition.

**Troubleshooting startup phase 5**

During the final phase of startup, the kernel starts the Session Manager (Smss.exe). The Session Manager initializes the system environment by creating system environment variables and starting the Win32 subsystem (Csrss.exe). This is the point at which Windows switches from the text presentation mode used initially to a graphics presentation mode. Generally, if the display adapter is broken or not properly seated, the computer won’t display in either text or graphics mode, but if the display adapter is configured improperly, you’ll often notice this when the computer switches to graphics mode.

The display is only one of several components that might first present problems during this late phase of startup. If startup fails during this phase, you can identify problem components by using boot logging. If the computer has a Stop error in this phase, use the information provided by the Stop message to help you identify the problem component.

The Session Manager starts the Windows Logon Manager (Winlogon.exe), which in turn starts the Services Control Manager (Services.exe) and the Local Security Authority (Lsass.exe) and waits for a user to log on. When a user logs on, the Windows Logon Manager runs Userinit.exe and the File Explorer shell. Userinit.exe initializes the user environment by creating user environment variables, running startup programs, and performing other essential tasks. The File Explorer shell provides the desktop, taskbar, and menu system.

If you encounter startup problems during or after logon, the problem is likely due to a misconfigured service or startup application. As part of troubleshooting, you can temporarily disable services and startup applications, as discussed in the section “Managing system boot configuration,” later in this chapter.
Managing startup and boot configuration

During startup of the operating system, you can press F8 or F12 to access the Advanced Boot Options menu, and then use this menu to select one of several advanced startup modes. These advanced modes don’t make permanent changes to the boot configuration or to the BCD store. Tools you can use to modify the boot configuration and manage the BCD store include the Startup And Recovery dialog box, the System Configuration utility, and the BCD Editor. The sections that follow discuss how these tools are used.

Setting startup and recovery options

The Startup And Recovery dialog box controls the basic options for the operating system during startup. You can use these options to set the default operating system, how long to display the list of available operating systems, and how long to display recovery options when needed. Whether or not you boot a computer to different operating systems, you’ll want to optimize these settings to reduce the wait time during startup and, in this way, speed up the startup process.

You can configure options in the Startup And Recovery dialog box by completing the following steps:

1. In Control Panel, tap or click System And Security, and then tap or click System to display the System window.

2. In the left pane of the System window, tap or click Advanced System Settings to display the System Properties dialog box.

3. On the Advanced tab of the System Properties dialog box, under Startup And Recovery, tap or click Settings. This displays the Startup And Recovery dialog box, shown in Figure 1-1.

4. On a computer with multiple operating systems, use the Default Operating System list to specify the operating system that you want to start by default.

5. Set the timeout interval for the operating system list by selecting the Time To Display List Of Operating Systems check box and specifying the interval in seconds. To speed up the startup process, you could use a value of 5 seconds.

6. Set the timeout interval for the recovery options list by selecting the Time To Display Recovery Options When Needed check box and specifying the interval in seconds. Again, to speed up the startup process, use a value of 5 seconds.

7. Under System Failure, select Write An Event To The System Log if you want to record events related to system failure. If you want the computer to automatically restart after a failure, select Automatically Restart.

8. Tap or click OK to save your settings.
Managing system boot configuration

The System Configuration utility (Msconfig.exe) enables you to fine-tune the way a computer starts. Typically, you use this utility during troubleshooting and diagnostics. For example, as part of troubleshooting, you can configure the computer to use a diagnostic startup in which only basic devices and services are loaded.

In Control Panel, the System Configuration utility is available under System And Security/Administrative Tools. You can also start the System Configuration utility by pressing the Windows key, typing `msconfig.exe` (which typically is entered automatically into the Apps Search box), and then pressing Enter. As shown in Figure 1-2, this utility has a series of tabs with options.

The General tab options enable you to configure the way startup works and are the starting point for troubleshooting and diagnostics. By using these options, you can choose to perform a normal startup, diagnostic startup, or selective startup. After you restart the computer and resolve any problems, open the System Configuration utility again, select Normal Startup on the General tab, and then tap or click OK.

The Boot tab options enable you to control the way that individual startup-related processes work. You can configure the computer to start in one of various Safe Boot modes and set additional options, such as No GUI Boot. If, after troubleshooting, you find that you want to keep these settings, select the Make All Boot Settings Permanent check box to save the settings to the boot configuration startup entry.
Managing firmware, boot configuration, and startup

FIGURE 1-2 Use the System Configuration utility for troubleshooting.

Tapping or clicking the Advanced Options button on the Boot tab displays the BOOT Advanced Options dialog box, shown in Figure 1-3. In addition to locking PCI and enabling debugging, you can use the advanced options to do the following:

- Specify the number of processors the operating system should use, regardless of whether the processors are discrete socketed CPUs or cores on a single CPU. You should use this option when you suspect a problem with additional processors that are available and you want to identify the problem as being related to multiprocessor configurations or parallelism. Consider the following scenario: A computer is shipped with a single CPU that has four processor cores. A custom application used in-house for inventory management performs very poorly while running on this computer, but very well on computers with single processors. You configure the computer to boot with only one processor and find that the application’s performance actually improves. You re-enable all the processors and let the software development team know that the application behaves as if it has not been properly optimized for parallelism.

- Specify the maximum amount of memory the operating system should use. Use this option when you suspect a problem with additional memory you’ve installed in a computer. Consider the following scenario: A computer is shipped with 8 gigabytes (GB) of RAM, and you installed another 8 GB of RAM. Later, you find that you cannot start Windows 8.1. You could eliminate the new RAM as the potential cause by limiting the computer to 8,192 megabytes (MB) of memory.
If you suspect that services installed on a computer are causing startup problems, you can quickly determine this by choosing a diagnostic or selective startup on the General tab. After you’ve identified that services are indeed causing startup problems, you can temporarily disable services by using the Services tab options and then rebooting to determine if the problem goes away. If the problem no longer appears, you might have pinpointed it. You can then permanently disable the service or check with the service vendor to find out if an updated executable file is available. You disable a service by clearing the related check box on the Services tab.

Similarly, if you suspect applications that run at startup are causing problems, you can quickly determine this by tapping or clicking Open Task Manager on the Startup tab. You disable a startup application by selecting it on the Startup tab and then tapping or clicking Disable. If the problem no longer appears, you might have pinpointed the cause of it. You can then permanently disable the startup application or check with the software vendor to find out if an updated version is available.

Keep in mind that if you use the System Configuration utility for troubleshooting and diagnostics, you should later remove your selective startup options. After you restart the computer and resolve any problems, open the System Configuration utility again, restore the original settings, and then tap or click OK.

Using the BCD editor
The BCD store contains multiple entries. On a BIOS-based computer, you’ll find the following entries:

- One Windows Boot Manager entry. There is only one boot manager, so only one boot manager entry is visible.
- One or more Windows Boot Loader application entries, with one for each instance of Windows Vista or later installed on the computer. If you’ve installed Windows Server 2008 or later, you’ll also find entries for each installation.
Windows Boot Manager is a boot loader application. There are also other boot loader applications, including:

- Operating system loader, identified as Osloader
- Windows Boot Sector Application, identified as Bootsector
- Firmware Boot Manager, identified as Fwbootmgr
- Windows Resume Loader, identified as Resume

You can view and manage the BCD store by using the BCD Editor (Bcdedit.exe). The BCD Editor is a command-line utility. You can use the BCD Editor to view the entries in the BCD store by following these steps:

1. Enter `cmd.exe` in the Apps Search box. One way to do this is to press the Windows key, and then enter `cmd.exe`.
2. Press and hold or right-click the command prompt, and then tap or click Run As Administrator.
3. Enter `bcdedit` at the command prompt.

Table 1-3 summarizes commands you can use when you are working with the BCD store. These commands make it possible for you to do the following:

- Create, import, export, and identify the entire BCD store
- Create, delete, and copy individual entries in the BCD store
- Set or delete entry option values in the BCD store
- Control the boot sequence and the boot manager
- Configure and control Emergency Management Services (EMS)
- Configure and control boot debugging, in addition to hypervisor debugging

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>/bootdebug</td>
<td>Enables or disables boot debugging for a boot application.</td>
</tr>
<tr>
<td>/bootems</td>
<td>Enables or disable EMS for a boot application.</td>
</tr>
<tr>
<td>/bootsequence</td>
<td>Sets the one-time boot sequence for the boot manager.</td>
</tr>
<tr>
<td>/copy</td>
<td>Makes copies of entries in the store.</td>
</tr>
<tr>
<td>/create</td>
<td>Creates new entries in the store.</td>
</tr>
<tr>
<td>/createstore</td>
<td>Creates a new (empty) boot configuration data store.</td>
</tr>
<tr>
<td>/dbgsettings</td>
<td>Sets the global debugger parameters.</td>
</tr>
<tr>
<td>/debug</td>
<td>Enables or disables kernel debugging for an operating system entry.</td>
</tr>
<tr>
<td>/default</td>
<td>Sets the default entry that the boot manager will use.</td>
</tr>
<tr>
<td>COMMAND</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>/delete</td>
<td>Deletes entries from the store.</td>
</tr>
<tr>
<td>/deletevalue</td>
<td>Deletes entry options from the store.</td>
</tr>
<tr>
<td>/displayorder</td>
<td>Sets the order in which the boot manager displays the multiboot menu.</td>
</tr>
<tr>
<td>/ems</td>
<td>Enables or disables EMS for an operating system entry.</td>
</tr>
<tr>
<td>/emssettings</td>
<td>Sets the global EMS parameters.</td>
</tr>
<tr>
<td>/enum</td>
<td>Lists entries in the store.</td>
</tr>
<tr>
<td>/export</td>
<td>Exports the contents of the system store to a file. This file can be used</td>
</tr>
<tr>
<td></td>
<td>later to restore the state of the system store.</td>
</tr>
<tr>
<td>/hypervisorsettings</td>
<td>Sets the hypervisor parameters.</td>
</tr>
<tr>
<td>/import</td>
<td>Restores the state of the system store by using a backup file created with</td>
</tr>
<tr>
<td></td>
<td>the /export command.</td>
</tr>
<tr>
<td>/mirror</td>
<td>Creates a mirror of entries in the store.</td>
</tr>
<tr>
<td>/set</td>
<td>Sets entry option values in the store.</td>
</tr>
<tr>
<td>/store</td>
<td>Sets the BCD store to use. If not specified, the system store is used.</td>
</tr>
<tr>
<td>/sysstore</td>
<td>Sets the system store device. This only affects EFI systems.</td>
</tr>
<tr>
<td>/timeout</td>
<td>Sets the boot manager timeout value.</td>
</tr>
<tr>
<td>/toolsdisplayorder</td>
<td>Sets the order in which the boot manager displays the tools menu.</td>
</tr>
<tr>
<td>/v</td>
<td>Sets output to verbose mode.</td>
</tr>
</tbody>
</table>

**Managing the BCD store**

The BCD Editor is an advanced command-line tool for viewing and manipulating the configuration of the pre–operating system boot environment. Although I discuss tasks related to modifying the BCD data store in the sections that follow, you should attempt to modify the BCD store only if you are an experienced IT pro. As a safeguard, you should make a full backup of the computer prior to making any changes to the BCD store. Why? If you make a mistake, your computer might end up in a nonbootable state, and you would then need to initiate recovery.
Viewing BCD entries

Computers can have system and nonsystem BCD stores. The system BCD store contains the operating system boot entries and related boot settings. Whenever you work with the BCD Editor, you work with the system BCD store.

On a computer with only one operating system, the BCD entries for your computer will look similar to those in Listing 1-1. As the listing shows, the BCD store for this computer has two entries: one for the Windows Boot Manager, and one for the Windows Boot Loader. Here, the Windows Boot Manager calls the boot loader, and the boot loader uses Winload.exe to boot Windows 8.1.

Listing 1-1 Entries in the BCD Store on a single-boot computer

Windows Boot Manager
----------------------
identifier             {bootmgr}
device                partition=\Device\HarddiskVolume1
description           Windows Boot Manager
locale                en-US
inherit               {globalsettings}
integrityservices      Enable
default               {current}
resumeobject          {16b857b4-9e02-11e0-9c17-b7d085eb0682}
displayorder          {current}
                      {16b857ad-9e02-11e0-9c17-b7d085eb0682}
toolsdisplayorder     {memdiag}
timeout               30
custom:26000025       Yes

Windows Boot Loader
-------------------
identifier             {current}
device                partition=C:
path                  \Windows\system32\winload.exe
description           Windows 8.1
locale                en-US
inherit               {bootloadersettings}
recoverysequence      {16b857b6-9e02-11e0-9c17-b7d085eb0682}
integrityservices      Enable
recoveryenabled       Yes
allowedinmemorysettings 0x15000075
osdevice               partition=C:
systemroot            \Windows
resumeobject          {16b857b4-9e02-11e0-9c17-b7d085eb0682}
xn                    OptIn
bootmenupolicy        Standard

BCD entries for Windows Boot Manager and Windows Boot Loader have similar properties. These properties include those summarized in Table 1-4.
### TABLE 1-4 BCD entry properties

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Shows descriptive information to help identify the type of entry.</td>
</tr>
<tr>
<td>Device</td>
<td>Shows the physical device path. For a partition on a physical disk, you'll find an entry such as <code>partition=C:</code>.</td>
</tr>
<tr>
<td>FileDevice</td>
<td>Shows the path to a file device, such as <code>partition=C:</code>.</td>
</tr>
<tr>
<td>FilePath</td>
<td>Shows the file path to a necessary file, such as <code>\Hiberfil.sys</code>.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Shows a descriptor for the entry. This can be a boot loader application type, such as Bootmgr or Ntldr, a reference to the current operating system entry, or the globally unique identifier (GUID) of a specific object. Well-known identifiers are listed in Table 1-5, later in this chapter.</td>
</tr>
<tr>
<td>Inherit</td>
<td>Shows the list of entries to be inherited.</td>
</tr>
<tr>
<td>Locale</td>
<td>Shows the computer's locale setting, such as <code>en-US</code>. The locale setting determines the language shown in the user interface (UI). The <code>\Boot</code> folder contains locale subfolders for each locale supported, and each of these subfolders has language-specific UI details for the Windows Boot Manager and the Windows Memory Diagnostic utility (<code>Memdiag.exe</code>).</td>
</tr>
<tr>
<td>Osdevice</td>
<td>Shows the path to the operating system device, such as <code>partition=C:</code>.</td>
</tr>
<tr>
<td>Path</td>
<td>Shows the actual file path to the boot loader application, such as <code>\Windows\System32\Winload.exe</code>.</td>
</tr>
</tbody>
</table>

When you are working with the BCD store and the BCD Editor, you'll find references to well-known identifiers, summarized in Table 1-5, in addition to GUIDs. When a GUID is used, it has the following format, where each `N` represents a hexadecimal value:

`{NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN}`

such as:

`{16b857ad-9e02-11e0-9c17-b7d085eb0682}`

The dashes that separate the parts of the GUID must be entered in the positions shown. Both well-known identifiers and GUIDs are enclosed in braces.
<table>
<thead>
<tr>
<th>IDENTIFIER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>{badmemory}</td>
<td>Contains the global RAM defect list that can be inherited by any boot application entry.</td>
</tr>
<tr>
<td>{bootloadersettings}</td>
<td>Contains the collection of global settings that should be inherited by all Windows Boot Loader application entries.</td>
</tr>
<tr>
<td>{bootmgr}</td>
<td>Indicates the Windows Boot Manager entry.</td>
</tr>
<tr>
<td>{current}</td>
<td>Represents a virtual identifier that corresponds to the operating system boot entry for the operating system that is currently running.</td>
</tr>
<tr>
<td>{dbgsettings}</td>
<td>Contains the global debugger settings that can be inherited by any boot application entry.</td>
</tr>
<tr>
<td>{default}</td>
<td>Represents a virtual identifier that corresponds to the boot manager default application entry.</td>
</tr>
<tr>
<td>{emssettings}</td>
<td>Contains the global EMS settings that can be inherited by any boot application entry.</td>
</tr>
<tr>
<td>{fwbootmgr}</td>
<td>Indicates the firmware boot manager entry. This entry is used on EFI systems.</td>
</tr>
<tr>
<td>{globalsettings}</td>
<td>Contains the collection of global settings that should be inherited by all boot application entries.</td>
</tr>
<tr>
<td>{hypervisorsettings}</td>
<td>Contains the hypervisor settings that can be inherited by any operating system loader entry.</td>
</tr>
<tr>
<td>{memdiag}</td>
<td>Indicates the memory diagnostic application entry.</td>
</tr>
<tr>
<td>{ntldr}</td>
<td>Indicates the Windows Legacy OS Loader (Ntldr) that can be used to start Windows operating systems earlier than Windows Vista. Used when you've installed a legacy operating system.</td>
</tr>
<tr>
<td>{ramdiskoptions}</td>
<td>Contains the additional options required by the boot manager for RAM disk devices.</td>
</tr>
<tr>
<td>{resumeloadersettings}</td>
<td>Contains the collection of global settings that should be inherited by all Windows resume-from-hibernation application entries.</td>
</tr>
</tbody>
</table>

When a computer has additional instances of Windows installed, the BCD store has additional entries for each additional operating system. For example, the BCD store might have one entry for the Windows Boot Manager and one Windows Boot Loader entry for each operating system.
Although the Windows Boot Manager and Windows Boot Loader are the primary types of entries that control startup, the BCD store also includes information about boot settings and boot utilities. The Windows Boot Loader entry can have parameters that track the status of boot settings, such as whether No Execute (NX) policy is set to Opt In or Opt Out. The Windows Boot Loader entry also can provide information about available boot utilities, such as the Windows Memory Diagnostic utility.

To view the actual value of the GUIDs needed to manipulate entries in the BCD store, enter `bcdedit /v` at an elevated command prompt.

**Creating and identifying the BCD store**

By using the BCD Editor, you can create a nonsystem BCD store by using the following command:

`bcdedit /createstore StorePath`

*StorePath* is the folder path to the location where you want to create the nonsystem store, such as:

`bcdedit /createstore c:\non-sys\bcd`

On an EFI system, you can temporarily set the system store device by using the `/sysstore` command. Use the following syntax:

`bcdedit /sysstore StoreDevice`

*StoreDevice* is the actual system store device identifier, such as:

`bcdedit /sysstore c:`

The device must be a system partition. Note that this setting does not persist across reboots and is used only in cases in which it is not clear which system store device should be used.

**Importing and exporting the BCD store**

The BCD Editor provides separate commands for importing and exporting the BCD store. You can use the `/export` command to export a copy of the system BCD store’s contents to a specified folder. Use the following command syntax:

`bcdedit /export StorePath`

*StorePath* is the actual folder path to which you want to export a copy of the system store, such as:

`bcdedit /export c:\backup\bcd`

To restore an exported copy of the system store, you can use the `/import` command. Use the following command syntax:

`bcdedit /import ImportPath`
ImportPath is the actual folder path from which you want to import a copy of the system store, such as:

```bash
bcdedit /import c:\backup\bcd
```

On an EFI system, you can add /clean to the /import command to specify that all existing firmware boot entries should be deleted. Here is an example:

```bash
bcdedit /import c:\backup\bcd /clean
```

### Creating and deleting BCD entries

The BCD Editor provides separate commands for creating, copying, and deleting entries in the BCD store. You can use the /create command to create identifier, application, and inherit entries in the BCD store.

As shown previously in Table 1-5, the BCD Editor recognizes many well-known identifiers, including {dbgsettings}, which is used to create a debugger settings entry; {ntldr}, used to create a Windows Legacy OS entry; and {ramdiskoptions}, used to create a RAM disk additional options entry. To create identifier entries, you use the following syntax:

```bash
bcdedit /create Identifier /d "Description"
```

`Identifier` is a well-known identifier for the entry you want to create, such as:

```bash
bcdedit /create {ntldr} /d "Legacy Windows OS Loader"
```

You can also create entries for specific boot loader applications, including:

- **Bootsector** Identifies a real-mode boot sector application; used to set the boot sector for a real-mode application
- **Osloader** Identifies an operating system loader application; used to load Windows Vista or later
- **Resume** Identifies a Windows Resume Loader application; used to resume the operating system from hibernation
- **Startup** Identifies a real-mode application

Use the following command syntax:

```bash
bcdedit /create /application AppType /d "Description"
```

`AppType` is one of the previously listed application types, such as:

```bash
bcdedit /create /application osloader /d "Windows 8.1"
```

You can delete entries in the system store by using the /delete command and the following syntax:

```bash
bcdedit /delete Identifier
```

If you are trying to delete a well-known identifier, you must use the /f command to force deletion, such as:

```bash
bcdedit /delete {ntldr} /f
```
By default, when the /delete command is used, the /cleanup option is implied, which means that the BCD Editor cleans up any other references to the entry being deleted. This ensures that the data store doesn’t have invalid references to the identifier you removed. Because entries are also removed from the display order, this could result in a different default operating system being set. If you want to delete the entry and clean up all other references except the display order entry, you can use the /nocleanup command.

Setting BCD entry values

After you create an entry, you need to set additional entry option values as necessary. The basic syntax for setting values is:

`bcdedit /set Identifier Option Value`

*Identifier* is the identifier of the entry to be modified, *Option* is the option you want to set, and *Value* is the option value, such as:

```
bcdedit /set {current} device partition=d:
```

To delete options and their values, use the /deletevalue command with the following syntax:

`bcdedit /deletevalue Identifier Option`

*Identifier* is the identifier of the entry to be modified, and *Option* is the option you want to delete, such as:

```
bcdedit /deletevalue {current} badmemorylist
```

When you are working with options, Boolean values can be entered in several different ways. For True, you can use 1, On, Yes, or True. For False, you can use 0, Off, No, or False.

To view the BCD entries for all boot utilities and the values for settings, enter `bcdedit /enum all /v` at an elevated command prompt. This command enumerates all BCD entries regardless of their current state and lists them in verbose mode. Each additional entry has a specific purpose and lists values that you can set, including the following:

- **Resume From Hibernate** The Resume From Hibernate entry shows the current configuration for the resume feature. The pre-operating system boot utility that controls resume is Winresume.exe, which in this example is stored in the C:\Windows\System32 folder. The hibernation data, as specified in the FilePath parameter, is stored in the Hiberfil.sys file in the root folder on the OSDevice (C: in this example). Because the resume feature works differently if the computer has Physical Address Extension (PAE) and debugging enabled, these options are tracked by the PAE and DebugOptionEnabled parameters.

- **Windows Memory Tester** The Windows Memory Tester entry shows the current configuration for the Windows Memory Diagnostic utility. Memtest is the pre-operating system boot utility that controls memory diagnostics. Because the Windows Memory Diagnostic utility is designed to detect bad memory by default, the BadMemoryAccess parameter is set to Yes by
default. You can turn this feature off by entering `bcdedit /set {memdiag} badmemoryaccess NO`. With memory diagnostics, you can configure the number of passes by using Passcount and the test mix as Basic or Extended by using Testmix. Here is an example: `bcdedit /set {memdiag} passcount 2 textmix basic`.

- **Windows Legacy OS Loader** The Windows Legacy OS Loader entry shows the current configuration for the loading of earlier versions of Windows. The Device parameter sets the default partition to use, such as C:, and the Path parameter sets the default path to the loader utility, such as Ntldr.

- **EMS Settings** The EMS Settings entry shows the configuration used when booting with EMS. Individual Windows Boot Loader entries control whether EMS is enabled. If EMS is provided by the BIOS and you want to use the BIOS settings, you can enter `bcdedit /emssettings bios`. With EMS, you can set an EMS port and an EMS baud rate. Here is an example: `bcdedit /emssettings EMSPORT:2 EMSBAUDRATE:115200`. You can enable or disable EMS for a boot application by using `/bootems`, following the identity of the boot application with the state you want, such as On or Off.

- **Debugger Settings** The Debugger Settings entry shows the configuration used when booting with the debugger turned on. Individual Windows Boot Loader entries control whether the debugger is enabled. You can view the hypervisor debugging settings by entering `bcdedit /dbgsettings`. When debug booting is turned on, DebugType sets the type of debugger as SERIAL, 1394, or USB. With SERIAL debugging, DebugPort specifies the serial port being used as the debugger port, and BaudRate specifies the baud rate to be used for debugging. With 1394 debugging, you can use Channel to set the debugging channel. With USB debugging, you can use TargetName to set the USB target name to be used for debugging. With any debug type, you can use the /Noumex flag to specify that user-mode exceptions should be ignored. Here are examples of setting the debugging mode: `bcdedit /dbgsettings SERIAL DEBUGPORT:1 BAUDRATE:115200`, `bcdedit /dbgsettings 1394 CHANNEL:23`, `bcdedit /dbgsettings USB TARGETNAME:DEBUGGING`.

- **Hypervisor Settings** The Hypervisor Settings entry shows the configuration used when working with the hypervisor with the debugger turned on. Individual Windows Boot Loader entries control whether the debugger is enabled. You can view the hypervisor debugging settings by entering `bcdedit /hypervisorsettings`. When hypervisor debug booting is turned on, HypervisorDebugType sets the type of debugger, HypervisorDebugPort specifies the serial port being used as the debugger port, and Hypervisor-BaudRate specifies the baud rate to be used for debugging. These parameters work the same as with Debugger Settings. Here is an example: `bcdedit /hypervisorsettings SERIAL DEBUGPORT:1 BAUDRATE:115200`. You can also use FireWire for hypervisor debugging. When you do, you must separate the word *channel* from the value with a colon, as shown in this example: `bcdedit /hypervisorsettings 1394 CHANNEL:23`. 

Table 1-6 summarizes key options that apply to entries for boot applications (Bootapp). Because Windows Boot Manager, Windows Memory Diagnostic, Windows OS Loader, and Windows Resume Loader are boot applications, these options also apply to them.

**TABLE 1-6 Key options for boot application entries**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>VALUE DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>BadMemoryAccess</td>
<td>When true, enables an application to use the memory on the bad memory list. When false, applications are prevented from using memory on the bad memory list.</td>
</tr>
<tr>
<td>BadMemoryList</td>
<td>An integer list that defines the list of Page Frame Numbers of faulty memory in the system.</td>
</tr>
<tr>
<td>BaudRate</td>
<td>Sets an integer value that defines the baud rate for the serial debugger.</td>
</tr>
<tr>
<td>BootDebug</td>
<td>Sets a Boolean value that enables or disables the boot debugger.</td>
</tr>
<tr>
<td>BootEMS</td>
<td>Sets a Boolean value that enables or disables EMS.</td>
</tr>
<tr>
<td>Channel</td>
<td>Sets an integer value that defines the channel for the 1394 debugger.</td>
</tr>
<tr>
<td>ConfigAccessPolicy</td>
<td>Sets the access policy as either DEFAULT or DISALLOWMMCONFIG.</td>
</tr>
<tr>
<td>DebugAddress</td>
<td>Sets an integer value that defines the address of a serial port for the debugger.</td>
</tr>
<tr>
<td>DebugPort</td>
<td>Sets an integer value that defines the serial port number for the serial debugger.</td>
</tr>
<tr>
<td>DebugStart</td>
<td>Can be set to ACTIVE, AUTOENABLE, or DISABLE.</td>
</tr>
<tr>
<td>DebugType</td>
<td>Can be set to SERIAL, 1394, or USB.</td>
</tr>
<tr>
<td>EMSBaudRate</td>
<td>Defines the baud rate for EMS.</td>
</tr>
<tr>
<td>EMSPort</td>
<td>Defines the serial port number for EMS.</td>
</tr>
<tr>
<td>FirstMegaBytePolicy</td>
<td>Sets the first megabyte policy as USENONE, USEALL, or USEPRIVATE.</td>
</tr>
<tr>
<td>GraphicsModeDisabled</td>
<td>Sets a Boolean value that enables or disables graphics mode.</td>
</tr>
<tr>
<td>GraphicsResolution</td>
<td>Defines the graphics resolution, such as 1024 × 768 or 800 × 600.</td>
</tr>
<tr>
<td>Locale</td>
<td>Sets the locale of the boot application.</td>
</tr>
<tr>
<td>OPTION</td>
<td>VALUE DESCRIPTION</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Noumex</td>
<td>When Noumex is set to TRUE, user-mode exceptions are ignored. When Noumex is set to FALSE, user-mode exceptions are not ignored.</td>
</tr>
<tr>
<td>NoVES A</td>
<td>Sets a Boolean value that enables or disables the use of Video Electronics Standards Association (VESA) display modes.</td>
</tr>
<tr>
<td>RecoveryEnabled</td>
<td>Sets a Boolean value that enables or disables the use of a recovery sequence.</td>
</tr>
<tr>
<td>RecoverySequence</td>
<td>Defines the recovery sequence to use.</td>
</tr>
<tr>
<td>TargetName</td>
<td>Defines the target name for the USB debugger as a string.</td>
</tr>
<tr>
<td>TestSigning</td>
<td>Sets a Boolean value that enables or disables use of prerelease test-code signing certificates.</td>
</tr>
<tr>
<td>TruncateMemory</td>
<td>Sets a physical memory address at or above which all memory is disregarded.</td>
</tr>
</tbody>
</table>

Table 1-7 summarizes key options that apply to entries for Windows OS Loader (Osloader) applications.

**TABLE 1-7** Key options for Windows OS Loader applications

<table>
<thead>
<tr>
<th>OPTION</th>
<th>VALUE DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdvancedOptions</td>
<td>Sets a Boolean value that enables or disables advanced options.</td>
</tr>
<tr>
<td>BootLog</td>
<td>Sets a Boolean value that enables or disables the boot initialization log.</td>
</tr>
<tr>
<td>BootStatusPolicy</td>
<td>Sets the boot status policy. Can be DisplayAllFailures, IgnoreAllFailures, IgnoreShutdownFailures, or Ignore-BootFailures.</td>
</tr>
<tr>
<td>ClusterMode</td>
<td>Sets the maximum number of processors to include in a single Advanced Programmable Interrupt Controller (APIC) cluster.</td>
</tr>
<tr>
<td>ConfigFlags</td>
<td>Sets processor-specific configuration flags.</td>
</tr>
<tr>
<td>DbgTransport</td>
<td>Sets the file name for a private debugger transport.</td>
</tr>
<tr>
<td>Debug</td>
<td>Sets a Boolean value that enables or disables kernel debugging.</td>
</tr>
<tr>
<td>DriverLoad</td>
<td>Sets the driver load failure policy. Can be Fatal or UseErrorControl.</td>
</tr>
<tr>
<td>FailurePolicy</td>
<td></td>
</tr>
<tr>
<td>OPTION</td>
<td>VALUE DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Ems</td>
<td>Sets a Boolean value that enables or disables kernel EMS.</td>
</tr>
<tr>
<td>Hal</td>
<td>Sets the file name for a private HAL.</td>
</tr>
<tr>
<td>HalBreakPoint</td>
<td>Sets a Boolean value that enables or disables the special HAL breakpoint.</td>
</tr>
<tr>
<td>HypervisorLaunchType</td>
<td>Configures the hypervisor launch type. Can be Off or Auto.</td>
</tr>
<tr>
<td>IncreaseUserVA</td>
<td>Sets an integer value (in megabytes) that increases the amount of virtual address space that the user-mode processes can use.</td>
</tr>
<tr>
<td>Kernel</td>
<td>Sets the file name for a private kernel.</td>
</tr>
<tr>
<td>LastKnownGood</td>
<td>Sets a Boolean value that enables or disables booting to the last known good configuration.</td>
</tr>
<tr>
<td>MaxProc</td>
<td>Sets a Boolean value that enables or disables the display of the maximum number of processors in the system.</td>
</tr>
<tr>
<td>Msi</td>
<td>Sets the message signaled interrupt (MSI). Can be Default or ForceDisable.</td>
</tr>
<tr>
<td>NoCrashAutoReboot</td>
<td>Sets a Boolean value that enables or disables automatic restart on crash.</td>
</tr>
<tr>
<td>NoLowMem</td>
<td>Sets a Boolean value that enables or disables the use of low memory.</td>
</tr>
<tr>
<td>NumProc</td>
<td>Sets the number of processors to use on startup.</td>
</tr>
<tr>
<td>Nx</td>
<td>Controls no-execute protection. Can be OptIn, OptOut, AlwaysOn, or AlwaysOff.</td>
</tr>
<tr>
<td>OneCPU</td>
<td>Sets a Boolean value that forces or does not force only the boot CPU to be used.</td>
</tr>
<tr>
<td>OptionsEdit</td>
<td>Sets a Boolean value that enables or disables the options editor.</td>
</tr>
<tr>
<td>OSDevice</td>
<td>Defines the device that contains the system root.</td>
</tr>
<tr>
<td>Pae</td>
<td>Controls PAE. Can be Default, ForceEnable, or ForceDisable.</td>
</tr>
<tr>
<td>PerfMem</td>
<td>Sets the size (in megabytes) of the buffer to allocate for performance data logging.</td>
</tr>
<tr>
<td>RemoveMemory</td>
<td>Sets an integer value (in megabytes) that removes memory from the total available memory that the operating system can use.</td>
</tr>
<tr>
<td>OPTION</td>
<td>VALUE DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RestrictAPICCluster</td>
<td>Sets the largest APIC cluster number to be used by the system.</td>
</tr>
<tr>
<td>ResumeObject</td>
<td>Sets the identifier for the resume object that is associated with this operating system object.</td>
</tr>
<tr>
<td>SafeBoot</td>
<td>Sets the computer to use a Safe Boot mode. Can be Minimal, Network, or DsRepair.</td>
</tr>
<tr>
<td>SafeBoot AlternateShell</td>
<td>Sets a Boolean value that enables or disables the use of the alternate shell when booted into safe mode.</td>
</tr>
<tr>
<td>Sos</td>
<td>Sets a Boolean value that enables or disables the display of additional boot information.</td>
</tr>
<tr>
<td>SystemRoot</td>
<td>Defines the path to the system root.</td>
</tr>
<tr>
<td>UseFirmwarePCISettings</td>
<td>Sets a Boolean value that enables or disables use of BIOS-configured PCI resources.</td>
</tr>
<tr>
<td>UsePhysicalDestination</td>
<td>Sets a Boolean value that forces or does not force the use of the physical APIC.</td>
</tr>
<tr>
<td>Vga</td>
<td>Sets a Boolean value that forces or does not force the use of the VGA display driver.</td>
</tr>
<tr>
<td>WinPE</td>
<td>Sets a Boolean value that enables or disables booting to Windows Preinstallation Environment (Windows PE).</td>
</tr>
</tbody>
</table>

### Changing Data execution prevention and physical Address extension options

Data Execution Prevention (DEP) is a memory-protection technology. Windows 8 and Windows 8.1 are the first versions of Windows that require a processor that supports DEP. Windows 8 and Windows 8.1 will not install on computers that aren’t DEP-enabled.

When DEP is enabled, the computer’s processor marks all memory locations in an application as nonexecutable unless the location explicitly contains executable code. If code is executed from a memory page marked as nonexecutable, the processor can raise an exception and prevent the code from executing. This behavior prevents malicious application code, such as virus code, from inserting itself into most areas of memory.

For computers with processors that support the non-execute (NX) page-protection feature, you can configure the operating system to opt in to NX protection by setting the nx parameter to OptIn, or opt out of NX protection by setting the nx parameter to OptOut. Here is an example:

```
bcdedit /set {current} nx optout
```
When you configure NX protection to OptIn, DEP is turned on only for essential Windows programs and services. This is the default. When you configure NX protection to OptOut, all programs and services—not just standard Windows programs and services—use DEP. Programs that shouldn’t use DEP must be specifically opted out. You can also configure NX protection to be always on or always off by using AlwaysOn or AlwaysOff, such as:

```
bcdedit /set {current} nx alwayson
```

**NOTE** You opt out of programs by using advanced system settings. In Control panel, select System And Security, select System, and then select Advanced System Settings. This opens the System properties dialog box to the Advanced tab. Select Settings on the performance panel of the Advanced tab. On the Data execution prevention tab in the performance Options dialog box, select Turn On Dep For All programs except Those I Select. Finally, click Add to specify a program that shouldn’t use Dep.

Processors that support and opt in to NX protection must be running in PAE mode. You can configure PAE by setting the PAE parameter to Default, ForceEnable, or ForceDisable. When you set the PAE state to Default, the operating system uses its default configuration for PAE. When you set the PAE state to ForceEnable, the operating system uses PAE. When you set the PAE state to ForceDisable, the operating system will not use PAE. Here is an example:

```
bcdedit /set {current} pae default
```

### Changing the operating system display order

You can change the display order of boot managers associated with a particular installation of Windows by using the /displayorder command. The syntax is:

```
bcdedit /displayorder id1 id2 ... idn
```

`id1` is the operating system identifier of the first operating system in the display order, `id2` is the identifier of the second, and so on. You could change the display order of the operating systems identified in these BCD entries:

**Windows Boot Loader**

```
identifier              {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

**Windows Boot Loader**

```
identifier              {14504de-e96b-11cd-a51b-89ace9305d5e}
```

**Windows Boot Loader**

```
identifier              {8b78e48f-02d0-11dd-af92-a72494804a8a}
```

by using the following command:

```
bcdedit /displayorder {8b78e48f-02d0-11dd-af92-a72494804a8a}
{16b857b4-9e02-11e0-9c17-b7d085eb0682}
{14504de-e96b-11cd-a51b-89ace9305d5e}
```
You can set a particular operating system as the first entry by using /addfirst with
/displayorder, as in:

```
bcdedit /displayorder {16b857b4-9e02-11e0-9c17-b7d085eb0682} /addfirst
```

You can set a particular operating system as the last entry by using /addlast with
/displayorder, as in:

```
bcdedit /displayorder {8b78e48f-02d0-11dd-af92-a72494804a8a} /addlast
```

### Changing the default operating system entry

You can change the default operating system entry by using the /default command. The syntax for this command is:

```
bcdedit /default id
```

`id` is the operating system ID in the boot loader entry. You could set the operating system identified in this BCD entry as the default:

**Windows Boot Loader**

```
identifier {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

by using the following command:

```
bcdedit /default {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

If you want to use a legacy operating system, such as Windows XP, as the default, use the identifier for the Windows Legacy OS Loader. The related BCD entry looks like this:

**Windows Legacy OS Loader**

```
identifier {466f5a88-0af2-4f76-9038-095b170dc21c}
device partition=C:
path \ntldr
description Early Microsoft Windows Operating System
```

Following this, you could set Ntldr as the default by entering:

```
bcdedit /default {466f5a88-0af2-4f76-9038-095b170dc21c}
```

### Changing the default timeout

You can change the timeout value associated with the default operating system by using the /timeout command. Set the /timeout command to the wait time you want to use (in seconds) as follows:

```
bcdedit /timeout 30
```

To boot automatically to the default operating system, set the timeout to 0 seconds.
Changing the boot sequence temporarily

Occasionally, you might want to boot to a particular operating system one time and then revert to the default boot order. To do this, you can use the `/bootsequence` command. Follow the command with the identifier of the operating system to which you want to boot after restarting the computer, such as:

```
bcdedit /bootsequence {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

When you restart the computer, the computer will set the specified operating system as the default for that restart only. Then, when you restart the computer again, the computer will use the original default boot order.
CHAPTER 6

Optimizing file security

- File security and sharing options 187
- Controlling access to files and folders with NTFS permissions 192
- Applying permissions through inheritance 206

Whether you are using Windows 8.1 in a domain, a workgroup, or a home-group, few aspects of the operating system are more important than file security and file sharing. File security and file sharing are so interconnected that talking about one without talking about the other is difficult. File security protects important data on your systems by restricting access, and file sharing enables you to share data so that it can be accessed by other users.

File security and sharing options

For computers running Windows 8.1, two factors control file security and sharing options: the disk format and computer settings. The format of the disk determines the degree of file security options available. Disks can be formatted for the FAT file system (FAT16, FAT32, or exFAT), the NTFS file system, or the Resilient File System (ReFS).

**IMPORTANT** ReFS is built on the foundations of NTFS and is designed specifically for storage technologies. Because ReFS maintains compatibility with the core features of NTFS, access permissions and share permissions work the same on both ReFS and NTFS volumes. Where NTFS and ReFS diverge is when it comes to extended features, such as compression, encryption, and disk quotas, which are supported by NTFS but not supported by ReFS.

The security options on FAT, NTFS, and ReFS volumes differ greatly:

- With FAT, you have very limited control over file access. Files can be marked only as read-only, hidden, or system. Although these flags can be set on files and folders, anyone with access to the FAT volume can override or change these settings, which means that there are no safeguards for file access or deletion. Any user can access or delete any file without restriction.
- With NTFS or ReFS, you can control access to files and folders by using NTFS permissions. NTFS permissions specifically allow or deny access and can be
Optimizing file security

Set for individual users and for groups of users. These permission settings give you very granular control over file and folder access. For example, you could specify that users in the Sales Managers group have full control over a folder and its files, but users in the Sales Reps group have no access to the folder whatsoever.

The settings on a computer determine the way in which files can be shared. For Server Message Block (SMB), Windows 8.1 supports two file-sharing models:

- **Standard folder sharing** Enables you to share the files in any folder on a computer, including those on FAT, NTFS, and ReFS volumes. Two sets of permissions are used to determine who has access to shared folders: access permissions (discussed in the “Controlling access to files and folders with NTFS permissions” section later in this chapter) and share permissions (discussed in the “Sharing files and folders over the network” section in Chapter 7 “Managing file sharing and auditing”). Access permissions and share permissions together enable you to control who has access to shared folders and the level of access assigned. You do not need to move the files you are sharing.

- **Public folder sharing** Enables you to share files that are in a computer’s %SystemDrive%\Users\Public folder. Access permissions on the Public folder determine which users and groups have access to publicly shared files, in addition to what level of access those users and groups have. When you copy or move files to the Public folder, access permissions on the files are changed to match those of the Public folder. Some additional permissions are also added. For more information, see the “Using and configuring public folder sharing” section in Chapter 7.

*NOTE* With standard folder sharing, local users don’t have automatic access to any data stored on a computer. Local access to files and folders is fully controlled by the security settings on the local disk. If a local disk is formatted with FAT, you can use the read-only, system, or hidden flags to help protect files and folders, but you cannot restrict access. If a local disk is formatted with NTFS or ReFS, you can control access by allowing or denying access to individual users and groups of users.

With public folder sharing, files copied or moved to the Public folder are available to anyone who logs on locally regardless of whether he or she has a standard user account or an administrator user account on the computer. Network access can be granted to the public folder. Doing so, however, makes the public folder and its contents open to everyone who can access the computer over the network.

Windows Server 2012 R2 adds new layers of security through compound identities, claims-based access controls, and central access policies. With both Windows 8.1 and Windows Server 2012 R2, you can assign claims-based access controls to file and folder resources on NTFS and ReFS volumes. With Windows Server 2012 R2, users are granted access to files and folder resources, either directly with access permissions and share permissions or indirectly with claims-based access controls and central access policies.
Unlike with early releases of Windows, where only one sharing model could be used at a time, computers running Windows 8.1 can use both sharing models at the same time. The key advantage to standard sharing is that users can share any folder on a computer and don’t have to move files or folders from their current location. Public folders, on the other hand, are open drop boxes. When users copy files and folders to public folders (and public folder sharing is enabled), the files and folders are available to other users on the computer and on the network.

File Explorer has several options when you are working with folders. Two key options are:

- **Include In Library**  Creates a link between the folder and its contents in the user’s Documents, Music, Pictures, Videos, or another library folder. This lets the user browse and work with the folder’s contents as if it were part of the specified library. However, anytime the user works with a file in a library folder, he is actually working with the file in its original location.

- **Share With**  Shares the folder by using standard folder sharing. In a homegroup, users have the option to share the folder with anyone in the homegroup as read-only or read/write. In a workgroup or domain, users have the option of sharing with specific people. In any configuration, users can also select the sharing option Nobody, which effectively removes sharing.

The default sharing configuration for computers depends on whether the computers are members of homegroups, workgroups, or domains. When you set up a homegroup, you specify the types of files to share, and whether to share printers. Computers that are members of the same homegroup can then automatically share printers and files such as pictures, music, videos, and documents.

Sharing folders within a homegroup as read-only or read/write is fairly straightforward. To enable sharing in a homegroup, you complete the following steps:

1. In File Explorer, press and hold or right-click the folder you want to share.
2. Select Share With, and then select Homegroup (View) or Homegroup (View And Edit).

This simple approach to sharing might make homegroups seem appealing to users in your office. However, it also grants very wide access to users’ data and is generally inadvisable for the workplace. This is why you should encourage users in a homegroup to share with specific people rather than with everyone. Sharing with specific people is the only technique you can use in workgroups and domains.

To enable sharing with specific people, you complete the following steps:

1. In File Explorer, press and hold or right-click the folder.
2. Select Share With, and then select Specific People. This displays the File Sharing Wizard. By default, the System group is specified as the owner of the share, and the currently logged-on user is granted read/write access.
3. In the File Sharing Wizard, use the options provided to choose the people with whom to share. For example, if you want to include all users with local accounts on the computer, enter **Users**, and then tap or click Add. This is different from sharing with everyone because the Everyone group includes anyone with access permission to the computer, not just those who are domain or local users.
4. The default sharing permission is read-only. To set a permission level for a user or group, tap or click the user or group name, and then select Read or Read/Write.

5. Tap or click Share to share the folder, and then tap or click Done.

To remove sharing, you complete the following steps:
1. In File Explorer, press and hold or right-click the folder.
2. Select Share With, and then select Stop Sharing.
3. In the File Sharing Wizard, select Stop Sharing.

By default, when you create the first standard folder share on a computer, Windows creates the File And Printer Sharing exception in Windows Firewall. This inbound exception makes it possible for other computers on the network to send inbound SMB traffic through Windows Firewall to access the share. To accommodate this, Windows opens the following ports:

- UDP port 137, which is used for NetBIOS name resolution
- UDP port 138, which is used for NetBIOS datagram transmission and reception
- TCP port 139, which is used by the NetBIOS Session service
- Dynamic ports for ICMPv4 and ICMPv6, which are used for echo requests, if applicable

In a nutshell, that is how standard folder sharing works. I'll go into more detail about sharing with specific people in Chapter 7. However, before anyone can share anything, network sharing must be enabled.

Network sharing settings are meant to provide the appropriate level of security for each of the various categories of networks to which a computer can connect. For this reason, Windows maintains a separate network profile for each type of network a computer uses. Generally, most network discovery and sharing settings are disabled by default. You can configure network discovery and sharing settings by following these steps:

1. In Control Panel, under Network And Internet, tap or click Choose Homegroup And Sharing Options, and then tap or click the Change Advanced Sharing Settings link.
2. Each available network profile has a separate management panel with configuration settings. Use the expand button to display the profile with which you want to work.
3. Network Discovery, an option for the Private, Guest Or Public, and Domain profiles, affects whether a computer can find other computers and devices on the network and whether other computers on the network can find this computer. Turn Network Discovery on or off by selecting the related option.
4. File And Printer Sharing, an option for the Private, Guest Or Public, and Domain profiles, controls whether a computer can share files and printers. Turn File And Printer Sharing on or off by selecting the related option.
5. In the All Networks profile, Public Folder Sharing controls whether a computer can share files in the Public folders. Turn Public Folder Sharing on or off by selecting an appropriate option.

6. In the All Networks profile, Media Streaming makes it possible for users to share music, videos, and pictures and to access music, videos, and pictures on other computers. Turn Media Streaming on by tapping or clicking the related button, and then configure the Media Streaming options as appropriate. Enabling other users to listen to music, play videos, and view pictures from another computer can adversely affect performance, so you might not want to enable this feature.

7. Windows uses encryption to securely transfer your shared data. By default, the encryption level is set to 128-bit encryption (in most configurations). However, you should be sure that the computers and devices you are sharing with support this level of encryption. Otherwise, select the lower encryption level or upgrade the encryption support on the other devices and computers.

8. In workgroups and homegroups, Password Protected Sharing allows only people with a user account and password on the local computer to access shared resources. Turn Password Protected Sharing on or off by selecting the related option.

9. Tap or click Save Changes to save your settings.

In Group Policy, you can prevent computers from joining homegroups by enabling the Prevent The Computer From Joining A Homegroup policy. This policy is found in the Administrative Templates policies for Computer Configuration under Windows Components\Homegroup.

In Group Policy, you also can restrict the way in which sharing works. The key restrictions on how sharing can be used come from the Prevent Users From Sharing Files Within Their Profile policy. This policy, found in Administrative Templates policies for User Configuration under Windows Components\Network Sharing, controls whether sharing is allowed within folders associated with user profiles, primarily the %SystemDrive%\Users folder. Keep the following in mind when working with the Prevent Users From Sharing Files Within Their Profile setting:

- When this setting is Not Configured, which is the default state, users are allowed to share files within their profile with other users on their network, if a user with administrator privileges on the computer opts in for file sharing. To opt in for file sharing, an administrator has only to share a file within his or her profile.

- When this setting is Enabled, users cannot share files within their profile by using the File Sharing Wizard, and the File Sharing Wizard will not create shares within the %SystemDrive%\Users folder.

- When this setting is Disabled, as might be necessary to override an inherited Enabled setting, users are allowed to share files within their profile with other users on their network, if a user with administrator privileges on the computer opts in for file sharing.
To configure the Prevent Users From Sharing Files Within Their Profile policy in Group Policy, follow these steps:

1. Open a Group Policy Object for editing in the appropriate Group Policy editor. Next, expand Administrative Templates policies for User Configuration under Windows Components\Network Sharing.

2. Double-tap or double-click Prevent Users From Sharing Files Within Their Profile.

3. Select Not Configured, Enabled, or Disabled, and then tap or click OK.

Although it is tempting to use public folder sharing, most organizations—even small businesses—should encourage the use of standard folder sharing for all company files and data. Simply put, standard folder sharing offers more security and better protection. Rather than opening the floodgates to data, standard folder sharing closes them and blocks access appropriately. Increasing security is essential to protecting one of the most valuable assets of any organization—its data.

Share permissions are used only when a user attempts to access a file or folder from a different computer on the network, whereas access permissions are always used whether the user is logged on locally or using a remote system to access the file or folder over the network. When data is accessed remotely, first the share permissions are applied, and then the access permissions are applied.

In many ways, this means that file access permissions and standard folder sharing permissions are like wrappers around your data. File access permissions, the first wrapper, protect your data with regard to local access. If a user logs on to a system locally, file access permissions can allow or deny access to files and folders. File sharing permissions, the second wrapper, are used when you want to enable remote access. If a user accesses data remotely, file sharing permissions allow or deny initial access, but because your data is also wrapped in a file security blanket, the user must successfully pass file access permissions before working with files and folders.

### Controlling access to files and folders with NTFS permissions

NTFS permissions, which apply to both NTFS and ReFS volumes, are always evaluated when a file is accessed. NTFS permissions are fairly complex, and to understand their management, you need to understand the following concepts:

- **Basic permissions**  What the basic permissions are and how they are used
- **Claims-based permissions**  What user and device claims are and how they are used
- **Special permissions**  What the special permissions are and how they are used
- **File ownership**  What is meant by file ownership and how file ownership is used
- **Inheritance**  What is meant by inheritance and how inheritance is used
- **Effective permissions**  How to determine the effective permissions on files
Understanding and using basic permissions

In Windows 8.1, the owner of a file or a folder has the right to allow or deny access to that file or folder, as do members of the Administrators group and other authorized users. By allowing a permission, you grant that permission to a user or a group. By denying a permission, you deny that permission to a user or a group. Keep in mind that entries that deny permissions take precedence over entries that allow permissions. As a result, if a user is a member of two groups, and one group is allowed a permission and the other is denied that permission, the user is denied that permission.

By using File Explorer, you can view the currently assigned basic permissions by pressing and holding or right-clicking a file or a folder, tapping or clicking Properties, and then tapping or clicking the Security tab in the Properties dialog box.

As shown in Figure 6-1, the Group Or User Names list shows the users and groups with permissions set for the selected resource. If you select a user or a group, the assigned permissions are shown in the Permissions For list. If permissions are shaded (unavailable), it means they have been inherited from a parent folder. Inheritance is covered in detail in the “Applying permissions through inheritance” section later in this chapter.

![Figure 6-1](image)

**Figure 6-1** The Security tab shows the currently assigned basic permissions.

Working with and setting basic permissions

All permissions are stored in the file system as part of the access control list (ACL) assigned to a file or a folder. As described in Table 6-1, six basic permissions are used with folders, and five are also used with files. Although some permissions are
inherited based on permissions of a parent folder, all permissions are defined explicitly at some level of the file system hierarchy. Permissions are listed in this table in approximate order of their scope, from Full Control, which grants the most permissions, to Read and Write, which grant specific permissions.

TABLE 6-1 Basic file and folder permissions

<table>
<thead>
<tr>
<th>PERMISSION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>Grants the user or group full control over the selected file or folder and permits reading, writing, changing, and deleting files and subfolders. A user with Full Control permission for a file or folder can change permissions, delete files in the folder regardless of the permission on the files, and also take ownership of a folder or a file. Selecting this permission also selects all the other permissions.</td>
</tr>
<tr>
<td>Modify</td>
<td>Allows the user or group to read, write, change, and delete files. A user with Modify permission can also create files and subfolders, but the user cannot take ownership of files. Selecting this permission selects all the permissions below it.</td>
</tr>
<tr>
<td>Read &amp; Execute</td>
<td>Permits viewing and listing files and subfolders in addition to executing files. If applied to a folder, this permission is inherited by all files and subfolders within the folder. Selecting this permission also selects the List Folder Contents and Read permissions.</td>
</tr>
<tr>
<td>List Folder Contents</td>
<td>Similar to the Read &amp; Execute permission, but available only for folders. Permits viewing and listing files and subfolders, in addition to executing files. Unlike Read &amp; Execute, this permission is inherited by subfolders, but not by files within the folder or subfolders.</td>
</tr>
<tr>
<td>(folders only)</td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td>Allows the user or group to view and list the contents of a folder. A user with this permission can view file attributes, read permissions, and synchronize files. Read is the only permission needed to run scripts. Read access is required to access a shortcut and its target.</td>
</tr>
<tr>
<td>Write</td>
<td>Allows the user or group to create new files and write data to existing files. A user with this permission can also view file attributes, read permissions, and synchronize files. Giving a user permission to write but not delete a file or a folder doesn’t prevent the user from deleting the folder’s or file’s contents.</td>
</tr>
</tbody>
</table>
Equally as important as the basic permissions are the users and groups to which you assign those permissions. If a user or a group whose permissions you want to assign is already selected in the Group Or User Names list on the Security tab, you can modify the assigned permissions by tapping or clicking Edit and then by using the Allow and Deny columns in the Permissions list. Select check boxes in the Allow column to add permissions, or clear check boxes to remove permissions, and then tap or click OK.

To expressly forbid a user or a group from using a permission, select the appropriate check boxes in the Deny column. Because denied permissions have precedence over other permissions, Deny is useful in two specific scenarios:

- If a user is a member of a group that has been granted a permission, but you don’t want the user to have the permission and don’t want to or can’t remove the user from the group, you can override the inherited permission by denying that specific user the right to use the permission.
- If a permission is inherited from a parent folder and you prefer that a user or a group not have the inherited permission, you can override the allowed permission (in most cases) by expressly denying the user or group the use of the permission.

If users or groups whose permissions you want to assign aren’t already available in the Group Or User Names list on the Security tab, you can easily add them. To set basic permissions for users or groups not already listed on a file or a folder’s Security tab, follow these steps:

1. On the Security tab, tap or click Edit. This displays the Permissions For dialog box.

2. In the Permissions For dialog box, tap or click Add to display the Select Users, Computers, Service Accounts, Or Groups dialog box, as shown in Figure 6-2.

![FIGURE 6-2 Use the Select Users, Computers, Service Accounts, Or Groups dialog box to specify users or groups whose permissions you want to configure.](image)

**NOTE** In a workgroup, this dialog box is titled “Select Users Or Groups.” Both dialog boxes serve the same purpose.
### Special identities and best practices for assigning permissions

When you work with basic permissions, it’s important to understand not only how the permissions are used, but how special identities can be used to help you assign permissions. The special identities you’ll encounter the most are Creator Owner and Users, but others are also used occasionally, as described in Table 6-2. Special identities are members of some groups automatically. To configure permissions for a special identity, enter the special identity’s name as you would the name of any other user or group.

<table>
<thead>
<tr>
<th>SPECIAL IDENTITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous Logon</td>
<td>Includes any network logons for which credentials are not provided. This special identity is used to enable anonymous access to resources, such as those available on a web server.</td>
</tr>
<tr>
<td>Authenticated Users</td>
<td>Includes users and computers who log on with a user name and password; does not include users who log on by using the Guest account, even if the account is assigned a password.</td>
</tr>
</tbody>
</table>
## SPECIAL IDENTITY | DESCRIPTION
--- | ---
**Creator Owner** | The special identity for the account that created a file or a folder. Windows 8.1 uses this group to identify the account that has ultimate authority over the file or folder.

**Dialup** | Includes any user who accesses the computer through a dial-up connection. This identity is used to distinguish dial-up users from other types of users.

**Everyone** | Includes all interactive, dial-up, and authenticated users. Although this group includes guests, it does not include anonymous users.

**Interactive** | Includes any user logged on locally or through a remote desktop connection.

**Network** | Includes any user who logs on over the network. This identity is used to allow remote users to access a resource and does not include interactive logons that use remote desktop connections.

**Users** | Includes authenticated users and domain users only. The built-in Users group is preferred over Everyone.

A solid understanding of these special identities can help you more effectively configure permissions on NTFS and ReFS volumes. Additionally, whenever you work with permissions, you should keep the following guidelines in mind:

- **Follow the file system hierarchy**  Inheritance plays a big part in how permissions are set. By default, permissions you set on a folder apply to all files and subfolders within that folder. With this in mind, start at the root folder of a local disk or at a user’s profile folder (both of which act as top-level folders) when you start configuring permissions.

- **Have a plan**  Don’t set permissions without a clear plan. If permissions on folders get out of sync, and you are looking for a way to start over so that you have some continuity, you might want to configure the permissions as they should be in a parent folder and then reset the permissions on all subfolders and files in that folder by using the technique discussed in the “Restoring inherited permissions” section later in this chapter.

- **Grant access only as necessary**  An important aspect of the file access controls built into NTFS is that permissions must be explicitly assigned. If you don’t grant a permission to a user and that user isn’t a member of a group that has a permission, the user doesn’t have that permission—it’s that simple. When assigning permissions, it’s especially important to keep this rule in mind because it’s tempting just to give users full control rather than the specific permissions they really need. Granting only the specific permissions users need to do their job is known as the *principle of least privilege*. 
Use groups to manage permissions more efficiently Whenever possible, you should make users members of appropriate groups, and then assign permissions to those groups rather than to individual users. In this way, you can grant permissions to new users by making them members of the appropriate groups. Then, when a user leaves or goes to another group, you can change the group membership as appropriate. For example, when Sarah joins the sales team, you can add her to the SalesUS and SalesCan groups so that she can access those groups’ shared data. If she later leaves the sales team and joins the marketing team, you can remove her from the SalesUS and SalesCan groups and add her to the MarketingUS and MarketingCan groups. This is much more efficient than editing the properties for every folder Sarah needs access to and assigning permissions.

Use central access policies to enhance existing access controls On your domain servers running Windows Server 2012 R2, use central access policies to very precisely define the specific attributes that users and devices must have to access resources.

Assigning special permissions
Windows 8.1 uses special permissions to carefully control the permissions of users and groups. Behind the scenes, whenever you work with basic permissions, Windows 8.1 manages a set of related special permissions that exactly specify the permitted actions. The special permissions that are applied for each of the basic permissions are as follows:

- Read
  - List Folder/Read Data
  - Read Attributes
  - Read Extended Attributes
  - Read Permissions
- Read & Execute or List Folder Contents
  - All special permissions for Read
  - Traverse Folder/Execute File
- Write
  - Create Files/Write Data
  - Create Folders/Append Data
  - Write Attributes
  - Write Extended Attributes
- Modify
  - All special permissions for Read
  - All special permissions for Write
  - Delete
- **Full Control**
  - All special permissions listed previously
  - Change Permissions
  - Delete Subfolders And Files
  - Take Ownership

Table 6-3 describes how Windows 8.1 uses each special permission.

<table>
<thead>
<tr>
<th>SPECIAL PERMISSION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Permissions</td>
<td>Allows you to change basic and special permissions assigned to a file or a folder.</td>
</tr>
<tr>
<td>Create Files/Write Data</td>
<td>Create Files allows you to put new files in a folder. Write Data allows you to overwrite existing data in a file (but not add new data to an existing file, which is covered by Append Data).</td>
</tr>
<tr>
<td>Create Folders/Append Data</td>
<td>Create Folders allows you to create subfolders within folders. Append Data allows you to add data to the end of an existing file (but not to overwrite existing data, which is covered by Write Data).</td>
</tr>
<tr>
<td>Delete</td>
<td>Allows you to delete a file or a folder. If a folder isn’t empty and you don’t have Delete permission for one or more of its files or subfolders, you won’t be able to delete it unless you have the Delete Subfolders And Files permission.</td>
</tr>
<tr>
<td>Delete Subfolders And Files</td>
<td>Allows you to delete the contents of a folder. If you have this permission, you can delete the subfolders and files in a folder even if you don’t specifically have Delete permission on the subfolder or the file.</td>
</tr>
<tr>
<td>List Folder/Read Data</td>
<td>List Folder lets you view file and folder names. Read Data allows you to view the contents of a file.</td>
</tr>
<tr>
<td>Read Attributes</td>
<td>Allows you to read the basic attributes of a file or a folder. These attributes include Read-Only, Hidden, System, and Archive.</td>
</tr>
<tr>
<td>Read Extended Attributes</td>
<td>Allows you to view the extended attributes (named data streams) associated with a file.</td>
</tr>
<tr>
<td>Read Permissions</td>
<td>Allows you to read all basic and special permissions assigned to a file or a folder.</td>
</tr>
<tr>
<td>Take Ownership</td>
<td>Allows you to take ownership of a file or a folder. By default, administrators can always take ownership of a file or a folder and can also grant this permission to others.</td>
</tr>
</tbody>
</table>
**SPECIAL PERMISSION** | **DESCRIPTION**
---|---
Traverse Folder/Execute File | Traverse Folder allows direct access to a folder in order to reach subfolders, even if you don’t have explicit access to read the data that the folder contains. Execute File allows you to run an executable file.

Write Attributes | Allows you to change the basic attributes of a file or a folder. These attributes include Read-Only, Hidden, System, and Archive.

Write Extended Attributes | Allows you to change the extended attributes (named data streams) associated with a file.

In File Explorer, you can view special permissions for a file or folder by pressing and holding or right-clicking the file or folder with which you want to work, and then tapping or clicking Properties. In the Properties dialog box, select the Security tab, and then tap or click Advanced to display the Advanced Security Settings dialog box, shown in Figure 6-3. In this dialog box, the permissions are presented much as they are on the Security tab. The key differences are that you view individual allow or deny permission sets, whether and from where permissions are inherited, and the resources to which the permissions apply.

**FIGURE 6-3** Use the Advanced Security Settings dialog box to configure special permissions.
MORE INFO  In Figure 6-3, note that the folder shows the GUID for the owner rather than a user name. With Windows 8.1, this typically is an indicator that the folder or file was created originally by a user running a different operating system on the computer, such as on a computer that is being dual booted.

After you open the Advanced Security Settings dialog box, you can set special permissions for a security principal by completing the following steps:

1. If the user or group already has directly assigned permissions for the file or folder, you can view or modify special permissions by tapping or clicking Edit and then skipping steps 2–5.

2. Tap or click Add to display the Permission Entry For dialog box. Tap or click Select A Principal to display the Select User, Computer, Service Account, Or Group dialog box.

3. Enter the name of a user or a group account. Be sure to reference the user account name rather than the user's full name. Only one name can be entered at a time.

4. Tap or click Check Names. If a single match is found for each entry, the dialog box is automatically updated, and the entry is underlined. Otherwise, you'll get an additional dialog box. If no matches are found, you've either entered the name incorrectly or you're working with an incorrect location. Modify the name in the Name Not Found dialog box and try again, or tap or click Locations to select a new location. When multiple matches are found, in the Multiple Names Found dialog box, select the name you want to use, and then tap or click OK.

5. Tap or click OK. The user and group is added as the Principal and the Permission Entry For dialog box is updated to show this.

6. Only basic permissions are listed by default. Tap or click Show Advanced Permissions to display the special permissions, as shown in Figure 6-4.

![FIGURE 6-4 Configure the special permissions that should be allowed or denied.](image-url)
7. Use the Type list to specify whether you are configuring allowed or denied special permissions, and then select the special permissions that you want to allow or deny. If any permissions are dimmed (unavailable), they are inherited from a parent folder.

**NOTE** You allow and deny special permissions separately. Therefore, if you want to both allow and deny special permissions, you’ll need to configure the allowed permissions and then repeat this procedure starting with step 1 to configure the denied permissions.

8. If the options in the Applies To list are available, choose the appropriate option to ensure that the permissions are properly inherited. The options include the following:

- **This Folder Only** The permissions apply only to the currently selected folder.
- **This Folder, Subfolders And Files** The permissions apply to this folder, any subfolders of this folder, and any files in any of these folders.
- **This Folder And Subfolders** The permissions apply to this folder and any subfolders of this folder. They do not apply to any files in any of these folders.
- **This Folder And Files** The permissions apply to this folder and any files in this folder. They do not apply to any subfolders of this folder.
- **Subfolders And Files Only** The permissions apply to any subfolders of this folder and any files in any of these folders. They do not apply to this folder itself.
- **Subfolders Only** The permissions apply to any subfolders of this folder but not to the folder itself or any files in any of these folders.
- **Files Only** The permissions apply to any files in this folder and any files in subfolders of this folder. They do not apply to this folder itself or to subfolders.

9. When you have finished configuring permissions, tap or click OK.

### Assigning claims-based permissions

Claims-based access controls use compound identities to control access to resources. When resources are remotely accessed, claims-based access controls and central access policies rely on Kerberos with armoring for authentication of computer device claims. Kerberos with armoring improves domain security by allowing domain-joined clients and domain controllers to communicate over secure, encrypted channels.

The most basic approach for creating a claim is to define conditions that limit access based on groups to which a user or device can or can’t be a member. More advanced approaches use access rules, claims types, and resources properties to carefully define specific criteria that must be met before access is granted.
Put another way, claims define the specific attributes that users and devices must have to access a file or folder. For example, with basic claims based on group membership, you can specify that:

- A user or device can be a member of a group listed in a claim. For example, the device can be a member of the Engineering Computers group.
- A user or device must be a member of each of the groups listed in a claim. For example, the device must be a member of the Engineering Computers and Restricted Access groups.
- A user or device cannot be a member of a group listed in a claim. For example, the device cannot be a member of the Temp Computers group.
- A user or device must not be a member of each group listed in a claim. For example, the device cannot be a member of the Temp Computer or Contract Computers group.

**MORE INFO** With central access policies, you define central access rules in Active Directory Domain Services (AD DS) and those rules are applied dynamically throughout the enterprise. Central access rules use conditional expressions that require you to determine the resource properties, claim types, and/or security groups required for the policy, in addition to the servers where the policy should be applied.

Before you can define and apply claim conditions to a computer’s files and folders, claims-based policy must be enabled. For non–domain-joined computers, you can do this by enabling and configuring the KDC Support For Claims, Compound Authentication And Kerberos Armoring policy in the Administrative Templates policies for Computer Configuration under System\KDC. The policy must be configured to use a specific mode. The available modes are:

- **Supported** Domain controllers support claims, compound identities, and Kerberos armoring. Client computers that don’t support Kerberos with armoring can be authenticated.
- **Always Provide Claims** Same as Supported, but domain controllers always return claims for accounts.
- **Fail Unarmored Authentication Requests** Kerberos with armoring is mandatory. Client computers that don’t support Kerberos with armoring cannot be authenticated.

For application throughout a domain, claims-based policy should be enabled for all domain controllers in a domain to ensure consistent application. Because of this, you typically enable and configure this policy through the Default Domain Controllers Group Policy Object, or the highest Group Policy Object linked to the domain controllers organizational unit (OU).
REAL WORLD  You might have heard that you cannot or should not edit the Default Domain Controllers Group policy Object. The truth is that this object should only be used to configure a very specific subset of policy.

In Group Policy Management, you’ll find the Default Domain Controllers Group policy Object in the Group policy Objects container. By default, the Default Domain Controllers policy GpO has the highest precedence among GpOs linked to the Domain Controllers OU and this is why the GpO has precedence. As a best practice, you should edit the Default Domain policy GpO only to manage password policy, account lockout policy, and Kerberos policy.

To manage other areas of policy, you should create a new GpO and link it to the domain or an appropriate OU within the domain. That said, several policy settings located under Computer Configuration\Policies\Windows Settings\Security Settings\Local policies\Security Options are exceptions to the rule, including:

- Accounts: Rename Administrator Account
- Accounts: Administrator Account Status
- Accounts: Guest Account Status
- Accounts: Rename Guest Account
- Network Security: Force Logoff When Logon hours expire
- Network Security: Do Not Store LAN Manager hash Value On Next password Change
- Network Access: Allow Anonymous SID/Name Translation

Kerberos Client Support For Claims, Compound Authentication And Kerberos Armoring policy controls whether the Kerberos client running on Windows 8.1 and Windows Server 2012 R2 requests claims and compound authentication. The policy must be enabled for compatible Kerberos clients to request claims and compound authentication for Dynamic Access Control and Kerberos armoring. You’ll find this policy in the Administrative Templates policies for Computer Configuration under System\Kerberos.

After you’ve enabled and configured claims-based policy, you can define claim conditions by completing these steps:

1. In File Explorer, press and hold or right-click the file or folder with which you want to work, and then tap or click Properties. In the Properties dialog box, select the Security tab, and then tap or click Advanced to display the Advanced Security Settings dialog box, shown earlier in Figure 6-3.
2. If the user or group already has directly assigned permissions for the file or folder, you can edit their existing permissions. Here, tap or click the user with which you want to work, tap or click Edit, and then skip steps 3–6.
3. Tap or click Add to display the Permission Entry For dialog box. Tap or click Select A Principal to display the Select User, Computer, Service Account, Or Group dialog box.
4. Enter the name of a user or a group account. Be sure to reference the user account name rather than the user’s full name. Only one name can be entered at a time.
5. Tap or click Check Names. If a single match is found for each entry, the dialog box is automatically updated, and the entry is underlined. Otherwise, you'll get an additional dialog box. If no matches are found, you've either entered the name incorrectly or you're working with an incorrect location. Modify the name in the Name Not Found dialog box and try again, or tap or click Locations to select a new location. When multiple matches are found, in the Multiple Names Found dialog box, select the name you want to use, and then tap or click OK.

6. Tap or click OK. The user and group are added as the Principal. Tap or click Add A Condition.

7. Use the options provided to define the condition or conditions that must be met to grant access. With users and groups, set basic claims based on group membership, previously defined claim types, or both. With resource properties, define conditions for property values.

8. When you have finished configuring conditions, tap or click OK.

File ownership and permission assignment

The owner of a file or a folder has the right to allow or deny access to that resource. Although members of the Administrators group and other authorized users also have the right to allow or deny access, the owner has the authority to lock out non-administrator users, and then the only way to regain access to the resource is for an administrator or a member of the Restore Operators group to take ownership of it. This makes the file or folder owner important with respect to what permissions are allowed or denied for a given resource.

The default owner of a file or folder is the person who creates the resource. Ownership can be taken or transferred in several different ways. The current owner of a file or folder can transfer ownership to another user or group. A member of the Administrators group can take ownership of a file or folder or transfer ownership to another user or group—even if administrators are locked out of the resource according to the permissions. Any user with the Take Ownership permission on the file or folder can take ownership, as can any member of the Backup Operators group (or anyone else with the Restore Files And Directories user right, for that matter).

To assign ownership of a file or a folder, complete these steps:

1. In File Explorer, open the file or folder’s Properties dialog box by pressing and holding or right-clicking the file or folder and then tapping or clicking Properties.

2. On the Security tab, tap or click Advanced to display the Advanced Security Settings dialog box where the current owner is listed under the file or folder name.

3. Tap or click Change. Use the options in the Select User, Computer, Service Account, Or Group dialog box to select the new owner. If you’re taking ownership of a folder, you can take ownership of all subfolders and files within the folder by selecting the Replace Owner On Subcontainers And Objects option (see Figure 6-5).
4. Tap or click OK twice when you have finished.

Applying permissions through inheritance

In the file and folder hierarchy used by Windows 8.1, the root folder of a local disk and the %UserProfile% folder are the parent folders of all the files and folders they contain by default. Anytime you add a resource, it inherits the permissions of the local disk’s root folder or the user’s profile folder. You can change this behavior by modifying a folder’s inheritance settings so that it no longer inherits permissions from its parent folder. This step creates a new parent folder, and any subfolders or files you add will then inherit the permissions of this folder.

Inheritance essentials

Inheritance is automatic, and inherited permissions are assigned when a file or folder is created. If you do not want a file or folder to have the same permissions as a parent, you have several choices:

- Stop inheriting permissions from the parent folder, and then either convert inherited permissions to explicit permissions or remove all inherited permissions.
- Access the parent folder, and then configure the permissions for the files and folders it contains.
- Try to override an inherited permission by selecting the opposite permission. In most cases, Deny overrides Allow.
Inherited permissions are shaded (unavailable) on the Security tab of a file or folder’s Properties dialog box. Also, when you assign new permissions to a folder, the permissions propagate to the subfolders and files contained in that folder and either supplement or replace existing permissions. This propagation lets you grant additional users and groups access to a folder’s resources or to further restrict access to a folder’s resources independently of a parent folder.

To better understand inheritance, consider the following examples:

- On drive C, you create a folder named Data, and then create a subfolder named CurrentProjects. By default, Data inherits the permissions of the C:\ folder, and these permissions are in turn inherited by the CurrentProjects folder. Any files you add to the C:\, C:\Data, and C:\Data\CurrentProjects folders have the same permissions—those set for or inherited from the C:\ folder.

- On drive C, you create a folder named Docs, and then create a subfolder named Working. You disable inheritance on the Working folder, and then remove the inherited permissions of the parent, C\. Any files you add to the C:\Docs\Working folder inherit the permissions of the C:\Docs folder and no other.

- On drive C, you create a folder named Backup, and then create a subfolder named Sales. You add permissions to the Sales folder that grant access to members of the Sales group. Any files added to the C:\Backup\Sales folder inherit the permissions of the C:\ folder and also have additional access permissions for members of the Sales group.

**REAL WORLD** Many new administrators wonder what the advantage of inheritance is and why it is used. Although inheritance occasionally seems like more trouble than it’s worth, inheritance enables you to very efficiently manage permissions. Without inheritance, you’d have to configure permissions on every file and folder you create. If you wanted to change permissions later, you’d have to go through all your files and folders again. With inheritance, all new files and folders automatically inherit a set of permissions. If you need to change permissions, you can make the changes in a top-level or parent folder, and the changes can be automatically applied to all subfolders and files in that folder. In this way, a single permission set can be applied to many files and folders without editing the security of individual files and folders.

**Viewing inherited permissions**

To view the inherited permissions on a file or folder, press and hold or right-click the file or folder in File Explorer, and then tap or click Properties. On the Security tab of the Properties dialog box, tap or click Advanced to display the Advanced Security Settings dialog box, shown earlier in Figure 6-3. The Access column lists the current permissions assigned to the resource. If the permission is inherited, the Inherited From column shows the parent folder. If the permission is inherited by other resources, the Applies To column shows the types of resources that inherit the permission.
Optimizing file security

Stopping inheritance

When you disable inheritance in a file or folder’s security settings, the file or folder stops inheriting permissions from parent folders. You can then elect to either convert inherited permissions to explicit permissions on the file or folder, which would make the permissions editable, or remove all inherited permissions from the file or folder.

If you want a file or folder to stop inheriting permissions from a parent folder, follow these steps:

1. In File Explorer, press and hold or right-click the file or folder, and then tap or click Properties. On the Security tab, tap or click Advanced. This opens the Advanced Security Settings dialog box with the Permissions tab selected by default.
2. On the Permissions tab, you’ll find a Disable Inheritance button if inheritance currently is enabled. Tap or click Disable Inheritance.
3. As shown in Figure 6-6, you can now either convert the inherited permissions to explicit permissions or remove all inherited permissions and apply only the permissions that you explicitly set on the folder or file.

**FIGURE 6-6** Copy or remove the inherited permissions.

**TIP** If you remove the inherited permissions and no other permissions are assigned, everyone but the owner of the resource is denied access. This effectively locks out everyone except the owner of a folder or file. However, administrators still have the right to take ownership of the resource regardless of the permissions. Thus, if an administrator is locked out of a file or a folder and truly needs access, she can take ownership and then have unrestricted access.

Restoring inherited permissions

Over time, the permissions on files and subfolders can become so dramatically different from those of a parent folder that it is nearly impossible to effectively manage access. To make managing file and folder access easier, you might want to take the drastic step of removing all existing permissions on all resources contained in a parent folder and replacing them with permissions inherited from that parent folder. In this way, permissions set on the folder you are working with (the parent folder)
To replace existing permissions with the inherited permissions of a parent folder, follow these steps:

1. In File Explorer, press and hold or right-click the folder, and then tap or click Properties. On the Security tab, tap or click Advanced.
2. On the Permissions tab, select Replace All Child Object Permission Entries With Inheritable Permission Entries From This Object, and then tap or click OK.
3. As shown in Figure 6-7, you receive a prompt explaining that this action will replace all explicitly defined permissions and enable propagation of inheritable permissions. Tap or click Yes.

However, you don’t have to completely replace existing permissions to start inheriting permissions from a parent folder. If a file or folder was configured to stop inheriting permissions from a parent folder, you can re-enable inheritance to have the file or folder include the inherited permissions from a parent folder. To do this, follow these steps:

1. In File Explorer, press and hold or right-click the file or folder that should include inherited permissions, and then tap or click Properties. On the Security tab, tap or click Advanced.
2. On the Permissions tab, tap or click Enable Inheritance, and then tap or click OK. Note that the Enable Inheritance button is available only if permission inheritance currently is disabled.

**Determining the effective permissions and troubleshooting**

NTFS permissions are complex and can be difficult to manage. Sometimes a change—even a very minor one—can have unintended consequences. Users might suddenly find that they are denied access to files they could previously access or that they have access to files to which access should never have been granted. In either scenario, something has gone wrong with permissions. You have a problem, and you need to fix it.

You should start troubleshooting these or other problems with permissions by determining the effective permissions for the files or folders in question. As the name implies, the effective permissions tell you exactly which permissions are in
effect with regard to a particular user or group. The effective permissions are important because they enable you to quickly determine the cumulative set of permissions that apply.

For a user, the effective permissions are based on all the permissions the user has been granted or denied, no matter whether the permissions are applied explicitly or obtained from groups of which the user is a member. For example, if JimB is a member of the Users, Sales, Marketing, SpecTeam, and Managers groups, the effective permissions on a file or a folder are the cumulative set of permissions that JimB has been explicitly assigned and the permissions assigned to the Users, Sales, Marketing, SpecTeam, and Managers groups. If JimB is a member of a group that is specifically denied a permission, JimB will also be denied that permission, even if another group is allowed that permission. This occurs because deny entries have precedence over allow entries.

The same is true for user and device claims. If you’ve configured a claims-based policy and added a user claim, that user claim can prevent access. Similarly, if there’s a device claim, that device claim can prevent access.

To determine the effective permissions for a user or a group with regard to a file or folder, complete the following steps:

1. In File Explorer, press and hold or right-click the file or folder with which you want to work, and then tap or click Properties. In the Properties dialog box, tap or click the Security tab, and then tap or click Advanced.

2. In the Advanced Security Settings dialog box, tap or click the Effective Access tab. Use the options provided to determine the effective permissions for users, groups, and devices. Keep the following in mind:
   - If you only want to determine access for a particular user or user group, tap or click Select A User, enter the name of the user or group, and then tap or click OK.
   - If you only want to determine access for a particular device or device group, tap or click Select A Device, enter the name of the device or the device group, and then tap or click OK.
   - If you want to determine access for a particular user or user group on a particular device or in a device group, specify both a user/user group and a device/device group.

3. Tap or click View Effective Access. The effective permissions for the specified user or group are displayed by using the complete set of special permissions. If a user has full control over the selected resource, he or she will have all the permissions, as shown in Figure 6-8. Otherwise, a subset of the permissions is selected, and you have to carefully consider whether the user or group has the appropriate permissions. Use Table 6-3, earlier in the chapter, to help you interpret the permissions.
FIGURE 6-8 Any checked permissions have been granted to the specified user or group.

NOTE  You must have appropriate permissions to view the effective permissions of any user or group. It’s also important to remember that you cannot determine the effective permissions for implicit groups or special identities, such as Authenticated Users or everyone. Furthermore, the effective permissions do not take into account those permissions granted to a user because he or she is the Creator Owner.
Symbols and Numbers

\$ (dollar sign), hidden shares and, 224
128-bit encryption, 191
512b drives, 85, 96
512e drives, 85
802.11 specifications, 338–341

A

Ability To Change Properties Of An All User Remote Access Connection policy, 177
access controls, claims-based, 202–205
access permissions, 192
access points
  connecting to, 344
defined, 337
wireless technologies and, 338, 339
access types, 275
Access-Denied Assistance policies, 227
ACPI (Advanced Configuration and Power Interface)
defined, 4
power states and, 12–15
UEFI and, 7
active boot partition, 19
Active Directory
  BitLocker recovery extensions, 65
  searching, 274
  TPM recovery extensions, 65
Active Directory–based Group Policy, 159, 163–165
active partitions, 99, 101–103
ad hoc mode, 342
adapters. See network adapters
adaptive query timeout, 279
Address Resolution Protocol (ARP), 7
Address Resolution Protocol Service Binding Protocol (ARPSBP), 7
ADM files, 166
ADMS$ share, 225
administrative shares, 224–226
administrative templates
  Access Denied Errors, 227
  adding and removing, 167
  Audit Object Access policy, 231
disk quota policies, 168–170
  File Explorer, 245, 246
hiding drives, 247
KDC, 203
logon policies, 184–186
network policies, 177, 178
Offline File policies, 171–175
process, 165–167
Remote Assistance policies, 178–180
script policies, 180–183
sharing, 191
slow-link mode, 222
startup policies, 184–186
System Restore policies, 170
Work Folders policies, 176, 177
Administrators and Non-Administrators local Group Policy, 161
ADMX files, 166
Advanced Boot Options menu, 22
Advanced Configuration and Power Interface (ACPI). See ACPI (Advanced Configuration and Power Interface)
Advanced Encryption Standard (AES) encryption, 59, 341
advanced sharing
  vs. basic sharing, 215
  process, 216, 217
AdvancedOptions option, 36
AES encryption, 59, 341
Airplane Mode, 303
allocating storage, 124–127
Allow Only Per User Or Approved Shell Extensions policy, 245
Allow Or Disallow Use Of The Offline Files Feature policy, 171
Allow Users To Select When A Password Is Required When Resuming policy, 184
alternate IP addressing, 283, 284
alternate phone numbers, 328
alternate private IP addresses, 281, 305, 306
Always Offline mode, 222
Always Use Classic Logon policy, 184
Always Wait For The Network At Computer Startup And Logon policy, 184
analog phone lines, 315
Anonymous Logon special identity, 196
APIPA (Automatic Private IP Addressing), 296, 305
Apply Policy To Removable Media policy, 168
ARM processor architecture, 2
ARP (Address Resolution Protocol), 7
ARPSBP (Address Resolution Protocol Service Binding Protocol), 7
assigning
claims-based permissions, 202–205
computer startup and shutdown
scripts, 182
ownership of a file or folder, 205
special permissions, 198–202
user logon and logoff scripts, 183
Audit Object Access policy, 231
auditing
file and folder access, 235–239
Work Folders, 231
Authenticated Users special identity, 196
authentication. See BitLocker Drive
Encryption
automated
defragmentation, 155, 156
maintenance, 151, 155
automatic
black hole router detection, 277
connections, 321
dead gateway retry, 277
disconnection, 326
proxy configuration, 323
Automatic connection type, 330
Automatic Private IP Addressing (APIPA),
296, 305
AutoPlay, 135

B
background processes
disk maintenance tools, 145
Windows SuperFetch and, 93
background sync, 171, 174, 175, 222
Backup Operators group, 205
(badmemory) identifier, 30
BadMemoryAccess option, 35
BadMemoryList option, 35
basic
drives, 106
partitions, 118
permissions, 193–198
sharing, 215
volumes, 82, 111, 112
basic disks
changing to dynamic, 82, 103, 104
defined, 82, 95
vs. dynamic disks, 96, 121
basic input/output system (BIOS), 2
batch scripts, 180
battery status, 302
BaudRate option, 35
BCD Editor (Bcdedit.exe)
commands, 26, 27
creating, copying and deleting BCD
defined, 27
entries, 32ndefault operating system, 40
defined, 27
importing and exporting BCD store,
31, 32
mirrored system volumes and, 157
nonsystem store, creating, 31
operating system display order, 39, 40
startup process and, 8
system BCD store and, 28
BCD store
commands, 26, 27
copying entries, 32
creating entries, 32
creating new, 26
defined, 3deleting entries, 32
GUIDs, 29
importing and exporting, 31, 32
multiple instances of Windows, 30
properties, of entries, 29
risk of modifying, 27
sample entries, 28
setting entry values, 33
viewing entries, 28–31
well-known identifiers, 29, 30
Windows Boot Loader, 25, 28, 31
Windows Boot Manager, 25, 28, 31
binding keys, TPM Services and, 44
BIOS-based firmware, validation profile
settings, 60
BitLocker Drive Encryption, 15
vs. BitLocker To Go, 56
boot file integrity and, 56, 57
changes since first release, 58, 59
checking status, 78–80
configuring, 68–70
defined, 43
deploying, 62–66
disabling, 80
disk compression and, 137
file encryption and, 137
installing, 67
managing, 78–80
options, 79
partitioning requirements, 63
passwords, 58
process, 56
recovering data protected by, 79
TPM modes, 57
TPM Services and, 44, 45
troubleshooting, 78–80
USB flash drives, 72–74
versions, 68
BitLocker To Go
defined, 43
vs. BitLocker Drive Encryption, 56
boot applications, 3
Boot Configuration Data (BCD) store.
See BCD store
boot environment, 3, 27
boot file integrity, 56, 57
Boot Integrity Services (BIS), 7
boot loader
BCD store and, 28, 31
sequence of startup events, 15
startup problems and, 19, 20
boot manager
BCD store and, 25, 28, 31
default, 3
sealing with TPM, 45
sequence of startup events, 15
startup problems and, 17, 19
timeout value, 27
tools menu, 27
boot partition or volume, 100
boot priority order
changing temporarily, 41
setting, 11
startup problems and, 18, 19
boot services
defined, 3
startup process and, 15
UEFI, 6
boot settings, 14, 15, 18, 19
/ bootdebug command, 26
BootDebug option, 35
bootems command, 26
BootEMS option, 35
{bootloadersettings} identifier, 30
BootLog option, 36
Bootmgfw.efi, 8, 20
{bootmgr} identifier, 30
Bootsector, 26, 32
/bootsequence command, 26, 41
BootStatusPolicy option, 36
branch caching, 266–269
breaking a mirrored set, 120
brightness, mobile devices and, 303
broadband
connections, 317, 318, 334, 335
defined, 301
protocols, 330
browsing computers in a domain, 295
burning
default options, 137
discs, Burn A Disc Wizard and, 133
discs with live file systems, 136, 137
ISO to disc, 134
mastered discs, 135, 136
C
C$ share, 225
caching
See also branch caching
offline files, 250–252
persistent, 279
policies for offline files, 172
redirected folders, 249
calling cards, 314
CD File System (CDFS), 134
central access policies, 188, 198, 202, 203
certificates
encryption, 44, 59, 140
network unlock, 62
public key, 140, 141
recovery, 69, 143
smart card, 57, 58
Change Permissions special permission, 199
Channel option, 35
Check Disk (Chkdsk.exe)
vs. legacy scan and repair, 152
options and switches, list of, 152, 153
repairing disk errors and inconsistencies, 151
running from the command line, 152
vs. self-healing NTFS, 150
syntax, 152
chipsets, 1
Cipher utility, 59
claims-based access controls, 188
claims-based permissions, 202–205
cleanmgr, 145
clearing the TPM, 53, 54
Client For Microsoft Networks, 311, 331
cluster size, 96–98, 108
ClusterModeAddressing option, 36
Compact.exe, 140
compound authentication, 204
compound TCP, 277
compressed
directories and files, 138, 139, 140
drives, 138, 139
files, color coding, 243
Computer Browser service, 295
Computer Management
automated defragmentation, 155
Check Disk, 153
disk quotas, 260–266
offline files, 250
Computer Management (continued)
opening, 85, 87
optimizing drives, 154
shared folders, making unavailable for offline use, 258
shared resources, 215, 217–219
special shares, 224, 225
volume labels, 115
computer policies
administrative templates, 166, 167
defined, 160
GPMC and, 165
logon and startup, 184–186
network, 177, 178
offline files, 171–175
remote assistance, 178–180
computer shutdown scripts, 180–183
computer startup scripts, 180–182
ConfigAccessPolicy option, 35
ConfigFlags option, 36
configuration scripts, 323
Configure Background Sync policy, 171, 175
Configure Slow-Link Mode policy, 171, 174
conflicts in offline file synchronization, 256
connections
automatic, 321, 322
broadband, 317–319
dial-up, 311–317
establishing, 332–337
logon information, 325
manual, 321
protocols by type, list of, 330
VPN, 318–320
wireless, 337–345
Control Panel, opening, 85
ControlSet subkey, 20
converting
basic disks to dynamic disks, 82, 98, 103, 104
volumes to NTFS, 116, 117
/copy command, 26
corruptions, detecting, 151
costed networks, 171
crash dump partitions, 100
/create command, 26
Create Files/Write Data special permission, 199
Create Folders/Append Data special permission, 199
/createstore command, 26
Creator Owner special identity, 197
credentials
connecting to a network share with, 223, 224
file sharing issues and, 226
Csrss.exe, 16, 21
{(current)} identifier, 30
D
D$ share, 225
data discs, 133–137
Data Execution Prevention (DEP), 38, 39
data Incomplete volume status, 148
data management policies, 168–177
data Not Redundant volume status, 148
data recovery, encryption and, 141
data transfer
offloading to storage devices, 249
rates, 131, 132
data volumes, decrypting, 80
data-recovery agents, 59
date, setting through firmware interface, 10
/dbgsettings command, 26
{dbgsettings} identifier, 30
DbgTransport option, 36
dead gateways, 277
/debug command, 26
debugging
boot applications, 26
booting, 34
kernel, 26
options, 35, 36
decrypting
data volumes, 80
files and directories, 144
USB flash drives, 80
/default command, 26, 40
default dialing location, 311, 312
Default Domain Controllers Policy GPO, 204
default gateways, 283, 284, 285
{default} identifier, 30
defragmenting disks, 154–156
/delete command, 27
Delete special permission, 199
Delete Subfolders And Files special permission, 199
/deletevalue command, 27
deleting
partitions, volumes, and logical drives, 115
scripts, 183
storage pools, 129
storage spaces, 128
denying permissions, 193, 195, 205, 214, 215
DEP, 38, 39
device drivers, startup process and, 15
Device Registration Service (DRS), 320
DHCP
dual TCP/IP stack and, 278
dynamic IP addresses and, 304
leases, 297, 298
mobile devices and, 301, 302
releasing and renewing settings, 297, 298
resolver cache and, 299
DHCPv4, 7, 281, 293
DHCPv6, 7
DHCPv6-capable DHCP client, 278
diagnostic startup, 23, 25
dialing locations, 313, 314
dialing rules, 311–313, 315, 327
dial-up connections
automatic disconnection, 326
creating, 311–317
establishing, 332–334
Group Policy and, 317
networking, 301, 308
networking protocols, 330
troubleshooting, 333, 334
Dialup special identity, 197
DirectAccess
defined, 301
mobile networking and, 308, 309, 310
network policies, 177
protocols, 330
directories and files
compressing, 138
encrypting, 141, 142
expanding compressed, 139
disabling
BitLocker Drive Encryption, 80
disk quotas, 265, 266
inherited permissions, 208
network connections, 290
network discovery, 272
offline files, 258
run-once lists, 185, 186
Windows Firewall, 332
disc burning
ISO images, 134, 135
live file systems, discs with, 137
mastered discs, 135, 136
process, 133
disconnecting
from a network, 290, 291, 345
network drives, 86, 222
open files, 226
user sessions, 225
discovery. See network discovery
Disk Cleanup tool, 145
disk compression, 137–140
Disk Defragmenter, as background
process, 93
disk drives. See drives
disk errors
checking for, 151–153
repairing, 150, 151
Disk Management
breaking a mirrored set, 120
converting basic disks to dynamic, 103
defined, 87–89
defragmenting disks, 154–156
deleting partitions, volumes, and logical
drives, 115
drive letters and paths, 113
extending volumes, 111, 112
formatting partitions and volumes, 113
logical drives, creating, 106–109
mirrored volumes, 119, 120
moving dynamic disks to another
system, 121
partitioning disks, 106–109
reactivating volumes, 156
removable disks, 132
removing a mirrored set, 120
repairing mirrored system volumes, 157, 158
rescanning disks, 157
rescanning missing drives, 118
shrinking volumes, 111, 112
simple volumes, creating, 106–109
status, 146, 147
switching table styles, 101
disk quotas
creating entries, 262, 263
deleting entries, 263, 264
disabling, 265, 266
enabling on NTFS volumes, 260–262
exporting and importing settings,
264, 265
policies, 168–170
process described, 259, 260
updating and customizing entries, 263
viewing entries, 262
disk space usage
Disk Cleanup tool and, 145
disk quotas and, 259–266
for offline files, 172, 257
DiskPart
defined, 89, 90
extending volumes, 111
setting active partition, 102
shrinking volumes, 111
switching table styles, 101
Diskpart.efi, 8
disks
- checking for errors, 151–153
- defragmenting, 154–156
- initializing, 100, 101
- installing, 100, 101
- logical structure, 98
- mirroring, 19, 96, 119, 120, 156, 157, 158
- optimizing, 154, 155
- performance, 90–95
- spanned, 95, 96
- statuses, list of, 146, 147
- striping, 96
- striping with parity, 124
- tools, 84
- types, 82

dismounting volumes for repair, 152
display
- mobile device settings, 303
- startup problems and, 21
Display Confirmation Dialog When Deleting Files policy, 245
Display Instructions In Logoff Scripts As They Run policy, 181
Display Instructions In Logon Scripts As They Run policy, 181
Display Instructions In Shutdown Scripts As They Run policy, 180
Display Instructions In Startup Scripts As They Run policy, 180
display order of boot managers, 39, 40
/displayorder command, 27
distributed branch caching, 268
distributed cache mode, 267
DNS
- adaptive query timeout, 279
- flushing, 298, 299
- parallel queries, 279
- persistent cache, 279
- query coalescing, 279
- resolution, 286, 287, 288
- resolver cache, 298, 299
DNS64, 310
dollar sign ($), hidden shares and, 224
domain controllers
- claims-based permissions and, 203
- default policy, 204
- Network Unlock servers, 62
domain networks, 272
domains
- administrative templates and, 166, 167
- GPMC and, 164
Do Not Enumerate Connected Users On Domain-Joined Computers policy, 184
Do Not Process The Legacy Run List policy, 185
dynamic disks
- vs. basic disks, 96
- changing to basic, 82, 104
- defined, 82, 96
- extending volumes, 111
- laptops and, 98
- moving to another system, 121, 122
- volume types, 99
Dynamic Host Configuration Protocol (DHCP). See DHCP
dynamic IP addresses
- configuring, 281, 283, 284, 304, 305
- troubleshooting, 296
dynamic volumes, 82

E
E$ share, 225
editing permissions, 195
EEPROM (Electronically Erasable Programmable Read-Only Memory), 17
effective permissions, 209–211
EFI
- boot manager, 20
- booting into the operating system and, 8
- creating BCD store, 31
- device drivers, UEFI and, 7
- system store device, 27
EFS (Encrypting File System)
- encrypting and decrypting automatically, 140
purpose, 44  
Work Folders, 230  
EIST, 14  
ejecting removable storage, 86  
Electronically Erasable Programmable Read-Only Memory (EEPROM), 17  
email invitations for Remote Assistance, 179  
EMS  
  enabling and disabling, 26  
  settings, 34  
/ems command, 27  
  Ems option, 37  
  EMSBaudRate option, 35  
  EMSPort option, 35  
/emssettings command, 27  
  (emssettings) identifier, 30  
Enable Disk Quotas policy, 168  
Enable File Screens policy, 171, 173  
Enable File Synchronization On Costed Networks policy, 171, 175  
Enable Transparent Caching policy, 172  
enabling  
BitLocker, on nonsystem volumes, 70, 71  
BitLocker, on system volumes, 74–77  
BitLocker, on USB flash drives, 72–74  
branch caching, 268  
disk quotas, on NTFS volumes, 260–262  
network connections, 290, 291  
network discovery, 272, 274, 296  
network sharing, 190, 191  
offline files, 258  
TPM, 48, 49  
Windows Firewall, 332  
Windows ReadyBoost, 91  
Encrypt The Offline Files Cache policy, 172  
encrypted files, color coding, 243  
enveloping  
  drives and data, 140–144  
  offline files, 172, 258  
  Work Folders, 230  
Encrypting File System (EFS). See EFS  
  (Encrypting File System)  
encryption  
  See also BitLocker Drive Encryption;  
  BitLocker To Go  
BitLocker Drive Encryption vs. BitLocker  
  To Go, 56  
certificates, 59  
data recovery and, 141  
directories and files, 141–144  
vs. disk compression, 137  
full volumes vs. used space only, 60  
hardware-based, 59, 84  
keys, 140, 230  
levels, 191  
nonsystem volumes, 70, 71  
roaming profiles, 140  
SMB, 214  
software-based, 59  
  storing keys for protected data volumes, 66  
  system volumes, 74–77  
  USB flash drives, 72–74  
  VPN and, 309  
wireless, 340  
end-of-file (EOF) markers, 98  
enforcing disk quotas, 168, 259  
Enhanced Intel SpeedStep Technology (EIST), 14  
enterprise encryption keys, 230  
/enum command, 27  
Enumerate Local Users On Domain-Joined Computers policy, 184  
environment variables, 220, 223  
esSATA, removable storage and, 131  
ESE databases, 267  
  event logging, disk quotas and, 261  
environment messages from Group Policy, 160  
Everyone special identity, 197  
exceptions, Windows Firewall, 190  
exFAT file system, 84, 97, 105  
Expand.exe, 140  
expanding  
  compressed directories and files, 139, 140  
  compressed drives, 139  
  explicit permissions, 208  
/export command, 27  
exporting  
  BCD store, 31, 32  
  disk quota settings, 264, 265  
extended FAT, 84. See exFAT file system  
  extended partitions, 82, 83, 96  
  extended selective acknowledgments, 277  
  extending volumes, 111, 112  
Extensible Firmware Interface (EFI). See EFI  
Extensible Storage Engine (ESE) data- 
  bases, 267  
external displays for mobile devices, 303  
F  
Failed drive status, 118  
Failed Redundancy drive status, 118  
Failed Redundancy volume status, 148, 149, 156  
Failed volume status, 148  
failed volumes, recovering, 118  
FAT volumes  
  encrypting, 58  
  file security options, 187
FAT12 file system, 97
FAT16 file system, 83, 97, 105
FAT32 file system, 83, 97, 105

fault tolerance
   Data Not Redundant volume status and, 148
   failed redundancy and, 148
   RAID levels and, 96, 110

Federal Information Processing Standard (FIPS) compliance, 66

File And Printer Sharing
default component configuration, 331
turning on and off, 190, 213
Windows Firewall exceptions, 190

file encryption. See encryption
File Explorer, configuring options, 241–248
file name extensions, 242, 243
file ownership, 205
file screens, 173
file security. See permissions
file sharing
   vs. file security, 187
   homegroups and, 189
   models, 188, 189
   offline availability, 249–252
   permissions, 192
   removing, 190
   restrictions, 191, 192
   with specific people, 189

file systems
disc options, 133
FAT types, 97
primary partitions and, 83
types, 84

Files Not Cached policy, 172
Filter Manager, 95

firewalls. See Windows Firewall
FireWire, removable storage and, 131, 132

firmware
   defined, 1
digital signatures, 61
initializing TPM and, 50
TCG compliant, 43
validating platform configuration registers, 60

Firmware Boot Manager, 26

firmware interfaces
   examining, 10–12
   power states and, 12–15
   startup process and, 8, 15
types, 2
   working with, 9
FirstMegaBytePolicy option, 35

fixed data drives, policies for, 64, 70

Flash drives. See USB flash drives
flushing DNS, 298, 299

folder sharing
   offline availability, 249–252
   process, 189, 190
   public vs. standard, 192, 213
   folders, inheritance and, 206–211
   Foreign disk status, 146

formatting
   data discs, 134
   partitions, 112
   volumes, 108, 112

Formatting volume status, 148
forward lookups, 298

FSUtil
   bytes per physical sector, 85
defined, 89, 90
Full Control permissions, 194

fwbootmgr, 26
{fwbootmgr} identifier, 30

G

gateways. See default gateways
get-help smbshare command, 215
Get-WindowsOptionalFeature cmdlet, 62
ghost entries, offline files and, 248
{globalsettings} identifier, 30
gpedit.msc, 162

gPMC (Group Policy Management Console), 163, 164, 166

GPME (Group Policy Management Editor)
   accessing, 162
   administrative templates, 166, 167
   nodes described, 165

GPOs (Group Policy objects)
   editing, 164
   local, 161
   resolving conflicts, 161

GPT (GUID partition table), 4, 6, 82–84, 101
gpupdate.exe, 160
GraphicsModeDisabled option, 35
GraphicsResolution option, 35

Group Policy
   administrative templates, 165–167
   auditing policies, 235
   BitLocker, 64, 66, 68
   branch caching, 268
   claims-based permissions, 203
   computer and user scripts, 180–183
   computer startup and shutdown scripts, 181–183
   Default Domain Controllers GPO, 204
defined, 159
dial-up connections, 311
disabling run lists, 185, 186
disk quota policies, 168–170
drive maps, 223, 224
File Explorer policies, 244–246
hiding drives, 247
local, 160–163
local vs. Active Directory–based, 159, 162
logon and logoff scripts, 181–183
network policies, 177
Offline File policies, 171–175
recovery agents, 143
Remote Assistance, 178–180
restricting file sharing, 191, 192
shared folders, 219–221
startup applications, 185
System Restore policies, 170
TPM Services, 64
VPN connections, 311, 319
Work Folders, 176, 177
Group Policy Management Editor (GPME)
accessing, 162
administrative templates, 166, 167
nodes described, 165
Group Policy Modeling Wizard, 164
Group Policy Object Editor
accessing, 162
creating and accessing local GPOs, 163
Group Policy Results Wizard, 164
GUID partition table (GPT), 4, 5, 82–84, 101

H
Hal option, 37
HalBreakPoint option, 37
Hal.dll, 15, 20
hard disks, sealing with TPM, 45
hardware abstraction layer (HAL)
loading, 15
startup problems and, 17, 20
hardware encryption, 59, 84. See also encryption
hardware failure, 17
Healthy (At Risk) volume status, 149
Healthy status, 148, 156, 157
Healthy (Unknown Partition) volume status, 149
Hiberfil.sys file, 33
Hibernate power state, 13
hidden items, viewing, 241, 242, 243
hidden shares, creating, 224
Hide These Specified Drives In My Computer policy, 245
Hides The Manage Item On The File Explorer Context Menu policy, 245
hiding drives, 247
HKEY_LOCAL_MACHINE
administrative templates, 166
run lists and, 185
shell extensions, 245
startup process, 20
startup process and, 15
HKEY_USER
administrative templates, 166
run lists and, 185
HomeGroup Troubleshooter, 273
homegroups
password protected sharing, 191
preventing computers from joining, 191
sharing folders, 189
host ID, IPv4 addresses and, 276
host name resolution, 286–288
hosted cache mode, 267–269
Human Interface Infrastructure support, 6
Hypervisor settings, 27, 34
HypervisorLaunchType option, 37
{hypervisorsettings} identifier, 30

I
Ia64ldr.efi, 8
identifier entries, 32
identity validation, 328, 329
IEEE 802.11 specification, 338
IEEE 1394, 132
IIS hostable web core, 229
IKEv2 connection protocol, 330
/import command, 27
importing
BCD store, 31, 32
disk quota settings, 264, 265
Include In Library option, 189
IncreaseUserVA option, 37
infrastructure mode, 342
inherited permissions
defined, 206, 207
disabling, 208
restoring, 208, 209
sync shares and, 233
viewing, 207
initial startup, troubleshooting, 17, 18, 19
initializing
disks, 100, 101, 147
TPM (Trusted Platform Module) Services, 50–52
Initializing volume status, 149
installing
BitLocker Drive Encryption, 67
network adapters, 279
new physical disks, 100, 101
installing (continued)
TCP/IP, 280
wireless adapters, 341
integrity checks, 75
Intel Multiple Monitor, 10
Intel Quick Resume Technology Driver (QRTD), 14
Intel SpeedStep, 10
Intel Turbo Boost, 10
Intel Virtualization, 10
Interactive special identity, 197
Internet connections, resolving problems with, 294
Internet Group Management Protocol version 3 (IGMPv3), 278
Internet Key Exchange (IKE), 278
Internet small computer system interface (iSCSI), 7
I/O errors, 146, 147
IP addresses
alternate private, 305, 306
configuration information, viewing, 292
dynamic, 281, 283, 284, 304, 305
resolving using DNS, 286–288
resolving using WINS, 288–290
static, 281–283
troubleshooting, 296
IP security, 278
IPSec share, 225
Ipconfig command, 293, 298, 299
IPsec, L2TP and, 309
IPv4
alternate IP addressing, 284, 305
connection status, 291
defined, 276
dynamic IP addresses, 284, 304
installing, 280
name resolution enhancements, 279
static addresses, configuring, 282, 283
TCP/IP and, 276
viewing address, 292
WINS and, 288–290
IPv6
connection status, 291
defined, 276
DirectAccess and, 310
dual TCP/IP stack features, 278
dynamic IP addresses, 284, 304
installing, 280
name resolution enhancements, 279
static addresses, configuring, 282, 283
TCP/IP and, 276
IPv6 over IPsec connection protocol, 330
IPv6 over Point-to-Point Protocol (PPPv6), 278
ISO images
burning to disc, 133, 134
mounting, 134
ISPs, creating dial-up connections to, 314, 315
J
joining devices to workplaces, 320
K
Kerberos with Armoring, 202, 203, 204
kernel
debugging, 26
loading, 15
Session Manager and, 16
startup problems and, 17, 20
Kernel option, 37
Kernel Transaction Manager (KTM), 150
keys
See also recovery keys
binding, 44
encryption, 66, 140, 230
network, 342
sealing, 44
L
L2TP IPsec VPN connection protocol, 330
last known good configuration, 21, 37
latency, as branch caching trigger, 269
Layer 2 Tunneling Protocol (L2TP), 309
leases, DHCP, 297, 298
legacy run lists, disabling, 185
Limit Disk Space Used By Offline Files policy, 172
link-local multicast name resolution (LLMNR), 278, 279
List Folder Contents (folders only) permissions, 194
List Folder Contents permission, 248
List Folder/Read Data special permission, 199
LMHOSTS, 288, 289, 290
local disk shares, 225
local Group Policy
accessing and using, 160–163
defined, 159
local Group Policy objects (GPOs), 161
Local Security Authority
startup problems and, 21
startup process and, 16
Locale option, 35
Location Where All Default Library Definition Files For Users/Machines Reside policy, 245
lock screens, Work Folders and, 230, 234
Lockout, TPM, 48
Log Event When Quota Limit Is Exceeded policy, 168
Log Event When Quota Warning Is Level Is Exceeded policy, 168
Logical drives
- creating, 106–109
- deleting, 115
Logoff scripts, 180–183
Logon information, 325
Logon policies, 184–186
Logon scripts, 180–183
Lsass.exe, 16, 21

M
Manage The TPM Security Hardware wizard, 45
Managed Network Protocol (MNP), 7
Managed Network Service Binding Protocol (MNSBP), 7
Manual Internet connections, 321
Mapping network drives, 85
- Group Policy and, 223, 224
- shared folders and, 213
- shared resources, 221–223
Master boot code, 83
Master boot record (MBR)
- vs. GUID partition table (GPT), 82, 83
- partitions, 4, 5
- startup problems and, 19
- switching to GPT, 101
- Unknown volume status and, 149
Master file table (MFT), 105, 117
Mastering discs, 133–136
MaxProc option, 37
MBR. See master boot record (MBR)
Measured boot, 61
Media access control (MAC) address, 292
Media state, 291
Media streaming, 191
(Memdiag) identifier, 30
Memory
- buffer, 277
- paging, 15
- protecting with DEP, 38
- specifying maximum usable amount, 24
- SuperFetch and, 94
Memtest.exe, 33
Metered connections, 345
MFT (master file table), 105, 117
/mirror command, 27
Mirrored sets
- resynchronizing and repairing, 149, 156, 157
- storage spaces and, 123
Mirrored system volumes, 157, 158
Mirroring disks, 19, 96, 119, 120
Missing drive status, 118
Missing status, 146, 156
Mobile devices
- Airplane Mode, 303
- battery status, 302
- DirectAccess and, 308
- display settings, 303
- network components, 330
- network projectors, 307
- presentation mode, 303
- Sync Center and, 303
- VPN and, 308
- Windows Mobility Center and, 302, 303
Modeling Group Policy, 164
Modem pools, 308
Modems, establishing a dial-up connection, 332
Modified fast recovery algorithm, 277
Modify permissions, 194
Motherboard-chipsets
- platform firmware and, 1
- power states and, 12
Mounting
- ISO images, 134
- volumes, 107
Msconfig.exe, 23
Msi option, 37
Ms-TPM-OwnerInformation, 65
Multiboot menu, 27
Multicast listener discovery version 2 (MLDv2), 278
Multiprocessor configurations, 24

N
Name resolution
- DNS, 286–288, 298, 299
- WINS, 288–290
NAT64, 310
Neighbor unreachability detection for IPv4, 277
Net share command, 215, 224
NetBIOS name resolution, 288, 289, 290
Network adapters
- configuration information, viewing, 292
- installing, 279
- network connections and, 281
- network address translators, 278
Network and Sharing Center
- accessing, 275
- broadband connections, 318
- configuration information, viewing, 292
- default gateways, 285
Network and Sharing Center (continued)
defined, 271, 275
diagnosing connection problems, 294
dial-up connections, 316
DNS, configuring, 286
dynamic IP addresses, 304
VPN connections, 318
wireless connections, 344
network categories, 272, 273
network connections
disabling, 290
enabling, 290, 291
network adapters and, 281
Network and Sharing Center and, 275
renaming, 293
resolving problems, 293
status, 291
troubleshooting, 277
Network Diagnostics, 271, 277
network discovery
configuring, 190
defined, 272
enabling, 274, 296
Network Explorer and, 274
Work Folders and, 176
Network Explorer
accessing, 273
defined, 271
network discovery and, 274
network ID, 276
network interface, 276
network interface cards (NICs), 279
network latency, as branch caching trigger, 269
Network Location Awareness, 160
network masks, 297
network policies, 177, 178
network projectors, 307
network sharing
See also sharing files and folders
enabling, 190, 191
permissions, 214
Network special identity, 197
network unlock, 57, 62, 63, 76
networking
components, 330–332
mobile devices, configuring for, 301–307
protocols, 329, 330
No Media disk status, 147
/nocleanup command, 33
NoCrashAutoReboot option, 37
no-execute (NX) policy, 31, 37, 38, 39
NoLowMem option, 37
non-metered connections, 345
nonsystem BCD store, 31
nonsystem volumes, enabling BitLocker on, 70, 71
nonvolatile memory, 17
Not Initialized disk status, 147
Noumex option, 36
NoVESA option, 36
NTFS
See also permissions
converting volumes to, 116, 117
defined, 105
extending volumes and, 111
file security options, 187
permissions, 106, 192
ReFS and, 187
self-healing, 150
transactional, 150
versions, 106
volumes, encrypting, 58
(ntldr) identifier, 30
Ntoskrnl.exe, 15, 20
NumProc option, 37
Nvrboot.efi, 8–12
nx option, 37, 38, 39

O
octets, 276
Off (disabled) state, 272
Off power state, 13
Offline disk status, 146
Offline drive status, 118
offline files
disk usage limits, 257
encryption, 258
making unavailable, 258
policies, 171–175
settings, 218
synchronizing, 222, 252–256
Offline status, 156
On (enabled) state, 272
On power state, 13
OneCPU option, 37
Online disk status, 146
Online (Errors) status
disks, 146
drives, 118
mirrored sets, 157
operating system
default BCD entry, 40
display order, 39, 40
drive policies, 64, 65
loaders, 3, 5, 17, 26
startup process and, 15
operational log, 160
optimizing drives, 154
OptionsEdit option, 37
OSDevice option, 37
Osloader, 26, 32, 36–38
OUs
See also Group Policy
administrative templates and, 166, 167
GPMC and, 164
owner authorization, TPM, 46, 47
ownership of a file or folder, assigning, 205

P
PAE option, 37, 39
page file partition or volume, 100
parallel queries, 279
parallelism, 24
parity volumes, storage spaces and, 124
partitioning, 4, 5
partitions
active, 101, 102
creating, 106–109
defined, 82
deleting, 115
Healthy (Unknown Partition) volume status and, 149
MBR vs. GUID, 82
switching table styles, 84, 101
volume labels, 114
password protected sharing, 191
passwords
BitLocker Drive Encryption, 58
firmware interface, 11
nonsystem volumes, 70
recovery, 69
TPM, 46, 47, 49, 50–52, 55
USB flash drives, 72, 74
Work Folders and, 230, 234
PC cards, 341
PCI cards, 341
PCRs (Platform Configuration Registers), 60
PerfMem option, 37
performance
disk space usage and, 145
Windows ReadyBoost and, 90, 91
Peripheral Component Interconnect (PCI), 7
permissions
advanced sharing, 216
assigning, 196–198
basic, 193–198
basic sharing, 216
claims-based, 202–205
default, for sharing, 190
denying, 193
effective, 209–211
encrypted files and, 141, 142
file ownership and, 205
inheritance and, 206–211
network shares, 214, 215, 218, 219, 226
NTFS, 106, 187
offline files, 252
public folder sharing, 228
share vs. access, 192
special, 198–203
sync shares, 233
persistent caching, 279
phone numbers
alternate, 327
primary, 327
Physical Address Extension (PAE) option, 38, 39
Ping command, 282, 295
Platform Configuration Registers (PCRs), 60
platform firmware, 1
Point-to-Point Tunneling Protocol (L2TP), 309
policies
See also computer policies; user policies
BitLocker Drive Encryption, 64
computer and user scripts, 180–183
configuring, 165–167
disabling, 167
disk quota, 168–170
enabling, 167
fixed drive, 64
logon, 184–186
network, 177, 178
offline files, 171–175
operating system drive, 64
order of application, 160
recovery, 143
Remote Assistance, 178–180
removable data drives, 65, 72
startup, 184–186
System Restore, 170
TPM Services, 64
Work Folders, 176, 177
policy preferences, 159
policy settings
defined, 159
Work Folders, 176
power plans for mobile devices, 302
power settings, 13, 14, 15
power states, 12–15
power-on self-test (POST), 15, 17
PowerShell scripts. See Windows PowerShell scripts
PPP, 330
PPPoE, 330
PPPV6, 278
PPTP VPN connection protocol, 330
Preboot Execution Environment (PXE), 7
precedence of policies, 160
preconfiguring wireless network connections, 344
prefetch data, 95
pre-operating system environment, 45
presentation mode, 303
Prevent Access To Drives From My Computer policy, 245
primary partitions
basic disks and, 96
defined, 82
marking as active, 102
MBR partitioning style, 83
principle of least privilege, 197
PRINT$ share, 225
private network IPv4 addresses, 281, 282
private networks
changing from public, 273
defined, 272
ProactiveScan task, 151
processes, Windows SuperFetch and, 93
processors, specifying number of, 24
Prohibit Deletion Of Remote Access Connections policy, 177
Prohibit Installation And Configuration Of Network Bridge On Your DNS Domain Network policy, 177
projectors, connecting to, 307
propagating permissions, 207
protective MBR, 5
protocols, 330. See also IPv4; IPv6
proxy server settings, mobile connections and, 322–325
public folder sharing
configuring, 228, 229
defined, 188
permissions, 228
process, 227
vs. standard folder sharing, 192
turning on or off, 191
public folders, 188, 189
public networks
changing to private, 273
defined, 272
Q
QR TD, 14
query coalescing, 279
quotas. See disk quotas
R
RAID 0, 109, 110
RAID 5, 109, 110, 118
RAID controller cards, 19
RAID levels, 96
{ramdiskoptions} identifier, 30
random interface IDs, 278
reactivating
disks, 146, 149
volumes, 148, 156, 157
Read & Execute permissions, 194
Read Attributes special permission, 199
Read Extended Attributes special permission, 199
Read permissions, 194
Read Permissions special permission, 199
read-only, sharing folders and, 189
read-write, sharing folders and, 189
ReadyBoost, 90–93
ReadyDrive, 93
receive window auto tuning, 277
recovering data protected by BitLocker Drive Encryption, 79
recovery agents, 141
recovery keys
FIPS compliance and, 66
nonsystem volumes, 70, 71
recovering data using, 79
system volumes, 75, 76
USB flash drives, 72, 74
Windows Live SkyDrive and, 67
Recovery mode, 56, 57, 66, 79
recovery options, 22
recovery policy, 143
RecoveryEnabled option, 36
RecoverySequence option, 36
Recycle Bin, File Explorer policies and, 245
redirected folders, 229, 249
redundancy, storage spaces and, 130
ReFS (Resilient File System)
data integrity and, 151
defined, 84
file security options, 187
NTFS and, 187
Regenerating status, 157
regenerating striped with parity volumes, 119
registry hive, loading, 15, 20
releasing DHCP settings, 297
remote access
DirectAccess and, 309, 310
file sharing permissions, 192
Remote Assistance policies, 178–180
Remote Server Administration Tools (RSAT), 164
removable data drive policies, 65, 72
removable storage devices, 86, 131–133
Remove CD Burning Features policy, 245
Remove DFS Tab policy, 245
Remove File Explorer’s Default Context Menu policy, 246
Remove File Menu From File Explorer policy, 246
Remove Hardware Tab policy, 246
Remove “Make Available Offline” Command policy, 172, 173
Remove “Map Network Drive” And “Disconnect Network Drive” policy, 245
Remove Security Tab policy, 246
Remove “Work Offline” Command policy, 172, 173
RemoveMemory option, 37
removing administrative templates, 167
sharing, 190
renaming network connections, 293
renewing DHCP settings, 297
repairing disk errors, 150, 151
mirrored sets, 156, 157
mirrored system volumes, 157, 158
Require Domain Users To Elevate When Setting A Network’s Location policy, 177
reregistering DNS, 299
rescanning disks, 119, 147, 149, 157
missing drives, 118
resiliency recovering, 129
type, 125
Resilient File System (ReFS), 84, 151, 187
resolving computer names to IPv4 addresses, 288
host names using DNS, 286–288
IP addressing problems, 296
synchronization conflicts, 256
resources, creating shared, 215–219
Restore Operators group, 205
restoring inherited permissions, 208, 209
system, configuring policies for, 170
RestrictAPICCluster option, 38
restricting drive access, 247
file sharing, 191, 192
Resume BCD entry, 32
Resume From Hibernate entry, 33
{resumeloadersettings} identifier, 30
ResumeObject option, 38
Resynching volume status, 149
resynchronizing mirrored sets, 156, 157
retransmissions, 277, 278
reverse lookups, 298
roaming profiles, 140
Robust Security Network (RSN), 341
Route All Traffic Through The Internal Networks policy, 177
Routing And Remote Access Service (RRAS), 308, 309
routing compartments, 277
RSN (Robust Security Network), 341
Run Legacy Logon Scripts Hidden policy, 181
Run Logon Scripts Synchronously policy, 181
Run Startup Scripts Asynchronously policy, 181
Run These Programs At User Logon policy, 185
Run Windows PowerShell Scripts First At Computer Startup, Shutdown policy, 181
Run Windows PowerShell Scripts First At User Logon, Logoff policy, 181
run-once lists, disabling, 185, 186
run-time services, 3, 6
S
SACK-based loss recovery, 277
Safe Boot modes, 23
SafeBoot option, 38
SafeBootAlternateShell option, 38
scheduling automated maintenance, 151
synchronization of offline files, 253–255
script policies, 180–183
sealing boot manager and boot files, 45
keys, 44
searching Active Directory, 274
secondary display, for mobile devices, 303
secure boot, 60, 61
security
See also BitLocker Drive Encryption; encryption; permissions
802.11i standard, 339
auditing policies, 235–239
disk format options, 187–192
files, options for, 187–192
firmware interfaces and, 11
offline files, 258
remembering passwords, 316
sync shares and, 233
wireless networks, 339–341, 344, 346
Work Folders, 234
security identifiers (SIDs), 260
Security Policy Editor, 66
Select subkey, 20
Selective Acknowledgments (SACKs), 277
self-healing NTFS, 150
Server Manager, creating sync shares in, 231–234
Server Message Block (SMB), 188, 214, 230, 231
Server service, 227
Services Control Manager
startup problems and, 21
startup process and, 16
Services for system management BIOS (SMBIOS), 4
services, startup problems and, 25
Services.exe, 16, 21
Session Manager
startup problems and, 17, 21
startup process and, 16
sessions
burning data discs in, 134
shared folders, 225
/set command, 27
Set-SyncServerSetting cmdlet, 231
setup, startup problems and, 17–19
Share With option, 189
shared resources
accessing, 221–225
creating, 215–219
sharing files and folders
default configuration, 189
defined, 213
models for, 188, 213
offline availability, 249–252
open files, 226
options for, 189
password protection, 191
permissions, 192, 214, 215, 218, 219
public folder sharing, 227–229
stopping, 217
sync shares, 229–235
troubleshooting, 226, 227
user sessions, 225
Work Folders, 229–235
shell extensions, 245
Show First Sign-in Animation policy, 184
shrinking volumes, 111, 112
shrpubw command, 217
shutdown scripts, 180–183
SIDs (security identifiers), 260
Simple Network Protocol (SNP), 7
simple volumes
creating, 106–109
defined, 82
extending, 111, 112
recovering from failures, 118
shrinking, 111, 112
storage spaces and, 123
sites
administrative templates and, 166, 167
GPMC and, 164
sleep power transition, 12
Sleep state, 13
SLIP, 330
slow-link mode, 171, 174, 175, 222, 249
small computer system interface (SCSI), 7
Smart Card Certificate Only mode, 58
smart cards with BitLocker
nonsystem volumes, 70
starting service, 78
USB flash drives, 72
SMB (Server Message Block), 188, 214, 230, 231
SmbShare module, 215
Smss.exe, 16, 21
software-based encryption, 59
Sos option, 38
sound settings for mobile devices, 303
spanned disks, 96
spanned volumes, 82, 109, 110
Data Incomplete volume status and, 148
extending, 111, 112
recovering from failures, 118
shrinking, 111, 112
special
identities, 196–198
permissions, 198–202
shares, 224–226
Specify Administratively Assigned Offline Files policy, 172, 173
Specify Default Quota Limit And Warning Level policy, 168
Specify Maximum Wait Time For Group Policy Scripts policy, 181
SpeedStep, 14
spurious retransmission timeout detection, 278
SRK (storage root key), 44
SSL, Work Folders and, 176
SSTP connection protocol, 330
Stale Data volume status, 149
standard folder sharing
defined, 188
vs. public folder sharing, 192, 213
turning on and off, 213
Start File Explorer With Ribbon Minimized policy, 246
Start subkey, 20
startup
applications, configuring through Group Policy, 185
diagnostic, 23
keys, 57, 58, 69, 76, 77
modes, 3
options, 22
PINs, 69, 77
policies, 184–186
process, 1, 2, 15, 16
scripts, 180–183
troubleshooting, 16–21
Startup And Recovery dialog box, 22
Startup BCD entry, 32
Startup Repair tool, 20
static IP addresses, configuring, 281–283
Static Root of Trust Measurement, 43
status
BitLocker, 78
Computer Browser service, 295
devices, 88
disk quotas, 262
disks, 87, 146, 147
correction, 144
file synchronization, 303
fragmentation, 154
mirrored volumes, 119, 120, 156, 157
mobile device batteries, 302
network connections, 291
networks, 275
recovering volumes and, 118
regenerating striped sets with parity, 118
removable media disks, 99
storage spaces, 130
TPM, 45, 46
times, 148, 149
wireless connections, 342, 343
storage
See also data discs; drives; file systems;
removable storage devices
pools, 122, 124–127, 129
spaces, 122–130
types, 82
storage root key (SRK), 44
/store command, 27
striped volumes, 109, 110, 118
striping disks, 96
striping with parity, 109, 118, 119, 124
strong invitation encryption, 178, 179
SuperFetch, 93–96
suspend mode, 13
symmetric network address translators, 278
Sync Center
disabling offline files, 258
disk usage limits, 257
encrypting offline files, 258
mobile devices and, 303
opening, 249
synchronizing offline files, 252–256
sync partnerships, 252
sync shares, 213, 229–235
synchronizing devices, Work Folders and, 176
synchronizing offline files
background sync, 222
changes only, 248
on costed networks, 249
managing, 252–256
policies, 171, 172
slow-link mode, 174
/sysstore command, 27
system
boot configuration, 23–25
cache, 90
log, 160
partitions, 99
properties, 85
volumes, 74–77, 157, 158
system abstraction layer (SAL), 6
System Configuration utility, 23
System on a Chip (SoC), 2
System Restore policies, 170
SystemRoot option, 38
T
taking ownership of files and folders, 194,
199, 205, 206
TargetName option, 36
Task Scheduler, 154
TCP extended statistics, 278
TCP port 139, 190
TCP/IP networking
alternate private IP addresses, 305, 306
default component configuration, 331
default gateways, configuring mul-
tiple, 285
DNS settings, 286–288
dynamic IP addresses, configuring, 304
features, list of, 277
installing, 280
IPv4 and IPv6 and, 276
protocols described, 276
WINS, 288–290
templates. See administrative templates
TestSigning option, 36
This PC console
defined, 85, 86
removable disks, 132
volume labels, 115
three-way mirrors, storage spaces and, 124.
See also mirrored sets
thumbnails, File Explorer and, 242
time, setting through firmware interface, 10
Time to Live (TTL) values, 298, 299
/timeout command, 27, 40
/toolsdisplayorder command, 27
touch-enabled UI, xiii
TPM Security Hardware Wizard, 50
TPM (Trusted Platform Module) Management console
defined, 45
initializing TPM, 52
managing TPM with, 46
TPM (Trusted Platform Module) Services
administrative delegation blob, 47
authentication methods, 68
BitLocker Drive Encryption and, 44, 45
clearing, 53, 54
defined, 43
enabling, 48, 49
initializing, 50–52
keys, 44
lockout, 48
modes, 57, 58
owner authorization, 46, 47, 65
owner passwords, 47, 48, 49, 50–52, 55
process, 44
states, 46
status, 45
turning off, 53
user delegation blob, 47
validation profile settings, 60
Transactional NTFS, 150
transfer rates, 131, 132
transferring ownership of a file, 205
transparent caching, 172
Traverse Folder/Execute File special permission, 200
troubleshooting
BitLocker Drive Encryption, 78–80
broadband connections, 335
dial-up connections, 333, 334
disk problems, 144–149
dynamic IP addresses, 296
Group Policy, 160
IP addresses, 296
network categories, 273
network connections, 275, 277
permissions, 209–211
sharing files and folders, 226, 227
startup, 15–21
storage spaces, 129
TCP/IP, 293–299
VPN connections, 336
wireless connections, 343
wireless networks, 345
TruncateMemory option, 36
trusted boot, 61
Trusted Computing Group (TCG)-compliant firmware, 43
Trusted Platform Module (TPM) Services.
See TPM (Trusted Platform Module) Services
Turn Off App Notifications On the Lock Screen policy, 184
Turn Off Caching Of Thumbnail Pictures policy, 246
Turn Off Configuration policy, 170
Turn Off Picture Password Sign-in policy, 185
Turn Off System Restore policy, 170
Turn Off The Display Of Thumbnails And Only Display Icons On Network Folders policy, 246
Turn Off The Display Of Thumbnails And Only Display Icons policy, 246
Turn Off Windows Libraries Features That Rely On Indexed File Data, 246
Turn On Economical Application Of Administratively Assigned Offline Files policy, 172
Turn On PIN Sign-In policy, 185
turning off
BitLocker Drive Encryption, 80
TPM, 53
two-way mirrors, storage spaces and, 123
U
UDF (Universal Disc Format), 134
UDP port 137, 190
UDP port 138, 190
UEFI (Unified Extensible Firmware Interface), 2, 5–8, 60, 61
UI changes since Windows 7, xiii, xiv
UNC path, 172, 173, 174, 216
unicast IPv4 addresses, 276
unicast IPv6 addresses, 276
uninstalling programs, 85
Universal Disc Format (UDF), 134
Universal Naming Convention (UNC) path.
See UNC path
Unknown volume status, 149
unlocking
nonsystem volumes, 70
operating system drive, 62
from Recovery mode, 79
system volumes, 75, 76, 77
USB flash drives, 72, 73
Unreadable status
disks, 147
drives, 118, 119, 157
Unrecognized disk status, 147
updating firmware interfaces, 9
USB
- removable storage and, 131, 132
- UEFI and, 7
USB Emulation, 11
USB flash drives
  - BitLocker To Go and, 56
  - decrypting, 80
  - encrypting, 72–74
  - Windows ReadyBoost and, 90–93
USB PowerShare, 11
USB Wake Support, 11
UseFirmwarePCISettings option, 38
UsePhysicalDestination option, 38
user interface changes since Windows 7, xiii, xiv
user logoff scripts, 180–183
user logon scripts, 180–183
user policies
  - administrative templates, 166, 167
  - defined, 160
  - GPMC and, 165
  - network, 177, 178
  - offline files, 171–175
user processes, Windows SuperFetch and, 93
Userinit.exe, 16, 21
User-specific local Group Policy, 161
Users special identity, 197

V
/v command, 27
validating platform configuration registers, 60
verbose mode, 27
Vga option, 38
viewing inherited permissions, 207
virtual discs, ISO images and, 134
virtual private network (VPN), 301
volumes
  - basic, 82
  - basic drives and, 106
  - deleting, 115
  - dynamic disks and, 82
  - extending, 111, 112
  - formatting, 108, 112
  - labels, 114, 115
  - mirroring, 119, 120
  - mobile devices, settings for, 303
  - mounting, 107
  - partitions, 112
  - shrinking, 111, 112
  - simple, 106–109
  - spanned, 109, 110
  - statuses, list of, 148, 149
  - striped, 109, 110
  - striped with parity, 109, 110

VPN connections
  - broadband connections and, 308
  - creating, 318–320
  - dial-up connections and, 309
  - establishing, 335
  - mobile networking and, 308
  - protocols, 330
  - troubleshooting, 336

W
wake power transition, 12
well-known identifiers, BCD store and, 30, 32
WEP (Wireless Equivalent Privacy), 340–342
Wi-Fi connections, 342–344
Wi-Fi Protected Access 2 (WPA2), 339–341
Win32 subsystem, 16, 21
Windows Boot Loader
  - BCD store and, 25, 28, 31
  - startup process and, 8, 19, 20
Windows Boot Manager
  - BCD store and, 25, 28, 31
  - as default, 3
  - startup process and, 8, 19, 20
Windows Boot Sector Application, 26
Windows BranchCache, 266–269
Windows executive, 15, 16, 17
Windows Filtering Platform, 278
Windows Firewall
  - connections, enabling and disabling for, 332
  - File and Printer Sharing exception, 190
  - network categories and, 273
  - network discovery and, 272
  - network projectors and, 307
Windows Live SkyDrive, recovery keys and, 67
Windows Logon Manager
  - startup problems and, 21
  - startup process and, 16
Windows Logon user interface, 184
Windows Memory Tester, 33
Windows Mobility Center, 302, 303
Windows Network Diagnostics, 293
Windows On Arm (WOA). See WOA (Windows On Arm)
Windows OS Loader, 34, 36–38
Windows Phone operating system, as Windows On Arm, 2
Windows PowerShell scripts, 180–182
Windows PreInstallation Environment (Windows PE), 62
Windows ReadyBoost, 90–93
Windows ReadyDrive, 93
Windows Recovery Environment (Windows RE), 63
Windows Resume Loader

Windows Resume Loader, 26
Windows RT, as Windows On Arm, 2
Windows scripts, 180. See also batch scripts;
   Windows PowerShell scripts
Windows SuperFetch, 93–96
Winlogon.exe
   startup problems and, 21
   startup process and, 16
WinPE option, 38
Winresume.exe, 33
WINS resolution, configuring, 288–290
Wired Equivalent Privacy (WEP), 340
wireless access points
   defined, 337
   connecting to, 344
   wireless technologies and, 338, 339
wireless base stations. See wireless access points
wireless gateways. See wireless access points
wireless network adapters
   defined, 337
   standards, 338, 339
wireless networks
   access points, 337–339, 344
   adapters, 337, 338, 339, 341
   connecting to, 344, 345
   connections, 342–344
   disconnecting from, 345
   managing, 345
   security, 339–341
   settings, 342
   technologies, list of, 338
   troubleshooting, 345
WOA (Windows On Arm)
   ACPI and, 7
   defined, 2
   startup process, 16
   UEFI and, 8
Work Folders, 176, 177, 229–235
workgroups, password protected sharing
   and, 191
workplaces
   connecting to, 337
   dial-up connections to, 316
   joining devices to, 320
WPA2, 339–341
wrapping keys, TPM Services and, 44
Write Attributes special permission, 200
Write Extended Attributes special permission, 200
Write permissions, 194
About the author

William Stanek (www.williamstanek.com) is the award-winning author and series editor of the bestselling Pocket Consultant series. William is one of the world’s leading technology experts and has more than 20 years of hands-on experience with advanced programming and development. Over the years, his practical advice has helped millions of programmers, developers, and network engineers all over the world. Dubbed “A Face Behind the Future” in 1998 by The Olympian, William has been helping to shape the future of the written word for more than two decades. William’s 150th book was published in 2013, and more than 7.5 million people have read his many works. William’s current books include Windows Server 2012 Inside Out, and the Pocket Consultants for Exchange Server 2013, Windows Server 2012 R2, and Windows 8.1.

William has been involved in the commercial Internet community since 1991. His core business and technology experience comes from more than 11 years of military service. He has substantial experience in developing server technology, encryption, and Internet solutions. He has written many technical white papers and training courses on a wide variety of topics. He frequently serves as a subject matter expert and consultant.

William has an MS with distinction in information systems, and a BS in computer science, magna cum laude. He is proud to have served in the Persian Gulf War as a combat crew member on an electronic warfare aircraft. He flew on numerous combat missions into Iraq and was awarded nine medals for his wartime service, including one of the United States of America’s highest flying honors, the Air Force Distinguished Flying Cross. Currently, he resides in the Pacific Northwest with his wife and children.

William recently rediscovered his love of the great outdoors. When he’s not writing, he can be found hiking, biking, backpacking, traveling, or trekking in search of adventure with his family!